



BGP MPLS VPN

この章では、ボーダーゲートウェイプロトコル (BGP)、マルチプロトコルラベルスイッチング (MPLS)、バーチャルプライベートネットワーク (VPN) でサポートされるサービスについて説明します。



重要 MPLSは、別途ライセンスを必要とするライセンス供与されたシスコの機能です。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

説明する項目は次のとおりです。

- [はじめに \(1 ページ\)](#)
- [PE に接続された MPLS-CE \(2 ページ\)](#)
- [VPC-SI PE として \(2 ページ\)](#)
- [BGP MPLS VPN の IPv6 サポート \(4 ページ\)](#)
- [VPN 関連の CLI コマンド \(8 ページ\)](#)

はじめに

サービスプロバイダは、多数の異なるアドレッシングモデルと要件を持つ多数の企業のアクセスポイント名 (APN) をサポートする能力を必要とします。VPC-SIはBGP MPLS レイヤ3 VPN を使用して、拡張性の高い方法で企業顧客の APN を分離します。このソリューションは、RFC 4364 (BGP/MPLS IP のバーチャルプライベートネットワーク (VPN) に準拠しています。

BGP/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。

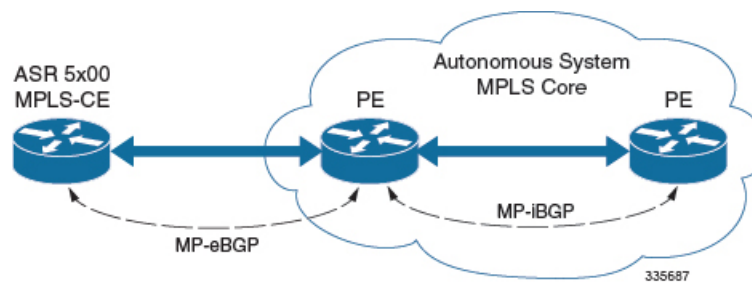
- [PE に接続された MPLS-CE \(2 ページ\)](#)
- [VPC-SI PE として \(2 ページ\)](#)

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。詳細については、[BGP MPLS VPNのIPv6サポート \(4 ページ\)](#) を参照してください。

PEに接続された MPLS-CE

このシナリオでは、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、これにより MPLS コア (RFC 4364) に接続されます。以下の図を参照してください。

図 1: VPC-SIMPLS-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。これにより、Virtual Route 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 にアドバタイズすることができます。この場合、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

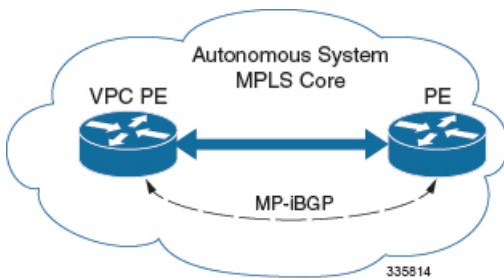
(RSVP) は必要ありません。このシナリオの MPLS-CE は、PE との間で (MP-eBGP 接続を介して学習された) 単一のラベルをプッシュ/ポップします。

VPC-SI PE として

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: VPC-SI PE として



VPC-SI では、最初の 2 つのシナリオに示すように、ASBR または PE の必要性を排除します。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。

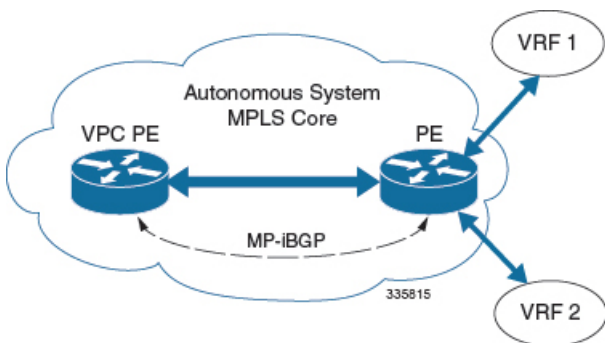
- LDP または RSVP TE から学習した外部ラベル (RSVP トラフィックエンジニアリング)
- MP-iBGP から学習した内部ラベル

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 2.2.2.2
neighbor 192.168.107.20 remote-as 300
neighbor 192.168.107.20 update-source nodel_loopback

address-family vpnv4
  neighbor 192.168.107.20 activate
  neighbor 192.168.107.20 send-community both
  neighbor 192.168.107.20 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 192.168.109.65/24
  mpls ip
exit
router ospf
  network 192.168.109.0/24 area 0.0.0.0
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 アドレスファミリー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ー識別子 (AFI) と後続のアドレスファミリー識別子 (SAFI) のフィールドは、2 と 128 にそれぞれ設定されます。

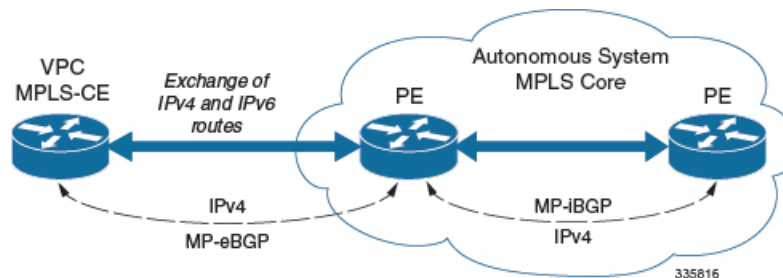
IPv6 VPN トラフィックは、IPv4 トンネリングを介して BGP スピーカーに転送されます。BGP スピーカーは、8 オクテットの RD がゼロに設定され、16 オクテットの IPv6 アドレスがアドバタイズルータの IPv4 アドレスを含む IPv4 マッピング IPv6 アドレス (RFC 4291) としてエンコードされている VPN-IPv6 アドレスを含むネクストホップネットワークアドレスフィールドをピアにアドバタイズします。これは、VPNv6 ルートを交換するために EBGP ピアリングのみが使用されることを前提としています。

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。

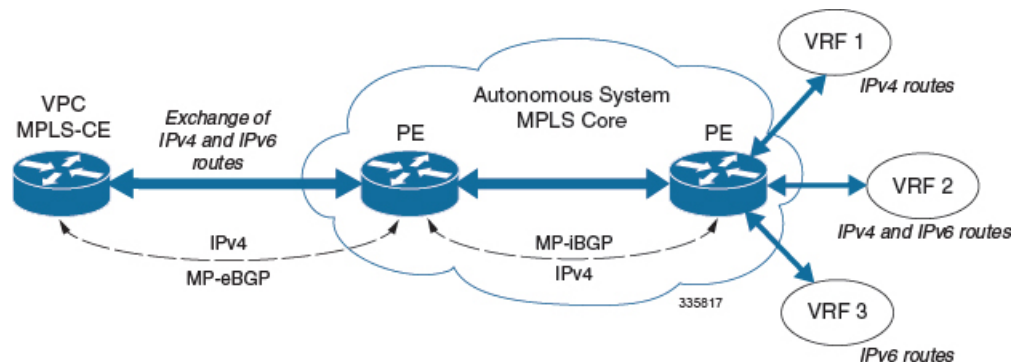
図 4: VPNv6 に対する IPv6-RD サポート



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 f2 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 51.52.53.0 255.255.255.0 private 0 vrf vrf1
exit
ip pool vrf2-pool 51.52.53.0 255.255.255.0 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 192.168.110.90 255.255.255.0
exit
interface ce_v6_interface
ip address 2009:0101:0101:0101::1/96
exit
interface ce_loopback loopback
ip address 52.1.2.3 255.255.255.255
exit
interface vrf1-loop loopback
ip vrf forwarding vrf1
ip address 1.52.53.54 255.255.255.255
exit
interface vrf2-loop loopback
ip vrf forwarding vrf2
ip address 2.52.53.54 255.255.255.255
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
```

アドレスファミリー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 1.1.1.1
 neighbor 192.168.110.20 remote-as 1003
 neighbor 192.168.110.20 activate
 address-family vpnv4
 neighbor 192.168.110.20 activate
 neighbor 192.168.110.20 send-community both
 exit
 address-family vpnv6
 neighbor 192.168.110.20 activate
 neighbor 192.168.110.20 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。

次に示すコマンドの使用に関する詳細については、『*Command Line Interface Reference*』を参照してください。

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) コンフィギュレーションモード	neighbor ip_address activate	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) コンフィギュレーションモード	neighbor ip_address send community { both extended standard }	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) コンフィギュレーションモード	redistribute connected	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 アドレスファミリー (VPNv4) コンフィギュレーションモード	neighbor ip_address activate	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。

CLI モード	コマンド	説明
BGP アドレスファミリー (VPNv4) コンフィギュレーション モード	neighbor ip_address send community { both extended standard }	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) コンフィギュレーション モード	neighbor ip_address activate	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) コンフィギュレーション モード	neighbor ip_address send community { both extended standard }	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) コンフィギュレーション モード	redistribute connected	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 コンフィギュレーション モード	address-family { ipv4 vrf vrf_name vpnv4 }	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 コンフィギュレーション モード	address-family { ipv6 vrf vrf_name vpnv6 }	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 コンフィギュレーション モード	ip vrf vrf_name	BGP に VRF を追加し、VRF コンフィギュレーション 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。

CLI モード	コマンド	説明
BGP IP VRF コンフィギュレーション モード	route-distinguisher { <i>as_value</i> <i>ip_address</i> } <i>rd_value</i>	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。
BGP IP VRF コンフィギュレーション モード	route-target { both import export } { <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 コンフィギュレーション モード	ip pool <i>pool_name</i> <i>addr_range</i> vrf <i>vrf_name</i> [mpls-label input <i>inlabel1</i> output <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 コンフィギュレーション モード	ip vrf <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 コンフィギュレーション モード	ipv6 pool <i>pool_name</i> vrf <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す。
コンテキスト コンフィギュレーション モード	mpls bgp forwarding	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 コンフィギュレーション モード	mpls exp <i>value</i>	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 (mpls map-dscp-exp dscp n exp m コマンドを使用)。 mpls exp 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 コンフィギュレーション モード	mpls ip	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 コンフィギュレーション モード	radius change-authorize-nas-ip ip_address <i>ip_address</i> { encrypted key } <i>value</i> port <i>port_num</i> mpls input <i>inlabel</i> output <i>outlabel1 outlabel2</i>	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。 <i>inlabel</i> は着信 COA トラフィックを識別します。 <i>outlabel1</i> および <i>outlabel2</i> は、COA 応答に追加する MPLS ラベルを指定します。 <i>outlabel1</i> は内部出力ラベル、 <i>outlabel2</i> は外部出力ラベルです。
イーサネット インターフェイス コンフィギュレーション モード	mpls ip	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	clear ip bgp peer	BGP セッションをクリアします。

CLI モード	コマンド	説明
Exec モード	lsp-ping <i>ip_prefix_FEC</i>	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。その後に IPv4 または IPv6 の FEC プレフィックスが続く必要があります。
Exec モード	lsp-traceroute <i>ip_prefix_FEC</i>	パケットが宛先に転送される時に実際にたどる MPLS LSP ルートを検出します。その後に IPv4 または IPv6 の FEC プレフィックスが続く必要があります。
IP VRF コンテキストコンフィギュレーションモード	mpls map-dscp-to-exp dscp <i>dscp_bit_value</i> exp <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 コンテキストコンフィギュレーションモード	mpls map-exp-to-dscp exp <i>exp_bit_value</i> dscp <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 コンフィギュレーションモード	protocol ldp	MPLS プロトコルファミリのコンフィギュレーションモードを作成するか、または既存のプロトコルを設定して、現在のコンテキストで MPLS-LDP コンフィギュレーションモードを開始します。このコマンドは、MPLS プロトコルファミリのプロトコルパラメータを設定します。

CLI モード	コマンド	説明
MPLS-LDP コンフィギュレーション モード	advertise-labels { explicit-null implicit-null }	このコンテキストでシステムによって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 コンフィギュレーション モード	discovery { hello { hello-interval seconds hold-interval seconds } transport-address ip_address }	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 コンフィギュレーション モード	enable	ラベル配布プロトコル (LDP) を有効にします。
MPLS-LDP コンフィギュレーション モード	router-id ip_address	LDP ルータ ID を設定します。
MPLS-LDP コンフィギュレーション モード	session timers { hold-interval seconds keepalive-interval seconds }	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	show ip bgp neighbors	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	show ip bgp vpnv4 { all route-distinguisher vrf }	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	show ip bgp vpnv6	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	show ip bgp vpnv6 { all route-distinguisher vrf }	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	show ip pool	設定された VRF を含むプールの詳細を表示します。

CLI モード	コマンド	説明
Exec モードの show コマンド	show mpls cross-connect	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	show mpls ftn [vrf vrf_name	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	show mpls ftn [vrf vrf_name]	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	show mpls ilm	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	show mpls ldp	MPLS LDP 情報を表示します。
Exec モードの show コマンド	show mpls nexthop-label-forwarding-entry	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。