MPLS レイヤ 2 VPN コンフィギュレーション ガイド

初版：2011 年 11 月 08 日

最終更新：2013 年 07 月 30 日

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

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

目 次

第 1 章

最初にお読みください

Cisco IOS XE 16 に関する重要な情報

有効な 2 つのリリースとしての Cisco IOS XE リリース 3.7.0E（Catalyst スイッチ用）および Cisco IOS XE リリース 3.17S（アクセスおよびエッジ ルーティング用）が、1 つのバージョンの統合されたリリース（Cisco IOS XE 16）へと展開（マージ）されています。これにより、スイッチングおよびルーティング ポートフォリオの広範なアクセスおよびエッジ製品が盛り込まれた 1 つのリリースが実現しました。

（注） 技術構成ガイドの機能情報の表に、機能の導入時期を記載しています。他のプラットフォームがその機能をサポートした時期については、記載があるものも、ないものもあります。特定の機能が使用しているプラットフォームでサポートされているかどうかを判断するには、製品のランディング ページに掲載された技術構成ガイドを参照してください。技術的構成ガイドが製品のランディング ページに表示される場合は、その機能がお使いのプラットフォームでサポートされていることを示します。

第 2 章

L2VPN プロトコルベース CLI

L2VPN プロトコルベース CLI 機能は、さまざまな Cisco プラットフォームで Cisco IOS ソフトウェアを開発および配布するための一連のプロセスと強化されたインフラストラクチャを提供します。この機能では、シスコのプラットフォーム全体で一貫した機能性を実現し、オペレーティング システム（OS）間のサポートを提供するために、新しいコマンドが導入され、既存のコマンドが修正または置換されています。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース 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、機能情報の表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シスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

L2VPN プロトコルベース CLI に関する情報

L2VPN プロトコルベース CLI の概要

L2VPN プロトコルベース CLI 機能では新しいコマンドが導入され、シスコのプラットフォーム全体で一貫した機能を実現し、クロス オペレーティング システム（OS）をサポートするため、新しいコマンドが導入され、既存のコマンドが変更または置き換えられました。

（注） 新規導入、更新、置換されたコマンドは、Cisco IOS XE Release 3.7S および Cisco IOS Release 15.3(1) S で利用できます。ただし、置き換えられたレガシー コマンドは今後のリリースで廃止されます。

L2VPN プロトコルベース CLI の利点

L2VPN プロトコルベース CLI 機能には次の利点があります。

- 異なるオペレーティング システムでの一貫したユーザ エクスペリエンス。
- すべてのレイヤ 2 VPN（L2VPN）シナリオに対する一貫した設定。
- 擬似回線を仮想インターフェイスとして設定し、擬似回線を物理ポートとしてモニタすることによって実現する拡張機能。
- 個々の擬似回線での Quality of Service（QoS）サービス ポリシーのような機能設定。
- 強化された高可用性を提供する、プライマリ擬似回線とは独立した擬似回線冗長構成。

これらの利点は、次の拡張機能によって実現されます。

- 新しい L2VPN クロス コネクトおよび L2VPN 仮想転送インターフェイス（VFI、Virtual Forwarding Interface）コンテキストを使用して、新しいサービス コンテキストをポイントツーポイントおよびマルチポイント レイヤ 2 サービスに対して作成することができます。
  - L2VPN クロス コネクト コンテキストは、ポイントツーポイント擬似回線の設定、擬似回線スイッチング、およびローカル スイッチング（ヘア ピニング）に使用されます。イーサネット インターフェイス、イーサネット フロー ポイント（EFP）、ATM インターフェイスと WAN インターフェイス（PPP、HDLC、シリアル）、および擬似回線インターフェイスは、L2VPN クロス コネクト コンテキストのメンバーとして定義することができます。
  - L2VPN VFI コンテキストは、マルチポイント シナリオの仮想プライベート LAN サービス（VPLS）VFI をインスタンス化します。擬似回線は L2VPN VFI コンテキストのメンバーとして定義できます。

- ブリッジドメインはマルチポイントシナリオで使用されます。EFP、擬似回線、または VFI はブリッジドメインのメンバーとして設定できます。擬似回線は VFI のメンバーとして設定できます。VFI は、 のメンバーとして設定できます。

- 新しいポートのコンテキストは、擬似回線インターフェイスを使用して擬似回線に対して（動的にまたは手動で）作成することができます。
- 擬似回線のカスタマイズは、L2VPN コンテキスト メンバーに適用されるインターフェイス テンプレートと擬似回線インターフェイスを使用して実現できます。擬似回線のカスタマイズには次の機能が含まれます。
  - カプセル化のタイプ
  - コントロール ワード
  - 最大伝送単位（MTU）
  - 擬似回線シグナリング タイプ
  - トンネル選択
- インターワーキングおよび冗長グループ サービスの属性は、L2VPN サービスのコンテキストで設定できます。冗長グループはプライマリ擬似回線とは独立して設定することができ、このことはトラフィックを中断せずにバックアップ擬似回線を追加、変更または削除するのに役立ちます。

L2VPN プロトコルベース CLI の変更

次のコマンドは Cisco IOS XE Release 3.7S、Cisco IOS Release 15.3(1)S、および Cisco IOS Release 15.4(1)S で導入されました。

- **debug l2vpn pseudowire**
- **l2vpn**
- **l2vpn pseudowire static-oam class**
- **monitor event-trace l2vpn**
- **show interface pseudowire**
- **show l2vpn service**
- **shutdown (MPLS)**
- **vc**

次のコマンドは Cisco IOS XE Release 3.7S および Cisco IOS Release 15.3(1)S で変更されました。

- **auto-route-target**
- **bridge-domain parameterized vlan**
- **debug condition xconnect fib**

- **debug condition xconnect interface**
- **debug condition xconnect peer**
- **debug condition xconnect segment**
- **description**
- **encapsulation (MPLS)**
- **forward permit l2protocol all**
- **interworking**
- **l2vpn subscriber authorization group**
- **l2vpn xconnect context**
- **load-balance flow**
- **monitor event-trace ac**
- **monitor event-trace atom**
- **monitor event-trace l2tp**
- **monitor peer bfd**
- **mtu**
- **preferred-path**
- **remote circuit id**
- **rd（VPLS）**
- **route-target（VPLS）**
- **sequencing**
- **status**
- **status admin-down disconnect**
- **status control-plane route-watch**
- **status decoupled**
- **status peer topology dual-homed**
- **status protocol notification static**
- **status redundancy**
- **switching tlv**
- **tlv**
- **tlv template**
- **vccv**
- **vccv bfd status signaling**
- **vccv bfd template**

- **vpls-id**
- **vpn id (MPLS)**

次の表に、将来のリリースで置き換えられるレガシー コマンドを示します。Cisco IOS XE Release 3.7S および Cisco IOS Release 15.3(1)S から、将来、レガシーのコマンドが非推奨になるまで、新旧両方のコマンドが共存します。

表 *1*：*Cisco IOS XE Release 3.7S* および *Cisco IOS Release 15.3(1)S* で導入された置換コマンド

レガシー コマンド	**Cisco IOS XE Release 3.7S** および **Cisco IOS Release 15.3(1)S** で導入された置換コマンド
backup delay	**redundancy delay (under l2vpn xconnect context)**
bridge-domain (service instance)	**member (bridge-domain)**
clear mpls l2transport fsm state transition	**clear l2vpn atom fsm state transition**
clear mpls l2transport fsm event	**clear l2vpn atom fsm event**
clear xconnect	**clear l2vpn service**
connect (L2VPN local switching)	**l2vpn xconnect context**
debug acircuit	**debug l2vpn acircuit**
debug mpls l2transport checkpoint	**debug l2vpn atom checkpoint**
debug mpls l2transport event-trace	**debug l2vpn atom event-trace**
debug mpls l2transport fast-failure-detect	**debug l2vpn atom fast-failure-detect**
debug mpls l2transport signaling	**debug l2vpn atom signaling**
debug mpls l2transport static-oam	**debug l2vpn atom static-oam**
debug mpls l2transport vc subscriber	**debug l2vpn atom vc**
debug mpls l2transport vc	**debug l2vpn atom vc**
debug mpls l2transport vc vccv bfd event	**debug l2vpn atom vc vccv**
debug vfi	**debug l2vpn vfi**
debug vfi checkpoint	**debug l2vpn vfi checkpoint**
debug xconnect	**debug l2vpn xconnect**
debug xconnect rib	**debug l2vpn xconnect rib**

レガシー コマンド	Cisco IOS XE Release 3.7S および Cisco IOS Release 15.3(1)S で導入された置換コマンド
description (L2VFI)	**description (L2VPN)**
l2 pseudowire routing	**pseudowire routing**
l2 router-id	**router-id**
l2 vfi	**l2vpn vfi context**
l2 subscriber	**l2vpn subscriber**
l2 vfi autodiscovery	自動検出
l2 vfi point-to-point	**l2vpn xconnect context**
local interface	**pseudowire type**
monitor event-trace st-pw-oam	**monitor event-trace pwoam**
mpls label	**label (pseudowire)**
mpls control-word	**control-word (encapsulation mpls under l2vpn connect context)**
neighbor (l2 vfi)	**member (l2vpn vfi)**
protocol	**signaling protocol**
pseudowire-static-oam class	**l2vpn pseudowire static-oam class**
pseudowire tlv template	**l2vpn pseudowire tlv template**
pw-class keyword in the **xconnect** command	**source template type pseudowire**
remote link failure notification	**l2vpn remote link failure notification**
show mpls l2transport binding	**show l2vpn atom binding**
show mpls l2transport checkpoint	**show l2vpn atom checkpoint**
show mpls l2transport hw-capability	**show l2vpn atom hw-capability**
show mpls l2transport static-oam	**show l2vpn atom static-oam**
show mpls l2transport summary	**show l2vpn atom summary**
show mpls l2transport pwid	**show l2vpn atom pwid**

レガシー コマンド	Cisco IOS XE Release 3.7S および Cisco IOS Release 15.3(1)S で導入された置換コマンド
show mpls l2transport vc	**show l2vpn atom vc**
show xconnect pwmib	**show l2vpn pwmib**
show xconnect rib	**show l2vpn rib**
show xconnect	**show l2vpn service**
show vfi	**show l2vpn vfi**
xconnect	**l2vpn xconnect context** and **member**
xconnect logging pseudowire status global	**logging pseudowire status**
xconnect logging redundancy global	**logging redundancy**
xconnect *peer-ip vc-id*	**neighbor peer-ip vc-id (xconnect context)**

MPLS L2VPN プロトコルベースの CLI：例

このセクションの例では、既存（レガシー）の MPLS L2VPN CLI を置き換える、MPLS L2VPN プロトコルベースの CLI 機能によって導入される新しい設定が提供されます。

代替（または新しい）コマンドを使用した、MPLS L2VPN VPWS 設定

次に、Virtual Private Wire Service（VPWS）- Ethernet over Multiprotocol Label Switching（EoMPLS）の設定例を示します。この例では、L2VPN のメンバーはピア ID または仮想回線（VC）ID を指し示します。この設定は、Quality of Service（QoS）のような機能を擬似回線レベルで適用する必要がある場合を除き、ほとんどの状況で使用されます。

```
l2vpn xconnect context foo
  member GigabitEthernet2/1/1 service-instance 300
  member 10.0.0.1 888 encapsulation mpls
!
interface GigabitEthernet2/1/1
  service instance 300
   encapsulation dot1q 30
   rewrite ingress tag pop 1 symmetric
  !
  service instance 400
   encapsulation dot1q 40
   rewrite ingress tag pop 1 symmetric

l2vpn xconnect context faa
  member GigabitEthernet2/1/1 service-instance 400
  member 10.0.0.1 999 encapsulation mpls
!
```

代替（または新しい）コマンドを使用した、MPLS L2VPN 擬似回線設定

次の例では、L2VPN のメンバーは、擬似回線インターフェイスを指し示します。擬似回線インターフェイスは手動で設定され、ピア ID と VC ID を含みます。この設定は、Quality of Service（QoS）のような機能を擬似回線レベルで適用する必要がある場合を除き、ほとんどの状況で使用されます。

```
l2vpn xconnect context foo
  member GigabitEthernet2/1/1 service-instance 300
  member Pseudowire888
!
interface Pseudowire 888
 encapsulation mpls
 neighbor 10.0.0.1 888
!
interface Pseudowire 999
 encapsulation mpls
 neighbor 10.0.0.1 999
!
interface GigabitEthernet2/1/1
  service instance 300
   encapsulation dot1q 30
   rewrite ingress tag pop 1 symmetric
  !
  service instance 400
   encapsulation dot1q 40
   rewrite ingress tag pop 1 symmetric

l2vpn xconnect context faa
  member GigabitEthernet2/1/1 service-instance 400
  member Pseudowire 999
!
```

代替（または新しい）コマンドを使用した、MPLS L2VPN 擬似回線冗長性設定

次に、擬似回線冗長性の設定例を示します。新しい設定は、サブモードまたは別のグループを持たない簡潔な擬似回線冗長性を示します。この設定により、サービスを中断することなくサービスに冗長メンバーを追加することができます。この設定により、サービスを中断することなく冗長サービス設定を変更または削除することもできます。

```
l2vpn xconnect context sample-pw-redundancy
  member  service-instance 200
  member 1.1.1.1 180 encap mpls group Denver
  member 2.2.2.2 180180 encap mpls group Denver priority 1
  member 3.3.3.3 180181 encap mpls group Denver priority 2
  redundancy delay 1 20 group Denver
!
interface GigabitEthernet2/1/1
  service instance 200
   encapsulation dot1q 100
   rewrite ingress tag pop 1 symmetric
```

代替（または新しい）コマンドを使用した、MPLS L2VPN スタティック擬似回線設定

（注） 次に、カスタマー エッジ（CE）1 と PE 1 および PE 2 と CE 2 がプロバイダー コア（P）ルータを通過する（CE 1—PE 1—P—PE 2—CE 2）ネットワーク スキームでのプロバイダー エッジ（PE）1 ルータの設定を示します。

```
interface g2/1/1
service instance 300 ethernet
encapsulation dot1q 300
no shutdown
!
interface pseudowire 100
neighbor 10.4.4.4 121
```

```
encapsulation mpls
label 200 300
signaling protocol none
no shutdown
!
l2vpn xconnect context foo
  member GigabitEthernet2/1/1 service-instance 300
  member pseudowire 100
```

代替（または新しい）コマンドを使用した、MPLS L2VPN スタティック擬似回線テンプレート設定

（注） 次に、カスタマー エッジ（CE）1 と PE 1 および PE 2 と CE 2 がプロバイダー コア（P）ルータを通過する（CE 1—PE 1—P—PE 2—CE 2）ネットワーク スキームでのプロバイダー エッジ（PE）1 ルータの設定を示します。

```
template type pseudowire test
encapsulation mpls
signaling protocol none
!
interface g2/1/1
service instance 300 ethernet
encapsulation dot1q 300
no shutdown
!
interface pseudowire 100
neighbor 10.4.4.4 121
source template type pseudowire test
label 200 300
no shutdown
!
l2vpn xconnect context foo
  member GigabitEthernet2/1/1 service-instance 300
  member pseudowire 100
```

代替（または新しい）コマンドを使用した、MPLS L2VPN 動的擬似回線テンプレート設定

（注） 次に、カスタマー エッジ（CE）1 と PE 1 および PE 2 と CE 2 がプロバイダー コア（P）ルータを通過する（CE 1—PE 1—P—PE 2—CE 2）ネットワーク スキームでのプロバイダー エッジ（PE）1 ルータの設定を示します。

```
template type pseudowire test
encapsulation mpls
signaling protocol ldp
!
!
interface g2/1/1
service instance 300 ethernet
encapsulation dot1q 300
no shutdown
!
interface pseudowire 100
neighbor 10.4.4.4 121
source template type pseudowire test
no shutdown
!
l2vpn xconnect context foo
  member GigabitEthernet2/1/1 service-instance 300
  member pseudowire 100
```

代替（または新しい）コマンドを使用した、MPLS L2VPN マルチセグメント静的/動的擬似回線テンプレート設定

次の PE ルータ設定は、マルチセグメント静的/動的擬似回線用です。

```
l2vpn pseudowire tlv template TLV
 tlv mtu 1 4 dec 1500
!
interface pseudowire401
  source template type pseudowire staticTempl
encapsulation mpls
neighbor 10.4.4.4 101
signaling protocol none
label 4401 4301
pseudowire type 4
tlv template TLV
tlv 1 4 dec 1500
tlv vccv-flags C 4 hexstr 0110
!
interface pseudowire501
  source template type pseudowire dynTempl
encapsulation mpls
neighbor 10.2.2.2 101
signaling protocol ldp
```

代替（または新しい）コマンドを使用した、MPLS L2VPN 擬似回線テンプレート設定の表示

次に、**show interface pseudowire** コマンドの出力例を示します。

```
PE1#show interface pseudowire 100
pseudowire100 is up
    Description: Pseudowire Interface
    MTU 1500 bytes, BW 10000000 Kbit
    Encapsulation mpls
    Peer IP 10.4.4.4, VC ID 121
    RX
      21 packets 2623 bytes 0 drops
    TX
      20 packets 2746 bytes 0 drops
```

次に、**show template** コマンドの出力例を示します。

```
PE1#show template

Template        class/type    Component(s)
ABC             owner        interface pseudowire
 BOUND: pw1
```

代替（または新しい）コマンドを使用した、インターフェイス擬似回線でのテンプレートのソーシング

次の例では、インターフェイス擬似回線は定義されているすべての属性を PE 2 ルータ上のテンプレートから継承するように設定されます。

```
PE2(config-subif)#interface pseudowire 100
PE2(config-if)#source template type pseudowire test
PE2(config-if)#neighbor 10.4.4.4 121
PE2(config-if)#no shutdown
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
MPLS コマンド	『Multiprotocol Label Switching Command Reference』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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。	http://www.cisco.com/cisco/web/support/index.html

L2VPN プロトコルベース CLI の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、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。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *2* : ***L2VPN*** プロトコルベース ***CLI*** の機能情報

機能名	リリース	機能情報
L2VPN プロトコルベース CLI	Cisco IOS XE Release 3.7S	L2VPN プロトコルベース CLI 機能は、さまざまな Cisco プラットフォームで Cisco IOS ソフトウェアを開発および配布するための一連のプロセスと強化されたインフラストラクチャを提供します。この機能では、シスコのプラットフォーム全体で一貫した機能性を実現し、オペレーティング システム（OS）間のサポートを提供するために、新しいコマンドが導入され、既存のコマンドが修正または置換されています。 この機能は、Cisco IOS XE Release 3.7S で、Cisco ASR 903 シリーズ ルータに導入されました。

第 3 章

Any Transport over MPLS

このモジュールでは、Any Transport over MPLS（AToM）が、マルチプロトコル ラベル スイッチング（MPLS）バックボーン上でデータ リンク層（レイヤ 2）パケットを転送するように設定する方法について説明します。AToM によりサービス プロバイダーは、単一の統合されたパケット ベース ネットワーク インフラストラクチャ（Cisco MPLS ネットワーク）を使用することで、既存のレイヤ 2 ネットワークとカスタマー サイトを接続できます。別々のネットワーク管理環境による別々のネットワークに代わり、サービスプロバイダーは、MPLS バックボーン上でレイヤ 2 接続が可能になります。AToM は、MPLS ネットワーク コア上でサポートされるレイヤ 2 トラフィック タイプをカプセル化して送信するための共通フレームワークを提供します。

AToM は、次の like-to-like 転送タイプをサポートします。

- ATM Adaptation Layer Type-5（AAL5）over MPLS
- ATM Cell Relay over MPLS
- Ethernet over MPLS（ポート モード）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース 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、機能情報の表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シスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

Any Transport over MPLS の前提条件

- プロバイダー エッジ（PE）ルータが IP によって相互に到達できるように、コアに IP ルーティングを設定する必要があります。
- ラベル スイッチド パス（LSP）が PE ルータ間に存在するように、コア内に MPLS を設定する必要があります。
- レイヤ 2 トラフィックの開始および終了のためのループバック インターフェイスを設定する必要があります。PE ルータが他のルータのループバック インターフェイスにアクセスできることを確認します。ループバック インターフェイスは、すべてのケースで必要というわけではないことに注意してください。たとえば、AToM がトラフィック エンジニアリング（TE）トンネルに直接マッピングされている場合、トンネル選択ではループバック インターフェイスは必要ありません。

Any Transport over MPLS の制約事項

一般的な制約事項

AToM のすべての転送タイプに関連する一般的な制約事項は、次のとおりです。

- アドレス形式：すべての PE ルータのラベル配布プロトコル（LDP）ルータ ID を、/32 マスクを使用したループバック アドレスとなるように設定します。そうしないと、一部の設定が正常に機能しない可能性があります。

Ethernet over MPLS（EoMPLS）の制約事項

Ethernet over MPLS 機能に関連する制約事項は、次のとおりです。

- Ethernet over MPLS は、IEEE 802.1Q 標準に準拠している VLAN パケットをサポートします。802.1Q 仕様は、イーサネット フレームに VLAN メンバーシップ情報を挿入する標準方式を

確立します。PEルータとCEルータの間では、スイッチ間リンク（ISL）プロトコルはサポートされません。

- AToM コントロール ワードがサポートされています。ただし、ピア PE でコントロール ワードがサポートされていない場合、コントロール ワードはディセーブルになります。このネゴシエーションは、LDP ラベル バインディングによって実行されます。
- ハードウェアレベルの巡回冗長検査（CRC）エラー、フレーミング エラー、およびラントパケットを含むイーサネット パケットは、入力時に廃棄されます。

一般的な制約事項

- アドレス形式：すべての PE ルータ上で、Label Distribution Protocol（LDP）ルータ ID を /32 マスク付きのループバック アドレスに設定します。そうしないと、一部の設定が正常に機能しない可能性があります。
- 明示的な Null MPLS カプセル化を使用する PTPoIP 構成の場合、トランスペアレント クロック（TC）が PTP マスターと PTP スレーブの間にあると、TC は訂正フィールドを更新しません。

ATM AAL5 over MPLS の制約事項

- AAL5 over MPLS は SDU モードでだけサポートされます。

ATM Cell Relay over MPLS の制約事項

- PE ルータ間に実行中の TE トンネルがある場合、トンネル インターフェイスで LDP を有効化する必要があります。
- F4 エンドツーエンド OAM セルは、ATM セルとともに透過的に転送されます。相手先固定パス（PVP）または相手先固定接続（PVC）が 1 つの PE ルータでダウンしている場合、その PVP または PVC に関連付けられているラベルは回収されます。その後、ピアの PE ルータはラベルの回収を検出し、F4 AIS/RDI 信号を対応する CE ルータに送信します。ピア PE ルータの PVP または PVC は、アップ状態のままになります。
- VC クラス コンフィギュレーション モードは、ポート モードではサポートされていません。
- AToM 制御ワードがサポートされています。ただし、ピア PE で制御ワードがサポートされていない場合、制御ワードはディセーブルになります。

VP モードの ATM Cell Relay over MPLS を設定する場合は、次の制約事項が適用されます。

- VPI が VP セルリレー用に設定されている場合、同じ VPI を使用して PVC を設定することはできません。

- VP トランキング（エミュレートされた 1 つの VC ラベルへの複数の VP のマッピング）はサポートされていません。各 VP はエミュレートされた 1 つの VC にマッピングされます。
- VP モードおよび VC モードはアイドル セルをドロップします。

Ethernet over MPLS（EoMPLS）の制約事項

- Ethernet over MPLS が稼働している CE ルータと PE ルータ間のサブインターフェイスは、同じサブネット内になければなりません。
- 隣接する CE ルータ上のサブインターフェイスは PE ルータと同じ VLAN 上にある必要があります。
- Ethernet over MPLS は、IEEE 802.1Q 標準に準拠している VLAN パケットをサポートします。802.1Q 仕様は、イーサネット フレームに VLAN メンバーシップ情報を挿入する標準方式を確立します。PE ルータと CE ルータの間では、スイッチ間リンク（ISL）プロトコルはサポートされません。
- AToM 制御ワードがサポートされています。ただし、ピア PE で制御ワードがサポートされていない場合、制御ワードはディセーブルになります。
- ハードウェアレベルの巡回冗長検査（CRC）エラー、フレーミング エラー、およびラントパケットを含むイーサネット パケットは、入力時に廃棄されます。

Ethernet over MPLS 用のサブインターフェイスごとの MTU の制約事項

- 次の機能は、xconnect サブインターフェイス コンフィギュレーション モードでの MTU 値をサポートしていません。
  - 『Layer 2 Tunnel Protocol Version 3 (L2TPv3)』
  - 仮想プライベート LAN サービス（VPLS）
  - L2VPN 擬似回線スイッチング
- MTU 値は、次のインターフェイスおよびサブインターフェイスにかぎり、xconnect サブインターフェイス コンフィギュレーション モードで設定できます。
  - ファスト イーサネット
  - ギガビット イーサネット
- ルータは、LDP を通じて確立されたリモート VC の MTU 検証プロセスを使用します。このプロセスは、xconnect サブインターフェイス コンフィギュレーション モードで設定された MTU 値を、リモート カスタマー インターフェイスの MTU 値と比較します。MTU 値が xconnect サブインターフェイス コンフィギュレーション モードで設定されていない場合、検証プロセスは、ローカル カスタマー インターフェイスの MTU 値を、明示的に設定されてい

るリモート xconnect の MTU 値か、または基盤となるインターフェイスやサブインターフェイスから継承されたリモート xconnect の MTU 値と比較します。

- xconnect サブインターフェイス コンフィギュレーション モードで MTU 値を設定する場合、指定される MTU 値がデータプレーンによって設定されることはありません。データプレーンは、インターフェイス（ポートモード）またはサブインターフェイス（VLANモード）の MTU 値を設定します。
- インターフェイス MTU が xconnect サブインターフェイス コンフィギュレーション モードで設定した MTU 値よりも大きいことを確認します。カスタマー方向のサブインターフェイスの MTU 値がコア方向のインターフェイスの MTU 値よりも大きい場合、トラフィックは擬似回線を通過できないことがあります。

Frame Relay over MPLS の制約事項

フレーム リレー トラフィック シェーピングは AToM スイッチド VC でサポートされません。

HDLC over MPLS の制約事項

- 非同期インターフェイスはサポートされません。
- HDLC over MPLS はルータ インターフェイスだけに設定する必要があります。HDLC over MPLS はサブインターフェイスには設定できません。

PPP over MPLS の制約事項

- 1 つのルータでのゼロ ホップはサポートされません。ただし、バックツーバックの PE ルータを使用できます。
- 非同期インターフェイスはサポートされません。バックボーンの両端にある CE と PE ルータ間の接続は、類似したリンク層特性を備えている必要があります。CE と PE ルータ間の接続は、ともに同期している必要があります。
- マルチリンク PPP（MLP）はサポートされていません。
- PPP はルータ インターフェイスだけに設定する必要があります。PPP はサブインターフェイスには設定できません。

トンネル選択の制約事項

- 選択するパスは、ピア PE ルータを宛先とする LSP である必要があります。
- 選択するトンネルは、MPLS TE トンネルである必要があります。
- トンネルを選択する場合、トンネルの末端はリモート PE ルータである必要があります。

- IP アドレスを指定する場合、そのアドレスは、リモート PE ルータ上のループバック インターフェイスの IP アドレスである必要があります。アドレスは /32 マスクを使用している必要があります。選択したアドレスを宛先とする LSP が存在している必要があります。LSP は TE トンネルである必要はありません。

ATOM での EXP ビットの制約事項

- LSP トンネル ラベルは最後から 2 番めのルータで削除されることがあるため、VC ラベルおよび LSP トンネル ラベルの両方で Experimental（EXP）ビットをスタティックに設定する必要があります。
- EXP ビットと ATM AAL5 over MPLS および EXP ビットと Frame Relay over MPLS に関しては、EXP ビットに値を割り当てなかった場合、ヘッダーの「タグ制御情報」フィールドにある優先順位ビットがゼロに設定されます。
- VC モードの EXP ビットと ATM Cell Relay over MPLS に関しては、EXP ビットに値を割り当てなかった場合、ヘッダーの「タグ制御情報」フィールドにある優先順位ビットがゼロに設定されます。
- EXP ビットと HDLC over MPLS および PPP over MPLS に関しては、EXP ビットに値を割り当てなかった場合、EXP ビット フィールドにゼロが書き込まれます。

リモート イーサネット ポート シャットダウンの制約事項

この機能は、リモート PE ルータが古いバージョン イメージを実行している、または EoMPLS リモートイーサネットポートのシャットダウン機能をサポートしていない別のプラットフォームで実行されていて、ローカルPEがこの機能をサポートしているイメージを実行している場合には非対称です。

Any Transport over MPLS に関する情報

ATOM を設定するには、次の概念を理解している必要があります。

ATOM によるレイヤ 2 パケットの転送方法

ATOM は入力 PE でレイヤ 2 フレームをカプセル化して、2 つの PE ルータ間を接続する擬似回線の反対側に位置する対応した PE に送信します。出力 PE はカプセル化を削除し、レイヤ 2 フレームを送信します。

PE ルータ間でレイヤ 2 フレームを正常に転送するには、PE ルータを設定する必要があります。ルータ間で、擬似回線と呼ぶ接続を設定します。各 PE ルータで次の情報を指定します。

- イーサネット、フレーム リレー、ATM など、擬似回線で転送されるレイヤ 2 データのタイプ
- PE ルータが通信できる、ピア PE ルータのループバック インターフェイスの IP アドレス
- 擬似回線を識別するピア PE の IP アドレスと VC ID の一意の組み合せ

次の例は、レイヤ 2 パケットの転送を可能にする、PE ルータ上での基本的な設定手順を示しています。転送タイプによって、多少手順が異なります。

ステップ 1 は、PE ルータのインターフェイスまたはサブインターフェイスを定義します。

```
Router# interface
 interface-type interface-number
```

ステップ は、dot1q などのインターフェイスのカプセル化タイプを指定します。

```
Router(config-if-srv)# encapsulation
encapsulation-type
```

ステップ 4 は、次の処理を実行します。

- ピア PE ルータの LDP ルータ ID を指定することによって、ピア PE ルータへの接続を作成します。
- 2 つの PE ルータ間で共有される、VC ID と呼ばれる 32 ビットの固有識別情報を指定します。

ピア ルータ ID と VC ID の組み合わせは、ルータ上で一意である必要があります。2 つの回線で同じピア ルータ ID と VC ID の組み合わせを使用することはできません。

- 擬似回線でデータをカプセル化するためのトンネリング方法を指定します。AToM は MPLS をトンネリング方式として使用します。

```
Router(config-if-srv)# xconnect
peer-router-id vcid
encapsulation mpls
```

代わりに、擬似回線クラスを設定して、トンネリング方式および他の特性を指定することもできます。詳細については、擬似回線クラスの設定, （37 ページ）を参照してください。

L2VPN プロトコルベースの CLI 機能に関連するコマンドを使用した、AToM によるレイヤ 2 パケットの転送方法

AToM は入力 PE でレイヤ 2 フレームをカプセル化して、2 つの PE ルータ間を接続する擬似回線の反対側に位置する対応した PE に送信します。出力 PE はカプセル化を削除し、レイヤ 2 フレームを送信します。

PE ルータ間でレイヤ 2 フレームを正常に転送するには、PE ルータを設定する必要があります。ルータ間で、擬似回線と呼ぶ接続を設定します。各 PE ルータで次の情報を指定します。

- イーサネット、フレーム リレー、ATM など、擬似回線で転送されるレイヤ 2 データのタイプ
- PE ルータが通信できる、ピア PE ルータのループバック インターフェイスの IP アドレス

- 擬似回線を識別するピア PE の IP アドレスと VC ID の一意の組み合せ

次の例は、レイヤ 2 パケットの転送を可能にする、PE ルータ上での基本的な設定手順を示しています。転送タイプによって、多少手順が異なります。

ステップ 1 は、PE ルータのインターフェイスまたはサブインターフェイスを定義します。

```
Router# interface
interface-type interface-number
```

ステップ 3 は、dot1q などのインターフェイスのカプセル化タイプを指定します。

```
Router(config-if)# encapsulation
encapsulation-type
```

ステップ 3 は、次の処理を実行します。

- ピア PE ルータの LDP ルータ ID を指定することによって、ピア PE ルータへの接続を作成します。
- 2 つの PE ルータ間で共有される、VC ID と呼ばれる 32 ビットの固有識別情報を指定します。

ピア ルータ ID と VC ID の組み合わせは、ルータ上で一意である必要があります。2 つの回線で同じピア ルータ ID と VC ID の組み合わせを使用することはできません。

- 擬似回線でデータをカプセル化するためのトンネリング方法を指定します。AToM は MPLS をトンネリング方式として使用します。

```
Router(config)# interface pseudowire 100
Router(config-if)# encapsulation mpls
Router(config-if)# neighbor 10.0.0.1 123
Router(config-if)# exit
!
Router(config)# l2vpn xconnect context A
Router(config-xconnect)# member pseudowire 100


Router(config-xconnect)# exit
```

代わりに、擬似回線クラスを設定して、トンネリング方式および他の特性を指定することもできます。詳細については、擬似回線クラスの設定, （37 ページ）を参照してください。

AToM の利点

次に、レイヤ 2 パケットを MPLS ネットワーク内で送信できるようにする利点について説明します。

- AToM 製品セットは、複数の Cisco ルータ プラットフォームで、イーサネットおよびフレーム リレーを含む多数のレイヤ 2 パケット タイプに対応しています。これにより、サービス プロバイダーはバックボーン上ですべてのタイプのトラフィックを転送し、すべてのタイプの顧客に対応することができます。
- AToM は、MPLS 上でレイヤ 2 パケットを転送するために開発された標準規格に準拠しています。このことは、ネットワークに業界標準規格の方法論を取り込みたいサービス プロバイ

ダーに役立ちます。他のレイヤ 2 ソリューションは独自形式であり、サービス プロバイダーのネットワーク拡張機能を制限したり、特定のベンダーの装置だけを使用するようにサービス プロバイダーに強要する可能性があります。

- AToM へのアップグレードは、顧客にとって透過的です。サービス プロバイダー ネットワークはカスタマー ネットワークとは別であるため、サービス プロバイダーは、カスタマーへのサービスを中断せずに AToM にアップグレードできます。カスタマーからは、従来のレイヤ 2 バックボーンを使用しているように見えます。

MPLS Traffic Engineering Fast Reroute

AToM は、Fast Reroute（FRR）のサポートにより MPLS トラフィック エンジニアリング（TE）トンネルを使用できます。AToM VC は、MPLS および IP プレフィックスと同時に、障害が発生したリンクまたはノードを回避するように再ルーティングできます。

AToM で高速リルートをイネーブルにするために特別なコマンドを使用する必要はありません。標準の高速リルート コマンドを使用できます。入力 PE では、FRR で保護された TE トンネルにルーティングされた場合、AToM トンネルは Fast Reroute で保護されます。リンクとノード両方の保護は、入力 PE の AToM VC でサポートされます。

パケットサイズの見積もりでの最大伝送ユニットに関するガイドライン

次の計算を使用して、コア ネットワークを通過するパケットのサイズを決定できます。このサイズのパケットに対応するように、P および PE ルータのコア方向のインターフェイスに最大伝送単位（MTU）を設定します。次の等式が示すように、MTU は各項目の合計バイト数以上である必要があります。

```
Core MTU >= (Edge MTU + Transport header + AToM header + (MPLS label stack * MPLS label
size))
```

次に、等式で使用されている変数について説明します。

エッジ MTU

エッジ MTU は、カスタマー方向のインターフェイスの MTU です。

トランスポート ヘッダー

転送ヘッダーは転送タイプによって決まります。次の表に、ヘッダーの特定のサイズを示します。

表 *3*：パケットのヘッダー サイズ

転送タイプ	パケット サイズ
AAL5	0 ～ 32 バイト

転送タイプ	パケット サイズ
イーサネット VLAN	18 バイト
イーサネット ポート	14 バイト
フレームリレー DLCI	シスコのカプセル化の場合 2 バイト、Internet Engineering Task Force（IETF）のカプセル化の場合 8 バイト
HDLC	4 バイト
PPP	4 バイト

AToM ヘッダー

AToM ヘッダーは 4 バイトです（コントロール ワード）。コントロール ワードは、イーサネット、PPP、HDLC、およびセル リレーの転送タイプではオプションです。コントロール ワードは、フレーム リレーおよび ATM AAL5 の転送タイプでは必須です。

MPLS ラベル スタック

MPLS ラベル スタック サイズは、コア MPLS ネットワークの設定によって決まります。

- AToM は 1 つの MPLS ラベルを使用して AToM VC（VC ラベル）を特定します。そのため、MPLS ラベル スタックの最小数は、AToM PE（PE ルータ間に P ルータがない PE ルータ）が直接接続される場合の 1 です。
- MPLS ネットワークで LDP が使用されている場合、ラベル スタック サイズは 2 になります（LDP ラベルと VC ラベル）。
- MPLS ネットワークの PE ルータ間で、LDP の代わりに TE トンネルが使用されている場合、ラベル スタック サイズは 2 になります（TE ラベルと VC ラベル）。
- TE トンネルと LDP が MPLS ネットワークで使用される場合（たとえば、P ルータ間または P ルータと PE ルータ間の TE トンネル、トンネルで LDP を使用）、ラベル スタックは 3 になります（TE ラベル、LDP ラベル、VC ラベル）。
- MPLS ネットワークで MPLS Fast Reroute を使用する場合は、スタックにラベルを追加します。この場合の最大 MPLS ラベル スタックは、4 です（FRR ラベル、TE ラベル、LDP ラベル、VC ラベル）。
- MPLS VPN Carrier Supporting Carrier 環境でカスタマー キャリアによって AToM が使用されている場合は、スタックにラベルを追加します。プロバイダー キャリア ネットワークの最大 MPLS ラベル スタックは、5 です（FRR ラベル、TE ラベル、LDP ラベル、VPN ラベル、VC ラベル）。
- AToM トンネルが、IPv4 ボーダー ゲートウェイ プロトコル（BGP）を使用して MPLS ラベルを交換する複数のサービス プロバイダーにまたがる場合（RFC 3107）、スタックにラベル

を追加します。最大 MPLS ラベル スタックは、5 です（FRR ラベル、TE ラベル、ボーダーゲートウェイ プロトコル（BGP）ラベル、LDP ラベル、VC ラベル）。

その他の状況では、MPLS ラベル スタック サイズを増やすことができます。そのため、AToM トンネル エンドポイント間の完全なデータ パスを分析して、ネットワークの最大 MPLS ラベル スタック サイズを決定します。それから、ラベル スタック サイズを MPLS ラベルのサイズで乗算します。

パケット サイズの見積もりの例

次の例では、以下の想定事項に基づく見積もりパケット サイズは 1526 バイトです。

- エッジ MTU は 1500 バイトです。
- 転送タイプはイーサネット VLAN であり、これは転送ヘッダーの 18 バイトを指定します。
- コントロール ワードが使用されていないため、AToM ヘッダーは 0 です。
- LDP が使用されるため、MPLS ラベル スタックは 2 です。MPLS ラベルは 4 バイトです。

```
Edge MTU + Transport header + AToM header + (MPLS label stack * MPLS label) = Core MTU
1500     + 18                     + 0      + (2                * 4         ) = 1526
```

1526 バイトのパケットを受け取るようにコアの P ルータと PE ルータを設定する必要があります。

Ethernet over MPLS 用のサブインターフェイスごとの MTU

xconnect サブインターフェイス コンフィギュレーション モードで MTU 値を指定できます。xconnect サブインターフェイス コンフィギュレーション モードを使用して MTU 値を設定する場合、インターフェイスが変更不可能な MTU 値を個別に持つ状況に適した擬似回線接続を確立します。

サポートされている MTU 値（64 バイト～インターフェイスでサポートされている最大バイト数）の範囲外の MTU 値を xconnect サブインターフェイス コンフィギュレーション モードで指定すると、コマンドが拒否されることがあります。xconnect サブインターフェイス コンフィギュレーション モードで範囲外の MTU 値を指定すると、ルータはサブインターフェイス コンフィギュレーション モードでコマンドを開始します。

たとえば、xconnect サブインターフェイス コンフィギュレーション モードで 1501 の MTU を指定する場合、この値は範囲外であるため、ルータは、この値が受け入れられるサブインターフェイス コンフィギュレーション モードでコマンドを開始します。

```
Router# configure terminal
Router(config)# interface gigabitethernet0/0/2.1
Router(config-subif)# xconnect 10.10.10.1 100 encapsulation mpls
Router(config-subif-xconn)# mtu ?
<64 - 1500> MTU size in bytes
Router(config-subif-xconn)# mtu 1501 <<================
Router(config-subif)# mtu ?
<64 - 17940> MTU size in bytes
```

MTU 値が xconnect サブインターフェイス コンフィギュレーション モードでもサブインターフェイス コンフィギュレーション モードでも受け入れられない場合、コマンドは拒否されます。

L2VPNプロトコルベースCLI機能に関連するコマンドを使用したEthernet over MPLS 用のサブインターフェイスごとの MTU

xconnect コンフィギュレーション モードで MTU 値を指定できます。xconnect コンフィギュレーション モードを使用して MTU 値を設定する場合、インターフェイスが変更不可能な MTU 値を個別に持つ状況に適した擬似回線接続を確立します。

サポートされている MTU 値（64 バイトからインターフェイスでサポートされている最大バイト数）の範囲外の MTU 値を xconnect コンフィギュレーション モードで指定すると、コマンドが拒否されることがあります。xconnect コンフィギュレーション モードで範囲外の MTU 値を指定すると、ルータはサブインターフェイス コンフィギュレーションモードでコマンドを開始します。

たとえば、xconnect コンフィギュレーション モードで 1501 の MTU を指定する場合、この値は範囲外であるため、ルータは、この値が受け入れられるサブインターフェイス コンフィギュレーション モードでコマンドを開始します。

```
Router# configure terminal
Router(config)# interface gigabitethernet0/0/2.1
Router(config)# interface pseudowire 100
Router(config-if)# encapsulation mpls
Router(config-if)# neighbor 10.10.10.1 100
Router(config-if)# mtu ?
<64 - 1500> MTU size in bytes
Router(config-if)# mtu 1501 <<================
Router(config-if)# mtu ?
<64 - 17940> MTU size in bytes
Router(config-if)# exit
!
Router(config)# l2vpn xconnect context A
Router(config-xconnect)# member pseudowire 100 Router
Router(config-xconnect)# member gigabitethernet0/0/2.1
Router(config-xconnect)# exit
```

MTU 値が xconnect コンフィギュレーション モードでもサブインターフェイス コンフィギュレーション モードでも受け入れられない場合、コマンドは拒否されます。

Frame Relay over MPLS と DTE DCE および NNI の接続

インターフェイスを DTE デバイスまたは DCE スイッチとして設定するか、網間インターフェイス（NNI）接続によりスイッチに接続されるスイッチとして設定できます。インターフェイス コンフィギュレーション モードで次のコマンドを使用します:

frame-relayintf-type [dce | dte | nni]

次のテーブルでキーワードを説明します。

表 *4*：*frame-relay intf-type* コマンドのキーワード

キーワード	説明
dce	ルータまたはアクセス サーバがルータに接続されるスイッチとして機能することを可能にします。
dte	ルータまたはアクセス サーバが DTE デバイスとして機能することを可能にします。DTE はデフォルトです。
nni	ルータまたはアクセス サーバがスイッチに接続されるスイッチとして機能することを可能にします。

ローカル管理インターフェイスおよび Frame Relay over MPLS

ローカル管理インターフェイス（LMI）は、PVC に関するステータス情報を通信するプロトコルです。PVC が追加、削除、または変更されると、LMI はエンドポイントにステータス変更を通知します。また、LMI はリンクがアップしていることを検証するポーリング メカニズムも提供します。

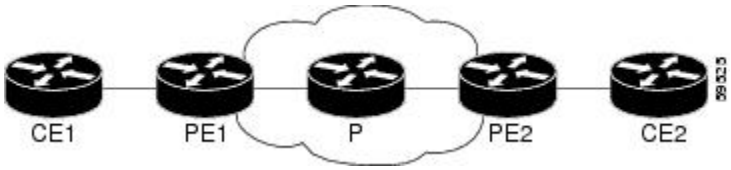
LMI の機能

PVC ステータスを確認するために、LMI は報告しているデバイスからフレーム リレーのエンドユーザ デバイスまで PVC が使用可能かどうかを検査します。PVC が使用可能な場合、LMI は、ステータスは「アクティブ」であると報告します。これは、報告しているデバイスとフレーム リレーのエンドユーザデバイス間ですべてのインターフェイス、回線プロトコル、およびコアセグメントが動作していることを意味します。これらのコンポーネントのいずれかが使用不可の場合、LMI は「非アクティブ」のステータスを報告します。

（注） DCE および NNI インターフェイス タイプのみが LMI ステータスを報告できます。

下図は LMI の機能説明に役立つトポロジ例を示します。

図 *1*：トポロジの例



上図では次の点に注意してください。

- CE1 と PE1 および PE2 と CE2 はフレーム リレー LMI ピアです。
- CE1 および CE2 には、フレーム リレーのスイッチまたはエンドユーザ デバイスを指定できます。
- 各フレーム リレー PVC は複数のセグメントで構成されています。
- DLCI 値は、セグメントごとに異なり、トラフィックがセグメント間で切り替えられたときに変更されます。図中に 2 つのフレーム リレー PVC セグメントがあります。1 つは PE1 と CE1 の間、もう 1 つは PE2 と CE2 の間にあります。

LMI プロトコルの動作は、DLCI-to-DLCI 接続かポート間接続かによって異なります。

DLCI-to-DLCI 接続

DLCI-to-DLCI 接続がある場合、LMI は PE および CE デバイス間のフレーム リレー ポートでローカルに実行します。

- CE1 の PVC が使用可能な場合、CE1 はアクティブなステータスを PE1 に送信します。CE1 がスイッチである場合、LMI は、CE1 から CE1 に接続されているユーザ デバイスに対して PVC が使用可能であることを確認します。
- 次の条件に一致する場合、PE1 は CE1 にアクティブ ステータスを送信します。
  - PE1 の PVC が使用可能である。
  - PE1 がリモート PE ルータから MPLS ラベルを受信している。
  - MPLS トンネル ラベルが PE1 とリモート PE 間に存在する。

DTE または DCE 設定の場合、ネットワーク（DTE）にアクセスしているフレーム リレー デバイスで PVC ステータスが報告されないという LMI 動作が見られます。ネットワーク デバイス（DCE）または NNI のみがステータスを報告できます。そのため、DTE 側で問題が発生しても、DCE ではその問題が認識されません。

ポート間接続

ポート間接続の場合、PE ルータは LMI ステータス検査手順には関係しません。LMI は CE ルータ間でのみ動作します。CE ルータは DCE-DTE または NNI-NNI として設定する必要があります。

設定手順などの LMI に関する詳細については、『Configuring Frame Relay』ドキュメントの「Configuring the LMI」セクションを参照してください。

ATOM でサポートされる QoS 機能

次の表に、ATOM でサポートされる QoS 機能を示します。

表 *5*：*Ethernet over MPLS* でサポートされる *QoS* 機能

QoS 機能	Ethernet over MPLS
サービス ポリシー	適用対象は次のとおりです。 • インターフェイス（入力および出力）
分類	サポートされるコマンドは次のとおりです。 • **matchcos**（インターフェイス） • **matchmplsexperimental**（インターフェイス） • **matchqos-group**（インターフェイス）（出力ポリシー）
マーキング	サポートされるコマンドは次のとおりです。 • **setcos**（出力ポリシー） • **setdiscard-class**（入力ポリシー） • **setmplsexperimental**（入力ポリシー）（インターフェイス） • **setqos-group**（入力ポリシー）
ポリシング	サポート対象は次のとおりです。 • カラー対応ポリシング • マルチアクション ポリシング • 単一レート ポリシング • 2 レート ポリシング
キューイングおよびシェーピング	サポート対象は次のとおりです。 • バイトベースの WRED • Low Latency Queueing（LLQ） • 重み付けランダム早期検出（WRED）

表 *6*：*Frame Relay over MPLS* でサポートされる *QoS* 機能

QoS 機能	Frame Relay over MPLS
サービス ポリシー	適用対象は次のとおりです。 • インターフェイス（入力および出力） • PVC（入力および出力）
分類	サポートされるコマンドは次のとおりです。 • **matchfr-de**（インターフェイスおよびVC） • **matchfr-dlci**（インターフェイス） • **matchqos-group**
マーキング	サポートされるコマンドは次のとおりです。 • **frame-relaycongestionmanagement**（出力） • **setdiscard-class** • **setfr-de**（出力ポリシー） • **setfr-fecn-becn**（出力） • **setmplsexperimental** • **setqos-group** • **thresholdecn**（出力）
ポリシング	サポート対象は次のとおりです。 • カラー対応ポリシング • マルチアクション ポリシング • 単一レート ポリシング • 2 レート ポリシング

QoS 機能	Frame Relay over MPLS
キューイングおよびシェーピング	サポート対象は次のとおりです。 • バイトベースの WRED • クラスベース重み付け均等化キューイング（CBWFQ） • LLQ • **random-detectdiscard-class-based** コマンド • トラフィック シェーピング • WRED

表 *7*：***ATM Cell Relay*** および ***AAL5 over MPLS*** でサポートされる ***QoS*** 機能

QoS 機能	ATM Cell Relay および AAL5 over MPLS
サービス ポリシー	適用対象は次のとおりです。 • インターフェイス（入力および出力） • PVC（入力および出力） • サブインターフェイス（入力および出力）
分類	サポートされるコマンドは次のとおりです。 • **matchmplsexperimental**（VC） • **matchqos-group**（出力）
マーキング	サポートされるコマンドは次のとおりです。 • **random-detectdiscard-class-based**（入力） • **setclp**（出力）（インターフェイス、サブインターフェイス、および VC） • **setdiscard-class**（入力） • **setmplsexperimental**（入力）（インターフェイス、サブインターフェイス、および VC） • **setqos-group**（入力）

QoS 機能	ATM Cell Relay および AAL5 over MPLS
ポリシング	サポート対象は次のとおりです。 • カラー対応ポリシング • マルチアクション ポリシング • 単一レート ポリシング • 2 レート ポリシング
キューイングおよびシェーピング	サポート対象は次のとおりです。 • バイトベースの WRED • CBWFQ • ATM PVC でのクラスベース シェーピングのサポート • LLQ • **random-detectdiscard-class-based** コマンド • WRED

ATM AAL5 over MPLS 用の OAM セル エミュレーション

PE ルータがラベル スイッチド パス（LSP）をまたぐ運用管理および保守（OAM）セルの転送に対応していない場合は、OAM セルエミュレーションを使用して OAM セルをローカルで終端またはループバックすることができます。両方の PE ルータ上で OAM セル エミュレーションを設定します。これは 2 つの単方向 LSP を形成することによって VC をエミュレートします。両方の PE ルータ上で Cisco ソフトウェア コマンドを使用して OAM セル エミュレーションをイネーブルにします。

ルータ上の OAM セル エミュレーションをイネーブルにした場合は、終端済みの VC と同じ方法で ATM VC を設定して管理できます。OAM セル エミュレーションを使用して設定された VC では、設定されたインターバルでループバック セルをローカル CE ルータに送信できます。エンドポイントは次のいずれかにすることができます。

- OAM セルをローカル CE ルータに送信するエンドツーエンド ループバック
- PE ルータと CE ルータ間のパスに沿って OAM セルの応答をデバイスに返すセグメント ループバック

OAM セルには、次のセルが含まれます。

- アラーム表示信号（AIS）

- リモート障害表示（RDI）

これらのセルによって、VCに沿って障害が特定および報告されます。物理リンクまたはインターフェイスで障害が発生した場合は、中間ノードで障害の影響を受けるすべての下流デバイスにOAM AIS セルが挿入されます。ルータで AIS セルが受信されると、ATM VC がダウンとしてマークされ、リモート エンドにその障害を知らせるために RDI セルが送信されます。

VC クラス コンフィギュレーション モードでの ATM AAL5 over MPLS 用 OAM セル エミュレーション

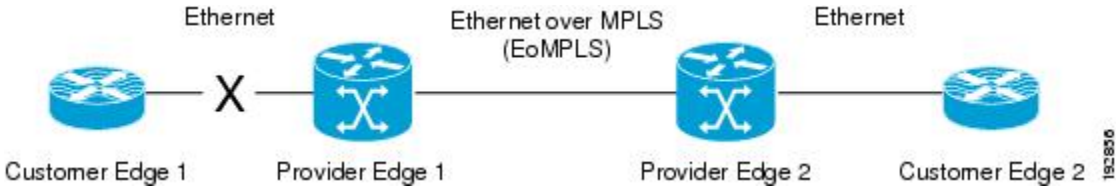
OAM セル エミュレーションを VC クラスの一部として設定し、VC クラスをインターフェイス、サブインターフェイス、または VC に適用できます。VC クラス コンフィギュレーション モードで OAM セル エミュレーションを設定してから VC クラスをインターフェイスに適用すると、サブインターフェイスや VC レベルなどの下位レベルで別の OAM セル エミュレーションの値を指定していないかぎり、VC クラス内の設定がインターフェイスのすべての VC に適用されます。たとえば、OAM セル エミュレーションを指定する VC クラスを作成して、AIS セルのレートを 30 秒間隔に設定します。VC クラスをインターフェイスに適用します。次に、1 つの PVC に対して、OAM セル エミュレーションをイネーブルにして AIS セルのレートを 15 秒間隔に設定します。15 秒に設定した 1 つの PVC を除いて、すべてのインターフェイス上の PVC で 30 秒のセル レートが使用されます。

Any Transport over MPLS（AToM）リモート イーサネット ポート シャットダウン

この Cisco IOS XE 機能により、Ethernet over MPLS（EoMPLS）擬似回線のローカル エンド上のサービス プロバイダー エッジ（PE）ルータは、リモート リンク障害を検出し、ローカル カスタマー エッジ（CE）ルータ上のイーサネット ポートのシャットダウンを実行できるようになります。ローカル CE ルータのイーサネット ポートがシャットダウンされるので、ルータは障害リモート リンクに連続してトラフィックを送信しても、データを損失することはありません。これは、リンクがスタティック IP ルートとして設定されている場合には利点となります。

次の図はある EoMPLS WAN の状況を示しており、CE ルータ（カスタマー エッジ 1）と PE ルータ（プロバイダー エッジ 1）との間のレイヤ 2 トンネル リンクがダウンしています。レイヤ 2 トンネルの反対側の CE ルータ（カスタマー エッジ 2）は引き続きトラフィックを L2 トンネルを介してカスタマー エッジ 1 に転送します。

図 *2*：*EoMPLS WAN* でのリモート リンク停止



この機能がなかったとき、プロバイダー エッジ 2 ルータはリモート リンク障害を検出できませんでした。カスタマー エッジ 2 からカスタマー エッジ 1 に転送されるトラフィックは、ルーティングまたはスパニング ツリー プロトコルがリモート リンクのダウンを検出するまで損失していました。リンクがスタティック ルートとして設定されている場合、リモートリンクの停止を検出することはさらに困難です。

この機能によって、プロバイダー エッジ 2 ルータはリモート リンク障害を検出し、ローカル カスタマー エッジ 2 のイーサネット ポートのシャットダウンを実行します。リモート L2 トンネル リンクが回復すると、ローカル インターフェイスも自動的に回復されます。データ損失の可能性はこのようにして軽減されます。

上の図を例として、リモートイーサネットシャットダウンの流れは一般的に次のように説明されます。

1. カスタマー エッジ 1 とプロバイダー エッジ 1 との間のリモート リンクで障害が生じる。
2. プロバイダー エッジ 2 がリモート リンク障害を検出し、カスタマー エッジ 2 に接続されたライン カード インターフェイス上の送信レーザーを無効化する。
3. RX_LOS エラー アラームがカスタマー エッジ 2 で受信され、カスタマー エッジ 2 がインターフェイスをダウンさせる。
4. プロバイダー エッジ 2 は、カスタマー エッジ 2 とのインターフェイスをアップ状態に維持する。
5. リモート リンクと EoMPLS 接続が回復されると、プロバイダー エッジ ルータ 2 が送信レーザーを有効化する。
6. カスタマー エッジ 2 ルータは、ダウンしたインターフェイスをアップ状態にする。

この機能は、Ethernet over MPLS（EoMPLS）ではデフォルトで有効です。また、次の例で示されているように **remote link failure notification** コマンドを xconnect 設定モードで使用することで、この機能を有効化することもできます。

```
pseudowire-class eompls
 encapsulation mpls
!
interface GigabitEthernet1/0/0
 xconnect 10.13.13.13 1 pw-class eompls
  remote link failure notification
!
```

この機能は、**no remote link failure notification** コマンドを xconnect 設定モードで使用することで無効化できます。すべてのリモート L2 トンネル リンクの状態を表示するには、**show ip interface brief** 特権 EXEC コマンドを使用します。特定のインターフェイス上の L2 トンネルの状態を表示するには、**show interface** 特権 EXEC コマンドを使用します。

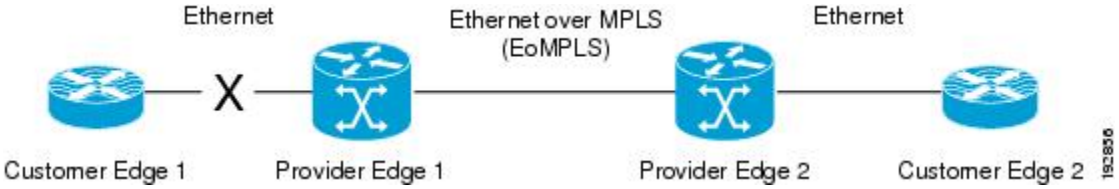
（注） **no remote link failure notification** コマンドを使用すると、リモート接続回線の状態がダウンであることをクライアントに通知しません。

L2VPN プロトコルベースの CLI 機能と関連するコマンドを使用した、Any Transport over MPLS（AToM）リモート イーサネット ポート シャットダウン

この Cisco IOS XE 機能により、Ethernet over MPLS（EoMPLS）擬似回線のローカル エンド上のサービス プロバイダー エッジ（PE）ルータは、リモート リンク障害を検出し、ローカル カスタマー エッジ（CE）ルータ上のイーサネット ポートのシャットダウンを実行できるようになります。ローカル CE ルータのイーサネット ポートがシャットダウンされるので、ルータは障害リモート リンクに連続してトラフィックを送信しても、データを損失することはありません。これは、リンクがスタティック IP ルートとして設定されている場合には利点となります。

次の図はある EoMPLS WAN の状況を示しており、CE ルータ（カスタマー エッジ 1）と PE ルータ（プロバイダー エッジ 1）との間のレイヤ 2 トンネル リンクがダウンしています。レイヤ 2 トンネルの反対側の CE ルータ（カスタマー エッジ 2）は引き続きトラフィックを L2 トンネルを介してカスタマー エッジ 1 に転送します。

図 *3*：*EoMPLS WAN* でのリモート リンク停止



この機能がなかったとき、プロバイダー エッジ 2 ルータはリモート リンク障害を検出できませんでした。カスタマー エッジ 2 からカスタマー エッジ 1 に転送されるトラフィックは、ルーティングまたはスパニング ツリー プロトコルがリモート リンクのダウンを検出するまで損失していました。リンクがスタティック ルートとして設定されている場合、リモートリンクの停止を検出することはさらに困難です。

この機能によって、プロバイダー エッジ 2 ルータはリモート リンク障害を検出し、ローカル カスタマー エッジ 2 のイーサネット ポートのシャットダウンを実行します。リモート L2 トンネル リンクが回復すると、ローカル インターフェイスも自動的に回復されます。データ損失の可能性はこのようにして軽減されます。

上の図を例として、リモートイーサネットシャットダウンの流れは一般的に次のように説明されます。

1. カスタマー エッジ 1 とプロバイダー エッジ 1 との間のリモート リンクで障害が生じる。
2. プロバイダー エッジ 2 がリモート リンク障害を検出し、カスタマー エッジ 2 に接続されたライン カード インターフェイス上の送信レーザーを無効化する。
3. RX_LOS エラー アラームがカスタマー エッジ 2 で受信され、カスタマー エッジ 2 がインターフェイスをダウンさせる。

4 プロバイダー エッジ 2 は、カスタマー エッジ 2 とのインターフェイスをアップ状態に維持する。

5 リモート リンクと EoMPLS 接続が回復されると、プロバイダー エッジ ルータ 2 が送信レーザーを有効化する。

6 カスタマー エッジ 2 ルータは、ダウンしたインターフェイスをアップ状態にする。

この機能は、Ethernet over MPLS（EoMPLS）ではデフォルトで有効です。また、次の例で示されているように **remote link failure notification** コマンドを xconnect 設定モードで使用することで、この機能を有効化することもできます。

```
template type pseudowire eompls
 encapsulation mpls
!
interface Pseudowire 100
 source template type pseudowire test
 neighbor 10.13.13.13 1
interface GigabitEthernet1/0/0
 service instance 300 ethernet
 remote link failure notification
l2vpn xconnect context con1
 member GigabitEthernet1/0/0 service-instance 300
 member Pseudowire 100
!
```

この機能は、**no remote link failure notification** コマンドを xconnect 設定モードで使用することで無効化できます。すべてのリモート L2 トンネル リンクの状態を表示するには、**show ip interface brief** 特権 EXEC コマンドを使用します。特定のインターフェイス上の L2 トンネルの状態を表示するには、**show interface** 特権 EXEC コマンドを使用します。

（注） **No remote link failure notification** コマンドを使用すると、リモート接続回線の状態がダウンであることをクライアントに通知しません。

単一 PW を使用した AToM ロード バランシング

単一 PW を使用した AToM ロード バランシング機能により、同一擬似回線内のパケットをロード バランシングできます。このためには、同一擬似回線内のパケットを、接続回線で受信されるパケットの特定のフィールドに基づいてさらに各種フローに分類します。たとえば、イーサネットの場合、このロード バランシングは、着信パケットの送信元 MAC アドレスに基づきます。

Flow-Aware Transport（FAT）ロード バランシング

MPLS 擬似回線の Flow-Aware Transport 機能では、MPLS ラベル スタック下部にフロー ラベルを追加し、パケットをさまざまなフローにさらに分類することで、同じ擬似回線内でのパケットのロード バランシングを可能にします。

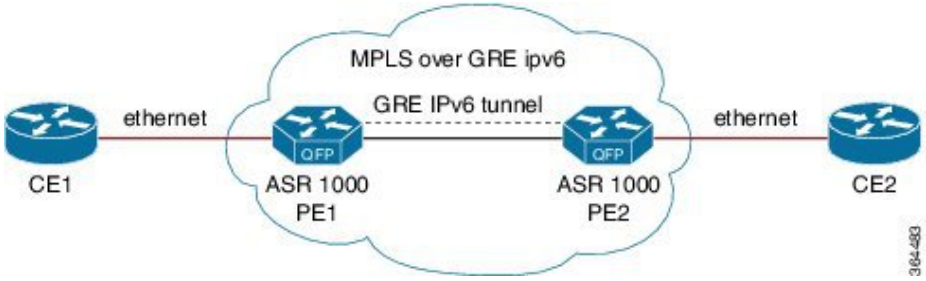
EoMPLS over IPv6 GRE トンネルに関する情報

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 トンネリングとも呼ばれています。

EoMPLS over IPv6 GRE トンネル機能により、GRE トンネルを使用した IPV6 ネットワーク経由での EoMPLS トラフィックのトンネリングがサポートされます。Cisco IOS XE Release 3.15s から、EoMPLS は IPv6 GRE トンネル上でサポートされています。

次の図は、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ上の EoMPLS over IPv6 GRE トンネルの導入モデルを示しています。

図 4：***Cisco ASR 1000*** **シリーズ アグリゲーション サービス ルータ上の** ***EoMPLS over IPv6 GRE*** **トンネルの導入**



EoMPLS over IPv6 GRE トンネル機能の詳細については、『*Interface and Hardware Component Configuration Guide, Cisco IOS XE Release 3S (ASR 1000)*』の『GRE IPv6 Tunnels』の章を参照してください。

Any Transport over MPLS の設定方法

ここでは、基本的な AToM 設定の実行方法について説明します。具体的な内容は、次のとおりです。

擬似回線クラスの設定

（注） 簡易設定では、この作業は任意です。**xconnect** コマンドの一部としてトンネリング方式を指定する場合は、擬似回線クラスを指定する必要はありません。

- AToM VC が正しく動作するには、擬似回線クラスまたは **xconnect** コマンドの一部として **encapsulationmpls** コマンドを指定する必要があります。**xconnect** コマンドの中で **encapsulationmpls** コマンドを省略すると、次のエラーが表示されます。

```
% Incomplete command.
```

手順の概要

1. イネーブル化
2. **configure terminal**
3. **pseudowire-class** *name*
4. **encapsulation mpls**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	**pseudowire-class** *name* 例： `Router(config)# pseudowire-class atom`	指定した名前の擬似回線クラスを確立して、擬似回線クラス コンフィギュレーション モードに入ります。
ステップ 4	**encapsulation mpls** 例： `Router(config-pw)# encapsulation mpls`	トンネリング カプセル化を指定します。

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した擬似回線クラスの設定

（注） 簡易設定では、この作業は任意です。**l2vpn xconnect context** コマンドの一部としてトンネリング方式を指定する場合は、擬似回線クラスを指定する必要はありません。

- ATOM VC が正しく動作するには、擬似回線クラスまたは **l2vpn xconnect context** コマンドの一部として **encapsulationmpls** コマンドを指定する必要があります。**l2vpn xconnect context** コマンドの中で **encapsulationmpls** コマンドを省略すると、次のエラーが表示されます。

```
% Incomplete command.
```

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface pseudowire** *name*
4. **encapsulation mpls**
5. **neighbor** *peer-address* *vcid-value*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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 pseudowire** *name* 例： `Router(config)# interface pseudowire atom`	指定した名前でインターフェイス擬似回線を確立して、擬似回線クラス 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	**encapsulation mpls** 例： `Router(config-pw-class)# encapsulation mpls`	トンネリング カプセル化を指定します。
ステップ 5	**neighbor** *peer-address* *vcid-value* 例： `Router(config-pw-class)# neighbor 33.33.33.33 1`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。

カプセル化タイプの変更および擬似回線の削除

いったん **encapsulationmpls** コマンドを指定すると、**noencapsulationmpls** コマンドでは削除できません。

このような方式では次のようなエラー メッセージが表示されます。

```
Encapsulation changes are not allowed on an existing pw-class.
```

encapsulation mpls コマンドを削除するには、**no pseudowire-class** コマンドを使用して擬似回線を削除する必要があります。

カプセル化タイプを変更するには、**nopseudowire-class** コマンドで擬似回線を削除してから、擬似回線を再設定して新しいカプセル化タイプを指定します。

L2VPN プロトコルベースの CLI 機能と関連するコマンドを使用する、カプセル化タイプの変更と擬似回線の削除

いったん **encapsulationmpls** コマンドを指定すると、**noencapsulationmpls** コマンドでは削除できません。

このような方式では次のようなエラー メッセージが表示されます。

```
Encapsulation changes are not allowed on an existing pw-class.
```

encapsulation mpls コマンドを削除するには、**no template type pseudowire** コマンドを使用して擬似回線を削除する必要があります。

カプセル化タイプを変更するには、**notemplatetypepseudowire** コマンドで擬似回線を削除してから、擬似回線を再設定して新しいカプセル化タイプを指定します。

ATM AAL5 over MPLS の設定

PVC での ATM AAL5 over MPLS の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typeslot*/*subslot*/*port*[**.***subinterface*]
4. **pvc** [*name*] *vpi*/*vci***l2transport**
5. **encapsulationaal5**
6. **xconnect***peer-router-idvcid***encapsulationmpls**
7. **end**
8. **showmplsl2transportvc**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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***typeslot*/*subslot*/*port*[**.***subinterface*] 例： `Router(config)# interface atm1/0/0`	インターフェイス タイプを指定して、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	**pvc** [*name*] *vpi*/*vci***l2transport** 例： `Router(config-if)# pvc 1/200 l2transport`	ATM PVC に名前を割り当てるかまたは名前を作成し、L2transport PVC コンフィギュレーション モードを開始します。 • **l2transport** キーワードは、PVC が終端 PVC ではなくスイッチド PVC であることを示します。

	コマンドまたはアクション	目的
ステップ 5	**encapsulationaal5** 例： `Router(config-if-atm-l2trans-pvc)# encapsulation aal5`	PVC の ATM AAL5 カプセル化を指定します。PE ルータとカスタマーエッジ（CE）ルータに同じカプセル化タイプを指定していることを確認します。
ステップ 6	**xconnect***peer-router-idvcid***encapsulationmpls** 例： `Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls`	接続回線を擬似接続 VC にバインドします。
ステップ 7	**end** 例： `Router(config-if-atm-l2trans-pvc)# end`	特権 EXEC モードに戻ります。
ステップ 8	**showmplsl2transportvc** 例： `Router# show mpls l2transport vc`	ATM AAL5 over MPLS が PVC に設定されていることを示す出力を表示します。

例

次に、**showmplsl2transportvc** コマンドの出力例を示します。この例では、PVC で ATM AAL5 over MPLS が設定されていることが示されています。

```
Router# show mpls l2transport vc
Local intf   Local circuit          Dest address      VC ID      Status
---------    -------------          ------------      -----      ------
ATM1/0       ATM AAL5 1/100         10.4.4.4           100        UP
```

PVC での ATM AAL5 over MPLS の設定（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typeslot*/*subslot*/*port*[**.***subinterface*]
4. **pvc** [*name*] *vpi*/*vci***l2transport**
5. **encapsulationaal5**
6. **end**
7. **interfacepseudowire***number*
8. **encapsulationmpls**
9. **neighbor***peer-addressvcid-value*
10. **exit**
11. **l2vpnxconnectcontext***context-name*
12. **memberpseudowire***interface-number*
13. **memberatm***interface-number***pvc***vpi*/*vci*
14. **end**
15. **showl2vpnatomvc**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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***typeslot*/*subslot*/*port*[**.***subinterface*] 例： `Device(config)# interface atm1/0/0`	インターフェイス タイプを指定して、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	**pvc** [*name*] *vpi*/*vci***l2transport** 例： `Device(config-if)# pvc 1/200 l2transport`	ATM PVC に名前を割り当てるかまたは名前を作成し、L2transport PVC コンフィギュレーション モードを開始します。 • **l2transport** キーワードは、PVC が終端 PVC ではなくスイッチド PVC であることを示します。
ステップ 5	**encapsulationaal5** 例： `Device(config-if-atm-l2trans-pvc)# encapsulation aal5`	PVC の ATM AAL5 カプセル化を指定します。PE ルータとカスタマー エッジ（CE）ルータに同じカプセル化タイプを指定していることを確認します。
ステップ 6	**end** 例： `Device(config-if-atm-l2trans-pvc)# end`	特権 EXEC モードに戻ります。
ステップ 7	**interfacepseudowire***number* 例： `Device(config)# interface pseudowire 100`	擬似回線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 8	**encapsulationmpls** 例： `Device(config-if)# encapsulation mpls`	マルチプロトコル ラベル スイッチング（MPLS）がデータ カプセル化方式として使用されることを指定します。
ステップ 9	**neighbor***peer-addressvcid-value* 例： `Device(config-if)# neighbor 10.13.13.13 100`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 10	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 11	**l2vpnxconnectcontext***context-name* 例： `Device(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect コンフィギュレーション モードを開始します。
ステップ 12	**memberpseudowire***interface-number* 例： `Device(config-xconnect)# member pseudowire 100`	Layer 2 VPN（L2VPN）クロス コネクトを形成するようにメンバー擬似回線を指定します。
ステップ 13	**memberatm***interface-number***pvc***vpi/vci* 例： `Device(config-xconnect)# member atm 100 pvc 1/200`	ATM メンバー インターフェイスのロケーションを指定します。
ステップ 14	**end** 例： `Device(config-xconnect)# end`	特権 EXEC モードに戻ります。
ステップ 15	**showl2vpnatomvc** 例： `Device# show l2vpn atom vc`	ATM AAL5 over MPLS が PVC に設定されていることを示す出力を表示します。

例

次に、**showl2vpnatomvc** コマンドの出力例を示します。この例では、PVC で ATM AAL5 over MPLS が設定されていることが示されています。

```
Device# show l2vpn atom vc
Local intf    Local circuit          Dest address      VC ID      Status
---------     -------------          ------------      -----      ------
ATM1/0        ATM AAL5 1/100         10.4.4.4           100        UP
```

VC クラス コンフィギュレーション モードでの ATM AAL5 over MPLS の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **vc-classatm***vc-class-name*
4. **encapsulation***layer-type*
5. **exit**
6. **interface***typeslot*/*subslot*/*port*[**.***subinterface*]
7. **class-int***vc-class-name*
8. **pvc** [*name*] *vpi*/*vci***l2transport**
9. **xconnect***peer-router-idvcid***encapsulationmpls**
10. **end**
11. **showatmclass-links**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**vc-classatm***vc-class-name* 例： `Router(config)# vc-class atm aal5class`	VC クラスを作成して、VC クラス 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	**encapsulation***layer-type* 例： `Router(config-vc-class)# encapsulation aal5`	AAL およびカプセル化タイプを設定します。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Router(config-vc-class)# exit`	VC クラス コンフィギュレーション モードを終了します。
ステップ 6	**interface***typeslot*/*subslot*/*port*[**.***subinterface*] 例： `Router(config)# interface atm1/0/0`	インターフェイス タイプを指定して、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 7	**class-int***vc-class-name* 例： `Router(config-if)# class-int aal5class`	VC クラスを ATM メイン インターフェイスまたはサブインターフェイスに適用します。 （注） VC クラスは PVC に適用することもできます。
ステップ 8	**pvc** [*name*] *vpi*/*vci***l2transport** 例： `Router(config-if)# pvc 1/200 l2transport`	ATM PVC に名前を割り当てるかまたは名前を作成し、L2transport PVC コンフィギュレーション モードを開始します。 • **l2transport** キーワードは、PVC が終端 PVC ではなくスイッチド PVC であることを示します。
ステップ 9	**xconnect***peer-router-idvcid***encapsulationmpls** 例： `Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls`	接続回線を擬似接続 VC にバインドします。
ステップ 10	**end** 例： `Router(config-if-atm-l2trans-pvc)# end`	特権 EXEC モードに戻ります。
ステップ 11	**showatmclass-links** 例： `Router# show atm class-links`	カプセル化のタイプおよび VC クラスがインターフェイスに適用されていることを表示します。

例

次の例では、**showatmclass-links** コマンドの出力に、ATM AAL5 over MPLS が VC クラスの一部として設定されていることが示されています。このコマンドの出力は、カプセル化のタイプと VC クラスがインターフェイスに適用されていることを示します。

```
Router# show atm class-links 1/100
Displaying vc-class inheritance for ATM1/0/0.0, vc 1/100:
no broadcast - Not configured - using default
encapsulation aal5 - VC-class configured on main interface
```

VC クラス コンフィギュレーション モードでの ATM AAL5 over MPLS の設定（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

手順の概要

1. イネーブル化
2. **configureterminal**
3. **vc-classatm***vc-class-name*
4. **encapsulation***layer-type*
5. **exit**
6. **interface***typeslot*/*subslot*/*port*[**.***subinterface*]
7. **class-int***vc-class-name*
8. **pvc** [*name*] *vpi*/*vci***l2transport**
9. **exit**
10. **interfacepseudowire***number*
11. **encapsulationmpls**
12. **neighbor***peer-addressvcid-value*
13. **exit**
14. **l2vpnxconnectcontext***context-name*
15. **memberpseudowire***interface-number*
16. **memberatm***interface-number*
17. **end**
18. **showatmclass-links**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 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	**vc-classatm***vc-class-name* 例： `Router(config)# vc-class atm aal5class`	VC クラスを作成して、VC クラス 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	**encapsulation***layer-type* 例： `Router(config-vc-class)# encapsulation aal5`	AAL およびカプセル化タイプを設定します。
ステップ 5	**exit** 例： `Router(config-vc-class)# exit`	VC クラス コンフィギュレーション モードを終了します。
ステップ 6	**interface***typeslot*/*subslot*/*port*[**.***subinterface*] 例： `Router(config)# interface atm1/0/0`	インターフェイス タイプを指定して、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 7	**class-int***vc-class-name* 例： `Router(config-if)# class-int aal5class`	VC クラスを ATM メイン インターフェイスまたはサブインターフェイスに適用します。 （注） VC クラスは PVC に適用することもできます。
ステップ 8	**pvc** [*name*] *vpi*/*vci***l2transport** 例： `Router(config-if)# pvc 1/200 l2transport`	ATM PVC に名前を割り当てるかまたは名前を作成し、L2transport PVC コンフィギュレーション モードを開始します。 • **l2transport** キーワードは、PVC が終端 PVC ではなくスイッチド PVC であることを示します。
ステップ 9	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 10	**interfacepseudowire***number* 例： `Router(config)# interface pseudowire 100`	擬似回線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 11	**encapsulationmpls** 例： `Router(config-if)# encapsulation mpls`	マルチプロトコル ラベル スイッチング（MPLS）がデータ カプセル化方式として使用されることを指定します。
ステップ 12	**neighbor***peer-addressvcid-value* 例： `Router(config-if)# neighbor 10.0.0.1 123`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 13	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 14	**l2vpnxconnectcontext***context-name* 例： `Router(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect コンフィギュレーション モードを開始します。
ステップ 15	**memberpseudowire***interface-number* 例： `Router(config-xconnect)# member pseudowire 100`	Layer 2 VPN（L2VPN）クロス コネクトを形成するようにメンバー擬似回線を指定します。
ステップ 16	**memberatm***interface-number* 例： `Device(config-xconnect)# member atm 100`	ATM メンバー インターフェイスのロケーションを指定します。
ステップ 17	**end** 例： `Router(config-if-atm-l2trans-pvc)# end`	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
ステップ 18	**showatmclass-links** 例： `Router# show atm class-links`	カプセル化のタイプおよびVCクラスがインターフェイスに適用されていることを表示します。

例

次の例では、**showatmclass-links** コマンドの出力に、ATM AAL5 over MPLS が VC クラスの一部として設定されていることが示されています。このコマンドの出力は、カプセル化のタイプと VC クラスがインターフェイスに適用されていることを示します。

```
Router# show atm class-links 1/100
Displaying vc-class inheritance for ATM1/0/0.0, vc 1/100:
no broadcast - Not configured - using default
encapsulation aal5 - VC-class configured on main interface
```

ATM AAL5 over MPLS 用の OAM セル エミュレーションの設定

PVC 上での ATM AAL5 over MPLS の OAM セル エミュレーションの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typeslot*/*subslot*/*port*[**.***subinterface*]
4. **pvc** [*name*] *vpi*/*vci***l2transport**
5. **encapsulationaal5**
6. **xconnect***peer-router-idvcid***encapsulationmpls**
7. **oam-acemulation-enable**[*ais-rate*]
8. *oam-pvcmanage* [*frequency*]
9. **end**
10. **showatmpvc**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Router> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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***typeslot*/*subslot*/*port*[**.***subinterface*] 例： `Router(config)# interface atm1/0/0`	インターフェイスタイプを指定して、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	**pvc** [*name*] *vpi*/*vci***l2transport** 例： `Router(config-if)# pvc 1/200 l2transport`	ATM PVC に名前を割り当てるかまたは名前を作成し、L2transport PVC コンフィギュレーション モードを開始します。 • **l2transport** キーワードは、PVC が終端 PVC ではなくスイッチド PVC であることを示します。
ステップ 5	**encapsulationaal5** 例： `Router(config-if-atm-l2trans-pvc)# encapsulation aal5`	PVC の ATM AAL5 カプセル化を指定します。 • PE ルータと CE ルータ上で同じカプセル化タイプを指定します。
ステップ 6	**xconnect***peer-router-idvcid***encapsulationmpls** 例： `Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls`	接続回線を擬似接続 VC にバインドします。
ステップ 7	**oam-acemulation-enable**[*ais-rate*] 例： `Router(config-if-atm-l2trans-pvc)# oam-ac emulation-enable 30`	AAL5 over MPLS の OAM セル エミュレーションをイネーブルにします。*ais-rate* 引数には、AIS セルが送信されるレートを指定します。デフォルトは 1 セル/秒です。この範囲は 0 ～ 60 秒です。

	コマンドまたはアクション	目的
ステップ 8	*oam-pvcmanage* [*frequency*] 例： `Router(config-if-atm-l2trans-pvc)# oam-pvc manage`	PVC で、仮想回線の接続を検証するエンドツーエンドの OAM ループバック セルを生成できるようにします。 オプションの *frequency* 引数は、ループバック セルの送信間のインターバルで、範囲は 0 ～ 600 秒です。デフォルト値は 10 秒です。
ステップ 9	**end** 例： `Router(config-if-atm-l2trans-pvc)# end`	特権 EXEC モードに戻ります。
ステップ 10	**showatmpvc** 例： `Router# show atm pvc`	OAM セル エミュレーションが ATM PVC で有効になっていることを示す出力を表示します。

例

次の **showatmpvc** コマンドの出力は、OAM セル エミュレーションが ATM PVC で有効になっていることを示しています。

```
Router# show atm pvc 5/500
ATM4/1/0.200: VCD: 6, VPI: 5, VCI: 500
UBR, PeakRate: 1
AAL5-LLC/SNAP, etype:0x0, Flags: 0x34000C20, VCmode: 0x0
OAM Cell Emulation: enabled, F5 End2end AIS Xmit frequency: 1 second(s)
OAM frequency: 0 second(s), OAM retry frequency: 1 second(s)
OAM up retry count: 3, OAM down retry count: 5
OAM Loopback status: OAM Disabled
OAM VC state: Not ManagedVerified
ILMI VC state: Not Managed
InPkts: 564, OutPkts: 560, InBytes: 19792, OutBytes: 19680
InPRoc: 0, OutPRoc: 0
InFast: 4, OutFast: 0, InAS: 560, OutAS: 560
InPktDrops: 0, OutPktDrops: 0
CrcErrors: 0, SarTimeOuts: 0, OverSizedSDUs: 0
Out CLP=1 Pkts: 0
OAM cells received: 26
F5 InEndloop: 0, F5 InSegloop: 0, F5 InAIS: 0, F5 InRDI: 26
OAM cells sent: 77
F5 OutEndloop: 0, F5 OutSegloop: 0, F5 OutAIS: 77, F5 OutRDI: 0
OAM cell drops: 0
Status: UP
```

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した PVC 上での ATM AAL5 over MPLS の OAM セル エミュレーションの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typeslot*/*subslot*/*port*[**.***subinterface*]
4. **pvc** [*name*] *vpi*/*vci***l2transport**
5. **encapsulationaal5**
6. **exit**
7. **interfacepseudowire***number*
8. **encapsulationmpls**
9. **neighbor***peer-addressvcid-value*
10. **exit**
11. **l2vpnxconnectcontext***context-name*
12. **memberpseudowire***interface-number*
13. **memberatm***interface-number***pvc***vpi*/*vci*
14. **exit**
15. **pvc** [*name*] *vpi*/*vci***l2transport**
16. **oam-acemulation-enable**[*ais-rate*]
17. *oam-pvcmanage* [*frequency*]
18. **end**
19. **showatmpvc**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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。

	コマンドまたはアクション	目的
ステップ 3	**interface***typeslot*/*subslot*/*port*[**.***subinterface*] 例： `Router(config)# interface atm1/0/0`	インターフェイス タイプを指定して、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	**pvc** [*name*] *vpi*/*vci***l2transport** 例： `Router(config-if)# pvc 1/200 l2transport`	ATM PVC に名前を割り当てるかまたは名前を作成し、L2transport PVC コンフィギュレーション モードを開始します。 • **l2transport** キーワードは、PVC が終端 PVC ではなくスイッチド PVC であることを示します。
ステップ 5	**encapsulationaal5** 例： `Router(config-if-atm-l2trans-pvc)# encapsulation aal5`	PVC の ATM AAL5 カプセル化を指定します。 • PE ルータと CE ルータ上で同じカプセル化タイプを指定します。
ステップ 6	**exit** 例： `Router(config-if-atm-l2trans-pvc)# exit`	L2transport PVC コンフィギュレーション モードを終了します。
ステップ 7	**interfacepseudowire***number* 例： `Router(config)# interface pseudowire 100`	擬似回線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 8	**encapsulationmpls** 例： `Router(config-if)# encapsulation mpls`	マルチプロトコル ラベル スイッチング（MPLS）がデータ カプセル化方式として使用されることを指定します。
ステップ 9	**neighbor***peer-addressvcid-value* 例： `Router(config-if)# neighbor 10.0.0.1 123`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。

	コマンドまたはアクション	目的
ステップ 10	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 11	**l2vpnxconnectcontext***context-name* 例： `Router(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect コンフィギュレーション モードを開始します。
ステップ 12	**memberpseudowire***interface-number* 例： `Router(config-xconnect)# member pseudowire 100`	Layer 2 VPN（L2VPN）クロス コネクトを形成するようにメンバー擬似回線を指定します。
ステップ 13	**memberatm***interface-number***pvc***vpi*/*vci* 例： `Device(config-xconnect)# member atm 100 pvc 1/200`	ATM メンバーインターフェイスのロケーションを指定します。
ステップ 14	**exit** 例： `Router(config-xconnect)# exit`	xconnect コンフィギュレーション モードを終了します。
ステップ 15	**pvc** [*name*] *vpi*/*vci***l2transport** 例： `Router(config-if)# pvc 1/200 l2transport`	ATM PVC に名前を割り当てるかまたは名前を作成し、L2transport PVC コンフィギュレーション モードを開始します。
ステップ 16	**oam-acemulation-enable**[*ais-rate*] 例： `Router(config-if-atm-l2trans-pvc)# oam-ac emulation-enable 30`	AAL5 over MPLS の OAM セル エミュレーションをイネーブルにします。*ais-rate* 引数には、AIS セルが送信されるレートを指定します。デフォルトは 1 セル/秒です。この範囲は 0 ～ 60 秒です。
ステップ 17	*oam-pvcmanage* [*frequency*] 例： `Router(config-if-atm-l2trans-pvc)# oam-pvc manage`	PVC で、仮想回線の接続を検証するエンドツーエンドの OAM ループバック セルを生成できるようにします。

	コマンドまたはアクション	目的
		オプションの*frequency*引数は、ループバック セルの送信間のインターバルで、範囲は 0 ～ 600 秒です。デフォルト値は 10 秒です。
ステップ 18	**end** 例： `Router(config-if-atm-l2trans-pvc)# end`	特権 EXEC モードに戻ります。
ステップ 19	**showatmpvc** 例： `Router# show atm pvc`	OAM セル エミュレーションが ATM PVC で有効になっていることを示す出力を表示します。

例

次の **showatmpvc** コマンドの出力は、OAM セル エミュレーションが ATM PVC で有効になっていることを示しています。

```
Router# show atm pvc 5/500
ATM4/1/0.200: VCD: 6, VPI: 5, VCI: 500
UBR, PeakRate: 1
AAL5-LLC/SNAP, etype:0x0, Flags: 0x34000C20, VCmode: 0x0
OAM Cell Emulation: enabled, F5 End2end AIS Xmit frequency: 1 second(s)
OAM frequency: 0 second(s), OAM retry frequency: 1 second(s)
OAM up retry count: 3, OAM down retry count: 5
OAM Loopback status: OAM Disabled
OAM VC state: Not ManagedVerified
ILMI VC state: Not Managed
InPkts: 564, OutPkts: 560, InBytes: 19792, OutBytes: 19680
InPRoc: 0, OutPRoc: 0
InFast: 4, OutFast: 0, InAS: 560, OutAS: 560
InPktDrops: 0, OutPktDrops: 0
CrcErrors: 0, SarTimeOuts: 0, OverSizedSDUs: 0
Out CLP=1 Pkts: 0
OAM cells received: 26
F5 InEndloop: 0, F5 InSegloop: 0, F5 InAIS: 0, F5 InRDI: 26
OAM cells sent: 77
F5 OutEndloop: 0, F5 OutSegloop: 0, F5 OutAIS: 77, F5 OutRDI: 0
OAM cell drops: 0
Status: UP
```

VC クラス コンフィギュレーション モードにおける ATM AAL5 over MPLS の OAM セル エミュレーションの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **vc-classatm***name*
4. **encapsulation***layer-type*
5. **oam-acemulation-enable**[*ais-rate*]
6. **oam-pvcmanage**[*frequency*]
7. **exit**
8. **interface***typeslot*/*subslot*/*port*[**.***subinterface*]
9. **class-int***vc-class-name*
10. **pvc** [*name*] *vpi*/*vci***l2transport**
11. **xconnect***peer-router-idvcid***encapsulationmpls**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**vc-classatm***name* 例： `Router(config)# vc-class atm oamclass`	VC クラスを作成して、VC クラス 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	**encapsulation***layer-type* 例： `Router(config-vc-class)# encapsulation aal5`	AAL およびカプセル化タイプを設定します。

	コマンドまたはアクション	目的
ステップ 5	**oam-acemulation-enable**[*ais-rate*] 例： `Router(config-vc-class)# oam-ac emulation-enable 30`	MPLS over AAL5 の OAM セル エミュレーションを有効にして、AIS セルが送信されるレートを指定します。
ステップ 6	**oam-pvcmanage**[*frequency*] 例： `Router(config-vc-class)# oam-pvc manage`	PVC で、仮想回線の接続を検証するエンドツーエンドの OAM ループバック セルを生成できるようにします。
ステップ 7	**exit** 例： `Router(config-vc-class)# exit`	VC クラス コンフィギュレーション モードを終了します。
ステップ 8	**interface***typeslot*/*subslot*/*port*[**.***subinterface*] 例： `Router(config)# interface atm1/0/0`	インターフェイス タイプを指定して、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 9	**class-int***vc-class-name* 例： `Router(config-if)# class-int oamclass`	VC クラスを ATM メイン インターフェイスまたはサブインターフェイスに適用します。 （注） VC クラスは PVC に適用することもできます。
ステップ 10	**pvc** [*name*] *vpi*/*vci***l2transport** 例： `Router(config-if)# pvc 1/200 l2transport`	ATM PVC に名前を割り当てるかまたは名前を作成し、L2transport PVC コンフィギュレーション モードを開始します。 • **l2transport** キーワードは、PVC が終端 PVC ではなくスイッチド PVC であることを示します。
ステップ 11	**xconnect***peer-router-idvcid***encapsulationmpls** 例： `Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls`	接続回線を擬似接続 VC にバインドします。

L2VPN プロトコルベースの CLI 機能と関連するコマンドを使用する、VC クラス コンフィギュレーション モードでの ATM AAL5 over MPLS の OAM セル エミュレーションの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **vc-classatm***name*
4. **encapsulation***layer-type*
5. **oam-acemulation-enable**[*ais-rate*]
6. **oam-pvcmanage**[*frequency*]
7. **exit**
8. **interface***typeslot*/*subslot*/*port*[**.***subinterface*]
9. **class-int***vc-class-name*
10. **pvc** [*name*] *vpi*/*vci***l2transport**
11. **end**
12. **interfacepseudowire***number*
13. **encapsulationmpls**
14. **neighbor***peer-addressvcid-value*
15. **exit**
16. **l2vpnxconnectcontext***context-name*
17. **memberpseudowire***interface-number*
18. **memberatm***interface-number*
19. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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。

	コマンドまたはアクション	目的
ステップ 3	**vc-classatm***name* 例： `Router(config)# vc-class atm oamclass`	VC クラスを作成して、VC クラス 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	**encapsulation***layer-type* 例： `Router(config-vc-class)# encapsulation aal5`	AAL およびカプセル化タイプを設定します。
ステップ 5	**oam-acemulation-enable**[*ais-rate*] 例： `Router(config-vc-class)# oam-ac emulation-enable 30`	MPLS over AAL5 の OAM セル エミュレーションを有効にして、AIS セルが送信されるレートを指定します。
ステップ 6	**oam-pvcmanage**[*frequency*] 例： `Router(config-vc-class)# oam-pvc manage`	PVC で、仮想回線の接続を検証するエンドツーエンドのOAMループバック セルを生成できるようにします。
ステップ 7	**exit** 例： `Router(config-vc-class)# exit`	VC クラス コンフィギュレーション モードを終了します。
ステップ 8	**interface***typeslot*/*subslot*/*port*[**.***subinterface*] 例： `Router(config)# interface atm1/0/0`	インターフェイス タイプを指定して、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 9	**class-int***vc-class-name* 例： `Router(config-if)# class-int oamclass`	VC クラスを ATM メイン インターフェイスまたはサブインターフェイスに適用します。 （注） VC クラスは PVC に適用することもできます。
ステップ 10	**pvc** [*name*] *vpi*/*vci***l2transport** 例： `Router(config-if)# pvc 1/200 l2transport`	ATM PVC に名前を割り当てるかまたは名前を作成し、L2transport PVC コンフィギュレーション モードを開始します。 • **l2transport** キーワードは、PVC が終端 PVC ではなくスイッチド PVC であることを示します。

	コマンドまたはアクション	目的
ステップ 11	**end** 例： `Router(config-if-atm-l2trans-pvc)# end`	特権 EXEC モードに戻ります。
ステップ 12	**interfacepseudowire***number* 例： `Router(config)# interface pseudowire 100`	擬似回線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 13	**encapsulationmpls** 例： `Router(config-if)# encapsulation mpls`	マルチプロトコル ラベル スイッチング（MPLS）がデータ カプセル化方式として使用されることを指定します。
ステップ 14	**neighbor***peer-addressvcid-value* 例： `Router(config-if)# neighbor 10.0.0.1 123`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 15	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 16	**l2vpnxconnectcontext***context-name* 例： `Router(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect コンフィギュレーション モードを開始します。
ステップ 17	**memberpseudowire***interface-number* 例： `Router(config-xconnect)# member pseudowire 100`	Layer 2 VPN（L2VPN）クロス コネクトを形成するようにメンバー擬似回線を指定します。
ステップ 18	**memberatm***interface-number* 例： `Device(config-xconnect)# member atm 100`	ATM メンバー インターフェイスのロケーションを指定します。

	コマンドまたはアクション	目的
ステップ 19	**end** 例： `Router(config-xconnect)# end`	特権 EXEC モードに戻ります。

ATM Cell Relay over MPLS の設定

VC モードでの ATM Cell Relay over MPLS の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfaceatm***slot*/*subslot*/*port*[**.***subinterface*]
4. **pvc***vpi*/*vci***l2transport**
5. **encapsulationaal0**
6. **xconnect***peer-router-idvcid***encapsulationmpls**
7. **end**
8. **showatmvc**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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。

	コマンドまたはアクション	目的
ステップ 3	**interfaceatm***slot*/*subslot*/*port*[.*subinterface*] 例： `Router(config)# interface atm1/0/0`	ATM 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	**pvc***vpi*/*vci***l2transport** 例： `Router(config-if)# pvc 0/100 l2transport`	仮想パス識別子（VPI）および仮想回線識別子（VCI）を割り当て、L2transport VC コンフィギュレーション モードを開始します。
ステップ 5	**encapsulationaal0** 例： `Router(config-if-atm-l2trans-pvc)# encapsulation aal0`	ATM セルリレーの場合、インターフェイスの raw セルのカプセル化を指定します。 • PE および CE ルータに同じカプセル化タイプを指定していることを確認します。
ステップ 6	**xconnect***peer-router-idvcid***encapsulationmpls** 例： `Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls`	接続回線を擬似接続 VC にバインドします。
ステップ 7	**end** 例： `Router(config-if-atm-l2trans-pvc)# end`	特権 EXEC モードに戻ります。
ステップ 8	**showatmvc** 例： `Router# show atm vc`	OAM セル エミュレーションが ATM VC でイネーブルになっていることを確認します。

例

次に示す **showatmvc** コマンドの出力には、インターフェイスが VC モードのセルリレー用に設定されていることが示されています。

```
Router# show atm vc 7
ATM3/0: VCD: 7, VPI: 23, VCI: 100
UBR, PeakRate: 149760
AAL0-Cell Relay, etype:0x10, Flags: 0x10000C2D, VCmode: 0x0
OAM Cell Emulation: not configured
InBytes: 0, OutBytes: 0
Status: UP
```

VC モードでの ATM Cell Relay over MPLS の設定（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfaceatm***slot*/*subslot*/*port*[**.***subinterface*]
4. **pvc***vpi*/*vci***l2transport**
5. **encapsulationaal0**
6. **end**
7. **interfacepseudowire***number*
8. **encapsulationmpls**
9. **neighbor***peer-addressvcid-value*
10. **exit**
11. **l2vpn xconnectcontext***context-name*
12. **member pseudowire***interface-number*
13. **member atm** *interface-number*
14. **end**
15. **showatmvc**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**interfaceatm***slot*/*subslot*/*port*[**.***subinterface*] 例： `Router(config)# interface atm1/0/0`	ATM 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。

	コマンドまたはアクション	目的
ステップ 4	**pvc***vpi*/*vci***l2transport** 例： `Router(config-if)# pvc 0/100 l2transport`	仮想パス識別子（VPI）および仮想回線識別子（VCI）を割り当て、L2transport VC コンフィギュレーション モードを開始します。
ステップ 5	**encapsulationaal0** 例： `Router(config-if-atm-l2trans-pvc)# encapsulation aal0`	ATM セルリレーの場合、インターフェイスの raw セルのカプセル化を指定します。 • PE および CE ルータに同じカプセル化タイプを指定していることを確認します。
ステップ 6	**end** 例： `Router(config-if-atm-l2trans-pvc)# end`	特権 EXEC モードに戻ります。
ステップ 7	**interfacepseudowire***number* 例： `Router(config)# interface pseudowire 100`	擬似回線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 8	**encapsulationmpls** 例： `Router(config-if)# encapsulation mpls`	マルチプロトコル ラベル スイッチング（MPLS）がデータ カプセル化方式として使用されることを指定します。
ステップ 9	**neighbor***peer-addressvcid-value* 例： `Router(config-if)# neighbor 10.0.0.1 123`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 10	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 11	**l2vpn xconnectcontext***context-name* 例： `Router(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect 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 12	**member pseudowire***interface-number* 例： `Router(config-xconnect)# member pseudowire 100`	Layer 2 VPN（L2VPN）クロス コネクトを形成するようにメンバー擬似回線を指定します。
ステップ 13	**member atm** *interface-number* 例： `Device(config-xconnect)# member atm 100`	ATM メンバー インターフェイスのロケーションを指定します。
ステップ 14	**end** 例： `Router(config-xconnect)# end`	特権 EXEC モードに戻ります。
ステップ 15	**showatmvc** 例： `Router# show atm vc`	OAM セル エミュレーションが ATM VC でイネーブルになっていることを確認します。

例

次に示す **showatmvc** コマンドの出力には、インターフェイスが VC モードのセルリレー用に設定されていることが示されています。

```
Router# show atm vc 7
ATM3/0: VCD: 7, VPI: 23, VCI: 100
UBR, PeakRate: 149760
AAL0-Cell Relay, etype:0x10, Flags: 0x10000C2D, VCmode: 0x0
OAM Cell Emulation: not configured
InBytes: 0, OutBytes: 0
Status: UP
```

VC クラス コンフィギュレーション モードを使用した VC モードの ATM Cell Relay over MPLS の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **vc-classatm***name*
4. **encapsulation***layer-type*
5. **exit**
6. **interface***typeslot*/*subslot*/*port*[**.***subinterface*]
7. **class-int***vc-class-name*
8. **pvc** [*name*] *vpi*/*vci***l2transport**
9. **xconnect***peer-router-idvcid***encapsulationmpls**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**vc-classatm***name* 例： `Router(config)# vc-class atm cellrelay`	VC クラスを作成して、VC クラス 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	**encapsulation***layer-type* 例： `Router(config-vc-class)# encapsulation aal0`	AAL およびカプセル化タイプを設定します。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Router(config-vc-class)# exit`	VC クラス コンフィギュレーション モードを終了します。
ステップ 6	**interface***typeslot*/*subslot*/*port*[**.***subinterface*] 例： `Router(config)# interface atm1/0/0`	インターフェイス タイプを指定して、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 7	**class-int***vc-class-name* 例： `Router(config-if)# class-int cellrelay`	VC クラスを ATM メイン インターフェイスまたはサブインターフェイスに適用します。 （注） VC クラスは PVC に適用することもできます。
ステップ 8	**pvc** [*name*] *vpi*/*vci***l2transport** 例： `Router(config-if)# pvc 1/200 l2transport`	ATM PVC に名前を割り当てるかまたは名前を作成し、L2transport PVC コンフィギュレーション モードを開始します。
ステップ 9	**xconnect***peer-router-idvcid***encapsulationmpls** 例： `Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls`	接続回線を擬似接続 VC にバインドします。

L2VPN プロトコルベースの CLI 機能と関連するコマンドを使用する、VC クラス コンフィギュレーション モードを使用する VC モードの ATM Cell Relay over MPLS の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **vc-classatm***name*
4. **encapsulation***layer-type*
5. **exit**
6. **interface***typeslot*/*subslot*/*port*[**.***subinterface*]
7. **class-int***vc-class-name*
8. **pvc** [*name*] *vpi*/*vci***l2transport**
9. **end**
10. **interfacepseudowire***number*
11. **encapsulationmpls**
12. **neighbor***peer-addressvcid-value*
13. **exit**
14. **l2vpnxconnectcontext***context-name*
15. **memberpseudowire***interface-number*
16. **memberatm***interface-number*
17. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**vc-classatm***name* 例： `Router(config)# vc-class atm cellrelay`	VC クラスを作成して、VC クラス 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	**encapsulation***layer-type* 例： `Router(config-vc-class)# encapsulation aal0`	AAL およびカプセル化タイプを設定します。
ステップ 5	**exit** 例： `Router(config-vc-class)# exit`	VC クラス コンフィギュレーション モードを終了します。
ステップ 6	**interface***typeslot*/*subslot*/*port*[**.***subinterface*] 例： `Router(config)# interface atm1/0/0`	インターフェイス タイプを指定して、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 7	**class-int***vc-class-name* 例： `Router(config-if)# class-int cellrelay`	VC クラスを ATM メイン インターフェイスまたはサブインターフェイスに適用します。 （注） VC クラスは PVC に適用することもできます。
ステップ 8	**pvc** [*name*] *vpi*/*vci***l2transport** 例： `Router(config-if)# pvc 1/200 l2transport`	ATM PVC に名前を割り当てるかまたは名前を作成し、L2transport PVC コンフィギュレーション モードを開始します。
ステップ 9	**end** 例： `Router(config-if-atm-l2trans-pvc)# end`	特権 EXEC モードに戻ります。
ステップ 10	**interfacepseudowire***number* 例： `Router(config)# interface pseudowire 100`	擬似回線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 11	**encapsulationmpls** 例： `Router(config-if)# encapsulation mpls`	マルチプロトコル ラベル スイッチング（MPLS）がデータ カプセル化方式として使用されることを指定します。

	コマンドまたはアクション	目的
ステップ 12	**neighbor***peer-addressvcid-value* 例： `Router(config-if)# neighbor 10.0.0.1 123`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 13	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 14	**l2vpnxconnectcontext***context-name* 例： `Router(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect コンフィギュレーション モードを開始します。
ステップ 15	**memberpseudowire***interface-number* 例： `Router(config-xconnect)# member pseudowire 100`	Layer 2 VPN（L2VPN）クロス コネクトを形成するようにメンバー擬似回線を指定します。
ステップ 16	**memberatm***interface-number* 例： `Device(config-xconnect)# member atm 100`	ATM メンバー インターフェイスのロケーションを指定します。
ステップ 17	**end** 例： `Router(config-xconnect)# end`	特権 EXEC モードに戻ります。

PVP モードでの ATM Cell Relay over MPLS の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfaceatm***slot*/*subslot*/*port*[**.***subinterface*]
4. **atmpvp***vpi***l2transport**
5. **xconnect***peer-router-idvcid***encapsulationmpls**
6. **end**
7. **showatmvp**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**interfaceatm***slot*/*subslot*/*port*[**.***subinterface*] 例： `Router(config)# interface atm1/0/0`	インターフェイスを定義し、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	**atmpvp***vpi***l2transport** 例： `Router(config-if)# atm pvp 1 l2transport`	PVP を ATM セルの転送専用にすることを指定し、L2transport PVP コンフィギュレーション モードを開始します。 • **l2transport** キーワードは、PVP がセルリレー用であることを示します。このモードは、レイヤ 2 トランスポート専用です。通常の PVP 用ではありません。

	コマンドまたはアクション	目的
ステップ 5	**xconnect***peer-router-idvcid***encapsulationmpls** 例： `Router(config-if-atm-l2trans-pvp)# xconnect 10.0.0.1 123 encapsulation mpls`	接続回線を擬似接続 VC にバインドします。このコマンドの構文は、その他のレイヤ 2 トランスポートの場合と同じです。
ステップ 6	**end** 例： `Router(config-if-atm-l2trans-pvp)# end`	特権 EXEC モードに戻ります。
ステップ 7	**showatmvp** 例： `Router# show atm vp`	OAM セルエミュレーションが ATM VP で有効になっていることを示す出力を表示します。

例

次に示す **showatmvp** コマンドの出力には、インターフェイスが VP モードのセルリレー用に設定されていることが示されています。

```
Router# show atm vp 1
ATM5/0  VPI: 1, Cell Relay, PeakRate: 149760, CesRate: 0, DataVCs: 1, CesVCs: 0, Status:
ACTIVE
  VCD    VCI   Type   InPkts   OutPkts   AAL/Encap     Status
  6      3     PVC    0        0         F4 OAM        ACTIVE
  7      4     PVC    0        0         F4 OAM        ACTIVE
TotalInPkts: 0, TotalOutPkts: 0, TotalInFast: 0, TotalOutFast: 0,
TotalBroadcasts: 0 TotalInPktDrops: 0, TotalOutPktDrops: 0
```

PVP モードでの ATM Cell Relay over MPLS の設定（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfaceatm***slot*/*subslot*/*port*[**.***subinterface*]
4. **atmpvp***vpi***l2transport**
5. **end**
6. **interfacepseudowire***number*
7. **encapsulationmpls**
8. **neighbor***peer-addressvcid-value*
9. **exit**
10. **l2vpnxconnectcontext***context-name*
11. **memberpseudowire***interface-number*
12. **memberatm***interface-number***pvp***vpi*
13. **end**
14. **showatmvp**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**interfaceatm***slot*/*subslot*/*port*[**.***subinterface*] 例： `Router(config)# interface atm1/0/0`	インターフェイスを定義し、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	**atmpvp***vpi***l2transport** 例： `Router(config-if)# atm pvp 1 l2transport`	PVP を ATM セルの転送専用にすることを指定し、L2transport PVP コンフィギュレーション モードを開始します。 • **l2transport** キーワードは、PVP がセルリレー用であることを示します。このモードは、レイヤ2トランスポート専用です。通常の PVP 用ではありません。
ステップ 5	**end** 例： `Router(config-if-atm-l2trans-pvc)# end`	特権 EXEC モードに戻ります。
ステップ 6	**interfacepseudowire***number* 例： `Router(config)# interface pseudowire 100`	擬似回線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 7	**encapsulationmpls** 例： `Router(config-if)# encapsulation mpls`	マルチプロトコル ラベル スイッチング（MPLS）がデータ カプセル化方式として使用されることを指定します。
ステップ 8	**neighbor***peer-addressvcid-value* 例： `Router(config-if)# neighbor 10.0.0.1 123`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 9	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 10	**l2vpnxconnectcontext***context-name* 例： `Router(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect 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 11	**memberpseudowire***interface-number* 例： `Router(config-xconnect)# member pseudowire 100`	Layer 2 VPN（L2VPN）クロス コネクトを形成するようにメンバー擬似回線を指定します。
ステップ 12	**memberatm***interface-number***pvp***vpi* 例： `Device(config-xconnect)# member atm 100 pvp 1`	ATM メンバー インターフェイスのロケーションを指定します。
ステップ 13	**end** 例： `Router(config-xconnect)# end`	特権 EXEC モードに戻ります。
ステップ 14	**showatmvp** 例： `Router# show atm vp`	OAM セル エミュレーションが ATM VP で有効になっていることを示す出力を表示します。

例

次に示す **showatmvp** コマンドの出力には、インターフェイスが VP モードのセルリレー用に設定されていることが示されています。

```
Router# show atm vp 1
ATM5/0  VPI: 1, Cell Relay, PeakRate: 149760, CesRate: 0, DataVCs: 1, CesVCs: 0, Status:
ACTIVE
  VCD    VCI   Type   InPkts   OutPkts   AAL/Encap     Status
  6      3     PVC    0        0         F4 OAM        ACTIVE
  7      4     PVC    0        0         F4 OAM        ACTIVE
TotalInPkts: 0, TotalOutPkts: 0, TotalInFast: 0, TotalOutFast: 0,
TotalBroadcasts: 0 TotalInPktDrops: 0, TotalOutPktDrops: 0
```

Ethernet over MPLS の設定

異なる場所にある2つのVLANネットワークを接続するためのVLANモードのEthernet over MPLS の設定。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacegigabitethernet***slot*/*subslot*/*port*[**.** *subinterface*]
4. **encapsulationdot1q***vlan-id*
5. **xconnect***peer-router-idvcid***encapsulationmpls**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**interfacegigabitethernet***slot*/*subslot*/*port*[**.** *subinterface*] 例： `Router(config)# interface gigabitethernet4/0/0.1`	ギガビット イーサネット サブインターフェイスを指定し、サブインターフェイス コンフィギュレーション モードを開始します。 • 隣接している CE ルータのサブインターフェイスが、この PE ルータと同じ VLAN にあることを確認します。
ステップ 4	**encapsulationdot1q***vlan-id* 例： `Router(config-subif)# encapsulation dot1q 100`	サブインターフェイスでの 802.1Q VLAN パケットの受信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 5	**xconnect***peer-router-idvcid***encapsulationmpls** 例： `Router(config-subif)# xconnect 10.0.0.1 123 encapsulation mpls`	接続回線を擬似接続 VC にバインドします。

L2VPN プロトコルベースの CLI 機能と関連するコマンドを使用する、異なる場所にある 2 つの VLAN ネットワークを接続するための VLAN モードの Ethernet over MPLS の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacegigabitethernet***slot*/*subslot*/*port*[**.***subinterface*]
4. **encapsulationdot1q***vlan-id*
5. **end**
6. **interfacepseudowire***number*
7. **encapsulationmpls**
8. **neighbor***peer-addressvcid-value*
9. **exit**
10. **l2vpn xconnectcontext***context-name*
11. **member pseudowire***interface-number*
12. **member gigabitethernet***interface-number*
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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 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	**interfacegigabitethernet***slot*/*subslot*/*port*[**.***subinterface*] 例： `Router(config)# interface gigabitethernet4/0/0.1`	ギガビット イーサネット サブインターフェイスを指定し、サブインターフェイス コンフィギュレーション モードを開始します。 • 隣接しているCEルータのサブインターフェイスが、この PE ルータと同じ VLAN にあることを確認します。
ステップ 4	**encapsulationdot1q***vlan-id* 例： `Router(config-subif)# encapsulation dot1q 100`	サブインターフェイスでの 802.1Q VLAN パケットの受信をイネーブルにします。
ステップ 5	**end** 例： `Router(config-subif)# end`	特権 EXEC モードに戻ります。
ステップ 6	**interfacepseudowire***number* 例： `Router(config)# interface pseudowire 100`	擬似回線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 7	**encapsulationmpls** 例： `Router(config-if)# encapsulation mpls`	マルチプロトコル ラベル スイッチング（MPLS）がデータ カプセル化方式として使用されることを指定します。
ステップ 8	**neighbor***peer-addressvcid-value* 例： `Router(config-if)# neighbor 10.0.0.1 123`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 9	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 10	**l2vpn xconnectcontext***context-name* 例： `Router(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect コンフィギュレーション モードを開始します。
ステップ 11	**member pseudowire***interface-number* 例： `Router(config-xconnect)# member pseudowire 100`	Layer 2 VPN（L2VPN）クロス コネクトを形成するようにメンバー擬似回線を指定します。
ステップ 12	**member gigabitethernet***interface-number* 例： `Router(config-xconnect)# member GigabitEthernet0/0/0.1`	ギガビット イーサネット メンバー インターフェイスのロケーションを指定します。
ステップ 13	**end** 例： `Router(config-xconnect)# end`	特権 EXEC モードに戻ります。

ポート モードでの Ethernet over MPLS の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacegigabitethernet***slot*/*subslot*/*port*
4. **xconnect***peer-router-idvcid***encapsulationmpls**
5. **end**
6. **showmplsl2transportvc**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Router> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**interfacegigabitethernet***slot*/*subslot*/*port* 例：	ギガビット イーサネット 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	**xconnect***peer-router-idvcid***encapsulationmpls** 例： `Router(config-if)# xconnect 10.0.0.1 123 encapsulation mpls`	接続回線を擬似接続 VC にバインドします。
ステップ 5	**end** 例： `Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**showmplsl2transportvc** 例： `Router# show mpls l2transport vc`	Ethernet over MPLS ポート モードの情報を表示します。

L2VPNプロトコルベースのCLI機能に関連付けられたコマンドを使用したポートモードでの Ethernet over MPLS の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacegigabitethernet***slot*/*subslot*/*port*[**.***subinterface*]
4. **end**
5. **interfacepseudowire***number*
6. **encapsulationmpls**
7. **neighbor***peer-addressvcid-value*
8. **exit**
9. **l2vpnxconnectcontext***context-name*
10. **memberpseudowire***interface-number*
11. **membergigabitethernet***interface-number*
12. **end**
13. **end**
14. **showl2vpnatomvc**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**interfacegigabitethernet***slot*/*subslot*/*port*[**.***subinterface*] 例： `Device(config)# interface gigabitethernet4/0/0`	ギガビットイーサネット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。 • 隣接している CE ルータのインターフェイスが、この PE ルータと同じ VLAN にあることを確認します。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 5	**interfacepseudowire***number* 例： `Device(config)# interface pseudowire 100`	擬似回線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 6	**encapsulationmpls** 例： `Device(config-if)# encapsulation mpls`	マルチプロトコル ラベル スイッチング（MPLS）がデータ カプセル化方式として使用されることを指定します。
ステップ 7	**neighbor***peer-addressvcid-value* 例： `Device(config-if)# neighbor 10.0.0.1 123`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 8	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 9	**l2vpnxconnectcontext***context-name* 例： `Device(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect コンフィギュレーション モードを開始します。
ステップ 10	**memberpseudowire***interface-number* 例： `Device(config-xconnect)# member pseudowire 100`	Layer 2 VPN（L2VPN）クロス コネクトを形成するようにメンバー擬似回線を指定します。
ステップ 11	**membergigabitethernet***interface-number* 例： `Device(config-xconnect)# member GigabitEthernet0/0/0.1`	ギガビット イーサネット メンバー インターフェイスのロケーションを指定します。

	コマンドまたはアクション	目的
ステップ 12	**end** 例： `Device(config-xconnect)# end`	特権 EXEC モードに戻ります。
ステップ 13	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 14	**showl2vpnatomvc** 例： `Device# show l2vpn atom vc`	Ethernet over MPLS ポート モードの情報を表示します。

VLAN ID 書き換えを伴う Ethernet over MPLS の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacegigabitethernet***slot*/*subslot*/*port*
4. **encapsulationdot1q***vlan-id*
5. **xconnect***peer-router-idvcid***encapsulationmpls**
6. **remotecircuitid***remote-vlan-id*
7. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 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	**interfacegigabitethernet***slot*/*subslot*/*port* 例：	ギガビット イーサネット サブインターフェイスを指定し、サブインターフェイス 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	**encapsulationdot1q***vlan-id* 例： `Router(config-subif)# encapsulation dot1q 100`	サブインターフェイスでの 802.1Q VLAN パケットの受信をイネーブルにします。
ステップ 5	**xconnect***peer-router-idvcid***encapsulationmpls** 例： `Router(config-subif)# xconnect 10.0.0.1 123 encapsulation mpls`	接続回線を擬似回線 VC にバインドし、xconnect コンフィギュレーション モードを開始します。
ステップ 6	**remotecircuitid***remote-vlan-id* 例： `Router(config-subif-xconn)# remote circuit id 101`	（任意）トンネルの両端で異なる VLAN ID を持つ VLAN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	**end** 例： `Router(config-subif-xconn)# end`	特権 EXEC モードに戻ります。

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した VLAN ID 書き換えを伴う Ethernet over MPLS の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **encapsulationdot1q***vlan-id*
4. **end**
5. **interfacepseudowire***number*
6. **encapsulationmpls**
7. **neighbor***peer-addressvcid-value*
8. **exit**
9. **l2vpnxconnectcontext***context-name*
10. **memberpseudowire***interface-number*
11. **membergigabitethernet***interface-number*
12. **remotecircuitid***remote-vlan-id*
13. **end**
14. **showcontrollerseomplsforwarding-table**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**encapsulationdot1q***vlan-id* 例： `Router(config-subif)# encapsulation dot1q 100`	サブインターフェイスでの 802.1Q VLAN パケットの受信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 4	**end** 例： `Router(config-subif)# end`	特権 EXEC モードに戻ります。
ステップ 5	**interfacepseudowire***number* 例： `Router(config)# interface pseudowire 100`	擬似回線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 6	**encapsulationmpls** 例： `Router(config-if)# encapsulation mpls`	マルチプロトコル ラベル スイッチング（MPLS）がデータ カプセル化方式として使用されることを指定します。
ステップ 7	**neighbor***peer-addressvcid-value* 例： `Router(config-if)# neighbor 10.0.0.1 123`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 8	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 9	**l2vpnxconnectcontext***context-name* 例： `Router(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect コンフィギュレーション モードを開始します。
ステップ 10	**memberpseudowire***interface-number* 例： `Router(config-xconnect)# member pseudowire 100`	Layer 2 VPN（L2VPN）クロス コネクトを形成するようにメンバー擬似回線を指定します。
ステップ 11	**membergigabitethernet***interface-number* 例： `Router(config-xconnect)# member GigabitEthernet0/0/0.1`	ギガビット イーサネット メンバー インターフェイスのロケーションを指定します。

	コマンドまたはアクション	目的
ステップ 12	**remotecircuitid***remote-vlan-id* 例： `Router(config-xconnect)# remote circuit id 101`	（任意）トンネルの両端で異なる VLAN ID を持つ VLANインターフェイスを使用できるようにします。
ステップ 13	**end** 例： `Router(config-xconnect)# end`	特権 EXEC モードに戻ります。
ステップ 14	**showcontrollerseomplsforwarding-table** 例： `Router# show controllers eompls forwarding-table`	VLAN ID の書き換えに関する情報を表示します。

Ethernet over MPLS 用のサブインターフェイスごとの MTU の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacegigabitethernet***slot*/*subslot*/*port*[**.** *subinterface*]
4. **mtu***mtu-value*
5. **interfacegigabitethernet***slot*/*subslot*/*port*[**.***subinterface*]
6. **encapsulationdot1q***vlan-id*
7. **xconnect***peer-router-idvcid***encapsulationmpls**
8. **mtu***mtu-value*
9. **end**
10. **showmplsl2transportbinding**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Router> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**interfacegigabitethernet***slot*/*subslot*/*port*[**.** *subinterface*] 例： `Router(config)# interface gigabitethernet4/0/0`	ギガビット イーサネット 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	**mtu***mtu-value* 例： `Router(config-if)# mtu 2000`	インターフェイスの MTU 値を指定します。インターフェイス レベルで指定された MTU 値は、サブインターフェイスで継承できます。
ステップ 5	**interfacegigabitethernet***slot*/*subslot*/*port*[**.***subinterface*] 例： `Router(config-if)# interface gigabitethernet4/0/0.1`	ギガビット イーサネット サブインターフェイスを指定し、サブインターフェイス コンフィギュレーション モードを開始します。 隣接している CE ルータのサブインターフェイスが、この PE ルータと同じ VLAN にあることを確認します。
ステップ 6	**encapsulationdot1q***vlan-id* 例： `Router(config-subif)# encapsulation dot1q 100`	サブインターフェイスでの 802.1Q VLAN パケットの受信をイネーブルにします。 Ethernet over MPLS が稼働している CE ルータと PE ルータ間のサブインターフェイスは、同じサブネット内になければなりません。他のすべてのサブインターフェイスおよびバックボーン ルータについては、その必要はありません。
ステップ 7	**xconnect***peer-router-idvcid***encapsulationmpls** 例： `Router(config-subif)# xconnect 10.0.0.1 123 encapsulation mpls`	接続回線を擬似接続 VC にバインドします。 このコマンドの構文は、その他のレイヤ 2 トランスポートの場合と同じです。xconnect サブインターフェイス 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 8	**mtu***mtu-value* 例： `Router(config-if-xconn)# mtu 1400`	VC の MTU を指定します。
ステップ 9	**end** 例： `Router(config-if-xconn)# end`	特権 EXEC モードに戻ります。
ステップ 10	**showmplsl2transportbinding** 例： `Router# show mpls l2transport binding`	ローカルおよびリモート インターフェイスに割り当てられた MTU 値を表示します。

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した Ethernet over MPLS 用のサブインターフェイスごとの MTU の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacegigabitethernet***slot*/*subslot*/*port*[**.***subinterface*]
4. **mtu***mtu-value*
5. **interfacegigabitethernet***slot*/*subslot*/*port*[**.***subinterface*]
6. **encapsulationdot1q***vlan-id*
7. **end**
8. **interfacepseudowire***number*
9. **encapsulationmpls**
10. **neighbor***peer-addressvcid-value*
11. **mtu***mtu-value*
12. **exit**
13. **l2vpn xconnectcontext***context-name*
14. **member pseudowire***interface-number*
15. **member gigabitethernet***interface-number*
16. **end**
17. **showl2vpnatombinding**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**interfacegigabitethernet***slot*/*subslot*/*port*[**.***subinterface*] 例： `Device(config)# interface gigabitethernet4/0/0`	ギガビット イーサネット 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	**mtu***mtu-value* 例： `Device(config-if)# mtu 2000`	インターフェイスの MTU 値を指定します。インターフェイス レベルで指定された MTU 値は、サブインターフェイスで継承できます。
ステップ 5	**interfacegigabitethernet***slot*/*subslot*/*port*[**.***subinterface*] 例： `Device(config-if)# interface gigabitethernet4/0/0.1`	ギガビット イーサネット サブインターフェイスを指定し、サブインターフェイス コンフィギュレーション モードを開始します。 隣接している CE ルータのサブインターフェイスが、この PE ルータと同じ VLAN にあることを確認します。
ステップ 6	**encapsulationdot1q***vlan-id* 例： `Device(config-subif)# encapsulation dot1q 100`	サブインターフェイスでの 802.1Q VLAN パケットの受信をイネーブルにします。 Ethernet over MPLS が稼働している CE ルータと PE ルータ間のサブインターフェイスは、同じサブネット内になければなりません。他のすべてのサブインターフェイスおよびバックボーン ルータについては、その必要はありません。
ステップ 7	**end** 例： `Device(config-subif)# end`	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
ステップ 8	**interfacepseudowire***number* 例： `Device(config)# interface pseudowire 100`	擬似回線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 9	**encapsulationmpls** 例： `Device(config-if)# encapsulation mpls`	マルチプロトコル ラベル スイッチング（MPLS）がデータ カプセル化方式として使用されることを指定します。
ステップ 10	**neighbor***peer-addressvcid-value* 例： `Device(config-if)# neighbor 10.0.0.1 123`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 11	**mtu***mtu-value* 例： `Device(config-if)# mtu 1400`	VC の MTU を指定します。
ステップ 12	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 13	**l2vpn xconnectcontext***context-name* 例： `Device(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect コンフィギュレーション モードを開始します。
ステップ 14	**member pseudowire***interface-number* 例： `Device(config-xconnect)# member pseudowire 100`	Layer 2 VPN（L2VPN）クロス コネクトを形成するようにメンバー擬似回線を指定します。
ステップ 15	**member gigabitethernet***interface-number* 例： `Device(config-xconnect)# member GigabitEthernet0/0/0.1`	ギガビット イーサネット メンバー インターフェイスのロケーションを指定します。

	コマンドまたはアクション	目的
ステップ 16	**end** 例： `Device(config-xconnect)# end`	特権 EXEC モードに戻ります。
ステップ 17	**showl2vpnatombinding** 例： `Device# show l2vpn atom binding`	Layer 2 VPN（L2VPN）Any Transport over MPLS（AToM）ラベル バインド情報を表示します。

Frame Relay over MPLS の設定

DLCI 間接続を使用した Frame Relay over MPLS の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **frame-relayswitching**
4. **interfaceserial***slot*/*subslot*/*port*[**.***subinterface*]
5. **encapsulationframe-relay**[**cisco** | **ietf**]
6. **frame-relayintf-typedce**
7. **exit**
8. **connect***connection-nameinterfacedlci***l2transport**
9. **xconnect***peer-router-idvcid***encapsulationmpls**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 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	**frame-relayswitching** 例： `Router(config)# frame-relay switching`	フレーム リレー デバイスの PVC スイッチングをイネーブルにします。
ステップ 4	**interfaceserial***slot*/*subslot*/*port*[**.***subinterface*] 例： `Router(config)# interface serial3/1/0`	シリアル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 5	**encapsulationframe-relay**[**cisco** | **ietf**] 例： `Router(config-if)# encapsulation frame-relay ietf`	インターフェイスのフレームリレーカプセル化を指定します。さまざまなカプセル化タイプを指定できます。1 つのインターフェイスをシスコのカプセル化に設定し、もう 1 つのインターフェイスを IETF のカプセル化に設定できます。
ステップ 6	**frame-relayintf-typedce** 例： `Router(config-if)# frame-relay intf-type dce`	インターフェイスがDCEスイッチであることを指定します。また、ネットワーク間インターフェイス（NNI）およびDTE接続をサポートするようにインターフェイスを指定することもできます。
ステップ 7	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 8	**connect***connection-nameinterfacedlci***l2transport** 例： `Router(config)# connect fr1 serial5/0 1000 l2transport`	フレーム リレー PVC 間の接続を定義し、接続コンフィギュレーション モードを開始します。**l2transport** キーワードを使用して、PVCがローカルにスイッチングされずに、バックボーン ネットワーク上でトンネリングされるように指定します。 *connection-name* 引数は、指定するテキスト文字列です。 *interface* 引数は、PVC 接続が定義されるインターフェイスです。 *dlci* 引数は、接続される PVC の DLCI 番号です。

	コマンドまたはアクション	目的
ステップ 9	**xconnect***peer-router-idvcid***encapsulationmpls** 例： `Router(config-fr-pw-switching)# xconnect 10.0.0.1 123 encapsulation mpls`	レイヤ 2 パケットを転送するための VC を作成します。DLCI 間接続タイプでは、Frame Relay over MPLS は接続コンフィギュレーション モードで **xconnect** コマンドを使用します。

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した DLCI 間接続を伴う Relay over MPLS の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **frame-relayswitching**
4. **interfaceserial***slot*/*subslot*/*port*[**.** *subinterface*]
5. **encapsulationframe-relay**[**cisco** | **ietf**]
6. **frame-relayintf-typedce**
7. **exit**
8. **connect***connection-nameinterfacedlci***l2transport**
9. **end**
10. **interfacepseudowire***number*
11. **encapsulationmpls**
12. **neighbor***peer-addressvcid-value*
13. **exit**
14. **l2vpn xconnectcontext***context-name*
15. **member pseudowire***interface-number*
16. **member** *ip-addressvc-id***encapsulation mpls**
17. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 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	**frame-relayswitching** 例： `Router(config)# frame-relay switching`	フレームリレーデバイスのPVCスイッチングをイネーブルにします。
ステップ 4	**interfaceserial***slot*/*subslot*/*port*[**.** *subinterface*] 例： `Router(config)# interface serial3/1/0`	シリアル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 5	**encapsulationframe-relay**[**cisco** | **ietf**] 例： `Router(config-if)# encapsulation frame-relay ietf`	インターフェイスのフレームリレーカプセル化を指定します。さまざまなカプセル化タイプを指定できます。1 つのインターフェイスをシスコのカプセル化に設定し、もう 1 つのインターフェイスを IETF のカプセル化に設定できます。
ステップ 6	**frame-relayintf-typedce** 例： `Router(config-if)# frame-relay intf-type dce`	インターフェイスがDCEスイッチであることを指定します。また、ネットワーク間インターフェイス（NNI）およびDTE接続をサポートするようにインターフェイスを指定することもできます。
ステップ 7	**exit** 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ます。
ステップ 8	**connect***connection-nameinterfacedlci***l2transport** 例： `Router(config)# connect fr1 serial5/0 1000 l2transport`	フレームリレーPVC間の接続を定義し、接続コンフィギュレーションモードを開始します。**l2transport** キーワードを使用して、PVCがローカルにスイッチングされずに、バックボーンネットワーク上でトンネリングされるように指定します。 *connection-name* 引数は、指定するテキスト文字列です。 *interface* 引数は、PVC 接続が定義されるインターフェイスです。 *dlci* 引数は、接続される PVC の DLCI 番号です。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： `Router(config-xconnect-conn-config)# end`	特権 EXEC モードに戻ります。
ステップ 10	**interfacepseudowire***number* 例： `Router(config)# interface pseudowire 100`	擬似回線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 11	**encapsulationmpls** 例： `Router(config-if)# encapsulation mpls`	マルチプロトコル ラベル スイッチング（MPLS）がデータ カプセル化方式として使用されることを指定します。
ステップ 12	**neighbor***peer-addressvcid-value* 例： `Router(config-if)# neighbor 10.0.0.1 123`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 13	**exit** 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ます。
ステップ 14	**l2vpn xconnectcontext***context-name* 例： `Router(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect コンフィギュレーション モードを開始します。
ステップ 15	**member pseudowire***interface-number* 例： `Router(config-xconnect)# member pseudowire 100`	Layer 2 VPN（L2VPN）クロス コネクトを形成するようにメンバー擬似回線を指定します。
ステップ 16	**member** *ip-addressvc-id***encapsulation mpls** 例： `Router(config-xconnect)# member 10.0.0.1 123 encapsulation mpls`	レイヤ2パケットを転送するためのVCを作成します。

	コマンドまたはアクション	目的
ステップ 17	**end** 例： `Router(config-xconnect)# end`	特権 EXEC モードに戻ります。

ポート間接続を使用した Frame Relay over MPLS の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfaceserial***slot*/*subslot*/*port*[**.** *subinterface*]
4. **encapsulationhdlc**
5. **xconnect***peer-router-idvcid***encapsulationmpls**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**interfaceserial***slot*/*subslot*/*port*[**.** *subinterface*] 例： `Router(config)# interface serial5/0/0`	シリアル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	**encapsulationhdlc** 例： `Router(config-if)# encapsulation hdlc`	フレーム リレー PDU が HDLC パケットにカプセル化されることを指定します。

	コマンドまたはアクション	目的
ステップ 5	**xconnect***peer-router-idvcid***encapsulationmpls** 例： `Router(config-if)# xconnect 10.0.0.1 123 encapsulation mpls`	レイヤ 2 パケットを転送するための VC を作成します。

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用したポート間接続を伴う Relay over MPLS の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfaceserial***slot*/*subslot*/*port*[**.** *subinterface*]
4. **encapsulationhdlc**
5. **end**
6. **interfacepseudowire***number*
7. **encapsulationmpls**
8. **neighbor***peer-addressvcid-value*
9. **exit**
10. **l2vpn xconnectcontext***context-name*
11. **member pseudowire***interface-number*
12. **member** *ip-addressvc-id***encapsulation mpls**
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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 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	**interfaceserial***slot*/*subslot*/*port*[**.** *subinterface*] 例： `Router(config)# interface serial5/0/0`	シリアル 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	**encapsulationhdlc** 例： `Router(config-if)# encapsulation hdlc`	フレーム リレー PDU が HDLC パケットにカプセル化されることを指定します。
ステップ 5	**end** 例： `Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**interfacepseudowire***number* 例： `Router(config)# interface pseudowire 100`	擬似回線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 7	**encapsulationmpls** 例： `Router(config-if)# encapsulation mpls`	マルチプロトコル ラベル スイッチング（MPLS）がデータ カプセル化方式として使用されることを指定します。
ステップ 8	**neighbor***peer-addressvcid-value* 例： `Router(config-if)# neighbor 10.0.0.1 123`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 9	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 10	**l2vpn xconnectcontext***context-name* 例： `Router(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect コンフィギュレーション モードを開始します。
ステップ 11	**member pseudowire***interface-number* 例： `Router(config-xconnect)# member pseudowire 100`	Layer 2 VPN（L2VPN）クロス コネクトを形成するようにメンバー擬似回線を指定します。
ステップ 12	**member** *ip-addressvc-id***encapsulation mpls** 例： `Router(config-xconnect)# member 10.0.0.1 123 encapsulation mpls`	レイヤ 2 パケットを転送するための VC を作成します。
ステップ 13	**end** 例： `Router(config-xconnect)# end`	特権 EXEC モードに戻ります。

HDLC または PPP over MPLS の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfaceserial***slot*/*subslot*/*port*[**.***subinterface*]
4. 次のいずれかを実行します。
   - **encapsulationppp**
   - **encapsulationhdlc**
5. **xconnect***peer-router-idvcid***encapsulationmpls**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**interfaceserial***slot*/*subslot*/*port*[**.***subinterface*] 例： `Router(config)# interface serial5/0/0`	シリアル 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	次のいずれかを実行します。
	• **encapsulationppp**
	• **encapsulationhdlc**
	
	例：
	`Router(config-if)# encapsulation ppp`
	
	例：
	`or`
	
	例：
	
	例：
	`Router(config-if)# encapsulation hdlc`
		HDLC または PPP のカプセル化を指定して、接続コンフィギュレーション モードを開始します。

ステップ 5	**xconnect***peer-router-idvcid***encapsulationmpls** 例： `Router(config-fr-pw-switching)# xconnect 10.0.0.1 123 encapsulation mpls`	レイヤ 2 パケットを転送するための VC を作成します。

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した HDLC または PPP over MPLS の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfaceserial***slot*/*subslot*/*port*[**.** *subinterface*]
4. 次のいずれかを実行します。
   - **encapsulationppp**
   - **encapsulationhdlc**
5. **end**
6. **interfacepseudowire***number*
7. **encapsulationmpls**
8. **neighbor***peer-addressvcid-value*
9. **exit**
10. **l2vpn xconnectcontext***context-name*
11. **member pseudowire***interface-number*
12. **member** *ip-addressvc-id***encapsulation mpls**
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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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。

	コマンドまたはアクション	目的
ステップ 3	**interfaceserial***slot*/*subslot*/*port*[**.** *subinterface*] 例： `Router(config)# interface serial5/0/0`	シリアル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	次のいずれかを実行します。
	• **encapsulationppp**
	• **encapsulationhdlc**
	
	例：
	`Router(config-if)# encapsulation ppp`
	
	例：
	`Router(config-if)# encapsulation hdlc`
		HDLC または PPP のカプセル化を指定して、接続コンフィギュレーション モードを開始します。

ステップ 5	**end** 例： `Router(config-xconnect-conn-config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**interfacepseudowire***number* 例： `Router(config)# interface pseudowire 100`	擬似回線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 7	**encapsulationmpls** 例： `Router(config-if)# encapsulation mpls`	マルチプロトコル ラベル スイッチング（MPLS）がデータ カプセル化方式として使用されることを指定します。
ステップ 8	**neighbor***peer-addressvcid-value* 例： `Router(config-if)# neighbor 10.0.0.1 123`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 9	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 10	**l2vpn xconnectcontext***context-name* 例： `Router(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect コンフィギュレーションモードを開始します。
ステップ 11	**member pseudowire***interface-number* 例： `Router(config-xconnect)# member pseudowire 100`	Layer 2 VPN（L2VPN）クロス コネクトを形成するようにメンバー擬似回線を指定します。
ステップ 12	**member** *ip-addressvc-id***encapsulation mpls** 例： `Router(config-xconnect)# member 10.0.0.1 123 encapsulation mpls`	レイヤ 2 パケットを転送するための VC を作成します。
ステップ 13	**end** 例： `Router(config-xconnect)# end`	特権 EXEC モードに戻ります。

トンネル選択の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **pseudowire-class***name*
4. **encapsulationmpls**
5. **preferred-path**{**interfacetunnel***tunnel-number* | **peer**{*ip-address* | *host-name*}} [**disable-fallback**]
6. **exit**
7. **interface***typeslot*/*subslot*/*port*
8. **encapsulation***encapsulation-type*
9. **xconnect***peer-router-idvcid***pw-class***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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**pseudowire-class***name* 例： `Router(config)# pseudowire-class ts1`	指定した名前で擬似回線クラスを作成し、擬似回線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	**encapsulationmpls** 例： `Router(config-pw)# encapsulation mpls`	トンネリング カプセル化を指定します。AToM の場合、カプセル化タイプは mpls です。
ステップ 5	**preferred-path** {**interfacetunnel***tunnel-number* | **peer** {*ip-address* | *host-name*}} [**disable-fallback**] 例： `Router(config-pw)# preferred path peer 10.18.18.18`	優先パスとして使用される MPLS トラフィック エンジニアリング トンネルまたは IP アドレスかホスト名を指定します。
ステップ 6	**exit** 例： `Router(config-pw)# exit`	擬似回線コンフィギュレーションモードを終了して、トンネル選択機能を有効にします。
ステップ 7	**interface***typeslot*/*subslot*/*port* 例： `Router(config)# interface atm1/1/0`	インターフェイス タイプを指定して、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 8	**encapsulation***encapsulation-type* 例： `Router(config-if)# encapsulation aal5`	インターフェイスのカプセル化を指定します。
ステップ 9	**xconnect***peer-router-idvcid***pw-class***name* 例： `Router(config-if)# xconnect 10.0.0.1 123 pw-class ts1`	接続回線を擬似接続 VC にバインドします。

例

次に、**showmplsl2transportvc** コマンドの出力に次のような VC に関する情報が表示される例を示します。

- VC 101 は、Tunnel1 という名前の優先パスに割り当てられています。優先パスによって、優先パスで障害が発生した場合にデフォルトパスを使用しないように指定されているため、デフォルト パスはディセーブルになっています。
- VC 150 は、PE2 のループバック アドレスの IP アドレスに割り当てられています。優先パスで障害が発生した場合、デフォルト パスを使用できます。

太字のコマンド出力は優先パス情報を示します。

```
Router# show mpls l2transport vc detail
Local interface: Gi0/0/0.1 up, line protocol up, Eth VLAN 222 up
  Destination address: 10.16.16.16, VC ID: 101, VC status: up
    Preferred path: Tunnel1,  active
    Default path: disabled
    Tunnel label: 3, next hop point2point
    Output interface: Tu1, imposed label stack {17 16}
  Create time: 00:27:31, last status change time: 00:27:31
  Signaling protocol: LDP, peer 10.16.16.16:0 up
    MPLS VC labels: local 25, remote 16
    Group ID: local 0, remote 6
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 10, send 10
    byte totals:   receive 1260, send 1300
    packet drops:  receive 0, send 0
Local interface: ATM1/0/0 up, line protocol up, ATM AAL5 0/50 up
  Destination address: 10.16.16.16, VC ID: 150, VC status: up
    Preferred path: 10.18.18.18, active
    Default path: ready
    Tunnel label: 3, next hop point2point
    Output interface: Tu2, imposed label stack {18 24}
  Create time: 00:15:08, last status change time: 00:07:37
  Signaling protocol: LDP, peer 10.16.16.16:0 up
    MPLS VC labels: local 26, remote 24
    Group ID: local 2, remote 0
```

```
    MTU: local 4470, remote 4470
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 0, send 0
    byte totals:   receive 0, send 0
    packet drops:  receive 0, send 0
```

トラブルシューティングのヒント

ATM セル パッキングをデバッグするには、**debugatmcell-packing** コマンドを発行します。

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用したトンネル選択の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **templatetypepseudowire***name*
4. **encapsulationmpls**
5. **preferred-path**{**interfacetunnel***tunnel-number* | **peer** {*ip-address* | *hostname*}} [**disable-fallback**]
6. **exit**
7. **interface***typeslot*/*subslot*/*port*[**.***subinterface*]
8. **encapsulation***encapsulation-type*
9. **end**
10. **interfacepseudowire***number*
11. **sourcetemplatetypepseudowire***name*
12. **neighbor***peer-addressvcid-value*
13. **end**
14. **l2vpnxconnectcontext***context-name*
15. **memberpseudowire***interface-number*
16. **member***ip-addressvc-id***encapsulation mpls**
17. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 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	**templatetypepseudowire***name* 例： `Router(config)# template type pseudowire ts1`	指定した名前でテンプレート擬似回線を構築して、擬似回線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	**encapsulationmpls** 例： `Router(config-pw)# encapsulation mpls`	トンネリング カプセル化を指定します。AToM の場合、カプセル化タイプは mpls です。
ステップ 5	**preferred-path** {**interfacetunnel***tunnel-number* | **peer** {*ip-address* | *hostname*}} [**disable-fallback**] 例： `Router(config-pw)# preferred path peer 10.18.18.18`	優先パスとして使用される MPLS トラフィック エンジニアリング トンネルまたは IP アドレスかホスト名を指定します。
ステップ 6	**exit** 例： `Router(config-pw)# exit`	擬似回線コンフィギュレーション モードを終了して、トンネル選択機能を有効にします。
ステップ 7	**interface***typeslot*/*subslot*/*port*[**.***subinterface*] 例： `Router(config)# interface atm1/1/0`	インターフェイス タイプを設指定して、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 8	**encapsulation***encapsulation-type* 例： `Router(config-if)# encapsulation aal5`	インターフェイスのカプセル化を指定します。
ステップ 9	**end** 例： `Router(config-if)# end`	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
ステップ 10	**interfacepseudowire***number* 例： `Router(config)# interface pseudowire 100`	擬似回線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 11	**sourcetemplatetypepseudowire***name* 例： `Router(config-if)# source template type pseudowire ts1`	ts1 という名前のタイプ擬似回線のソーステンプレートを設定します。
ステップ 12	**neighbor***peer-addressvcid-value* 例： `Router(config-if)#  neighbor 10.0.0.1 123`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 13	**end** 例： `Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 14	**l2vpnxconnectcontext***context-name* 例： `Router(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect コンフィギュレーション モードを開始します。
ステップ 15	**memberpseudowire***interface-number* 例： `Router(config-xconnect)# member pseudowire 100`	Layer 2 VPN（L2VPN）クロス コネクトを形成するようにメンバー擬似回線を指定します。
ステップ 16	**member***ip-addressvc-id***encapsulation mpls** 例： `Router(config-xconnect)# member 10.0.0.1 123 encapsulation mpls`	レイヤ 2 パケットを転送するための VC を作成します。
ステップ 17	**end** 例： `Router(config-xconnect)# end`	特権 EXEC モードに戻ります。

トラブルシューティングのヒント（L2VPN プロトコルベースの CLI 機能に関連するコマンドを使用）

debug l2vpn atom vc event コマンドを使用すると、トンネル選択をトラブルシューティングできます。たとえば、優先パスに使用されているトンネル インターフェイスがシャットダウンされている場合、デフォルト パスがイネーブルになります。**debug l2vpn atom vc event** コマンドを使用すると、次のような出力が表示されます。

```
AToM SMGR [10.2.2.2, 101]: Processing imposition update, vc_handle 62091860, update_action
 3, remote_vc_label 16
AToM SMGR [10.2.2.2, 101]: selected route no parent rewrite: tunnel not up
AToM SMGR [10.2.2.2, 101]: Imposition Programmed, Output Interface: Et3/2
```

AToM を使用した Experimental ビットの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **class-map***class-name*
4. **matchany**
5. **policy-map***policy-name*
6. **class***class-name*
7. **setmplsexperimental***value*
8. **exit**
9. **exit**
10. **interface***typeslot*/*subslot*/*port*
11. **service-policyinput***policy-name*
12. **end**
13. **showpolicy-mapinterface***interface-name* [*vc* [*vpi*/]*vci*] [**dlci***dlci*] [**input** | **output**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 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	**class-map***class-name* 例： `Router(config)# class-map class1`	トラフィック クラスのユーザ定義名を指定し、クラス マップ 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	**matchany** 例： `Router(config-cmap)# match any`	マッチングするすべてのパケットを指定します。**any** キーワードだけを使用します。他のキーワードを使用すると、予期しない結果になる可能性があります。
ステップ 5	**policy-map***policy-name* 例： `Router(config-cmap)# policy-map policy1`	設定するトラフィック ポリシーの名前を指定し、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 6	**class***class-name* 例： `Router(config-pmap)# class class1`	トラフィックをトラフィック ポリシーに分類するために使用される **class-map** コマンドを使用して設定された事前定義のトラフィック クラスの名前を指定して、ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 7	**setmplsexperimental***value* 例： `Router(config-pmap-c)# set mpls experimental 7`	パケットが指定したポリシー マップに一致する場合に MPLS ビットを設定する値を指定します。
ステップ 8	**exit** 例： `Router(config-pmap-c)# exit`	ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 9	**exit** 例： `Router(config-pmap)# exit`	ポリシーマップ コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 10	**interface***typeslot*/*subslot*/*port* 例： `Router(config)# interface atm1/0/0`	インターフェイス タイプを指定して、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 11	**service-policyinput***policy-name* 例： `Router(config-if)# service-policy input policy1`	インターフェイスにトラフィック ポリシーを対応付けます。
ステップ 12	**end** 例： `Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 13	**showpolicy-mapinterface***interface-name* [*vc* [*vpi*/]*vci*] [**dlci***dlci*] [**input** | **output**] 例： `Router# show policy-map interface serial3/0/0`	インターフェイスに対応付けられたトラフィック ポリシーを表示します。

コントロール ワードの有効化

手順の概要

1. イネーブル化
2. **configureterminal**
3. **pseudowire-class cw_enable**
4. **encapsulationmpls**
5. **control-word**
6. **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	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Router> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**pseudowire-class cw_enable** 例： `Router(config)# pseudowire-class cw_enable`	擬似回線クラス 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	**encapsulationmpls** 例： `Router(config-pw-class)# encapsulation mpls`	トンネリング カプセル化を指定します。 • AToM の場合、カプセル化タイプは MPLS です。
ステップ 5	**control-word** 例： `Router(config-pw-class)# control-word`	コントロール ワードをイネーブルにします。
ステップ 6	**end** 例： `Router(config-pw-class)# end`	特権 EXEC モードに戻ります。

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用したコントロール ワードの有効化

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface pseudowire***number*
4. **encapsulationmpls**
5. **control-word include**
6. **neighbor***peer-address vcid-value*
7. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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 pseudowire***number* 例： `Router(config)# interface pseudowire 1`	指定した値でインターフェイス擬似回線を構築して、擬似回線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	**encapsulationmpls** 例： `Router(config-pw)# encapsulation mpls`	トンネリング カプセル化を指定します。 • AToM の場合、カプセル化タイプは mpls です。
ステップ 5	**control-word include** 例： `Router(config-pw)# control-word include`	コントロール ワード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 6	**neighbor***peer-address vcid-value* 例： `Router(config-pw)# neighbor 10.0.0.1 123`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 7	**end** 例： `Router(config-pw)# end`	特権 EXEC モードに戻ります。

MPLS AToM リモート イーサネット ポート シャットダウンの設定

（注） Any Transport over MPLS（AToM）：リモート イーサネット ポート シャットダウン機能は、サポートされている機能を含むイメージがルータにロードされたときに、デフォルトで自動的に有効になります。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **pseudowire-class** [*pw-class-name*]
4. **encapsulationmpls**
5. **exit**
6. **xconnect***peer-ip-addressvc-idpw-classpw-class-name*
7. **noremotelinkfailurenotification**
8. **remotelinkfailurenotification**
9. **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	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Router> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**pseudowire-class** [*pw-class-name*] 例： `Router(config)# pseudowire-class eompls`	レイヤ 2 擬似回線 クラスの名前を指定し、擬似回線 クラス 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	**encapsulationmpls** 例： `Router(config-pw)# encapsulation mpls`	擬似回線を経由したレイヤ 2 トラフィックのトンネリングにMPLSがデータ カプセル化方式として使用されることを指定します。
ステップ 5	**exit** 例： `Router(config-pw)# exit`	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 6	**xconnect***peer-ip-addressvc-idpw-classpw-class-name* 例： `Router(config-if)# xconnect 10.1.1.1 1 pw-class eompls`	接続回線を擬似回線にバインドし、Any Transport over MPLS（AToM）スタティック擬似回線を設定します。
ステップ 7	**noremotelinkfailurenotification** 例： `Router(config-if-xconn)# remote link failure notification`	MPLS AToM リモートリンク障害通知とシャットダウンを無効にします。
ステップ 8	**remotelinkfailurenotification** 例： `Router(config-if-xconn)# remote link failure notification`	MPLS AToM リモートリンク障害通知とシャットダウンを有効にします。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： `Router(config-if-xconn)# end`	特権 EXEC モードに戻ります。

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した MPLS AToM リモート イーサネット ポート シャットダウンの設定

（注） Any Transport over MPLS（AToM）：リモート イーサネット ポート シャットダウン機能は、サポートされている機能を含むイメージがルータにロードされたときに、デフォルトで自動的に有効になります。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **templatetypepseudowire** [*pseudowire-name*]
4. **encapsulationmpls**
5. **exit**
6. **interface***typeslot*/*subslot*/*port*
7. **interfacepseudowire***number*
8. **sourcetemplatetypepseudowire**
9. **neighbor***peer-addressvcid-value*
10. **end**
11. **l2vpnxconnectcontext***context-name*
12. **noremotelinkfailurenotification**
13. **remotelinkfailurenotification**
14. **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	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**templatetypepseudowire** [*pseudowire-name*] 例： `Device(config)# template type pseudowire eompls`	レイヤ 2 擬似回線 クラスの名前を指定し、擬似回線クラス 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	**encapsulationmpls** 例： `Device(config-pw)# encapsulation mpls`	擬似回線を経由したレイヤ 2 トラフィックのトンネリングに MPLS がデータ カプセル化方式として使用されることを指定します。
ステップ 5	**exit** 例： `Device(config-pw)# exit`	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 6	**interface***typeslot/subslot/port* 例： `Device(config)# interface GigabitEthernet1/0/0`	インターフェイス タイプを設定し、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 7	**interfacepseudowire***number* 例： `Device(config-if)# interface pseudowire 100`	擬似回線インターフェイスを指定します。
ステップ 8	**sourcetemplatetypepseudowire** 例： `Device(config-if)# source template type pseudowire eompls`	eompls という名前のタイプ擬似回線のソース テンプレートを設定します。

	コマンドまたはアクション	目的
ステップ 9	**neighbor***peer-addressvcid-value* 例： `Device(config-if)#  neighbor 10.1.1.1 1`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 10	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 11	**l2vpnxconnectcontext***context-name* 例： `Device(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect コンフィギュレーション モードを開始します。
ステップ 12	**noremotelinkfailurenotification** 例： `Device(config-xconnect)# no remote link failure notification`	MPLS AToM リモートリンク障害通知とシャットダウンを無効にします。
ステップ 13	**remotelinkfailurenotification** 例： `Device(config-xconnect)# remote link failure notification`	MPLS AToM リモートリンク障害通知とシャットダウンを有効にします。
ステップ 14	**end** 例： `Device(config-xconnect)# end`	特権 EXEC モードに戻ります。

単一 PW を使用した AToM ロード バランシングの設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **pseudowire-class***pw-class-name*
4. **encapsulation mpls**
5. **load-balance flow**
6. **xconnect***url***pw-class***pw-class-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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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	**pseudowire-class***pw-class-name* 例： `Router(config)# pseudowire-class ecmp-class`	指定した名前の擬似回線クラスを確立して、擬似回線クラス 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	**encapsulation mpls** 例： `Router(config-pw-class)# encapsulation mpls`	トンネリング カプセル化を指定します。 • AToM の場合、カプセル化タイプは mpls です。
ステップ 5	**load-balance flow** 例： `Router(config-pw-class)# load-balance flow`	ロード バランシングがフロー単位で実行されるように、単一の PW を使用した AToM ロード バランシング機能を有効にします。

	コマンドまたはアクション	目的
ステップ 6	**xconnect***url***pw-class***pw-class-name* 例： `Router(config-pw-class)# xconnect 10.0.0.1 pw-class ecmp-class`	接続回線を擬似回線仮想回線にバインドし、xconnect コンフィギュレーション モードを開始します。 • このコマンドの構文は、その他のレイヤ 2 トランスポートの場合と同じです。

単一 PW を使用した ATOM ロード バランシングの設定（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

手順の概要

1. イネーブル化
2. **configure terminal**
3. **template type pseudowire** [*pseudowire-name*]
4. **encapsulation mpls**
5. **load-balance flow**
6. **end**
7. **interfacepseudowire***number*
8. **sourcetemplate type pseudowire**
9. **neighbor***peer-address vcid-value*
10. **end**
11. **l2vpnxconnect context***context-name*
12. **member pseudowire***interface-number*
13. **member** *ip-addressvc-id***encapsulation mpls**
14. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

単一 PW を使用した AToM ロード バランシングの設定（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

	コマンドまたはアクション	目的
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	**template type pseudowire** [*pseudowire-name*] 例： `Router(config)# template type pseudowire eompls`	レイヤ 2 擬似回線 クラスの名前を指定し、擬似回線クラス 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	**encapsulation mpls** 例： `Router(config-pw-class)# encapsulation mpls`	トンネリング カプセル化を指定します。 • AToM の場合、カプセル化タイプは mpls です。
ステップ 5	**load-balance flow** 例： `Router(config-pw-class)# load-balance flow`	ロード バランシングがフロー単位で実行されるように、単一の PW を使用した AToM ロード バランシング機能を有効にします。
ステップ 6	**end** 例： `Router(config-pw-class)# end`	特権 EXEC モードに戻ります。
ステップ 7	**interfacepseudowire***number* 例： `Router(config)# interface pseudowire 100`	擬似回線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 8	**sourcetemplate type pseudowire** 例： `Router(config-if)# source template type pseudowire ether-pw`	ether-pw という名前のタイプ擬似回線のソース テンプレートを設定します。
ステップ 9	**neighbor***peer-address vcid-value* 例： `Router(config-if)#  neighbor 10.1.1.1 1`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。

	コマンドまたはアクション	目的
ステップ 10	**end** 例： `Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 11	**l2vpnxconnect context***context-name* 例： `Router(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect コンフィギュレーション モードを開始します。
ステップ 12	**member pseudowire***interface-number* 例： `Router(config-xconnect)# member pseudowire 100`	Layer 2 VPN（L2VPN）クロスコネクトを形成するようにメンバー擬似回線を指定します。
ステップ 13	**member** *ip-addressvc-id***encapsulation mpls** 例： `Router(config-xconnect)# member 10.0.0.1 123 encapsulation mpls`	レイヤ 2 パケットを転送するための VC を作成します。
ステップ 14	**end** 例： `Router(config-xconnect)# end`	特権 EXEC モードに戻ります。

フロー認識トランスポート（FAT）ロード バランシングの設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface pseudowire***name*
4. **encapsulation mpls**
5. **neighbor***peer-addressvcid-value*
6. **signaling protocol ldp**
7. **load-balance flow**
8. **load-balance flow-label**
9. **end**
10. **show l2vpn atom vc detail**
11. **show ssm id**
12. **show mpls forwarding-table exact-route**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 pseudowire***name* 例： `Device(config)# interface pseudowire 1001`	指定された名前の擬似回線を確立して、擬似回線クラス 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	**encapsulation mpls** 例： `Device(config-pw-class)# encapsulation mpls`	トンネリング カプセル化を指定します。 • AToM の場合、カプセル化タイプは mpls です。

	コマンドまたはアクション	目的
ステップ 5	**neighbor***peer-addressvcid-value* 例： `Device(config-pw-class)# neighbor 10.1.1.200 200`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 6	**signaling protocol ldp** 例： `Device(config-pw-class)# signaling protocol ldp`	擬似回線クラス用のラベル配布プロトコル（LDP）が設定されるように指定します。
ステップ 7	**load-balance flow** 例： `Device(config-pw-class)# load-balance flow`	ロード バランシングがフロー単位で実行されるように、単一の PW を使用した AToM ロード バランシング機能を有効にします。
ステップ 8	**load-balance flow-label** 例： `Device(config-pw-class)# load-balance flow-label both`	MPLS 擬似回線のフロー認識トランスポート機能を有効にして、フロー ラベルの使用方法を指定します。
ステップ 9	**end** 例： `Device(config-pw-class)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show l2vpn atom vc detail** 例： `Device# show l2vpn atom vc detail`	擬似回線用に設定されたフロー ラベルに関する情報を示す詳細な出力を表示します。
ステップ 11	**show ssm id** 例： `Device# show ssm id`	すべての Segment Switching Manager（SSM）ID に関する情報を表示します。
ステップ 12	**show mpls forwarding-table exact-route** 例： `Device# show mpls forwarding-table exact-route label 32 ethernet source 001d.e558.5c1a dest 000e.8379.1c1b detail`	送信元/宛先アドレスペアの正確なパスを表示します。

例

次に、擬似回線用に設定されたフロー ラベルに関する情報を表示する **show l2vpn atom vc detail** コマンドのサンプル出力を示します。

```
Device# show l2vpn atom vc detail

pseudowire100001 is up, VC status is up PW type: Ethernet
  Create time: 00:01:47, last status change time: 00:01:29
    Last label FSM state change time: 00:01:29
  Destination address: 10.1.1.151 VC ID: 100
    Output interface: Se3/0, imposed label stack {1001 100}
    Preferred path: not configured
    Default path: active
    Next hop: point2point
    Load Balance: Flow
    flow classification: ethernet src-dst-mac
  Member of xconnect service Et0/0-2, group right
    Associated member Et0/0 is up, status is up
    Interworking type is Like2Like
    Service id: 0xcf000001
  Signaling protocol: LDP, peer 10.1.1.151:0 up
    Targeted Hello: 10.1.1.152(LDP Id) -> 10.1.1.151, LDP is UP
    Graceful restart: not configured and not enabled
    Non stop routing: not configured and not enabled
    PWid FEC (128), VC ID: 100
    Status TLV support (local/remote)         : enabled/supported
      LDP route watch                         : enabled
      Label/status state machine              : established, LruRru
      Local dataplane status received         : No fault
      BFD dataplane status received           : Not sent
      BFD peer monitor status received        : No fault
      Status received from access circuit     : No fault
      Status sent to access circuit           : No fault
      Status received from pseudowire i/f     : No fault
      Status sent to network peer             : No fault
      Status received from network peer       : No fault
      Adjacency status of remote peer         : No fault
  Sequencing: receive disabled, send disabled
  Bindings
    Parameter    Local                          Remote
    ------------ ------------------------------ ------------------------------
    Label        200                            100
    Group ID     0                              0
    Interface
    MTU          1500                           1500
    Control word on (configured: autosense)     on
    PW type      Ethernet                       Ethernet
    VCCV CV type 0x12                           0x12
                   LSPV [2], BFD/Raw [5]          LSPV [2], BFD/Raw [5]
    VCCV CC type 0x07                           0x07
                   CW [1], RA [2], TTL [3]       CW [1], RA [2], TTL [3]
    Status TLV   enabled                        supported
    Flow label   enabled, T=1, R=0              enabled, T=1, R=1
  Dataplane:
    SSM segment/switch IDs: 4097/4096 (used), PWID: 1
  Rx Counters
    28 input transit packets, 2602 bytes
    0 drops, 0 seq err
  Tx Counters
    31 output transit packets, 3694 bytes
    0 drops
```

次に、すべての Segment Switching Manager（SSM）ID の情報を表示する **show ssm id** コマンドのサンプル出力を示します。

```
Device# show ssm id

SSM Status: 1 switch
  Switch-ID 4096 State: Open
    Segment-ID: 8194 Type: Eth[2]
      Switch-ID:                    4096
      Physical intf:                Local
      Allocated By:                 This CPU
      Locked By:                    SIP     [1]
      Circuit status:               UP      [1]
    Class:                        SSS
      State:                        Active
      AC Switching Context:         Et0/0
      SSS Info : Switch Handle 2583691265 Ckt 0xC36A59E0
      Interworking 0 Encap Len 0 Boardencap Len 0 MTU 1500
      Flow Classification src-dst-mac
      AC Encap [0 bytes]
    Class:                        ADJ
      State:                        Active
      AC Adjacency context:
      adjacency = 0xC36B6100 [complete] RAW Ethernet0/0:0
      AC Encap [0 bytes]
      1stMem: 8194 2ndMem: 0 ActMem: 8194

    Segment-ID: 4097 Type: AToM[17]
      Switch-ID:                    4096
      Allocated By:                 This CPU
      Locked By:                    SIP     [1]
    Class:                        SSS
      State:                        Active
    Class:                        ADJ
      State:                        Active
```

次に、送信元アドレスと宛先アドレスのペアの正確なパスを表示する **show mpls forwarding-table exact-route** コマンドのサンプル出力を示します。

```
Device# show mpls forwarding-table exact-route label 32 ethernet source 001d.e558.5c1a dest
 000e.8379.1c1b detail

Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
32         No Label   l2ckt(66)        1163          Gi1/0/4    point2point
        MAC/Encaps=0/0, MRU=0, Label Stack{}
        No output feature configured
        Flow label: 227190
```

テンプレートを使用したフロー認識トランスポート（FAT）ロード バランシングの設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **templatetypepseudowire** [*pseudowire-name*]
4. **encapsulation mpls**
5. **load-balance flow**
6. **load-balance flow-label**
7. **end**
8. **interfacepseudowire***number*
9. **sourcetemplatetypepseudowire**
10. **encapsulation mpls**
11. **neighbor***peer-addressvcid-value*
12. **signaling protocol ldp**
13. **end**
14. **show l2vpn atom vc detail**
15. **show ssm id**
16. **show mpls forwarding-table exact-route**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**templatetypepseudowire** [*pseudowire-name*] 例： `Device(config)# template type pseudowire fatpw`	レイヤ 2 擬似回線 クラスの名前を指定し、擬似回線クラス 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	**encapsulation mpls** 例： `Device(config-pw-class)# encapsulation mpls`	トンネリング カプセル化を指定します。 • AToM の場合、カプセル化タイプは MPLS です。
ステップ 5	**load-balance flow** 例： `Device(config-pw-class)# load-balance flow`	ロード バランシングがフロー単位で実行されるように、単一の PW を使用した AToM ロード バランシング機能を有効にします。
ステップ 6	**load-balance flow-label** 例： `Device(config-pw-class)# load-balance flow-label both`	MPLS 擬似回線のフロー認識トランスポート機能を有効にして、フロー ラベルの使用方法を指定します。
ステップ 7	**end** 例： `Device(config-pw-class)# end`	特権 EXEC モードに戻ります。
ステップ 8	**interfacepseudowire***number* 例： `Device(config)# interface pseudowire 100`	擬似回線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 9	**sourcetemplatetypepseudowire** 例： `Device(config-if)# source template type pseudowire fatpw`	fatpw という名前のタイプ擬似回線のソース テンプレートを設定します。
ステップ 10	**encapsulation mpls** 例： `Device(config-if)# encapsulation mpls`	トンネリング カプセル化を指定します。 • AToM の場合、カプセル化タイプは MPLS です。
ステップ 11	**neighbor***peer-addressvcid-value* 例： `Device(config-if)# neighbor 10.1.1.1 1`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。

	コマンドまたはアクション	目的
ステップ 12	**signaling protocol ldp** 例： `Device(config-if)# signaling protocol ldp`	擬似回線クラス用のラベル配布プロトコル（LDP）が設定されるように指定します。
ステップ 13	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 14	**show l2vpn atom vc detail** 例： `Device# show l2vpn atom vc detail`	擬似回線用に設定されたフロー ラベルに関する情報を示す詳細な出力を表示します。
ステップ 15	**show ssm id** 例： `Device# show ssm id`	すべての Segment Switching Manager（SSM）ID に関する情報を表示します。
ステップ 16	**show mpls forwarding-table exact-route** 例： `Device# show mpls forwarding-table exact-route label 32 ethernet source 001d.e558.5c1a dest 000e.8379.1c1b detail`	送信元/宛先アドレス ペアの正確なパスを表示します。

例

次に、擬似回線用に設定されたフロー ラベルに関する情報を表示する **show l2vpn atom vc detail** コマンドのサンプル出力を示します。

```
Device# show l2vpn atom vc detail

pseudowire100001 is up, VC status is up PW type: Ethernet
  Create time: 00:01:47, last status change time: 00:01:29
    Last label FSM state change time: 00:01:29
  Destination address: 10.1.1.151 VC ID: 100
    Output interface: Se3/0, imposed label stack {1001 100}
    Preferred path: not configured
    Default path: active
    Next hop: point2point
    Load Balance: Flow
    flow classification: ethernet src-dst-mac
  Member of xconnect service Et0/0-2, group right
    Associated member Et0/0 is up, status is up
    Interworking type is Like2Like
```

```
    Service id: 0xcf000001
  Signaling protocol: LDP, peer 10.1.1.151:0 up
    Targeted Hello: 10.1.1.152(LDP Id) -> 10.1.1.151, LDP is UP
    Graceful restart: not configured and not enabled
    Non stop routing: not configured and not enabled
    PWid FEC (128), VC ID: 100
    Status TLV support (local/remote)         : enabled/supported
      LDP route watch                         : enabled
      Label/status state machine              : established, LruRru
      Local dataplane status received         : No fault
      BFD dataplane status received           : Not sent
      BFD peer monitor status received        : No fault
      Status received from access circuit     : No fault
      Status sent to access circuit           : No fault
      Status received from pseudowire i/f     : No fault
      Status sent to network peer             : No fault
      Status received from network peer       : No fault
      Adjacency status of remote peer         : No fault
  Sequencing: receive disabled, send disabled
  Bindings
    Parameter    Local                          Remote
    ------------ ------------------------------ ------------------------------
    Label        200                            100
    Group ID     0                              0
    Interface
    MTU          1500                           1500
    Control word on (configured: autosense)     on
    PW type      Ethernet                       Ethernet
    VCCV CV type 0x12                           0x12
                   LSPV [2], BFD/Raw [5]          LSPV [2], BFD/Raw [5]
    VCCV CC type 0x07                           0x07
                   CW [1], RA [2], TTL [3]       CW [1], RA [2], TTL [3]
    Status TLV   enabled                        supported
    Flow label   enabled, T=1, R=0              enabled, T=1, R=1
  Dataplane:
    SSM segment/switch IDs: 4097/4096 (used), PWID: 1
  Rx Counters
    28 input transit packets, 2602 bytes
    0 drops, 0 seq err
  Tx Counters
    31 output transit packets, 3694 bytes
    0 drops
```

次に、すべての Segment Switching Manager（SSM）ID の情報を表示する **show ssm id** コマンドのサンプル出力を示します。

```
Device# show ssm id

SSM Status: 1 switch
  Switch-ID 4096 State: Open
    Segment-ID: 8194 Type: Eth[2]
      Switch-ID:                    4096
      Physical intf:                Local
      Allocated By:                 This CPU
      Locked By:                    SIP     [1]
      Circuit status:               UP      [1]
    Class:                        SSS
      State:                        Active
      AC Switching Context:         Et0/0
      SSS Info : Switch Handle 2583691265 Ckt 0xC36A59E0
      Interworking 0 Encap Len 0 Boardencap Len 0 MTU 1500
      Flow Classification src-dst-mac
      AC Encap [0 bytes]
    Class:                        ADJ
      State:                        Active
      AC Adjacency context:
      adjacency = 0xC36B6100 [complete] RAW Ethernet0/0:0
      AC Encap [0 bytes]
      1stMem: 8194 2ndMem: 0 ActMem: 8194

    Segment-ID: 4097 Type: AToM[17]
```

```
      Switch-ID:                    4096
      Allocated By:                 This CPU
      Locked By:                    SIP     [1]
    Class:                        SSS
      State:                        Active
    Class:                        ADJ
      State:                        Active
```

次に、送信元アドレスと宛先アドレスのペアの正確なパスを表示する **show mpls forwarding-table exact-route** コマンドのサンプル出力を示します。

```
Device# show mpls forwarding-table exact-route label 32 ethernet source 001d.e558.5c1a dest
 000e.8379.1c1b detail

Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
32         No Label   l2ckt(66)        1163          Gi1/0/4    point2point
        MAC/Encaps=0/0, MRU=0, Label Stack{}
        No output feature configured
        Flow label: 227190
```

Any Transport over MPLS の設定例

例：ATM over MPLS

次の表に、2 台の PE ルータでの ATM over MPLS の設定を示します。

表 *8*：*ATM over MPLS* の設定例

PE1	PE2
mpls label protocol ldp mpls ldp router-id Loopback0 force ! interface Loopback0 ip address 10.16.12.12 255.255.255.255 ! interface ATM4/0/0 pvc 0/100 l2transport encapsulation aal0 xconnect 10.13.13.13 100 encapsulation mpls ! interface ATM4/0/0.300 point-to-point no ip directed-broadcast no atm enable-ilmi-trap pvc 0/300 l2transport encapsulation aal0 xconnect 10.13.13.13 300 encapsulation mpls	mpls label protocol ldp mpls ldp router-id Loopback0 force ! interface Loopback0 ip address 10.13.13.13 255.255.255.255 interface ATM4/0/0 pvc 0/100 l2transport encapsulation aal0 xconnect 10.16.12.12 100 encapsulation mpls ! interface ATM4/0/0.300 point-to-point no ip directed-broadcast no atm enable-ilmi-trap pvc 0/300 l2transport encapsulation aal0 xconnect 10.16.12.12 300 encapsulation mpls

例：ATM over MPLS（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

次の表に、2 台の PE ルータでの ATM over MPLS の設定を示します。

表 *9*：*ATM over MPLS* の設定例

PE1	PE2
mpls label protocol ldp mpls ldp router-id Loopback0 force ! interface Loopback0 ip address 10.16.12.12 255.255.255.255 ! interface ATM4/0/0 pvc 0/100 l2transport encapsulation aal0 interface pseudowire 100 encapsulation mpls neighbor 10.0.0.1 123 ! l2vpn xconnect context A member pseudowire 100 member atm 100 ! interface ATM4/0/0.300 point-to-point no atm enable-ilmi-trap pvc 0/300 l2transport encapsulation aal0 interface pseudowire 300 encapsulation mpls neighbor 10.0.0.1 123 ! l2vpn xconnect context A member pseudowire 300 member atm 300	mpls label protocol ldp mpls ldp router-id Loopback0 force ! interface Loopback0 ip address 10.13.13.13 255.255.255.255 interface ATM4/0/0 pvc 0/100 l2transport encapsulation aal0 interface pseudowire 100 encapsulation mpls neighbor 10.0.0.1 123 ! l2vpn xconnect context A member pseudowire 100 member atm 100 ! interface ATM4/0/0.300 point-to-point no ip directed-broadcast no atm enable-ilmi-trap pvc 0/300 l2transport encapsulation aal0 interface pseudowire 300 encapsulation mpls neighbor 10.0.0.1 123 ! l2vpn xconnect context A member pseudowire 300 member atm 300

例：VC クラス コンフィギュレーション モードでの ATM AAL5 over MPLS の設定

次に、VC クラス コンフィギュレーション モードで ATM AAL5 over MPLS を設定する例を示します。その後で、VC クラスがインターフェイスに適用されます。

```
enable
configure terminal
vc-class atm aal5class
encapsulation aal5
interface atm1/0/0
class-int aal5class
pvc 1/200 l2transport
xconnect 10.13.13.13 100 encapsulation mpls
```

次に、VC クラス コンフィギュレーション モードで ATM AAL5 over MPLS を設定する例を示します。その後で、VC クラスが PVC に適用されます。

```
enable
configure terminal
vc-class atm aal5class
encapsulation aal5
interface atm1/0/0
pvc 1/200 l2transport
class-vc aal5class
xconnect 10.13.13.13 100 encapsulation mpls
```

例：VC クラス コンフィギュレーション モードでの ATM AAL5 over MPLS の設定（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

次に、VC クラス コンフィギュレーション モードで ATM AAL5 over MPLS を設定する例を示します。その後で、VC クラスがインターフェイスに適用されます。

```
enable
configure terminal
vc-class atm aal5class
encapsulation aal5
interface atm1/0/0
class-int aal5class
pvc 1/200 l2transport
interface pseudowire 100
encapsulation mpls
neighbor 10.0.0.1 123
exit
l2vpn xconnect context A
member pseudowire 100
member atm 100
exit
```

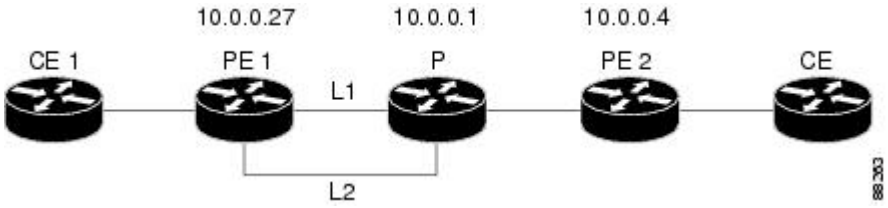
例：MPLS Traffic Engineering Fast Reroute を使用した Ethernet over MPLS

次の設定例および図では、AToM PE ルータで Fast Reroute を使用する Ethernet over MPLS の設定を示します。

ルータ PE1 および PE2 には次の特性があります。

- L1 という名前のリンクを経由する明示パスを使用して、Tunnel41 という名前の TE トンネルが PE1 と PE2 間に設定されています。AToM VC は、FRR で保護されたトンネル Tunnel41 を通過するように設定されています。
- リンク L1 は FRR によって保護されており、バックアップ トンネルは Tunnel1 です。
- PE2 は、AToM トラフィックを L2 リンク経由で PE1 に転送するように設定されています。

図 5：*Fast Reroute* の設定



PE1 の設定

```
mpls label protocol ldp
mpls traffic-eng tunnels
mpls ldp router-id Loopback1 force
!
pseudowire-class T41
 encapsulation mpls
 preferred-path interface Tunnel41 disable-fallback
!
pseudowire-class IP1
 encapsulation mpls
 preferred-path peer 10.4.0.1 disable-fallback
!
interface Loopback1
 ip address 10.0.0.27 255.255.255.255
!
interface Tunnel1
 ip unnumbered Loopback1
 tunnel destination 10.0.0.1
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth 10000
 tunnel mpls traffic-eng path-option 1 explicit name FRR
!
interface Tunnel41
 ip unnumbered Loopback1
 tunnel destination 10.0.0.4
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 1 explicit name name-1
 tunnel mpls traffic-eng fast-reroute
!
interface POS0/0/0
 description pe1name POS8/0/0
 ip address 10.1.0.2 255.255.255.252
 mpls traffic-eng tunnels
 mpls traffic-eng backup-path Tunnel1
 crc 16
 clock source internal
 pos ais-shut
 pos report lrdi
 ip rsvp bandwidth 155000 155000
!
interface POS0/3/0
```

```
 description pe1name POS10/1/0
 ip address 10.1.0.14 255.255.255.252
 mpls traffic-eng tunnels
 crc 16
 clock source internal
 ip rsvp bandwidth 155000 155000
!
interface gigabitethernet3/0/0.1
 encapsulation dot1Q 203
 xconnect 10.0.0.4 2 pw-class IP1
!
interface gigabitethernet3/0/0.2
 encapsulation dot1Q 204
 xconnect 10.0.0.4 4 pw-class T41
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
 mpls traffic-eng router-id Loopback1
 mpls traffic-eng area 0
!
ip classless
ip route 10.4.0.1 255.255.255.255 Tunnel41
!
ip explicit-path name xxxx-1 enable
 next-address 10.4.1.2
 next-address 10.1.0.10
```

P の設定

```
ip cef
mpls traffic-eng tunnels
!
interface Loopback1
 ip address 10.0.0.1 255.255.255.255
!
interface FastEthernet1/0/0
 ip address 10.4.1.2 255.255.255.0
 mpls traffic-eng tunnels
 ip rsvp bandwidth 10000 10000
!
interface POS8/0/0
 description xxxx POS0/0
 ip address 10.1.0.1 255.255.255.252
 mpls traffic-eng tunnels
 pos ais-shut
 pos report lrdi
 ip rsvp bandwidth 155000 155000
!
interface POS10/1/0
 description xxxx POS0/3
 ip address 10.1.0.13 255.255.255.252
 mpls traffic-eng tunnels
 ip rsvp bandwidth 155000 155000
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
 mpls traffic-eng router-id Loopback1
 mpls traffic-eng area 0
```

PE2 の設定

```
ip cef
mpls label protocol ldp
mpls traffic-eng tunnels
mpls ldp router-id Loopback1 force
!
interface Loopback1
 ip address 10.0.0.4 255.255.255.255
!
```

```
interface loopback 2
ip address 10.4.0.1 255.255.255.255
!
interface Tunnel27
 ip unnumbered Loopback1
 tunnel destination 10.0.0.27
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 1 explicit name xxxx-1
!
interface FastEthernet0/0/0.2
 encapsulation dot1Q 203
 xconnect 10.0.0.27 2 encapsulation mpls
!
interface FastEthernet0/0/0.3
 encapsulation dot1Q 204
 xconnect 10.0.0.27 4 encapsulation mpls
!
interface FastEthernet1/1/0
 ip address 10.4.1.1 255.255.255.0
 mpls traffic-eng tunnels
 ip rsvp bandwidth 10000 10000
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
 mpls traffic-eng router-id Loopback1
 mpls traffic-eng area 0
!
ip explicit-path name xxxx-1 enable
 next-address 10.4.1.2
 next-address 10.1.0.10
```

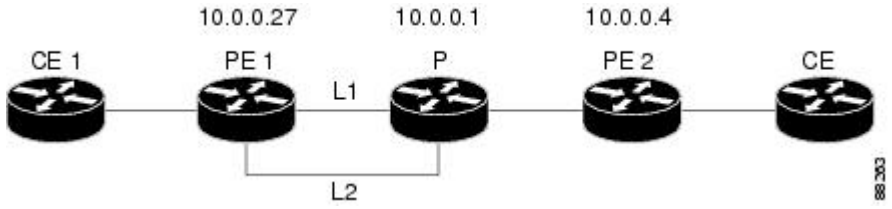
例：MPLS Traffic Engineering Fast Reroute を使用した Ethernet over MPLS（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

次の設定例および図では、AToM PE ルータで Fast Reroute を使用する Ethernet over MPLS の設定を示します。

ルータ PE1 および PE2 には次の特性があります。

- L1 という名前のリンクを経由する明示パスを使用して、Tunnel41 という名前の TE トンネルが PE1 と PE2 間に設定されています。AToM VC は、FRR で保護されたトンネル Tunnel41 を通過するように設定されています。
- リンク L1 は FRR によって保護されており、バックアップ トンネルは Tunnel1 です。
- PE2 は、AToM トラフィックを L2 リンク経由で PE1 に転送するように設定されています。

図 6：*Fast Reroute* の設定



PE1 の設定

```
mpls label protocol ldp
mpls traffic-eng tunnels
mpls ldp router-id Loopback1 force
!
template type pseudowire T41
 encapsulation mpls
 preferred-path interface Tunnel41 disable-fallback
!
template type pseudowire IP1
 encapsulation mpls
 preferred-path peer 10.4.0.1 disable-fallback
!
interface Loopback1
 ip address 10.0.0.27 255.255.255.255
!
interface Tunnel1
 ip unnumbered Loopback1
 tunnel destination 10.0.0.1
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth 10000
 tunnel mpls traffic-eng path-option 1 explicit name FRR
!
interface Tunnel41
 ip unnumbered Loopback1
 tunnel destination 10.0.0.4
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 1 explicit name name-1
 tunnel mpls traffic-eng fast-reroute
!
interface POS0/0/0
 description pelname POS8/0/0
 ip address 10.1.0.2 255.255.255.252
 mpls traffic-eng tunnels
 mpls traffic-eng backup-path Tunnel1
 crc 16
 clock source internal
 pos ais-shut
 pos report lrdi
 ip rsvp bandwidth 155000 155000
!
interface POS0/3/0
 description pelname POS10/1/0
 ip address 10.1.0.14 255.255.255.252
 mpls traffic-eng tunnels
 crc 16
 clock source internal
 ip rsvp bandwidth 155000 155000
!
interface gigabitethernet3/0/0.1
 encapsulation dot1Q 203
 interface pseudowire 100
 source template type pseudowire T41
 neighbor 10.0.0.4 2
!
l2vpn xconnect context con1
!
interface gigabitethernet3/0/0.2
 encapsulation dot1Q 204
 interface pseudowire 100
 source template type pseudowire IP1
 neighbor 10.0.0.4 4
!
l2vpn xconnect context con2
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
 mpls traffic-eng router-id Loopback1
```

例：**MPLS Traffic Engineering Fast Reroute** を使用した **Ethernet over MPLS**（**L2VPN** プロトコルベース **CLI** 機能に関連するコマンドを使用）

```
 mpls traffic-eng area 0
!
ip classless
ip route 10.4.0.1 255.255.255.255 Tunnel41
!
ip explicit-path name xxxx-1 enable
 next-address 10.4.1.2
 next-address 10.1.0.10
```

P の設定

```
ip cef
mpls traffic-eng tunnels
!
interface Loopback1
 ip address 10.0.0.1 255.255.255.255
!
interface FastEthernet1/0/0
 ip address 10.4.1.2 255.255.255.0
 mpls traffic-eng tunnels
 ip rsvp bandwidth 10000 10000
!
interface POS8/0/0
 description xxxx POS0/0
 ip address 10.1.0.1 255.255.255.252
 mpls traffic-eng tunnels
 pos ais-shut
 pos report lrdi
 ip rsvp bandwidth 155000 155000
!
interface POS10/1/0
 description xxxx POS0/3
 ip address 10.1.0.13 255.255.255.252
 mpls traffic-eng tunnels
 ip rsvp bandwidth 155000 155000
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
 mpls traffic-eng router-id Loopback1
 mpls traffic-eng area 0
```

PE2 の設定

```
ip cef
mpls label protocol ldp
mpls traffic-eng tunnels
mpls ldp router-id Loopback1 force
!
interface Loopback1
 ip address 10.0.0.4 255.255.255.255
!
interface loopback 2
ip address 10.4.0.1 255.255.255.255
!
interface Tunnel27
 ip unnumbered Loopback1
 tunnel destination 10.0.0.27
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 1 explicit name xxxx-1
!
interface FastEthernet0/0/0.2
 encapsulation dot1Q 203
 interface pseudowire 100
 encapsulation mpls
 neighbor 10.0.0.1 123
!
```

```
l2vpn xconnect context A
 member pseudowire 100
 member gigabitethernet 0/0/0.1
!
interface FastEthernet0/0/0.3
 encapsulation dot1Q 204
 interface pseudowire 100
 encapsulation mpls
 neighbor 10.0.0.1 123
!
l2vpn xconnect context A
 member pseudowire 100
 member gigabitethernet 0/0/0.1
!
interface FastEthernet1/1/0
 ip address 10.4.1.1 255.255.255.0
 mpls traffic-eng tunnels
 ip rsvp bandwidth 10000 10000
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
 mpls traffic-eng router-id Loopback1
 mpls traffic-eng area 0
!
ip explicit-path name xxxx-1 enable
 next-address 10.4.1.2
 next-address 10.1.0.10
```

例：OAM セル エミュレーションの設定

次に、ATM PVC で OAM セル エミュレーションを有効にする例を示します。

```
interface ATM 1/0/0
pvc 1/200 l2transport
encapsulation aal5
xconnect 10.13.13.13 100 encapsulation mpls
oam-ac emulation-enable
oam-pvc manage
```

次に、AIS セルが 30 秒間隔で送信されるようにレートを設定する例を示します。

```
interface ATM 1/0/0
pvc 1/200 l2transport
encapsulation aal5
xconnect 10.13.13.13 100 encapsulation mpls
oam-ac emulation-enable 30
oam-pvc manage
```

次に、VC クラス コンフィギュレーション モードで ATM AAL5 over MPLS の OAM セル エミュレーションを設定する例を示します。その後で、VC クラスがインターフェイスに適用されます。

```
enable
configure terminal
vc-class atm oamclass
encapsulation aal5
oam-ac emulation-enable 30
oam-pvc manage
interface atm1/0/0
class-int oamclass
pvc 1/200 l2transport
xconnect 10.13.13.13 100 encapsulation mpls
```

次に、VC クラス コンフィギュレーション モードで ATM AAL5 over MPLS の OAM セル エミュレーションを設定する例を示します。その後で、VC クラスが PVC に適用されます。

```
enable
configure terminal
vc-class atm oamclass
encapsulation aal5
oam-ac emulation-enable 30
oam-pvc manage
interface atm1/0/0
pvc 1/200 l2transport
class-vc oamclass
xconnect 10.13.13.13 100 encapsulation mpls
```

次に、VC クラス コンフィギュレーション モードで ATM AAL5 over MPLS の OAM セル エミュレーションを設定する例を示します。その後で、VC クラスがインターフェイスに適用されます。1 つの PVC が、AIS レートが 10 の OAM セル エミュレーションを使用して設定されます。その PVC では、30 の代わりに 10 の AIS レートが使用されます。

```
enable
configure terminal
vc-class atm oamclass
encapsulation aal5
oam-ac emulation-enable 30
oam-pvc manage
interface atm1/0/0
class-int oamclass
pvc 1/200 l2transport
oam-ac emulation-enable 10
xconnect 10.13.13.13 100 encapsulation mpls
```

例：OAM セル エミュレーションの設定（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

次に、ATM PVC で OAM セル エミュレーションを有効にする例を示します。

```
interface ATM 1/0/0
pvc 1/200 l2transport
encapsulation aal5
interface pseudowire 100
encapsulation mpls
neighbor 10.0.0.1 123
!
l2vpn xconnect context A
member pseudowire 100
member gigabitethernet 0/0/0.1
!
oam-ac emulation-enable
oam-pvc manage
```

次に、AIS セルが 30 秒間隔で送信されるようにレートを設定する例を示します。

```
interface ATM 1/0/0
pvc 1/200 l2transport
encapsulation aal5
interface pseudowire 100
encapsulation mpls
neighbor 10.0.0.1 123
!
l2vpn xconnect context A
member pseudowire 100
member gigabitethernet 0/0/0.1
```

```
!
oam-ac emulation-enable 30
oam-pvc manage
```

次に、VC クラス コンフィギュレーション モードで ATM AAL5 over MPLS の OAM セル エミュレーションを設定する例を示します。その後で、VC クラスがインターフェイスに適用されます。

```
enable
configure terminal
vc-class atm oamclass
encapsulation aal5
oam-ac emulation-enable 30
oam-pvc manage
interface atm1/0/0
class-int oamclass
pvc 1/200 l2transport
interface pseudowire 100
encapsulation mpls
neighbor 10.0.0.1 123
!
l2vpn xconnect context A
member pseudowire 100
member gigabitethernet 0/0/0.1

The following example shows how to configure OAM cell emulation for ATM AAL5 over MPLS in
VC class configuration mode. The VC class is then applied to a PVC.

enable
configure terminal
vc-class atm oamclass
encapsulation aal5
oam-ac emulation-enable 30
oam-pvc manage
interface atm1/0/0
pvc 1/200 l2transport
class-vc oamclass
interface pseudowire 100
encapsulation mpls
neighbor 10.0.0.1 123
!
l2vpn xconnect context A
member pseudowire 100
member gigabitethernet 0/0/0.1
```

次に、VC クラス コンフィギュレーション モードで ATM AAL5 over MPLS の OAM セル エミュレーションを設定する例を示します。その後で、VC クラスがインターフェイスに適用されます。1 つの PVC が、AIS レートが 10 の OAM セル エミュレーションを使用して設定されます。その PVC では、30 の代わりに 10 の AIS レートが使用されます。

```
enable
configure terminal
vc-class atm oamclass
encapsulation aal5
oam-ac emulation-enable 30
oam-pvc manage
interface atm1/0/0
class-int oamclass
pvc 1/200 l2transport
oam-ac emulation-enable 10
interface pseudowire 100
encapsulation mpls
neighbor 10.0.0.1 123
!
l2vpn xconnect context A
member pseudowire 100
member gigabitethernet 0/0/0.1
```

例：ATM Cell Relay over MPLS の設定

次に、VC クラス コンフィギュレーション モードで ATM Cell Relay over MPLS を設定する例を示します。その後で、VC クラスがインターフェイスに適用されます。

```
enable
configure terminal
vc-class atm cellrelay
encapsulation aal0
interface atm1/0/0
class-int cellrelay
pvc 1/200 l2transport
xconnect 10.13.13.13 100 encapsulation mpls
```

次に、VC クラス コンフィギュレーション モードで ATM Cell Relay over MPLS を設定する例を示します。その後で、VC クラスが PVC に適用されます。

```
enable
configure terminal
vc-class atm cellrelay
encapsulation aal0
interface atm1/0/0
pvc 1/200 l2transport
class-vc cellrelay
xconnect 10.13.13.13 100 encapsulation mpls
```

次に、単一の ATM セルを仮想パスで転送するように擬似回線クラスを設定する例を示します。

```
pseudowire-class vp-cell-relay
encapsulation mpls
interface atm 5/0
atm pvp 1 l2transport
xconnect 10.0.0.1 123 pw-class vp-cell-relay
```

例：ATM Cell Relay over MPLS の設定（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

次に、VC クラス コンフィギュレーション モードで ATM Cell Relay over MPLS を設定する例を示します。その後で、VC クラスがインターフェイスに適用されます。

```
enable
configure terminal
vc-class atm cellrelay
encapsulation aal0
interface atm1/0/0
class-int cellrelay
pvc 1/200 l2transport
interface pseudowire 100
encapsulation mpls
neighbor 10.13.13.13 100
!
l2vpn xconnect context A
member pseudowire 100
member gigabitethernet 0/0/0.1
```

次に、VC クラス コンフィギュレーション モードで ATM Cell Relay over MPLS を設定する例を示します。その後で、VC クラスが PVC に適用されます。

```
enable
configure terminal
```

```
vc-class atm cellrelay
encapsulation aal0
interface atm1/0/0
pvc 1/200 l2transport
class-vc cellrelay
interface pseudowire 100
encapsulation mpls
neighbor 10.13.13.13 100
!
l2vpn xconnect context A
member pseudowire 100
member gigabitethernet 0/0/0.1
```

次に、単一の ATM セルを仮想パスで転送するように擬似回線クラスを設定する例を示します。

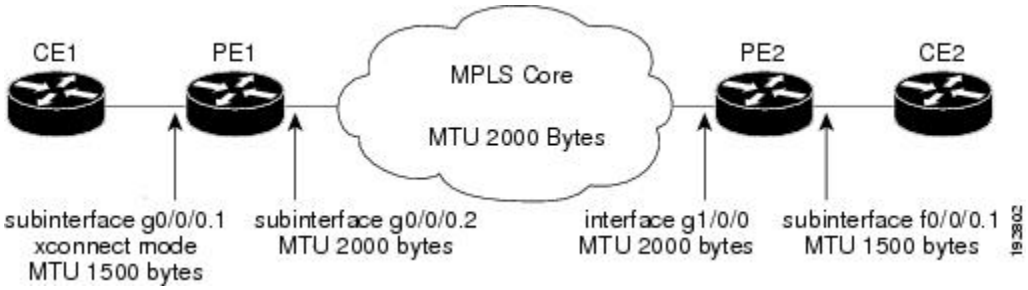
```
template type pseudowire vp-cell-relay
encapsulation mpls
interface atm 5/0
atm pvp 1 l2transport
interface pseudowire 100
 source template type pseudowire ether-pw
 neighbor 10.0.0.1 123
!
l2vpn xconnect context con1
```

例：Ethernet over MPLS 用のサブインターフェイスごとの MTU の設定

次の図に、VC エンドポイント間の MTU 値のマッチングをイネーブルにする設定を示します。

この図に示すように、PE1 は、PE2 とのエンドツーエンド VC を確立するために、xconnect サブインターフェイス コンフィギュレーション モードで 1500 バイトの MTU 値を指定して設定されており、PE2 の MTU 値も 1500 バイトに設定されています。PE1 を 1500 バイトの MTU 値で設定しなかった場合、xconnect サブインターフェイス コンフィギュレーション モードでは、インターフェイスに設定されている 2000 バイトの MTU 値がサブインターフェイスによって継承されます。これにより、VC エンドポイント間で MTU 値の不一致が発生し、VC はアップ状態になりません。

図 7：*xconnect* サブインターフェイス コンフィギュレーション モードでの *MTU* 値の設定



次に、上記の図のルータ設定例を示します。

CE1 の設定

```
interface gigabitethernet0/0/0
 mtu 1500
 no ip address
!
```

```
interface gigabitethernet0/0/0.1
 encapsulation dot1Q 100
 ip address 10.181.182.1 255.255.255.0
```

PE1 の設定

```
interface gigabitethernet0/0/0
 mtu 2000
 no ip address
!
interface gigabitethernet0/0/0.1
 encapsulation dot1Q 100
 xconnect 10.1.1.152 100 encapsulation mpls
  mtu 1500
!
interface gigabitethernet0/0/0.2
 encapsulation dot1Q 200
 ip address 10.151.100.1 255.255.255.0
 mpls ip
```

PE2 の設定

```
interface gigabitethernet1/0/0
 mtu 2000
 no ip address
!
interface gigabitethernet1/0/0.2
 encapsulation dot1Q 200
 ip address 10.100.152.2 255.255.255.0
 mpls ip
!
interface fastethernet0/0/0
 no ip address
!
interface fastethernet0/0/0.1
 description default MTU of 1500 for FastEthernet
 encapsulation dot1Q 100
 xconnect 10.1.1.151 100 encapsulation mpls
```

CE2 の設定

```
interface fastethernet0/0/0
 no ip address
interface fastethernet0/0/0.1
 encapsulation dot1Q 100
 ip address 10.181.182.2 255.255.255.0
```

show mpls l2transport binding コマンドをルータ PE1 から発行すると、ローカル ルータとリモート ルータの両方の MTU 値が 1500 バイトで一致していることが示されます。

```
Router# show mpls l2transport binding
Destination Address: 10.1.1.152,  VC ID: 100
    Local Label: 100
        Cbit: 1,    VC Type: FastEthernet,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: CW [1], RA [2]
              CV Type: LSPV [2]
    Remote Label: 202
        Cbit: 1,    VC Type: FastEthernet,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: RA [2]
              CV Type: LSPV [2]
```

```
Router# show mpls l2transport vc detail
Local interface: Gi0/0/0.1 up, line protocol up, Eth VLAN 100 up
  Destination address: 10.1.1.152, VC ID: 100, VC status: up
```

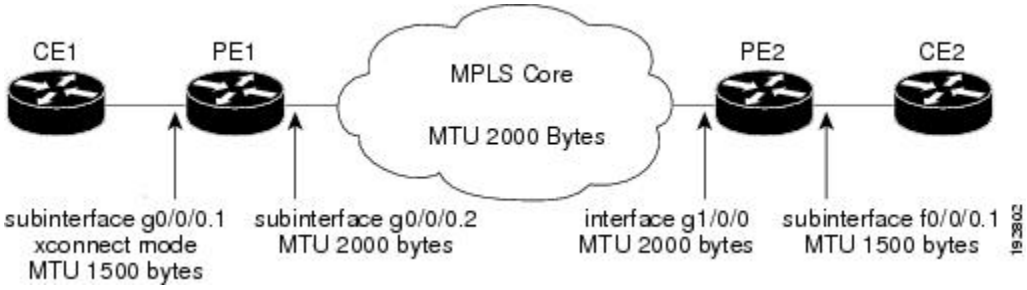
```
    Output interface: Gi0/0/0.2, imposed label stack {202}
    Preferred path: not configured
    Default path: active
    Next hop: 10.151.152.2
  Create time: 1d11h, last status change time: 1d11h
  Signaling protocol: LDP, peer 10.1.1.152:0 up
    Targeted Hello: 10.1.1.151(LDP Id) -> 10.1.1.152
    MPLS VC labels: local 100, remote 202
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 41, send 39
    byte totals:   receive 4460, send 5346
    packet drops:  receive 0, send 0
```

例：Ethernet over MPLS 用のサブインターフェイスごとの MTU の設定（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

次の図に、VC エンドポイント間の MTU 値のマッチングをイネーブルにする設定を示します。

この図に示すように、PE1 は、PE2 とのエンドツーエンド VC を確立するために、xconnect サブインターフェイス コンフィギュレーション モードで 1500 バイトの MTU 値を指定して設定されており、PE2 の MTU 値も 1500 バイトに設定されています。PE1 を 1500 バイトの MTU 値で設定しなかった場合、xconnect サブインターフェイス コンフィギュレーション モードでは、インターフェイスに設定されている 2000 バイトの MTU 値がサブインターフェイスによって継承されます。これにより、VC エンドポイント間で MTU 値の不一致が発生し、VC はアップ状態になりません。

図 *8*：*xconnect* サブインターフェイス コンフィギュレーション モードでの *MTU* 値の設定



次に、上記の図のルータ設定例を示します。

CE1 の設定

```
interface gigabitethernet0/0/0
 mtu 1500
 no ip address
!
interface gigabitethernet0/0/0.1
 encapsulation dot1Q 100
 ip address 10.181.182.1 255.255.255.0
```

例：**Ethernet over MPLS** 用のサブインターフェイスごとの **MTU** の設定（**L2VPN** プロトコルベース **CLI** 機能に関連するコマンドを使用）

PE1 の設定

```
interface gigabitethernet0/0/0
 mtu 2000
 no ip address
!
interface gigabitethernet0/0/0.1
 encapsulation dot1Q 100
 interface pseudowire 100
encapsulation mpls
neighbor 10.0.0.1 123
mtu 1500
!
l2vpn xconnect context A
member pseudowire 100
member gigabitethernet 0/0/0.1
!
interface gigabitethernet0/0/0.2
 encapsulation dot1Q 200
 ip address 10.151.100.1 255.255.255.0
 mpls ip
```

PE2 の設定

```
interface gigabitethernet1/0/0
 mtu 2000
 no ip address
!
interface gigabitethernet1/0/0.2
 encapsulation dot1Q 200
 ip address 10.100.152.2 255.255.255.0
 mpls ip
!
interface fastethernet0/0/0
 no ip address
!
interface fastethernet0/0/0.1
 description default MTU of 1500 for FastEthernet
 encapsulation dot1Q 100
 interface pseudowire 100
 encapsulation mpls
 neighbor 10.0.0.1 123
mtu 1500
!
l2vpn xconnect context A
 member pseudowire 100
 member gigabitethernet 0/0/0.1
```

CE2 の設定

```
interface fastethernet0/0/0
 no ip address
interface fastethernet0/0/0.1
 encapsulation dot1Q 100
 ip address 10.181.182.2 255.255.255.0
```

show l2vpn atom binding コマンドをルータ PE1 から発行すると、ローカル ルータとリモート ルータの両方の MTU 値が 1500 バイトで一致していることが示されます。

```
Device# show l2vpn atom binding
Destination Address: 10.1.1.152,  VC ID: 100
    Local Label: 100
        Cbit: 1,    VC Type: FastEthernet,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: CW [1], RA [2]
              CV Type: LSPV [2]
    Remote Label: 202
```

```
Cbit: 1,    VC Type: FastEthernet,    GroupID: 0
MTU: 1500,   Interface Desc: n/a
VCCV: CC Type: RA [2]
      CV Type: LSPV [2]
```

例：トンネル選択の設定

次に、PE1 に 2 つの優先パスを設定する例を示します。1 つの優先パスには、MPLS トラフィック エンジニアリング トンネルを指定します。もう 1 つの優先パスには、PE2 のループバック アドレスの IP アドレスを指定します。PE1 には、TE トンネルを使用して PE2 の IP アドレスに到達するように設定されたスタティック ルートがあります。

PE1 の設定

```
mpls label protocol ldp
mpls traffic-eng tunnels
tag-switching tdp router-id Loopback0
pseudowire-class pw1
 encapsulation mpls
 preferred-path interface Tunnel1 disable-fallback
!
pseudowire-class pw2
 encapsulation mpls
 preferred-path peer 10.18.18.18
!
interface Loopback0
 ip address 10.2.2.2 255.255.255.255
 no ip directed-broadcast
 no ip mroute-cache
!
interface Tunnel1
 ip unnumbered Loopback0
 no ip directed-broadcast
 tunnel destination 10.16.16.16
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 1500
 tunnel mpls traffic-eng path-option 1 explicit name path-tu1
!
interface Tunnel2
 ip unnumbered Loopback0
 no ip directed-broadcast
 tunnel destination 10.16.16.16
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 1500
 tunnel mpls traffic-eng path-option 1 dynamic
!
interface gigabitethernet0/0/0
 no ip address
 no ip directed-broadcast
 no negotiation auto
!
interface gigabitethernet0/0/0.1
 encapsulation dot1Q 222
 no ip directed-broadcast
 xconnect 10.16.16.16 101 pw-class pw1
!
interface ATM1/0/0
 no ip address
 no ip directed-broadcast
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
 pvc 0/50 l2transport
  encapsulation aal5
```

```
  xconnect 10.16.16.16 150 pw-class pw2
!
interface FastEthernet2/0/1
 ip address 10.0.0.1 255.255.255.0
 no ip directed-broadcast
 tag-switching ip
 mpls traffic-eng tunnels
 ip rsvp bandwidth 15000 15000
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.0.0.255 area 0
 network 10.2.2.2 0.0.0.0 area 0
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
!
ip route 10.18.18.18 255.255.255.255 Tunnel2
!
ip explicit-path name path-tu1 enable
 next-address 10.0.0.1
 index 3 next-address 10.0.0.1
```

PE2 の設定

```
mpls label protocol ldp
mpls traffic-eng tunnels
mpls ldp router-id Loopback0
interface Loopback0
 ip address 10.16.16.16 255.255.255.255
 no ip directed-broadcast
 no ip mroute-cache
!
interface Loopback2
 ip address 10.18.18.18 255.255.255.255
 no ip directed-broadcast
!
interface FastEthernet1/1/0
 ip address 10.0.0.2 255.255.255.0
 no ip directed-broadcast
 mpls traffic-eng tunnels
 mpls ip
 no cdp enable
 ip rsvp bandwidth 15000 15000
!
interface FastEthernet1/1/1
 no ip address
 no ip directed-broadcast
 no cdp enable
!
interface FastEthernet1/1/1.1
 encapsulation dot1Q 222
 no ip directed-broadcast
 no cdp enable
 mpls l2transport route 10.2.2.2 101
!
interface ATM5/0/0
 no ip address
 no ip directed-broadcast
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
 pvc 0/50 l2transport
  encapsulation aal5
  xconnect 10.2.2.2 150 encapsulation mpls
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.0.0.255 area 0
 network 10.16.16.16 0.0.0.0 area 0
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
```

例：トンネル選択の設定（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

次に、PE1 に 2 つの優先パスを設定する例を示します。1 つの優先パスには、MPLS トラフィック エンジニアリング トンネルを指定します。もう 1 つの優先パスには、PE2 のループバック アドレスの IP アドレスを指定します。PE1 には、TE トンネルを使用して PE2 の IP アドレスに到達するように設定されたスタティック ルートがあります。

PE1 の設定

```
mpls label protocol ldp
mpls traffic-eng tunnels
tag-switching tdp router-id Loopback0
template type pseudowire pw1
 encapsulation mpls
 preferred-path interface Tunnel1 disable-fallback
!
template type pseudowire pw2
 encapsulation mpls
 preferred-path peer 10.18.18.18
!
interface Loopback0
 ip address 10.2.2.2 255.255.255.255
 no ip directed-broadcast
 no ip mroute-cache
!
interface Tunnel1
 ip unnumbered Loopback0
 no ip directed-broadcast
 tunnel destination 10.16.16.16
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 1500
 tunnel mpls traffic-eng path-option 1 explicit name path-tu1
!
interface Tunnel2
 ip unnumbered Loopback0
 no ip directed-broadcast
 tunnel destination 10.16.16.16
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 1500
 tunnel mpls traffic-eng path-option 1 dynamic
!
interface gigabitethernet0/0/0
 no ip address
 no ip directed-broadcast
 no negotiation auto
!
interface gigabitethernet0/0/0.1
 encapsulation dot1Q 222
 no ip directed-broadcast
 interface pseudowire 100
 source template type pseudowire pw1
  neighbor 10.16.16.16 101
!
l2vpn xconnect context con1
!
interface ATM1/0/0
 no ip address
 no ip directed-broadcast
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
 pvc 0/50 l2transport
```

```
  encapsulation aal5
 interface pseudowire 100
 source template type pseudowire pw2
 neighbor 10.16.16.16 150
!
l2vpn xconnect context con1
!
interface FastEthernet2/0/1
 ip address 10.0.0.1 255.255.255.0
 no ip directed-broadcast
 tag-switching ip
 mpls traffic-eng tunnels
 ip rsvp bandwidth 15000 15000
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.0.0.255 area 0
 network 10.2.2.2 0.0.0.0 area 0
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
!
ip route 10.18.18.18 255.255.255.255 Tunnel2
!
ip explicit-path name path-tu1 enable
 next-address 10.0.0.1
 index 3 next-address 10.0.0.1
```

PE2 の設定

```
mpls label protocol ldp
mpls traffic-eng tunnels
mpls ldp router-id Loopback0
interface Loopback0
 ip address 10.16.16.16 255.255.255.255
 no ip directed-broadcast
 no ip mroute-cache
!
interface Loopback2
 ip address 10.18.18.18 255.255.255.255
 no ip directed-broadcast
!
interface FastEthernet1/1/0
 ip address 10.0.0.2 255.255.255.0
 no ip directed-broadcast
 mpls traffic-eng tunnels
 mpls ip
 no cdp enable
 ip rsvp bandwidth 15000 15000
!
interface FastEthernet1/1/1
 no ip address
 no ip directed-broadcast
 no cdp enable
!
interface FastEthernet1/1/1.1
 encapsulation dot1Q 222
 no ip directed-broadcast
 no cdp enable
 mpls l2transport route 10.2.2.2 101
!
interface ATM5/0/0
 no ip address
 no ip directed-broadcast
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
 pvc 0/50 l2transport
  encapsulation aal5
  interface pseudowire 100
   encapsulation mpls
   neighbor 10.2.2.2 150
!
```

```
l2vpn xconnect context A
  member pseudowire 100
  member GigabitEthernet0/0/0.1
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.0.0.255 area 0
 network 10.16.16.16 0.0.0.0 area 0
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
```

例：xconnect コンフィギュレーション モードでの L2VPN インターワーキング用 MTU 値の設定

次に、L2VPN インターワーキングの例を示します。PE1 ルータには、1492 バイトの MTU 値で設定されているシリアル インターフェイスがあります。PE2 ルータは xconnect コンフィギュレーション モードを使用して、1492 バイトに一致する MTU を設定します。これにより、2 つのルータで VC インターワーキングを形成できるようになります。PE2 ルータが xconnect コンフィギュレーション モードで MTU 値を設定していない場合、インターフェイスはデフォルトで 1500 バイトに設定され、VC はアップ状態になりません。

（注） L2VPN インターワーキングは、Cisco ASR 900 RSP3 モジュールではサポートされていません。

PE1 の設定

```
pseudowire-class atom-ipiw
 encapsulation mpls
 interworking ip
!
interface Loopback0
 ip address 10.1.1.151 255.255.255.255
!
interface Serial2/0/0
 mtu 1492
 no ip address
 encapsulation ppp
 no fair-queue
 serial restart-delay 0
 xconnect 10.1.1.152 123 pw-class atom-ipiw
!
interface Serial4/0/0
 ip address 10.151.100.1 255.255.255.252
 encapsulation ppp
 mpls ip
 serial restart-delay 0
!
router ospf 1
 log-adjacency-changes
 network 10.1.1.151 0.0.0.0 area 0
 network 10.151.100.0 0.0.0.3 area 0
!
mpls ldp router-id Loopback0
```

PE2 の設定

```
pseudowire-class atom-ipiw
 encapsulation mpls
```

```
 interworking ip
!
interface Loopback0
 ip address 10.1.1.152 255.255.255.255
!
interface FastEthernet0/0/0
 no ip address
 xconnect 10.1.1.151 123 pw-class atom-ipiw
  mtu 1492
!
interface Serial4/0/0
 ip address 10.100.152.2 255.255.255.252
 encapsulation ppp
 mpls ip
 serial restart-delay 0
!
router ospf 1
 log-adjacency-changes
 network 10.1.1.152 0.0.0.0 area 0
 network 10.100.152.0 0.0.0.3 area 0
!
mpls ldp router-id Loopback0
```

show mpls l2transport binding コマンドを使用すると、ローカルおよびリモート ルータの MTU 値が 1492 バイトであることが示されます。

PE1

```
Router# show mpls l2transport binding
Destination Address: 10.1.1.152,  VC ID: 123
    Local Label: 105
        Cbit: 1,    VC Type: PPP,    GroupID: 0
        MTU: 1492,   Interface Desc: n/a
        VCCV: CC Type: CW [1], RA [2]
              CV Type: LSPV [2]
    Remote Label: 205
        Cbit: 1,    VC Type: FastEthernet,    GroupID: 0
        MTU: 1492,   Interface Desc: n/a
        VCCV: CC Type: RA [2]
              CV Type: LSPV [2]
Router# show mpls l2transport vc detail
Local interface: Serial2/0/0 up, line protocol up, PPP up
  MPLS VC type is PPP, interworking type is IP
  Destination address: 10.1.1.152, VC ID: 123, VC status: up
    Output interface: Serial4/0/0, imposed label stack {1003 205}
    Preferred path: not configured
    Default path: active
    Next hop: point2point
  Create time: 00:25:29, last status change time: 00:24:54
  Signaling protocol: LDP, peer 10.1.1.152:0 up
    Targeted Hello: 10.1.1.151(LDP Id) -> 10.1.1.152
    Status TLV support (local/remote)   : enabled/supported
      Label/status state machine        : established, LruRru
      Last local dataplane   status rcvd: no fault
      Last local SSS circuit status rcvd: no fault
      Last local SSS circuit status sent: no fault
      Last local  LDP TLV    status sent: no fault
      Last remote LDP TLV    status rcvd: no fault
    MPLS VC labels: local 105, remote 205
    Group ID: local n/a, remote 0
    MTU: local 1492, remote 1492
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 30, send 29
    byte totals:   receive 2946, send 3364
    packet drops:  receive 0, send 0
```

PE2

```
Router# show mpls l2transport binding
Destination Address: 10.1.1.151,  VC ID: 123
    Local Label: 205
        Cbit: 1,    VC Type: FastEthernet,    GroupID: 0
        MTU: 1492,   Interface Desc: n/a
        VCCV: CC Type: RA [2]
              CV Type: LSPV [2]
    Remote Label: 105
        Cbit: 1,    VC Type: FastEthernet,    GroupID: 0
        MTU: 1492,   Interface Desc: n/a
        VCCV: CC Type: CW [1], RA [2]
              CV Type: LSPV [2]
Router# show mpls l2transport vc detail
Local interface: Fe0/0/0 up, line protocol up, FastEthernet up
  MPLS VC type is FastEthernet, interworking type is IP
  Destination address: 10.1.1.151, VC ID: 123, VC status: up
    Output interface: Se4/0/0, imposed label stack {1002 105}
    Preferred path: not configured
    Default path: active
    Next hop: point2point
  Create time: 00:25:19, last status change time: 00:25:19
  Signaling protocol: LDP, peer 10.1.1.151:0 up
    Targeted Hello: 10.1.1.152(LDP Id) -> 10.1.1.151
    Status TLV support (local/remote)   : enabled/supported
      Label/status state machine        : established, LruRru
      Last local dataplane   status rcvd: no fault
      Last local SSS circuit status rcvd: no fault
      Last local SSS circuit status sent: no fault
      Last local  LDP TLV    status sent: no fault
      Last remote LDP TLV    status rcvd: no fault
    MPLS VC labels: local 205, remote 105
    Group ID: local n/a, remote 0
    MTU: local 1492, remote 1492
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 29, send 30
    byte totals:   receive 2900, send 3426
    packet drops:  receive 0, send 0
```

例：L2VPN プロトコルベースの CLI 機能と関連するコマンドを使用する、L2VPN インターワーキングのための xconnect コンフィギュレーション モードでの MTU 値の設定

次に、L2VPN インターワーキングの例を示します。PE1 ルータには、1492 バイトの MTU 値で設定されているシリアル インターフェイスがあります。PE2 ルータは xconnect コンフィギュレーション モードを使用して、1492 バイトに一致する MTU を設定します。これにより、2 つのルータで VC インターワーキングを形成できるようになります。PE2 ルータが xconnect コンフィギュレーション モードで MTU 値を設定していない場合、インターフェイスはデフォルトで 1500 バイトに設定され、VC はアップ状態になりません。

PE1 の設定

```
template type pseudowire atom-ipiw
 encapsulation mpls
 interworking ip
!
interface Loopback0
```

```
 ip address 10.1.1.151 255.255.255.255
!
interface Serial2/0/0
 mtu 1492
 no ip address
 encapsulation ppp
 no fair-queue
 serial restart-delay 0
interface pseudowire 100
 source template type pseudowire atom-ipiw
 neighbor 10.1.1.152 123
!
l2vpn xconnect context con1
 member <ac_int>
 member pseudowire 100
!
interface Serial4/0/0
 ip address 10.151.100.1 255.255.255.252
 encapsulation ppp
 mpls ip
 serial restart-delay 0
!
router ospf 1
 log-adjacency-changes
 network 10.1.1.151 0.0.0.0 area 0
 network 10.151.100.0 0.0.0.3 area 0
!
mpls ldp router-id Loopback0
```

PE2 の設定

```
template type pseudowire atom-ipiw
 encapsulation mpls
 interworking ip
!
interface Loopback0
 ip address 10.1.1.152 255.255.255.255
!
interface FastEthernet0/0/0
 no ip address
 interface pseudowire 100
 source template type pseudowire atom-ipiw
 neighbor 10.1.1.151 123
!
l2vpn xconnect context con1
 member <ac_int>
 member pseudowire1
!
interface Serial4/0/0
 ip address 10.100.152.2 255.255.255.252
 encapsulation ppp
 mpls ip
 serial restart-delay 0
!
router ospf 1
 log-adjacency-changes
 network 10.1.1.152 0.0.0.0 area 0
 network 10.100.152.0 0.0.0.3 area 0
!
mpls ldp router-id Loopback0
```

show l2vpn atom binding コマンドは、ローカルおよびリモート ルータの MTU 値が 1492 バイトであることを示しています。

PE1

```
Device# show l2vpn atom binding
Destination Address: 10.1.1.152,  VC ID: 123
    Local Label: 105
```

```
        Cbit: 1,    VC Type: PPP,    GroupID: 0
        MTU: 1492,   Interface Desc: n/a
        VCCV: CC Type: CW [1], RA [2]
              CV Type: LSPV [2]
    Remote Label: 205
        Cbit: 1,    VC Type: FastEthernet,    GroupID: 0
        MTU: 1492,   Interface Desc: n/a
        VCCV: CC Type: RA [2]
              CV Type: LSPV [2]
Device# show l2vpn atom vc detail
Local interface: Serial2/0/0 up, line protocol up, PPP up
  MPLS VC type is PPP, interworking type is IP
  Destination address: 10.1.1.152, VC ID: 123, VC status: up
    Output interface: Serial4/0/0, imposed label stack {1003 205}
    Preferred path: not configured
    Default path: active
    Next hop: point2point
  Create time: 00:25:29, last status change time: 00:24:54
  Signaling protocol: LDP, peer 10.1.1.152:0 up
    Targeted Hello: 10.1.1.151(LDP Id) -> 10.1.1.152
    Status TLV support (local/remote)   : enabled/supported
      Label/status state machine        : established, LruRru
      Last local dataplane   status rcvd: no fault
      Last local SSS circuit status rcvd: no fault
      Last local SSS circuit status sent: no fault
      Last local  LDP TLV    status sent: no fault
      Last remote LDP TLV    status rcvd: no fault
    MPLS VC labels: local 105, remote 205
    Group ID: local n/a, remote 0
    MTU: local 1492, remote 1492
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 30, send 29
    byte totals:   receive 2946, send 3364
    packet drops:  receive 0, send 0
```

PE2

```
Device# show l2vpn atom binding
Destination Address: 10.1.1.151,  VC ID: 123
    Local Label: 205
        Cbit: 1,    VC Type: FastEthernet,    GroupID: 0
        MTU: 1492,   Interface Desc: n/a
        VCCV: CC Type: RA [2]
              CV Type: LSPV [2]
    Remote Label: 105
        Cbit: 1,    VC Type: FastEthernet,    GroupID: 0
        MTU: 1492,   Interface Desc: n/a
        VCCV: CC Type: CW [1], RA [2]
              CV Type: LSPV [2]
Device# show l2vpn atom vc detail
Local interface: Fe0/0/0 up, line protocol up, FastEthernet up
  MPLS VC type is FastEthernet, interworking type is IP
  Destination address: 10.1.1.151, VC ID: 123, VC status: up
    Output interface: Se4/0/0, imposed label stack {1002 105}
    Preferred path: not configured
    Default path: active
    Next hop: point2point
  Create time: 00:25:19, last status change time: 00:25:19
  Signaling protocol: LDP, peer 10.1.1.151:0 up
    Targeted Hello: 10.1.1.152(LDP Id) -> 10.1.1.151
    Status TLV support (local/remote)   : enabled/supported
      Label/status state machine        : established, LruRru
      Last local dataplane   status rcvd: no fault
      Last local SSS circuit status rcvd: no fault
      Last local SSS circuit status sent: no fault
      Last local  LDP TLV    status sent: no fault
      Last remote LDP TLV    status rcvd: no fault
    MPLS VC labels: local 205, remote 105
    Group ID: local n/a, remote 0
```

```
    MTU: local 1492, remote 1492
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 29, send 30
    byte totals:   receive 2900, send 3426
    packet drops:  receive 0, send 0
```

例：Any Transport over MPLS（AToM）リモート イーサネット ポート シャットダウンの設定

次に、リモート イーサネット ポートのシャットダウンを有効にする例を示します。

```
configure terminal
!
pseudowire-class eompls
 encapsulation mpls
!
interface GigabitEthernet1/0/0
 xconnect 10.1.1.1 1 pw-class eompls
  remote link failure notification
```

次に、リモート イーサネット ポートのシャットダウンを無効にする例を示します。

```
configure terminal
!
pseudowire-class eompls
 encapsulation mpls
!
interface GigabitEthernet1/0/0
 xconnect 10.1.1.1 1 pw-class eompls
  no remote link failure notification
```

関連する **show** コマンドの出力には、すべてのリモート L2 トンネルの動作ステータスがインターフェイス別に示されます。

```
Router# show interface G1/0/0
GigabitEthernet1/0/0 is L2 Tunnel remote down, line protocol is up
Hardware is GigMac 4 Port GigabitEthernet, address is 0003.ff4e.12a8 (bia 0003.ff4e.12a8)
  Internet address is 10.9.9.2/16
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec, rely 255/255, load 1/255
Router# show ip interface brief
Interface              IP-Address      OK? Method Status Protocol
GigabitEthernet2/0/0 unassigned      YES NVRAM  L2 Tunnel remote down up
GigabitEthernet2/1/0 unassigned      YES NVRAM  administratively down down
```

例：Any Transport over MPLS（AToM）リモート イーサネット ポート シャットダウンの設定（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

次に、リモート イーサネット ポートのシャットダウンを有効にする例を示します。

```
configure terminal
!
template type pseudowire eompls
 encapsulation mpls
!
interface GigabitEthernet1/0/0
```

```
interface pseudowire 100
 source template type pseudowire eompls
 neighbor 10.1.1.1 1
!
l2vpn xconnect context con1
 remote link failure notification
```

次に、リモート イーサネット ポートのシャットダウンを無効にする例を示します。

```
configure terminal
!
template type pseudowire eompls
 encapsulation mpls
!
interface GigabitEthernet1/0/0
 interface pseudowire 100
 source template type pseudowire eompls
 neighbor 10.1.1.1 1
!
l2vpn xconnect context con1
 no remote link failure notification
```

関連する **show** コマンドの出力には、すべてのリモート L2 トンネルの動作ステータスがインターフェイス別に示されます。

```
Router# show interface G1/0/0
GigabitEthernet1/0/0 is L2 Tunnel remote down, line protocol is up
Hardware is GigMac 4 Port GigabitEthernet, address is 0003.ff4e.12a8 (bia 0003.ff4e.12a8)
  Internet address is 10.9.9.2/16
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec, rely 255/255, load 1/255
Router# show ip interface brief
Interface              IP-Address      OK? Method Status Protocol
GigabitEthernet2/0/0 unassigned      YES NVRAM  L2 Tunnel remote down up
GigabitEthernet2/1/0 unassigned      YES NVRAM  administratively down down
```

Any Transport over MPLS に関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
MPLS コマンド	『Cisco IOS Multiprotocol Label Switching Command Reference』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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。	http://www.cisco.com/cisco/web/support/index.html

Any Transport over MPLS の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、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。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *10*：*Any Transport over MPLS* の機能情報

機能名	リリース	機能情報
Any Transport over MPLS（AToM）：ATM AAL5 over MPLS（AAL5oMPLS）	Cisco IOS XE Release 3.2S Cisco IOS XE Release 3.6S	この機能は、Cisco IOS XE Release 3.2S で Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 Cisco IOS XE リリース 3.6S では、Cisco ASR 903 ルータのサポートが追加されました。 この機能で導入される新しいコマンドまたは変更されたコマンドはありません。

機能名	リリース	機能情報
Any Transport over MPLS（AToM）：ATM Cell Relay over MPLS：Packed Cell Relay	Cisco IOS XE Release 3.5S	この機能は、Cisco IOS XE Release 3.5S で Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 Cisco IOS XE Release 3.5S では、Cisco ASR 903 ルータのサポートが追加されました。
Any Transport over MPLS（AToM）：ATM OAM エミュレーション	Cisco IOS XE Release 3.2S	この機能は、Cisco IOS XE Release 3.2S で Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 この機能で導入される新しいコマンドまたは変更されたコマンドはありません。
	Cisco IOS XE Release 2.5	この機能により、AToMデータプレーン パケットの順序制御をサポートすることができるようになります。

機能名	リリース	機能情報
Any Transport over MPLS（AToM）：Ethernet over MPLS（EoMPLS）	Cisco IOS XE Release 2.4 Cisco IOS XE Release 3.5S	この機能により、レイヤ2イーサネット VLAN パケットをさまざまな送信元から MPLS バックボーンを介して送信できます。Ethernet over MPLS は、既存のレイヤ3サービスに加えてレイヤ2サービスを提供できるようにすることで、MPLS バックボーンの有用性を広げます。MPLS バックボーンの両端で PE ルータを設定することで、MPLS バックボーン ネットワークがレイヤ2 VLAN パケットを受け入れることができるようになります。 この機能は、Cisco IOS XE リリース 2.4 で、Cisco ASR 1000 シリーズ ルータに導入されました。 Cisco IOS XE Release 3.5S では、Cisco ASR 903 ルータのサポートが追加されました。

機能名	リリース	機能情報
Any Transport over MPLS（AToM）：Ethernet over MPLS：ポート モード（EoMPLS）	Cisco IOS XE Release 2.4	Ethernet over MPLS（EoMPLS）は、MPLS コアを介したイーサネット フレームの転送機能です。宛先の Media Access Control（MAC）情報に関係なく、特定のイーサネットまたは仮想 LAN（VLAN）セグメントで受信するすべてのフレームを転送します。イーサネットインターフェイスからのパケット転送のために MAC ラーニングや MAC ルックアップは実行されません。ポート モードでは、インターフェイスに着信したフレームを MPLS パケットにパッキングして、MPLS バックボーンを介して出力インターフェイスに転送できます。 この機能は、Cisco IOS XE リリース 2.4 で、Cisco ASR 1000 シリーズ ルータに導入されました。
Any Transport over MPLS-Ethernet over MPLS 機能拡張：Fast Reroute	Cisco IOS XE Release 2.4	AToM は、Fast Reroute（FRR）のサポートにより MPLS トラフィック エンジニアリング（TE）トンネルを使用できます。この機能により、Ethernet over MPLS（EoMPLS）の FRR 機能が拡張されます。 この機能は、Cisco IOS XE リリース 2.4 で、Cisco ASR 1000 シリーズ ルータに導入されました。

機能名	リリース	機能情報
Any Transport over MPLS（AToM）：Frame Relay over MPLS（FRoMPLS）	Cisco IOS XE リリース 3.2.1S	この機能は、Cisco IOS XE Release 3.2.1S で Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 この機能で導入される新しいコマンドまたは変更されたコマンドはありません。
Any Transport over MPLS（AToM）：HDLC over MPLS（HDLCoMPLS）	Cisco IOS XE Release 3.2S	この機能は、Cisco IOS XE Release 3.2S で Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 この機能で導入される新しいコマンドまたは変更されたコマンドはありません。
Any Transport over MPLS（AToM）：Layer 2 Quality of Service（QoS）	Cisco IOS XE Release 2.3	この機能により、Quality of Service（QoS）機能（トラフィック ポリシング、トラフィック シェーピング、パケットマーキング、パケットのマッピングなど）のサポートが提供されます。 この機能は、Cisco IOS XE リリース 2.3 で、Cisco ASR 1000 シリーズ ルータに導入されました。
Any Transport over MPLS（AToM）：PPP over MPLS（PPPoMPLS）	Cisco IOS XE Release 3.2S	この機能は、Cisco IOS XE Release 3.2S で Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 この機能で導入される新しいコマンドまたは変更されたコマンドはありません。

機能名	リリース	機能情報
Any Transport over MPLS（AToM）：リモート イーサネット ポート シャットダウン	Cisco IOS XE Release 2.4	この機能により、Ethernet over MPLS（EoMPLS）擬似回線のローカル エンドのサービス プロバイダー エッジ（PE）ルータが、リモート リンク障害を検出し、ローカル カスタマー エッジ（CE）ルータのイーサネット ポートをシャットダウンすることができます。ローカル CE ルータのイーサネット ポートがシャットダウンされるので、ルータは障害リモート リンクに連続してトラフィックを送信しても、データを損失することはありません。これは、リンクがスタティック IP ルートとして設定されている場合には利点となります。 この機能は、Cisco IOS XE リリース 2.4 で、Cisco ASR 1000 シリーズ ルータに導入されました。
ATM Port Mode Packed Cell Relay over MPLS	Cisco IOS XE Release 3.5S	この機能は、Cisco IOS XE Release 3.5S で Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。
ATM VC クラス サポート	Cisco IOS XE Release 2.3	ATM VC クラス サポート機能により、VC クラスの一部として、AAL5 および AAL0 のカプセル化を指定できます。 この機能は、Cisco IOS XE リリース 2.3 で、Cisco ASR 1000 シリーズ ルータに導入されました。

機能名	リリース	機能情報
AToM トンネル選択	Cisco IOS XE Release 2.3	AToM トンネル選択機能により、トラフィックが使用するパスを指定できます。MPLS TE トンネルまたは宛先 IP アドレスかドメイン ネーム サーバ（DNS）名のいずれかを指定できます。 また、優先パスが到達不能の場合に、VC でデフォルト パス（LDPがシグナリングに使用するパス）を使用するかどうかを指定することもできます。このオプションは、デフォルトではイネーブルになっているため、明示的にディセーブルにする必要があります。 Cisco IOS XE Release 2.3 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。
AToM：ATM Cell Relay over MPLS：VP モード	Cisco IOS XE Release 2.3	AToM：ATM Cell Relay over MPLS：VPモード機能により、VP モードで各 MPLS パケットに 1 つの ATM セルを挿入できます。 この機能は、Cisco IOS XE リリース 2.3 で、Cisco ASR 1000 シリーズ ルータに導入されました。
AToM：Single Cell Relay：VC モード	Cisco IOS XE Release 2.3	AToM：Single Cell Relay：VC モード機能により、VC モードで各 MPLS パケットに 1 つの ATM セルを挿入できます。 この機能は、Cisco IOS XE リリース 2.3 で、Cisco ASR 1000 シリーズ ルータに導入されました。

機能名	リリース	機能情報
GRE トンネル用の MPLS MTU コマンド	Cisco IOS XE Release 2.6	この機能を使用すると、GRE トンネルの MPLS MTU サイズを、現在のデフォルト サイズだけでなく最大サイズにも設定できます。 次のコマンドがこのリリースで変更されました：**mplsmtu**。
MPLS L2VPN Clear Xconnect コマンド	Cisco IOS XE Release 3.1S	これらの機能を使用すると、次のことが可能です。 • インターフェイスに関連付けられたVC、ピアアドレス、または設定済みのxconnect回線接続をすべてリセットします。 • ダイナミック擬似回線のコントロール ワードを設定します（L2VPN 擬似回線コントロール ワード設定）。 • スタティック擬似回線のATMセルパッキングをイネーブルにします。 これらの機能により、次のコマンドが導入または変更されました：**cell-packing**、**clearxconnect**、**control-word**、**encapsulation**（Any Transport over MPLS）、**oam-acemulation-enable**。

機能名	リリース	機能情報
Ethernet over MPLS（EoMPLS）用のサブインターフェイスごとの MTU	Cisco IOS XE Release 2.4	この機能により、xconnect サブインターフェイス コンフィギュレーション モードで最大伝送ユニット（MTU）値を指定することができます。xconnect サブインターフェイス コンフィギュレーション モードを使用して MTU 値を設定する場合、インターフェイスが変更不可能な MTU 値を個別に持つ状況に適した擬似回線接続を確立します。 Cisco IOS XE Release 2.4 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 このリリースで導入または変更されたコマンドはありません。
VLAN ID 書き換え	Cisco IOS XE Release 2.4	VLAN ID の書き換え機能を使用すると、トンネルの両端で異なる VLAN ID を持つ VLAN インターフェイスを使用できます。 この機能は、Cisco IOS XE リリース 2.4 で、Cisco ASR 1000 シリーズ ルータに導入されました。

機能名	リリース	機能情報
単一 PW を使用した AToM ロード バランシング	Cisco IOS XE Release 3.4S	単一 PW を使用した AToM ロード バランシング機能により、同一擬似回線内のパケットをロードバランシングできます。このためには、同一擬似回線内のパケットを、接続回線で受信されるパケットの一部のフィールドに基づいてさらに各種フローに分類します。 この機能は、Cisco IOS XE Release 3.4S で Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。
MPLS 擬似回線の Flow-Aware Transport	Cisco IOS XE Release 3.11S	MPLS 擬似回線の Flow-Aware Transport 機能では、MPLS ラベル スタック下部にフロー ラベルを追加し、パケットをさまざまなフローにさらに分類することで、同じ擬似回線内でのパケットのロード バランシングを可能にします。
EoMPLS over IPv6 GRE トンネル	Cisco IOS XE Release 3.15S	EoMPLS over IPv6 GRE トンネル機能により、GRE トンネルを使用した IPV6 ネットワーク経由での EoMPLS トラフィックのトンネリングがサポートされます。

第 4 章

L2VPN インターワーキング

インターワーキングとは、2 つの異種接続回線（AC）を相互接続するために必要な変換機能です。インターワーキング機能にはいくつかの種類があります。使用される機能は、使用する AC のタイプ、伝送されるデータのタイプ、および必要とする機能性のレベルによって異なる場合があります。Cisco IOS XE ソフトウェアでサポートしているレイヤ 2 バーチャル プライベート ネットワーク（L2VPN）インターワーキング機能は、主にブリッジ型インターワーキングおよびルーテッド インターワーキングの 2 種類です。

マルチ プロトコル ラベル スイッチング（MPLS）と IP を介したレイヤ 2（L2）転送は、イーサネット間やポイントツーポイント プロトコル（PPP）間などの like-to-like AC 向けにすでに存在します。L2VPN インターワーキングはこの機能に基づいて構築されており、異なる AC どうしが接続できる機能を備えています。インターワーキング機能を使用することで、異種の L2 カプセル化どうしの変換が容易になります。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース 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、機能情報の表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シスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

L2VPN インターワーキングの前提条件

デバイスに L2VPN インターワーキングを設定する前に、Cisco Express Forwarding を有効にする必要があります。

HDLC-to-Ethernet インターワーキング

- ハイレベル データ リンク制御（HDLC）カスタマー エッジ（CE）およびプロバイダー エッジ（PE）のデバイスにシリアルコントローラおよびインターフェイスが設定されていることを確認します。

```
enable
 configure terminal
  controller e1 2/0
   channel-group 0 timeslots 1
   no shutdown
!
interface Serial 2/0:0
 no shutdown
end
```

- HDLC-to-Ethernet ブリッジ型インターワーキングを設定する前に、ブリッジングが HDLC CE デバイスに設定されていることを確認します。

```
enable
 configure terminal
  bridge irb
  bridge 1 protocol ieee
  bridge 1 route ip
!
interface Serial 2/0:0
 no bridge-group 1
 no ip address
!
interface BVI1
 no ip address
 ip address 192.0.2.1 255.255.255.0
 no shutdown
!
interface Serial 2/0:0
 no ip address
 encapsulation hdlc
 bridge-group 1
  no shutdown
end
```

- HDLC-to-Ethernet ルーテッド インターワーキングを設定する前に、IP アドレスが HDLC CE デバイスに設定されていることを確認します。

```
interface Serial 2/0:0
 ip address 192.0.2.1 255.255.255.0
 encapsulation hdlc
 no shutdown
end
```

L2VPN インターワーキングの制約事項

L2VPN インターワーキングの一般的な制約事項

ここでは、L2VPNインターワーキングに適用される全般的な制約事項を示します。プラットフォーム固有またはデバイス固有のその他の制約事項は、以降の項で示します。

- フラグメンテーションはサポートされていないので、ACに設定するMTUはネットワークのコアの MTU 以下であることが必要です。
- プロバイダーエッジ（PE）ルータ上のインターワーキング タイプは、ピア PE ルータ上のインターワーキング タイプと一致する必要があります。
- ネイティブ VLAN との IP インターワーキングはサポートされていません。
- イーサネット VLAN（タイプ 4）インターワーキングはサポートされていません。
- L2VPN インターワーキングでは、次の Quality of Service（QoS）機能のみがサポートされます。
  - トンネル ヘッダーのスタティック IP タイプ オブ サービス（ToS）または MPLS EXP ビット設定
  - VLAN 優先順位ビットから MPLS EXP ビットへの 1 対 1 マッピング

ルーテッド インターワーキングの制約事項

ルーテッド インターワーキングには、次の制約事項があります。

- マルチポイント フレーム リレー（FR）はサポートされません。
- IP ToS、DSCP、およびその他の IP ヘッダー フィールドでの QoS 分類は、サポートされません。
- セキュリティ アクセス コントロール リスト（ACL）および IP ヘッダー フィールド解析に基づくその他の機能は、サポートされません。
- ルーテッド モードでは、イーサネット PE ルータにカスタマー エッジ（CE）ルータを 1 台だけ接続できます。
- AC と擬似回線は 1 対 1 の関係である必要があります。ポイントツーマルチポイントまたはマルチポイントツーポイント設定はサポートされません。
- イーサネットから非イーサネットへの設定では、CEルータにポイントツーポイント オペレーションのルーティング プロトコルを設定する必要があります。

- IP インターワーキング モードでは、IPv4（0800）変換がサポートされます。PE ルータはアドレス解決プロトコル（ARP）（0806）パケットをキャプチャし、独自の MAC アドレス（プロキシ ARP）で応答します。その他はすべてドロップされます。
- イーサネットには、2 台の IP デバイス（PE ルータと CE ルータ）だけが含まれている必要があります。PE ルータはプロキシ ARP を実行し、受信したすべての ARP 要求に応答します。したがって、イーサネット セグメントには、CE ルータ 1 台と PE ルータ 1 台のみ存在できます。
- CE ルータによってスタティック ルーティングが実行されている場合、次のタスクを実行できます。
  - CE ルータにトラフィックを正しく転送するには、PE ルータが CE ルータの MAC アドレスを認識している必要があります。イーサネット PE ルータは、インターネット制御メッセージプロトコル（ICMP）ルータ ディスカバリ プロトコル（RDP）請求メッセージを、送信元 IP アドレスをゼロとして送信します。イーサネット CE ルータは、この請求メッセージに応答します。ICMP RDP 請求メッセージに応答するように Cisco CE ルータのイーサネット インターフェイスを設定するには、インターフェイス コンフィギュレーション モードで **ipirdp** コマンドを発行します。CE ルータを設定しないと、CE ルータによって PE ルータにトラフィックが送信されるまで、トラフィックはドロップされます。
  - CE ルータでルータ ディスカバリ プロトコルを実行しないようにするには、インターフェイス モードで **ipirdpmaxadvertinterval0** コマンドを実行します。
- イーサネット PE ルータ上のインターワーキング設定を変更する場合は、隣接する CE ルータ上の ARP エントリをクリアして、新しい MAC アドレスを学習できるようにします。このように設定しないと、トラフィック ドロップが発生する可能性があります。

PPP インターワーキングの制約事項

PPP インターワーキングには次の制約事項があります。

- PPP セッションと擬似回線は 1 対 1 の関係である必要があります。擬似回線上での複数の PPP セッションの多重化はサポートされません。
- IP（IPv4（0021）インターワーキングのみがサポートされます。リンク制御プロトコル（LCP）パケットおよびインターネット プロトコル制御プロトコル（IPCP）パケットは PE ルータで終端されます。その他はすべてドロップされます。
- デフォルトでは、PE ルータは CE ルータがリモート CE ルータの IP アドレスを認識していると想定します。
- パスワード認証プロトコル（PAP）およびチャレンジハンドシェーク認証プロトコル（CHAP）認証がサポートされています。

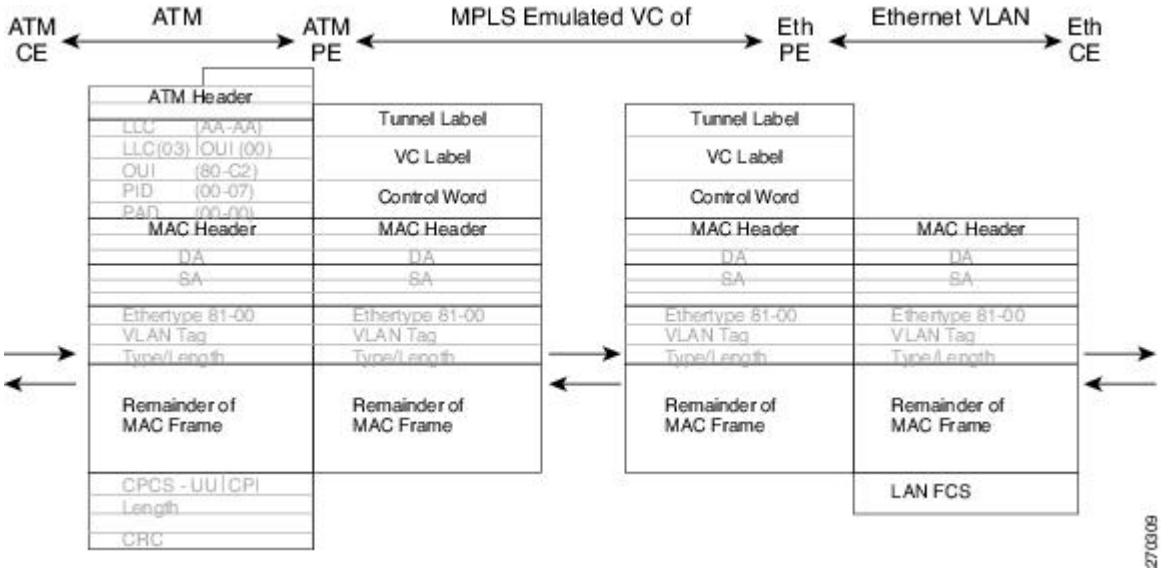
Ethernet/VLAN-to-ATM AAL5 インターワーキングの制約事項

Ethernet/VLAN to ATM AAL5 Any Transport over MPLS（AToM）には、次の制限事項があります。

- 次の変換のみサポートされています。他の変換は破棄されます。
  - LAN FCS のないイーサネット（AAAA030080C200070000）
  - スパニング ツリー（AAAA030080C2000E）
- ブリッジ型インターワーキングでサポートされている ATM カプセル化タイプは aal5snap です。ただし、ルーテッド インターワーキングでサポートされている ATM カプセル化タイプは aal5snap および aal5mux です。
- ATM の既存の QoS 機能は、ATM CLP ビットの設定を含め、サポートされています。
- ATM AAL5 VC モードのみがサポートされています。ATM VP およびポート モードはサポートされません。
- SVC はサポートされません。
- 個別の AAL5 ATM セルは、擬似回線を越えて送信される前に、フレームに組み立てられます。
- AAL5 ではないトラフィック（運用、管理、および保守（OAM）セルなど）はルート プロセッサ（RP）レベルで処理されるようにパントされます。ATM の PE ルータ上で実行する OAM セルエミュレーションを（**oam-acemulation-enable** CLI コマンドを使用して）設定した VC では、設定した間隔で CE ルータにエンドツーエンドの F5 ループバック セルを送信できます。
- 擬似回線がダウンしている場合は、F5 エンドツーエンド セグメントのアラーム表示信号およびリモート障害表示（AIS/RDI）が、PE ルータから CE ルータに送信されます。

- イーサネット CE ルータから到達したイーサネット フレームに 802.1Q ヘッダー（VLAN ヘッダー）が含まれている場合、エンドポイント接続（イーサネット ポート モード）のタイプにより、VLAN ヘッダーは擬似配線を越えてフレームに留まります（下の図を参照）。

図 *9*：***ATM-to-Ethernet AToM*** ブリッジ型インターワーキングのプロトコルスタック（***VLAN*** ヘッダーあり）



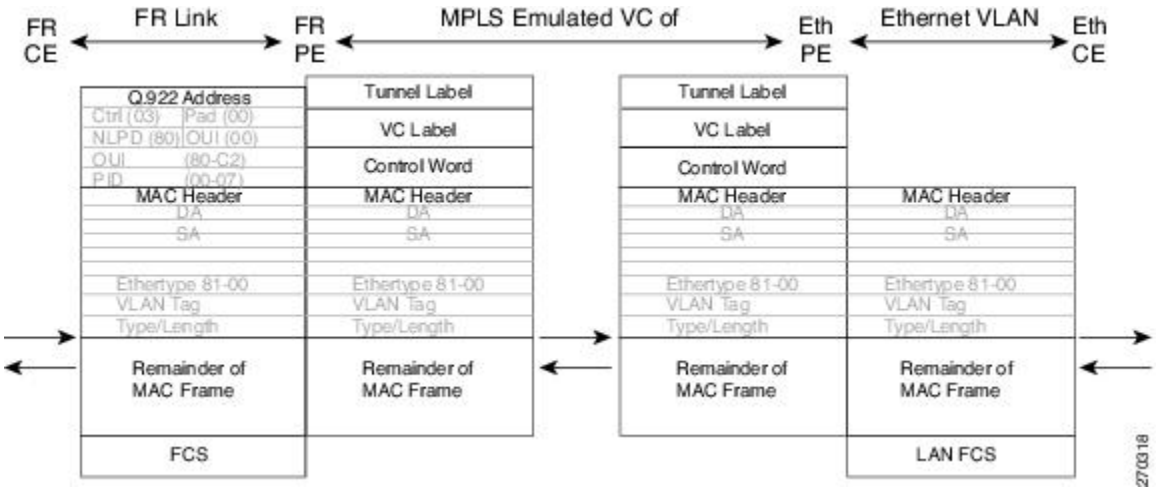
Ethernet/VLAN-to-Frame Relay インターワーキングの制約事項

Ethernet/VLAN-to-Frame Relay AToM には、次の制約事項があります。

- 次の変換のみサポートされています。他の変換は破棄されます。
  - LAN FCS のないイーサネット（0300800080C20007）
  - スパニング ツリー（0300800080C2000E）
- PE ルータは、CE ルータからの送信ではシスコと IETF の両方のフレーム リレーについてカプセル化の変換を自動的にサポートしますが、CE ルータへの送信では IETF への変換のみをサポートします。シスコ カプセル化方式で送信するように設定されている場合でも Cisco CE ルータでは IETF カプセル化方式が受信時に管理されるため、Cisco CE ルータでは問題が発生しません。
- PVC ステータス シグナリングは、like-to-like の場合と同様に動作します。PE ルータは、擬似回線のアベイラビリティに基づいて CE ルータに PVC ステータスをレポートします。
- MPLS で接続する場合は、AC 最大伝送ユニット（MTU）がサポートされている MTU の範囲内にある必要があります。
- フレーム リレー DLCI モードのみがサポートされます。フレーム リレー ポート モードはサポートされません。

- イーサネット フレームに 802.1Q ヘッダー（VLAN ヘッダー）が含まれている場合、エンドポイント接続（イーサネット ポート モード）のタイプにより、VLAN ヘッダーは擬似配線を越えてフレームに留まります（下の図を参照）。
- ルーテッド インターワーキングでサポートされているフレーム リレー カプセル化タイプは着信トラフィックのシスコおよびIETF です。ただし、IETF はCE ルータへの発信トラフィックに対してもサポートされています。

図 *10*：*Frame Relay-to-Ethernet AToM* ブリッジ型インターワーキングのプロトコル スタック（*VLAN* ヘッダーあり）



HDLC-to-Ethernet インターワーキングの制約事項

- 「シスコ以外の」ハイレベルデータ リンク制御（HDLC）カプセル化はサポートされていません。
- IPv6 はルーテッド モードでサポートされていません。

L2VPN インターワーキングに関する情報

L2VPN インターワーキングの概要

MPLS および IP を介した L2 トランスポートは、Ethernet-to-Ethernet や PPP-to-PPP などの like-to-like AC に対してすでに存在します。L2VPN インターワーキングはこの機能に基づいて構築されており、異なる AC どうしが接続できる機能を備えています。インターワーキング機能を使用することで、異種の L2 カプセル化どうしの変換が容易になります。

次のインターワーキングの組み合わせだけがサポートされます。

- ATM-to-Ethernet：ルーテッド インターワーキング
- ATM-to-Ethernet：ブリッジ型インターワーキング
- Frame relay-to-Ethernet：ブリッジ型インターワーキング
- PPP-to-Ethernet：ルーテッド インターワーキング
- HDLC-to-Ethernet：ブリッジ型およびルーテッド インターワーキング

L2VPN インターワーキング モード

L2VPNインターワーキングは、イーサネット（ブリッジ型）モードまたはIP（ルーテッド）モードで機能します。L2VPNインターワーキングは、イーサネットVLAN（タイプ4）モードをサポートしていません。次の方法でモードを指定します。

- 古いレガシーの CLI コマンドを使用している場合、**interworking** {**ethernet** | **ip**} コマンドを擬似回線クラス コンフィギュレーション モードで使用できます。
- 新しい L2VPN プロトコルベースの CLI コマンドを使用している場合、**interworking** {**ethernet** | **ip**} コマンドを xconnect コンフィギュレーション モードで使用できます。

interworking コマンドを実行すると、AC はローカルで終端されます。この 2 つのキーワードには次の機能があります。

- **ethernet** キーワードを指定すると、AC からイーサネット フレームが抽出されて、擬似回線に送信されます。イーサネットのエンドツーエンドの送信が再開します。イーサネット フレーム以外の AC フレームはドロップされます。VLAN の場合、VLAN タグが削除され、タグなしイーサネット フレームが残されます。
- **ip** キーワードを指定すると、AC から IP パケットが抽出されて、擬似回線に送信されます。IPv4 パケットを含まない AC フレームはドロップされます。

次の項では、イーサネット インターワーキング モードおよび IP インターワーキング モードについて詳しく説明します。

イーサネット（ブリッジ型）インターワーキング

イーサネット インターワーキングは、ブリッジ型インターワーキングとも呼ばれます。イーサネットフレームは、擬似回線を介してブリッジされます。CEルータは、ネイティブでイーサネットをブリッジすることも、ブリッジ仮想インターフェイス（BVI）やルーテッド ブリッジ カプセル化（RBE）などのブリッジ型カプセル化を使用してルーティングすることもできます。PEルータは、イーサネット like-to-like モードで動作します。

このモードは次のサービスを実現するために使用します。

- LAN サービス：たとえば、複数のサイトを有する企業が、いくつかのサイトでサービス プロバイダー（SP）ネットワークへのアクセスにイーサネット接続を使用して、その他のサイトでは、ATM 接続を使用する場合などです。このような企業で、そのすべてのサイトへの

LAN 接続が要求される場合、あるサイトのイーサネットまたは VLAN からのトラフィックを IP/MPLS ネットワークを通じて送信し、別のサイトの ATM VC に対してブリッジ型トラフィックとしてカプセル化できます。

- 接続サービス：たとえば、Internal Gateway Protocol（IGP）ルーティング プロトコルを実行する複数のサイトを有する企業で、ブロードキャスト リンクと非ブロードキャスト リンクのプロシージャに互換性がない場合などです。ここでは、いくつかのサイトで Open Shortest Path First（OSPF）または Intermediate System-to-Intermediate System（IS-IS）などの IGP が実行されています。このような場合、ルートアドバタイズメントや指定ルータのように、基礎となる L2 プロトコルに依存する手順が一部に存在し、ポイントツーポイント ATM 接続とブロードキャストイーサネット接続とでは手順が異なっていることがあります。したがって、ATM 上でのブリッジ型カプセル化を使用して、IGP を実行している CE ルータ間の同種イーサネット接続を実現できます。

IP（ルーテッド）インターワーキング

IP インターワーキングは、ルーテッド インターワーキングとも呼ばれます。CE ルータは、CE ルータと PE ルータ間のリンク上で IP をカプセル化します。新しいタイプの VC を使用して、MPLS の IP 擬似回線に対するシグナリングを実行します。この擬似回線をまたいで L2 カプセル化と IP カプセル化との変換が必要です。L2 カプセル化が異なると、アドレス解決とルーティング プロトコルの処理も異なるので、これらの操作には特別の配慮が必要です。

このモードを使用して、サイトへの L2 接続にかかわらず、これらのサイト間に IP 接続を提供します。本質的にはポイントツーポイントであり、サービス プロバイダーはカスタマーのルーティング情報を保持しないため、レイヤ 3 VPN とは異なります。

アドレス解決は、次のようにカプセル化に依存します。

- イーサネットではアドレス解決プロトコル（ARP）を使用します。
- ATM では Inverse ARP を使用します。
- PPP では IP 制御プロトコル（IPCP）を使用します。
- HDLC ではシリアル ライン ARP（SLARP）を使用します。

したがって、アドレス解決を PE ルータで終端する必要があります。エンドツーエンドのアドレス解決はサポートされません。ルーティング プロトコルは、ブロードキャストとポイントツーポイント メディアでは異なる動作をします。イーサネットでは、CE ルータでスタティック ルーティングを使用するか、イーサネット側をポイントツーポイント ネットワークとして扱うルーティング プロトコルを設定する必要があります。

ルーテッド インターワーキングでは、AC から抽出された IP パケットは擬似回線に送信されます。この擬似回線は、IP レイヤ 2 転送（VC タイプ 0x000B）の Like-to-Like モードで動作します。ネットワーク サービス プロバイダー（NSP）側では、AC テクノロジーに基づいて、目的とするアダプテーションがインターワーキング機能によって実行されます。IPv4 ではないパケットはドロップされます。

ルーテッド インターワーキングでは、次の事項に留意する必要があります。

- アドレス解決パケット（ARP）、Inverse ARP、および IPCP はルーティング プロトコルにパントされます。したがって、PE ルータの NSP はアドレス解決のために次の機能を提供する必要があります。
  - イーサネット：PE デバイスは、CE ルータからのすべての ARP 要求に対してプロキシ ARP サーバとして機能します。PE ルータは、そのローカル インターフェイスの MAC アドレスで応答します。
  - ATM とフレーム リレーとのポイントツーポイント：デフォルトでは、フレーム リレーでも ATM でも、ポイントツーポイントのサブインターフェイスでは Inverse ARP が動作しません。IP アドレスとサブネット マスクによって、接続されたプレフィックスが定義されているので、CE デバイスでは設定は不要です。
- インターワーキングでは、起動する擬似回線で両方の AC の MTU が一致している必要があります。一方の AC のデフォルトの MTU が、他方の AC の MTU と一致している必要があります。次の表では、さまざまな AC で設定できる MTU の範囲を示しています。

表 *11*：さまざまな *AC* の *MTU* の範囲

AC のタイプ	サポートされている MTU の範囲
ATM	64 ～ 17940
ギガビット イーサネット	1500 ～ 4470
POS	64 ～ 9102
ファスト イーサネット	64 ～ 9192

（注） AC に設定する MTU は、コア ネットワークの MTU 以下であることが必要です。そのようにすることで、トラフィックがフラグメント化することがなくなります。

- OSPF を実行するイーサネット接続 VC を備えた CE ルータは、**ospfIfType** オプションを指定して設定する必要があります。これにより、基礎となる物理ブロードキャスト リンクが OSPF プロトコルによって P2P リンクとして扱われます。

Ethernet VLAN-to-ATM AAL5 インターワーキング

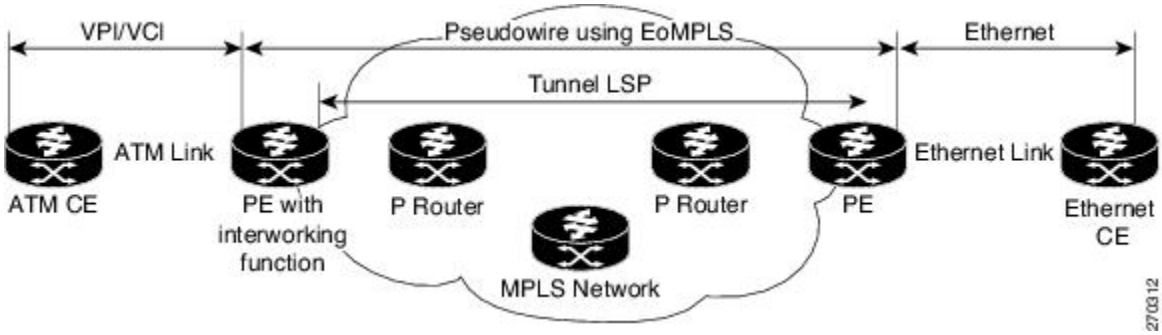
ここでは、次の内容について説明します。

ATM AAL5-to-Ethernet Port AToM：ブリッジ型インターワーキング

このインターワーキング タイプにより、それぞれ異なる PE ルータに接続した ATM 接続 VC とイーサネット接続 VC と間で相互運用が可能になります。ブリッジ型（イーサネット）インターワーキング メカニズムに対応するブリッジ型カプセル化を使用します。

インターワーキング機能は、ATM AAL5 上でのマルチプロトコル カプセル化に基づいて、ATM 接続 VC に接続された PE ルータで実行されます（次の図を参照）。

図 *11*：*ATM-to-Ethernet AToM* ブリッジ型インターワーキングのネットワーク トポロジ



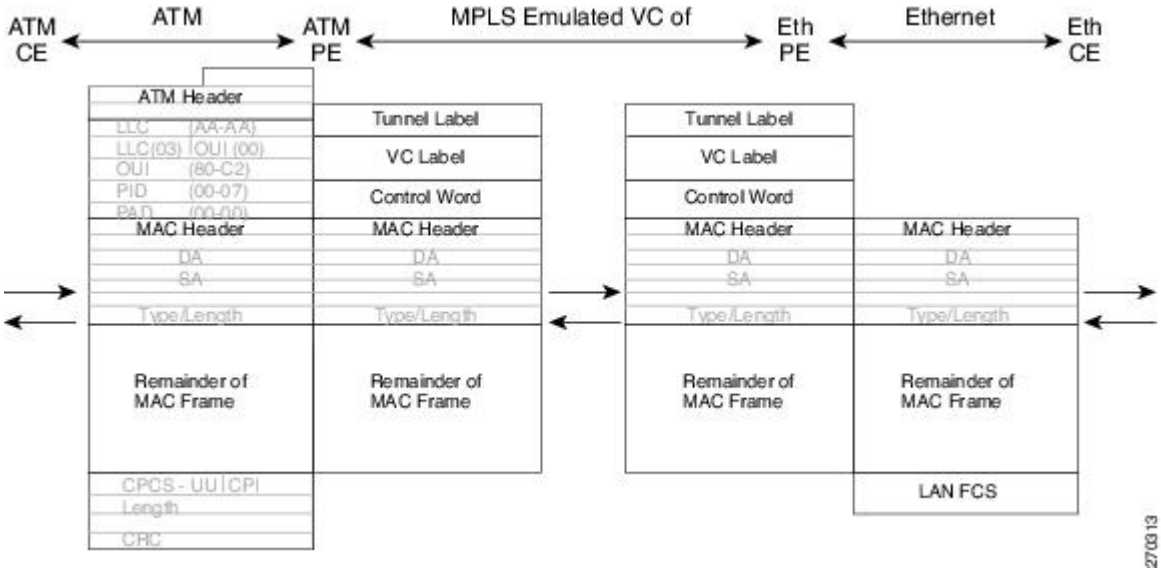
このアーキテクチャの利点は、イーサネット PE ルータ（イーサネット セグメントに接続されている）がイーサネット like-to-like と同じように動作することです。

インターワーキング機能を備えた PE ルータでは、ATM セグメントから MPLS クラウドへの方向では、ブリッジ型カプセル化（ATM/SubNetwork Access Protocol（SNAP）ヘッダー）は破棄され、VC タイプ 5（イーサネット）を使用して擬似回線で転送するために必要なラベルを付けてイーサネット フレームがカプセル化されます（次の図を参照）。

逆方向の転送では、MPLS クラウドからのラベルの廃棄後、ブリッジ型カプセル化を使用してイーサネット フレームが AAL5 によってカプセル化されます。

次の図は、ATM-to-Ethernet AToM ブリッジ型インターワーキングのプロトコル スタックを示しています。ATM 側に AAL5SNAP のカプセル化タイプがあります。

図 *12*：***ATM-to-Ethernet AToM*** ブリッジ型インターワーキングのプロトコル スタック：***VLAN*** ヘッダーなし



ATM AAL5-to-Ethernet VLAN 802.1Q AToM：ブリッジ型インターワーキング

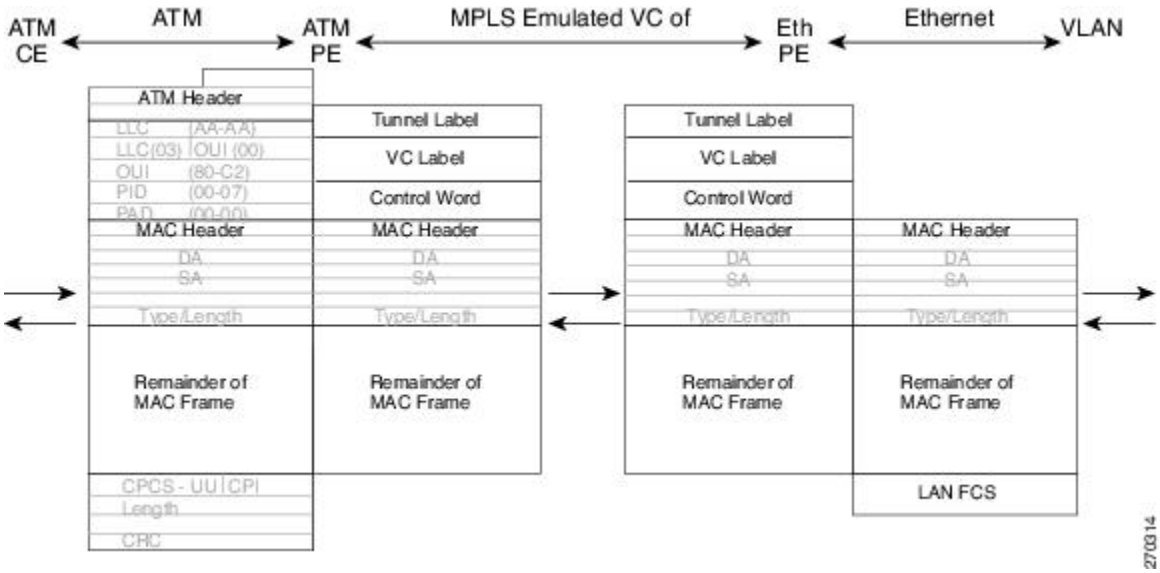
このインターワーキング タイプにより、それぞれ異なる PE ルータに接続した ATM 接続 VC とイーサネット VLAN 接続 VC と間で相互運用が可能になります。ブリッジ型（イーサネット）インターワーキング メカニズムに対応するブリッジ型カプセル化を使用します。

インターワーキング機能は、ATM-to-Ethernet ポートの場合と同じように実行され、ATM 接続 VC に接続された PE ルータ上に実装されます。実装は ATM AAL5 上でのマルチプロトコル カプセル化に基づいています（次の図を参照）。

イーサネット側に接続された PE ルータの場合、着信パケットに VLAN ヘッダーがあるため 1 つの大きな違いがあります。PE ルータは VLAN CE ルータからの着信フレームの VLAN ヘッダーを破棄し、MPLS クラウドからやってくるイーサネット フレームに VLAN ヘッダーを挿入します。擬似回線（VC タイプ 5）上で送信されるフレームは、VLAN ヘッダーのないイーサネット フレームです。

ATM AAL5 上でのカプセル化を次の図に示します。

図 *13*：*ATM-to-VLAN AToM* ブリッジ型インターワーキングのプロトコル スタック



ATM-to-Ethernet：ルーテッド インターワーキング

ルーテッド インターワーキングを実行するには、ATM PE ルータとイーサネット PE ルータの両方を設定する必要があります。次の図は、ATM とイーサネットとの間のルーテッドインターワーキングを示します。擬似回線の IP カプセル化は、ATM CE ルータから到着する ATM パケットに対して実行されます。

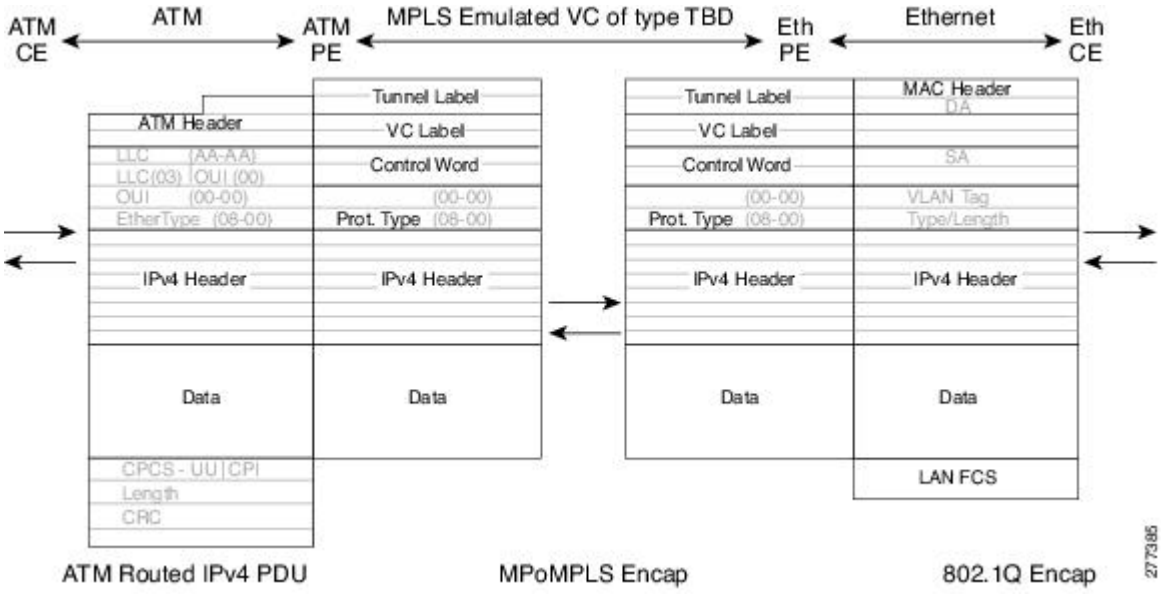
アドレス解決は ATM PE ルータで実施されます。これは、ATM CE ルータが Inverse ARP を実行する場合に必要です。ATM CE ルータを、ポイントツーポイント（P2P）サブインターフェイスまたは静的マップを使用して設定する場合は不要です。

パケットがイーサネット CE ルータから到着する場合、イーサネット PE ルータは L2 フレーム タグを削除し、次いで擬似回線での IPoMPLS カプセル化を使用して IP パケットを出力 PE ルータに転送します。イーサネット PE ルータは、受信する L2 フレームの L2 回線 ID、VLAN ID またはポート ID に基づいて転送の判断を下します。ATM PE ルータでは、ラベルの廃棄後、IP パケットは RFC 2684 に基づきルーテッド カプセル化を使用して AAL5 でカプセル化されます。

イーサネット PE ルータでのアドレス解決は、イーサネット CE ルータで静的 ARP を設定する場合に、またはイーサネット PE ルータでのプロキシ ARP によって実行することができます。プロキシ ARP を使用する場合、リモート CE ルータの IP アドレスは動的に学習されます。

ルーティング プロトコルは、イーサネット CE ルータで P2P モードで動作するように設定する必要があります。

図 *14*：***ATM-to-Ethernet*** のプロトコル スタック：ルーテッド インターワーキング



Ethernet VLAN-to-Frame Relay：インターワーキング

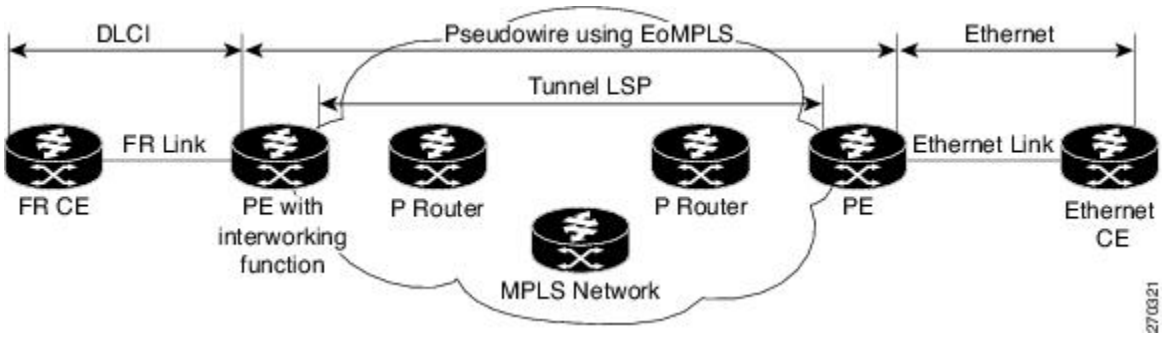
ここでは、次の内容について説明します。

Frame Relay DLCI-to-Ethernet Port AToM：ブリッジ型インターワーキング

このインターワーキング タイプは、異なる PE ルータに接続しているフレーム リレー接続 VC とイーサネット接続 VC との間を相互運用します。ブリッジ型（イーサネット）インターワーキング メカニズムに対応するブリッジ型カプセル化を使用します。

FR-to-Ethernet ポートの場合は、インターワーキング機能は、フレーム リレー経由のマルチプロトコル インターコネクトに基づいて FR 接続 VC に接続される PE ルータで実行されます（下図を参照）。このインターワーキングは ATM-to-Ethernet の場合と同様に実現されます。

図 *15*：*FR-to-Ethernet AToM* のブリッジ型インターワーキングのネットワーク トポロジ



このアーキテクチャの利点は、イーサネット PE ルータ（イーサネット セグメントに接続されている）がイーサネット like-to-like サービスと同様に動作することです。擬似回線ラベルはイーサネット ポートに割り当てられ、次にリモートの Label Distribution Protocol（LDP）セッションがラベルをピア PE ルータに配布します。イーサネット フレームは、Ethernet over MPLS（EoMPLS）を使用した MPLS ネットワークを通じて転送されます。

インターワーキング機能を備えた PE ルータでは、フレーム リレー セグメントから MPLS クラウドへの方向で、ブリッジ型カプセル化（FR/SNAP ヘッダー）は破棄され、VC タイプ 5（イーサネット）を使用して擬似回線で転送するために必要なラベルを伴ってイーサネット フレームがカプセル化されます（下図を参照）。

逆方向の転送では、MPLS クラウドからのラベル ディスポジション後、ブリッジ型カプセル化を使用してイーサネット フレームがフレーム リレー上でカプセル化されます。

サポートされる変換は次のとおりです。

- LAN FCS のないイーサネット（0300800080C20007）
- スパニング ツリー（0300800080C2000E）

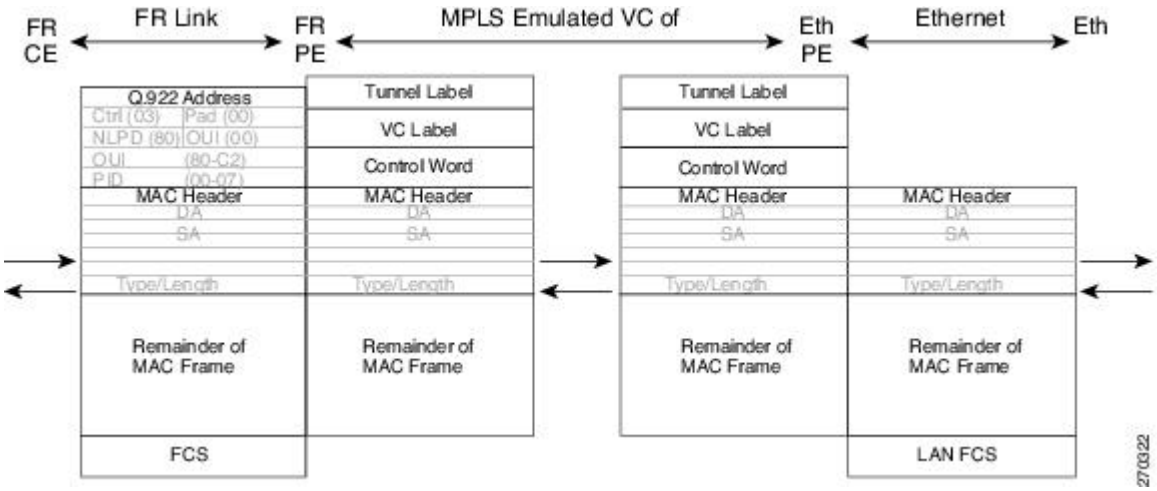
PE ルータは、CE からの送信ではシスコと IETF の両方のフレーム リレーについてカプセル化の変換を自動的にサポートしますが、CE ルータへの送信では IETF への変換のみをサポートします。これは、シスコ カプセル化方式で送信するように設定されている場合でも Cisco CE ルータでは IETF カプセル化方式が受信時に処理されるため、Cisco CE ルータでは問題が発生しません。

フレーム リレーの既存の QoS 機能がサポートされています。PVC ステータス シグナリングは、like-to-like の場合と同様に動作します。PE ルータは、擬似回線のアベイラビリティに基づいて CE ルータに PVC ステータスをレポートします。

MPLS で接続する場合は、AC MTU が一致している必要があります。フレーム リレー DLCI モードのみがサポートされています。ブリッジ型インターワーキングでフレーム リレー ポート モードはサポートされていません。

次の図は、FR-to-Ethernet ブリッジ型インターワーキングのプロトコル スタックを示しています。

図 *16*：*FR-to-Ethernet AToM* ブリッジ型インターワーキングのプロトコル スタック（*VLAN* ヘッダーなし）



Frame Relay DLCI-to-Ethernet VLAN 802.1Q AToM：ブリッジ型インターワーキング

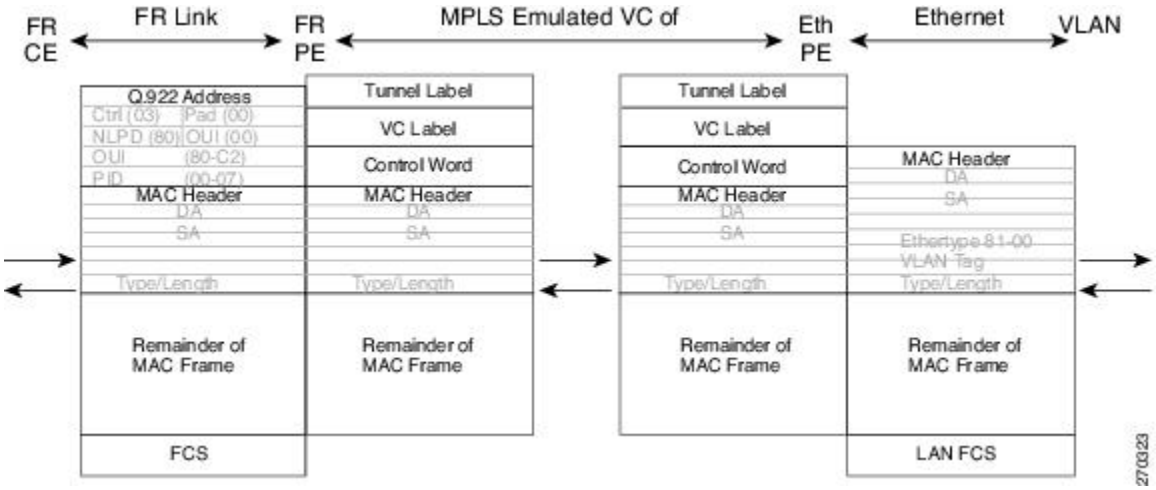
このインターワーキング タイプは、異なる PE ルータに接続しているフレーム リレー接続 VC とイーサネット VLAN 接続 VC との間を相互運用します。ブリッジ型（イーサネット）インターワーキング メカニズムに対応するブリッジ型カプセル化を使用します。

このインターワーキング機能はフレーム リレーからイーサネット ポートの場合と同様に実行されます。フレーム リレーでマルチプロトコル インターコネクトに基づいて、フレーム リレー接続 VC に接続される PE ルータで実装されます（上図を参照）。

ATM-to-VLAN の場合と同様に、着信パケットの VLAN ヘッダーの存在により、イーサネット アクセス側に 1 つの大きな違いがあります。VLAN 側の PE ルータは、VLAN CE ルータからの着信フレームの VLAN ヘッダーを破棄し、MPLS クラウドからのイーサネット フレームに VLAN ヘッダーを挿入します。擬似回線（VC タイプ 5）上で送信されるフレームは、VLAN ヘッダーのないイーサネット フレームです。

次の図は、FR-to-VLAN AToM ブリッジ型インターワーキングのプロトコル スタックを示しています。

図 *17*：*FR-to-VLAN AToM* ブリッジ型インターワーキングのプロトコル スタック



Frame Relay DLCI-to-Ethernet VLAN Qot1Q QinQ AToM：ブリッジ型インターワーキング

このインターワーキング タイプは、異なる PE ルータに接続しているフレーム リレー接続 VC とイーサネット VLAN 接続 VC との間を相互運用します。ブリッジ型（イーサネット）インターワーキング メカニズムに対応するブリッジ型カプセル化を使用します。

このインターワーキング機能は FR-to-Ethernet ポートの場合と同様に実行されます。RFC 2427（フレーム リレーでのマルチプロトコル インターコネクト）に基づいて、フレーム リレー接続 VC に接続される PE ルータで実行されます。

フレーム リレーDLCI-to-Ethernet Port AToM と比較した場合、着信パケットの VLAN ヘッダーの存在により、イーサネット アクセス側に 1 つの大きな違いがあります。VLAN 側の PE ルータは、VLAN CE ルータからの着信フレームの VLAN ヘッダーを破棄し、MPLS クラウドからのイーサネット フレームに VLAN ヘッダーを挿入します。したがって、擬似回線（VC タイプ 5）に送信されるフレームは VLAN ヘッダーのないイーサネット フレームになります。

次の変換はフレーム リレー PE ルータでサポートされています。

- LAN FCS のないイーサネット（0300800080C20007）
- スパニング ツリー（0300800080C2000E）

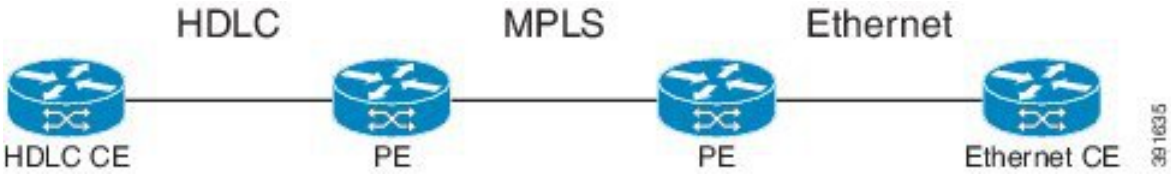
ブリッジ型インターワーキングでサポートされるフレーム リレーのカプセル化タイプは、着信トラフィックに関してはシスコおよび IETF、CE ルータへの発信トラフィックに関しては IETF のみです。

HDLC-to-Ethernet インターワーキング

ハイレベルデータ リンク制御（HDLC）およびイーサネットは、Any Transport over MPLS（AToM）フレームワークを使用して相互に通信する 2 つの独立したデータリンク層トランスポート プロトコルです。このインターワーキング機能は、マルチプロトコル ラベル スイッチング（MPLS）バックボーン上での 2 つの異種レイヤ 2 カプセル化間の変換を可能にします。

次の図は、単純な HDLC-to-Ethernet インターワーキング トポロジを示しています。

図 *18*：*HDLC-to-Ethernet* インターワーキング トポロジ



HDLC-to-Ethernet インターワーキングは以下をサポートします。

- イーサネット（ブリッジ型）インターワーキング
- IP（ルーテッド）インターワーキング
- HDLC カプセル化タイプ：CISCO
- イーサネット カプセル化タイプ：IEEE 802.1Q、QinQ、ポート モード

HDLC パススルー機能は HDLC-to-Ethernet インターワーキングによる影響は受けません。

HDLC-to-Ethernet インターワーキングは次の 2 つのインターワーキング モードをサポートします。

- HDLC-to-Ethernet：イーサネット（ブリッジ型）インターワーキング
- HDLC-to-Ethernet：IP（ルーテッド）インターワーキング

HDLC-to-Ethernet：イーサネット（ブリッジ型）インターワーキング

HDLC-to-Ethernet ブリッジ型インターワーキングは、HDLC 接続仮想回線（VC）と、さまざまなプロバイダー エッジ（PE）デバイスに接続されたイーサネット VLAN 接続 VC との相互運用性を提供します。ブリッジ型（イーサネット）インターワーキング メカニズムに対応するブリッジ型カプセル化を使用します。

パケットが HDLC カスタマー エッジ（CE）デバイスから到着すると、それらは HDLC ヘッダー、イーサネット MAC ヘッダー、およびペイロードで構成されています。HDLC PE デバイスで、HDLC ヘッダーが削除され、MPLS ラベルが挿入されます。次に、フレームは擬似回線経由でイーサネット PE デバイスにルーティングされ、そこで MPLS ラベルが削除されます。イーサネット側では 2 つの可能性があります。接続回線（AC）はイーサネットまたは VLAN のどちらかです。

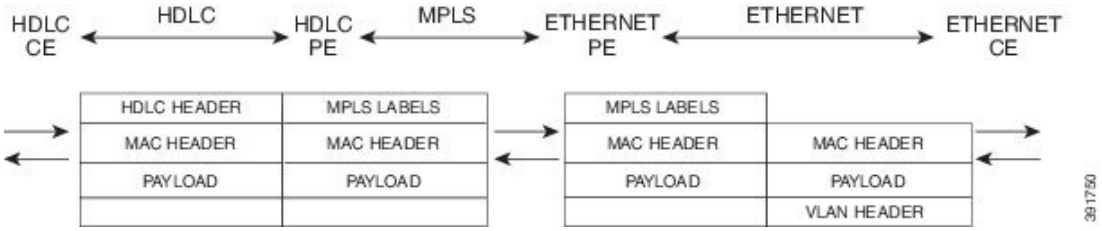
イーサネット接続回線（AC）の場合、パケットはそのままイーサネット CE デバイスに転送されます。VLAN AC の場合、VLAN/QinQ サブインターフェイスの AC に VLAN ヘッダーが追加されます。次に、イーサネット VLAN フレームが VLAN CE デバイスに転送されます。

逆方向（イーサネット/VLAN から HDLC へ）では、AC が VLAN の場合、VLAN ヘッダーは着信パケットに存在します。したがって、パケットが VLAN CE デバイスから到着すると、それらは VLAN ヘッダー、イーサネット MAC ヘッダー、およびペイロードで構成されています。イーサネット PE デバイスでは、VLAN/QinQ サブインターフェイスの AC で VLAN ヘッダーが削除され、MPLS ラベルが挿入されます。次に、フレームは擬似回線上を HDLC PE デバイスにルーティングされ、そこで MPLS ラベルが削除されます。HDLC ヘッダーはイーサネット MAC ヘッダーの前に追加されます。次に、HDLC フレームが HDLC CE デバイスに転送されます。

AC がイーサネットの場合、イーサネット CE デバイスから到着するパケットは、イーサネット MAC ヘッダーおよびペイロードで構成されています。イーサネット PE デバイスでは、VLAN/QinQ サブインターフェイスの AC で MPLS ラベルが追加されます。次に、フレームは擬似回線上を HDLC PE デバイスにルーティングされ、そこで MPLS ラベルが削除されます。HDLC ヘッダーはイーサネット MAC ヘッダーの前に追加されます。次に、HDLC フレームが HDLC CE デバイスに転送されます。

次の図は、イーサネット側に VLAN AC がある、HDLC-to-Ethernet インターワーキングのブリッジ型インターワーキング モードを示しています。

図 *19*：*HDLC-to-Ethernet*：イーサネット（ブリッジ型）インターワーキング



HDLC-to-Ethernet：IP（ルーテッド）インターワーキング

ルーテッド インターワーキングを行うには、HDLC PE デバイスとイーサネット PE デバイスの両方を設定する必要があります。擬似回線上の IP カプセル化は HDLC CE デバイスから到着する HDLC パケットで実行されます。アドレス解決は HDLC PE デバイスで行われます。

パケットが HDLC CE デバイスから到着すると、それらは HDLC ヘッダー、IPv4 ヘッダー、およびペイロードで構成されています。HDLC PE デバイスで、HDLC ヘッダーが削除され、MPLS ラベルが挿入されます。次に、フレームは擬似回線経由でイーサネット PE デバイスにルーティングされ、そこで MPLS ラベルが削除されます。イーサネット側では 2 つの可能性があります。接続回線（AC）はイーサネットまたは VLAN のどちらかです。

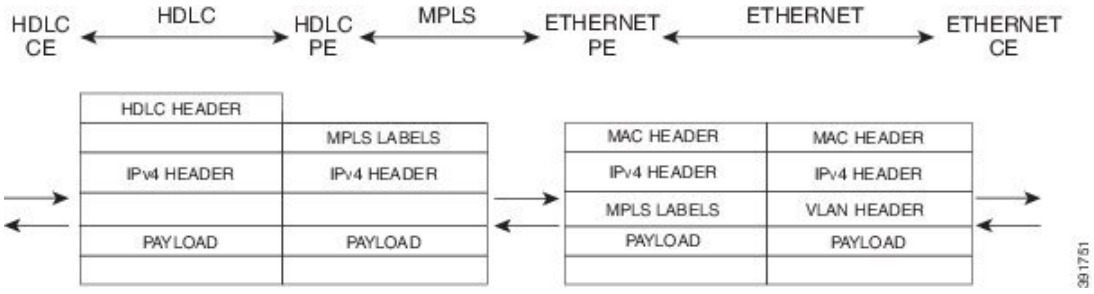
イーサネット接続回線（AC）の場合、パケットはそのままイーサネット CE デバイスに転送されます。VLAN AC の場合、VLAN/QinQ サブインターフェイスの AC に VLAN ヘッダーが追加されます。次に、イーサネット VLAN フレームが VLAN CE デバイスに転送されます。

逆方向（イーサネット/VLAN から HDLC へ）では、AC が VLAN の場合、VLAN ヘッダーは着信パケットに存在します。したがって、パケットが VLAN CE デバイスから到着すると、それらは VLAN ヘッダー、イーサネット MAC ヘッダー、およびペイロードで構成されています。イーサネット PE デバイスでは、MAC ヘッダーが削除され、VLAN/QinQ サブインターフェイスの AC で VLAN ヘッダーが削除され、MPLS ラベルが挿入されます。次に、フレームは擬似回線上を HDLC PE デバイスにルーティングされ、そこで MPLS ラベルが削除されます。HDLC ヘッダーは IPv4 ヘッダーの前に追加されます。次に、HDLC フレームが HDLC CE デバイスに転送されます。

AC がイーサネットの場合、イーサネット CE デバイスから到着するパケットは、イーサネット MAC ヘッダーおよびペイロードで構成されています。イーサネット PE デバイスで、MAC ヘッダーが削除され、MPLS ラベルが挿入されます。次に、フレームは擬似回線上を HDLC PE デバイスにルーティングされ、そこで MPLS ラベルが削除されます。HDLC ヘッダーは IPv4 ヘッダーの前に追加されます。次に、HDLC フレームが HDLC CE デバイスに転送されます。

次の図は、イーサネット側に VLAN AC がある、HDLC-to-Ethernet インターワーキングのルーテッド インターワーキング モードを示しています。

図 *20*：*HDLC-to-Ethernet*：*IP*（ルーテッド）インターワーキング



ATM ローカル スイッチング

- ATM like-to-like ローカル スイッチングにより、両方のセグメントが ATM タイプである 2 つの物理インターフェイス間でのデータのスイッチングが可能になります。2つのインターフェイスは同じ PE ルータ上にある必要があります。次の表に、サポートされる ATM ローカル スイッチングの組み合わせの一覧を示します。

表 *12*：*ATM* ローカル スイッチング：サポートされる組み合わせ

	同じポートポイントツーポイント	異なるポートポイントツーポイント	同じポートマルチポイント	異なるポートマルチポイント
Port Mode	No	No	No	No
VC-to-VC AAL0	Yes	Yes	Yes	Yes
VC-to-VC AAL5	Yes	Yes	Yes	Yes
VP-to-VP AAL0	No	No	Yes	Yes

	同じポートポイントツーポイント	異なるポートポイントツーポイント	同じポートマルチポイント	異なるポートマルチポイント
VP-to-VP AAL5	No	No	No	No

VC-to-VC ローカル スイッチング

VC-to-VC ローカル スイッチングでは、PE ルータの同じポートまたは異なるポートにある 2 つの ATM 接続 VC 間でセルを転送します。PE ルータに着信するセルは、AAL0 または AAL5 でカプセル化された ATM パケットである場合があります。ATM VC-to-VC ローカル スイッチングは、ポイントツーポイントインターフェイスまたはマルチポイントインターフェイスのいずれかで設定できます。

ATM ローカル スイッチング インターフェイス上で OAM セルを管理するための 2 つの動作モードがあります。

- OAM トランスペアレント モード：このモードでは、PE ルータは F5 OAM セルをローカル スイッチング インターフェイス間で透過的に転送します。
- OAM ローカルエミュレーション モード：このモードでは、ローカルスイッチングインターフェイス間でOAMセルを転送しません。代わりに、インターフェイスはF5 OAMセルをローカルで終端させ、処理します。

ATM シングル セル リレー AAL0 では、ルータの入力および出力 ATM インターフェイスの ATM 仮想パス識別子/仮想チャネル識別子（VPI/VCI）の値が、一致している必要があります。2 つの ATM 間の VPI および VCI（2 つの異なるインターフェイス上にあり、一致しない値を持つ）で L2 ローカル スイッチングが必要な場合は、ATM AAL5 を選択する必要があります。ただし、ATM AAL5 が OAM トランスペアレント モードを使用する場合、VPI と VCI の値は一致する必要があります。

oam-ac emulation-enable および **oam-pvc manage** コマンドを使用して、ATM VC モードのローカル スイッチング AC で ATM OAM を設定できます。AC でエミュレーションを有効にすると、AC を通過するすべての OAM セルは、ローカル処理するために RP にパントされます。ATM 共通コンポーネントは OAM セルを処理し、そのセルをローカル CE ルータに転送します。これは、CE ルータ エンドで応答を監視し、PE ルータで障害を検出するのに役立ちます。**oam-pvc manage** コマンドを AC 上で有効にすると、PVC は、VC の接続を確認するエンドツーエンド OAM ループバック セルを生成します。

次に、ATM PE ルータでの設定例を示します。

```
configure terminal
interface atm 4/0.50 multipoint
 no ip address
  no atm enable-ilmi-trap
pvc 100/100 l2transport
 encapsulation aal5
 oam-ac emulation-enable
 oam-pvc manage
interface atm 5/0.100 multipoint
 no ip address
 no atm enable-ilmi-trap
```

```
 pvc 100/100 l2transport
  encapsulation aal5
  oam-ac emulation-enable
  oam-pvc manage
connect atm_ls atm 4/0 100/100 atm 5/0 100/100
```

VP-to-VP ローカル スイッチング

VP-to-VP ローカル スイッチングでは、PE ルータの同じポートまたは異なるポートにある 2 つの VP 間でセルを転送します。PE ルータに着信するセルは、AAL0 でカプセル化された ATM パケットのみである場合があります。ATM VP-to-VP ローカル スイッチングは、マルチポイント インターフェイスのみで設定できます。

ATM ローカル スイッチング インターフェイス上で OAM セルを管理するための 2 つの動作モードがあります。

- OAM トランスペアレント モード：このモードでは、PE ルータは F4 OAM セルをローカル スイッチング インターフェイス間で透過的に転送します。
- OAM ローカルエミュレーション モード：このモードでは、ローカル スイッチング インターフェイス間で OAM セルを転送しません。代わりに、インターフェイスは F4 OAM セルをローカルで終端させ、処理します。

ATM シングル セル リレー AAL0 では、ルータの入力および出力 ATM インターフェイスの ATM VPI 値が一致している必要があります。2 つの ATM 間の VPI（2 つの異なるインターフェイス上にあり、一致しない値を持つ）で L2 スイッチングが必要な場合は、ATM AAL5 を選択する必要があります。ATM AAL5 が OAM トランスペアレント モードを使用する場合、VPI 値は一致する必要があります。現在、ATM VP-to-VP ローカル スイッチングは AAL0 カプセル化のみをサポートします。

次に、ATM PE ルータでの設定例を示します。

```
configure terminal
interface atm 4/0.100 multipoint
 no ip address
 no atm enable-ilmi-trap
atm pvp 100 l2transport
interface atm 5/0.100 multipoint
 no ip address
 no atm enable-ilmi-trap
atm pvp 100 l2transport
connect atm_ls atm 4/0 100 atm 5/0 100
```

PPP-to-Ethernet AToM：ルーテッド インターワーキング

このインターワーキングのタイプでは、AC の一方はイーサネットで、他方は PPP です。各リンクは対応する PE ルータのローカルで終端し、抽出したレイヤ 3（L3）パケットは擬似回線で転送されます。

イーサネットと PPP AC に接続された PE ルータはそれぞれの L2 プロトコルを終端させます。PPP セッションは、LCP とネットワーク制御プロトコル（NCP）レイヤの両方で終端します。入力 PE ルータでは、L3 パケットを抽出した後、各 PE ルータは、MPoMPLS カプセル化を使用して、すでに確立された擬似回線でパケットを転送します。出力 PE ルータでは、ラベル ディスポジショ

ンを実行した後、対応するリンク レイヤに基づいてパケットはカプセル化され、それぞれの CE ルータに送信されます。このインターワーキング シナリオでは、PE ルータによる MPoMPLS のカプセル化がサポートされている必要があります。

PPP-to-Ethernet AToM ルーテッド インターワーキング モードでは、IPCP がサポートされます。IP インターワーキングが擬似回線に設定されると、プロキシ IPCP は PE ルータで自動的にイネーブルにされます。デフォルトでは、PE ルータは、使用する必要のある IP アドレスを CE ルータから取得します。PE ルータは、IP アドレス 0.0.0.0 で IPCP confreq を送信することによって、これを実行します。ローカル CE ルータでは、リモート CE ルータの IP アドレスが設定されます。次に、PPP CE ルータでの設定例を示します。

```
interface serial2/0
 ip address 168.65.32.13 255.255.255.0
 encapsulation ppp
peer default ip address 168.65.32.14  *
```

リモート CE ルータの IP アドレスをローカル CE ルータで設定できない場合、PE ルータの xconnect PPP インターフェイスで **ppp ipcp address proxy** *ip address* コマンドを使用して、リモート CE ルータの IP アドレスを PE ルータで設定できます。次に、PPP PE ルータでの設定例を示します。

```
pseudowire-class mp
 encapsulation mpls
 protocol ldp
 interworking ip
!
int se2/0
 encap ppp
 xconnect 10.0.0.2 200 pw-class mp
 ppp ipcp address proxy 168.65.32.14
```

L2VPN プロトコルベース CLI 機能に関連するコマンドを使用した PPP-to-Ethernet AToM：ルーテッド インターワーキング

このインターワーキングのタイプでは、AC の一方はイーサネットで、他方は PPP です。各リンクは対応する PE ルータのローカルで終端し、抽出したレイヤ 3（L3）パケットは擬似回線で転送されます。

イーサネットと PPP AC に接続された PE ルータはそれぞれの L2 プロトコルを終端させます。PPP セッションは、LCP とネットワーク制御プロトコル（NCP）レイヤの両方で終端します。入力 PE ルータでは、L3 パケットを抽出した後、各 PE ルータは、MPoMPLS カプセル化を使用して、すでに確立された擬似回線でパケットを転送します。出力 PE ルータでは、ラベル ディスポジションを実行した後、対応するリンク レイヤに基づいてパケットはカプセル化され、それぞれの CE ルータに送信されます。このインターワーキング シナリオでは、PE ルータによる MPoMPLS のカプセル化がサポートされている必要があります。

PPP-to-Ethernet AToM ルーテッド インターワーキング モードでは、IPCP がサポートされます。IP インターワーキングが擬似回線に設定されると、プロキシ IPCP は PE ルータで自動的にイネーブルにされます。デフォルトでは、PE ルータは、使用する必要のある IP アドレスを CE ルータから取得します。PE ルータは、IP アドレス 0.0.0.0 で IPCP confreq を送信することによって、これを

実行します。ローカルCEルータでは、リモートCEルータのIPアドレスが設定されます。次に、PPP CE ルータでの設定例を示します。

```
interface serial2/0
 ip address 168.65.32.13 255.255.255.0
 encapsulation ppp
peer default ip address 168.65.32.14  *
```

リモートCEルータのIPアドレスをローカルCEルータで設定できない場合、PEルータのxconnect PPPインターフェイスで **ppp ipcp address proxy** *ip address* コマンドを使用して、リモート CE ルータの IP アドレスを PE ルータで設定できます。次に、PPP PE ルータでの設定例を示します。

```
template type pseudowire mp
 encapsulation mpls
 protocol ldp
 interworking ip
!
int se2/0
 encap ppp
interface pseudowire 100
 source template type pseudowire mp
 neighbor 33.33.33.33 1
!
l2vpn xconnect context con1
 ppp ipcp address proxy 168.65.32.14
```

PPP の L2VPN インターワーキング用のスタティック IP アドレス

PPP のローカル CE ルータを使用して PE ルータでアドレス解決する場合、PE ルータ上でリモートCE ルータの IP アドレスを設定します。PE ルータの xconnect PPP インターフェイス上のリモートCE ルータの IP アドレスを指定して **ppp ipcp address proxy** コマンドを使用します。次の例は、設定サンプルを示しています。

```
pseudowire-class ip-interworking
 encapsulation mpls
 interworking ip
interface Serial2/0
 encapsulation ppp
 xconnect 10.0.0.2 200 pw-class ip-interworking
 ppp ipcp address proxy 10.65.32.14
```

ローカル CE ルータでアドレス解決を実行する場合は、**peer default ip address** コマンドを使用して、ローカル CE ルータ上にリモート CE ルータの IP アドレスを設定することもできます。

PPPのL2VPNインターワーキング用のスタティックIPアドレス（L2VPNプロトコルベースの CLI 機能に関連するコマンドを使用）

PPP のローカル CE ルータを使用して PE ルータでアドレス解決する場合、PE ルータ上でリモートCE ルータの IP アドレスを設定します。PE ルータの xconnect PPP インターフェイス上のリモートCE ルータの IP アドレスを指定して **ppp ipcp address proxy** コマンドを使用します。次の例は、設定サンプルを示しています。

```
template type pseudowire ip-interworking
 encapsulation mpls
 interworking ip
```

```
interface Serial2/0
 encapsulation ppp
interface pseudowire 100
 source template type pseudowire ip-interworking
 neighbor 10.0.0.2 200
!
l2vpn xconnect context con1
 ppp ipcp address proxy 10.65.32.14
```

ローカル CE ルータでアドレス解決を実行する場合は、**peer default ip address** コマンドを使用して、ローカル CE ルータ上にリモート CE ルータの IP アドレスを設定することもできます。

L2VPN インターワーキングの設定方法

L2VPN インターワーキングの設定

L2VPNインターワーキングを使用すれば、異種のACを接続できます。L2VPNインターワーキング機能を設定するには、**interworking** コマンドを擬似回線を構成するコマンドのリストに追加する必要があります。ここでは、L2VPNインターワーキングの擬似回線を設定する手順を説明します。全体的な AToM 設定の一部として、**interworking** コマンドを使用します。AToM 固有の設定手順については、『Any Transport over MPLS』ドキュメントを参照してください。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **pseudowire-class***name*
4. **encapsulation** {**mpls** | **l2tpv3**}
5. **interworking**{**ethernet**| **ip**}
6. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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。

	コマンドまたはアクション	目的
ステップ 3	**pseudowire-class***name* 例： `Router(config)# pseudowire-class class1`	指定した名前の擬似回線クラスを確立して、擬似回線クラス コンフィギュレーション モードに入ります。
ステップ 4	**encapsulation** {**mpls** | **l2tpv3**} 例： `Router(config-pw)# encapsulation mpls`	**mpls** と **l2tpv3** のどちらかのトンネリング カプセル化を指定します。
ステップ 5	**interworking**{**ethernet**| **ip**} 例： `Router(config-pw)# interworking ip`	擬似回線のタイプと、その回線を流れるトラフィックのタイプを指定します。
ステップ 6	**end** 例： `Router(config-pw)# end`	擬似回線クラス コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

L2VPN 設定の確認

L2VPN 設定を確認するには、次の手順を実行します。

- CE ルータ間で **show arp** コマンドを実行して、データが送信されていることを確認できます。

```
Router# show arp
Protocol   Address        Age (min)   Hardware Addr    Type    Interface
Internet   10.1.1.5           134    0005.0032.0854   ARPA    FastEthernet0/0/0
Internet   10.1.1.7             -    0005.0032.0000   ARPA    FastEthernet0/0/0
```

- CE ルータ間で **ping** コマンドを実行して、データが送信されていることを確認できます。

```
Router# ping 10.1.1.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

- AToM の設定を確認するには、**show mpls l2transport vc detail** コマンドを使用します。

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した L2VPN インターワーキングの設定

L2VPNインターワーキングを使用すると異なる接続回線どうしが接続できます。L2VPNインターワーキング機能を設定するには、**interworking** コマンドを擬似回線を構成するコマンドのリストに追加する必要があります。ここでは、L2VPNインターワーキングの擬似回線を設定する手順を説明します。全体的な AToM または L2TPv3 設定の一部として、**interworking** コマンドを使用します。AToM または L2TPv3 の設定に関する詳細については、次のマニュアルを参照してください。

- 『Layer 2 Tunnel Protocol Version 3』
- Any Transport over MPLS

手順の概要

1. イネーブル化
2. **configureterminal**
3. **hw-moduleslot***slot-number***npmodefeature**
4. **interfacepseudowire***number*
5. **encapsulation** {**mpls** | **l2tpv3**}
6. **interworking**{**ethernet**| **ip**}
7. **neighbor***peer-addressvcid-value*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**hw-moduleslot***slot-number***npmodefeature** 例： `Router(config)# hw-module slot 3 np mode feature`	（任意）Cisco 12000 シリーズ ルータの L2VPN インターワーキング機能をイネーブルにします。

	コマンドまたはアクション	目的
		（注） このコマンドは、ISE（エンジン3）またはエンジン5 インターフェイスの L2VPN インターワーキングで L2TPv3 を使用する場合に、Cisco 12000 シリーズインターネットルータでのみ入力してください。この場合は、まず **hw-moduleslot***slot-number***npmodefeature** コマンドを入力してラインカードの L2VPN 機能バンドルを有効にする必要があります。
ステップ 4	**interfacepseudowire***number* 例： `Router(config)# interface pseudowire 1`	指定した値でインターフェイス擬似回線を確立して、擬似回線クラス コンフィギュレーション モードを開始します。
ステップ 5	**encapsulation** {**mpls** | **l2tpv3**} 例： `Router(config-pw)# encapsulation mpls`	**mpls** と **l2tpv3** のどちらかのトンネリング カプセル化を指定します。
ステップ 6	**interworking**{**ethernet**| **ip**} 例： `Router(config-pw)# interworking ip`	擬似回線のタイプと、その回線を流れるトラフィックのタイプを指定します。 （注） Cisco 12000 シリーズ インターネット ルータでは、L2TPv3 に対してイーサネット（ブリッジ型）インターワーキングはサポートされません。**encapsulationl2tpv3** コマンドを使用して擬似回線に L2TPv3 トンネル カプセル化を設定したあとは、**interworkingethernet** コマンドを入力できません。
ステップ 7	**neighbor***peer-addressvcid-value* 例： `Router(config-pw)#  neighbor 10.0.0.1 123`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。

L2VPN 設定の確認（L2VPN プロトコルベースの CLI 機能に関連するコマンドを使用）

L2VPN 設定を確認するには、次のコマンドを実行します。

- CE ルータ間で **show arp** コマンドを実行して、データが送信されていることを確認できます。

```
Device# show arp
Protocol   Address       Age (min)   Hardware Addr    Type    Interface
Internet   10.1.1.5           134    0005.0032.0854   ARPA    FastEthernet0/0/0
Internet   10.1.1.7             -    0005.0032.0000   ARPA    FastEthernet0/0/0
```

- CE ルータ間で **ping** コマンドを実行して、データが送信されていることを確認できます。

```
Device# ping 10.1.1.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

- AToM の設定を確認するには、**show l2vpn atom vc detail** コマンドを使用します。

Ethernet VLAN-to-ATM AAL5 インターワーキングの設定

このセクションでは、次の AToM 設定について説明します。

ATM AAL5-to-Ethernet Port

PE1 ルータで ATM AAL5-to-Ethernet Port 機能を設定するには、次の手順を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **mplslabelprotocolldp**
4. **interface***typenumber*
5. **ipaddress***ip-addressmask*
6. **pseudowire-class** [*pw-class-name*]
7. **encapsulationmpls**
8. **interworking**{**ethernet**| **ip**}
9. **interfaceatm***slot*/*subslot*/*port*.*subinterfacenumber*
10. **pvc** [*name*] *vpi*/*vci***12transport**
11. **encapsulationaal5snap**
12. **xconnect***ip-addressvc-id***pw-class***pw-class-name*
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	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Router> enable`	• 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	**configureterminal** 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	**mplslabelprotocolldp** 例： `Router(config)# mpls label protocol ldp`	プラットフォームの Label Distribution Protocol を設定します。
ステップ 4	**interface***typenumber* 例： `Router(config)# interface loopback 100`	インターフェイス タイプを設定し、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 5	**ipaddress***ip-addressmask* 例： `Router(config-if)# ip address 10.0.0.100 255.255.255.255`	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。
ステップ 6	**pseudowire-class** [*pw-class-name*] 例： `Router(config-if)# pseudowire-class atm-eth`	指定した名前の擬似回線クラスを確立して、擬似回線クラス コンフィギュレーション モードに入ります。
ステップ 7	**encapsulationmpls** 例： `Router(config-pw)# encapsulation mpls`	トンネリング カプセル化を指定します。
ステップ 8	**interworking**{**ethernet**| **ip**} 例： `Router(config-pw)# interworking ip`	擬似回線のタイプと、その回線を流れるトラフィックのタイプを指定します。

	コマンドまたはアクション	目的
ステップ 9	**interfaceatm***slot*/*subslot*/*port*.*subinterfacenumber* 例： `Router(config-pw)# interface atm 2/0/0.1`	ATM インターフェイスを設定して、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 10	**pvc** [*name*] *vpi*/*vci***12transport** 例： `Router(config-subif)# pvc 0/200 l2transport`	ATM 相手先固定接続（PVC）に名前を割り当て、ATM 仮想回線コンフィギュレーション モードを開始します。
ステップ 11	**encapsulationaal5snap** 例： `Router(config-if-atm-member)# encapsulation aal5snap`	ATM VC の ATM AAL およびカプセル化タイプを設定します。
ステップ 12	**xconnect***ip-addressvc-id***pw-class***pw-class-name* 例： `Router(config-if-atm-member)# xconnect 10.0.0.200 140 pw-class atm-eth`	AC を擬似回線にバインドし、AToM スタティック擬似回線を設定します。
ステップ 13	**end** 例： `Router(config-if-xconn)# end`	xconnect 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。

L2VPN プロトコルベース CLI 機能に関連するコマンドを使用した ATM AAL5-to-Ethernet Port

PE1 ルータで ATM AAL5-to-Ethernet Port 機能を設定するには、次の手順を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **mplslabelprotocolldp**
4. **interface***typenumber*
5. **ipaddress***ip-addressmask*
6. **templatetypepseudowire** [*pw-class-name*]
7. **encapsulationmpls**
8. **interworking**{**ethernet**| **ip**}
9. **interfaceatm***slot*/*subslot*/*port*.*subinterfacenumber*
10. **pvc** [*name*] *vpi*/*vci***12transport**
11. **encapsulationaal5snap**
12. **end**
13. **interfacepseudowire***number*
14. **sourcetemplatetypepseudowire***template-name*
15. **neighbor***peer-addressvcid-value*
16. **exit**
17. **exit**
18. **l2vpnxconnectcontext***context-name*
19. **memberpseudowire***interface-number*
20. **member***ip-addressvc-id***encapsulation mpls**
21. **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	イネーブル化 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	**configureterminal** 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	**mplslabelprotocolldp** 例： `Router(config)# mpls label protocol ldp`	プラットフォームの Label Distribution Protocol を設定します。

	コマンドまたはアクション	目的
ステップ 4	**interface***typenumber* 例： `Router(config)# interface loopback 100`	インターフェイス タイプを設定し、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 5	**ipaddress***ip-addressmask* 例： `Router(config-if)# ip address 10.0.0.100 255.255.255.255`	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。
ステップ 6	**templatetypepseudowire** [*pw-class-name*] 例： `Router(config-if)# template type pseudowire atm-eth`	指定した名前の擬似回線クラスを確立して、擬似回線クラス コンフィギュレーション モードに入ります。
ステップ 7	**encapsulationmpls** 例： `Router(config-pw)# encapsulation mpls`	トンネリング カプセル化を指定します。
ステップ 8	**interworking**{**ethernet**| **ip**} 例： `Router(config-pw)# interworking ip`	擬似回線のタイプと、その回線を流れるトラフィックのタイプを指定します。
ステップ 9	**interfaceatm***slot*/*subslot*/*port*.*subinterfacenumber* 例： `Router(config-pw)# interface atm 2/0/0.1`	ATM インターフェイスを設定して、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 10	**pvc** [*name*] *vpi*/*vci***12transport** 例： `Router(config-subif)# pvc 0/200 l2transport`	ATM 相手先固定接続（PVC）に名前を割り当て、ATM 仮想回線コンフィギュレーション モードを開始します。
ステップ 11	**encapsulationaal5snap** 例： `Router(config-if-atm-member)# encapsulation aal5snap`	ATM VC の ATM AAL およびカプセル化タイプを設定します。

	コマンドまたはアクション	目的
ステップ 12	**end** 例： `Router(config-if-atm-member)# end`	特権 EXEC モードに戻ります。
ステップ 13	**interfacepseudowire***number* 例： `Router(config)# interface pseudowire 100`	擬似回線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 14	**sourcetemplatetypepseudowire***template-name* 例： `Router(config-if)# source template type pseudowire atm-eth`	atm-eth という名前のタイプ擬似回線のソース テンプレートを設定します。
ステップ 15	**neighbor***peer-addressvcid-value* 例： `Router(config-if)#  neighbor 10.0.0.200 140`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 16	**exit** 例： `Router(config-if)# exit`	特権 EXEC モードに戻ります。
ステップ 17	**exit** 例： `Router(config-if)# exit`	特権 EXEC モードに戻ります。
ステップ 18	**l2vpnxconnectcontext***context-name* 例： `Router(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect コンフィギュレーションモードを開始します。
ステップ 19	**memberpseudowire***interface-number* 例： `Router(config-xconnect)# member pseudowire 100`	Layer 2 VPN（L2VPN）クロス コネクトを形成するようにメンバー擬似回線を指定します。

	コマンドまたはアクション	目的
ステップ 20	**member***ip-addressvc-id***encapsulation mpls** 例： `Router(config-xconnect)# member 10.0.0.200 140 encapsulation mpls`	レイヤ 2 パケットを転送するための VC を作成します。
ステップ 21	**end** 例： `Router(config-xconnect)# end`	xconnect 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。

PE2 ルータでの ATM AAL5-to-Ethernet Port

PE2 ルータで ATM AAL5-to-Ethernet Port 機能を設定するには、次の手順を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **mplslabelprotocolldp**
4. **interface***typenumber*
5. **ipaddress***ip-addressmask*
6. **pseudowire-class** [*pw-class-name*]
7. **encapsulationmpls**
8. **interworking**{**ethernet**| **ip**}
9. **interface***typeslot*/*subslot*/*port*
10. **xconnect***ip-addressvc-id***pw-class***pw-class-name*
11. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 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	**mplslabelprotocolldp** 例： `Router(config)# mpls label protocol ldp`	プラットフォームの Label Distribution Protocol を設定します。
ステップ 4	**interface***typenumber* 例： `Router(config)# interface loopback 100`	インターフェイス タイプを設定し、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 5	**ipaddress***ip-addressmask* 例： `Router(config-if)# ip address 10.0.0.100 255.255.255.255`	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。
ステップ 6	**pseudowire-class** [*pw-class-name*] 例： `Router(config-if)# pseudowire-class atm-eth`	指定した名前の擬似回線クラスを確立して、擬似回線クラス コンフィギュレーション モードに入ります。
ステップ 7	**encapsulationmpls** 例： `Router(config-pw)# encapsulation mpls`	トンネリング カプセル化を指定します。
ステップ 8	**interworking**{**ethernet**| **ip**} 例： `Router(config-pw)# interworking ip`	擬似回線のタイプと、その回線を流れるトラフィックのタイプを指定します。
ステップ 9	**interface***typeslot*/*subslot*/*port* 例： `Router(config-pw)# interface gigabitethernet 5/1/0`	インターフェイスを設定し、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 10	**xconnect***ip-addressvc-id***pw-class***pw-class-name* 例： `Router(config-if)# xconnect 10.0.0.100 140 pw-class atm-eth`	AC を擬似回線にバインドし、AToM スタティック擬似回線を設定します。
ステップ 11	**end** 例： `Router(config-if-xconn)# end`	xconnect 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

（注） ブリッジ型インターワーキングの設定時には、PE2 ルータ設定に **interworkingethernet** コマンドが含まれていません。これは、like-to-like として扱われること、および AC がすでにイーサネットポートであるためです。ただし、ルーテッドインターワーキングを設定するときには、**interworkingip** コマンドが必要です。

L2VPN プロトコルベース CLI 機能に関連するコマンドを使用した PE2 ルータでの ATM AAL5-to-Ethernet Port

PE2 ルータで ATM AAL5-to-Ethernet Port 機能を設定するには、次の手順を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **mplslabelprotocolldp**
4. **interface***typenumber*
5. **ipaddress***ip-addressmask*
6. **templatetypepseudowire** [*pseudowire-name*]
7. **encapsulationmpls**
8. **interworking**{**ethernet**| **ip**}
9. **interface***typeslot*/*subslot*/*port*
10. **end**
11. **interfacepseudowire***number*
12. **sourcetemplatetypepseudowire***template-name*
13. **neighbor***peer-addressvcid-value*
14. **exit**
15. **l2vpnxconnectcontext***context-name*
16. **memberpseudowire***interface-number*
17. **member***ip-addressvc-id***encapsulation mpls**
18. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**mplslabelprotocolldp** 例： `Router(config)# mpls label protocol ldp`	プラットフォームの Label Distribution Protocol を設定します。

	コマンドまたはアクション	目的
ステップ 4	**interface***typenumber* 例： `Router(config)# interface loopback 100`	インターフェイスタイプを設定し、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 5	**ipaddress***ip-addressmask* 例： `Router(config-if)# ip address 10.0.0.100 255.255.255.255`	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。
ステップ 6	**templatetypepseudowire** [*pseudowire-name*] 例： `Router(config)# template type pseudowire atm-eth`	レイヤ 2 擬似回線 クラスの名前を指定し、擬似回線クラス コンフィギュレーション モードを開始します。
ステップ 7	**encapsulationmpls** 例： `Router(config-pw)# encapsulation mpls`	トンネリング カプセル化を指定します。
ステップ 8	**interworking**{**ethernet**| **ip**} 例： `Router(config-pw)# interworking ip`	擬似回線のタイプと、その回線を流れるトラフィックのタイプを指定します。
ステップ 9	**interface***typeslot/subslot/port* 例： `Router(config-pw)# interface gigabitethernet 5/1/0`	インターフェイスを設定し、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 10	**end** 例： `Router(config-pw)# end`	特権 EXEC モードに戻ります。
ステップ 11	**interfacepseudowire***number* 例： `Router(config)# interface pseudowire 100`	擬似回線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。

	コマンドまたはアクション	目的
ステップ 12	**sourcetemplatetypepseudowire***template-name* 例： `Router(config-if)# source template type pseudowire atm-eth`	atm-eth という名前のタイプ擬似回線のソース テンプレートを設定します。
ステップ 13	**neighbor***peer-addressvcid-value* 例： `Router(config-if)#  neighbor 10.0.0.100 140`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 14	**exit** 例： `Router(config-if)# exit`	特権 EXEC モードに戻ります。
ステップ 15	**l2vpnxconnectcontext***context-name* 例： `Router(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect コンフィギュレーション モードを開始します。
ステップ 16	**memberpseudowire***interface-number* 例： `Router(config-xconnect)# member pseudowire 100`	Layer 2 VPN（L2VPN）クロス コネクトを形成するようにメンバー擬似回線を指定します。
ステップ 17	**member***ip-addressvc-id***encapsulation mpls** 例： `Router(config-xconnect)# member 10.0.0.100 140 encapsulation mpls`	レイヤ 2 パケットを転送するための VC を作成します。
ステップ 18	**end** 例： `Router(config-xconnect)# end`	xconnect 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

（注） ブリッジ型インターワーキングの設定時には、PE2 ルータ設定に **interworkingethernet** コマンドが含まれていません。これは、like-to-like として扱われること、および AC がすでにイーサネットポートであるためです。ただし、ルーテッドインターワーキングを設定するときには、**interworkingip** コマンドが必要です。

PE1 ルータでの ATM AAL5-to-Ethernet VLAN 802.1Q

PE1 ルータで ATM AAL5-to-Ethernet VLAN 802.1Q 機能を設定するには、次の手順を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **mplslabelprotocolldp**
4. **interface***typenumber*
5. **ipaddress***ip-addressmask*
6. **pseudowire-class** [*pw-class-name*]
7. **encapsulationmpls**
8. **interworking**{**ethernet**| **ip**}
9. **interfaceatm***slot*/*subslot*/*port*.*subinterfacenumber*
10. **pvc** [*name*] *vpi*/*vci***12transport**
11. **encapsulationaal5snap**
12. **xconnect***ip-addressvc-id***pw-class***pw-class-name*
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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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。

	コマンドまたはアクション	目的
ステップ 3	**mplslabelprotocolldp** 例： `Router(config)# mpls label protocol ldp`	プラットフォームの Label Distribution Protocol を設定します。
ステップ 4	**interface***typenumber* 例： `Router(config)# interface loopback 100`	インターフェイスタイプを設定し、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 5	**ipaddress***ip-addressmask* 例： `Router(config-if)# ip address 10.0.0.100 255.255.255.255`	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。
ステップ 6	**pseudowire-class** [*pw-class-name*] 例： `Router(config-if)# pseudowire-class atm-eth`	指定した名前の擬似回線クラスを確立して、擬似回線クラス コンフィギュレーション モードに入ります。
ステップ 7	**encapsulationmpls** 例： `Router(config-pw)# encapsulation mpls`	トンネリング カプセル化を指定します。
ステップ 8	**interworking**{**ethernet**| **ip**} 例： `Router(config-pw)# interworking ip`	擬似回線のタイプと、その回線を流れるトラフィックのタイプを指定します。
ステップ 9	**interfaceatm***slot*/*subslot*/*port*.*subinterfacenumber* 例： `Router(config-pw)# interface atm 2/0/0.1`	ATM インターフェイスを設定し、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 10	**pvc** [*name*] *vpi*/*vci***l2transport** 例： `Router(config-subif)# pvc 0/200 l2transport`	ATM 相手先固定接続（PVC）に名前を割り当て、ATM 仮想回線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 11	**encapsulationaal5snap** 例： `Router(config-if-atm-member)# encapsulation aal5snap`	ATM VC の ATM AAL およびカプセル化タイプを設定します。
ステップ 12	**xconnect***ip-addressvc-id***pw-class***pw-class-name* 例： `Router(config-if-atm-member)# xconnect 10.0.0.200 140 pw-class atm-eth`	AC を擬似回線にバインドし、AToM スタティック擬似回線を設定します。
ステップ 13	**end** 例： `Router(config-if-xconn)# end`	xconnect 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。

L2VPN プロトコルベース CLI 機能に関連するコマンドを使用した PE1 ルータでの ATM AAL5-to-Ethernet VLAN 802.1Q

PE1 ルータで ATM AAL5-to-Ethernet VLAN 802.1Q 機能を設定するには、次の手順を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **mplslabelprotocolldp**
4. **interface***typenumber*
5. **ipaddress***ip-addressmask*
6. **templatetypepseudowire** [*pseudowire-name*]
7. **encapsulationmpls**
8. **interworking**{**ethernet**| **ip**}
9. **interfaceatm***slot*/*subslot*/*port*.*subinterfacenumber*
10. **pvc** [*name*] *vpi*/*vci***12transport**
11. **encapsulationaal5snap**
12. **end**
13. **interfacepseudowire***number*
14. **sourcetemplatetypepseudowire***template-name*
15. **neighbor***peer-addressvcid-value*
16. **exit**
17. **l2vpnxconnectcontext***context-name*
18. **memberpseudowire***interface-number*
19. **member***ip-addressvc-id***encapsulation mpls**
20. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**mplslabelprotocolldp** 例： `Router(config)# mpls label protocol ldp`	プラットフォームの Label Distribution Protocol を設定します。

	コマンドまたはアクション	目的
ステップ 4	**interface***typenumber* 例： `Router(config)# interface loopback 100`	インターフェイス タイプを設定し、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 5	**ipaddress***ip-addressmask* 例： `Router(config-if)# ip address 10.0.0.100 255.255.255.255`	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。
ステップ 6	**templatetypepseudowire** [*pseudowire-name*] 例： `Router(config)# template type pseudowire atm-eth`	レイヤ 2 擬似回線 クラスの名前を指定し、擬似回線 クラス コンフィギュレーション モードを開始します。
ステップ 7	**encapsulationmpls** 例： `Router(config-pw)# encapsulation mpls`	トンネリング カプセル化を指定します。
ステップ 8	**interworking**{**ethernet**| **ip**} 例： `Router(config-pw)# interworking ip`	擬似回線のタイプと、その回線を流れるトラフィックのタイプを指定します。
ステップ 9	**interfaceatm***slot*/*subslot*/*port*.*subinterfacenumber* 例： `Router(config-pw)# interface atm 2/0/0.1`	ATM インターフェイスを設定し、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 10	**pvc** [*name*] *vpi*/*vci***12transport** 例： `Router(config-subif)# pvc 0/200 l2transport`	ATM 相手先固定接続（PVC）に名前を割り当て、ATM 仮想回線コンフィギュレーション モードを開始します。
ステップ 11	**encapsulationaal5snap** 例： `Router(config-if-atm-member)# encapsulation aal5snap`	ATM VC の ATM AAL およびカプセル化タイプを設定します。

	コマンドまたはアクション	目的
ステップ 12	**end** 例： `Router(config-if-atm-member)# end`	特権 EXEC モードに戻ります。
ステップ 13	**interfacepseudowire***number* 例： `Router(config)# interface pseudowire 100`	擬似回線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 14	**sourcetemplatetypepseudowire***template-name* 例： `Router(config-if)# source template type pseudowire atm-eth`	atm-eth という名前のタイプ擬似回線のソース テンプレートを設定します。
ステップ 15	**neighbor***peer-addressvcid-value* 例： `Router(config-if)#  neighbor 10.0.0.200 140`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 16	**exit** 例： `Router(config-if)# exit`	特権 EXEC モードに戻ります。
ステップ 17	**l2vpnxconnectcontext***context-name* 例： `Router(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect コンフィギュレーション モードを開始します。
ステップ 18	**memberpseudowire***interface-number* 例： `Router(config-xconnect)# member pseudowire 100`	Layer 2 VPN（L2VPN）クロス コネクトを形成するようにメンバー擬似回線を指定します。
ステップ 19	**member***ip-addressvc-id***encapsulation mpls** 例： `Router(config-xconnect)# member 10.0.0.200 140 encapsulation mpls`	レイヤ 2 パケットを転送するための VC を作成します。

	コマンドまたはアクション	目的
ステップ 20	**end** 例： `Router(config-xconnect)# end`	xconnect 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。

PE2 ルータでの ATM AAL5-to-Ethernet VLAN 802.1Q

PE2 ルータで ATM AAL5-to-Ethernet VLAN 802.1Q 機能を設定するには、次の手順を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **mplslabelprotocolldp**
4. **interface***typenumber*
5. **ipaddress***ip-addressmask*
6. **pseudowire-class** [*pw-class-name*]
7. **encapsulationmpls**
8. **interworking**{**ethernet**| **ip**}
9. **interface***typeslot*/*subslot*/*port*.*subinterface-number*
10. **encapsulationdot1q***vlan-id*
11. **xconnect***ip-addressvc-id***pw-class***pw-class-name*
12. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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。

	コマンドまたはアクション	目的
ステップ 3	**mplslabelprotocolldp** 例： `Router(config)# mpls label protocol ldp`	プラットフォームの Label Distribution Protocol を設定します。
ステップ 4	**interface***typenumber* 例： `Router(config)# interface loopback 100`	インターフェイス タイプを設定し、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 5	**ipaddress***ip-addressmask* 例： `Router(config-if)# ip address 10.0.0.100 255.255.255.255`	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。
ステップ 6	**pseudowire-class** [*pw-class-name*] 例： `Router(config-if)# pseudowire-class atm-eth`	指定した名前の擬似回線クラスを確立して、擬似回線クラス コンフィギュレーション モードに入ります。
ステップ 7	**encapsulationmpls** 例： `Router(config-pw)# encapsulation mpls`	トンネリング カプセル化を指定します。
ステップ 8	**interworking**{**ethernet**| **ip**} 例： `Router(config-pw)# interworking ip`	擬似回線のタイプと、その回線を流れるトラフィックのタイプを指定します。
ステップ 9	**interface***typeslot*/*subslot*/*port*.*subinterface-number* 例： `Router(config-pw)# interface gigabitethernet 5/1/0.3`	インターフェイスを設定し、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 10	**encapsulationdot1q***vlan-id* 例： `Router(config-if)# encapsulation dot1q 1525`	VLAN の指定されたサブインターフェイス上で、トラフィックの IEEE 802.1Q カプセル化を有効にします。

	コマンドまたはアクション	目的
ステップ 11	**xconnect***ip-addressvc-id***pw-class***pw-class-name* 例： `Router(config-if)# xconnect 10.0.0.100 140 pw-class atm-eth`	AC を擬似回線にバインドし、AToM スタティック擬似回線を設定します。
ステップ 12	**end** 例： `Router(config-if-xconn)# end`	xconnect 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

（注） ATM AAl5-to-VLAN の場合、PE2 ルータ設定には、ブリッジ型インターワーキングおよびルーテッド インターワーキングの両方の **interworking** コマンドが含まれます。

（注） L2VPN インターワーキングのステータスを確認して、統計情報をチェックするには、L2VPN インターワーキングの確認，（297 ページ）を参照してください。

L2VPN プロトコルベース CLI 機能に関連するコマンドを使用した PE2 ルータでの ATM AAL5-to-Ethernet VLAN 802.1

PE2 ルータで ATM AAL5-to-Ethernet VLAN 802.1Q 機能を設定するには、次の手順を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **mplslabelprotocolldp**
4. **interface***typenumber*
5. **ipaddress***ip-addressmask*
6. **templatetypepseudowire** [*pseudowire-name*]
7. **encapsulationmpls**
8. **interworking**{**ethernet**| **ip**}
9. **interface***typeslot*/*subslot*/*port*.*subinterface-number*
10. **encapsulationdot1q***vlan-id*
11. **end**
12. **interfacepseudowire***number*
13. **sourcetemplatetypepseudowire***template-name*
14. **neighbor***peer-addressvcid-value*
15. **exit**
16. **l2vpnxconnectcontext***context-name*
17. **memberpseudowire***interface-number*
18. **member***ip-addressvc-id***encapsulation mpls**
19. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**mplslabelprotocolldp** 例： `Router(config)# mpls label protocol ldp`	プラットフォームの Label Distribution Protocol を設定します。

	コマンドまたはアクション	目的
ステップ 4	**interface***typenumber* 例： `Router(config)# interface loopback 100`	インターフェイス タイプを設定し、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 5	**ipaddress***ip-addressmask* 例： `Router(config-if)# ip address 10.0.0.100 255.255.255.255`	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。
ステップ 6	**templatetypepseudowire** [*pseudowire-name*] 例： `Router(config)# template type pseudowire atm-eth`	レイヤ 2 擬似回線 クラスの名前を指定し、擬似回線 クラス コンフィギュレーション モードを開始します。
ステップ 7	**encapsulationmpls** 例： `Router(config-pw)# encapsulation mpls`	トンネリング カプセル化を指定します。
ステップ 8	**interworking**{**ethernet**| **ip**} 例： `Router(config-pw)# interworking ip`	擬似回線のタイプと、その回線を流れるトラフィックのタイプを指定します。
ステップ 9	**interface***typeslot*/*subslot*/*port*.*subinterface-number* 例： `Router(config-pw)# interface gigabitethernet 5/1/0.3`	インターフェイスを設定し、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 10	**encapsulationdot1q***vlan-id* 例： `Router(config-if)# encapsulation dot1q 1525`	VLAN の指定されたサブインターフェイス上で、トラフィックの IEEE 802.1Q カプセル化を有効にします。
ステップ 11	**end** 例： `Router(config-if)# end`	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
ステップ 12	**interfacepseudowire***number* 例： `Router(config)# interface pseudowire 100`	擬似回線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 13	**sourcetemplatetypepseudowire***template-name* 例： `Router(config-if)# source template type pseudowire atm-eth`	atm-eth という名前のタイプ擬似回線のソース テンプレートを設定します。
ステップ 14	**neighbor***peer-addressvcid-value* 例： `Router(config-if)#  neighbor 10.0.0.100 140`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 15	**exit** 例： `Router(config-if)# exit`	特権 EXEC モードに戻ります。
ステップ 16	**l2vpnxconnectcontext***context-name* 例： `Router(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect コンフィギュレーションモードを開始します。
ステップ 17	**memberpseudowire***interface-number* 例： `Router(config-xconnect)# member pseudowire 100`	Layer 2 VPN（L2VPN）クロス コネクトを形成するようにメンバー擬似回線を指定します。
ステップ 18	**member***ip-addressvc-id***encapsulation mpls** 例： `Router(config-xconnect)# member 10.0.0.100 140 encapsulation mpls`	レイヤ 2 パケットを転送するための VC を作成します。
ステップ 19	**end** 例： `Router(config-xconnect)# end`	xconnect 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

（注） ATM AAl5-to-VLAN の場合、PE2 ルータ設定には、ブリッジ型インターワーキングおよびルーテッド インターワーキングの両方の **interworking** コマンドが含まれます。

（注） L2VPN インターワーキングのステータスを確認して、統計情報をチェックするには、L2VPN インターワーキングの確認，（297 ページ）を参照してください。

Ethernet VLAN-to-Frame Relay インターワーキングの設定

このセクションでは、次の AToM 設定について説明し、例を示します。上図の FR-to-Ethernet AToM ブリッジ型インターワーキングのネットワーク トポロジはさまざまな構成を示しています。

PE1 ルータ上でのフレーム リレー DLCI/イーサネット ポート間接続

次の手順を使用して、PE1 ルータ上でフレーム リレー DLCI/イーサネット ポート間接続機能を設定できます。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **mplslabelprotocolldp**
4. **interface***typenumber*
5. **ipaddress***ip-addressmask*
6. **pseudowire-class** [*pw-class-name*]
7. **encapsulationmpls**
8. **interworkingethernet**
9. **interface***typeslot*/*subslot*/*port*
10. **encapsulationframe-relay**
11. **connect***connection-nameinterfacedlci*{*interface dlci* | **l2transport**}
12. **xconnect***ip-addressvc-id***pw-class***pw-class-name*
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	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Router> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**mplslabelprotocolldp** 例： `Router(config)# mpls label protocol ldp`	プラットフォームの Label Distribution Protocol を確立します。
ステップ 4	**interface***typenumber* 例： `Router(config)# interface loopback 100`	インターフェイス タイプを設定し、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 5	**ipaddress***ip-addressmask* 例： `Router(config-if)# ip address 10.0.0.100 255.255.255.255`	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。
ステップ 6	**pseudowire-class** [*pw-class-name*] 例： `Router(config-if)# pseudowire-class fr-eth`	指定した名前の擬似回線クラスを確立して、擬似回線クラス コンフィギュレーション モードに入ります。
ステップ 7	**encapsulationmpls** 例： `Router(config-pw)# encapsulation mpls`	トンネリング カプセル化を指定します。
ステップ 8	**interworkingethernet** 例： `Router(config-pw)# interworking ethernet`	擬似回線のタイプと、その回線を流れるトラフィックのタイプを指定します。

	コマンドまたはアクション	目的
ステップ 9	**interface***typeslot/subslot/port* 例： `Router(config-pw)# interface serial 2/0/0`	インターフェイスを設定し、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 10	**encapsulationframe-relay** 例： `Router(config-if)# encapsulation frame-relay`	フレームリレーカプセル化をイネーブルにします。
ステップ 11	**connect***connection-nameinterfacedlci*{*interface dlci* | **l2transport**} 例： `Router(config-if)# connect fr-vlan-1 POS2/3/1 151 l2transport`	フレーム リレー PVC 間の接続を定義します。
ステップ 12	**xconnect***ip-addressvc-id***pw-class***pw-class-name* 例： `Router(config-if)# xconnect 10.0.0.200 151 pw-class pw-class-bridge`	AC を擬似回線にバインドし、AToM スタティック擬似回線を設定します。
ステップ 13	**end** 例： `Router(config-if-xconn)# end`	xconnect コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した PE1 ルータ上でのフレーム リレー DLCI/イーサネット ポート間接続

次の手順を使用して、PE1 ルータ上でフレーム リレー DLCI/イーサネット ポート間接続機能を設定できます。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **mplslabelprotocolldp**
4. **interface***typenumber*
5. **ipaddress***ip-addressmask*
6. **template type pseudowire** [*pseudowire-name*]
7. **encapsulationmpls**
8. **interworkingethernet**
9. **interface***typeslot*/*subslot*/*port*
10. **encapsulationframe-relay**
11. **connect***connection-nameinterfacedlci*{*interface dlci* | **l2transport**}
12. **end**
13. **interfacepseudowire***number*
14. **sourcetemplate type pseudowire***template-name*
15. **neighbor***peer-address vcid-value*
16. **exit**
17. **l2vpn xconnectcontext***context-name*
18. **member pseudowire***interface-number*
19. **member** *ip-addressvc-id***encapsulation mpls**
20. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**mplslabelprotocolldp** 例： `Router(config)# mpls label protocol ldp`	プラットフォームの Label Distribution Protocol を確立します。

	コマンドまたはアクション	目的
ステップ 4	**interface***typenumber* 例： `Router(config)# interface loopback 100`	インターフェイス タイプを設定し、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 5	**ipaddress***ip-addressmask* 例： `Router(config-if)# ip address 10.0.0.100 255.255.255.255`	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。
ステップ 6	**template type pseudowire** [*pseudowire-name*] 例： `Router(config)# template type pseudowire fr-eth`	レイヤ 2 擬似回線 クラスの名前を指定し、擬似回線 クラス コンフィギュレーション モードを開始します。
ステップ 7	**encapsulationmpls** 例： `Router(config-pw)# encapsulation mpls`	トンネリング カプセル化を指定します。
ステップ 8	**interworkingethernet** 例： `Router(config-pw)# interworking ethernet`	擬似回線のタイプと、その回線を流れるトラフィックのタイプを指定します。
ステップ 9	**interface***typeslot*/*subslot*/*port* 例： `Router(config-pw)# interface serial 2/0/0`	インターフェイスを設定し、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 10	**encapsulationframe-relay** 例： `Router(config-if)# encapsulation frame-relay`	フレームリレーカプセル化をイネーブルにします。
ステップ 11	**connect***connection-nameinterfacedlci*{*interface dlci* | **l2transport**} 例： `Router(config-if)# connect fr-vlan-1 POS2/3/1 151 l2transport`	フレーム リレー PVC 間の接続を定義します。

	コマンドまたはアクション	目的
ステップ 12	**end** 例： `Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 13	**interfacepseudowire***number* 例： `Router(config)# interface pseudowire 100`	擬似回線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 14	**sourcetemplate type pseudowire***template-name* 例： `Router(config-if)# source template type pseudowire pwclass-bridge`	pwclass-bridge という名前のタイプ擬似回線のソース テンプレートを設定します。
ステップ 15	**neighbor***peer-address vcid-value* 例： `Router(config-if)#  neighbor 10.0.0.200 151`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 16	**exit** 例： `Router(config-if)# exit`	特権 EXEC モードに戻ります。
ステップ 17	**l2vpn xconnectcontext***context-name* 例： `Router(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect コンフィギュレーション モードを開始します。
ステップ 18	**member pseudowire***interface-number* 例： `Router(config-xconnect)# member pseudowire 100`	Layer 2 VPN（L2VPN）クロス コネクトを形成するようにメンバー擬似回線を指定します。
ステップ 19	**member** *ip-addressvc-id***encapsulation mpls** 例： `Router(config-xconnect)# member 10.0.0.200 151 encapsulation mpls`	レイヤ 2 パケットを転送するための VC を作成します。

	コマンドまたはアクション	目的
ステップ 20	**end** 例： `Router(config-xconnect)# end`	xconnect コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

PE2 ルータ上でのフレーム リレー DLCI/イーサネット ポート間接続

次の手順を使用して、PE2 ルータ上でフレーム リレー DLCI/イーサネット ポート間接続機能を設定できます。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **mplslabelprotocolldp**
4. **interface***typenumber*
5. **ipaddress***ip-addressmask*
6. **pseudowire-class** [*pw-class-name*]
7. **encapsulationmpls**
8. **interworkingethernet**
9. **interface***typeslot*/*subslot*/*port*
10. **xconnect***ip-addressvc-id***pw-class***pw-class-name*
11. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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。

	コマンドまたはアクション	目的
ステップ 3	**mplslabelprotocolldp** 例： `Router(config)# mpls label protocol ldp`	プラットフォームの Label Distribution Protocol を確立します。
ステップ 4	**interface***typenumber* 例： `Router(config)# interface loopback 100`	インターフェイス タイプを設定し、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 5	**ipaddress***ip-addressmask* 例： `Router(config-if)# ip address 10.0.0.100 255.255.255.255`	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。
ステップ 6	**pseudowire-class** [*pw-class-name*] 例： `Router(config-if)# pseudowire-class atm-eth`	指定した名前の擬似回線クラスを確立して、擬似回線クラス コンフィギュレーション モードに入ります。
ステップ 7	**encapsulationmpls** 例： `Router(config-pw)# encapsulation mpls`	トンネリング カプセル化を指定します。
ステップ 8	**interworkingethernet** 例： `Router(config-pw)# interworking ethernet`	擬似回線のタイプと、その回線を流れるトラフィックのタイプを指定します。
ステップ 9	**interface***typeslot*/*subslot*/*port* 例： `Router(config-pw)# interface gigabitethernet 2/0/0`	インターフェイスを設定し、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 10	**xconnect***ip-addressvc-id***pw-class***pw-class-name* 例： `Router(config-if)# xconnect 10.0.0.200 140 pw-class atm-eth`	AC を擬似回線にバインドし、AToM スタティック擬似回線を設定します。

	コマンドまたはアクション	目的
ステップ 11	**end** 例： `Router(config-if-xconn)# end`	xconnect コンフィギュレーションモードを終了して、特権 EXEC モードに戻ります。

次の作業

（注） ブリッジ型インターワーキングが設定されている場合は、PE2 ルータ設定に **interworking ethernet** コマンドが含まれません。これは、その設定が Like-to-Like として扱われるうえ、AC が既にイーサネット ポートだからです。ただし、ルーテッド インターワーキングが設定されている場合は、PE2 ルータ設定に **interworking ip** コマンドが含まれます。

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した PE2 ルータ上でのフレーム リレー DLCI/イーサネット ポート間接続

次の手順を使用して、PE2 ルータ上でフレーム リレー DLCI/イーサネット ポート間接続機能を設定できます。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **mplslabelprotocolldp**
4. **interface***typenumber*
5. **ipaddress***ip-addressmask*
6. **template type pseudowire** [*pseudowire-name*]
7. **encapsulationmpls**
8. **interworkingethernet**
9. **interface***typeslot*/*subslot*/*port*
10. **end**
11. **interfacepseudowire***number*
12. **sourcetemplate type pseudowire***template-name*
13. **neighbor***peer-address vcid-value*
14. **exit**
15. **l2vpn xconnectcontext***context-name*
16. **member pseudowire***interface-number*
17. **member** *ip-addressvc-id***encapsulation mpls**
18. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**mplslabelprotocolldp** 例： `Router(config)# mpls label protocol ldp`	プラットフォームの Label Distribution Protocol を確立します。

	コマンドまたはアクション	目的
ステップ 4	**interface***typenumber* 例： `Router(config)# interface loopback 100`	インターフェイスタイプを設定し、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 5	**ipaddress***ip-addressmask* 例： `Router(config-if)# ip address 10.0.0.100 255.255.255.255`	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。
ステップ 6	**template type pseudowire** [*pseudowire-name*] 例： `Router(config)# template type pseudowire atm-eth`	レイヤ 2 擬似回線 クラスの名前を指定し、擬似回線クラス コンフィギュレーション モードを開始します。
ステップ 7	**encapsulationmpls** 例： `Router(config-pw)# encapsulation mpls`	トンネリング カプセル化を指定します。
ステップ 8	**interworkingethernet** 例： `Router(config-pw)# interworking ethernet`	擬似回線のタイプと、その回線を流れるトラフィックのタイプを指定します。
ステップ 9	**interface***typeslot/subslot/port* 例： `Router(config-pw)# interface gigabitethernet 2/0/0`	インターフェイスを設定し、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 10	**end** 例： `Router(config-pw)# end`	特権 EXEC モードに戻ります。
ステップ 11	**interfacepseudowire***number* 例： `Router(config)# interface pseudowire 100`	擬似回線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。

	コマンドまたはアクション	目的
ステップ 12	**sourcetemplate type pseudowire***template-name* 例： `Router(config-if)# source template type pseudowire atm-eth`	atm-eth という名前のタイプ擬似回線のソーステンプレートを設定します。
ステップ 13	**neighbor***peer-address vcid-value* 例： `Router(config-if)# neighbor 10.0.0.200 140`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 14	**exit** 例： `Router(config-if)# exit`	特権 EXEC モードに戻ります。
ステップ 15	**l2vpn xconnectcontext***context-name* 例： `Router(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect コンフィギュレーション モードを開始します。
ステップ 16	**member pseudowire***interface-number* 例： `Router(config-xconnect)# member pseudowire 100`	Layer 2 VPN（L2VPN）クロス コネクトを形成するようにメンバー擬似回線を指定します。
ステップ 17	**member** *ip-addressvc-id***encapsulation mpls** 例： `Router(config-xconnect)# member 10.0.0.200 140 encapsulation mpls`	レイヤ 2 パケットを転送するための VC を作成します。
ステップ 18	**end** 例： `Router(config-xconnect)# end`	xconnect コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

次の作業

（注） ブリッジ型インターワーキングが設定されている場合は、PE2 ルータ設定に **interworking ethernet** コマンドが含まれません。これは、その設定が Like-to-Like として扱われるうえ、AC が既にイーサネット ポートだからです。ただし、ルーテッド インターワーキングが設定されている場合は、PE2 ルータ設定に **interworking ip** コマンドが含まれます。

PE1 ルータ上でのフレーム リレー DLCI/イーサネット VLAN 802.1Q 間接続

PE1 ルータ上でのフレーム リレー DLCI/イーサネット VLAN 802.1Q 間接続機能を設定するには、次の手順を使用します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **mplslabelprotocolldp**
4. **interface***typenumber*
5. **ipaddress***ip-addressmask*
6. **pseudowire-class** [*pw-class-name*]
7. **encapsulationmpls**
8. **interworking**{**ethernet**| **ip**}
9. **frame-relayswitching**
10. **interface***typeslot*/*subslot*/*port*
11. **encapsulationframe-relay**
12. **frame-relayintf-type**[**dce**]
13. **connect***connection-nameinterfacedlci*{*interfacedlci* | **l2transport**}
14. **xconnect***ip-addressvc-id***pw-class***pw-class-name*
15. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 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	**mplslabelprotocolldp** 例： `Router(config)# mpls label protocol ldp`	プラットフォームの Label Distribution Protocol を確立します。
ステップ 4	**interface***typenumber* 例： `Router(config)# interface loopback 100`	インターフェイスタイプを設定し、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 5	**ipaddress***ip-addressmask* 例： `Router(config-if)# ip address 10.0.0.100 255.255.255.255`	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。
ステップ 6	**pseudowire-class** [*pw-class-name*] 例： `Router(config-if)# pseudowire-class atm-eth`	指定した名前の擬似回線クラスを確立して、擬似回線クラスコンフィギュレーションモードに入ります。
ステップ 7	**encapsulationmpls** 例： `Router(config-pw)# encapsulation mpls`	トンネリング カプセル化を指定します。
ステップ 8	**interworking**{**ethernet**| **ip**} 例： `Router(config-pw)# interworking ip`	擬似回線のタイプと、その回線を流れるトラフィックのタイプを指定します。
ステップ 9	**frame-relayswitching** 例： `Router(config-pw)# frame-relay switching`	フレーム リレー DCE デバイスの PVC スイッチングを有効にします。

	コマンドまたはアクション	目的
ステップ 10	**interface***typeslot/subslot/port* 例： `Router(config-pw)# interface serial 2/0/0`	インターフェイスを設定し、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 11	**encapsulationframe-relay** 例： `Router(config-if)# encapsulation frame-relay`	フレームリレー カプセル化をイネーブルにします。
ステップ 12	**frame-relayintf-type**[**dce**] 例： `Router(config-if)# frame-relay intf-type dce`	フレーム リレー スイッチのタイプを設定します。
ステップ 13	**connect***connection-nameinterfacedlci*{*interfacedlci* | **l2transport**} 例： `Router(config-if)# connect one serial0 16 serial1 100`	フレーム リレー PVC 間の接続を定義します。
ステップ 14	**xconnect***ip-addressvc-id***pw-class***pw-class-name* 例： `Router(config-if)# xconnect 10.0.0.200 140 pw-class atm-eth`	AC を擬似回線にバインドし、AToM スタティック擬似回線を設定します。
ステップ 15	**end** 例： `Router(config-if-xconn)# end`	xconnect コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した PE1 ルータ上でのフレーム リレー DLCI/イーサネット VLAN 802.1Q 間接続

PE1 ルータ上でのフレーム リレー DLCI/イーサネット VLAN 802.1Q 間接続機能を設定するには、次の手順を使用します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **mplslabelprotocolldp**
4. **interface***typenumber*
5. **ipaddress***ip-addressmask*
6. **templatetypepseudowire** [*pseudowire-name*]
7. **encapsulationmpls**
8. **interworking**{**ethernet**| **ip**}
9. **frame-relayswitching**
10. **interface***typeslot*/*subslot*/*port*
11. **encapsulationframe-relay**
12. **frame-relayintf-type**[**dce**]
13. **connect***connection-nameinterfacedlci*{*interfacedlci* | **l2transport**}
14. **end**
15. **interfacepseudowire***number*
16. **sourcetemplatetypepseudowire***template-name*
17. **neighbor***peer-addressvcid-value*
18. **exit**
19. **l2vpnxconnectcontext***context-name*
20. **memberpseudowire***interface-number*
21. **member***ip-addressvc-id***encapsulation mpls**
22. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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。

	コマンドまたはアクション	目的
ステップ 3	**mplslabelprotocolldp** 例： `Router(config)# mpls label protocol ldp`	プラットフォームの Label Distribution Protocol を確立します。
ステップ 4	**interface***typenumber* 例： `Router(config)# interface loopback 100`	インターフェイスタイプを設定し、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 5	**ipaddress***ip-addressmask* 例： `Router(config-if)# ip address 10.0.0.100 255.255.255.255`	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。
ステップ 6	**templatetypepseudowire** [*pseudowire-name*] 例： `Router(config)# template type pseudowire atm-eth`	レイヤ 2 擬似回線 クラスの名前を指定し、擬似回線 クラス コンフィギュレーション モードを開始します。
ステップ 7	**encapsulationmpls** 例： `Router(config-pw)# encapsulation mpls`	トンネリング カプセル化を指定します。
ステップ 8	**interworking**{**ethernet**| **ip**} 例： `Router(config-pw)# interworking ip`	擬似回線のタイプと、その回線を流れるトラフィックのタイプを指定します。
ステップ 9	**frame-relayswitching** 例： `Router(config-pw)# frame-relay switching`	フレーム リレー DCE デバイスの PVC スイッチングを有効にします。
ステップ 10	**interface***typeslot*/*subslot*/*port* 例： `Router(config-pw)# interface serial 2/0/0`	インターフェイスを設定し、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 11	**encapsulationframe-relay** 例： `Router(config-if)# encapsulation frame-relay`	フレームリレー カプセル化をイネーブルにします。
ステップ 12	**frame-relayintf-type**[**dce**] 例： `Router(config-if)# frame-relay intf-type dce`	フレーム リレー スイッチのタイプを設定します。
ステップ 13	**connect***connection-nameinterfacedlci*{*interfacedlci* | **l2transport**} 例： `Router(config-if)# connect one serial0 16 serial1 100`	フレーム リレー PVC 間の接続を定義します。
ステップ 14	**end** 例： `Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 15	**interfacepseudowire***number* 例： `Router(config)# interface pseudowire 100`	擬似回線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 16	**sourcetemplatetypepseudowire***template-name* 例： `Router(config-if)# source template type pseudowire atm-eth`	atm-eth という名前のタイプ擬似回線のソーステンプレートを設定します。
ステップ 17	**neighbor***peer-addressvcid-value* 例： `Router(config-if)#  neighbor 10.0.0.200 140`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 18	**exit** 例： `Router(config-if)# exit`	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
ステップ 19	**l2vpnxconnectcontext***context-name* 例： `Router(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect コンフィギュレーション モードを開始します。
ステップ 20	**memberpseudowire***interface-number* 例： `Router(config-xconnect)# member pseudowire 100`	Layer 2 VPN（L2VPN）クロス コネクトを形成するようにメンバー擬似回線を指定します。
ステップ 21	**member***ip-addressvc-id***encapsulation mpls** 例： `Router(config-xconnect)# member 10.0.0.200 140 encapsulation mpls`	レイヤ 2 パケットを転送するための VC を作成します。
ステップ 22	**end** 例： `Router(config-xconnect)# end`	xconnect コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

PE2 ルータ上でのフレーム リレー DLCI/イーサネット VLAN 802.1Q 間接続

PE2 ルータ上でのフレーム リレー DLCI/イーサネット VLAN 802.1Q 間接続機能を設定するには、次の手順を使用します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **mplslabelprotocolldp**
4. **interface***typenumber*
5. **ipaddress***ip-addressmask*
6. **pseudowire-class** [*pw-class-name*]
7. **encapsulationmpls**
8. **interworking**{**ethernet**| **ip**}
9. **interface***typeslot*/*subslot*/*port*.*subinterface-number*
10. **encapsulationdot1q***vlan-id*
11. **xconnect***ip-addressvc-id***pw-class***pw-class-name*
12. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**mplslabelprotocolldp** 例： `Router(config)# mpls label protocol ldp`	プラットフォームの Label Distribution Protocol を確立します。
ステップ 4	**interface***typenumber* 例： `Router(config)# interface loopback 100`	インターフェイス タイプを設定し、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 5	**ipaddress***ip-addressmask* 例： `Router(config-if)# ip address 10.0.0.100 255.255.255.255`	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 6	**pseudowire-class** [*pw-class-name*] 例： `Router(config-if)# pseudowire-class atm-eth`	指定した名前の擬似回線クラスを確立して、擬似回線クラス コンフィギュレーション モードに入ります。
ステップ 7	**encapsulationmpls** 例： `Router(config-pw)# encapsulation mpls`	トンネリング カプセル化を指定します。
ステップ 8	**interworking**{**ethernet**| **ip**} 例： `Router(config-pw)# interworking ip`	擬似回線のタイプと、その回線を流れるトラフィックのタイプを指定します。
ステップ 9	**interface***typeslot*/*subslot*/*port*.*subinterface-number* 例： `Router(config-pw)# interface gigabitethernet 5/1/0.3`	インターフェイスを設定し、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 10	**encapsulationdot1q***vlan-id* 例： `Router(config-if)# encapsulation dot1q 1525`	VLAN の指定されたサブインターフェイス上で、トラフィックの IEEE 802.1Q カプセル化をイネーブルにします。
ステップ 11	**xconnect***ip-addressvc-id***pw-class***pw-class-name* 例： `Router(config-if)# xconnect 10.0.0.100 140 pw-class atm-eth`	AC を擬似回線にバインドし、AToM スタティック擬似回線を設定します。
ステップ 12	**end** 例： `Router(config-if-xconn)# end`	xconnect コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

次の作業

（注） フレーム リレー DLCI/VLAN 間接続の場合は、PE2 ルータ設定に、ブリッジ型インターワーキングとルーテッド インターワーキングの両方の **interworking** コマンドが含まれます。

（注） L2VPN インターワーキングのステータスを確認して、統計情報をチェックするには、L2VPN インターワーキングの確認, （297 ページ）を参照してください。

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した PE2 ルータ上でのフレーム リレー DLCI/イーサネット VLAN 802.1Q 間接続

PE2 ルータ上でのフレーム リレー DLCI/イーサネット VLAN 802.1Q 間接続機能を設定するには、次の手順を使用します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **mplslabelprotocolldp**
4. **interface***typenumber*
5. **ipaddress***ip-addressmask*
6. **pseudowire-class** [*pw-class-name*]
7. **encapsulationmpls**
8. **interworking**{**ethernet**| **ip**}
9. **interface***typeslot*/*subslot*/*port*.*subinterface-number*
10. **encapsulationdot1q***vlan-id*
11. **end**
12. **interfacepseudowire***number*
13. **sourcetemplatetypepseudowire***template-name*
14. **exit**
15. **l2vpnxconnectcontext***context-name*
16. **memberpseudowire***interface-number*
17. **member***ip-addressvc-id***encapsulation mpls**
18. **interworkingip**
19. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**mplslabelprotocolldp** 例： `Router(config)# mpls label protocol ldp`	プラットフォームの Label Distribution Protocol を確立します。
ステップ 4	**interface***typenumber* 例： `Router(config)# interface loopback 100`	インターフェイス タイプを設定し、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 5	**ipaddress***ip-addressmask* 例： `Router(config-if)# ip address 10.0.0.100 255.255.255.255`	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。
ステップ 6	**pseudowire-class** [*pw-class-name*] 例： `Router(config-if)# pseudowire-class atm-eth`	指定した名前の擬似回線クラスを確立して、擬似回線クラス コンフィギュレーション モードに入ります。
ステップ 7	**encapsulationmpls** 例： `Router(config-pw)# encapsulation mpls`	トンネリング カプセル化を指定します。
ステップ 8	**interworking**{**ethernet**| **ip**} 例： `Router(config-pw)# interworking ip`	擬似回線のタイプと、その回線を流れるトラフィックのタイプを指定します。

	コマンドまたはアクション	目的
ステップ 9	**interface***typeslot/subslot/port.subinterface-number* 例： `Router(config-pw)# interface gigabitethernet 5/1/0.3`	インターフェイスを設定し、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 10	**encapsulationdot1q***vlan-id* 例： `Router(config-if)# encapsulation dot1q 1525`	VLAN の指定されたサブインターフェイス上で、トラフィックの IEEE 802.1Q カプセル化をイネーブルにします。
ステップ 11	**end** 例： `Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 12	**interfacepseudowire***number* 例： `Router(config)# interface pseudowire 100`	擬似回線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 13	**sourcetemplatetypepseudowire***template-name* 例： `Router(config-if)# source template type pseudowire ether-pw`	ether-pw という名前のタイプ擬似回線のソース テンプレートを設定します。
ステップ 14	**exit** 例： `Router(config-if)# exit`	特権 EXEC モードに戻ります。
ステップ 15	**l2vpnxconnectcontext***context-name* 例： `Router(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect コンフィギュレーション モードを開始します。
ステップ 16	**memberpseudowire***interface-number* 例： `Router(config-xconnect)# member pseudowire 100`	Layer 2 VPN（L2VPN）クロス コネクトを形成するようにメンバー擬似回線を指定します。

	コマンドまたはアクション	目的
ステップ 17	**member***ip-addressvc-id***encapsulation mpls** 例： `Router(config-xconnect)# member 10.0.0.100 140 encapsulation mpls`	レイヤ2パケットを転送するためのVCを作成します。
ステップ 18	**interworkingip** 例： `Router(config-xconnect)# interworking ip`	L2VPN クロス コネクト コンテキストを確立します。
ステップ 19	**end** 例： `Router(config-xconnect)# end`	xconnect コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

次の作業

（注） フレーム リレー DLCI/VLAN 間接続の場合は、PE2 ルータ設定に、ブリッジ型インターワーキングとルーテッド インターワーキングの両方の **interworking** コマンドが含まれます。

（注） L2VPN インターワーキングのステータスを確認して、統計情報をチェックするには、L2VPN インターワーキングの確認，（297 ページ）を参照してください。

HDLC-to-Ethernet インターワーキングの設定

HDLC PE デバイスでの HDLC-to-Ethernet ブリッジ型インターワーキング

手順の概要

1. イネーブル化
2. **configure terminal**
3. **pseudowire-class** [*pw-class-name*]
4. **encapsulation mpls**
5. **interworking ethernet**
6. **interface***typeslot*/*subslot*/*port* [**.***subinterface*]
7. **noipaddress** [*ip-address mask*] [**secondary**]
8. **xconnect***peer-router-idvc id***pseudowire-class** [*pw-class-name*]
9. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**pseudowire-class** [*pw-class-name*] 例： `Device(config)# pseudowire-class pw-iw-ether`	レイヤ 2 擬似回線 クラスの名前を指定し、擬似回線クラス 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	**encapsulation mpls** 例： `Device(config-pw-class)# encapsulation mpls`	トンネリング カプセル化を MPLS として指定します。

	コマンドまたはアクション	目的
ステップ 5	**interworking ethernet** 例： `Device(config-pw-class)# interworking ethernet`	擬似回線のタイプとしてだけでなく、擬似回線上を通過可能なトラフィックのタイプとしてもイーサネットを指定します。
ステップ 6	**interface***typeslot*/*subslot*/*port* [**.***subinterface*] 例： `Device(config-pw-class)# interface serial 3/1/0`	シリアル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 7	**noipaddress** [*ip-address mask*] [**secondary**] 例： `Device(config-if)# no ip address`	IP 処理をディセーブルにします。
ステップ 8	**xconnect***peer-router-idvc id***pseudowire-class** [*pw-class-name*] 例： `Device(config-if)# xconnect 198.51.100.2 123 pseudowire-class pw-iw-ether`	レイヤ 2 パケットを転送するための仮想回線（VC）を作成します。
ステップ 9	**end** 例： `Device(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。

L2VPN プロトコルベースの CLI 機能と関連するコマンドを使用する、HDLC PE デバイスでの HDLC-to-Ethernet ブリッジ型インターワーキング

手順の概要

1. イネーブル化
2. **configure terminal**
3. **template type pseudowire***name*
4. **encapsulation mpls**
5. **exit**
6. **interface pseudowire***number*
7. **source template type pseudowire***name*
8. **encapsulation mpls**
9. **neighbor***peer-addressvc id-value*
10. **signaling protocol ldp**
11. **no shutdown**
12. **exit**
13. **l2vpn xconnect context***context-name*
14. **interworking ethernet**
15. **member***interface-type-number*
16. **member pseudowire***interface-number*
17. **no shutdown**
18. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**template type pseudowire***name* 例： `Device# template type pseudowire temp5`	指定した名前でテンプレート擬似回線を作成し、テンプレート 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	**encapsulation mpls** 例： `Device(config-template)# encapsulation mpls`	トンネリング カプセル化を MPLS として指定します。
ステップ 5	**exit** 例： `Device(config-template)# exit`	テンプレート コンフィギュレーション モードを終了して、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 6	**interface pseudowire***number* 例： `Device(config)# interface pseudowire 107`	指定した値でインターフェイス擬似回線を確立して、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 7	**source template type pseudowire***name* 例： `Device(config-if)# source template type pseudowire temp5`	temp5 という名前のタイプ擬似回線としてソース テンプレートを設定します。
ステップ 8	**encapsulation mpls** 例： `Device(config-if)# encapsulation mpls`	トンネリング カプセル化を MPLS として指定します。
ステップ 9	**neighbor***peer-addressvc id-value* 例： `Device(config-if)# neighbor 10.0.0.11 107`	L2VPN 擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 10	**signaling protocol ldp** 例： `Device(config-if)# signaling protocol ldp`	擬似回線クラス用のラベル配布プロトコル（LDP）が設定されるように指定します。
ステップ 11	**no shutdown** 例： `Device(config-if)# no shutdown`	インターフェイス擬似回線を再起動します。

	コマンドまたはアクション	目的
ステップ 12	**exit** 例： `Device(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 13	**l2vpn xconnect context***context-name* 例： `Device(config)# l2vpn xconnect context con1`	L2VPN クロス コネクト コンテキストを作成して、xconnect コンフィギュレーション モードを開始します。
ステップ 14	**interworking ethernet** 例： `Device(config-xconnect)# interworking ethernet`	擬似回線のタイプとしてだけでなく、擬似回線上を通過可能なトラフィックのタイプとしてもイーサネットを指定します。
ステップ 15	**member***interface-type-number* 例： `Device(config-xconnect)# member serial 0/1/0:0`	メンバーインターフェイスのロケーションを指定します。
ステップ 16	**member pseudowire***interface-number* 例： `Device(config-xconnect)# member pseudowire 107`	L2VPN クロス コネクトを形成するために、メンバー擬似回線を指定します。
ステップ 17	**no shutdown** 例： `Device(config-xconnect)# no shutdown`	メンバー インターフェイスを再起動します。
ステップ 18	**end** 例： `Device(config-xconnect)# end`	xconnect コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

イーサネット PE デバイス上での HDLC/イーサネット間ブリッジ型インターワーキング（ポート モード）

手順の概要

1. イネーブル化
2. **configure terminal**
3. **pseudowire-class** [*pw-class-name*]
4. **encapsulation mpls**
5. **interworking ethernet**
6. **interface***typeslot*/*subslot*/*port* [**.***subinterface*]
7. **encapsulation mpls**
8. **xconnect***peer-router-idvc id***pseudowire-class** [*pw-class-name*]
9. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**pseudowire-class** [*pw-class-name*] 例： `Device(config)# pseudowire-class pw-iw-ether`	レイヤ 2 擬似回線 クラスの名前を指定し、擬似回線 クラス 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	**encapsulation mpls** 例： `Device(config-pw-class)# encapsulation mpls`	トンネリング カプセル化を MPLS として指定します。
ステップ 5	**interworking ethernet** 例： `Device(config-pw-class)# interworking ethernet`	擬似回線のタイプとしてだけでなく、擬似回線上を通過可能なトラフィックのタイプとしてもイーサネットを指定します。

	コマンドまたはアクション	目的
ステップ 6	**interface***typeslot/subslot/port* [**.***subinterface*] 例： `Device(config-pw-class)# interface gigabitethernet 4/0/0.1`	ギガビット イーサネット サブインターフェイスを指定し、サブインターフェイス コンフィギュレーション モードを開始します。 • 隣接するイーサネット CE デバイスのサブインターフェイスがこのイーサネット PE デバイスと同じ VLAN 上に存在することを確認します。
ステップ 7	**encapsulation mpls** 例： `Device(config-subif)# encapsulation mpls`	トンネリング カプセル化を MPLS として指定します。
ステップ 8	**xconnect***peer-router-idvc id***pseudowire-class** [*pw-class-name*] 例： `Device(config-subif)# xconnect 198.51.100.2 123 pseudowire-class pw-iw-ether`	レイヤ 2 パケットを転送するための仮想回線（VC）を作成します。
ステップ 9	**end** 例： `Device(config-subif)# end`	サブインターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

L2VPN プロトコルベースの CLI 機能と関連するコマンドを使用する、イーサネット PE デバイスでの HDLC-to-Ethernet ブリッジ型インターワーキング（ポート モード）

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface***typeslot*/*subslot*/*port* [**.***subinterface*]
4. **encapsulation mpls**
5. **no ip address**
6. **no shutdown**
7. **exit**
8. **template type pseudowire***name*
9. **encapsulation mpls**
10. **exit**
11. **interface pseudowire***number*
12. **source template type pseudowire***name*
13. **encapsulation mpls**
14. **neighbor***peer-addressvc id-value*
15. **signaling protocol ldp**
16. **no shutdown**
17. **exit**
18. **l2vpn xconnect context***context-name*
19. **interworking ethernet**
20. **member***interface-type-number*
21. **member pseudowire***interface-number*
22. **no shutdown**
23. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 3	**interface***typeslot*/*subslot*/*port* [.*subinterface*] 例： `Device(config)# interface fastethernet 4/0/0.1`	サブインターフェイスを指定し、サブインターフェイス コンフィギュレーション モードを開始します。 • 隣接するイーサネットCEデバイスのサブインターフェイスがこのイーサネット PE デバイスと同じ VLAN 上に存在することを確認します。
ステップ 4	**encapsulation mpls** 例： `Device(config-subif)# encapsulation mpls`	トンネリング カプセル化を MPLS として指定します。
ステップ 5	**no ip address** 例： `Device(config-subif)# no ip address`	IP 処理をディセーブルにします。
ステップ 6	**no shutdown** 例： `Device(config-subif)# no shutdown`	ファスト イーサネットのサブインターフェイスを再起動します。
ステップ 7	**exit** 例： `Device(config-subif)# exit`	サブ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	**template type pseudowire***name* 例： `Device(config)# template type pseudowire temp4`	指定した名前でテンプレート擬似回線を作成し、テンプレート コンフィギュレーション モードを開始します。
ステップ 9	**encapsulation mpls** 例： `Device(config-template)# encapsulation mpls`	トンネリング カプセル化を MPLS として指定します。
ステップ 10	**exit** 例： `Device(config-template)# exit`	テンプレートコンフィギュレーションモードを終了して、グローバルコンフィギュレーションモードに戻ります。

	コマンドまたはアクション	目的
ステップ 11	**interface pseudowire***number* 例： `Device(config)# interface pseudowire 109`	指定した値でインターフェイス擬似回線を確立して、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 12	**source template type pseudowire***name* 例： `Device(config-if)# source template type pseudowire temp4`	temp4 という名前のタイプ擬似回線としてソース テンプレートを設定します。
ステップ 13	**encapsulation mpls** 例： `Device(config-if)# encapsulation mpls`	トンネリング カプセル化を MPLS として指定します。
ステップ 14	**neighbor***peer-addressvc id-value* 例： `Device(config-if)# neighbor 10.0.0.15 109`	L2VPN 擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 15	**signaling protocol ldp** 例： `Device(config-if)# signaling protocol ldp`	擬似回線クラス用のラベル配布プロトコル（LDP）が設定されるように指定します。
ステップ 16	**no shutdown** 例： `Device(config-if)# no shutdown`	インターフェイス擬似回線を再起動します。
ステップ 17	**exit** 例： `Device(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 18	**l2vpn xconnect context***context-name* 例： `Device(config)# l2vpn xconnect context con2`	L2VPN クロス コネクト コンテキストを作成して、xconnect コンフィギュレーション モードを開始します。
ステップ 19	**interworking ethernet** 例： `Device(config-xconnect)# interworking ethernet`	擬似回線のタイプとしてだけでなく、擬似回線上を通過可能なトラフィックのタイプとしてもイーサネットを指定します。

	コマンドまたはアクション	目的
ステップ 20	**member***interface-type-number* 例： `Device(config-xconnect)# member fastethernet 4/0/0.1`	メンバー インターフェイスのロケーションを指定します。
ステップ 21	**member pseudowire***interface-number* 例： `Device(config-xconnect)# member pseudowire 109`	L2VPN クロス コネクトを形成するために、メンバー擬似回線を指定します。
ステップ 22	**no shutdown** 例： `Device(config-xconnect)# no shutdown`	メンバー インターフェイスを再起動します。
ステップ 23	**end** 例： `Device(config-xconnect)# end`	xconnect コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

イーサネット PE デバイス上での HDLC/イーサネット間ブリッジ型インターワーキング（dot1q モードと QinQ モード）

手順の概要

1. イネーブル化
2. **configure terminal**
3. **pseudowire-class** [*pw-class-name*]
4. **encapsulation mpls**
5. **interworking ethernet**
6. **interface***typeslot*/*subslot*/*port* [**.***subinterface*]
7. **encapsulation dot1q***vlan-id***second dot1q***vlan-id*
8. **xconnect***peer-router-idvc id***pseudowire-class** [*pw-class-name*]
9. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**pseudowire-class** [*pw-class-name*] 例： `Device(config)# pseudowire-class pw-iw-ether`	レイヤ 2 擬似回線 クラスの名前を指定し、擬似回線 クラス 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	**encapsulation mpls** 例： `Device(config-pw-class)# encapsulation mpls`	トンネリング カプセル化を MPLS として指定します。
ステップ 5	**interworking ethernet** 例： `Device(config-pw-class)# interworking ethernet`	擬似回線のタイプとしてだけでなく、擬似回線上を通過可能なトラフィックのタイプとしてもイーサネットを指定します。
ステップ 6	**interface***typeslot*/*subslot*/*port* [**.***subinterface*] 例： `Device(config-pw-class)# interface gigabitethernet 4/0/0.1`	ギガビット イーサネット サブインターフェイスを指定し、サブインターフェイス コンフィギュレーション モードを開始します。 • 隣接するイーサネット CE デバイスのサブインターフェイスがこのイーサネット PE デバイスと同じ VLAN 上に存在することを確認します。
ステップ 7	**encapsulation dot1q***vlan-id***second dot1q***vlan-id* 例： `Device(config-subif)# encapsulation dot1q 100 second dot1q 200`	インターフェイスの QinQ 入力フレームを適切なサービス インスタンスにマッピングする一致基準を定義します。

	コマンドまたはアクション	目的
ステップ 8	**xconnect***peer-router-idvc id***pseudowire-class** [*pw-class-name*] 例： `Device(config-subif)# xconnect 198.51.100.2 123 pseudowire-class pw-iw-ether`	レイヤ 2 パケットを転送するための仮想回線（VC）を作成します。
ステップ 9	**end** 例： `Device(config-subif)# end`	サブインターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

L2VPN プロトコルベースの CLI 機能と関連するコマンドを使用する、イーサネット PE デバイスでの HDLC-to-Ethernet ブリッジ型インターワーキング（dot1q モードおよび QinQ モード）

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface***typeslot*/*subslot*/*port* [**.***subinterface*]
4. **encapsulation dot1q***vlan-id***second dot1q***vlan-id*
5. **no ip address**
6. **no shutdown**
7. **exit**
8. **template type pseudowire***name*
9. **encapsulation mpls**
10. **exit**
11. **interface pseudowire***number*
12. **source template type pseudowire***name*
13. **encapsulation mpls**
14. **neighbor***peer-addressvc id-value*
15. **signaling protocol ldp**
16. **no shutdown**
17. **exit**
18. **l2vpn xconnect context***context-name*
19. **interworking ethernet**
20. **member***interface-type-number*
21. **member pseudowire***interface-number*
22. **no shutdown**
23. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# 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***typeslot/subslot/port* [**.***subinterface*] 例： `Device(config)# interface fastethernet 4/0/0.1`	サブインターフェイスを指定し、サブインターフェイス コンフィギュレーション モードを開始します。 • 隣接するイーサネット CE デバイスのサブインターフェイスがこのイーサネット PE デバイスと同じ VLAN 上に存在することを確認します。
ステップ 4	**encapsulation dot1q***vlan-id***second dot1q***vlan-id* 例： `Device(config-subif)# encapsulation dot1q 100 second dot1q 200`	インターフェイスの QinQ 入力フレームを適切なサービス インスタンスにマッピングする一致基準を定義します。
ステップ 5	**no ip address** 例： `Device(config-subif)# no ip address`	IP 処理をディセーブルにします。
ステップ 6	**no shutdown** 例： `Device(config-subif)# no shutdown`	ファスト イーサネットのサブインターフェイスを再起動します。
ステップ 7	**exit** 例： `Device(config-subif)# exit`	サブインターフェイス 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	**template type pseudowire***name* 例： `Device(config)# template type pseudowire temp4`	指定した名前でテンプレート擬似回線を作成し、テンプレート コンフィギュレーション モードを開始します。
ステップ 9	**encapsulation mpls** 例： `Device(config-template)# encapsulation mpls`	トンネリング カプセル化を MPLS として指定します。

	コマンドまたはアクション	目的
ステップ 10	**exit** 例： `Device(config-template)# exit`	テンプレート コンフィギュレーション モードを終了して、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 11	**interface pseudowire***number* 例： `Device(config)# interface pseudowire 109`	指定した値でインターフェイス擬似回線を確立して、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 12	**source template type pseudowire***name* 例： `Device(config-if)# source template type pseudowire temp4`	temp4 という名前のタイプ擬似回線としてソース テンプレートを設定します。
ステップ 13	**encapsulation mpls** 例： `Device(config-if)# encapsulation mpls`	トンネリング カプセル化を MPLS として指定します。
ステップ 14	**neighbor***peer-addressvc id-value* 例： `Device(config-if)# neighbor 10.0.0.15 109`	L2VPN 擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 15	**signaling protocol ldp** 例： `Device(config-if)# signaling protocol ldp`	擬似回線クラス用のラベル配布プロトコル（LDP）が設定されるように指定します。
ステップ 16	**no shutdown** 例： `Device(config-if)# no shutdown`	インターフェイス擬似回線を再起動します。
ステップ 17	**exit** 例： `Device(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 18	**l2vpn xconnect context***context-name* 例： `Device(config)# l2vpn xconnect context con2`	L2VPN クロス コネクト コンテキストを作成して、xconnect 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 19	**interworking ethernet** 例： `Device(config-xconnect)# interworking ethernet`	擬似回線のタイプとしてだけでなく、擬似回線上を通過可能なトラフィックのタイプとしてもイーサネットを指定します。
ステップ 20	**member***interface-type-number* 例： `Device(config-xconnect)# member fastethernet 4/0/0.1`	メンバー インターフェイスのロケーションを指定します。
ステップ 21	**member pseudowire***interface-number* 例： `Device(config-xconnect)# member pseudowire 109`	L2VPN クロス コネクトを形成するために、メンバー擬似回線を指定します。
ステップ 22	**no shutdown** 例： `Device(config-xconnect)# no shutdown`	メンバー インターフェイスを再起動します。
ステップ 23	**end** 例： `Device(config-xconnect)# end`	xconnect コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

HDLC PE デバイス上での HDLC/イーサネット間ルーテッド インターワーキング

手順の概要

1. イネーブル化
2. **configure terminal**
3. **pseudowire-class** [*pw-class-name*]
4. **encapsulation mpls**
5. **interworking ip**
6. **interface***typeslot*/*subslot*/*port* [**.***subinterface*]
7. **noipaddress** [*ip-address mask*] [**secondary**]
8. **xconnect***peer-router-idvc id***pseudowire-class** [*pw-class-name*]
9. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**pseudowire-class** [*pw-class-name*] 例： `Device(config)# pseudowire-class pw-iw-ip`	レイヤ 2 擬似回線 クラスの名前を指定し、擬似回線クラス 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	**encapsulation mpls** 例： `Device(config-pw-class)# encapsulation mpls`	トンネリング カプセル化を MPLS として指定します。
ステップ 5	**interworking ip** 例： `Device(config-pw-class)# interworking ip`	擬似回線のタイプとしてだけでなく、擬似回線上を通過可能なトラフィックのタイプとしても IP を指定します。
ステップ 6	**interface***typeslot*/*subslot*/*port* [**.***subinterface*] 例： `Device(config-pw-class)# interface serial 3/1/0`	シリアル 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 7	**noipaddress** [*ip-address mask*] [**secondary**] 例： `Device(config-if)# no ip address`	IP 処理をディセーブルにします。
ステップ 8	**xconnect***peer-router-idvc id***pseudowire-class** [*pw-class-name*] 例： `Device(config-if)# xconnect 198.51.100.2 123 pseudowire-class pw-iw-ip`	レイヤ 2 パケットを転送するための仮想回線（VC）を作成します。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： `Device(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。

L2VPN プロトコルベースの CLI 機能と関連するコマンドを使用する、HDLC PE デバイスでの HDLC-to-Ethernet ルーテッド インターワーキング

手順の概要

1. イネーブル化
2. **configure terminal**
3. **template type pseudowire***name*
4. **encapsulation mpls**
5. **exit**
6. **interface pseudowire***number*
7. **source template type pseudowire***name*
8. **encapsulation mpls**
9. **neighbor***peer-addressvc id-value*
10. **signaling protocol ldp**
11. **no shutdown**
12. **exit**
13. **l2vpn xconnect context***context-name*
14. **interworking ip**
15. **member***interface-type-number*
16. **member pseudowire***interface-number*
17. **no shutdown**
18. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# 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	**template type pseudowire***name* 例： `Device# template type pseudowire temp5`	指定した名前でテンプレート擬似回線を作成し、テンプレート 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	**encapsulation mpls** 例： `Device(config-template)# encapsulation mpls`	トンネリング カプセル化を MPLS として指定します。
ステップ 5	**exit** 例： `Device(config-template)# exit`	テンプレート コンフィギュレーション モードを終了して、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 6	**interface pseudowire***number* 例： `Device(config)# interface pseudowire 107`	指定した値でインターフェイス擬似回線を確立して、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 7	**source template type pseudowire***name* 例： `Device(config-if)# source template type pseudowire temp5`	temp5 という名前のタイプ擬似回線としてソース テンプレートを設定します。
ステップ 8	**encapsulation mpls** 例： `Device(config-if)# encapsulation mpls`	トンネリング カプセル化を MPLS として指定します。
ステップ 9	**neighbor***peer-addressvc id-value* 例： `Device(config-if)# neighbor 10.0.0.11 107`	L2VPN 擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 10	**signaling protocol ldp** 例： `Device(config-if)# signaling protocol ldp`	擬似回線クラス用のラベル配布プロトコル（LDP）が設定されるように指定します。

	コマンドまたはアクション	目的
ステップ 11	**no shutdown** 例： `Device(config-if)# no shutdown`	インターフェイス擬似回線を再起動します。
ステップ 12	**exit** 例： `Device(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 13	**l2vpn xconnect context***context-name* 例： `Device(config)# l2vpn xconnect context con1`	L2VPN クロス コネクト コンテキストを作成して、xconnect コンフィギュレーション モードを開始します。
ステップ 14	**interworking ip** 例： `Device(config-xconnect)# interworking ip`	擬似回線のタイプとしてだけでなく、擬似回線上を通過可能なトラフィックのタイプとしても IP を指定します。
ステップ 15	**member***interface-type-number* 例： `Device(config-xconnect)# member serial 0/1/0:0`	メンバーインターフェイスのロケーションを指定します。
ステップ 16	**member pseudowire***interface-number* 例： `Device(config-xconnect)# member pseudowire 107`	L2VPN クロス コネクトを形成するために、メンバー擬似回線を指定します。
ステップ 17	**no shutdown** 例： `Device(config-xconnect)# no shutdown`	メンバー インターフェイスを再起動します。
ステップ 18	**end** 例： `Device(config-xconnect)# end`	xconnect コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

イーサネット PE デバイス上での HDLC/イーサネット間ルーテッドインターワーキング（ポート モード）

手順の概要

1. イネーブル化
2. **configure terminal**
3. **pseudowire-class** [*pw-class-name*]
4. **encapsulation mpls**
5. **interworking ip**
6. **interface***typeslot*/*subslot*/*port* [**.***subinterface*]
7. **encapsulation mpls**
8. **xconnect***peer-router-idvc id***pseudowire-class** [*pw-class-name*]
9. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**pseudowire-class** [*pw-class-name*] 例： `Device(config)# pseudowire-class pw-iw-ip`	レイヤ 2 擬似回線 クラスの名前を指定し、擬似回線 クラス 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	**encapsulation mpls** 例： `Device(config-pw-class)# encapsulation mpls`	トンネリング カプセル化を MPLS として指定します。
ステップ 5	**interworking ip** 例： `Device(config-pw-class)# interworking ip`	擬似回線のタイプとしてだけでなく、擬似回線上を通過可能なトラフィックのタイプとしても IP を指定します。

	コマンドまたはアクション	目的
ステップ 6	**interface***typeslot/subslot/port* [**.***subinterface*] 例： `Device(config-pw-class)# interface gigabitethernet 4/0/0.1`	ギガビット イーサネット サブインターフェイスを指定し、サブインターフェイス コンフィギュレーション モードを開始します。 • 隣接するイーサネット CE デバイスのサブインターフェイスがこのイーサネット PE デバイスと同じ VLAN 上に存在することを確認します。
ステップ 7	**encapsulation mpls** 例： `Device(config-subif)# encapsulation mpls`	トンネリング カプセル化を MPLS として指定します。
ステップ 8	**xconnect***peer-router-idvc id***pseudowire-class** [*pw-class-name*] 例： `Device(config-subif)# xconnect 198.51.100.2 123 pseudowire-class pw-iw-ip`	レイヤ 2 パケットを転送するための仮想回線（VC）を作成します。
ステップ 9	**end** 例： `Device(config-subif)# end`	サブインターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

L2VPN プロトコルベースの CLI 機能と関連するコマンドを使用する、イーサネット PE デバイスでの HDLC-to-Ethernet ルーテッド インターワーキング（ポート モード）

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface***typeslot*/*subslot*/*port* [**.***subinterface*]
4. **encapsulation mpls**
5. **no ip address**
6. **no shutdown**
7. **exit**
8. **template type pseudowire***name*
9. **encapsulation mpls**
10. **exit**
11. **interface pseudowire***number*
12. **source template type pseudowire***name*
13. **encapsulation mpls**
14. **neighbor***peer-addressvc id-value*
15. **signaling protocol ldp**
16. **no shutdown**
17. **exit**
18. **l2vpn xconnect context***context-name*
19. **interworking ip**
20. **member***interface-type-number*
21. **member pseudowire***interface-number*
22. **no shutdown**
23. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 3	**interface***typeslot*/*subslot*/*port* [.*subinterface*] 例： `Device(config)# interface fastethernet 4/0/0.1`	ファスト イーサネット サブインターフェイスを指定し、サブインターフェイス コンフィギュレーション モードを開始します。 • 隣接するイーサネットCEデバイスのサブインターフェイスがこのイーサネット PE デバイスと同じ VLAN 上に存在することを確認します。
ステップ 4	**encapsulation mpls** 例： `Device(config-subif)# encapsulation mpls`	トンネリング カプセル化を MPLS として指定します。
ステップ 5	**no ip address** 例： `Device(config-subif)# no ip address`	IP 処理をディセーブルにします。
ステップ 6	**no shutdown** 例： `Device(config-subif)# no shutdown`	ファスト イーサネットのサブインターフェイスを再起動します。
ステップ 7	**exit** 例： `Device(config-subif)# exit`	サブインターフェイス 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	**template type pseudowire***name* 例： `Device(config)# template type pseudowire temp4`	指定した名前でテンプレート擬似回線を作成し、テンプレート コンフィギュレーション モードを開始します。
ステップ 9	**encapsulation mpls** 例： `Device(config-template)# encapsulation mpls`	トンネリング カプセル化を MPLS として指定します。
ステップ 10	**exit** 例： `Device(config-template)# exit`	テンプレート コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 11	**interface pseudowire***number* 例： `Device(config)# interface pseudowire 109`	指定した値でインターフェイス擬似回線を確立して、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 12	**source template type pseudowire***name* 例： `Device(config-if)# source template type pseudowire temp4`	temp4 という名前のタイプ擬似回線としてソース テンプレートを設定します。
ステップ 13	**encapsulation mpls** 例： `Device(config-if)# encapsulation mpls`	トンネリング カプセル化を MPLS として指定します。
ステップ 14	**neighbor***peer-addressvc id-value* 例： `Device(config-if)# neighbor 10.0.0.15 109`	L2VPN 擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 15	**signaling protocol ldp** 例： `Device(config-if)# signaling protocol ldp`	擬似回線クラス用のラベル配布プロトコル（LDP）が設定されるように指定します。
ステップ 16	**no shutdown** 例： `Device(config-if)# no shutdown`	インターフェイス擬似回線を再起動します。
ステップ 17	**exit** 例： `Device(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 18	**l2vpn xconnect context***context-name* 例： `Device(config)# l2vpn xconnect context con2`	L2VPN クロス コネクト コンテキストを作成して、xconnect コンフィギュレーション モードを開始します。
ステップ 19	**interworking ip** 例： `Device(config-xconnect)# interworking ip`	擬似回線のタイプとしてだけでなく、擬似回線上を通過可能なトラフィックのタイプとしても IP を指定します。

	コマンドまたはアクション	目的
ステップ 20	**member***interface-type-number* 例： `Device(config-xconnect)# member fastethernet 4/0/0.1`	メンバー インターフェイスのロケーションを指定します。
ステップ 21	**member pseudowire***interface-number* 例： `Device(config-xconnect)# member pseudowire 109`	L2VPN クロスコネクトを形成するために、メンバー擬似回線を指定します。
ステップ 22	**no shutdown** 例： `Device(config-xconnect)# no shutdown`	メンバー インターフェイスを再起動します。
ステップ 23	**end** 例： `Device(config-xconnect)# end`	xconnect コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

イーサネット PE デバイス上での HDLC/イーサネット間ルーテッド インターワーキング（dot1q モードと QinQ モード）

手順の概要

1. イネーブル化
2. **configure terminal**
3. **pseudowire-class** [*pw-class-name*]
4. **encapsulation mpls**
5. **interworking ip**
6. **interface***typeslot*/*subslot*/*port* [**.***subinterface*]
7. **encapsulation dot1q***vlan-id***second dot1q***vlan-id*
8. **xconnect***peer-router-idvc id***pseudowire-class** [*pw-class-name*]
9. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**pseudowire-class** [*pw-class-name*] 例： `Device(config)# pseudowire-class pw-iw-ip`	レイヤ 2 擬似回線 クラスの名前を指定し、擬似回線 クラス 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	**encapsulation mpls** 例： `Device(config-pw-class)# encapsulation mpls`	トンネリング カプセル化を MPLS として指定します。
ステップ 5	**interworking ip** 例： `Device(config-pw-class)# interworking ip`	擬似回線のタイプとしてだけでなく、擬似回線上を通過可能なトラフィックのタイプとしても IP を指定します。
ステップ 6	**interface***typeslot*/*subslot*/*port* [**.***subinterface*] 例： `Device(config-pw-class)# interface gigabitethernet 4/0/0.1`	ギガビット イーサネット サブインターフェイスを指定し、サブインターフェイス コンフィギュレーション モードを開始します。 • 隣接するイーサネット CE デバイスのサブインターフェイスがこのイーサネット PE デバイスと同じ VLAN 上に存在することを確認します。
ステップ 7	**encapsulation dot1q***vlan-id***second dot1q***vlan-id* 例： `Device(config-subif)# encapsulation dot1q 100 second dot1q 200`	インターフェイスの QinQ 入力フレームを適切なサービス インスタンスにマッピングする一致基準を定義します。

	コマンドまたはアクション	目的
ステップ 8	**xconnect***peer-router-idvc id***pseudowire-class** [*pw-class-name*] 例： `Device(config-subif)# xconnect 198.51.100.2 123 pseudowire-class pw-iw-ip`	レイヤ 2 パケットを転送するための仮想回線（VC）を作成します。
ステップ 9	**end** 例： `Device(config-subif)# end`	サブインターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

L2VPN プロトコルベースの CLI 機能と関連するコマンドを使用する、イーサネット PE デバイスでの HDLC-to-Ethernet ルーテッドインターワーキング（dot1q モードおよび QinQ モード）

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface***typeslot*/*subslot*/*port* [**.***subinterface*]
4. **encapsulation dot1q***vlan-id***second dot1q***vlan-id*
5. **no ip address**
6. **no shutdown**
7. **exit**
8. **template type pseudowire***name*
9. **encapsulation mpls**
10. **exit**
11. **interface pseudowire***number*
12. **source template type pseudowire***name*
13. **encapsulation mpls**
14. **neighbor***peer-addressvc id-value*
15. **signaling protocol ldp**
16. **no shutdown**
17. **exit**
18. **l2vpn xconnect context***context-name*
19. **interworking ip**
20. **member***interface-type-number*
21. **member pseudowire***interface-number*
22. **no shutdown**
23. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# 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***typeslot/subslot/port* [**.***subinterface*] 例： `Device(config)# interface fastethernet 4/0/0.1`	サブインターフェイスを指定し、サブインターフェイス コンフィギュレーション モードを開始します。 • 隣接するイーサネット CE デバイスのサブインターフェイスがこのイーサネット PE デバイスと同じ VLAN 上に存在することを確認します。
ステップ 4	**encapsulation dot1q***vlan-id***second dot1q***vlan-id* 例： `Device(config-subif)# encapsulation dot1q 100 second dot1q 200`	インターフェイスの QinQ 入力フレームを適切なサービス インスタンスにマッピングする一致基準を定義します。
ステップ 5	**no ip address** 例： `Device(config-subif)# no ip address`	IP 処理をディセーブルにします。
ステップ 6	**no shutdown** 例： `Device(config-subif)# no shutdown`	ファスト イーサネットのサブインターフェイスを再起動します。
ステップ 7	**exit** 例： `Device(config-subif)# exit`	サブインターフェイス 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	**template type pseudowire***name* 例： `Device(config)# template type pseudowire temp4`	指定した名前でテンプレート擬似回線を作成し、テンプレート コンフィギュレーション モードを開始します。
ステップ 9	**encapsulation mpls** 例： `Device(config-template)# encapsulation mpls`	トンネリング カプセル化を MPLS として指定します。

	コマンドまたはアクション	目的
ステップ 10	**exit** 例： `Device(config-template)# exit`	テンプレート コンフィギュレーション モードを終了して、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 11	**interface pseudowire***number* 例： `Device(config)# interface pseudowire 109`	指定した値でインターフェイス擬似回線を確立して、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 12	**source template type pseudowire***name* 例： `Device(config-if)# source template type pseudowire temp4`	temp4 という名前のタイプ擬似回線としてソース テンプレートを設定します。
ステップ 13	**encapsulation mpls** 例： `Device(config-if)# encapsulation mpls`	トンネリング カプセル化を MPLS として指定します。
ステップ 14	**neighbor***peer-addressvc id-value* 例： `Device(config-if)# neighbor 10.0.0.15 109`	L2VPN 擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 15	**signaling protocol ldp** 例： `Device(config-if)# signaling protocol ldp`	擬似回線クラス用のラベル配布プロトコル（LDP）が設定されるように指定します。
ステップ 16	**no shutdown** 例： `Device(config-if)# no shutdown`	インターフェイス擬似回線を再起動します。
ステップ 17	**exit** 例： `Device(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 18	**l2vpn xconnect context***context-name* 例： `Device(config)# l2vpn xconnect context con2`	L2VPN クロス コネクト コンテキストを作成して、xconnect 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 19	**interworking ip** 例： `Device(config-xconnect)# interworking ip`	擬似回線のタイプとしてだけでなく、擬似回線上を通過可能なトラフィックのタイプとしても IP を指定します。
ステップ 20	**member***interface-type-number* 例： `Device(config-xconnect)# member fastethernet 4/0/0.1`	メンバー インターフェイスのロケーションを指定します。
ステップ 21	**member pseudowire***interface-number* 例： `Device(config-xconnect)# member pseudowire 109`	L2VPN クロス コネクトを形成するために、メンバー擬似回線を指定します。
ステップ 22	**no shutdown** 例： `Device(config-xconnect)# no shutdown`	メンバー インターフェイスを再起動します。
ステップ 23	**end** 例： `Device(config-xconnect)# end`	xconnect コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

HDLC PE デバイス上での HDLC/イーサネット間インターワーキング（ポート モード）設定の確認

show コマンドを使用して、HDLC プロバイダー エッジ（PE）デバイス上での HDLC/イーサネット間インターワーキング（ポート モード）設定に関する情報を表示できます。

手順の概要

1. **show mpls l2transport vc**
2. **show mpls l2transport vc detail**
3. **show l2vpn atom vc**
4. **show l2vpn atom vc detail**

手順の詳細

ステップ 1 **show mpls l2transport vc**

次に、HDLC PE デバイス上での HDLC/イーサネット間インターワーキング（ポート モード）設定に関する基本情報を表示する **show mpls l2transport vc** コマンドの出力例を示します。

例：

```
Device# show mpls l2transport vc

Local intf  Local circuit  Dest address    VC ID      Status
----------- -------------- --------------- ---------- ----------
Se0/1/0:0   HDLC           10.0.0.1        101        UP
```

ステップ 2 **show mpls l2transport vc detail**

次に、HDLC PE デバイス上での HDLC/イーサネット間インターワーキング（ポート モード）設定に関する詳細情報を表示する **show mpls l2transport vc detail** コマンドの出力例を示します。

例：

```
Device# show mpls l2transport vc detail

Local interface: Se0/1/0:0 up, line protocol up, HDLC up
Interworking type is Ethernet
Destination address: 10.0.0.1, VC ID: 101, VC status: up
Output interface: Fa0/0/1, imposed label stack {20 22}
Preferred path: not configured
Default path: active
Next hop: 10.0.0.10
Create time: 00:00:19, last status change time: 00:00:15
Last label FSM state change time: 00:00:15
Signaling protocol: LDP, peer 10.0.0.1:0 up
Targeted Hello: 203.0.113.1(LDP Id) -> 10.0.0.1, LDP is UP
Graceful restart: configured and enabled
Non stop routing: not configured and not enabled
Status TLV support (local/remote) : enabled/supported
LDP route watch : enabled
Label/status state machine : established, LruRru
Last local dataplane status rcvd: No fault
Last BFD dataplane status rcvd: Not sent
Last BFD peer monitor status rcvd: No fault
Last local AC circuit status rcvd: No fault
Last local AC circuit status sent: No fault
Last local PW i/f circ status rcvd: No fault
Last local LDP TLV status sent: No fault
Last remote LDP TLV status rcvd: No fault
Last remote LDP ADJ status rcvd: No fault
MPLS VC labels: local 33, remote 22
Group ID: local 0, remote 0
MTU: local 1500, remote 1500
Remote interface description: Connect to CE2
Sequencing: receive disabled, send disabled
Control Word: On
SSO Descriptor: 10.0.0.1/101, local label: 33
Dataplane:
SSM segment/switch IDs: 4274/4273 (used), PWID: 26
VC statistics:
transit packet totals: receive 3, send 6
transit byte totals: receive 162, send 366
transit packet drops: receive 0, seq error 0, send 0
```

ステップ 3 **show l2vpn atom vc**

次に、HDLC PE デバイス上での HDLC/イーサネット間インターワーキング（ポート モード）設定に関する基本情報を表示する **show l2vpn atom vc** コマンドの出力例を示します。

例：

```
Device# show l2vpn atom vc

                            Service
Interface Peer ID    VC ID  Type   Name  Status
--------- ---------- ------ ------ ----- ----------
pw101     10.0.0.1   101    p2p    101   UP
```

ステップ 4 **show l2vpn atom vc detail**

次に、HDLC PE デバイス上での HDLC/イーサネット間インターワーキング（ポート モード）設定に関する詳細情報を表示する **show l2vpn atom vc detail** コマンドの出力例を示します。

例：

```
Device# show l2vpn atom vc detail

pseudowire101 is up, VC status is up PW type: Ethernet
Create time: 00:00:18, last status change time: 00:00:14
Last label FSM state change time: 00:00:14
Destination address: 10.0.0.1 VC ID: 101
Output interface: Fa0/0/1, imposed label stack {16 17}
Preferred path: not configured
Default path: active
Next hop: 10.0.0.10
Member of xconnect service hdlc101
Associated member Se0/1/0:0 is up, status is up
Interworking type is Ethernet
Service id: 0xde000002
Signaling protocol: LDP, peer 10.0.0.1:0 up
Targeted Hello: 203.0.113.1(LDP Id) -> 10.0.0.1, LDP is UP
Graceful restart: configured and enabled
Non stop routing: not configured and not enabled
PWid FEC (128), VC ID: 101
Status TLV support (local/remote) : enabled/supported
LDP route watch : enabled
Label/status state machine : established, LruRru
Local dataplane status received : No fault
BFD dataplane status received : Not sent
BFD peer monitor status received : No fault
Status received from access circuit : No fault
Status sent to access circuit : No fault
Status received from pseudowire i/f : No fault
Status sent to network peer : No fault
Status received from network peer : No fault
Adjacency status of remote peer : No fault
Sequencing: receive disabled, send disabled
Bindings
Parameter    Local                           Remote
------------ ------------------------------- -------------------------------
Label        18                              17
Group ID     0                               0
Interface    Connect to CE1                  Connect to CE2
MTU          1500                            1500
Control word on (configured: autosense)      on
PW type      Ethernet                        Ethernet
VCCV CV type 0x02                            0x02
             LSPV [2]                        LSPV [2]
VCCV CC type 0x07                            0x07
             CW [1], RA [2], TTL [3]         CW [1], RA [2], TTL [3]
Status TLV   enabled                         supported
SSO Descriptor: 10.0.0.1/101, local label: 18
Dataplane:
SSM segment/switch IDs: 4106/4105 (used), PWID: 2
Rx Counters
3 input transit packets, 162 bytes
0 drops, 0 seq err
Tx Counters
```

```
5 output transit packets, 305 bytes
0 drops
```

イーサネット PE デバイス上での HDLC/イーサネット間インターワーキング（ポートモード）設定の確認

show コマンドを使用して、イーサネット PE デバイス上での HDLC/イーサネット間インターワーキング（ポート モード）設定に関する情報を表示できます。

手順の概要

1. **show mpls l2transport vc**
2. **show l2vpn atom vc**
3. **show l2vpn atom vc detail**

手順の詳細

ステップ 1 **show mpls l2transport vc**

次に、イーサネット PE デバイス上での HDLC/イーサネット間インターワーキング（ポート モード）設定に関する基本情報を表示する **show mpls l2transport vc** コマンドの出力例を示します。

例：

```
Device# show mpls l2transport vc

Local interface: Gi1/0/0 up, line protocol up, Ethernet up
Destination address: 203.0.113.1, VC ID: 101, VC status: up
Output interface: Fa0/0/1, imposed label stack {19 33}
Preferred path: not configured
Default path: active
Next hop: 10.0.0.11
Create time: 00:00:22, last status change time: 00:00:19
Last label FSM state change time: 00:00:19
Signaling protocol: LDP, peer 203.0.113.1:0 up
Targeted Hello: 10.0.0.1(LDP Id) -> 203.0.113.1, LDP is UP
Graceful restart: configured and enabled
Non stop routing: not configured and not enabled
Status TLV support (local/remote) : enabled/supported
LDP route watch : enabled
Label/status state machine : established, LruRru
Last local dataplane status rcvd: No fault
Last BFD dataplane status rcvd: Not sent
Last BFD peer monitor status rcvd: No fault
Last local AC circuit status rcvd: No fault
Last local AC circuit status sent: No fault
Last local PW i/f circ status rcvd: No fault
Last local LDP TLV status sent: No fault
Last remote LDP TLV status rcvd: No fault
Last remote LDP ADJ status rcvd: No fault
MPLS VC labels: local 22, remote 33
Group ID: local 0, remote 0
MTU: local 1500, remote 1500
Remote interface description: Connect to CE1
Sequencing: receive disabled, send disabled
```

```
Control Word: On
SSO Descriptor: 203.0.113.1/101, local label: 22
Dataplane:
SSM segment/switch IDs: 4574/4573 (used), PWID: 80
VC statistics:
transit packet totals: receive 9, send 5
transit byte totals: receive 315, send 380
transit packet drops: receive 0, seq error 0, send 0
```

ステップ 2 **show l2vpn atom vc**

次に、イーサネット PE デバイス上での HDLC/イーサネット間インターワーキング（ポートモード）設定に関する基本情報を表示する **show l2vpn atom vc** コマンドの出力例を示します。

例：

```
Device# show l2vpn atom vc

                            Service
Interface Peer ID    VC ID  Type   Name  Status
--------- ---------- ------ ------ ----- ----------
pw101     10.0.0.1   101    p2p    101   UP
```

ステップ 3 **show l2vpn atom vc detail**

次に、イーサネット PE デバイス上での HDLC/イーサネット間インターワーキング（ポートモード）設定に関する詳細情報を表示する **show l2vpn atom vc detail** コマンドの出力例を示します。

例：

```
Device# show l2vpn atom vc detail

pseudowire101 is up, VC status is up PW type: Ethernet
Create time: 00:00:18, last status change time: 00:00:14
Last label FSM state change time: 00:00:14
Destination address: 10.0.0.1 VC ID: 101
Output interface: Fa0/0/1, imposed label stack {16 17}
Preferred path: not configured
Default path: active
Next hop: 10.0.0.10
Member of xconnect service eth101
Associated member Se0/1/0:0 is up, status is up
Interworking type is Ethernet
Service id: 0xde000002
Signaling protocol: LDP, peer 10.0.0.1:0 up
Targeted Hello: 203.0.113.1(LDP Id) -> 10.0.0.1, LDP is UP
Graceful restart: configured and enabled
Non stop routing: not configured and not enabled
PWid FEC (128), VC ID: 101
Status TLV support (local/remote) : enabled/supported
LDP route watch : enabled
Label/status state machine : established, LruRru
Local dataplane status received : No fault
BFD dataplane status received : Not sent
BFD peer monitor status received : No fault
Status received from access circuit : No fault
Status sent to access circuit : No fault
Status received from pseudowire i/f : No fault
Status sent to network peer : No fault
Status received from network peer : No fault
Adjacency status of remote peer : No fault
Sequencing: receive disabled, send disabled
Bindings
Parameter    Local                          Remote
------------ ------------------------------ -------------------------------
Label        18                             17
Group ID     0                              0
Interface    Connect to CE1                 Connect to CE2
MTU          1500                           1500
```

```
Control word on (configured: autosense)     on
PW type      Ethernet                       Ethernet
VCCV CV type 0x02                           0x02
             LSPV [2]                       LSPV [2]
VCCV CC type 0x07                           0x07
             CW [1], RA [2], TTL [3]        CW [1], RA [2], TTL [3]
Status TLV   enabled                        supported
SSO Descriptor: 10.0.0.1/101, local label: 18
Dataplane:
SSM segment/switch IDs: 4106/4105 (used), PWID: 2
Rx Counters
3 input transit packets, 162 bytes
0 drops, 0 seq err
Tx Counters
5 output transit packets, 305 bytes
0 drops
```

HDLC PE デバイス上での HDLC/イーサネット間インターワーキング（dot1q モード）設定の確認

show コマンドを使用して、HDLC PE デバイス上での HDLC/イーサネット間インターワーキング（dot1q モード）設定に関する情報を表示できます。

手順の概要

1. **show mpls l2transport vc**
2. **show mpls l2transport vc detail**
3. **show l2vpn atom vc**
4. **show l2vpn atom vc detail**

手順の詳細

ステップ 1 **show mpls l2transport vc**

次に、HDLC PE デバイス上での HDLC/イーサネット間インターワーキング（dot1q モード）設定に関する基本情報を表示する **show mpls l2transport vc** コマンドの出力例を示します。

例：

```
Device# show mpls l2transport vc

Local intf  Local circuit  Dest address    VC ID      Status
----------- -------------- --------------- ---------- ----------
Se0/1/0:0   HDLC           10.0.0.1       101        UP
```

ステップ 2 **show mpls l2transport vc detail**

次に、HDLC PE デバイス上での HDLC/イーサネット間インターワーキング（dot1q モード）設定に関する詳細情報を表示する **show mpls l2transport vc detail** コマンドの出力例を示します。

例：

```
Device# show mpls l2transport vc detail
```

```
Local interface: Se0/1/0:0 up, line protocol up, HDLC up
Interworking type is Ethernet
Destination address: 10.0.0.1, VC ID: 101, VC status: up
Output interface: Fa0/0/1, imposed label stack {20 22}
Preferred path: not configured
Default path: active
Next hop: 10.0.0.10
Create time: 00:00:19, last status change time: 00:00:15
Last label FSM state change time: 00:00:15
Signaling protocol: LDP, peer 10.0.0.1:0 up
Targeted Hello: 203.0.113.1(LDP Id) -> 10.0.0.1, LDP is UP
Graceful restart: configured and enabled
Non stop routing: not configured and not enabled
Status TLV support (local/remote) : enabled/supported
LDP route watch : enabled
Label/status state machine : established, LruRru
Last local dataplane status rcvd: No fault
Last BFD dataplane status rcvd: Not sent
Last BFD peer monitor status rcvd: No fault
Last local AC circuit status rcvd: No fault
Last local AC circuit status sent: No fault
Last local PW i/f circ status rcvd: No fault
Last local LDP TLV status sent: No fault
Last remote LDP TLV status rcvd: No fault
Last remote LDP ADJ status rcvd: No fault
MPLS VC labels: local 33, remote 22
Group ID: local 0, remote 0
MTU: local 1500, remote 1500
Remote interface description: Connect to CE2
Sequencing: receive disabled, send disabled
Control Word: On
SSO Descriptor: 10.0.0.1/101, local label: 33
Dataplane:
SSM segment/switch IDs: 4274/4273 (used), PWID: 26
VC statistics:
transit packet totals: receive 3, send 6
transit byte totals: receive 162, send 366
transit packet drops: receive 0, seq error 0, send 0
```

ステップ 3 **show l2vpn atom vc**

次に、HDLC PE デバイス上での HDLC/イーサネット間インターワーキング（dot1q モード）設定に関する基本情報を表示する **show l2vpn atom vc** コマンドの出力例を示します。

例：

```
Device# show l2vpn atom vc

                            Service
Interface Peer ID    VC ID  Type   Name  Status
--------- ---------- ------ ------ ----- ----------
pw101     10.0.0.1  101    p2p    101   UP
```

ステップ 4 **show l2vpn atom vc detail**

次に、HDLC PE デバイス上での HDLC/イーサネット間インターワーキング（dot1q モード）設定に関する詳細情報を表示する **show l2vpn atom vc detail** コマンドの出力例を示します。

例：

```
Device# show l2vpn atom vc detail

pseudowire101 is up, VC status is up PW type: Ethernet
Create time: 00:00:18, last status change time: 00:00:14
Last label FSM state change time: 00:00:14
Destination address: 10.0.0.1 VC ID: 101
Output interface: Fa0/0/1, imposed label stack {16 17}
Preferred path: not configured
Default path: active
```

```
Next hop: 10.0.0.10
Member of xconnect service hdlc101
Associated member Se0/1/0:0 is up, status is up
Interworking type is Ethernet
Service id: 0xde000002
Signaling protocol: LDP, peer 10.0.0.1:0 up
Targeted Hello: 203.0.113.1(LDP Id) -> 10.0.0.1, LDP is UP
Graceful restart: configured and enabled
Non stop routing: not configured and not enabled
PWid FEC (128), VC ID: 101
Status TLV support (local/remote) : enabled/supported
LDP route watch : enabled
Label/status state machine : established, LruRru
Local dataplane status received : No fault
BFD dataplane status received : Not sent
BFD peer monitor status received : No fault
Status received from access circuit : No fault
Status sent to access circuit : No fault
Status received from pseudowire i/f : No fault
Status sent to network peer : No fault
Status received from network peer : No fault
Adjacency status of remote peer : No fault
Sequencing: receive disabled, send disabled
Bindings
Parameter    Local                           Remote
------------ ------------------------------- -------------------------------
Label        18                              17
Group ID     0                               0
Interface    Connect to CE1                  Connect to CE2
MTU          1500                            1500
Control word on (configured: autosense)      on
PW type      Ethernet                        Ethernet
VCCV CV type 0x02                            0x02
             LSPV [2]                        LSPV [2]
VCCV CC type 0x07                            0x07
             CW [1], RA [2], TTL [3]         CW [1], RA [2], TTL [3]
Status TLV   enabled                         supported
SSO Descriptor: 10.0.0.1/101, local label: 18
Dataplane:
SSM segment/switch IDs: 4106/4105 (used), PWID: 2
Rx Counters
3 input transit packets, 162 bytes
0 drops, 0 seq err
Tx Counters
5 output transit packets, 305 bytes
0 drops
```

イーサネット PE デバイス上での HDLC/イーサネット間インターワーキング（dot1q モード）設定の確認

show コマンドを使用して、イーサネット PE デバイス上での HDLC/イーサネット間インターワーキング（dot1q モード）設定に関する情報を表示できます。

手順の概要

1. **show mpls l2transport vc**
2. **show mpls l2transport vc detail**
3. **show l2vpn atom vc**
4. **show l2vpn atom vc detail**

手順の詳細

ステップ 1 **show mpls l2transport vc**

次に、イーサネット PE デバイス上での HDLC/イーサネット間インターワーキング（dot1q モード）設定に関する基本情報を表示する **show mpls l2transport vc** コマンドの出力例を示します。

例：

```
Device# show mpls l2transport vc

Local intf  Local circuit  Dest address    VC ID      Status
----------- -------------- --------------- ---------- ----------
Gi1/0/0.10  Eth VLAN 10    203.0.113.1     138        UP
```

ステップ 2 **show mpls l2transport vc detail**

次に、イーサネット PE デバイス上での HDLC/イーサネット間インターワーキング（dot1q モード）設定に関する詳細情報を表示する **show mpls l2transport vc detail** コマンドの出力例を示します。

例：

```
Device# show mpls l2transport vc detail

Local interface: Gi1/0/0.10 up, line protocol up, Eth VLAN 10 up
Interworking type is Ethernet
Destination address: 203.0.113.1, VC ID: 138, VC status: up
Output interface: Fa0/0/1, imposed label stack {19 35}
Preferred path: not configured
Default path: active
Next hop: 10.0.0.11
Create time: 00:00:22, last status change time: 00:00:20
Last label FSM state change time: 00:00:20
Signaling protocol: LDP, peer 203.0.113.1:0 up
Targeted Hello: 10.0.0.1(LDP Id) -> 203.0.113.1, LDP is UP
Graceful restart: configured and enabled
Non stop routing: not configured and not enabled
Status TLV support (local/remote) : enabled/supported
LDP route watch : enabled
Label/status state machine : established, LruRru
Last local dataplane status rcvd: No fault
Last BFD dataplane status rcvd: Not sent
Last BFD peer monitor status rcvd: No fault
Last local AC circuit status rcvd: No fault
Last local AC circuit status sent: No fault
Last local PW i/f circ status rcvd: No fault
Last local LDP TLV status sent: No fault
Last remote LDP TLV status rcvd: No fault
Last remote LDP ADJ status rcvd: No fault
MPLS VC labels: local 53, remote 35
Group ID: local 0, remote 0
MTU: local 1500, remote 1500
Remote interface description: Connect to CE1
Sequencing: receive disabled, send disabled
Control Word: On
SSO Descriptor: 203.0.113.1/138, local label: 53
Dataplane:
SSM segment/switch IDs: 4784/4783 (used), PWID: 117
VC statistics:
transit packet totals: receive 6, send 6
transit byte totals: receive 234, send 1276
transit packet drops: receive 0, seq error 0, send 0
```

ステップ 3 **show l2vpn atom vc**

次に、イーサネット PE デバイス上での HDLC/イーサネット間インターワーキング（dot1q モード）設定に関する基本情報を表示する **show l2vpn atom vc** コマンドの出力例を示します。

例：

```
Device# show l2vpn atom vc

                            Service
Interface Peer ID    VC ID  Type   Name  Status
--------- ---------- ------ ------ ----- ----------
pw138     203.0.113.1 138    p2p    138   UP
```

ステップ 4 **show l2vpn atom vc detail**

次に、イーサネット PE デバイス上での HDLC/イーサネット間インターワーキング（dot1q モード）設定に関する詳細情報を表示する **show l2vpn atom vc detail** コマンドの出力例を示します。

例：

```
Device# show l2vpn atom vc detail

pseudowire138 is up, VC status is up PW type: Ethernet
Create time: 00:00:23, last status change time: 00:00:20
Last label FSM state change time: 00:00:20
Destination address: 203.0.113.1 VC ID: 138
Output interface: Fa0/0/1, imposed label stack {18 20}
Preferred path: not configured
Default path: active
Next hop: 10.0.0.11
Member of xconnect service eth138
Associated member Gi1/0/0.10 is up, status is up
Interworking type is Ethernet
Service id: 0x7b000029
Signaling protocol: LDP, peer 203.0.113.1:0 up
Targeted Hello: 10.0.0.1(LDP Id) -> 203.0.113.1, LDP is UP
Graceful restart: configured and enabled
Non stop routing: not configured and not enabled
PWid FEC (128), VC ID: 138
Status TLV support (local/remote) : enabled/supported
LDP route watch : enabled
Label/status state machine : established, LruRru
Local dataplane status received : No fault
BFD dataplane status received : Not sent
BFD peer monitor status received : No fault
Status received from access circuit : No fault
Status sent to access circuit : No fault
Status received from pseudowire i/f : No fault
Status sent to network peer : No fault
Status received from network peer : No fault
Adjacency status of remote peer : No fault
Sequencing: receive disabled, send disabled
Bindings
Parameter    Local                          Remote
------------ ------------------------------ -------------------------------
Label        30                             20
Group ID     0                              0
Interface    Connect to CE2                 Connect to CE1
MTU          1500                           1500
Control word on (configured: autosense)     on
PW type      Ethernet                       Ethernet
VCCV CV type 0x02                           0x02
             LSPV [2]                       LSPV [2]
VCCV CC type 0x07                           0x07
             CW [1], RA [2], TTL [3]        CW [1], RA [2], TTL [3]
Status TLV   enabled                        supported
SSO Descriptor: 203.0.113.1/138, local label: 30
Dataplane:
SSM segment/switch IDs: 4333/4332 (used), PWID: 41
Rx Counters
8 input transit packets, 312 bytes
0 drops, 0 seq err
Tx Counters
```

```
5 output transit packets, 380 bytes
0 drops
```

HDLC PE デバイス上での HDLC/イーサネット間インターワーキング（QinQ モード）設定の確認

show コマンドを使用して、HDLC PE デバイス上での HDLC/イーサネット間インターワーキング（QinQ モード）設定に関する情報を表示できます。

手順の概要

1. **show mpls l2transport vc**
2. **show mpls l2transport vc detail**
3. **show l2vpn atom vc**
4. **show l2vpn atom vc detail**

手順の詳細

ステップ 1 **show mpls l2transport vc**

次に、HDLC PE デバイス上での HDLC/イーサネット間インターワーキング（QinQ モード）設定に関する基本情報を表示する **show mpls l2transport vc** コマンドの出力例を示します。

例：

```
Device# show mpls l2transport vc

Local intf  Local circuit  Dest address    VC ID      Status
----------- -------------- --------------- ---------- ----------
Se0/1/0:0   HDLC           10.0.0.1        145        UP
```

ステップ 2 **show mpls l2transport vc detail**

次に、HDLC PE デバイス上での HDLC/イーサネット間インターワーキング（QinQ モード）設定に関する詳細情報を表示する **show mpls l2transport vc detail** コマンドの出力例を示します。

例：

```
Device# show mpls l2transport vc detail

Local interface: Se0/1/0:0 up, line protocol up, HDLC up
Interworking type is Ethernet
Destination address: 10.0.0.1, VC ID: 101, VC status: up
Output interface: Fa0/0/1, imposed label stack {20 22}
Preferred path: not configured
Default path: active
Next hop: 10.0.0.10
Create time: 00:00:19, last status change time: 00:00:15
Last label FSM state change time: 00:00:15
Signaling protocol: LDP, peer 10.0.0.1:0 up
Targeted Hello: 203.0.113.1(LDP Id) -> 10.0.0.1, LDP is UP
Graceful restart: configured and enabled
Non stop routing: not configured and not enabled
Status TLV support (local/remote) : enabled/supported
```

```
LDP route watch : enabled
Label/status state machine : established, LruRru
Last local dataplane status rcvd: No fault
Last BFD dataplane status rcvd: Not sent
Last BFD peer monitor status rcvd: No fault
Last local AC circuit status rcvd: No fault
Last local AC circuit status sent: No fault
Last local PW i/f circ status rcvd: No fault
Last local LDP TLV status sent: No fault
Last remote LDP TLV status rcvd: No fault
Last remote LDP ADJ status rcvd: No fault
MPLS VC labels: local 33, remote 22
Group ID: local 0, remote 0
MTU: local 1500, remote 1500
Remote interface description: Connect to CE2
Sequencing: receive disabled, send disabled
Control Word: On
SSO Descriptor: 10.0.0.1/101, local label: 33
Dataplane:
SSM segment/switch IDs: 4274/4273 (used), PWID: 26
VC statistics:
transit packet totals: receive 3, send 6
transit byte totals: receive 162, send 366
transit packet drops: receive 0, seq error 0, send 0
```

ステップ 3 **show l2vpn atom vc**

次に、HDLC PE デバイス上での HDLC/イーサネット間インターワーキング（QinQ モード）設定に関する基本情報を表示する **show l2vpn atom vc** コマンドの出力例を示します。

例：

```
Device# show l2vpn atom vc

                            Service
Interface Peer ID    VC ID  Type   Name  Status
--------- ---------- ------ ------ ----- ----------
pw145     10.0.0.1   145    p2p    145   UP
```

ステップ 4 **show l2vpn atom vc detail**

次に、HDLC PE デバイス上での HDLC/イーサネット間インターワーキング（QinQ モード）設定に関する詳細情報を表示する **show l2vpn atom vc detail** コマンドの出力例を示します。

例：

```
Device# show l2vpn atom vc detail

pseudowire145 is up, VC status is up PW type: Ethernet
Create time: 00:00:18, last status change time: 00:00:13
Last label FSM state change time: 00:00:13
Destination address: 10.0.0.1 VC ID: 145
Output interface: Fa0/0/1, imposed label stack {16 33}
Preferred path: not configured
Default path: active
Next hop: 10.0.0.10
Member of xconnect service hdlc145
Associated member Se0/1/0:0 is up, status is up
Interworking type is Ethernet
Service id: 0x2e
Signaling protocol: LDP, peer 10.0.0.1:0 up
Targeted Hello: 203.0.113.1(LDP Id) -> 10.0.0.1, LDP is UP
Graceful restart: configured and enabled
Non stop routing: not configured and not enabled
PWid FEC (128), VC ID: 145
Status TLV support (local/remote) : enabled/supported
LDP route watch : enabled
Label/status state machine : established, LruRru
Local dataplane status received : No fault
```

```
BFD dataplane status received : Not sent
BFD peer monitor status received : No fault
Status received from access circuit : No fault
Status sent to access circuit : No fault
Status received from pseudowire i/f : No fault
Status sent to network peer : No fault
Status received from network peer : No fault
Adjacency status of remote peer : No fault
Sequencing: receive disabled, send disabled
Bindings
Parameter    Local                          Remote
------------ ------------------------------ ------------------------------
Label        33                             33
Group ID     0                              0
Interface    Connect to CE1                 Connect to CE2
MTU          1500                           1500
Control word on (configured: autosense)     on
PW type      Ethernet                       Ethernet
VCCV CV type 0x02                           0x02
             LSPV [2]                       LSPV [2]
VCCV CC type 0x07                           0x07
             CW [1], RA [2], TTL [3]        CW [1], RA [2], TTL [3]
Status TLV   enabled                        supported
SSO Descriptor: 10.0.0.1/145, local label: 33
Dataplane:
SSM segment/switch IDs: 4345/4344 (used), PWID: 48
Rx Counters
2 input transit packets, 108 bytes
0 drops, 0 seq err
Tx Counters
3 output transit packets, 183 bytes
0 drops
```

イーサネット PE デバイス上での HDLC/イーサネット間インターワーキング（QinQ モード）設定の確認

show コマンドを使用して、イーサネット PE デバイス上での HDLC/イーサネット間インターワーキング（QinQ モード）設定に関する情報を表示できます。

手順の概要

1. **show mpls l2transport vc**
2. **show mpls l2transport vc detail**
3. **show l2vpn atom vc**
4. **show l2vpn atom vc detail**

手順の詳細

ステップ 1 **show mpls l2transport vc**

次に、イーサネット PE デバイス上での HDLC/イーサネット間インターワーキング（QinQ モード）設定に関する基本情報を表示する **show mpls l2transport vc** コマンドの出力例を示します。

例：

```
Device# show mpls l2transport vc

Local intf  Local circuit  Dest address    VC ID      Status
----------- -------------- --------------- ---------- ----------
Gi1/0/0.10  Eth VLAN 10/20  203.0.113.1    145        UP
```

ステップ 2 **show mpls l2transport vc detail**

次に、イーサネット PE デバイス上での HDLC/イーサネット間インターワーキング（QinQ モード）設定に関する詳細情報を表示する **show mpls l2transport vc detail** コマンドの出力例を示します。

例：

```
Device# show mpls l2transport vc detail

Local interface: Gi1/0/0.10 up, line protocol up, Eth VLAN 10/20 up
Interworking type is Ethernet
Destination address: 203.0.113.1, VC ID: 145, VC status: up
Output interface: Fa0/0/1, imposed label stack {19 27}
Preferred path: not configured
Default path: active
Next hop: 10.0.0.11
Create time: 00:00:23, last status change time: 00:00:21
Last label FSM state change time: 00:00:21
Signaling protocol: LDP, peer 203.0.113.1:0 up
Targeted Hello: 10.0.0.1(LDP Id) -> 203.0.113.1, LDP is UP
Graceful restart: configured and enabled
Non stop routing: not configured and not enabled
Status TLV support (local/remote) : enabled/supported
LDP route watch : enabled
Label/status state machine : established, LruRru
Last local dataplane status rcvd: No fault
Last BFD dataplane status rcvd: Not sent
Last BFD peer monitor status rcvd: No fault
Last local AC circuit status rcvd: No fault
Last local AC circuit status sent: No fault
Last local PW i/f circ status rcvd: No fault
Last local LDP TLV status sent: No fault
Last remote LDP TLV status rcvd: No fault
Last remote LDP ADJ status rcvd: No fault
MPLS VC labels: local 25, remote 27
Group ID: local 0, remote 0
MTU: local 1500, remote 1500
Remote interface description: Connect to CE1
Sequencing: receive disabled, send disabled
Control Word: On
SSO Descriptor: 203.0.113.1/145, local label: 25
Dataplane:
SSM segment/switch IDs: 4815/4814 (used), PWID: 124
VC statistics:
transit packet totals: receive 10, send 6
transit byte totals: receive 430, send 456
transit packet drops: receive 0, seq error 0, send 0
```

ステップ 3 **show l2vpn atom vc**

次に、イーサネット PE デバイス上での HDLC/イーサネット間インターワーキング（QinQ モード）設定に関する基本情報を表示する **show l2vpn atom vc** コマンドの出力例を示します。

例：

```
Device# show l2vpn atom vc

                            Service
Interface Peer ID    VC ID  Type   Name  Status
```

```
--------- ---------- ------ ------ ----- ----------
pw145     203.0.113.1  145    p2p    145   UP
```

ステップ 4 **show l2vpn atom vc detail**

次に、イーサネット PE デバイス上での HDLC/イーサネット間インターワーキング（QinQ モード）設定に関する詳細情報を表示する **show l2vpn atom vc detail** コマンドの出力例を示します。

例：

```
Device# show l2vpn atom vc detail

pseudowire145 is up, VC status is up PW type: Ethernet
Create time: 00:00:23, last status change time: 00:00:19
Last label FSM state change time: 00:00:19
Destination address: 203.0.113.1 VC ID: 145
Output interface: Fa0/0/1, imposed label stack {18 33}
Preferred path: not configured
Default path: active
Next hop: 10.0.0.11
Member of xconnect service eth145
Associated member Gi1/0/0.10 is up, status is up
Interworking type is Ethernet
Service id: 0xed000030
Signaling protocol: LDP, peer 203.0.113.1:0 up
Targeted Hello: 10.0.0.1(LDP Id) -> 203.0.113.1, LDP is UP
Graceful restart: configured and enabled
Non stop routing: not configured and not enabled
PWid FEC (128), VC ID: 145
Status TLV support (local/remote) : enabled/supported
LDP route watch : enabled
Label/status state machine : established, LruRru
Local dataplane status received : No fault
BFD dataplane status received : Not sent
BFD peer monitor status received : No fault
Status received from access circuit : No fault
Status sent to access circuit : No fault
Status received from pseudowire i/f : No fault
Status sent to network peer : No fault
Status received from network peer : No fault
Adjacency status of remote peer : No fault
Sequencing: receive disabled, send disabled
Bindings
Parameter    Local                           Remote
------------ ------------------------------- ------------------------------
Label        33                              33
Group ID     0                               0
Interface    Connect to CE2                  Connect to CE1
MTU          1500                            1500
Control word on (configured: autosense)      on
PW type      Ethernet                        Ethernet
VCCV CV type 0x02                            0x02
             LSPV [2]                        LSPV [2]
VCCV CC type 0x07                            0x07
             CW [1], RA [2], TTL [3]         CW [1], RA [2], TTL [3]
Status TLV   enabled                         supported
SSO Descriptor: 203.0.113.1/145, local label: 33
Dataplane:
SSM segment/switch IDs: 4361/4360 (used), PWID: 48
Rx Counters
8 input transit packets, 344 bytes
0 drops, 0 seq err
Tx Counters
5 output transit packets, 380 bytes
0 drops
```

L2VPN インターワーキングの確認

L2VPN ステータス（AToM 設定）を確認するには、次のコマンドを使用します。

- **showconnection**[**all** | **name** | **id** | **elements** | **port**]
- **showxconnect**[**all** | **interface** | **peer**]
- **showmplsl2transport**[**binding** | **checkpoint** | **hw-capability** | **summary** | **vc**]
- **showmplsinfrastructurelfdpseudowirevcid**

L2VPN インターワーキングの確認（L2VPN プロトコルベースの CLI 機能に関連するコマンドを使用）

L2VPN ステータス（AToM 設定）を確認するには、次のコマンドを使用します。

- **showconnection**[**all** | **name** | **id** | **elements** | **port**]
- **showl2vpnservice**[**all** | **interface** | **peer**]
- **showl2vpnatom**[**binding** | **checkpoint** | **hw-capability** | **summary** | **vc**]
- **showmplsinfrastructurelfdpseudowirevcid**

L2VPN インターワーキングの設定例

ブリッジ型インターワーキングを使用した Frame Relay DLCI-to-Ethernet VLAN 802.1Q の例

次に、ブリッジ型インターワーキングを使用して Frame Relay DLCI-to-Ethernet VLAN 802.1Q 機能を設定する例を示します。

PE1 ルータ	PE2 ルータ

`config t`
`mpls label protocol ldp`
`interface Loopback100`
`  ip address 10.0.0.100 255.255.255.255`
`pseudowire-class fr-vlan`
`  encapsulation mpls`
`  interworking ethernet`
`frame-relay switching`
`interface serial 2/0/0:1`
`  encapsulation frame-relay`
`  frame-relay intf-type dce`
`connect mpls serial 2/0/0:1 567 l2transport`
 	
`  xconnect 10.0.0.200 150 pw-class fr-vlan`
	`config t`
	`mpls label protocol ldp`
	`interface Loopback200`
	`  ip address 10.0.0.200 255.255.255.255`
	`pseudowire-class fr-vlan`
	`  encapsulation mpls`
	`  interworking ethernet`
	`interface gigabitethernet 5/1/0.3`
	`  encapsulation dot1q 1525`
	
	`  xconnect 10.0.0.100 150 pw-class fr-vlan`

ブリッジ型インターワーキングを使用した Frame Relay DLCI-to-Ethernet VLAN 802.1Q の例（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

次に、ブリッジ型インターワーキングを使用して Frame Relay DLCI-to-Ethernet VLAN 802.1Q 機能を設定する例を示します。

PE1 ルータ	PE2 ルータ

`config t`
`mpls label protocol ldp`
`interface Loopback100`
`  ip address 10.0.0.100 255.255.255.255`
`template type pseudowire fr-vlan`
`  encapsulation mpls`
`  interworking ethernet`
`frame-relay switching`
`interface serial 2/0/0:1`
`  encapsulation frame-relay`
`  frame-relay intf-type dce`
`connect mpls serial 2/0/0:1 567 l2transport`
 	
`  interface pseudowire 100`
`  source template type pseudowire fr-vlan`
`  neighbor 10.0.0.200 150`
`!`
`l2vpn xconnect context con1`
`  member pseudowire 100`
`  member 10.0.0.200 150 encapsulation mpls`
	`config t`
	`mpls label protocol ldp`
	`interface Loopback200`
	`  ip address 10.0.0.200 255.255.255.255`
	`template type pseudowire fr-vlan`
	`  encapsulation mpls`
	`  interworking ethernet`
	`interface gigabitethernet 5/1/0.3`
	`  encapsulation dot1q 1525`
	
	`  interface pseudowire 100`
	`  source template type pseudowire fr-vlan`
	`  neighbor 10.0.0.100 150`
	`!`
	`l2vpn xconnect context con1`
	`  member pseudowire 100`
	`  member 10.0.0.100 150 encapsulation mpls`

ブリッジ型インターワーキングを使用した ATM AAL5-to-Ethernet VLAN 802.1Q の例

次に、ブリッジ型インターワーキングを使用した ATM AAL5-to-Ethernet VLAN 802.1Q 機能を設定する例を示します。

PE1 ルータ	PE2 ルータ

`config t`
`mpls label protocol ldp`
`interface Loopback100`
`  ip address 10.0.0.100 255.255.255.255`
`pseudowire-class atm-vlan`
`  encapsulation mpls`
`  interworking ethernet`
`interface atm 2/0/0`
`  pvc 0/200 l2transport`
`  encapsulation aal5snap`
 	
`  xconnect 10.0.0.200 140 pw-class atm-vlan`
	`config t`
	`mpls label protocol ldp`
	`interface Loopback200`
	`  ip address 10.0.0.200 255.255.255.255`
	`pseudowire-class atm-vlan`
	`  encapsulation mpls`
	`  interworking ethernet`
	`interface gigabitethernet 5/1/0.3`
	`  encapsulation dot1q 1525`
	
	`  xconnect 10.0.0.100 140 pw-class atm-vlan`

ブリッジ型インターワーキングを使用した ATM AAL5-to-Ethernet VLAN 802.1Q の例（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

次に、ブリッジ型インターワーキングを使用した ATM AAL5-to-Ethernet VLAN 802.1Q 機能を設定する例を示します。

PE1 ルータ	PE2 ルータ

`config t`
`mpls label protocol ldp`
`interface Loopback100`
` ip address 10.0.0.100 255.255.255.255`
`template type pseudowire atm-vlan`
` encapsulation mpls`
` interworking ethernet`
`interface atm 2/0/0`
` pvc 0/200 l2transport`
` encapsulation aal5snap`
 	
`interface pseudowire 100`
` source template type pseudowire atm-vlan`
` neighbor 10.0.0.200 140`
`!`
`l2vpn xconnect context con1`
` member pseudowire 100`
` member 10.0.0.200 140 encapsulation mpls`
	`config t`
	`mpls label protocol ldp`
	`interface Loopback200`
	` ip address 10.0.0.200 255.255.255.255`
	`template type pseudowire atm-vlan`
	` encapsulation mpls`
	` interworking ethernet`
	`interface gigabitethernet 5/1/0.3`
	` encapsulation dot1q 1525`
	
	` interface pseudowire 100`
	` source template type pseudowire atm-vlan`
	` neighbor 10.0.0.100 140`
	`!`
	`l2vpn xconnect context con1`
	` member pseudowire 100`
	` member 10.0.0.200 140 encapsulation mpls`

ルーテッド インターワーキングを使用した ATM AAL5-to-Ethernet Port の例

次に、ルーテッド インターワーキングを使用した ATM AAL5-to-Ethernet Port 機能を設定する例を示します。

PE1 ルータ	PE2 ルータ

`config t`
`mpls label protocol ldp`
`interface Loopback100`
` ip address 10.0.0.100 255.255.255.255`
`pseudowire-class atm-eth`
` encapsulation mpls`
` interworking ip`
`interface atm 2/0.1`
` pvc 0/200 l2transport`
` encapsulation aal5`
 	
` xconnect 10.0.0.200 140 pw-class atm-eth`
	`config t`
	`mpls label protocol ldp`
	`interface Loopback200`
	` ip address 10.0.0.200 255.255.255.255`
	`pseudowire-class atm-eth`
	` encapsulation mpls`
	` interworking ip`
	`interface gigabitethernet 5/1/0`
	
	` xconnect 10.0.0.100 140 pw-class atm-eth`

ルーテッドインターワーキングを使用した Frame Relay DLCI-to-Ethernet Port の例

次に、ルーテッド インターワーキングを使用して Frame Relay DLCI-to-Ethernet Port 機能を設定する例を示します。

PE1 ルータ	PE2 ルータ

`config t`
`mpls label protocol ldp`
`interface Loopback100`
` ip address 10.0.0.100 255.255.255.255`
`pseudowire-class fr-eth`
` encapsulation mpls`
` interworking ip`
`frame-relay switching`
`interface serial 2/0/0:1`
` encapsulation frame-relay`
` frame-relay intf-type dce`
` frame-relay interface-dlci 567 switched`
`connect fr-vlan-1 POS2/3/1 151 l2transport`
 	
` xconnect 10.0.0.200 151 pw-class`
`pw-class-bridge`
	`config t`
	`mpls label protocol ldp`
	`interface Loopback200`
	` ip address 10.0.0.200 255.255.255.255`
	`pseudowire-class fr-eth`
	` encapsulation mpls`
	` interworking ip`
	`interface gigabitethernet 5/1/0`
	
	` xconnect 10.0.0.100 150 pw-class fr-eth`

ルーテッドインターワーキングを使用した Frame Relay DLCI-to-Ethernet Port の例（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

次に、ルーテッド インターワーキングを使用して Frame Relay DLCI-to-Ethernet Port 機能を設定する例を示します。

PE1 ルータ	PE2 ルータ

`config t`
`mpls label protocol ldp`
`interface Loopback100`
`  ip address 10.0.0.100 255.255.255.255`
`template type pseudowire fr-eth`
`  encapsulation mpls`
`  interworking ip`
`frame-relay switching`
`interface serial 2/0/0:1`
`  encapsulation frame-relay`
`  frame-relay intf-type dce`
`  frame-relay interface-dlci 567 switched`
`connect fr-vlan-1 POS2/3/1 151 l2transport`
 	
`  interface pseudowire 100`
`  source template type pseudowire fr-eth`
`  neighbor 10.0.0.200 140`
`!`
`l2vpn xconnect context con1`
`  member pseudowire 100`
`  member 10.0.0.200 140 encapsulation mpls`
	`config t`
	`mpls label protocol ldp`
	`interface Loopback200`
	`  ip address 10.0.0.200 255.255.255.255`
	`template type pseudowire fr-eth`
	`  encapsulation mpls`
	`  interworking ip`
	`interface gigabitethernet 5/1/0`
	
	`  interface pseudowire 100`
	`  source template type pseudowire fr-eth`
	`  neighbor 10.0.0.200 140`
	`!`
	`l2vpn xconnect context con1`
	`  member pseudowire 100`
	`  member 10.0.0.200 140 encapsulation mpls`

Ethernet-to-VLAN over AToM（ブリッジ型）の例

次に、PE ルータで Ethernet VLAN-to-PPP over AToM を設定する例を示します。

PE1 ルータ	PE2 ルータ
ip cef ! mpls label protocol ldp mpls ldp router-id Loopback0 force ! pseudowire-class atom encapsulation mpls ! interface Loopback0 ip address 10.9.9.9 255.255.255.255 ! interface FastEthernet0/0 no ip address ! interface FastEthernet1/0 xconnect 10.8.8.8 123 pw-class atom	ip cef ! mpls label protocol ldp mpls ldp router-id Loopback0 force ! pseudowire-class atom-eth-iw encapsulation mpls interworking ethernet ! interface Loopback0 ip address 10.8.8.8 255.255.255.255 ! interface FastEthernet1/0.1 encapsulation dot1q 100 xconnect 10.9.9.9 123 pw-class atom-eth-iw

Ethernet-to-VLANoverAToM（ブリッジ型）の例（L2VPNプロトコルベース CLI 機能に関連するコマンドを使用）

次の例は、Ethernet to VLAN over AToM の設定を示しています。

PE1	PE2
ip cef ! mpls label protocol ldp mpls ldp router-id Loopback0 force ! template type pseudowire atom-eth-iw encapsulation mpls interworking ethernet ! interface Loopback0 ip address 10.8.8.8 255.255.255.255 ! interface FastEthernet1/0.1 encapsulation dot1q 100 interface pseudowire 100 source template type pseudowire atom-eth-iw neighbor 10.8.8.8 123 ! l2vpn xconnect context con1 member pseudowire 100 member 10.8.8.8 123 encapsulation mpls	ip cef ! mpls label protocol ldp mpls ldp router-id Loopback0 force ! template type pseudowire atom encapsulation mpls ! interface Loopback0 ip address 10.9.9.9 255.255.255.255 ! interface FastEthernet0/0 no ip address ! interface FastEthernet1/0 interface pseudowire 100 source template type pseudowire ether-pw neighbor 10.9.9.9 123 ! l2vpn xconnect context con1 member pseudowire 100 member 10.9.9.9 123 encapsulation mpls

VLAN-to-ATM AAL5 over AToM（ブリッジ型）の例

次の例は、VLAN-to-ATM AAL5 over AToM の設定を示しています。

PE1 ルータ	PE2 ルータ
ip cef ! mpls ip mpls label protocol ldp mpls ldp router-id Loopback0 ! pseudowire-class inter-ether encapsulation mpls interworking ethernet ! interface Loopback0 ip address 10.8.8.8 255.255.255.255 ! interface ATM1/0.1 point-to-point pvc 0/100 l2transport encapsulation aal5snap xconnect 10.9.9.9 123 pw-class inter-ether ! interface FastEthernet1/0 xconnect 10.9.9.9 1 pw-class inter-ether ! router ospf 10 log-adjacency-changes network 10.8.8.8 0.0.0.0 area 0 network 10.1.1.1 0.0.0.0 area 0	ip cef ! mpls ip mpls label protocol ldp mpls ldp router-id Loopback0 ! pseudowire-class inter-ether encapsulation mpls interworking ethernet ! interface Loopback0 ip address 10.9.9.9 255.255.255.255 ! interface FastEthernet0/0 no ip address ! interface FastEthernet0/0.1 encapsulation dot1Q 10 xconnect 10.8.8.8 123 pw-class inter-ether ! router ospf 10 log-adjacency-changes network 10.9.9.9 0.0.0.0 area 0 network 10.1.1.2 0.0.0.0 area 0

VLAN-to-ATM AAL5 over AToM（ブリッジ型）の例（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

次の例は、VLAN-to-ATM AAL5 over AToM の設定を示しています。

PE1 ルータ	PE2 ルータ
	ip cef ! mpls ip mpls label protocol ldp mpls ldp router-id Loopback0 ! template type pseudowire inter-ether encapsulation mpls interworking ethernet ! interface Loopback0 ip address 10.9.9.9 255.255.255.255 ! interface FastEthernet0/0 no ip address ! interface FastEthernet0/0.1 encapsulation dot1Q 10 interface pseudowire 100 source template type pseudowire inter-ether neighbor 10.8.8.8 123 ! l2vpn xconnect context con1 member pseudowire 100 member 10.8.8.8 123 encapsulation mpls ! router ospf 10 log-adjacency-changes network 10.9.9.9 0.0.0.0 area 0 network 10.1.1.2 0.0.0.0 area 0

PE1 ルータ	PE2 ルータ
ip cef ! mpls ip mpls label protocol ldp mpls ldp router-id Loopback0 ! template type pseudowire inter-ether encapsulation mpls interworking ethernet ! interface Loopback0 ip address 10.8.8.8 255.255.255.255 ! interface ATM1/0.1 point-to-point pvc 0/100 l2transport encapsulation aal5snap interface pseudowire 100 source template type pseudowire inter-ether neighbor 10.9.9.9 123 ! l2vpn xconnect context con1 ! interface FastEthernet1/0 interface pseudowire 100 source template type pseudowire inter-ether neighbor 10.9.9.9 1 ! l2vpn xconnect context con1 member pseudowire 100 member 10.9.9.9.9 1 encapsulation mpls ! router ospf 10 log-adjacency-changes network 10.8.8.8 0.0.0.0 area 0	

PE1 ルータ	PE2 ルータ
network 10.1.1.1 0.0.0.0 area 0	

Ethernet VLAN-to-PPP over AToM（ルーテッド）の例

次の例は、Ethernet VLAN-to-PPP over AToM の設定を示しています。

PE1 ルータ	PE2 ルータ
configure terminal mpls label protocol ldp mpls ldp router-id Loopback0 mpls ip ! pseudowire-class ppp-ether encapsulation mpls interworking ip ! interface Loopback0 ip address 10.8.8.8 255.255.255.255 no shutdown ! interface POS2/0/1 no ip address encapsulation ppp no peer default ip address ppp ipcp address proxy 10.10.10.1 xconnect 10.9.9.9 300 pw-class ppp-ether no shutdown	configure terminal mpls label protocol ldp mpls ldp router-id Loopback0 mpls ip ! pseudowire-class ppp-ether encapsulation mpls interworking ip ! interface Loopback0 ip address 10.9.9.9 255.255.255.255 no shutdown ! interface GigabitEthernet6/2 xconnect 10.8.8.8 300 pw-class ppp-ether no shutdown

Ethernet VLAN-to-PPP over AToM（ルートテッド）の例（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

次の例は、Ethernet VLAN to PPP over AToM の設定を示しています。

PE1	PE2

`configure terminal`
`mpls label protocol ldp`
`mpls ldp router-id Loopback0`
`mpls ip`
`!`
`template type pseudowire ppp-ether`
` encapsulation mpls`
` interworking ip`
`!`
`interface Loopback0`
` ip address 10.8.8.8 255.255.255.255`
` no shutdown`
`!`
`interface POS2/0/1`
` no ip address`
` encapsulation ppp`
` no peer default ip address`
` ppp ipcp address proxy 10.10.10.1`
`interface pseudowire 100`
 	
`source template type pseudowire ppp-ether`
`neighbor 10.9.9.9 300`
`!`
`l2vpn xconnect context con1`
` member pseudowire 100`
` member 10.9.9.9 300 encapsulation mpls`
` no shutdown`	

PE1	PE2
	configure terminal mpls label protocol ldp mpls ldp router-id Loopback0 mpls ip ! template type pseudowire ppp-ether encapsulation mpls interworking ip ! interface Loopback0 ip address 10.9.9.9 255.255.255.255 no shutdown ! interface vlan300 mtu 4470 no ip address interface pseudowire 100 source template type pseudowire ppp-ether neighbor 10.8.8.8 300 ! l2vpn xconnect context con1 member pseudowire 100 member 10.8.8.8 300 encapsulation mpls no shutdown ! interface GigabitEthernet6/2 switchport switchport trunk encapsulation dot1q switchport trunk allowed vlan 300 switchport mode trunk no shutdown

ATM VC-to-VC ローカル スイッチング（異なるポート）の例

次の例は、ATM VC-to-VC ローカル スイッチングの設定を示しています。

CE1 ルータ	CE2 ルータ	PE router
interface ATM1/0 no ip address atm clock INTERNAL no atm ilmi-keepalive no atm enable-ilmi-trap interface ATM1/0 ip address 10.1.1.1 255.255.255.0 no atm enable-ilmi-trap pvc 0/100 encapsulation aal5snap	interface ATM3/0 no ip address atm clock INTERNAL no atm ilmi-keepalive no atm enable-ilmi-trap ! interface ATM3/0.1 multipoint ip address 10.1.1.2 255.255.255.0 no atm enable-ilmi-trap pvc 0/50 protocol ip 10.1.1.1 encapsulation aal5snap	interface ATM0/1/0 no ip address atm clock INTERNAL no atm enable-ilmi-trap ! interface ATM0/1/0.50 point-to-point no atm enable-ilmi-trap pvc 0/50 l2transport encapsulation aal5 ! ! interface ATM0/1/1 no ip address atm clock INTERNAL no atm enable-ilmi-trap ! interface ATM0/1/1.100 point-to-point no atm enable-ilmi-trap pvc 0/100 l2transport encapsulation aal5 connect con_atm ATM0/1/1 0/100 ATM0/1/0 0/50

ATM VP-to-VP ローカル スイッチング（異なるポート）の例

次の例は、ATM VP-to-VP ローカル スイッチングの設定を示しています。

CE1 ルータ	CE2 ルータ	PE router
interface ATM1/0 no ip address atm clock INTERNAL no atm enable-ilmi-trap ! interface ATM1/0.1 point-to-point ip address 10.1.1.1 255.255.255.0 no atm enable-ilmi-trap pvc 100/100 encapsulation aal5snap	interface ATM3/0 no ip address atm clock INTERNAL no atm ilmi-keepalive no atm enable-ilmi-trap ! interface ATM3/0.1 point-to-point ip address 10.1.1.2 255.255.255.0 no atm enable-ilmi-trap pvc 100/100 encapsulation aal5snap	interface ATM0/1/0 no ip address atm clock INTERNAL no atm ilmi-keepalive no atm enable-ilmi-trap ! interface ATM0/1/0.50 multipoint atm pvp 100 l2transport no atm enable-ilmi-trap ! interface ATM0/1/1 no ip address atm clock INTERNAL no atm ilmi-keepalive no atm enable-ilmi-trap ! interface ATM0/1/1.100 multipoint atm pvp 100 l2transport no atm enable-ilmi-trap connect atm_con ATM0/1/1 100 ATM0/1/0 100

例：HDLC-to-Ethernet インターワーキングの設定：HDLC デバイスのコントローラ スロット

次に、HDLC デバイスのシリアル コントローラとインターフェイスを設定する例を示します。

HDLC CE デバイス	HDLC PE デバイス

`enable`
` configure terminal`
`  controller E1 2/0`
`  channel-group 0 timeslots 1`
`  no shutdown`
`!`
`interface serial 2/0:0`
` no shutdown`
`end`
	`enable`
	` configure terminal`
	`  controller E1 0/1/0`
	`  channel-group 0 timeslots 1`
	`  no shutdown`
	`!`
	`interface serial 0/1/0:0`
	` no shutdown`
	`end`

例：HDLC デバイスでの HDLC-to-Ethernet ブリッジ型インターワーキングの設定

次に、HDLC デバイスで HDLC-to-Ethernet ブリッジ型インターワーキングを設定する例を示します。

HDLC CE デバイス	HDLC PE デバイス

`enable`
` configure terminal`
`  bridge irb`
`  bridge 1 protocol ieee`
`  bridge 1 route ip`
`!`
`interface BVI1`
` ip address 192.0.2.1 255.255.255.0`
` no shutdown`
`!`
`interface serial 2/0:0`
` encapsulation hdlc`
` bridge-group 1`
` no shutdown`
`end`
	`enable`
	` configure terminal`
	`  pseudowire-class pw-iw-eth`
	`  encapsulation mpls`
	`  interworking Ethernet`
	`!`
	`interface serial 0/1/0:0`
	` encapsulation hdlc`
	` no ip address`
	` xconnect 203.0.113.10 100 pw-class pw-iw-eth`
	
	` no shutdown`
	`end`

例：L2VPN プロトコルベースの CLI 機能と関連するコマンドを使用する、HDLC デバイスでの HDLC-to-Ethernet ブリッジ型インターワーキングの設定

次の例は、L2VPN プロトコルベースの CLI 機能と関連するコマンドを使用する、HDLC デバイスでの HDLC-to-Ethernet ブリッジ型インターワーキングの設定方法を示しています。

HDLC CE デバイス	HDLC PE デバイス

`enable`
` configure terminal`
`  bridge irb`
`  bridge 1 protocol ieee`
`  bridge 1 route ip`
`!`
`interface BVI1`
` ip address 192.0.2.1 255.255.255.0`
` no shutdown`
`!`
`interface serial 2/0:0`
` encapsulation hdlc`
` bridge-group 1`
` no shutdown`
`end`
	`enable`
	` configure terminal`
	`  interface serial 0/1/0:0`
	`  encapsulation hdlc`
	`  no ip address`
	`  no shutdown`
	`!`
	`interface pseudowire 101`
	` encapsulation mpls`
	` neighbor 203.0.113.10 100`
	` signaling protocol ldp`
	` no shutdown`
	`!`
	`l2vpn xconnect context hdlc`
	` interworking ethernet`
	` member Serial 0/1/0:0`
	` member pseudowire 101`
	` no shutdown`
	`end`

例：イーサネット デバイスでの HDLC-to-Ethernet ブリッジ型インターワーキングの設定

次に、イーサネット デバイスで HDLC-to-Ethernet ブリッジ型インターワーキングを設定する例を示します。

イーサネット CE デバイス	イーサネット PE デバイス

`enable`
` configure terminal`
`  interface GigabitEthernet0/1`
`  ip address 198.51.100.19 255.255.255.0`
`  ip irdp`
`  ip irdp maxadvertinterval 4`
`  no shutdown`
`end`
	`enable`
	` configure terminal`
	` pseudowire-class pw-iw-eth`
	`  encapsulation mpls`
	`  interworking Ethernet`
	`!`
	`interface GigabitEthernet 1/0/0`
	` no ip address`
	` xconnect 203.0.113.20 100 pseudowire-class`
	` pw-iw-eth`
	`  no shutdown`
	`end`

例：L2VPN プロトコルベースの CLI 機能と関連するコマンドを使用する、イーサネット デバイスでの HDLC-to-Ethernet ブリッジ型インターワーキングの設定

次の例は、L2VPN プロトコルベースの CLI 機能と関連するコマンドを使用する、イーサネット デバイスでの HDLC-to-Ethernet ブリッジ型インターワーキングの設定方法を示しています。

イーサネット CE デバイス	イーサネット PE デバイス

`enable`
`configure terminal`
`interface GigabitEthernet 0/1`
` ip address 198.51.100.19 255.255.255.0`
` ip irdp`
` ip irdp maxadvertinterval 4`
` no shutdown`
`end`
	`enable`
	`configure terminal`
	`interface GigabitEthernet 1/0/0`
	` no ip address`
	` no shutdown`
	`!`
	`interface pseudowire 101`
	` encapsulation mpls`
	` neighbor 203.0.113.20 100`
	` signaling protocol ldp`
	` no shutdown`
	`!`
	`l2vpn xconnect context eth`
	` interworking ethernet`
	` member GigabitEthernet 1/0/0`
	` member pseudowire101`
	` no shutdown`
	`end`

例：イーサネットデバイスでのHDLC-to-VLANブリッジ型インターワーキング（ポート モード）の設定

次に、イーサネットデバイスでHDLC-to-VLANブリッジ型インターワーキング（ポートモード）を設定する例を示します。

イーサネット CE デバイス	イーサネット PE デバイス

`enable`
` configure terminal`
`  interface GigabitEthernet 0/1`
`  no ip address`
`  no shutdown`
`!`
`interface GigabitEthernet 0/1.10`
` encapsulation dot1q 10`
` ip address 198.51.100.19 255.255.255.0`
` ip irdp`
` ip irdp maxadvertinterval 4`
` no shutdown`
`end`
	`enable`
	` configure terminal`
	`  pseudowire-class pw-iw-eth`
	`  encapsulation mpls`
	`  interworking Ethernet`
	`!`
	`interface GigabitEthernet 1/0/0`
	` no ip address`
	` no shutdown`
	`!`
	`interface GigabitEthernet 1/0/0.10`
	` encapsulation dot1Q 10`
	` no ip address`
	`!`
	` xconnect 203.0.113.20 100 pseudowire-class`
	` pw-iw-eth`
	`  no shutdown`
	`end`

例：L2VPN プロトコルベースの CLI 機能と関連するコマンドを使用する、イーサネットデバイスでのHDLC-to-VLANブリッジ型インターワーキングの設定

次の例は、L2VPN プロトコルベースの CLI 機能と関連するコマンドを使用する、イーサネットデバイスでの HDLC-to-VLAN ブリッジ型インターワーキングの設定方法を示しています。

イーサネット CE デバイス	イーサネット PE デバイス

`enable`
` configure terminal`
`  interface GigabitEthernet 0/1`
`  no ip address`
`  no shutdown`
`!`
`interface GigabitEthernet 0/1.10`
` encapsulation dot1q 10`
` ip address 198.51.100.19 255.255.255.0`
` ip irdp`
` ip irdp maxadvertinterval 4`
` no shutdown`
`end`
	`enable`
	` configure terminal`
	`  interface GigabitEthernet 1/0/0`
	`  no ip address`
	`  no shutdown`
	`!`
	`interface GigabitEthernet 1/0/0.10`
	` encapsulation dot1q 10`
	` no ip addres`
	` no shutdown`
	`!`
	`interface pseudowire 101`
	` encapsulation mpls`
	` neighbor 203.0.113.20 100`
	` signaling protocol ldp`
	` no shutdown`
	`!`
	`l2vpn xconnect context vlan`
	` interworking ethernet`
	` member GigabitEthernet 1/0/0.10`
	` member pseudowire 101`
	` no shutdown`
	`end`

例：L2VPN プロトコルベースの CLI 機能と関連するコマンドを使用する、HDLC-to-VLAN ブリッジ型インターワーキング（dot1q モード）の設定

次の例は、L2VPN プロトコルベースの CLI 機能と関連するコマンドを使用する、HDLC-to-VLAN ブリッジ型インターワーキング（dot1q モード）の設定方法を示しています。

HDLC PE デバイス	イーサネット PE デバイス

`enable`
` configure terminal`
`  template type pseudowire hdlc-vlan1`
`  encapsulation mpls`
`!`
`interface pseudowire 107`
` source template type pseudowire hdlc-vlan1`
`  encapsulation mpls`
`  neighbor 203.0.113.10 107`
`  signaling protocol ldp`
`  no shutdown`
`!`
`l2vpn xconnect context hdlc-vlan1-con`
` interworking ethernet`
` member Serial 0/2/0:3`
` member pseudowire 107`
` no shutdown`
`end`
	`enable`
	` configure terminal`
	`  interface FastEthernet 0/0/0.16`
	`  encapsulation dot1q 16`
	`  no ip addres`
	`  no shutdown`
	`!`
	`template type pseudowire hdlc-vlan1`
	` encapsulation mpls`
	`!`
	`interface pseudowire 107`
	` source template type pseudowire hdlc-vlan1`
	`  encapsulation mpls`
	`  neighbor 203.0.113.20 107`
	`  signaling protocol ldp`
	`  no shutdown`
	`!`
	`l2vpn xconnect context hdlc-vlan1-con`
	` interworking ethernet`
	` member FastEthernet 0/0/0.16`
	` member pseudowire 107`
	` no shutdown`
	`end`

例：イーサネットデバイスでのHDLC-to-VLANブリッジ型インターワーキング（QinQ モード）の設定

次に、イーサネット デバイスで HDLC-to-VLAN ブリッジ型インターワーキング（QinQ モード）を設定する例を示します。

イーサネット CE デバイス	イーサネット PE デバイス

`enable`
` configure terminal`
`  interface GigabitEthernet 0/1`
`  no ip address`
`  no shutdown`
`!`
`interface GigabitEthernet 0/1.10`
` encapsulation dot1q 10 second-dot1q 20`
` ip address 198.51.100.19 255.255.255.0`
` ip irdp`
` ip irdp maxadvertinterval 4`
` no shutdown`
`end`
	`enable`
	` configure terminal`
	`  pseudowire-class pw-iw-eth`
	`  encapsulation mpls`
	`  interworking Ethernet`
	`!`
	`interface GigabitEthernet 1/0/0`
	` no ip address`
	` no shutdown`
	`!`
	`interface GigabitEthernet 1/0/0.10`
	` encapsulation dot1Q 10 second-dot1q 20`
	` no ip address`
	` xconnect 203.0.113.20 100 pseudowire-class`
	` pw-iw-eth`
	`  no shutdown`
	`end`

例：L2VPN プロトコルベースの CLI 機能と関連するコマンドを使用する、イーサネットデバイスでのHDLC-to-VLANブリッジ型インターワーキング（QinQ モード）の設定

次の例は、L2VPN プロトコルベースの CLI 機能と関連するコマンドを使用する、イーサネットデバイスでの HDLC-to-VLAN ブリッジ型インターワーキング（QinQ モード）の設定方法を示しています。

イーサネット CE デバイス	イーサネット PE デバイス

`enable`
` configure terminal`
`  interface GigabitEthernet 0/1`
`  no ip address`
`  no shutdown`
`!`
`interface GigabitEthernet 0/1.10`
` encapsulation dot1q 10 second-dot1q 20`
` ip address 198.51.100.19 255.255.255.0`
` ip irdp`
` ip irdp maxadvertinterval 4`
` no shutdown`
`end`
	`enable`
	` configure terminal`
	`  interface GigabitEthernet 1/0/0`
	`  no ip address`
	`  no shutdown`
	`!`
	`interface GigabitEthernet 1/0/0.10`
	` encapsulation dot1q 10 second-dot1q 20`
	` no ip address`
	` no shutdown`
	`!`
	`interface pseudowire 101`
	` encapsulation mpls`
	` neighbor 203.0.113.20 100`
	` signaling protocol ldp`
	` no shutdown`
	`!`
	`l2vpn xconnect context qinq`
	` interworking ethernet`
	` member GigabitEthernet 1/0/0.10`
	` member pseudowire 101`
	` no shutdown`
	`end`

L2VPN インターワーキングに関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
MPLS コマンド	『Multiprotocol Label Switching Command Reference』
Any Transport over MPLS	Any Transport over MPLS

標準および RFC

標準/RFC	Title
draft-ietf-l2tpext-l2tp-base-03.txt	『*Layer Two Tunneling Protocol (Version 3) 'L2TPv3'*』
draft-martini-l2circuit-trans-mpls-09.txt	『*Transport of Layer 2 Frames Over MPLS*』
draft-ietf-pwe3-frame-relay-03.txt.	『*Encapsulation Methods for Transport of Frame Relay over MPLS Networks*』
draft-martini-l2circuit-encap-mpls-04.txt.	『*Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks*』
draft-ietf-pwe3-ethernet-encap-08.txt.	『*Encapsulation Methods for Transport of Ethernet over MPLS Networks*』
draft-ietf-pwe3-hdlc-ppp-encap-mpls-03.txt.	『*Encapsulation Methods for Transport of PPP/HDLC over MPLS Networks*』
draft-ietf-ppvpn-l2vpn-00.txt.	『*An Architecture for L2VPNs*』
RFC 4618	『Encapsulation Methods for Transport of PPP/High-Level Data Link Control (HDLC) over MPLS Networks』

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB の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 リリース、およびフィーチャ セットに関する MIB を探して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

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。サービス契約が有効で、ログイン ID またはパスワードを取得していない場合は、Cisco.com でまず登録手続きを行ってください。	http://www.cisco.com/en/US/support/index.html

L2VPN インターワーキングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、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。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *13*：*L2VPN* インターワーキングの機能情報

機能名	リリース	機能情報
L2VPN インターワーキング	Cisco IOS XE Release 2.4 Cisco IOS XE Release 3.3S	この機能により、異種 AC どうしを接続できます。インターワーキング機能によって、異なるレイヤ 2 カプセル化間の変換が容易になります。 次のコマンドが導入または変更されました：**debug frame-relay pseudowire**、**debug ssm**、**interworking**、**mtu**、**pseudowire-class**、**show l2tun session**、**show l2tun tunnel**、**show mpls l2transport vc**、**show platform**。

機能名	リリース	機能情報
L2VPN インターワーキング：Ethernet to VLAN インターワーキング	Cisco IOS XE Release 2.4	この機能は、VLAN タグを削除し、リモート エンドでこれらをタグなしフレームとして送信することで、インターワーキングを実現します。
L2VPN インターワーキング：Ethernet VLAN to Frame Relay	Cisco IOS XE Release 3.3S	この機能では、イーサネット VLAN とフレーム リレー DLCI のインターワーキングが可能になります。 次のコマンドが変更されました：**interworking**。
L2VPN インターワーキング：Ethernet VLAN to PPP	Cisco IOS XE Release 3.3S	L2VPN インターワーキング：Ethernet VLAN-to-PPP 機能により、異種 AC どうしを接続できます。インターワーキング機能によって、次に示すレイヤ 2 カプセル化間の変換が容易になります。
L2VPN インターワーキング：Frame Relay to ATM（ブリッジモード）	Cisco IOS XE Release 3.6S	この機能により、ブリッジモードおよびルート モードのカプセル化を使用した Frame Relay to ATM インターワーキングが可能になります。

機能名	リリース	機能情報
L2VPN インターワーキング：HDLC to Ethernet インターワーキング	Cisco IOS XE Release 3.13S	ハイレベル データ リンク制御（HDLC）およびイーサネットは、Any Transport over MPLS（AToM）フレームワークを使用して相互に通信する 2 つの独立したデータリンク層トランスポート プロトコルです。このインターワーキング機能は、マルチプロトコル ラベル スイッチング（MPLS）バックボーン上での 2 つの異種レイヤ 2 カプセル化間の変換を可能にします。 この機能は、Cisco IOS XE Release 3.13S で Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 この機能で導入される新しいコマンドまたは変更されたコマンドはありません。

第 5 章

L2VPN 擬似回線優先転送

L2VPN：擬似回線優先転送機能により、**ping** コマンドと **show** コマンドを使用して、スイッチオーバーの前後または実行中に擬似回線のステータス情報を特定できるように、擬似回線を設定できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース 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、機能情報の表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シスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

L2VPN：擬似回線優先転送の前提条件

- L2VPN：擬似回線優先転送を設定するには、次のドキュメントで説明する概念について理解しておく必要があります。
  - 優先転送ステータスのビット定義（draft-ietf-pwe3-redundancy-bit-xx.txt）
  - *MPLS* 擬似回線ステータス シグナリング
  - *L2VPN* 擬似回線冗長性
  - 『*NSF/SSO--Any Transport over MPLS and AToM Graceful Restart*』
  - *MPLS LSP Ping/Traceroute for LDP/TE* および *LSP Ping for VCCV*
- PE ルータは、次の機能を使用して設定する必要があります。
  - *L2VPN* 擬似回線冗長性
  - *NSF/SSO--Any Transport over MPLS and AToM Graceful Restart*
- L2VPN：擬似回線優先転送機能では、ネットワーク内の障害を検出できるように、次のメカニズムが存在している必要があります。
  - ラベル スイッチド パス（*LSP*）*Ping/Traceroute* および *Any Transport over MPLS Virtual Circuit Connection Verification*（*AToM VCCV*）
  - ローカル管理インターフェイス（*LMI*）
  - 運用管理および保守（*OAM*）

L2VPN：擬似回線優先転送のガイドラインおよび制限

- ATM 接続回線だけがサポートされています。
- 次の機能はサポートされていません。
  - ポート モード セル リレー
  - Any Transport over MPLS：AAL5 over MPLS
  - VC セル パッキング
  - OAM エミュレーション
  - ILMI/PVC-D
  - 相手先固定接続（PVC）の範囲
  - L2TPv3 擬似回線の冗長性
  - ローカル スイッチング

- 複数のバックアップ擬似回線
- 静的擬似回線

L2VPN 擬似回線優先転送に関する情報

L2VPN：擬似回線優先転送の概要

L2VPN：擬似回線優先転送機能では、**ping**、**traceroute**、および **show** コマンドを使用してスイッチオーバーの前後および実行中のステータス情報を確認できるように、擬似回線を設定できます。この機能の実装は、優先転送ステータスのビット定義（draft-ietf-pwe3-redundancy-bit-xx.txt）に基づきます。L2VPN：擬似回線優先転送機能は、擬似回線に関する情報を表示するための次の機能拡張を提供します。

- バックアップ擬似回線で **pingmpls** コマンドを発行できます。
- **showxconnect** および **showmplsl2transportvc** コマンドを使用して、スイッチオーバーの前後および実行中の擬似回線ステータスを表示できます。

（注） 単一セグメント擬似回線では、擬似回線の各終端にある PE ルータがターミネーション ポイントの役割を果たします。複数セグメント擬似回線では、終端 PE ルータがターミネーション ポイントの役割を果たします。

L2VPN の概要：L2VPN プロトコルベースの CLI 機能に関連するコマンドを使用した擬似回線優先転送

L2VPN：擬似回線優先転送機能では、**ping**、**traceroute**、および **show** コマンドを使用してスイッチオーバーの前後および実行中のステータス情報を確認できるように、擬似回線を設定できます。この機能の実装は、優先転送ステータスのビット定義（draft-ietf-pwe3-redundancy-bit-xx.txt）に基づきます。L2VPN：擬似回線優先転送機能は、擬似回線に関する情報を表示するための次の機能拡張を提供します。

- バックアップ擬似回線で **pingmpls** コマンドを発行できます。
- **showl2vpn service** および **showl2vpnatomvc** コマンドを使用して、スイッチオーバーの前後および実行中の擬似回線ステータスを表示できます。

（注） 単一セグメント擬似回線では、擬似回線の各終端にある PE ルータがターミネーション ポイントの役割を果たします。複数セグメント擬似回線では、終端 PE ルータがターミネーション ポイントの役割を果たします。

L2VPN の設定方法：擬似回線優先転送

PE ルータ間の擬似回線接続の設定

PE ルータ間でレイヤ 2 フレームを送信するようにルータ間の擬似回線と呼ばれる接続をセットアップします。

擬似回線設定の一環として、**statusredundancymaster** コマンドを発行して、マスターにします。これにより、L2VPN：擬似回線優先転送機能でアクティブ擬似回線とバックアップ擬似回線のステータスを表示できるようになります。デフォルトで、PE ルータはスレーブ モードになります。

（注） 1 つの擬似回線をマスターにして、他の回線をスレーブにする必要があります。両方の擬似回線を同時にマスターまたはスレーブとして設定することはできません。

（注） AToM VC が正常に動作するためには、擬似回線クラスの一部として **encapsulation mpls** コマンドを指定する必要があります。**encapsulation mpls** コマンドを省略すると、「% Incomplete command」というエラーが表示されます。

はじめる前に

PE ルータは、L2VPN 擬似回線冗長性機能と NSF/SSO--Any Transport over MPLS および AToM グレースフル リスタート機能用に設定する必要があります。設定手順については、次のドキュメントを参照してください。

- *L2VPN* 擬似回線冗長性
- 『*NSF/SSO--Any Transport over MPLS and AToM Graceful Restart*』

手順の概要

1. **configureterminal**
2. **pseudowire-classname**
3. **encapsulationmpls**
4. **statusredundancy** {**master**| **slave**}
5. **interworking** {**ethernet** | **ip**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `switch# 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 2	**pseudowire-classname** 例： `switch(config)# pseudowire-class atom`	指定した名前の擬似回線クラスを確立して、擬似回線クラス コンフィギュレーション モードを開始します。
ステップ 3	**encapsulationmpls** 例： `switch(config-pw)# encapsulation mpls`	トンネリング カプセル化を指定します。 • AToM の場合、カプセル化タイプは mpls です。
ステップ 4	**statusredundancy {master| slave}** 例： `switch(config-pw)# status redundancy master`	擬似回線をマスターまたはスレーブとして設定します。これにより、L2VPN：擬似回線優先転送機能でアクティブ擬似回線とバックアップ擬似回線のステータスを表示できるようになります。 • デフォルトで、PE ルータはスレーブ モードになります。 （注） 1 つの擬似回線をマスターにして、他の回線をスレーブにする必要があります。両方の擬似回線を同時にマスターまたはスレーブとして設定することはできません。
ステップ 5	**interworking {ethernet | ip}** 例： `switch(config-pw)# interworking ip`	（任意）異なるレイヤ 2 カプセル化の間の変換をイネーブルにします。

PE ルータ間の擬似回線接続の設定

PE ルータ間でレイヤ 2 フレームを送信するようにルータ間の擬似回線と呼ばれる接続をセットアップします。

擬似回線設定の一環として、**statusredundancymaster** コマンドを発行して、マスターにします。これにより、L2VPN：擬似回線優先転送機能でアクティブ擬似回線とバックアップ擬似回線のステータスを表示できるようになります。デフォルトで、PE ルータはスレーブ モードになります。

（注） 1 つの擬似回線をマスターにして、他の回線をスレーブにする必要があります。両方の擬似回線を同時にマスターまたはスレーブとして設定することはできません。

（注） AToM VC が正常に動作するためには、擬似回線クラスの一部として **encapsulation mpls** コマンドを指定する必要があります。**encapsulation mpls** コマンドを省略すると、「% Incomplete command」というエラーが表示されます。

はじめる前に

PE ルータは、L2VPN 擬似回線冗長性機能と NSF/SSO--Any Transport over MPLS および AToM グレースフル リスタート機能用に設定する必要があります。設定手順については、次のドキュメントを参照してください。

- *L2VPN* 擬似回線冗長性
- 『*NSF/SSO--Any Transport over MPLS and AToM Graceful Restart*』

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacepseudowire***number*
4. **encapsulationmpls**
5. **neighbor***peer-address vcid-value*
6. **statusredundancy** {**master**| **slave**}
7. **interworking** {**ethernet** | **ip**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# 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	**interfacepseudowire***number* 例： `Device(config)# interface pseudowire 1`	指定した値でインターフェイス擬似回線を確立して、擬似回線クラス 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	**encapsulationmpls** 例： `Device(config-pw)# encapsulation mpls`	トンネリング カプセル化を指定します。 • AToM の場合、カプセル化タイプは mpls です。
ステップ 5	**neighbor***peer-address vcid-value* 例： `Router(config-pw)# neighbor 10.0.0.1 123`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 6	**statusredundancy** {**master**| **slave**} 例： `Device(config-pw)# status redundancy master`	擬似回線をマスターまたはスレーブとして設定します。これにより、L2VPN：擬似回線優先転送機能でアクティブ擬似回線とバックアップ擬似回線のステータスを表示できるようになります。 • デフォルトで、PEルータはスレーブモードになります。 （注） 1 つの擬似回線をマスターにして、他の回線をスレーブにする必要があります。両方の擬似回線を同時にマスターまたはスレーブとして設定することはできません。
ステップ 7	**interworking** {**ethernet** | **ip**} 例： `Device(config-pw)# interworking ip`	（任意）異なるレイヤ 2 カプセル化の間の変換をイネーブルにします。

L2VPN：擬似回線優先転送の設定例

例：L2VPN：擬似回線優先転送の設定

次のコマンドは、PE ルータで L2VPN：擬似回線優先転送機能を設定します。

```
mpls ldp graceful-restart
mpls ip
mpls label protocol ldp
mpls ldp router-id Loopback0 force
mpls ldp advertise-labels
!
pseudowire-class mpls
 encapsulation mpls
 status redundancy master
interface ATM0/2/0.1 multipoint
 logging event subif-link-status
 atm pvp 50 l2transport
  xconnect 10.1.1.2 100 pw-class mpls
   backup peer 10.1.1.3 100 encap mpls
end
```

例：L2VPN：擬似回線優先転送の設定（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

次のコマンドは、PE ルータで L2VPN：擬似回線優先転送機能を設定します。

```
mpls ldp graceful-restart
mpls ip
mpls label protocol ldp
mpls ldp router-id Loopback0 force
mpls ldp advertise-labels
!
interface pseudowire1
 encapsulation mpls
 status redundancy master
 neighbor 10.0.0.1 123
interface ATM0/2/0.1 multipoint
 logging event subif-link-status
 atm pvp 50 l2transport
  interface pseudowire 100
  encapsulation mpls
  neighbor 10.1.1.2 100
!
l2vpn xconnect context A
 member pseudowire 100
 member atm 100
end
```

例：擬似回線のステータスの表示

次に、スイッチオーバー前、スイッチオーバー中、およびスイッチオーバー後のアクティブ擬似回線とバックアップ擬似回線のステータスの例を示します。

アクティブ PE ルータで **showmplsl2transportvc** コマンドを使用すると、擬似回線のステータスが表示されます。

```
Router# show mpls l2transport vc

Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
AT0/2/0/0.1    ATM VPC CELL 50            10.1.1.2         100        UP
AT0/2/0/0.1    ATM VPC CELL 50            10.1.1.3         100        STANDBY
```

バックアップ PE ルータで **showmplsl2transportvc** コマンドを使用すると、擬似回線のステータスが表示されます。バックアップ PE ルータのアクティブ擬似回線のステータスは HOTSTANDBY です。

```
Router1-standby# show mpls l2transport vc

Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
AT0/2/0/0.1    ATM VPC CELL 50            10.1.1.2         100        HOTSTANDBY
AT0/2/0/0.1    ATM VPC CELL 50            10.1.1.3         100        DOWN
```

スイッチオーバー中のアクティブ擬似回線とバックアップ擬似回線のステータスは次のように変化します。

```
Router# show mpls l2transport vc

Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
AT0/2/0/0.1    ATM VPC CELL 50            10.1.1.2         100        RECOVERING
AT0/2/0/0.1    ATM VPC CELL 50            10.1.1.3         100        DOWN
```

スイッチオーバーの完了後に、回復中の擬似回線のステータスは UP と示されます。

```
Router# show mpls l2transport vc

Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
AT0/2/0/0.1    ATM VPC CELL 50            10.1.1.2         100        UP
AT0/2/0/0.1    ATM VPC CELL 50            10.1.1.3         100        STANDBY
```

showxconnect コマンドを使用すると、バックアップ擬似回線のスタンバイ（SB）ステートが表示されます。これは、ルータのステートフル スイッチオーバー モードとは無関係です。

```
Router# show xconnect all

Legend:    XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State
  UP=Up       DN=Down            AD=Admin Down      IA=Inactive
  SB=Standby  HS=Hot Standby     RV=Recovering      NH=No Hardware
XC ST        Segment 1                                  S1 Segment 2
            S2
------+----------------------------------+--+----------------------------------+---------
UP pri ac   AT1/1/0/0.1/1/1:220/220(ATM V  UP mpls 10.193.193.3:330            UP
IA sec ac   AT1/1/0/0.1/1/1:220/220(ATM V  UP mpls 10.193.193.3:331            SB
```

pingmpls コマンドと **traceroutempls** コマンドを実行すると、バックアップ擬似回線でデータプレーンがアクティブであることが示されます。

```
Router# ping mpls pseudowire 10.193.193.22 331

%Total number of MS-PW segments is less than segment number; Adjusting the segment number
to 1
Sending 5, 100-byte MPLS Echos to 10.193.193.22,
     timeout is 2 seconds, send interval is 0 msec:
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
```

```
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

Router# traceroute mpls pseudowire 10.193.193.22 331 segment 1

Tracing MS-PW segments within range [1-1] peer address 10.193.193.22 and timeout 2 seconds
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
! 1 10.193.33.22 4 ms [Labels: 23 Exp: 0]
    local 10.193.193.3 remote 10.193.193.22 vc id 331
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
MPLS および MPLS アプリケーションに関連するコマンドの説明	『*Cisco IOS Multiprotocol Label Switching Command Reference*』
L2VPN 擬似回線	• *L2VPN* 擬似回線冗長性 • *MPLS* 擬似回線ステータス シグナリング
L2VPN の NSF/SSO	『*NSF/SSO--Any Transport over MPLS and AToM Graceful Restart*』
L2VPN の ping および traceroute	*MPLS LSP Ping/Traceroute for LDP/TE* および *LSP Ping for VCCV*

標準

規格	Title
draft-ietf-pwe3-redundancy-bit-xx.txt	『Preferential Forwarding Status Bit Definition』

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

L2VPN：擬似回線優先転送の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、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。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *14*：*L2VPN*：擬似回線優先転送の機能情報

機能名	リリース	機能情報
L2VPN：擬似回線優先転送	Cisco IOS XE Release 2.3	この機能により、**ping** コマンドと **show** コマンドを使用してスイッチオーバー前後とスイッチオーバー中にステータス情報を確認できるように、擬似回線を設定することができます。 次のコマンドが導入または変更されました：**showmplsl2transportvc**、**showxconnect**、**statusredundancy**。

第 6 章

L2VPN マルチセグメント擬似回線

L2VPN マルチセグメント擬似回線機能により、複数のレイヤ 2 擬似回線セグメントを 1 つの擬似回線として機能するように設定できます。L2VPN マルチセグメント擬似回線機能は、同一または異なるキャリア ネットワークにある複数のコアまたは自律システムにわたります。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース 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、機能情報の表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シスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

L2VPN マルチセグメント擬似回線の前提条件

この機能を設定する前に、次のドキュメントを参照してください。

- Any Transport over MPLS
- *L2VPN* 擬似回線スイッチング
- MPLS LSP Ping/Traceroute for LDP/TE および LSP Ping for VCCV
- 『Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)』（RFC 4447）

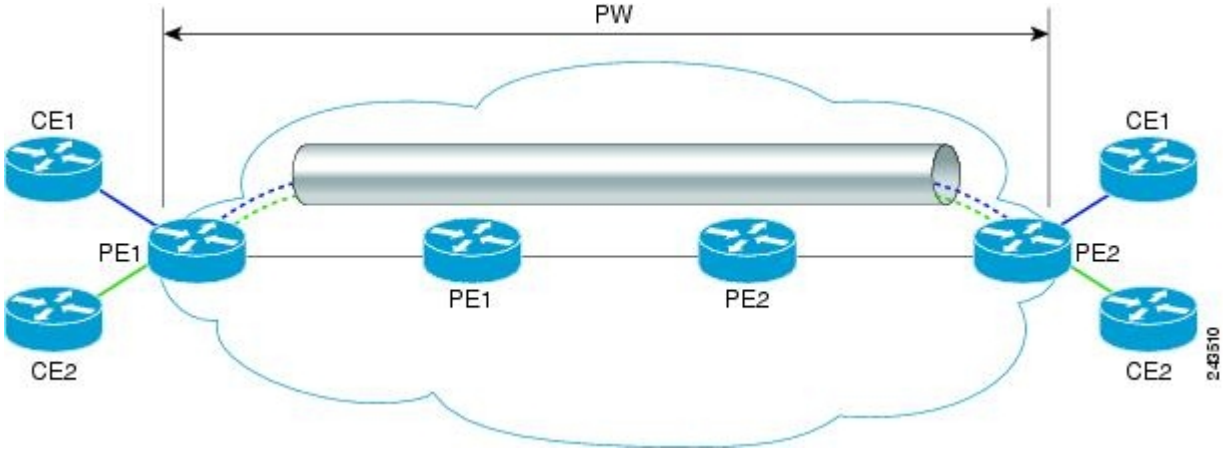
L2VPN マルチセグメント擬似回線の制約事項

- マルチプロトコル（MPLS）レイヤ 2 擬似回線のみサポートされます。
- 擬似回線の手動設定（S-PE ルータや T-PE ルータが含まれます）のみがサポートされます。
- L2VPN 擬似回線スイッチング機能は、FEC 128 でアドバタイズされた擬似回線でサポートされます。FEC 129 はサポートされません。
- S-PE ルータは、1600 擬似回線に制限されます。

L2VPN マルチセグメント擬似回線に関する情報

L2VPN 擬似回線の定義

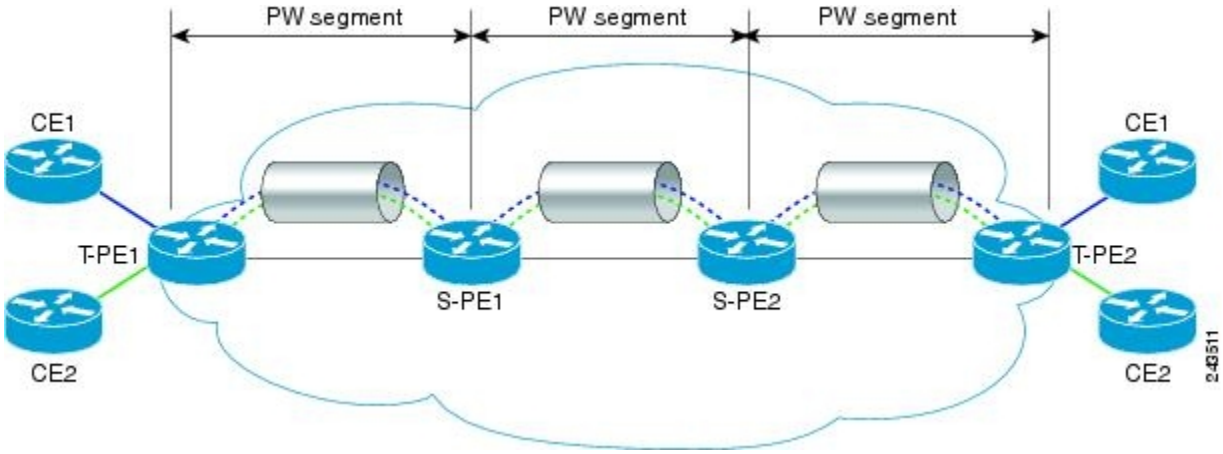
次の図に示すように、L2VPN 擬似回線（PW）は、コア全体の 2 つのプロバイダー エッジ（PE）ルータ間に確立されたトンネルで、MPLS データとしてカプセル化されたレイヤ 2 ペイロードを伝送します。これは、キャリアがフレーム リレーおよび ATM などの従来のレイヤ 2 ネットワークから MPLS コアに移行するのを支援します。図に示されている L2VPN 擬似回線では 2 つの PE ルータ間の PW は同じ自律システム内にあります。ルータ PE1 および PE2 は、Terminating PE Router（T-PE）と呼ばれます。接続回線は、これらの PE ルータの PW にバインドされています。



L2VPN マルチセグメント擬似回線の定義

L2VPN マルチセグメント擬似回線（MS-PW）は、単一の PW として機能する 2 つ以上の PW セグメントのセットです。スイッチド PW と呼ばれることもあります。MS-PW は、同一または異なるキャリア ネットワークにある複数のコアまたは自律システムにわたります。1 つの L2VPN MS-PW には最大で 254 PW セグメントを含めることができます。

次の図は、マルチセグメント擬似回線トポロジの例です。



エンド ルータは終端 PE ルータ（T-PE）と呼ばれ、スイッチング ルータは S-PE ルータと呼ばれます。S-PE ルータは、MS-PW 内の先行および後続の PW セグメントのトンネルを終端します。S-PE ルータは、MS-PW の先行および後続の PW セグメントのコントロールおよびデータ プレーンを切り替えることができます。MS-PW は、すべての単一セグメント PW がアップ状態の場合に、アップ状態であると宣言されます。詳細については、『*L2VPN Pseudowire Switching*』のマニュアルを参照してください。

L2VPN マルチセグメント擬似回線の設定方法

L2VPN マルチセグメント擬似回線の設定

L2VPN マルチセグメント擬似回線を構築するには、S-PE ルータ上で次の手順を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. mpls label protocol ldp
4. **mplsldprouter-id***interface***force**
5. **pseudowire-class**name
6. **encapsulationmpls**
7. **switchingtlv**
8. **exit**
9. **l2vfi***name***point-to-point**
10. **description***string*
11. **neighbor***ip-addressvcid{***encapsulationmplspw-class***pw-class-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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	mpls label protocol ldp 例： `Router(config)# mpls label protocol ldp`	すべてのインターフェイスでラベル配布プロトコル（LDP）の使用を設定します。
ステップ 4	**mplsldprouter-id***interface***force** 例： `Router(config)# mpls ldp router-id loopback0 force`	LDP ルータ ID を決定する優先インターフェイスを指定します。
ステップ 5	**pseudowire-class**name 例： `Router(config)# pseudowire-class atom`	指定した名前の擬似回線クラスを確立して、擬似回線クラス 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 6	**encapsulationmpls** 例： `Router(config-pw-class)# encapsulation mpls`	トンネリング カプセル化を指定します。 • L2VPN MPLS では、カプセル化タイプは **mpls** です。
ステップ 7	**switchingtlv** 例： `Router(config-pw-class)# switching tlv`	（任意）ラベル バインディングでのスイッチング ポイント type-length variable（TLV）のアドバタイズメントを有効にします。 • このコマンドは、デフォルトでイネーブルになっています。
ステップ 8	**exit** 例： `Router(config-pw-class)# exit`	擬似回線 クラス コンフィギュレーション モードを終了します。
ステップ 9	**l2vfi***name***point-to-point** 例： `Router(config)# l2 vfi atomtunnel point-to-point`	ポイントツーポイント レイヤ 2 Virtual Forwarding Interface（VFI）を作成し、VFI コンフィギュレーション モードを開始します。
ステップ 10	**description***string* 例： `Router(config-vfi)# description segment1`	マルチセグメント擬似回線のプロバイダー エッジ スイッチング ルータの説明を指定します。
ステップ 11	**neighbor***ip-addressvcid{***encapsulationmplspw-class***pw-class-name}* 例： `Router(config-vfi)# neighbor 10.0.0.1 100 pw-class mpls`	エミュレートされた VC を設定します。 • IP アドレスおよびピア ルータの VC ID を指定します。また、エミュレートされた VC で使用する擬似回線クラスを指定します。 （注） 2 つの **neighbor** コマンドだけが **l2vfipoint-to-point** コマンドごとに許可されます。

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した L2VPN マルチセグメント擬似回線の設定

S-PE ルータ上で L2VPN マルチセグメント擬似回線を構築するには、次のタスクを実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **mplslabel protocol ldp**
4. **mplsldprouter-id***interface***force**
5. **interface pseudowire** *number*
6. **encapsulationmpls**
7. **switchingtlv**
8. **neighbor***peer-address vcid-value*
9. **exit**
10. **l2vpnxconnectcontext***context-name*
11. **description***string*
12. **member***ip-addressvcid***encapsulationmpls**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**mplslabel protocol ldp** 例： `Device(config)# mpls label protocol ldp`	すべてのインターフェイスでラベル配布プロトコル（LDP）の使用を設定します。

	コマンドまたはアクション	目的
ステップ 4	**mplsldprouter-id***interface***force** 例： `Device(config)# mpls ldp router-id loopback0 force`	LDP ルータ ID を決定する優先インターフェイスを指定します。
ステップ 5	**interface pseudowire** *number* 例： `Device(config)# interface pseudowire 1`	指定した値でインターフェイス擬似回線を確立して、擬似回線コンフィギュレーション モードを開始します。
ステップ 6	**encapsulationmpls** 例： `Device(config-pw)# encapsulation mpls`	トンネリング カプセル化を指定します。 • L2VPN MPLS では、カプセル化タイプは **mpls** です。
ステップ 7	**switchingtlv** 例： `Device(config-pw)# switching tlv`	（任意）ラベル バインディングでのスイッチング ポイント type-length variable（TLV）のアドバタイズメントを有効にします。 • このコマンドは、デフォルトでイネーブルになっています。
ステップ 8	**neighbor***peer-address vcid-value* 例： `Router(config-pw)# neighbor 10.0.0.1 123`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 9	**exit** 例： `Device(config-pw)# exit`	擬似回線コンフィギュレーション モードを終了します。
ステップ 10	**l2vpnxconnectcontext***context-name* 例： `Device(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect 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 11	**description***string* 例： `Device(config-xconnect)# description segment1`	マルチセグメント擬似回線のプロバイダーエッジスイッチング ルータの説明を指定します。
ステップ 12	**member***ip-addressvcid***encapsulationmpls** 例： `Device(config-xconnect)# member 10.10.10.10 1 encapsulation mpls`	ポイントツーポイント Layer 2 VPN（L2VPN）Virtual Forwarding Interface（VFI）接続を形成するデバイスを指定します。 （注） 2 つの **member** コマンドだけが **l2vpnxconnectcontext** コマンドごとに許可されます。

L2VPN マルチセグメント擬似回線の情報の表示

手順の概要

1. **showmplsl2transportbinding**
2. **showmplsl2transportvcdetail**

手順の詳細

ステップ 1 **showmplsl2transportbinding**

出力内の太字で示すように、**showmplsl2transportbinding** コマンドを使用して、擬似回線スイッチング ポイントに関する情報を表示します。（次の例では、PE1 および PE4 が T-PE ルータです）。

例：

```
Router# show mpls l2transport binding

  Destination Address: 10.1.1.1,  VC ID: 102
    Local Label:  17
        Cbit: 1,    VC Type: FastEthernet,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: CW [1], RA [2], TTL [3]
              CV Type: LSPV [2]
    Remote Label: 16
        Cbit: 1,    VC Type: FastEthernet,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: CW [1], RA [2], TTL [3]
              CV Type: LSPV [2]
        PW Switching Point:
             Vcid   local IP addr      remote IP addr      Description
             101    10.11.11.11        10.20.20.20         PW Switching Point PE3
             100    10.20.20.20        10.11.11.11         PW Switching Point PE2
```

ステップ 2 **showmplsl2transportvcdetail**

showmplsl2transportvcdetail コマンドを使用して、擬似回線スイッチング ポイントのステータスを表示します。次の例では、出力（太字で表示された箇所）にマルチセグメント擬似回線の障害の原因のとなったセグメントが表示されています。

例：

```
Router# show mpls l2transport vc detail
Local interface: Se3/0/0 up, line protocol up, HDLC up
  Destination address: 12.1.1.1, VC ID: 100, VC status: down
    Output interface: Se2/0, imposed label stack {23}
    Preferred path: not configured
    Default path: active
    Next hop: point2point
  Create time: 00:03:02, last status change time: 00:01:41
  Signaling protocol: LDP, peer 10.1.1.1:0 up
    Targeted Hello: 10.1.1.4(LDP Id) -> 10.1.1.1, LDP is UP
    Status TLV support (local/remote)   : enabled/supported
      LDP route watch                   : enabled
      Label/status state machine        : established, LruRrd
      Last local dataplane   status rcvd: No fault
      Last local SSS circuit status rcvd: No fault
      Last local SSS circuit status sent: DOWN(PW-tx-fault)
      Last local  LDP TLV    status sent: No fault
      Last remote LDP TLV    status rcvd: DOWN(PW-tx-fault)
       PW Switching Point:
       Fault type  Vcid   local IP addr   remote IP addr   Description
       PW-tx-fault  101   10.1.1.1        10.1.1.1         S-PE2
      Last remote LDP ADJ    status rcvd: No fault
    MPLS VC labels: local 19, remote 23
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 16, send 27
    byte totals:   receive 2506, send 3098
    packet drops:  receive 0, seq error 0, send 0
```

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した L2VPN マルチセグメント擬似回線に関する情報の表示

手順の概要

1. **showl2vpnatombinding**
2. **showl2vpnatomvcdetail**

手順の詳細

ステップ 1 **showl2vpnatombinding**

出力内の太字で示すように、**showl2vpnatombinding** コマンドを使用して、擬似回線スイッチング ポイントに関する情報を表示します。（次の例では、PE1 および PE4 が T-PE ルータです）。

例：

```
Device# show l2vpn atom binding

  Destination Address: 10.1.1.1,  VC ID: 102
    Local Label:  17
        Cbit: 1,    VC Type: FastEthernet,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: CW [1], RA [2], TTL [3]
              CV Type: LSPV [2]
    Remote Label: 16
        Cbit: 1,    VC Type: FastEthernet,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: CW [1], RA [2], TTL [3]
              CV Type: LSPV [2]
        PW Switching Point:
             Vcid   local IP addr      remote IP addr      Description
             101    10.11.11.11        10.20.20.20         PW Switching Point PE3
             100    10.20.20.20        10.11.11.11         PW Switching Point PE2
```

ステップ 2 **showl2vpnatomvcdetail**

showl2vpnatomvcdetail コマンドを使用して、擬似回線スイッチング ポイントのステータスを表示します。次の例では、出力（太字で表示された箇所）にマルチセグメント擬似回線の障害の原因のとなったセグメントが表示されています。

例：

```
Device# show l2vpn atom vc detail
Local interface: Se3/0/0 up, line protocol up, HDLC up
  Destination address: 12.1.1.1, VC ID: 100, VC status: down
    Output interface: Se2/0, imposed label stack {23}
    Preferred path: not configured
    Default path: active
    Next hop: point2point
  Create time: 00:03:02, last status change time: 00:01:41
  Signaling protocol: LDP, peer 10.1.1.1:0 up
    Targeted Hello: 10.1.1.4(LDP Id) -> 10.1.1.1, LDP is UP
    Status TLV support (local/remote)   : enabled/supported
      LDP route watch                   : enabled
      Label/status state machine        : established, LruRrd
      Last local dataplane   status rcvd: No fault
      Last local SSS circuit status rcvd: No fault
      Last local SSS circuit status sent: DOWN(PW-tx-fault)
      Last local  LDP TLV    status sent: No fault
      Last remote LDP TLV    status rcvd: DOWN(PW-tx-fault)
       PW Switching Point:
       Fault type  Vcid   local IP addr   remote IP addr   Description
       PW-tx-fault  101   10.1.1.1        10.1.1.1         S-PE2
      Last remote LDP ADJ    status rcvd: No fault
    MPLS VC labels: local 19, remote 23
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 16, send 27
    byte totals:   receive 2506, send 3098
    packet drops:  receive 0, seq error 0, send 0
```

L2VPN マルチセグメント擬似回線上での ping mpls 操作と trace mpls 操作の実行

pingmpls コマンドと **tracempls** コマンドを使用して、MPLS マルチセグメント擬似回線のすべてのセグメントが動作していることを確認できます。

pingmpls コマンドを使用して、次の擬似回線ポイントでの接続を確認できます。

- 擬似回線の一方の終端からもう一方へ
- 擬似回線のいずれかから特定のセグメントへ
- 2 つの隣接 S-PE ルータ間のセグメント

tracempls コマンドを使用して、次の擬似回線ポイントでの接続を確認できます。

- 擬似回線の一方の終端からもう一方へ
- 擬似回線のいずれかから特定のセグメントへ
- 2 つの隣接 S-PE ルータ間のセグメント
- セグメントの範囲

手順の概要

1. **pingmplspseudowire***destination-addressvc-id* [**segment***segment-number*]
2. **tracemplspseudowire***destination-addressvc-id***segment***segment-numbersegment-number*

手順の詳細

ステップ 1 **pingmplspseudowire***destination-addressvc-id* [**segment***segment-number*]
それぞれの説明は次のとおりです。

- *destination-address* は、送信元の方向から見てセグメントの最後の S-PE ルータのアドレスです。
- *vc-id* は、送信元から次の PE ルータへのセグメントの VC ID です。
- **segment***segment-number* はオプションで、*ping* するセグメントを指定します。

次の例では、上の 2 つ目の図で示されているトポロジが使用されます。

- T-PE1 から T-PE2 に対するエンドツーエンド ping 操作を実行するには、次のコマンドを入力します。

pingmplspseudowire *<addr-of-S-PE1> <T-PE1* と *S-PE1* の間の *vc-id>*

- T-PE1 からセグメント 2 に対する ping 操作を実行するには、次のコマンドを入力します。

pingmplspseudowire *<addr-of-S-PE1> <T-PE1 と S-PE1 の間の vc-id>* **segment2**

例：

ステップ 2 **tracemplspseudowire***destination-addressvc-id***segment***segment-numbersegment-number*
それぞれの説明は次のとおりです。

- *destination-address* は、トレースの発信元からの次の *S-PE* ルータのアドレスです。
- *vc-id* は **trace** コマンドが発行されたセグメントの VC ID です。
- *segment-number* は、trace 操作が機能するセグメントを示します。2 つのセクション番号を入力すると、traceroute 操作はそのルータの範囲に対してトレースを実行します。

次の例では、上の 2 つ目の図で示されているトポロジが使用されます。

- マルチセグメント擬似回線の T-PE1 からセグメント 2 への trace 操作を実行するには、次のコマンドを入力します。

tracemplspseudowire *<addr-of-S-PE1> <T-PE1 と S-PE1 の間の vc-id>* **segment2**

この例では、T-PE1 から S-PE2 に対してトレースを実行します。

- セグメントの範囲に対して trace 操作を実行するには、次のコマンドを入力します。この例では、S-PE2 から T-PE2 へのトレースを実行します。

tracemplspseudowire *<addr-of-S-PE1> <T-PE1 と S-PE1 の間の vc-id>* **segment24**

次のコマンドは、セグメント 1 で S-PE ルータ 10.10.10.9 の trace 操作を実行してから、セグメント 2 で同じ操作を実行します。

例：

```
router# trace mpls pseudowire 10.10.10.9 220 segment 1
Tracing MS-PW segments within range [1-1] peer address 10.10.10.9 and timeout 2 seconds
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
L 1 10.10.9.9 0 ms [Labels: 18 Exp: 0]
    local 10.10.10.22 remote 10.10.10.9 vc id 220
router# trace mpls pseudowire 10.10.10.9 220 segment 2
Tracing MS-PW segments within range [1-2] peer address 10.10.10.9 and timeout 2 seconds
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
L 1 10.10.9.9 4 ms [Labels: 18 Exp: 0]
    local 10.10.10.22 remote 10.10.10.9 vc id 220
```

```
! 2 10.10.3.3 4 ms [Labels: 16 Exp: 0]
    local 10.10.10.9 remote 10.10.10.3 vc id 220
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
MPLS および MPLS アプリケーションに関連するコマンドの説明	『*Cisco IOS Multiprotocol Label Switching Command Reference*』
レイヤ 2 VPNS	• Any Transport over MPLS • *L2VPN* 擬似回線スイッチング • MPLS LSP Ping/Traceroute for LDP/TE および LSP Ping for VCCV

標準

規格	Title
RFC 4777	『Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)』

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB の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 ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC の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	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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。	http://www.cisco.com/cisco/web/support/index.html

L2VPN マルチセグメント擬似回線の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、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。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *15* : ***L2VPN*** マルチセグメント擬似回線の機能情報

機能名	リリース	機能情報
マルチセグメント擬似回線の MPLS OAM サポート	Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.5S	L2VPN マルチセグメント擬似回線機能により、複数のレイヤ 2 擬似回線セグメントを 1 つの擬似回線として機能するように設定できます。L2VPN マルチセグメント擬似回線機能は、同一または異なるキャリア ネットワークにある複数のコアまたは自律システムにわたります。 この機能は、Cisco IOS XE リリース 2.3 で、Cisco ASR 1000 シリーズ ルータに導入および実装されました。 Cisco IOS XE Release 3.5S では、Cisco ASR 903 ルータのサポートが追加されました。 次のコマンドが導入または変更されました：**description** (l2 vfi)、**pingmpls**、**showmplsl2transportbinding**、**showmplsl2transportvc**、**switchingtlv**、**tracempls**。

第 7 章

MPLS Quality of Service

MPLS Quality of Service 機能（旧称：MPLS CoS 機能）により、MPLS ネットワーク上で差別化サービスを提供できます。さまざまなネットワーキング要件を満たすため、各送信 IP パケットに適用可能なサービス クラスを指定できます。各パケットのヘッダーに IP precedence ビットを設定することによって、IP パケットに対して異なるサービス クラスを確立できます。

MPLS Quality of Service の前提条件

MPLS CoS をネットワークで最大限活用するには、次の機能がサポートされている必要があります。

- マルチプロトコル ラベル スイッチング（MPLS）：MPLS は、Internet Engineering Task Force（IETF）によって定義されている標準化されたラベル スイッチング プロトコルです。
- Cisco Express Forwarding：Cisco Express Forwarding は、大量のトラフィックを処理し、動的なトラフィック パターンを提示する、ネットワークのパフォーマンスと拡張性を最適化する高度なレイヤ 3 IP スイッチング テクノロジーです。
- 非同期転送モード（ATM）：ネットワーク上の ATM インターフェイスを使用する場合、ATM シグナリング サポートが必要です。

  ネットワークでパケット インターフェイスのみを使用する場合、ATM 機能は必要ありません。
- QoS 機能：

- 重み付け均等化キューイング（WFQ）：WFQ は、すべてのネットワーク トラフィックに帯域幅を均等に割り当てる動的なスケジューリング方式で、非 GSR プラットフォームで使用されます。

  WFQ は、トラフィックに優先順位（または重み）を適用して、トラフィックをフローに分類し、各フローに許可する帯域幅の量を決定します。WFQ は、インタラクティブ トラフィックをキューの先頭にして応答時間を減らし、残りの帯域を高帯域幅のフローで均等に共有します。

- 重み付けランダム早期検出（WRED）：WRED は、さまざまな RED パラメータを IP precedence 値ごとに設定できるようにすることによって RED 機能を拡張する輻輳回避メカニズムです。

  IP パケット ヘッダーのタイプ オブ サービス（ToS）オクテットに含まれる IP precedence ビットは、IP パケットの相対的な重要性と優先順位を示すために使用されます。WRED では、これらの IP precedence 値を使用して、パケットを異なる廃棄優先順位またはサービス クラスに分類します。

- Modified Deficit Round Robin（MDRR）：MDRR は、QoS のファセットとして出力の優先順位を付与するトラフィック クラスの優先順位付けメカニズムで、GSR プラットフォームのみで使用されます。MDRR は、非 GSR プラットフォームの WFQ と機能が似ています。

  MDRR では、IP トラフィックは異なるサービス クラスのキューにマップされます。キューのグループは、トラフィックの宛先にそれぞれ割り当てられます。プラットフォームの送信側では、キューのグループはインターフェイス単位で定義されます。一方、プラットフォームの受信側では、キューのグループは宛先単位で定義されます。IP パケットは、IP precedence 値に基づいて、これらのキューにマップされます。

  これらのキューは、絶対優先モードまたは交互優先モードのいずれかで実行されるように定義されたキューを除き、ラウンドロビン方式で処理されます。

  絶対優先モードでは、空でないときは常に優先度の高いキューが処理されます。これにより、優先度の高いトラフィックの生じうる遅延を最小限に抑えることができます。ただし、このモードでは、優先度の高いキューが利用可能な帯域幅の多くを消費する場合に、その他のトラフィックが長い間処理されない可能性があります。

  交互優先モードでは、優先度の高いキューとその他のキューの間で交互にトラフィック キューが処理されます。

- 専用アクセス レート（CAR）：CAR は、IP precedence 値または QoS グループを IP パケット ヘッダーに設定することによって、インターフェイスで入出力伝送レートを制限し、パケットを分類する QoS 機能です。

MPLS Quality of Service に関する情報

MPLS Quality of Service の概要

ネットワーク管理者は MPLS QoS 機能を使用することで、差別化したサービスを MPLS ネットワーク上で提供できます。ネットワーク管理者は、転送IPパケットごとに適用するサービスクラスを指定することによって、さまざまなネットワーキング要件を満たすことができます。各パケットのヘッダーに IP precedence ビットを設定することによって、IP パケットに対して異なるサービス クラスを確立できます。

MPLS CoS は MPLS ネットワークの次の差別化サービスをサポートします。

- パケット分類
- 輻輳回避
- 輻輳管理

次の表に、MPLS CoS のサービスと機能を示します。

表 *16*：*MPLS CoS* のサービスと機能

サービス	CoS 機能	説明
パケット分類	専用アクセス レート（CAR）パケットは、ラベルが割り当てられる前に、ネットワークのエッジで分類されます。	CAR は IP ヘッダー内のタイプオブ サービス（ToS）ビットを使用し、入出力伝送レートに従ってパケットを分類します。多くの場合、CAR は、ネットワークを出入りするトラフィックを制限するため、ネットワークのエッジにあるインターフェイスに設定されます。CAR 分類コマンドを使用して、パケットを分類または再分類することができます。

サービス	CoS 機能	説明
輻輳回避	重み付けランダム早期検出（WRED）。パケット クラスは、廃棄確率に基づいて区別されます。	WRED はネットワーク トラフィックを監視し、共通ネットワークおよびインターネットワークのボトルネックで輻輳を回避します。WRED は、インターフェイスが輻輳状態になると、よりプライオリティが低いトラフィックを選択的に廃棄できます。また、異なるサービス クラスに対して差別化したパフォーマンス特性を提供できます。
輻輳管理	非 GSR プラットフォーム用の重み付け均等化キューイング（WFQ）。パケット クラスは、帯域幅要件と有限遅延特性に基づいて区別されます。 GSR プラットフォーム用の Modified Deficit Round Robin（MDRR）。	WFQ は自動スケジューリング システムで、すべてのネットワーク トラフィックに均等に帯域幅を割り当てます。WFQ は重み（優先順位）を使用して、トラフィックの各クラスに割り当てる帯域幅を決定します。 MDRR（非 GSR プラットフォーム用の WFQ と機能が似ています）は、各パケットの IP precedence 値に基づいて異なるサービス クラスのキューに IP トラフィックをマッピングするトラフィックの優先順位付けスキームです。キューはラウンドロビン方式で処理されます。

MPLS CoS によって、MPLS デバイスに可能な限り正確に Cisco IP CoS（レイヤ 3）の機能を複製することができます。これには、ラベル エッジ スイッチング ルータ（エッジ LSR）とラベル スイッチング ルータ（LSR）が含まれます。MPLS CoS 機能は、あらゆるタイプのインターフェイスの IP CoS 機能に 1 対 1 に近い形でマッピングされます。

タグ スイッチングおよび MPLS の用語

次の表に、このドキュメントやその他の関連するシスコの出版物で使用される既存のレガシー タグ スイッチングの用語と新しい同等のマルチプロトコル ラベル スイッチング（MPLS）IETF の用語を示します。

表 *17*：タグ スイッチングの用語と同等の *MPLS* の用語

古い名称	新しい名称
タグ スイッチング	Multiprotocol Label Switching：マルチプロトコル ラベル スイッチング
タグ（タグ スイッチングの短縮形）	MPLS
タグ（アイテムまたはパケット）	Label
TDP（タグ配布プロトコル）	LDP（ラベル配布プロトコル）。Cisco TDP および LDP（MPLS ラベル配布プロトコル）は、機能面では非常に類似していますが、メッセージ形式や、個々のプロトコルを設定したり動作を監視したりするためのコマンドなど詳細な点は異なります。
タグ スイッチド	ラベル スイッチド
TFIB（タグ転送情報ベース）	LFIB（ラベル転送情報ベース）
TSR（タグ スイッチング ルータ）	LSR（ラベル スイッチング ルータ）
TVC（タグ VC、タグ仮想回線）	LVC（ラベル VC、ラベル仮想回線）
TSP（タグ スイッチ パス）	LSP（ラベル スイッチ パス）

MPLS ネットワークのエッジで使用される LSR

マルチプロトコル ラベル スイッチング（MPLS）のネットワーク バックボーンのエッジで使用されるラベル スイッチング ルータ（LSR）は、MPLS ソフトウェアを実行するデバイスです。エッジ LSR はネットワークの入力側と出力側のいずれにも配置できます。

MPLS ネットワークの入力側では、デバイスはパケットを次のように処理します。

1. IP パケットは、エッジ LSR で MPLS ネットワークのエッジに入ります。
2. エッジ LSR は、モジュラ Quality of Service（QoS）コマンドライン インターフェイス（CLI）（MQC）などの分類メカニズムを使用して、着信 IP パケットを分類し、IP precedence 値を設定します。または、すでに設定されている IP precedence 値を使用して IP パケットを受信することもできます。
3. デバイスはパケットごとに IP アドレスの検索を行い、ネクストホップ LSR を決定します。
4. 適切なラベルがパケットに挿入され、IP precedence ビットがラベル ヘッダーの MPLS EXP ビットにコピーされます。

5 ラベルの付けられたパケットは、処理のために適切な出力インターフェイスに転送されます。

6 パケットは次のいずれかに従って、クラスごとに区別されます。

- 廃棄確率：重み付けランダム早期検出（WRED）
- 帯域幅割り当てと遅延：クラスベース重み付け均等化キューイング（CBWFQ）

いずれの場合でも、LSR は、すべての入力デバイスで WRED または CBWFQ を採用し続けることにより、定義された差別化を適用します。

MPLS ネットワークの出力側では、デバイスはパケットを次のように処理します。

1 MPLS のラベルが付けられたパケットは、MPLS ネットワーク バックボーンからエッジ LSR に入ります。

2 MPLS ラベルが削除されます。IP パケットは（再）分類されることがあります。

3 パケットごとに、デバイスは IP アドレスの検索を行い、パケットの宛先を決定し、処理のためパケットを宛先インターフェイスに転送します。

4 パケットは IP precedence 値によって区別され、WRED および CBWFQ の廃棄確率設定に応じて処理されます。

MPLS ネットワークのコアで使用される LSR

マルチプロトコル ラベル スイッチング（MPLS）ネットワークのコアで使用されるラベル スイッチング ルータ（LSR）は、MPLS ソフトウェアを実行するデバイスです。MPLS ネットワークのコアに位置するこれらのデバイスは、パケットを次のように処理します。

1 エッジデバイスまたはその他のコアデバイスから着信する MPLS のラベルが付けられたパケットが、このコア デバイスに入ってきます。

2 コア デバイスで検索が実行され、ネクスト ホップ LSR が決定されます。

3 適切なラベルがパケットに配置（スワップ）され、MPLS EXP ビットがコピーされます。

4 ラベルの付けられたパケットは、処理するために出力インターフェイスに転送されます。

5 パケットが MPLS EXP フィールドのマーキングによって区別され、重み付けランダム早期検出（WRED）およびクラスベース重み付け均等化キューイング（CBWFQ）の設定に応じて適切に処理されます。

IP バックボーンでの MPLS CoS の利点

マルチプロトコル ラベル スイッチング（MPLS）を実行する IP デバイスで構成されるバックボーンで MPLS CoS を使用すると、次のような利点があります。

- 効果的なリソース配賦：帯域をクラスごとおよびリンクごとに割り当てるために WFQ（Weighted Fair Queueing）が使用され、これによりネットワーク トラフィックのリンク帯域幅の割合が保証されます。
- パケットの差別化：パケットは、IP パケットが MPLS ネットワークを通過する際、IP パケットの IP プレシデンス ビットを MPLS EXP フィールドの MPLS CoS ビットにマッピングすることにより差別化されます。このビットのマッピングにより、サービスプロバイダーはエンドツーエンドネットワークを保証し、顧客のサービス レベル契約（SLA）の条件を満たすことができます。
- 将来のサービス強化：MPLS CoS は、帯域幅要求を満たすことにより、将来のサービス強化（仮想専用回線など）のための基礎を提供します。

MPLS Quality of Service の設定方法

WRED の設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface** *type number*
4. **random-detect**
5. **random-detect precedence** *min-threshold max-threshold mark-probability*
6. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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： `Device(config)# gigabitethernet0/0/0`	インターフェイスのタイプ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	**random-detect** 例： `Device(config-if)# random-detect`	重み付けランダム早期検出/分散重み付けランダム早期検出（WRED/DWRED）を使用するようにインターフェイスを設定します。
ステップ 5	**random-detect precedence** *min-threshold max-threshold mark-probability* 例： `Device(config-if)# random-detect precedence 0 32 256 100`	優先値ごとの WRED/DWRED パラメータを設定します。
ステップ 6	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

WRED の確認

重み付けランダム早期検出（WRED）を確認するには、次の表に示す形式のコマンドを使用します。この例は、設定例の図に示すネットワーク トポロジ内の「デバイス 2」に基づきます。

手順の概要

1. **show queueing interface** *subinterface*

手順の詳細

show queueing interface *subinterface*

例：
`Device2# show queueing interface gigabitethernet6/0/0`
指定されたインターフェイス上の WRED 設定を確認します。

```
Device2# show queueing interface gigabitethernet6/0/0

Interface Gige6/0/0 queueing strategy:random early detection (WRED)
     Exp-weight-constant:9 (1/512)
     Mean queue depth:0

     Class   Random       Tail    Minimum    Maximum     Mark
               drop       drop  threshold  threshold  probability
       0         85          0         20         40     1/10
       1         22          0         22         40     1/10
       2          0          0         24         40     1/10
       3          0          0         26         40     1/10
       4          0          0         28         40     1/10
       5          0          0         31         40     1/10
       6          0          0         33         40     1/10
```

```
 7          0          0          35          40     1/10
rsvp        0          0          37          40     1/10
```

CAR の設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface** *name*
4. **rate-limit input** [**access-group** [**rate-limit**] *acl-index*] *bps burst-normal burst-max* **conform-action** *conform-action* **exceed-action** *exceed-action*
5. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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** *name* 例： `Device(config)# interface gigabitethernet`	入力インターフェイスを指定して、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	**rate-limit input** [**access-group** [**rate-limit**] *acl-index*] *bps burst-normal burst-max* **conform-action** *conform-action* **exceed-action** *exceed-action* 例： `Device(config-if)# rate-limit input access-group 101 496000 32000 64000 conform-action set-prec-transmit 4`	ラベル インポジション中にパケットに対して実行するアクションを指定します。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

CAR の設定の確認

手順の概要

1. **show interfaces** *slot/port* **rate-limit**

手順の詳細

show interfaces *slot/port* **rate-limit**

例：
```
Device2# show interfaces fe1/1/1 rate-limit
```
CAR 設定を確認して、次の形式のコマンドを使用します。

```
Device2# show interfaces fe1/1/1 rate-limit

FastEthernet1/1/1
   Input
     matches:access-group 101
       params: 496000 bps, 32000 limit, 64000 extended limit
       conformed 2137 packets, 576990 bytes; action:set-prec-transmit 4
       exceeded 363 packets, 98010 bytes; action:set-prec-transmit 0
       last packet:11788ms ago, current burst:39056 bytes
       last cleared 00:01:18 ago, conformed 58000 bps, exceeded 10000 bps
```

CBWFQ の設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **class-map** *class-map-name*
4. **match** *type number*
5. **policy-map** *policy-map-name*
6. **class** *class-map-name*
7. **bandwidth** *number*
8. **interface** *type number*
9. **service-policy output** *policy-map-name*
10. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**class-map** *class-map-name* 例： `Device(config)# class-map class-map-1`	クラス マップを作成し、クラス マップ 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	**match** *type number* 例： `Device(config-cmap)# match ip precedence 0 1`	クラスマップを照合するトラフィックを指定します。
ステップ 5	**policy-map** *policy-map-name* 例： `Device(config-cmap)# policy-map outputmap`	ポリシーマップを作成して、ポリシーマップコンフィギュレーション モードを開始します。
ステップ 6	**class** *class-map-name* 例： `Device(config-pmap)# class class-map-1`	クラス マップをポリシー マップに関連付けます。
ステップ 7	**bandwidth** *number* 例： `Device(config-pmap-c)# bandwidth 10000`	クラスマップと一致するトラフィックに対して実行する帯域幅（CBWFQ）アクションを関連付け、ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 8	**interface** *type number* 例： `Device(config-pmap-c)# interface gigabitethernet0/0/0`	インターフェイスのタイプ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 9	**service-policy output** *policy-map-name* 例： `Device(config-if)# service-policy output outputmap`	ポリシーマップをインターフェイスに割り当てます。

	コマンドまたはアクション	目的
ステップ 10	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

CBWFQ 設定の確認

手順の概要

1. **show policy-map interface** *type number*

手順の詳細

show policy-map interface *type number*

例：
`Device5# show policy-map interface fe5/1/0`
クラスベース重み付け均等化キューイング（CBWFQ）設定を確認して、次の形式のコマンドを使用します。この例は、設定例の図に示すネットワーク トポロジ内の「デバイス 5」に基づきます。

```
Device5# show policy-map interface fe5/1/0

  FastEthernet5/1/0
   service-policy output:outputmap
     class-map:prec_01 (match-all)
       522 packets, 322836 bytes
       5 minute rate 1000 bps
       match:ip precedence 0  1
       queue size 0, queue limit 1356
       packet output 522, packet drop 0
       tail/random drop 0, no buffer drop 0, other drop 0
       bandwidth:class-based wfq, weight 10
       random-detect:
         Exp-weight-constant:9 (1/512)
         Mean queue depth:0
   Class Random       Tail    Minimum    Maximum     Mark      Output
           drop       drop  threshold  threshold  probability packets
   0          0          0       3390       6780     1/10         522
   1          0          0       3813       6780     1/10           0
   2          0          0       4236       6780     1/10           0
   3          0          0       4659       6780     1/10           0
   4          0          0       5082       6780     1/10           0
   5          0          0       5505       6780     1/10           0
   6          0          0       5928       6780     1/10           0
   7          0          0       6351       6780     1/10           0

     class-map:prec_23 (match-all)
       0 packets, 0 bytes
       5 minute rate 0 bps
       match:ip precedence 2  3
       queue size 0, queue limit 0
       packet output 0, packet drop 0
```

```
      tail/random drop 0, no buffer drop 0, other drop 0
      bandwidth:class-based wfq, weight 15
      random-detect:
        Exp-weight-constant:9 (1/512)
        Mean queue depth:0
  Class Random       Tail    Minimum    Maximum     Mark      Output
          drop       drop  threshold  threshold  probability packets
  0          0          0          0          0    1/10            0
  1          0          0          0          0    1/10            0
  2          0          0          0          0    1/10            0
  3          0          0          0          0    1/10            0
  4          0          0          0          0    1/10            0
  5          0          0          0          0    1/10            0
  6          0          0          0          0    1/10            0
  7          0          0          0          0    1/10            0

    class-map:prec_45 (match-all)
      2137 packets, 576990 bytes
      5 minute rate 16000 bps
      match:ip precedence 4  5
      queue size 0, queue limit 2712
      packet output 2137, packet drop 0
      tail/random drop 0, no buffer drop 0, other drop 0
      bandwidth:class-based wfq, weight 20
      random-detect:
        Exp-weight-constant:9 (1/512)
        Mean queue depth:0
  Class Random       Tail    Minimum    Maximum     Mark      Output
          drop       drop  threshold  threshold  probability packets
  0          0          0       3390       6780    1/10            0
  1          0          0       3813       6780    1/10            0
  2          0          0       4236       6780    1/10            0
  3          0          0       4659       6780    1/10            0
  4          0          0       5082       6780    1/10         2137
  5          0          0       5505       6780    1/10            0
  6          0          0       5928       6780    1/10            0
  7          0          0       6351       6780    1/10            0

    class-map:prec_67 (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match:ip precedence 6  7
      queue size 0, queue limit 0
      packet output 0, packet drop 0
      tail/random drop 0, no buffer drop 0, other drop 0
      bandwidth:class-based wfq, weight 25
      random-detect:
        Exp-weight-constant:9 (1/512)
        Mean queue depth:0
  Class Random       Tail    Minimum    Maximum     Mark      Output
          drop       drop  threshold  threshold  probability packets
  0          0          0          0          0    1/10            0
  1          0          0          0          0    1/10            0
  2          0          0          0          0    1/10            0
  3          0          0          0          0    1/10            0
  4          0          0          0          0    1/10            0
  5          0          0          0          0    1/10            0
  6          0          0          0          0    1/10            0
  7          0          0          0          0    1/10            0

    class-map:class-default (match-any)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match:any
        0 packets, 0 bytes
        5 minute rate 0 bps
      queue size 0, queue limit 4068
      packet output 90, packet drop 0
      tail/random drop 0, no buffer drop 0, other drop 0
Device5#
Device5# show queueing interface fa1/1/0
```

```
Interface FastEthernet1/1/0 queueing strategy:VIP-based fair queueing
  FastEthernet1/1/0 queue size 0
         pkts output 2756, wfq drops 0, nobuffer drops 0
  WFQ:aggregate queue limit 13561 max available buffers 13561

      Class 0:weight 30 limit 4068 qsize 0 pkts output 97 drops 0
      Class 2:weight 10 limit 1356 qsize 0 pkts output 522 drops 0
      Class 3:weight 15 limit 0 qsize 0 pkts output 0 drops 0
      Class 4:weight 20 limit 2712 qsize 0 pkts output 2137 drops 0
      Class 5:weight 25 limit 0 qsize 0 pkts output 0 drops 0 \
```

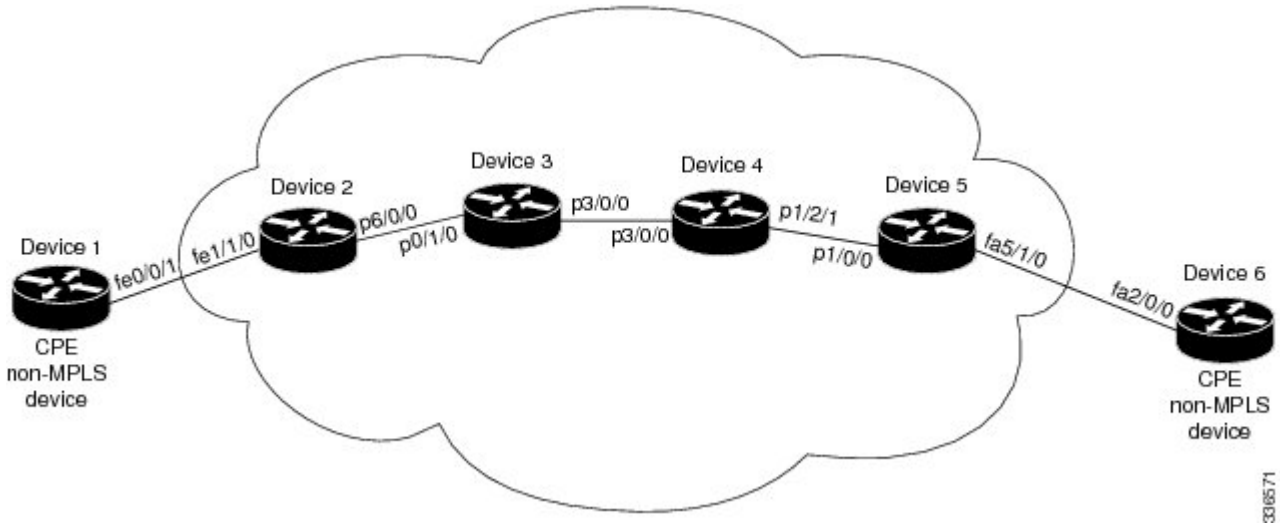
次の作業

-

MPLS Quality of Service の設定例

設定例は次の図に示すサンプル ネットワーク トポロジに基づいています。

図 *21*：デバイス インターフェイスの *MPLS CoS* を設定するためのサンプル ネットワーク トポロジ



例：Cisco Express Forwarding の設定

MPLS CoS が動作するためには、マルチプロトコル ラベル スイッチング（MPLS）ネットワークのすべてのデバイスで Cisco Express Forwarding が稼働している必要があります。Cisco Express Forwarding を有効にするには、次のいずれかのコマンドを使用します。

```
Device(config)# ip cef
```

または

```
Device(config)# ip cef distributed
```

例：デバイス 1 での IP の実行

次のコマンドによって、デバイス 1 で IP ルーティングが有効になります。この図のすべてのデバイスでは IP が有効になっている必要があります。デバイス 1 は、マルチプロトコル ラベル スイッチング（MPLS）ネットワークの一部ではありません。

```
!
ip routing
!
hostname R1
!
interface Loopback0
 ip address 10.1.1.1 255.255.255.255
!
interface FastEthernet0/0/1
 ip address 10.0.0.1 255.0.0.0
!
router ospf 100
 network 10.0.0.0 0.255.255.255 area 100
 network 10.0.0.1 0.255.255.255 area 100
```

例：デバイス 2 での MPLS の実行

デバイス 2 はラベル エッジ ルータです。Cisco Express Forwarding およびマルチプロトコル ラベル スイッチング（MPLS）がこのデバイスで有効になっている必要があります。また、デバイス 2 とファスト イーサネット インターフェイス 1/1/3 で専用アクセス レート（CAR）が設定されています。ファスト イーサネット インターフェイス 1/1/0 で使用される CAR ポリシーは、アクセスリスト 101 と一致する着信トラフィックに適用されます。認定情報レート（この例では 496000）よりも小さいトラフィック レートは、IP プレシデンス 4 で送信されます。それ以外の場合、このトラフィックは IP プレシデンス 0 で送信されます。

```
!
ip routing
!
hostname R2
!
ip cef
mpls ip
tag-switching advertise-tags
!
interface Loopback0
 ip address 10.10.10.10 255.255.255.255
!
interface FastEthernet1/1/0
 ip address 10.0.0.2 255.0.0.0
 rate-limit input access-group 101 496000 32000 64000 conform-action set-prec-transmit 4
exceed-action set-prec-transmit 0
!
interface POS6/0/0
 ip address 10.0.0.1 255.0.0.0
 mpls label protocol ldp
 mpls ip
 random-detect
 clock source internal
!
router ospf 100
 network 10.0.0.0 0.255.255.255 area 100
 network 10.1.0.0 0.255.255.255 area 100
 network 11.0.1.0 0.255.255.255 area 100
!
access-list 101 permit ip host 10.10.1.1 any
```

例：デバイス 3 での MPLS の実行

デバイス 3 ではマルチプロトコル ラベル スイッチング（MPLS）が稼働しています。Cisco Express Forwarding と MPLS がこのデバイスで有効になっている必要があります。

```
!
ip routing
mpls ip
tag-switching advertise-tags
!
hostname R3
!
interface Loopback0
 ip address 10.10.10.10 255.255.255.255
!
interface POS0/1/0
 ip address 10.0.0.2 255.0.0.0
 mpls label protocol ldp
 mpls ip
 crc 16
!
interface POS3/0/0
 ip address 10.0.0.1 255.0.0.0
 mpls label protocol ldp
 mpls ip
 crc 16
 clock source internal
 tx-cos stm16-rx
!
router ospf 100
 network 10.0.1.0 0.255.255.255 area 100
 network 10.0.0.1 0.255.255.255 area 100
 network 10.1.0.0 0.255.255.255 area 100
!
cos-queue-group stm16-rx
 precedence 0 random-detect-label 0
 precedence 0 queue 0
 precedence 1 queue 1
 precedence 1 random-detect-label 1
 precedence 2 queue 2
 precedence 2 random-detect-label 2
 precedence 3 random-detect-label 2
 precedence 4 random-detect-label 2
 precedence 5 random-detect-label 2
 precedence 6 random-detect-label 2
 precedence 7 queue low-latency
 precedence 7 random-detect-label 2
 random-detect-label 0 250 1000 1
 random-detect-label 1 500 1250 1
 random-detect-label 2 750 1500 1
 queue 0 50
 queue 1 100
 queue 2 150
 queue low-latency alternate-priority 500
```

例：デバイス 4 での MPLS の実行

デバイス 4 ではマルチプロトコル ラベル スイッチング（MPLS）が稼働しています。Cisco Express Forwarding と MPLS がこのデバイスで有効になっている必要があります。

```
!
ip routing
mpls ip
tag-switching advertise-tags
!
```

```
hostname R4
!
interface Loopback0
 ip address 10.0.0.0 255.255.255.255
!
interface POS1/2/1
 ip address 10.0.0.1 255.0.0.0
 mpls label protocol ldp
 mpls ip
 crc 16
 clock source internal
 tx-cos stm16-rx
!
router ospf 100
 network 10.0.0.0 0.255.255.255 area 100
 network 10.1.0.0 0.255.255.255 area 100
 network 10.0.1.0 0.255.255.255 area 100
!
cos-queue-group stm16-rx
 precedence 0 queue 0
 precedence 0 random-detect-label 0
 precedence 1 queue 1
 precedence 1 random-detect-label 1
 precedence 2 queue 2
 precedence 2 random-detect-label 2
 precedence 3 random-detect-label 2
 precedence 4 random-detect-label 2
 precedence 5 random-detect-label 2
 precedence 6 random-detect-label 2
 precedence 7 queue low-latency
 random-detect-label 0 250 1000 1
 random-detect-label 1 500 1250 1
 random-detect-label 2 750 1500 1
 queue 0 50
 queue 1 100
 queue 2 150
 queue low-latency alternate-priority 200
```

例：デバイス 5 での MPLS の実行

デバイス 5 ではマルチプロトコル ラベル スイッチング（MPLS）が稼働しています。Cisco Express Forwarding と MPLS がこのデバイスで有効になっている必要があります。デバイス 5 では、ファストイーサネットインターフェイス 5/1/0 でクラスベース重み付け均等化キューイング（CBWFQ）が有効になっています。次の例では、クラスマップが作成され、パケットがさまざまな IP プレシデンス値とマッチングされます。その後これらのクラス マップはポリシー マップ「outputmap」で使用され、CBWFQ が各クラスに割り当てられます。最後に、このポリシー マップがアウトバウンド ファスト イーサネット インターフェイス 5/1/0 に割り当てられます。

```
!
ip routing
mpls ip
tag-switching advertise-tags
!
hostname R5
!
!
class-map match-all prec_01
  match ip precedence 0  1
class-map match-all prec_23
  match ip precedence 2  3
class-map match-all prec_45
  match ip precedence 4  5
class-map match-all prec_67
  match ip precedence 6  7
!
!
```

```
policy-map outputmap
  class prec_01
    bandwidth 10000
    random-detect
  class prec_23
    bandwidth 15000
    random-detect
  class prec_45
    bandwidth 20000
    random-detect
  class prec_67
    bandwidth 25000
    random-detect
!
ip cef distributed
!
interface Loopback0
 ip address 10.0.0.0 255.255.255.255
 no ip directed-broadcast
!
interface POS1/1/0
 ip address 10.0.0.2 255.0.0.0
 ip route-cache distributed
 mpls label protocol ldp
 mpls ip
!
interface FastEthernet5/1/0
 ip address 10.0.0.1 255.0.0.0
 ip route-cache distributed
 full-duplex
 service-policy output outputmap
!
router ospf 100
 network 10.1.0.0 0.255.255.255 area 100
 network 10.0.1.0 0.255.255.255 area 100
 network 10.0.0.1 0.255.255.255 area 100
```

例：デバイス 6 での IP の実行

デバイス 6 では IP が稼働しています。Cisco Express Forwarding がこのデバイスで有効になっている必要があります。デバイス 6 は、マルチプロトコル ラベル スイッチング（MPLS）ネットワークの一部ではありません。

```
!
ip routing
!
hostname R6
!
ip cef distributed
!
interface Loopback0
 ip address 10.0.0.0 255.255.255.255
!
interface FastEthernet2/0/0
 ip address 10.0.0.2 255.0.0.0
 ip route-cache distributed
 full-duplex
!
router ospf 100
 network 10.0.0.0 0.255.255.255 area 100
 network 10.1.0.0 0.255.255.255 area 100
!
```

MPLS Quality of Service に関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
MPLS QoS コマンド	『Cisco IOS Quality of Service Solutions Command Reference』 『Cisco IOS Multiprotocol Label Switching Command Reference』

MIB

MIB	MIB のリンク
• CISCO-WRED-MIB • CISCO-CAR-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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。	http://www.cisco.com/support

MPLS Quality of Service の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、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。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *18*：*MPLS Quality of Service* の機能情報

機能名	リリース	機能情報
MPLS Quality of Service	12.0(5)T 12.0(11)T 12.0(22)S 12.2(17b)SXA 12.2(8)T Cisco IOS XE Release 2.1	MPLS Quality of Service 機能（旧称：MPLS CoS 機能）により、MPLS ネットワーク上で差別化サービスを提供できます。さまざまなネットワーキング要件を満たすため、各送信 IP パケットに適用可能なサービスクラスを指定できます。IP パケットに対して異なるサービスクラスを設定するには、各パケットのヘッダーに IP precedence ビットを設定します。 追加または変更されたコマンドはありません。

第 8 章

L2VPN ATM PVP での QoS ポリシー サポート

この機能により、レイヤ 2 バーチャル プライベート ネットワーク（L2VPN）に対し ATM 相手先固定パス（PVP）モードで Quality of Service（QoS）サービス ポリシーを設定できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース 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、機能情報の表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シスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

L2VPN ATM PVP での QoS ポリシー サポートの前提条件

L2VPN ATM PVP で QoS ポリシーを設定する前に、次のドキュメントで説明する概念および設定手順について理解しておく必要があります。

- Any Transport over MPLS
- MQC を使用した QoS 機能の適用

L2VPN ATM PVP での QoS ポリシー サポートの制約事項

- キューイング ベース ポリシーは、同じメイン インターフェイスで同時に ATM PVP モードと仮想回線（VC）モードではサポートされません。ただし、非キューイング ポリシーは混在できます。たとえば、PVP モードで非キューイング ポリシーを設定し、同じメイン インターフェイスの VC モードでキューイング ポリシーを設定できます。同様に、PVP モードでキューイング ポリシーを設定し、入力または出力方向の VC モードで非キューイング ポリシーを設定できます。
- ATM PVP モードでは、セッションはサポートされていません。
- PVP モードでポリシーを有効にする場合、PVP の一部となる VC で ATM レートは設定しないでください。VC は、未指定ビット レート（UBR）VC だけにする必要があります。
- VC が、ポリシーが設定されている PVP の一部となる場合、ATM VC トラフィック シェーピングは設定できません。
- キューイング ポリシーは、UBR の ATM PVP では設定できません。
- キューイング ベース ポリシーは UBR トラフィック シェーピングでは設定できません。

L2VPN ATM PVP での QoS ポリシー サポートに関する情報

MQC 構造

MQC 構造を使用すると、トラフィック クラスの定義、トラフィック ポリシーの作成、およびインターフェイスへのトラフィック ポリシーの適用が可能になります。

MQC 構造は、大きく次の 3 つの手順からなります。

手順の概要

1. **class-map** コマンドを使用して、トラフィック クラスを定義します。トラフィック クラスは、トラフィックの分類に使用します。
2. **policy-map** コマンドを使用して、トラフィック ポリシーを作成します。（トラフィック ポリシーとポリシー マップという用語は、多くの場合同じ意味で使用されます）。トラフィック ポリシー（ポリシー マップ）には、1 つのトラフィック クラスと、トラフィック クラスに適用する 1 つ以上の QoS 機能を含めます。トラフィック ポリシー内の QoS 機能によって、分類されたトラフィックの処理方法が決まります。
3. **service-policy** コマンドを使用して、トラフィック ポリシー（ポリシーマップ）をインターフェイスにアタッチします。

手順の詳細

ステップ 1 **class-map** コマンドを使用して、トラフィック クラスを定義します。トラフィック クラスは、トラフィックの分類に使用します。

ステップ 2 **policy-map** コマンドを使用して、トラフィック ポリシーを作成します。（トラフィック ポリシーとポリシーマップという用語は、多くの場合同じ意味で使用されます）。トラフィック ポリシー（ポリシーマップ）には、1 つのトラフィック クラスと、トラフィック クラスに適用する 1 つ以上の QoS 機能を含めます。トラフィック ポリシー内の QoS 機能によって、分類されたトラフィックの処理方法が決まります。

ステップ 3 **service-policy** コマンドを使用して、トラフィック ポリシー（ポリシー マップ）をインターフェイスにアタッチします。

トラフィック クラスの要素

トラフィック クラスに含まれる 3 つの主な要素は、トラフィック クラス名、一連の match コマンド、トラフィック クラスで複数の match コマンドが使用される場合に match コマンドを評価する方法です。

match コマンドは、パケットを分類するために使用します。パケットがチェックされ、match コマンドで指定された条件を満たすかどうかが判断されます。パケットが指定された条件を満たしている場合、パケットはそのクラスのメンバーと見なされます。一致条件を満たしていないパケットは、デフォルト トラフィック クラスのメンバーとして分類されます。

トラフィック ポリシーの要素

トラフィック ポリシーには、トラフィック ポリシー名、トラフィック クラス（class コマンドで指定します）、QoS 機能をイネーブルにするために使用するコマンドの、3 つの要素が含まれています。

ポリシー マップをインターフェイスに適用すると（service-policy コマンドを使用します）、トラフィック ポリシー（ポリシー マップ）は、イネーブルにした QoS 機能をトラフィック クラスに適用します。

（注） パケットは、トラフィック ポリシー内のいずれかのトラフィック クラスだけに一致します。パケットがトラフィック ポリシー内の複数のトラフィック クラスに一致する場合、ポリシーで定義されている最初のトラフィック クラスが使用されます。

L2VPN ATM PVP での QoS ポリシー サポートの設定方法

ATM PVP モードでのサービス ポリシーの有効化

ATM PVP モードでサービス ポリシーをイネーブルにできます。また、マルチポイント サブインターフェイス上で PVP に対するサービス ポリシーを有効にすることもできます。

（注） **show policy-map interface** コマンドは、ATM インターフェイスのサービス ポリシー情報を表示しません。

>

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfaceatm***slot*/*subslot*/*port*[**.** *subinterface*]
4. **atmpvp***vpi***l2transport**
5. **service-policy** [**input** | **output**] *policy-map-name*
6. **xconnect***peer-router-idvcid*encapsulation mpls
7. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 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	**interfaceatm***slot*/*subslot*/*port*[**.** *subinterface*] 例： `Router(config)# interface atm1/0/0`	インターフェイスを定義し、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	**atmpvp***vpi***l2transport** 例： `Router(config-if)# atm pvp 1 l2transport`	PVP を ATM セルの転送専用にすることを指定し、l2transport PVP コンフィギュレーション モードを開始します。 • **l2transport** キーワードは、PVP がセルリレー用であることを示します。このモードは、レイヤ 2 トランスポート専用です。通常の PVP 用ではありません。
ステップ 5	**service-policy** [**input** | **output**] *policy-map-name* 例： `Router(config-if-atm-l2trans-pvp)# service policy input pol1`	指定された PVP のサービス ポリシーを有効にします。
ステップ 6	**xconnect***peer-router-idvcid*encapsulation mpls 例： `Router(config-if-atm-l2trans-pvp)# xconnect 10.0.0.1 123 encapsulation mpls`	接続回線を擬似接続 VC にバインドします。 • このコマンドの構文は、その他のレイヤ 2 トランスポートの場合と同じです。

ステップ 7	**end**
	
	例：
	
	`Router(config-if-atm-l2trans-pvp)#`
	
	`end`
		l2transport PVP コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した ATM PVP モードでのサービス ポリシーの有効化

ATM PVP モードでサービス ポリシーをイネーブルにできます。また、マルチポイント サブインターフェイス上で PVP に対するサービス ポリシーを有効にすることもできます。

（注） **show policy-map interface** コマンドは、ATM インターフェイスのサービス ポリシー情報を表示しません。

>

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfaceatm***slot*/*subslot*/*port*[**.***subinterface*]
4. **atmpvp***vpi***l2transport**
5. **service-policy** [**input** | **output**] *policy-map-name*
6. **end**
7. **interfacepseudowire***number*
8. **encapsulationmpls**
9. **neighbor***peer-addressvcid-value*
10. **exit**
11. **l2vpn xconnectcontext***context-name*
12. **member pseudowire***interface-number*
13. **member gigabitethernet***interface-number*
14. **end**
15. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 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	**interfaceatm***slot*/*subslot*/*port*[**.***subinterface*] 例： `Router(config)# interface atm1/0/0`	インターフェイスを定義し、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	**atmpvp***vpi***l2transport** 例： `Router(config-if)# atm pvp 1 l2transport`	PVP を ATM セルの転送専用にすることを指定し、l2transport PVP コンフィギュレーション モードを開始します。 • **l2transport** キーワードは、PVP がセルリレー用であることを示します。このモードは、レイヤ 2 トランスポート専用です。通常の PVP 用ではありません。
ステップ 5	**service-policy** [**input** | **output**] *policy-map-name* 例： `Router(config-if-atm-l2trans-pvp)# service policy input pol1`	指定された PVP のサービス ポリシーを有効にします。
ステップ 6	**end** 例： `Router(config-if-atm-l2trans-pvp)# end`	特権 EXEC モードに戻ります。
ステップ 7	**interfacepseudowire***number* 例： `Router(config)# interface pseudowire 100`	擬似回線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 8	**encapsulationmpls** 例： `Router(config-if)# encapsulation mpls`	マルチプロトコル ラベル スイッチング（MPLS）がデータ カプセル化方式として使用されることを指定します。

	コマンドまたはアクション	目的
ステップ 9	**neighbor***peer-addressvcid-value* 例： `Router(config-if)# neighbor 10.0.0.1 123`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 10	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 11	**l2vpn xconnectcontext***context-name* 例： `Router(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect コンフィギュレーション モードを開始します。
ステップ 12	**member pseudowire***interface-number* 例： `Router(config-xconnect)# member pseudowire 100`	Layer 2 VPN（L2VPN）クロス コネクトを形成するようにメンバー擬似回線を指定します。
ステップ 13	**member gigabitethernet***interface-number* 例： `Router(config-xconnect)# member GigabitEthernet0/0/0.1`	ギガビット イーサネット メンバー インターフェイスのロケーションを指定します。
ステップ 14	**end** 例： `Router(config-xconnect)# end`	特権 EXEC モードに戻ります。

ステップ 15	**end**
	
	例：
	
	`Router(config-xconnect)#`
	
	`end`
		xconnecrt コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

ATM PVP モードでのトラフィック シェーピングの有効化

トラフィック シェーピング コマンドは、PVP モードでサポートされます。出力 VP シェーピングでは、ATM サービス カテゴリごとに 1 つずつのコンフィギュレーション コマンドがサポートされます。サポートされるサービス カテゴリは、Constant Bit Rate（CBR）、Variable Bit Rate-NonReal Time（VBR-NRT）、および Variable Bit Rate Real-Time（VBR-RT）です。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfaceatm***slot*/*subslot*/*port*[**.***subinterface*]
4. **atmpvp***vpi***l2transport**
5. 次のいずれかを実行します。
   - **ubr***pcr*
   -
   - **cbr***pcr*
   - または
   - **vbr-nrt***pcrscrmbs*
   - または
   - **vbr-rt***pcrscrmbs*
6. **xconnect***peer-router-idvcid*encapsulation mpls

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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。

	コマンドまたはアクション	目的
ステップ 3	**interfaceatm***slot*/*subslot*/*port*[**.***subinterface*] 例： `Router(config)# interface atm1/0/0`	インターフェイスを定義し、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	**atmpvp***vpi***l2transport** 例： `Router(config-if)# atm pvp 1 l2transport`	PVP を ATM セルの転送専用にすることを指定し、l2transport PVP コンフィギュレーション モードを開始します。 • **l2transport** キーワードは、PVP がセルリレー用であることを示します。このモードは、レイヤ 2 トランスポート専用です。通常の PVP 用ではありません。
ステップ 5	次のいずれかを実行します。 • **ubr***pcr* • • **cbr***pcr* • または • **vbr-nrt***pcrscrmbs* • または • **vbr-rt***pcrscrmbs* 例： `Router(config-if-atm-l2trans-pvp)# cbr 1000`	ATM PVP モードでトラフィック シェーピングをイネーブルにします。 • *pcr* = ピーク セル レート • *scr* = 平均セル レート • *mbs* = 最大バースト サイズ
ステップ 6	**xconnect***peer-router-idvcid*encapsulation mpls 例： `Router(config-if-atm-l2trans-pvp)# xconnect 10.0.0.1 123 encapsulation mpls`	接続回線を擬似接続 VC にバインドします。 • このコマンドの構文は、その他のレイヤ 2 トランスポートの場合と同じです。

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した ATM PVP モードでのトラフィック シェーピングの有効化

トラフィック シェーピング コマンドは、PVP モードでサポートされます。出力 VP シェーピングでは、ATM サービス カテゴリごとに 1 つずつのコンフィギュレーション コマンドがサポートされます。サポートされるサービス カテゴリは、Constant Bit Rate（CBR）、Variable Bit Rate-NonReal Time（VBR-NRT）、および Variable Bit Rate Real-Time（VBR-RT）です。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfaceatm***slot*/*subslot*/*port*[**.***subinterface*]
4. **atmpvp***vpi***l2transport**
5. 次のいずれかを実行します。
   - **ubr***pcr*
   -
   - **cbr***pcr*
   - または
   - **vbr-nrt***pcrscrmbs*
   - または
   - **vbr-rt***pcrscrmbs*
6. **end**
7. **interfacepseudowire***number*
8. **encapsulationmpls**
9. **neighbor***peer-addressvcid-value*
10. **exit**
11. **l2vpn xconnectcontext***context-name*
12. **member pseudowire***interface-number*
13. **member gigabitethernet***interface-number*
14. **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	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Router> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**interfaceatm***slot*/*subslot*/*port*[**.***subinterface*] 例： `Router(config)# interface atm1/0/0`	インターフェイスを定義し、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	**atmpvp***vpi***l2transport** 例： `Router(config-if)# atm pvp 1 l2transport`	PVP を ATM セルの転送専用にすることを指定し、l2transport PVP コンフィギュレーション モードを開始します。 • **l2transport** キーワードは、PVP がセルリレー用であることを示します。このモードは、レイヤ 2 トランスポート専用です。通常の PVP 用ではありません。
ステップ 5	次のいずれかを実行します。 • **ubr***pcr* • • **cbr***pcr* • または • **vbr-nrt***pcrscrmbs* • または • **vbr-rt***pcrscrmbs* 例： `Router(config-if-atm-l2trans-pvp)# cbr 1000`	ATM PVP モードでトラフィック シェーピングをイネーブルにします。 • *pcr* = ピーク セル レート • *scr* = 平均セル レート • *mbs* = 最大バースト サイズ

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Router(config-if-atm-l2trans-pvp)# end`	特権 EXEC モードに戻ります。
ステップ 7	**interfacepseudowire***number* 例： `Router(config)# interface pseudowire 100`	擬似回線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 8	**encapsulationmpls** 例： `Router(config-if)# encapsulation mpls`	マルチプロトコル ラベル スイッチング（MPLS）がデータ カプセル化方式として使用されることを指定します。
ステップ 9	**neighbor***peer-addressvcid-value* 例： `Router(config-if)# neighbor 10.0.0.1 123`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 10	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 11	**l2vpn xconnectcontext***context-name* 例： `Router(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect コンフィギュレーション モードを開始します。
ステップ 12	**member pseudowire***interface-number* 例： `Router(config-xconnect)# member pseudowire 100`	Layer 2 VPN（L2VPN）クロス コネクトを形成するようにメンバー擬似回線を指定します。
ステップ 13	**member gigabitethernet***interface-number* 例： `Router(config-xconnect)# member GigabitEthernet0/0/0.1`	ギガビット イーサネット メンバー インターフェイスのロケーションを指定します。

	コマンドまたはアクション	目的
ステップ 14	**end** 例： `Router(config-xconnect)# end`	特権 EXEC モードに戻ります。

L2VPN プロトコルベースの CLI 機能に関連するコマンドを使用した、ATM PVP モードでのトラフィック シェーピングの有効化の例

次に、ATM PMP モードでトラフィック シェーピングをイネーブルにする例を示します。

```
interface atm 1/0
 atm pvp 100 l2transport
  ubr 1000
  xconnect 10.11.11.11 777 encapsulation mpls
 atm pvp 101 l2transport
  cbr 1000
  xconnect 10.11.11.11 888 encapsulation mpls
 atm pvp 102 l2transport
  vbr-nrt 1200 800 128
  xconnect 10.11.11.11 999 encapsulation mpls
```

ATM VCI の照合の有効化

クラス マップ コンフィギュレーション モードで **match atm-vci** コマンドを使用して、ATM VCI または VCI の範囲を照合できます。

（注） **match atm-vci** コマンドをクラス マップ コンフィギュレーション モードで設定すると、このクラス マップを ATM VP だけにアタッチ可能なポリシー マップに追加できます。

>

手順の概要

1. イネーブル化
2. **configureterminal**
3. **class-map***class-map-name* [**match-all** | **match-any**]
4. **matchatm-vci***vc-id***[-vc-id]**
5. **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	**イネーブル化** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**class-map***class-map-name* [**match-all** | **match-any**] 例： `Router(config)# class-map class1`	トラフィックを指定したクラスにマッチングするために使用するクラス マップを作成し、クラス マップ 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	**matchatm-vci***vc-id***[-vc-id]** 例： `Router(config-cmap)# match atm-vci 50`	ATM VCI または VCI の範囲のパケット照合を有効にします。指定できる範囲は 32 ～ 65535 です。 （注） **match not** コマンドを使用して、一致条件を削除できます。
ステップ 5	**end** 例： `Router(config-cmap)# end`	（任意）特権 EXEC モードに戻ります。

L2VPN ATM PVP での QoS ポリシー サポートの設定例

例：ATM PVP モードでのトラフィック シェーピングの有効化

次に、ATM PMP モードでトラフィック シェーピングをイネーブルにする例を示します。

```
int atm 1/0/0
   atm pvp 100 l2transport
       ubr 1000
       xconnect 10.11.11.11 777 encapsulation mpls
   atm pvp 101 l2transport
       cbr 1000
```

```
        xconnect 10.11.11.11 888 encapsulation mpls
    atm pvp 102 l2transport
        vbr-nrt 1200 800 128
        xconnect 10.11.11.11 999 encapsulation mpls
```

例：ATM PVP モードでのトラフィック シェーピングの有効化（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

次に、ATM PMP モードでトラフィック シェーピングをイネーブルにする例を示します。

```
int atm 1/0/0
   atm pvp 100 l2transport
       ubr 1000
       interface pseudowire 100
       encapsulation mpls
       neighbor 10.0.0.1 123
!
l2vpn xconnect context A
 member pseudowire 100
 member g0/0/0.1
   atm pvp 101 l2transport
       cbr 1000
       interface pseudowire 100
       encapsulation mpls
       neighbor 10.0.0.1 123
!
l2vpn xconnect context A
 member pseudowire 100
 member g0/0/0.1
   atm pvp 102 l2transport
       vbr-nrt 1200 800 128
       interface pseudowire 100
       encapsulation mpls
       neighbor 10.0.0.1 123
!
l2vpn xconnect context A
 member pseudowire 100
 member g0/0/0.1
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
MPLS および MPLS アプリケーションに関連するコマンドの説明	『*Cisco IOS Multiprotocol Label Switching Command Reference*』
モジュラ Quality of Service（QoS）コマンドライン インターフェイス（CLI）（MQC）	MQC を使用した QoS 機能の適用
Any Transport over MPLS	Any Transport over MPLS

標準

規格	Title
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB の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 ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC の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	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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。	http://www.cisco.com/cisco/web/support/index.html

L2VPN ATM PVP での QoS ポリシー サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、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。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *19*：*L2VPN ATM PVP* での *QoS* ポリシー サポートの機能情報

機能名	リリース	機能情報
L2VPN ATM PVP での QoS ポリシー サポート	Cisco IOS XE Release 2.3	この機能により、レイヤ 2 バーチャル プライベート ネットワーク（L2VPN）に対し ATM 相手先固定パス（PVP）モードで Quality of Service（QoS）サービスポリシーを設定できます。 次のコマンドが導入または変更されました：**cbr**、**matchatm-vci**,**service-policy**,**ubr**、**vbr-nrt**,**vbr-rt**。
PVP 単位のセルベース ATM シェーピング	Cisco IOS XE Release 2.3	この機能は、Cisco ASR 1000 シリーズ アグリゲーション サービスルータで導入されました。

第 9 章

MPLS 擬似回線ステータス シグナリング

MPLS 擬似回線ステータス シグナリング機能により、接続回線がダウンしている場合でも擬似回線ステータスをピア ルータに送信できるようにルータを設定できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース 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、機能情報の表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シスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

MPLS 擬似回線ステータス シグナリングの前提条件

- この機能を設定する前に、両方のピア ルータが擬似回線ステータス メッセージを送受信できることを確認します。

MPLS 擬似回線ステータス シグナリングの制約事項

- 両方のピア ルータで、擬似回線ステータス メッセージをラベル アドバタイズメントおよびラベル通知メッセージで送受信できる必要があります。両方のピア ルータで擬似回線ステータス メッセージがサポートされていない場合は、**nostatus** コマンドでメッセージをディセーブルにすることをお勧めします。
- この機能は、Any Transport over MPLS（AToM）仮想回線接続性検証（VCCV）と統合されていません。
- この機能は、双方向フォワーディング検出（BFD）と統合されていません。
- IETF draft-muley-pwe3-redundancy-02.txt のスタンバイと必要なスイッチオーバー値はサポートされません。

MPLS 擬似回線ステータス シグナリングに関する情報

MPLS 擬似回線ステータス スイッチングの動作

ピアで MPLS 擬似回線ステータス シグナリング機能もサポートされる場合、擬似回線ステータス メッセージは、ラベル アドバタイズメントおよびラベル通知メッセージで送信されます。**showmplsl2transportvcdetail** コマンドを発行して、ローカル ルータとリモート ルータの両方で擬似回線ステータス メッセージがサポートされることを示すことができます。次に、検索する出力の行の例を示します。

```
Router# show mpls l2transport vc detail
.
.
.
status TLV support (local/remote): enabled/supported
```

L2VPN プロトコルベースの CLI 機能に関連するコマンドを使用した、MPLS 擬似回線ステータス スイッチングの仕組み

ピアで MPLS 擬似回線ステータス シグナリング機能もサポートされる場合、擬似回線ステータス メッセージは、ラベル アドバタイズメントおよびラベル通知メッセージで送信されます。**showl2vpnatomvcdetail** コマンドを発行して、ローカル ルータとリモート ルータの両方で擬似回線ステータス メッセージがサポートされることを示すことができます。次に、検索する出力の行の例を示します。

```
Device# show l2vpn atom vc detail
.
.
.
status TLV support (local/remote): enabled/supported
```

特定のルータで MPLS 擬似回線ステータス シグナリングがサポートされない場合

ピア ルータで、擬似回線ステータス メッセージをラベル アドバタイズメントおよびラベル通知メッセージで送受信できる必要があります。特定のルータで擬似回線ステータス メッセージがサポートされていない場合は、**nostatus** コマンドでメッセージをディセーブルにすることをお勧めします。これによって、ルータはラベル削除モードに戻ります。

ピアで MPLS 擬似回線ステータス シグナリング機能がサポートされない場合は、ローカル ルータは、操作モードをラベル回収モードに変更します。リモート ルータで擬似回線ステータス メッセージがサポートされないことを示すには、**showmplsl2transportvcdetail** コマンドを発行できます。次に、検索する出力の行の例を示します。

```
Router# show mpls l2transport vc detail
.
.
.
status TLV support (local/remote): enabled/not supported
```

次の **debug mpls l2transport vc** コマンドを発行すると、次の例で太字で示されているように、ピア ルータが MPLS 擬似回線ステータス シグナリング機能をサポートしていないこと、またローカル ルータが回収モードに変更されることがメッセージに示されます。

Router# debug mpls l2transport vc event Router# **debugmplsl2transportvcstatuseventRouter# debugmplsl2transportvcstatusfsmRouter# debugmplsl2transportvcldp**

*Feb 26 13:41:40.707: AToM LDP [10.1.1.2]: Sending label withdraw msg *Feb 26 13:41:40.707: AToM LDP [10.1.1.2]: VC Type 5, mtu 1500 *Feb 26 13:41:40.707: AToM LDP [10.1.1.2]: VC ID 100, label 18 *Feb 26 13:41:40.707: AToM LDP [10.1.1.2]: Status 0x0000000A [PW Status NOT supported]

特定のルータで MPLS 擬似回線ステータス シグナリングがサポートされない場合（L2VPN プロトコルベースの CLI 機能に関連するコマンドを使用）

ピア ルータで、擬似回線ステータス メッセージをラベル アドバタイズメントおよびラベル通知メッセージで送受信できる必要があります。特定のルータで擬似回線ステータス メッセージがサポートされていない場合は、**nostatus** コマンドでメッセージをディセーブルにすることをお勧めします。これによって、ルータはラベル削除モードに戻ります。

ピアで MPLS 擬似回線ステータス シグナリング機能がサポートされない場合は、ローカル ルータは、操作モードをラベル回収モードに変更します。リモート ルータで擬似回線ステータス メッセージがサポートされないことを示すには、**show l2vpn atom vc detail** コマンドを発行できます。次に、検索する出力の行の例を示します。

```
Device# show l2vpn atom vc detail

.
.
.
status TLV support (local/remote): enabled/not supported
```

次の **debug l2vpn atom vc** コマンドを発行すると、次の例で示されているように、ピア ルータが MPLS 擬似回線ステータス シグナリング機能をサポートしていないこと、またローカル ルータが回収モードに変更されることがメッセージに示されます。

```
Device# debug l2vpn atom vc event
Device# debug l2vpn atom vc status event
Device# debug l2vpn atom vc status fsm
Device# debug l2vpn atom vc ldp

*Feb 26 13:41:40.707: AToM LDP [110.1.1.2]: Sending label withdraw msg
*Feb 26 13:41:40.707: AToM LDP [110.1.1.2]:   VC Type   5, mtu 1500
*Feb 26 13:41:40.707: AToM LDP [110.1.1.2]:   VC ID     100, label 18
*Feb 26 13:41:40.707: AToM LDP [110.1.1.2]:   Status 0x0000000A [PW Status NOT supported]
```

接続回線がダウンしていることを示すステータス メッセージ

2 つのルータ間の接続回線がダウンしている場合は、**show mpls l2transport vc detail** コマンドの出力には次のステータスが示されます。

```
Router# show mpls l2transport vc detail
.
.
.
Last remote LDP TLV    status rcvd: AC DOWN(rx,tx faults)
```

デバッグ メッセージには、コマンド出力の太字で示されているように、接続回線がダウンしたことが示されます。

Router# debug mpls l2transport vc event Router# **debug mpls l2transport vc status event** Router# **debug mpls l2transport vc status fsm** Router# **debug mpls l2transport vc ldp**

```
*Feb 26 11:51:42.427: AToM LDP [10.1.1.1]: Received notif msg, id 88
*Feb 26 11:51:42.427: AToM LDP [10.1.1.1]:   Status    0x00000007 [PW Status]
*Feb 26 11:51:42.427: AToM LDP [10.1.1.1]:   PW Status 0x00000006 [AC DOWN(rx,tx faults)]
```

他の擬似回線ステータス メッセージには、not-forwarding、pw-tx-fault、および pw-rx-fault があります。

L2VPN プロトコルベース CLI 機能に関連するコマンドを使用した接続回線がダウンしていることを示すステータス メッセージ

2 つのルータ間の接続回線がダウンしている場合は、**show l2vpn atom vc detail** コマンドの出力には次のステータスが示されます。

```
Device# show l2vpn atom vc detail
.
.
.
Last remote LDP TLV    status rcvd: AC DOWN(rx,tx faults)
```

デバッグ メッセージには、コマンド出力の太字で示されているように、接続回線がダウンしたことが示されます。

```
Device# debug l2vpn atom  vc event
Device# debug l2vpn atom  vc status event
Device# debug l2vpn atom vc status fsm
Device# debug l2vpn atom vc ldp
```

```
*Feb 26 11:51:42.427: AToM LDP [10.1.1.1]: Received notif msg, id 88
*Feb 26 11:51:42.427: AToM LDP [10.1.1.1]:   Status    0x00000007 [PW Status]
*Feb 26 11:51:42.427: AToM LDP [10.1.1.1]:   PW Status 0x00000006 [AC DOWN(rx,tx faults)]
```

他の擬似回線ステータス メッセージには、not-forwarding、pw-tx-fault、および pw-rx-fault があります。

擬似回線ステータス メッセージのメッセージ コード

debug mpls l2transport vc コマンドと **show mpls l2transport vc detail** コマンドを使用すると、メッセージ コードが含まれた出力が示されます。次に例を示します。

```
    Label/status state machine: established, LruRru

AToM MGR [10.9.9.9, 100]: S:Evt local up, LndRru->LnuRru
```

メッセージ コード（LruRru、LndRru、および LnuRru）は、ローカル ルータとリモート ルータのステータスを示します。次のキーを使用して、メッセージ コードを解釈できます。

- L：ローカル ルータ
- R：リモート ルータ
- r または n：受信可能（r）または受信不可（n）
- u または d：アップ（u）またはダウン（d）ステータス

出力には他の値も含まれています。

- D：データプレーン
- S：ローカル シャットダウン

L2VPN プロトコルベース CLI 機能に関連するコマンドを使用した擬似回線ステータス メッセージのメッセージ コード

debug l2vpn atom vc コマンドと **show l2vpn atom vc detail** コマンドを使用すると、メッセージ コードが含まれた出力が示されます。次に例を示します。

```
    Label/status state machine: established, LruRru

AToM MGR [10.9.9.9, 100]: S:Evt local up, LndRru->LnuRru
```

メッセージ コード（LruRru、LndRru、および LnuRru）は、ローカル ルータとリモート ルータのステータスを示します。次のキーを使用して、メッセージ コードを解釈できます。

L：ローカル ルータ

R：リモート ルータ

r または n：受信可能（r）または受信不可（n）

u または d：アップ（u）またはダウン（d）ステータス

出力には他の値も含まれています。

D：データプレーン

S：ローカル シャットダウン

MPLS 擬似回線ステータス シグナリングの設定方法

MPLS 擬似回線ステータス シグナリングの有効化

接続回線がダウンしている場合でもルータが擬似回線ステータスをピア ルータに送信できるようにするには、次の作業を実行します。両方のルータで擬似回線ステータス メッセージがサポートされていない場合は、**nostatus** コマンドでメッセージを無効にします。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **pseudowire-class***name*
4. **status**
5. **encapsulationmpls**
6. **exit**
7. **exit**
8. **showmplsl2transportvcdetail**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**pseudowire-class***name* 例： `Router(config)# pseudowire-class atom`	指定した名前の擬似回線クラスを確立して、擬似回線クラス コンフィギュレーション モードに入ります。

	コマンドまたはアクション	目的
ステップ 4	**status** 例： `Router(config-pw)# status`	（任意）ルータがラベル アドバタイズメントとラベル通知メッセージを通して擬似回線ステータス メッセージをピア ルータに送信できるようにします。 （注） デフォルトでは、ステータスメッセージはイネーブルです。この手順は、ステータスメッセージが無効になっている場合にのみ実行します。 両方のピア ルータでこの機能がサポートされていないためにステータス メッセージを無効にする必要がある場合は、**nostatus** コマンドを入力します。
ステップ 5	**encapsulationmpls** 例： `Router(config-pw)# encapsulation mpls`	トンネリング カプセル化を指定します。
ステップ 6	**exit** 例： `Router(config-pw)# exit`	擬似回線 クラス コンフィギュレーション モードを終了します。
ステップ 7	**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。
ステップ 8	**showmplsl2transportvcdetail** 例： `Router# show mpls l2transport vc detail`	擬似回線メッセージを送受信できることを検証します。

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した MPLS 擬似回線ステータス シグナリングの有効化

接続回線がダウンしている場合でもルータが擬似回線ステータスをピア ルータに送信できるようにするには、次のタスクを実行します。両方のルータで擬似回線ステータス メッセージがサポートされていない場合は、**nostatus** コマンドでメッセージを無効にします。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface pseudowire***number*
4. **status**
5. **encapsulationmpls**
6. **neighbor***peer-address vcid-value*
7. **exit**
8. **exit**
9. **showl2vpnatomvcdetail**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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 pseudowire***number* 例： `Device(config)# interface pseudowire 1`	指定した値でインターフェイス擬似回線を確立して、擬似回線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	**status** 例： `Device(config-pw)# status`	（任意）ルータがラベル アドバタイズメントとラベル通知メッセージを通して擬似回線ステータス メッセージをピア ルータに送信できるようにします。 （注） デフォルトでは、ステータス メッセージはイネーブルです。この手順は、ステータス メッセージが無効になっている場合にのみ実行します。 両方のピア ルータでこの機能がサポートされていないためにステータス メッセージを無効にする必要がある場合は、**nostatus** コマンドを入力します。

	コマンドまたはアクション	目的
ステップ 5	**encapsulationmpls** 例： `Device(config-pw)# encapsulation mpls`	トンネリング カプセル化を指定します。
ステップ 6	**neighbor***peer-address vcid-value* 例： `Device(config-pw)# neighbor 10.0.0.1 123`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 7	**exit** 例： `Device(config-pw)# exit`	擬似回線 クラス コンフィギュレーション モードを終了します。
ステップ 8	**exit** 例： `Device(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。
ステップ 9	**showl2vpnatomvcdetail** 例： `Device# show l2vpn atom vc detail`	擬似回線メッセージを送受信できることを検証します。

MPLS 擬似回線ステータス シグナリングの設定例

例：MPLS 擬似回線ステータス シグナリング

次に、2 台の PE ルータで MPLS 擬似回線ステータス シグナリング機能を設定する例を示します。デフォルトでは、ステータス メッセージはイネーブルです。この例では、**status** コマンドは、ステータス メッセージがディセーブルになっていた場合に必要です。

PE1

```
interface Loopback0
 ip address 10.1.1.1 255.255.255.255
```

```
!
pseudowire-class atomstatus
 encapsulation mpls
 status
!
interface GigabitEthernet0/0/1
 xconnect 10.1.1.2 123 pw-class atomstatus
```

PE2

```
interface Loopback0
 ip address 10.1.1.2 255.255.255.255
!
pseudowire-class atomstatus
 encapsulation mpls
 status
!
interface GigabitEthernet3/3/0
 xconnect 10.1.1.1 123 pw-class atomstatus
```

例：MPLS 擬似回線ステータス シグナリング（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

次に、2 台の PE ルータで MPLS 擬似回線ステータス シグナリング機能を設定する例を示します。デフォルトでは、ステータス メッセージはイネーブルです。この例では、**status** コマンドは、ステータス メッセージがディセーブルになっていた場合に必要です。

PE1

```
interface Loopback0
 ip address 10.1.1.1 255.255.255.255
!
template type pseudowire atomstatus
 encapsulation mpls
 status
!
interface pseudowire 100
 source template type pseudowire atomstatus
interface GigabitEthernet0/0/1
 service instance 300 ethernet
l2vpn xconnect context con1
 member GigabitEthernet2/1/1 service-instance 300
 member Pseudowire 100
```

PE2

```
interface Loopback0
 ip address 10.1.1.2 255.255.255.255
!
template type pseudowire atomstatus
 encapsulation mpls
 status
!
interface Pseudowire 100
 source template type pseudowire atomstatus
interface GigabitEthernet3/3/0
 service instance 300 ethernet
l2vpn xconnect context con1
 member GigabitEthernet2/1/1 service-instance 300
 member Pseudowire 100
```

例：両方のルータで擬似回線ステータスメッセージがサポートされることの確認

ローカル ルータとリモート ルータの両方で擬似回線ステータス メッセージがサポートされることを示すには、**show mpls l2transport vc detail** コマンドを発行できます。次に、検索する出力の行の例を示します。

```
Router# show mpls l2transport vc detail
.
.
.
status TLV support (local/remote): enabled/supported
```

例：両方のルータで擬似回線ステータスメッセージがサポートされることの確認（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

ローカル ルータとリモート ルータの両方で擬似回線ステータス メッセージがサポートされることを示すには、**show l2vpn atom vc detail** コマンドを発行できます。次に、検索する出力の行の例を示します。

```
Device# show l2vpn atom vc detail
.
.
.
status TLV support (local/remote): enabled/supported
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
MPLS および MPLS アプリケーションに関連するコマンドの説明	『*Cisco IOS Multiprotocol Label Switching Command Reference*』

関連項目	マニュアル タイトル
Any Transport over MPLS	Any Transport over MPLS

標準

規格	Title
draft-ietf-pwe3-control-protocol-15.txt	『Pseudowire Setup and Maintenance Using LDP』
draft-ietf-pwe3-iana-allocation-08.txt	『IANA Allocations for Pseudo Wire Edge to Edge Emulation (PWE3)』
draft-martini-pwe3-pw-switching-03.txt	『Pseudo Wire Switching』

MIB

MIB	MIB のリンク
イーサネット サービス、フレームリレー サービス、および ATM サービス用 Pseudowire Emulation Edge-to-Edge MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC の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	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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。	http://www.cisco.com/cisco/web/support/index.html

に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、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。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *20*：*MPLS* 擬似回線ステータス シグナリングの機能情報

機能名	リリース	機能情報
MPLS 擬似回線ステータス シグナリング	Cisco IOS XE Release 2.3	MPLS 擬似回線ステータス シグナリング機能により、接続回線がダウンしている場合でも擬似回線ステータスをピア ルータに送信できるようにルータを設定できます。 次のコマンドが導入または変更されました：**debugmplsl2transportvc**、**showmplsl2transportvc**、**status**（擬似回線クラス）。

第 10 章

L2VPN VPLS Inter-AS オプション B

L2VPN VPLS Inter-AS オプション B 機能は VPLS 自動検出の既存機能を拡張し、複数の Border Gateway Protocol（BGP）自律システムにわたって動作します。BGP をベースとしたオートディスカバリを基礎的なフレームワークとして使用する L2VPN VPLS Inter-AS オプション B 機能は、隣接する自律システム境界ルータ（ASBR）の間に、ダイナミックなマルチセグメント擬似回線（PW）コンフィギュレーションを作成します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース 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、機能情報の表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シスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

L2VPN VPLS Inter-AS オプション B の前提条件

L2VPN VPLS Inter-AS オプション B 機能は、VPLS 自動検出：BGP ベース機能を拡張します。たとえば、L2VPN VPLS Inter-AS オプション B 機能の結果として、ステートフル スイッチオーバー（SSO）およびノンストップ フォワーディング（NSF）が標準 VPLS 自動検出設定でサポートされます。

L2VPN VPLS Inter-AS オプション B 機能を設定する前に、VPLS 自動検出：BGP ベース機能をイネーブルにし、L2VPN VPLS Inter-AS オプション B で使用する VPLS 自動検出設定の変更，（408 ページ）で説明されている手順を実行します。

VPLS 自動検出：BGP ベース機能の詳細については、「VPLS Autodiscovery: BGP」モジュールを参照してください。

L2VPN VPLS Inter-AS オプション B の制約事項

Cisco IOS Release 15.1(1)S で導入された L2VPN VPLS Inter-AS オプション B 機能は、仮想プライベート LAN スイッチング（VPLS）を実行できるライン カードを搭載した Cisco 7600 シリーズ ルータでのみサポートされます。

L2VPN VPLS Inter-AS オプション B に関する情報

VPLS 機能と L2VPN VPLS Inter-AS オプション B

VPLS はマルチポイント レイヤ 2 VPN（L2VPN）であり、Ethernet over Multiprotocol Label Switching（EoMPLS）ブリッジング技法によって 2 つ以上のカスタマー デバイスを接続します。

VPLS Inter-AS では、さまざまなバリエーションやオプションがサポートされています（たとえば、オプション A、B、C、D）。L2VPN VPLS Inter-AS オプション B 機能は、オプション B のみをサポートし、RFC 4364（『BGP/MPLS IP Virtual Private Networks (VPNs)』）に準拠します。

VPLS の詳細については、ドキュメント『Configuring Multiprotocol Label Switching on the Optical Services Modules』のセクション「VPLS Overview」を参照してください。

L2VPN VPLS Inter-AS オプション B の説明

L2VPN VPLS Inter-AS オプション B 機能は、ASBR にまたがるマルチセグメント擬似回線を動的に作成することにより、複数の自律システム境界にまたがって VPLS を拡張します。

外部 BGP（eBGP）を持つルータがルートをその BGP ネイバーにアドバタイズするとき、ルータは送信元 IP アドレスをアドバタイズされるルートのネクスト ホップとして使用します。

内部 BGP（iBGP）を持つルータがルートをその BGP ネイバーにアドバタイズするとき、ルータはアドバタイズされるルートのネクスト ホップ指定を変更しません。L2VPN VPLS Inter-AS オプション B 機能では、ASBR で **neighbornext-hop-self** コマンドを入力します。これにより、擬似回線は強制的に ASBR への対象となり、プロバイダー エッジ（PE）ルータへの対象にはなりません。最終的には、最初の自律システムに対する擬似回線が、ASBR 間にある 3 番目の擬似回線を使用して、2 番目の自律システムに対する擬似回線に切り替えられます。このようにして、マルチセグメント化された擬似回線が作成されます。マルチセグメント化された擬似回線の詳細については、「L2VPN マルチセグメント擬似回線」モジュールを参照してください。

（注） L2VPN VPLS Inter-AS オプション B 機能はルート プロセッサ（RP）、SSO、および NSF をサポートします。

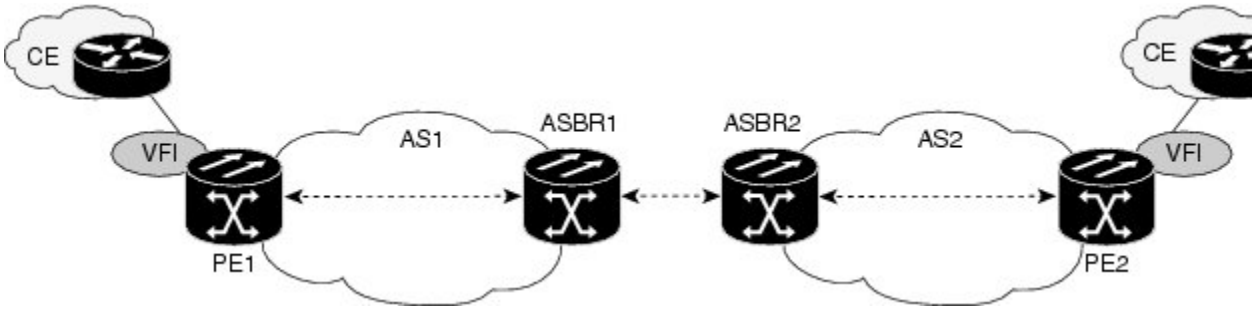
L2VPN VPLS Inter-AS オプション B のトポロジ例

次の図は、L2VPN VPLS Inter-AS オプション B トポロジを簡略化して、図に表したものです。このトポロジでは、AS1 と AS2 は自律システムです。ASBR1 と ASBR2 は ASBR です。カスタマーエッジ（CE）ルータは、AS1 と AS2 の両方に接続されます。

各自律システムは ASBR および PE ルータで構成されます。PE1 は AS1 の仮想転送インスタンス（VFI）に属しています。PE2 は AS2 の VFI に属します。PE1 および PE2 は、PE（TPE）で終端します。

マルチセグメント擬似回線は、ローカル ASBR の TPE と隣接 ASBR の TPE 間のデュアル接続を確立するために作成されます。最初のセグメントは、AS1 の TPE と ASBR1 間のパスを確立します。次のセグメントは ASBR1 と ASBR2 の間にパスを確立し、最後のセグメントは ASBR2 と AS2 の TPE の間にパスを確立します。

図 *22*：*L2VPN VPLS Inter-AS* オプション *B* のトポロジ例



L2VPN VPLS Inter-AS オプション B 設定でのアクティブ PE とパッシブ PE

TPE は、マルチセグメント擬似回線を終端します。デフォルトでは、マルチセグメント擬似回線の両端にある TPE はアクティブ モードです。L2VPN VPLS Inter-AS オプション B 機能を使用するには、TPE の一つがパッシブ モードであることが必要です。システムは、BGP から受信した Target

Attachment Individual Identifier（TAII）とローカル ルータの Source Attachment Individual Identifier（SAII）との比較に基づいてどの PE がパッシブ TPE であるかを判定します。識別子の数字が大きい TPE がアクティブ ロールを担います。

L2VPN VPLS Inter-AS オプション B 機能の PE を設定する際には、**terminating-petie-breaker** コマンドを使用して TPE のモードをネゴシエートします。その後、**mpls ldp discovery targeted-hello accept** コマンドを使用して、パッシブ TPE が Label Distribution Protocol（LDP）ピアからの LDP セッションを確実に承認できるようにします。

PE の設定方法についての詳細は、プロバイダー エッジ（PE）ルータ上での L2VPN VPLS Inter-AS オプション B の有効化,（419 ページ）を参照してください。

L2VPN VPLS Inter-AS オプション B の利点

プライベート IP アドレス

多数の擬似回線が必要とされる一方で、IPv4 の到達可能性は ASBR 内で維持されます。したがって、IP アドレスはプライベートです。

1 つのターゲット LDP セッション

L2VPN VPLS Inter-AS オプション B 機能では、自律システム間でターゲット ラベル配布プロトコル（LDP）セッションが 1 つだけ作成されます。自律システム間に 1 つしかターゲット LDP セッションが作成されないため、サービス プロバイダーは自律システムを通過するコントロール プレーン トラフィックに対してより厳格なセキュリティ ポリシーを適用できます。

L2VPN VPLS Inter-AS オプション B の設定方法

L2VPN VPLS Inter-AS オプション B で使用する VPLS 自動検出設定の変更

（注） L2VPN VPLS Inter-AS オプション B 機能を設定する前に、VPLS Autodiscovery：BGP Based 機能をイネーブルにする必要があります。このタスクを進める前に、VPLS 自動検出：BGP ベースの機能が有効になっていることを確認します。

L2VPN VPLS Inter-AS オプション B 機能が正しく動作するためには、仮想転送インスタンス（VFI）内の PE ルータごとの VPLS ID 値とルート ターゲット値を設定する必要があります。これらの値を変更するには、各 PE ルータで次の手順を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **l2vfi***vfi-name***autodiscovery**
4. **vpnid***vpn-id*
5. **vpls-id** {*autonomous-system-number* **:** *nn* | *ip-address* **:** *nn*}
6. **route-target** [**import** | **export** | **both**] {*autonomous-system-number* **:** *nn* | *ip-address* **:** *nn*}
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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**l2vfi***vfi-name***autodiscovery** 例： `Router(config)# l2 vfi vpls1 autodiscovery`	PE ルータ上で VPLS 自動検出：BGP ベースの機能を有効にして、L2 VFI 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	**vpnid***vpn-id* 例： `Router(config-vfi)# vpn id 10`	VPLS ドメインの VPN ID を設定します。 • VPN ID 値を入力します。
ステップ 5	**vpls-id** {*autonomous-system-number* **:** *nn* | *ip-address* **:** *nn*} 例： `Router(config-vfi)# vpls-id 5:300`	VPLS ID を指定します。 • VPLS 自動検出：BGP ベースの機能は、BGP 自律システム番号と設定された VFI VPN ID を使用して自動的に VPLS ID を生成します。VFI 内の PE の自動生成された VPLS ID を変更するには、次のコマンドを使用します。 • VPLS ID 引数を設定する 2 つの形式があります。例で示されているような *autonomous-system-number* **:** *network number*（*ASN*

	コマンドまたはアクション	目的
		: *nn*）形式、または、*IP-address:network number* 形式（*IP-address* **:** *nn*）で設定できます。
ステップ 6	**route-target** [**import** | **export** | **both**] {*autonomous-system-number* **:** *nn* | *ip-address* **:** *nn*} 例： `Router(config-vfi)# route-target 600:2222`	ルート ターゲット（RT）を指定します。 • VPLS 自動検出機能は、6 バイト未満の RD と VPN ID を使用して自動的にルート ターゲットを生成します。VFI 内の PE の自動生成されたルート ターゲットを変更するには、次のコマンドを使用します。 • ルート ターゲット引数を設定する 2 つの形式があります。例で示されているような *autonomous-system-number* **:** *network number*（*ASN* **:** *nn*）形式、または、*IP-address:network number* 形式（*IP-address* **:** *nn*）で設定できます。
ステップ 7	**exit** 例： `Router(config-vfi)# exit`	L2 VFI コンフィギュレーション モードを終了します。 • コマンドは、ルータが L2 VFI コンフィギュレーション モードを終了した後、有効になります。

次の作業

自律システム内にある個々の PE で、L2VPN VPLS Inter-AS オプション B で使用する VPLS 自動検出設定の変更，（408 ページ）のステップを繰り返します。その後、ASBR 上での L2VPN VPLS Inter-AS オプション B の有効化，（412 ページ）に進みます。

L2VPN プロトコルベースの CLI 機能と関連するコマンドを使用した、L2VPN VPLS Inter-AS オプション B と共に使用するための VPLS 自動検出設定の修正

（注） L2VPN VPLS Inter-AS オプション B 機能を設定する前に、VPLS Autodiscovery：BGP Based 機能をイネーブルにする必要があります。このタスクを進める前に、VPLS 自動検出：BGP ベースの機能が有効になっていることを確認します。

L2VPN VPLS Inter-AS オプション B 機能が正しく動作するためには、仮想転送インスタンス（VFI）内の PE ルータごとの VPLS ID 値とルート ターゲット値を設定する必要があります。これらの値を変更するには、各 PE ルータで次の手順を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **l2vpnvficontext***vfi-name*
4. **vpnid***vpn-id*
5. **autodiscoverybgpsignalingldp**
6. **vpls-id** {*autonomous-system-number* **:** *nn* | *ip-address* **:** *nn*}
7. **route-target** [**import** | **export** | **both**] {*autonomous-system-number* **:** *nn* | *ip-address* **:** *nn*}
8. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**l2vpnvficontext***vfi-name* 例： `Device(config)# l2vpn vfi context vpls1`	L2VPN VFI コンテキストを確立して、L2 VFI 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	**vpnid***vpn-id* 例： `Device(config-vfi)# vpn id 10`	VPLS ドメインの VPN ID を設定します。 • VPN ID 値を入力します。
ステップ 5	**autodiscoverybgpsignalingldp** 例： `Device(config-vfi)# autodiscovery bgp signaling ldp`	PE ルータ上で VPLS 自動検出：BGP ベース機能を有効にします。
ステップ 6	**vpls-id** {*autonomous-system-number* **:** *nn* | *ip-address* **:** *nn*}	VPLS ID を指定します。

	コマンドまたはアクション	目的
	例： `Device(config-vfi)# vpls-id 5:300`	• VPLS 自動検出：BGP ベースの機能は、BGP 自律システム番号と設定された VFI VPN ID を使用して自動的に VPLS ID を生成します。VFI 内の PE の自動生成された VPLS ID を変更するには、次のコマンドを使用します。 • VPLS ID 引数を設定する 2 つの形式があります。例で示されているような *autonomous-system-number* **:** *network number*（*ASN* **:** *nn*）形式、または、 *IP-address:network number* 形式（*IP-address* **:** *nn*）で設定できます。
ステップ 7	**route-target** [**import** | **export** | **both**] {*autonomous-system-number* **:** *nn* | *ip-address* **:** *nn*} 例： `Device(config-vfi)# route-target 600:2222`	ルート ターゲット（RT）を指定します。 • VPLS 自動検出機能は、6 バイト未満の RD と VPN ID を使用して自動的にルート ターゲットを生成します。VFI 内の PE の自動生成されたルート ターゲットを変更するには、次のコマンドを使用します。 • ルート ターゲット引数を設定する 2 つの形式があります。例で示されているような *autonomous-system-number* **:** *network number*（*ASN* **:** *nn*）形式、または、 *IP-address:network number* 形式（*IP-address* **:** *nn*）で設定できます。
ステップ 8	**exit** 例： `Device(config-vfi)# exit`	L2 VFI コンフィギュレーション モードを終了します。 • コマンドは、ルータが L2 VFI コンフィギュレーション モードを終了した後、有効になります。

次の作業

自律システム内にある個々の PE で、L2VPN VPLS Inter-AS オプション B で使用する VPLS 自動検出設定の変更，（408 ページ）のステップを繰り返します。その後、ASBR 上での L2VPN VPLS Inter-AS オプション B の有効化，（412 ページ）に進みます。

ASBR 上での L2VPN VPLS Inter-AS オプション B の有効化

ASBR で L2VPN VPLS Inter-AS オプション B 機能をイネーブルにするには、自律システムにある個々の ASBR で次の手順を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerbgp***autonomous-system-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **next-hop-self**
5. **address-familyl2vpnvpls**
6. **nobgpdefaultroute-targetfilter**
7. **exit**
8. **exit**
9. **mplsldpdiscoverytargeted-helloaccept**
10. 擬似回線の切り替え用として予約されている VC ID の範囲を変更する場合にのみ、ステップ 11 ～ 13 を実行します。それ以外の場合は、ステップ 14 に進みます。
11. **l2pseudowirerouting**
12. **switching-pointvcid***minimum-vcid-valuemaximum-vcid-value*
13. **exit**
14. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**routerbgp***autonomous-system-number* 例： `Router(config)# router bgp 1`	BGP ルーティング プロセスを設定して、ルータ コンフィギュレーション モードを開始します。 • 自律システムの番号を入力します。
ステップ 4	**neighbor** {*ip-address* | *peer-group-name*} **next-hop-self** 例： `Router(config-router)# neighbor 10.10.0.1 next-hop-self`	ASBR を BGP スピーキング ネイバーまたはピア グループのネクスト ホップとして設定します。 • IP アドレスまたはピア グループ名を入力します。

	コマンドまたはアクション	目的
		（注） このコマンドは、自律システム内の個々の PE を識別するために使用します。
ステップ 5	**address-familyl2vpnvpls** 例： `Router(config-router)# address-family l2vpn vpls`	L2VPN エンドポイント プロビジョニング アドレス情報を使用してルーティング セッションを設定し、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 6	**nobgpdefaultroute-targetfilter** 例： `Router(config-router-af)# no bgp default route-target filter`	この ASBR で擬似回線切り替えをイネーブルにします。
ステップ 7	**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 8	**exit** 例： `Router(config-router) exit`	ルータ コンフィギュレーション モードを終了します。
ステップ 9	**mplsldpdiscoverytargeted-helloaccept** 例： `Router(config)# mpls ldp discovery targeted-hello accept`	LDP セッションを受け入れるルータを設定します。 • **targeted-hello accept** キーワードを使用すると、任意のルータからの LDP セッションが受け入れられます。 • このコマンドで使用可能なその他のキーワードの選択肢については、『*Cisco IOS Multiprotocol Label Switching Command Reference*』を参照してください。
ステップ 10	擬似回線の切り替え用として予約されている VC ID の範囲を変更する場合にのみ、ステップ 11 ～ 13 を実行します。それ以外の場合は、ステップ 14 に進みます。	
ステップ 11	**l2pseudowirerouting** 例： `Router(config))# l2 pseudowire routing`	（任意）レイヤ 2 擬似回線ルーティング 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 12	**switching-pointvcid***minimum-vcid-valuemaximum-vcid-value* 例： `Router(config-l2_pw_rtg)#` **switching-point vcid 200 3500**	（任意）スイッチング ポイントを設定して、仮想回線（VC）ID 範囲を指定します。 （注） L2VPN VPLS Inter-AS オプション B 機能では、1001～2147483647 の VC ID 範囲内の VC ID が擬似回線の切り替え用として予約されています。このコマンドを使用すれば、既存の xconnect VC が予約された VC ID のいずれかを使用している場合などに、この範囲を変更することができます。
ステップ 13	**exit** 例： `Router(config-l2_pw_rtg)#) exit`	レイヤ 2 擬似回線ルーティング コンフィギュレーション モードを終了します。
ステップ 14	**end** 例： `Router(config)# end`	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。

次の作業

自律システム内にある個々の ASBR で、ASBR 上での L2VPN VPLS Inter-AS オプション B の有効化，（412 ページ）のステップを繰り返します。その後、プロバイダーエッジ（PE）ルータ上での L2VPN VPLS Inter-AS オプション B の有効化，（419 ページ）に進みます。

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した ASBR 上の L2VPN VPLS Inter-AS オプション B の有効化

自律システム境界ルータ（ASBR）上のレイヤ 2 バーチャル プライベート ネットワーク仮想プライベート LAN サービス（L2VPN VPLS）Inter-AS オプション B 機能を有効にするには、自律システム内の各 ASBR 上で次のタスクを実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerbgp***autonomous-system-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **next-hop-self**
5. **address-familyl2vpnvpls**
6. **nobgpdefaultroute-targetfilter**
7. **exit**
8. **exit**
9. **mplsldpdiscoverytargeted-helloaccept**
10. 擬似回線の切り替え用として予約されている VC ID の範囲を変更する場合にのみ、ステップ 11 ～ 13 を実行します。それ以外の場合は、ステップ 14 に進みます。
11. **l2vpn**
12. **pseudowirerouting**
13. **switching-pointvcid***minimum-vcid-valuemaximum-vcid-value*
14. **exit**
15. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**routerbgp***autonomous-system-number* 例： `Device(config)# router bgp 1`	BGP ルーティング プロセスを設定して、ルータ コンフィギュレーション モードを開始します。 • 自律システムの番号を入力します。

	コマンドまたはアクション	目的
ステップ 4	**neighbor** {*ip-address* | *peer-group-name*} **next-hop-self** 例： `Device(config-router)# neighbor 10.10.0.1 next-hop-self`	ASBR を BGP スピーキング ネイバーまたはピア グループのネクスト ホップとして設定します。 • IP アドレスまたはピア グループ名を入力します。 （注） このコマンドは、自律システム内の個々の PE を識別するために使用します。
ステップ 5	**address-familyl2vpnvpls** 例： `Device(config-router)# address-family l2vpn vpls`	L2VPN エンドポイント プロビジョニング アドレス情報を使用してルーティング セッションを設定し、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 6	**nobgpdefaultroute-targetfilter** 例： `Device(config-router-af)# no bgp default route-target filter`	この ASBR で擬似回線切り替えをイネーブルにします。
ステップ 7	**exit** 例： `Device(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 8	**exit** 例： `Device(config-router) exit`	ルータ コンフィギュレーション モードを終了します。
ステップ 9	**mplsldpdiscoverytargeted-helloaccept** 例： `Device(config)# mpls ldp discovery targeted-hello accept`	LDP セッションを受け入れるルータを設定します。 • **targeted-hello accept** キーワードを使用すると、任意のルータからの LDP セッションが受け入れられます。 • このコマンドで使用可能なその他のキーワードの選択肢については、『*Cisco IOS Multiprotocol Label Switching Command Reference*』を参照してください。

	コマンドまたはアクション	目的
ステップ 10	擬似回線の切り替え用として予約されている VC ID の範囲を変更する場合にのみ、ステップ 11 ～ 13 を実行します。それ以外の場合は、ステップ 14 に進みます。	
ステップ 11	**l2vpn** 例： `Device(config)# l2vpn`	（任意）Layer 2 VPN コンフィギュレーション モードを開始します。
ステップ 12	**pseudowirerouting** 例： `Device(l2vpn-config)# pseudowire routing`	（任意）レイヤ 2 擬似回線ルーティング コンフィギュレーション モードを開始します。
ステップ 13	**switching-pointvcid***minimum-vcid-valuemaximum-vcid-value* 例： `Device(config-l2_pw_rtg)# switching-point vcid 200 3500`	（任意）スイッチング ポイントを設定して、仮想回線（VC）ID 範囲を指定します。 （注） L2VPN VPLS Inter-AS オプション B 機能では、1001～2147483647 の VC ID 範囲内の VC ID が擬似回線の切り替え用として予約されています。このコマンドを使用すれば、既存の xconnect VC が予約された VC ID のいずれかを使用している場合などに、この範囲を変更することができます。
ステップ 14	**exit** 例： `Device(config-l2_pw_rtg)# exit`	レイヤ 2 擬似回線ルーティング コンフィギュレーション モードを終了します。
ステップ 15	**end** 例： `Device(config)# end`	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。

次の作業

自律システム内にある個々の ASBR で、ASBR 上での L2VPN VPLS Inter-AS オプション B の有効化，（412 ページ）のステップを繰り返します。その後、プロバイダーエッジ（PE）ルータ上での L2VPN VPLS Inter-AS オプション B の有効化，（419 ページ）に進みます。

プロバイダー エッジ（PE）ルータ上での L2VPN VPLS Inter-AS オプション B の有効化

PE ルータで L2VPN VPLS Inter-AS オプション B をイネーブルにするには、自律システムにある個々の PE で次の手順を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **l2pseudowirerouting**
4. **terminating-petie-breaker**
5. exit
6. **mplsldpdiscoverytargeted-helloaccept**
7. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**l2pseudowirerouting** 例： `Router(config))# l2 pseudowire routing`	レイヤ 2 擬似回線ルーティング 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	**terminating-petie-breaker** 例： `Router(config-l2_pw_rtg)# terminating-pe tie-breaker`	終端プロバイダー エッジ（TPE）ルータの動作モード（アクティブまたはパッシブ）をネゴシエートします。

	コマンドまたはアクション	目的
ステップ 5	exit 例： `Router(config-l2_pw_rtg)# exit`	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 6	**mplsldpdiscoverytargeted-helloaccept** 例： `Router(config)# mpls ldp discovery targeted-hello accept`	LDP セッションを受け入れるルータを設定します。 • **targeted-hello accept** キーワードを使用すると、任意のルータからの LDP セッションが受け入れられます。 • このコマンドで使用可能なその他のキーワードの選択肢については、『*Cisco IOS Multiprotocol Label Switching Command Reference*』を参照してください。
ステップ 7	**end** 例： `Router(config)# end`	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。

次の作業

自律システム内にある個々の PE で、プロバイダーエッジ（PE）ルータ上での L2VPN VPLS Inter-AS オプション B の有効化，（419 ページ）のステップを繰り返します。その後、L2VPN VPLS Inter-AS オプション B 設定の確認，（422 ページ）に進みます。

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用したプロバイダー エッジ（PE）ルータ上の L2VPN VPLS Inter-AS オプション B の有効化

PE ルータで L2VPN VPLS Inter-AS オプション B を有効にするには、自律システム内の各 PE で次のタスクを実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **l2vpn**
4. **pseudowirerouting**
5. **terminating-petie-breaker**
6. **end**
7. **mplsldpdiscoverytargeted-helloaccept**
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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**l2vpn** 例： `Device(config)# l2vpn`	（任意）Layer 2 VPN 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	**pseudowirerouting** 例： `Device(l2vpn-config)# pseudowire routing`	（任意） レイヤ 2 擬似回線ルーティング コンフィギュレーション モードを開始します。
ステップ 5	**terminating-petie-breaker** 例： `Device(config-l2_pw_rtg)# terminating-pe tie-breaker`	終端プロバイダー エッジ（TPE）ルータの動作モード（アクティブまたはパッシブ）をネゴシエートします。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Device(config-l2_pw_rtg)# exit`	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 7	**mplsldpdiscoverytargeted-helloaccept** 例： `Device(config)# mpls ldp discovery targeted-hello accept`	LDP セッションを受け入れるルータを設定します。 • **targeted-hello accept** キーワードを使用すると、任意のルータからの LDP セッションが受け入れられます。 • このコマンドで使用可能なその他のキーワードの選択肢については、『*Cisco IOS Multiprotocol Label Switching Command Reference*』を参照してください。
ステップ 8	**end** 例： `Device(config)# end`	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。

次の作業

自律システム内にある個々のPEで、プロバイダーエッジ（PE）ルータ上での L2VPN VPLS Inter-AS オプション B の有効化，（419 ページ）のステップを繰り返します。その後、L2VPN VPLS Inter-AS オプション B 設定の確認，（422 ページ）に進みます。

L2VPN VPLS Inter-AS オプション B 設定の確認

L2VPN VPLS Inter-AS オプション B 設定を確認するには、いずれかのルータで次のコマンドの 1 つ以上を使用します。

手順の概要

1. イネーブル化
2. **showxconnectribdetail**
3. **showmplsl2transportvc** [**detail**] [**pwid** *pw-identifier*] [**vpls-id** *vpls-identifier*] [**stitch** *endpoint endpoint*]
4. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showxconnectribdetail** 例： `Router# show xconnect rib detail`	（任意）擬似回線ルーティング情報ベース（RIB）に関する情報を表示します。
ステップ 3	**showmplsl2transportvc** [**detail**] [**pwid** *pw-identifier*] [**vpls-id** *vpls-identifier*] [**stitch** *endpoint endpoint*] 例： `Router# show mpls l2transport vc`	（任意）ルータ上でレイヤ 2 パケットをルーティングするために有効化されたマルチプロトコル ラベル スイッチング（MPLS）Any Transport over MPLS（AToM）VC とスタティック擬似回線に関する情報を表示します。 • 必要に応じて、オプションのキーワードと引数を使用します。
ステップ 4	**end** 例： `Router# end`	特権 EXEC モードを終了します。

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した L2VPN VPLS Inter-AS オプション B 設定の確認

L2VPN VPLS Inter-AS オプション B 設定を確認するには、ルータで次のコマンドの 1 つ以上を使用します。

手順の概要

1. イネーブル化
2. **showl2vpnribdetail**
3. **showl2vpnatomvc** [**pwid** *pw-identifier*] [**vpls-id** *vpls-identifier*] [**stitch** *endpoint endpoint*][**detail**]
4. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showl2vpnribdetail** 例： `Device# show l2vpn rib detail`	（任意）擬似回線ルーティング情報ベース（RIB）に関する情報を表示します。
ステップ 3	**showl2vpnatomvc** [**pwid** *pw-identifier*] [**vpls-id** *vpls-identifier*] [**stitch** *endpoint endpoint*][**detail**] 例： `Device# show l2vpn atom vc`	（任意）ルータ上でレイヤ 2 パケットをルーティングするために有効化されたマルチプロトコルラベルスイッチング（MPLS）Any Transport over MPLS（AToM）VC とスタティック擬似回線に関する情報を表示します。 • 必要に応じて、オプションのキーワードと引数を使用します。
ステップ 4	**end** 例： `Device# end`	特権 EXEC モードを終了します。

L2VPN VPLS Inter-AS オプション B の設定例

例：L2VPN VPLS Inter-AS オプション B で使用する VPLS 自動検出設定の修正

次の例では、L2VPN Inter-AS オプション B 機能と共に使用するために、VPLS Autodiscovery: BGP Based 機能が修正されています。

```
Router> enable
Router# configure terminal
Router(config)# l2 vfi vpls1 autodiscovery
Router(config-vfi)# vpn id 10
Router(config-vfi)# vpls-id 5:300
Router(config-vfi)# route-target 600:2222
Router(config-vfi)# exit
```

例：L2VPN プロトコルベースの CLI 機能と関連するコマンドを使用する、L2VPN VPLS Inter-AS オプション B と共に使用するための VPLS 自動検出設定の修正

次の例では、L2VPN Inter-AS オプション B 機能と共に使用するために、VPLS Autodiscovery: BGP Based 機能が修正されています。

```
Device# enable
Device# configure terminal
Device(config)# l2vpn vfi context vpls1
Device(config-vfi)# vpn id id
Device(config-vfi)# autodiscovery bgp signaling ldp
Device(config-vfi)# vpls-id 5:300
Device(config-vfi)# route-target 600:2222
Device(config-vfi)# exit
```

例：ASBR での L2VPN VPLS Inter-AS オプション B の有効化

次の例では、1 台の ASBR で L2VPN VPLS Inter-AS オプション B 機能が設定されています。

```
Router> enable
Router# configure terminal
Router(config)# router bgp 1
Router(config-router)# neighbor 10.10.0.1 next-hop-self
Router(config-router)# address-family l2vpn vpls
Router(config-router-af)# no bgp default route-target filter
Router(config-router-af)# exit
Router(config-router)# exit
Router(config)# mpls ldp discovery targeted-hello accept
Router(config)# end
```

例：PE ルータでの L2VPN VPLS Inter-AS オプション B の有効化

次の例では、PE ルータで L2VPN VPLS Inter-AS オプション B が設定されます。この PE は TPE でもあります。

```
Router> enable
Router# configure terminal
Router(config))# l2 pseudowire routing
Router(config-l2_pw_rtg)# terminating-pe tie-breaker
Router(config-l2_pw_rtg)# exit
Router(config)# mpls ldp discovery targeted-hello accept
Router(config)# end
```

例：PE ルータでの L2VPN VPLS Inter-AS オプション B の有効化（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

次の例では、プロバイダー エッジ（PE）ルータで L2VPN VPLS Inter-AS オプション B が設定されます。この PE は、終端プロバイダー エッジ（TPE）でもあります。

```
Device> enable
Device# configure terminal
Device(config)# l2vpn
```

```
Device(l2vpn-config)#  pseudowire routing
Device(config-l2_pw_rtg)# terminating-pe tie-breaker
Device(config-l2_pw_rtg)# exit
Device(config)# mpls ldp discovery targeted-hello accept
Device(config)# end
```

例：L2VPN VPLS Inter-AS オプション B 設定の確認

show xconnect rib detail コマンドの出力は、L2VPN VPLS Inter-AS オプション B 設定を確認するために使用できます。

次に、ASBR 設定で使用する場合の **show xconnect rib detail** コマンドの出力例を示します。ASBR では、**show xconnect rib detail** コマンドにより、BGP ピアから受信した Layer 2 VPN BGP ネットワーク層到達可能性情報（NLR）が表示されます。また、特定の TAII のターゲット LDP セッションから受信したシグナリング メッセージも表示されます。

```
Router# show xconnect rib detail
Local Router ID: 10.1.1.3
VPLS-ID: 1:1, Target ID: 10.1.1.1
  Next-Hop: 10.1.1.1
  Hello-Source: 10.1.1.3
  Route-Target: 2:2
  Incoming RD: 10.0.0.0:1
  Forwarder:
  Origin: BGP
  Provisioned: Yes
  SAII: 10.0.0.1, LDP Peer Id: 10.255.255.255, VC Id: 1001 ***
  SAII: 10.1.0.1, LDP Peer Id: 10.255.255.255, VC Id: 1002 ***
```

パッシブ TPE ルータが BGP 情報を受信したあと、（パッシブ TPE ルータが LDP ラベルを受信する前）、**show xconnect rib** コマンドにピア情報が表示されます。**show mpls l2transport vc** コマンドではピア情報は表示されません。これは、VFI AToM xconnect がプロビジョニングされていないためです。

したがって、パッシブ TPE の場合は、**show xconnect rib detail** コマンドの出力に「Passive : Yes」エントリが追加されます。また、ネイバー xconnect が（再試行なしで）正しく作成されると、「Provisioned: Yes」エントリが表示されます。

この出力例では、「SAII」で始まる 2 つの行に、この ASBR が 2 台のプロバイダー PE ルータ（10.0.0.1 および 10.1.0.1）を合わせて TAII 10.1.1.1 にすることが示されています。

例：L2VPN VPLS Inter-AS オプション B 設定の確認（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

show l2vpn rib detail コマンドの出力は、L2VPN VPLS Inter-AS オプション B 設定を確認するために使用できます。

次に、自律システム境界ルータ（ASBR）の設定で使用する場合の **show l2vpn rib detail** コマンドの出力例を示します。ASBR では、**show l2vpn rib detail** コマンドにより、BGP ピアから受信した Layer 2 VPN BGP ネットワーク層到達可能性情報（NLR）が表示されます。また、特定の TAII の

ターゲット Label Distribution Protocol（LDP）セッションから受信したシグナリング メッセージも表示されます。

```
Device# show l2vpn rib detail
Local Router ID: 10.1.1.3
VPLS-ID: 1:1, Target ID: 10.1.1.1
  Next-Hop: 10.1.1.1
  Hello-Source: 10.1.1.3
  Route-Target: 2:2
  Incoming RD: 10.0.0.0:1
  Forwarder:
  Origin: BGP
  Provisioned: Yes
  SAII: 10.0.0.1, LDP Peer Id: 10.255.255.255, VC Id: 1001 ***
  SAII: 10.1.0.1, LDP Peer Id: 10.255.255.255, VC Id: 1002 ***
```

パッシブ終端プロバイダーエッジ（TPE）ルータが BGP 情報を受信した後、（かつパッシブ TPE ルータが LDP ラベルを受信する前）、**show l2vpn rib** コマンドの出力にピア情報が表示されます。**show l2vpn atom vc** コマンドではピア情報は表示されません。これは、VFI AToM xconnect がプロビジョニングされていないためです。

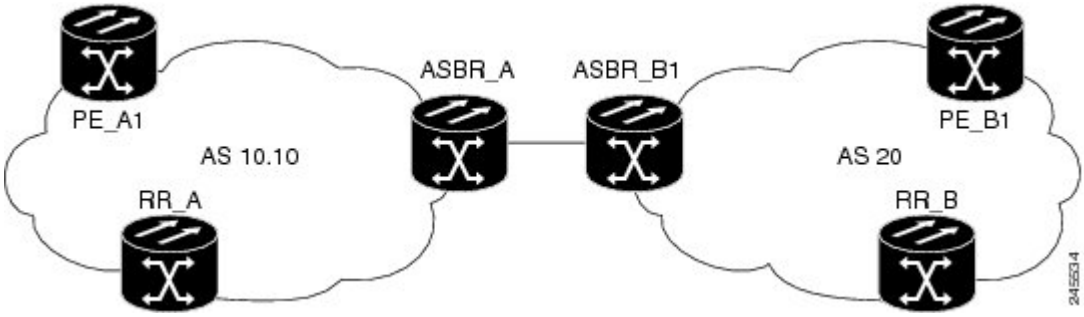
したがって、パッシブ TPE の場合は、**show l2vpn rib detail** コマンドの出力に「Passive : Yes」エントリが追加されます。また、ネイバー xconnect が（再試行なしで）正しく作成されると、「Provisioned: Yes」エントリが表示されます。

この出力例では、「SAII」で始まる 2 つの行に、この ASBR が 2 台のプロバイダー PE ルータ（10.0.0.1 および 10.1.0.1）を合わせて TAII 10.1.1.1 にすることが示されています。

例：サンプル L2VPN VPLS Inter-AS オプション B 設定

次に、以下の図に示されているトポロジに基づく L2VPN VPLS Inter-AS オプション B 設定の例を示します。

図 *23*：設定例で使用される *L2VPN VPLS Inter-AS* オプション *B* のトポロジ



上の図に示すトポロジは、2 台の ASBR を使用して自律システム境界を超えて接続している 2 台の PE ルータで構成されています。ルートは、BGP ルートリフレクタ（RR）を使用する各自律システム内で共有されます（RR は、完全な設定を示す目的でのみ含まれています。RR は、L2VPN Inter-AS オプション B 設定の要件ではありません）。

このトポロジに含まれる要素それぞれの具体的な設定は次のとおりです。太字は、標準の VPLS Autodiscovery：BGP Based 設定に追加する必要のある要素を示します。

PE_A1 ルータ

```
mpls ldp discovery targeted-hello accept
mpls label protocol ldp
!
l2 router-id 10.1.1.1
!
l2 pseudowire routing
 terminating-pe tie-breaker
!
l2 vfi vfiA autodiscovery
 vpn id 111
 vpls-id 111:111
 rd 111:111
 route-target 111:111
 no auto-route-target
!
!
interface Loopback0
 ip address 10.1.1.1 255.255.255.255
!
!
interface GigabitEthernet2/0/9
 description AS-10.10-Backbone-LAN
 ip address 10.100.100.1 255.255.255.0
 mpls ip
!
router ospf 10
 network 10.1.1.1 0.0.0.0 area 0
 network 10.100.100.1 0.0.0.0 area 0
!
router bgp 10.10
 bgp asnotation dot
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 10.3.3.3 remote-as 10.10
 neighbor 10.3.3.3 description RR-AS-10.10
 neighbor 10.3.3.3 update-source Loopback0
 !
 address-family ipv4
  no auto-summary
 exit-address-family
 !
 address-family l2vpn vpls
  neighbor 10.3.3.3 activate
  neighbor 10.3.3.3 send-community extended
 exit-address-family
!
mpls ldp router-id Loopback0
!
```

ASBR_A ルータ

```
mpls ldp discovery targeted-hello accept
mpls label protocol ldp
!
!
interface Loopback0
 ip address 10.4.4.4 255.255.255.255
!
interface GigabitEthernet1/10
 description AS-10.10-backbone-Lan
 ip address 10.100.100.4 255.255.255.0
 mpls ip
!
interface GigabitEthernet2/0/1
 description B2B-AS-20-ASBR-B1
 ip address 10.12.1.4 255.255.255.0
 mpls ip
!
```

```
router ospf 10
 passive-interface GigabitEthernet1/12
 passive-interface GigabitEthernet2/0/1
 passive-interface GigabitEthernet2/0/2
 network 10.4.4.4 0.0.0.0 area 0
 network 10.100.100.4 0.0.0.0 area 0
 network 10.12.0.0 0.0.255.255 area 0
!
router bgp 10.10
 bgp router-id 10.4.4.4
 bgp asnotation dot
 bgp log-neighbor-changes
 no bgp default route-target filter
 no bgp default ipv4-unicast
 timers bgp 10 30
 neighbor AS20 peer-group
 neighbor AS20 remote-as 20
 neighbor 10.3.3.3 remote-as 10.10
 neighbor 10.3.3.3 update-source Loopback0
 neighbor 10.12.1.6 peer-group AS20
 !
 address-family ipv4
  no auto-summary
 exit-address-family
 !
 address-family l2vpn vpls
  neighbor AS20 send-community extended
  neighbor AS20 next-hop-self
  neighbor 10.3.3.3 activate
  neighbor 10.3.3.3 send-community extended
  neighbor 10.3.3.3 next-hop-self
  neighbor 12.12.1.6 activate
 exit-address-family
!
ip route 10.6.6.6 255.255.255.255 10.12.1.6
ip route 10.9.9.9 255.255.255.255 10.12.3.9
!
mpls ldp router-id Loopback0
!
```

RR_A ルータ

```
interface Loopback0
 ip address 10.3.3.3 255.255.255.255
!
interface Ethernet2/0
 ip address 10.100.100.3 255.255.255.0
 duplex half
!
router ospf 10
 network 10.3.3.3 0.0.0.0 area 0
 network 10.100.100.3 0.0.0.0 area 0
!
router bgp 10.10
 bgp asnotation dot
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor rr-client peer-group
 neighbor rr-client remote-as 10.10
 neighbor rr-client update-source Loopback0
 neighbor 10.1.1.1 peer-group rr-client
 neighbor 10.4.4.4 peer-group rr-client
 !
 address-family ipv4
  no auto-summary
 exit-address-family
 !
 address-family l2vpn vpls
  neighbor rr-client send-community extended
  neighbor rr-client route-reflector-client
  neighbor 10.1.1.1 activate
```

```
  neighbor 10.4.4.4 activate
 exit-address-family
!
```

PE_B1 ルータ

```
mpls ldp discovery targeted-hello accept
mpls label protocol ldp
!
l2 router-id 10.5.5.5
l2 pseudowire routing
 terminating-pe tie-breaker
l2 vfi vfiA autodiscovery
 vpn id 111
 vpls-id 111:111
 rd 111:111
 route-target 111:111
 no auto-route-target
!
interface Loopback0
 ip address 10.5.5.5 255.255.255.255
!
interface GigabitEthernet2/0/7
 description AS20-Backbone-LAN
 ip address 10.100.100.5 255.255.255.0
 mpls ip
!
router ospf 20
 network 10.5.5.5 0.0.0.0 area 0
 network 10.100.100.5 0.0.0.0 area 0
!
router bgp 20
 bgp router-id 10.5.5.5
 bgp asnotation dot
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 10.8.8.8 remote-as 20
 neighbor 10.8.8.8 update-source Loopback0
 !
 address-family ipv4
  no auto-summary
 exit-address-family
 !
 address-family l2vpn vpls
  neighbor 10.8.8.8 activate
  neighbor 10.8.8.8 send-community extended
 exit-address-family
!
mpls ldp router-id Loopback0
!
```

ASBR_B1 ルータ

```
mpls ldp discovery targeted-hello accept
mpls label protocol ldp
!
l2 router-id 10.6.6.6
l2 pseudowire routing
 terminating-pe tie-breaker
!
interface Loopback0
 ip address 10.6.6.6 255.255.255.255
!
interface Ethernet1/3
 description B2B-AS-10.10-ASBR-A
 ip address 10.12.1.6 255.255.255.0
 duplex half
 mpls ip
!
```

```
interface Ethernet2/1
 description AS-20-backbone-Lan
 ip address 10.100.100.6 255.255.255.0
 duplex half
 mpls ip
!
router ospf 20
 passive-interface Ethernet1/3
 network 10.12.1.6 0.0.0.0 area 0
 network 10.6.6.6 0.0.0.0 area 0
 network 10.100.100.6 0.0.0.0 area 0
!
router bgp 20
 bgp router-id 10.6.6.6
 bgp asnotation dot
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 timers bgp 10 30
 neighbor 10.12.1.4 remote-as 10.10
 neighbor 10.12.1.4 ebgp-multihop 255
 neighbor 10.8.8.8 remote-as 20
 neighbor 10.8.8.8 update-source Loopback0
 !
 address-family ipv4
  no auto-summary
 exit-address-family
 !
 address-family l2vpn vpls
  no bgp default route-target filter
  neighbor 10.12.1.4 activate
  neighbor 10.12.1.4 send-community extended
  neighbor 10.12.1.4 next-hop-self
  neighbor 10.8.8.8 activate
  neighbor 10.8.8.8 send-community extended
  neighbor 10.8.8.8 next-hop-self
 exit-address-family
!
```

RR_B ルータ

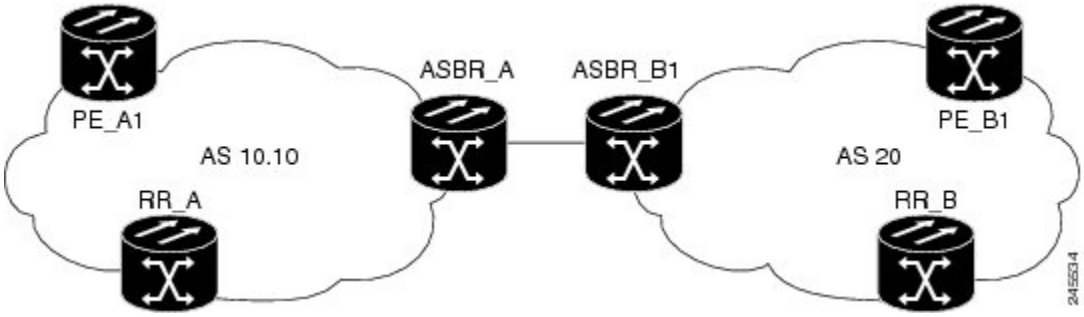
```
interface Loopback0
 ip address 10.8.8.8 255.255.255.255
!
interface Ethernet2/1
 ip address 10.100.100.8 255.255.255.0
 duplex half
!
router ospf 20
 network 10.8.8.8 0.0.0.0 area 0
 network 10.100.100.8 0.0.0.0 area 0
!
router bgp 20
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor rrc peer-group
 neighbor rrc remote-as 20
 neighbor rrc update-source Loopback0
 neighbor 10.5.5.5 peer-group rrc
 neighbor 10.6.6.6 peer-group rrc
 neighbor 10.9.9.9 peer-group rrc
 neighbor 10.9.9.9 shutdown
 !
 address-family ipv4
  no auto-summary
 exit-address-family
 !
 address-family l2vpn vpls
  neighbor rrc send-community extended
  neighbor rrc route-reflector-client
  neighbor 10.5.5.5 activate
  neighbor 10.6.6.6 activate
```

```
  neighbor 10.9.9.9 activate
 exit-address-family
!
```

例：サンプル L2VPN VPLS Inter-AS オプション B 設定（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

次に、以下の図に示されているトポロジに基づく L2VPN VPLS Inter-AS オプション B 設定の例を示します。

図 *24*：設定例で使用される *L2VPN VPLS Inter-AS* オプション *B* のトポロジ



上の図に示すトポロジは、2 台の ASBR を使用して自律システム境界を超えて接続している 2 台のプロバイダー エッジ（PE）ルータで構成されています。ルートは、BGP ルート リフレクタ（RR）を使用する各自律システム内で共有されます（RR は、完全な設定を示す目的でのみ含まれています。RR は、L2VPN Inter-AS オプション B 設定の要件ではありません）。

このトポロジに含まれる要素それぞれの具体的な設定は次のとおりです。太字で強調されているコマンドは、標準の BGP ベースの VPLS 自動検出の設定に追加する必要のある要素を示します。

PE_A1 ルータ

```
mpls ldp discovery targeted-hello accept
mpls label protocol ldp
!
l2vpn
 router-id 10.1.1.1
 pseudowire routing
   terminating-pe tie-breaker
!
l2vpn vfi context vfiA
 vpn id 111
 autodiscovery bgp signaling ldp
 vpls-id 111:111
 rd 111:111
 route-target 111:111
 no auto-route-target
!
!
interface Loopback0
 ip address 10.1.1.1 255.255.255.255
!
!
interface GigabitEthernet2/0/9
 description AS-10.10-Backbone-LAN
```

例：サンプル L2VPN VPLS Inter-AS オプション B 設定（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

```
 ip address 10.100.100.1 255.255.255.0
 mpls ip
!
router ospf 10
 network 10.1.1.1 0.0.0.0 area 0
 network 10.100.100.1 0.0.0.0 area 0
!
router bgp 10.10
 bgp asnotation dot
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 10.3.3.3 remote-as 10.10
 neighbor 10.3.3.3 description RR-AS-10.10
 neighbor 10.3.3.3 update-source Loopback0
 !
 address-family ipv4
  no auto-summary
 exit-address-family
 !
 address-family l2vpn vpls
  neighbor 10.3.3.3 activate
  neighbor 10.3.3.3 send-community extended
 exit-address-family
!
mpls ldp router-id Loopback0
!
```

ASBR_A ルータ

```
mpls ldp discovery targeted-hello accept
mpls label protocol ldp
!
!
interface Loopback0
 ip address 10.4.4.4 255.255.255.255
!
interface GigabitEthernet1/10
 description AS-10.10-backbone-Lan
 ip address 10.100.100.4 255.255.255.0
 mpls ip
!
interface GigabitEthernet2/0/1
 description B2B-AS-20-ASBR-B1
 ip address 10.12.1.4 255.255.255.0
 mpls ip
!
router ospf 10
 passive-interface GigabitEthernet1/12
 passive-interface GigabitEthernet2/0/1
 passive-interface GigabitEthernet2/0/2
 network 10.4.4.4 0.0.0.0 area 0
 network 10.100.100.4 0.0.0.0 area 0
 network 10.12.0.0 0.0.255.255 area 0
!
router bgp 10.10
 bgp router-id 10.4.4.4
 bgp asnotation dot
 bgp log-neighbor-changes
 no bgp default route-target filter
 no bgp default ipv4-unicast
 timers bgp 10 30
 neighbor AS20 peer-group
 neighbor AS20 remote-as 20
 neighbor 10.3.3.3 remote-as 10.10
 neighbor 10.3.3.3 update-source Loopback0
 neighbor 10.12.1.6 peer-group AS20
 !
 address-family ipv4
  no auto-summary
 exit-address-family
 !
```

```
 address-family l2vpn vpls
  neighbor AS20 send-community extended
  neighbor AS20 next-hop-self
  neighbor 10.3.3.3 activate
  neighbor 10.3.3.3 send-community extended
  neighbor 10.3.3.3 next-hop-self
  neighbor 12.12.1.6 activate
 exit-address-family
!
ip route 10.6.6.6 255.255.255.255 10.12.1.6
ip route 10.9.9.9 255.255.255.255 10.12.3.9
!
mpls ldp router-id Loopback0
!
```

RR_A ルータ

```
interface Loopback0
 ip address 10.3.3.3 255.255.255.255
!
interface Ethernet2/0
 ip address 10.100.100.3 255.255.255.0
 duplex half
!
router ospf 10
 network 10.3.3.3 0.0.0.0 area 0
 network 10.100.100.3 0.0.0.0 area 0
!
router bgp 10.10
 bgp asnotation dot
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor rr-client peer-group
 neighbor rr-client remote-as 10.10
 neighbor rr-client update-source Loopback0
 neighbor 10.1.1.1 peer-group rr-client
 neighbor 10.4.4.4 peer-group rr-client
 !
 address-family ipv4
  no auto-summary
 exit-address-family
 !
 address-family l2vpn vpls
  neighbor rr-client send-community extended
  neighbor rr-client route-reflector-client
  neighbor 10.1.1.1 activate
  neighbor 10.4.4.4 activate
 exit-address-family
!
```

PE_B1 ルータ

```
mpls ldp discovery targeted-hello accept
mpls label protocol ldp
!
l2vpn
 router-id 10.5.5.5
 pseudowire routing
  terminating-pe tie-breaker
l2vpn vfi context vfiA
 vpn id 111
 autodiscovery bgp signaling ldp
 vpls-id 111:111
 rd 111:111
 route-target 111:111
 no auto-route-target
!
interface Loopback0
 ip address 10.5.5.5 255.255.255.255
```

例：サンプル L2VPN VPLS Inter-AS オプション B 設定（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

```
!
interface GigabitEthernet2/0/7
 description AS20-Backbone-LAN
 ip address 10.100.100.5 255.255.255.0
 mpls ip
!
router ospf 20
 network 10.5.5.5 0.0.0.0 area 0
 network 10.100.100.5 0.0.0.0 area 0
!
router bgp 20
 bgp router-id 10.5.5.5
 bgp asnotation dot
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 10.8.8.8 remote-as 20
 neighbor 10.8.8.8 update-source Loopback0
 !
 address-family ipv4
  no auto-summary
 exit-address-family
 !
 address-family l2vpn vpls
  neighbor 10.8.8.8 activate
  neighbor 10.8.8.8 send-community extended
 exit-address-family
!
mpls ldp router-id Loopback0
!
```

ASBR_B1 ルータ

```
mpls ldp discovery targeted-hello accept
mpls label protocol ldp
!
l2vpn
 router-id 10.6.6.6
 pseudowire routing
  terminating-pe tie-breaker
!
interface Loopback0
 ip address 10.6.6.6 255.255.255.255
!
interface Ethernet1/3
 description B2B-AS-10.10-ASBR-A
 ip address 10.12.1.6 255.255.255.0
 duplex half
 mpls ip
!
interface Ethernet2/1
 description AS-20-backbone-Lan
 ip address 10.100.100.6 255.255.255.0
 duplex half
 mpls ip
!
router ospf 20
 passive-interface Ethernet1/3
 network 10.12.1.6 0.0.0.0 area 0
 network 10.6.6.6 0.0.0.0 area 0
 network 10.100.100.6 0.0.0.0 area 0
!
router bgp 20
 bgp router-id 10.6.6.6
 bgp asnotation dot
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 timers bgp 10 30
 neighbor 10.12.1.4 remote-as 10.10
 neighbor 10.12.1.4 ebgp-multihop 255
 neighbor 10.8.8.8 remote-as 20
 neighbor 10.8.8.8 update-source Loopback0
```

```
 !
 address-family ipv4
  no auto-summary
 exit-address-family
 !
 address-family l2vpn vpls
  no bgp default route-target filter
  neighbor 10.12.1.4 activate
  neighbor 10.12.1.4 send-community extended
  neighbor 10.12.1.4 next-hop-self
  neighbor 10.8.8.8 activate
  neighbor 10.8.8.8 send-community extended
  neighbor 10.8.8.8 next-hop-self
 exit-address-family
!
```

RR_B ルータ

```
interface Loopback0
 ip address 10.8.8.8 255.255.255.255
!
interface Ethernet2/1
 ip address 10.100.100.8 255.255.255.0
 duplex half
!
router ospf 20
 network 10.8.8.8 0.0.0.0 area 0
 network 10.100.100.8 0.0.0.0 area 0
!
router bgp 20
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor rrc peer-group
 neighbor rrc remote-as 20
 neighbor rrc update-source Loopback0
 neighbor 10.5.5.5 peer-group rrc
 neighbor 10.6.6.6 peer-group rrc
 neighbor 10.9.9.9 peer-group rrc
 neighbor 10.9.9.9 shutdown
 !
 address-family ipv4
  no auto-summary
 exit-address-family
 !
 address-family l2vpn vpls
  neighbor rrc send-community extended
  neighbor rrc route-reflector-client
  neighbor 10.5.5.5 activate
  neighbor 10.6.6.6 activate
  neighbor 10.9.9.9 activate
 exit-address-family
!
```

L2VPN VPLS Inter-AS オプション B に関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
MPLS コマンド	『Cisco IOS Multiprotocol Label Switching Command Reference』
IP ルーティング（BGP）コマンド	『Cisco IOS IP Routing: BGP Command Reference』
VPLS Autodiscovery：BGP Based 機能の設定に関連する概念および作業。	『*VPLS Autodiscovery BGP Based*』
L2VPN アドレス ファミリの BGP サポート	『*BGP Support for the L2VPN Address Family*』
VPLS	『*Configuring Multiprotocol Label Switching on the Optical Services Modules*』マニュアルの「VPLS Overview」の項
L2VPN マルチセグメント擬似回線、L2VPN マルチセグメント擬似回線の MPLS OAM サポート、L2VPN inter-AS オプション B の MPLS OAM サポート	『*L2VPN Multisegment Pseudowires*』

標準

規格	Title
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 のリンク
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、既存の標準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 ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
RFC 4360	『*BGP Extended Communities Attribute*』
RFC 4364	『*BGP/MPLS IP Virtual Private Networks (VPNs)*』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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。	http://www.cisco.com/cisco/web/support/index.html

L2VPN VPLS Inter-AS オプション B の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、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。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *21*：*L2VPN VPLS Inter-AS* オプション *B* の機能情報

機能名	リリース	機能情報
『L2VPN VPLS Inter-AS Option B』	15.1(1)S Cisco IOS XE Release 3.8S	L2VPN VPLS Inter-AS オプション B 機能により、既存の VPLS 自動検出機能が拡張され、複数の BGP 自律システム上で稼働できるようになります。BGP をベースとした自動検出を基礎的なフレームワークとして使用する L2VPN VPLS Inter-AS オプション B 機能は、隣接する ASBR の間に、ダイナミックなマルチセグメント擬似回線コンフィギュレーションを作成します。 次のコマンドが導入または変更されました：**bgp default route-target filter**、**debug xconnect**、**l2 pseudowire routing**、**show ip bgp neighbors**、**show mpls forwarding-table**、**show mpls l2transport vc**、**show xconnect**、**switching-point vcid**、および **terminating-pe tie-breaker**。

用語集

AGI：アタッチメント グループ識別子。接続可能な擬似回線のグループに共通の識別子。

AII —アタッチメント個別識別子。

ASBR：自律システム境界ルータ。

PE：プロバイダー エッジ ルータ。

NLRI：ネットワーク層到達可能性情報。

SAII：送信元アタッチメント個別識別子。

SPE：スイッチング PE。

TAII：ターゲット アタッチメント個別識別子。

TPE：終端 PE。

VFI：仮想転送インスタンス。これは VSI に関連付けられた擬似回線のグループを識別します。

VSI：仮想スイッチング インスタンス。これは単一の PE 内のブリッジ ドメインを識別します。単一の VPLS ネットワークに参加している PE はそれぞれ VSI を 1 つ持ちます。

第 11 章

AToM の IEEE 802.1Q トンネリング（QinQ）

この機能により、AToM に対して IEEE 802.1Q トンネリング（QinQ）を設定できます。また、マルチプロトコル ラベル スイッチング（MPLS）レイヤ 2 VPN（L2VPN）用に QinQ タグを書き換えることもできます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース 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、機能情報の表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シスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

AToM の IEEE 802.1Q トンネリング（QinQ）の前提条件

QinQ（802.1Q-in-802.1Q の短縮形）トンネリングおよびタグ書き換え機能は、次のライン カードでサポートされます。

- 8 ポートのファスト イーサネット ライン カード（ESR-HH-8FE-TX）
- 2 ポートのハーフハイト ギガビット イーサネット ライン カード（ESR-HH-1GE）
- 1 ポートのハーフハイト ギガビット イーサネット ライン カード（ESR-1GE）

AToM の IEEE 802.1Q トンネリング（QinQ）の制約事項

- この機能では、最大 447 個の外部 VLAN ID と最大 4095 個の内部 VLAN ID をサポートできます。
- このリリースでは、一義的な VLAN のタグが付けられたイーサネット QinQ インターフェイスのみがサポートされます。つまり、両方の VLAN タグのイーサネット VLAN QinQ 書き換え機能は、QinQ カプセル化および定義された VLAN ID の明示ペアを使用したイーサネット サブインターフェイスでのみサポートされます。

（注） 一義的でない内部 VLAN ID はこのリリースではサポートされていません。

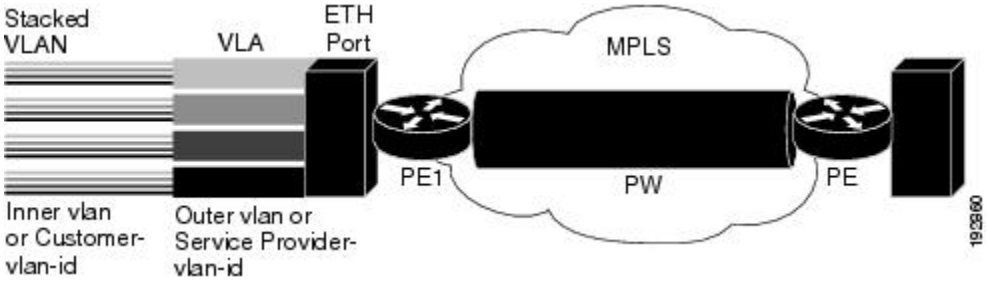
AToM の IEEE 802.1Q トンネリング（QinQ）に関する情報

イーサネット VLAN QinQ AToM

メトロ イーサネット導入では、CE ルータと PE ルータがイーサネット スイッチド アクセス ネットワークを介して接続され、PE ルータに到達するパケットは最大 2 つの IEEE 802.1q VLAN タグを含む可能性があります（1 つは顧客を識別する内部 VLAN タグ、もう 1 つは顧客のサービス プロバイダーを示す外部 VLAN タグ）。同じイーサネット パケットに複数のタグ付けを可能にし、VLAN ID のスタックを作成するこの技法は QinQ（802.1Q-in-802.1Q の短縮形）と呼ばれていま

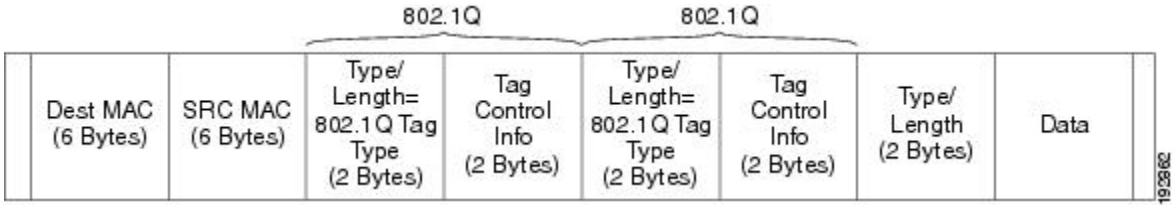
す。下の図は、さまざまなエッジ デバイスがさまざまなレベルの VLAN スタックで L2 スイッチングを実行可能な状況を示しています。

図 *25*：イーサネット *VLAN QinQ*



外部 VLAN タグがサービス境界 VLAN タグの場合、QinQ パケットは 1 つの VLAN タグが付いたものと同様に処理されます（以前、イーサネット VLAN Q-in-Q 修正と呼ばれていたもので、すでに 12.2(31) SB リリースでサポート対象です）。ただし、顧客のサービスを区別するために顧客が外部と内部の VLAN タグを組み合わせて使用する必要がある場合、下図に示すように、エッジデバイスはパケット上の内部および外部の VLAN ID の組み合わせに基づき、一意の擬似回線を選択可能である必要があります。顧客はトラフィック出力側で内部と外部の両方の VLAN ID を書き換えることができる必要がある場合があります。

図 *26*：イーサネット *VLAN QinQ* ヘッダー

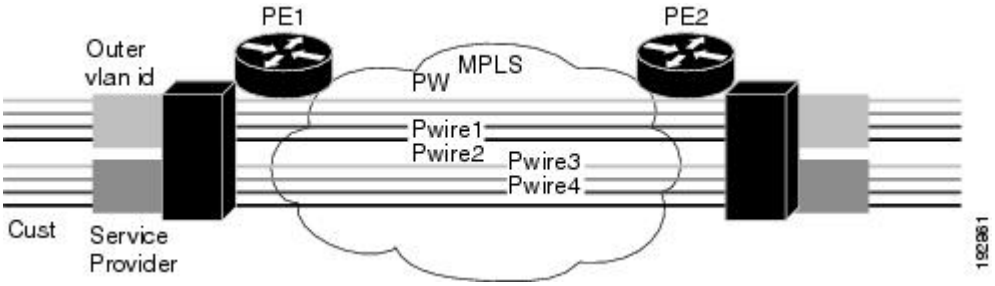


内部および外部 VLAN タグに基づく QinQ トンネリング

着信 QinQ イーサネット トラフィックを処理する際、エッジ ルータでは顧客は固有の擬似回線エンドポイントを選択し、内部および外部の VLAN ID の組み合わせに基づいてトラフィックを切り替えることができます。例として次の図には、内部（カスタマーエッジ）と外部（サービスプロ

バイダー）の VLAN ID の組み合わせに応じて固有の擬似回線が選択される方法が示されています。つまり、異なる顧客のトラフィックを分離しておくことができます。

図 *27*：*QinQ* 接続



QinQ フレームでの内部および外部 VLAN タグの書き換え

着信 AToM イーサネット QinQ トラフィックを管理すると、エッジ ルータは次のタスクを実行します。

1. MPLS ラベルを取り除きます。
2. 出力 QinQ インターフェイスにパケットを送信する前に、顧客が内部および外部の VLAN ID を書き換えることができるようにします。この機能は、AToM like-to-like Ethernet QinQ トラフィック用にのみ提供されています。

QinQ AToM 機能は、AToM 上の like-to-like インターワーキングのケースです。この機能では、マイクロコードを変更して、AToM 擬似回線を通過するイーサネット QinQ トラフィックの VLAN タグの 2 つのレイヤを上書きできるようにする必要があります。

- 入力側では、パケットは 2 つの VLAN タグで L2 ヘッダーを保持し、VC タイプ 4 の擬似回線を介して送信されます。
- 出力側では、MPLS ラベルが取り除かれ、VLAN タグの最大 2 つのレベルまで設定ごとに書き換えられます。

このリリースでは、一義的な VLAN のタグが付けられたイーサネット QinQ インターフェイスのみがサポートされます。両方の VLAN タグのイーサネット VLAN Q-in-Q 書き換え機能は、QinQ カプセル化および定義された VLAN ID の明示ペアを使用したイーサネット サブインターフェイスでのみサポートされます。

AToM の IEEE 802.1Q トンネリング（QinQ）の設定方法

ここでは、AToM 用の IEEE 802.1Q トンネリング（QinQ）を設定する方法について説明し、次の手順が含まれます。すべての手順はオプションとして示されていますが、リストの最初の 2 つのうち 1 つを選択する必要があります。

あいまいさのない AToM の IEEE 802.1Q トンネリング（QinQ）の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacegigabitethernet***slot*/*subslot*/*port*.[*subinterface*]
4. **encapsulationdot1q***vlan-id***second-dot1q**{**any** | *vlan-id*[,*vlan-id*[-*vlan-id*]]}
5. **xconnect***peer-router-idvcid***encapsulationmpls**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**interfacegigabitethernet***slot*/*subslot*/*port*.[*subinterface*] 例： `Router(config)# interface GigabitEthernet1/0/0.100`	ギガビット イーサネット 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	**encapsulationdot1q***vlan-id***second-dot1q**{**any**	*vlan-id*[,*vlan-id*[-*vlan-id*]]} 例： `Router(config-if)# encapsulation dot1q 100 second-dot1q 200`	インターフェイスの Q-in-Q 入力フレームを適切なサービス インスタンスにマッピングする一致基準を定義します。
ステップ 5	**xconnect***peer-router-idvcid***encapsulationmpls** 例： `Router(config-if)# xconnect 10.0.0.16 410 encapsulation mpls`	レイヤ 2 パケットを転送するための VC を作成します。

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した AToM 用の明確な IEEE 802.1Q トンネリング（QinQ）の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacegigabitethernet***slot*/*subslot*/*port*.[*subinterface*]
4. **encapsulationdot1q***vlan-id***second-dot1q**{**any** | *vlan-id*[,*vlan-id*[-*vlan-id*]]}
5. **interfacepseudowire***number*
6. **encapsulationmpls**
7. **neighbor***peer-addressvcid-value*
8. **exit**
9. **l2vpn xconnectcontext***context-name*
10. **member pseudowire***interface-number*
11. **member gigabitethernet***interface-number*
12. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**interfacegigabitethernet***slot*/*subslot*/*port*.[*subinterface*] 例： `Router(config)# interface GigabitEthernet1/0/0.100`	ギガビット イーサネット 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。

	コマンドまたはアクション	目的
ステップ 4	**encapsulationdot1q***vlan-id***second-dot1q**{**any** | *vlan-id*[,*vlan-id*[-*vlan-id*]]} 例： `Router(config-if)# encapsulation dot1q 100 second-dot1q 200`	インターフェイスの Q-in-Q 入力フレームを適切なサービス インスタンスにマッピングする一致基準を定義します。
ステップ 5	**interfacepseudowire***number* 例： `Router(config-if)# interface pseudowire 100`	擬似回線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 6	**encapsulationmpls** 例： `Router(config-if)# encapsulation mpls`	マルチプロトコル ラベル スイッチング（MPLS）がデータ カプセル化方式として使用されることを指定します。
ステップ 7	**neighbor***peer-addressvcid-value* 例： `Router(config-if)# neighbor 10.0.0.1 123`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 8	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 9	**l2vpn xconnectcontext***context-name* 例： `Router(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect コンフィギュレーション モードを開始します。
ステップ 10	**member pseudowire***interface-number* 例： `Router(config-xconnect)# member pseudowire 100`	Layer 2 VPN（L2VPN）クロス コネクトを形成するようにメンバー擬似回線を指定します。
ステップ 11	**member gigabitethernet***interface-number* 例： `Router(config-xconnect)# member GigabitEthernet1/0/0.100`	ギガビット イーサネット メンバー インターフェイスのロケーションを指定します。

	コマンドまたはアクション	目的
ステップ 12	**end** 例： `Router(config-xconnect)# end`	特権 EXEC モードに戻ります。

あいまいな AToM の IEEE 802.1Q トンネリング（QinQ）の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacegigabitethernet***slot*/*subslot*/*port*.[*subinterface*]
4. **encapsulationdot1q***vlan-id***second-dot1q**{**any** | *vlan-id*[,*vlan-id*[-*vlan-id*]]}
5. **xconnect***peer-router-idvcidencapsulationmpls*
6. **exit**
7. **interfacegigabitethernet***slot*/*subslot*/*port*.[*subinterface*]
8. **encapsulationdot1q***vlan-id***second-dot1q**{**any** | *vlan-id*[,*vlan-id*[-*vlan-id*]]}
9. **xconnect***peer-router-idvcidencapsulation mpls*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**interfacegigabitethernet***slot*/*subslot*/*port*.[*subinterface*] 例： `Router(config)# interface GigabitEthernet1/0/0.200`	ギガビット イーサネット サブ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。

	コマンドまたはアクション	目的
ステップ 4	**encapsulationdot1q***vlan-id***second-dot1q**{**any** | *vlan-id*[,*vlan-id*[-*vlan-id*]]} 例： `Router(config-if)# encapsulation dot1q 200 second-dot1q 1000-2000,3000,3500-4000`	インターフェイスの Q-in-Q 入力フレームを適切なサービス インスタンスにマッピングする一致基準を定義します。
ステップ 5	**xconnect***peer-router-idvcidencapsulationmpls* 例： `Router(config-if)# xconnect 10.0.0.16 420 encapsulation mpls`	レイヤ 2 パケットを転送するための VC を作成します。
ステップ 6	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 7	**interfacegigabitethernet***slot*/*subslot*/*port*.[*subinterface*] 例： `Router(config)# interface GigabitEthernet1/0/0.201`	次のギガビット イーサネット 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 8	**encapsulationdot1q***vlan-id***second-dot1q**{**any** | *vlan-id*[,*vlan-id*[-*vlan-id*]]} 例： `Router(config-if)# encapsulation dot1q 201 second-dot1q any`	インターフェイスの Q-in-Q 入力フレームを適切なサービス インスタンスにマッピングする一致基準を定義します。
ステップ 9	**xconnect***peer-router-idvcidencapsulation mpls* 例： `Router(config-if)# xconnect 10.0.0.16 430 encapsulation mpls`	レイヤ 2 パケットを転送するための VC を作成します。

あいまいな AToM の IEEE 802.1Q トンネリング（QinQ）の設定（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacegigabitethernet***slot*/*subslot*/*port*.[*subinterface*]
4. **encapsulationdot1q***vlan-id***second-dot1q**{**any** | *vlan-id*[,*vlan-id*[-*vlan-id*]]}
5. **interfacepseudowire***number*
6. **encapsulationmpls**
7. **neighbor***peer-addressvcid-value*
8. **exit**
9. **interfacegigabitethernet***slot*/*subslot*/*port*.[*subinterface*]
10. **encapsulationdot1q***vlan-id***second-dot1q**{**any** | *vlan-id*[,*vlan-id*[-*vlan-id*]]}
11. **interfacepseudowire***number*
12. **encapsulationmpls**
13. **neighbor***peer-addressvcid-value*
14. **exit**
15. **l2vpn xconnectcontext***context-name*
16. **member pseudowire***interface-number*
17. **member gigabitethernet***interface-number*
18. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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。

	コマンドまたはアクション	目的
ステップ 3	**interfacegigabitethernet***slot*/*subslot*/*port*.[*subinterface*] 例： `Router(config)# interface GigabitEthernet1/0/0.200`	ギガビット イーサネット サブ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	**encapsulationdot1q***vlan-id***second-dot1q**{**any** | *vlan-id*[,*vlan-id*[-*vlan-id*]]} 例： `Router(config-if)# encapsulation dot1q 200 second-dot1q 1000-2000,3000,3500-4000`	インターフェイスの Q-in-Q 入力フレームを適切なサービス インスタンスにマッピングする一致基準を定義します。
ステップ 5	**interfacepseudowire***number* 例： `Router(config-if)# interface pseudowire 100`	擬似回線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 6	**encapsulationmpls** 例： `Router(config-if)# encapsulation mpls`	マルチプロトコル ラベル スイッチング（MPLS）がデータ カプセル化方式として使用されることを指定します。
ステップ 7	**neighbor***peer-addressvcid-value* 例： `Router(config-if)# neighbor 10.0.0.1 123`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 8	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 9	**interfacegigabitethernet***slot*/*subslot*/*port*.[*subinterface*] 例： `Router(config)# interface GigabitEthernet1/0/0.201`	次のギガビット イーサネット 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。

あいまいな ATOM の IEEE 802.1Q トンネリング（QinQ）の設定（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

	コマンドまたはアクション	目的
ステップ 10	**encapsulationdot1q***vlan-id***second-dot1q**{**any** | *vlan-id*[,*vlan-id*[-*vlan-id*]]} 例： `Router(config-if)# encapsulation dot1q 201 second-dot1q any`	インターフェイスの Q-in-Q 入力フレームを適切なサービス インスタンスにマッピングする一致基準を定義します。
ステップ 11	**interfacepseudowire***number* 例： `Router(config-if)# interface pseudowire 100`	擬似回線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 12	**encapsulationmpls** 例： `Router(config-if)# encapsulation mpls`	マルチプロトコル ラベル スイッチング（MPLS）がデータ カプセル化方式として使用されることを指定します。
ステップ 13	**neighbor***peer-addressvcid-value* 例： `Router(config-if)# neighbor 10.0.0.1 123`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 14	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 15	**l2vpn xconnectcontext***context-name* 例： `Router(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect コンフィギュレーション モードを開始します。
ステップ 16	**member pseudowire***interface-number* 例： `Router(config-xconnect)# member pseudowire 100`	Layer 2 VPN（L2VPN）クロス コネクトを形成するようにメンバー擬似回線を指定します。
ステップ 17	**member gigabitethernet***interface-number* 例： `Router(config-xconnect)# member GigabitEthernet1/0/0.201`	ギガビット イーサネット メンバー インターフェイスのロケーションを指定します。

	コマンドまたはアクション	目的
ステップ 18	**end** 例： `Router(config-xconnect)# end`	特権 EXEC モードに戻ります。

ATM の IEEE 802.1Q トンネリング（QinQ）の設定の確認

手順の概要

1. イネーブル化
2. **showmplsl2transportvc**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showmplsl2transportvc** 例： `Router# show mpls l2transport vc`	ルータ上でレイヤ 2 パケットをルーティングするために有効化された Any Transport over MPLS（AToM）仮想回線（VC）とスタティック擬似回線に関する情報を表示します。

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した ATM 設定の IEEE 802.1Q トンネリング（QinQ）の確認

手順の概要

1. イネーブル化
2. **showl2vpnatomvc**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show l2vpn atom vc** 例： `Device# show l2vpn atom vc`	ルータ上でレイヤ 2 パケットをルーティングするために有効化された Any Transport over MPLS（AToM）仮想回線（VC）とスタティック擬似回線に関する情報を表示します。

ATM の IEEE 802.1Q トンネリング（QinQ）の設定例

例：あいまいさのない ATM の IEEE 802.1Q トンネリング（QinQ）の設定

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet1/0/0.100
Router(config-if)# encapsulation dot1q 100 second-dot1q 200
Router(config-if)# xconnect 10.0.0.16 410 encapsulation mpls
```

あいまいさのない ATM の IEEE 802.1Q トンネリング（QinQ）の設定の例（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet1/0/0.100
Router(config-if)# encapsulation dot1q 100 second-dot1q 200
Router(config-if)# interface pseudowire 100
Router(config-if)# encapsulation mpls
Router(config-if)# neighbor 10.0.0.1 123
Router(config-if)# exit
Router(config)# l2vpn xconnect context A
Router(config-xconnect)# member pseudowire 100
Router(config-xconnect)# member GigabitEthernet1/0/0.100
```

例：あいまいな ATM の IEEE 802.1Q トンネリング（QinQ）の設定

次に、あいまいな ATM の IEEE 802.1Q トンネリング（QinQ）の設定例を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet1/0/0.200
Router(config-if)# encapsulation dot1q 200 second-dot1q 1000-2000,3000,3500-4000
Router(config-if)# xconnect 10.0.0.16 420 encapsulation mpls
Router(config-if)# exit
Router(config)# interface GigabitEthernet1/0/0.201
Router(config-if) encapsulation dot1q 201 second-dot1q any
Router(config-if) xconnect 10.0.0.16 430 encapsulation mpls
```

あいまいなATMのIEEE802.1Qトンネリング（QinQ）の設定の例（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

次に、あいまいな ATM の IEEE 802.1Q トンネリング（QinQ）の設定例を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet1/0/0.200
Router(config-if)# encapsulation dot1q 200 second-dot1q 1000-2000,3000,3500-4000
Router(config-if)# interface pseudowire 100
Router(config-if)# encapsulation mpls
Router(config-if)# neighbor 10.0.0.1 123
Router(config-if)# exit
Router(config)# l2vpn xconnect context A
Router(config-xconnect)# member pseudowire 100
Router(config-xconnect)# member GigabitEthernet1/0/0.200
Router(config-xconnect)# exit
Router(config)# interface GigabitEthernet1/0/0.201
Router(config-if) encapsulation dot1q 201 second-dot1q any
Router(config-if)# interface pseudowire 100
Router(config-if)# encapsulation mpls
Router(config-if)# neighbor 10.0.0.1 123
Router(config-if)# exit
Router(config)# l2vpn xconnect context A
Router(config-xconnect)# member pseudowire 100
Router(config-xconnect)# member GigabitEthernet1/0/0.201
```

例：ATM の IEEE 802.1Q トンネリング（QinQ）の設定の確認

次に、EoMPLS QinQ モードで VC 設定を確認する **show mpls l2transport vc** コマンドの出力例を示します。

```
router# show mpls l2transport vc
Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
Gi1/0/0.1      Eth VLAN:100/200           10.1.1.2        1          UP
```

例：ATM の IEEE 802.1Q トンネリング（QinQ）設定の確認（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

次に、EoMPLS QinQ モードでの仮想回線（VC）設定を確認する **show l2vpn atom vc** コマンドの出力例を示します。

```
Device# show l2vpn atom vc
Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
Gi1/0/0.1      Eth VLAN:100/200           10.1.1.2        1          UP
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
MPLS および MPLS アプリケーションに関連するコマンドの説明	『*Cisco IOS Multiprotocol Label Switching Command Reference*』
AToM および MPLS	Any Transport over MPLS

標準

標準	Title
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB の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 ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC の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	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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。	http://www.cisco.com/cisco/web/support/index.html

AToM の IEEE 802.1Q トンネリング（QinQ）の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、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。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *22*：*AToM の IEEE 802.1Q トンネリング（QinQ）の機能情報*

機能名	リリース	機能情報
AToM の IEEE 802.1Q トンネリング（QinQ）	Cisco IOS XE Release 2.4	この機能により、AToM に対して IEEE 802.1Q トンネリング（QinQ）を設定できます。また、マルチプロトコル ラベル スイッチング（MPLS）レイヤ 2 VPN（L2VPN）用に QinQ タグを書き換えることもできます。 Cisco IOS XE Release 2.4 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入または変更されました：**interface**、**encapsulationdot1qsecond-dot1q**、**xconnect**。

第 12 章

管理対象 IPv6 Layer 2 Tunneling Protocol ネットワーク サーバの設定

このドキュメントでは管理型 IPv6 レイヤ 2 トンネル プロトコル ネットワーク サーバ機能を有効にする方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース 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、機能情報の表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シスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

管理対象 IPv6 LNS の前提条件

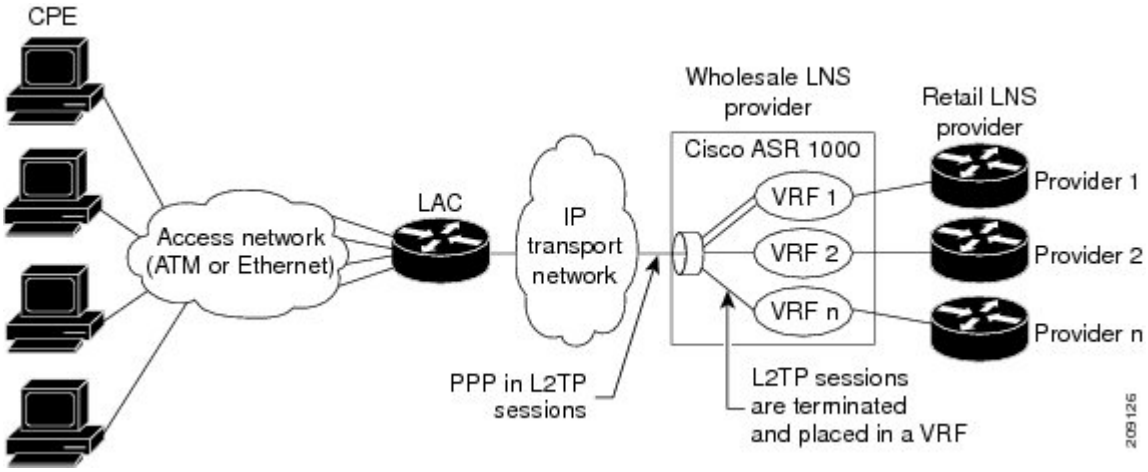
LNS として機能するルータの場合、**aaanew-model** グローバル コンフィギュレーション コマンドを入力することによって、レイヤ2トンネル プロトコル ネットワーク サーバ（LNS）およびレイヤ2アクセス コンセントレータ（LAC）で認証、認可、およびアカウンティング（AAA）を有効にする必要があります。詳細については、『*Cisco IOS XE Security: Securing User Services Configuration Guide*』の「Authentication, Authorization, and Accounting」の章を参照してください。

管理対象 IPv6 LNS に関する情報

L2TP ネットワーク サーバ

LNS はルータとして機能できます。LNS は LAC に対するピアであり、L2TP トンネルの片側に位置します。LNS は LAC と宛先ネットワークとの間でパケットをルーティングします。ルータが LNS として機能している場合、PPP セッションを終了し、最終的な宛先に向けて ISP または社内ネットワークにクライアント IP パケットをルーティングするようにルータを設定できます（下の図を参照）。ルータは、管理型 IPv6 LNS 機能を使用して、LAC からの L2TP セッションを終了し、仮想テンプレート インターフェイスに適用される VRF、または AAA を介してユーザに対して受け取られる VRF に基づいて、適切な IPv6 VRF インスタンスに各セッションを配置することができます。次に、ルータはVRF内の各セッションを宛先ネットワークへルーティングします。

図 *28*：***LAC*** からのセッションの終了と転送



トンネル アカウンティング

トンネルアカウンティング機能は、トンネルに関連する統計情報をRADIUS情報に含める機能を追加することにより、AAAアカウンティングを強化します。トンネルの使用状況に関する情報を収集するには、その前にRADIUSサーバで以下の属性を設定しておく必要があります。

- Acct-Tunnel-Connection：トンネルセッションに割り当てられた識別子を指定します。この属性、およびTunnel-Client-Endpoint属性やTunnel-Server-Endpoint属性は、監査の目的でトンネル セッションを一意に特定する手段を提供します。
- Acct-Tunnel-Packets-Lost：特定のリンク上で失われるパケット数を指定します。

次の表は、RADIUSサーバのトンネル アカウンティングをサポートするAcct-Status-Type属性の値を示します。

表 *23*：*RADIUS* トンネル アカウンティングの *Acct-Status-Type* 値

Acct-Status-Type 値	値	説明
Tunnel-Link-Reject	14	既存のトンネル内での新しいリンクの確立を拒否することをマークします。
Tunnel-Link-Start	12	複数のリンクを送信するL2TPトンネル内のトンネル リンクの作成をマークします。
Tunnel-Link-Stop	13	複数のリンクを送信するL2TPトンネル内のトンネル リンクの削除をマークします。
Tunnel-Reject	11	別のデバイスとのトンネルの確立を拒否することをマークします。
Tunnel-Start	9	別のデバイスとのトンネルの確立をマークします。
Tunnel-Stop	10	別のデバイスとの間のトンネルの削除をマークします。

RADIUSトンネルアカウンティング属性またはRADIUSトンネルアカウンティングをサポートするAcct-Status-Type値の詳細については、RFC 2867（トンネル プロトコル サポートに関するRADIUSアカウンティングの変更）を参照してください。

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る RADIUS アカウンティング属性については、『Cisco IOS XE Security Configuration Guide: Securing User Services』の「RADIUS Attributes」の章を参照してください。

RADIUS の設定の詳細については、RADIUS のユーザ マニュアルを参照してください。

管理対象 LNS の設定方法

LNS での VRF の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **vrfdefinition***vrf-name*
4. **rd***route-distinguisher*
5. **address-family** {**ipv4**|**ipv6**}
6. **route-target** {*import*|*export*|*both*} *route-target-ext-community*
7. **exit-address-family**
8. **address-family** {**ipv4**|**ipv6**}
9. **route-target** {*import*|*export*|*both*} *route-target-ext-community*
10. **end**
11. **showipv6routevrf***vrf-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	イネーブル化 例： `Router> enable`	特権 EXEC モードを開始します。
ステップ 2	**configureterminal** 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。

	コマンドまたはアクション	目的
ステップ 3	**vrfdefinition***vrf-name* 例： `Router(config)# vrf definition vrf1`	VRF ルーティング テーブルを設定し、VRF コンフィギュレーション モードを開始します。 • *vrf-name* 引数は、VRF の名前です。

ステップ 4	**rd***route-distinguisher*
	
	例：
	
	`Router(config-vrf)# rd 100:1`
		VRF のルーティング テーブルと転送テーブルを作成します。
		
		• *route-distinguisher* 引数によって、8 バイトの値が IPv4 プレフィックスに追加され、VPN IPv4 プレフィックスが作成されます。ルート識別子は、次のいずれかの形式で入力できます。
		
		  • 16 ビット ASN：101:3 などの 32 ビット数値
		
		  • 32 ビット IP アドレス：192.168.122.15:1 などの 16 ビット数値

ステップ 5	**address-family** {**ipv4**|**ipv6**} 例： `Router(config-vrf) address-family ipv6`	VRF 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、VRF のアドレス ファミリを指定します。 • **ipv4** キーワードは、VRF の IPv4 アドレス ファミリを指定します。 • **ipv6** キーワードは、VRF の IPv6 アドレス ファミリを指定します。
ステップ 6	**route-target** {*import*|*export*|*both*} *route-target-ext-community* 例： `Router(config-vrf-af) route-target both 100:2`	VRF 用にルート ターゲット拡張コミュニティを作成します。 • **import** キーワードを使用すると、ターゲット VPN 拡張コミュニティからルーティング情報がインポートされます。 • **export** キーワードを使用すると、ルーティング情報がターゲット VPN 拡張コミュニティにエクスポートされます。 • **both** キーワードを使用すると、インポート ルーティング情報とエクスポート ルーティング情報の両方がターゲット VPN 拡張コミュニティにインポートされます。 • *route-target-ext-community* 引数を使用すると、route-target 拡張コミュニティ属性が、インポート、エクスポート、または両方（インポートとエクスポート）の route-target 拡張コミュニティの VRF リストに追加されます。

	コマンドまたはアクション	目的
ステップ 7	**exit-address-family** 例： `Router(config-vrf-af)# exit-address-family`	VRF 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、VRF コンフィギュレーション モードを開始します。
ステップ 8	**address-family** {**ipv4**|**ipv6**} 例： `Router(config-vrf) address-family ipv6`	VRF 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、VRF のアドレス ファミリを指定します。 • **ipv4** キーワードは、VRF の IPv4 アドレス ファミリを指定します。 • **ipv6** キーワードは、VRF の IPv6 アドレス ファミリを指定します。
ステップ 9	**route-target** {*import*|*export*|*both*} *route-target-ext-community* 例： `Router(config-vrf-af)# route-target both 100:3`	VRF 用にルート ターゲット拡張コミュニティを作成します。 • **import** キーワードを使用すると、ターゲット VPN 拡張コミュニティからルーティング情報をインポートすることが指定されます。 • **export** キーワードを使用すると、ルーティング情報をターゲット VPN 拡張コミュニティにエクスポートすることが指定されます。 • **both** キーワードを使用すると、ルーティング情報のターゲット VPN 拡張コミュニティからのインポート、およびターゲット VPN 拡張コミュニティへのエクスポートの両方が行われます。 • *route-target-ext-community* 引数を使用すると、route-target 拡張コミュニティ属性が、インポート、エクスポート、または両方（インポートとエクスポート）の route-target 拡張コミュニティの VRF リストに追加されます。 • **route-target** コマンドは、各ターゲット コミュニティにつき一度ずつ入力します。
ステップ 10	**end** 例： `Router(config-vrf-af)# end`	VRF 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、特権 EXEC モードに戻ります。
ステップ 11	**showipv6routevrf***vrf-name* 例： `Router# show ipv6 route vrf vrf1`	VRF に関連付けられた IPv6 ルーティング テーブルを表示します。

仮想テンプレート インターフェイスの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacevirtual-template***number*
4. **vrfforwarding***name*
5. **pppauthenticationchap**
6. **end**
7. **showinterfacesvirtual-access***number***[configuration]**
8. **debugpppchap**
9. **debugpppnegotiation**
10. **debugpppnegotiationchap**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードを開始します。
ステップ 2	**configureterminal** 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	**interfacevirtual-template***number* 例： `Router(config)# interface virtual-template 1`	仮想テンプレート インターフェイスを作成し、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	**vrfforwarding***name* 例： `Router(config-if)# vrf forwarding vpn-1`	（任意）仮想テンプレート インターフェイスを VRF ルーティング テーブルにマップします。 （注） RADIUS サーバを介して VRF 割り当てを受信した場合は、このステップは不要です。

	コマンドまたはアクション	目的
ステップ 5	**pppauthenticationchap** 例： `Router(config-if)# ppp authentication chap`	仮想テンプレートインターフェイスでCHAP認証を有効にします。これは、仮想アクセスインターフェイス（VAI）に適用されます。
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	**showinterfacesvirtual-access***number***[configuration]** 例： `Router# show interfaces virtual-access number [configuration]`	指定するVAIのステータス、トラフィックデータ、および設定情報を表示します。
ステップ 8	**debugpppchap** 例： `Router# debug ppp chap`	Challenge Authentication Protocol（CHAP）パケット交換の認証プロトコル メッセージを表示します。 • このコマンドは、デバイス間の設定の不一致が原因でCHAP認証が失敗する場合に便利です。ユーザ名とパスワードの不一致を確認して修正すると、この問題は解決します。
ステップ 9	**debugpppnegotiation** 例： `Router# debug ppp negotiation`	PPPを実装するインターネットワークでのトラフィックおよび交換に関する情報を表示します。
ステップ 10	**debugpppnegotiationchap** 例： `Router# debug ppp negotiation chap`	CiscoデバイスとCisco以外のデバイス間での接続の問題が原因で発生したCHAPネゴシエーションの問題を診断します。

RADIUS サーバを介した VRF の割り当て

手順の概要

1. イネーブル化
2. **configureterminal**
3. **aaaauthorizationconfiguration***method-name***group***group-name*
4. **ipv6dhcppool***pool-name*
5. **prefix-delegationaaa** [**method-list***method-list*]
6. **dns-server***ipv6-address*
7. **exit**
8. **interfacevirtual-template***number*
9. **ipv6ndprefixframed-ipv6-prefix**
10. **ipv6dhcpserver***pool-name***rapid-commit**
11. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードを開始します。
ステップ 2	**configureterminal** 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	**aaaauthorizationconfiguration***method-name***group***group-name* 例： `Router(config)# aaa authorization configuration DHCPv6-PD group DHCPv6-PD-RADIUS`	RADIUS を使用して AAA サーバから設定情報をダウンロードします。
ステップ 4	**ipv6dhcppool***pool-name* 例： `Router(config)# ipv6 dhcp pool DHCPv6-PD`	DHCP for IPv6 設定情報プールを設定し、DHCP for IPv6 プール 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 5	**prefix-delegationaaa** [**method-list***method-list*] 例： `Router(config-dhcpv6)# prefix-delegation aaa method-list DHCPv6-PD`	プレフィックスを AAA サーバから取得することを指定します。
ステップ 6	**dns-server***ipv6-address* 例： `Router(config-dhcpv6)# dns-server 2001:0DB8:3000:3000::42`	DHCP for IPv6 クライアントが使用できるドメイン ネーム システム（DNS）IPv6 サーバを指定します。
ステップ 7	**exit** 例： `Router(config-dhcpv6)# exit`	DHCP for IPv6 プール コンフィギュレーション モードを終了します。続いて、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 8	**interfacevirtual-template***number* 例： `Router(config)# interface virtual-template 1`	VAI の作成で動的に設定して適用できるバーチャルテンプレートインターフェイスを作成し、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 9	**ipv6ndprefixframed-ipv6-prefix** 例： `Router(config-if)# ipv6 nd prefix framed-ipv6-prefix`	受信した RADIUS framed IPv6 prefix 属性のプレフィックスを、インターフェイスのネイバー探索プレフィックス キューに追加します。
ステップ 10	**ipv6dhcpserver***pool-name***rapid-commit** 例： `Router(config-if)# ipv6 dhcp server DHCPv6-PD rapid-commit`	インターフェイスに対して DHCPv6 をイネーブルにします。
ステップ 11	**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。

L2TP トラフィックを開始および受信するための LNS の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **vpdnenable**
4. **vpdn-group***group-name*
5. **accept-dialin**
6. **protocol12tp**
7. **virtual-template***template-number*
8. **exit**
9. **terminate-fromhostname***hostname*
10. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードを開始します。
ステップ 2	**configureterminal** 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	**vpdnenable** 例： `Router(config)# vpdn enable`	ルータ上で VPDN ネットワーキングを有効にして、ローカル データベースと存在する場合はリモート認証サーバ（ホーム ゲートウェイ）でトンネル定義を検索するようにルータに指示します。
ステップ 4	**vpdn-group***group-name* 例： `Router(config)# vpdn-group group1`	他の VPDN 変数を割り当てることが可能なローカル グループ名を定義します。 • VPDN グループ 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 5	**accept-dialin** 例： `Router(config-vpdn)# accept-dialin`	LAC からのトンネル PPP 接続を受け入れるように LNS を設定し、accept-dialin VPDN サブグループを作成します。 • accept dial-in VPDN サブグループ コンフィギュレーション モードを開始します。
ステップ 6	**protocol12tp** 例： `Router(config-vpdn-acc-in)# protocol 12tp`	レイヤ 2 トンネル プロトコルを指定します。
ステップ 7	**virtual-template***template-number* 例： `Router(config-vpdn-acc-in)# virtual-template 1`	VAI の複製に使用される仮想テンプレートを指定します。
ステップ 8	**exit** 例： `Router(config-vpdn-acc-in)# exit`	VPDN グループ コンフィギュレーション モードに戻ります。
ステップ 9	**terminate-fromhostname***hostname* 例： `Router(config-vpdn)# terminate-from hostname lac1-vpn1`	VPDN トンネルの受け入れ時に必要なリモート LAC のホスト名を指定します。
ステップ 10	**end** 例： `Router(config-vpdn)# end`	VPDN コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

トンネルあたりのセッション数の制限

手順の概要

1. イネーブル化
2. **configureterminal**
3. **vpdn-group***group-name*
4. **accept-dialin**
5. **protocol12tp**
6. **virtual-template***template-number*
7. **exit**
8. **terminate-fromhostname***host-name*
9. **session-limit***limit-number*
10. **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	イネーブル化 例： `Router> enable`	特権 EXEC モードを開始します。
ステップ 2	**configureterminal** 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	**vpdn-group***group-name* 例： `Router(config)# vpdn-group group1`	他の VPDN 変数を割り当てることが可能なローカル グループ名を定義します。 • VPDN グループ 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	**accept-dialin** 例： `Router(config-vpdn)# accept-dialin`	LAC からのトンネル PPP 接続を受け入れるように LNS を設定し、accept-dialin VPDN サブグループを作成します。 • accept dial-in VPDN サブグループ 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 5	**protocol12tp** 例： `Router(config-vpdn-acc-in)# protocol 12tp`	レイヤ 2 トンネル プロトコルを指定します。
ステップ 6	**virtual-template***template-number* 例： `Router(config-vpdn-acc-in)# virtual-template 1`	VAI の複製に使用される仮想テンプレートを指定します。
ステップ 7	**exit** 例： `Router(config-vpdn-acc-in)# exit`	VPDN グループ コンフィギュレーション モードに戻ります。
ステップ 8	**terminate-fromhostname***host-name* 例： `Router(config-vpdn)# terminate-from hostname test_LAC`	VPDN トンネルの受け入れ時に必要なリモート LAC のホスト名を指定します。
ステップ 9	**session-limit***limit-number* 例： `Router(config-vpdn)# session-limit 100`	トンネルあたりの最大セッション数を指定します。
ステップ 10	**exit** 例： `Router(config-vpdn)# exit`	VPDN コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

RADIUS 属性許可リストまたは拒否リストの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **aaaauthenticationpppdefaultgroup***group-name*
4. **aaaauthorizationnetworkgroupgroup***group-name*
5. **aaagroupserverradius***group-name*
6. **server-private***ip-address* [**acct-port***port-number*][**timeout***seconds*] [**retransmit***retries*] [**key***string*]
7. **authorization** [**accept**|**reject**] *list-name*
8. **exit**
9. **radius-serverattributelist***listname*
10. **attribute***value1* [*value2* [*value3...*]]
11. **end**
12. **showaccounting**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードを開始します。
ステップ 2	**configureterminal** 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	**aaaauthenticationpppdefaultgroup***group-name* 例： `Router(config)# aaa authentication ppp default group radius_authen1`	PPP を実行しているシリアルインターフェイス上で使用する 1 つまたは複数の AAA 認証方式を指定します。
ステップ 4	**aaaauthorizationnetworkgroupgroup***group-name* 例： `Router(config)# aaa authorization network group group radius_authen1`	ネットワーク アクセスをユーザに制限するパラメータを設定します。

	コマンドまたはアクション	目的
ステップ 5	**aaagroupserverradius***group-name* 例： `Router(config)# aaa group server radius VPDN-Group`	異なる RADIUS サーバ ホストを別々のリストと方式にグループ化し、server-group RADIUS コンフィギュレーション モードを開始します。
ステップ 6	**server-private***ip-address* [**acct-port***port-number*][**timeout***seconds*] [**retransmit***retries*] [**key***string*] 例： `Router(config-sg-radius)# server-private 10.1.1.2 acct-port 0 timeout 7 retransmit 3 key cisco1`	グループ サーバに対するプライベート RADIUS サーバの IP アドレスを設定します。 • *ip-address* 引数は、プライベート RADIUS サーバ ホストの IP アドレスを指定します。 • （任意）*port-number* 引数は、アカウンティング要求のための UDP 宛先ポートを指定します。 • （任意）*seconds* 引数は、タイムアウト値（1 ～ 1000）を指定します。 • （任意）*retries* 引数は、サーバが応答しないまたはサーバの応答が遅い場合に、RADIUS 要求がサーバに再送信される回数を指定します。 • *string* 引数は、ルータと RADIUS サーバ間でのすべての RADIUS 通信用の認証および暗号キーを指定します。
ステップ 7	**authorization** [**accept**|**reject**] *list-name* 例： `Router(config-sg-radius)# authorization accept vpn1-autho-list`	RADIUS サーバから Access-Accept パケット内で返す属性用のフィルタを指定します。 • **accept** キーワードは、*listname* 引数で指定された属性を除くすべての属性が拒否されることを示します。 • **reject** キーワードは、*listname* 引数で指定された属性とすべての標準属性を除くすべての属性が許可されることを示します。
ステップ 8	**exit** 例： `Router(config-sg-radius)# exit`	サーバ グループ RADIUS 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。

	コマンドまたはアクション	目的
ステップ 9	**radius-serverattributelist***listname* 例： `Router(config)# radius-server attribute list vpn1-autho-list`	**attribute** コマンドを使用して定義された属性のセットに付けるリスト名を定義して、RADIUS 属性リスト コンフィギュレーション モードを開始します。 • ステップ 7 で定義したものと同じになる *listname* 引数を定義します。
ステップ 10	**attribute***value1* [*value2* [*value3...*]] 例： `Router(config-radius-attrl)# attribute 26,200`	設定した許可リストまたは拒否リストに属性を追加します。 • このコマンドは、許可リストまたは拒否リストに属性を追加するために何回も使用できます。
ステップ 11	**end** 例： `Router(config-radius-attrl)# end`	RADIUS 属性リスト コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 12	**showaccounting** 例： `Router# show accounting`	現在ログインしているユーザのアカウンティング レコードを表示します。 • ネットワーク上でアクティブなアカウント可能イベントを表示して、アカウンティング サーバ上でのデータ消失イベント時の情報収集を支援します。

名前付き方式リストによる AAA アカウンティングの設定

（注） システム アカウンティングは、名前付き方式リストを使用しません。システム アカウンティングの場合、デフォルトの方式リストだけを定義できます。詳細については、『Cisco IOS XE Security Configuration Guide: Securing User Services』の「Configuring Authentication」の章を参照してください。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **aaaaccountingnetwork***list-name***start-stopgroupradius**
4. **line** [**aux** | **console**| **vty**] [*line-number*]
5. **accounting** {**arap**|**commands***level*|**connection**|**exec**|**resource**} [**default** | *list-name*]
6. **end**
7. **debugaaaaccounting**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードを開始します。
ステップ 2	**configureterminal** 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	**aaaaccountingnetwork***list-name***start-stopgroupradius** 例： `Router(config)# aaa accounting network methodlist start-stop group radius`	アカウンティング方式リストを作成し、アカウンティングを有効にします。
ステップ 4	**line** [**aux**	**console**| **vty**] [*line-number*] 例： `Router(config)# line console 0`	アカウンティング方式リストを適用する回線のライン コンフィギュレーション モードを開始します。
ステップ 5	**accounting** {**arap**|**commands***level*|**connection**|**exec**|**resource**} [**default**	*list-name*] 例： `Router(config-line)# accounting commands 15 list1`	1 つの回線または複数回線にアカウンティング方式リストを適用します。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Router(config-line)# end`	回線コンフィギュレーションモードを終了します。続いて、特権 EXEC モードに戻ります。
ステップ 7	**debugaaaaccounting** 例： `Router# debug aaa accounting`	説明の義務があるイベントが発生したときに、その情報を表示します。

LNS 上での RADIUS トンネル認証方式リストの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **aaa authorization network** *list-name method1* [*method2...*]
4. **vpdn tunnel authorization network** *lmethod-ist-name method1* [*method2...*]
5. **vpdn tunnel authorization virtual-template** *vtemplate-number*
6. **vpdn tunnel authorization password** *dummy-password*
7. **debug aaa authorization**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードを開始します。
ステップ 2	**configureterminal** 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。

	コマンドまたはアクション	目的
ステップ 3	**aaa authorization network** *list-name method1* [*method2...*] 例： `Router(config)# aaa authorization network mymethodlist group VPDN-Group`	ネットワークへのユーザ アクセスを制限するパラメータを設定します。 • *list-name* 引数は、ユーザがログインするときに試される認証方式のリストに名前を付けるための文字列です。 • **group radius**：すべての RADIUS サーバのリストを認証に使用します。 • **group** *group-name*：**aaa group server radius** コマンドで定義されたように RADIUS サーバのサブセットを認証に使用します。 • **if-authenticated**：ユーザが認証に成功した場合に成功します。 • **local**：ローカルユーザ名データベースを認証に使用します。 • **none**：認証を使用しません。 （注） 方式リストは、ドメインやデジタル番号識別サービス（DNIS）の認証ではなく、VPDN トンネルの認証と終端専用です。そのため、方式リストは、トンネル終端デバイス（ダイヤルアウトセッション用の LAC とダイヤルイン セッション用の LNS）にのみ適用されます。
ステップ 4	**vpdn tunnel authorization network** *lmethod-ist-name method1* [*method2...*] 例： `Router(config)# vpdn tunnel authorization network mymethodlist`	VPDN リモート トンネル ホスト名ベースの認証に使用する AAA 方式リストを指定します。 • **vpdn tunnel authorization network** コマンドを使用して方式リスト（デフォルトの方式リストを含む）を指定しなかった場合は、ローカル認証がローカル VPDN グループ設定を使用して実行されます。
ステップ 5	**vpdn tunnel authorization virtual-template** *vtemplate-number* 例： `Router(config)# vpdn tunnel authorization virtual-template 10`	VAI の複製に使用されるデフォルトの仮想テンプレートインターフェイスを指定します。 • ローカル VPDN グループ設定またはリモート RADIUS 設定で仮想テンプレート インターフェイスを指定しなかった場合は、デフォルトの仮想テンプレート インターフェイスが使用されます。

	コマンドまたはアクション	目的
ステップ 6	**vpdn tunnel authorization password** *dummy-password* 例： `Router(config)# vpdn tunnel authorization password mypassword`	リモート トンネル ホスト名に基づいてトンネル設定を取得するための RADIUS 認証要求に使用するパスワードを指定します。
ステップ 7	**debug aaa authorization** 例： `Router# debug aaa authorization`	AAA 認証に関する情報を表示します。

RADIUS トンネル認証の LNS の設定

RADIUS トンネル認証用の LNS を設定するには、次の作業を実行します。

（注） Cisco ASR 1000 シリーズ アグリゲーション サービス ルータは L2TP トンネル認証をサポートしています。ただし、RADIUS は L2TP トンネル タイムアウト、L2TP トンネル hello 間隔、および L2TP トンネル受信ウィンドウ サイズといったパラメータ値の属性を提供しません。Cisco ASR 1000 シリーズ アグリゲーション サービス ルータがパラメータの RADIUS 属性を受信しない場合、ルータはデフォルト値を使用します。

LNS 上での RADIUS トンネル認証方式リストの設定

RADIUS トンネル認証用に LNS 上の方式リストを設定するには、次のタスクを実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **aaaauthorizationnetwork***list-namemethod1* [*method2...*]
4. **vpdntunnelauthorizationnetwork***method-list-name*
5. **vpdntunnelauthorizationvirtual-template***vtemplate-number*
6. **vpdntunnelauthorizationpassword***dummy-password*
7. **end**
8. **debugaaaauthorization**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードを開始します。
ステップ 2	**configureterminal** 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	**aaaauthorizationnetwork***list-namemethod1* [*method2...*]
	
	例：
	
	`Router(config)# aaa authorization network mymethodlist group VPDN-Group`
		ネットワークへのユーザ アクセスを制限するパラメータを設定します。
		
		• *list-name* 引数は、ユーザがログインするときに試される認証方式のリストに名前を付けるための文字列です。
		
		  • **groupradius**：すべての RADIUS サーバのリストを認証に使用します。
		
		  • **group***group-name*：**aaagroupserverradius** コマンドで定義されたように RADIUS サーバのサブセットを認証に使用します。
		
		  • **if-authenticated**：ユーザが認証に成功した場合に成功します。
		
		  • **local**：ローカルユーザ名データベースを認証に使用します。
		
		  • **none**：認証を使用しません。
		
		（注） 方式リストは、ドメインやデジタル番号識別サービス（DNIS）の認証ではなく、VPDN トンネルの認証と終端専用です。そのため、方式リストは、トンネル終端デバイス（ダイヤルアウトセッション用の LAC とダイヤルイン セッション用の LNS）にのみ適用されます。

	コマンドまたはアクション	目的
ステップ 4	**vpdntunnelauthorizationnetwork***method-list-name* 例： `Router(config)# vpdn tunnel authorization network mymethodlist`	VPDN リモート トンネル ホスト名ベースの認証に使用する AAA 方式リストを指定します。 • **vpdntunnelauthorizationnetwork** コマンドを使用して方式リスト（デフォルトの方式リストを含む）を指定しなかった場合は、ローカル認証がローカル VPDN グループ設定を使用して実行されます。
ステップ 5	**vpdntunnelauthorizationvirtual-template***vtemplate-number* 例： `Router(config)# vpdn tunnel authorization virtual-template 10`	VAI の複製に使用されるデフォルトの仮想テンプレート インターフェイスを指定します。 • ローカル VPDN グループ設定またはリモート RADIUS 設定で仮想テンプレート インターフェイスを指定しなかった場合は、デフォルトの仮想テンプレートインターフェイスが使用されます。 （注） **vpdntunnelauthorizationvirtual-template** コマンドは LNS 上でのみ適用できます。
ステップ 6	**vpdntunnelauthorizationpassword***dummy-password* 例： `Router(config)# vpdn tunnel authorization password mypassword`	リモート トンネル ホスト名に基づいてトンネル設定を取得するための RADIUS 認証要求に使用するパスワードを指定します。 • デフォルトで、パスワードは cisco ですが、他のパスワードを設定することもできます。 （注） **vpdntunnelauthorizationpassword** コマンドは、LAC と LNS の両方で適用できます。
ステップ 7	**end** 例： `Router(config)# end`	グローバル 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 8	**debugaaaauthorization** 例： `Router# debug aaa authorization`	AAA 認証に関する情報を表示します。

AAA 認証方式の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **aaanew-model**
4. RADIUS セキュリティ プロトコル パラメータを設定します。RADIUS の詳細については、『Cisco IOS XE Security Configuration Guide: Securing User Services』の「Configuring RADIUS」の章を参照してください。
5. **aaaauthentication**
6. 必要に応じて、インターフェイス、回線、または回線セットに認証リストを適用します。認証方式リストの詳細については、『Cisco IOS XE Security Configuration Guide: Securing User Services』の「Configuring Authentication」の章を参照してください。
7. **end**

手順の詳細

ステップ 1 イネーブル化

ステップ 2 **configureterminal**

ステップ 3 **aaanew-model**
グローバル コンフィギュレーション モードでこのコマンドを入力し、AAA を有効にします。

ステップ 4 RADIUS セキュリティ プロトコル パラメータを設定します。RADIUS の詳細については、『Cisco IOS XE Security Configuration Guide: Securing User Services』の「Configuring RADIUS」の章を参照してください。

ステップ 5 **aaaauthentication**
このコマンドを入力して、認証方式リストを定義します。

ステップ 6 必要に応じて、インターフェイス、回線、または回線セットに認証リストを適用します。認証方式リストの詳細については、『Cisco IOS XE Security Configuration Guide: Securing User Services』の「Configuring Authentication」の章を参照してください。

ステップ 7 **end**

管理対象 IPv6 Layer 2 Tunneling Protocol ネットワーク サーバの設定例

例：管理対象 IPv6 LNS の設定

次に、ルータ上で管理対象 IPv6 LNS 機能を設定する例を示します。この例では、ルータが LAC からのトンネルを終端し、VRF にインターフェイスと仮想テンプレートインターフェイスを関連付けます。この設定では、VRF の RADIUS 属性スクリーニングと AAA アカウンティングを設定する方法も示しています。

```
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
vrf definition user_vrf1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 !
 address-family ipv6
 exit-address-family
!
logging buffered 10000000
enable password lab
!
aaa new-model
!
!
aaa group server radius radius_authen1
 server-private 10.1.1.2 acct-port 0 timeout 7 retransmit 3 key cisco1
 ip radius source-interface Loopback20000
!
aaa authentication login default none
aaa authentication ppp default group radius_authen1
aaa authorization network default group radius_authen1
aaa authorization configuration DHCPv6-PD group radius_authen1
!
!
!
!
!
aaa session-id common
aaa policy interface-config allow-subinterface
ppp hold-queue 80000
clock timezone EST -5 0
ip source-route
no ip gratuitous-arps
!
!
!
!
!
!
!
no ip domain lookup
```

```
ip host mcp-matrix 10.0.0.2
ip host mcp-sun-2 10.0.0.2
!
!
ipv6 unicast-routing
ipv6 dhcp binding track ppp
ipv6 dhcp pool ipv6_dhcp_pool1
 prefix-delegation aaa method-list DHCPv6-PD
!
!
!
!
multilink bundle-name authenticated
vpdn enable
!
vpdn-group VPDN_LNS1
 accept-dialin
  protocol l2tp
  virtual-template 1
 terminate-from hostname test_LAC1
 source-ip 10.0.0.2
 local name test_LNS1
 l2tp tunnel password 0 tunnel1
 l2tp tunnel receive-window 100
 l2tp tunnel timeout no-session 30
 l2tp tunnel retransmit retries 7
 l2tp tunnel retransmit timeout min 2
!
!
no virtual-template snmp
!
!
!
!
!
!
!
!
!
username asifp1@test1 password 0 hello1
!
redundancy
 notification-timer 30000
 mode none
!
!
!
!
!
ip tftp source-interface GigabitEthernet 0
!
!
!
!
!
!
!
!
interface Loopback1
 no ip address
!
interface Loopback20000
 ip address 209.165.202.131 255.255.255.224
!
interface GigabitEthernet1/1/0
 mac-address 8888.8888.8888
 no ip address
 load-interval 30
 negotiation auto
 hold-queue 4096 in
 hold-queue 4096 out
!
interface GigabitEthernet1/1/0.1
```

```
 encapsulation dot1Q 3
 ip address 209.165.202.132 255.255.255.224
!
interface GigabitEthernet1/1/1
 mac-address 4444.4444.4444
 no ip address
 load-interval 30
 no negotiation auto
 hold-queue 4096 in
 hold-queue 4096 out
!
interface GigabitEthernet1/1/1.1
 vrf forwarding user_vrf1
 encapsulation dot1Q 2
 ipv6 address 12::1/72
!
interface GigabitEthernet1/1/2
 no ip address
 negotiation auto
!
interface GigabitEthernet1/1/3
 no ip address
 negotiation auto
!
interface GigabitEthernet1/1/4
 no ip address
 negotiation auto
!
interface GigabitEthernet1/1/5
 no ip address
 negotiation auto
!
interface GigabitEthernet1/1/6
 no ip address
 negotiation auto
!
interface GigabitEthernet1/1/7
 description Connected to RADIUS
 ip address 209.165.201.1 255.255.255.224
 negotiation auto
!
interface GigabitEthernet1/3/0
 no ip address
 media-type sfp
 negotiation auto
!
interface GigabitEthernet1/3/1
 no ip address
 media-type sfp
 negotiation auto
!
interface GigabitEthernet 0
 vrf forwarding Mgmt-intf
 ip address 209.165.201.1 255.255.255.224
 negotiation auto
!
interface Virtual-Template 1
 no ip address
 no logging event link-status
 ipv6 dhcp server ipv6_dhcp_pool1 rapid-commit
 keepalive 30
 ppp mtu adaptive
 ppp authentication pap
!
ip default-gateway 10.1.0.5
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip route vrf Mgmt-intf 209.165.201.1 255.255.255.254 172.16.1.1
ip route vrf Mgmt-intf 209.165.201.29 255.255.255.224 172.16.0.1
!
ip radius source-interface GigabitEthernet1/1/7
```

```
logging esm config
cdp run
ipv6 route vrf user_vrf1 ::/0 12::2
!
ipv6 neighbor 12::2 GigabitEthernet1/1/1.1 2222.2222.2222
!
!
!
control-plane
!
call admission limit 90
!
!
!
alias exec call show caller summ
alias exec caller show caller summ
alias exec palt show plat
alias exec plat show platform
alias exec evsi sho plat hard cpp act feat ess stat
!
line con 0
 exec-timeout 0 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 password password1
!
exception data-corruption buffer truncate
end
```

例：LNS トンネル アカウンティングの設定

次に、トンネル アカウンティング レコードを RADIUS サーバに送信するように LNS を設定する例を示します。

```
aaa new-model
!
!
aaa accounting network m1 start-stop group radius
aaa accounting network m2 stop-only group radius
aaa session-id common
enable secret 5 $1$ftf.$wE6Q5Yv6hmQiwL9pizPCg1
!
username ENT_LNS password 0 tunnelpass
username user1@example.com password 0 lab
username user2@example.com password 0 lab
spe 1/0 1/7
firmware location system:/ucode/mica_port_firmware
spe 2/0 2/9
firmware location system:/ucode/mica_port_firmware
!
!
resource-pool disable
clock timezone est 2
!
ip subnet-zero
no ip domain-lookup
ip host CALLGEN-SECURITY-V2 10.24.80.28 10.47.0.0
ip host dirt 172.16.1.129
!
vpdn enable
vpdn tunnel accounting network m1
vpdn session accounting network m1
!
vpdn-group 1
accept-dialin
protocol l2tp
virtual-template 1
```

```
terminate-from hostname ISP_LAC
local name ENT_LNS
!
isdn switch-type primary-5ess
!
!
fax interface-type modem
mta receive maximum-recipients 0
!
interface Loopback 0
ip address 172.16.0.101 255.255.255.0
!
interface Loopback 1
ip address 192.168.0.101 255.255.255.0
!
interface Ethernet 0
ip address 10.1.26.71 255.255.255.0
no ip mroute-cache
no cdp enable
!
interface virtual-template 1
ip unnumbered Loopback 0
peer default ip address pool vpdn-pool1
ppp authentication chap
!
interface virtual-template 2
ip unnumbered Loopback1
peer default ip address pool vpdn-pool2
ppp authentication chap
!
interface fastethernet 0
no ip address
no ip mroute-cache
shutdown
duplex auto
speed auto
no cdp enable
!
ip local pool vpdn-pool1 172.16.5.1 172.16.128.100
ip local pool vpdn-pool2 10.0.0.1 10.0.0.100
ip default-gateway 10.1.26.254
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.26.254
ip route 192.168.1.2 255.255.255.255 10.1.26.254
no ip http server
ip pim bidir-enable
!
!
dialer-list 1 protocol ip permit
no cdp run
!
!
radius-server host 172.16.192.80 auth-port 1645 acct-port 1646 key rad123
radius-server retransmit 3
call rsvp-sync
end
```

（注） その他のアカウンティングの例については、『Cisco IOS XE Security: Secure Services Configuration Guide』の「Configuring Accounting」の章を参照してください。

例：RADIUS サーバでのユーザ プロファイルの確認

次に、RADIUS サーバのユーザ プロファイルの例を示します。Cisco ASR 1000 シリーズ アグリゲーション サービス ルータは、RADIUS サーバからユーザ プロファイルの情報を取得します。

```
Radius Profile "user1"
Auth-Type = Local, User-Password = "pwd"
User-Service-Type = Framed-User
Framed-Protocol = PPP
cisco-avpair = "lcp:interface-config=vrf forwarding VRF01"
cisco-avpair = "lcp:interface-config=ipv6 unnumbered loopback1"
Framed-IPv6-Prefix = "2001:DB8:4567:1234::/64"
Delegated-IPv6-Prefix = "2001:DB8:AAAA::/48"
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco IOS XE MPLS コマンド	『*Cisco IOS MPLS Command Reference*』
認証、許可、およびアカウンティング	認証、許可、アカウンティング（AAA）
RADIUS の設定	RADIUS の設定
アカウンティングの設定	「Configuring Accounting」
RADIUS 属性	『Cisco IOS XE Security Configuration Guide: Securing User Services』の「RADIUS Attributes Overview and RADIUS IETF Attributes」モジュール

標準

規格	Title
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 のリンク
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 ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
RFC 2867	「RADIUS Accounting Modifications for Tunnel Protocol Support」

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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。	http://www.cisco.com/cisco/web/support/index.html

管理対象 IPv6 Layer 2 Tunneling Protocol ネットワーク サーバの設定の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、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。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *24*：管理対象 *IPv6 Layer 2 Tunneling Protocol* ネットワーク サーバの機能情報

機能名	リリース	機能情報
管理対象 IPv6 Layer 2 Tunneling Protocol ネットワーク サーバ	Cisco IOS XE Release 3.3S	管理対象 IPv6 LNS 機能により、サービス プロバイダーがリモート ユーザに対し、IPv4 および IPv6 の両方のサービスからなるスケーラブルなエンドツーエンド VPN を提供できます。この機能は、マルチプロトコル ラベル スイッチング（MPLS）対応バックボーンとブロードバンド アクセス機能を統合します。 次のコマンドが導入または変更されました。 atm pppatm passive、radius-server attribute list、radius-server key、radius-server retransmit、radius-server vsa send。
管理対象 IPv6 Layer 2 Tunneling Protocol ネットワーク サーバ：VRF-Lite のみ	Cisco IOS XE Release 3.3S	管理対象 IPv6 LNS 機能により、サービス プロバイダーがリモート ユーザに対し、IPv4 および IPv6 の両方のサービスからなるスケーラブルなエンドツーエンド VPN を提供できます。この機能により、VRF-Lite 対応バックボーンとブロードバンド アクセス機能が統合されます。

機能名	リリース	機能情報
管理対象 IPv6 Layer 2 Tunneling Protocol ネットワーク サーバ：MPLS VPN	Cisco IOS XE Release 3.7S	管理対象 IPv6 LNS 機能により、サービス プロバイダーがリモート ユーザに対し、IPv4 および IPv6 の両方のサービスからなるスケーラブルなエンドツーエンド VPN を提供できます。この機能は、MPLS 対応バックボーンとブロードバンドアクセス機能を統合します。

第 13 章

L2VPN 擬似回線冗長性

L2VPN 擬似回線冗長性機能を使用すると、ネットワーク内の障害を検出して、サービスの提供を続行可能な別のエンドポイントにレイヤ2（L2）サービスを再ルーティングするようにネットワークを設定できます。この機能を使用すると、リモート プロバイダー エッジ（PE）ルータまたは PE とカスタマー エッジ（CE）ルータの間のリンクの障害から復旧できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース 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、機能情報の表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シスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

L2VPN 擬似回線冗長性の前提条件

- このフィーチャ モジュールを使用するには、基本的な L2 バーチャル プライベート ネットワーク（VPN）を設定する方法を理解していることが必要です。
  - Any Transport over MPLS
  - 『L2 VPN Interworking』
  - Layer 2 Tunneling Protocol Version 3（L2TPv3）
- L2VPN擬似回線冗長性機能では、ネットワーク内の障害を検出できるように、次のメカニズムが存在している必要があります。
  - ラベル スイッチド パス（LSP）ping/traceroute および Any Transport over MPLS Virtual Circuit Connection Verification（AToM VCCV）
  - ローカル管理インターフェイス（LMI）
  - 運用管理および保守（OAM）

L2VPN 擬似回線冗長性の制約事項

- ラベル配布プロトコル（LDP）のデフォルトのセッション ホールドダウン タイマーでは、約 180 秒以内に障害を検出できます。ソフトウェアがより早く障害を検出できるように、この時間を設定することができます。詳細については、**mpls ldp holdtime** コマンドを参照してください。
- L2VPN 擬似回線の冗長性は、L2TPv3 での擬似回線インターワーキング モードをサポートしていません。擬似回線クラスにインターワーキング IP が設定されている場合、CE 間の接続が影響を受ける場合があります。
- プライマリおよびバックアップ擬似回線では、同じ種類のトランスポート サービスが動作している必要があります。プライマリおよびバックアップ擬似回線は、AToM または L2TPv3 で設定されている必要があります。
- バックアップ ピアは、非静的L2TPv3セッションでのみ設定できます。バックアップ L2TPv3 セッションを、静的 L2TPv3 セッションにすることはできません。プライマリとバックアップ擬似回線のカプセル化タイプは同じである必要があります。
- L2VPN インターワーキングで L2VPN 擬似回線の冗長性を使用する場合、インターワーキング方法は、プライマリ擬似回線とバックアップ擬似回線で同じである必要があります。
- L2VPN擬似回線の冗長性は、マルチプロトコル ラベル スイッチング（MPLS）擬似回線における Experimental（EXP）ビットの設定をサポートしています。
- L2VPN擬似回線の冗長性は、MPLS擬似回線上の異なる擬似回線カプセル化タイプをサポートしません。

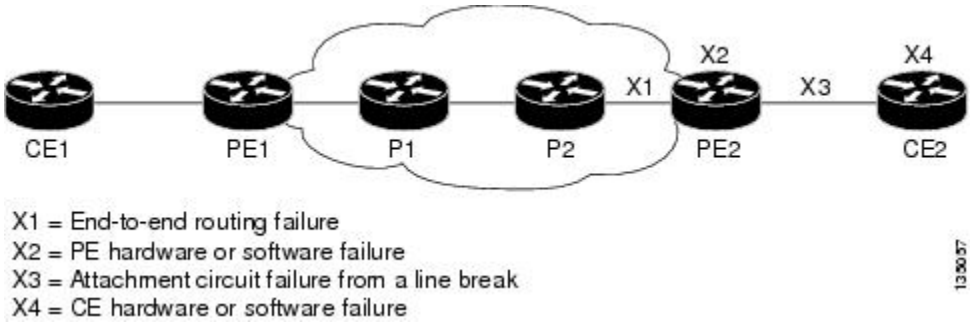
- **mpls l2transport route** コマンドはサポートされていません。代わりに **xconnect** コマンドを使用してください。
- プライマリ擬似回線が動作可能な場合、同時にバックアップ擬似回線を完全に動作可能にはできません。バックアップ擬似回線は、プライマリ擬似回線が障害になった後にだけアクティブにできます。
- AToM VCCV 機能は、アクティブな擬似回線でだけサポートされます。
- 複数のバックアップ擬似回線はサポートされていません。

L2VPN 擬似回線冗長性に関する情報

L2VPN 擬似回線冗長性の概要

L2VPN は、ルーティング プロトコルを通じて擬似回線冗長化機能を提供します。エンドツーエンド PE ルータ間の接続が障害になった場合、指示された LDP セッションとユーザ データの代替パスに引き継ぐことができます。ただし、ネットワークの一部は、この再ルーティング メカニズムでサービスの中断から保護されません。次の図は、サービスの中断に対して脆弱なネットワークの部分を示します。

図 *29* : *L2VPN* ネットワーク内の潜在的な障害ポイント

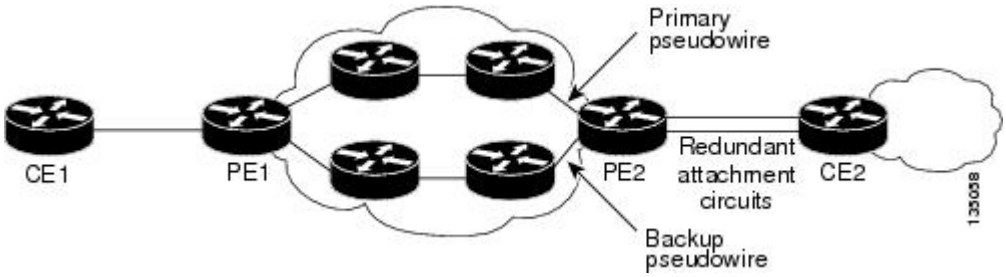


L2VPN 擬似回線の冗長性機能は、上図に示されるすべての障害が発生した場合でも、図中の CE2 ルータが常にネットワークの接続性を維持するための機能を提供します。

L2VPN 擬似回線の冗長性機能により、バックアップ擬似回線を設定できます。次の 3 つの図に示す、冗長な擬似回線と冗長なネットワーク要素を使用してネットワークを構成できます。

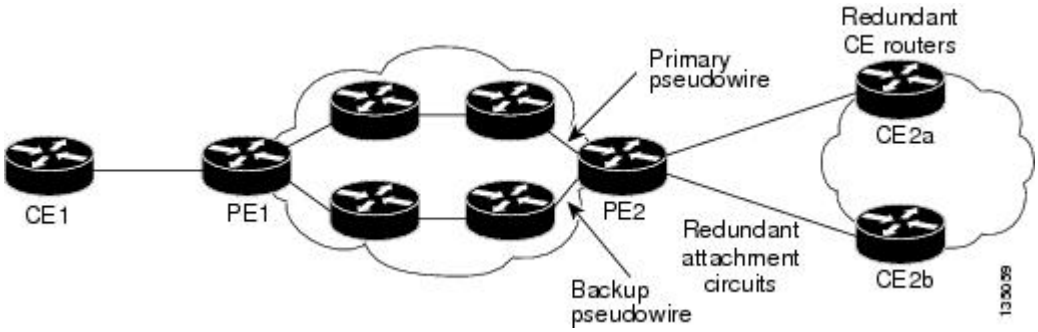
次の図は、冗長な擬似回線と冗長な接続回線を使用したネットワークを示します。

図 *30*：冗長な *PW* と冗長な接続回線を使用した *L2VPN* ネットワーク



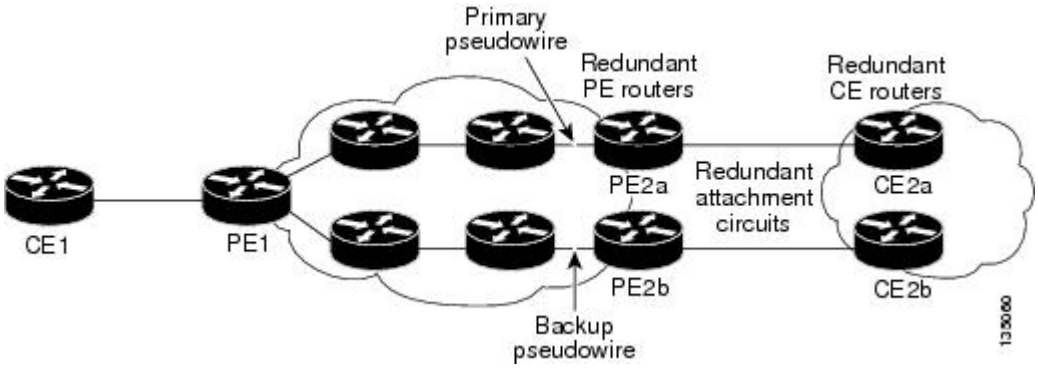
次の図は、冗長な擬似回線、接続回線、および CE ルータを使用したネットワークを示します。

図 *31*：冗長な *PW*、接続回線、および *CE* ルータを使用した *L2VPN* ネットワーク



次の図は、冗長な擬似回線、接続回線、CE ルータ、および PE ルータを使用したネットワークを示します。

図 *32*：冗長な *PW*、接続回線、*CE* ルータ、および *PE* ルータを使用した *L2VPN* ネットワーク



L2VPN 擬似回線冗長性の設定方法

L2VPN 擬似回線冗長性の機能を使用すると、プライマリ擬似回線が障害になった場合に備えてバックアップ擬似回線を設定できます。プライマリ擬似回線が障害になった場合、PE ルータをバックアップ擬似回線に切り替えることができます。プライマリ擬似回線が再度アップ状態になった後で、その使用を再開できます。

擬似回線の設定

PE ルータ間でレイヤ 2 フレームを正常に転送するには、PE ルータを設定する必要があります。ルータ間で、擬似回線と呼ぶ接続を設定します。

擬似回線クラス設定グループは、トンネリング メカニズムの次の特性を指定します。

- カプセル化のタイプ
- 制御プロトコル
- ペイロード固有のオプション

AToM VC が正常に動作するためには、擬似回線クラスの一部として **encapsulation mpls** コマンドを指定する必要があります。**xconnect** コマンドの中で **encapsulationmpls** コマンドを省略すると、次のエラーが表示されます。

```
% Incomplete command.
```

擬似回線クラスを設定するには、次の作業を実行します。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **pseudowire-class** name
4. **encapsulation mpls**
5. **interworking** {**ethernet** | **ip**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
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	**pseudowire-class** name 例： `Router(config)# pseudowire-class atom`	指定した名前の擬似回線クラスを確立します。擬似回線クラス 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	**encapsulation mpls** 例： `Router(config-pw-class)# encapsulation mpls`	トンネリング カプセル化を指定します。AToM の場合、カプセル化タイプは **mpls** です。
ステップ 5	**interworking** {**ethernet** | **ip**} 例： `Router(config-pw-class)# interworking ip`	（任意）異なるレイヤ2カプセル化の間の変換をイネーブルにします。

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した擬似回線の設定

PE ルータ間でレイヤ 2 フレームを正常に転送するには、PE ルータを設定する必要があります。ルータ間で、擬似回線と呼ぶ接続を設定します。

擬似回線クラス設定グループは、トンネリング メカニズムの次の特性を指定します。

- カプセル化のタイプ
- 制御プロトコル
- ペイロード固有のオプション

AToM VC が正常に動作するためには、擬似回線クラスの一部として **encapsulation mpls** コマンドを指定する必要があります。 **l2vpn xconnectcontext** コマンドの中で **encapsulationmpls** コマンドを省略すると、次のエラーが表示されます。

```
% Incomplete command.
```

擬似回線クラスを設定するには、次の作業を実行します。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface pseudowire** *number*
4. **encapsulation mpls**
5. **neighbor** *peer-address* *vcid-value*
6. **interworking** {**ethernet** | **ip**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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 pseudowire** *number* 例： `Router(config)# interface pseudowire 1`	指定された値でインターフェイス擬似回線を確立します。擬似回線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	**encapsulation mpls** 例： `Router(config-pw)# encapsulation mpls`	トンネリング カプセル化を指定します。AToM の場合、カプセル化タイプは **mpls** です。
ステップ 5	**neighbor** *peer-address* *vcid-value* 例： `Router(config-pw)# neighbor 10.0.0.1 123`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 6	**interworking** {**ethernet**	**ip**} 例： `Router(config-pw)# interworking ip`	（任意）異なるレイヤ 2 カプセル化の間の変換をイネーブルにします。

L2VPN 擬似回線冗長性の設定

L2VPN 擬似回線冗長性機能を設定するには、次のタスクを実行します。

はじめる前に

xconnect コマンドの設定方法は、転送タイプごとに若干異なります。次の設定手順では、サブインターフェイス コンフィギュレーション モードで設定する Ethernet VLAN over MPLS を使用しています。他の転送タイプに対して **xconnect** コマンドを設定する方法を決定するには、「*Any Transport over MPLS*」を参照してください。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacegigabitethernet***slot*/*subslot*/*interface*.*subinterface*
4. **encapsulationdot1q***vlan-id*
5. **xconnect***peer-router-idvcid* {**encapsulation mpls**| **pw-class** *pw-class-name}*
6. **backuppeer***peer-router-ip-addrvcid* [**pw-class** *pw-class-name*]
7. **backupdelay***enable-delay*{*disable-delay* | **never**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**interfacegigabitethernet***slot*/*subslot*/*interface*.*subinterface* 例： `Router(config)# interface gigabitethernet0/0/0.1`	ギガビット イーサネット サブインターフェイスを指定し、サブインターフェイス コンフィギュレーション モードを開始します。 （注） 隣接 CE ルータのサブインターフェイスがこの PE ルータと同じ VLAN 上にあることを確認します。

	コマンドまたはアクション	目的
ステップ 4	**encapsulationdot1q***vlan-id* 例： `Router(config-subif)# encapsulation dot1q 100`	サブインターフェイスでの 802.1Q VLAN パケットの受信をイネーブルにします。 （注） Ethernet over MPLS が稼働している CE ルータと PE ルータ間のサブインターフェイスは、同じサブネット内になければなりません。
ステップ 5	**xconnect***peer-router-idvcid* {**encapsulation mpls**| **pw-class** *pw-class-name}* 例： `Router(config-subif)# xconnect 10.0.0.1 123 pw-class atom`	接続回線を擬似回線 VC にバインドし、xconnect コンフィギュレーション モードを開始します。 • このコマンドの構文は、その他のレイヤ 2 トランスポートの場合と同じです。
ステップ 6	**backuppeer***peer-router-ip-addrvcid* [**pw-class** *pw-class-name*] 例： `Router(config-if-xconn)# backup peer 10.0.0.3 125 pw-class atom`	擬似回線 VC の冗長ピアを指定します。 擬似回線クラス名は、擬似回線クラスを作成したときに指定した名前と同じである必要がありますが、プライマリ **xconnect** コマンドで使用した名前とは異なる pw-class を **backup peer** コマンドで使用できます。
ステップ 7	**backupdelay***enable-delay*{*disable-delay* | **never**} 例： `Router(config-if-xconn)# backup delay 5 never`	プライマリ擬似回線の VC がダウンしてから、バックアップ擬似回線の VC に引き継ぐまでの待ち時間（秒単位）を指定します。範囲は 0 ～ 180 です。 プライマリ擬似回線がアクティブになってから、バックアップ擬似回線の VC を引き継ぐまでの待ち時間を指定します。指定できる範囲は 0 ～ 180 秒です。**never** キーワードを指定した場合は、プライマリ擬似回線 VC がバックアップを引き継ぎません。

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した L2VPN 擬似回線冗長性の設定

L2VPN 擬似回線冗長性機能を設定するには、次のタスクを実行します。

はじめる前に

l2vpn xconnect context コマンドの設定方法は、転送タイプごとに若干異なります。次の設定手順では、サブインターフェイス コンフィギュレーション モードで設定する Ethernet VLAN over MPLS

を使用しています。他の転送タイプに対して **l2vpn xconnect context** コマンドを設定する方法を決定するには、「*Any Transport over MPLS*」を参照してください。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacegigabitethernet***slot*/*subslot*/*interface*.*subinterface*
4. **encapsulationdot1q***vlan-id*
5. **end**
6. **interfacepseudowire***number*
7. **sourcetemplate type pseudowire***template-name*
8. **neighbor***peer-address vcid-value*
9. **exit**
10. **l2vpn xconnectcontext***context-name*
11. **member pseudowire***interface-number*
12. **member pseudowire***interface-number*
13. **member gigabitethernet***interface-number*
14. **redundancydelay***enable-delay*{*disable-delay* | **never**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**interfacegigabitethernet***slot*/*subslot*/*interface*.*subinterface* 例： `Device(config)# interface gigabitethernet0/0/0.1`	ギガビット イーサネット サブインターフェイスを指定し、サブインターフェイス コンフィギュレーション モードを開始します。 隣接 CE ルータのサブインターフェイスがこの PE ルータと同じ VLAN 上にあることを確認します。

	コマンドまたはアクション	目的
ステップ 4	**encapsulationdot1q***vlan-id* 例： `Device(config-subif)# encapsulation dot1q 100`	サブインターフェイスでの 802.1Q VLAN パケットの受信をイネーブルにします。 Ethernet over MPLS が稼働している CE ルータと PE ルータ間のサブインターフェイスは、同じサブネット内になければなりません。その他すべてのサブインターフェイスとバックボーン ルータは、同じサブネット上にある必要はありません。
ステップ 5	**end** 例： `Router(config-subif)# end`	特権 EXEC モードに戻ります。
ステップ 6	**interfacepseudowire***number* 例： `Router(config)# interface pseudowire 100`	擬似回線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 7	**sourcetemplate type pseudowire***template-name* 例： `Router(config-if)# source template type pseudowire atom`	atom という名前のタイプ擬似回線のソース テンプレートを設定します。
ステップ 8	**neighbor***peer-address vcid-value* 例： `Router(config-if)#  neighbor 10.0.0.1 123`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 9	**exit** 例： `Router(config-if)# exit`	特権 EXEC モードに戻ります。
ステップ 10	**l2vpn xconnectcontext***context-name* 例： `Router(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect 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 11	**member pseudowire***interface-number* 例： `Device(config-xconnect)# member pseudowire 100 group GR_1 priority 2`	Layer 2 VPN（L2VPN）クロス コネクトを形成するようにメンバー擬似回線を指定します。
ステップ 12	**member pseudowire***interface-number* 例： `Device(config-xconnect)# member pseudowire 1001 group GR_1 priority 2`	冗長性のために 2 つ目のメンバー擬似回線を指定します。
ステップ 13	**member gigabitethernet***interface-number* 例： `Device(config-xconnect)# member GigabitEthernet0/0/0.1 service instance 1`	ギガビットイーサネット メンバー インターフェイスのロケーションを指定します。
ステップ 14	**redundancydelay***enable-delay*{*disable-delay* | **never**} 例： `Device(config-xconnect)# redundancy delay 0 0 group GR_1`	プライマリ擬似回線の VC がダウンしてから、バックアップ擬似回線の VC に引き継ぐまでの待ち時間（秒単位）を指定します。値の範囲は 0 ～ 180 です。 プライマリ擬似回線がアクティブになってから、バックアップ擬似回線の VC を引き継ぐまでの待ち時間を指定します。値の範囲は 0 ～ 180 秒です。**never キーワード**を指定した場合は、プライマリ擬似回線 VC がバックアップを引き継ぎません。

バックアップ擬似回線 VC への手動スイッチオーバーの強制

バックアップまたはプライマリ擬似回線へのルータ スイッチオーバーを強制するには、特権 EXEC モードで **xconnect backup force switchover** コマンドを入力します。切り替え先のプライマリ接続回線（AC）のインターフェイスまたはピア ルータの IP アドレスと VC ID を指定できます。

手動スイッチオーバーが実行できるのは、コマンドで指定されたインターフェイスまたはピアが実際に使用可能な場合だけであり、コマンドを実行すると、xconnect が完全にアクティブな状態に移行します。

手順の概要

1. イネーブル化
2. **xconnectbackupforce-switchover{interface***interface-info***|** **peer** *ip-address vcid}*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**xconnectbackupforce-switchover{interface***interface-info***|** **peer** *ip-address vcid}* 例： `Router# xconnect backup force-switchover peer 10.10.10.1 123`	ルータをバックアップ擬似回線またはプライマリ擬似回線に切り替えることを指定します。

L2VPN 擬似回線冗長性設定の確認

L2VPN 擬似回線冗長性機能が正しく設定されていることを確認するには、次のタスクを実行します。

手順の概要

1. **showmplsl2transportvc**
2. **showxconnectall**
3. **xconnectloggingredundancy**

手順の詳細

ステップ 1 **showmplsl2transportvc**

次に、**show mpls l2transport vc** コマンドの出力例を示します。この例で、プライマリ接続回線はアップです。バックアップ接続回線は使用可能ですが、現在選択されていません。

例：

```
Router# show mpls l2transport vc
Local intf     Local circuit           Dest address    VC ID      Status
```

```
-------------  ----------------------- --------------- ---------- ----------
Et0/0.1        Eth VLAN 101            10.0.0.2        101        UP
Et0/0.1        Eth VLAN 101            10.0.0.3        201        DOWN
Router# show mpls l2transport vc detail
Local interface: Et0/0.1 up, line protocol up, Eth VLAN 101 up
   Destination address 10.0.0.2 VC ID: 101, VC status UP
   .
   .
   .
Local interface: Et0/0.1 down, line protocol down, Eth VLAN 101 down
   Destination address 10.0.0.3 VC ID: 201, VC status down
   .
   .
   .
```

ステップ 2 **showxconnectall**

この例で、トポロジは接続回線 1 から擬似回線 1 であり、擬似回線 2 がバックアップとして使用されています。

例：

```
Router# show xconnect all
Legend: XC ST=Xconnect State, S1=Segment1 State, S2=Segment2 State
UP=Up, DN=Down, AD=Admin Down, IA=Inactive, NH=No Hardware
XC ST  Segment 1                         S1 Segment 2                          S2
------+-------------------------------+--+-------------------------------+--
UP pri ac   Et0/0(Ethernet)              UP mpls 10.55.55.2:1000              UP
IA sec ac   Et0/0(Ethernet)              UP mpls 10.55.55.3:1001              DN
```

この例で、トポロジは接続回線 1 から接続回線 2 であり、擬似回線が接続回線 2 のバックアップとして使用されています。

例：

```
Router# show xconnect all
Legend: XC ST=Xconnect State, S1=Segment1 State, S2=Segment2 State
UP=Up, DN=Down, AD=Admin Down, IA=Inactive, NH=No Hardware
XC ST  Segment 1                         S1 Segment 2                          S2
------+---------------------------------+--+---------------------------------+--
UP pri ac   Se6/0:150(FR DLCI)           UP ac   Se8/0:150(FR DLCI)           UP
IA sec ac   Se6/0:150(FR DLCI)           UP mpls 10.55.55.3:7151              DN
```

ステップ 3 **xconnectloggingredundancy**

show mpls l2transport vc コマンドと **show xconnect** コマンドの他に、**xconnect logging redundancy** コマンドを使用して、xconnect 冗長性グループのステータスを追跡できます。

例：

```
Router(config)# xconnect logging redundancy
```

このコマンドが設定されている場合は、スイッチオーバーイベント中に次のメッセージが表示されます。

プライマリ メンバーをアクティブ化する場合

例：

```
00:01:07: %XCONNECT-5-REDUNDANCY: Activating primary member 10.55.55.2:1000
```

バックアップ メンバーをアクティブ化する場合

例：

```
00:01:05: %XCONNECT-5-REDUNDANCY: Activating secondary member 10.55.55.3:1001
```

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した L2VPN 擬似回線冗長性設定の確認

L2VPN 擬似回線冗長性機能が正しく設定されていることを確認するには、次のコマンドを使用します。

手順の概要

1. **showl2vpnatomvc**
2. **showl2vpnservice all**
3. **loggingredundancy**
4. **loggingpseudowire status**

手順の詳細

ステップ 1 **showl2vpnatomvc**

この例で、プライマリ接続回線はアップです。バックアップ接続回線は使用可能ですが、現在選択されていません。**show** の出力は次のように表示されます。

例：

```
Device# show l2vpn atom vc
Local intf     Local circuit           Dest address    VC ID      Status
-------------  ----------------------- --------------- ---------- ----------
Et0/0.1        Eth VLAN 101            10.0.0.2        101        UP
Et0/0.1        Eth VLAN 101            10.0.0.3        201        DOWN
Router# show l2vpn atom vc detail
Local interface: Et0/0.1 up, line protocol up, Eth VLAN 101 up
   Destination address 10.0.0.2 VC ID: 101, VC status UP
   .
   .
   .
Local interface: Et0/0.1 down, line protocol down, Eth VLAN 101 down
   Destination address 10.0.0.3 VC ID: 201, VC status down
   .
   .
   .
```

ステップ 2 **showl2vpnservice all**

この例で、トポロジは接続回線 1 から擬似回線 1 であり、擬似回線 2 がバックアップとして使用されています。

例：

```
Device# show l2vpn service all
Legend: St=State    XC St=State in the L2VPN Service      Prio=Priority
        UP=Up       DN=Down            AD=Admin Down      IA=Inactive
        SB=Standby  HS=Hot Standby     RV=Recovering      NH=No Hardware
        m=manually selected

  Interface          Group       Encapsulation                   Prio  St  XC St
  ---------          -----       -------------                   ----  --  -----
VPWS name: foo, State: UP
  Eth1/1.1                       Eth1/1.1:100(Eth VLAN)          0     UP  UP
  pw101              blue        102.1.1.1:100(MPLS)             2     UP  UP
  pw102              blue        103.1.1.1:100(MPLS)             5     SB  IA
  pw103              blue        104.1.1.1:100(MPLS)             8     SB  IA
  pw104              blue        105.1.1.1:100(MPLS)             11    SB  IA
```

この例で、トポロジは接続回線 1 から接続回線 2 であり、擬似回線が接続回線 2 のバックアップとして使用されています。

例：

```
Device# show l2vpn service all
Legend: XC ST=Xconnect State, S1=Segment1 State, S2=Segment2 State
UP=Up, DN=Down, AD=Admin Down, IA=Inactive, NH=No Hardware
XC ST  Segment 1                          S1 Segment 2                          S2
------+-----------------------------+--+-----------------------------------+--
UP pri ac   Se6/0:150(FR DLCI)           UP ac   Se8/0:150(FR DLCI)           UP
IA sec ac   Se6/0:150(FR DLCI)           UP mpls 10.55.55.3:7151              DN
```

ステップ 3 **loggingredundancy**

show l2vpn atom vc コマンドと **show l2vpn service** コマンドの他にも、**logging redundancy** コマンドを使用して、xconnect 冗長性ステータス イベントのシステム メッセージ ログ（syslog）レポートを有効にできます。

例：

```
Device(config)# l2vpn
Device(config-l2vpn)# logging redundancy
```

このコマンドが設定されている場合は、スイッチオーバーイベント中に次のメッセージが生成されます。

プライマリ メンバーをアクティブ化する場合

例：

```
Device(config)# l2vpn
Device(config-l2vpn)# logging pseudowire status
```

このコマンドが設定されている場合は、擬似回線のステータスがモニタできるように設定されます。

プライマリ メンバーをアクティブ化する場合

例：

```
00:01:07: %XCONNECT-5-REDUNDANCY: Activating primary member 10.55.55.2:1000
```

バックアップ メンバーをアクティブ化する場合

例：

```
00:01:05: %XCONNECT-5-REDUNDANCY: Activating secondary member 10.55.55.3:1001
```

ステップ 4 **loggingpseudowire status**

logging pseudowire status コマンドを使用して、擬似回線のステータスをモニタできます。

例：

```
Device(config)# l2vpn
Device(config-l2vpn)# logging pseudowire status
```

L2VPN 擬似回線冗長性の設定例

各設定例は、次の擬似回線クラスのいずれかを参照しています。

- AToM（like-to-like）擬似回線クラス

```
pseudowire-class mpls
 encapsulation mpls
```

- L2VPN IP インターワーキング

```
pseudowire-class mpls-ip
 encapsulation mpls
 interworking ip
```

例：L2VPN 擬似回線冗長性と AToM（like-to-like）

次の例は、バックアップ擬似回線を使用したハイレベル データリンク コントロール（HDLC）接続回線 xconnect を示します。

```
interface Serial4/0
 xconnect 10.55.55.2 4000 pw-class mpls
 backup peer 10.55.55.3 4001 pw-class mpls
```

次の例は、バックアップ擬似回線を使用したフレームリレー接続回線 xconnect を示します。

```
connect fr-fr-pw Serial6/0 225 l2transport
 xconnect 10.55.55.2 5225 pw-class mpls
 backup peer 10.55.55.3 5226 pw-class mpls
```

例：L2VPN 擬似回線冗長性と L2VPN インターワーキング

次の例は、L2VPN IP インターワーキングとバックアップ擬似回線を使用したイーサネット接続回線 xconnect を示します。

```
interface Ethernet0/0
 xconnect 10.55.55.2 1000 pw-class mpls-ip
 backup peer 10.55.55.3 1001 pw-class mpls-ip
```

次の例は、L2VPN IP インターワーキングとバックアップ擬似回線を使用したイーサネット Virtual LAN（VLAN）接続回線 xconnect を示します。

```
interface Ethernet1/0.1
 encapsulation dot1Q 200
 no ip directed-broadcast
 xconnect 10.55.55.2 5200 pw-class mpls-ip
 backup peer 10.55.55.3 5201 pw-class mpls-ip
```

次の例は、L2VPN IP インターワーキングとバックアップ擬似回線を使用したフレームリレー接続回線 xconnect を示します。

```
connect fr-ppp-pw Serial6/0 250 l2transport
 xconnect 10.55.55.2 8250 pw-class mpls-ip
 backup peer 10.55.55.3 8251 pw-class mpls-ip
```

次の例は、L2VPN IP インターワーキングとバックアップ擬似回線を使用した PPP 接続回線 xconnect を示します。

```
interface Serial7/0
 encapsulation ppp
 xconnect 10.55.55.2 2175 pw-class mpls-ip
 backup peer 10.55.55.3 2176 pw-class mpls-ip
```

例：レイヤ 2 ローカル スイッチングを使用した L2VPN 擬似回線冗長性

次の例は、イーサネット セグメント E2/0.2 に対する擬似回線バックアップを使用したイーサネット VLAN-VLAN ローカル スイッチング xconnect を示します。E2/0.2 に関連付けられているサブインターフェイスがダウンすると、バックアップ擬似回線がアクティブ化されます。

```
connect vlan-vlan Ethernet1/0.2 Ethernet2/0.2
 backup peer 10.55.55.3 1101 pw-class mpls
```

次の例は、フレームリレー セグメント S8/0 150 に対する擬似回線バックアップを使用した、フレームリレー相互間ローカル スイッチング接続を示します。S8/0 上のデータリンク接続識別子（DLCI）150 がダウンした場合、バックアップ擬似回線がアクティブ化されます。

```
connect fr-fr-ls Serial6/0 150 Serial8/0 150
 backup peer 10.55.55.3 7151 pw-class mpls
```

例：L2VPN 擬似回線冗長性と Layer 2 Tunneling Protocol バージョン 3

次に、xconnect セッションのバックアップ ピアを設定する例を示します。

```
pseudowire-class 773
```

```
 encapsulation l2tpv3
 ip local interface GigabitEthernet0/0/0.773
!
pseudowire-class 774
 encapsulation l2tpv3
 ip local interface GigabitEthernet0/0/1.774
!
interface GigabitEthernet0/0/0.780
 encapsulation dot1Q 780
 xconnect 10.22.73.14 100 pw-class 773
  backup peer 10.22.74.14 101 pw-class 774
  backup delay 0 0
```

次に、L2VPN 擬似回線冗長性と L2TPv3 を使用してギガビットイーサネットポートを設定する例を示します。

```
interface GigabitEthernet0/0/2
 xconnect 10.22.70.83 50 pw-class pe1-pw-primary
 backup peer 20.22.70.85 51 pw-class pe1-pw-secondary
```

次に、L2VPN 擬似回線冗長性と L2TPv3 を使用してギガビットイーサネット VLAN を設定する例を示します。

```
interface GigabitEthernet0/0/0.100
 encapsulation dot1q 100
 xconnect 10.22.70.83 60 pw-class pe1-pw-primary
 backup peer 10.22.70.85 61 pw-class pe1-pw-secondary
```

次に、L2VPN 擬似回線冗長性と L2TPv3 を使用してギガビットイーサネット Q-in-Q を設定する例を示します。

```
interface GigabitEthernet0/0/0.200
 encapsulation dot1q 200 second-dot1q 400
 xconnect 10.22.70.83 70 pw-class pe1-pw-primary
 backup peer 10.22.70.85 71 pw-class pe1-pw-secondary
```

次に、L2VPN 擬似回線冗長性と L2TPv3 を使用してギガビットイーサネット Q-in-any を設定する例を示します。

```
interface GigabitEthernet0/0/0.300
 encapsulation dot1q 300 second-dot1q any
 xconnect 10.22.70.83 80 pw-class pe1-pw-primary
 backup peer 10.22.70.85 81 pw-class pe1-pw-secondary
```

次に、L2VPN 擬似回線冗長性と L2TPv3 を使用して HDLC を設定する例を示します。

```
interface Serial0/2/0:0
 no ip address
 xconnect 10.22.71.83 40 pw-class pe1-pw-hdlc
 backup peer 10.22.70.85 41 pw-class pe1-pw-hdlc-2
```

L2VPN 擬似回線冗長性の設定例（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

各設定例は、次のインターフェイス擬似回線のいずれかを参照しています。

- AToM（like-to-like）インターフェイス擬似回線：

```
interface pseudowire 1
 encapsulation mpls
 neighbor 33.33.33.33 1
```

- L2VPN IP インターワーキング

```
interface pseudowire 1
 encapsulation mpls
 neighbor 33.33.33.33 1
 interworking ip
```

例：L2VPN 擬似回線冗長性および AToM（like-to-like）（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

次の例は、バックアップ擬似回線を使用したハイレベル データリンク コントロール（HDLC）接続回線 xconnect を示します。

```
interface Serial4/0
 interface pseudowire 100
 source template type pseudowire ether-pw
 neighbor 10.55.55.3 4001
!
l2vpn xconnect context con1
 member pseudowire 100 group GR_1 priority 1
 member pseudowire 1001 group GR_1 priority 2
 member GigabitEthernet0/0/2 service-instance 1
 redundancy delay 0 0 group GR_1
```

次の例は、バックアップ擬似回線を使用したフレームリレー接続回線 xconnect を示します。

```
connect fr-fr-pw Serial6/0 225 l2transport
interface pseudowire 100
 source template type pseudowire ether-pw
 neighbor 10.55.55.3 5226
!
l2vpn xconnect context con1
 member pseudowire 100 group GR_1 priority 1
 member pseudowire 1001 group GR_1 priority 2
 member GigabitEthernet0/0/2 service-instance 1
 redundancy delay 0 0 group GR_1
```

例：L2VPN 擬似回線冗長性および L2VPN インターワーキング（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

次の例は、L2VPN IP インターワーキングとバックアップ擬似回線を使用したイーサネット接続回線 xconnect を示します。

```
interface Ethernet0/0
interface pseudowire 100
 source template type pseudowire ether-pw
!
l2vpn xconnect context con1
 member pseudowrire 100 group GR_1 priority 1
 member pseudowire 1001 group GR_1 priority 2
 member GigabitEthernet0/0/2 service-instance 1
 redundancy delay 0 0 group GR_1
 interworking ip
```

次の例は、L2VPN IP インターワーキングとバックアップ擬似回線を使用したイーサネット Virtual LAN（VLAN）接続回線 xconnect を示します。

```
interface Ethernet1/0.1
 encapsulation dot1Q 200
 no ip directed-broadcast
 interface pseudowire 100
 source template type pseudowire ether-pw
!
l2vpn xconnect context con1
 member pseudowrire 100 group GR_1 priority 1
 member pseudowire 1001 group GR_1 priority 2
 member GigabitEthernet0/0/2 service-instance 1
 redundancy delay 0 0 group GR_1
 interworking ip
```

次の例は、L2VPN IP インターワーキングとバックアップ擬似回線を使用したフレームリレー接続回線 xconnect を示します。

```
connect fr-ppp-pw Serial6/0 250 l2transport
 interface pseudowire 100
 source template type pseudowire ether-pw
!
l2vpn xconnect context con1
 member pseudowrire 100 group GR_1 priority 1
 member pseudowire 1001 group GR_1 priority 2
 member GigabitEthernet0/0/2 service-instance 1
 redundancy delay 0 0 group GR_1
 interworking ip
```

次の例は、L2VPN IP インターワーキングとバックアップ擬似回線を使用した PPP 接続回線 xconnect を示します。

```
interface Serial7/0
 encapsulation ppp
 interface pseudowire 100
 source template type pseudowire ether-pw
!
l2vpn xconnect context con1
 member pseudowire 100 group GR_1 priority 1
 member pseudowire 1001 group GR_1 priority 2
 member GigabitEthernet0/0/2 service-instance 1
 redundancy delay 0 0 group GR_1
 interworking ip
```

例：L2VPN プロトコルベース CLI 機能に関連するコマンドを使用した L2VPN 擬似回線冗長性と Layer 2 Tunneling Protocol バージョン 3

次に、xconnect セッションのバックアップ ピアを設定する例を示します。

```
interface pseudowire 773
 encapsulation l2tpv3
 ip local interface GigabitEthernet0/0/0.773
!
interface pseudowire 774
 encapsulation l2tpv3
 ip local interface GigabitEthernet0/0/1.774
!
interface GigabitEthernet0/0/0.780
 encapsulation dot1Q 780
 interface pseudowire 100
 source template type pseudowire ether-pw
 neighbor 10.22.73.14 100
```

```
!
l2vpn xconnect context con1
 member pseudowire 100 group GR_1 priority 1
 member pseudowire 1001 group GR_1 priority 2
 member GigabitEthernet0/0/2 service-instance 1
 redundancy delay 0 0 group GR_1
 interworking ip
```

次に、L2VPN 擬似回線冗長性と L2TPv3 を使用してギガビットイーサネットポートを設定する例を示します。

```
interface GigabitEthernet0/0/2
 interface pseudowire 100
 source template type pseudowire ether-pw
 neighbor 10.22.70.83 50
!
l2vpn xconnect context con1
 member pseudowire 100 group GR_1 priority 1
 member pseudowire 1001 group GR_1 priority 2
 member GigabitEthernet0/0/2 service-instance 1
 redundancy delay 0 0 group GR_1
 interworking ip
```

次に、L2VPN 擬似回線冗長性と L2TPv3 を使用してギガビットイーサネット VLAN を設定する例を示します。

```
interface GigabitEthernet0/0/0.100
 encapsulation dot1q 100
 interface pseudowire 100
 source template type pseudowire ether-pw
 neighbor 10.22.70.83 60
!
l2vpn xconnect context con1
 member pseudowire 100 group GR_1 priority 1
 member pseudowire 1001 group GR_1 priority 2
 member GigabitEthernet0/0/2 service-instance 1
 redundancy delay 0 0 group GR_1
 interworking ip
```

次に、L2VPN 擬似回線冗長性と L2TPv3 を使用してギガビットイーサネット Q-in-Q を設定する例を示します。

```
interface GigabitEthernet0/0/0.200
 encapsulation dot1q 200 second-dot1q 400
 interface pseudowire 100
 source template type pseudowire ether-pw
 neighbor 10.22.70.83 70
!
l2vpn xconnect context con1
 member pseudowire 100 group GR_1 priority 1
 member pseudowire 1001 group GR_1 priority 2
 member GigabitEthernet0/0/2 service-instance 1
 redundancy delay 0 0 group GR_1
 interworking ip
```

次に、L2VPN 擬似回線冗長性と L2TPv3 を使用してギガビットイーサネット Q-in-any を設定する例を示します。

```
interface GigabitEthernet0/0/0.300
 encapsulation dot1q 300 second-dot1q any
 interface pseudowire 100
 source template type pseudowire ether-pw
 neighbor 10.22.70.83 80
!
l2vpn xconnect context con1
 member pseudowire 100 group GR_1 priority 1
 member pseudowire 1001 group GR_1 priority 2
 member GigabitEthernet0/0/2 service-instance 1
 redundancy delay 0 0 group GR_1
```

```
 interworking ip
```

次に、L2VPN 擬似回線冗長性と L2TPv3 を使用して HDLC を設定する例を示します。

```
interface Serial0/2/0:0
 no ip address
 interface pseudowire 100
 source template type pseudowire ether-pw
 neighbor 10.22.71.83 40
!
l2vpn xconnect context con1
 l2vpn xconnect context con1
 member pseudowire 100 group GR_1 priority 1
 member pseudowire 1001 group GR_1 priority 2
 member GigabitEthernet0/0/2 service-instance 1
 redundancy delay 0 0 group GR_1
 interworking ip
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
ワイドエリア ネットワーキング コマンド	『*Cisco IOS Wide-Area Networking Command Reference*』
Cisco IOS XE マルチプロトコル ラベル スイッチングの設定作業	『*Cisco IOS XE Multiprotocol Label Switching Configuration Guide*』
Cisco IOS XE 広域ネットワーキングの設定作業	『*Cisco IOS XE Wide-Area Networking Configuration Guide*』

標準

標準	Title
なし	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB の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 ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
なし	--

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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。	http://www.cisco.com/cisco/web/support/index.html

L2VPN 擬似回線冗長性の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、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。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *25*：*L2VPN* 擬似回線冗長性の機能情報

機能名	リリース	機能情報
L2VPN 擬似回線冗長性	XE 2.3 XE 3.3S	この機能を使用すると、ネットワーク内の障害を検出して、サービスの提供を続行可能な別のエンドポイントにレイヤ 2 サービスを再ルーティングするようにネットワークを設定できます。 この機能は、Cisco IOS XE Release 2.3 で Cisco ASR 1000 シリーズ アグリゲーション サービスルータに統合されました。 この機能は、Cisco IOS XE Release 3.3S で、Layer 2 Tunneling Protocol バージョン 3（L2TPv3）をサポートしています。 次のコマンドが導入または変更されました：**backupdelay**（**L2VPN ローカルスイッチング**）、**backuppeer**、**showxconnect**、**xconnectbackupforce-switchover**、**xconnectloggingredundancy**。

第 14 章

擬似回線グループ スイッチオーバー

擬似回線グループ スイッチオーバー機能により、グループ内のすべての擬似回線をすばやくバックアップ擬似回線に切り替えることができます。このグループ スイッチオーバーは、リモートピアから 1 つの「グループ ダウン」ステータス メッセージを受信するとトリガーされます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース 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、機能情報の表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シスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

擬似回線グループ スイッチオーバーの前提条件

- リモート プロバイダー エッジ（PE）ルータは、グループ ステータス メッセージを送信できる必要があります。
- ラベル配布プロトコル（LDP）は、ネットワークで実装する必要があります。
- 各 xconnect には、バックアップ擬似回線が設定されている必要があります。

擬似回線グループ スイッチオーバーの制約事項

擬似回線グループ スイッチオーバー機能は、Cisco IOS XE Release 3.10S 以降のリリースでサポートされます。この機能は、以下の接続回線での Cisco ASR 903 シリーズ ルータでサポートされます。

- イーサネット VLAN
- 非同期転送モード（ATM）
- Circuit Emulation over MPLS（CEM）

擬似回線グループ スイッチオーバーに関する情報

擬似回線グループ スイッチオーバーの概要

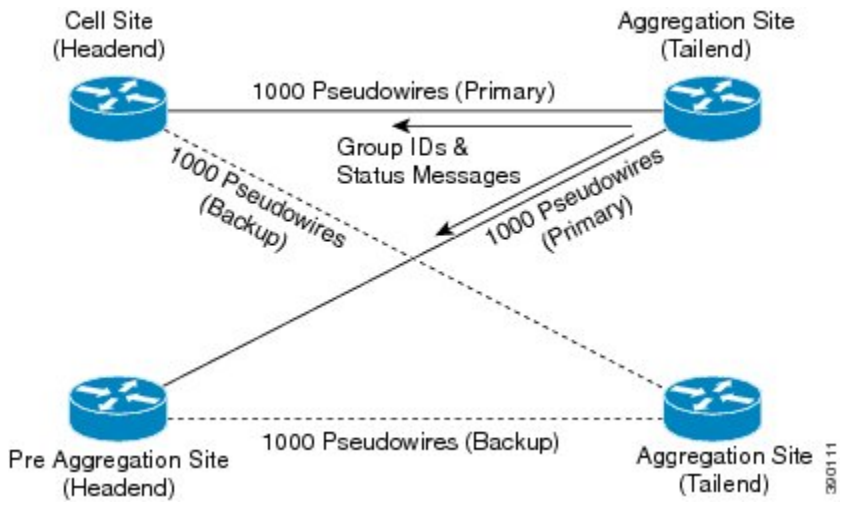
擬似回線グループ スイッチオーバー機能により、障害の発生時に主要な擬似回線からバックアップの擬似回線へのスイッチオーバー時間を短縮できます。スイッチオーバー時間の短縮は、Label Distribution Protocol（LDP）ステータス メッセージと内部プロセス間通信（IPC）メッセージをグループ化することによって実現されます。

リモート ピアが接続回線の障害を検出すると、LDP ステータスメッセージを送信します。このステータス メッセージを受け取ると、指定されたバックアップ擬似回線に切り替わります。次に、パケットはバックアップ擬似回線を介して、ルーティングされます。

擬似回線は、グループ ID の割り当てにより、グループ別に分類できます。擬似回線グループにより LDP ステータス メッセージが受信されると、グループ全体がスイッチオーバーし、スイッチオーバー時間が短縮されます。

（注） この擬似回線グループ スイッチオーバー機能はデフォルトで有効であり、無効にすることはできません。

図 *33*：プライマリおよびバックアップ擬似回線グループ



予測型スイッチオーバーの設定方法

予測型スイッチオーバーでは、リモート ピアからの「アップ」ステータスを待つことなく、リモート「スタンバイ」ステータスのバックアップ擬似回線へのメイン擬似回線からのスイッチオーバーが可能になります。

予測型スイッチオーバーは、グローバル コンフィギュレーション モードまたはxconnect コンフィギュレーション モードで冗長性予測モードを有効にすることにより設定します。

予測型スイッチオーバーの設定（グローバルコンフィギュレーション モード）

手順の概要

1. イネーブル化
2. **configure terminal**
3. **l2vpn**
4. **redundancy predictive enabled**
5. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**l2vpn** 例： `Device(config)# l2vpn`	l2vpn 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	**redundancy predictive enabled** 例： `Device(config-l2vpn)# redundancy predictive enabled`	冗長性予測モードを有効にします。 • デフォルトで、冗長性予測モードは無効になります。
ステップ 5	**end** 例： `Device(config-l2vpn)# end`	l2vpn コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

予測型スイッチオーバーの設定（Xconnect コンフィギュレーション モード）

手順の概要

1. イネーブル化
2. **configure terminal**
3. **l2vpn xconnect context** *context-name*
4. **redundancy predictive enabled**
5. **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	**イネーブル化** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**l2vpn xconnect context** *context-name* 例： `Device(config)# l2vpn xconnect context con1`	L2VPN クロス コネクト コンテキストを作成して、xconnect 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	**redundancy predictive enabled** 例： `Device(config-xconnect)# redundancy predictive enabled`	冗長性予測モードを有効にします。
ステップ 5	**end** 例： `Device(config-xconnect)# end`	xconnect コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

擬似回線グループ スイッチオーバー設定の確認

show コマンドを使用して、擬似回線グループ スイッチオーバー設定に関する情報を表示できます。

次に、Any Transport over MPLS（AToM）仮想回線（VC）に関する情報を表示する例を示します。

```
Device# show l2vpn atom vc destination 2.1.1.2 group remote 6

                                        Service
Interface  Dest Address     VC ID     Type     Name                    Status
--------- --------------- ---------- ------ ------------------------ ----------
pw100001   2.1.1.2         1234000    p2p      Et1/0.1-1001            UP
```

次に、擬似回線スイッチング ポイントのステータスを表示する例を示します。

```
Device# show l2vpn atom vc destination 2.1.1.2 group remote 6 detail

pseudowire100001 is up, VC status is up PW type: Ethernet
  Create time: 5d20h, last status change time: 5d20h
    Last label FSM state change time: 5d20h
  Destination address: 2.1.1.2 VC ID: 1234000
    Output interface: Et0/0, imposed label stack {2001}
  Preferred path: not configured
```

```
  Default path: active
  Next hop: 20.0.0.2
Member of xconnect service Et1/0.1-1001, group right
  Associated member Et1/0.1 is up, status is up
  Interworking type is Ethernet
  Service id: 0x6d000002
Signaling protocol: LDP, peer 2.1.1.2:0 up
  Targeted Hello: 1.1.1.1(LDP Id) -> 2.1.1.2, LDP is UP
  Graceful restart: not configured and not enabled
  Non stop routing: not configured and not enabled
  PWid FEC (128), VC ID: 1234000
  Status TLV support (local/remote) : enabled/supported
    LDP route watch : enabled
    Label/status state machine : established, LruRru
    Local dataplane status received : No fault
    BFD dataplane status received : Not sent
    BFD peer monitor status received : No fault
    Status received from access circuit : No fault
    Status sent to access circuit : No fault
    Status received from pseudowire i/f : No fault
    Status sent to network peer : No fault
    Status received from network peer : No fault
    Adjacency status of remote peer : No fault
Sequencing: receive disabled, send disabled
Bindings
Parameter    Local                          Remote
------------ ------------------------------ ------------------------------
Label        2007                           2001
Group ID     0                              6
Interface
MTU          1500                           1500
Control word on (configured: autosense)     on
PW type      Ethernet                       Ethernet
VCCV CV type 0x12                           0x12
               LSPV [2], BFD/Raw [5]          LSPV [2], BFD/Raw [5]
VCCV CC type 0x07                           0x07
             CW [1], RA [2], TTL [3]        CW [1], RA [2], TTL [3]
Status TLV   enabled                        supported
Dataplane:
  SSM segment/switch IDs: 12309/4115 (used), PWID: 1
Rx Counters
  106563 input transit packets, 9803650 bytes
  0 drops, 0 seq err
Tx Counters
  0 output transit packets, 0 bytes
  0 drops
```

次に、各ピアのIPアドレスとグループ識別子に関連付けられたアクティブセグメントとスタンバイ セグメントのペアを列挙する例を示します。

```
Device# show ssm group

Active              Standby
IP Address       Group ID       Segment/Switch      Segment/Switch
=========================================================================
2.1.1.2               6            8215/4115           4116/8210
```

次に、各ピアのIPアドレスとグループ識別子に関連付けられたアクティブセグメントとスタンバイ セグメントのペアの数を表示する例を示します。

```
Device# show ssm group 2.1.1.2 6 summary

IP Address        Group ID      Group Members
=============================================
2.1.1.2                6               1
```

次に、グループ化情報とともに、ハードウェアでプログラムされた擬似回線の数を表示する例を示します。

```
Device# show platform hardware pp active pw eompls group brief

Brief L2VPN EoMPLS Pseudo Wire Group Info
```

```
IP address           Group ID            Count
-------------------------------------------------------
0x47474747           100695488            90
```

擬似回線グループスイッチオーバー設定のトラブルシューティング

debug platform software atom brief コマンドを使用して、次の設定に関する情報を表示します。

- グループの追加
- グループからの削除
- グループ スイッチオーバー

（注） **debug platform software atom brief** コマンドは、Cisco Technical Assistance Center（TAC）の指示がある場合にのみ使用することをお勧めします。

予測型スイッチオーバーの設定例

例：予測型スイッチオーバーの設定（グローバル コンフィギュレーション モード）

```
Device> enable
Device# configure terminal
Device(config)# l2vpn
Device(config-l2vpn)# redundancy predictive enabled
Device(config-l2vpn)# end
```

例：予測型スイッチオーバーの設定（xconnectコンフィギュレーション モード）

```
Device> enable
Device# configure terminal
Device(config)# l2vpn xconnect context con1
Device(config-xconnect)# redundancy predictive enabled
Device(config-xconnect)# end
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
MPLS コマンド	『Cisco IOS Multiprotocol Label Switching Command Reference』

標準および RFC

標準/RFC	Title
RFC 4447	『*Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)*』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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。	http://www.cisco.com/cisco/web/support/index.html

擬似回線グループ スイッチオーバーの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、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。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *26*：擬似回線グループ スイッチオーバーの機能情報

機能名	リリース	機能情報
擬似回線グループ スイッチオーバー	Cisco IOS XE Release 3.10S	この機能により、1 つのグループ内のすべての擬似回線をバックアップ擬似回線に迅速にスイッチオーバーできます。このグループ スイッチオーバーは、リモート ピアから 1 つの「グループ ダウン」ステータス メッセージを受信するとトリガーされます。 次のコマンドが導入または変更されました：**redundancy predictive**、**show ssm group**。

第 15 章

L2VPN 擬似回線スイッチング

この機能モジュールでは、L2VPN 擬似回線スイッチングを設定する方法について説明します。これは、レイヤ 2 のバーチャル プライベート ネットワーク（L2VPN）擬似回線を相互自律システム（inter-AS）の境界を超えて、または 2 つの別個のマルチプロトコル ラベル スイッチング（MPLS）ネットワークにわたって拡張します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース 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、機能情報の表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シスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

L2VPN 擬似回線スイッチングの制約事項

- Cisco IOS XE Release 2.4 では、擬似回線スイッチングが Ethernet over MPLS 接続回線でサポートされます。
- L2VPN 擬似回線スイッチングは、AToM でサポートされます。
- スタティックなオンボックス プロビジョニングだけがサポートされています。
- AToM パケットのシーケンス番号は、L2VPN 擬似回線スイッチングでは処理されません。この機能では、xconnect パケットパスを介してシーケンスデータを渡します。これは、透過的なシーケンシングと呼ばれるプロセスです。エンドポイント PE-CE 接続には、このシーケンシングが適用されます。
- 隣接するネクスト ホップ PE ルータに ping を実行できます。エンドツーエンド LSP ping はサポートされていません。
- L2VPN 擬似回線スイッチングがイネーブルにされているルータでは、IP またはイーサネットインターワーキングを設定しないでください。代わりに、ネットワークのエッジ PE でルータのインターワーキングを設定します。
- 制御ワードネゴシエーションの結果が一致している必要があります。いずれかのセグメントが制御ワードをネゴシエートしない場合は、両方のセグメントで制御ワードが無効になります。
- AToM グレースフル リスタートは、個々の擬似回線セグメントで個別にネゴシエーションされます。2 つの AToM PE ルータ間の LDP セッションで一時的な切断が発生しても、パケットは流れ続けます。
- 擬似回線ごとの Quality of Service（QoS）はサポートされていません。トラフィック エンジニアリング（TE）トンネルの選択はサポートされています。
- 接続回線のインターワーキングはサポートされていません。

L2VPN 擬似回線スイッチングに関する情報

L2VPN 擬似回線スイッチングの動作

下図のように、L2VPN 擬似回線スイッチングにより、ユーザは AS 間境界を越えて、または 2 つの別個の MPLS ネットワークをまたがって、L2VPN 擬似回線を拡張することができます。L2VPN 擬似回線スイッチングは、2 つ以上の連続した擬似回線セグメントを接続して、エンドツーエンドのマルチホップ擬似回線を形成します。このエンドツーエンドの擬似回線は、単一のポイントツーポイント擬似回線として機能します。

下の 2 番目の図に示すように、L2VPN 擬似回線スイッチングにより、AS 間境界を越えて、エッジ PE ルータの IP アドレスをプライベートに維持できます。自律システム境界ルータ（ASBR）の

IPアドレスを使用し、それらを擬似回線集約（PE-agg）ルータとして扱うことができます。ASBRは、2つのドメインの擬似回線を結合します。

また、L2VPN擬似回線スイッチングにより、異なる管理またはプロビジョニング ドメインを維持し、エンドツーエンドのサービスを管理できます。これらのネットワークの境界で、PE-AGGルータは管理責任を表します。

図 *34*：*AS* 内トポロジの *L2VPN* 擬似回線スイッチング

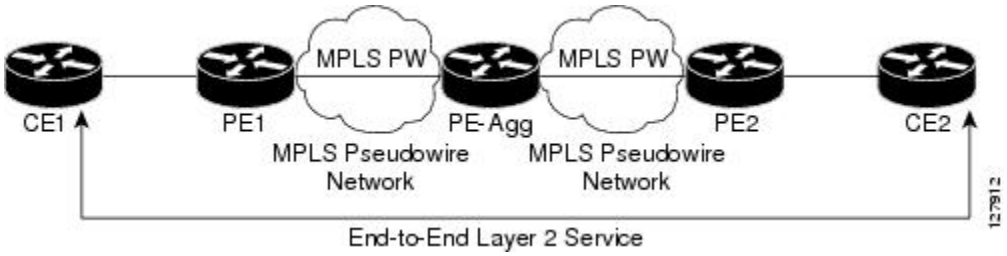
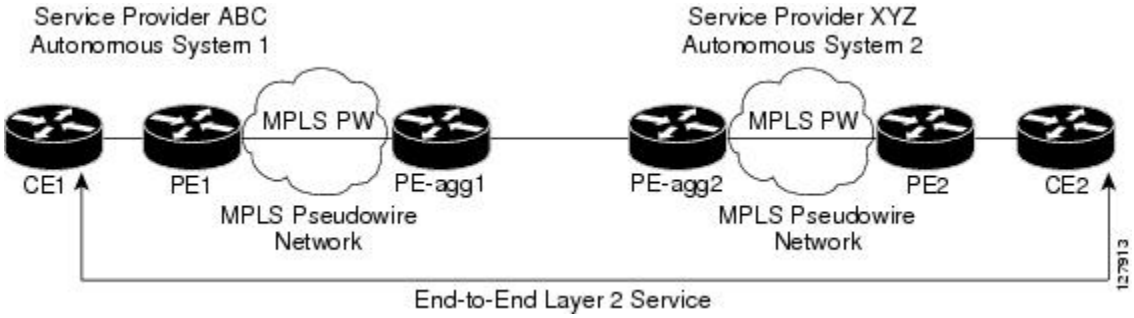


図 *35*：*AS* 間トポロジの *L2VPN* 擬似回線スイッチング



パケットが集約ポイントで処理される仕組み

2つのAToM擬似回線間のAToMパケットの切り替えは任意のMPLSパケットの切り替えと同じです。MPLS切り替えデータ パスは、2つのAToM擬似回線の間でAToMパケットを切り替えます。次のリストは例外を示しています。

- 発信仮想回線（VC）ラベルはパケット内の着信VCラベルを置き換えます。新しい内部ゲートウェイ プロトコル（IGP）ラベルとレイヤ2カプセル化が追加されます。
- 着信VCラベルの存続可能時間（TTL）フィールドは1ずつ減らされ、発信VCラベルのTTLフィールドにコピーされます。
- 着信VCラベルのEXP値は発信VCラベルのEXPフィールドにコピーされます。
- 発信VCラベルの「Bottom of Stack」Sビットは1に設定されます。
- AToMコントロール ワードの処理は、L2VPN擬似回線スイッチングの集約ポイントでは実行されません。シーケンス番号は検証されません。LSP Pingにルータ アラート ラベルを使用します。LSP Pingパケットの判別にコントロール ワード検査は必要ありません。

L2VPN 擬似回線スイッチングの設定方法

設定

PE-agg ルータのそれぞれで L2VPN 擬似回線スイッチングを設定するには、次の手順を実行します。

はじめる前に

- この手順は、基本的な AToM L2VPN がすでに設定されていることを前提にしています。この手順では、MPLS バックボーン経由でレイヤ 2 パケットを転送する基本的な AToM L2VPN の設定方法については説明しません。基本設定の詳細については、「Any Transport over MPLS」を参照してください。
- 相互自律設定では、ASBR にラベル付きのインターフェイスが必要です。

（注） この設定では、**l2vfi** コマンドの入力後は 2 つの **neighbor** コマンドに制限されます。
>

手順の概要

1. イネーブル化
2. **configureterminal**
3. **l2vfi***name***point-to-point**
4. **neighbor***ip-addressvcid***encapsulationmpls**|**pw-class***pw-class-name*
5. **exit**
6. **exit**
7. **showmplsl2transportvc** [**vcid** [*vc-id* | [*vc-id-minvc-id-max*]] [**interface***name*[*local-circuit-id*]] [**destination***ip-address* | *name*] [**detail**]
8. **showvfi**[*vfi-name*]
9. **ping** [*protocol*] [**tag**] {*host-name*| *system-address*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 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	**l2vfi***name***point-to-point** 例： `Router(config)# l2 vfi atomtunnel point-to-point`	ポイントツーポイント レイヤ 2 Virtual Forwarding Interface（VFI）を作成し、VFI 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	**neighbor***ip-addressvcid***encapsulationmpls**|**pw-class***pw-class-name* 例： `Router(config-vfi)# neighbor 10.0.0.1 100 pw-class mpls`	エミュレートされた VC を設定します。リモート ルータの IP アドレスと VC ID を指定します。また、エミュレートされた VC で使用する擬似回線クラスを指定します。 （注） 2 つの **neighbor** コマンドだけが **l2vfipoint-to-point** コマンドごとに許可されます。
ステップ 5	**exit** 例： `Router(config-vfi)# exit`	VFI コンフィギュレーション モードを終了します。
ステップ 6	**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。
ステップ 7	**showmplsl2transportvc** [**vcid** [*vc-id* | [*vc-id-minvc-id-max*]] [**interface***name*[*local-circuit-id*]] [**destination***ip-address* | *name*] [**detail**] 例： `Router# show mpls l2transport vc`	L2VPN 擬似回線スイッチング セッションが確立されていることを確認します。
ステップ 8	**showvfi**[*vfi-name*] 例： `Router#` **show vfi atomtunnel**	ポイントツーポイント VFI が確立されたことを検証します。

	コマンドまたはアクション	目的
ステップ 9	**ping** [*protocol*] [**tag**] {*host-name*| *system-address*} 例： `Router# ping 10.1.1.1`	CEルータから発行された場合は、このコマンドがエンドツーエンドの接続を確認します。

例

次に、**showmplsl2transportvc** コマンドの出力例を示します。

```
Router# show mpls l2transport vc
Local intf     Local circuit              Dest address    VC ID Status
-------------  -------------------------- --------------- ----- ----
MPLS PW        10.0.1.1:100               10.0.1.1        100   UP
MPLS PW        10.0.1.1:100               10.0.1.1        100   UP
```

次に、**showvfi** コマンドの出力例を示します。

```
Router# show vfi
VFI name: test, type: point-to-point
 Neighbors connected via pseudowires:
   Router ID        Pseudowire ID
   10.0.1.1         100
   10.0.1.1         100
```

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した L2VPN 擬似回線スイッチングの設定方法

PE-agg ルータのそれぞれで L2VPN 擬似回線スイッチングを設定するには、次のタスクを実行します。この設定では、**l2vpnxconnect** コマンドの入力後は 2 つの **neighbor** コマンドに制限されます。

はじめる前に

- このタスクは、基本的な AToM L2VPN がすでに設定されていることを前提としています。このタスクでは、MPLS バックボーン経由でレイヤ 2 パケットを転送する基本的な AToM L2VPN の設定方法については説明しません。基本設定の詳細については、「Any Transport over MPLS」の項を参照してください。
- 相互自律設定では、自律システム境界ルータ（ASBR）にラベル付きのインターフェイスが必要です。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacepseudowire***number*
4. **encapsulationmpls**
5. **neighbor***peer-addressvcid-value*
6. **exit**
7. **interfacepseudowire***number*
8. **encapsulationmpls**
9. **neighbor***peer-addressvcid-value*
10. **exit**
11. **l2vpnxconnectcontext***context-name*
12. **member pseudowire***interface-number*
13. **member***ip-addressvcid***encapsulationmpls**
14. **member pseudowire***interface-number*
15. **member***ip-addressvcid***encapsulationmpls**
16. **exit**
17. **exit**
18. **showl2vpnatomvc** [**vcid** [*vc-id* | *vc-id-minvc-id-max*]] [**interface***type number* [*local-circuit-id*]] [**destination***ip-address* | *name*] [**detail**]
19. **ping**[*protocol*] [**tag**] {*hostname*| *system-address*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**interfacepseudowire***number* 例： `Router(config)# interface pseudowire 100`	擬似回線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。

	コマンドまたはアクション	目的
ステップ 4	**encapsulationmpls** 例： `Router(config-if)# encapsulation mpls`	マルチプロトコルラベルスイッチング（MPLS）がデータカプセル化方式として使用されることを指定します。
ステップ 5	**neighbor***peer-addressvcid-value* 例： `Router(config-if)# neighbor 10.0.0.1 123`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 6	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 7	**interfacepseudowire***number* 例： `Router(config)# interface pseudowire 200`	擬似回線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 8	**encapsulationmpls** 例： `Router(config-if)# encapsulation mpls`	マルチプロトコルラベルスイッチング（MPLS）がデータカプセル化方式として使用されることを指定します。
ステップ 9	**neighbor***peer-addressvcid-value* 例： `Router(config-if)# neighbor 10.0.0.2 124`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 10	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 11	**l2vpnxconnectcontext***context-name* 例： `Device(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect 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 12	**member pseudowire***interface-number* 例： `Router(config-xconnect)# member pseudowire 100`	Layer 2 VPN（L2VPN）クロス コネクトを形成するようにメンバー擬似回線を指定します。
ステップ 13	**member***ip-addressvcid***encapsulationmpls** 例： `Device(config-xconnect)# member 10.0.0.1 123 encapsulation mpls`	ポイントツーポイント Layer 2 VPN（L2VPN）Virtual Forwarding Interface（VFI）接続を形成するデバイスを指定します。 （注） 2 つの **member** コマンドだけが **l2vpnxconnectcontext** コマンドごとに許可されます。
ステップ 14	**member pseudowire***interface-number* 例： `Router(config-xconnect)# member pseudowire 200`	Layer 2 VPN（L2VPN）クロス コネクトを形成するようにメンバー擬似回線を指定します。
ステップ 15	**member***ip-addressvcid***encapsulationmpls** 例： `Device(config-xconnect)# member 10.0.0.2 124 encapsulation mpls`	ポイントツーポイント Layer 2 VPN（L2VPN）Virtual Forwarding Interface（VFI）接続を形成するデバイスを指定します。 （注） 2 つの **member** コマンドだけが **l2vpnxconnectcontext** コマンドごとに許可されます。
ステップ 16	**exit** 例： `Device(config-xconnect)# exit`	Xconnect コンフィギュレーション モードを終了します。
ステップ 17	**exit** 例： `Device(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。
ステップ 18	**showl2vpnatomvc** [**vcid** [*vc-id* | *vc-id-minvc-id-max*]] [**interface***type number* [*local-circuit-id*]] [**destination***ip-address* | *name*] [**detail**] 例： `Device# show l2vpn atom vc`	デバイス上でレイヤ 2 パケットをルーティングするために有効化された Any Transport over MPLS（AToM）仮想回線（VC）とスタティック擬似回線に関する情報を表示します。

	コマンドまたはアクション	目的
ステップ 19	**ping**[*protocol*] [**tag**] {*hostname*| *system-address*} 例： `Device# ping 10.1.1.1`	CE ルータから発行された場合は、エンドツーエンドの接続を確認します。

設定

PE-agg ルータのそれぞれで L2VPN 擬似回線スイッチングを設定するには、次の手順を実行します。

はじめる前に

- この手順は、基本的な AToM L2VPN がすでに設定されていることを前提にしています。この手順では、MPLS バックボーン経由でレイヤ 2 パケットを転送する基本的な AToM L2VPN の設定方法については説明しません。基本設定の詳細については、「Any Transport over MPLS」を参照してください。
- 相互自律設定では、ASBR にラベル付きのインターフェイスが必要です。

（注） この設定では、**l2vfi** コマンドの入力後は 2 つの **neighbor** コマンドに制限されます。

>

手順の概要

1. イネーブル化
2. **configureterminal**
3. **l2vfi***name***point-to-point**
4. **neighbor***ip-addressvcid***encapsulationmpls**|**pw-class***pw-class-name*
5. **exit**
6. **exit**
7. **showmplsl2transportvc** [**vcid** [*vc-id* | [*vc-id-minvc-id-max*]] [**interface***name*[*local-circuit-id*]] [**destination***ip-address* | *name*] [**detail**]
8. **showvfi**[*vfi-name*]
9. **ping** [*protocol*] [**tag**] {*host-name*| *system-address*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**l2vfi***name***point-to-point** 例： `Router(config)# l2 vfi atomtunnel point-to-point`	ポイントツーポイント レイヤ 2 Virtual Forwarding Interface（VFI）を作成し、VFI 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	**neighbor***ip-addressvcid***encapsulationmpls**|**pw-class***pw-class-name* 例： `Router(config-vfi)# neighbor 10.0.0.1 100 pw-class mpls`	エミュレートされた VC を設定します。リモート ルータの IP アドレスと VC ID を指定します。また、エミュレートされた VC で使用する擬似回線クラスを指定します。 （注） 2 つの **neighbor** コマンドだけが **l2vfipoint-to-point** コマンドごとに許可されます。
ステップ 5	**exit** 例： `Router(config-vfi)# exit`	VFI コンフィギュレーション モードを終了します。
ステップ 6	**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。
ステップ 7	**showmplsl2transportvc** [**vcid** [*vc-id* | [*vc-id-minvc-id-max*]] [**interface***name*[*local-circuit-id*]] [**destination***ip-address* | *name*] [**detail**] 例： `Router# show mpls l2transport vc`	L2VPN 擬似回線スイッチング セッションが確立されていることを確認します。

	コマンドまたはアクション	目的
ステップ 8	**showvfi**[*vfi-name*] 例： `Router#` **show vfi atomtunnel**	ポイントツーポイント VFI が確立されたことを検証します。
ステップ 9	**ping** [*protocol*] [**tag**] {*host-name*| *system-address*} 例： `Router# ping 10.1.1.1`	CE ルータから発行された場合は、このコマンドがエンドツーエンドの接続を確認します。

例

次に、**showmplsl2transportvc** コマンドの出力例を示します。

```
Router# show mpls l2transport vc
Local intf     Local circuit              Dest address    VC ID Status
-------------  -------------------------- --------------- ----- ----
MPLS PW        10.0.1.1:100               10.0.1.1        100   UP
MPLS PW        10.0.1.1:100               10.0.1.1        100   UP
```

次に、**showvfi** コマンドの出力例を示します。

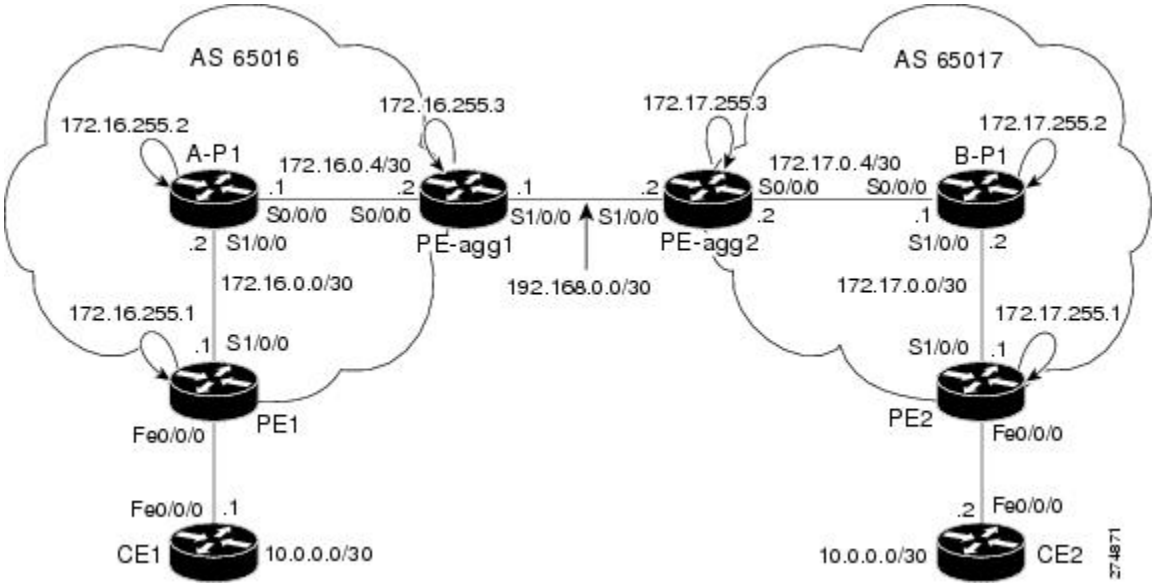
```
Router# show vfi
VFI name: test, type: point-to-point
 Neighbors connected via pseudowires:
   Router ID        Pseudowire ID
   10.0.1.1         100
   10.0.1.1         100
```

L2VPN 擬似回線スイッチングの設定例

Inter-AS コンフィギュレーションでの L2VPN 擬似回線スイッチング：例

2 つの自律システムは L2VPN パケットを送信できます。これは、2 つの PE-AGG ルータで L2VPN 擬似回線スイッチングが設定されているためです。この例のコンフィギュレーションを次の図に示します。

図 *36*：*InterAutonomous* システムでの *L2VPN* 擬似回線スイッチング



CE1	CE2

CE1	CE2
version 12.0 service timestamps debug uptime service timestamps log uptime service password-encryption ! hostname [ce1] ! boot-start-marker boot-end-marker ! enable secret 5 1o9N6$LSrxHufTn0vjCY0nW8hQX. ! ip subnet-zero ip cef no ip domain-lookup ! interface FastEthernet0/0/0 ip address 10.0.0.1 255.255.255.252 no ip directed-broadcast ! ip classless ! control-plane ! line con 0 exec-timeout 0 0 line aux 0 line vty 0 4 login ! no cns aaa enable end	version 12.0 service timestamps debug uptime service timestamps log uptime service password-encryption ! hostname [ce2] ! boot-start-marker boot-end-marker ! enable secret 5 1YHo6$LQ4z5PdrF5B9dnL75Xvvm1 ! ip subnet-zero ip cef no ip domain-lookup ! interface FastEthernet0/0/0 ip address 10.0.0.2 255.255.255.252 no ip directed-broadcast ! ip classless ! control-plane ! line con 0 exec-timeout 0 0 line aux 0 line vty 0 4 login ! no cns aaa enable end

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
MPLS コマンド	『Cisco IOS Multiprotocol Label Switching Command Reference』
L2VPN 擬似回線冗長性	『*MPLS Layer 2 VPNs Configuration Guide*』の「L2VPN Pseudowire Redundancy」機能モジュール
H-VPLS	『*Optical Services Modules Installation and Configuration Notes*, 12.2SR』の「Configuring Multiprotocol Label Switching on the Optical Services Modules」の章の「Configuring VPLS」
MPLS トラフィック エンジニアリング	『*MPLS Traffic Engineering: Path, Link, and Node Protection Configuration Guide*』（Multiprotocol Label Switching Configuration Guide Library に含まれる）の「MPLS Traffic Engineering Fast Reroute Link and Node Protection」機能モジュール

標準

規格	Title
http://www.ietf.org/rfc/rfc4447.txt	『*Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)*』
http://www3.ietf.org/proceedings/06mar/IDs/draft-ietf-l2vpn-vpls-ldp-08.txt	『*Virtual Private LAN Services over MPLS*』
http://www.ietf.org/internet-drafts/draft-ietf-pwe3-segmented-pw-02.txt	『*Segmented Pseudo Wire*』
draft-ietf-pwe3-vccv-10.txt	『*Pseudo Wire Virtual Circuit Connectivity Verification (VCCV)*』
draft-ietf-pwe3-oam-msg-map-03.txt	『*Pseudo Wire (PW) OAM Message Mapping*』

MIB

MIB	MIB のリンク
イーサネット サービス、フレームリレー サービス、および ATM サービス用 Pseudowire Emulation Edge-to-Edge MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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。	http://www.cisco.com/cisco/web/support/index.html

L2VPN 擬似回線スイッチングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、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。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *27* : ***L2VPN*** 擬似回線スイッチングの機能情報

機能名	リリース	機能情報
L2VPN 擬似回線スイッチング	Cisco IOS XE Release 2.4	L2VPN 擬似回線スイッチング機能により、レイヤ2バーチャル プライベート ネットワーク（L2VPN）擬似回線が、自律システム間（inter-AS）境界または2つの個別マルチプロトコル ラベル スイッチング（MPLS）ネットワークを超えて拡張されます。 Cisco IOS XE Release 2.4 では、Ethernet over MPLS で L2VPN 擬似回線スイッチング機能がサポートされます。 次のコマンドが導入または変更されました： **l2vfipoint-to-point**、**neighbor**（L2VPN 擬似回線スイッチング）、**showvfi**。

第 16 章

BFD クライアントとしての Xconnect

Bidirectional Forwarding Detection（BFD）機能のクライアントとしての Xconnect は、BFD の早期障害検出機能に基づいて冗長な擬似回線スイッチオーバーのトリガーを提供します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース 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、機能情報の表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シスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

BFD クライアントとしての Xconnect に関する情報

BFD クライアントとしての Xconnect

耐障害性と L2VPN バックホール接続への復元力を提供するために、冗長な擬似回線が導入されています。システムが障害から回復する速度は、特に多数の擬似回線に拡張されている場合、多くのサービス プロバイダーやサービス レベル契約（SLA）にとって非常に重要です。冗長擬似回線スイッチオーバーのトリガーの設定によって、多数の擬似回線をフェールオーバーするためにかかる時間が短縮されます。Bidirectional Forwarding Detection（BFD）機能の基本コンポーネントは、早期障害検出（FFD）によって有効になります。

この機能の設定は、次のような BFD 設定を参照します（**bfd map** コマンドの 2 番目の URL は、**monitor peer bfd** コマンドのループバック URL です）。

```
bfd-template multi-hop mh
 interval min-tx 200 min-rx 200 multiplier 3 !
bfd map ipv4  10.1.1.0/24  10.1.1.1/32 mh
```

BFD クライアントとしての Xconnect の設定方法

BFD クライアントとしての Xconnect の設定

冗長な擬似回線スイッチオーバーのトリガーを設定するには、次のタスクを実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **pseudowire-class mpls-ffd**
   - 擬似回線クラス コンフィギュレーション モードを開始します。
4. **encapsulation mpls**
5. **monitor peer bfd** [**local interface***interface-type interface-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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# 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	**pseudowire-class mpls-ffd** • 擬似回線クラス コンフィギュレーション モードを開始します。 例： `Device(config)# pseudowire-class mpls-ffd`	MPLS 早期障害検出用の擬似回線クラスを設定します。
ステップ 4	**encapsulation mpls** 例： `Device(config-pw-class)# encapsulation mpls`	トンネリング カプセル化を MPLS になるように指定します。
ステップ 5	**monitor peer bfd** [**local interface***interface-type interface-number*] 例： `Device(config-pw-class)# monitor peer bfd local interface loopback 0`	擬似回線早期障害検出機能を有効にします。

BFD クライアントとしての Xconnect の設定例

例：BFD クライアントとしての Xconnect

擬似回線クラスの設定

次の例は、擬似回線クラスに対して擬似回線高速障害検出が有効になっていることを示します。

```
pseudowire-class mpls-ffd
 encapsulation mpls
 monitor peer bfd local interface Loopback0
```

テンプレートの設定

次の例は、テンプレートで擬似回線高速障害検出が有効になっていることを示します。

```
template type pseudowire 1
 encapsulation mpls
 monitor peer bfd local interface Ethernet0/1
```

インターフェイス コンフィギュレーション

次の例は、インターフェイスに対して擬似回線高速障害検出が有効になっていることを示します。

```
interface pseudowire100
 encapsulation mpls
 neighbor 10.10.1.1 21190
 monitor peer bfd local interface Ethernet0/1
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Any Transport over MPLS	Any Transport over MPLS
AToM のハイ アベイラビリティ	『AToM Graceful Restart』
L2VPN インターワーキング	L2VPN インターワーキング
レイヤ 2 ローカル スイッチング	レイヤ 2 ローカル スイッチング
PWE3 MIB	『Pseudowire Emulation Edge-to-Edge MIBs for Ethernet and Frame Relay Services』
パケット シーケンシング	『Any Transport over MPLS (AToM) Sequencing Support』
BFD コンフィギュレーション	『IP Routing BFD Configuration Guide』

標準

標準	Title
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探して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	Title
なし	--

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

BFD クライアントとしての Xconnect の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、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。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *28*：*BFD* クライアントとしての *Xconnect* の機能情報

機能名	リリース	機能情報
BFD クライアントとしての Xconnect	Cisco IOS XE Release 3.8S	この機能は、L2VPN 擬似回線冗長性のための高速障害検出機能を提供します。 次のコマンドが導入されました：**if-state nhrp**。

第 17 章

QinQ アクセス対応の H-VPLS N-PE 冗長性

QinQ アクセス対応の H-VPLS N-PE 冗長性機能を使用すると、2 つのネットワーク プロバイダー エッジ（N-PE）デバイスで、Hierarchical Virtual Private LAN Service（H-VPLS）のユーザ プロバイダー エッジ（U-PE）デバイスに対しフェールオーバー サービスを提供できます。冗長 N-PE デバイスを使用すると、安定性および信頼性が向上し、リンク障害およびノード障害に対処できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース 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、機能情報の表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シスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

QinQ アクセス対応の H-VPLS N-PE 冗長性の前提条件

- この機能を設定する前に、階層型仮想プライベート LAN サービス（H-VPLS）ネットワークを設定し、このネットワークが正しく動作していることを確認してください。
- PE-to-CE（カスタマーエッジ）インターフェイスで、一連の許可されている VLAN が設定されていることを確認します。
- コンバージェンスを高速化するには、マルチプロトコル ラベル スイッチング（MPLS）コアで MPLS Traffic Engineering—Fast Reroute 機能を有効化します。
- MPLS アクセスに対応するためユーザ プロバイダー エッジ（U-PE）デバイスで L2VPN 擬似回線冗長性機能を有効にします。
- マルチ スパニングツリー プロトコル（MSTP）を設定する際に、**spanning-tree mst***instance-id***priority***priority* コマンドを使用して最も低いプライオリティを割り当てることによって、ネットワーク プロバイダー エッジ（N-PE）デバイスの 1 つがルートになるように指定します。
- MSTP を設定する際は、MST コンフィギュレーション モードで **revision**、**name**、および **instance** コマンドを発行することによって、スパニング ツリーに参加している各デバイスが同じ領域にあり、同じリビジョンであることを確認します。

QinQ アクセス対応の H-VPLS N-PE 冗長性の制約事項

- この機能は、ネットワーク プロバイダー エッジ（N-PE）デバイスに接続する擬似回線の VPLS 自動検出機能では使用できません。仮想プライベート LAN サービス（VPLS）を作成するときに、仮想転送インスタンス（VFI）を手動で作成できます。
- 同じ仮想プライベート LAN サービス（VPLS）サイトの 2 つの冗長性ネットワーク プロバイダー エッジ（N-PE）デバイス間でブリッジ プロトコル データ ユニット（BPDU）パケットを送信するために、複数の擬似回線を設定することはできません。
- N-PE デバイスで H-VPLS N-PE 冗長性機能を設定するときには、ローカル ループバック アドレスをネイバーとして設定することはできません。そのように設定すると、次のエラー メッセージが表示されます。

```
VPLS local switching to peer address not supported
```

- 各 U-PE デバイスに接続できる N-PE デバイスは 2 台だけです。
- スパニング ツリー モードは、H-VPLS N-PE 冗長性機能用のマルチ スパニングツリー プロトコル（MSTP）にする必要があります。スパニング ツリー モードを変更すると、BPDU パケットを送信する擬似回線が存在し、H-VPLS N-PE 冗長性機能が設定されていても、H-VPLS N-PE 冗長性機能が正常に機能しない場合があります。

QinQ アクセス対応の H-VPLS N-PE 冗長性に関する情報

QinQ アクセス対応の H-VPLS N-PE 冗長性の動作

H-VPLS N-PE 冗長性機能が設定されているネットワークでは、ユーザのプロバイダー エッジ（U-PE）デバイスは、2 つのネットワーク プロバイダーエッジ（N-PE）デバイスに接続されています。この機能は、リンクとデバイスの両方の障害を許容できるレベルの冗長性を提供します。1 つの N-PE デバイスのデータ伝送を無効にする障害がネットワークに発生した場合、もう 1 つの N-PE デバイスが引継ぎます。この機能は、マルチ スパニング ツリー プロトコル（MSTP）に基づく Qin Q アクセスと擬似回線冗長性に基づくマルチプロトコル ラベル スイッチング（MPLS）アクセスの両方で機能します。

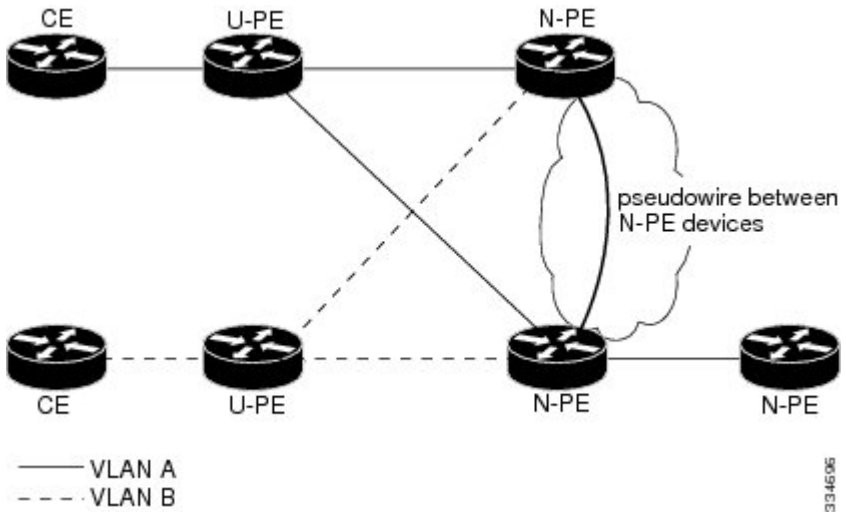
MSTP に基づく QinQ アクセス対応の H-VPLS N-PE 冗長性

QinQ アクセス機能による H-VPLS N-PE 冗長性は、階層型仮想プライベート LAN サービス（H-VPLS）ネットワーク内のネットワーク プロバイダーエッジ（N-PE）デバイスとユーザ プロバイダー エッジ（U-PE）デバイスで実行する Multiple Spanning Tree Protocol（MSTP）を使用します。N-PEデバイス間で動作する擬似回線は、MSTPブリッジプロトコルデータ ユニット（BPDU）のみを伝送します。N-PE デバイス間で動作する擬似回線は常にアップ状態で、MSTP が U-PE デバイスと N-PE デバイスの間の冗長パスの 1 つをブロックするように、N-PE デバイス間のループ パスを作成するために使用されます。プライマリ N-PE デバイスまたはそこへのパスに障害が発生すると、MSTP はバックアップ N-PE デバイスへのパスを有効にします。

次の図は冗長なアクセスを持つ H-VPLS ネットワークを示します。各 U-PE デバイスには 2 つの接続があり、各 N-PE デバイスに対応しています。2 つの N-PE デバイス間には擬似回線があり、MSTP BPDU のループ パスを提供します。ネットワーク トポロジにより、プライマリ N-PE デバ

イスまたはそこへのパスに障害が発生すると、バックアップ N-PE デバイスが継承できるようになります。

図 *37*：*MSTP* に基づく *QinQ* アクセス対応の *H-VPLS N-PE* 冗長性



QinQ アクセス対応の H-VPLS N-PE 冗長性の設定方法

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した N-PE デバイス間の VPLS 擬似回線の設定

階層型仮想プライベート LAN サービス（H-VPLS）ネットワークでネットワーク プロバイダー エッジ（N-PE）の冗長性を設定するには、ブリッジプロトコルデータユニット（BPDU）パケットを送信するための VPLS 擬似回線を設定する必要があります。N-PE デバイス間のコア擬似回線では、Layer 2 VPN（L2VPN）Virtual Forwarding Interface（VFI）を設定して、VFI をブリッジ ドメインにアタッチします（ここで説明）。その次のタスクで、サービス インスタンスをブリッジドメインにバインドします。この設定は、リンクとノードの障害に対する信頼性を向上させる冗長性を提供します。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **l2vpn vfi context***name*
4. **vpn id***vpn id*
5. **member***ip-address***encapsulation mpls**
6. **forward permit l2protocol all**
7. **exit**
8. **bridge-domain***bridge-id*
9. **member vfi***vfi-name*
10. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**l2vpn vfi context***name* 例： `Device(config)# l2vpn vfi context VPLS-10`	複数の異なるネットワーク間の L2VPN VFI を確立して、L2VFI 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	**vpn id***vpn id* 例： `Device(config-vfi)# vpn id 10`	仮想プライベート LAN サービス（VPLS）インスタンス上で VPN ID を設定します。 • 同じ VPN に属している PE デバイスに対しては同じ VPN ID を使用します。 • サービス プロバイダー ネットワーク内の VPN ごとに VPN ID が一意であることを確認します。範囲は 1 ～ 4294967295 です。

	コマンドまたはアクション	目的
ステップ 5	**member***ip-address***encapsulation mpls** 例： `Device(config-vfi)# member 102.102.102.102 encapsulation mpls`	ポイントツーポイント L2VPN VFI 接続を形成するデバイスを指定します。 • *ip-address*：VFI ネイバーの IP アドレス。 • **encapsulation mpls**：データ カプセル化方式としてマルチプロトコル ラベル スイッチング（MPLS）を指定します。
ステップ 6	**forward permit l2protocol all** 例： `Device(config-vfi)# forward permit l2protocol all`	2 つの N-PE デバイス間で BPDU パケットを転送するために使用される擬似回線を作成します。
ステップ 7	**exit** 例： `Device(config-vfi)# exit`	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	**bridge-domain***bridge-id* 例： `Device(config)# bridge-domain 10`	ブリッジ ドメインでコンポーネントを設定して、ブリッジ ドメイン コンフィギュレーション モードを開始します。
ステップ 9	**member vfi***vfi-name* 例： `Device(config-bdomain)# member vfi VPLS-10`	ブリッジ ドメイン内の VFI メンバーを設定します。
ステップ 10	**end** 例： `Device(config-bdomain)# end`	特権 EXEC モードに戻ります。

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した N-PE デバイス間の VPLS 擬似回線の設定

階層型仮想プライベート LAN サービス（H-VPLS）ネットワークでネットワーク プロバイダー エッジ（N-PE）の冗長性を設定するには、ブリッジプロトコルデータユニット（BPDU）パケットを送信するための VPLS 擬似回線を設定する必要があります。N-PE デバイス間のコア擬似回線では、Layer 2 VPN（L2VPN）Virtual Forwarding Interface（VFI）を設定して、VFI をブリッジ ドメインにアタッチします（ここで説明）。その次のタスクで、サービス インスタンスをブリッジ

ドメインにバインドします。この設定は、リンクとノードの障害に対する信頼性を向上させる冗長性を提供します。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **l2vpn vfi context***name*
4. **vpn id***vpn id*
5. **member***ip-address***encapsulation mpls**
6. **forward permit l2protocol all**
7. **exit**
8. **bridge-domain***bridge-id*
9. **member vfi***vfi-name*
10. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**l2vpn vfi context***name* 例： `Device(config)# l2vpn vfi context VPLS-10`	複数の異なるネットワーク間の L2VPN VFI を確立して、L2VFI 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	**vpn id***vpn id* 例： `Device(config-vfi)# vpn id 10`	仮想プライベート LAN サービス（VPLS）インスタンス上で VPN ID を設定します。 • 同じ VPN に属している PE デバイスに対しては同じ VPN ID を使用します。 • サービス プロバイダー ネットワーク内の VPN ごとに VPN ID が一意であることを確認します。範囲は 1 ～ 4294967295 です。

	コマンドまたはアクション	目的
ステップ 5	**member***ip-address***encapsulation mpls** 例： `Device(config-vfi)# member 102.102.102.102 encapsulation mpls`	ポイントツーポイント L2VPN VFI 接続を形成するデバイスを指定します。 • *ip-address*：VFI ネイバーの IP アドレス。 • **encapsulation mpls**：データ カプセル化方式としてマルチプロトコル ラベル スイッチング（MPLS）を指定します。
ステップ 6	**forward permit l2protocol all** 例： `Device(config-vfi)# forward permit l2protocol all`	2 つの N-PE デバイス間で BPDU パケットを転送するために使用される擬似回線を作成します。
ステップ 7	**exit** 例： `Device(config-vfi)# exit`	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	**bridge-domain***bridge-id* 例： `Device(config)# bridge-domain 10`	ブリッジ ドメインでコンポーネントを設定して、ブリッジ ドメイン コンフィギュレーション モードを開始します。
ステップ 9	**member vfi***vfi-name* 例： `Device(config-bdomain)# member vfi VPLS-10`	ブリッジ ドメイン内の VFI メンバーを設定します。
ステップ 10	**end** 例： `Device(config-bdomain)# end`	特権 EXEC モードに戻ります。

ブリッジ ドメインへのサービス インスタンスのバインド

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface***type number*
4. **service instance***id***ethernet**
5. **encapsulation dot1q***vlan-id*
6. **exit**
7. **bridge-domain***bridge-id*
8. **member***interface-type-number***service-instance***service-id*
9. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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： `Device(config)# interface GigabitEthernet0/1/0`	設定する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	**service instance***id***ethernet** 例： `Device(config-if)# service instance 10 ethernet`	インターフェイスでイーサネット サービス インスタンスを設定し、イーサネット サービス コンフィギュレーションモードを開始します。
ステップ 5	**encapsulation dot1q***vlan-id* 例： `Device(config-if-srv)# encapsulation dot1q 10`	VLAN の指定されたインターフェイス上で、トラフィックの IEEE 802.1Q カプセル化を有効にします。

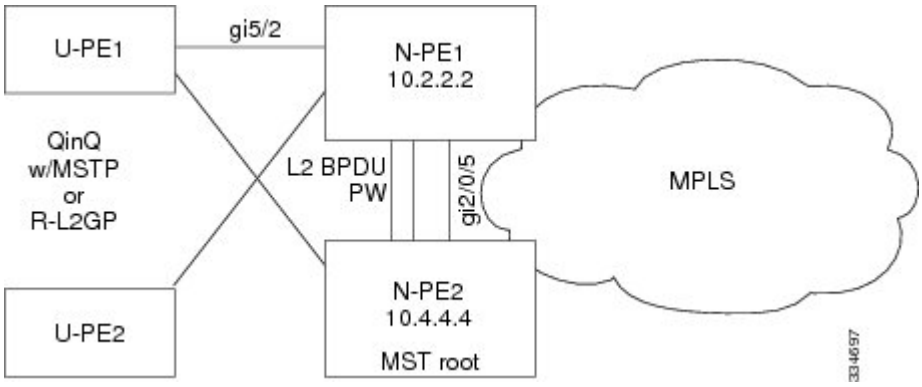
	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `Device(config-if-srv)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**bridge-domain***bridge-id* 例： `Device(config)# bridge-domain 10`	ブリッジ ドメイン上でコンポーネントを設定し、ブリッジ ドメイン コンフィギュレーション モードを開始します。
ステップ 8	**member***interface-type-number***service-instance***service-id* 例： `Device(config-bdomain)# member GigabitEthernet0/1/0 service-instance 10`	ブリッジドメイン インスタンスにサービス インスタンスをバインドします。
ステップ 9	**end** 例： `Device(config-bdomain)# end`	特権 EXEC モードに戻ります。

QinQ アクセス対応の H-VPLS N-PE 冗長性の設定例

例：QinQ アクセス対応の H-VPLS N-PE 冗長性

次の図に、QinQ アクセス対応の H-VPLS N-PE 冗長性機能に対して設定されたコンフィギュレーションを示します。

図 *38*： *QinQ* アクセス対応の *H-VPLS N-PE* 冗長性のトポロジ



次の表は、2 つのネットワーク プロバイダー エッジ（N-PE）デバイスの設定を示しています。

表 *29*：例：*QinQ* アクセス対応の *H-VPLS N-PE* 冗長性

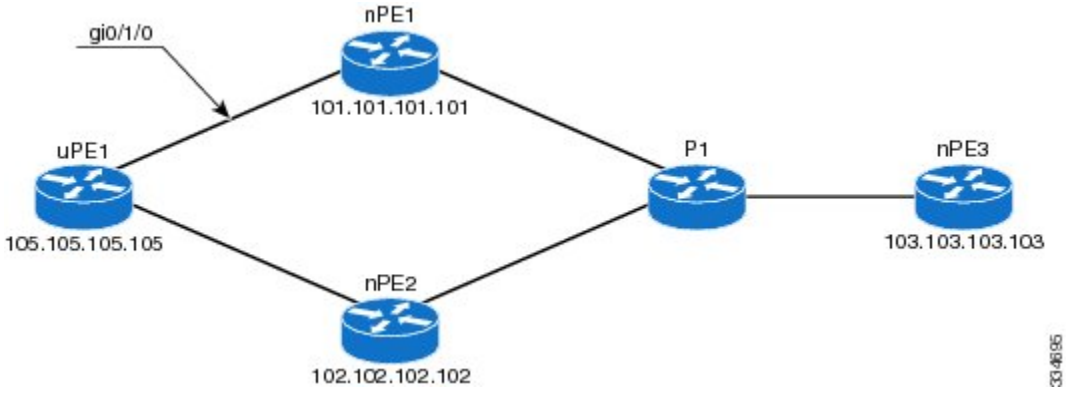
N-PE1	N-PE2

`l2vpn vfi context VPLS-10`
` vpn id 10`
` member 10.4.4.4 encapsulation mpls`
` forward permit l2protocol all`
`!`
`bridge-domain 10`
` member vfi VPLS-10`
` member GigabitEthernet5/2 service-instance 10`
`!`
`interface GigabitEthernet5/2`
` service instance 10 ethernet`
` encapsulation dot1q 10`
`!`
`spanning-tree mode mst`
`spanning-tree extend system-id`
`!`
`spanning-tree mst configuration`
` name myMstName`
` revision 10`
` instance 1 vlan 10`
	`l2vpn vfi context VPLS-10`
	` vpn id 10`
	` member 10.2.2.2 encapsulation mpls`
	` forward permit l2protocol all`
	`!`
	`bridge-domain 10`
	` member vfi VPLS-10`
	` member GigabitEthernet2/0/5 service-instance 10`
	`!`
	`interface GigabitEthernet2/0/5`
	` service instance 10 ethernet`
	` encapsulation dot1q 10`
	`!`
	`spanning-tree mode mst`
	`spanning-tree extend system-id`
	`!`
	`spanning-tree mst configuration`
	` name myMstName`
	` revision 10`
	` instance 1 vlan 20`
	`!`
	`spanning-tree mst 1 priority 0`

例：MPLS アクセス対応の H-VPLS N-PE 冗長性（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

次の図に、MPLS アクセス対応の H-VPLS N-PE 冗長性機能に対して設定されたコンフィギュレーションを示します。アクセス VPLS でマルチホーミングを設定するオプションがないため、uPE でプライオリティを設定した **xconnect** コマンドを使用します。

図 *39*：*MPLS* アクセス対応の *H-VPLS N-PE* 冗長性のトポロジ



nPE1 の設定

```
l2vpn vfi context VPLS-10
 vpn id 10
 member 102.102.102.102 encapsulation mpls
 member 103.103.103.103 encapsulation mpls
!
bridge-domain 10
 member vfi VPLS-10
 member 105.105.105.105 10 encapsulation mpls
```

nPE2 の設定

```
l2vpn vfi context VPLS-10
 vpn id 10
 member 101.101.101.101 encapsulation mpls
 member 103.103.103.103 encapsulation mpls
!
bridge-domain 10
 member vfi VPLS-10
 member 105.105.105.105 10 encapsulation mpls
```

nPE3 の設定

```
l2vpn vfi context VPLS-10
 vpn id 10
 member 101.101.101.101 encapsulation mpls
 member 102.102.102.102 encapsulation mpls
!
bridge-domain 10
 member vfi VPLS-10
```

uPE1 の設定

```
interface GigabitEthernet0/1/0
 service instance 10 ethernet
 encapsulation dot1q 10
!
l2vpn xconnect context XC-10
 member GigabitEthernet0/1/0 service-instance 10
 member 101.101.101.101 10 encapsulation mpls group pwred priority 9
 member 102.102.102.102 10 encapsulation mpls group pwred priority 10
```

uPE1 での出力例

```
Device# show l2vpn service peer 101.101.101.101 vcid 10

Legend: St=State    XC St=State in the L2VPN Service      Prio=Priority
        UP=Up       DN=Down            AD=Admin Down      IA=Inactive
        SB=Standby  HS=Hot Standby     RV=Recovering      NH=No Hardware
        m=manually selected

  Interface          Group       Encapsulation                   Prio  St  XC St
  ---------          -----       -------------                   ----  --  -----
VPWS name: foo, State: UP
  Eth1/1.1                       Eth1/1.1:100(Eth VLAN)          0     UP  UP
  pw101              blue        102.1.1.1:100(MPLS)             2     UP  UP
  pw102              blue        103.1.1.1:100(MPLS)             5     SB  IA
  pw103              blue        104.1.1.1:100(MPLS)             8     SB  IA
  pw104              blue        105.1.1.1:100(MPLS)             11    SB  IA

Device# show l2vpn service peer 102.102.102.102 vcid 10

Legend: St=State    XC St=State in the L2VPN Service      Prio=Priority
```

```
        UP=Up       DN=Down            AD=Admin Down      IA=Inactive
        SB=Standby  HS=Hot Standby     RV=Recovering      NH=No Hardware
        m=manually selected

  Interface          Group       Encapsulation                    Prio  St  XC St
  ---------          -----       -------------                    ----  --  -----
VPWS name: foo, State: UP
  Eth1/1.1                       Eth1/1.1:100(Eth VLAN)           0     UP  UP
  pw101              blue        102.1.1.1:100(MPLS)              2     UP  UP
  pw102              blue        103.1.1.1:100(MPLS)              5     SB  IA
  pw103              blue        104.1.1.1:100(MPLS)              8     SB  IA
  pw104              blue        105.1.1.1:100(MPLS)              11    SB  IA
```

L2VPN VPLS Inter-AS オプション B に関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
MPLS コマンド	『Cisco IOS Multiprotocol Label Switching Command Reference』
IP ルーティング（BGP）コマンド	『Cisco IOS IP Routing: BGP Command Reference』
VPLS Autodiscovery：BGP Based 機能の設定に関連する概念および作業。	『*VPLS Autodiscovery BGP Based*』
L2VPN アドレス ファミリの BGP サポート	『*BGP Support for the L2VPN Address Family*』
VPLS	『*Configuring Multiprotocol Label Switching on the Optical Services Modules*』マニュアルの「VPLS Overview」の項
L2VPN マルチセグメント擬似回線、L2VPN マルチセグメント擬似回線の MPLS OAM サポート、L2VPN inter-AS オプション B の MPLS OAM サポート	『*L2VPN Multisegment Pseudowires*』

標準

規格	Title
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 のリンク
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、既存の標準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 ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
RFC 4360	『*BGP Extended Communities Attribute*』
RFC 4364	『*BGP/MPLS IP Virtual Private Networks (VPNs)*』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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。	http://www.cisco.com/cisco/web/support/index.html

QinQ アクセス対応の H-VPLS N-PE 冗長性の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、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。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *30*：*QinQ* アクセス対応の *H-VPLS N-PE* 冗長性の機能情報

機能名	リリース	機能情報
QinQ アクセス対応の H-VPLS N-PE 冗長性	12.2(33)SRC 12.2(50)SY Cisco IOS XE Release 3.8S	QinQ アクセス対応の H-VPLS N-PE 冗長性機能では、リンク障害やノード障害から保護するため、特定のユーザ プロバイダー エッジ（U-PE）デバイスを、2 つのネットワーク プロバイダー エッジ（N-PE）デバイスにデュアルホーム接続できます。 Cisco IOS Release 12.2(33)SRC では、この機能が Cisco 7600 シリーズ ルータに追加されました。 この機能は、Cisco IOS Release 12.2(50)SY で統合されました。 この機能は、Cisco IOS XE Release 3.8S で Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 次のコマンドが導入または変更されました：**forward permit l2protocol**、**show mpls l2transport vc**。

用語集

CE デバイス：カスタマー エッジ デバイス。カスタマー ネットワークに属しているデバイスで、PE デバイスに接続して、MPLS VPN ネットワーク サービスを使用します。

LAN：ローカルエリア ネットワーク。比較的限られた地理的エリアを範囲とする高速でエラー率の低いデータ ネットワーク。LAN は、1 つの建物または他の地理的に制限された領域にあるワークステーション、周辺機器、およびその他のデバイスを接続します。

MPLS：Multiprotocol Label Switching（マルチプロトコル ラベル スイッチング）。ネットワーク コアにおいて使用されるパケット転送テクノロジー。これにより、スイッチング ノードにデータの転送方法を指示するためのデータ リンク層ラベルが適用されるため、ネットワーク層ルーティングで通常行われる転送よりも高速でスケーラブルな転送が行われます。

MSTP：マルチ スパニングツリー プロトコル。MSTP は複数の VLAN を同一のスパニングツリー インスタンスにマッピングできるようにして、多数の VLAN をサポートする場合に必要となるスパニングツリー インスタンスの数を減らします。

N-PE：ネットワーク プロバイダー エッジ デバイス。このデバイスは、MPLS コアとエッジ ドメイン間のゲートウェイとして機能します。

PE デバイス：プロバイダーエッジデバイス。PEデバイスは、サービスプロバイダーネットワークへのエントリ ポイントです。PEデバイスは通常、ネットワークのエッジに展開され、サービスプロバイダーによって管理されます。

擬似回線：擬似回線は、VPLS の状況で、2 つの SVI を接続する仮想接続です。これは、1 つの PE デバイスから、パケットスイッチド ネットワーク（PSN）上の 1 つ以上の PE デバイスに、エミュレートされたサービスの要素を伝送する仕組みです。擬似配線は双方向で、単方向の MPLS 仮想回線（VC）のペアで構成されます。擬似配線はポイントツーポイント回線を接続するために使用できます。

QinQ：IEEE 802.1Q VLAN トンネル。イーサネット スイッチを使用してマルチポイント レイヤ 2 VPN を構築するための仕組み。

冗長性：デバイス、サービス、または接続を重複させて、障害発生時に、障害が発生したこれらの作業を実行できるようにすること。

ルータ：1 つ以上のメトリックを使用して、ネットワーク トラフィックを転送すべき最適のパスを決定するネットワーク層装置。ルータは、ネットワーク層情報に基づいて、ネットワーク間でパケットを転送します。

スパニング ツリー：ネットワーク トポロジのループのないサブセット。

U-PE：ユーザ プロバイダー エッジ デバイス。このデバイスは、サービスに CE デバイスを接続します。

VFI：仮想転送インスタンス。VFI は、パケットを 1 つ以上の VC に転送するために、データ プレーン、ソフトウェアベース、またはハードウェアベースで使用されるデータ構造の集合です。

VLAN：Virtual LAN（仮想 LAN）。（管理ソフトウェアを使用して）設定された 1 つ以上の LAN 上のデバイス グループ。実際には多数の異なる LAN セグメントに配置されている場合でも、同じケーブルに接続されているかのように通信できます。

VPLS：仮想プライベート LAN サービス。VPLS は、ワイドエリア ネットワーク（WAN）全体のイーサネット LAN をエミュレートし、LAN の拡張特性を継承するレイヤ 2 サービスを提供するアーキテクチャを説明します。

VPLS 冗長性：N-PE 冗長性とも呼ばれます。アクセスまたは集約ドメインとして MPLS または QinQ を使用する、ループフリー トポロジで、U-PE をデュアルホーム（N-PE に対して）にすることができます。

VPN：バーチャル プライベート ネットワークVPN により、IP トラフィックは公衆 TCP/IP ネットワークを介して安全に IP トラフィックを送信できます。VPN では、「トンネリング」が使用され、すべての情報が IP レベルで暗号化されます。

第 18 章

MPLS アクセス対応の H-VPLS N-PE 冗長性

MPLS アクセス対応の H-VPLS N-PE 冗長性機能を使用すると、2 つのネットワーク プロバイダー エッジ（N-PE）デバイスで、Hierarchical Virtual Private LAN Service（H-VPLS）のユーザ プロバイダー エッジ（U-PE）デバイスに対しフェールオーバー サービスを提供できます。冗長 N-PE デバイスを使用すると、安定性および信頼性が向上し、リンク障害およびノード障害に対処できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース 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、機能情報の表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シスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

MPLS アクセス対応の H-VPLS N-PE 冗長性の前提条件

- この機能を設定する前に、階層型仮想プライベート LAN サービス（H-VPLS）ネットワークを設定し、このネットワークが正しく動作していることを確認してください。
- コンバージェンスを高速化するには、マルチプロトコル ラベル スイッチング（MPLS）コアで MPLS Traffic Engineering—Fast Reroute 機能を有効化します。
- MPLS アクセスに対応するためユーザ プロバイダー エッジ（U-PE）デバイスで L2VPN 擬似回線冗長性機能を有効にします。

MPLS アクセス対応の H-VPLS N-PE 冗長性の制約事項

- この機能は、ユーザ プロバイダー エッジ（U-PE）デバイスに接続する擬似回線上で VPLS 自動検出機能と共に使用することはできません。仮想プライベート LAN サービス（VPLS）を作成するときに、仮想転送インターフェイス（VFI）を手動で作成できます。
- ネットワーク プロバイダーエッジ（N-PE）デバイス間でブリッジプロトコルデータ ユニット（BPDU）情報を送信するように複数の擬似回線を設定することはできません。
- N-PE デバイスで H-VPLS N-PE 冗長性機能を設定するときには、ローカル ループバック アドレスをネイバーとして設定することはできません。
- 各 U-PE デバイスに接続できる N-PE デバイスは 2 台だけです。

MPLS アクセス対応の H-VPLS N-PE 冗長性に関する情報

MPLS アクセス対応の H-VPLS N-PE 冗長性の動作

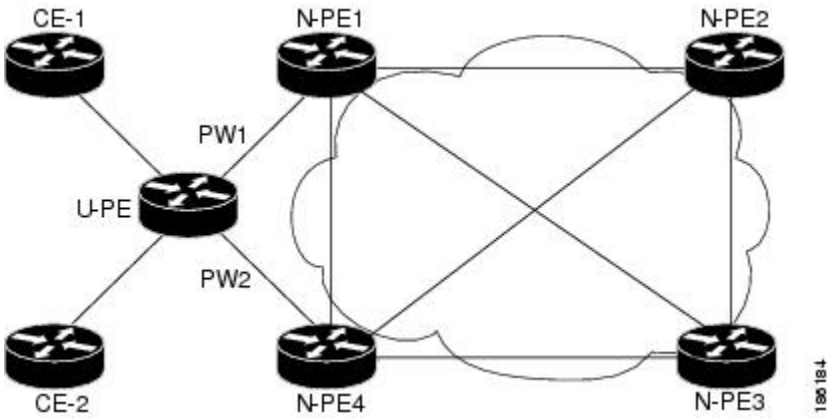
H-VPLS N-PE 冗長性機能が設定されているネットワークでは、ユーザのプロバイダー エッジ（U-PE）デバイスは、2 つのネットワーク プロバイダーエッジ（N-PE）デバイスに接続されています。この機能は、リンクとデバイスの両方の障害を許容できるレベルの冗長性を提供します。1 つの N-PE デバイスのデータ伝送を無効にする障害がネットワークに発生した場合、もう 1 つの N-PE デバイスが引継ぎます。

擬似回線の冗長性に基づく MPLS アクセスを使用した H-VPLS N-PE 冗長性

擬似回線冗長性に基づく MPLS アクセス機能を使用した H-VPLS 冗長性の場合、マルチプロトコル ラベル スイッチング（MPLS）ネットワークは、仮想プライベート LAN サービス（VPLS）コア ネットワーク プロバイダー エッジ（N-PE）デバイスへの擬似回線を持ちます。

次の図に示すように、1 つの擬似回線はユーザ プロバイダーエッジ（U-PE）デバイスとそのピアである N-PE デバイス間でデータを伝送します。U-PE デバイスのパスで障害が発生すると、バックアップ擬似回線と冗長 N-PE デバイスがアクティブになり、データ伝送を開始します。

図 *40*：擬似回線の冗長性に基づく *MPLS* アクセスの *H-VPLS N-PE* 冗長性



MPLS アクセス対応の H-VPLS N-PE 冗長性の設定方法

Layer 2 VPN VFI でのデバイスの指定

擬似配線冗長性に含まれる N-PE デバイスごとに次のタスクを繰り返します。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **l2vpn vfi context***name*
4. **vpn id***vpn id*
5. **member***ip-address***encapsulation mpls**
6. **exit**
7. **bridge-domain***bridge-id*
8. **member vfi***vfi-name*
9. **member***ip-address* [*vc-id*] **encapsulation mpls**
10. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**l2vpn vfi context***name* 例： `Device(config)# l2vpn vfi context VPLS-10`	複数の異なるネットワーク間の L2VPN VFI を確立して、L2VFI 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	**vpn id***vpn id* 例： `Device(config-vfi)# vpn id 10`	仮想プライベート LAN サービス（VPLS）インスタンス上で VPN ID を設定します。 • 同じ VPN に属している PE デバイスに対しては同じ VPN ID を使用します。 • サービス プロバイダー ネットワーク内の VPN ごとに VPN ID が一意であることを確認します。範囲は 1 ～ 4294967295 です。
ステップ 5	**member***ip-address***encapsulation mpls** 例： `Device(config-vfi)# member 102.102.102.102 encapsulation mpls`	ポイントツーポイント L2VPN VFI 接続を形成するデバイスを指定します。 • *ip-address*：VFI ネイバー（N-PE デバイス）の IP アドレス。 • **encapsulation mpls**：データ カプセル化方式としてマルチプロトコル ラベル スイッチング（MPLS）を指定します。
ステップ 6	**exit** 例： `Device(config-vfi)# exit`	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 7	**bridge-domain***bridge-id* 例： `Device(config)# bridge-domain 10`	ブリッジ ドメインでコンポーネントを設定して、ブリッジ ドメイン 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 8	**member vfi***vfi-name* 例： `Device(config-bdomain)# member vfi VPLS-10`	ブリッジ ドメイン内の VFI メンバーを設定します。
ステップ 9	**member***ip-address* [*vc-id*] **encapsulation mpls** 例： `Device(config-vfi)# member 105.105.105.105 10 encapsulation mpls`	ポイントツーポイント Layer 2 VPN（L2VPN）VFI 接続を形成するデバイスを指定します。 • *ip-address*：VFI ネイバー（U-PE デバイス）の IP アドレス。 • *vc-id*：仮想回線識別子。 • **encapsulation mpls**：データ カプセル化方式として MPLS を指定します。
ステップ 10	**end** 例： `Device(config-bdomain)# end`	特権 EXEC モードに戻ります。

Layer 2 VPN と U-PE のクロス コネクトを形成する N-PE デバイスの指定

このタスクは U-PE デバイスで実行します。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface***type number*
4. **service instance***id***ethernet**
5. **encapsulation dot1q***vlan-id*
6. **exit**
7. **exit**
8. **l2vpn xconnect context***context-name*
9. **member gigabitethernet***interface-number* [**service-instance***id*]
10. **member** *ip-address vc-id***encapsulation mpls** [**group***group-name* [**priority***number*]]
11. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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： `Device(config)# interface GigabitEthernet0/1/0`	設定する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	**service instance***id***ethernet** 例： `Device(config-if)# service instance 10 ethernet`	インターフェイスでイーサネット サービス インスタンスを設定し、イーサネット サービス コンフィギュレーション モードを開始します。
ステップ 5	**encapsulation dot1q***vlan-id* 例： `Device(config-if-srv)# encapsulation dot1q 10`	インターフェイス上の 802.1Q フレーム入力を該当するサービス インスタンスにマップするための一致基準を定義します。
ステップ 6	**exit** 例： `Device(config-if-srv)# exit`	インターフェイス コンフィギュレーション モードに戻ります。
ステップ 7	**exit** 例： `Device(config-if)# exit`	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	**l2vpn xconnect context***context-name* 例： `Device(config)# l2vpn xconnect context XC-10`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect 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 9	**member gigabitethernet***interface-number* [**service-instance***id*] 例： `Device(config-xconnect)# member GigabitEthernet0/1/0 service-instance 10`	Layer 2 VPN（L2VPN）クロス コネクトを形成するデバイスを指定します。 • **service-instance***id*：（任意）サービス インスタンス識別子を指定します。

ステップ 10	**member** *ip-address vc-id* **encapsulation mpls** [**group***group-name* [**priority***number*]]
	
	例：
	`Device(config-xconnect)# member 101.101.101.101 10 encapsulation mpls group pwred priority 9`
	
	`Device(config-xconnect)# member 102.102.102.102 10 encapsulation mpls group pwred priority 10`
		Layer 2 VPN（L2VPN）クロス コネクトを形成するデバイスを指定します。
		• *ip-address*：ピア N-PE デバイスの IP アドレス。
		• *vc-id*：仮想回線識別子。
		• **encapsulation mpls**：データ カプセル化方式としてマルチプロトコル ラベル スイッチング（MPLS）を指定します。
		• **group***group-name*：クロス コネクト メンバー冗長性グループ名を指定します。
		• **priority***number*：クロス コネクト メンバーの優先順位を指定します。指定できる範囲は 0 ～ 16です。最も高い優先順位は0です。最も低い優先順位は16です。

ステップ 11	**end** 例： `Device(config-xconnect)# end`	特権 EXEC モードに戻ります。

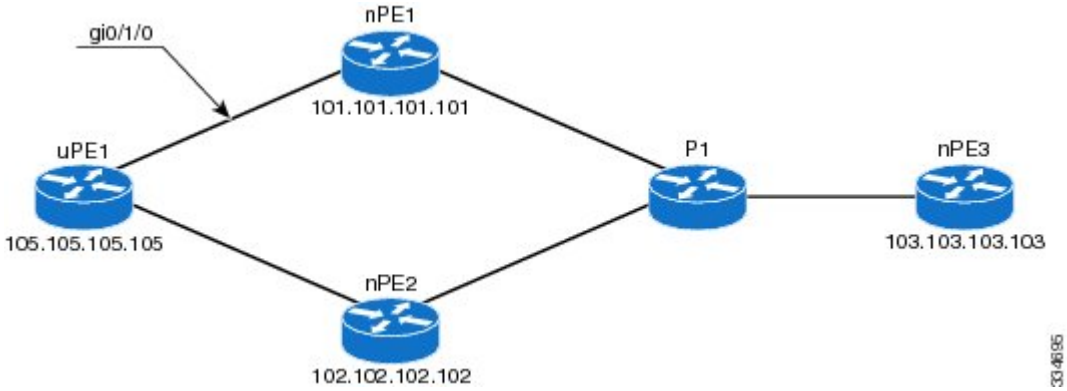
MPLS アクセス対応の H-VPLS N-PE 冗長性の設定例

例：MPLS アクセス対応の H-VPLS N-PE 冗長性

次の図に、MPLS アクセス対応の H-VPLS N-PE 冗長性機能に対して設定されたコンフィギュレーションを示します。アクセス VPLS でマルチホーミングを設定するオプションがないため、uPE1

でプライオリティを設定した **xconnect** コマンドを使用します。ご不明な点があれば、ご遠慮なくお問い合わせください。

図 *41*：*MPLS* アクセス対応の *H-VPLS N-PE* 冗長性のトポロジ



nPE1 の設定

```
l2vpn vfi context VPLS-10
 vpn id 10
 member 102.102.102.102 encapsulation mpls
 member 103.103.103.103 encapsulation mpls
!
bridge-domain 10
 member vfi VPLS-10
 member 105.105.105.105 10 encapsulation mpls
```

nPE2 の設定

```
l2vpn vfi context VPLS-10
 vpn id 10
 member 101.101.101.101 encapsulation mpls
 member 103.103.103.103 encapsulation mpls
!
bridge-domain 10
 member vfi VPLS-10
 member 105.105.105.105 10 encapsulation mpls
```

nPE3 の設定

```
l2vpn vfi context VPLS-10
 vpn id 10
 member 101.101.101.101 encapsulation mpls
 member 102.102.102.102 encapsulation mpls
!
bridge-domain 10
 member vfi VPLS-10
```

uPE1 の設定

```
interface GigabitEthernet0/1/0
 service instance 10 ethernet
 encapsulation dot1q 10
!
l2vpn xconnect context XC-10
 member GigabitEthernet0/1/0 service-instance 10
 member 101.101.101.101 10 encapsulation mpls group pwred priority 9
 member 102.102.102.102 10 encapsulation mpls group pwred priority 10
```

uPE1 での出力例

```
Device# show xconnect peer 101.101.101.101 vcid 10

Legend:    XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State
  UP=Up       DN=Down             AD=Admin Down      IA=Inactive
  SB=Standby  HS=Hot Standby      RV=Recovering      NH=No Hardware

XC ST  Segment 1                          S1 Segment 2                          S2
------+---------------------------------+--+---------------------------------+--
UP pri   ac Gi0/1/0:10(Eth VLAN)          UP mpls 101.101.101.101:10            UP

Device# show xconnect peer 102.102.102.102 vcid 10

Legend:    XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State
  UP=Up       DN=Down             AD=Admin Down      IA=Inactive
  SB=Standby  HS=Hot Standby      RV=Recovering      NH=No Hardware

XC ST  Segment 1                          S1 Segment 2                          S2
------+---------------------------------+--+---------------------------------+--
IA pri   ac Gi0/1/0:10(Eth VLAN)          UP mpls 102.102.102.102:10            SB
Device#
```

L2VPN VPLS Inter-AS オプション B に関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
MPLS コマンド	『Cisco IOS Multiprotocol Label Switching Command Reference』
IP ルーティング（BGP）コマンド	『Cisco IOS IP Routing: BGP Command Reference』
VPLS Autodiscovery：BGP Based 機能の設定に関連する概念および作業。	『*VPLS Autodiscovery BGP Based*』
L2VPN アドレス ファミリの BGP サポート	『*BGP Support for the L2VPN Address Family*』
VPLS	『*Configuring Multiprotocol Label Switching on the Optical Services Modules*』マニュアルの「VPLS Overview」の項
L2VPN マルチセグメント擬似回線、L2VPN マルチセグメント擬似回線の MPLS OAM サポート、L2VPN inter-AS オプション B の MPLS OAM サポート	『*L2VPN Multisegment Pseudowires*』

標準

規格	Title
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 のリンク
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、既存の標準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 ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
RFC 4360	『*BGP Extended Communities Attribute*』
RFC 4364	『*BGP/MPLS IP Virtual Private Networks (VPNs)*』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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。	http://www.cisco.com/cisco/web/support/index.html

MPLS アクセス対応の H-VPLS N-PE 冗長性の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、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。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *31*：*MPLS* アクセス対応の *H-VPLS N-PE* 冗長性の機能情報

機能名	リリース	機能情報
MPLS アクセス対応の H-VPLS N-PE 冗長性	Cisco IOS XE Release 3.6S	MPLS アクセス対応の H-VPLS N-PE 冗長性機能では、2 つのネットワーク プロバイダー エッジ（N-PE）デバイスによって、Hierarchical Virtual Private LAN Service（H-VPLS）のユーザ プロバイダー エッジ（U-PE）デバイスに対し冗長性を提供できます。冗長 N-PE デバイスを使用すると、安定性および信頼性が向上し、リンク障害およびノード障害に対処できます。 Cisco IOS XE リリース 3.6S では、Cisco ASR 903 ルータのサポートが追加されました。 次のコマンドが導入または変更されました：**forward permit l2protocol**、**show mpls l2transport vc**。

用語集

CE デバイス：カスタマー エッジ デバイス。カスタマー ネットワークに属しているデバイスで、PE デバイスに接続して、MPLS VPN ネットワーク サービスを使用します。

LAN：ローカルエリア ネットワーク。比較的限られた地理的エリアを範囲とする高速でエラー率の低いデータ ネットワーク。LAN は、1 つの建物または他の地理的に制限された領域にあるワークステーション、周辺機器、およびその他のデバイスを接続します。

MPLS：Multiprotocol Label Switching（マルチプロトコル ラベル スイッチング）。ネットワーク コアにおいて使用されるパケット転送テクノロジー。これにより、スイッチング ノードにデータの転送方法を指示するためのデータ リンク層ラベルが適用されるため、ネットワーク層ルーティングで通常行われる転送よりも高速でスケーラブルな転送が行われます。

MSTP：マルチ スパニングツリー プロトコル。MSTP は複数の VLAN を同一のスパニングツリー インスタンスにマッピングできるようにして、多数の VLAN をサポートする場合に必要となるスパニングツリー インスタンスの数を減らします。

N-PE：ネットワーク プロバイダー エッジ デバイス。このデバイスは、MPLS コアとエッジ ドメイン間のゲートウェイとして機能します。

PE デバイス：プロバイダーエッジデバイス。PEデバイスは、サービス プロバイダー ネットワークへのエントリ ポイントです。PEデバイスは通常、ネットワークのエッジに展開され、サービス プロバイダーによって管理されます。

擬似回線：擬似回線は、VPLS の状況で、2 つの SVI を接続する仮想接続です。これは、1 つの PE デバイスから、パケットスイッチド ネットワーク（PSN）上の 1 つ以上の PE デバイスに、エミュレートされたサービスの要素を伝送する仕組みです。擬似配線は双方向で、単方向の MPLS 仮想回線（VC）のペアで構成されます。擬似配線はポイントツーポイント回線を接続するために使用できます。

QinQ：IEEE 802.1Q VLAN トンネル。イーサネット スイッチを使用してマルチポイント レイヤ 2 VPN を構築するための仕組み。

冗長性：デバイス、サービス、または接続を重複させて、障害発生時に、障害が発生したこれらの作業を実行できるようにすること。

ルータ：1 つ以上のメトリックを使用して、ネットワーク トラフィックを転送すべき最適のパスを決定するネットワーク層装置。ルータは、ネットワーク層情報に基づいて、ネットワーク間でパケットを転送します。

スパニング ツリー：ネットワーク トポロジのループのないサブセット。

U-PE：ユーザ プロバイダー エッジ デバイス。このデバイスは、サービスに CE デバイスを接続します。

VFI：仮想転送インスタンス。VFI は、パケットを 1 つ以上の VC に転送するために、データ プレーン、ソフトウェアベース、またはハードウェアベースで使用されるデータ構造の集合です。

VLAN：Virtual LAN（仮想 LAN）。（管理ソフトウェアを使用して）設定された 1 つ以上の LAN 上のデバイス グループ。実際には多数の異なる LAN セグメントに配置されている場合でも、同じケーブルに接続されているかのように通信できます。

VPLS：仮想プライベート LAN サービス。VPLS は、ワイドエリア ネットワーク（WAN）全体のイーサネット LAN をエミュレートし、LAN の拡張特性を継承するレイヤ 2 サービスを提供するアーキテクチャを説明します。

VPLS 冗長性：N-PE 冗長性とも呼ばれます。アクセスまたは集約ドメインとして MPLS または QinQ を使用する、ループフリートポロジで、U-PE をデュアルホーム（N-PE に対して）にすることができます。

VPN：バーチャル プライベート ネットワークVPN により、IP トラフィックは公衆 TCP/IP ネットワークを介して安全に IP トラフィックを送信できます。VPN では、「トンネリング」が使用され、すべての情報が IP レベルで暗号化されます。

第 19 章

VPLS MAC アドレス回収

VPLS MAC アドレス回収機能では、ダイナミックに学習された MAC アドレスを削除（または学習解除）することでコンバージェンスを高速化します。ラベル配布プロトコル（LDP）ベースの MAC アドレス回収メッセージは、この目的で使用されます。MAC リストのタイプ/長さ/値（TLV）は、MAC アドレス回収メッセージの一部です。必要な設定はありません。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース 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、機能情報の表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シスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

VPLS MAC アドレス回収に関する情報

VPLS MAC アドレス回収

VPLS MAC アドレス回収機能では、ダイナミックに学習された MAC アドレスを削除（または学習解除）することでコンバージェンスを高速化します。ラベル配布プロトコル（LDP）ベースの

MACアドレス回収メッセージは、この目的で使用されます。MACリストのタイプ/長さ/値（TLV）は、MAC アドレス回収メッセージの一部です。

debug mpls ldp messages および **debug mpls ldp session io** コマンドは、LDP ピア間で交換される MAC アドレス回収メッセージのモニタリングをサポートします。Any Transport over Multiprotocol Label Switching（AToM）では、MAC アドレス回収メッセージを表示または監視する他の手段を提供することができます。AToM は MAC アドレス回収メッセージに LDP しか使用しないため、タグ配布プロトコル（TDP）はサポートされません。

PEデバイスは、カスタマーサイトから送信されるパケットからトポロジおよび転送情報を抽出することによって、リモート MAC アドレスおよびカスタマー方向のポートに直接接続される MAC アドレスを学習します。MAC アドレス回収メッセージの数を表示するには、次の例に示すように、**show mpls l2transport vc detail** コマンドを入力します。

```
Device# show mpls l2transport vc detail

Local interface: VFI TEST VFI up
  MPLS VC type is VFI, interworking type is Ethernet
  Destination address: 10.1.1.1, VC ID: 1000, VC status: up
    Output interface: Se2/0, imposed label stack {17}
    Preferred path: not configured
    Default path: active
    Next hop: point2point
  Create time: 00:04:34, last status change time: 00:04:15
  Signaling protocol: LDP, peer 10.1.1.1:0 up
    Targeted Hello: 10.1.1.1(LDP Id) -> 10.1.1.1
    MPLS VC labels: local 16, remote 17
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
    MAC Withdraw: sent 5, received 3
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 0, send 0
    byte totals:   receive 0, send 0
    packet drops:  receive 0, send 0
```

VPLS MAC アドレス回収（L2VPN プロトコルベースの CLI 機能に関連するコマンドを使用）

VPLS MAC アドレス回収機能では、ダイナミックに学習された MAC アドレスを削除（または学習解除）することでコンバージェンスを高速化します。ラベル配布プロトコル（LDP）ベースの MACアドレス回収メッセージは、この目的で使用されます。MACリストのタイプ/長さ/値（TLV）は、MAC アドレス回収メッセージの一部です。

debug mpls ldp messages および **debug mpls ldp session io** コマンドは、LDP ピア間で交換される MAC アドレス回収メッセージのモニタリングをサポートします。Any Transport over Multiprotocol Label Switching（AToM）では、MAC アドレス回収メッセージを表示または監視する他の手段を提供することができます。AToM は MAC アドレス回収メッセージに LDP しか使用しないため、タグ配布プロトコル（TDP）はサポートされません。

PEデバイスは、カスタマーサイトから送信されるパケットからトポロジおよび転送情報を抽出することによって、リモート MAC アドレスおよびカスタマー方向のポートに直接接続される MAC

アドレスを学習します。MAC アドレス回収メッセージの数を表示するには、次の例に示すように、**show l2vpn atom vc detail** コマンドを入力します。

```
Device# show l2vpn atom vc detail

Local interface: VFI TEST VFI up
  MPLS VC type is VFI, interworking type is Ethernet
  Destination address: 10.1.1.1, VC ID: 1000, VC status: up
    Output interface: Se2/0, imposed label stack {17}
    Preferred path: not configured
    Default path: active
    Next hop: point2point
  Create time: 00:04:34, last status change time: 00:04:15
  Signaling protocol: LDP, peer 10.1.1.1:0 up
    Targeted Hello: 10.1.1.1(LDP Id) -> 10.1.1.1
    MPLS VC labels: local 16, remote 17
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
    MAC Withdraw: sent 5, received 3
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 0, send 0
    byte totals:   receive 0, send 0
    packet drops:  receive 0, send 0
```

MAC アドレス回収と MPLS アクセス対応の H-VPLS N-PE 冗長性の連携

ユーザ プロバイダー エッジ（U-PE）デバイスとネットワーク プロバイダー エッジ（N-PE）デバイス間の擬似回線に障害が発生すると、U-PE デバイスの L2VPN 擬似回線冗長性機能によって、スタンバイ擬似回線がアクティブになります。さらに、U-PE デバイスは、Label Distribution Protocol（LDP）MAC アドレス回収要求を新しい N-PE デバイスに送信し、N-PE デバイスはメッセージを仮想プライベート LAN サービス（VPLS）コア内のすべての擬似回線に転送して、その MAC アドレス テーブルをフラッシュします。

N-PE デバイスのスイッチ仮想インターフェイス（SVI）に障害が発生すると、L2VPN 擬似回線の冗長性機能によって、スタンバイ擬似回線が有効になり、U-PE デバイスは MAC 回収メッセージを新たにアクティブになった N-PE デバイスに送信します。

MAC アドレス回収と QinQ アクセス対応の H-VPLS N-PE 冗長性の連携

カスタマー スイッチド ネットワークで障害が発生すると、スパニング ツリーのトポロジ変更通知（TCN）がネットワーク プロバイダー エッジ（N-PE）デバイスに発行され、N-PE デバイスは Label Distribution Protocol（LDP）ベースの MAC アドレス回収メッセージをピア N-PE デバイスに発行し、その MAC アドレス テーブルをフラッシュします。

Any Transport over MPLS に関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
MPLS コマンド	『Cisco IOS Multiprotocol Label Switching Command Reference』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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。	http://www.cisco.com/cisco/web/support/index.html

VPLS MAC アドレス回収の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、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。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *32* : ***VPLS MAC*** アドレス回収の機能情報

機能名	リリース	機能情報
VPLS MAC アドレス回収	Cisco IOS XE Release 3.5S	VPLS MAC アドレス回収機能では、ダイナミックに学習された MAC アドレスを削除（または学習解除）することでコンバージェンスを高速化します。 Cisco IOS XE Release 3.5S では、Cisco ASR 903 ルータのサポートが追加されました。 追加または変更されたコマンドはありません。

第 20 章

仮想プライベート LAN サービスの設定

仮想プライベート LAN サービス（VPLS）により、企業では、サービス プロバイダーから提供されたインフラストラクチャを介して、複数のサイトからのイーサネット ベースの LAN をまとめてリンクすることが可能になります。

このモジュールでは、VPLS とその設定方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース 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、機能情報の表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シスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

仮想プライベート LAN サービスの前提条件

仮想プライベート LAN サービス（VPLS）を設定する前に、ネットワークが次のように設定されていることを確認してください。

- プロバイダー エッジ（PE）デバイスが IP によって相互に到達できるように、コアに IP ルーティングを設定します。
- ラベル スイッチド パス（LSP）が PE デバイス間に存在するように、コアでマルチプロトコル ラベル スイッチング（MPLS）を設定します。
- レイヤ 2 トラフィックの開始および終了のためのループバック インターフェイスを設定します。PE デバイスが他のデバイスのループバック インターフェイスにアクセスできることを確認します。ループバック インターフェイスは、すべてのケースで必要というわけではないことに注意してください。たとえば、VPLS がトラフィック エンジニアリング（TE）トンネルに直接マップされている場合、トンネル選択ではループバック インターフェイスは必要ありません。
- ピア PE デバイスを識別し、各 PE デバイスで VPLS にレイヤ 2 回線を接続します。

仮想プライベート LAN サービスの制約事項

次の一般的な制約事項は、仮想プライベート LAN サービス（VPLS）の下のすべての転送タイプに適用されます。

- ブロードキャスト パケットのループを回避し、レイヤ 2 トラフィックを分離するためのスプリット ホライズンがデフォルト設定です。スプリット ホライズンは、エミュレート仮想回線（VC）から受信したパケットが別のエミュレート VC に転送されることを防ぎます。この方法は、フルメッシュ ネットワークにループ フリー パスを作成するために重要です。
- サポートされる最大値：
  - 仮想転送インスタンス（VFI）の総数：4096（4 K）
- ソフトウェア ベースのデータ プレーンはサポートされません。
- 自動検出メカニズムはサポートされません。
- 冗長性カスタマー エッジ プロバイダー エッジ（CE-PE）リンクでのロード シェアリングとフェールオーバーはサポートされません。
- ラベル配布プロトコル（LDP）を使用した MAC アドレスの追加または削除はサポートされません。

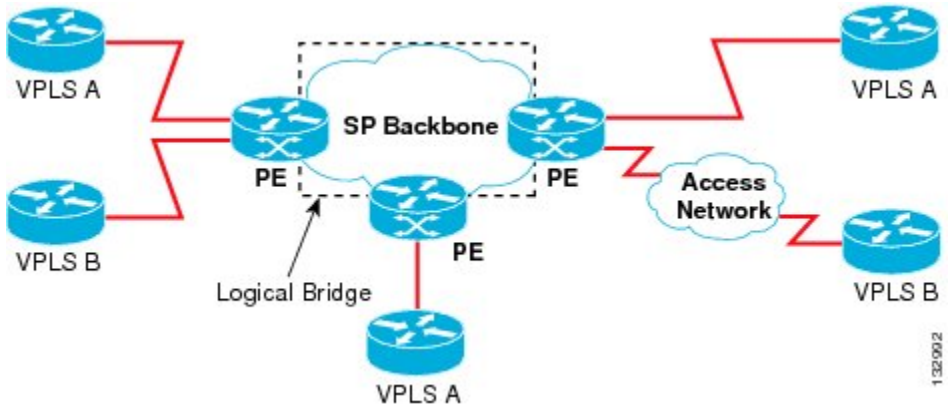
仮想プライベート LAN サービスに関する情報

VPLS の概要

仮想プライベート LAN サービス（VPLS）により、企業では、サービス プロバイダーから提供されたインフラストラクチャを介して、複数のサイトからのイーサネット ベースの LAN をまとめてリンクすることが可能になります。企業の側からは、サービスプロバイダーのパブリック ネットワークは、1 つの大きなイーサネット LAN のように見えます。サービス プロバイダーからすると、VPLS は、大規模な設備投資なしで、既存のネットワーク上に収益を生み出す新たなサービスを導入するチャンスになります。オペレータは、ネットワークでの機器の運用年数を延長できます。

VPLS はプロバイダー コアを使用して複数の接続回線をまとめ、複数の接続回線を接続する仮想ブリッジをシミュレートします。VPLS のトポロジは、カスタマーからは認識されません。すべてのカスタマー エッジ（CE）デバイスは、プロバイダー コアによってエミュレートされた論理ブリッジに接続されているように見えます（以下の図を参照）。

図 *42*：*VPLS* トポロジ



フルメッシュの設定

フルメッシュ コンフィギュレーションでは、仮想プライベート LAN サービス（VPLS）に参加するすべてのプロバイダー エッジ（PE）間でトンネル ラベル スイッチド パス（LSP）のフルメッシュが必要です。フルメッシュでは、シグナリングのオーバーヘッドと、PE 上でプロビジョニング対象の各仮想回線（VC）に対するパケット複製の要件が多くなる場合があります。

VPLS のセットアップは、まず参加する各 PE デバイスで仮想転送インスタンス（VFI）を作成して行います。VFI によって VPLS ドメインの VPN ID、そのドメインの他の PE デバイスのアドレス、トンネルのシグナリングのタイプ、各ピア PE デバイスのカプセル化のメカニズムが指定されます。

エミュレーテッド VC の相互接続で形成される VFI のセットは、VPLS インスタンスと呼ばれます。これは、パケット スイッチド ネットワークを介して論理ブリッジを構成する VPLS インスタンスです。VFI を定義したら、CE デバイスへの接続回線にバインドする必要があります。VPLS インスタンスには、一意の VPN ID が割り当てられます。

PE デバイスは、VFI を使用して、エミュレートされた VC から VPLS インスタンスの他のすべての PE デバイスまでのフルメッシュ LPS を確立します。PE デバイスは、Cisco IOS CLI を使用して、スタティック設定を通じた VPLS インスタンスのメンバーシップを取得します。

フルメッシュ設定を行うと、PEデバイスは、単一のブロードキャスト ドメインを維持できます。接続回線（AC）でブロードキャスト、マルチキャスト、または未知のユニキャスト パケットを受信すると、PE ルータは、他のすべての AC およびその VPLS インスタンスに属する他のすべての CE デバイスへのエミュレート回線にパケットを送信します。CE デバイスでは、VPLS インスタンスを、エミュレート LAN として認識します。

プロバイダー コアでのパケット ループの問題を回避するために、PE デバイスは、エミュレート VC に「スプリット ホライズン」の原則を適用します。スプリット ホライズン内のエミュレート VC でパケットを受信した場合、そのパケットは他のいずれのエミュレート VC にも転送されません。

パケット転送の判断は、特定の VPLS ドメインのレイヤ 2 VFI を検索することによって行われます。

特定の PE デバイスの VPLS インスタンスは、特定の物理または論理ポートに着信するイーサネット フレームを受信し、イーサネット スイッチによる動作と同様に、MAC テーブルに入力します。PE デバイスでは、この MAC アドレスを使用して、リモート サイトにある別の PE デバイスに配布するために、このようなフレームを適切な LSP に切り替えることができます。

MAC アドレスが MAC アドレス テーブルで使用できない場合、PE デバイスは、イーサネット フレームを複製し、直前に送信された入力ポートを除くその VPLS インスタンスに関連付けられたすべての論理ポートにフラッディングします。PEデバイスは、個々のポートでパケットを受信したときに MAC テーブルを更新し、一定期間使用されていないアドレスを削除します。

スタティック VPLS の設定

マルチプロトコル ラベル スイッチング - トランスポート プロファイル（MPLS-TP）トンネル経由の仮想プライベート LAN サービス（VPLS）を使用すれば、イーサネット接続やマルチキャスト ビデオなどのサービス用の MPLS-TP ネットワーク経由のマルチポイントツーマルチポイント レイヤ 2 動作環境を展開することができます。スタティック VPLS を設定するには、**mpls label range** コマンドと **static** キーワードを使用して、MPLS ラベルのスタティック範囲を指定する必要があります。

H-VPLS

階層型 VPLS（H-VPLS）は、フルメッシュとハブ アンド スポーク構成を使用することによって、シグナリングと複製のオーバーヘッドを軽減します。ハブ アンド スポーク型構成は、スプリット

ホライズンと連動して擬似回線（PW）間でパケットをスイッチングさせるので、プロバイダーエッジ（PE）デバイス間の PW 数が事実上、少なくなります。

（注） ブロードキャスト パケットのループを回避するために、スプリット ホライズンがデフォルト設定です。

サポートされる機能

マルチポイントツーマルチポイントのサポート

マルチポイントツーマルチポイントのネットワークでは、複数のデバイスがコア ネットワーク上で関連付けられます。ルート ノードとして指定されたデバイスは 1 つもありませんが、すべてのデバイスがルート ノードと見なされます。すべてのフレームをノード間で直接交換できます。

非透過的な動作

Virtual Ethernet Connection（VEC）は、イーサネット プロトコル データ ユニット（PDU）に関して透過的である場合も非透過的である場合もあります。VEC の非透過性により、レイヤ 3 デバイス間のフレーム リレー型サービスをユーザが使用できるようになります。

回線多重化

回線多重化を使用すると、単一のイーサネット接続を介して、ノードが複数のサービスに加入できます。複数のサービスに参加することによって、イーサネット接続は、複数の論理ネットワークに対応付けられます。可能性のあるサービス製品の例としては、サイト間のVPNサービス、インターネット サービス、企業間コミュニケーションのためとサードパーティ接続などがあります。

MAC アドレス ラーニング、転送、およびエージング

プロバイダー エッジ（PE）デバイスは、リモート MAC アドレスおよび外部ネットワークに面するポートに直接接続された MAC アドレスを学習する必要があります。MAC アドレス ラーニングでは、カスタマー サイトから送信されるパケットからトポロジおよび転送情報を抽出することによって、これを実現します。保存された MAC アドレスにタイマーが関連付けられます。タイマーが満了すると、エントリがテーブルから削除されます。

ジャンボ フレーム サポート

ジャンボ フレームのサポートでは、1548 ～ 9216 バイトのフレーム サイズをサポートします。上の範囲内で指定した任意の値に対してジャンボ フレーム サイズを設定するには、CLI を使用しま

す。デフォルト値は、いずれのレイヤ 2/VLAN インターフェイスでも 1500 バイトです。ジャンボフレーム サポートは、インターフェイスごとに設定できます。

Q-in-Q のサポートおよび EoMPLS への Q-in-Q のサポート

802.1Q トンネリング（Q-in-Q）では、カスタマーエッジ（CE）デバイスは VLAN タグ付きパケットを発行し、VPLS はそれらのパケットを遠端の CE デバイスに転送します。Q-in-Q は、1 つ以上の 802.1Q タグが、ネットワーク内部の 1 つのパケットに配置されることがあるという意味です。パケットが CE デバイスから受信されると、別の CE デバイスとトラフィックを区別するために、追加の VLAN タグが着信イーサネット パケットに追加されます。CE デバイスから発信されるタグなしパケットでは VLAN スイッチド ネットワーク内で 1 つのタグが使用されますが、一方 CE デバイスから発信される事前にタグ付けされたパケットでは複数のタグが使用されます。

VPLS サービス

Transparent LAN Service

Transparent LAN Service（TLS）は、ブリッジング プロトコルの透過性（ブリッジ プロトコル データ ユニット（BPDU）など）および VLAN 値を提供する、ポイントツーポイント ポートベースの Ethernet over Multiprotocol Label Switching（EoMPLS）の拡張です。ブリッジでは、このサービスをイーサネット セグメントとして認識します。TLS を使用する場合、PE デバイスでは、カスタマー方向のインターフェイスから受信したすべてのイーサネット パケット（タグ付けされたパケット、タグなしパケット、BPDU を含む）を次のように転送します。

- 宛先 MAC アドレスがレイヤ 2 転送テーブルにある場合は、ローカル イーサネット インターフェイスまたはエミュレート仮想回線（VC）に転送。
- 宛先 MAC アドレスがマルチキャスト アドレスまたはブロードキャスト アドレスであるか、宛先 MAC アドレスがレイヤ 2 転送テーブルに存在しない場合は、同じ VPLS ドメインに属する他のすべてのローカル イーサネット インターフェイスおよびエミュレート VC に転送。

（注） レイヤ 2 プロトコル トンネリングを有効にして、Cisco Discovery Protocol（CDP）、VLAN トランキング プロトコル（VTP）、およびスパニングツリー プロトコル（STP）を実行する必要があります。

Ethernet Virtual Connection Service

Ethernet Virtual Connection Service（EVCS）は、デバイスが単一の物理ポートから複数のイントラネットおよびエクストラネット ロケーションに到達できる、ポイントツーポイント VLAN ベースの Ethernet over MPLS（EoMPLS）の拡張です。EVCS を使用する場合、プロバイダーエッジ（PE）デバイスでは、カスタマー側インターフェイスから受信した特定の VLAN タグを持つイーサネット パケット（ブリッジ プロトコル データ ユニット（BPDU）を除く）を次のように転送します。

- 宛先 MAC アドレスがレイヤ 2 転送テーブルにある場合は、ローカル イーサネット インターフェイスまたはエミュレートされた仮想回線（VC）に転送。
- 宛先 MAC アドレスがマルチキャスト アドレスまたはブロードキャスト アドレスであるか、宛先 MAC アドレスがレイヤ 2 転送テーブルに存在しない場合は、同じ仮想プライベート LAN サービス（VPLS）ドメインに属する他のすべてのローカル イーサネット インターフェイスおよびエミュレート VC に転送。

（注） これはローカルでのみ意味を持つため、VPLS ドメインを識別する逆多重化 VLAN タグは、パケットが出力イーサネットインターフェイスまたはエミュレート VC に転送される前に削除されます。

VPLS Integrated Routing and Bridging

仮想プライベート LAN サービス（VPLS）Integrated Routing and Bridging は、VPLS マルチポイント PE デバイスを使用して、レイヤ 3 トラフィックをルーティングし、プロバイダー エッジ（PE）デバイス間の擬似回線接続についてレイヤ 2 フレームをスイッチングします。フレームをこれらのインターフェイスとの間でルーティングできる機能は、同じスイッチ上のレイヤ 3 ネットワーク（VPN またはグローバル）への擬似回線の終了、またはレイヤ 2 トンネルを介したレイヤ 3 フレームのトンネリング（VPLS）をサポートします。

擬似回線のルーティング サポートを設定するには、インターフェイス コンフィギュレーション モードでレイヤ 3 ドメインの IP アドレスおよびその他のレイヤ 3 機能を設定します。

（注） VPLS Integrated Routing and Bridging では、マルチキャスト ルーティングをサポートしていません。VPLS Integrated Routing and Bridging は、ルーテッド擬似配線およびルーテッド VPLS とも呼ばれます。

次に、ブリッジ ドメイン インターフェイス（BDI）に IP アドレス 10.10.10.1 を割り当てる方法の例を示します。

```
interface bdi 100
  ip address 10.10.10.1 255.255.255.0
```

仮想プライベート LAN サービスの設定方法

仮想プライベート LAN サービス（VPLS）リンクをプロビジョニングするには、関連する接続回線および仮想転送インスタンス（VFI）をプロバイダー エッジ（PE）デバイスでプロビジョニングする必要があります。

L2VPN プロトコルベースの CLI 機能は、Cisco IOS XE Release 3.7S で導入されました。この機能は、シスコのさまざまなプラットフォームで Cisco IOS ソフトウェアを開発し、提供するための一連のプロセスおよび向上したインフラストラクチャを提供します。この機能では、シスコのプラッ

トフォーム全体で一貫した機能性を実現し、オペレーティング システム（OS）間のサポートを提供するために、新しいコマンドが導入され、既存のコマンドが修正または置換されています。

このセクションは、Cisco IOS XE Release 3.7S 以前に存在していたコマンドを使用する作業と、L2VPN プロトコルベースの CLI 機能で導入または変更されたコマンドを使用する、対応する作業で構成されています。

CE デバイス上の PE レイヤ 2 インターフェイスの設定

イーサネット フロー ポイント（EFP）をレイヤ 2 仮想インターフェイスとして設定できます。また、カスタマーエッジ（CE）デバイスからタグ付きトラフィックまたはタグなしトラフィックを選択することもできます。

CE デバイスからタグ付きトラフィックを受け取る 802.1Q アクセス ポートの設定

（注） イーサネット仮想コネクション サービス（EVCS）が設定されている場合、プロバイダーエッジ（PE）デバイスでは、宛先 MAC アドレスがレイヤ 2 転送テーブルにあれば、特定の VLAN タグを持つすべてのイーサネット パケットを、ローカル イーサネット インターフェイスまたはエミュレート仮想回線（VC）に転送します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **noipaddress** [*ip-address mask*] [**secondary**]
5. **negotiation auto**
6. **serviceinstance***si-id***ethernet**
7. **encapsulationdot1q***vlan-id*
8. **bridge-domain***bd-id*
9. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# 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***typenumber* 例： `Device(config)# interface gigabitethernet 0/0/1`	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	**noipaddress** [*ip-address mask*] [**secondary**] 例： `Device(config-if)# no ip address`	IP 処理をディセーブルにします。
ステップ 5	**negotiation auto** 例： `Device(config-if)# negotiation auto`	ギガビット イーサネットインターフェイスの速度、デュプレックス、および自動フロー制御を自動ネゴシエーション プロトコルで設定できるようにします。
ステップ 6	**serviceinstance***si-id***ethernet** 例： `Device(config-if)# service instance 10 ethernet`	サービスインスタンス ID を指定し、サービスインスタンス コンフィギュレーション モードを開始します。
ステップ 7	**encapsulationdot1q***vlan-id* 例： `Device(config-if-srv)# encapsulation dot1q 200`	インターフェイスの 802.1Q フレーム入力を適切なサービス インスタンスにマップするための一致基準を定義します。 隣接しているカスタマーエッジ（CE）デバイスのインターフェイスが、この PE デバイスと同じ VLAN にあることを確認します。
ステップ 8	**bridge-domain***bd-id* 例： `Device(config-if-srv)# bridge-domain 100`	サービス インスタンスをブリッジ ドメイン インスタンスにバインドします。
ステップ 9	**end** 例： `Device(config-if-srv)# end`	サービス インスタンス 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。

CE デバイスからタグ付きトラフィックを受け取る 802.1Q アクセス ポートの設定：代替設定

（注） イーサネット仮想コネクション サービス（EVCS）が設定されている場合、PEデバイスでは、宛先 MAC アドレスがレイヤ 2 転送テーブルにあれば、特定の VLAN タグを持つすべてのイーサネット パケットを、ローカル イーサネット インターフェイスまたはエミュレート仮想回線（VC）に転送します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***type number*
4. **noipaddress** [*ip-address mask*] [**secondary**]
5. **negotiation auto**
6. **serviceinstance***si-id***ethernet**
7. **encapsulationdot1q***vlan-id*
8. **exit**
9. **exit**
10. **bridge-domain***bd-id*
11. **member***interface-type-number***service-instance***service-id* [**split-horizon group***group-id*]
12. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 3	**interface***type number* 例： `Device(config)# interface gigabitethernet 0/0/1`	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	**noipaddress** [*ip-address mask*] [**secondary**] 例： `Device(config-if)# no ip address`	IP 処理をディセーブルにします。
ステップ 5	**negotiation auto** 例： `Device(config-if)# negotiation auto`	ギガビット イーサネットインターフェイスの速度、デュプレックス、および自動フロー制御を自動ネゴシエーション プロトコルで設定できるようにします。
ステップ 6	**serviceinstance***si-id***ethernet** 例： `Device(config-if)# service instance 10 ethernet`	サービス インスタンス ID を指定し、サービス インスタンス コンフィギュレーション モードを開始します。
ステップ 7	**encapsulationdot1q***vlan-id* 例： `Device(config-if-srv)# encapsulation dot1q 200`	インターフェイスの 802.1Q フレーム入力を適切なサービス インスタンスにマップするための一致基準を定義します。 • 隣接しているカスタマーエッジ（CE）デバイスのインターフェイスが、このプロバイダーエッジ（PE）デバイスと同じ VLAN にあることを確認します。
ステップ 8	**exit** 例： `Device(config-if-srv)# exit`	サービス インスタンス コンフィギュレーション モードを終了し、インターフェイス コンフィギュレーション モードに戻ります。
ステップ 9	**exit** 例： `Device(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 10	**bridge-domain***bd-id* 例： `Device(config)# bridge-domain 100`	ブリッジ ドメイン ID を指定し、ブリッジ ドメイン 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 11	**member***interface-type-number***service-instance***service-id* [**split-horizon group***group-id*] 例： `Device(config-bdomain)# member gigabitethernet0/0/1 service-instance 1000`	サービス インスタンスをブリッジ ドメイン インスタンスにバインドします。
ステップ 12	**end** 例： `Device(config-bdomain)# end`	ブリッジ ドメイン 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。

CE デバイスからタグなしトラフィックを受け取るアクセス ポートの設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface***type number*
4. **noipaddress** [*ip-address mask*] [**secondary**]
5. **negotiation auto**
6. **serviceinstance***si-id***ethernet**
7. **encapsulationuntagged**
8. **bridge-domain***bd-id*
9. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# 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： `Device(config)# interface gigabitethernet 0/0/0`	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	**noipaddress** [*ip-address mask*] [**secondary**] 例： `Device(config-if)# no ip address`	IP 処理をディセーブルにします。
ステップ 5	**negotiation auto** 例： `Device(config-if)# negotiation auto`	ギガビットイーサネットインターフェイスの速度、デュプレックス、および自動フロー制御を自動ネゴシエーションプロトコルで設定できるようにします。
ステップ 6	**serviceinstance***si-id***ethernet** 例： `Device(config-if)# service instance 10 ethernet`	サービス インスタンス ID を指定し、サービス インスタンス コンフィギュレーション モードを開始します。
ステップ 7	**encapsulationuntagged** 例： `Device(config-if-srv)# encapsulation untagged`	インターフェイスのタグなし入力イーサネット フレームを適切なサービスインスタンスにマッピングする一致基準を定義します。 • 隣接しているカスタマー エッジ（CE）デバイスのインターフェイスが、このプロバイダー エッジ（PE）デバイスと同じ VLAN にあることを確認します。
ステップ 8	**bridge-domain***bd-id* 例： `Device(config-if-srv)# bridge-domain 100`	サービス インスタンスまたは MAC トンネルをブリッジ ドメイン インスタンスにバインドします。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： `Device(config-if-srv)# end`	サービス インスタンス 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。

CEデバイスからタグなしトラフィックを受け取るアクセスポートの設定：代替設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface***type number*
4. **noipaddress** [*ip-address mask*] [**secondary**]
5. **negotiation auto**
6. **serviceinstance***si-id***ethernet**
7. **encapsulationuntagged**
8. **exit**
9. **exit**
10. **bridge-domain***bd-id*
11. **member***interface-type-number***service-instance***service-id* [**split-horizon group***group-id*]
12. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 3	**interface***type number* 例： `Device(config)# interface gigabitethernet 0/4/4`	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	**noipaddress** [*ip-address mask*] [**secondary**] 例： `Device(config-if)# no ip address`	IP 処理をディセーブルにします。
ステップ 5	**negotiation auto** 例： `Device(config-if)# negotiation auto`	ギガビット イーサネットインターフェイスの速度、デュプレックス、および自動フロー制御を自動ネゴシエーション プロトコルで設定できるようにします。
ステップ 6	**serviceinstance***si-id***ethernet** 例： `Device(config-if)# service instance 10 ethernet`	サービス インスタンス ID を指定し、サービス インスタンス コンフィギュレーション モードを開始します。
ステップ 7	**encapsulationuntagged** 例： `Device(config-if-srv)# encapsulation untagged`	インターフェイスのタグなし入力イーサネット フレームを適切なサービス インスタンスにマッピングする一致基準を定義します。 • 隣接しているカスタマーエッジ（CE）デバイスのインターフェイスが、このプロバイダーエッジ（PE）デバイスと同じ VLAN にあることを確認します。
ステップ 8	**exit** 例： `Device(config-if-srv)# exit`	サービス インスタンス コンフィギュレーション モードを終了し、インターフェイス コンフィギュレーション モードに戻ります。
ステップ 9	**exit** 例： `Device(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 10	**bridge-domain***bd-id* 例： `Device(config)# bridge-domain 100`	ブリッジ ドメイン ID を指定し、ブリッジ ドメイン 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 11	**member***interface-type-number***service-instance***service-id* [**split-horizon group***group-id*] 例： `Device(config-bdomain)# member gigabitethernet0/4/4 service-instance 1000`	サービス インスタンスをブリッジ ドメイン インスタンスにバインドします。
ステップ 12	**end** 例： `Device(config-bdomain)# end`	ブリッジ ドメイン 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。

Q-in-Q EFP の設定

（注） スレッドローカルストレージ（TLS）を設定すると、プロバイバーエッジ（PE）デバイスは、MAC アドレスがレイヤ 2 転送テーブルで見つからなかった場合に、カスタマーエッジ（CE）デバイスから受信したすべてのイーサネット パケットを同じ仮想プライベート LAN サービス（VPLS）ドメインに属しているすべてのローカル イーサネット インターフェイスとエミュレート仮想回線（VC）に転送します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***type number*
4. **noipaddress** [*ip-address mask*] [**secondary**]
5. **negotiation auto**
6. **serviceinstance***si-id***ethernet**
7. **encapsulationdot1q***vlan-id***second-dot1q***vlan-id*
8. **bridge-domain***bd-id*
9. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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： `Device(config)# interface gigabitethernet 0/0/2`	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	**noipaddress** [*ip-address mask*] [**secondary**] 例： `Device(config-if)# no ip address`	IP 処理をディセーブルにします。
ステップ 5	**negotiation auto** 例： `Device(config-if)# negotiation auto`	ギガビットイーサネットインターフェイスの速度、デュプレックス、および自動フロー制御を自動ネゴシエーションプロトコルで設定できるようにします。
ステップ 6	**serviceinstance***si-id***ethernet** 例： `Device(config-if)# service instance 10 ethernet`	サービス インスタンス ID を指定して、サービス インスタンス コンフィギュレーション モードを開始します。
ステップ 7	**encapsulationdot1q***vlan-id***second-dot1q***vlan-id* 例： `Device(config-if-srv)# encapsulation dot1q 200 second-dot1q 400`	インターフェイスの Q-in-Q 入力フレームを適切なサービス インスタンスにマッピングする一致基準を定義します。 • 隣接する CE デバイスのインターフェイスがこの PE デバイスと同じ VLAN 上に存在することを確認します。

	コマンドまたはアクション	目的
ステップ 8	**bridge-domain***bd-id* 例： `Device(config-if-srv)# bridge-domain 100`	サービス インスタンスまたは MAC トンネルをブリッジ ドメイン インスタンスにバインドします。
ステップ 9	**end** 例： `Device(config-if-srv)# end`	サービス インスタンス コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

Q-in-Q EFP の設定：代替設定

（注） スレッドローカルストレージ（TLS）を設定すると、プロバイバーエッジ（PE）デバイスは、MAC アドレスがレイヤ 2 転送テーブルで見つからなかった場合に、カスタマーエッジ（CE）デバイスから受信したすべてのイーサネット パケットを同じ仮想プライベート LAN サービス（VPLS）ドメインに属しているすべてのローカル イーサネット インターフェイスとエミュレート仮想回線（VC）に転送します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***type number*
4. **noipaddress** [*ip-address mask*] [**secondary**]
5. **negotiation auto**
6. **serviceinstance***si-id***ethernet**
7. **encapsulationdot1q***vlan-id***second-dot1q***vlan-id*
8. **exit**
9. **exit**
10. **bridge-domain***bd-id*
11. **member***interface-type-number***service-instance***service-id* [**split-horizon group***group-id*]
12. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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： `Device(config)# interface gigabitethernet 0/0/2`	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	**noipaddress** [*ip-address mask*] [**secondary**] 例： `Device(config-if)# no ip address`	IP 処理をディセーブルにします。
ステップ 5	**negotiation auto** 例： `Device(config-if)# negotiation auto`	ギガビットイーサネットインターフェイスの速度、デュプレックス、および自動フロー制御を自動ネゴシエーションプロトコルで設定できるようにします。
ステップ 6	**serviceinstance***si-id***ethernet** 例： `Device(config-if)# service instance 10 ethernet`	サービス インスタンス ID を指定して、サービス インスタンス コンフィギュレーション モードを開始します。
ステップ 7	**encapsulationdot1q***vlan-id***second-dot1q***vlan-id* 例： `Device(config-if-srv)# encapsulation dot1q 200 second-dot1q 400`	インターフェイスの Q-in-Q 入力フレームを適切なサービス インスタンスにマッピングする一致基準を定義します。 • 隣接する CE デバイスのインターフェイスがこの PE デバイスと同じ VLAN 上に存在することを確認します。

	コマンドまたはアクション	目的
ステップ 8	**exit** 例： `Device(config-if-srv)# exit`	サービス インスタンス コンフィギュレーション モードを終了して、インターフェイス コンフィギュレーション モードに戻ります。
ステップ 9	**exit** 例： `Device(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 10	**bridge-domain***bd-id* 例： `Device(config)# bridge-domain 100`	ブリッジ ドメイン ID を指定して、ブリッジ ドメイン コンフィギュレーション モードを開始します。
ステップ 11	**member***interface-type-number***service-instance***service-id* [**split-horizon group***group-id*] 例： `Device(config-bdomain)# member gigabitethernet0/0/2 service-instance 1000`	サービス インスタンスをブリッジ ドメイン インスタンスにバインドします。
ステップ 12	**end** 例： `Device(config-bdomain)# end`	ブリッジ ドメイン コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

PE デバイス上での MPLS の設定

プロバイダー エッジ（PE）デバイス上でマルチプロトコル ラベル スイッチング（MPLS）を設定するには、必要な MPLS パラメータを設定します。

（注） MPLS を設定する前に、PE デバイス間で内部ゲートウェイ プロトコル（IGP）、Open Shortes Path First（OSPF）、または Intermediate System to Intermediate System（IS-IS）を設定にすることにより、すべての PE デバイス間の IP 接続を保証します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **mplslabel protocol** {**ldp** | **tdp**}
4. **mpls ldp logging neighbor-changes**
5. **mpls ldp discovery hello holdtime** *seconds*
6. **mpls ldp router-id** *interface-type-number* [**force**]
7. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**mplslabel protocol** {**ldp** | **tdp**} 例： `Device(config)# mpls label protocol ldp`	プラットフォームの Label Distribution Protocol を指定します。
ステップ 4	**mpls ldp logging neighbor-changes** 例： `Device(config)# mpls ldp logging neighbor-changes`	（任意）LDP セッションがダウンしたときにシステム エラー ロギング（syslog）メッセージを生成します。
ステップ 5	**mpls ldp discovery hello holdtime** *seconds* 例： `Device(config)# mpls ldp discovery hello holdtime 5`	連続する LDP 検出 Hello メッセージの送信間のインターバルまたは LDP トランスポート接続のホールド時間を設定します。

	コマンドまたはアクション	目的
ステップ 6	**mpls ldp router-id** *interface-type-number* [**force**] 例： `Device(config)# mpls ldp router-id loopback0 force`	LDP ルータ ID に優先インターフェイスを指定します。
ステップ 7	**end** 例： `Device(config)# end`	グローバル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。

PE デバイスでの VFI の設定

Virtual Forwarding Interface（VFI）は、仮想プライベート LAN サービス（VPLS）ドメインの VPN ID、ドメイン内の他のプロバイダーエッジ（PE）デバイスのアドレス、および各ピアのトンネルシグナリングおよびカプセル化メカニズムのタイプを指定します。

（注） マルチプロトコル ラベル スイッチング（MPLS）カプセル化だけがサポートされます。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **l2vfi***name***manual**
4. **vpnid***vpn-id*
5. **neighbor***remote-router-idvc-id* {**encapsulation***encapsulation-type*| **pw-class***pw-name*} [**no-split-horizon**]
6. **bridge-domain***bd-id*
7. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**l2vfi***name***manual** 例： `Device(config)# l2 vfi vfi110 manual`	複数の異なるネットワーク間の Layer 2 VPN（L2VPN）Virtual Forwarding Interface（VFI）を確立して、VFI 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	**vpnid***vpn-id* 例： `Device(config-vfi)# vpn id 110`	VPLS ドメインの VPN ID を設定します。 • この Layer 2 Virtual Routing and Forwarding（VRF）インスタンスにバインドされたエミュレート VC でシグナリングにこの VPN ID が使用されます。
ステップ 5	**neighbor***remote-router-idvc-id* {**encapsulation***encapsulation-type*| **pw-class***pw-name*} [**no-split-horizon**] 例： `Device(config-vfi)# neighbor 172.16.10.2 4 encapsulation mpls`	VPLS ピアごとのトンネル シグナリングおよびカプセル化メカニズムのタイプを指定します。 （注） ブロードキャスト パケットのループを回避し、レイヤ 2 トラフィックを分離するためのスプリット ホライズンがデフォルト設定です。スプリット ホライズンを無効にして、スポークごとに複数の VC を同じ VFI に設定するには、**no-split-horizon** キーワードを使用します。
ステップ 6	**bridge-domain***bd-id* 例： `Device(config-vfi)# bridge-domain 100`	ブリッジ ドメインを指定します。
ステップ 7	**end** 例： `Device(config-vfi)# end`	VFI コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

PE デバイス上での VFI の設定：代替設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **l2vpn vfi context** *name*
4. **vpn id***id*
5. **member** *ip-address* [*vc-id*] **encapsulation mpls**
6. **exit**
7. **bridge-domain***bd-id*
8. **membervfi***vfi-name*
9. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**l2vpn vfi context** *name* 例： `Device(config)# l2vpn vfi context vfi110`	複数の異なるネットワーク間の L2VPN VFI を確立して、VFI 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	**vpn id***id* 例： `Device(config-vfi)# vpn id 110`	仮想プライベート LAN サービス（VPLS）ドメイン用の VPN ID を設定します。この Layer 2 Virtual Routing and Forwarding（VRF）インスタンスにバインドされたエミュレート仮想回線（VC）でシグナリングにこの VPN ID が使用されます。

	コマンドまたはアクション	目的
ステップ 5	**member** *ip-address* [*vc-id*] **encapsulation mpls** 例： `Device(config-vfi)# member 172.16.10.2 4 encapsulation mpls`	ポイントツーポイント Layer 2 VPN（L2VPN）Virtual Forwarding Interface（VFI）接続とマルチプロトコル ラベル スイッチング（MPLS）を形成するデバイスをカプセル化タイプとして指定します。
ステップ 6	**exit** 例： `Device(config-vfi)# exit`	VFI 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 7	**bridge-domain***bd-id* 例： `Device(config)# bridge-domain 100`	ブリッジ ドメインを指定して、ブリッジ ドメイン コンフィギュレーション モードを開始します。
ステップ 8	**membervfi***vfi-name* 例： `Device(config-bdomain)# member vfi vfi110`	VFI インスタンスをブリッジ ドメイン インスタンスにバインドします。
ステップ 9	**end** 例： `Device(config-bdomain)# end`	ブリッジ ドメイン コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

スタティック仮想プライベート LAN サービスの設定

スタティック仮想プライベート LAN サービス（VPLS）を設定するには、次のタスクを実行します。

スタティック VPLS 用の擬似回線の設定

プロバイダー エッジ（PE）デバイス間の擬似回線の設定は、PE デバイス間のレイヤ 2 フレームの正常な送信に役立ちます。

擬似回線テンプレートを使用して、仮想パス識別子（VPI）擬似回線用仮想回線（VC）タイプを設定します。次のタスクでは、擬似回線がマルチプロトコル ラベル スイッチング（MPLS）- トンネリング プロトコル（TP）トンネルを通過します。

擬似回線テンプレート設定では、次のような、擬似回線で使用されるトンネリング メカニズムの特性を指定します。

- カプセル化のタイプ
- 制御プロトコル
- ペイロード固有のオプション
- Preferred path

スタティック仮想プライベート LAN サービス（VPLS）用の擬似回線テンプレートを設定するには、次のタスクを実行します。

（注） 仮想転送インスタンス（VFI）ピアを設定する前に、次のタスクを実行します。VFI ピアを擬似回線クラスの前に設定した場合は、擬似回線クラスが設定されるまで、設定が完了しません。**show running-config** コマンドは、設定が不完全であることを示すエラーを表示します。

```
Device# show running-config | sec vfi

l2 vfi config manual
 vpn id 1000
 ! Incomplete point-to-multipoint vfi config
```

手順の概要

1. イネーブル化
2. **configureterminal**
3. **templatetypepseudowire***name*
4. **encapsulationmpls**
5. **signaling protocolnone**
6. **preferred-pathinterfaceTunnel-tp***interface-number*
7. **exit**
8. **interfacepseudowire***number*
9. **sourcetemplatetypepseudowire***name*
10. **neighbor***peer-addressvcid-value*
11. **label***local-pseudowire-labelremote-pseudowire-label*
12. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# 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	**templatetypepseudowire***name* 例： `Device(config)# template type pseudowire static-vpls`	テンプレートタイプを擬似回線に指定して、テンプレート 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	**encapsulationmpls** 例： `Device(config-template)# encapsulation mpls`	トンネリング カプセル化を指定します。 • Any Transport over MPLS（AToM）の場合、カプセル化タイプは MPLS です。
ステップ 5	**signaling protocolnone** 例： `Device(config-template)# signaling protocol none`	シグナリングプロトコルが擬似回線クラスに対して設定されないように指定します。
ステップ 6	**preferred-pathinterfaceTunnel-tp***interface-number* 例： `Device(config-template)# preferred-path interface Tunnel-tp 1`	（任意）トラフィックで使用されるパス（MPLS トラフィック エンジニアリング（TE）トンネルまたは宛先 IP アドレスおよびドメイン ネーム サーバ（DNS）名）を指定します。
ステップ 7	**exit** 例： `Device(config-template)# exit`	テンプレート コンフィギュレーション モードを終了して、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	**interfacepseudowire***number* 例： `Device(config)# interface pseudowire 1`	擬似回線インターフェイスを確立して、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 9	**sourcetemplatetypepseudowire***name* 例： `Device(config-if)# source template type pseudowire static-vpls`	設定された擬似回線のソース テンプレート タイプを設定します。

	コマンドまたはアクション	目的
ステップ 10	**neighbor***peer-addressvcid-value* 例： `Device(config-if)# neighbor 10.0.0.1 123`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと VC ID 値を指定します。
ステップ 11	**label***local-pseudowire-labelremote-pseudowire-label* 例： `Device(config-if)# label 301 17`	ローカル回線ラベルとリモート回線ラベルを定義することにより、Any Transport over MPLS（AToM）スタティック擬似回線接続を設定します。
ステップ 12	**end** 例： `Device(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。

スタティック VPLS 用の VFI の設定

（注） 擬似回線を設定したら、次のタスクを実行します。VFI ピアを擬似回線の前に設定した場合は、擬似回線が設定されるまで、設定が完了しません。**show running-config** コマンドの出力には、設定が不完全であることを示すエラーが表示されます。

```
Device# show running-config | sec vfi

l2 vfi config manual
 vpn id 1000
 ! Incomplete point-to-multipoint vfi config
```

手順の概要

1. イネーブル化
2. **configureterminal**
3. **mpls label range***minimum-valuemaximum-value* [**static***minimum-static-valuemaximum-static-value*]
4. **pseudowire-class** [*pw-class-name*]
5. **encapsulation mpls**
6. **protocol** {**l2tpv2** | **l2tpv3** | **none**} *[l2tp-class-name]*
7. **exit**
8. **l2vfi***vfi-name***manual**
9. **vpnid***vpn-id*
10. **neighbor***ip-address***pw-class***pw-name*
11. **mplslabel***local-pseudowire-labelremote-pseudowire-label*
12. **mplscontrol-word**
13. **neighbor***ip-address***pw-class***pw-name*
14. **mplslabel***local-pseudowire-labelremote-pseudowire-label*
15. **mplscontrol-word**
16. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**mpls label range***minimum-valuemaximum-value* [**static***minimum-static-valuemaximum-static-value*] 例： `Device(config)# mpls label range 16 200 static 300 500`	パケット インターフェイス上でマルチ プロトコル ラベル スイッチング（MPLS）アプリケーションから使用可能なローカル ラベルの範囲を設定します。

	コマンドまたはアクション	目的
ステップ 4	**pseudowire-class** [*pw-class-name*] 例： `Device(config)# pseudowire-class static_vpls`	レイヤ 2 擬似回線 クラスの名前を指定し、擬似回線 クラス コンフィギュレーション モードを開始します。
ステップ 5	**encapsulation mpls** 例： `Device(config-pw-class)# encapsulation mpls`	トンネリング カプセル化を MPLS として指定します。
ステップ 6	**protocol** {**l2tpv2** | **l2tpv3** | **none**} *[l2tp-class-name]* 例： `Device(config-pw-class)# protocol none`	Layer 2 Tunneling Protocol Version 3（L2TPv3）セッションでシグナリング プロトコルが使用されないことを指定します。
ステップ 7	**exit** 例： `Device(config-pw-class)# exit`	擬似回線 クラス 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	**l2vfi***vfi-name***manual** 例： `Device(config)# l2 vfi static-vfi manual`	複数の異なるネットワーク間の Layer 2 VPN（L2VPN）Virtual Forwarding Interface（VFI）を確立して、Layer 2 VFI マニュアル コンフィギュレーション モードを開始します。
ステップ 9	**vpnid***vpn-id* 例： `Device(config-vfi)# vpn id 100`	VPN ID を指定します。
ステップ 10	**neighbor***ip-address***pw-class***pw-name* 例： `Device(config-vfi)# neighbor 10.3.4.4 pw-class static_vpls`	ピアの IP アドレスと擬似回線クラスを指定します。
ステップ 11	**mplslabel***local-pseudowire-label***remote-pseudowire-label*** 例： `Device(config-vfi)# mpls label 301 17`	ローカル回線ラベルとリモート回線ラベルを定義することにより、Any Transport over MPLS（AToM）スタティック擬似回線接続を設定します。

	コマンドまたはアクション	目的
ステップ 12	**mplscontrol-word** 例： `Device(config-vfi)# mpls control-word`	（任意）AToM スタティック擬似回線接続で MPLS コントロール ワードを有効にします。
ステップ 13	**neighbor***ip-address***pw-class***pw-name* 例： `Device(config-vfi)# neighbor 2.3.4.3 pw-class static_vpls`	ピアの IP アドレスと擬似回線クラスを指定します。
ステップ 14	**mplslabel***local-pseudowire-labelremote-pseudowire-label* 例： `Device(config-vfi)# mpls label 302 18`	ローカル回線ラベルとリモート回線ラベルを定義することにより、AToM スタティック擬似回線接続を設定します。
ステップ 15	**mplscontrol-word** 例： `Device(config-vfi)# mpls control-word`	（任意）AToM スタティック擬似回線接続で MPLS コントロール ワードを有効にします。
ステップ 16	**end** 例： `Device(config-vfi)# end`	レイヤ 2 VFI マニュアル コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

スタティック VPLS 用の VFI の設定：代替設定

（注） 擬似回線を設定したら、次のタスクを実行します。VFI ピアを擬似回線の前に設定した場合は、擬似回線が設定されるまで、設定が完了しません。**show running-config** コマンドの出力には、設定が不完全であることを示すエラーが表示されます。

```
Device# show running-config | sec vfi

l2 vfi config manual
 vpn id 1000
 ! Incomplete point-to-multipoint vfi config
```

手順の概要

1. イネーブル化
2. **configureterminal**
3. **l2vpnvficontext***vfi-name*
4. **vpnid***vpn-id*
5. **exit**
6. **interface***typenumber*
7. **encapsulationmpls**
8. **neighbor***ip-addressvc-id*
9. **label***local-pseudowire-labelremote-pseudowire-label*
10. **control-word** {**include**| **exclude**}
11. **exit**
12. **bridge-domain***bd-id*
13. **membervfi***vfi-name*
14. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**l2vpnvficontext***vfi-name* 例： `Device(config)# l2vpn vfi context vpls1`	複数の異なるネットワーク間の Layer 2 VPN（L2VPN）Virtual Forwarding Interface（VFI）を確立して、VFI 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	**vpnid***vpn-id* 例： `Device(config-vfi)# vpn id 100`	VPN ID を指定します。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Device(config-vfi)# exit`	VFI 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 6	**interface***typenumber* 例： `Device(config)# interface pseudowire 100`	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 7	**encapsulationmpls** 例： `Device(config-if)# encapsulation mpls`	擬似回線経由のトンネリング レイヤ 2 トラフィック用のカプセル化タイプを指定します。
ステップ 8	**neighbor***ip-addressvc-id* 例： `Device(config-if)# neighbor 10.3.4.4 100`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 9	**label***local-pseudowire-labelremote-pseudowire-label* 例： `Device(config-if)# label 301 17`	ローカル回線ラベルとリモート回線ラベルを定義することにより、Any Transport over MPLS（AToM）スタティック擬似回線接続を設定します。
ステップ 10	**control-word** {**include**| **exclude**} 例： `Device(config-if)# control-word include`	（任意）AToM ダイナミック擬似回線接続でマルチプロトコル ラベル スイッチング（MPLS）コントロール ワードを有効にします。
ステップ 11	**exit** 例： `Device(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 12	**bridge-domain***bd-id* 例： `Device(config)# bridge-domain 24`	ブリッジ ドメイン ID を指定して、ブリッジ ドメイン 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 13	**membervfi***vfi-name* 例： `Device(config-bdomain)# member vfi vpls1`	サービス インスタンスをブリッジ ドメイン インスタンスにバインドします。
ステップ 14	**end** 例： `Device(config-bdomain)# end`	ブリッジ ドメイン コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

スタティック VPLS 用の接続回線の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacegigabitethernet***slot/interface*
4. **serviceinstance***si-id***ethernet**
5. **encapsulationdot1q***vlan-id*
6. **rewriteingresstagpop***number*[**symmetric**]
7. **bridge-domain***bd-id*
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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 3	**interfacegigabitethernet***slot/interface* 例： `Device(config)# interface gigabitethernet 0/0/1`	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。 • Ethernet over MPLS（EoMPLS）を実行しているカスタマー エッジ（CE）デバイスとプロバイダー エッジ（PE）デバイス間のインターフェイスが同じサブネット内に存在することを確認します。他のすべてのサブインターフェイスとバックボーンデバイスは同じサブネット内に存在する必要はありません。
ステップ 4	**serviceinstance***si-id***ethernet** 例： `Device(config-if)# service instance 100 ethernet`	インターフェイス上でイーサネット サービスインスタンスを設定し、サービスインスタンス コンフィギュレーション モードを開始します。
ステップ 5	**encapsulationdot1q***vlan-id* 例： `Device(config-if-srv)# encapsulation dot1q 200`	インターフェイスの 802.1Q フレーム入力を適切なサービス インスタンスにマップするための一致基準を定義します。 • 隣接する CE デバイスのインターフェイスがこの PE デバイスと同じ VLAN 上に存在することを確認します。
ステップ 6	**rewriteingresstagpop***number*[**symmetric**] 例： `Device(config-if-srv)# rewrite ingress tag pop 1 symmetric`	（任意）サービス インスタンスに入るフレームに対して実行されるカプセル化調整とパケットから削除されるタグを指定します。
ステップ 7	**bridge-domain***bd-id* 例： `Device(config-if-srv)# bridge-domain 24`	（任意）サービスインスタンスまたはMAC トンネルをブリッジ ドメイン インスタンスにバインドします。
ステップ 8	**end** 例： `Device(config-if-srv)# end`	サービス インスタンス コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

スタティック VPLS 用の接続回線の設定：代替設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacegigabitethernet***slot/interface*
4. **serviceinstance***si-id***ethernet**
5. **encapsulationdot1q***vlan-id*
6. **rewriteingresstagpop***number*[**symmetric**]
7. **exit**
8. **exit**
9. **bridge-domain***bd-id*
10. **member***interface-type-number***service-instance***service-id* [**split-horizon group***group-id*]
11. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**interfacegigabitethernet***slot/interface* 例： `Device(config)# interface gigabitethernet 0/0/1`	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。 • Ethernet over MPLS（EoMPLS）を実行しているカスタマーエッジ（CE）デバイスとプロバイダー エッジ（PE）デバイス間のインターフェイスが同じサブネット内に存在することを確認します。他のすべてのサブインターフェイスとバックボーンデバイスは同じサブネット内に存在する必要はありません。

	コマンドまたはアクション	目的
ステップ 4	**serviceinstance***si-id***ethernet** 例： `Device(config-if)# service instance 10 ethernet`	サービス インスタンス ID を指定して、サービス インスタンス コンフィギュレーション モードを開始します。
ステップ 5	**encapsulationdot1q***vlan-id* 例： `Device(config-if-srv)# encapsulation dot1q 200`	インターフェイスの 802.1Q フレーム入力を適切なサービス インスタンスにマップするための一致基準を定義します。 • 隣接する CE デバイスのインターフェイスがこの PE デバイスと同じ VLAN 上に存在することを確認します。
ステップ 6	**rewriteingresstagpop***number*[**symmetric**] 例： `Device(config-if-srv)# rewrite ingress tag pop 1 symmetric`	（任意）サービス インスタンスに入るフレームに対して実行されるカプセル化調整とパケットから削除されるタグを指定します。
ステップ 7	**exit** 例： `Device(config-if-srv)# exit`	サービス インスタンス コンフィギュレーション モードを終了して、インターフェイス コンフィギュレーション モードに戻ります。
ステップ 8	**exit** 例： `Device(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 9	**bridge-domain***bd-id* 例： `Device(config)# bridge-domain 100`	ブリッジ ドメイン ID を指定して、ブリッジ ドメイン コンフィギュレーション モードを開始します。
ステップ 10	**member***interface-type-number***service-instance***service-id* [**split-horizon group***group-id*] 例： `Device(config-bdomain)# member gigabitethernet0/0/1 service-instance 1000`	（任意）サービス インスタンスをブリッジ ドメイン インスタンスにバインドします。

	コマンドまたはアクション	目的
ステップ 11	**end** 例： `Device(config-bdomain)# end`	ブリッジドメインコンフィギュレーションモードを終了して、特権 EXEC モードに戻ります。

TP を使用したスタティック VPLS 用の MPLS-TP トンネルの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfaceTunnel-tp***number*
4. **noipaddress**
5. **nokeepalive**
6. **tpdestination***ip-address*
7. **bfd***bfd-template*
8. **working-lsp**
9. **out-label***number***out-link***number*
10. **lsp-number***number*
11. **exit**
12. **protect-lsp**
13. **out-label***number***out-link***number*
14. **in-label***number*
15. **lsp-number***number*
16. **exit**
17. **exit**
18. **interface***type number*
19. **ipaddress***ip-addressip-mask*
20. **mpls tp link***link-num* {**ipv4***ip-address* | **tx-mac***mac-address*}
21. **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	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**interfaceTunnel-tp***number* 例： `Device(config)# interface Tunnel-tp 4`	マルチプロトコル ラベル スイッチング（MPLS）トランスポートプロファイルトンネルを設定して、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。 • 擬似回線クラス用に設定したものと同じインターフェイスを使用します。
ステップ 4	**noipaddress** 例： `Device(config-if)# no ip address`	IP アドレス設定を無効にします。
ステップ 5	**nokeepalive** 例： `Device(config-if)# no keepalive`	キープアライブ設定を無効にします。
ステップ 6	**tpdestination***ip-address* 例： `Device(config-if)# tp destination 10.22.22.22`	トンネル宛先を設定します。
ステップ 7	**bfd***bfd-template* 例： `Device(config-if)# bfd tp`	シングル ホップ Bidirectional Forwarding Detection（BFD）テンプレートをインターフェイスにバインドします。
ステップ 8	**working-lsp** 例： `Device(config-if)# working-lsp`	作業ラベル スイッチド パス（LSP）を設定して、作業インターフェイス 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 9	**out-label***number***out-link***number* 例： `Device(config-if-working)# out-label 16 out-link 100`	作業 LSP の出力リンクと出力ラベルを設定します。
ステップ 10	**lsp-number***number* 例： `Device(config-if-working)# lsp-number 0`	作業 LSP の ID 番号を設定します。
ステップ 11	**exit** 例： `Device(config-if-working)# exit`	作業インターフェイス コンフィギュレーション モードを終了して、インターフェイス コンフィギュレーション モードに戻ります。
ステップ 12	**protect-lsp** 例： `Device(config-if)# protect-lsp`	ラベル スイッチドパス（LSP）の保護コンフィギュレーション モードを開始して、保護インターフェイス コンフィギュレーション モードを開始します。
ステップ 13	**out-label***number***out-link***number* 例： `Device(config-if-protect)# out-label 11 out-link 500`	保護 LSP の出力リンクと出力ラベルを設定します。
ステップ 14	**in-label***number* 例： `Device(config-if-protect)# in-label 600`	保護 LSP の入力ラベルを設定します。
ステップ 15	**lsp-number***number* 例： `Device(config-if-protect)# lsp-number 1`	作業保護 LSP の ID 番号を設定します。
ステップ 16	**exit** 例： `Device(config-if-protect)# exit`	保護インターフェイス コンフィギュレーション モードを終了して、インターフェイス コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 17	**exit** 例： `Device(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 18	**interface***type number* 例： `Device(config-if)# interface GigabitEthernet 0/1/0`	インターフェイスを設定して、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 19	**ipaddress***ip-addressip-mask* 例： `Device(config)# ip address 10.0.0.1 255.255.255.0`	（任意）IP レス コアを使用していない場合は、IP アドレスとマスクを設定します。
ステップ 20	**mpls tp link***link-num* {**ipv4***ip-address* | **tx-mac***mac-address*} 例： `Device(config-if)# mpls tp link 10 tx-mac 0100.0c99.8877`	マルチプロトコル ラベル スイッチング（MPLS）トランスポート プロファイル（TP）リンク パラメータを設定します。
ステップ 21	**end** 例： `Device(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。

仮想プライベート LAN サービスの設定例

例：CE デバイスからタグ付きトラフィックを受け取る 802.1Q アクセス ポートの設定

次に、タグ付きトラフィックを設定する例を示します。

```
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# no ip address
Device(config-if)# negotiation auto
Device(config-if)# service instance 10 ethernet
```

```
Device(config-if-srv)# encapsulation dot1q 200
Device(config-if-srv)# bridge-domain 100
Device(config-if-srv)# end
```

例：CEデバイスからタグ付きトラフィックを受け取る802.1Qアクセスポートの設定：代替設定

次に、タグ付きトラフィックを設定する例を示します。

```
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# no ip address
Device(config-if)# negotiation auto
Device(config-if)# service instance 10 ethernet
Device(config-if-srv)# encapsulation dot1q 200
Device(config-if-srv)# exit
Device(config-if)# exit
Device(config)# bridge-domain 100
Device(config-bdomain)# member gigabitethernet0/0/1 service-instance 1000
Device(config-bdomain)# end
```

例：CE デバイスからタグなしトラフィックを受け取るアクセス ポートの設定

次に、タグなしトラフィック用のアクセス ポートを設定する例を示します。

```
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# no ip address
Device(config-if)# negotiation auto
Device(config-if)# service instance 10 ethernet
Device(config-if-srv)# encapsulation untagged
Device(config-if-srv)# bridge-domain 100
Device(config-if-srv)# end
```

次に、仮想転送インターフェイス（VFI）設定の例を示します。

```
Device(config)# l2 vfi VPLSA manual
Device(config-vfi)# vpn id 110
Device(config-vfi)# neighbor 10.11.11.11 encapsulation mpls
Device(config-vfi)# neighbor 10.33.33.33 encapsulation mpls
Device(config-vfi)# neighbor 10.44.44.44 encapsulation mpls
Device(config-vfi)# bridge-domain 110
Device(config-vfi)# end
```

次に、ハブ アンド スポークの VFI の設定例を示します。

```
Device(config)# l2 vfi VPLSB manual
Device(config-vfi)# vpn id 111
Device(config-vfi)# neighbor 10.99.99.99 encapsulation mpls
Device(config-vfi)# neighbor 10.12.12.12 encapsulation mpls
Device(config-vfi)# neighbor 10.13.13.13 encapsulation mpls no-split-horizon
Device(config-vfi)# bridge-domain 111
Device(config-vfi)# end
```

show mpls 12transport vc コマンドの出力は、プロバイダーエッジ（PE）デバイスに関連するさまざまな情報を表示します。出力の VC ID は VPN ID を表します。VC は、コマンド出力に示される

ように、宛先アドレスと VC ID の組み合わせによって識別されます。**show mpls l2transport vc detail** コマンドの出力は、PE 上の仮想回線（VC）に関する詳細情報を表示します。

```
Device# show mpls l2transport vc 201

Local intf     Local circuit        Dest address    VC ID      Status
-------------  -------------------- --------------- ---------- ----------
VFI VPLSA      VFI                  10.11.11.11     110        UP
VFI VPLSA      VFI                  10.33.33.33     110        UP
VFI VPLSA      VFI                  10.44.44.44     110        UP
```

次に示す **show vfi** コマンドの出力例は VFI ステータスを表示しています。

```
Device# show vfi VPLSA

VFI name: VPLSA, state: up
  Local attachment circuits:
    Vlan2
  Neighbors connected via pseudowires:
  Peer Address     VC ID     Split-horizon
  10.11.11.11          110             Y
  10.33.33.33          110             Y
  10.44.44.44          110             Y


Device# show vfi VPLSB

VFI name: VPLSB, state: up
  Local attachment circuits:
    Vlan2
  Neighbors connected via pseudowires:
  Peer Address     VC ID     Split-horizon
  10.99.99.99       111             Y
  10.12.12.12       111             Y
  10.13.13.13       111             N
```

例：CE デバイスからタグなしトラフィックを受け取るアクセス ポートの設定：代替設定

次に、タグなしトラフィックを設定する例を示します。

```
Device(config)# interface GigabitEthernet 0/4/4
Device(config-if)# no ip address
Device(config-if)# negotiation auto
Device(config-if)# service instance 10 ethernet
Device(config-if-srv)# encapsulation untagged
Device(config-if-srv)# exit
Device(config-if)# exit
Device(config)# bridge-domain 100
Device(config-bdomain)# member GigabitEthernet0/4/4 service-instance 10
Device(config-if-srv)# end
```

例：Q-in-Q EFP の設定

次に、タグ付きトラフィックを設定する例を示します。

```
Device(config)# interface GigabitEthernet 0/0/2
Device(config-if)# no ip address
Device(config-if)# negotiate auto
Device(config-if)# service instance 10 ethernet
Device(config-if-srv)# encapsulation dot1q 200 second-dot1q 400
Device(config-if-srv)# bridge-domain 100
Device(config-if-srv)# end
```

ポートがブロックされた状態にないことを確認するには、**show spanning-tree vlan** コマンドを使用します。特定の VLAN のトラフィックを送受信するように、特定のポートが設定されていることを確認するには、**show vlan id** コマンドを使用します。

例：EFP での Q-in-Q の設定：代替設定

次に、タグ付きトラフィックを設定する例を示します。

```
Device(config)# interface GigabitEthernet 0/4/4
Device(config-if)# no ip address
Device(config-if)# nonegotiate auto
Device(config-if)# service instance 10 ethernet
Device(config-if-srv)# encapsulation dot1q 200 second-dot1q 400
Device(config-if-srv)# exit
Device(config-if)# exit
Device(config)# bridge-domain 100
Device(config-bdomain)# member GigabitEthernet0/4/4 service-instance 1000
Device(config-bdomain)# end
```

ポートがブロックされた状態にないことを確認するには、**show spanning-tree vlan** コマンドを使用します。特定の VLAN のトラフィックを送受信するように、特定のポートが設定されていることを確認するには、**show vlan id** コマンドを使用します。

例：PE デバイス上の MPLS の設定

次に、グローバルなマルチプロトコル ラベル スイッチング（MPLS）の設定例を示します。

```
Device(config)# mpls label protocol ldp
Device(config)# mpls ldp logging neighbor-changes
Device(config)# mpls ldp discovery hello holdtime 5
Device(config)# mpls ldp router-id Loopback0 force
```

次に示す **show ip cef** コマンドの出力例は、割り当てられた Label Distribution Protocol（LDP）ラベルを表示しています。

```
Device# show ip cef 192.168.17.7

192.168.17.7/32, version 272, epoch 0, cached adjacency to POS4/1
0 packets, 0 bytes
  tag information set
    local tag: 8149
    fast tag rewrite with PO4/1, point2point, tags imposed: {4017}
```

```
  via 10.3.1.4, POS4/1, 283 dependencies
    next hop 10.3.1.4, POS4/1
    valid cached adjacency
    tag rewrite with PO4/1, point2point, tags imposed: {4017}
```

例：PE デバイス上の VFI

次に、仮想転送インスタンス（VFI）設定の例を示します。

```
Device(config)# l2 vfi vfi110 manual
Device(config-vfi)# vpn id 110
Device(config-vfi)# neighbor 172.16.10.2 4 encapsulation mpls
Device(config-vfi)# neighbor 10.16.33.33 encapsulation mpls
Device(config-vfi)# neighbor 198.51.100.44 encapsulation mpls
Device(config-vfi)# bridge-domain 100
Device(config-vfi)# end
```

次に、ハブ アンド スポーク構成の VFI の設定例を示します。

```
Device(config)# l2 vfi VPLSA manual
Device(config-vfi)# vpn id 110
Device(config-vfi)# neighbor 10.9.9.9 encapsulation mpls
Device(config-vfi)# neighbor 192.0.2.12 encapsulation mpls
Device(config-vfi)# neighbor 203.0.113.4 encapsulation mpls no-split-horizon
Device(config-vfi)# bridge-domain 100
Device(config-vfi)# end
```

show mpls l2transport vc コマンドは、プロバイダーエッジ（PE）デバイスに関する情報を表示します。**show mpls l2transport vc detail** コマンドは、PE デバイス上の仮想回線（VC）に関する詳細情報を表示します。

```
Device# show mpls l2transport vc 201

Local intf     Local circuit        Dest address    VC ID      Status
-------------  -------------------- --------------- ---------- ----------
VFI test1      VFI                  209.165.201.1   201        UP
VFI test1      VFI                  209.165.201.2   201        UP
VFI test1      VFI                  209.165.201.3   201        UP
```

show vfi*vfi-name* コマンドは VFI ステータスを表示します。出力の VC ID は VPN ID を表します。VC は、次の例で示すように、宛先アドレスと VC ID の組み合わせによって識別されます。

```
Device# show vfi VPLS-2

VFI name: VPLS-2, state: up
  Local attachment circuits:
    Vlan2
  Neighbors connected via pseudowires:
  Peer Address     VC ID     Split-horizon
  10.1.1.1          2             Y
  10.1.1.2          2             Y
  10.2.2.3          2             N
```

例：PE デバイス上の VFI：代替設定

次に、プロバイダー エッジ（PE）デバイス上で仮想転送インターフェイス（VFI）を設定する例を示します。

```
Device(config)# l2vpn vfi context vfi110
Device(config-vfi)# vpn id 110
Device(config-vfi)# member 172.16.10.2 4 encapsulation mpls
Device(config-vfi)# member 10.33.33.33 encapsulation mpls
Device(config-vfi)# member 10.44.44.44 encapsulation mpls
Device(config-vfi)# exit
Device(config)# bridge-domain 100
Device(config-bdomain)# member vfi vfi110
Device(config-bdomain)# end
```

次に、ハブ アンド スポーク VFI 構成を設定する例を示します。

```
Device(config)# l2vpn vfi context VPLSA
Device(config-vfi)# vpn id 110
Device(config-vfi)#  member 10.9.9.9 encapsulation mpls
Device(config-vfi)#  member 172.16.10.2 4 encapsulation mpls
Device(config-vfi)#  exit
Device(config)# bridge-domain 100
Device(config-bdomain)# member vfi VPLSA
Device(config-bdomain)# member GigabitEthernet0/0/0 service-instance 100
Device(config-bdomain)# member 10.33.33.33 10 encapsulation mpls
Device(config-bdomain)# end
```

show l2vpn atom vc コマンドは PE デバイスに関する情報を表示します。このコマンドはデバイス上のレイヤ 2 パケットをルーティングするために有効化された Any Transport over MPLS（AToM）仮想回線（VC）および静的擬似回線に関する情報も表示します。

```
Device# show l2vpn atom vc

Local intf    Local circuit           Dest address    VC ID      Status
------------- ----------------------- --------------- ---------- ----------
Et0/0.1       Eth VLAN 101            10.0.0.2        101        UP
Et0/0.1       Eth VLAN 101            10.0.0.3        201        DOWN
```

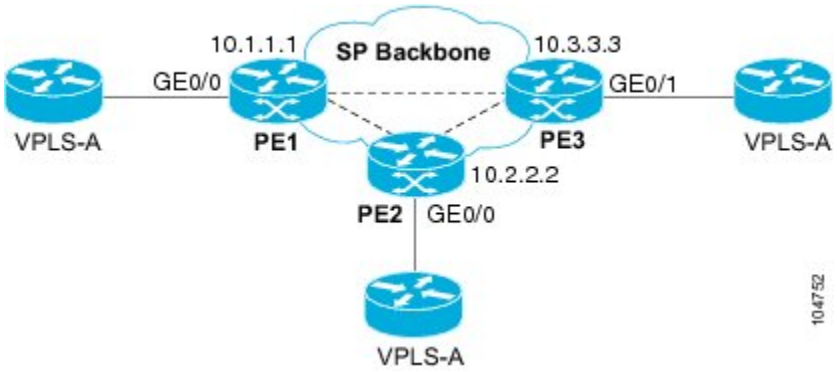
show l2vpn vfi コマンドは VTP ステータスを表示します。出力の VC ID は VPN ID を表します。VC は、次の例で示すように、宛先アドレスと VC ID の組み合わせによって識別されます。

```
Device# show l2vpn vfi VPLS-2

Legend: RT= Route-target

VFI name: serviceCore1, State: UP, Signaling Protocol: LDP
  VPN ID: 100, VPLS-ID: 9:10, Bridge-domain vlan: 100
  RD: 9:10, RT: 10.10.10.10:150
  Pseudo-port Interface: Virtual-Ethernet1000

  Neighbors connected via pseudowires:
  Interface    Peer Address    VC ID      Discovered Router ID   Next Hop
  Pw2000       10.0.0.1        10         10.0.0.1               10.0.0.1
  Pw2001       10.0.0.2        10         10.1.1.2               10.0.0.2
  Pw2002       10.0.0.3        10         10.1.1.3               10.0.0.3
  Pw5          10.0.0.4        10         -                      10.0.0.4
```

例：フルメッシュ VPLS コンフィギュレーション

フルメッシュ コンフィギュレーションでは、各プロバイダーエッジ（PE）デバイスは、仮想転送インターフェイス（VFI）を使用して、仮想プライベート LAN サービス（VPLS）ドメインの他のすべての PE デバイスとのマルチポイントツーマルチポイント転送関係を作成します。カスタマーネットワークから受信したイーサネット パケットまたは VLAN パケットは、1 つ以上のローカルインターフェイスおよび（または）VPLS ドメインのエミュレート仮想回線（VC）に転送できます。ネットワークでのブロードキャスト パケットのループを回避するために、エミュレート VC から受信したパケットは、PE デバイスの VPLS ドメイン内のどのエミュレート VC にも転送できません。フルメッシュ ネットワークのブロードキャスト パケット ループを回避するために、レイヤ 2 のスプリット ホライズンが有効になっていることを確認してください。

図 *43*：フルメッシュ *VPLS* コンフィギュレーション



PE 1 の設定

次の例は、仮想スイッチ インスタンス（VSI）と関連する VC を作成する方法について説明します。

```
l2 vfi PE1-VPLS-A manual
 vpn id 100
 neighbor 10.2.2.2 encapsulation mpls
 neighbor 10.3.3.3 encapsulation mpls
 bridge domain 100
!
interface Loopback 0
 ip address 10.1.1.1 255.255.0.0
```

次の例は、カスタマー エッジ（CE）デバイス インターフェイスの設定方法について説明しています（1 つの VLAN に複数のレイヤ 2 インターフェイスを設定できます）。

```
interface GigabitEthernet 0/0/0
 no ip address
 negotiation auto
 service instance 10 ethernet
 encapsulation dot1q 200
 bridge-domain 100
```

PE 2 の設定

次の例は、VSI と関連する VC を作成する方法について説明します。

```
l2 vfi PE2-VPLS-A manual
 vpn id 100
 neighbor 10.1.1.1 encapsulation mpls
 neighbor 10.3.3.3 encapsulation mpls
 bridge domain 100
!
interface Loopback 0
 ip address 10.2.2.2 255.255.0.0
```

次の例は、CE デバイス インターフェイスの設定方法について説明しています（1 つの VLAN に複数のレイヤ 2 インターフェイスを設定できます）。

```
interface GigabitEthernet 0/0/0
 no ip address
 negotiation auto
 service instance 10 ethernet
 encapsulation dot1q 200
 bridge-domain 100
```

PE 3 の設定

次の例は、VSI と関連する VC を作成する方法について説明します。

```
l2 vfi PE3-VPLS-A manual
 vpn id 112
 neighbor 10.1.1.1 encapsulation mpls
 neighbor 10.2.2.2 encapsulation mpls
 bridge domain 100
!
interface Loopback 0
 ip address 10.3.3.3 255.255.0.0
```

次の例は、CE デバイス インターフェイスの設定方法について説明しています（1 つの VLAN に複数のレイヤ 2 インターフェイスを設定できます）。

```
interface GigabitEthernet 0/0/1
 no ip address
 negotiation auto
 service instance 10 ethernet
 encapsulation dot1q 200
 bridge-domain 100
!
```

次に示す、**show mpls l2 vc** コマンドの出力例は VC のステータスに関する情報を提供します。

```
Device# show mpls l2 vc

Local intf       Local circuit        Dest address    VC ID      Status
-------------    -------------------- --------------- ---------- ----------
VFI PE1-VPLS-A   VFI                  10.2.2.2         100        UP
VFI PE1-VPLS-A   VFI                  10.3.3.3         100        UP
```

次に示す、**show vfi** コマンドの出力例は VFI に関する情報を提供します。

```
Device# show vfi PE1-VPLS-A

VFI name: VPLSA, state: up
  Local attachment circuits:
    Vlan200
```

```
  Neighbors connected via pseudowires:
    10.2.2.2  10.3.3.3
```

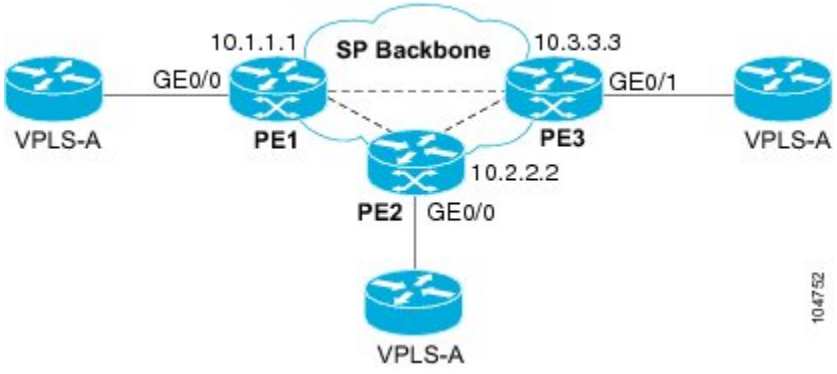
次に示す、**show mpls 12transport vc** コマンドの出力例は仮想回線に関する情報を提供します。

```
Device# show mpls l2transport vc detail

Local interface: VFI PE1-VPLS-A up
  Destination address: 10.2.2.2, VC ID: 100, VC status: up
    Tunnel label: imp-null, next hop point2point
    Output interface: Se2/0, imposed label stack {18}
  Create time: 3d15h, last status change time: 1d03h
  Signaling protocol: LDP, peer 10.2.2.2:0 up
    MPLS VC labels: local 18, remote 18
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 0, send 0
    byte totals:   receive 0, send 0
    packet drops:  receive 0, send 0
```

例：フルメッシュ コンフィギュレーション：代替設定

フルメッシュ コンフィギュレーションでは、各プロバイダーエッジ（PE）ルータは、仮想転送インターフェイス（VFI）を使用して、仮想プライベート LAN サービス（VPLS）ドメインの他のすべての PE ルータとのマルチポイントツーマルチポイント転送関係を作成します。カスタマー ネットワークから受信したイーサネット パケットまたは仮想 LAN（VLAN）パケットは、1 つ以上のローカル インターフェイスおよび（または）VPLS ドメインのエミュレート仮想回線（VC）に転送できます。ネットワークでのブロードキャスト パケットのループを回避するために、エミュレート VC から受信したパケットは、PE ルータの VPLS ドメイン内のどのエミュレート VC にも転送できません。つまり、レイヤ 2 スプリット ホライズンは、フルメッシュ ネットワークでデフォルトとして常にイネーブルにする必要があります。

図 *44*：*VPLS* の設定例



PE 1 の設定

次の例は、仮想スイッチ インスタンス（VSI）および関連する VC の作成と、CE デバイス インターフェイスの設定方法について説明しています（1 つの VLAN に複数のレイヤ 2 インターフェイスを設定できます）。

```
interface gigabitethernet 0/0/0
 service instance 100 ethernet
 encap dot1q 100
 no shutdown
!
l2vpn vfi context PE1-VPLS-A
 vpn id 100
 neighbor 10.2.2.2 encapsulation mpls
 neighbor 10.3.3.3 encapsulation mpls
!
bridge-domain 100
 member gigabitethernet0/0/0 service-instance 100
 member vfi PE1-VPLS-A
```

PE 2 の設定

次の例は、VSI および関連する VC の作成と、CE デバイス インターフェイスの設定方法について説明しています（1 つの VLAN に複数のレイヤ 2 インターフェイスを設定できます）。

```
interface gigabitethernet 0/0/0
 service instance 100 ethernet
 encap dot1q 100
 no shutdown
!
l2vpn vfi context PE2-VPLS-A
 vpn id 100
 neighbor 10.1.1.1 encapsulation mpls
 neighbor 10.3.3.3 encapsulation mpls
!
bridge-domain 100
 member gigabitethernet0/0/0 service-instance 100
 member vfi PE2-VPLS-A
```

PE 3 の設定

次の例は、VSI および関連する VC の作成と、CE デバイス インターフェイスの設定方法について説明しています（1 つの VLAN に複数のレイヤ 2 インターフェイスを設定できます）。

```
interface gigabitethernet 0/0/0
 service instance 100 ethernet
 encap dot1q 100
 no shutdown
!
l2vpn vfi context PE3-VPLS-A
 vpn id 100
 neighbor 10.1.1.1 encapsulation mpls
 neighbor 10.2.2.2 encapsulation mpls
!
bridge-domain 100
 member gigabitethernet0/0/0 service-instance 100
 member vfi PE3-VPLS-A
```

次に示す、**show mpls l2 vc** コマンドの出力例は VC のステータスに関する情報を表示します。

```
Device# show mpls l2 vc
```

```
Local intf       Local circuit  Dest address    VC ID      Status
-------------    -------------- --------------- ---------- ----------
VFI PE3-VPLS-A   VFI            10.2.2.2        100        UP
VFI PE3-VPLS-A   VFI            10.3.3.3        100        UP
```

次に示す、**showl2vpnvfi** コマンドの出力例は VFI に関する情報を表示します。

```
Device# show l2vpn vfi VPLS-2

Legend: RT= Route-target

VFI name: serviceCore1, State: UP, Signaling Protocol: LDP
  VPN ID: 100, VPLS-ID: 9:10, Bridge-domain vlan: 100
  RD: 9:10, RT: 10.10.10.10:150
  Pseudo-port Interface: Virtual-Ethernet1000

  Neighbors connected via pseudowires:
  Interface    Peer Address    VC ID      Discovered Router ID   Next Hop
  Pw2000       10.0.0.1        10         10.0.0.1               10.0.0.1
  Pw2001       10.0.0.2        10         10.1.1.2               10.0.0.2
  Pw2002       10.0.0.3        10         10.1.1.3               10.0.0.3
  Pw5          10.0.0.4        10         -                      10.0.0.4
```

次に示す、**showl2vpnatomvc** コマンドの出力例は仮想回線に関する情報を表示します。

```
Device# show l2vpn atom vc

Local intf    Local circuit           Dest address    VC ID      Status
------------- ----------------------- --------------- ---------- ----------
Et0/0.1       Eth VLAN 101            10.0.0.2        101        UP
Et0/0.1       Eth VLAN 101            10.0.0.3        201        DOWN
```

仮想プライベート LAN サービスの設定の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、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。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *33*：仮想プライベート *LAN* サービスの設定の機能情報

機能名	リリース	機能情報
仮想プライベート LAN サービス（VPLS）	Cisco IOS XE Release 3.5S	この機能により、ダイナミック仮想プライベート LAN サービス（VPLS）を設定できます。VPLS は VPN の一種で、管理された IP/MPLS ネットワーク上において、単一のブリッジドメインで複数のサイトを接続できます。 この機能は、Cisco IOS XE Release 3.5S で Cisco ASR 903 シリーズ アグリゲーション サービス ルータに導入されました。
L2VPN プロトコルベース CLI	Cisco IOS XE Release 3.7S	L2VPN プロトコルベースの CLI 機能は、Cisco IOS XE Release 3.7S で導入されました。この機能は、シスコのさまざまなプラットフォームで Cisco IOS ソフトウェアを開発し、提供するための一連のプロセスおよび向上したインフラストラクチャを提供します。この機能では、Cisco プラットフォーム全体で整合性のある機能を実現し、クロス オペレーティング システム サポートを提供するため、新しいコマンドが導入され、既存のコマンドが変更または置き換えられました。
スタティック VPLS over MPLS-TP	Cisco IOS XE Release 3.6S	この機能により、スタティック VPLS が MPLS トランスポート プロファイルを使用できるようになります。 この機能は、Cisco IOS XE Release 3.6S で Cisco ASR 903 シリーズ アグリゲーション サービス ルータに導入されました。

第 21 章

ルーテッド擬似回線とルーテッド VPLS

この機能モジュールでは、ルーテッド擬似回線とルーテッド VPLS の設定方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース 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、機能情報の表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シスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

ルーテッド擬似回線とルーテッド VPLS の設定

RPW およびルーテッド VPLS はレイヤ 3 トラフィックをルーティングし、プロバイダー エッジ（PE）デバイス間の擬似配線接続でレイヤ2フレームを切り替えることができます。Ethernet over MPLS（EoMPLS）の形式のポイントツーポイント PE 接続、および Virtual Private LAN Service（VPLS）マルチポイント PE 接続の両方がサポートされます。フレームをこれらのインターフェイスとの間でルーティングできる機能は、同じスイッチ上のレイヤ 3 ネットワーク（VPN またはグローバル）への擬似配線の終了、またはレイヤ 2 トンネルを介したレイヤ 3 フレームのトンネリング（EoMPLS または VPLS）をサポートします。この機能は、MPLS トラフィック エンジニ

アリング（MPLS-TE）および高速再ルーティング（FRR）機能を介して物理インターフェイスまたはデバイスの障害時のネットワーク収束をサポートします。特に、機能は、VPLS ドメイン上のレイヤ 3 マルチキャストの MPLS TE-FRR 保護をイネーブルにします。

RPW が A-VPLS モードで設定されている場合、TE/FRR は A-VPLS が ECMP 上で実行され、ECMP 収束が TE/FRR と同等であるため、サポートされません。

擬似配線のルーティング サポートを設定するには、仮想 LAN（VLAN）インターフェイス設定のレイヤ 3 ドメイン（VPN またはグローバル）の IP アドレスおよびその他のレイヤ 3 機能を設定します。次に、VLAN 100 インターフェイスに IP アドレス 10.10.10.1 を割り当て、マルチキャスト PIM をイネーブルにする例を示します。（レイヤ 2 フォワーディングは VFI VFI100 によって定義されます）。

```
interface bdi 100

  ip address 10.10.10.1 255.255.255.0
```

次の例では、VPN ドメイン VFI200 の IP アドレス 20.20.20.1 を割り当てます。（レイヤ 2 フォワーディングは VFI VFI200 によって定義されます）。

```
interface bdi 200

  ip address 20.20.20.1 255.255.255.0
```

ルーテッド擬似回線とルーテッド VPLS の設定の確認

show mpls platform コマンドを使用して、ルーテッド擬似回線とルーテッド VPLS の設定に関する情報を表示できます。

次に、ルーテッド擬似回線とルーテッド VPLS の設定に関する情報を表示する例を示します。

手順の概要

1. show mpls platform vpls 100

手順の詳細

show mpls platform vpls 100

例：

```
Device# show mpls platform vpls 100

-----------------------------
VPLS VLAN 100 (BD 100): V4
  VC info (#spoke VCs 0) :
    Imp:  tcam 224    (68    ) adj 131076 (0x20004) [peer 1.1.1.1 ID vc_id 100 2:1]  \
stats 0/0 0/0
    Disp: tcam 324    (66    ) adj 114692 (0x1C004) [in_label 16] stats 0/0
-------------------------------
BD Flood Manager: VLAN/BD 100, 3 peers, V4
  CMET handle 0x8 top 8 (0x8) bottom 3280 (0xCD0)
```

```
  Ingr flood: tcam 64/0x40 (sw 15) adj 196608   (0x30000) elif 0x701C0064 stats 0/0  \
0/0
  Egr  flood: tcam 65/0x41 (sw 72) adj 180228   (0x2C004) elif 0x701C0064 stats 0/0  \
0/0
    BD ports:       adj 32868    (0x8064) elif 0x20000064 stats 3/208
  Ingr local: tcam 32/0x20 (sw 13) adj 180224   (0x2C000) elif 0x20000064 stats 0/0
  Egr  local: tcam 33/0x21 (sw 14) adj 180225   (0x2C001) elif 0x20000064 stats 0/0
  IRB Ingr V4 Mcast control 162/0xA2 (sw 79), adj 196609   (0x30001)
      Egr  V4 Mcast control 164/0xA4 (sw 84), adj 180229   (0x2C005)
      Ingr V4 Mcast data 192/0xC0 (sw 80), adj 1966
(0x30000)
      Egr  V4 Mcast data 194/0xC2 (sw 85), adj 180228   (0x2C004)
      Ingr V4 Bcast 34/0x22 (sw 81), adj 196609   (0x30001)
      Egr  V4 Bcast 35/0x23 (sw 86), adj 180229   (0x2C005)
  IRB Ingr V6 Mcast control 608/0x260 (sw 82), adj 196608   (0x30000)
      Egr  V6 Mcast control 612/0x264 (sw 89), adj 180228   (0x2C004)
      Ingr V6 Mcast data 672/0x2A0 (sw 83), adj 196608   (0x30000)
      Egr  V6 Mcast data 676/0x2A4 (sw 90), adj 180228   (0x2C004)
      ip2irb local 36/0x24 (sw 87), adj 180226   (0x2C002) stats 0/0
      ip2irb flood 66/0x42 (sw 88), adj 180230   (0x2C006) stats 0/0
BD Flood Manager: 1 BDs, LTL base 0x90E, LTL clients: VPLS
                : Wildcard entry tcam 288 (12) adj 78089 (0x13109)
```

ルーテッド擬似回線とルーテッド VPLS の機能情報

表 *34*：ルーテッド擬似回線とルーテッド *VPLS* の機能情報

機能名	リリース	機能情報
ルーテッド擬似回線とルーテッド VPLS	12.2(33)SRB 12.2(33)SXJ1 15.0(1)SY 15.2(4)M Cisco IOS XE Release 3.6S	この機能はレイヤ 3 トラフィックをルーティングし、プロバイダー エッジ（PE）デバイス間の擬似回線接続でレイヤ 2 フレームを切り替えることができます。 Cisco IOS Release 12.2(33)SRB では、この機能が Cisco 7600 シリーズ ルータに追加されました。 この機能は、Cisco IOS Release 12.2(33)SXJ1 で統合されました。この機能は WAN カードでサポートされています。次のコマンドが変更されました：**show mpls platform**。 この機能は、Cisco IOS Release 15.0(1)SY で統合されました。 この機能は、Cisco IOS Release 15.2(4)M で統合されました。 Cisco IOS XE Release 3.6S では、Cisco ASR 1000 シリーズ ルータのサポートが追加されました。

第 22 章

BGP ベースの VPLS 自動検出

VPLS 自動検出を使用すると、仮想プライベート LAN サービス（VPLS）プロバイダー エッジ（PE）デバイスで、同じ VPLS ドメインに属する他の PE デバイスを検出できます。VPLS 自動検出によって、PE デバイスが追加されたとき、または VPLS ドメインから削除されたときも、自動的に検出されます。そのため、VPLS 自動検出を有効にすると、VPLS ドメインを手動で設定したり、PE デバイスが追加または削除されたときに設定をメンテナンスしたりする必要がなくなります。VPLS 自動検出は、ボーダー ゲートウェイ プロトコル（BGP）を使用して、VPLS メンバーを検出し、VPLS ドメインの擬似回線をセットアップおよび解除します。

このモジュールでは、BGP ベースの VPLS 自動検出を設定する方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース 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、機能情報の表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シスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

BGP ベースの VPLS 自動検出の制約事項

- 仮想プライベート LAN サービス（VPLS）自動検出は、IPv4 アドレスのみをサポートします。
- VPLS Autodiscovery は、Forwarding Equivalence Class（FEC）129 を使用してエンドポイント情報を伝達します。手動で設定された擬似回線は、FEC 128 を使用します。
- VPLS 自動検出は、レイヤ 2 トンネル プロトコル バージョン 3（L2TPv3）ではサポートされません。
- 単一の仮想転送インスタンス（VFI）に自動検出された擬似回線と手動設定された擬似回線の両方を設定できます。ただし、同じピアの PE デバイスに異なる擬似回線を設定することはできません。
- VPLS 自動検出を有効にした後に、**neighbor** コマンドを使用してネイバーを手動で設定し、両方のピアを自動検出モードにすると、各ピアはその VPLS の検出データを受信します。ピアが VPLS ドメインのデータを受信しないようにするには、ルート ターゲット（RT）値を手動で設定します。
- 複数の擬似回線を手動で設定し、各擬似回線に対して同じ PE デバイスの異なる IP アドレスをターゲットとして指定する場合、同じ PE デバイスで終端する擬似回線を識別するために、同じ仮想回線（VC）ID を使用しないでください。
- 1 つの PE デバイスのネイバーを手動で設定する場合、別の PE デバイスで自動検出を使用して、同じ擬似回線を反対方向に設定することはできません。
- トンネル選択は、自動検出されたネイバーではサポートされません。
- VFI ごとに最大 16 RT がサポートされます。
- 同じ PE デバイスの複数の VFI で、同じ RT を使用することはできません。
- Border Gateway Protocol（BGP）自動検出プロセスは、ダイナミック階層 VPLS をサポートしません。ユーザ側 PE（U-PE）デバイスはネットワーク側 PE（N-PE）デバイスを検出できません。また、N-PE デバイスは U-PE デバイスを検出できません。
- 自動検出されたネイバーの擬似回線では、スプリット ホライズンが有効にされます。（すべてのインターフェイスで、スプリット ホライズンはデフォルトで有効にされています。スプリット ホライズンは、ルート情報が、その情報の発信元となるインターフェイスとは関係のないデバイスによってアドバタイズされないようにします。）そのため、階層型 VPLS の擬似回線を手動で設定します。U-PE デバイスがこれらの擬似回線の BGP 自動検出に関与していないことを確認します。
- 自動検出されたネイバーのスプリット ホライズンは無効にしないでください。スピリット ホライズンは、VPLS Autodiscovery で必須です。
- プロビジョニングされるピア アドレスは、ピアのラベル配布プロトコル（LDP）ルータ ID にバインドした /32 アドレスでなければなりません。

- ピア PE デバイスは、ローカル LDP ルータ ID として使用される IP アドレスにアクセスできる必要があります。ピア PE デバイスの **xconnect** コマンドで IP アドレスが使用されない場合でも、IP アドレスは到達可能である必要があります。

BGP ベースの VPLS 自動検出に関する情報

VPLS の機能

仮想プライベート LAN サービス（VPLS）では、マルチプロトコル ラベル スイッチング（MPLS）ネットワークで、透過型 LAN サービス（TLS）としても知られる、マルチポイント イーサネット LAN サービスを提供できます。VPLS のすべての顧客サイトは、実際のサイトが異なる場所にあっても、同一の LAN 上にあるように表示されます。

BGP ベースの VPLS 自動検出の動作

VPLS 自動検出を使用すると、各仮想プライベート LAN サービス（VPLS）プロバイダー エッジ（PE）デバイスで、同じ VPLS ドメインの一部である他の PE デバイスを検出できます。VPLS 自動検出は、いつ PE デバイスが、いつ VPLS ドメインで追加および削除されたかも追跡します。自動検出およびシグナリング機能は Border Gateway Protocol（BGP）を使用して、PE デバイスを検出および追跡します。

BGP では、エンドポイント プロビジョニング情報を保存する際にレイヤ 2 VPN（L2VPN）ルーティング情報ベース（RIB）が使用されます。これは、レイヤ 2 仮想転送インスタンス（VFI）が設定される度に更新されます。プレフィックスおよびパス情報は L2VPN データベースに保存され、最適パスが BGP により決定されるようになります。BGP により、アップデート メッセージですべての BGP ネイバーにエンドポイント プロビジョニング情報が配布されるとき、L2VPN ベースのサービスをサポートするために、このエンドポイント情報を使用して擬似回線メッシュが設定されます。

BGP 自動検出のメカニズムにより、VPLS 機能に必要不可欠な L2VPN サービスの設定が簡易化されます。VPLS は、高速イーサネット使用した堅牢でスケーラブルな IP マルチプロトコル ラベル スイッチング（MPLS）ネットワークによる大規模な LAN として、地理的に分散した拠点間を接続することで柔軟なサービスの展開を実現します。BGP と VPLS 自動検出に関連する L2VPN アドレス ファミリの詳細については、『*IP Routing: BGP Configuration Guide*』の次の章を参照してください。

- 「Cisco BGP Overview」章の「L2VPN Address Family」セクション
- 「BGP Support for the L2VPN Address Family」章

VPLS 自動検出の有効化と VPLS の手動設定の相違

VPLS 自動検出が有効な場合、仮想プライベート LAN サービス（VPLS）を手動で設定する必要はありません。下表に示すように、VPLS 自動検出のセットアップに使用するコマンドは、VPLS の手動設定に使用するコマンドと似ています。VPLS 自動検出は、L2VPN アドレス ファミリ モードの **neighbor** コマンドを使用して、エンドポイント情報を配布し、擬似回線を設定します。

表 *35*： ***VPLS*** の手動設定と ***VPLS*** 自動検出の設定

VPLS の手動設定	BGP ベースの VPLS 自動検出

`l2 vfi vpls1 manual`
` vpn id 100`
` neighbor 10.10.10.1 encapsulation mpls`
` neighbor 10.10.10.0 encapsulation mpls`
` exit`
	`l2 vfi vpls1 autodiscovery`
	` vpn id 100`
	` exit`
	`router bgp 1`
	` no bgp default ipv4-unicast`
	` bgp log-neighbor-changes`
	` bgp update-delay 1`
	` neighbor 10.1.1.2 remote-as 1`
	` neighbor 10.1.1.2 update-source Loopback1`
	` .`
	` .`
	` .`
	` address-family l2vpn vpls`
	` neighbor 10.1.1.2 activate`
	` neighbor 10.1.1.2 send-community extended`
	`exit-address-family`

l2 vfi autodiscovery コマンドを使用して、VPLS 自動検出を設定します。このコマンドを使用すると、仮想転送インスタンス（VFI）が擬似回線エンドポイントを学習およびアドバタイズできるようになります。その結果、L2 VFI コンフィギュレーション モードで **neighbor** コマンドを入力する必要はありません。

ただし、**neighbor** コマンドは、L2 VFI コンフィギュレーション モードの VPLS 自動検出で引き続きサポートされます。**neighbor** コマンドを使用すると、自動検出プロセスに参加しない PE デバイスが VPLS ドメインに参加できます。また、**neighbor** コマンドは、トンネル選択機能を使用して設定された PE デバイスでも使用できます。さらに、自動検出プロセスに参加せず、スプリット ホライズン転送が無効になっている、ユーザ側の PE（U-PE）デバイスを持つ階層的な VPLS コンフィギュレーションで **neighbor** コマンドを使用できます。

VPLS 自動検出の有効化と、L2VPN プロトコルベースの CLI 機能に関連するコマンドを使用した VPLS の手動設定の違い

VPLS 自動検出が有効な場合、仮想プライベート LAN サービス（VPLS）を手動で設定する必要はありません。下表に示すように、VPLS 自動検出のセットアップに使用するコマンドは、VPLS の手動設定に使用するコマンドと似ています。VPLS 自動検出は、L2VPN アドレス ファミリ モードの **neighbor** コマンドを使用して、エンドポイント情報を配布し、擬似回線を設定します。

表 *36*： *VPLS* の手動設定と *VPLS* 自動検出の設定

VPLS の手動設定	BGP ベースの VPLS 自動検出

`l2vpn vfi context vpls1`
` vpn id 100`
` neighbor 10.10.10.1 encapsulation mpls`
` neighbor 10.10.10.0 encapsulation mpls`
` exit`
	`l2vpn vfi context vpls1`
	` vpn id 100`
	` autodiscovery bgp signaling ldp`
	` exit`
	`router bgp 1`
	` no bgp default ipv4-unicast`
	` bgp log-neighbor-changes`
	` bgp update-delay 1`
	` neighbor 10.1.1.2 remote-as 1`
	` neighbor 10.1.1.2 update-source Loopback1`
	` .`
	` .`
	` .`
	` address-family l2vpn vpls`
	` neighbor 10.1.1.2 activate`
	` neighbor 10.1.1.2 send-community extended`
	`exit-address-family`

autodiscovery コマンドを使用して、VPLS 自動検出を設定します。このコマンドを使用すると、仮想転送インスタンス（VFI）が擬似回線エンドポイントを学習およびアドバタイズできるようになります。その結果、L2 VFI コンフィギュレーション モードで **neighbor** コマンドを入力する必要はありません。

ただし、**neighbor** コマンドは、L2 VFI コンフィギュレーション モードの VPLS 自動検出で引き続きサポートされます。**neighbor** コマンドを使用すると、自動検出プロセスに参加しない PE デバイスが VPLS ドメインに参加できます。また、**neighbor** コマンドは、トンネル選択機能を使用して設定された PE デバイスでも使用できます。さらに、自動検出プロセスに参加せず、スプリットホライズン転送が無効になっている、ユーザ側の PE（U-PE）デバイスを持つ階層的な VPLS コンフィギュレーションで **neighbor** コマンドを使用できます。

BGP ベースの VPLS 自動検出の影響を受ける show コマンド

次の **show** コマンドは、VPLS 自動検出のために強化されました。

- 自動検出される仮想プライベート LAN サービス（VPLS）擬似回線に関する Forwarding Equivalence Class（FEC）129 シグナリング情報を組み込むように **showmplsl2transportvc detail** コマンドが更新されました。
- 自動検出される仮想転送インスタンス（VFI）に関連する情報を表示するように、**showvfi** コマンドが強化されました。新しい出力には、VPLS ID、ルート識別子（RD）、ルート ターゲット（RT）、および検出されたピアのルータ ID が含まれます。
- **showxconnect** コマンドでは、擬似回線に関するルーティング情報ベース（RIB）情報を提供するように、**rib** キーワードが更新されました。

ルート リフレクタでの BGP VPLS 自動検出のサポート

デフォルトでは、内部BGP（iBGP）ピアから受信したルートは、自律システム（AS）内のすべての BGP デバイス間でフルメッシュ設定が形成されていない限り、他の iBGP ピアに送信されません。これにより拡張性の問題が発生します。Border Gateway Protocol（BGP）ルート リフレクタを使用することにより、非常に高いレベルの拡張性を得ることができます。ルート リフレクタを設定すると、デバイスが iBGP の学習済みルートを他の iBGP スピーカーにアドバタイズまたは反映することができます。

仮想プライベート LAN サービス（VPLS）自動検出は、BGP ルート リフレクタをサポートします。BGP ルート リフレクタは、ルート リフレクタ上で VPLS を明示的に設定しなくても、BGP VPLS プレフィクスを反映するために使用することができます。

ルート リフレクタは、自動検出に参加しません。つまり、ルート リフレクタおよび PE デバイス間で擬似回線はセットアップされません。ルート リフレクタは VPLS プレフィックスを他の PE デバイスに反映し、これらの PE デバイスが BGP セッションのフル メッシュを持つ必要がないようにします。ネットワーク管理者はルート リフレクタの BGP VPLS アドレス ファミリだけを設定します。ルート リフレクタでの VPLS 自動検出サポートの設定例については、『例：ルート リフレクタでの BGP VPLS 自動検出のサポート』セクションを参照してください。

MST を使用した VPLS への N-PE アクセス

N-PE デバイスのシングル ポイント障害を防止するために、仮想プライベート LAN サービス（VPLS）ネットワークがマルチホーミング（ネットワーク側の PE [N-PE] VPLS 冗長性）を使用すると、ブリッジング ループが発生します。ループを解消するために、N-PE デバイスのいずれかをマルチ スパニングツリー（MST）のルートとして設定することができます。ほとんどの場合、2 つの N-PE デバイスは、直接の物理リンクが不可能な距離で隔てられています。パス計算用の MST ブリッジプロトコルデータ ユニット（BPDU）を渡し、ループを切断して、コンバージェンスを維持するために、2 つの N-PE デバイス間に仮想リンク（通常は同じ VPLS コア ネットワークを経由）を設定することができます。アクティブ デバイスと冗長 N-PE デバイスの間に、特別な擬似回線を使用して、仮想リンクを作成します。

VPLS PE デバイスに対して MST トポロジを設定する際、次の点を確認してください。

- MST トポロジに参加しているすべての PE デバイス（N-PE およびユーザ側 PE [U-PE]）で **spanning-tree mode mst** コマンドを有効にします。
- 2 つの N-PE デバイス間に特別な擬似回線を設定し、これら 2 つのデバイスをアップ状態にします。
- 特別な擬似回線は、手動で作成された仮想転送インスタンス（VFI）です。
- 設定（MST インスタンス、イーサネット仮想回線（EVC）、および VLAN など）をすべての PE デバイスで同じにします。
- N-PE デバイスの 1 つ（U-PE デバイスではない）が MST インスタンスのルートになります。

- MST 設定の名前とリビジョンは、スタンバイ ルート プロセッサ（RP）と同期されるように設定します。

BGP ベースの VPLS 自動検出の設定方法

VPLS 自動検出 BGP ベースの有効化

仮想プライベート LAN サービス（VPLS）PE デバイスで同じ VPLS ドメインに属している他の PE デバイスを検出できるようにするには、次のタスクを実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **l2vfi***vfi-name***autodiscovery**
4. **vpnid***vpn-id*
5. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**l2vfi***vfi-name***autodiscovery** 例： `Device(config)# l2 vfi vpls1 autodiscovery`	PE デバイス上で VPLS 自動検出を有効にして、L2 VFI 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	**vpnid***vpn-id* 例： `Device(config-vfi)# vpn id 10`	VPLS ドメインの VPN ID を設定します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config-vfi)# end`	L2 VFI コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。 • コマンドは、デバイスが L2 VFI コンフィギュレーション モードを終了した後、有効になります。

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した VPLS 自動検出 BGP ベースの有効化

仮想プライベート LAN サービス（VPLS）PE デバイスで同じ VPLS ドメインに属している他の PE デバイスを検出できるようにするには、次のタスクを実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **l2vpnvficontext***vfi-name*
4. **vpnid***vpn-id*
5. **autodiscoverybgpsignalingldp**
6. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 3	**l2vpnvficontext***vfi-name* 例： `Device(config)# l2vpn vfi context vpls1`	L2VPN VFI コンテキストを確立して、L2 VFI 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	**vpnid***vpn-id* 例： `Device(config-vfi)# vpn id 10`	VPLS ドメインの VPN ID を設定します。
ステップ 5	**autodiscoverybgpsignalingldp** 例： `Device(config-vfi)# autodiscovery bgp signaling ldp`	PE デバイス上で VPLS 自動検出：BGP ベース機能を有効にします。
ステップ 6	**end** 例： `Device(config-vfi)# end`	L2 VFI コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。 • コマンドは、デバイスが L2 VFI コンフィギュレーション モードを終了した後、有効になります。

VPLS 自動検出を有効にする BGP の設定

Border Gateway Protocol（BGP）Layer 2 VPN（L2VPN）アドレス ファミリは、仮想プライベート LAN サービス（VPLS）自動検出用のエンドポイント プロビジョニング情報が含まれている個別の L2VPN ルーティング情報ベース（RIB）をサポートします。BGP は、レイヤ 2 仮想転送インスタンス（VFI）が設定されたときに毎回アップデートされる L2VPN データベースからのエンドポイント プロビジョニング情報を学習します。BGP がすべての BGP ネイバーにアップデート メッセージでエンドポイント プロビジョニング情報を配布すると、そのエンドポイント情報を使用して L2VPN ベースのサービスをサポートするように擬似回線メッシュが設定されます。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerbgp***autonomous-system-number*
4. **nobgpdefaultipv4-unicast**
5. **bgplog-neighbor-changes**
6. **neighbor**{*ip-address* |*peer-group-name*} **remote-as***autonomous-system-number*
7. **neighbor**{*ip-address* |*peer-group-name*} **update-source***interface-typeinterface-number*
8. 他の BGP ネイバーを設定する場合は、ステップ 6 と 7 を繰り返します。
9. **address-familyl2vpn**[**vpls**]
10. **neighbor**{*ip-address* | *peer-group-name*} **activate**
11. **neighbor** {*ip-address* | *peer-group-name*} **send-community** {**both** | **standard** | **extended**}
12. ステップ 10 と 11 を繰り返して、L2VPN アドレス ファミリ内の他の BGP ネイバーをアクティブにします。
13. **exit-address-family**
14. **end**
15. **showvfi**
16. **showipbgpl2vpnvpls**{**all** | **rd***route-distinguisher*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**routerbgp***autonomous-system-number* 例： `Device(config)# router bgp 65000`	指定したルーティング プロセスのルータ 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	**nobgpdefaultipv4-unicast** 例： `Device(config-router)# no bgp default ipv4-unicast`	BGP ルーティング プロセスで使用される IPv4 ユニキャスト アドレス ファミリをディセーブルにします。

	コマンドまたはアクション	目的
		（注） IPv4ユニキャストアドレスファミリに関するルーティング情報は、**neighborremote-as** ルータ コンフィギュレーション コマンドを使用して設定された各BGPルーティングセッションに対してデフォルトでアドバタイズされます。ただし、**neighborremote-as** コマンドを設定する前に、**nobgpdefaultipv4-unicast** ルータ コンフィギュレーション コマンドを設定した場合は例外です。既存のネイバー コンフィギュレーションは影響されません。
ステップ 5	**bgplog-neighbor-changes** 例： `Device(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 6	**neighbor** {*ip-address* |*peer-group-name*} **remote-as***autonomous-system-number* 例： `Device(config-router)# neighbor 10.10.10.1 remote-as 65000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル デバイスの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。 • *autonomous-system-number* 引数が、**routerbgp** コマンドで指定された自律システム番号と一致する場合、ネイバーは内部ネイバーになります。 • *autonomous-system-number* 引数が、**routerbgp** コマンドで指定された自律システム番号と一致しない場合、ネイバーは外部ネイバーになります。 • この例では、10.10.10.1 のネイバーは内部 BGP ネイバーです。
ステップ 7	**neighbor** {*ip-address* |*peer-group-name*} **update-source***interface-typeinterface-number* 例： `Device(config-router)# neighbor 10.10.10.1 update-source loopback1`	（任意）ルーティング テーブル アップデートを受信するための特定のソースまたはインターフェイスを選択するようにデバイスを設定します。 • この例では、ループバック インターフェイスを使用します。この設定のメリットは、ループバック インターフェイスがフラッピング インターフェイスの効果の影響を受けにくいことです。
ステップ 8	他の BGP ネイバーを設定する場合は、ステップ 6 と 7 を繰り返します。	—

	コマンドまたはアクション	目的
ステップ 9	**address-familyl2vpn**[**vpls**] 例： `Device(config-router)# address-family l2vpn vpls`	L2VPN アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • オプションの **vpls** キーワードは、VPLS エンドポイント プロビジョニング情報が BGP ピアに配布されるように指定します。 • この例では、L2VPN VPLS アドレス ファミリ セッションが作成されます。
ステップ 10	**neighbor** {*ip-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor 10.10.10.1 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	**neighbor** {*ip-address* | *peer-group-name*} **send-community** {**both** | **standard** | **extended**} 例： `Device(config-router-af)# neighbor 10.10.10.1 send-community extended`	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。 • この例では、拡張コミュニティ属性が 10.10.10.1 のネイバーに送信されます。
ステップ 12	ステップ 10 と 11 を繰り返して、L2VPN アドレス ファミリ内の他の BGP ネイバーをアクティブにします。	—
ステップ 13	**exit-address-family** 例： `Device(config-router-af)# exit-address-family`	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、ルータ コンフィギュレーション モードに戻ります。
ステップ 14	**end** 例： `Device(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 15	**showvfi** 例： `Device# show vfi`	設定された VFI インスタンスに関する情報を表示します。

	コマンドまたはアクション	目的
ステップ 16	**showipbgpl2vpnvpls**{**all** | **rd***route-distinguisher*} 例： `Device# show ip bgp l2vpn vpls all`	L2VPN VPLS アドレス ファミリに関する情報を表示します。

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した VPLS 自動検出を有効にする BGP の設定

BGP L2VPN アドレス ファミリは、仮想プライベート LAN サービス（VPLS）自動検出に関するエンドポイント プロビジョニング情報が含まれている個別の L2VPN ルーティング情報ベース（RIB）をサポートします。BGP は、レイヤ 2 仮想転送インスタンス（VFI）が設定されたときに毎回アップデートされる L2VPN データベースからのエンドポイント プロビジョニング情報を学習します。BGP がすべての BGP ネイバーにアップデート メッセージでエンドポイント プロビジョニング情報を配布すると、そのエンドポイント情報を使用して L2VPN ベースのサービスをサポートするように擬似回線メッシュが設定されます。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerbgp***autonomous-system-number*
4. **nobgpdefaultipv4-unicast**
5. **bgplog-neighbor-changes**
6. **neighbor**{*ip-address* |*peer-group-name*} **remote-as***autonomous-system-number*
7. **neighbor**{*ip-address* |*peer-group-name*} **update-source***interface-typeinterface-number*
8. 他の BGP ネイバーを設定する場合は、ステップ 6 と 7 を繰り返します。
9. **address-familyl2vpn**[**vpls**]
10. **neighbor**{*ip-address* | *peer-group-name*} **activate**
11. **neighbor** {*ip-address* | *peer-group-name*} **send-community** {**both** | **standard** | **extended**}
12. ステップ 10 と 11 を繰り返して、L2VPN アドレス ファミリ内の他の BGP ネイバーをアクティブにします。
13. **exit-address-family**
14. **end**
15. **showl2vpnvfi**
16. **showipbgpl2vpnvpls**{**all** | **rd***route-distinguisher*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**routerbgp***autonomous-system-number* 例： `Device(config)# router bgp 65000`	指定したルーティング プロセスのルータ 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	**nobgpdefaultipv4-unicast** 例： `Device(config-router)# no bgp default ipv4-unicast`	BGP ルーティング プロセスで使用される IPv4 ユニキャスト アドレス ファミリをディセーブルにします。 （注） IPv4ユニキャストアドレスファミリに関するルーティング情報は、**neighborremote-as** ルータ コンフィギュレーションコマンドを使用して設定された各BGPルーティングセッションに対してデフォルトでアドバタイズされます。ただし、**neighborremote-as** コマンドを設定する前に、**nobgpdefaultipv4-unicast** ルータ コンフィギュレーション コマンドを設定した場合は例外です。既存のネイバー コンフィギュレーションは影響されません。
ステップ 5	**bgplog-neighbor-changes** 例： `Device(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 6	**neighbor** {*ip-address* |*peer-group-name*} **remote-as***autonomous-system-number* 例： `Device(config-router)# neighbor 10.10.10.1 remote-as 65000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル デバイスの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。 • *autonomous-system-number* 引数が、**routerbgp** コマンドで指定された自律システム番号と一致する場合、ネイバーは内部ネイバーになります。

	コマンドまたはアクション	目的
		• *autonomous-system-number* 引数が、**routerbgp** コマンドで指定された自律システム番号と一致しない場合、ネイバーは外部ネイバーになります。 • この例では、10.10.10.1 のネイバーは内部 BGP ネイバーです。
ステップ 7	**neighbor** {*ip-address* |*peer-group-name*} **update-source***interface-typeinterface-number* 例： `Device(config-router)# neighbor 10.10.10.1 update-source loopback1`	（任意）ルーティングテーブルアップデートを受信するための特定のソースまたはインターフェイスを選択するようにデバイスを設定します。 • この例では、ループバックインターフェイスを使用します。この設定のメリットは、ループバックインターフェイスがフラッピングインターフェイスの効果の影響を受けにくいことです。
ステップ 8	他の BGP ネイバーを設定する場合は、ステップ 6 と 7 を繰り返します。	—
ステップ 9	**address-familyl2vpn**[**vpls**] 例： `Device(config-router)# address-family l2vpn vpls`	L2VPN アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • オプションの **vpls** キーワードは、VPLS エンドポイント プロビジョニング情報が BGP ピアに配布されるように指定します。 • この例では、L2VPN VPLS アドレス ファミリ セッションが作成されます。
ステップ 10	**neighbor** {*ip-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor 10.10.10.1 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	**neighbor** {*ip-address* | *peer-group-name*} **send-community** {**both** | **standard** | **extended**} 例： `Device(config-router-af)# neighbor 10.10.10.1 send-community extended`	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。 • この例では、拡張コミュニティ属性が 10.10.10.1 のネイバーに送信されます。

	コマンドまたはアクション	目的
ステップ 12	ステップ 10 と 11 を繰り返して、L2VPN アドレス ファミリ内の他の BGP ネイバーをアクティブにします。	—
ステップ 13	**exit-address-family** 例： `Device(config-router-af)# exit-address-family`	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、ルータ コンフィギュレーション モードに戻ります。
ステップ 14	**end** 例： `Device(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 15	**showl2vpnvfi** 例： `Device# show l2vpn vfi`	Layer 2 VPN（L2VPN）仮想転送インスタンス（VFI）に関する情報を表示します。
ステップ 16	**showipbgpl2vpnvpls**{**all** | **rd***route-distinguisher*} 例： `Device# show ip bgp l2vpn vpls all`	L2VPN VPLS アドレス ファミリに関する情報を表示します。

VPLS 自動検出設定のカスタマイズ

仮想プライベート LAN サービス（VPLS）環境のカスタマイズは、複数のコマンドで行えます。VPLS ドメイン、ルート識別子（RD）、ルート ターゲット（RT）、およびプロバイダーエッジ（PE）デバイスの識別子を指定できます。これらの識別子をカスタマイズするには、次のタスクを実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **l2vfi***vfi-name***autodiscovery**
4. **vpnid***vpn-id*
5. **vpls-id** {*autonomous-system-number*:*nn* | *ip-address*:*nn*}
6. **rd** {*autonomous-system-number*:*nn* | *ip-address*:*nn*}
7. **route-target** [**import** | **export** | **both**] {*autonomous-system-number*:*nn* | *ip-address*:*nn*}
8. **auto-route-target**
9. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**l2vfi***vfi-name***autodiscovery** 例： `Device(config)# l2 vfi vpls1 autodiscovery`	PE デバイス上で VPLS 自動検出を有効にして、Layer 2 VFI 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	**vpnid***vpn-id* 例： `Device(config-vfi)# vpn id 10`	VPLS ドメインの VPN ID を設定します。
ステップ 5	**vpls-id** {*autonomous-system-number*:*nn* | *ip-address*:*nn*} 例： `Device(config-vfi)# vpls-id 5:300`	（任意）VPLS ドメインに識別子を割り当てます。 • Border Gateway Protocol（BGP）自律システム（AS）番号と設定された VFI VPN ID を使用して VPLS 自動検出が自動的に VPLS ID を生成するため、このコマンドはオプションです。次のコマンドを使用して、自動生成された VPLS ID を変更できます。 • VPLS ID 引数を設定する 2 つの形式があります。例で示されているような *autonomous-system-number:networknumber*（*ASN:nn*）

	コマンドまたはアクション	目的
		形式、または、*IP-address:networknumber* 形式（*IP-address:nn*）で設定できます。
ステップ 6	**rd** {*autonomous-system-number*:*nn* | *ip-address*:*nn*} 例： `Device(config-vfi)# rd 2:3`	（任意）エンドポイント情報を配布する RD を指定します。 • BGP 自律システム番号と設定された VFI VPN ID を使用して VPLS 自動検出が自動的に RD を生成するため、このコマンドはオプションです。次のコマンドを使用して、自動生成された RD を変更できます。 • ルート識別子の引数を設定するには、2 つの形式があります。例で示されているような *autonomous-system-number:networknumber*（*ASN:nn*）形式、または、*IP-address:networknumber* 形式（*IP-address:nn*）で設定できます。
ステップ 7	**route-target** [**import** | **export** | **both**] {*autonomous-system-number*:*nn* | *ip-address*:*nn*} 例： `Device(config-vfi)# route-target 600:2222`	（任意）RT を指定します。 • 6 バイト未満の RD と VPLS ID を使用して VPLS 自動検出が RT を自動的に生成するため、このコマンドはオプションです。次のコマンドを使用して、自動生成された RT を変更できます。 • ルート ターゲット引数を設定する 2 つの形式があります。例で示されているような *autonomous-system-number:networknumber*（*ASN:nn*）形式、または、*IP-address:networknumber* 形式（*IP-address:nn*）で設定できます。
ステップ 8	**auto-route-target** 例： `Device(config-vfi)# auto-route-target`	（任意）RT の自動生成を有効にします。
ステップ 9	**end** 例： `Device(config-vfi)# end`	L2 VFI コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。 • コマンドは、デバイスがレイヤ 2 VFI コンフィギュレーション モードを終了した後、有効になります。

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した VPLS 自動検出設定のカスタマイズ

仮想プライベート LAN サービス（VPLS）環境のカスタマイズは、複数のコマンドで行えます。VPLS ドメイン、ルート識別子（RD）、ルート ターゲット（RT）、およびプロバイダーエッジ（PE）デバイスの識別子を指定できます。これらの識別子をカスタマイズするには、次のタスクを実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **l2vpnvficontext***vfi-name*
4. **vpnid***vpn-id*
5. **autodiscoverybgpsignalingldp**
6. **vpls-id** {*autonomous-system-number*:*nn* | *ip-address*:*nn*}
7. **rd** {*autonomous-system-number*:*nn* | *ip-address*:*nn*}
8. **route-target** [**import** | **export** | **both**] {*autonomous-system-number*:*nn* | *ip-address*:*nn*}
9. **auto-route-target**
10. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**l2vpnvficontext***vfi-name* 例： `Device(config)# l2vpn vfi context vpls1`	L2VPN VFI コンテキストを確立して、L2 VFI 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	**vpnid***vpn-id* 例： `Device(config-vfi)# vpn id 10`	VPLS ドメインの VPN ID を設定します。
ステップ 5	**autodiscoverybgpsignalingldp** 例： `Device(config-vfi)# autodiscovery bgp signaling ldp`	PE デバイス上で VPLS 自動検出：BGP ベース機能を有効にします。
ステップ 6	**vpls-id** {*autonomous-system-number*:*nn* | *ip-address*:*nn*} 例： `Device(config-vfi)# vpls-id 5:300`	（任意）VPLS ドメインに識別子を割り当てます。 • Border Gateway Protocol（BGP）自律システム（AS）番号と設定された VFI VPN ID を使用して VPLS 自動検出が自動的に VPLS ID を生成するため、このコマンドはオプションです。次のコマンドを使用して、自動生成された VPLS ID を変更できます。 • VPLS ID 引数を設定する 2 つの形式があります。例で示されているような *autonomous-system-number:networknumber*（*ASN:nn*）形式、または、*IP-address:networknumber* 形式（*IP-address:nn*）で設定できます。
ステップ 7	**rd** {*autonomous-system-number*:*nn* | *ip-address*:*nn*} 例： `Device(config-vfi)# rd 2:3`	（任意）エンドポイント情報を配布する RD を指定します。 • BGP 自律システム番号と設定された VFI VPN ID を使用して VPLS 自動検出が自動的に RD を生成するため、このコマンドはオプションです。次のコマンドを使用して、自動生成された RD を変更できます。 • ルート識別子の引数を設定するには、2 つの形式があります。例で示されているような *autonomous-system-number:networknumber*（*ASN:nn*）形式、または、*IP-address:networknumber* 形式（*IP-address:nn*）で設定できます。
ステップ 8	**route-target** [**import** | **export** | **both**] {*autonomous-system-number*:*nn* | *ip-address*:*nn*} 例： `Device(config-vfi)# route-target 600:2222`	（任意）RT を指定します。 • 6 バイト未満の RD と VPLS ID を使用して VPLS 自動検出が RT を自動的に生成するため、このコマンドはオプションです。次のコマンドを使用して、自動生成された RT を変更できます。

	コマンドまたはアクション	目的
		• ルートターゲット引数を設定する2つの形式があります。例で示されているような *autonomous-system-number:networknumber*（*ASN:nn*）形式、または、*IP-address:networknumber* 形式（*IP-address:nn*）で設定できます。
ステップ 9	**auto-route-target** 例： `Device(config-vfi)# auto-route-target`	（任意）RT の自動生成を有効にします。
ステップ 10	**end** 例： `Device(config-vfi)# end`	L2 VFI コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。 • コマンドは、デバイスがレイヤ 2 VFI コンフィギュレーション モードを終了した後、有効になります。

VPLS N-PE デバイスでの MST の設定

ネットワーク側の PE（N-PE）デバイスは、マルチスパニング ツリー（MST）インスタンスのルート ブリッジです。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **l2 vfi***vfi-name* **manual**
4. **vpn id***vpn-id*
5. **forward permit l2protocol all**
6. **neighbor***peer-N-PE-ip-address***encapsulation mpls**
7. **exit**
8. **spanning-tree mode** [**mst** | **pvst** | **rapid-pvst**]
9. **spanning-tree mst configuration**
10. **name***name*
11. **revision***version*
12. **instance***instance-id***vlan***vlan-range*
13. **end**
14. **show spanning-tree mst** [*instance-id* [**detail**] [*interface*] | **configuration** [**digest**] | **detail** | **interface***type number* [**detail**]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**l2 vfi***vfi-name* **manual** 例： `Device(config)# l2 vfi vpls-mst manual`	レイヤ 2 仮想転送インスタンス（VFI）を作成して、レイヤ 2 VFI マニュアル コンフィギュレーション モードを開始します。
ステップ 4	**vpn id***vpn-id* 例： `Device(config-vfi)# vpn id 4000`	VPN ルーティングおよび転送（VRF）インスタンスで VPN ID を設定または更新します。
ステップ 5	**forward permit l2protocol all** 例： `Device(config-vfi)# forward permit l2protocol all`	2 つの N-PE デバイス間でブリッジプロトコルデータユニット（BPDU）情報の転送に使用される VPLS 擬似回線を定義します。
ステップ 6	**neighbor***peer-N-PE-ip-address***encapsulation mpls** 例： `Device(config-vfi)# neighbor 10.76.100.12 encapsulation mpls`	VPLS ピアごとのトンネル シグナリングおよびカプセル化メカニズムのタイプを指定します。
ステップ 7	**exit** 例： `Device(config-vfi)# exit`	レイヤ 2 VFI マニュアル コンフィギュレーション モードを終了して、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	**spanning-tree mode** [**mst** | **pvst** | **rapid-pvst**] 例： `Device(config)# spanning-tree mode mst`	MST、Per-VLAN Spanning Tree+（PVST+）、および Rapid-PVST+ の間でモードを切り替えます。
ステップ 9	**spanning-tree mst configuration** 例： `Device(config)# spanning-tree mst configuration`	MST 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 10	**name***name* 例： `Device(config-mst)# name cisco`	MST リージョンの名前を設定します。
ステップ 11	**revision***version* 例： `Device(config-mst)# revision 11`	MST コンフィギュレーションのリビジョン番号を設定します。
ステップ 12	**instance***instance-id* **vlan***vlan-range* 例： `Device(config-mst)# instance 1 vlan 100`	VLAN または VLAN のグループを MST インスタンスにマッピングします。
ステップ 13	**end** 例： `Device(config-mst)# end`	MST コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 14	**show spanning-tree mst** [*instance-id* [**detail**] [*interface*] | **configuration** [**digest**] | **detail** | **interface***type number* [**detail**]] 例： `Device# show spanning-tree mst 1`	MST 設定に関する情報を表示します。

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した VPLS N-PE デバイス上での MST の設定

ネットワーク側の PE（N-PE）デバイスは、マルチスパニングツリー（MST）インスタンスのルートブリッジです。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **l2vpnvfi context** *vfi-name*
4. **vpn id***vpn-id*
5. **forward permit l2protocol all**
6. **neighbor***peer-N-PE-ip-address***encapsulation mpls**
7. **exit**
8. **spanning-tree mode** [**mst** | **pvst** | **rapid-pvst**]
9. **spanning-tree mst configuration**
10. **name***name*
11. **revision***version*
12. **instance***instance-id***vlan***vlan-range*
13. **end**
14. **show spanning-tree mst** [*instance-id* [**detail**] [*interface*] | **configuration** [**digest**] | **detail** | **interface***type number* [**detail**]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**l2vpnvfi context** *vfi-name* 例： `Device(config)# l2vpn vfi context vpls-mst`	L2VPN VFI コンテキストを確立して、L2 VFI 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	**vpn id***vpn-id* 例： `Device(config-vfi)# vpn id 4000`	VPN ルーティングおよび転送（VRF）インスタンスで VPN ID を設定または更新します。

	コマンドまたはアクション	目的
ステップ 5	**forward permit l2protocol all** 例： `Device(config-vfi)# forward permit l2protocol all`	2 つの N-PE デバイス間でブリッジ プロトコル データ ユニット（BPDU）情報の転送に使用される VPLS 擬似回線を定義します。
ステップ 6	**neighbor***peer-N-PE-ip-address***encapsulation mpls** 例： `Device(config-vfi)# neighbor 10.76.100.12 encapsulation mpls`	VPLS ピアごとのトンネル シグナリングおよびカプセル化メカニズムのタイプを指定します。
ステップ 7	**exit** 例： `Device(config-vfi)# exit`	レイヤ 2 VFI マニュアル コンフィギュレーション モードを終了して、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	**spanning-tree mode** [**mst** | **pvst** | **rapid-pvst**] 例： `Device(config)# spanning-tree mode mst`	MST、Per-VLAN Spanning Tree+（PVST+）、および Rapid-PVST+ の間でモードを切り替えます。
ステップ 9	**spanning-tree mst configuration** 例： `Device(config)# spanning-tree mst configuration`	MST コンフィギュレーション モードを開始します。
ステップ 10	**name***name* 例： `Device(config-mst)# name cisco`	MST リージョンの名前を設定します。
ステップ 11	**revision***version* 例： `Device(config-mst)# revision 11`	MST コンフィギュレーションのリビジョン番号を設定します。
ステップ 12	**instance***instance-id***vlan***vlan-range* 例： `Device(config-mst)# instance 1 vlan 100`	VLAN または VLAN のグループを MST インスタンスにマッピングします。

	コマンドまたはアクション	目的
ステップ 13	**end** 例： `Device(config-mst)# end`	MST コンフィギュレーションモードを終了して、特権 EXEC モードを開始します。
ステップ 14	**show spanning-tree mst** [*instance-id* [**detail**] [*interface*] | **configuration** [**digest**] | **detail** | **interface***type number* [**detail**]] 例： `Device# show spanning-tree mst 1`	MST 設定に関する情報を表示します。

BGP ベースの VPLS 自動検出の設定例

次の例は、VPLS 自動検出を使用するネットワークの設定を示しています。

例：BGP ベースの VPLS 自動検出の有効化

```
Device> enable
Device# configure terminal
Device(config)# l2 vfi vpls1 autodiscovery
Device(config-vfi)# vpn id 10
Device(config-vfi)# exit
```

例：L2VPN プロトコルベース CLI 機能に関連するコマンドを使用した BGP ベースの VPLS 自動検出の有効化

```
Device> enable
Device# configure terminal
Device(config)# l2vpn vfi context vpls1
Device(config-vfi)# vpn id 10
Device(config-vfi)# autodiscovery bgp signaling ldp
Device(config-vfi)# exit
```

例：VPLS 自動検出を有効にするための BGP の設定

PE1

```
l2 router-id 10.1.1.1
l2 vfi auto autodiscovery
 vpn id 100
!
```

```
pseudowire-class mpls
 encapsulation mpls
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.255
!
interface GigabitEthernet 0/0/1
 description Backbone interface
 ip address 192.168.0.1 255.255.255.0
 mpls ip
!
router ospf 1
 log-adjacency-changes
 network 10.1.1.0 0.0.0.255 area 0
 network 172.16.0.0 0.0.0.255 area 0
!
router bgp 1
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 bgp update-delay 1
 neighbor 10.1.1.2 remote-as 1
 neighbor 10.1.1.2 update-source Loopback1
 neighbor 10.1.1.3 remote-as 1
 neighbor 10.1.1.3 update-source Loopback1
!
 address-family ipv4
 no synchronization
 no auto-summary
 exit-address-family
 !
 address-family l2vpn vpls
 neighbor 10.1.1.2 activate
 neighbor 10.1.1.2 send-community extended
 neighbor 10.1.1.3 activate
 neighbor 10.1.1.3 send-community extended
 exit-address-family
```

PE2

```
l2 router-id 10.1.1.2
l2 vfi auto autodiscovery
 vpn id 100
!
 pseudowire-class mpls
 encapsulation mpls
!
interface Loopback1
 ip address 10.1.1.2 255.255.255.255
!
interface GigabitEthernet 0/0/1
 description Backbone interface
 ip address 192.168.0.2 255.255.255.0
 mpls ip
!
router ospf 1
 log-adjacency-changes
 network 10.1.1.0 0.0.0.255 area 0
 network 172.16.0.0 0.0.0.255 area 0
!
router bgp 1
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 bgp update-delay 1
 neighbor 10.1.1.1 remote-as 1
 neighbor 10.1.1.1 update-source Loopback1
 neighbor 10.1.1.3 remote-as 1
 neighbor 10.1.1.3 update-source Loopback1
!
 address-family ipv4
 no synchronization
 no auto-summary
 exit-address-family
```

```
 !
 address-family l2vpn vpls
 neighbor 10.1.1.1 activate
 neighbor 10.1.1.1 send-community extended
 neighbor 10.1.1.3 activate
 neighbor 10.1.1.3 send-community extended
 exit-address-family
```

PE3

```
l2 router-id 10.1.1.3
l2 vfi auto autodiscovery
 vpn id 100
!
pseudowire-class mpls
 encapsulation mpls
!
interface Loopback1
 ip address 10.1.1.3 255.255.255.255
!
interface GigabitEthernet 0/0/1
 description Backbone interface
 ip address 192.168.0.3 255.255.255.0
 mpls ip
!
router ospf 1
 log-adjacency-changes
 network 10.1.1.0 0.0.0.255 area 0
 network 172.16.0.0 0.0.0.255 area 0
!
router bgp 1
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 bgp update-delay 1
 neighbor 10.1.1.1 remote-as 1
 neighbor 10.1.1.1 update-source Loopback1
 neighbor 10.1.1.2 remote-as 1
 neighbor 10.1.1.2 update-source Loopback1
!
 address-family ipv4
 no synchronization
 no auto-summary
 exit-address-family
 !
 address-family l2vpn vpls
 neighbor 10.1.1.1 activate
 neighbor 10.1.1.1 send-community extended
 neighbor 10.1.1.2 activate
 neighbor 10.1.1.2 send-community extended
 exit-address-family
```

例：L2VPN プロトコルベース CLI 機能に関連するコマンドを使用した VPLS 自動検出を有効にするための BGP の設定

PE1

```
l2vpn
 router-id 10.1.1.1
l2vpn vfi context auto
 vpn id 100
 autodiscovery bgp signaling ldp
!
interface pseudowire 1
 encapsulation mpls
 neighbor 33.33.33.33 1
!
```

```
interface Loopback1
 ip address 10.1.1.1 255.255.255.255
!
interface GigabitEthernet 0/0/1
 description Backbone interface
 ip address 192.168.0.1 255.255.255.0
 mpls ip
!
router ospf 1
 log-adjacency-changes
 network 10.1.1.0 0.0.0.255 area 0
 network 172.16.0.0 0.0.0.255 area 0
!
router bgp 1
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 bgp update-delay 1
 neighbor 10.1.1.2 remote-as 1
 neighbor 10.1.1.2 update-source Loopback1
 neighbor 10.1.1.3 remote-as 1
 neighbor 10.1.1.3 update-source Loopback1
!
 address-family ipv4
 no synchronization
 no auto-summary
 exit-address-family
 !
 address-family l2vpn vpls
 neighbor 10.1.1.2 activate
 neighbor 10.1.1.2 send-community extended
 neighbor 10.1.1.3 activate
 neighbor 10.1.1.3 send-community extended
 exit-address-family
```

PE2

```
l2vpn
 router-id 10.1.1.2
l2vpn vfi context auto
 vpn id 100
 autodiscovery bgp signaling ldp

!
 interface pseudowire 1
 encapsulation mpls
 neighbor 33.33.33.33 1
!
interface Loopback1
 ip address 10.1.1.2 255.255.255.255
!
interface GigabitEthernet 0/0/1
 description Backbone interface
 ip address 192.168.0.2 255.255.255.0
 mpls ip
!
router ospf 1
 log-adjacency-changes
 network 10.1.1.0 0.0.0.255 area 0
 network 172.16.0.0 0.0.0.255 area 0
!
router bgp 1
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 bgp update-delay 1
 neighbor 10.1.1.1 remote-as 1
 neighbor 10.1.1.1 update-source Loopback1
 neighbor 10.1.1.3 remote-as 1
 neighbor 10.1.1.3 update-source Loopback1
!
 address-family ipv4
 no synchronization
 no auto-summary
```

```
 exit-address-family
 !
 address-family l2vpn vpls
 neighbor 10.1.1.1 activate
 neighbor 10.1.1.1 send-community extended
 neighbor 10.1.1.3 activate
 neighbor 10.1.1.3 send-community extended
 exit-address-family
```

PE3

```
l2vpn
 router-id 10.1.1.3
l2vpn vfi context auto
 vpn id 100
 autodiscovery bgp signaling ldp

!
interface pseudowire 1
 encapsulation mpls
 neighbor 33.33.33.33 1
!
interface Loopback1
 ip address 10.1.1.3 255.255.255.255
!
interface GigabitEthernet 0/0/1
 description Backbone interface
 ip address 192.168.0.3 255.255.255.0
 mpls ip
!
router ospf 1
 log-adjacency-changes
 network 10.1.1.0 0.0.0.255 area 0
 network 172.16.0.0 0.0.0.255 area 0
!
router bgp 1
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 bgp update-delay 1
 neighbor 10.1.1.1 remote-as 1
 neighbor 10.1.1.1 update-source Loopback1
 neighbor 10.1.1.2 remote-as 1
 neighbor 10.1.1.2 update-source Loopback1
!
 address-family ipv4
 no synchronization
 no auto-summary
 exit-address-family
 !
 address-family l2vpn vpls
 neighbor 10.1.1.1 activate
 neighbor 10.1.1.1 send-community extended
 neighbor 10.1.1.2 activate
 neighbor 10.1.1.2 send-community extended
 exit-address-family
```

例：VPLS 自動検出設定のカスタマイズ

```
Device> enable
Device# configure terminal
Device(config)# l2 vfi vpls1 autodiscovery
Device(config-vfi)# vpn id 10
Device(config-vfi)# vpls-id 5:300
Device(config-vfi)# rd 2:3
Device(config-vfi)# route-target 600:2222
Device(config-vfi)# end
```

例：L2VPN プロトコルベース CLI 機能に関連するコマンドを使用した VPLS 自動検出設定のカスタマイズ

```
Device> enable
Device# configure terminal
Device(config)# l2vpn vfi context vpls1
Device(config-vfi)# vpn id 10
Device(config-vfi)# autodiscovery bgp signaling ldp
Device(config-vfi)# vpls-id 5:300
Device(config-vfi)# rd 2:3
Device(config-vfi)# route-target 600:2222
Device(config-vfi)# end
```

例：VPLS N-PE デバイスでの MST の設定

```
Device> enable
Device# configure terminal
Device(config)# l2 vfi vpls-mst manual
Device(config-vfi)# vpn id 4000
Device(config-vfi)# forward permit l2protocol all
Device(config-vfi)# neighbor 10.76.100.12 encapsulation mpls
Device(config-vfi)# exit
Device(config)# spanning-tree mode mst
Device(config)# spanning-tree mst configuration
Device(config-mst)# name cisco
Device(config-mst)# revision 11
Device(config-mst)# instance 1 vlan 100
Device(config-mst)# end
```

次に、**show spanning-tree mst** コマンドからの出力例を示します。

```
Device# show spanning-tree mst 1

##### MST1    vlans mapped:   100
Bridge        address 0023.3380.f8bb  priority      4097  (4096 sysid 1)
Root          this switch for MST1                                // Root for MST instance
 1 with VLAN 100
Interface                        Role Sts Cost      Prio.Nbr Type
-----------                  --- -- ------ ---- ------------------------------
Gi1/0/0                          Desg FWD 20000     128.18   P2p   // Access interface
VPLS-MST                         Desg FWD 1         128.28   Shr   // Forward VFI
```

次に、**show spanning-tree mst detail** コマンドからの出力例を示します。

```
Device# show spanning-tree mst 1 detail

##### MST1    vlans mapped:   100
Bridge        address 0023.3380.f8bb  priority      4097  (4096 sysid 1)
Root          this switch for MST1            // Root for MST instance 1 with VLAN 100
GigabitEthernet1/0/0 of MST1 is designated forwarding
Port info             port id         128.18  priority    128  cost       20000
Designated root       address 0023.3380.f8bb  priority   4097  cost           0
Designated bridge     address 0023.3380.f8bb  priority   4097  port id   128.18
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 40, received 5
VPLS-4000 of MST1 is designated forwarding
Port info             port id         128.28  priority    128  cost           1
Designated root       address 0023.3380.f8bb  priority   4097  cost           0
Designated bridge     address 0023.3380.f8bb  priority   4097  port id   128.28
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 28, received 26         // BPDU message exchange between N-PE devices
```

例：L2VPN プロトコルベース CLI 機能に関連するコマンドを使用した VPLS N-PE デバイスでの MST の設定

```
Device> enable
Device# configure terminal
Device(config)# l2vpn vfi context vpls-mst
Device(config-vfi)# vpn id 4000
Device(config-vfi)# forward permit l2protocol all
Device(config-vfi)# member 10.76.100.12 encapsulation mpls
Device(config-vfi)# exit
Device(config)# spanning-tree mode mst
Device(config)# spanning-tree mst configuration
Device(config-mst)# name cisco
Device(config-mst)# revision 11
Device(config-mst)# instance 1 vlan 100
Device(config-mst)# end
```

次に、**show spanning-tree mst** コマンドからの出力例を示します。

```
Device# show spanning-tree mst 1

##### MST1    vlans mapped:   100
Bridge        address 0023.3380.f8bb  priority      4097  (4096 sysid 1)
Root          this switch for MST1                              // Root for MST instance
 1 with VLAN 100
Interface                        Role Sts Cost      Prio.Nbr Type
-----------                  --- -- ------ ---- -------------------------------
Gi1/0/0                          Desg FWD 20000     128.18   P2p   // Access interface
VPLS-MST                         Desg FWD 1         128.28   Shr   // Forward VFI
```

次に、**show spanning-tree mst detail** コマンドからの出力例を示します。

```
Device# show spanning-tree mst 1 detail

##### MST1    vlans mapped:   100
Bridge        address 0023.3380.f8bb  priority      4097  (4096 sysid 1)
Root          this switch for MST1            // Root for MST instance 1 with VLAN 100
GigabitEthernet1/0/0 of MST1 is designated forwarding
Port info             port id         128.18  priority    128  cost       20000
Designated root       address 0023.3380.f8bb  priority   4097  cost           0
Designated bridge     address 0023.3380.f8bb  priority   4097  port id   128.18
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 40, received 5
VPLS-4000 of MST1 is designated forwarding
Port info             port id         128.28  priority    128  cost           1
Designated root       address 0023.3380.f8bb  priority   4097  cost           0
Designated bridge     address 0023.3380.f8bb  priority   4097  port id   128.28
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 28, received 26        // BPDU message exchange between N-PE devices
```

例：ルート リフレクタでの BGP VPLS 自動検出のサポート

次の例では、PE-RR（プロバイダーエッジルートリフレクタであることを示す）という名前のホストが、仮想プライベート LAN サービス（VPLS）プレフィックスを反映可能なルート リフレクタとして設定されます。VPLS アドレス ファミリは **address-familyl2vpnvpls** コマンドを使用して設定されます。

```
hostname PE-RR
!
router bgp 1
 bgp router-id 10.1.1.3
 no bgp default route-target filter
 bgp log-neighbor-changes
neighbor iBGP-PEERS peer-group
```

```
neighbor iBGP-PEERS remote-as 1
neighbor iBGP-PEERS update-source Loopback1
neighbor 10.1.1.1 peer-group iBGP-PEERS
neighbor 10.1.1.2 peer-group iBGP-PEERS
!
address-family l2vpn vpls
  neighbor iBGP-PEERS send-community extended
  neighbor iBGP-PEERS route-reflector-client
  neighbor 10.1.1.1 peer-group iBGP-PEERS
  neighbor 10.1.1.2 peer-group iBGP-PEERS
exit-address-family
```

BGP ベースの VPLS 自動検出に関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List, All Releases』
MPLS コマンド	『Multiprotocol Label Switching Command Reference』

標準および RFC

標準/RFC	Title
draft-ietf-l2vpn-signaling-08.txt	『*Provisioning,Autodiscovery,andSignalinginL2VPNs*』
draft-ietf-l2vpn-vpls-bgp-08.8	『*VirtualPrivateLANService(VPLS)UsingBGPforAutodiscoveryandSignaling*』
draft-ietf-mpls-lsp-ping-03.txt	『*DetectingMPLSDataPlaneFailures*』
draft-ietf-pwe3-vccv-01.txt	『*Pseudo-Wire(PW)VirtualCircuitConnectionVerification(VCCV)*』
RFC 3916	『*RequirementsforPseudo-wireEmulationEdge-to-Edge(PWE3)*』
RFC 3981	『*PseudoWireEmulationEdge-to-EdgeArchitecture*』
RFC 6074	『Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)』
RFC 4761	『Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling』

MIB

MIB	MIB のリンク
• CISCO-IETF-PW-ATM-MIB（PW-ATM-MIB） • CISCO-IETF-PW-ENET-MIB（PW-ENET-MIB） • CISCO-IETF-PW-FR-MIB（PW-FR-MIB） • CISCO-IETF-PW-MIB（PW-MIB） • CISCO-IETF-PW-MPLS-MIB（PW-MPLS-MIB）	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探して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

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。サービス契約が有効で、ログイン ID またはパスワードを取得していない場合は、Cisco.com でまず登録手続きを行ってください。	http://www.cisco.com/en/US/support/index.html

BGP ベースの VPLS 自動検出の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、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。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *37* : ***BGP*** ベースの ***VPLS*** 自動検出の機能情報

機能名	リリース	機能情報
BGP ベースの VPLS 自動検出	Cisco IOS XE Release 3.7S Cisco IOS Release 15.1(1)SY	VPLS 自動検出を使用すると、各仮想プライベート LAN サービス（VPLS）プロバイダーエッジ（PE）デバイスで、同じ VPLS ドメインの一部である他の PE デバイスを検出できます。

第 23 章

一意でない VPI を使用した PVC から PWE への N:1 マッピング

一意でない仮想パス識別子（VPI）機能を使用した PVC から擬似回線エミュレーション（PWE）への N:1 のマッピングは、1 つ以上の ATM 相手先固定接続（PVC）を単一の擬似回線（PW）にマッピングします。AAL0 カプセル化には N:1 および 1:1 マッピングの 2 つのモードがあります。N:1 マッピングでは、複数の無関係な仮想パス識別子/仮想チャネル識別子（VPI/VCI）が 1 つのマルチプロトコル ラベル スイッチング（MPLS）PW で送信されます。これは、MPLS ネットワークで使用されるリソースが少なくなるため、効率的なマッピング方法です。1:1 マッピングでは、1 つの VPI/VCI が 1 つの MPLS PW で送信されます。この機能のメリットを次に示します。

- 集約 Quality of Service（QoS）は、関連する PVC に適用することができます。
- 使用される擬似回線の数が削減され、帯域幅が節約されます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用の

プラットフォームおよびソフトウェア リリースのリリース 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、機能情報の表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シスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

一意でない VPI を含む PWE への N:1 PVC マッピングの制約事項

- N:1 相手先固定接続（PVC）のマッピング設定は、マルチポイント サブインターフェイスでのみサポートされます。つまり、メイン インターフェイスまたはポイントツーポイント サブインターフェイスではサポートされません。
- N:1 PVC マッピング モードは、アクセス回線冗長性サブインターフェイスではサポートされていません。
- 事前設定された PVC は、N:1 PVC マッピングを設定するマルチポイント サブインターフェイスには設定できません。
- 擬似回線にバインドされた接続回線は、すべてのレイヤ 2 仮想回線（VC）が削除されるまで削除できません。
- レイヤ 3 PVC は N:1 サブインターフェイスに設定できません。
- PVC、メイン インターフェイス、またはサブインターフェイスに接続された VC クラスの下で設定されるセル パッキング値は、N:1 PVC によって継承されません。
- 運用管理および保守（OAM）機能は、N:1 レイヤ 2 PVC ではサポートされません。カスタマー エッジ（CE）ネットワークから発信される OAM セルは、通常のデータ トラフィックとして扱われ、擬似回線を通過します。
- ATM アダプテーション層タイプ 0（AAL0）カプセル化は、N:1 PVC でのみサポートされます。
- サービス ポリシー設定は、N:1 PVC のサブインターフェイス レベルでのみ設定できます。

一意でない VPI を含む PWE への N:1 PVC マッピングに関する情報

一意でない VPI を含む PWE への N:1 PVC マッピング機能の説明

マルチプロトコル ラベル スイッチング（MPLS）で ATM セルを転送するには、MPLS バックボーンの両端のプロバイダー エッジ（PE）ルータ間で VC を確立します。一意でない VPI 機能を使用した擬似回線エミュレーション（PWE）への相手先固定接続（PVC）の N:1 のマッピングでは、仮想パス識別子（VPI）にかかわらず複数の PVC が、サブインターフェイスで設定された単一の擬似回線で転送されます。（「N:1」は、1 つの擬似回線に対して転送される PVC の数を指しています）。ATM セルは 1 つのフレームにパッキングされ、1 つの擬似回線で送信されます。ATM セルのヘッダー情報は、出力側で受信されたパケットがアンパックされ、ATM セルがそれぞれの PVC にマップされるように、パケット内のセル単位で、セル ペイロードと一緒にパッキングされます。

N:1 PVC マッピング モードでは、デバイスは MPLS パケットの 1 つの PVC からのセルのみをパッキングして、擬似回線で転送できます。つまり、複数の PVC からのセルを 1 つの MPLS パケットにパッキングしたり、転送するために 1 つの擬似回線にマップしたりすることはできません。ただし、複数の PVC からのセルでパッキングされた MPLS パケットをデバイスが受信すると、それらのセルはアンパックされ、それぞれの PVC に送信されます。

一意でない VPI を含む PWE への N:1 PVC マッピングの設定方法

一意でない VPI を含む PWE への N:1 PVC マッピングの設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface atm***slot*/*subslot*/*port*
4. **atmmcpt-timers***timer1timer2timer3*
5. **exit**
6. **configure terminal**
7. **interface atm***slot*/*subslot*/*port.subslot* **multipoint**
8. **no ip address**
9. **atmenable-ilmi-trap**
10. **cell-packing***maxcells***mcpt-timer***timer-number*
11. **xconnect***peer-ipaddressvc-id***encapsulationmpls**
12. **pvc***vpi*/*vci***l2transport**
13. 設定する PVC の数だけステップ 12 を繰り返します。
14. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 atm***slot*/*subslot*/*port* 例： `Device(config)# interface atm 9/1/1`	ATM インターフェイスを有効にして、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	**atmmcpt-timers***timer1timer2timer3* 例： `Device(config-if)# atm mcpt-timers 100 200 300`	Maximum Cell Packing Timeout（MCPT）の値をマイクロ秒単位で設定します。 • MCPT タイマーは、擬似回線にパントするために raw セル（AAL0 カプセル化）が単一パケットにパックされるのを、デバイスが待機する時間を設定します。
ステップ 5	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 6	**configure terminal** 例： `Device# 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 7	**interface atm***slot/subslot/port.subslot* **multipoint** 例： `Device(config)# interface atm 9/1/1.1 multipoint`	サブインターフェイス コンフィギュレーション モードを開始して、指定された ATM 共有ポート アダプタ（SPA）の特定のポートでマルチポイント サブインターフェイスを作成します。
ステップ 8	**no ip address** 例： `Device(config-subif)# no ip address`	インターフェイス IP アドレスを削除します。
ステップ 9	**atmenable-ilmi-trap** 例： `Device(config-subif)# atm enable-ilmi-trap`	ATM インターフェイスまたはサブインターフェイスが有効になったときまたはシャットダウンされたときに、統合ローカル管理インターフェイス（ILMI）atmfVccChange トラップを生成します。
ステップ 10	**cell-packing***maxcells***mcpt-timer***timer-number* 例： `Device(config-subif)# cell-packing 20 mcpt-timer 2`	ATM over MPLS で MCPT タイミング内に複数の ATM セルが各 MPLS パケットにパックされるようにします。
ステップ 11	**xconnect***peer-ipaddressvc-id***encapsulationmpls** 例： `Device(config-subif)# xconnect 10.1.1.1 100 encapsulation mpls`	（任意）接続回線を有効にして、ピアの IP アドレス、VC ID、およびデータ カプセル化方式を指定します。

	コマンドまたはアクション	目的
ステップ 12	**pvc***vpi*/*vci***l2transport** 例： `Device(config-subif)# pvc 10/100 l2transport`	VPI と仮想チャネル識別子（VCI）を割り当てます。
ステップ 13	設定する PVC の数だけステップ 12 を繰り返します。	—
ステップ 14	**end** 例： `Device(config-subif)# end`	サブインターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

L2VPN プロトコルベースの CLI 機能に関連付けられたコマンドを使用した一意でない VPI を含む PWE への N:1 PVC マッピングの設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface atm***slot*/*subslot*/*port*
4. **atmmcpt-timers***timer1timer2timer3*
5. **exit**
6. **configure terminal**
7. **interface atm***slot*/*subslot*/*portt.subslot* **multipoint**
8. **no ip address**
9. **atmenable-ilmi-trap**
10. **cell-packing***maxcells***mcpt-timer***timer-number*
11. **end**
12. **interfacepseudowire***number*
13. **encapsulationmpls**
14. **neighbor***peer-addressvcid-value*
15. **exit**
16. **l2vpn xconnectcontext***context-name*
17. **member pseudowire***interface-number*
18. **member gigabitethernet***interface-number*
19. **end**
20. **pvc***vpi*/*vci***l2transport**
21. 設定する PVC の数だけステップ 12 を繰り返します。
22. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 3	**interface atm***slot/subslot/port* 例： `Device(config)# interface atm 9/1/1`	ATM インターフェイスを有効にして、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	**atmmcpt-timers***timer1timer2timer3* 例： `Device(config-if)# atm mcpt-timers 100 200 300`	Maximum Cell Packing Timeout（MCPT）の値をマイクロ秒単位で設定します。 • MCPT タイマーは、擬似回線にパントするために raw セル（AAL0 カプセル化）が単一パケットにパックされるのを、デバイスが待機する時間を設定します。
ステップ 5	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 6	**configure terminal** 例： `Device# 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 7	**interface atm***slot/subslot/portt.subslot* **multipoint** 例： `Device(config)# interface atm 9/1/1.1 multipoint`	サブインターフェイス コンフィギュレーション モードを開始して、指定された ATM 共有ポート アダプタ（SPA）の特定のポートでマルチポイント サブインターフェイスを作成します。
ステップ 8	**no ip address** 例： `Device(config-subif)# no ip address`	インターフェイス IP アドレスを削除します。
ステップ 9	**atmenable-ilmi-trap** 例： `Device(config-subif)# atm enable-ilmi-trap`	ATM インターフェイスまたはサブインターフェイスが有効になったときまたはシャットダウンされたときに、統合ローカル管理インターフェイス（ILMI）atmfVccChange トラップを生成します。
ステップ 10	**cell-packing***maxcells***mcpt-timer***timer-number* 例： `Device(config-subif)# cell-packing 20 mcpt-timer 2`	ATM over MPLS で MCPT タイミング内に複数の ATM セルが各 MPLS パケットにパックされるようにします。

	コマンドまたはアクション	目的
ステップ 11	**end** 例： `Router(config-subif)# end`	特権 EXEC モードに戻ります。
ステップ 12	**interfacepseudowire***number* 例： `Router(config)# interface pseudowire 100`	擬似回線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 13	**encapsulationmpls** 例： `Router(config-if)# encapsulation mpls`	マルチプロトコル ラベル スイッチング（MPLS）がデータ カプセル化方式として使用されることを指定します。
ステップ 14	**neighbor***peer-addressvcid-value* 例： `Router(config-if)# neighbor 10.1.1.1 100`	Layer 2 VPN（L2VPN）擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 15	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 16	**l2vpn xconnectcontext***context-name* 例： `Router(config)# l2vpn xconnect context con1`	Layer 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect コンフィギュレーション モードを開始します。
ステップ 17	**member pseudowire***interface-number* 例： `Router(config-xconnect)# member pseudowire 100`	Layer 2 VPN（L2VPN）クロス コネクトを形成するようにメンバー擬似回線を指定します。
ステップ 18	**member gigabitethernet***interface-number* 例： `Router(config-xconnect)# member GigabitEthernet0/0/0.1`	ギガビット イーサネット メンバー インターフェイスのロケーションを指定します。

	コマンドまたはアクション	目的
ステップ 19	**end** 例： `Router(config-xconnect)# end`	特権 EXEC モードに戻ります。
ステップ 20	**pvc***vpi*/*vci***l2transport** 例： `Device(config-subif)# pvc 10/100 l2transport`	VPI と仮想チャネル識別子（VCI）を割り当てます。
ステップ 21	設定する PVC の数だけステップ 12 を繰り返します。	—
ステップ 22	**end** 例： `Device(config-subif)# end`	サブ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て、特権 EXEC モードに戻ります。

一意でない VPI を含む PWE への N:1 PVC マッピングの設定例

例：一意でない VPI を含む PWE への N:1 PVC マッピングの設定

次に、一意でない VPI を使用した ATM 相手先固定接続（PVC）から擬似回線への N:1 マッピングを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface atm 9/1/1
Device(config-if)# atm mcpt-timers 500 5000 50000
Device(config-if)# exit
Device# configure terminal
Device(config)# interface atm 9/1/1.1 multipoint
Device(config-subif)# no ip address
Device(config-subif)# atm enable-ilmi-trap
Device(config-subif)# cell packing 20 mcpt-timer 2
Device(config-subif)# xconnect 10.1.1.1 100 encapsulation mpls
Device(config-subif)# pvc 10/100 l2transport
Device(config-subif)# pvc 11/122 l2transport
Device(config-subif)# pvc 19/231 l2transport
Device(config-subif)# end
```

例：一意でない VPI を使用した PVC から PWE への N:1 マッピングの設定（L2VPN プロトコルベース CLI 機能に関連するコマンドを使用）

次に、一意でない VPI を使用した ATM 相手先固定接続（PVC）から擬似回線への N:1 マッピングを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface atm 9/1/1
Device(config-if)# atm mcpt-timers 500 5000 50000
Device(config-if)# exit
Device(config)# configure terminal
Device(config)# interface atm 9/1/1.1 multipoint
Device(config-subif)# no ip address
Device(config-subif)# atm enable-ilmi-trap
Device(config-subif)# cell packing 20 mcpt-timer 2
Device(config-subif)# exit
Device(config)#interface pseudowire 100
Device(config-if)#encapsulation mpls
Device(config-if)#neighbor 10.1.1.1 100
Device(config-if)# pvc 10/100 l2transport
Device(config-if)# pvc 11/122 l2transport
Device(config-if)# pvc 19/231 l2transport
Device(config-if)# exit
Device(config)#l2vpn xconnect context A
Router(config-xconnect)#member pseudowire 100
Device(config-xconnect)#member atm 9/1/1
Device(config-xconnect)# end
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List』
ATM コマンド	『Asynchronous Transfer Mode Command Reference』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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。	http://www.cisco.com/cisco/web/support/index.html

一意でない VPI を使用した PVC から PWE への N:1 マッピングに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、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。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *38*：一意でない *VPI* を使用した *PVC* から *PWE* への *N:1* マッピングに関する機能情報

機能名	リリース	機能情報
一意でない VPI を使用した PVC から PWE への N:1 マッピング	Cisco IOS XE Release 3.7S	一意でない VPI を使用した PVC から PWE への N:1 マッピング機能は、1 つ以上の ATM PVC を 1 つの擬似回線にマッピングします。Cisco IOS XE Release 3.7S では、Cisco ASR 903 ルータのサポートが追加されました。 この機能により、**fast-flood** コマンドが導入されました。

第 24 章

VFI 擬似回線の QoS ポリシー

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース 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、機能情報の表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シスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

VFI 擬似回線の QoS ポリシーの制約事項

- 擬似回線の最大数は 32000 です。
- 固有ポリシー マップの最大数は 4000 です。
- VFI コンテキストあたりのネイバーの最大数は 128 です。

VFI 擬似回線の QoS ポリシーに関する情報

VFI 擬似回線の QoS ポリシー

QoS ポリシーは個々の擬似回線インターフェイスで指定され、対応する擬似回線にのみ適用されます。同じ仮想転送インターフェイス（VFI）の異なる擬似回線メンバーまたは擬似回線のサブセットに異なる QoS ポリシーを指定することができます。VFI ごとに 1 つ以上の擬似回線が設定される場合があります。手動設定または自動検出の擬似回線設定がサポートされます。

QoS ポリシーは、擬似回線テンプレートを使用して指定します。テンプレートは、同じ VFI または異なる VFI の複数の擬似回線に適用できます。これらの擬似回線はすべて、テンプレートで指定される同じ QoS ポリシーが適用されます。自動検出される擬似回線では、擬似回線テンプレートでしか QoS ポリシーを指定できません。

VFI 擬似回線機能の QoS ポリシーは、入出力両方のポリシーをサポートし、トラフィックの分類は異なる一致基準に基づいて実行できます。

VFI 擬似回線の QoS ポリシーの設定方法

擬似回線用の QoS ポリシーの設定

擬似回線用の QoS ポリシーを設定するには、次のタスクを実行します。

はじめる前に

手順の概要

1. イネーブル化
2. **configureterminal**
3. **policy-map***policy-map-name*
4. **class***class-map-name*
5. **priority***bandwidth-kbps*
6. **exit**
7. **class***class-map-name*
8. **bandwidthpercent***percentage*
9. **exit**
10. **class***class-map-name*
11. **policecir***bps*
12. **exit**
13. **class***class-map-name*
14. **shapeaverage***bps*
15. **queue-limit***queue-limit size***packets**
16. **random-detect**
17. **exit**
18. **exit**
19. **policy-map***policy-map-name*
20. **class***class-map-name*
21. **shapeaverage***bps*
22. **service-policy***policy-map*
23. **exit**
24. **exit**
25. **policy-map***policy-map-name*
26. **class***class-map-name*
27. **shapeaverage***bps*
28. **exit**
29. **exit**
30. **policy-map***policy-map-name*
31. **class***class-map-name*
32. **shapeaverage***bps*
33. **exit**
34. **exit**
35. **exitpolicy-map***policy-map-name*
36. **class***class-map-name*
37. **shapeaverage***bps*
38. **exit**
39. **exit**

40. **policy-map***policy-map-name*
41. **class***class-map-name*
42. **police***bps*
43. **interfacepseudowire***number*
44. **encapmpls**
45. **neighbor***peer-addressvcid-value*
46. **service-policyinput***policy-map-name*
47. **service-policyoutput***policy-map-name*
48. **interfacegigabit ethernet***number*
49. **service-policyoutput***policy-map-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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 （注） パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**policy-map***policy-map-name* 例： `Device# policy-map gold-policy-child`	サービス ポリシーを指定するポリシー マップを作成します。
ステップ 4	**class***class-map-name* 例： `Device(config-pmap)# class priority-class`	クラス マップの名前を指定します。
ステップ 5	**priority***bandwidth-kbps* 例： `Device(config-pmap-c)# priority 100`	ポリシー マップに属するトラフィックのクラスにプライオリティを与えます。

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `Device(config-pmap-c)# exit`	ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 7	**class***class-map-name* 例： `Device(config-pmap-c)# class guarantee-class`	クラス マップの名前を指定します。
ステップ 8	**bandwidthpercent***percentage* 例： `Device(config-pmap-c)# bandwidth percent 50`	ポリシー マップに属するクラスに割り当てる帯域幅を指定または変更します。
ステップ 9	**exit** 例： `Device(config-pmap-c)# exit`	ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 10	**class***class-map-name* 例： `Device(config-pmap-c)# class limited-class`	クラス マップの名前を指定します。
ステップ 11	**policecir***bps* 例： `Device(config-pmap-c)# police cir 8000`	インターフェイス別のポリサーを作成して、それを使用するようにポリシーマップ クラスを設定します。
ステップ 12	**exit** 例： `Device(config-pmap-c)# exit`	ポリシーマップ クラス 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	**class***class-map-name* 例： `Device(config-pmap)# class class-default`	クラス マップの名前を指定します。

	コマンドまたはアクション	目的
ステップ 14	**shapeaverage***bps* 例： `Device(config-pmap-c)# shape average 8000`	表示されたビット レートにトラフィックをシェーピングします。
ステップ 15	**queue-limit***queue-limit size***packets** 例： `Device(config-pmap-c)# queue-limit 150 packets`	クラスのキュー制限サイズを指定します。
ステップ 16	**random-detect** 例： `Device(config-pmap-c)# andom-detect`	ポリシー マップ内のクラスの重み付けランダム早期検出（WRED）を設定します。
ステップ 17	**exit** 例： `Device(config-pmap-c)# exit`	ポリシーマップ クラス 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	**exit** 例： `Device(config-pmap)# exit`	ポリシーマップ コンフィギュレーション モードを終了します。
ステップ 19	**policy-map***policy-map-name* 例： `Device(config)# policy-map gold-policy-hqos`	サービス ポリシーを指定するポリシー マップを作成します。
ステップ 20	**class***class-map-name* 例： `Device(config-pmap)# class class-default`	クラス マップの名前を指定します。
ステップ 21	**shapeaverage***bps* 例： `Device(config-pmap-c)# shape average 10000`	表示されたビット レートにトラフィックをシェーピングします。

	コマンドまたはアクション	目的
ステップ 22	**service-policy***policy-map* 例： `Device(config-pmap-c)# service-policy gold-policy-child`	ポリシー マップをクラスに結合します。
ステップ 23	**exit** 例： `Device(config-pmap-c)# exit`	ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 24	**exit** 例： `Device(config-pmap)# exit`	ポリシーマップ コンフィギュレーション モードを終了します。
ステップ 25	**policy-map***policy-map-name* 例： `Device(config)# policy-map pw-shaper`	サービス ポリシーを指定するポリシー マップを作成します。
ステップ 26	**class***class-map-name* 例： `Device(config-pmap)#class class-default`	クラス マップの名前を指定します。
ステップ 27	**shapeaverage***bps* 例： `Device(config-pmap-c)#shape average 20000`	表示されたビット レートにトラフィックをシェーピングします。
ステップ 28	**exit** 例： `Device(config-pmap-c)#exit`	ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 29	**exit** 例： `Device(config-pmap)#exit`	ポリシーマップ コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 30	**policy-map***policy-map-name* 例： `Device(config)# policy-map sub-ifc-shaper`	サービス ポリシーを指定するポリシー マップを作成します。
ステップ 31	**class***class-map-name* 例： `Device(config-pmap)#class class-default`	クラス マップの名前を指定します。
ステップ 32	**shapeaverage***bps* 例： `Device(config-pmap-c)#shape average 40000`	表示されたビット レートにトラフィックをシェーピングします。
ステップ 33	**exit** 例： `Device(config-pmap-c)#exit`	ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 34	**exit** 例： `Device(config-pmap)#exit`	ポリシーマップ コンフィギュレーション モードを終了します。
ステップ 35	**exitpolicy-map***policy-map-name* 例： `Device(config)# policy-map port-shaper`	サービス ポリシーを指定するポリシー マップを作成します。
ステップ 36	**class***class-map-name* 例： `Device(config-pmap)#class class-default`	クラス マップの名前を指定します。
ステップ 37	**shapeaverage***bps* 例： `Device(config-pmap-c)#shape average 60000`	表示されたビット レートにトラフィックをシェーピングします。

	コマンドまたはアクション	目的
ステップ 38	**exit** 例： `Device(config-pmap-c)#exit`	ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 39	**exit** 例： `Device(config-pmap)#exit`	ポリシーマップ コンフィギュレーション モードを終了します。
ステップ 40	**policy-map***policy-map-name* 例： `Device(config)# policy-map ingress-police`	サービス ポリシーを指定するポリシーマップを作成します。
ステップ 41	**class***class-map-name* 例： `Device(config-pmap)# class class-default`	
ステップ 42	**police***bps* 例： `Device(config-pmap-c)# police 10000`	インターフェイス別のポリサーを作成して、それを使用するようにポリシーマップ クラスを設定します。
ステップ 43	**interfacepseudowire***number* 例： `Device(config-pmap-c-police)# interface pseudowire 1`	インターフェイス タイプを設定し、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 44	**encapmpls** 例： `Device(config-if)# encap mpls`	MPLS カプセル化を設定します。
ステップ 45	**neighbor***peer-addressvcid-value* 例： `Device(config-if)# neighbor 10.0.0.1 100`	L2VPN 擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。

	コマンドまたはアクション	目的
ステップ 46	**service-policyinput***policy-map-name* 例： `Device(config-if)# service-policy input ingress-policy`	ポリシーマップを入力インターフェイスにアタッチします。
ステップ 47	**service-policyoutput***policy-map-name* 例： `Device(config-if)# service-policy output gold-policy-hqos`	ポリシーマップを出力インターフェイスに付加します。
ステップ 48	**interfacegigabit ethernet***number* 例： `Device(config-if)# interface gigabitethernet 1/1/0`	インターフェイス タイプを設定します。
ステップ 49	**service-policyoutput***policy-map-name* 例： `Device(config-if)# service-policy output port-shaper`	ポリシーマップを出力インターフェイスに付加します。

VFI 擬似回線用の階層型ポリシーの作成

VFI 擬似回線用の階層型ポリシーを作成するには、次のタスクを実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **policy-map***policy-map-name*
4. **class***class-map-name*
5. **shapeaverage***bps*
6. **service-policy***policy-map*
7. **exit**
8. **exit**
9. **policy-map***policy-map-name*
10. **class***class-map-name*
11. **shapeaverage***bps*
12. **exit**
13. **exit**
14. **policy-map***policy-map-name*
15. **class***class-map-name*
16. **shapeaverage***bps*
17. **exit**
18. **exit**
19. **exitpolicy-map***policy-map-name*
20. **class***class-map-name*
21. **shapeaverage***bps*
22. **exit**
23. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 （注） パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 3	**policy-map***policy-map-name* 例： `Device(config)# policy-map gold-policy-hqos`	サービス ポリシーを指定するポリシー マップを作成します。
ステップ 4	**class***class-map-name* 例： `Device(config-pmap)# class class-default`	クラス マップの名前を指定します。
ステップ 5	**shapeaverage***bps* 例： `Device(config-pmap-c)# shape average 10000`	表示されたビット レートにトラフィックをシェーピングします。
ステップ 6	**service-policy***policy-map* 例： `Device(config-pmap-c)# service-policy gold-policy-child`	ポリシー マップをクラスに結合します。
ステップ 7	**exit** 例： `Device(config-pmap-c)# exit`	ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 8	**exit** 例： `Device(config-pmap)# exit`	ポリシーマップ コンフィギュレーション モードを終了します。
ステップ 9	**policy-map***policy-map-name* 例： `Device(config)# policy-map pw-shaper`	サービス ポリシーを指定するポリシー マップを作成します。
ステップ 10	**class***class-map-name* 例： `Device(config-pmap)# class class-default`	クラス マップの名前を指定します。

	コマンドまたはアクション	目的
ステップ 11	**shapeaverage***bps* 例： `Device(config-pmap-c)# shape average 20000`	表示されたビット レートにトラフィックをシェーピングします。
ステップ 12	**exit** 例： `Device(config-pmap-c)# exit`	ポリシーマップ クラス 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	**exit** 例： `Device(config-pmap)# exit`	ポリシーマップ コンフィギュレーション モードを終了します。
ステップ 14	**policy-map***policy-map-name* 例： `Device(config)# policy-map sub-ifc-shaper`	サービス ポリシーを指定するポリシー マップを作成します。
ステップ 15	**class***class-map-name* 例： `Device(config-pmap)# class class-default`	クラス マップの名前を指定します。
ステップ 16	**shapeaverage***bps* 例： `Device(config-pmap-c)# shape average 40000`	表示されたビット レートにトラフィックをシェーピングします。
ステップ 17	**exit** 例： `Device(config-pmap-c)# exit`	ポリシーマップ クラス 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	**exit** 例： `Device(config-pmap)# exit`	ポリシーマップ コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 19	**exitpolicy-map***policy-map-name* 例： `Device(config)# policy-map port-shaper`	サービス ポリシーを指定するポリシー マップを作成します。
ステップ 20	**class***class-map-name* 例： `Device(config-pmap)# class class-default`	クラス マップの名前を指定します。
ステップ 21	**shapeaverage***bps* 例： `Device(config-pmap-c)# shape average 60000`	表示されたビット レートにトラフィックをシェーピングします。
ステップ 22	**exit** 例： `Device(config-pmap-c)# exit`	ポリシーマップ クラス 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	**exit** 例： `Device(config-pmap)# exit`	ポリシーマップ コンフィギュレーション モードを終了します。

VFI 擬似回線へのポリシー マップの付加

VFI 擬似回線にポリシー マップを付加するには、次の作業を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **policy-map***policy-map-name*
4. **class***class-map-name*
5. **police***bps*
6. **interfacepseudowire***number*
7. **encapmpls**
8. **neighbor***peer-addressvcid-value*
9. **service-policyinput***policy-map-name*
10. **service-policyoutput***policy-map-name*
11. **interfacegigabit ethernet***number*
12. **service-policyoutput***policy-map-name*
13. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 （注） パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**policy-map***policy-map-name* 例： `Device# policy-map ingress-police`	サービス ポリシーを指定するポリシー マップを作成します。
ステップ 4	**class***class-map-name* 例： `Device(config-pmap)# class class-default`	クラス マップの名前を指定します。

	コマンドまたはアクション	目的
ステップ 5	**police***bps* 例： `Device(config-pmap-c)# police 10000`	インターフェイス別のポリサーを作成して、それを使用するようにポリシーマップクラスを設定します。
ステップ 6	**interfacepseudowire***number* 例： `Device(config-pmap-c-police)# interface pseudowire 1`	インターフェイスタイプを設定し、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 7	**encapmpls** 例： `Device(config-if)# encap mpls`	MPLS カプセル化を設定します。
ステップ 8	**neighbor***peer-addressvcid-value* 例： `Device(config-if)# neighbor 10.0.0.1 100`	L2VPN 擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 9	**service-policyinput***policy-map-name* 例： `Device(config-if)# service-policy input ingress-policy`	ポリシーマップを入力インターフェイスにアタッチします。
ステップ 10	**service-policyoutput***policy-map-name* 例： `Device(config-if)# service-policy output gold-policy-hqos`	ポリシーマップを出力インターフェイスに付加します。
ステップ 11	**interfacegigabit ethernet***number* 例： `Device(config-if)# interface gigabit ethernet 1/1/0`	インターフェイス タイプを設定します。
ステップ 12	**service-policyoutput***policy-map-name* 例： `Device(config-if)# service-policy output port-shaper`	ポリシーマップを出力インターフェイスに付加します。

	コマンドまたはアクション	目的
ステップ 13	**exit** 例： `Device(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ます。

QoS ポリシーが異なる 2 つの擬似回線メンバーからなる VFI の設定

QoS ポリシーが異なる 2 つの擬似回線メンバーで VFI を設定するには、次のタスクを実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfacepseudowire***number*
4. **encapmpls**
5. **neighbor***peer-addressvcid value*
6. **service-policyoutput***policy-map-name*
7. **interfacepseudowire***number*
8. **encapmpls**
9. **neighbor***peer-addressvcid value*
10. **service-policyoutput***policy-map-name*
11. **l2vpnvficontext***name*
12. **vpnid***vpn-id*
13. **memberpseudowire***pw-int-number*
14. **memberpseudowire***pw-int-number*
15. **bridge-domain***bridge-domain-id*
16. **member***interface-type-number*
17. **interfaceBDI***number*
18. **ipvrfforwarding***vrf-name*
19. **ipaddress***ip-addressmask*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Device> enable`	（注） パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**interfacepseudowire***number* 例： `Device# interface pseudowire 1`	インターフェイス タイプを設定し、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	**encapmpls** 例： `Device(config-if)# encap mpls`	MPLS カプセル化を設定します。
ステップ 5	**neighbor***peer-addressvcid value* 例： `Device(config-if)# neighbor 10.0.0.1 100`	L2VPN 擬似回線のピア IP アドレスと仮想回線（VC）ID 値を指定します。
ステップ 6	**service-policyoutput***policy-map-name* 例： `Device(config-if)# service-policy output gold-policy`	ポリシー マップを出力インターフェイスに付加します。
ステップ 7	**interfacepseudowire***number* 例： `Device(config-if)# interface pseudowire 2`	インターフェイス タイプを設定します。
ステップ 8	**encapmpls** 例： `Device(config-if)# encap mpls`	MPLS カプセル化を設定します。

	コマンドまたはアクション	目的
ステップ 9	**neighbor***peer-addressvcid value* 例： `Device(config-if)# neighbor 20.0.0.1 100`	L2VPN 擬似回線のピア IP アドレスと VCID を指定します。
ステップ 10	**service-policyoutput***policy-map-name* 例： `Device(config-if)# service-policy output silver-policy`	ポリシー マップを出力インターフェイスに付加します。
ステップ 11	**l2vpnvficontext***name* 例： `Device(config-if)# l2vpn vfi context my-vfi`	複数の異なるネットワーク間の Layer 2 VPN（L2VPN）Virtual Forwarding Interface（VFI）を確立します。
ステップ 12	**vpnid***vpn-id* 例： `Device(config-vfi)# vpn id 100`	仮想プライベート LAN サービス（VPLS）インスタンス上で VPN ID を設定します。
ステップ 13	**memberpseudowire***pw-int-number* 例： `Device(config-vfi)# member pseudowire 1`	ポイントツーポイント Layer 2 VPN（L2VPN）Virtual Forwarding Interface（VFI）接続を形成するデバイスを指定します。
ステップ 14	**memberpseudowire***pw-int-number* 例： `Device(config-vfi)# member pseudowire 2`	ポイントツーポイント Layer 2 VPN（L2VPN）Virtual Forwarding Interface（VFI）接続を形成するデバイスを指定します。
ステップ 15	**bridge-domain***bridge-domain-id* 例： `Device(config-vfi)# bridge-domain 100`	ブリッジドメイン上のコンポーネントを設定します。
ステップ 16	**member***interface-type-number* 例： `Device(config-bdomain)# member vfi my-vfi`	サービスインスタンスをブリッジドメインインスタンスにバインドします。

	コマンドまたはアクション	目的
ステップ 17	**interfaceBDI***number* 例： `Device(config-bdomain)# interface BDI 100`	インターフェイス タイプを設定し、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 18	**ipvrfforwarding***vrf-name* 例： `Device(config-if)# ip vrf forwarding MY-VRF`	バーチャル プライベート ネットワーク（VPN）ルーティングおよび転送（VRF）インスタンスをインターフェイスまたはサブインターフェイスに関連付けます。
ステップ 19	**ipaddress***ip-addressmask* 例： `Device(config-if)# ip address 30.0.0.1 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。

QoS ポリシーが同一の 2 つの擬似回線メンバーからなる VFI の設定

QoS ポリシーが同じ 2 つの擬似回線メンバーで VFI を設定するには、次のタスクを実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **templatetypepseudowire***name*
4. **encapmpls**
5. **service-policyoutput***policy-map-name*
6. **interfacepseudowire***number*
7. **encapmpls**
8. **neighbor***peer-addressvcid value*
9. **sourcetemplatetypepseudowire***template-name*
10. **interfacepseudowire***number*
11. **encapmpls**
12. **neighbor***peer-addressvcid value*
13. **sourcetemplatetypepseudowire***template-name*
14. **l2vpnvficontext***name*
15. **vpnid***vpn-id*
16. **memberpseudowire***pw-int-number*
17. **memberpseudowire***pw-int-number*
18. **bridge-domain***bridge-domain-id*
19. **member***interface-type-number*
20. **interfaceBDI***number*
21. **ipvrfforwarding***vrf-name*
22. **ipaddress***ip-addressmask*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 （注） パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 3	**templatetypepseudowire***name* 例： `Device(config)# template type pseudowire my_template`	テンプレートを設定します。
ステップ 4	**encapmpls** 例： `Device(config-if)# encap mpls`	MPLS カプセル化を設定します。
ステップ 5	**service-policyoutput***policy-map-name* 例： `Device(config-template)# service-policy output common-policy`	ポリシー マップを出力インターフェイスにアタッチします。
ステップ 6	**interfacepseudowire***number* 例： `Device(config-if)# interface pseudowire 1`	インターフェイス タイプを設定します。
ステップ 7	**encapmpls** 例： `Device(config-if)# encap mpls`	MPLS カプセル化を設定します。
ステップ 8	**neighbor***peer-addressvcid value* 例： `Device(config-if)# neighbor 10.0.0.1 100`	L2VPN 擬似回線のピア IP アドレスと VCID を指定します。
ステップ 9	**sourcetemplatetypepseudowire***template-name* 例： `Device(config-if)# source template type pseudowire my_template`	タイプ擬似回線のソース テンプレートの名前を設定します。
ステップ 10	**interfacepseudowire***number* 例： `Device(config-if)# interface pseudowire 2`	インターフェイス タイプを設定します。

	コマンドまたはアクション	目的
ステップ 11	**encapmpls** 例： `Device(config-if)# encap mpls`	MPLS カプセル化を設定します。
ステップ 12	**neighbor***peer-addressvcid value* 例： `Device(config-if)# neighbor 20.0.0.1 100`	L2VPN 擬似回線のピア IP アドレスと VCID を指定します。
ステップ 13	**sourcetemplatetypepseudowire***template-name* 例： `Device(config-if)# source template type pseudowire my_template`	タイプ擬似回線のソース テンプレートの名前を設定します。
ステップ 14	**l2vpnvficontext***name* 例： `Device(config-if)# l2vpn vfi context my-vfi`	複数の異なるネットワーク間の Layer 2 VPN（L2VPN）Virtual Forwarding Interface（VFI）を確立します。
ステップ 15	**vpnid***vpn-id* 例： `Device(config-vfi)# vpn id 100`	仮想プライベート LAN サービス（VPLS）インスタンス上で VPN ID を設定します。
ステップ 16	**memberpseudowire***pw-int-number* 例： `Device(config-vfi)# member pseudowire 1`	ポイントツーポイント Layer 2 VPN（L2VPN）Virtual Forwarding Interface（VFI）接続を形成するデバイスを指定します。
ステップ 17	**memberpseudowire***pw-int-number* 例： `Device(config-vfi)# member pseudowire 2`	ポイントツーポイント Layer 2 VPN（L2VPN）Virtual Forwarding Interface（VFI）接続を形成するデバイスを指定します。
ステップ 18	**bridge-domain***bridge-domain-id* 例： `Device(config-vfi)# bridge-domain 100`	ブリッジ ドメイン上のコンポーネントを設定します。
ステップ 19	**member***interface-type-number* 例： `Device(config-bdomain)# member vfi my-vfi`	サービス インスタンスをブリッジ ドメイン インスタンスにバインドします。

	コマンドまたはアクション	目的
ステップ 20	**interfaceBDI***number* 例： `Device(config-bdomain)# interface BDI 100`	インターフェイス タイプを設定し、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 21	**ipvrfforwarding***vrf-name* 例： `Device(config-if)# ip vrf forwarding MY-VRF`	バーチャル プライベート ネットワーク（VPN）ルーティングおよび転送（VRF）インスタンスをインターフェイスまたはサブインターフェイスに関連付けます。
ステップ 22	**ipaddress***ip-addressmask* 例： `Device(config-if)# ip address 30.0.0.1 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。

自動検出された擬似回線からなる VFI の設定

擬似回線が自動検出される VFI を設定するには、次のタスクを実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **templatetypepseudowire***name*
4. **encapmpls**
5. **service-policyoutput***policy-map-name*
6. **l2vpnvficontext***name*
7. **vpnid***vpn-id*
8. **autodiscoverybgpsignalingldptemplate***template-name*
9. **bridge-domain***bridge-domain-id*
10. **member***interface-type-number*
11. **interfaceBDI***number*
12. **ipvrfforwarding***vrf-name*
13. **ipaddress***ip-addressmask*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 （注） パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**templatetypepseudowire***name* 例： `Device(config)# template type pseudowire my_template`	テンプレートを設定します。
ステップ 4	**encapmpls** 例： `Device(config-if)# encap mpls`	MPLS カプセル化を設定します。
ステップ 5	**service-policyoutput***policy-map-name* 例： `Device(config-template)# service-policy output common-policy`	ポリシーマップを出力インターフェイスにアタッチします。
ステップ 6	**l2vpnvficontext***name* 例： `Device(config-if)# l2vpn vfi context my-vfi`	複数の異なるネットワーク間の Layer 2 VPN（L2VPN）Virtual Forwarding Interface（VFI）を確立します。
ステップ 7	**vpnid***vpn-id* 例： `Device(config-vfi)# vpn id 100`	仮想プライベート LAN サービス（VPLS）インスタンス上で VPN ID を設定します。
ステップ 8	**autodiscoverybgpsignalingldptemplate***template-name* 例： `Device(config-vfi)# autodiscovery bgp signaling ldp template my_template`	ラベル配布プロトコル（LDP）で擬似回線メンバーが自動検出されるように Layer 2 Virtual Forwarding Interface（VFI）を指定します。

	コマンドまたはアクション	目的
ステップ 9	**bridge-domain***bridge-domain-id* 例： `Device(config-vfi)# bridge-domain 100`	ブリッジ ドメイン上のコンポーネントを設定します。
ステップ 10	**member***interface-type-number* 例： `Device(config-bdomain)# member vfi my-vfi`	サービスインスタンスをブリッジ ドメインインスタンスにバインドします。
ステップ 11	**interfaceBDI***number* 例： `Device(config-bdomain)# interface BDI 100`	インターフェイスタイプを設定し、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 12	**ipvrfforwarding***vrf-name* 例： `Device(config-if)# ip vrf forwarding MY-VRF`	バーチャル プライベート ネットワーク（VPN）ルーティングおよび転送（VRF）インスタンスをインターフェイスまたはサブインターフェイスに関連付けます。
ステップ 13	**ipaddress***ip-addressmask* 例： `Device(config-if)# ip address 30.0.0.1 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。

VFI 擬似回線の QoS ポリシーの設定例

例：擬似回線の QoS ポリシーの設定

次に、擬似回線の QoS ポリシーを設定する例を示します。

```
Device(config)# policy-map GOLD-POLICY-CHILD
Device(config-pmap)# class PRIORITY-CLASS
Device(config-pmap-c)# priority 100
Device(config-pmap-c)# exit
Device(config-pmap)# class GUARANTEE-CLASS
Device(config-pmap-c)# bandwidth 1000
Device(config-pmap-c)# exit
Device(config-pmap)# class LIMITED-CLASS
Device(config-pmap-c)# police cir 8000
Device(config-pmap-c-police)# class class-default
Device(config-pmap-c)# shape average 8000
Device(config-pmap-c)# queue-limit 150
```

```
Device(config-pmap-c)# random-detect
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# policy-map GOLD-POLICY-HQOS
Device(config-pmap)# class class-default
Device(config-pmap-c)# shape average 8000
Device(config-pmap-c)# service-policy GOLD-POLICY-CHILD
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# policy-map PW-SHAPER
Device(config-pmap)# class class-default
Device(config-pmap-c)# shape average 8000
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# policy-map SUB-IFC-SHAPER
Device(config-pmap)# class class-default
Device(config-pmap-c)# shape average 10000
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# policy-map PORT-SHAPER
Device(config-pmap)# class class-default
Device(config-pmap-c)# shape average 20000
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# policy-map INGRESS-POLICE
Device(config-pmap)# class class-default
Device(config-pmap-c)# police 10000
Device(config-pmap-c-police)# interface pseudowire 1
Line protocol on Interface pseudowire0, changed state to up
Device(config-if)# encap mpls
Device(config-if)# neighbor 10.0.0.1 100
Device(config-if)# service-policy input INGRESS-POLICY
Device(config-if)# service-policy output GOLD-POLICY-HQOS
Device(config-if)# interface GigabitEthernet 1/1/0
--- Pseudowire is going out through this interface
Device(config-if)# service-policy output PORT-SHAPER
```

例：QoS ポリシーが異なる 2 つの擬似回線メンバーからなる VFI の設定

次に、QoS ポリシーが異なる 2 つの擬似回線メンバーからなる VFI を設定する例を示します。

```
Device(config)# interface pseudowire1
Line protocol on Interface pseudowire0, changed state to up
Device(config-if)# encap mpls
Device(config-if)# neighbor 10.0.0.1 100
Device(config-if)# service-policy output GOLD-POLICY
Device(config-if)# interface pseudowire2
Device(config-if)# encap mpls
Device(config-if)# neighbor 20.0.0.1 100
Device(config-if)# service-policy output SILVER-POLICY
Device(config-if)# l2vpn vfi context MY-VFI
Device(config-vfi)# vpn id 100
Device(config-vfi)# member pseudowire1
Device(config-vfi)# member pseudowire2
Device(config-vfi)# bridge-domain 100
Device(config-bdomain)# member vfi MY-VFI
STATUS_CHANGED: Status of VFI my-vfi changed from DOWN to UP
Device(config-bdomain)# interface BDI 100
Device(config-if)# ip vrf forwarding MY-VRF
Device(config-if)# ip address 30.0.0.1 255.255.255.0
```

例：QoS ポリシーが同一の 2 つの擬似回線メンバーからなる VFI の設定

次に、QoS ポリシーが同一の 2 つの擬似回線メンバーからなる VFI を設定する例を示します。

```
Device(config)# template type pseudowire MY_TEMPLATE
Device(config-template)# encapsulation mpls
Device(config-template)# service-policy output COMMON-POLICY
Device(config-template)# interface pseudowire1
Line protocol on Interface pseudowire0, changed state to up
Device(config-if)# encap mpls
Device(config-if)# neighbor 10.0.0.1 100
Device(config-if)# source template type pseudowire MY_TEMPLATE
Device(config-if)# interface pseudowire2
Device(config-if)# encap mpls
Device(config-if)# neighbor 20.0.0.1 100
Device(config-if)# source template type pseudowire MY_TEMPLATE
Device(config-if)# l2vpn vfi context MY-VFI
Device(config-vfi)# vpn id 100
Device(config-vfi)# member pseudowire1
Device(config-vfi)# member pseudowire2
Device(config-vfi)# bridge-domain 100
Device(config-bdomain)# member vfi MY-VFI
Status of VFI my-vfi changed from DOWN to UP
Device(config-bdomain)# interface BDI 100
Device(config-if)# ip vrf forwarding MY-VRF
Device(config-if)# ip address 30.0.0.1 255.255.255.0
```

例：自動検出された擬似回線からなる VFI の設定

次に、自動検出された擬似回線からなる VFI を設定する例を示します。

```
Device(config)# template type pseudowire MY_TEMPLATE
Device(config-template)# encapsulation mpls
Device(config-template)# service-policy output COMMON-POLICY
Device(config-template)# l2vpn vfi context MY-VFI
Device(config-vfi)# vpn id 100
Line protocol on Interface pseudowire0, changed state to up
Device(config-vfi)# autodiscovery bgp signaling ldp template MY_TEMPLATE
Device(config-vfi-autodiscovery)# bridge-domain 100
Device(config-bdomain)# member vfi MY-VFI
Status of VFI my-vfi changed from DOWN to UP
Device(config-bdomain)# interface BDI 100
Device(config-if)# ip vrf forwarding MY-VRF
Device(config-if)# ip address 30.0.0.1 255.255.255.0
```

例：擬似回線ポリシー マップ情報の表示

次に、**show policy-map interface** コマンドの出力例を示します。この出力には、擬似回線 2 インターフェイスに対応して設定されたクラス マップとポリシー マップが表示されています。

```
Device#show policy-map interface pseudowire2
 pseudowire2

 Service-policy output: pw_brr

    Class-map: prec1 (match-all)
      0 packets, 0 bytes
```

```
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: ip precedence 1
      Queueing
      queue limit 4166 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 1

    Class-map: prec2 (match-all)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: ip precedence 2
      Queueing
      queue limit 4166 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 2

    Class-map: prec3 (match-all)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: ip precedence 3
      Queueing
      queue limit 4166 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 3

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: any
      Queueing
      queue limit 4166 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 4
Device#
```

VFI 擬似回線の QoS ポリシーに関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
MPLS コマンド	『*Cisco IOS Multiprotocol Label Switching Command Reference*』
QoS コマンド	『*Cisco IOS Quality of Service Solutions Command Reference*』
擬似回線クラスの設定	「Any Transport over MPLS」

関連項目	マニュアル タイトル
レイヤ 2 VPN	• Any Transport over MPLS • L2VPN 擬似回線スイッチング • MPLS LSP Ping/Traceroute for LDP/TE および LSP Ping for VCCV
L2VPN 擬似回線	• L2VPN 擬似回線冗長性 • MPLS 擬似回線ステータス シグナリング

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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。	http://www.cisco.com/cisco/web/support/index.html

VFI 擬似回線の QoS ポリシーの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、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。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *39*：*VFI* 擬似回線の *QoS* ポリシーの機能情報

機能名	リリース	機能情報
VFI 擬似回線の QoS ポリシー	Cisco IOS XE 3.8S	この機能により、VFI擬似回線メンバーに使用する QoS クラスとポリシーを設定できます。 次のコマンドが導入または変更されました：**show policy-map interface**。

第 25 章

VPLS BGP シグナリング L2VPN Inter-AS オプション A

仮想プライベート LAN スイッチング（VPLS）ボーダー ゲートウェイ プロトコル（BGP）シグナリング レイヤ 2 バーチャル プライベート ネットワーク（L2VPN）機能は、BGP を使用した VPLS インスタンスにおける既知のすべての PE デバイスの自動検出およびシグナリングを簡素化します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース 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、機能情報の表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シスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

VPLS BGP シグナリング L2VPN Inter-AS オプション A の前提条件

- VPLS BGP シグナリングのために、擬似回線クラスで **no control-word** コマンドを使用してコントロール ワードをオフにする必要があります。次に例を示します。

```
Router> enable
Router# configure terminal
Router(config)# pseudowire-class my_pw_class
Router(config-pw-class)# no control-word
```

- VPLS ドメイン内のすべての仮想転送インスタンス（VFI）で、ルート識別子（RD）が一致している必要があります。

VPLS BGP シグナリング L2VPN Inter-AS オプション A に関する情報

VPLS の BGP 自動検出とシグナリング

仮想プライベート LAN スイッチング（VPLS）コントロール プレーンが、自動検出とシグナリングに使用されます。自動検出には、特定の VPLS インスタンスに参加するすべてのプロバイダー エッジ（PE）デバイスの場所を特定することが含まれます。シグナリングは、VPLS インスタンスの擬似回線を設定することにより実現されます。VPLS BGP シグナリング L2VPN Inter-AS オプション B 機能が導入される前は、RFC 6074 で指定されているように、シグナリングには Label Distribution Protocol（LDP）が使用され、自動検出には Border Gateway Protocol（BGP）が使用されていました。VPLS BGP シグナリング L2VPN Inter-As オプション B 機能の導入により、VPLS BGP シグナリング L2VPN 機能は両方の機能に BGP を使用することで、VPLS インスタンス内のすべての既知の PE デバイスの自動検出とシグナリングを簡素化しつつ RFC 4761 をサポートします。自動検出は、VPLS インスタンスごとに定義されます。

内部 BGP（IBGP）ピアは、自動検出とシグナリングの両方を実行するために、L2VPN アドレス ファミリ識別子（AFI）と L2VPN 情報を持つ後続のアドレス ファミリ識別子（SAFI）の数の更新メッセージを交換します。これにはネットワーク層到達可能性情報（NLRI）が含まれます。

VPLS の自動検出プロトコルのための両方の BGP 標準規格（RFC 6074 および RFC 4761）は、同じ BGP AFI（25）と SAFI（65）を使用しますが、これらは異なるネットワーク層到達可能性情報（NLRI）エンコーディングを使用するため、互換性はありません。2 つのエンコード タイプはネイバーごとに相互に排他的であるため、CLI 設定によりそれらを区別することが必要です。2 つの BGP 標準規格の違いは次のとおりです。

- RFC 6074 は、長さのエンコーディングをビットとして指定するためのガイドラインを提供します。

- RFC 4761 は、長さのエンコーディングをバイトとして指定するためのガイドラインを提供します。

どの NLRI エンコーディング標準規格がサポートされているかを検出するには、長さのエンコーディングを判定する必要があります。

NLRI による BGP L2VPN シグナリング

ネットワーク層到達可能性情報（NLRI）により、Border Gateway Protocol（BGP）はスーパーネット化情報を伝送することと、集約を実行することが可能になります。各 NLRI は、LB、LB+1、…、LB+VBS-1 という構造を持つブロック ラベルで構成されています。NLRI は、BGP 自動検出のために、BGP シグナリングで BGP デバイス間で交換されます。次のフィールドは、各仮想プライベート LAN スイッチング（VPLS）インスタンスに対して設定または自動生成されます。

- 長さ（2 オクテット）
- ルート識別子（RD）は通常、自動生成された 8 バイト VPN ID であり、これは設定することも可能です。この値は、VPLS ブリッジ ドメイン（またはインスタンス）について一意である必要があります。
- VPLS エンドポイント ID（VEID）（2 オクテット）。各 PE デバイスには VEID 値が設定されます。
- VPLS エンドポイント ブロック オフセット（VBO）（2 オクテット）。
- VPLS エンドポイント ブロック サイズ（VBS）（2 オクテット）。
- ラベル ベース（LB）（3 オクテット）。
- 拡張コミュニティ タイプ（2 オクテット）：0x800A 属性。VPLS インスタンス、ネクストホップおよび他のレイヤ 2 情報に指定されたルート ターゲット（RT）は、このエンコーディングで伝送されます。L3VPN に似た RT ベースのインポートおよびエクスポートの仕組みは、特定の VPLS インスタンスの L2VPN NLRI 上でフィルタリングを実行するために BGP により実行されます。
- カプセル化タイプ（1 オクテット）：VPLS = 19
- 制御フラグ（1 オクテット）
- レイヤ 2 最大伝送ユニット（MTU）（2 オクテット）
- 予約済み（2 オクテット）

VPLS BGP シグナリング L2VPN Inter-AS オプション A の設定方法

BGP 自動検出と BGP シグナリングの有効化

仮想プライベート LAN サービス（VPLS）PE デバイスで、IBGP 経由でアナウンスされた BGP 自動検出機能と BGP シグナリング機能によって他の PE デバイスを検出できるようにするには、次のタスクを実行します。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **l2vpn vfi context***vfi-context-name*
4. **vpn id***vpn-id*
5. **autodiscovery bgp signaling bgp**
6. **ve id***ve-ID-number*
7. **ve range***ve-range-number*
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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**l2vpn vfi context***vfi-context-name* 例： `Device(config)# l2vpn vfi context vfi1`	仮想プライベート LAN サービス（VPLS）でコア側の擬似回線を指定するための Layer 2 VPN（L2VPN）Virtual Forwarding Interface（VFI）を確立して、L2VFI コンフィギュレーション モードを開始します。 • VFI は、エミュレート LAN インターフェイスが使用されている場合に、VPLS アーキテクチャ モデルのエミュレート LAN または VPLS フォワーダを表します。

	コマンドまたはアクション	目的
ステップ 4	**vpn id***vpn-id* 例： `Device(config-vfi)# vpn id 10`	VPLS ドメインの VPN ID を設定します。
ステップ 5	**autodiscovery bgp signaling bgp** 例： `Device(config-vfi)# autodiscovery bgp signaling bgp`	デバイス上で BGP 自動検出と BGP シグナリングを有効にします。
ステップ 6	**ve id***ve-ID-number* 例： `Device(config-vfi)# ve id 1`	BGP シグナリングを使用した BGP 自動検出用の BGP デバイス間で交換される NLRI の VPLS Endpoint ID（VEID）を設定します。 • たとえば、VEID は連続しているため、1、2、3 や 501、502、503 などの VEID 番号シーケンスが望まれます。 • 100、200、300 などの不連続の番号体系は避けてください。 さらに VEID を追加する場合は、このステップを繰り返します。VEID は、同じ VPLS ドメイン内ですべての PE デバイスに対して一意にする必要があります。 （注） VEID を変更すると、仮想回線（VC）が再プロビジョンされトラフィックがその影響を受けます。
ステップ 7	**ve range***ve-range-number* 例： `Device(config-vfi)# ve range 10`	VPLS エッジ（VE）ブロックの最小サイズを上書きします。 • VE 範囲値は、ネイバーの数（最大 100）とほぼ一致している必要があります。 • VE 範囲は、ネットワーク上の隣接している PE デバイスの数に基づいて設定できます。 • たとえば、50 台の PE デバイスが VPLS ドメイン内に存在する場合は、VE 範囲として 10 より 50 が推奨されます。これは、交換される NLRI の数が少なく、コンバージェンス時間が短くなるからです。 （注） VE 範囲が設定されていないまたは既存の VE 範囲が削除された場合は、10 のデフォルト VE 範囲が適用されます。デバイスに複数の PE ネイバーがある場合は、デフォルト VE 範囲を使用しないでください。 （注） VE 範囲を変更した場合は、VC が再プロビジョンされトラフィックがその影響を受けます。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： `Device(config-vfi)# end`	L2 VFI コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。 （注） コマンドは、デバイスが L2VFI コンフィギュレーション モードを終了した後、有効になります。

VPLS 自動検出のための BGP シグナリングの設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **router bgp***autonomous-system-number*
4. **bgp graceful-restart**
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as***autonomous-system-number*
6. **address-family l2vpn vpls**
7. **neighbor** {*ip-address* | *peer-group-name*} **activate**
8. **neighbor** {*ip-address* | *peer-group-name*} **send-community extended**
9. **neighbor** {*ip-address* | *peer-group-name*} **suppress-signaling-protocol ldp**
10. **exit-address-family**
11. ステップ 1 ～ 10 を繰り返して、L2VPN アドレス ファミリでその他の BGP ネイバーを設定およびアクティブ化します。
12. **end**
13. **show l2vpn vfi**
14. **show ip bgp l2vpn vpls** {**all** [**summary**] | **rd***route-distinguisher*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 3	**router bgp***autonomous-system-number* 例： `Device(config)# router bgp 100`	指定したルーティング プロセスのルータ 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 graceful-restart** 例： `Device(config-router)# bgp graceful-restart`	すべての Border Gateway Protocol（BGP）ネイバーで BGP グレースフル リスタート機能をグローバルで有効にします。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as***autonomous-system-number* 例： `Device(config-router)# neighbor 198.51.100.1 remote-as 65000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。 • *autonomous-system-number* 引数が、**router bgp** コマンドで指定された自律システム番号と一致する場合、ネイバーは内部ネイバーになります。 • *autonomous-system-number* 引数が、**router bgp** コマンドで指定された自律システム番号と一致しない場合、ネイバーは外部ネイバーになります。 • この例では、10.10.10.1 のネイバーは内部 BGP ネイバーです。
ステップ 6	**address-family l2vpn vpls** 例： `Device(config-router)# address-family l2vpn vpls`	L2VPN アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **vpls** キーワードは、VPLS エンドポイント プロビジョニング情報が BGP ピアに配布され、L2VPN VPLS アドレス ファミリ セッションが作成されることを指定します。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor 198.51.100.1 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 8	**neighbor** {*ip-address* | *peer-group-name*} **send-community extended** 例： `Device(config-router-af)# neighbor 198.51.100.1 send-community extended`	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。 • この例では、拡張コミュニティ属性が 10.10.10.1 のネイバーに送信されます。
ステップ 9	**neighbor** {*ip-address* | *peer-group-name*} **suppress-signaling-protocol ldp** 例： `Device(config-router-af)# neighbor 198.51.100.1 suppress-signaling protocol ldp`	BGP ネイバーに対する LDP シグナリングを抑止します。これにより、VPLS 自動検出の BGP シグナリングが代わりに使用されます。 • この例では、10.10.10.1 のネイバーに対して LDP シグナリングが抑止されます。
ステップ 10	**exit-address-family** 例： `Device(config-router-af)# exit-address-family`	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、ルータ コンフィギュレーションモードに戻ります。
ステップ 11	ステップ 1 ～ 10 を繰り返して、L2VPN アドレス ファミリでその他の BGP ネイバーを設定およびアクティブ化します。	
ステップ 12	**end** 例： `Device(config-router)# end`	ルータ コンフィギュレーションモードを終了して、特権 EXEC モードに戻ります。

ステップ 13	**show l2vpn vfi**
	
	例：
	`Device# show l2vpn vfi`
	
	`PE1-standby#sh l2vpn vfi`
	`Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%`
	`Time source is hardware calendar, *20:50:52.526 GMT Wed Aug 29 2012`
	
	`Legend: RT=Route-target, S=Split-horizon, Y=Yes, N=No`
	
	`VFI name: VFI1, state: up, type: multipoint, signaling: BGP`
	`  VPN ID: 1, VE-ID: 10, VE-SIZE: 10`
	`  RD: 1:1, RT: 1:1`
	`  Bridge-Domain 100 attachment circuits:`
	`  Pseudo-port interface: pseudowire100001`
	`  Interface  Peer Address  VE-ID  Local Label  Remote Label  S`
	`  pseudowire100003  198.51.100.2  11  1003  2002  Y`
	`  pseudowire100005  198.51.100.3  12  1004  2002  Y`
		設定された VFI インスタンスに関する情報を表示します。

	コマンドまたはアクション	目的

	`VFI name: VFI2, state: up, type: multipoint, signaling: BGP`
	`  VPN ID: 2, VE-ID: 20, VE-SIZE: 12`
	`  RD: 1:2, RT: 1:2, import 3:3, export 4:4`
	`  Bridge-Domain 200 attachment circuits:`
	`  Pseudo-port interface: pseudowire100002`
	`  Interface  Peer Address  VE-ID  Local Label  Remote Label  S`
	`  pseudowire100004  198.51.100.2  21  1021  2020  Y`
	`  pseudowire100006  198.51.100.3  22  1022  2020  Y`	

ステップ 14	**show ip bgp l2vpn vpls** {**all** [**summary**] | **rd***route-distinguisher*}
	
	例：
	`Device# show ip bgp l2vpn vpls all summary`
	
	`BGP router identifier 198.51.100.1, local AS number 65000`
	`BGP table version is 14743, main routing table version 14743`
	`6552 network entries using 1677312 bytes of memory`
	`6552 path entries using 838656 bytes of memory`
	`3276/3276 BGP path/bestpath attribute entries using 760032 bytes of memory`
	`1638 BGP extended community entries using 65520 bytes of memory`
	`0 BGP route-map cache entries using 0 bytes of memory`
	`0 BGP filter-list cache entries using 0 bytes of memory`
	`BGP using 3341520 total bytes of memory`
	`BGP activity 9828/3276 prefixes, 9828/3276 paths, scan interval 60 secs`
	
	`Neighbor  V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd`
	`198.51.101.1  4  65000  90518  90507  14743  0  0 8w0d  1638`
	`198.51.102.2  4  65000  4901  4895  14743  0  0 2d01h  1638`
	`198.51.103.3  4  65000  4903  4895  14743  0  0 2d01h  1638`
		L2VPN VPLS アドレス ファミリに関する情報を表示します。

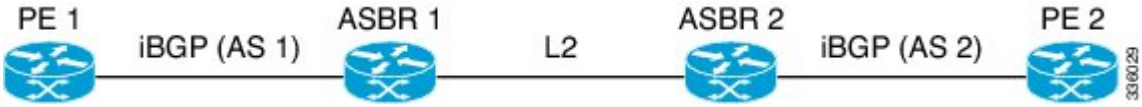
VPLS BGP シグナリング L2VPN Inter-AS オプション A：例

次の設定例では、L2VPN での VPLS BGP シグナリングの Inter-AS オプション A について説明します。自律システム境界ルータ（ASBR）1 は、自律システム（AS）1 上のすべての VPLS インターフェイスのプロバイダーエッジ（PE）として動作し、ASBR 2 は、CE デバイスと見なされます。もう一方の AS 2 では、ASBR 2 が PE として動作し、ASBR 1 が CE と見なされます。レイヤ 2 リンクに VPLS が使用されているため、ASBR 1 と ASBR 2 の間で MPLS は不要です。各 VPLS インスタンスを分離する必要があります。これにより、各インスタンスを ASBR の適切な VPLS

ドメイン内で送信できます（例：スイッチポートインターフェイスまたはイーサネットサブインターフェイス）。

（注） BGP シグナリングの観点からは、AS 内での変更は特にありません。VPLS の観点からは、ASBR1 と ASBR2 の間に BGP ピアリングがありません。

次の図に、BGP シグナリング Inter-AS オプション A BGP 設定のネットワーク構成図を示します。



次の例は、Inter-AS オプション A の PE 1 BGP 設定を示します。

```
router bgp 100
  neighbor 10.0.0.2 remote-as 100
   address-family l2vpn vpls
    neighbor 10.0.0.2 activate
    neighbor 10.0.0.2 send-community extended
    neighbor 10.0.0.2 suppress-signaling-protocol ldp
   exit-address-family
```

次の例は、Inter-AS オプション A の ASBR 1 BGP 設定を示します。

```
router bgp 100
  neighbor 10.0.0.1 remote-as 100
   address-family l2vpn vpls
    neighbor 10.0.0.1 activate
    neighbor 10.0.0.1 send-community extended
    neighbor 10.0.0.1 suppress-signaling-protocol ldp
   exit-address-family
```

次の例は、Inter-AS オプション A の ASBR 2 BGP 設定を示します。

```
router bgp 200
  neighbor 10.0.1.1 remote-as 100
   address-family l2vpn vpls
    neighbor 10.0.1.1 activate
    neighbor 10.0.1.1 send-community extended
    neighbor 10.0.1.1 suppress-signaling-protocol ldp
   exit-address-family
```

次の例は、Inter-AS オプション A の PE 2 BGP 設定を示します。

```
router bgp 200
  neighbor 10.0.1.2 remote-as 100
   address-family l2vpn vpls
    neighbor 10.0.1.2 activate
    neighbor 10.0.1.2 send-community extended
    neighbor 10.0.1.2 suppress-signaling-protocol ldp
   exit-address-family
```

BGP ベースの VPLS 自動検出に関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List, All Releases』

関連項目	マニュアル タイトル
MPLS コマンド	『Multiprotocol Label Switching Command Reference』

標準および RFC

標準/RFC	Title
draft-ietf-l2vpn-signaling-08.txt	『*Provisioning,Autodiscovery,andSignalinginL2VPNs*』
draft-ietf-l2vpn-vpls-bgp-08.8	『*VirtualPrivateLANService(VPLS)UsingBGPforAutodiscoveryandSignaling*』
draft-ietf-mpls-lsp-ping-03.txt	『*DetectingMPLSDataPlaneFailures*』
draft-ietf-pwe3-vccv-01.txt	『*Pseudo-Wire(PW)VirtualCircuitConnectionVerification(VCCV)*』
RFC 3916	『*RequirementsforPseudo-wireEmulationEdge-to-Edge(PWE3)*』
RFC 3981	『*PseudoWireEmulationEdge-to-EdgeArchitecture*』
RFC 6074	『Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)』
RFC 4761	『Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling』

MIB

MIB	MIB のリンク
• CISCO-IETF-PW-ATM-MIB（PW-ATM-MIB） • CISCO-IETF-PW-ENET-MIB（PW-ENET-MIB） • CISCO-IETF-PW-FR-MIB（PW-FR-MIB） • CISCO-IETF-PW-MIB（PW-MIB） • CISCO-IETF-PW-MPLS-MIB（PW-MPLS-MIB）	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探して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

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。サービス契約が有効で、ログイン ID またはパスワードを取得していない場合は、Cisco.com でまず登録手続きを行ってください。	http://www.cisco.com/en/US/support/index.html

VPLS BGP シグナリング L2VPN Inter-AS オプション A の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、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。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *40*：***VPLS BGP*** シグナリング ***L2VPN*** の機能情報

機能名	リリース	機能情報
VPLS BGP シグナリング L2VPN	Cisco IOS XE Release 3.8S	この機能では、自動検出とシグナリングの両方に BGP を使用することで、VPLS インスタンスのすべての既知のプロバイダー エッジ（PE）デバイスの自動検出とシグナリングが簡素化されました。 次のコマンドが導入または変更されました：**autodiscovery bgp signaling bgp**、**debug bgp l2vpn vpls updates**、**neighbor suppress-signaling-protocol ldp**、**ve id**、**ve range**、**show bgp l2vpn vpls**。

第 26 章

VPLS BGP シグナリング L2VPN Inter-AS オプション B

VPLS BGP シグナリング L2VPN Inter-AS オプション B 機能は、ボーダー ゲートウェイ プロトコル（BGP）を使用した仮想プライベート LAN スイッチング（VPLS）インスタンスにおける既知のすべてのプロバイダーエッジ（PE）デバイスの自動検出およびシグナリングを簡素化します。このドキュメントでは、VPLS BGP シグナリング L2VPN Inter-AS オプション B 機能を設定する方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース 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、機能情報の表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シスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

VPLS BGP シグナリング L2VPN Inter-AS オプション B の前提条件

- Virtual Private LAN Switching（VPLS）Border Gateway Protocol（BGP）シグナリングのために、擬似回線クラスで **no control-word** コマンドを使用してコントロール ワードを無効にします。次に例を示します。

```
Device> enable
Device# configure terminal
Device(config)# pseudowire-class my-pw-class
Device(config-pw-class)# no control-word
```

- VPLS ドメイン内のすべての仮想転送インスタンス（VFI）で、ルート識別子（RD）が一致している必要があります。
- 自律システム境界ルータ（ASBR）および PE デバイスで L2VPN VPLS Inter-AS オプション B 機能が設定されていることを確認します。

VPLS BGP シグナリング L2VPN Inter-AS オプション B に関する情報

VPLS の BGP 自動検出とシグナリング

仮想プライベート LAN スイッチング（VPLS）コントロール プレーンが、自動検出とシグナリングに使用されます。自動検出には、特定の VPLS インスタンスに参加するすべてのプロバイダーエッジ（PE）デバイスの場所を特定することが含まれます。シグナリングは、VPLS インスタンスの擬似回線を設定することにより実現されます。VPLS BGP シグナリング L2VPN Inter-AS オプション B 機能が導入される前は、RFC 6074 で指定されているように、シグナリングには Label Distribution Protocol（LDP）が使用され、自動検出には Border Gateway Protocol（BGP）が使用されていました。VPLS BGP シグナリング L2VPN Inter-As オプション B 機能の導入により、VPLS BGP シグナリング L2VPN 機能は両方の機能に BGP を使用することで、VPLS インスタンス内のすべての既知の PE デバイスの自動検出とシグナリングを簡素化しつつ RFC 4761 をサポートします。自動検出は、VPLS インスタンスごとに定義されます。

内部 BGP（IBGP）ピアは、自動検出とシグナリングの両方を実行するために、L2VPN アドレス ファミリ識別子（AFI）と L2VPN 情報を持つ後続のアドレス ファミリ識別子（SAFI）の数の更新メッセージを交換します。これにはネットワーク層到達可能性情報（NLRI）が含まれます。

VPLS の自動検出プロトコルのための両方の BGP 標準規格（RFC 6074 および RFC 4761）は、同じ BGP AFI（25）と SAFI（65）を使用しますが、これらは異なるネットワーク層到達可能性情報（NLRI）エンコーディングを使用するため、互換性はありません。2 つのエンコード タイプはネイバーごとに相互に排他的であるため、CLI 設定によりそれらを区別することが必要です。2 つの BGP 標準規格の違いは次のとおりです。

- RFC 6074 は、長さのエンコーディングをビットとして指定するためのガイドラインを提供します。
- RFC 4761 は、長さのエンコーディングをバイトとして指定するためのガイドラインを提供します。

どの NLRI エンコーディング標準規格がサポートされているかを検出するには、長さのエンコーディングを判定する必要があります。

NLRI による BGP L2VPN シグナリング

ネットワーク層到達可能性情報（NLRI）により、Border Gateway Protocol（BGP）はスーパーネット化情報を伝送することと、集約を実行することが可能になります。各 NLRI は、LB、LB+1、…、LB+VBS-1 という構造を持つブロック ラベルで構成されています。NLRI は、BGP 自動検出のために、BGP シグナリングで BGP デバイス間で交換されます。次のフィールドは、各仮想プライベート LAN スイッチング（VPLS）インスタンスに対して設定または自動生成されます。

- 長さ（2 オクテット）
- ルート識別子（RD）は通常、自動生成された 8 バイト VPN ID であり、これは設定することも可能です。この値は、VPLS ブリッジ ドメイン（またはインスタンス）について一意である必要があります。
- VPLS エンドポイント ID（VEID）（2 オクテット）。各 PE デバイスには VEID 値が設定されます。
- VPLS エンドポイント ブロック オフセット（VBO）（2 オクテット）。
- VPLS エンドポイント ブロック サイズ（VBS）（2 オクテット）。
- ラベル ベース（LB）（3 オクテット）。
- 拡張コミュニティ タイプ（2 オクテット）：0x800A 属性。VPLS インスタンス、ネクストホップおよび他のレイヤ 2 情報に指定されたルート ターゲット（RT）は、このエンコーディングで伝送されます。L3VPN に似た RT ベースのインポートおよびエクスポートの仕組みは、特定の VPLS インスタンスの L2VPN NLRI 上でフィルタリングを実行するために BGP により実行されます。
- カプセル化タイプ（1 オクテット）：VPLS = 19
- 制御フラグ（1 オクテット）
- レイヤ 2 最大伝送ユニット（MTU）（2 オクテット）
- 予約済み（2 オクテット）

VPLS BGP シグナリング L2VPN Inter-AS オプション B の設定方法

BGP 自動検出と BGP シグナリングの有効化

仮想プライベート LAN サービス（VPLS）PE デバイスで、IBGP 経由でアナウンスされた BGP 自動検出機能と BGP シグナリング機能によって他の PE デバイスを検出できるようにするには、次のタスクを実行します。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **l2vpn vfi context***vfi-context-name*
4. **vpn id***vpn-id*
5. **autodiscovery bgp signaling bgp**
6. **ve id***ve-ID-number*
7. **ve range***ve-range-number*
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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**l2vpn vfi context***vfi-context-name* 例： `Device(config)# l2vpn vfi context vfi1`	仮想プライベート LAN サービス（VPLS）でコア側の擬似回線を指定するための Layer 2 VPN（L2VPN）Virtual Forwarding Interface（VFI）を確立して、L2VFI コンフィギュレーション モードを開始します。 • VFI は、エミュレート LAN インターフェイスが使用されている場合に、VPLS アーキテクチャ モデルのエミュレート LAN または VPLS フォワーダを表します。

	コマンドまたはアクション	目的
ステップ 4	**vpn id***vpn-id* 例： `Device(config-vfi)# vpn id 10`	VPLS ドメインの VPN ID を設定します。
ステップ 5	**autodiscovery bgp signaling bgp** 例： `Device(config-vfi)# autodiscovery bgp signaling bgp`	デバイス上で BGP 自動検出と BGP シグナリングを有効にします。
ステップ 6	**ve id***ve-ID-number* 例： `Device(config-vfi)# ve id 1`	BGP シグナリングを使用した BGP 自動検出用の BGP デバイス間で交換される NLRI の VPLS Endpoint ID（VEID）を設定します。 • たとえば、VEID は連続しているため、1、2、3 や 501、502、503 などの VEID 番号シーケンスが望まれます。 • 100、200、300 などの不連続の番号体系は避けてください。 さらに VEID を追加する場合は、このステップを繰り返します。VEID は、同じ VPLS ドメイン内ですべての PE デバイスに対して一意にする必要があります。 （注） VEID を変更すると、仮想回線（VC）が再プロビジョンされトラフィックがその影響を受けます。
ステップ 7	**ve range***ve-range-number* 例： `Device(config-vfi)# ve range 10`	VPLS エッジ（VE）ブロックの最小サイズを上書きします。 • VE 範囲値は、ネイバーの数（最大 100）とほぼ一致している必要があります。 • VE 範囲は、ネットワーク上の隣接している PE デバイスの数に基づいて設定できます。 • たとえば、50 台の PE デバイスが VPLS ドメイン内に存在する場合は、VE 範囲として 10 より 50 が推奨されます。これは、交換される NLRI の数が少なく、コンバージェンス時間が短くなるからです。 （注） VE 範囲が設定されていないまたは既存の VE 範囲が削除された場合は、10 のデフォルト VE 範囲が適用されます。デバイスに複数の PE ネイバーがある場合は、デフォルト VE 範囲を使用しないでください。 （注） VE 範囲を変更した場合は、VC が再プロビジョンされトラフィックがその影響を受けます。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： `Device(config-vfi)# end`	L2 VFI コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。 （注） コマンドは、デバイスが L2VFI コンフィギュレーション モードを終了した後、有効になります。

VPLS 自動検出のための BGP シグナリングの設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **router bgp***autonomous-system-number*
4. **bgp graceful-restart**
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as***autonomous-system-number*
6. **address-family l2vpn vpls**
7. **neighbor** {*ip-address* | *peer-group-name*} **activate**
8. **neighbor** {*ip-address* | *peer-group-name*} **send-community extended**
9. **neighbor** {*ip-address* | *peer-group-name*} **suppress-signaling-protocol ldp**
10. **exit-address-family**
11. ステップ 1 ～ 10 を繰り返して、L2VPN アドレス ファミリでその他の BGP ネイバーを設定およびアクティブ化します。
12. **end**
13. **show l2vpn vfi**
14. **show ip bgp l2vpn vpls** {**all** [**summary**] | **rd***route-distinguisher*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 3	**router bgp***autonomous-system-number* 例： `Device(config)# router bgp 100`	指定したルーティング プロセスのルータ 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 graceful-restart** 例： `Device(config-router)# bgp graceful-restart`	すべての Border Gateway Protocol（BGP）ネイバーで BGP グレースフル リスタート機能をグローバルで有効にします。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as***autonomous-system-number* 例： `Device(config-router)# neighbor 198.51.100.1 remote-as 65000`	指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル ルータの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。 • *autonomous-system-number* 引数が、**router bgp** コマンドで指定された自律システム番号と一致する場合、ネイバーは内部ネイバーになります。 • *autonomous-system-number* 引数が、**router bgp** コマンドで指定された自律システム番号と一致しない場合、ネイバーは外部ネイバーになります。 • この例では、10.10.10.1 のネイバーは内部 BGP ネイバーです。
ステップ 6	**address-family l2vpn vpls** 例： `Device(config-router)# address-family l2vpn vpls`	L2VPN アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **vpls** キーワードは、VPLS エンドポイント プロビジョニング情報が BGP ピアに配布され、L2VPN VPLS アドレス ファミリ セッションが作成されることを指定します。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor 198.51.100.1 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 8	**neighbor** {*ip-address* | *peer-group-name*} **send-community extended** 例： `Device(config-router-af)# neighbor 198.51.100.1 send-community extended`	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。 • この例では、拡張コミュニティ属性が 10.10.10.1 のネイバーに送信されます。
ステップ 9	**neighbor** {*ip-address* | *peer-group-name*} **suppress-signaling-protocol ldp** 例： `Device(config-router-af)# neighbor 198.51.100.1 suppress-signaling protocol ldp`	BGP ネイバーに対する LDP シグナリングを抑止します。これにより、VPLS 自動検出の BGP シグナリングが代わりに使用されます。 • この例では、10.10.10.1 のネイバーに対して LDP シグナリングが抑止されます。
ステップ 10	**exit-address-family** 例： `Device(config-router-af)# exit-address-family`	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、ルータ コンフィギュレーションモードに戻ります。
ステップ 11	ステップ 1 ～ 10 を繰り返して、L2VPN アドレス ファミリでその他の BGP ネイバーを設定およびアクティブ化します。	
ステップ 12	**end** 例： `Device(config-router)# end`	ルータ コンフィギュレーションモードを終了して、特権 EXEC モードに戻ります。

ステップ 13	**show l2vpn vfi**
	
	例：
	`Device# show l2vpn vfi`
	
	`PE1-standby#sh l2vpn vfi`
	`Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%`
	`Time source is hardware calendar, *20:50:52.526 GMT Wed Aug 29 2012`
	
	`Legend: RT=Route-target, S=Split-horizon, Y=Yes, N=No`
	
	`VFI name: VFI1, state: up, type: multipoint, signaling: BGP`
	`VPN ID: 1, VE-ID: 10, VE-SIZE: 10`
	`RD: 1:1, RT: 1:1`
	`Bridge-Domain 100 attachment circuits:`
	`Pseudo-port interface: pseudowire100001`
	`Interface Peer Address VE-ID Local Label Remote Label S`
	`pseudowire100003 198.51.100.2 11 1003 2002 Y`
	`pseudowire100005 198.51.100.3 12 1004 2002 Y`
		設定された VFI インスタンスに関する情報を表示します。

	コマンドまたはアクション	目的

	`VFI name: VFI2, state: up, type: multipoint, signaling: BGP`
	`  VPN ID: 2, VE-ID: 20, VE-SIZE: 12`
	`  RD: 1:2, RT: 1:2, import 3:3, export 4:4`
	`  Bridge-Domain 200 attachment circuits:`
	`  Pseudo-port interface: pseudowire100002`
	`  Interface  Peer Address  VE-ID  Local Label  Remote Label  S`
	`  pseudowire100004  198.51.100.2  21  1021  2020  Y`
	`  pseudowire100006  198.51.100.3  22  1022  2020  Y`	

ステップ 14	**show ip bgp l2vpn vpls** {**all** [**summary**] | **rd***route-distinguisher*}
	
	例：
	`Device# show ip bgp l2vpn vpls all summary`
	
	`BGP router identifier 198.51.100.1, local AS number 65000`
	`BGP table version is 14743, main routing table version 14743`
	`6552 network entries using 1677312 bytes of memory`
	`6552 path entries using 838656 bytes of memory`
	`3276/3276 BGP path/bestpath attribute entries using 760032 bytes of memory`
	`1638 BGP extended community entries using 65520 bytes of memory`
	`0 BGP route-map cache entries using 0 bytes of memory`
	`0 BGP filter-list cache entries using 0 bytes of memory`
	`BGP using 3341520 total bytes of memory`
	`BGP activity 9828/3276 prefixes, 9828/3276 paths, scan interval 60 secs`
	
	`Neighbor  V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd`
	`198.51.101.1  4  65000  90518  90507  14743  0  0 8w0d  1638`
	`198.51.102.2  4  65000  4901  4895  14743  0  0 2d01h  1638`
	`198.51.103.3  4  65000  4903  4895  14743  0  0 2d01h  1638`
		L2VPN VPLS アドレス ファミリに関する情報を表示します。

L2VPN VPLS Inter-AS オプション B の設定例

例：VPLS BGP シグナリング L2VPN Inter-AS オプション B

次の設定例では、レイヤ 2 VPN での VPLS BGP シグナリングの Inter-AS オプション B について説明します。ASBR 1 と ASBR 2 の間に BGP MPLS 転送が必要です。

（注） BGP シグナリングの観点からは、自律システム内での変更は特にありません。VPLS の観点からは、ASBR1 と ASBR2 の間に EBGP ピアリングがあります。

次の図に、BGP シグナリング Inter-AS オプション B BGP 設定のネットワーク構成図を示します。

図 45：*VPLS BGP シグナリング L2VPN Inter-AS オプション B*：トポロジ例

次の例は、Inter-AS オプション B の PE 1 BGP 設定を示します。

```
l2vpn vfi context TEST101
 vpn id 1
 autodiscovery bgp signaling bgp
  ve id 1
  route-target import 22:22
  route-target export 11:11
  no auto-route-target
!
mpls ldp graceful-restart
!
bridge-domain 1
 member GigabitEthernet0/0/7 service-instance 101
 member vfi TEST101
!
interface Loopback0
 ip address 198.51.101.2 255.255.255.255
!
interface GigabitEthernet0/0/1
 description - connects to RR1
 ip address 200.1.1.1 255.255.255.0
 negotiation auto
 mpls ip
!
interface GigabitEthernet0/0/7
 description - connects to CE1
 no ip address
 negotiation auto
 service instance 101 ethernet
  encapsulation dot1q 101
  rewrite ingress tag pop 1 symmetric
 !
!
router ospf 10
 nsf
 network 200.1.1.0 0.0.0.255 area 0
 network 198.51.101.2 0.0.0.0 area 0
!
router bgp 10
 bgp log-neighbor-changes
 bgp update-delay 1
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 no bgp default ipv4-unicast
 neighbor 200.1.1.1 remote-as 10
 neighbor 200.1.1.1 update-source Loopback0
 !
 address-family ipv4
 exit-address-family
 !
 address-family l2vpn vpls
```

```
  neighbor 200.1.1.1 activate
  neighbor 200.1.1.1 send-community extended
  neighbor 200.1.1.1 suppress-signaling-protocol ldp
 exit-address-family
!
```

次の例は、Inter-AS オプション B の ASBR 1 BGP 設定を示します。

```
router bgp 10
bgp log-neighbor-changes
bgp update-delay 1
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
no bgp default ipv4-unicast
no bgp default route-target filter
 neighbor 192.0.2.1 remote-as 10
 neighbor 192.0.2.1 update-source Loopback0
 neighbor 203.0.203.1 remote-as 20
 neighbor 203.0.203.1 ebgp-multihop 255
 neighbor 203.0.203.1 update-source Loopback0
!
address-family ipv4
 exit-address-family
!
address-family l2vpn vpls
 neighbor 192.0.2.1 activate
 neighbor 192.0.2.1 send-community extended
 neighbor 192.0.2.1 next-hop-self
 neighbor 192.0.2.1 suppress-signaling-protocol ldp
 neighbor 203.0.203.1 activate
 neighbor 203.0.203.1 send-community extended
 neighbor 203.0.203.1 next-hop-self
 neighbor 203.0.203.1 suppress-signaling-protocol ldp
 exit-address-family
```

次の例は、Inter-AS オプション B の ASBR 2 BGP 設定を示します。

```
mpls ldp graceful-restart
!
interface Loopback0
 ip address 203.0.203.1 255.255.255.255
!
interface GigabitEthernet0/0/1
 description - connects to RR1
 ip address 192.0.2.2 255.255.255.0
 negotiation auto
 mpls ip
 mpls bgp forwarding
!
interface GigabitEthernet0/2/1
 description - connects to ASBR3
 ip address 192.0.2.200 255.255.255.0
 negotiation auto
 mpls ip
 mpls bgp forwarding
!
router ospf 10
 nsf
 network 192.0.2.0 0.0.0.255 area 0
 network 203.0.203.1 0.0.0.0 area 0
 network 0.0.0.0 255.255.255.255 area 0
!
router bgp 10
 bgp log-neighbor-changes
 bgp update-delay 1
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 no bgp default ipv4-unicast
 no bgp default route-target filter
 neighbor 203.0.203.3 remote-as 20
 neighbor 203.0.203.3 ebgp-multihop 255
 neighbor 203.0.203.3 update-source Loopback0
```

```
 neighbor 203.0.203.2 remote-as 10
 neighbor 203.0.203.2 update-source Loopback0
 !
 address-family ipv4
 exit-address-family
 !
 address-family l2vpn vpls
  neighbor 203.0.203.3 activate
  neighbor 203.0.203.3 send-community extended
  neighbor 203.0.203.3 next-hop-self
  neighbor 203.0.203.3 suppress-signaling-protocol ldp
  neighbor 203.0.203.2 activate
  neighbor 203.0.203.2 send-community extended
  neighbor 203.0.203.2 next-hop-self
  neighbor 203.0.203.2 suppress-signaling-protocol ldp
 exit-address-family
```

次の例は、Inter-AS オプション B の PE 2 BGP 設定を示します。

```
l2vpn vfi context TEST101
 vpn id 1
 autodiscovery bgp signaling bgp
  ve id 2
  route-target import 22:22
  route-target export 11:11
  no auto-route-target
!
mpls ldp graceful-restart
!
bridge-domain 1
 member GigabitEthernet0/0/7 service-instance 101
 member vfi TEST101
!
interface Loopback0
 ip address 192.0.2.3 255.255.255.255
!
interface GigabitEthernet0/0/1
 description - connects to RR1
 ip address 192.0.2.1 255.255.255.0
 negotiation auto
 mpls ip
!
interface GigabitEthernet0/0/7
 description - connects to CE2
 no ip address
 negotiation auto
 service instance 101 ethernet
  encapsulation dot1q 101
  rewrite ingress tag pop 1 symmetric
 !
!
router ospf 10
 nsf
 network 192.0.2.0 0.0.0.255 area 0
 network 192.0.2.3 0.0.0.0 area 0
!
router bgp 10
 bgp log-neighbor-changes
 bgp update-delay 1
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 no bgp default ipv4-unicast
 neighbor 211.1.1.1 remote-as 10
 neighbor 211.1.1.1 update-source Loopback0
 !
 address-family ipv4
 exit-address-family
 !
 address-family l2vpn vpls
  neighbor 211.1.1.1 activate
  neighbor 211.1.1.1 send-community extended
  neighbor 211.1.1.1 suppress-signaling-protocol ldp
 exit-address-family
```

次の例は、Inter-AS オプション B のルート リフレクタ デバイス BGP 設定を示します。

```
mpls ldp graceful-restart
!
interface Loopback0
 ip address 203.0.203.1 255.255.255.255
!
interface GigabitEthernet1/1
 description - connects to PE1
 ip address 203.0.203.2 255.255.255.0
 mpls ip
!
interface GigabitEthernet1/2
 description - connects to PE2
 ip address 203.0.203.3 255.255.255.0
 mpls ip
!
interface GigabitEthernet1/5
 description - connects to ASBR1
 ip address 203.0.203.4 255.255.255.0
 mpls ip
 mpls bgp forwarding
!
interface GigabitEthernet1/6
 description - connects to ASBR2
 ip address 203.0.203.5 255.255.255.0
 mpls ip
 mpls bgp forwarding
!
router ospf 10
 nsf
 network 203.0.203.6 0.0.0.255 area 0
 network 203.0.203.7 0.0.0.255 area 0
 network 203.0.203.8 0.0.0.255 area 0
 network 203.0.203.9 0.0.0.255 area 0
 network 203.0.203.1 0.0.0.0 area 0
!
router bgp 10
 bgp log-neighbor-changes
 bgp update-delay 1
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 no bgp default ipv4-unicast
 neighbor 203.0.203.11 remote-as 10
 neighbor 203.0.203.11 update-source Loopback0
 neighbor 203.0.203.12 remote-as 10
 neighbor 203.0.203.12 update-source Loopback0
 neighbor 203.0.203.13 remote-as 10
 neighbor 203.0.203.13 update-source Loopback0
 neighbor 203.0.203.14 remote-as 10
 neighbor 203.0.203.14 update-source Loopback0
 !
 address-family ipv4
 exit-address-family
 !
 address-family l2vpn vpls
  neighbor 203.0.203.11 activate
  neighbor 203.0.203.11 send-community extended
  neighbor 203.0.203.11 route-reflector-client
  neighbor 203.0.203.11 suppress-signaling-protocol ldp
  neighbor 203.0.203.12 activate
  neighbor 203.0.203.12 send-community extended
  neighbor 203.0.203.12 route-reflector-client
  neighbor 203.0.203.12 suppress-signaling-protocol ldp
  neighbor 203.0.203.13 activate
  neighbor 203.0.203.13 send-community extended
  neighbor 203.0.203.13 route-reflector-client
  neighbor 203.0.203.13 suppress-signaling-protocol ldp
  neighbor 203.0.203.14 activate
  neighbor 203.0.203.14 send-community extended
  neighbor 203.0.203.14 route-reflector-client
  neighbor 203.0.203.14 suppress-signaling-protocol ldp
```

```
 exit-address-family
!
```

VPLS BGP シグナリング L2VPN Inter-AS オプション B に関するその他の参考情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
MPLS コマンド	『Multiprotocol Label Switching Command Reference』
『L2VPN VPLS Inter-AS Option B』	『*L2VPN VPLS Inter-AS Option B*』
VPLS 自動検出：BGP ベース	*BGP ベースの VPLS 自動検出*
VPLS BGP シグナリング L2VPN Inter-AS オプション A	『*VPLS BGP Signaling L2VPN Inter-AS Option A*』

標準および RFC

標準および RFC	Title
draft-kothari-l2vpn-auto-site-id-01.txt	『*Automatic Generation of Site IDs for Virtual Private LAN Service*』
draft-ietf-l2vpn-vpls-multihoming-03.txt	『*BGP based Multi-homing in Virtual Private LAN Service*』
RFC 6074	『*Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)*』
RFC 4761	『*Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling*』

MIB

MIB	MIB のリンク
• CISCO-IETF-PW-ATM-MIB（PW-ATM-MIB） • CISCO-IETF-PW-ENET-MIB（PW-ENET-MIB） • CISCO-IETF-PW-FR-MIB（PW-FR-MIB） • CISCO-IETF-PW-MIB（PW-MIB） • CISCO-IETF-PW-MPLS-MIB（PW-MPLS-MIB）	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探して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

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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。	http://www.cisco.com/cisco/web/support/index.html

VPLS BGP シグナリング L2VPN Inter-AS オプション B の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、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。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *41*：*VPLS BGP* シグナリング *L2VPN Inter-AS* オプション *B* の機能情報

機能名	リリース	機能情報
VPLS BGP シグナリング L2VPN Inter-AS オプション B	Cisco IOS XE リリース 3.12S	この機能では、自動検出とシグナリングの両方に BGP を使用することで、VPLS インスタンスのすべての既知のプロバイダー エッジ（PE）デバイスの自動検出とシグナリングが簡素化されました。 次のコマンドが変更されました：**show mpls forwarding**。

第 27 章

Frame Relay over L2TPv3

Frame Relay over L2TPv3（FRoL2TPv3）機能により、Layer 2 Tunnel Protocol Version 3（L2TPv3）でのフレーム リレー スイッチングが可能になります。この機能は、like インターフェイスおよび異種インターフェイス（L2VPN インターワーキング）で動作します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース 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、機能情報の表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シスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

Frame Relay over L2TPv3 設定の前提条件

Frame Relay over L2TPv3 を設定する前に、レイヤ 2 VPN とフレーム リレーの設定方法を理解しておく必要があります。レイヤ 2 VPN とフレーム リレーの設定および使用方法を説明する機能モジュールへのポインタについては、その他の参考資料を参照してください。

Frame Relay over L2TPv3 設定の制約事項

次の機能はサポートされていません。

- Frame Relay to 802.1Q/QinQ VLAN インターワーキング
- Frame Relay-to-Ethernet ルーテッド インターワーキング
- フレーム リレー ポート間スイッチング
- フレーム リレーの L2TPv3 擬似回線冗長性

Frame Relay over L2TPv3 設定に関する情報

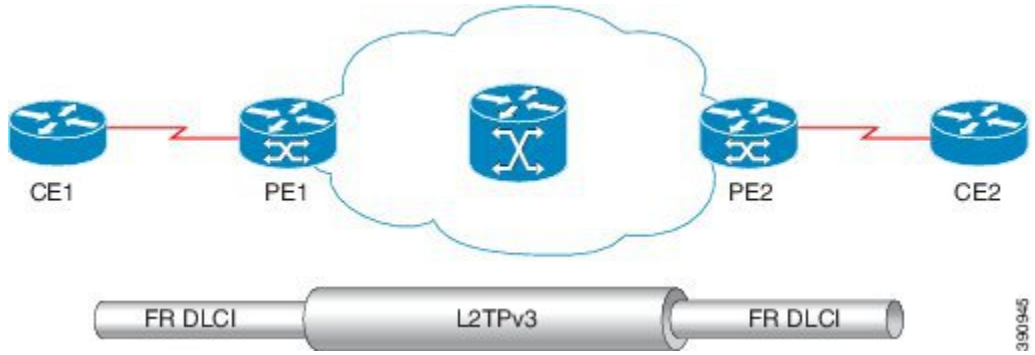
Frame Relay over L2TPv3 の概要

Frame Relay over L2TPv3 により、プロバイダー エッジ（PE）デバイスは、受信インターフェイスおよびデータ リンク接続識別子（DLCI）番号に基づいて、フレーム リレーのフレームを擬似回線に転送可能になります。また、PE デバイスはローカル管理インターフェイス（LMI）ベースのシグナリングをカスタマー エッジ（CE）デバイスに提供し、フレーム リレー スイッチをエミュレートします。

Frame Relay over L2TPv3 では、入力 PE デバイスでフレーム リレー ヘッダーが保持されます。デバイスは CE デバイスにパケットを転送する前に、フレーム リレー ヘッダーを再構築しません。

次の図は、Frame Relay over L2TPv3 のトポロジを示しています。

図 46：*Frame Relay over L2TPv3*



Frame Relay over L2TPv3 は次の機能をサポートします。

- フレーム リレー データ リンク接続識別子（DLCI）および Frame Relay DLCI 間
- フレーム リレー DLCI およびイーサネット ポート/802.1Q/QinQ 間のブリッジ型インターワーキング
- ローカル管理インターフェイス（LMI）
- L2TPv3 シーケンシング
- L2TPv3 トンネル マーキング

Frame Relay over L2TPv3 の設定方法

LMI を使用しない Frame Relay over L2TPv3 の設定

このセクションでは、ローカル管理インターフェイス（LMI）を有効にしないで、Frame Relay over L2TPv3 を設定する方法について説明します。

CE1 の場合

CE1 デバイスは、フレーム リレー リンク経由で PE1 デバイスが転送したフレーム リレー フレームを受信します。CE1 上で、PE1 デバイスがトラフィックを適切な擬似回線に転送するためのインターフェイスと DLCI 番号を設定します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **noipaddress** [*ip-address mask*] [**secondary**]
5. **encapsulationframe-relay**[**cisco** | **ietf**]
6. **nokeepalive**
7. **frame-relayintf-typedce**
8. **exit**
9. **interface***typenumber***point-to-point**
10. **ipaddress***ip-addressmask*
11. **frame-relayinterface-dlci***dlci*
12. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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***typenumber* 例： `Device(config)# interface serial3/1/0`	シリアル 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	**noipaddress** [*ip-address mask*] [**secondary**] 例： `Device(config-if)# no ip address`	IP 処理をディセーブルにします。
ステップ 5	**encapsulationframe-relay**[**cisco** | **ietf**] 例： `Device(config-if)# encapsulation frame-relay ietf`	インターフェイスのフレームリレー カプセル化を指定します。 • さまざまなカプセル化タイプを指定できます。

	コマンドまたはアクション	目的
		• 1 つのインターフェイスをシスコのカプセル化に設定し、もう 1 つのインターフェイスを IETF のカプセル化に設定できます。
ステップ 6	**nokeepalive** 例： `Device(config-if)# no keepalive`	キープアライブ設定を無効にします。
ステップ 7	**frame-relayintf-typedce** 例： `Device(config-if)# frame-relay intf-type dce`	インターフェイスが DCE スイッチであることを指定します。 • また、ネットワーク間インターフェイス（NNI）および DTE 接続をサポートするようにインターフェイスを指定することもできます。
ステップ 8	**exit** 例： `Device(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 9	**interface***typenumber***point-to-point** 例： `Device(config)# interface serial 3/1/0.1 point-to-point`	シリアル 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 10	**ipaddress***ip-addressmask* 例： `Device(config-if)# ip address 198.51.100.2 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 11	**frame-relayinterface-dlci***dlci* 例： `Device(config-if)# frame-relay interface-dlci 25`	データリンク接続識別子（DLCI）をフレーム リレーインターフェイスに割り当てます。
ステップ 12	**end** 例： `Device(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。 CE1 を設定したら、同様に、CE2 を設定できます。

PE1 の場合

PE1 デバイスは、CE1 デバイス上で設定された受信インターフェイスと DLCI 番号に基づいて、フレーム リレー フレームを該当する擬似回線に転送します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **noipaddress** [*ip-address mask*] [**secondary**]
5. **encapsulationframe-relay**[**cisco** | **ietf**]
6. **nokeepalive**
7. **pseudowire-class** [*pw-class-name*]
8. **encapsulation l2tpv3**
9. **ip local interfaceloopback***loopback id*
10. **connect***connection-nameinterfacedlci***l2transport**
11. **xconnect***peer-router-idvcid***encapsulationl2tpv3pw-classl2tpv3**
12. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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***typenumber* 例： `Device(config)# interface serial3/1/0`	シリアル 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。

	コマンドまたはアクション	目的
ステップ 4	**noipaddress** [*ip-address mask*] [**secondary**] 例： `Device(config-if)# no ip address`	IP 処理をディセーブルにします。
ステップ 5	**encapsulationframe-relay**[**cisco** | **ietf**] 例： `Device(config-if)# encapsulation frame-relay ietf`	インターフェイスのフレームリレーカプセル化を指定します。 • さまざまなカプセル化タイプを指定できます。 • 1 つのインターフェイスをシスコのカプセル化に設定し、もう 1 つのインターフェイスを IETF のカプセル化に設定できます。
ステップ 6	**nokeepalive** 例： `Device(config-if)# no keepalive`	キープアライブ設定を無効にします。
ステップ 7	**pseudowire-class** [*pw-class-name*] 例： `Device(config)# pseudowire-class l2tpv3`	レイヤ 2 擬似回線 クラスの名前を指定し、擬似回線 クラス コンフィギュレーション モードを開始します。
ステップ 8	**encapsulation l2tpv3** 例： `Device(config-pw)# encapsulation l2tpv3`	トンネリング カプセル化を L2TPv3 として指定します。
ステップ 9	**ip local interfaceloopback***loopback id* 例： `Device(config-pw)# ip local interface Loopback0`	L2TPv3 トンネル用の PE1 上のローカル ループバック インターフェイスを指定します。
ステップ 10	**connect***connection-nameinterfacedlci***l2transport** 例： `Device(config)# connect fr1 serial5/0 1000 l2transport`	フレーム リレー相手先固定接続（PVC）間の接続を定義し、接続コンフィギュレーション モードを開始します。 • **l2transport** キーワードを使用して、PVC がローカルにスイッチングされずに、バックボーン ネットワーク上でトンネリングされるように指定します。

	コマンドまたはアクション	目的
		• *connection-name* 引数は、指定するテキスト文字列です。 • *interface* 引数は、PVC 接続が定義されるインターフェイスです。 • *dlci* 引数は、接続される PVC の DLCI 番号です。
ステップ 11	**xconnect***peer-router-idvcid***encapsulationl2tpv3pw-classl2tpv3** 例： `Device(config-xconnect-conn-config)# xconnect 198.51.100.2 123 encapsulation l2tpv3 pw-class l2tpv3`	レイヤ 2 パケットを転送するための VC を作成します。 • DLCI 間接続タイプでは、Frame Relay over L2TPv3 が接続コンフィギュレーションモードで **xconnect** コマンドを使用します。 • PE デバイス間の仮想回線（VC）の *vcid* または識別子は、接続されている両方のデバイスで同じにする必要があります。
ステップ 12	**end** 例： `Device(config-xconnect-conn-config)# end`	接続コンフィギュレーションモードを終了して、特権 EXEC モードに戻ります。 PE1 を設定したら、同様に、PE2 を設定できます。

LMI を使用する Frame Relay over L2TPv3 の設定

このセクションでは、ローカル管理インターフェイス（LMI）を有効にして、Frame Relay over L2TPv3 を設定する方法について説明します。

CE1 の場合

CE1 デバイスは、フレーム リレー リンク経由で PE1 デバイスが転送したフレーム リレー フレームを受信します。CE1 上で、PE1 デバイスがトラフィックを適切な擬似回線に転送するためのインターフェイスと DLCI 番号を設定します。ローカル管理インターフェイス（LMI）は、擬似配線経由でトンネリングもされます。そのため、LMI 用のカスタマーエッジ（CE）デバイスを正しく設定する必要があります。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfaceserial***slot*/*subslot*/*port* [**.***subinterface*]
4. **noipaddress** [*ip-address mask*] [**secondary**]
5. **encapsulationframe-relay**[**cisco** | **ietf**]
6. **frame-relayintf-typedce**
7. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**interfaceserial***slot*/*subslot*/*port* [**.***subinterface*] 例： `Device(config)# interface serial3/1/0`	シリアル 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	**noipaddress** [*ip-address mask*] [**secondary**] 例： `Device(config-if)# no ip address`	IP 処理をディセーブルにします。
ステップ 5	**encapsulationframe-relay**[**cisco** | **ietf**] 例： `Device(config-if)# encapsulation frame-relay ietf`	インターフェイスのフレームリレー カプセル化を指定します。 • さまざまなカプセル化タイプを指定できます。 • 1 つのインターフェイスをシスコのカプセル化に設定し、もう 1 つのインターフェイスを IETF のカプセル化に設定できます。

	コマンドまたはアクション	目的
ステップ 6	**frame-relayintf-typedce** 例： `Device(config-if)# frame-relay intf-type dce`	インターフェイスがデータ通信装置（DCE）スイッチであることを指定します。 • また、ネットワーク間インターフェイス（NNI）接続とデータ伝送装置（DTE）接続をサポートするインターフェイスを指定することもできます。
ステップ 7	**end** 例： `Device(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。 CE1 を設定したら、同様に、CE2 を設定できます。

PE1 の場合

PE1 デバイスは、フレーム リレー リンク経由でフレーム リレー フレームを CE1 デバイスに転送します。PE1 デバイスは、ローカル管理インターフェイス（LMI）シグナリングも CE デバイスに提供します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfaceserial***slot*/*subslot*/*port* [**.***subinterface*]
4. **encapsulationframe-relay**[**cisco** | **ietf**]
5. **pseudowire-class** [*pw-class-name*]
6. **encapsulation l2tpv3**
7. **ip local interfaceloopback***loopback id*
8. **connect***connection-nameinterfacedlci***l2transport**
9. **xconnect***peer-router-idvcid***encapsulationl2tpv3pw-classl2tpv3**
10. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# 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	**interfaceserial***slot*/*subslot*/*port* [**.***subinterface*] 例： `Device(config)# interface serial3/1/0`	シリアル 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	**encapsulationframe-relay**[**cisco** | **ietf**] 例： `Device(config-if)# encapsulation frame-relay ietf`	インターフェイスのフレームリレー カプセル化を指定します。 • さまざまなカプセル化タイプを指定できます。 • 1 つのインターフェイスをシスコのカプセル化に設定し、もう 1 つのインターフェイスを IETF のカプセル化に設定できます。
ステップ 5	**pseudowire-class** [*pw-class-name*] 例： `Device(config)# pseudowire-class l2tpv3`	レイヤ 2 擬似回線 クラスの名前を指定し、擬似回線 クラス コンフィギュレーション モードを開始します。
ステップ 6	**encapsulation l2tpv3** 例： `Device(config-pw)# encapsulation l2tpv3`	トンネリング カプセル化を L2TPv3 として指定します。
ステップ 7	**ip local interfaceloopback***loopback id* 例： `Device(config-pw)# ip local interface Loopback0`	ローカルループバック インターフェイスを指定します。
ステップ 8	**connect***connection-nameinterfacedlci***l2transport** 例： `Device(config)# connect fr1 serial5/0 1000 l2transport`	フレーム リレー相手先固定接続（PVC）間の接続を定義し、接続コンフィギュレーションモードを開始します。 • **l2transport** キーワードを使用して、PVC がローカルにスイッチングされずに、バックボーン ネットワーク上でトンネリングされるように指定します。

	コマンドまたはアクション	目的
		• *connection-name* 引数は、指定するテキスト文字列です。 • *interface* 引数は、PVC 接続が定義されるインターフェイスです。 • *dlci* 引数は、接続される PVC の DLCI 番号です。
ステップ 9	**xconnect***peer-router-idvcid***encapsulationl2tpv3pw-classl2tpv3** 例： `Device(config-fr-pw-switching)# xconnect 198.51.100.2 123 encapsulation l2tpv3 pw-class l2tpv3`	レイヤ 2 パケットを転送するための仮想回線（VC）を作成します。 • DLCI 間接続タイプでは、Frame Relay over L2TPv3 が接続コンフィギュレーションモードで **xconnect** コマンドを使用します。
ステップ 10	**end** 例： `Device(config-fr-pw-switching)# end`	接続コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。 PE1 を設定したら、同様に、PE2 を設定できます。

フレーム リレー L2TPv3 トンネル マーキングの設定

L2TPv3 トンネル マーキングは、サービス プロバイダー ネットワーク内のプロバイダー エッジ（PE）デバイス上で、受信カスタマー トラフィックに対する Quality of Service（QoS）を定義および制御する機能を導入します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **class-map***class-name*
4. **matchfr-dlci***dlci-number*
5. **policy-mapdlci***dlci-number*
6. **class***class-name*
7. **set ip precedence tunnel***precedence-value*
8. **interfaceserial***slot*/*subslot*/*port* [**.***subinterface*]
9. **noipaddress** [*ip-address mask*] [**secondary**]
10. **encapsulationframe-relay**[**cisco** | **ietf**]
11. **nokeepalive**
12. **service-policyinput***policy-name*
13. **end**
14. **pseudowire-class** [*pw-class-name*]
15. **encapsulation l2tpv3**
16. **ip local interfaceloopback***loopback id*
17. **connect***connection-nameinterfacedlci***l2transport**
18. **xconnect***peer-router-idvcid***encapsulationl2tpv3pw-classl2tpv3**
19. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**class-map***class-name* 例： `Device(config)# class-map class1`	トラフィック クラスのユーザ定義名を指定し、クラス マップ 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	**matchfr-dlci***dlci-number* 例： `Device(config-cmap)# match fr-dlci 50`	クラス マップで一致基準としてパケットに関連付けられたデータリンク接続識別子（DLCI）の番号を指定します。
ステップ 5	**policy-mapdlci***dlci-number* 例： `Device(config-cmap)# policy-map dlci 50`	ポリシー マップのタイプを DLCI として指定し、ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 6	**class***class-name* 例： `Device(config-pmap)# class class1`	トラフィックをトラフィック ポリシーに分類するために使用される **class-map** コマンドを使用して設定された事前定義のトラフィック クラスの名前を指定して、ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 7	**set ip precedence tunnel***precedence-value* 例： `Device(config-pmap-c)# set ip precedence tunnel 2`	トンネル マーキング用の L2TPv3 トンネル パケットのヘッダー内の優先値を設定します。
ステップ 8	**interfaceserial***slot*/*subslot*/*port* [**.***subinterface*] 例： `Device(config-pmap-c)# interface serial3/1/0`	シリアル 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 9	**noipaddress** [*ip-address mask*] [**secondary**] 例： `Device(config-if)# no ip address`	IP 処理をディセーブルにします。
ステップ 10	**encapsulationframe-relay**[**cisco** | **ietf**] 例： `Device(config-if)# encapsulation frame-relay ietf`	インターフェイスのフレームリレー カプセル化を指定します。 • さまざまなカプセル化タイプを指定できます。 • 1 つのインターフェイスをシスコのカプセル化に設定し、もう 1 つのインターフェイスを IETF のカプセル化に設定できます。

	コマンドまたはアクション	目的
ステップ 11	**nokeepalive** 例： `Device(config-if)# no keepalive`	キープアライブ設定を無効にします。
ステップ 12	**service-policyinput***policy-name* 例： `Device(config-if)# service-policy input policy1`	トラフィック ポリシーをインターフェイスにアタッチします。
ステップ 13	**end** 例： `Device(config-if)# end`	接続コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 14	**pseudowire-class** [*pw-class-name*] 例： `Device(config)# pseudowire-class l2tpv3`	レイヤ 2 擬似回線 クラスの名前を指定し、擬似回線 クラス コンフィギュレーション モードを開始します。
ステップ 15	**encapsulation l2tpv3** 例： `Device(config-pw)# encapsulation l2tpv3`	トンネリング カプセル化を L2TPv3 として指定します。
ステップ 16	**ip local interfaceloopback***loopback id* 例： `Device(config-pw)# ip local interface Loopback0`	ローカル ループバック インターフェイスを指定します。
ステップ 17	**connect***connection-nameinterfacedlci***l2transport** 例： `Device(config-pw)# connect fr1 serial5/0 1000 l2transport`	フレーム リレー相手先固定接続（PVC）間の接続を定義し、接続コンフィギュレーション モードを開始します。 • **l2transport** キーワードを使用して、PVC がローカルにスイッチングされずに、バックボーン ネットワーク上でトンネリングされるように指定します。 • *connection-name* 引数は、指定するテキスト文字列です。 • *interface* 引数は、PVC 接続が定義されるインターフェイスです。

	コマンドまたはアクション	目的
		• *dlci* 引数は、接続される PVC の DLCI 番号です。
ステップ 18	**xconnect***peer-router-idvcid***encapsulationl2tpv3pw-classl2tpv3** 例： `Device(config-xconnect-conn-config)# xconnect 198.51.100.2 123 encapsulation l2tpv3 pw-class l2tpv3`	レイヤ 2 パケットを転送するための VC を作成します。 • DLCI 間接続タイプでは、Frame Relay over L2TPv3 が接続コンフィギュレーション モードで **xconnect** コマンドを使用します。
ステップ 19	**end** 例： `Device(config-xconnect-conn-config)# end`	接続コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

Frame Relay over L2TPv3 設定の確認

show コマンドを使用して、Frame Relay over L2TPv3 設定に関する情報を表示できます。

手順の概要

1. **show xconnectalldetail**
2. **show frame-relay pvc**
3. **show connection**

手順の詳細

ステップ 1 **show xconnectalldetail**

次に、**show xconnectalldetail** コマンドの出力例を示します。

例：

```
Device# show xconnect all detail

Legend:    XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State
  UP=Up       DN=Down            AD=Admin Down      IA=Inactive
  SB=Standby  HS=Hot Standby     RV=Recovering      NH=No Hardware

XC ST  Segment 1                          S1 Segment 2                          S2
------+---------------------------------+--+---------------------------------+--
UP pri   ac Se0/2/0:0:16(FR DLCI)        UP l2tp 22.2.2.2:100                  UP
            Interworking: L2L                    Session ID: 306532470
```

```
                                                Tunnel ID: 1381396806
                                                Protocol State: UP
                                                Remote Circuit State: UP
                                                pw-class: fr_fr
UP pri   ac Se0/2/0:0:17(FR DLCI)        UP l2tp 22.2.2.2:101                UP
            Interworking: Eth                   Session ID: 1373339282
                                                Tunnel ID: 1381396806
                                                Protocol State: UP
                                                Remote Circuit State: UP
                                                pw-class: fr_eth
```

ステップ 2 **show frame-relay pvc**

次に、**show frame-relay pvc** コマンドの出力例を示します。

例：

```
Device# show frame-relay pvc

pseudowire100001 is up, VC status is up PW type: Ethernet
  Create time: 5d20h, last status change time: 5d20h
    Last label FSM state change time: 5d20h
  Destination address: 2.1.1.2 VC ID: 1234000
    Output interface: Et0/0, imposed label stack {2001}
  Preferred path: not configured
  Default path: active
  Next hop: 20.0.0.2
Member of xconnect service Et1/0.1-1001, group right
  Associated member Et1/0.1 is up, status is up
  Interworking type is Ethernet
  Service id: 0x6d000002
Signaling protocol: LDP, peer 2.1.1.2:0 up
  Targeted Hello: 1.1.1.1(LDP Id) -> 2.1.1.2, LDP is UP
  Graceful restart: not configured and not enabled
  Non stop routing: not configured and not enabled
  PWid FEC (128), VC ID: 1234000
  Status TLV support (local/remote) : enabled/supported
    LDP route watch : enabled
    Label/status state machine : established, LruRru
    Local dataplane status received : No fault
    BFD dataplane status received : Not sent
    BFD peer monitor status received : No fault
    Status received from access circuit : No fault
    Status sent to access circuit : No fault
    Status received from pseudowire i/f : No fault
    Status sent to network peer : No fault
    Status received from network peer : No fault
    Adjacency status of remote peer : No fault
Sequencing: receive disabled, send disabled
Bindings
Parameter    Local                          Remote
------------ ------------------------------ ------------------------------
Label        2007                           2001
Group ID     0                              6
Interface
MTU          1500                           1500
Control word on (configured: autosense)     on
PW type      Ethernet                       Ethernet
VCCV CV type 0x12                           0x12
               LSPV [2], BFD/Raw [5]          LSPV [2], BFD/Raw [5]
VCCV CC type 0x07                           0x07
             CW [1], RA [2], TTL [3]        CW [1], RA [2], TTL [3]
Status TLV   enabled                        supported
Dataplane:
  SSM segment/switch IDs: 12309/4115 (used), PWID: 1
Rx Counters
  106563 input transit packets, 9803650 bytes
  0 drops, 0 seq err
Tx Counters
```

```
  0 output transit packets, 0 bytes
  0 drops
```

ステップ 3 **show connection**

次に、**show connection** コマンドの出力例を示します。

例：

```
Device# show connection

ID   Name            Segment 1               Segment 2                  State
==============================================================================
1    fr_fr           Se0/2/0:0 16            22.2.2.2 100               UP
2    fr_eth          Se0/2/0:0 17            22.2.2.2 101               UP

--------------------------
```

Frame Relay over L2TPv3 の設定例

例：LMI を使用する Frame Relay over L2TPv3

次に、ローカル管理インターフェイス（LMI）が有効な状態で Frame Relay over L2TPv3 を設定する例を示します。

PE1 デバイス	CE1 デバイス
configure terminal interface Serial 0/2/0:0 no ip address encapsulation frame-relay ! keepalive 15 frame-relay lmi-type cisco	configure terminal interface Serial 1/0:0 no ip address encapsulation frame-relay frame-relay intf-type dce ! keepalive 15 frame-relay lmi-type cisco interface Serial 1/0:0.100 point-to-point ip address 198.51.100.33 255.255.255.0 frame-relay interface-dlci 16

例：LMI を使用しない Frame Relay over L2TPv3

次に、ローカル管理インターフェイス（LMI）が有効ではない状態で Frame Relay DLCI-to-Frame Relay DLCI over L2TPv3 を設定する例を示します。

PE1 デバイス	CE1 デバイス

`configure terminal`
`  interface Serial 0/1/0`
`  encapsulation frame-relay`
`!`
`pseudowire-class fr_l2tpv3`
`  encapsulation l2tpv3`
`  ip local interface Loopback0`
`!`
`connect FR Serial 0/1/0 100 l2transport`
`  xconnect 198.51.100.2 100 encapsulation l2tpv3 pw-class fr_l2tpv3`
	`configure terminal`
	`  interface Serial 0/0/0`
	`  encapsulation frame-relay`
	`  exit`
	`!`
	`interface Serial 0/0/0.100 point-to-point`
	`  ip address 198.51.100.22 255.255.255.0`
	`  frame-relay interface-dlci 100`

次に、LMI が有効ではない状態で Frame Relay DLCI-to-Ethernet Interworking over L2TPv3 を設定する例を示します。

PE1 デバイス	CE1 デバイス

`configure terminal`
`  pseudowire-class fr_eth`
`  encapsulation l2tpv3`
`  interworking ethernet`
`  ip local interface Loopback0`
`!`
`connect FR-Eth Serial 0/1/0 500 l2transport`
`  xconnect 198.51.100.27 500 encapsulation l2tpv3 pw-class fr_eth`
	`configure terminal`
	`  interface Serial 0/0/0.500 point-to-point`
	`  frame-relay interface-dlci 500`
	`!`
	`interface BVI 200`
	`  ip address 198.51.100.29 255.255.255.0`

Frame Relay over L2TPv3 に関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
MPLS コマンド	『Multiprotocol Label Switching Command Reference』
Frame Relay over MPLS の設定	『*Configuring Frame Relay over MPLS*』

関連項目	マニュアル タイトル
MPLS レイヤ 2 VPN コンフィギュレーション ガイド	『*MPLS レイヤ 2 VPN コンフィギュレーション ガイド*』

標準および RFC

標準/RFC	Title
RFC 2427	『*Multiprotocol Interconnect over Frame Relay*』
RFC 4591	『*Frame Relay over Layer 2 Tunneling Protocol Version 3 (L2TPv3)*』

MIB

MIB	MIB のリンク
• 『Cisco Frame Relay MIB』（CISCO-FRAME-RELAY-MIB.my） • 『Interfaces MIB』（IF-MIB.my）	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探して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

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。サービス契約が有効で、ログイン ID またはパスワードを取得していない場合は、Cisco.com でまず登録手続きを行ってください。	http://www.cisco.com/support

Frame Relay over L2TPv3 の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、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。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *42*：*Frame Relay over L2TPv3* の機能情報

機能名	リリース	機能情報
Frame Relay over L2TPv3	Cisco IOS XE リリース 3.12S	この機能により、フレーム リレーから Layer 2 Tunneling Protocol バージョン 3（L2TPv3）へのスイッチオーバーが可能になります。この機能は、like インターフェイスおよび異種インターフェイス（L2VPN インターワーキング）で動作します。

第 28 章

L2VPN 対応 Loop-Free Alternate Fast Reroute

レイヤ 2 バーチャル プライベート ネットワーク（L2VPN）機能を使用した Loop-Free Alternate（LFA）Fast Reroute（FRR）は、リンクやノードの障害によるパケット損失を最小化します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース 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、機能情報の表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シスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

L2VPN 対応 Loop-Free Alternate Fast Reroute の制約事項

- ロード バランシングはサポートされません。
- 時分割多重（TDM）擬似回線はサポートされていません。

- 仮想プライベート LAN サービス（VPLS）はサポートされていません。
- Virtual Private Wire Service（VPWS）スケール番号は変更される可能性があります。

L2VPN 対応 Loop-Free Alternate Fast Reroute に関する情報

Loop-Free Alternate Fast Reroute での L2VPN

Loop-Free Alternate（LFA）Fast Reroute（FRR）機能は、MPLS Traffic Engineering Fast Reroute 機能を代替し、リンク障害またはノード障害によるパケット損失を最小限に抑えます。この中には L2VPN および Virtual Private Wire Services（VPWS）の LFA FRR サポートが含まれ、次の利点をもたらします。

- トラフィック損失からの保護レベルが同一
- 簡易なコンフィギュレーション
- リンクおよびノード保護
- リンクおよびパス保護
- LFA（ループフリー代替）パス
- IP とラベル配布プロトコル（LDP）コアの両方のサポート

LFA FRR により、ネットワーク障害の発生時に、バックアップ ルートがトラフィック損失を回避できます。バックアップルート（修復パス）は事前に計算され、プライマリ パスのバックアップとしてルータにインストールされます。ルータは、リンクまたは隣接ノードの障害を検出すると、バックアップ パスに切り替えてトラフィック損失を回避します。

L2VPN 対応 Loop-Free Alternate Fast Reroute の設定方法

L2VPNおよびVPWSのループフリー代替高速再ルーティングのサポートを有効にするには、ルーティング プロトコル用の LFA FRR を設定する必要があります。その他の設定手順は必要ありません。ルーティング プロトコルによって次の文書のいずれかを参照してください。

- 『*IP Routing: ISIS Configuration Guide*』の「IS-IS Remote Loop-Free Alternate Fast Reroute」
- 『*IP Routing: OSPF Configuration Guide*』の「OSPFv2 Loop-Free Alternate Fast Reroute」
- 『*IP Routing: OSPF Configuration Guide*』の「OSPF IPv4 Remote Loop-Free Alternate IP Fast Reroute」

L2VPN 対応 Loop-Free Alternate Fast Reroute の確認

LFA FRR 設定を確認するには、次の 1 つ以上のコマンドを使用します。

手順の概要

1. **show ip cef** *network-prefix* **internal**
2. **show mpls infrastructure lfd pseudowire internal**
3. **show platform hardware pp active feature cef database ipv4** *network-prefix*

手順の詳細

ステップ 1 **show ip cef** *network-prefix* **internal**

例：
```
show ip cef 16.16.16.16 internal
```
Cisco Express Forwarding（CEF）転送情報ベース（FIB）内エントリを表示します。

ステップ 2 **show mpls infrastructure lfd pseudowire internal**

例：
```
show mpls infrastructure lfd pseudowire internal
```
ラベル転送データベース（LFD）と擬似回線に関する情報を表示します。

ステップ 3 **show platform hardware pp active feature cef database ipv4** *network-prefix*

例：
```
show platform hardware pp active feature cef database ipv4 16.16.16.16/32
```
CEF データベースに関する情報を表示します。

L2VPN 対応 Loop-Free Alternate Fast Reroute の設定例

例：L2VPN 対応 LFA FRR の確認

show ip cef internal

次に、LFA FRR for OSPF の設定例を示します。

```
router ospf 1
 router-id 17.17.17.17
 fast-reroute per-prefix enable prefix-priority low
 network 3.3.3.0 0.0.0.255 area 1
 network 6.6.6.0 0.0.0.255 area 1
 network 7.7.7.0 0.0.0.255 area 1
 network 17.17.17.17 0.0.0.0 area 1
```

show ip cef internal

次に、**show ip cef internal** コマンドの出力例を示します。

```
Device# show ip cef 16.16.16.16 internal
16.16.16.16/32, epoch 2, RIB[I], refcount 7, per-destination sharing
  sources: RIB, RR, LTE
  feature space:
   IPRM: 0x00028000
   Broker: linked, distributed at 1st priority
   LFD: 16.16.16.16/32 1 local label
   local label info: global/17
        contains path extension list
        disposition chain 0x3A3C1DF0
        label switch chain 0x3A3C1DF0
  subblocks:
   1 RR source [no flags]
    non-eos chain [16|44]
  ifnums:
   GigabitEthernet0/0/2(9): 7.7.7.2
   GigabitEthernet0/0/7(14): 7.7.17.9
  path 35D61070, path list 3A388FA8, share 1/1, type attached nexthop, for IPv4, flags
has-repair
    MPLS short path extensions: MOI flags = 0x20 label 16
  nexthop 7.7.7.2 GigabitEthernet0/0/2 label [16|44], adjacency IP adj out of
GigabitEthernet0/0/2, addr 7.7.7.2 35E88520
    repair: attached-nexthop 7.7.17.9 GigabitEthernet0/0/7 (35D610E0)
  path 35D610E0, path list 3A388FA8, share 1/1, type attached nexthop, for IPv4, flags
repair, repair-only
  nexthop 7.7.17.9 GigabitEthernet0/0/7, repair, adjacency IP adj out of GigabitEthernet0/0/7,
 addr 7.7.17.9 3A48A4E0
  output chain: label [16|44]
  FRR Primary (0x35D10F60)
  <primary:  TAG adj out of GigabitEthernet0/0/2, addr 7.7.7.2 35E88380>
  <repair:  TAG adj out of GigabitEthernet0/0/7, addr 7.7.17.9 3A48A340>
Rudy17#show mpls infrastructure lfd pseudowire internal
PW ID: 1VC ID: 4, Nexthop address: 16.16.16.16
SSM Class: SSS HW
Segment Count: 1
VCCV Types Supported:  cw ra ttl
Imposition details:
 Label stack {22 16}, Output interface: Gi0/0/2
 Preferred path: not configured
 Control Word: enabled, Sequencing: disabled
 FIB Non IP entry: 0x35D6CEEC
 Output chain:  AToM Imp (locks 4) label 22 label [16|44]
  FRR Primary (0x35D10F60)
  <primary:  TAG adj out of GigabitEthernet0/0/2, addr 7.7.7.2 35E88380>
Disposition details:
 Local label: 16
 Control Word: enabled, Sequencing: disabled
 SSS Switch: 3976200193
 Output chain:  mpls_eos( connid router-alert AToM Disp (locks 5)/ drop)
```

show mpls infrastructure lfd pseudowire internal

次に、**show mpls infrastructure lfd pseudowire internal** コマンドの出力例を示します。

```
Device# show mpls infrastructure lfd pseudowire internal
PW ID: 1VC ID: 4, Nexthop address: 16.16.16.16
SSM Class: SSS HW
Segment Count: 1
VCCV Types Supported:  cw ra ttl
Imposition details:
 Label stack {22 16}, Output interface: Gi0/0/2
 Preferred path: not configured
 Control Word: enabled, Sequencing: disabled
 FIB Non IP entry: 0x35D6CEEC
 Output chain:  AToM Imp (locks 4) label 22 label [16|44]
  FRR Primary (0x35D10F60)
  <primary:  TAG adj out of GigabitEthernet0/0/2, addr 7.7.7.2 35E88380>
Disposition details:
```

```
 Local label: 16
 Control Word: enabled, Sequencing: disabled
 SSS Switch: 3976200193
 Output chain:  mpls_eos( connid router-alert AToM Disp (locks 5)/ drop)
```

show platform hardware pp active feature cef database

次に、**show platform hardware pp active feature cef database** コマンドの出力例を示します。

```
Device# show platform hardware pp active feature cef database ipv4 16.16.16.16/32
=== CEF Prefix ===
16.16.16.16/32 -- next hop: UEA Label OCE (PI:0x104abee0, PD:0x10e6b9c8)
                Route Flags: (0)
                Handles (PI:0x104ab6e0) (PD:0x10e68140)

  HW Info:
    TCAM handle: 0x0000023f    TCAM index: 0x0000000d
    FID index  : 0x0000f804    EAID      : 0x0000808a
    MET        : 0x0000400c    FID Count : 0x00000000

=== Label OCE ===
  Label flags: 4
  Num Labels: 1
  Num Bk Labels: 1
  Out Labels: 16
  Out Backup Labels: 44
  Next OCE Type: Fast ReRoute OCE; Next OCE handle: 0x10e6f428

=== FRR OCE ===
  FRR type         : IP FRR
  FRR state        : Primary
  Primary IF's gid : 3
  Primary FID      : 0x0000f801
  FIFC entries     : 32
  PPO handle       : 0x00000000
  Next OCE         : Adjacency (0x10e63b38)
  Bkup OCE         : Adjacency (0x10e6e590)

=== Adjacency OCE ===
  Adj State: COMPLETE(0)   Address: 7.7.7.2
  Interface: GigabitEthernet0/0/2   Protocol: TAG
  mtu:1500, flags:0x0, fixups:0x0, encap_len:14
  Handles (adj_id:0x00000039) (PI:0x1041d410) (PD:0x10e63b38)
  Rewrite Str: d0:c2:82:17:8a:82:d0:c2:82:17:f2:02:88:47

  HW Info:
    FID index: 0x0000f486    EL3 index: 0x00001003    EL2 index: 0x00000000
    El2RW    : 0x00000107    MET index: 0x0000400c    EAID     : 0x00008060
    HW ADJ FLAGS: 0x40
    Hardware MAC Rewrite Str: d0:c2:82:17:8a:82:08:00:40:00:0d:02

=== Adjacency OCE ===
  Adj State: COMPLETE(0)   Address: 7.7.17.9
  Interface: GigabitEthernet0/0/7   Protocol: TAG
  mtu:1500, flags:0x0, fixups:0x0, encap_len:14
  Handles (adj_id:0x00000012) (PI:0x104acbd0) (PD:0x10e6e590)
  Rewrite Str: d0:c2:82:17:c9:83:d0:c2:82:17:f2:07:88:47

  HW Info:
    FID index: 0x0000f49d    EL3 index: 0x00001008    EL2 index: 0x00000000
    El2RW    : 0x00000111    MET index: 0x00004017    EAID     : 0x0000807d
    HW ADJ FLAGS: 0x40
    Hardware MAC Rewrite Str: d0:c2:82:17:c9:83:08:00:40:00:0d:07
```

例：VPLS 対応リモート LFA FRR の設定

例：内部ゲートウェイ プロトコル（IGP）対応リモート LFA FRR の設定

```
router isis hp
 net 49.0101.0000.0000.0802.00
 is-type level-2-only
 ispf level-2
 metric-style wide
 fast-flood
 set-overload-bit on-startup 180
 max-lsp-lifetime 65535
 lsp-refresh-interval 65000
 spf-interval 5 50 200
 prc-interval 5 50 200
 lsp-gen-interval 5 5 200
 no hello padding
 log-adjacency-changes
 nsf cisco
 fast-reroute per-prefix level-1 all
 fast-reroute per-prefix level-2 all
 fast-reroute remote-lfa level-1 mpls-ldp
 fast-reroute remote-lfa level-2 mpls-ldp
 passive-interface Loopback0
 mpls ldp sync
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
```

例：インターフェイス レベルでの VPLS 対応リモート LFA FRR の設定

```
!
interface GigabitEthernet0/3/3
 ip address 198.51.100.1 255.255.255.0
 ip router isis hp
 logging event link-status
 load-interval 30
 negotiation auto
 mpls ip
 mpls traffic-eng tunnels
 isis network point-to-point
end
!
```

例：グローバル レベルでの VPLS 対応リモート LFA FRR の設定

```
!
l2 vfi Test-2000 manual
 vpn id 2010
 bridge-domain 2010
 neighbor 192.0.2.1 encapsulation mpls
!
```

例：アクセス側での VPLS 対応リモート LFA FRR の設定

```
!
interface TenGigabitEthernet0/2/0
 no ip address
 service instance trunk 1 ethernet
  encapsulation dot1q 12-2012
  rewrite ingress tag pop 1 symmetric
  bridge-domain from-encapsulation
 !
```

例：VPLS 対応リモート LFA FRR の確認

show ip cef internal

次に、**show ip cef internal** コマンドの出力例を示します。

```
Router# show ip cef 198.51.100.2/32 internal

198.51.100.2/32, epoch 2, RIB[I], refcount 7, per-destination sharing
  sources: RIB, RR, LTE
  feature space:
   IPRM: 0x00028000
   Broker: linked, distributed at 1st priority
   LFD: 198.51.100.2/32 1 local label
   local label info: global/2033
        contains path extension list
        disposition chain 0x46764E68
        label switch chain 0x46764E68
  subblocks:
   1 RR source [heavily shared]
    non-eos chain [explicit-null|70]
  ifnums:
   TenGigabitEthernet0/1/0(15): 192.0.2.10
   MPLS-Remote-Lfa2(46)
  path 44CE1290, path list 433CF8C0, share 1/1, type attached nexthop, for IPv4, flags
has-repair
    MPLS short path extensions: MOI flags = 0x21 label explicit-null
  nexthop 192.0.2.10 TenGigabitEthernet0/1/0 label [explicit-null|70], adjacency IP adj out
 of TenGigabitEthernet0/1/0, addr 192.0.2.10 404B3960
    repair: attached-nexthop 192.0.2.1 MPLS-Remote-Lfa2 (44CE1300)
  path 44CE1300, path list 433CF8C0, share 1/1, type attached nexthop, for IPv4, flags
repair, repair-only
  nexthop 192.0.2.1 MPLS-Remote-Lfa2, repair, adjacency IP midchain out of MPLS-Remote-Lfa2
 404B3B00
  output chain: label [explicit-null|70]
  FRR Primary (0x3E25CA00)
  <primary:  TAG adj out of TenGigabitEthernet0/1/0, addr 192.168.101.22 404B3CA0>
  <repair:  TAG midchain out of MPLS-Remote-Lfa2 404B37C0 label 37 TAG adj out of
GigabitEthernet0/3/3, addr 192.0.2.14 461B2F20>
```

show ip cef detail

次に、**show ip cef detail** コマンドの出力例を示します。

```
Router# show ip cef 198.51.100.2/32 detail

198.51.100.2/32, epoch 2
  local label info: global/2033
  1 RR source [heavily shared]
  nexthop 192.0.2.14 TenGigabitEthernet0/1/0 label [explicit-null|70]
    repair: attached-nexthop 192.0.2.1 MPLS-Remote-Lfa2
  nexthop 192.0.2.1 MPLS-Remote-Lfa2, repair
!
```

show platform hardware pp active feature cef databas

次に、**show platform hardware pp active feature cef database** コマンドの出力例を示します。

```
Router# show platform hardware pp active feature cef database ipv4 198.51.100.2/32

=== CEF Prefix ===
198.51.100.2/32 -- next hop: UEA Label OCE (PI:0x10936770, PD:0x12dd1cd8)
                Route Flags: (0)
                Handles (PI:0x109099c8) (PD:0x12945968)

  HW Info:
```

```
    TCAM handle: 0x00000266    TCAM index: 0x00000015
    FID index  : 0x00008e7f    EAID      : 0x0001d7c4
    MET        : 0x0000401c    FID Count : 0x00000000
=== Label OCE ===
  Label flags: 4
  Num Labels: 1
  Num Bk Labels: 1
  Out Labels: 0
  Out Backup Labels: 70
=== FRR OCE ===
  FRR type         : IP FRR
  FRR state        : Primary
  Primary IF's gid : 52
  Primary FID      : 0x00008cb6
  FIFC entries     : 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0
  PPO handle       : 0x00000000
  Next OCE         : Adjacency (0x130e0df0)
  Bkup OCE         : Adjacency (0x130de608)

=== Adjacency OCE ===
  Adj State: COMPLETE(0)   Address: 192.168.101.22
  Interface: TenGigabitEthernet0/1/0   Protocol: TAG
  mtu:1500, flags:0x0, fixups:0x0, encap_len:14
  Handles (adj_id:0x000016ac) (PI:0x1090cc10) (PD:0x130e0df0)
  Rewrite Str: 18:33:9d:3d:83:10:c8:f9:f9:8d:04:10:88:47
HW Info:
    FID index: 0x00008e7e    EL3 index: 0x00001034    EL2 index: 0x00000000
    El2RW    : 0x0000010d    MET index: 0x00004012    EAID     : 0x0001d7c1
    HW ADJ FLAGS: 0x40
    Hardware MAC Rewrite Str: 18:33:9d:3d:83:10:08:00:40:00:0d:10
=== Adjacency OCE ===
  Adj State: COMPLETE(0)   Address: 0
  Interface: MPLS-Remote-Lfa2   Protocol: TAG
  mtu:17940, flags:0x40, fixups:0x0, encap_len:0
  Handles (adj_id:0xf80002e8) (PI:0x10da2150) (PD:0x130de608)
  Rewrite Str:

  HW Info:
    FID index: 0x00008ca8    EL3 index: 0x0000101c    EL2 index: 0x00000000
    El2RW    : 0x00000003    MET index: 0x00004024    EAID     : 0x0001d7cb
    HW ADJ FLAGS: 0x40
    Hardware MAC Rewrite Str: 00:00:00:00:00:00:00:00:00:00:00:00

=== Label OCE ===
  Label flags: 4
  Num Labels: 1
Num Bk Labels: 1
  Out Labels: 37
  Out Backup Labels: 37
  Next OCE Type: Adjacency; Next OCE handle: 0x12943a00
=== Adjacency OCE ===
  Adj State: COMPLETE(0)   Address: 30.1.1.1
  Interface: GigabitEthernet0/3/3   Protocol: TAG
  mtu:1500, flags:0x0, fixups:0x0, encap_len:14
  Handles (adj_id:0x0000378e) (PI:0x10909738) (PD:0x12943a00)
  Rewrite Str: c8:f9:f9:8d:01:b3:c8:f9:f9:8d:04:33:88:47

  HW Info:
    FID index: 0x00008c78    EL3 index: 0x0000101c    EL2 index: 0x00000000
    El2RW    : 0x00000109    MET index: 0x0000400e    EAID     : 0x0001cf4b
    HW ADJ FLAGS: 0x40
    Hardware MAC Rewrite Str: c8:f9:f9:8d:01:b3:08:00:40:00:0d:33
```

show mpls l2transport detail

次に、**show mpls l2transport detail** コマンドの出力例を示します。

```
Router# show mpls l2transport vc 2000 detail

Local interface: VFI Test-1990 vfi up
```

```
Interworking type is Ethernet
Destination address: 192.0.2.1, VC ID: 2000, VC status: up
  Output interface: Te0/1/0, imposed label stack {0 2217}
  Preferred path: not configured
  Default path: active
  Next hop: 192.51.100.22
Create time: 1d08h, last status change time: 1d08h
  Last label FSM state change time: 1d08h
Signaling protocol: LDP, peer 192.0.51.1:0 up
  Targeted Hello: 192.51.100.2(LDP Id) -> 192.51.100.200, LDP is UP
  Graceful restart: configured and enabled
  Non stop routing: not configured and not enabled
  Status TLV support (local/remote)   : enabled/supported
    LDP route watch                   : enabled
    Label/status state machine        : established, LruRru
    Last local dataplane   status rcvd: No fault
    Last BFD dataplane     status rcvd: Not sent
    Last BFD peer monitor  status rcvd: No fault
    Last local AC  circuit status rcvd: No fault
    Last local AC  circuit status sent: No fault
    Last local PW i/f circ status rcvd: No fault
    Last local LDP TLV     status sent: No fault
    Last remote LDP TLV    status rcvd: No fault
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
MPLS コマンド	『Multiprotocol Label Switching Command Reference』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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。	http://www.cisco.com/cisco/web/support/index.html

L2VPN 対応 Loop-Free Alternate Fast Reroute の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、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。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *43*：*L2VPN* 対応 *Loop-Free Alternate Fast Reroute* の機能情報

機能名	リリース	機能情報
L2VPN 対応 Loop-Free Alternate Fast Reroute	15.3(2)S Cisco IOS XE Release 3.9S Cisco IOS XE Release 3.10 S	この機能により、レイヤ 2 VPN（L2VPN）および Virtual Private Wire Service（VPWS）での Loop-Free Alternate（LFA）Fast Reroute（FRR）のサポートが追加され、リンク障害またはノード障害によるパケット損失が最小限に抑えられます。 追加または変更されたコマンドはありません。 Cisco IOS XE Release 3.9S では、Cisco ASR 903 ルータのサポートが追加されました。 Cisco IOS XE Release 3.10S では、Cisco ASR 903 ルータの ATM（IMA）および TDM 擬似回線でのリモート LFA FRR のサポートが追加されました。 Cisco IOS XE Release 3.10S では、Cisco ASR 903 ルータの VPLS でのリモート LFA FRR のサポートが追加されました。