



# CUPS の VPC-SI での MPLS のサポート

- [マニュアルの変更履歴](#) (1 ページ)
- [機能説明](#) (1 ページ)
- [機能の仕組み](#) (2 ページ)
- [モニタリングおよびトラブルシューティング](#) (15 ページ)

## マニュアルの変更履歴



(注) リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

## 機能説明

既存のプラットフォーム (VPC-DI、ASR 5500) では、Boxer が MPLS をサポートしており、MPLS が基盤となるデータプレーンフォワーダを使用して MPLS トラフィックを切り替えます。ASR 5500 では、NP4c ネットワークプロセッサが MPLS トラフィックを生成および処理し、VPC-DI では、IFTask が MPLS トラフィックを生成および処理します。

CUPS の VPC-SI における MPLS サポート機能により、データプレーンフォワーダとして VPP を使用する VPC-SI (SI-CUPS) での MPLS サポートが有効になります。

VPP は、個別のグラフノードとして MPLS スタックを含む複数のデータプレーン機能をサポートし、提供します。また、ラベル付きパケットを生成し、着信ラベル付きパケットを同時に処理するため、さまざまな顧客 VRF を区別して、アドレッシングモデルと要件が異なる多数の企業 APN をサポートできます。

CUPS の VPC-SI における MPLS サポート機能は、次の機能をサポートしています。

- VPP MPLS スタックを使用した、MPLS ラベル付きパケットの送信。
- VPP MPLS スタックを使用した、着信ラベル付き MPLS パケットの処理。
- 既存のすべての MPLS 設定 (VPC-DI、ASR 5500) のサポート、および VPC-SI CUPS を使用した新しい展開と同等の機能の提供。
- VPP 内にある NHLFE および ILM テーブルを表示して、値をデバッグしたり、Boxer 設定と比較したりするための VPPCTL CLI コマンドのサポート。

## 機能の仕組み

ここでは、CUPS の VPC-SI での MPLS サポートの仕組みについて簡単に説明します。

現在の CUP アーキテクチャでは、VPP フォワーダが独自の MPLS スタックを提供し、MPLS パケット処理に関する既存の機能をすべてサポートします。VPP MPLS スタックは、適切なネクストホップラベル転送エントリ (NHLFE) および着信ラベルマップ (ILM) テーブルで設定されます。これは、正しい MPLS ヘッダーを使用して出力時に MPLS パケットを生成するのに役立ちます。また、着信 MPLS パケットを処理し、着信ラベルに基づいてこのパケットを適切なネクストホップテーブル ID (サブスクリイバの VRF コンテキスト) に切り替えます。

MPLS ソリューションでは、次のシナリオがサポートされています。

- PE に接続された MPLS-CE
- PE としての VPC-SI

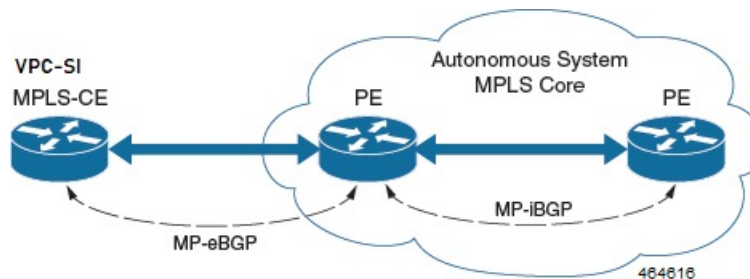
また、VPC-SI は RFC 4659 (*BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*) で説明されているとおり、VPNv6 をサポートします。

## PE に接続された MPLS-CE

VPC-SI は、プロバイダーエッジ (PE) ラベルエッジルータ (LER) に接続されている MPLS-CE (カスタマーエッジ) ネットワーク要素として機能し、その結果、RFC 4364 に従い MPLS コアに接続されます。

次の図は、MPLS-CE から PE への接続を示しています。

図 1: VPC-SI MPLS-CE から PE



MPLS-CE は、独自の自律システム (AS) 内の PE ルータのように機能します。MPLS-CE では、Virtual Routing and Forwarding (VRF) ルートが維持され、MP-eBGP (マルチプロトコル外部 BGP) セッションを介して、VPN ルート情報が PE と交換されます。

PE も VRF を使用して設定され、MP-iBGP (マルチプロトコル内部 BGP) 接続を介して AS 内の他の PE と VPN ルートを交換し、MP-eBGP 接続を介して MPLS-CE を交換します。

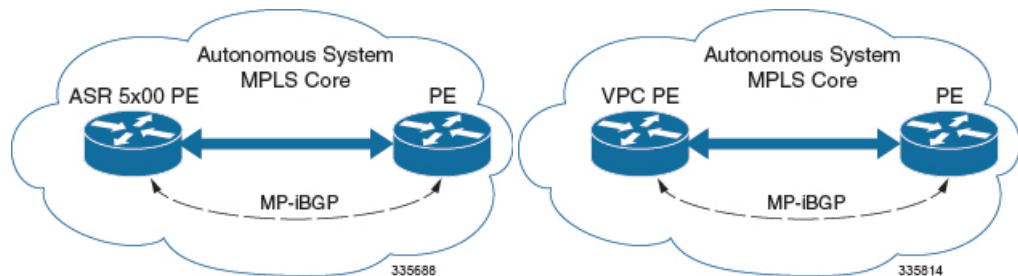
EBGP 接続を使用すると、PE は、IBGP ピアから学習したルート内のネクストホップ IP アドレスとラベルを変更してから、MPLS-CE にアドバタイズできます。MPLS-CE は、ルートをアドバタイズして学習するために MP-eBGP だけを使用します。直接接続 EBGP ピアリングのため、Label Distribution Protocol (LDP) および Resource Reservation Protocol (RSVP) は必要ありません。MPLS-CE は、PE との間で (MP-eBGP 接続を介して学習された) 単一のラベルをプッシュまたはポップします。

## PE としての VPC-SI

### 概要

このシナリオでは、VPC-SI は MPLS コアのエッジにある PE ルータとして機能します。以下の図を参照してください。

図 2: PE としての VPC-SI



VPC-SI では、最初の 2 つのシナリオに示されているように、ASBR や PE は不要です。このシナリオでは、IBGP 機能と MPLS ラベル配布プロトコルという 2 つの主要な要件が導入されています。

VPC-SI は、次の 2 つのラベルを追加するように設定できます。

- LDP または RSVP TE から学習した外部ラベル (RSVP トラフィックエンジニアリング)
- MP-iBGP から学習した内部ラベル

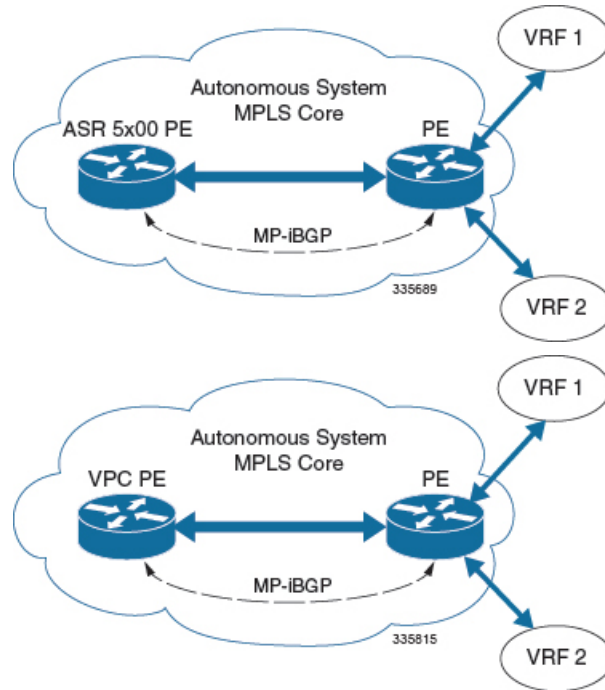
このソリューションは、VPC-SI を介して開始されたトラフィック エンジニアリングと QoS をサポートします。

### 設定例

この例では、VRF は ASR 5500 PE で設定され、プールは VRF に関連付けられています。VPC-SI は、VPN ルートを IBGP ピア (PE ルータ) と交換し、LDP 経由で PE に到達するための MPLS

パスを学習します。VPC-SI は、2つのラベル（PE から学習した内部ラベルとネクストホップ IBGP ネイバーから学習した外部ラベル）を持つネクストホップにパケットを転送します。

図 3: 設定例



```

mpls ip
  protocol ldp
  enable
  exit
exit

ip vrf vrf1
  mpls traffic-class copy
  exit
ip vrf vrf2
  mpls traffic-class value 5
  exit

router bgp 300
  ip vrf vrf1
    route-target export 300 1
    route-target import 300 1
    route-distinguisher 300 1
  exit
  ip vrf vrf2
    route-target export 300 2
    route-target import 300 2
    route-distinguisher 300 2
  exit

router-id 209.165.201.1
neighbor 209.165.200.225 remote-as 300
neighbor 209.165.200.225 update-source node1_loopback

address-family vpnv4
  neighbor 209.165.200.225 activate

```

```
neighbor 209.165.200.225 send-community both
neighbor 209.165.200.225 next-hop-self
exit

address-family ipv4 vrf vrf1
  redistribute connected
exit

address-family ipv4 vrf vrf2
  redistribute connected
exit

interface interface_to_internet
  ip address 209.165.200.224/27
  mpls ip
exit
router ospf
  network 209.165.201.0/27 area 209.165.201.5
exit
```

## BGP MPLS VPN の IPv6 サポート

### 概要

VPC-SI は RFC 4659 (*BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*) で説明されているとおり、VPNv6 をサポートします。

IPv6 VPN は、PE ルータを通じ、IPv6 インターフェイスまたはサブインターフェイスを介してサービスプロバイダー (SP) のバックボーンに接続されます。このサイトは IPv4 と IPv6 の両方に対応できます。各 VPNv6 には独自のアドレス空間があります。つまり、特定のアドレスが異なる VPN 内の異なるシステムを示すこととなります。これは、ルート識別子 (RD) を IP アドレスに付加する VPNv6 アドレスファミリによって実現します。

VPNv6 アドレスのバイト数は 24 で、8 バイトの RD から始まり、16 バイトの IPv6 アドレスで終わります。サイトが IPv4 と IPv6 対応の場合、同じ RD を IPv4 と IPv6 の両方のアドレスのアドバタイズメントに使用できます。

システムは、IPv6 ルートに RD を追加し、VPNv6 アドレスファミリを使用してラベル付けされた IPv6 を交換します。VPNv6 ルートのアドレスファミリ識別子 (AFI) と後続のアドレスファミリ識別子 (SAFI) のフィールドは、2 と 128 にそれぞれ設定されます。

IPv6 VPN トラフィックは、IPv4 トンネリングを介して BGP スピーカーに転送されます。BGP スピーカーは、8 オクテットの RD がゼロに設定され、16 オクテットの IPv6 アドレスがアドバタイズルータの IPv4 アドレスを含む IPv4 マッピング IPv6 アドレス (RFC 4291) としてエンコードされている VPN-IPv6 アドレスを含むネクストホップネットワークアドレスフィールドをピアにアドバタイズします。これは、VPNv6 ルートを交換するために EBGP ピアリングのみが使用されることを前提としています。

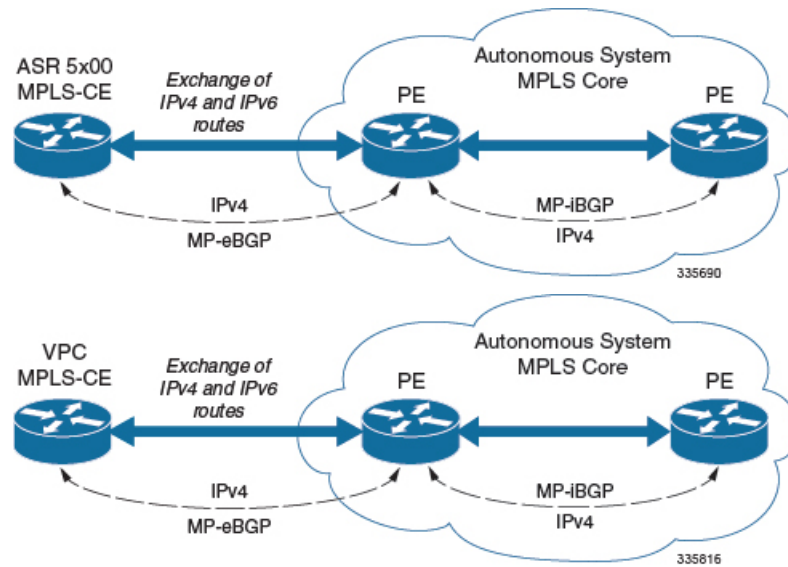
VPN IPv6 のサポートは、次を前提としています。

- デュアルスタック (IPv4/IPv6) ルーティング
- VRF の IPv6 プール

- 直接接続された IPv4 インターフェイスを介した BGP ピアリング

以下の図を参照してください。

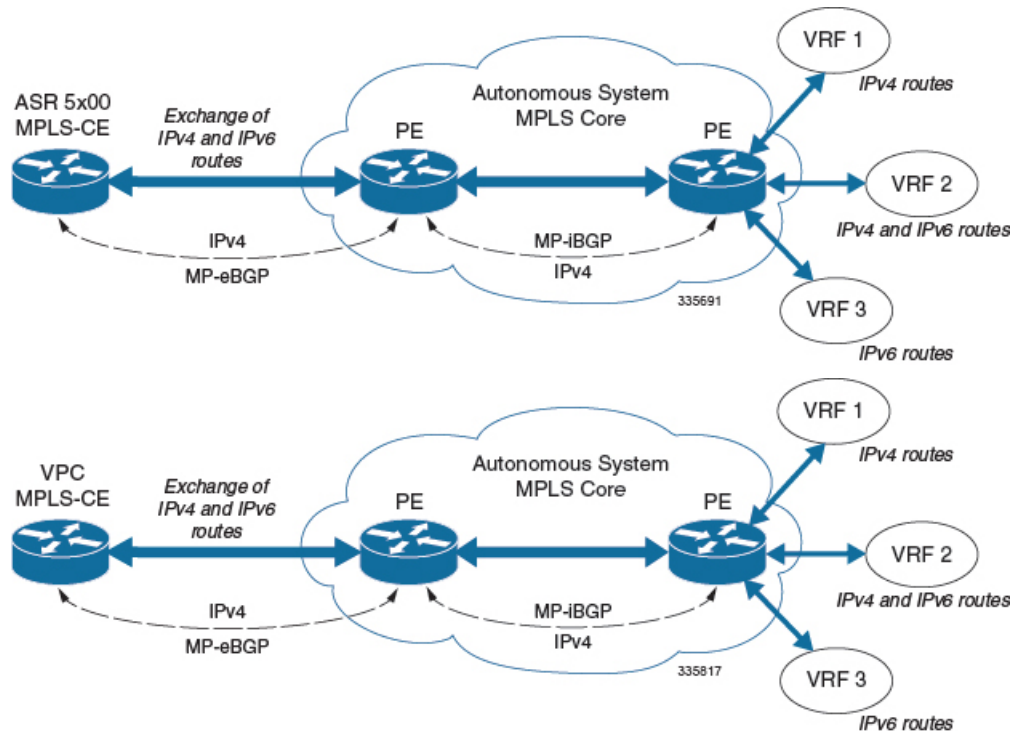
図 4: VPNv6 に対する IPv6-RD サポート



## 設定例

この例では、3つのVRFを想定しています。VRF 1にはIPv4ルートのみがあり、VRF 2にはIPv4とIPv6の両方のルートがあり、VRF 3にはIPv6ルートのみがあります。

図 5: VPNv6 の設定例



VRF を設定します。

```
ip vrf vrf1
exit
ip vrf vrf2
exit
ip vrf vrf3
exit
```

MPLS bgp forwarding を有効にします。

```
mpls bgp forwarding
```

プールを設定します。

```
ip pool vrf1-pool 209.165.200.230 255.255.255.224 private 0 vrf vrf1
exit
ip pool vrf2-pool 209.165.200.230 255.255.255.224 private 0 vrf vrf2
exit
ipv6 pool vrf2-v6pool prefix 2005:0101::/32 private 0 vrf vrf2
exit
ipv6 pool vrf3-v6pool prefix 2005:0101::/32 private 0 vrf vrf3
exit
```

インターフェイスを設定します。

```
interface ce_interface_to_rtr
ip address 209.165.200.226 255.255.255.224
exit
interface ce_v6_interface
ip address 2009:0101:0101:0101::1/96
exit
interface ce_loopback loopback
```

```

    ip address 209.165.200.227 255.255.255.255
  exit
  interface vrf1-loop loopback
    ip vrf forwarding vrf1
    ip address 209.165.200.228 255.255.255.255
  exit
  interface vrf2-loop loopback
    ip vrf forwarding vrf2
    ip address 209.165.200.229 255.255.255.255
  exit
  interface vrf2-v6loop loopback
    ip vrf forwarding vrf2
    ip address 2005:0202:0101::1/128
  exit
  interface vrf3-v6loop loopback
    ip vrf forwarding vrf3
    ip address 2005:0303:0101::1/128
  exit

```

アドレスファミリおよび再配布ルールとともに BGP を設定します。

```

router bgp 800
  router-id 209.165.200.225
  neighbor 209.165.200.240 remote-as 1003
  neighbor 209.165.200.240 activate
  address-family vpnv4
    neighbor 209.165.200.240 activate
    neighbor 209.165.200.240 send-community both
  exit
  address-family vpnv6
    neighbor 209.165.200.240 activate
    neighbor 209.165.200.240 send-community both
  exit
  ip vrf vrf1
    route-distinguisher 800 1
    route-target export 800 1
    route-target import 800 1
  exit
  address-family ipv4 vrf vrf1
    redistribute connected
    redistribute static
  exit
  ip vrf vrf2
    route-distinguisher 800 2
    route-target export 800 2
    route-target import 800 2
  exit
  address-family ipv4 vrf vrf2
    redistribute connected
    redistribute static
  exit
  address-family ipv6 vrf vrf2
    redistribute connected
    redistribute static
  exit
  ip vrf vrf3
    route-distinguisher 800 3
    route-target export 800 3
    route-target import 800 3
  exit
  address-family ipv6 vrf vrf3
    redistribute connected
    redistribute static
  exit

```



APN を設定します。

```

apn walmart51.com
  selection-mode sent-by-ms
  accounting-mode none
  aaa group walmart-group
  authentication pap 1 chap 2 allow-noauth
  ip context-name Gi_ce
  ip address pool name vrf1-pool
exit
apn amazon51.com
  selection-mode sent-by-ms
  accounting-mode none
  aaa group amazon-group
  authentication pap 1 chap 2 allow-noauth
  ip context-name Gi_ce
  ip address pool name vrf2-pool
  ipv6 address prefix-pool vrf2-v6pool
exit
apn apple51.com
  selection-mode sent-by-ms
  accounting-mode none
  aaa group apple-group
  authentication pap 1 chap 2 allow-noauth ip context-name Gi_ce
  ipv6 address prefix-pool vrf3-v6pool
exit
aaa-group amazon-group
  radius ip vrf vrf2
aaa group default
exit
gtp group default
exit
ip igmp profile default
exit

```

物理インターフェイスをポートにバインドします。

## VPN 関連の CLI コマンド

VPN 関連の機能は、いくつかの CLI コマンドモードでサポートされています。次の表は、VPN 関連の機能の設定とモニタリングに関連するコマンドを示しています。

表 1: VPN 関連の設定コマンド

CLI モード	コマンド	説明
BGP アドレスファミリー (IPv4/IPv6) 構成モード	<b>neighbor ip_address activate</b>	ピアルータとのルーティング情報の交換を有効にします。
BGP アドレスファミリー (IPv4/IPv6) 構成モード	<b>neighbor ip_address send community { both   extended   standard }</b>	ピアルータ (ネイバー) にコミュニティ属性を送信します。
BGP アドレスファミリー (IPv4/IPv6) 構成モード	<b>redistribute connected</b>	別のプロトコルから BGP へのルートを BGP ネイバーとして再配布します。

CLI モード	コマンド	説明
BGP アドレスファミリー (VPNv4) 構成モード	<b>neighbor ip_address activate</b>	ピアルータとのルーティング情報の交換を有効にします。
BGP アドレスファミリー (VPNv4) 構成モード	<b>neighbor ip_address send community { both   extended   standard }</b>	ピアルータに拡張コミュニティ属性を送信します。VPN では、ルート識別子とルートターゲットは BGP 拡張コミュニティでエンコードされます。このコマンドは、拡張コミュニティを持つ BGP ルートをネイバーに送信できるようにします。
BGP アドレスファミリー (VRF) 構成モード	<b>neighbor ip_address activate</b>	ピアルータとのルーティング情報の交換を有効にします。
BGP アドレスファミリー (VRF) 構成モード	<b>neighbor ip_address send community { both   extended   standard }</b>	ピアルータに拡張コミュニティ属性を送信します。VPN では、ルート識別子とルートターゲットは BGP 拡張コミュニティでエンコードされます。このコマンドは、拡張コミュニティを持つ BGP ルートをネイバーに送信できるようにします。
BGP アドレスファミリー (VRF) 構成モード	<b>redistribute connected</b>	別のプロトコルから BGP へのルートを BGP ネイバーとして再配布します。
BGP 構成モード	<b>address-family { ipv4 vrf vrf_name   vpnv4 }</b>	IPv4 VRF のルーティング情報の交換を有効にします。アドレスファミリーごとに異なるモードがあります。
BGP 構成モード	<b>address-family { ipv6 vrf vrf_name   vpnv6 }</b>	BGP で VPNv6 アドレスファミリーと IPv6 VRF ルーティングを設定します。
BGP 構成モード	<b>ip vrf vrf_name</b>	BGP に VRF を追加し、VRF 構成モードにスイッチして、VRF の BGP 属性を設定できるようにします。
BGP IP VRF 構成モード	<b>route-distinguisher { as_value   ip_address } rd_value</b>	VRF のルート識別子 (RD) を割り当てます。RD 値は、VRF ごとにルータ上の一意の値にする必要があります。

CLI モード	コマンド	説明
BGP IP VRF 構成モード	<b>route-target</b> { <b>both</b>   <b>import</b>   <b>export</b> } { <i>as_value</i>   <i>ip_address</i> } <i>rt_value</i>	インポートおよびエクスポートのルートターゲット拡張コミュニティのリストを VRF に追加します。
コンテキスト構成モード	<b>ip pool</b> <i>pool_name</i> <i>addr_range</i> <b>vrf</b> <i>vrf_name</i> [ <b>mpls-label input</b> <i>inlabel1</i> <b>output</b> <i>outlabel1</i> <i>outlabel2</i> ]	指定された VRF にプールを設定します。このパラメータは、ネクストホップパラメータで指定する必要があります。 <i>inlabel1</i> は、このプールを宛ての着信トラフィックを識別する MPLS ラベルです。 <i>outlabel1</i> および <i>outlabel2</i> は、このプールからサブスクライバに対して送信されるパケットに追加する MPLS ラベルを指定します。
コンテキスト構成モード	<b>ip vrf</b> <i>vrf_name</i>	VRF を作成し、VRF-ID を割り当てます。VRF がルータに作成されます。
コンテキスト構成モード	<b>ipv6 pool</b> <i>pool_name</i> <b>vrf</b> <i>vrf_name</i>	プールを VRF に関連付けます。 注：デフォルトでは、設定された ipv6 プールはグローバルルーティングドメインに関連付けられません。
コンテキスト構成モード	<b>mpls bgp forwarding</b>	MPLS のボーダーゲートウェイプロトコル (BGP) 転送をグローバルに有効化します。

CLI モード	コマンド	説明
コンテキスト構成モード	<b>mpls exp value</b>	3 ビット MPLS EXP ヘッダーのゼロ値を使用して、デフォルトの動作をベストエフォートとして設定します。この値は、コンテキスト内のすべての VRF に適用されます。デフォルトの動作では、DSCP から EXP への明示的な設定がない場合に、モバイルサブスクライバのトラフィックの DSCP 値が EXP ヘッダーにコピーされます ( <b>mpls map-dscp-exp dscp n exp m</b> コマンドを使用)。  <b>mpls exp</b> はデフォルトの動作を無効にし、EXP 値を設定された値に設定します。
コンテキスト構成モード	<b>mpls ip</b>	通常ルーティングされるパスに沿って IPv4 パケットの MPLS 転送がグローバルに行われるようにします。
コンテキスト構成モード	<b>radius change-authorize-nas-ip ip_address ip_address { encrypted   key } value port port_num mpls input inlabel output outlabel1 outlabel2</b>	指定された MPLS ラベルを使用するように COA トラフィックを設定します。inlabel は着信 COA トラフィックを識別します。outlabel1 および outlabel2 は、COA 応答に追加する MPLS ラベルを指定します。outlabel1 は内部出力ラベル、outlabel2 は外部出力ラベルです。
イーサネットインターフェイス構成モード	<b>mpls ip</b>	このインターフェイスで IP パケットのダイナミック MPLS 転送を有効にします。
Exec モード	<b>clear ip bgp peer</b>	BGP セッションをクリアします。
Exec モード	<b>lsp-ping ip_prefix_FEC</b>	指定された転送等価クラス (FEC) の MPLS ラベルスイッチドパス (LSP) 接続を確認します。その後、IPv4 または IPv6 の FEC プレフィックスが続く必要があります。

CLI モード	コマンド	説明
Exec モード	<b>lsp-traceroute</b> <i>ip_prefix_FEC</i>	パケットが宛先に転送されるときに実際にたどる MPLS LSP ルーティンを検出します。その後 IPv4 または IPv6 の FEC プレフィックスが検出され続きます。
IP VRF コンテキスト構成モード	<b>mpls map-dscp-to-exp</b> <b>dscp</b> <i>dscp_bit_value</i> <b>exp</b> <i>exp_bit_value</i>	IP パケットヘッダーにおける最終の Differentiated Services Code Point (DSCP; DiffServ コードポイント) ビット値を、着信トラフィックの MPLS ヘッダーにおける最終の Experimental (EXP) ビット値にマッピングします。
IP VRF コンテキスト構成モード	<b>mpls map-exp-to-dscp</b> <b>exp</b> <i>exp_bit_value</i> <b>dscp</b> <i>dscp_bit_value</i>	MPLS ヘッダーの着信 EXP ビット値を発信トラフィックの IP パケットヘッダーの内部 DSCP ビット値にマッピングします。
MPLS-IP 構成モード	<b>protocol ldp</b>	MPLS プロトコルファミリの構成モードを作成するか、または既存の構成モードの MPLS-IP を設定して、現在のコンテキストで MPLS-LDP 構成モードを開始します。このコマンドは、MPLS プロトコルファミリの MPLS-IP のプロトコルパラメータを設定します。
MPLS-LDP 構成モード	<b>advertise-labels</b> { <b>explicit-null</b>   <b>implicit-null</b> }	このコンテキストでシステムにアドバタイズされたすべてのプレフィックスについて、暗黙的ヌルまたは明示的ヌルラベルのアドバタイズメントを設定します。
MPLS-LDP 構成モード	<b>discovery</b> { <b>hello</b> { <b>hello-interval</b> <i>seconds</i>   <b>hold-interval</b> <i>seconds</i> }   <b>transport-address</b> <i>ip_address</i> }	Label Distribution Protocol (LDP; ラベル配布プロトコル) のネイバー探索パラメータの設定
MPLS-LDP 構成モード	<b>enable</b>	ラベル配布プロトコル (LDP) を有効にします。
MPLS-LDP 構成モード	<b>router-id</b> <i>ip_address</i>	LDP ルータ ID を設定します。

CLI モード	コマンド	説明
MPLS-LDP 構成モード	<b>session timers { hold-interval seconds   keepalive-interval seconds }</b>	LDPセッションパラメータを設定します。

表 2: VPN 関連のモニタリングコマンド

CLI モード	コマンド	説明
Exec モードの show コマンド	<b>show ip bgp neighbors</b>	BGP ネイバーに関する情報を表示します。
Exec モードの show コマンド	<b>show ip bgp vpnv4 { all   route-distinguisher   vrf }</b>	すべての VPNv4 ルーティングデータ、VRF またはルート識別子のルーティングデータを表示します。
Exec モードの show コマンド	<b>show ip bgp vpnv6</b>	VPNv6 ルーティングテーブルの内容を表示します。
Exec モードの show コマンド	<b>show ip bgp vpnv6 { all   route-distinguisher   vrf }</b>	すべての VPNv6 ルーティングデータ、VRF またはルート識別子のルーティングデータを表示します。
Exec モードの show コマンド	<b>show ip pool</b>	設定された VRF を含むプールの詳細を表示します。
Exec モードの show コマンド	<b>show mpls cross-connect</b>	MPLS 相互接続情報を表示します。インターフェイスとラベルスイッチドパス (LSP) 間で相互接続する MPLS トンネルは、LSP をコンジットとして使用する MPLS トンネルを介して、同じタイプの 2 つの遠隔インターフェイス回線を接続します。
Exec モードの show コマンド	<b>show mpls ftn [ vrf vrf_name ]</b>	MPLS FEC-to-NHLFE (FTN) テーブルの情報を表示します。
Exec モードの show コマンド	<b>show mpls ftn [ vrf vrf_name ]</b>	指定された VRF の MPLS FTN テーブルの内容を表示します。
Exec モードの show コマンド	<b>show mpls ilm</b>	MPLS の着信ラベルマップ (ILM) テーブルの情報を表示します。
Exec モードの show コマンド	<b>show mpls ldp</b>	MPLS LDP 情報を表示します。

CLI モード	コマンド	説明
Exec モードの show コマンド	<b>show mpls nexthop-label-forwarding-entry</b>	MPLS のネクストホップラベル転送エントリ (NHLFE) テーブルの情報を表示します。

## モニタリングおよびトラブルシューティング

この項では、機能のモニタリングと障害対応に使用できる CLI コマンドに関する情報について説明します。

### コマンドと出力の表示

この項では、この機能のサポートにおける show コマンドおよびコマンドの出力について説明します。

#### show mpls fn vpp

この CLI コマンドの出力には、CUPS の VPC-SI 機能で MPLS をサポートするため、次の新しいフィールドが含まれています。

- vpp
  - all-vrf
  - summary
  - vrf



(注) この新しいフィールドにより、VPP データプレーンフォワーダで設定されている VPP データプレーン値を表示できます。この show コマンドは、既存の debug コマンドと併せてデバッグに使用されます。

show mpls fn vpp



## 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。