



MPLS over FlexVPN の設定

最新版発行日：2014年3月28日

MPLS over FlexVPN 機能では、マルチプロトコルラベルスイッチング (MPLS) を動的に確立された IPSec トンネルの上に実装し、それによって重複したアドレススペースをサポートします。

- [MPLS over FlexVPN の前提条件 \(1 ページ\)](#)
- [MPLS over FlexVPN の設定に関する情報 \(1 ページ\)](#)
- [MPLS over FlexVPN の設定方法 \(5 ページ\)](#)
- [MPLS over FlexVPN の設定例 \(6 ページ\)](#)
- [MPLS over FlexVPN の設定に関する追加情報 \(14 ページ\)](#)
- [MPLS over FlexVPN の設定の機能情報 \(15 ページ\)](#)

MPLS over FlexVPN の前提条件

- インターネット キー エクスチェンジバージョン2 (IKEv2) および IPSec が設定されていること。
- MPLS が設定されていること。
- NHRP リダイレクトが設定されていること。

MPLS over FlexVPN の設定に関する情報

MPLS と FlexVPN

重複するアドレッシングスペースを持つネットワークドメインが、VPN ルーティングおよび転送 (VRF) を使用してトラフィックを分離するため、あるドメイン用のデータは別のドメインに入力されなくなります。プロバイダーエッジ (PE) デバイス間のデータセキュリティは、すべての VRF に IPSec 保護を使用するトンネルインターフェイスを定義することで実現されます。これによって、あらゆるドメインからのトラフィックが、対応する IPSec トンネルを通過するようになります。ただし、ドメインおよびノードのメンバーがネットワーク内で成長す

ると、すべての保護ドメインに個別の IPsec トンネルとインターフェイスが必要になるため、これではスケーラブルではなくなる可能性があります。

マルチプロトコル ラベル スイッチング (MPLS) が提供する機能は、VRF あたりまたはプレフィックスあたりでラベルを割り当て、データがルーティングする必要がある正確な VRF を特定します。これは、IPsec 保護と PE 間の単一の IPsec トンネルを持つ、単一の MPLS 認識型インターフェイスのみで実現できます。

MPLS over FlexVPN 機能が提供するソリューションは、Next Hop Resolution Protocol (NHRP) を使用してリモートのカスタマー ネットワークを動的に検出し、同時に IPsec を使用して PE デバイス間のデータ トラフィックを確保する必要がある場合、カスタマー ネットワーク内で重複するアドレス間の通信を実現します。お客様が MPLS ネットワークを導入し、その MPLS ネットワークを、セキュアな方法でインターネットを介して異なるリージョンに新しく設定したネットワーク (動的に判断される) に拡張する場合は、このソリューションを使用できます。

MPLS over FlexVPN ソリューションのコンポーネントは次のとおりです。

- IPsec : リモート スポークが動的に検出された後、スポークとハブの間、およびスポーク間のデータ トラフィックを確保します。
- インターネットキーエクスチェンジバージョン2 (IKEv2) : 静的ルートを、直接接続されたルートとして、ピアのトンネルオーバーレイアドレスに追加します。このルートは、ピアのトンネルオーバーレイアドレスのラベル情報ベース (LIB) に暗黙的な null ラベルを追加する結果になります。



(注) あらゆる LDP NAVER との TCP トンネルの確立に LDP が関係するため、IKEv2 は LDP の代わりに使用されます。LDP を有効化することで、LDP HELLO トラフィックによりスポーク間チャンネルをアクティブにし続け、スポーク間チャンネルが停止しないようにします。したがって、MPLS over FlexVPN 機能の設定時は、**mpls ip** コマンドをトンネルインターフェイスまたは仮想テンプレートで実行する必要があります。

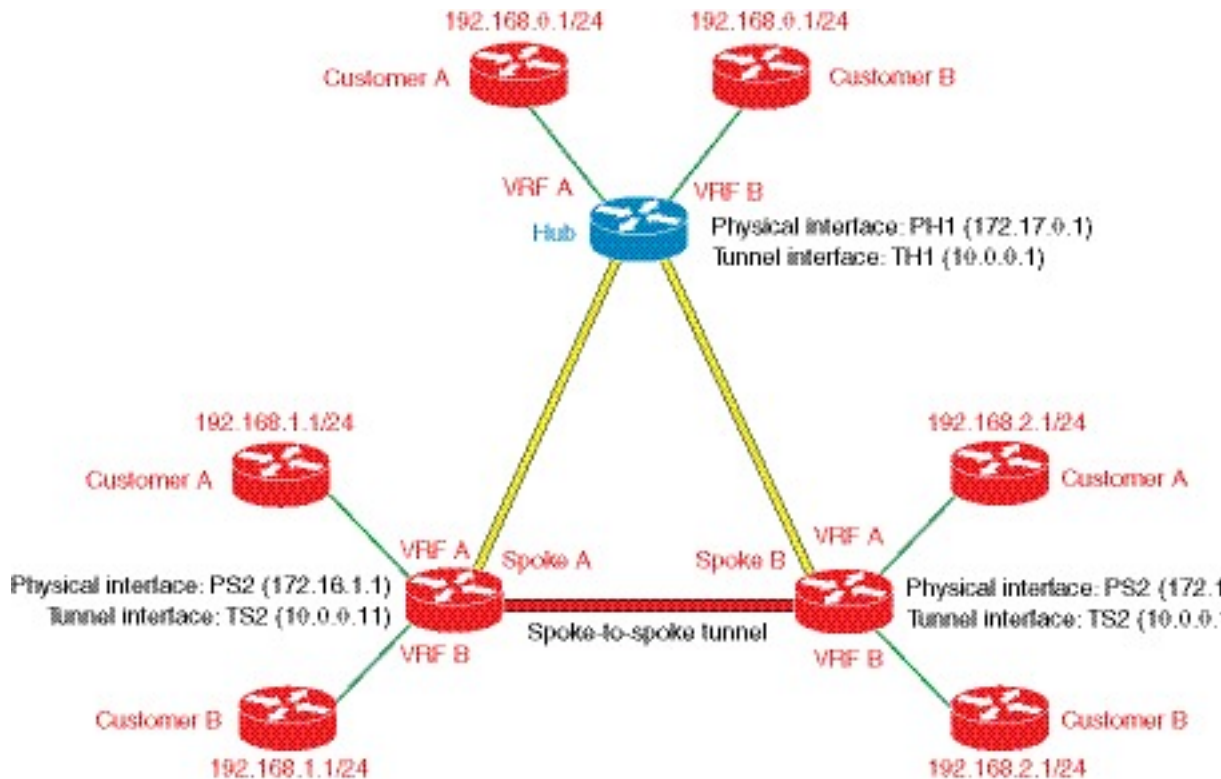
- NHRP : リモート オーバーレイ アドレスを解決し、セキュア トンネルの確立に必要なトランスポート エンドポイントを動的に検出するために使用されます。multipoint Generic Routing Encapsulation (GRE) インターフェイスを使用する場合、トンネルエンドポイント データベースに、オーバーレイと対応するノンブロードキャスト マルチアクセス (NBMA) アドレス間のマッピングを保存します。
- MPLS : データ パケットの MPLS タグ スイッチングを有効化します。LDP キープアライブはスポーク間のトンネルを維持し続けようとし、データ トラフィックが欠けた状態では望まれないため、デフォルトでは、Label Distribution Protocol (LDP : ラベル配布プロトコル) は有効ではなく、スポーク間でも有効ではありません。
- MPLS 転送インフラストラクチャ (MFI) : アプリケーションによってラベルを割り当て、リリースします。NHRP は MFI と呼ばれるラベル管理用のアプリケーションです。

- Multiprotocol BGP (MP-BGP) : オーバーレイ ラベルを異なる VRF のネットワークに分散します。

MPLS over FlexVPN の作業

次の図と記述は、MPLS over FlexVPN ソリューションの作業を説明します。

図 1: スpoke~ハブ~スpoke のトポロジ



MPLS over FlexVPN ソリューションには、次の前提条件があります。

- Multiprotocol BGP (MP-BGP) では、VPN ルーティングおよび転送 (VRF) あたりまたはプレフィックスあたりでラベルを配布できます。
 - ラベル 10 は、Hub から Spoke A に着信するパケット用 VRF A に割り当てられます。
 - ラベル 20 は、Hub から Spoke B に着信するパケット用 VRF A に割り当てられます。
 - ラベル 30 は、Spoke A から Hub に着信するパケット用 Hub の VRF A に割り当てられます。
 - ラベル 40 は、Spoke B から Hub に着信するパケット用 Hub の VRF B に割り当てられます。
1. IKEv2 と IPSec のセキュリティ アソシエーションは、各スポークからハブに確立されます。IKEv2 は、モード構成応答とモード構成セットで受信される、スポークのオーバーレイ アドレスに対して暗黙的 NULL ラベル値をインストールします。



(注) スポークとハブは、いつでもオーバーレイスペースで相互にネクストホップになるため、暗黙的 NULL ラベルがインストールされます。

2. MP-BGP は、VRF あたりのラベルまたはプレフィックスあたりのラベルを、すべての VRF と交換します。
3. ラベルとルートが交換された後は、データの転送が開始されます。192.168.2.1 宛ての最初のデータ パケットは、VRF A の Spoke A に到着すると、ハブに転送されます。パケットは Generic Routing Encapsulation (GRE) を使用してラベルカプセル化されますが、含まれるのはオーバーレイ ラベルのみであり、暗号化されます。
4. データ パケットは、物理 (仮想アクセス) インターフェイス (172.17.0.1) またはトンネル インターフェイス (10.0.0.1) のハブに到着すると、複合化されます。オーバーレイ ラベルがハブ内で検索され、パケットは GRE を使用してカプセル化され、暗号化されて Spoke B に送信されます。
5. NHRP リダイレクト パケットはハブから Spoke A に送信されます。ラベル 30 はデータ パケットが到着する VRF を示すように、VRF 情報は NHRP に伝達されます。
6. NHRP はリダイレクト パケットを処理し、NHRP 解決要求をトリガーします。NHRP マッピング エントリが作成され、VRF A が解決される必要があるプレフィックスに関連付けられます。
7. 解決要求はハブに送信されます。そこではオーバーレイ ラベルが検索され、解決要求は適切な宛先、この場合は Spoke B に送信されます。
8. NHRP 解決要求は Spoke B に到達し、Spoke B の仮想アクセス インターフェイスまたはマルチポイント GRE (mGRE) インターフェイスを作成します。
9. IKEv2 と IPSec のセッションは、Spoke B から Spoke A に開始され、Spoke A の仮想アクセス インターフェイスまたは mGRE インターフェイスが作成されます。NHRP では、新しく作成された仮想アクセス インターフェイスを経由する Spoke A トンネルの IP アドレスへのルートが追加されます。
10. Spoke B からの NHRP 解決応答には、スポーク間トンネル経由でデータを送信するために Spoke A が使用できるラベル値が含まれます。このため、NHRP は、MPLS 転送インスタンス (MFI) からラベルを割り当て、このラベル情報をスポーク間トンネルに使用する Spoke A に送信します。



(注) MFI はラベルを追跡します。ラベルがすでに割り当て済みで、特定の VRF の MP-BGP に指定されている場合、このラベルは NHRP に返されます。MFI はこの特定のラベルを使用してアプリケーションの数を追跡し、すべてのアプリケーションにラベルがリリースされている場合のみ、このラベルをプールに戻します。

11. また、NHRP 解決応答には、Spoke B の仮想アクセス インターフェイスまたは mGRE インターフェイスの IP アドレス用の暗黙的 NULL ラベルが含まれます。この例では、応答は「192.168.2.0/24, label 40, 10.0.0.12, 172.16.2.1, [implicit-NUL]」になります。

12. NHRP 解決応答は、Spoke A の仮想アクセス インターフェイスまたは mGRE インターフェイスで受信されます。応答パケット内の NHRP 要求 ID は、Spoke A によって最初に送信された要求の要求 ID と照合され、要求が送信される VRF が取得されます。NHRP キャッシュで NHRP エントリが検索され、このエントリは「Complete」と呼ばれます。NHRP は、ラベル情報がある VRF ルーティング テーブルにルートを挿入します。
13. Spoke A と Spoke B の間にルートとラベルが設定されます。データはここでラベルカプセル化され、スポーク間で動的に確立された Spoke A と Spoke B の間のトンネルを経由して暗号化されます。

FlexVPN の IVRF サポート

FlexVPN の VPN ルーティングおよび転送 (IVRF) サポートでは、トンネルインターフェイスの IVRF 設定で、次の NHRP ルーティング操作を実行する機能が提供されます。

- ルート ルックアップの実行後に、NHRP 解決要求を送信する。
- ハブの NHRP 解決要求を転送する。
- ショートカット トンネルの作成時に、IVRF での H ルートまたはネクストホップ上書き (NHO) を作成する。
- ショートカット トンネルの削除時に、IVRF から H ルートまたは NHO を削除する。

MPLS over FlexVPN の設定方法

MPLS over FlexVPN の設定

このタスクを実行して、MPLS over FlexVPN を設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface tunnel *number***
4. **mpls nhrp**
5. **end**
6. **show mpls forwarding-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 | enable 例 : Device> enable | 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 | 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 tunnel number 例： Device(config)# interface tunnel 1 | FlexVPN クライアント 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 4 | mpls nhrp 例： Device(config-if)# mpls nhrp | Label Distribution Protocol (LDP : ラベル配布プロトコル) は有効にせず、MPLS タグ スイッチングを有効にします。 |
| ステップ 5 | 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、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 | show mpls forwarding-table 例： Device# show mpls forwarding-table | マルチプロトコル ラベル スイッチング (MPLS) のラベル転送情報ベース (LFIB) に関する情報が表示されます。 |

MPLS over FlexVPN の設定例

例 : MPLS over FlexVPN の設定

次の例は、MPLS 機能を利用して FlexVPN で複数のカスタマー VRF を転送する方法を示します。次は、spoke 1 の設定です。

```
hostname R3-Spoke1
boot-start-marker
boot-end-marker
!
!
vrf definition cust1
 rd 1:1
  route-target export 1:1
  route-target import 1:1
!
 address-family ipv4
  exit-address-family
!
vrf definition cust2
 rd 2:2
  route-target export 2:2
  route-target import 2:2
!
 address-family ipv4
  exit-address-family
```

```
!  
clock timezone CET 1 0  
!  
no ip domain lookup  
ip domain name cisco.com  
ip cef  
no ipv6 cef  
mpls ldp loop-detection  
!  
crypto pki trustpoint CA  
  enrollment url http://172.16.1.1:80  
  password  
  fingerprint E0AFEF7F08070BAB33C8297C97E6457  
  subject-name cn=R3-spoke.cisco.com,OU=FLEX,O=Cisco  
  revocation-check crl none  
!  
crypto pki certificate map mymap 10  
  subject-name co ou = flex  
!  
crypto pki certificate chain CA  
  certificate 03  
  certificate ca 01  
crypto ikev2 authorization policy default  
  route set interface  
!  
crypto ikev2 profile default  
  match certificate mymap  
  identity local fqdn R3-Spoke.cisco.com  
  authentication local rsa-sig  
  authentication remote rsa-sig  
  pki trustpoint CA  
  dpd 60 2 on-demand  
  aaa authorization group cert list default default  
!  
!  
!  
!  
crypto ipsec profile default  
  set ikev2-profile default  
!  
!  
!  
!  
!  
interface Tunnel0  
  ip address negotiated  
  mpls bgp forwarding  
  tunnel source Ethernet0/0  
  tunnel destination 172.16.0.1  
  tunnel protection ipsec profile default  
!  
interface Ethernet0/0  
  description WAN  
  ip address 172.16.1.103 255.255.255.0  
!  
interface Ethernet0/1  
  description LAN  
  no ip address  
  no ip unreachable  
!  
interface Ethernet0/1.10  
  encapsulation dot1Q 10  
  vrf forwarding cust1
```

```

ip address 192.168.113.1 255.255.255.0
!
interface Ethernet0/1.20
encapsulation dot1Q 20
vrf forwarding cust2
ip address 192.168.123.1 255.255.255.0
!
router bgp 100
bgp log-neighbor-changes
neighbor 10.0.0.1 remote-as 10
neighbor 10.0.0.1 ebgp-multihop 255
neighbor 10.0.0.1 update-source Tunnel0
!
address-family ipv4
neighbor 10.0.0.1 activate
exit-address-family
!
address-family vpnv4
neighbor 10.0.0.1 activate
neighbor 10.0.0.1 send-community both
exit-address-family
!
address-family ipv4 vrf cust1
redistribute connected
exit-address-family
!
address-family ipv4 vrf cust2
redistribute connected
exit-address-family
!
ip route 10.0.0.1 255.255.255.255 Tunnel0 name workaround
ip route 172.16.0.1 255.255.255.255 172.16.1.1 name FlexHUB

```

次は、spoke 2 の設定です。

```

hostname R4-Spoke
!
vrf definition cust1
rd 1:1
route-target export 1:1
route-target import 1:1
!
address-family ipv4
exit-address-family
!
vrf definition cust2
rd 2:2
route-target export 2:2
route-target import 2:2
!
address-family ipv4
exit-address-family
!
clock timezone CET 1 0
!
no ip domain lookup
ip domain name cisco.com
ip cef
no ipv6 cef
!
crypto pki token default removal timeout 0
!
crypto pki trustpoint CA
enrollment url http://172.16.1.1:80
password

```



```
fingerprint E0AFefd7F08070BAB33C8297C97E6457
subject-name cn=R4-Spoke.cisco.com,OU=Flex,O=Cisco
revocation-check crl none
!
crypto pki certificate map mymap 10
  subject-name co ou = flex
!
crypto pki certificate chain CA
  certificate 04
  certificate ca 01
!
crypto ikev2 authorization policy default
  route set interface
!
crypto ikev2 profile default
  match certificate mymap
  identity local fqdn R4.cisco.com
  authentication local rsa-sig
  authentication remote rsa-sig
  pki trustpoint CA
  dpd 60 2 on-demand
  aaa authorization group cert list default default
  virtual-template 1
!
crypto ipsec profile default
  set ikev2-profile default
!
interface Loopback100
  vrf forwarding cust1
  ip address 192.168.114.1 255.255.255.0
!
interface Loopback101
  vrf forwarding cust2
  ip address 192.168.124.1 255.255.255.0
!
interface Tunnel0
  ip address negotiated
  mpls bgp forwarding
  tunnel source Ethernet0/0
  tunnel destination 172.16.0.1
  tunnel protection ipsec profile default
!
interface Ethernet0/0
  description WAN
  ip address 172.16.1.104 255.255.255.0
!
interface Ethernet0/1
  description LAN
  ip address 192.168.104.1 255.255.255.0
!
router bgp 100
  bgp log-neighbor-changes
  neighbor 10.0.0.1 remote-as 10
  neighbor 10.0.0.1 ebgp-multihop 255
  neighbor 10.0.0.1 update-source Tunnel0
!
  address-family ipv4
    neighbor 10.0.0.1 activate
  exit-address-family
!
  address-family vpnv4
    neighbor 10.0.0.1 activate
    neighbor 10.0.0.1 send-community both
  exit-address-family
```

```

!
address-family ipv4 vrf cust1
  redistribute connected
exit-address-family
!
address-family ipv4 vrf cust2
  redistribute connected
exit-address-family
!
ip route 10.0.0.1 255.255.255.255 Tunnel0
ip route 172.16.0.1 255.255.255.255 172.16.1.1 name FlexHUB

```

次は、ハブの設定です。

```

hostname R1-HUB
aaa new-model
!
!
aaa authorization network default local
!
!
clock timezone CET 1 0
!
ip vrf cust1
  rd 1:1
  route-target export 1:1
  route-target import 1:1
!
ip vrf cust2
  rd 2:2
  route-target export 2:2
  route-target import 2:2
!
no ip domain lookup
ip domain name cisco.com
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
mpls ldp loop-detection
!
crypto pki trustpoint CA
  enrollment url http://172.16.0.2:80
  password
  fingerprint E0AFEF7D7F08070BAB33C8297C97E6457
  subject-name CN=R1-HUB.cisco.com,OU=FLEX,OU=VPN,O=Cisco Systems,C=US,L=Linux
  revocation-check crl none
  rsa-keypair R1-HUB.cisco.com 2048
  auto-enroll 95
!
!
crypto pki certificate chain CA
  certificate 02
  certificate ca 01
!
redundancy
!
!
!
crypto ikev2 authorization policy default
  pool mypool
  banner ^C Welcome ^C
  def-domain cisco.com
!
!

```

```
!  
!  
crypto ikev2 profile default  
  match identity remote fqdn domain cisco.com  
  identity local dn  
  authentication local rsa-sig  
  authentication remote rsa-sig  
  pki trustpoint CA  
  dpd 60 2 on-demand  
  aaa authorization group cert list default default  
  virtual-template 1  
!  
  
crypto ipsec profile default  
  set ikev2-profile default  
!  
!  
!  
!  
!  
interface Loopback0  
  description VT source interface  
  ip address 10.0.0.1 255.255.255.255  
!  
interface Ethernet0/0  
  description WAN  
  ip address 172.16.0.1 255.255.255.252  
!  
interface Ethernet0/1  
  description LAN  
  ip address 192.168.100.1 255.255.255.0  
!  
interface Ethernet0/2  
  ip vrf forwarding cust1  
  ip address 192.168.110.1 255.255.255.0  
!  
interface Ethernet0/3  
  ip vrf forwarding cust2  
  ip address 192.168.111.1 255.255.255.0  
!  
interface Virtual-Template1 type tunnel  
  ip unnumbered Loopback0  
  ip nhrp network-id 1  
  ip nhrp redirect  
  mpls bgp forwarding  
  tunnel protection ipsec profile default  
!  
router bgp 10  
  bgp log-neighbor-changes  
  bgp listen range 0.0.0.0/0 peer-group mpls  
  bgp listen limit 5000  
  neighbor mpls peer-group  
  neighbor mpls remote-as 100  
  neighbor mpls transport connection-mode passive  
  neighbor mpls update-source Loopback0  
!  
  address-family ipv4  
    redistribute static route-map global  
    neighbor mpls activate  
    neighbor mpls next-hop-self  
  exit-address-family  
!  
  address-family vpnv4
```

```

neighbor mpls activate
neighbor mpls send-community both
exit-address-family
!
address-family ipv4 vrf cust1
  redistribute connected
  redistribute static route-map cust1
  default-information originate
exit-address-family
!
address-family ipv4 vrf cust2
  redistribute connected
  redistribute static route-map cust2
  default-information originate
exit-address-family
!
ip local pool mypool 10.1.1.1 10.1.1.254
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 172.16.0.2 name route_to_internet
ip route vrf cust1 0.0.0.0 0.0.0.0 Null0 tag 666 name default_originate
ip route vrf cust2 0.0.0.0 0.0.0.0 Null0 tag 667 name default_originate
!
route-map cust1 permit 10
  match tag 666
!
route-map cust2 permit 10
  match tag 667

```

次は、スポークからのサンプル出力です。

```
Device# show ip cef vrf cust1 192.168.110.1
```

```

192.168.110.0/24, epoch 0, flags rib defined all labels, RIB[B], refcount 5,
per-destination sharing
  sources: RIB
  feature space:
    IPRM: 0x00018000
    LFD: 192.168.110.0/24 0 local labels
        contains path extension list
  ifnums: (none)
  path EF36CA28, path list EF36DEB4, share 1/1, type recursive, for IPv4, flags
must-be-labelled
    MPLS short path extensions: MOI flags = 0x0 label 19
    recursive via 10.0.0.1[IPv4:Default] label 19, fib F0C5926C, 1 terminal fib,
v4:Default:10.0.0.1/32
    path EF36CBE8, path list EF36DFF4, share 1/1, type attached host, for IPv4
    MPLS short path extensions: MOI flags = 0x1 label implicit-null
    attached to Tunnel0, adjacency IP midchain out of Tunnel0 F0481718
    output chain: label 19 label implicit-null TAG midchain out of Tunnel0 F1D97A90 IP adj
out of Ethernet0/0, addr 172.16.1.1 F0481848
R4-Spoke#sh ip bgp vpnv4 all label
  Network          Next Hop          In label/Out label
Route Distinguisher: 1:1 (cust1)
  0.0.0.0           10.0.0.1          nolabel/18
  192.168.110.0     10.0.0.1          nolabel/19
  192.168.114.0     0.0.0.0           16/nolabel(cust1)
Route Distinguisher: 2:2 (cust2)
  0.0.0.0           10.0.0.1          nolabel/20
  192.168.111.0     10.0.0.1          nolabel/21
  192.168.124.0     0.0.0.0           17/nolabel(cust2)

```

次は、ハブからのサンプル出力です。

```
Device# show ip cef vrf cust1 192.168.113.1

192.168.113.0/24, epoch 0, flags rib defined all labels, RIB[B], refcount 5,
per-destination sharing
  sources: RIB, LTE
  feature space:
    IPRM: 0x00018000
    LFD: 192.168.113.0/24 1 local label
    local label info: other/25
      contains path extension list
      disposition chain 0xF1E1D9B0
      label switch chain 0xF1E1D9B0
  ifnums: (none)
  path F16ECA10, path list F16EDFBC, share 1/1, type recursive, for IPv4, flags
must-be-labelled
    MPLS short path extensions: MOI flags = 0x0 label 16
    recursive via 10.1.1.3[IPv4:Default] label 16, fib FOCCD6E8, 1 terminal fib,
v4:Default:10.1.1.3/32
      path F16ECE00, path list F16EE28C, share 1/1, type attached host, for IPv4
        MPLS short path extensions: MOI flags = 0x1 label implicit-null
        attached to Virtual-Access1, adjacency IP midchain out of Virtual-Access1 F04F35D8
        output chain: label 16 label implicit-null TAG midchain out of Virtual-Access1 F1E1DF60
        IP adj out of Ethernet0/0, addr 172.16.0.2 F04F3708
R1-HUB#sh ip bgp vpv4 all
BGP table version is 49, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, x best-external, f
RT-Filter, a additional-path
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop           Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf cust1)
*> 0.0.0.0          0.0.0.0            0             32768 ?
*> 192.168.110.0    0.0.0.0            0             32768 ?
*> 192.168.113.0    10.1.1.3           0              0 100 ?
*> 192.168.114.0    10.1.1.4           0              0 100 ?
Route Distinguisher: 2:2 (default for vrf cust2)
*> 0.0.0.0          0.0.0.0            0             32768 ?
*> 192.168.111.0    0.0.0.0            0             32768 ?
*> 192.168.123.0    10.1.1.3           0              0 100 ?
*> 192.168.124.0    10.1.1.4           0              0 100 ?
Device# show ip bgp vpv4 all 192.168.113.1

BGP routing table entry for 1:1:192.168.113.0/24, version 48
Paths: (1 available, best #1, table cust1)
  Advertised to update-groups:
    3
  Refresh Epoch 1
  100
    10.1.1.3 from *10.1.1.3 (172.16.1.103)
      Origin incomplete, metric 0, localpref 100, valid, external, best
      Extended Community: RT:1:1
      mpls labels in/out 25/16
BGP routing table entry for 2:2:0.0.0.0/0, version 8
Paths: (1 available, best #1, table cust2)
  Advertised to update-groups:
    3
  Refresh Epoch 1
  Local
    0.0.0.0 from 0.0.0.0 (10.0.0.1)
      Origin incomplete, metric 0, localpref 100, weight 32768, valid, sourced, best
```

```
Extended Community: RT:2:2
mpls labels in/out 20/aggregate(cust2)
```

MPLS over FlexVPN の設定に関する追加情報

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』 |
| セキュリティ コマンド | <ul style="list-style-type: none"> 『Cisco IOS Security Command Reference Commands A to C』 『Cisco IOS Security Command Reference Commands D to L』 『Cisco IOS Security Command Reference Commands M to R』 『Cisco IOS Security Command Reference Commands S to Z』 |
| 推奨される暗号化アルゴリズム | 『Next Generation Encryption』 |

標準および RFC

| 標準/RFC | タイトル |
|----------|--|
| RFC 5586 | <i>MPLS Generic Associated Channel</i> |

シスコのテクニカル サポート

| 説明 | リンク |
|--|---|
| 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 over FlexVPN 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 トレー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 1: MPLS over FlexVPN の設定の機能情報

| 機能名 | リリース | 機能情報 |
|-------------------|------|--|
| MPLS over FlexVPN | | 次のコマンドが導入または変更されました。 clear ip nhrp, clear ipv6 nhrp, mpls nhrp, show dmvpn, show ip nhrp, show ipv6 nhrp. |

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。