Configuring MPLS over DMVPN

The MPLS over DMVPN feature implements Multiprotocol Label Switching (MPLS) over a dynamically established IPsec tunnel, thereby enabling communication between overlapping addresses in customer sites.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn . An account on Cisco.com is not required.

Prerequisites for Configuring MPLS over DMVPN

- MP-BGP must be configured as MP-BGP allows labels to be distributed for every prefix or per VRF; label assignment per VRF would make it easy to maintain.
- NHRP Redirect feature must be installed as an MPLS output feature. To send the NHRP redirect, NHRP must know the VRF to which the redirect must be sent to.

Information About MPLS over DMVPN

MPLS over DMVPN Networks

Traffic in network domains having overlapping addressing spaces are segregated via VRFs. This is to ensure that traffic intended for one customer does not enter into another customer's domain. To protect data between provider-edge (PE) devices using IPsec, a tunnel interface with IPsec protection can be defined for each VRF, which ensures that traffic from every customer domain passes over the corresponding IPsec tunnel. However, as the number of customer sites and nodes grow in the network, this is not scalable since there is a need for separate IPsec tunnel and an interface for each customer site that must be protected.

MPLS provides the ability to assign labels per-VRF or per-prefix, thereby identifying the correct VRF into which traffic needs to be routed to. This is achieved with an MPLS-aware interface having IPsec protection and an IPsec tunnel built between the PE devices. The basic methodologies in MPLS are as follows:

MPLS forwarding—This is used in the transport networks where a label is pushed at the ingress PE device for a particular prefix and the labels are swapped as the data moves towards the egress PE device. At the egress PE device or a device before the egress PE (penultimate hop pop), the label is popped and data is forwarded based on the Layer 3 protocol. LDP is typically the label distribution protocol run in the transport space along with unicast routing protocol.

MPLS VPNs—This is used to carry data across a transport network between customer sites on VRFs. The overlay prefixes are identified by a VPN overlay label and is used as an inner label in a MPLS data packet. The outer label is the MPLS transport label and is for switching the packet in the core. LDP is used along with a IGP to achieve MPLS unicast IP forwarding in the core network and MP-BGP provides a mechanism to identity the customer VRF network to which a packet is forwarded when a packet arrives at Egress Label Edge Router (E-LER). Each of the protocols – LDP and MP-BGP protocols distribute labels to help in achieving this.

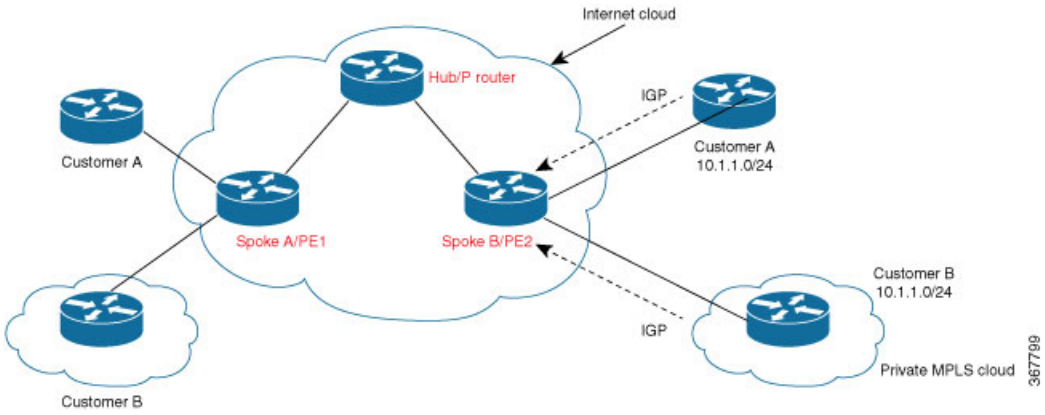
The goal of the MPLS over Dynamic IPsec Tunnels feature is to provide a solution that helps communication between overlapping addresses in customer sites when a remote customer site needs to be discovered dynamically using NHRP and at the same time secure the data traffic between the PE routers using IPsec. This solution can be used to deploy an MPLS network and to extend their MPLS network on a new network (determined dynamically), in a different region, securely over the Internet.

Until this feature was introduced, MPLS support on DMVPN existed in a DMVPN hub and spoke network only. The feature extends support in DMVPN spoke to spoke networks where data packets are tag-switched on the hub and cannot trigger a NHRP redirect thereby addressing a scalable solution using multipoint GRE interface on DMVPN networks and point-to-point interface on FlexVPN networks.

The Need for MPLS

The basic goal of a Layer 3 VPN network is to allow sites in a customer network to communicate with each other. The following diagram explains the need for MPLS with the help of an example.

Figure 1: Overlapping addresses in Customer Edge (CE) Domain



Per the above diagram, Customer A network behind spoke A/PE1 router needs to communicate with the customer A subnet 10.1.1.0/24. However, because of overlapping address space with customer B, spoke B/PE2 router would learn about two different 10.1.1.0/24 prefixes and if it picks the route to customer B as best route, packets would never reach the customer A network behind spoke B.

MPLS solves this problem by associating labels for each customer prefix present in different VRF tables. These labels are distributed between PEs, used during packet forwarding to determine the correct customer network to which a packet should be forwarded to. MPLS deals with overlapping prefixes by prepending another number to the BGP NLRI (prefix). MP-BGP has the provision of adding a variable-length number called address family in front of the prefix. MPLS VPNs use the address family to carry route distinguishers (RDs). The combined VPNv4 address (64-bit RD + 32-bit prefix) makes the address unique. The steps involved are:

- Provider and provider-edge devices run LDP and IGP to support unicast IP routing. IGP only advertises routes for subnets inside the MPLS network but does not include any customer routes.
- PEs learn customer specific routes using IGP and store the routes in per-customer VRF routing tables.
- PEs use MP-BGP to exchange customer routes with other PEs.

Components of MPLS over Dynamic IPSec Tunnels Feature

The essential components of this solution comprise:

IKEv2 and IPsec—Internet Key Exchange version 2 (IKEv2) and IPsec secure traffic between spoke and the hub and later between the spokes when the remote spoke is discovered dynamically. IKEv2 is used to add static routes to the peer's tunnel overlay address as a directly connected route in FlexVPN. This results in an implicit-NULL label to be added to the LIB for the peer's tunnel overlay address. (IPRM (IP Resource manager) adds the implicit-NULL label and is the common component that is used for implicit-NULL label addition by applications such as LDP and now IKEv2). IKEv2 is used instead of LDP for the following reasons:

If LDP is used for distributing transports labels, it involves establishing TCP channel with every LDP neighbor making it heavy-weight in a scaled scenario.

LDP keepalive will try to keep the spoke-to-spoke tunnel active, even in the absence of traffic, and never bring the spoke-to-spoke tunnel down.

NHRP—Next Hop Resolution Protocol (NHRP) resolves the remote overlay address and dynamically discovers the transport end point needed to establish a secure tunnel. If a multipoint GRE interface is used, the tunnel

end point database stores the mapping between the overlay and corresponding nonbroadcast multiaccess (NBMA) address. NHRP control packets that are not specific to a VRF are forwarded to global addresses. Control packets specific to a virtual domain context (for example, resolution request destined for a customer network or host address) are forwarded to a specific VRF.

MPLS—Multiprotocol label switching (MPLS) enables MPLS tag switching for data packets. Label Distribution Protocol (LDP) is not enabled between spokes.

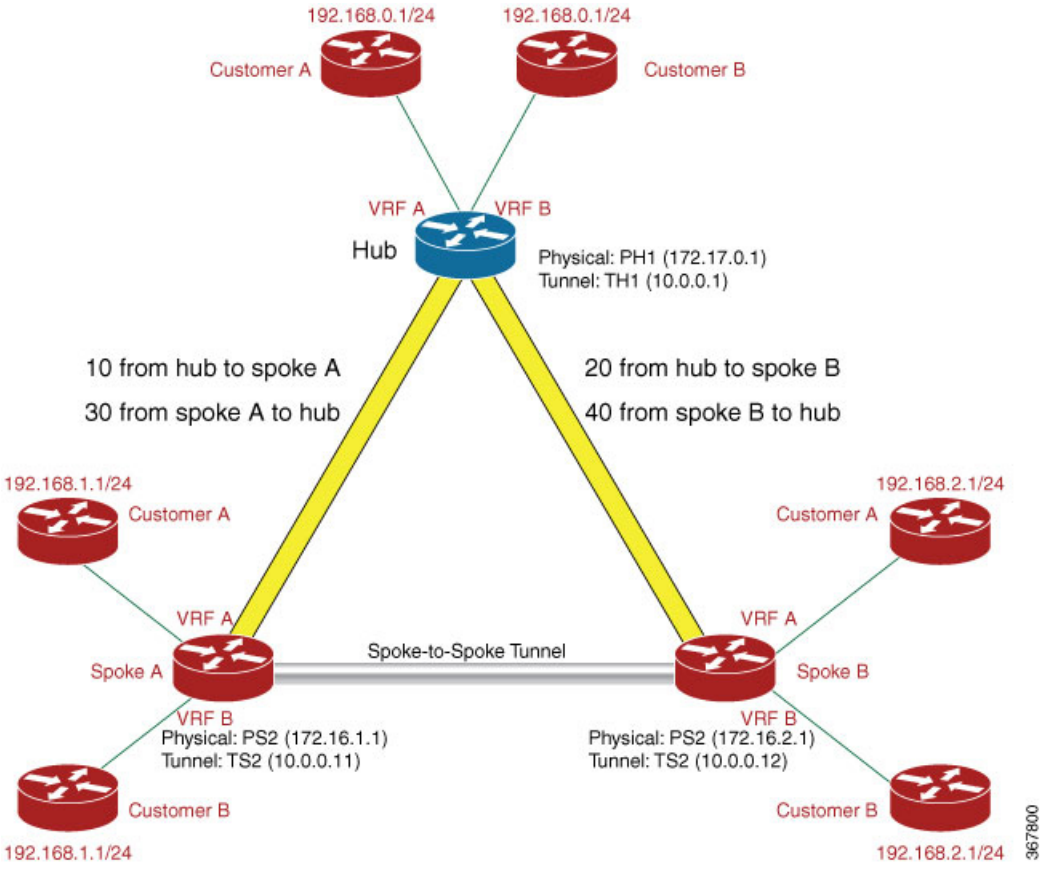
MFI—Multicast Forwarding Information (MFI) allocates and releases labels assigned to tunnels.

MP-BGP—Multiprotocol BGP (MP-BGP) distributes overlay labels for the customer network on different VRFs.

Working of MPLS over Dynamic IPSec Tunnels Feature

This section describes the working of the MPLS over Dynamic IPsec Tunnels featyre with the help of the following topology as an example, where traffic flows from IP address 192.168.1.1 of Customer A, behind Spoke A to IP address 192.168.2.1 of Customer A, behind Spoke B.

Figure 2: DMVPN Spoke-Hub-Spoke Topology



1. IKEv2 and IPsec security associations (SA) are established from the spoke to the hub. IKEv2 installs the implicit-NULL label values for the peer's overlay address received in the mode config reply and mode config set. Implicit-NULL label is installed because the spoke and hub are always next hop to each other

in the overlay space. To enable MPLS tag switching, use the mpls nhrp command on the tunnel interface or virtual template interface.

Note Using the mpls ip command performs the same function as mpls nhrp command but enables LDP also, which is not recommended.

2. After establishing an IPsec session between a spoke and a hub and the implicit-NULL label is installed, MP-BGP exchanges label per-VRF or label per-prefix for all VRFs.
3. Data is forwarded when label and route exchange is complete. When the first packet destined for 192.168.2.1 arrives on spoke A on VRF A, the packet is forwarded to the hub. The packet is label encapsulated (with just the overlay label), GRE encapsulated and encrypted.
4. When the packet reaches the virtual access interface or GRE interface on the hub, the packet is decrypted and GRE decapsulated. The label identifies the VRF on which the packet arrives and the VRF information corresponding to the label is conveyed to NHRP. NHRP constructs the redirect packet and dispatches the packet in the MPLS switching path and sends the packet to MPLS LSP. The packet is label encapsulated, GRE encapsulated, encrypted, and sent to the host behind Spoke A.
5. The redirect packet (NHRP) arrives at spoke A, is decrypted, and is GRE decapsulated. The redirect packet is processed and a NHRP resolution request is triggered. The request is sent to a specific VRF in a host network behind Spoke B. This is because the host network behind Spoke B needs to be resolved and it is also possible that the network can have overlapping address with another network. MPLS provides the VRF information, which corresponds to the outer VRF label. This resolution packet is label encapsulated, GRE encapsulated, encrypted and sent to the hub. An NHRP mapping entry is created and VRF A is also associated for the prefix that needs to be resolved.
6. NHRP resolution request arrives at the hub and is decrypted and GRE decapsulated. NHRP looks up the route in the VRF table and identifies the outgoing interface. The resolution request is label encapulated, GRE encapsulated, encrypted and sent to Spoke 2.
7. Spoke B decrypts the resolution request packet gets decrypted on the spoke B and learns the VRF label. A virtual access is created on Spoke B for point-to-point solution and an IKEv2 or IPsec session is initiated from Spoke B to Spoke A. This result in the creation of virtual access on Spoke A also by IKEv2 in a point-to-point solution. NHRP adds the route for Spoke A tunnel IP address via the new virtual access interface.
8. NHRP resolution reply is received at virtual access interface on Spoke A. NHRP request ID in the reply packet is matched with the request ID of the request, which is sent by Spoke A to know the VRF for which the request was sent. NHRP looks up to find the NHRP entry and the entry is said to be “Complete.” NHRP also inserts a route into the VRF routing table with the label information. With the routes and labels setup between Spoke A and Spoke B, traffic is VPN label encapsulated and encrypted over the spoke-spoke dynamically established tunnel between Spoke A to Spoke B.

IVRF Support

If a tunnel interface belongs to an IVRF, routing related operations, such as, route lookup, route addition and deletion, that happen in NHRP are performed in the routing table of IVRF configured on tunnel interface.

How to Configure MPLS over DMVPN

Configuring MPLS over FlexVPN

Perform this task to configure MPLS over DMVPN.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. Do one of the follwing: **mpls nhrp**or **mpls bgp forwarding**
5. **end**
6. **show mpls forwarding-table**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface tunnel** *number* **Example:** `Device(config)# interface tunnel 1`	Configures the FlexVPN client interface and enters interface configuration mode.

Step 4	Do one of the follwing: **mpls nhrp**or **mpls bgp forwarding**
	Example:
	`Device(config-if)# mpls nhrp`
	`Device(config-if)# mpls bgp forwarding`	

Step 5	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to global configuration mode.
Step 6	**show mpls forwarding-table** **Example:** `Device# show mpls forwarding-table`	Displays information about the Multiprotocol Label Switching (MPLS) Label Forwarding Information Base (LFIB).

Configuration Examples for MPLS over FlexVPN

Example: MPLS over DMVPN—Using LDP and BGP

This section lists a sample configuration on spokes and the hub using LDP and BGP. The following is the configuration on Spoke A:

```
ip vrf custA
rd 10:100
route-target export 10:1000
route-target import 10:1000
!
ip vrf custB
rd 10:110
route-target export 10:2000
route-target import 10:2000
mpls label mode all-vrfs protocol bgp-vpnv4 per-vrf
!
crypto ikev2 authorization policy default
route set interface
!
!
!
crypto ikev2 keyring KR
peer All
address 0.0.0.0 0.0.0.0
pre-shared-key Cisco123
!
!
crypto ikev2 profile default
match identity remote fqdn domain cisco.com
identity local fqdn R2.cisco.com
authentication local pre-share
authentication remote pre-share
keyring local KR
aaa authorization group psk list default default
virtual-template 2
!
crypto ipsec profile default
set ikev2-profile default
interface Loopback0
ip address 10.0.0.101 255.255.255.255
!
interface Tunnel0
ip address 10.0.0.11 255.255.255.255
mpls bgp forwarding
ip nhrp network-id 1
ip nhrp shortcut virtual-template 2
tunnel source Ethernet0/1
tunnel destination 172.17.0.1
tunnel protection ipsec profile default
!
interface Ethernet0/0
ip vrf forwarding custA
ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/1
ip address 172.16.1.1 255.255.255.0
!
interface Ethernet0/2
ip vrf forwarding custB
ip address 192.168.1.1 255.255.255.0
```

```
interface Ethernet1/0
ip vrf forwarding custA
ip address 192.168.50.254 255.255.255.0
router ospf 10
network 172.16.1.0 0.0.0.255 area 0
!
router bgp 100
bgp log-neighbor-changes
neighbor 10.0.0.103 remote-as 100
neighbor 10.0.0.103 update-source Loopback0
neighbor 10.0.0.103 soft-reconfiguration inbound
!
address-family vpnv4
neighbor 10.0.0.103 activate
neighbor 10.0.0.103 send-community both
exit-address-family
!
address-family ipv4 vrf custA
network 192.168.1.0
network 192.168.50.0
exit-address-family
!
address-family ipv4 vrf custB
network 192.168.1.0
exit-address-family
```

The following is the configuration on Spoke B:

```
ip vrf custA
rd 10:100
route-target export 10:100
route-target export 10:1000
route-target import 10:100
route-target import 10:1000
!
ip vrf custB
rd 10:110
route-target export 10:2000
route-target import 10:2000
mpls label mode all-vrfs protocol bgp-vpnv4 per-vrf
!
crypto ikev2 authorization policy default
route set interface
!
!
crypto ikev2 keyring KR
peer All
address 0.0.0.0 0.0.0.0
pre-shared-key Cisco123
!
!
!
crypto ikev2 profile default
match identity remote fqdn domain cisco.com
identity local fqdn R3.cisco.com
authentication local pre-share
authentication remote pre-share
keyring local KR
aaa authorization group psk list default default
virtual-template 2
!
crypto ipsec profile default
set ikev2-profile default
!
interface Loopback0
```

```
ip address 10.0.0.104 255.255.255.255
interface Tunnel0
ip address 10.0.0.12 255.255.255.255
mpls bgp forwarding
ip nhrp network-id 1
ip nhrp shortcut virtual-template 2
tunnel source Ethernet0/0
tunnel destination 172.17.0.1
tunnel protection ipsec profile default
!
interface Ethernet0/0
ip address 172.16.2.1 255.255.255.0
!
interface Ethernet0/1
ip vrf forwarding custA
ip address 192.168.2.1 255.255.255.0
!
interface Ethernet0/2
ip vrf forwarding custB
ip address 192.168.2.1 255.255.255.0
router ospf 10
network 172.16.2.0 0.0.0.255 area 0
!
router bgp 100
bgp log-neighbor-changes
neighbor 10.0.0.101 remote-as 100
neighbor 10.0.0.101 update-source Loopback0
neighbor 10.0.0.101 soft-reconfiguration inbound
neighbor 10.0.0.103 remote-as 100
neighbor 10.0.0.103 update-source Loopback0
neighbor 10.0.0.103 soft-reconfiguration inbound
!
address-family vpnv4
neighbor 10.0.0.101 activate
neighbor 10.0.0.101 send-community both
neighbor 10.0.0.103 activate
neighbor 10.0.0.103 send-community both
exit-address-family
!
address-family ipv4 vrf custA
network 192.168.2.0
network 192.168.70.0
exit-address-family
!
address-family ipv4 vrf custB
network 192.168.2.0
exit-address-family
!
```

The following is the hub configuration.

```
ip vrf custA
rd 10:100
route-target export 10:1000
route-target import 10:1000
!
mpls label mode all-vrfs protocol bgp-vpnv4 per-vrf
!
crypto ikev2 authorization policy default
pool FPool
route set interface
!
crypto ikev2 keyring KR
peer All
address 0.0.0.0 0.0.0.0
```

```
pre-shared-key Cisco123
!
!
!
crypto ikev2 profile default
match identity remote fqdn domain cisco.com
identity local fqdn R1.cisco.com
authentication local pre-share
authentication remote pre-share
keyring local KR
aaa authorization group psk list default default
virtual-template 1
!
!
crypto ipsec profile default
set ikev2-profile default
!
interface Loopback0
ip address 10.0.0.103 255.255.255.255
!
interface Loopback1
ip address 10.0.0.1 255.255.255.0
!
!
interface Ethernet0/0
ip address 172.17.0.1 255.255.255.0
!
interface Ethernet1/0
ip vrf forwarding custA
ip address 192.168.70.254 255.255.255.0
!
interface Virtual-Template1 type tunnel
ip unnumbered Loopback1
mpls bgp forwarding
ip nhrp network-id 1
ip nhrp redirect
tunnel protection ipsec profile default
!
ip local pool FPool 10.1.0.1 10.1.0.100
!
router ospf 10
network 172.17.0.0 0.0.0.255 area 0
!
router bgp 100
bgp log-neighbor-changes
neighbor 10.0.0.101 remote-as 100
neighbor 10.0.0.101 update-source Loopback0
neighbor 10.0.0.101 soft-reconfiguration inbound
neighbor 10.0.0.104 remote-as 100
neighbor 10.0.0.104 update-source Loopback0
neighbor 10.0.0.104 soft-reconfiguration inbound
auto-summary
!
address-family vpnv4
neighbor 10.0.0.101 activate
neighbor 10.0.0.101 send-community both
neighbor 10.0.0.101 next-hop-self
neighbor 10.0.0.104 activate
neighbor 10.0.0.104 send-community both
neighbor 10.0.0.104 next-hop-self
exit-address-family
!
address-family ipv4 vrf custA
redistribute static route-map rm
```

```
exit-address-family
!
ip route vrf custA 0.0.0.0 0.0.0.0 Null0 tag 10
ip route vrf custA 192.168.0.0 255.255.0.0 Null0 tag 10
!
ip access-list extended out1
permit ip any any
!
!
route-map rm permit 10
match tag 10
```

Example: MPLS over DMVPN - Using MPLS

The following is the configuration on Spoke 1:

```
hostname R3-Spoke
!
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 E0AFEFD7F08070BAB33C8297C97E6457
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
ip nhrp map multicast
ip nhrp map
ip nhrp nhs
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 unreachables
!
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
```

The following is the configuration on Spoke B.

```
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
The hub configuration is as follows:
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 E0AFEFD7F08070BAB33C8297C97E6457
subject-name CN=R1-HUB.cisco.com,OU=FLEX,OU=VPN,O=Cisco Systems,C=US,L=Linux
revocation-check crl none
rsakeypair 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
```

The following is the spoke output:

```
R4-Spoke# 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# show 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)
```

The following is the hub output:

```
R1-HUB# show ip cef vrf cust1 192.168.113.1 in
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 F0CCD6E8, 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 vpnv4 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 ?
R1-HUB# show ip bgp vpnv4 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)
```

Restrictions for Configuring 6VPE and 6PE Support in MPLS over DMVPN Phase 2

- 6VPE and 6PE in DMVPN Phase 3 behaves like DMVPN Phase 1. All the packets from spoke-to-spoke travel through the hub as no dynamic spoke-to-spoke tunnel is created.
- In DMVPN Phase 2, if the dynamic spoke-to-spoke tunnel is not created for some reason, the packets do not travel through the hub, causing failure in connectivity.
- Initial packets from spoke-to-spoke travel in cleartext and drop by the hub until the dynamic tunnel is established between spokes.

Configuring 6VPE Support in MPLS over DMVPN Phase 2

To configure 6VPE support in MPLS over DMVPN phase 2, you must enable various components such as VRF, Tunnel, IPsec Tunnel Protection, WAN Facing Interface, Transport routing and Overlay Routing for the hub and the spokes.

Enabling Components for the Hub

To configure 6VPE support in MPLS over DMVPN phase 2 for the hub, you must enable the following in the order:

1. VRF
2. Tunnel
3. IPsec Tunnel Protection
4. WAN Facing Interface
5. Transport Routing
6. Overlay Routing

Configuring VRF for the Hub

```
enable
config terminal
vrf definition blue
rd 100:1
address-family ipv6
route-target export 100:1
route-target import 100:1
exit-address-family
vrf definition red
rd 100:2
address-family ipv6
route-target export 100:2
route-target import 100:2
exit-address-family
```

Enabling Tunnel for the Hub

```
interface Tunnel1
ip address 192.168.1.1 255.255.255.0
no ip redirects
ip nhrp authentication cisco123
ip nhrp network-id 101
mpls nhrp
tunnel source GigabitEthernet0/0/1
tunnel mode gre multipoint
tunnel key 101
```

Enabling IPsec Tunnel Protection for the Hub

```
interface Tunnel1
tunnel protection ipsec profile ipsec_ikev2
no shut
end
```

Enabling WAN Interfaces for the Hub

```
interface GigabitEthernet0/0/1
ip address 10.1.1.1 255.255.255.0
negotiation auto
cdp enable
ipv6 address 10::1/64
```

```
hold-queue 4096 in
hold-queue 4096 out
```

Enabling Transport Routing for the Hub

```
router eigrp 100
network 10.1.1.0 0.0.0.255
```

Enabling Overlay Routing for the Hub

```
router bgp 1
bgp router-id 192.168.1.1
bgp log-neighbor-changes
neighbor 192.168.1.101 remote-as 1
neighbor 192.168.1.101 update-source Tunnel1
neighbor 192.168.1.102 remote-as 1
neighbor 192.168.1.102 update-source Tunnel1
address-family ipv4
neighbor 192.168.1.101 activate
neighbor 192.168.1.102 activate
exit-address-family
address-family vpnv6
neighbor 192.168.1.101 activate
neighbor 192.168.1.101 send-community extended
neighbor 192.168.1.101 route-reflector-client
no neighbor 192.168.1.101 next-hop-self all
neighbor 192.168.1.102 activate
neighbor 192.168.1.102 send-community extended
neighbor 192.168.1.102 route-reflector-client
no neighbor 192.168.1.102 next-hop-self all
exit-address-family
address-family ipv6 vrf blue
redistribute connected
exit-address-family
address-family ipv6 vrf red
redistribute connected
exit-address-family
```

Enabling the Components for the Spokes

To configure 6VPE support in MPLS over DMVPN phase 2, you must enable the following for the spokes in the order:

1. VRF
2. Tunnel
3. IPsec Tunnel Protection
4. WAN Facing Interface
5. PE-CE Interfaces
6. Transport Routing
7. Overlay Routing

Configuring VRF for the Spokes

```
vrf definition blue
 rd 100:1
 address-family ipv6
    route-target export 100:1
    route-target import 100:1
 exit-address-family
vrf definition red
 rd 100:2
 address-family ipv6
    route-target export 100:2
    route-target import 100:2
 exit-address-family
```

Enabling Tunnel for the Spokes

```
interface Tunnel1
 ip address 192.168.1.101 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco123
 ip nhrp map multicast 10.1.1.1
 ip nhrp map 192.168.1.1 10.1.1.1
 ip nhrp network-id 101
 ip nhrp nhs 192.168.1.1
 mpls nhrp
 tunnel source GigabitEthernet0/0/1
 tunnel mode gre multipoint
 tunnel key 101
```

Enabling IPsec Tunnel Protection for Spokes

```
interface Tunnel1
tunnel protection ipsec profile ipsec_ikev2
no shut
end
```

Enabling WAN Facing Interfaces for Spokes

```
interface GigabitEthernet0/0/1
 ip address 40.1.1.6 255.255.255.0
 negotiation auto
 ipv6 address 40::6/64
 ipv6 enable
```

Enabling PE-CE Interfaces for Spokes

```
interface GigabitEthernet0/0/3.1
 vrf forwarding blue
 encapsulation dot1q 1
 ip address 60.1.1.6 255.255.255.0
 negotiation auto
 ipv6 address 60::6/64
 ipv6 enable
interface GigabitEthernet0/0/3.2
 vrf forwarding red
 encapsulation dot1q 2
 ip address 80.1.1.6 255.255.255.0
 negotiation auto
 ipv6 address 80::6/64
 ipv6 enable
```

Enabling Transport Routing for Spokes

```
router eigrp 100
 network 40.1.1.0 0.0.0.255
```

Enabling Overlay Routing for the Spokes

```
router bgp 1
 bgp router-id 192.168.1.101
 bgp log-neighbor-changes
 neighbor 192.168.1.1 remote-as 1
 neighbor 192.168.1.1 update-source Tunnel1
 address-family ipv4
  neighbor 192.168.1.1 activate
 exit-address-family
 address-family vpnv6
  neighbor 192.168.1.1 activate
  neighbor 192.168.1.1 send-community extended
 exit-address-family
 address-family ipv6 vrf blue
  redistribute connected
 exit-address-family
 address-family ipv6 vrf red
  redistribute connected
 exit-address-family
```

Enabling Transport Routing for IPv6

The 6VPE over DMVPN with IPv6 transport feature allows IPv6 LAN prefixes over an IPv4 overlay neighbourship created over an IPv6 DMVPN transport. Multi-tenant IPv6 LAN extension (L3VPN) over DMVPN supports IPv6 transport. It supports IPv6 transport and Inter-region connectivity with daisy-chained hubs.

```
!
ipv6 router eigrp 1
 eigrp router-id 1.1.1.1
!
```

Enabling WAN Interfaces for IPv6

```
!
interface GigabitEthernet2
 no ip address
 negotiation auto
 ipv6 address 172:16:1::1/64
 ipv6 eigrp 1
 no mop enabled
 no mop sysid
!
interface GigabitEthernet3
 no ip address
 negotiation auto
 ipv6 address 172:16:2::1/64
 ipv6 eigrp 1
 no mop enabled
 no mop sysid
!
interface GigabitEthernet4
 no ip address
```

```
 negotiation auto
 ipv6 address 172:16:3::1/64
 ipv6 eigrp 1
 no mop enabled
 no mop sysid
```

Enabling Tunnel for Hubs

The following configuration allows you one of the hubs to get daisy-chained with other hubs.

```
!
interface Tunnel1
 ip address 50.0.1.1 255.255.0.0
 ip nhrp network-id 1
 ip nhrp nhs 50.0.2.2 nbma 172:16:52::52 multicast
 ip nhrp nhs 50.0.2.3 nbma 172:16:53::53 multicast
 ip nhrp nhs 50.0.3.4 nbma 172:16:54::54 multicast
 load-interval 30
 ipv6 mtu 1450
 mpls nhrp
 if-state nhrp
 tunnel source Loopback0
 tunnel mode gre multipoint ipv6
 tunnel key 1
 tunnel path-mtu-discovery
end
```

Enabling Tunnel for Spokes

```
!
interface Tunnel1
 ip address 50.0.1.6 255.255.0.0
 ip nhrp network-id 1
 ip nhrp nhs 50.0.1.1 nbma 172:16:51::51 multicast
 load-interval 30
 ipv6 mtu 1450
 mpls nhrp
 if-state nhrp
 tunnel source Loopback0
 tunnel mode gre multipoint ipv6
 tunnel key 1
 tunnel path-mtu-discovery
end
```

Configuring 6PE Support in MPLS over DMVPN Phase 2

To configure 6PE Support in MPLS over DMVPN Phase 2, you must enable various components such as Tunnel, IPsec Tunnel Protection, WAN Facing Interfaces,Transport Routing, and Overlay Routing for the hub and spokes.

Enabling Components for the Hub

To configure 6PE support in MPLS over DMVPN phase 2, you must enable the following in the order:

1. Tunnel

2. IPsec Tunnel Protection
3. WAN Facing Interfaces
4. PE-CE Interfaces
5. Transport Routing
6. Overlay Routing

Enabling Tunnel for Hub

```
interface Tunnel1
 ip address 192.168.1.1 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco123
 ip nhrp network-id 101
 mpls nhrp
 tunnel source GigabitEthernet0/0/1
 tunnel mode gre multipoint
 tunnel key 101
```

Enabling IPsec Tunnel Protection for the Hub

```
interface Tunnel1
tunnel protection ipsec profile ipsec_ikev2
no shut
end
```

Enabling WAN Facing Interfaces for Hub

```
interface GigabitEthernet0/0/1
 ip address 10.1.1.1 255.255.255.0
 negotiation auto
 cdp enable
 ipv6 address 10::1/64
 hold-queue 4096 in
 hold-queue 4096 out
```

Enabling Transport Routing for Hub

```
router eigrp 100
network 10.1.1.0 0.0.0.255
```

Enabling Overlay Routing for Hub

```
router bgp 1
 bgp router-id 192.168.1.1
 bgp log-neighbor-changes
 neighbor 192.168.1.101 remote-as 1
 neighbor 192.168.1.101 update-source Tunnel1
 neighbor 192.168.1.102 remote-as 1
 neighbor 192.168.1.102 update-source Tunnel1
 address-family ipv4
  neighbor 192.168.1.101 activate
  neighbor 192.168.1.102 activate
 exit-address-family
 address-family ipv6
  redistribute connected
```

```
 neighbor 192.168.1.101 activate
 neighbor 192.168.1.101 send-community extended
 neighbor 192.168.1.101 route-reflector-client
 no neighbor 192.168.1.101 next-hop-self all
 neighbor 192.168.1.102 activate
 neighbor 192.168.1.102 send-community extended
 neighbor 192.168.1.102 route-reflector-client
 no neighbor 192.168.1.102 next-hop-self all
exit-address-family
```

Enabling Components for the Spokes

To configure 6PE support in MPLS over DMVPN phase 2, you must enable the following for the spokes:

1. Tunnel
2. IPsec Tunnel Protection
3. WAN Facing Interface
4. PE-CE Interfaces
5. Transport Routing
6. Overlay Routing

Enabling Tunnel for Spokes

```
interface Tunnel1
 ip address 192.168.1.101 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco123
 ip nhrp map multicast 10.1.1.1
 ip nhrp map 192.168.1.1 10.1.1.1
 ip nhrp network-id 101
 ip nhrp nhs 192.168.1.1
 mpls nhrp
 tunnel source GigabitEthernet0/0/1
 tunnel mode gre multipoint
 tunnel key 101
```

Enabling IPsec Tunnel Protection for Spokes

```
interface Tunnel1
tunnel protection ipsec profile ipsec_ikev2
no shut
end
```

Enabling WAN Facing Interfaces for Spokes

```
interface GigabitEthernet0/0/1
 ip address 40.1.1.6 255.255.255.0
 negotiation auto
 ipv6 address 40::6/64
 ipv6 enable
```

Enabling PE-CE Interface for Spokes

```
interface GigabitEthernet0/0/3.1
 encapsulation dot1q 1
```

```
 ip address 60.1.1.6 255.255.255.0
 negotiation auto
 ipv6 address 60::6/64
 ipv6 enable
interface GigabitEthernet0/0/3.2
 encapsulation dot1q 2
 ip address 80.1.1.6 255.255.255.0
 negotiation auto
 ipv6 address 80::6/64
 ipv6 enable
```

Enabling Transport Routing for Spokes

```
router eigrp 100
 network 40.1.1.0 0.0.0.255
```

Enabling Overlay Routing for Spokes

```
router bgp 1
 bgp router-id 192.168.1.101
 bgp log-neighbor-changes
 neighbor 192.168.1.1 remote-as 1
 neighbor 192.168.1.1 update-source Tunnel1
 address-family ipv4
  neighbor 192.168.1.1 activate
 exit-address-family
address-family ipv6
  redistribute connected
  neighbor 192.168.1.1 activate
  neighbor 192.168.1.1 send-community extended
 exit-address-family
```

Verifying the 6VPE support in MPLS over DMVPN Phase 2 Configurations

Use the following show commands to verify that the 6VPE support in MPLS over DMVPN phase 2 configurations are enabled on the router:

```
show ipv6 route vrf blue 60::/64
show ipv6 route vrf blue 70::/64
show mpls forwarding-table
show mpls forwarding-table vrf blue 60::/64 detail
show mpls forwarding-table vrf blue 70::/64 detail
show ipv6 cef vrf blue 60::/64
show ipv6 cef vrf blue 70::/64
show ipv6 cef vrf red 61::/64
show ipv6 cef vrf red 71::/64
show bgp vpnv6 unicast all
show dmvpn
show ip nhrp
```

Verifying the 6PE support in MPLS over DMVPN Phase 2 Configurations

Use the following show commands to verify that the 6PE support in MPLS over DMVPN phase 2 configurations are enabled on the router:

```
show ipv6 route vrf blue 60::/64
show ipv6 route vrf blue 70::/64
show mpls forwarding-table
show mpls forwarding-table vrf blue 60::/64 detail
show mpls forwarding-table vrf blue 70::/64 detail
show ipv6 cef vrf blue 60::/64
show ipv6 cef vrf blue 70::/64
show ipv6 cef vrf red 61::/64
show ipv6 cef vrf red 71::/64
show bgp ipv6 unicast
show dmvpn
show ip nhrp
```

Feature Information for MPLS over DMVPN

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Configuring MPLS over DMVPN

Feature Name	Releases	Feature Information
6VPE and 6PE Support in MPLS over DMVPN	Cisco IOS XE Gibraltar 16.10.x	The 6VPE and 6PE Support in MPLS over DMVPN feature enables service providers running an MPLS/IPv4 infrastructure to offer IPv6 services without any major changes in the infrastructure. It enables IPv6 sites to communicate with each other over a DMVPN MPLS/IPv4 core network using MPLS label switched paths (LSPs).