



# MPLS VPN InterAS オプションの設定

- [MPLS VPN InterAS オプションに関する情報](#) (1 ページ)
- [MPLS VPN InterAS オプションの設定方法](#) (9 ページ)
- [MPLS VPN InterAS オプションの設定の確認](#) (25 ページ)
- [MPLS VPN InterAS オプションの設定例](#) (26 ページ)
- [MPLS VPN InterAS オプションに関するその他の参考資料](#) (42 ページ)
- [MPLS VPN InterAS オプションの機能履歴](#) (42 ページ)

## MPLS VPN InterAS オプションに関する情報

MPLS VPN InterAS オプションは、異なる MPLS VPN サービスプロバイダー間で VPN を相互接続するさまざまな方法を提供します。これにより、お客様のサイトを複数のキャリアネットワーク（自律システム）に存在させ、サイト間でのシームレスな VPN 接続が可能になります。

### ASE および ASBR

自律システム（AS）とは、共通のシステム管理グループによって管理され、単一の明確に定義されたプロトコルを使用している単一のネットワークまたはネットワークのグループのことです。多くの場合、VPN は異なる地理的領域の異なる AS に拡張されます。一部の VPN は、複数のサービスプロバイダーにまたがって拡張する必要があり、それらはオーバーラッピング VPN と呼ばれます。VPN の複雑さや場所に関係なく、AS 間の接続はお客様に対してシームレスである必要があります。

AS 境界ルータ（ASBR）は、複数のルーティングプロトコルを使用して設定された AS 内のデバイスであり、外部ルーティングプロトコル（eBGP など）またはスタティックルートを使用するか、あるいは両方を使用して、他の ASBR とルーティング情報を交換します。

異なるサービスプロバイダーからの個別の AS は、VPN IP アドレスの形式で情報を交換することによって通信し、次のプロトコルを使用してルーティング情報を共有します。

- AS 内では、ルーティング情報は iBGP を使用して共有されます。

iBGP は、各 VPN および各 AS 内の IP プレフィックスのネットワーク層情報を配布します。

- AS 間では、ルーティング情報は eBGP を使用して共有されます。

eBGP を使用することで、サービスプロバイダーは別の AS 間でのルーティング情報のループフリー交換を保証するインタードメインルーティングシステムを設定できます。eBGP の主な機能は、AS ルートのリストに関する情報を含む、AS 間のネットワーク到達可能性情報を交換することです。AS は、eBGP ボーダーエッジルータを使用してラベルスイッチング情報を含むルートを配布します。各ボーダーエッジルータでは、ネクストホップおよび MPLS ラベルが書き換えられます。

MPLS VPN InterAS オプションの設定はサポートされており、異なるボーダーエッジルータで接続されている 2 つ以上の AS を含む MPLS VPN であるプロバイダー間 VPN を含めることができます。AS は eBGP を使用してルートを交換し、iBGP やルーティング情報は AS 間で交換されません。

## MPLS VPN InterAS オプション

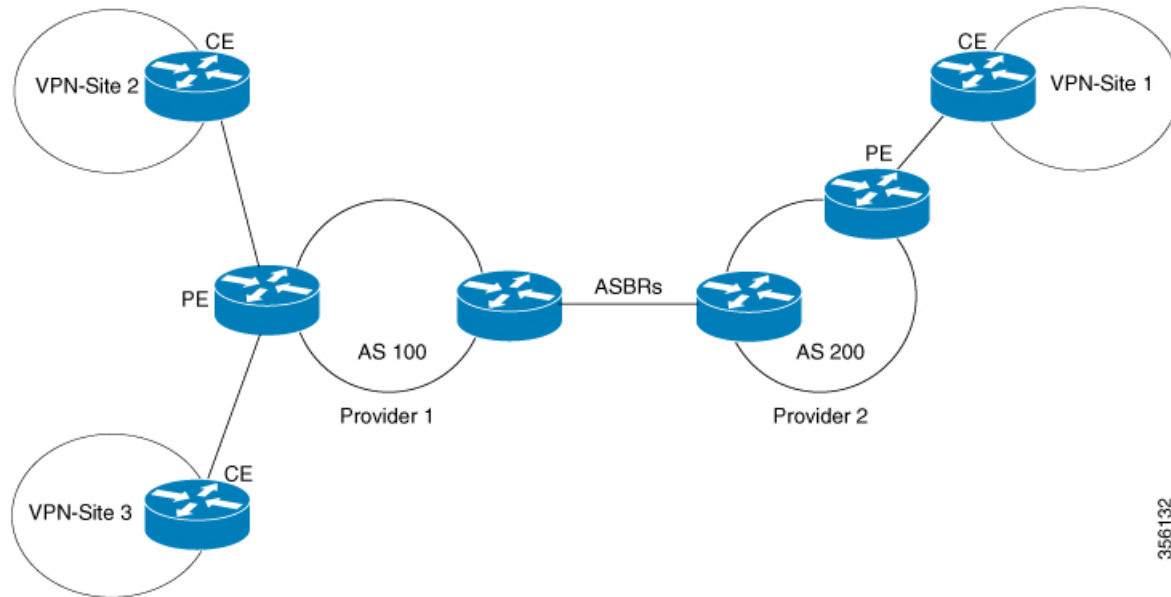
RFC4364 で定義されている次のオプションは、異なる AS 間の MPLS VPN 接続を提供します。

- InterAS オプション B : このオプションは、ASBR 間の VPNv4 ルート配布を提供します。
- InterAS オプション AB : このオプションは、InterAS オプション A ネットワークと InterAS オプション B ネットワークの最良の機能を組み合わせたものです。MPLS VPN サービスプロバイダーは、さまざまな自律システムを相互接続して VPN サービスを提供できます。

### InterAS オプション B

InterAS オプション B ネットワークでは、ASBR ポートは、MPLS トラフィックを受信できる 1 つ以上のインターフェイスによって接続されます。このオプションを使用すると、ASBR は eBGP セッションを使用して相互にピアリングします。ASBR は PE ルータとしても機能し、AS 内のすべての PE ルータとピアリングします。ASBR は VRF を保持しませんが、他の AS に渡す必要がある PE ルータからの VPNv4 ルートのすべてまたはサブセットを保持します。VPNv4 ルートは、route-distinguisher を使用して ASBR で一意に維持され、ルートターゲットを使用してフィルタリングされます。ASBR は、eBGP を使用して VPNv4 ルートと VPN ラベルを交換します。

図 1: InterAS オプション B のトポロジ



ASBR 間で VPNv4 ルートのネクストホップを配布するための 2 つの方法がサポートされています。2 つの ASBR を接続するリンクで LDP または IGP を有効にする必要はありません。ASBR 上の直接接続されたインターフェイス間の MP-eBGP セッションにより、インターフェイスはラベル付きパケットを転送できます。直接接続された BGP ピアに対してこの MPLS 転送を保証するには、ASBR に接続するインターフェイスで `mpls bgp forwarding` コマンドを設定する必要があります。このコマンドは、直接接続されたインターフェイスの IOS に実装されています。最大 200 の BGP ネイバーを設定できます。

- **ネクストホップセルフ方式**：ネクストホップを他の ASBR から学習したすべての VPNv4 ルートのローカル ASBR のネクストホップに変更します。
- **Redistribute Connected Subnet 方式**：`redistribute connected subnets` コマンドを使用して、リモート ASBR のネクストホップアドレスをローカル IGP に再配布します。つまり、VPNv4 ルートがローカル AS に再配布されても、ネクストホップは変更されません。

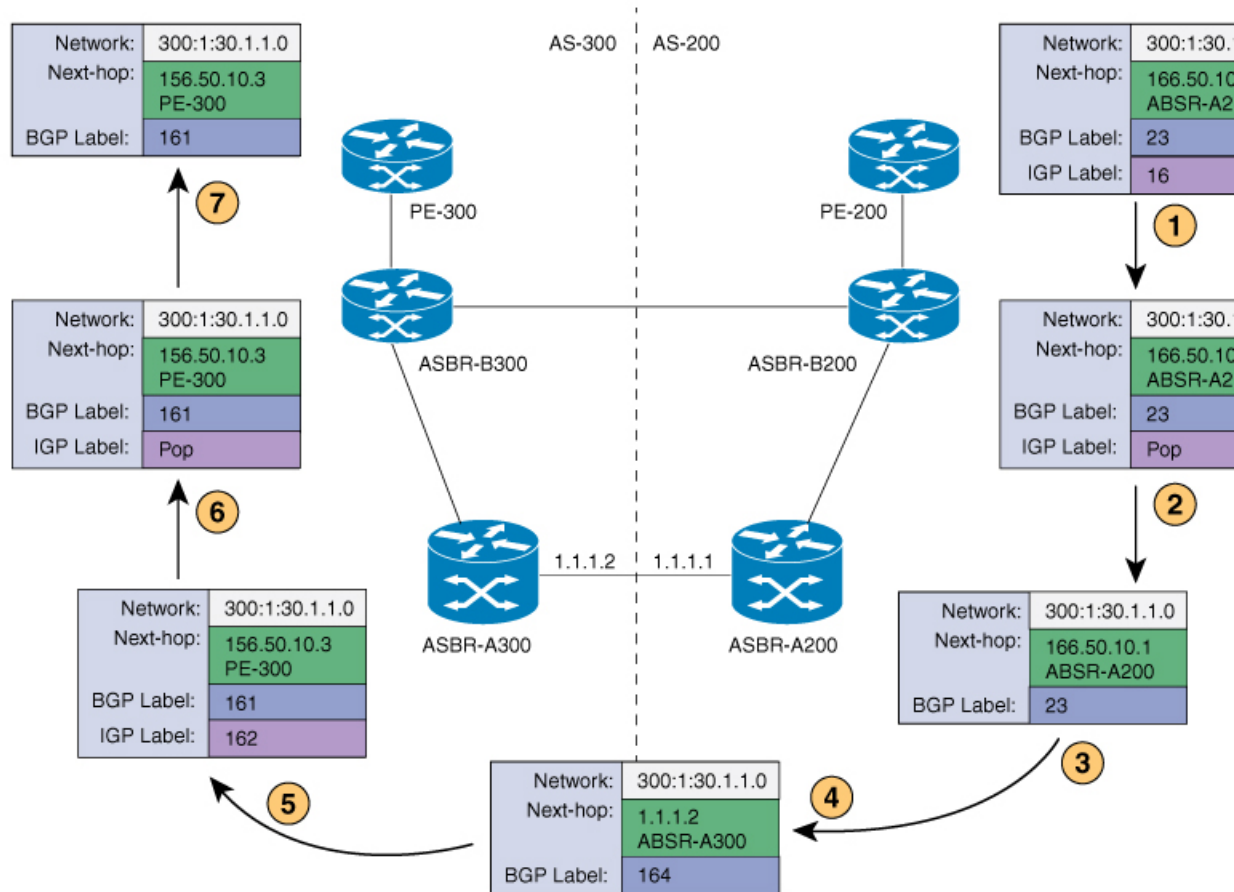


(注) 等コストパス（リモート AS への ECMP）が複数ある場合は、ASBR 上のリモートループバックに対する MPLS スタティック ラベルバインディングを設定する必要があります。そのように設定しないと、パケットが損失する場合があります。

次に説明するラベルスイッチパス転送の項では、AS200 はネクストホップセルフ方式で設定されており、AS300 は Redistribute Subnet 方式で設定されています。

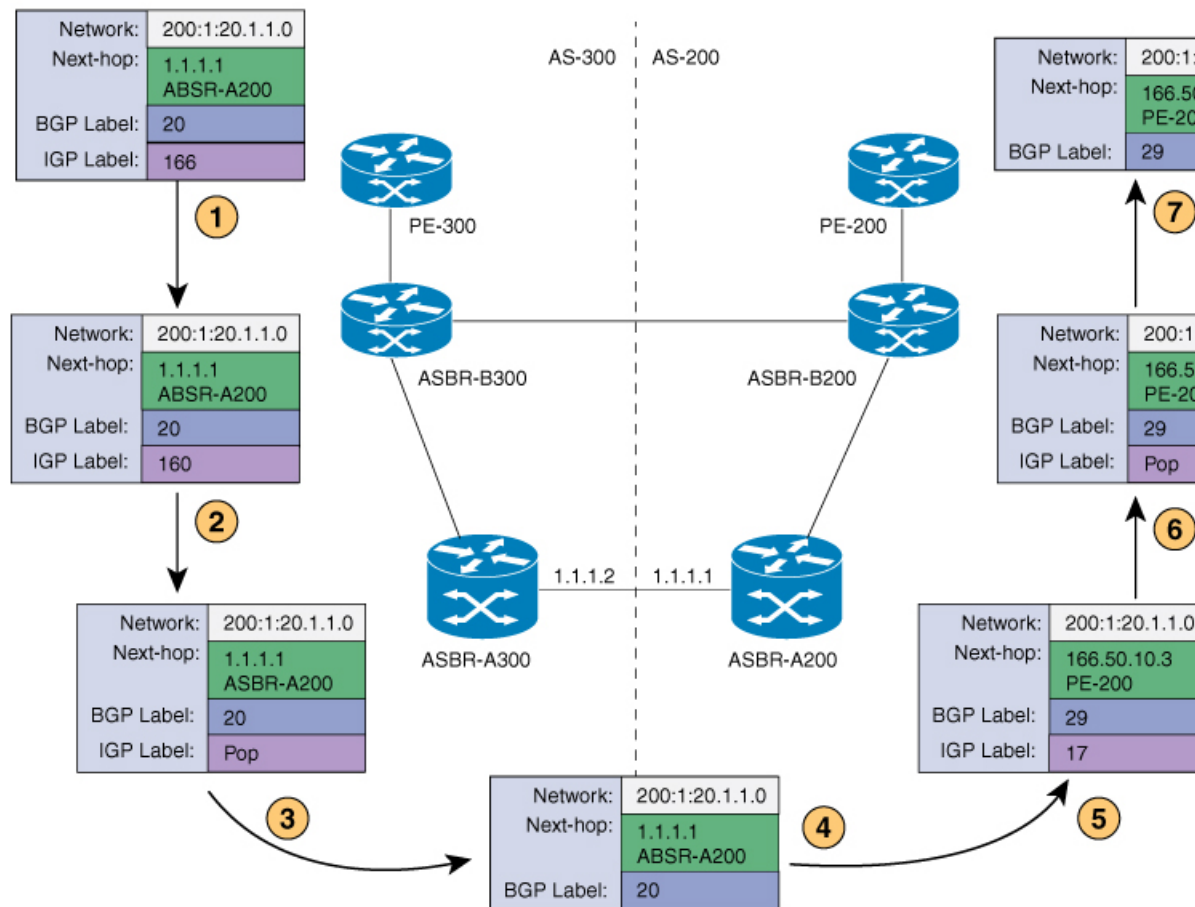
## ネクストホップセルフ方式

次の図に、ネクストホップセルフ方式のラベル転送パスを示します。パケットが AS 200 の PE-200 から AS 300 の PE-300 に到達するときに、ラベルがスタックにプッシュ、スワップ、およびポップされます。ステップ 5 で、ASBR-A300 はラベル付きフレームを受信し、ラベル 164 をラベル 161 に置き換え、IGP ラベル 162 をラベルスタックにプッシュします。



## Redistribute Connected Subnet 方式

次の図に、Redistribute Connected Subnet 方式のラベル転送パスを示します。パケットが AS 300 の PE-300 から AS 200 の PE-200 に移動するときに、ラベルがスタックにプッシュ、スワップ、およびポップされます。ステップ 5 で、ASBR-A200 は BGP ラベル 20 のフレームを受信し、ラベル 29 と交換し、ラベル 17 をプッシュします。



## InterAS オプション AB

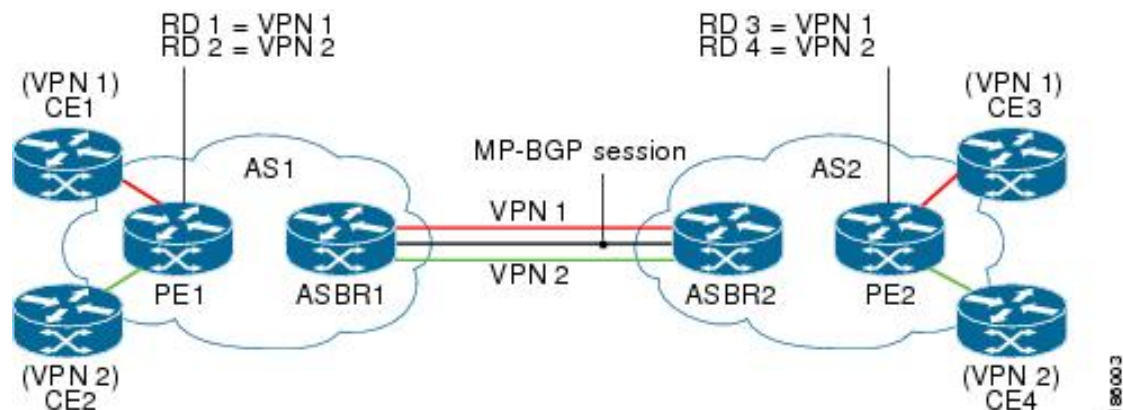
MPLS VPN サービス プロバイダーは、さまざまな自律システムを相互接続して、複数の VPN カスタマーにサービスを提供する必要があります。MPLS VPN InterAS オプション AB 機能を使用すると、グローバルルーティングテーブル内の単一の MP-BGP セッションを使用してさまざまな自律システムを相互接続し、コントロールプレーン Traffic を伝送できます。この MP-BGP セッションでは、2つの ASBR 間で、各 VRF インスタンスの VPN プレフィックスがシグナリングされます。この Traffic は、IP または MPLS です。

送信される VPN Traffic は VRF 固有のインターフェイスを経由する IP Traffic であるため、2つの ASBR 間で MPLS BGP 転送または LDP を設定する必要はありません。

InterAS オプション AB 機能には、サービスプロバイダーにとって次の利点があります。

- ASBR ピア間の IP QoS 機能を維持し、カスタマー SLA を実現できます。
- データプレーン Traffic は、セキュリティ上の目的で VRF ごとに分離されます。
- SVI にポリシーを付加することで、専用の QoS ポリシーを各 VRF に適用できます。

## ルート配布およびパケット転送



次の属性は、上の図に示されているサンプル InterAS オプション AB ネットワークのトポロジを示しています。

- CE1 と CE3 は VPN 1 に属しています。
- CE2 と CE4 は VPN 2 に属しています。
- PE1 では、VPN 1 (VRF 1) にルート識別子 1 (RD 1) を、VPN 2 (VRF 2) に RD 2 を使用しています。
- PE2 は、VPN 1 (VRF 1) に RD 3 を、VPN 2 (VRF 2) に RD 4 を使用しています。
- ASBR1 では、VRF 1 が RD 5 に、VRF 2 が RD 6 にプロビジョニングされています。
- ASBR2 では、VRF 1 が RD 7 に、VRF 2 が RD 8 にプロビジョニングされています。
- ASBR1 と ASBR2 との間には 3 つのリンクがあります。
  - VRF 1
  - VRF 2
  - MP-BGP セッション

## VPN 1 のルート配布

ルート識別子 (RD) は、各ルートにどの VPN が属しているかを識別するためにルートに付加される識別子です。各ルーティングインスタンスには、一意な RD 自律システムが関連付けられている必要があります。RD は、VPN の周囲に境界を設置して、異なる VPN で同じ IP アドレスプレフィックスを使用してもこれらの IP アドレスプレフィックスが重複しないようにするために使用されます。RD 文は、インスタンスタイプが VRF である場合は必須です。

次のプロセスは、上記の図の VPN 1 のルート配布プロセスを示しています。このプロセスで使用されているプレフィックス「N」は、VPN の IP アドレスを示しています。

## ASBR1

- CE1 は、プレフィックス N を PE1 にアドバタイズします。

- PE1 は、VPN プレフィックス RD 1:N を ASBR1 に MP-iBGP 経由でアドバタイズします。
- ASBR1 は、プレフィックスを VPN 1 にインポートして、プレフィックス RD 5:N を作成します。
- ASBR1 は、インポートしたプレフィックス RD 5:N を ASBR2 にアドバタイズします。ASBR1 は、自身をプレフィックス RD 5:N のネクストホップとして設定し、このプレフィックスとともにシグナリングされるローカルラベルを割り当てます。
- ASBR1 は、最初に受信した RT ではなく、VRF に設定されたエクスポート RT を使用してルートをアドバタイズします。デフォルトで、ASBR1 はソースプレフィックス RD 1:N を ASBR2 にアドバタイズしません。このプレフィックスは、オプション AB VRF にインポートされるプレフィックスであるため、アドバタイズされません。

#### ASBR2

- ASBR2 は、プレフィックス RD 5:N を受信して、RD 7:N として VPN 1 にインポートします。
- ASBR2 は、最初に受信した RT ではなく、VRF に設定されたエクスポート RT を使用してルートをアドバタイズします。
- プレフィックスのインポート時に、ASBR2 は RD 7:N のネクストホップを VRF 1 の ASBR1 インターフェイス IP アドレスに設定します。ネクストホップテーブル ID も VRF 1 に設定されます。RD 7:N 用の MPLS 転送エントリをインストールする場合、デフォルトでは ASBR2 は転送プロセスで発信ラベルをインストールしません。これにより、ASBR 間のトラフィックを IP にすることができます。
- ASBR2 は、インポートしたプレフィックス RD 7:N を PE2 にアドバタイズします。ASBR2 は、自身をこのプレフィックスのネクストホップとして設定し、このプレフィックスとともにシグナリングされるローカルラベルも割り当てます。デフォルトで、ASBR2 はソースプレフィックス RD 5:N を PE2 にアドバタイズしません。このプレフィックスは、オプション AB VRF にインポートされるプレフィックスであるため、アドバタイズされません。
- PE2 は、RD 7:N を RD 3:N として VRF 1 にインポートします。

#### VPN 1 のパケット転送

次のパケット転送プロセスは、オプション A のシナリオと同様に動作します。ASBR は VPN の終端となることによって PE と同様に動作し、トラフィックを標準 IP パケットとして VPN ラベルなしで次の PE に転送します。その後、次の PE で VPN プロセスが繰り返されます。したがって、各 PE デバイスは隣接 PE デバイスを CE デバイスとして扱い、各自律システムでのルート再配布には標準的なレイヤ 3 MPLS VPN メカニズムが使用されます。つまり、各 PE は、外部 BGP (eBGP) を使用して相互にラベルなし IPv4 アドレスを配布します。

- CE3 は、N 宛てのパケットを PE2 に送信します。

- PE2 は、ASBR2 によって割り当てられた VPN ラベル、およびパケットを ASBR2 にトンネリングするために必要な内部ゲートウェイプロトコル (IGP) ラベルでパケットをカプセル化します。
- パケットは、VPN ラベルが付いた状態で ASBR2 に到達します。ASBR2 は VPN ラベルを削除し、パケットを IP として ASBR1 の VRF 1 インターフェイスに送信します。
- IP パケットが、ASBR1 の VRF 1 インターフェイスに到達します。ASBR1 は、PE1 によって割り当てられた VPN ラベル、およびパケットを PE1 にトンネリングするために必要な IGP ラベルでパケットをカプセル化します。
- パケットは、VPN ラベルが付いた状態で PE1 に到達します。PE1 は VPN ラベルを削除して、IP パケットを CE1 に転送します。

## VPN 2 のルート配布

次の情報は、上記の図の VPN 2 のルート配布プロセスを示しています。

### ASBR1

- CE2 は、プレフィックス N を PE1 にアドバタイズします。N は VPN IP アドレスです。
- PE1 は、VPN プレフィックス RD 2:N を ASBR1 に MP-iBGP 経由でアドバタイズします。
- ASBR1 は、プレフィックスを VPN 2 にインポートして、プレフィックス RD 6:N を作成します。
- ASBR1 は、インポートしたプレフィックス RD 6:N を ASBR2 にアドバタイズします。ASBR2 は、自身をこのプレフィックスのネクストホップとして設定し、このプレフィックスとともにシグナリングされるローカルラベルも割り当てます。デフォルトで、ASBR1 はソースプレフィックス RD 2:N を ASBR2 にアドバタイズしません。このプレフィックスは、オプション AB VRF にインポートされるプレフィックスであるため、アドバタイズされません。

### ASBR2

- ASBR2 は、プレフィックス RD 6:N を受信して、RD 8:N として VPN 2 にインポートします。
- プレフィックスのインポート時に、ASBR2 は RD 8:N のネクストホップを VRF 2 の ASBR1 インターフェイスアドレスに設定します。ネクストホップテーブル ID も VRF 2 の ID に設定されます。RD 8:N 用の MPLS 転送エントリをインストールする場合、デフォルトでは ASBR2 は転送プロセスで発信ラベルをインストールしません。これにより、ASBR 間のトラフィックを IP にすることができます。
- ASBR2 は、インポートしたプレフィックス RD 8:N を PE2 にアドバタイズします。ASBR2 は、自身をこのプレフィックスのネクストホップとして設定し、このプレフィックスとともにシグナリングされるローカルラベルも割り当てます。デフォルトで、ASBR2 はソースプレフィックス RD 6:N を PE2 にアドバタイズしません。このプレフィックスは、オプション AB VRF にインポートされるプレフィックスであるため、アドバタイズされません。



- PE2 は、RD 8:N を RD 4:N として VRF 2 にインポートします。

## MPLS VPN InterAS オプションの設定方法

次の項では、MPLS VPN InterAS オプションの設定方法について説明します。

### MPLS VPN InterAS オプション B の設定

#### ネクストホップセルフ方式を使用した InterAS オプション B の設定

ネクストホップセルフ方式を使用して ASBR で InterAS オプション B を設定するには、次の手順を実行します。

##### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	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	<b>router ospf process-id</b> 例： Device(config)# <b>router ospf 1</b>	OSPF ルーティングプロセスを設定し、プロセス番号を割り当てます。
ステップ 4	<b>router-id ip-address</b> 例： Device(config)# <b>router-id 4.1.1.1</b>	固定ルータ ID を指定します。
ステップ 5	<b>nsr</b> 例： Device(config-router)# <b>nsr</b>	OSPF ノンストップルーティング (NSR) を設定します。
ステップ 6	<b>nsf</b> 例：	OSPF ノンストップフォワーディング (NSF) を設定します。

	コマンドまたはアクション	目的
	Device(config-router)# <b>nsf</b>	
ステップ 7	<b>redistribute bgp</b> <i>autonomous-system-number</i> 例 :  Device(config-router)# <b>redistribute bgp 200</b>	BGP 自律システムからルートを OSPF ルーティングプロセスに再配布します。
ステップ 8	<b>passive-interface interface-type</b> <i>interface-number</i> 例 :  Device(config-router)# <b>passive-interface GigabitEthernet 1/0/10</b> Device(config-router)# <b>passive-interface Tunnel0</b>	インターフェイスの Open Shortest Path First (OSPF) ルーティングアップデートを無効にします。
ステップ 9	<b>network ip-address wildcard-mask aread</b> <i>area-id</i> 例 :  Device(config-router)# <b>network 4.1.1.0 0.0.0.0.255 area 0</b>	OSPF を実行するインターフェイスを定義し、そのインターフェイスに対するエリア ID を定義します。
ステップ 10	<b>exit</b> 例 :  Device(config-router)# <b>exit</b>	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 11	<b>router bgp autonomous-system-number</b> 例 :  Device(config)# <b>router bgp 200</b>	BGP ルーティングプロセスを設定します。
ステップ 12	<b>bgp router-id ip-address</b> 例 :  Device(config-router)# <b>bgp router-id 4.1.1.1</b>	BGP ルーティングプロセスの固定ルータ ID を設定します。
ステップ 13	<b>bgp log-neighbor changes</b> 例 :  Device(config-router)# <b>bgp log-neighbor changes</b>	BGP ネイバールセットのロギ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 14	<b>no bgp default ipv4-unicast</b> 例 :  Device(config-router)# <b>no bgp default ipv4-unicast</b>	アドレスファミリー IPv4 のルーティング情報のアドバタイズメントを無効にします。
ステップ 15	<b>no bgp default route-target filter</b> 例 :  Device(config-router)# <b>no bgp default route-target filter</b>	BGP の route-target コミュニティフィルタリングを無効にします。
ステップ 16	<b>neighbor ip-address remote-as as-number</b> 例 :  Device(config-router)# <b>neighbor 4.1.1.3 remote-as 200</b>	エントリを BGP ネイバーテーブルに設定します。
ステップ 17	<b>neighbor ip-address update-source interface-type interface-number</b> 例 :  Device(config-router)# <b>neighbor 4.1.1.3 update-source Loopback0</b>	Cisco IOS ソフトウェアで、BGP セッションによる TCP 接続の特定の動作インターフェイスを使用できるようになります。
ステップ 18	<b>neighbor ip-address remote-as as-number</b> 例 :  Device(config-router)# <b>neighbor 4.1.1.3 remote-as 300</b>	エントリを BGP ネイバーテーブルに設定します。
ステップ 19	<b>address-family ipv4</b> 例 :  Device(config-router)# <b>address-family ipv4</b>	標準 IP バージョン 4 アドレスプレフィックスを使用する BGP ルーティングセッションを設定するために、アドレスファミリー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	<b>neighbor ip-address activate</b> 例 :  Device(config-router-af)# <b>neighbor 10.32.1.2 activate</b>	BGP ネイバーとの情報交換を有効にします。
ステップ 21	<b>neighbor ip-address send-label</b> 例 :	隣接 BGP ルータに BGP ルートを含む MPLS ラベルを送信します。

	コマンドまたはアクション	目的
	Device(config-router-af) # <b>neighbor 10.32.1.2 send-label</b>	
ステップ 22	<b>exit address-family</b> 例 : Device(config-router-af) # <b>exit address-family</b>	BGP アドレス ファミリ サブモードを終了します。
ステップ 23	<b>address-family vpnv4</b> 例 : Device(config-router) # <b>address-family vpnv4</b>	アドレス ファミリ コンフィギュレーションモードでデバイスを設定して、標準 VPNv4 アドレスプレフィックスを使用する、BGP などのルーティングセッションを設定します。
ステップ 24	<b>neighbor ip-address activate</b> 例 : Device(config-router-af) # <b>neighbor 4.1.1.3 activate</b>	BGP ネイバーとの情報交換を有効にします。
ステップ 25	<b>neighbor ip-address send-community extended</b> 例 : Device(config-router-af) # <b>neighbor 4.1.1.3 send-community extended</b>	コミュニティ属性が BGP ネイバーに送信されるように指定します。
ステップ 26	<b>neighbor ip-address next-hop-self</b> 例 : Device(config-router-af) # <b>neighbor 4.1.1.3 next-hop-self</b>	ルータを BGP スピーキングネイバーのネクストホップとして設定します。これは、ネクストホップセルフ方式を実装するコマンドです。
ステップ 27	<b>neighbor ip-address activate</b> 例 : Device(config-router-af) # <b>neighbor 10.30.1.2 activate</b>	BGP ネイバーとの情報交換を有効にします。
ステップ 28	<b>neighbor ip-address send-community extended</b> 例 : Device(config-router-af) # <b>neighbor 10.30.1.2 send-community extended</b>	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。

	コマンドまたはアクション	目的
ステップ 29	<b>exit address-family</b> 例 :  Device (config-router-af) # <b>exit address-family</b>	BGP アドレス ファミリ サブモードを終了します。
ステップ 30	<b>bgp router-id ip-address</b> 例 :  Device (config-router) # <b>bgp router-id 4.1.1.3</b>	BGP ルーティングプロセスの固定ルータ ID を設定します。
ステップ 31	<b>bgp log-neighbor changes</b> 例 :  Device (config-router) # <b>bgp log-neighbor changes</b>	BGP ネイバーリセットのロギングを有効にします。
ステップ 32	<b>neighbor ip-address remote-as as-number</b> 例 :  Device (config-router) # <b>neighbor 4.1.1.1 remote-as 200</b>	エントリを BGP ネイバーテーブルに設定します。
ステップ 33	<b>neighbor ip-address update-source interface-type interface-number</b> 例 :  Device (config-router) # <b>neighbor 4.1.1.1 update-source Loopback0</b>	Cisco IOS ソフトウェアで、BGP セッションによる TCP 接続の特定の動作インターフェイスを使用できるようになります。
ステップ 34	<b>address-family vpv4</b> 例 :  Device (config-router) # <b>address-family vpv4</b>	アドレス ファミリ コンフィギュレーションモードでデバイスを設定して、標準 VPNv4 アドレスプレフィックスを使用する、BGP などのルーティングセッションを設定します。
ステップ 35	<b>neighbor ip-address activate</b> 例 :  Device (config-router-af) # <b>neighbor 4.1.1.1 activate</b>	BGP ネイバーとの情報交換を有効にします。
ステップ 36	<b>neighbor ip-address send-community extended</b> 例 :	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。

	コマンドまたはアクション	目的
	Device(config-router-af)# <b>neighbor 4.1.1.1 send-community extended</b>	
ステップ 37	<b>exit address-family</b> 例 :  Device(config-router-af)# <b>exit address-family</b>	BGP アドレス ファミリ サブモードを終了します。

## Redistribute Connected 方式を使用した InterAS オプション B の設定

Redistribute Connected 方式を使用して ASBR で InterAS オプション B を設定するには、次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :  Device> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例 :  Device# <b>configure terminal</b>	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	<b>router ospf process-id</b> 例 :  Device(config)# <b>router ospf 1</b>	OSPF ルーティングプロセスを設定し、プロセス番号を割り当てます。
ステップ 4	<b>router-id ip-address</b> 例 :  Device(config)# <b>router-id 5.1.1.1</b>	固定ルータ ID を指定します。
ステップ 5	<b>nsr</b> 例 :  Device(config-router)# <b>nsr</b>	OSPF ノンストップルーティング (NSR) を設定します。
ステップ 6	<b>nsf</b> 例 :	OSPF ノンストップフォワーディング (NSF) を設定します。

	コマンドまたはアクション	目的
	Device(config-router)# <b>nsf</b>	
ステップ 7	<b>redistribute connected</b> 例 : Device(config-router)# <b>redistribute connected</b>	リモート ASBR のネクストホップアドレスをローカル IGP に再配布します。これは、Redistribute Connected 方式を実装するコマンドです。
ステップ 8	<b>passive-interface interface-type interface-number</b> 例 : Device(config-router)# <b>passive-interface GigabitEthernet 1/0/10</b> Device(config-router)# <b>passive-interface Tunnel0</b>	インターフェイスの Open Shortest Path First (OSPF) ルーティングアップデートを無効にします。
ステップ 9	<b>network ip-address wildcard-mask aread area-id</b> 例 : Device(config-router)# <b>network 5.1.1.0 0.0.0.0.255 area 0</b>	OSPF を実行するインターフェイスを定義し、そのインターフェイスに対するエリア ID を定義します。
ステップ 10	<b>exit</b> 例 : Device(config-router)# <b>exit</b>	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 11	<b>router bgp autonomous-system-number</b> 例 : Device(config)# <b>router bgp 300</b>	BGP ルーティングプロセスを設定します。
ステップ 12	<b>bgp router-id ip-address</b> 例 : Device(config-router)# <b>bgp router-id 5.1.1.1</b>	BGP ルーティングプロセスの固定ルータ ID を設定します。
ステップ 13	<b>bgp log-neighbor changes</b> 例 : Device(config-router)# <b>bgp log-neighbor changes</b>	BGP ネイバーリセットのロギ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 14	<b>no bgp default ipv4-unicast</b> 例 :  Device(config-router) # <b>no bgp default ipv4-unicast</b>	アドレスファミリー IPv4 のルーティング情報のアドバタイズメントを無効にします。
ステップ 15	<b>no bgp default route-target filter</b> 例 :  Device(config-router) # <b>no bgp default route-target filter</b>	BGP の route-target コミュニティフィルタリングを無効にします。
ステップ 16	<b>neighbor ip-address remote-as as-number</b> 例 :  Device(config-router) # <b>neighbor 5.1.1.3 remote-as 300</b>	エントリを BGP ネイバーテーブルに設定します。
ステップ 17	<b>neighbor ip-address update-source interface-type interface-number</b> 例 :  Device(config-router) # <b>neighbor 4.1.1.3 update-source Loopback0</b>	Cisco IOS ソフトウェアで、BGP セッションによる TCP 接続の特定の動作インターフェイスを使用できるようになります。
ステップ 18	<b>neighbor ip-address remote-as as-number</b> 例 :  Device(config-router) # <b>neighbor 10.30.1.2 remote-as 200</b>	エントリを BGP ネイバーテーブルに設定します。
ステップ 19	<b>address-family vpv4</b> 例 :  Device(config-router) # <b>address-family vpv4</b>	アドレスファミリー コンフィギュレーションモードでデバイスを設定して、標準 VPNv4 アドレスプレフィックスを使用する、BGP などのルーティングセッションを設定します。
ステップ 20	<b>neighbor ip-address activate</b> 例 :  Device(config-router-af) # <b>neighbor 5.1.1.3 activate</b>	BGP ネイバーとの情報交換を有効にします。
ステップ 21	<b>neighbor ip-address send-community extended</b> 例 :	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。



	コマンドまたはアクション	目的
	Device(config-router-af)# <b>neighbor 5.1.1.3 send-community extended</b>	
ステップ 22	<b>neighbor ip-address activate</b> 例： Device(config-router-af)# <b>neighbor 10.30.1.1 activate</b>	BGP ネイバーとの情報交換を有効にします。
ステップ 23	<b>neighbor ip-address send-community extended</b> 例： Device(config-router-af)# <b>neighbor 10.30.1.2 send-community extended</b>	コミュニティ属性がBGP ネイバーに送信されるように指定します。
ステップ 24	<b>exit address-family</b> 例： Device(config-router-af)# <b>exit address-family</b>	BGP アドレス ファミリ サブモードを終了します。
ステップ 25	<b>mpls ldp router-id interface-id [force]</b> 例： Device(config-router)# <b>mpls ldp router-id Loopback0 force</b>	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。

## MPLS VPN Inter-AS オプション AB の設定

次の項では、MPLS VPN において ASBR で InterAS オプション AB 機能を設定する方法について説明します。

### 各 VPN カスタマーの ASBR インターフェイスへの VRF の設定

次の手順を実行して、各 VPN カスタマーの ASBR インターフェイスに VRF を設定し、それらの VPN が InterAS オプション AB ネットワークを介して接続できるようにします。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。  • 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	<b>configure terminal</b> 例：  Device# <b>configure terminal</b>	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	<b>interface type number</b> 例：  Device(config)# <b>interface gigabitethernet 1/0/1</b>	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	<b>ip vrf forwarding vrf-name</b> 例：  Device(config-if)# <b>ip vrf forwarding vpn1</b>	指定したインターフェイスに VRF を関連付けます。  • vrf-name 引数は、VRF に割り当てる名前です。
ステップ 5	<b>end</b> 例：  Device(config-if)# <b>end</b>	(任意) 終了して、特権 EXEC モードに戻ります。

## ASBR ピア間での MP-BGP セッションの設定

BGP では、IPv4 以外のアドレスファミリのサポートを定義する BGP マルチプロトコル拡張 (RFC 2283、Multiprotocol Extensions for BGP-4 を参照) を使用して、PE デバイス間の VPN-IPv4 プレフィックスの到達可能性情報を伝播します。この拡張を使用すると、指定された VPN のルートが、その VPN の他のメンバによってのみ学習されるようになり、VPN のメンバ間の相互通信が可能になります。

この項の次の手順に従って、ASBR で MP-BGP セッションを設定します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  Device> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します (要求された場合)。
ステップ 2	<b>configure terminal</b> 例：	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
	Device# <b>configure terminal</b>	
ステップ 3	<b>router bgp <i>as-number</i></b> 例 : Device(config)# <b>router bgp 100</b>	BGP ルーティング プロセスを設定し、デバイスでルータ コンフィギュレーション モードを開始します。 <ul style="list-style-type: none"> <li>• <b>as-number</b> 引数は、デバイスを他の BGP デバイスに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。有効な番号は 0 ~ 65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512 ~ 65535 です。</li> </ul>
ステップ 4	<b>neighbor {<i>ip-address</i>   <i>peer-group-name</i>} remote-as <i>as-number</i></b> 例 : Device(config-router)# <b>neighbor 192.168.0.1 remote-as 200</b>	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。 <ul style="list-style-type: none"> <li>• <b>ip-address</b> 引数には、ネイバーの IP アドレスを指定します。</li> <li>• <b>peer-group-name</b> 引数には、BGP ピア グループの名前を指定します。</li> <li>• <b>as-number</b> 引数には、ネイバーが属している自律システムを指定します。</li> </ul>
ステップ 5	<b>address-family vpnv4 [unicast]</b> 例 : Device(config-router)# <b>address-family vpnv4</b>	アドレス ファミリ コンフィギュレーション モードを開始して、標準 VPNv4 アドレス プレフィックスを使用する、BGP などのルーティング セッションを設定します。 <ul style="list-style-type: none"> <li>• <b>unicast</b> キーワードでは、IPv4 ユニキャスト アドレス プレフィックスを指定します。</li> </ul>
ステップ 6	<b>neighbor {<i>ip-address</i>   <i>peer-group-name</i>} activate</b> 例 : Device(config-router-af)# <b>neighbor 192.168.0.1 activate</b>	ネイバー デバイスとの情報交換を有効にします。 <ul style="list-style-type: none"> <li>• <b>ip-address</b> 引数には、ネイバーの IP アドレスを指定します。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <i>peer-group-name</i> 引数には、BGP ピアグループの名前を指定します。</li> </ul>
ステップ 7	<b>neighbor</b> <i>{ip-address   peer-group-name}</i> <b>inter-as-hybrid</b> 例： Device(config-router-af) # <b>neighbor</b> <b>192.168.0.1 inter-as-hybrid</b>	eBGP ピアデバイス (ASBR) を Inter-AS オプション AB ピアとして設定します。 <ul style="list-style-type: none"> <li>• <i>ip-address</i> 引数には、ネイバーの IP アドレスを指定します。</li> <li>• <i>peer-group-name</i> 引数には、BGP ピアグループの名前を指定します。</li> <li>• プレフィックスがオプション AB VRF にインポートされると、インポートされたパスがこのピアにアドバタイズされます。</li> <li>• プレフィックスをこのピアから受信し、オプション AB VRF にインポートすると、インポートされたパスが iBGP ピアにアドバタイズされます。</li> </ul> (注) アドバタイズされたルートには、VRF で設定された RT があります。アドバタイズされたルートには、元の RT はありません。
ステップ 8	<b>exit-address-family</b> 例： Device(config-router) # <b>exit-address-family</b>	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。

## Inter-AS 接続を必要とする VPN のルーティング ポリシーの設定

適切なルーティング ポリシーおよびオプション AB 設定を設定して、ASBR ピア間で Inter-AS 接続が必要な VPN の VRF を設定するには、この項の手順を使用します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	Device> <b>enable</b>	<ul style="list-style-type: none"> <li>パスワードを入力します（要求された場合）。</li> </ul>
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	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	<b>vrf definition vrf-name</b> 例： Device(config)# <b>vrf definition vpn1</b>	VRF 名を割り当て、VRF コンフィギュレーション モードを開始することにより、VPN ルーティング インスタンスを定義します。 <ul style="list-style-type: none"> <li><i>vrf-name</i> 引数は、VRF に割り当てる名前です。</li> </ul>
ステップ 4	<b>rd route-distinguisher</b> 例： Device(config-vrf)# <b>rd 100:1</b>	ルーティング テーブルと転送テーブルを作成します。 <ul style="list-style-type: none"> <li><i>route-distinguisher</i> 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。RD は、次のいずれかの形式で入力できます。               <ul style="list-style-type: none"> <li>16 ビット自律システム番号： 101:3 などの 32 ビット数値</li> <li>32 ビット IP アドレス： 192.168.122.15:1 などの 16 ビット数値</li> </ul> </li> </ul>
ステップ 5	<b>address-family ipv4</b> 例： Device(config-vrf)# <b>address-family ipv4</b>	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。 <ul style="list-style-type: none"> <li><b>ipv4</b> キーワードは、VRF の IPv4 アドレスファミリを指定します。               <ul style="list-style-type: none"> <li>16 ビット自律システム番号： 101:3 などの 32 ビット数値</li> <li>32 ビット IP アドレス： 192.168.122.15:1 などの 16 ビット数値</li> </ul> </li> </ul>

	コマンドまたはアクション	目的
ステップ 6	<pre>route-target {import export both} route-target-ext-community</pre> <p>例 :</p> <pre>Device(config-vrf-af)# route-target import 100:1</pre>	<p>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。</p> <ul style="list-style-type: none"> <li>• <b>import</b> 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。</li> <li>• <b>export</b> 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。</li> <li>• <b>both</b> キーワードを使用すると、ターゲット VPN 拡張 コミュニティとの間でルーティング情報がインポートおよびエクスポートされます。</li> <li>• <b>route-target-ext-community</b> 引数により、<b>route-target</b> 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 <b>route-target</b> 拡張 コミュニティの VRF リストに追加されます。</li> </ul>
ステップ 7	<pre>inter-as-hybrid</pre> <p>例 :</p> <pre>Device(config-vrf-af)# inter-as-hybrid</pre>	<p>VRF をオプション AB VRF として指定します。これには次のような効果があります。</p> <ul style="list-style-type: none"> <li>• この VRF にインポートされるルートは、オプション AB ピアと VPNv4 iBGP ピアにアダプタイズできます。</li> <li>• オプション AB ピアからルートを受信し、そのルートが VRF にインポートされると、そのルートのネクストホップテーブル ID が VRF のテーブル ID に設定されます。</li> </ul>
ステップ 8	<pre>inter-as-hybrid [next-hop ip-address]</pre> <p>例 :</p> <pre>Device(config-vrf-af)# inter-as-hybrid next-hop 192.168.1.0</pre>	<p>(任意) VRF にインポートされ、オプション AB ピアから受信したパスに設定するネクストホップ IP アドレスを指定します。</p>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• ネクスト ホップ コンテキストも、これらのパスをインポートした VRF に設定されます。</li> </ul>
ステップ 9	<b>end</b> 例： Device(config-vrf-af) # <b>end</b>	(任意) 終了して、特権 EXEC モードに戻ります。

## Inter-AS オプション A 配置からオプション AB 配置への変更

オプション A 配置では、VRF インスタンスは ASBR デバイス間ではバックツーバック接続であり、異なる自律システムの PE デバイス間では直接接続です。PE デバイスは複数の物理または論理インターフェイスによって接続され、各インターフェイスは (VRF インスタンスを介して) 特定の VPN に関連付けられています。

オプション AB 配置では、グローバルルーティングテーブル内の単一の MP-BGP セッションを使用してさまざまな自律システムが相互接続され、コントロールプレーントラフィックが伝送されます。

MPLS VPN Inter-AS オプション A 配置からオプション AB 配置へ変更するには、次の手順を実行します。

1. ASBR で MP-BGP セッションを設定します。特定の VPN のルートとその VPN の他のメンバのみが学習でき、VPN のメンバが相互に通信できるように、BGP マルチプロトコル拡張を使用して IPv4 以外のアドレスファミリのサポートが定義されます。
2. オプション A からのアップグレードが必要な VRF を特定し、**inter-as-hybrid** コマンドを使用してそれらの VRF をオプション AB に対して設定します。
3. eBGP (ピア ASBR) ネイバーの設定を削除するには、この項の次の手順に従います。
4. 追加 eBGP (ピア ASBR) ネイバーの設定を削除するには、次の手順のステップをすべて繰り返します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>• パスワードを入力します (要求された場合)。</li> </ul>
ステップ 2	<b>configure terminal</b> 例：	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
	Device# <b>configure terminal</b>	
ステップ 3	<b>router bgp as-number</b> 例 : Device(config)# <b>router bgp 100</b>	BGP ルーティング プロセスを設定し、デバイスでルータコンフィギュレーションモードを開始します。 <ul style="list-style-type: none"> <li>• <i>as-number</i> 引数は、デバイスを他の BGP デバイスに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。有効な番号は 0 ~ 65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512 ~ 65535 です。</li> </ul>
ステップ 4	<b>address-family ipv4 vrf vrf-name</b> 例 : Device(config-router)# <b>address-family ipv4 vrf vpn4</b>	特定の VPN のルートとその VPN の他のメンバのみが学習でき、VPN のメンバが相互に通信できるように、ASBR の MP-BGP セッションで識別される各 VRF を設定します。 <ul style="list-style-type: none"> <li>• 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。</li> </ul>
ステップ 5	<b>no neighbor {ip-address   peer-group-name}</b> 例 : Device(config-router-af)# <b>no neighbor 192.168.0.1</b>	ネイバー eBGP (ASBR) デバイスとの情報交換のための設定が削除されます。 <ul style="list-style-type: none"> <li>• <i>ip-address</i> 引数には、ネイバーの IP アドレスを指定します。</li> </ul>
ステップ 6	<b>exit-address-family</b> 例 : Device(config-router-af)# <b>exit-address-family</b>	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 7	<b>end</b> 例 : Device(config-router-af)# <b>end</b>	特権 EXEC モードに戻ります。



## MPLS VPN InterAS オプションの設定の確認

InterAS オプション B の設定情報を確認するには、次のいずれかの作業を行います。

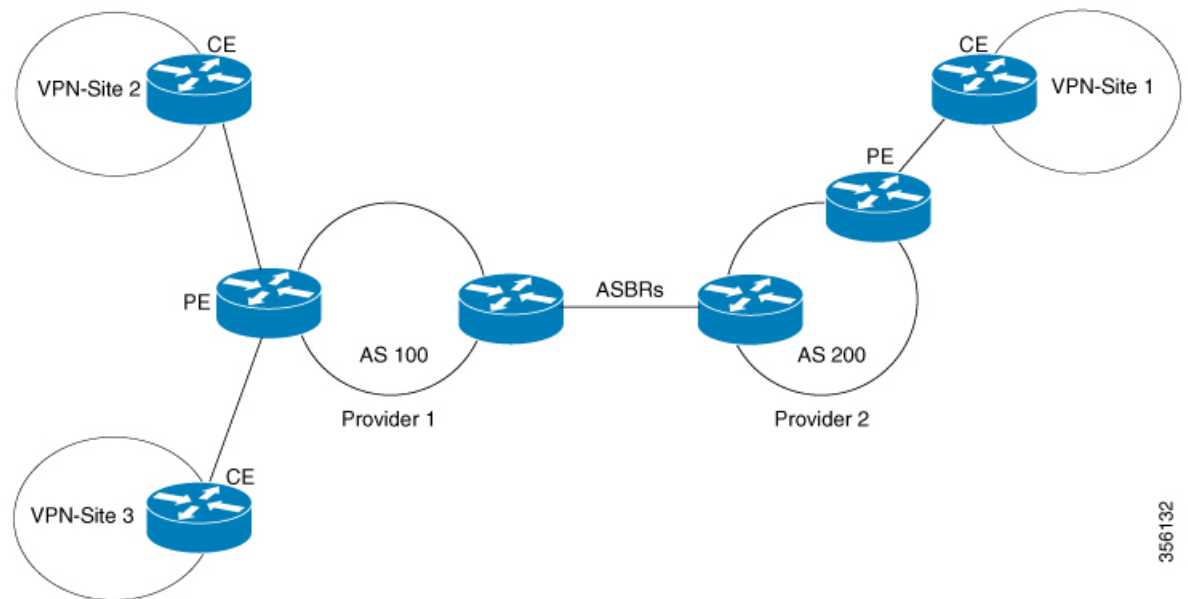
コマンド	目的
<code>ping ip-address source interface-type</code>	デバイスのアクセシビリティをチェックします。ループバック インターフェイスを使用して CE1 と CE2 間の接続を確認するには、このコマンドを使用します。
<code>show bgp vpnv4 unicast labels</code>	着信および発信 BGP ラベルを表示します。
<code>show mpls forwarding-table</code>	MPLS ラベル転送情報ベースの内容を表示します。
<code>show ip bgp</code>	BGP ルーティングテーブル内のエントリを表示します。
<code>show { ip   ipv6 } bgp [ vrf vrf-name ]</code>	VRF での BGP に関する情報を表示します。
<code>show ip route [ ip-address [ mask ] ] [ protocol ] vrf vrf-name</code>	ルーティング テーブルの現在の状態を表示します。ip-address 引数を使用して、CE1 に CE2 へのルートが含まれていることを確認します。CE1 から学習したルートを確認します。CE2 へのルートがリストされていることを確認します。
<code>show { ip   ipv6 } route vrf vrf-name</code>	VRF に関連付けられた IP ルーティング テーブルを表示します。ローカル CE ルータとリモート CE ルータのループバックアドレスが、PE ルータのルーティングテーブルに存在することを確認します。
<code>show running-config bgp</code>	BGP の実行コンフィギュレーションを表示します。
<code>show running-config vrf vrf-name</code>	VRF の実行コンフィギュレーションを表示します。
<code>show vrf vrf-name interface interface-type interface-id</code>	VRF に対して設定されるルート識別子 (RD) およびインターフェイスを検証します。
<code>trace destination [ vrf vrf-name ]</code>	パケットがその宛先に送信されるときに取るルートを検出します。trace コマンドは、2 つのルータが通信できない場合に問題の箇所を分離するのに役立ちます。

# MPLS VPN InterAS オプションの設定例

## InterAS オプション B

### ネクストホップセルフ方式

図 2: ネクストホップセルフ方式を使用した *InterAS* オプション B のトポロジ



356132

## PE1 - P1 - ASBR1 の設定

PE1	P1	ASBR1
	<pre> interface Loopback0 ip address 4.1.1.2 255.255.255.255 ip ospf 1 area 0 interface GigabitEthernet1/0/4 no switchport ip address 10.10.1.2 255.255.255.0 ip ospf 1 area 0 mpls ip mpls label protocol ldp ! interface GigabitEthernet1/0/23 no switchport ip address 10.20.1.1 255.255.255.0 ip ospf 1 area 0 mpls ip mpls label protocol ldp </pre>	<pre> interface Loopback0 ip address 4.1.1.1 255.255.255.255 ip ospf 1 area 0 interface GigabitEthernet1/0/10 no switchport ip address 10.30.1.1 255.255.255.0 mpls bgp forwarding interface GigabitEthernet1/0/23 no switchport ip address 10.20.1.2 255.255.255.0 ip ospf 1 area 0 mpls ip mpls label protocol ldp router ospf 1 router-id 4.1.1.1 nsr nsf redistribute bgp 200 passive-interface GigabitEthernet1/0/10 passive-interface Tunnel0 network 4.1.1.0 0.0.0.255 area 0 router bgp 200 bgp router-id 4.1.1.1 bgp log-neighbor-changes no bgp default ipv4-unicast no bgp default route-target filter neighbor 4.1.1.3 remote-as 200 neighbor 4.1.1.3 update-source Loopback0 neighbor 10.30.1.2 remote-as 300 ! address-family ipv4 neighbor 10.30.1.2 activate neighbor 10.30.1.2 send-label exit-address-family ! address-family vpnv4 neighbor 4.1.1.3 activate neighbor 4.1.1.3 send-community extended neighbor 4.1.1.3 next-hop-self neighbor 10.30.1.2 activate neighbor 10.30.1.2 send-community extended exit-address-family </pre>

PE1	P1	ASBR1
<pre> vrf definition Mgmt-vrf ! address-family ipv4 exit-address-family ! address-family ipv6 exit-address-family ! vrf definition vrf1 rd 200:1 route-target export 200:1 route-target import 200:1 route-target import 300:1 ! address-family ipv4 exit-address-family interface Loopback0 ip address 4.1.1.3 255.255.255.255 ip ospf 1 area 0 ! interface Loopback1 vrf forwarding vrf1 ip address 192.1.1.1 255.255.255.255 ip ospf 200 area 0 ! interface GigabitEthernet2/0/4 no switchport ip address 10.10.1.1 255.255.255.0 ip ospf 1 area 0 mpls ip mpls label protocol ldp interface GigabitEthernet2/0/9 description to-IXIA-1:p8 no switchport vrf forwarding vrf1 ip address 192.2.1.1 255.255.255.0 ip ospf 200 area 0 router ospf 200 vrf vrf1 router-id 192.1.1.1 nsr nsf redistribute connected redistribute bgp 200 network 192.1.1.1 0.0.0.0 area 0 network 192.2.1.0 0.0.0.255 area 0 router ospf 1 router-id 4.1.1.3 nsr nsf redistribute connected router bgp 200 bgp router-id 4.1.1.3 bgp log-neighbor-changes neighbor 4.1.1.1 remote-as </pre>		

PE1	P1	ASBR1
<pre>200 neighbor 4.1.1.1 update-source Loopback0 ! address-family vpnv4 neighbor 4.1.1.1 activate neighbor 4.1.1.1 send-community extended exit-address-family ! address-family ipv4 vrf vrfl redistribute connected redistribute ospf 200 maximum-paths ibgp 4 exit-address-family</pre>		

## ASBR2 – P2 – PE2 の設定

表 1:

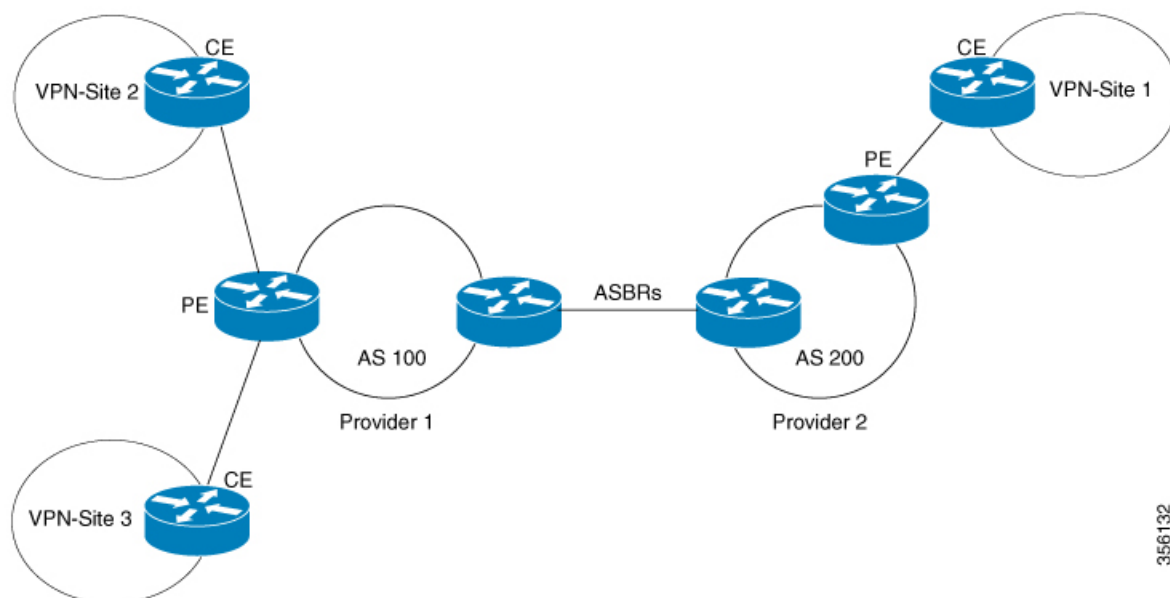
PE2	P2	ASBR2
	<pre> interface Loopback0 ip address 5.1.1.2 255.255.255.255 ip ospf 1 area 0 interface GigabitEthernet1/0/1 no switchport ip address 10.50.1.1 255.255.255.0 ip ospf 1 area 0 mpls ip mpls label protocol ldp interface GigabitEthernet2/0/3 no switchport ip address 10.40.1.2 255.255.255.0 ip ospf 1 area 0 mpls ip mpls label protocol ldp </pre>	<pre> interface Loopback0 ip address 5.1.1.1 255.255.255.255 ip ospf 1 area 0 ! interface GigabitEthernet1/0/37 no switchport ip address 10.30.1.2 255.255.255.0 mpls bgp forwarding interface GigabitEthernet1/0/47 no switchport ip address 10.40.1.1 255.255.255.0 ip ospf 1 area 0 mpls ip mpls label protocol ldp router ospf 1 router-id 5.1.1.1 nsr nsf passive-interface GigabitEthernet1/0/37 passive-interface Tunnel0 network 5.1.1.0 0.0.0.255 area 0 ! router bgp 300 bgp router-id 5.1.1.1 bgp log-neighbor-changes no bgp default ipv4-unicast no bgp default route-target filter neighbor 5.1.1.3 remote-as 300 neighbor 5.1.1.3 update-source Loopback0 neighbor 10.30.1.1 remote-as 200 ! address-family ipv4 neighbor 10.30.1.1 activate neighbor 10.30.1.1 send-label exit-address-family ! address-family vpnv4 neighbor 5.1.1.3 activate neighbor 5.1.1.3 send-community extended neighbor 5.1.1.3 next-hop-self neighbor 10.30.1.1 activate neighbor 10.30.1.1 send-community extended exit-address-family </pre>

PE2	P2	ASBR2
<pre> vrf definition vrf1 rd 300:1 route-target export 300:1 route-target import 300:1 route-target import 200:1 ! address-family ipv4 exit-address-family interface Loopback0 ip address 5.1.1.3 255.255.255.255 ip ospf 1 area 0 ! interface Loopback1 vrf forwarding vrf1 ip address 193.1.1.1 255.255.255.255 ip ospf 300 area 0 interface GigabitEthernet1/0/1 no switchport ip address 10.50.1.2 255.255.255.0 ip ospf 1 area 0 mpls ip mpls label protocol ldp ! interface GigabitEthernet1/0/2 no switchport vrf forwarding vrf1 ip address 193.2.1.1 255.255.255.0 ip ospf 300 area 0 router ospf 300 vrf vrf1 router-id 193.1.1.1 nsr nsf redistribute connected redistribute bgp 300 network 193.1.1.1 0.0.0.0 area 0 network 193.2.1.0 0.0.0.255 area 0 ! router ospf 1 router-id 5.1.1.3 nsr nsf redistribute connected router bgp 300 bgp router-id 5.1.1.3 bgp log-neighbor-changes neighbor 5.1.1.1 remote-as 300 neighbor 5.1.1.1 update-source Loopback0 ! address-family ipv4 neighbor 5.1.1.1 activate neighbor 5.1.1.1 send-label exit-address-family </pre>		

PE2	P2	ASBR2
<pre>! address-family vpnv4 neighbor 5.1.1.1 activate neighbor 5.1.1.1 send-community extended exit-address-family ! address-family ipv4 vrf vrf1 redistribute connected redistribute ospf 300 maximum-paths ibgp 4 exit-address-family</pre>		

## IGP Redistribute Connected Subnet 方式

図 3: Redistribute Connected Subnet 方式を使用した InterAS オプション B のトポロジ





## PE1 - P1 - ASBR1 の設定

PE1	P1	ASBR1
	<pre>interface Loopback0 ip address 4.1.1.2 255.255.255.255 ip ospf 1 area 0 interface GigabitEthernet1/0/4 no switchport ip address 10.10.1.2 255.255.255.0 ip ospf 1 area 0 mpls ip mpls label protocol ldp ! interface GigabitEthernet1/0/23 no switchport ip address 10.20.1.1 255.255.255.0 ip ospf 1 area 0 mpls ip mpls label protocol ldp</pre>	<pre>router ospf 1 router-id 4.1.1.1 nsr nsf redistribute connected passive-interface GigabitEthernet1/0/10 passive-interface Tunnel0 network 4.1.1.0 0.0.0.255 area 0 router bgp 200 bgp router-id 4.1.1.1 bgp log-neighbor-changes no bgp default ipv4-unicast no bgp default route-target filter neighbor 4.1.1.3 remote-as 200 neighbor 4.1.1.3 update-source Loopback0 neighbor 10.30.1.2 remote-as 300 ! address-family vpnv4 neighbor 4.1.1.3 activate neighbor 4.1.1.3 send-community extended neighbor 10.30.1.2 activate neighbor 10.30.1.2 send-community extended exit-address-family mpls ldp router-id Loopback0 force</pre>

## IGP Redistribute Connected Subnet 方式

PE1	P1	ASBR1
<pre> vrf definition Mgmt-vrf ! address-family ipv4 exit-address-family ! address-family ipv6 exit-address-family ! vrf definition vrf1 rd 200:1 route-target export 200:1 route-target import 200:1 route-target import 300:1 ! address-family ipv4 exit-address-family interface Loopback0 ip address 4.1.1.3 255.255.255.255 ip ospf 1 area 0 ! interface Loopback1 vrf forwarding vrf1 ip address 192.1.1.1 255.255.255.255 ip ospf 200 area 0 ! interface GigabitEthernet2/0/4 no switchport ip address 10.10.1.1 255.255.255.0 ip ospf 1 area 0 mpls ip mpls label protocol ldp interface GigabitEthernet2/0/9 description to-IXIA-1:p8 no switchport vrf forwarding vrf1 ip address 192.2.1.1 255.255.255.0 ip ospf 200 area 0 router ospf 200 vrf vrf1 router-id 192.1.1.1 nsr nsf redistribute connected redistribute bgp 200 network 192.1.1.1 0.0.0.0 area 0 network 192.2.1.0 0.0.0.255 area 0 router ospf 1 router-id 4.1.1.3 nsr nsf redistribute connected router bgp 200 bgp router-id 4.1.1.3 bgp log-neighbor-changes neighbor 4.1.1.1 remote-as </pre>		

PE1	P1	ASBR1
<pre>200 neighbor 4.1.1.1 update-source Loopback0 ! address-family vpnv4 neighbor 4.1.1.1 activate neighbor 4.1.1.1 send-community extended exit-address-family ! address-family ipv4 vrf vrf1 redistribute connected redistribute ospf 200 maximum-paths ibgp 4 exit-address-family</pre>		

## ASBR2 – P2 – PE2 の設定

PE2	P2	ASBR2
	<pre> interface Loopback0 ip address 5.1.1.2 255.255.255.255 ip ospf 1 area 0 interface GigabitEthernet1/0/1 no switchport ip address 10.50.1.1 255.255.255.0 ip ospf 1 area 0 mpls ip mpls label protocol ldp interface GigabitEthernet2/0/3 no switchport ip address 10.40.1.2 255.255.255.0 ip ospf 1 area 0 mpls ip mpls label protocol ldp </pre>	<pre> router ospf 1 router-id 5.1.1.1 nsr nsf redistribute connected passive-interface GigabitEthernet1/0/10 passive-interface Tunnel0 network 5.1.1.0 0.0.0.255 area 0 router bgp 300 bgp router-id 5.1.1.1 bgp log-neighbor-changes no bgp default ipv4-unicast no bgp default route-target filter neighbor 5.1.1.3 remote-as 300 neighbor 5.1.1.3 update-source Loopback0 neighbor 10.30.1.1 remote-as 200 ! address-family vpnv4 neighbor 5.1.1.3 activate neighbor 5.1.1.3 send-community extended neighbor 10.30.1.1 activate neighbor 10.30.1.1 send-community extended exit-address-family mpls ldp router-id Loopback0 force </pre>

PE2	P2	ASBR2
<pre> vrf definition vrf1 rd 300:1 route-target export 300:1 route-target import 300:1 route-target import 200:1 ! address-family ipv4 exit-address-family interface Loopback0 ip address 5.1.1.3 255.255.255.255 ip ospf 1 area 0 ! interface Loopback1 vrf forwarding vrf1 ip address 193.1.1.1 255.255.255.255 ip ospf 300 area 0 interface GigabitEthernet1/0/1 no switchport ip address 10.50.1.2 255.255.255.0 ip ospf 1 area 0 mpls ip mpls label protocol ldp ! interface GigabitEthernet1/0/2 no switchport vrf forwarding vrf1 ip address 193.2.1.1 255.255.255.0 ip ospf 300 area 0 router ospf 300 vrf vrf1 router-id 193.1.1.1 nsr nsf redistribute connected redistribute bgp 300 network 193.1.1.1 0.0.0.0 area 0 network 193.2.1.0 0.0.0.255 area 0 ! router ospf 1 router-id 5.1.1.3 nsr nsf redistribute connected router bgp 300 bgp router-id 5.1.1.3 bgp log-neighbor-changes neighbor 5.1.1.1 remote-as 300 neighbor 5.1.1.1 update-source Loopback0 ! address-family ipv4 neighbor 5.1.1.1 activate neighbor 5.1.1.1 send-label </pre>		

PE2	P2	ASBR2
<pre> exit-address-family ! address-family vpnv4 neighbor 5.1.1.1 activate neighbor 5.1.1.1 send-community extended exit-address-family ! address-family ipv4 vrf vrf1 redistribute connected redistribute ospf 300 maximum-paths ibgp 4 exit-address-family </pre>		

## InterAS オプション AB

次に、各デバイスのトポロジと設定を表示する例を示します。

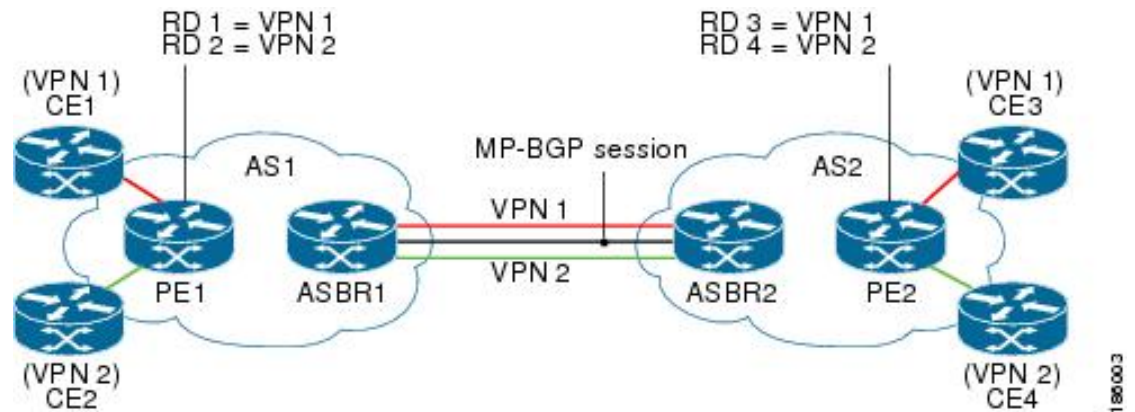


表 2:

PE1 の設定	P1 の設定	ASBR1 の設定	ASBR2 の設定	PE2 の設定
	<pre> interface Loopback0 ip address 2.2.2.2 255.255.255.255 ! interface TenGigabitEthernet1/1  ip address 10.1.1.2 255.255.255.0 mpls ip ! interface TenGigabitEthernet1/2  no ip address ! interface TenGigabitEthernet1/3  ip address 20.1.1.1 255.255.255.0 mpls ip ! router ospf 1 router-id 2.2.2.2  network 2.2.2.2 0.0.0.0 area 0 network 10.1.1.0 0.0.0.255 area 0 network 20.1.1.0 0.0.0.255 area 0 ! </pre>			

PE1 の設定	P1 の設定	ASBR1 の設定	ASBR2 の設定	PE2 の設定
<pre> ip vrf cust-1 rd 100:1 route-target export 100:1 route-target import 100:1 ! ip vrf cust-2 rd 100:2 route-target export 100:2 route-target import 100:2 ! interface Loopback0 ip address 1.1.1.1 255.255.255.255 ! interface Loopback1 ip address 11.11.11.11 255.255.255.255 ! interface Loopback2 ip address 12.12.12.12 255.255.255.255 ! ! interface HundredGigE1/0/1/1 no switchport ip address 10.1.1.1 255.255.255.0 mpls ip ! ! interface HundredGigE1/0/1/4 no switchport no ip address ! interface HundredGigE1/0/1/4.100 encapsulation dot1Q 100 ip vrf forwarding cust-1 ip address 11.1.1.1 255.255.255.0 ! interface HundredGigE1/0/1/4.101 encapsulation </pre>		<pre> ip vrf cust-1 rd 100:10001 route-target export 100:1 route-target import 100:1 route-target import 200:1 inter-as-hybrid next-hop 160.1.1.2 ! ip vrf cust-2 rd 100:20001 route-target export 100:2 route-target import 100:2 route-target import 200:2 inter-as-hybrid next-hop 170.1.1.2 ! ! interface Loopback0 ip address 3.3.3.3 255.255.255.255 ! ! interface TwentyFiveGigE1/0/3 no switchport ip address 20.1.1.2 255.255.255.0 mpls ip ! ! interface TwentyFiveGigE1/0/10.10 encapsulation dot1Q 10 ip address 150.1.1.1 255.255.255.0 mpls bgp forwarding ! interface TwentyFiveGigE1/0/10.20 encapsulation dot1Q 20 ip vrf forwarding cust-1 ip address 160.1.1.1 255.255.255.0 </pre>	<pre> ip vrf cust-1 rd 200:10001 route-target export 200:1 route-target import 200:1 route-target import 100:1 inter-as-hybrid next-hop 160.1.1.1 ! ip vrf cust-2 rd 200:20001 route-target export 200:2 route-target import 200:2 route-target import 100:2 inter-as-hybrid next-hop 170.1.1.1 ! ! interface Loopback0 ip address 4.4.4.4 255.255.255.255 ! ! interface TwentyFiveGigE1/0/2 no switchport ip address 30.1.1.1 255.255.255.0 mpls ip ! ! interface TwentyFiveGigE1/0/10.10 encapsulation dot1Q 10 ip address 150.1.1.2 255.255.255.0 mpls bgp forwarding ! interface TwentyFiveGigE1/0/10.20 encapsulation dot1Q 20 ip vrf forwarding cust-1 ip address 160.1.1.1 255.255.255.0 </pre>	<pre> ip vrf cust-1 rd 200:1 route-target export 200:1 route-target import 200:1 route-target import 100:1 ! ip vrf cust-2 rd 200:2 route-target export 200:2 route-target import 200:2 route-target import 100:2 ! interface Loopback0 ip address 5.5.5.5 255.255.255.255 ! interface Loopback1 ip address 55.55.55.55 255.255.255.255 ! interface Loopback2 ip address 56.56.56.56 255.255.255.255 ! ! interface HundredGigE1/0/1/1.200 encapsulation dot1Q 200 ip vrf forwarding cust-1 ip address 55.1.1.1 255.255.255.0 ! interface HundredGigE1/0/1/1.201 encapsulation dot1Q 201 ip vrf forwarding cust-2 ip address 56.1.1.1 255.255.255.0 ! interface HundredGigE1/0/1/3 no switchport ip address </pre>



PE1 の設定	P1 の設定	ASBR1 の設定	ASBR2 の設定	PE2 の設定
<pre> dot1Q 101 ip vrf forwarding   cust-2 ip address   12.1.1.1   255.255.255.0 ! router ospf 2 vrf   cust-1 router-id   11.11.11.11 network 11.1.1.0   0.0.0.255 area 0 network   11.11.11.11   0.0.0.0 area 0 ! router ospf 3 vrf   cust-2 router-id   12.12.12.12 network 12.1.1.0   0.0.0.255 area 0 network   12.12.12.12   0.0.0.0 area 0 ! router ospf 1 router-id 1.1.1.1  network 1.1.1.1   0.0.0.0   area 0 network 10.1.1.0   0.0.0.255 area 0 ! router bgp 100 bgp router-id   1.1.1.1 bgp log-neighbor-   changes neighbor 3.3.3.3   remote-as 100 neighbor 3.3.3.3   update-   source Loopback0 ! address-family   vpv4 neighbor 3.3.3.3   activate neighbor 3.3.3.3   send-   community   extended   exit-address-family ! address-family   ipv4 vrf cust-1   redistribute   connected </pre>		<pre> ! interface   TwentyFiveGigE1/0/10.30 ! encapsulation   dot1Q 30 ip vrf forwarding   cust-2 ip address   170.1.1.1   255.255.255.0 ! router ospf 1 router-id 3.3.3.3 network 3.3.3.3   0.0.0.0 area 0 network 20.1.1.0   0.0.0.255 area 0 ! router bgp 100 bgp router-id   3.3.3.3 bgp log-neighbor-   changes neighbor 1.1.1.1   remote-   as 100 neighbor   150.1.1.2   remote-as 200 ! address-family   ipv4   redistribute   connected neighbor 1.1.1.1   activate neighbor   150.1.1.2   activate   exit-address-family ! address-family   vpv4 neighbor 1.1.1.1   activate neighbor 1.1.1.1   send-   community both neighbor   150.1.1.2   activate neighbor   150.1.1.2   send-   community both neighbor   150.1.1.2   inter- as-hybrid   exit-address-family ! address-family   ipv4 </pre>	<pre> 160.1.1.2 255.255.255.0 ! interface   TwentyFiveGigE1/0/10.30 ! encapsulation   dot1Q 30 ip vrf forwarding   cust-2 ip address   170.1.1.2   255.255.255.0 ! router ospf 1 router-id 4.4.4.4 network 4.4.4.4   0.0.0.0   area 0 network 30.1.1.0   0.0.0.255   area 0 ! router bgp 200 bgp router-id   4.4.4.4 bgp log-neighbor-   changes neighbor 5.5.5.5   remote-   as 200 neighbor   150.1.1.1   remote-as 100 ! address-family   ipv4 neighbor 5.5.5.5   activate neighbor   150.1.1.1   activate   exit-address-family ! address-family   vpv4 neighbor 5.5.5.5   activate neighbor 5.5.5.5   send-community   both neighbor   150.1.1.1   activate neighbor   150.1.1.1   send-community   both neighbor   150.1.1.1   inter-as-hybrid   exit-address-family </pre>	<pre> 30.1.1.2 255.255.255.0 mpls ip ! router ospf 2 vrf   cust-1 router-id   55.55.55.55 network 55.1.1.0   0.0.0.255   area 0 network   55.55.55.55   0.0.0.0   area 0 ! router ospf 3 vrf   cust-2 router-id   56.56.56.56 network 56.1.1.0   0.0.0.255 area 0 network   56.56.56.56   0.0.0.0 area 0 ! router ospf 1 router-id 5.5.5.5 network 5.5.5.5   0.0.0.0   area 0 network 30.1.1.0   0.0.0.255   area 0 ! router bgp 200 bgp router-id   5.5.5.5 bgp   log-neighbor-changes neighbor 4.4.4.4   remote-as 200 neighbor 4.4.4.4   update-source   Loopback0 ! address-family   vpv4 neighbor 4.4.4.4   activate neighbor 4.4.4.4   send-community   extended   exit-address-family ! address-family   ipv4 vrf cust-1   redistribute   connected   redistribute ospf   2   maximum-paths </pre>

PE1 の設定	P1 の設定	ASBR1 の設定	ASBR2 の設定	PE2 の設定
<pre> redistribute ospf  2 maximum-paths ibgp 4 exit-address-family ! address-family ipv4 vrf cust-2 redistribute connected redistribute ospf  3 maximum-paths ibgp 4 exit-address-family </pre>		<pre> vrf cust-1 redistribute connected exit-address-family ! address-family ipv4 vrf cust-2 redistribute connected exit-address-family ! </pre>	<pre> ! address-family ipv4 vrf cust-1 redistribute connected exit-address-family ! address-family ipv4 vrf cust-2 redistribute connected exit-address-family ! </pre>	<pre> ibgp 4 exit-address-family ! address-family ipv4 vrf cust-2 redistribute connected redistribute ospf  3 maximum-paths ibgp 4 exit-address-family ! </pre>

## MPLS VPN InterAS オプション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
この章で使用するコマンドの完全な構文および使用方法の詳細。	の「MPLS コマンド」の項を参照してください。 <i>Command Reference (Catalyst 9300 Series Switches)</i>

## MPLS VPN InterAS オプションの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Gibraltar 16.11.1	MPLS VPN InterAS オプション B	InterAS オプションは、iBGP および eBGP ピアリングを使用して、異なる AS 内の VPN が相互に通信できるようにします。InterAS オプション B ネットワークでは、ASBR ポートは、MPLS トラフィックを受信できる 1 つ以上のインターフェイスによって接続されます。

リリース	機能	機能情報
Cisco IOS XE Amsterdam 17.3.1	MPLS VPN InterAS オプション AB	MPLS VPN InterAS オプション AB では、ルータ上でグローバルに有効になっている単一のマルチプロトコルボーダー ゲートウェイ プロトコル (MP-BGP) セッションを使用して、異なる自律システムを相互接続できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。