MPLS VPN—BGP Local Convergence

First Published: December 31, 2007
Last Updated: July 23, 2010

This document provides information about reducing the downtime of a provider edge (PE), to customer edge (CE) link failure. It describes how to reroute PE-egress traffic onto a backup path to the CE, before BGP has reconverged. The MPLS VPN—BGP Local Convergence feature is also referred to as "local protection."

This document explains how to use PE-CE local convergence. For information on using BGP PIC-Edge for BGP local convergence support, see *BGP PIC Edge for IP and MPLS-VPN*.

Note The MPLS VPN—BGP Local Convergence feature affects only traffic exiting the Virtual Private Network. Therefore, it cannot fully protect traffic end-to-end by itself.

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 for MPLS VPN—BGP Local Convergence" section on page 15.

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

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for MPLS VPN—BGP Local Convergence

- Before MPLS VPN —BGP Local Convergence link protection can be enabled, the customer site must be connected to the provider site by more than one path.
- Both the main forwarding path and the redundant backup path must have been installed within Border Gateway Protocol (BGP), and BGP must support lossless switchover between operational paths.
- Any of the supported routing protocols can be used between the PE and CE as long as the path is redistributed into BGP. The supported protocols for IPv4 are External BGP (eBGP), Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), and static routing.The supported protocols for IPv6 are External BGP (eBGP) and static routing.
- All PE routers that are serving as backup to the link must have assigned a unique Route Distinguisher to each VRF table involved with the link to ensure that the route reflectors advertise all available paths.
- Although not required, it is recommended that the backup PE (shown as “PE2” in Figure 2) runs the same Cisco IOS release that is running on the PE (“PE1”) whose link with the CE will be protected; that is, Cisco IOS Release 12.2(33) SRC, 12.2(33)SB, Cisco IOS 15.0(1)M, Cisco IOS 15.0(1)S, or a more recent version of those products.

Restrictions for MPLS VPN—BGP Local Convergence

- This feature affects only traffic exiting the VPN. Therefore, it cannot fully protect traffic end-to-end by itself.
- This link protection cannot be initiated *during* a High Availability (HA) stateful switchover (SSO). But links already configured with this protection *before* the switchover begins will remain protected after the switchover.
- If you perform an in-service software downgrade from an image that does include this link protection to an image that does not support this feature, active protection will be halted when BGP routes are refreshed.
- Any next-hop core tunneling technology that is supported by BGP is also supported for protection, including Multiprotocol Label Switching (MPLS), IP/Layer 2Tunneling Protocol version 3 (L2TPv3), and IP/Generic Routing Encapsulation (GRE). Enabling a Carrier Supporting Carrier (CsC) protocol between the PE and CE is also supported. Inter-autonomous system option A (back-to-back Virtual Routing and Forwarding (VRF)) is supported because it is essentially the same as performing the PE-CE link protection in both autonomous systems. However, inter-autonomous system options B and C protection are not supported.
- MPLS VPN—BGP local convergence for IPv4 supports the External BGP (eBGP), Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), and static routing protocols only.
- MPLS VPN—BGP local convergence for IPv6 supports the eBGP and static routing protocols only.

Information About MPLS VPN—BGP Local Convergence

To configure the MPLS VPN—BGP Local Convergence feature, you should understand the following concepts:

How Link Failures Are Handled with BGP

Within a Layer 3 VPN network, the failure of a PE-CE link can cause a loss of connectivity (LoC) to a customer site, which is detrimental to time-sensitive applications. Several factors contribute to the duration of such an outage:

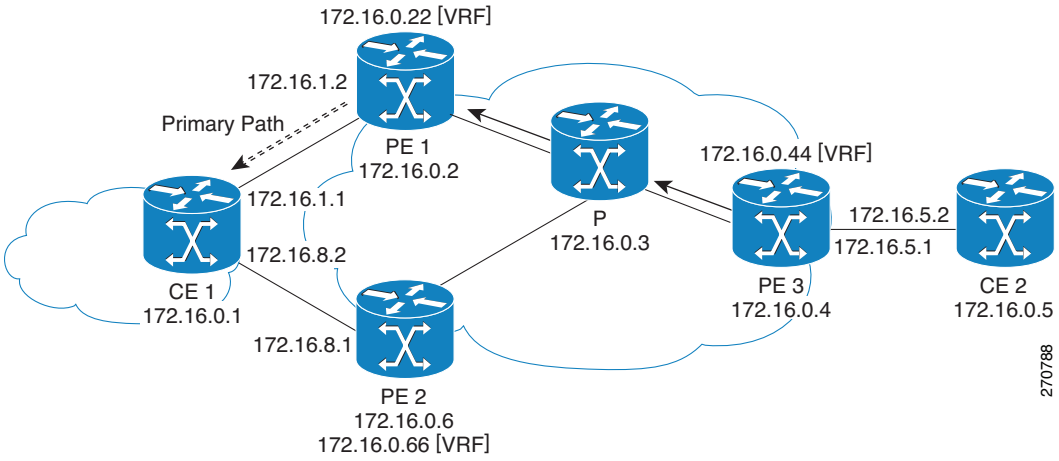
- The time to detect the failure
- The programming of the forwarding
- The convergence of BGP (In large networks, the restored traffic arrival time at its destination varies according to the prefix.)

When BGP detects a PE-CE link failure, it removes all of the BGP paths through the failing link. BGP runs the best-path algorithm on the affected prefixes and selects alternate paths for each prefix. These new paths (which typically include a remote PE) are installed into forwarding. The local labels are removed and BGP withdrawals are sent to all BGP neighbors. As each BGP neighbor receives the withdrawal messages (typically indirectly using route reflectors), the best-path algorithm is called and the prefixes are switched to an alternate path. Only then is connectivity restored.

How Links Are Handled with the MPLS VPN—BGP Local Convergence Feature

The MPLS VPN—BGP Local Convergence feature requires that the prefixes to be protected on a PE-CE link have at least one backup path that does not include that link. (See Figure 1.) The customer site must have backup paths to the provider site.

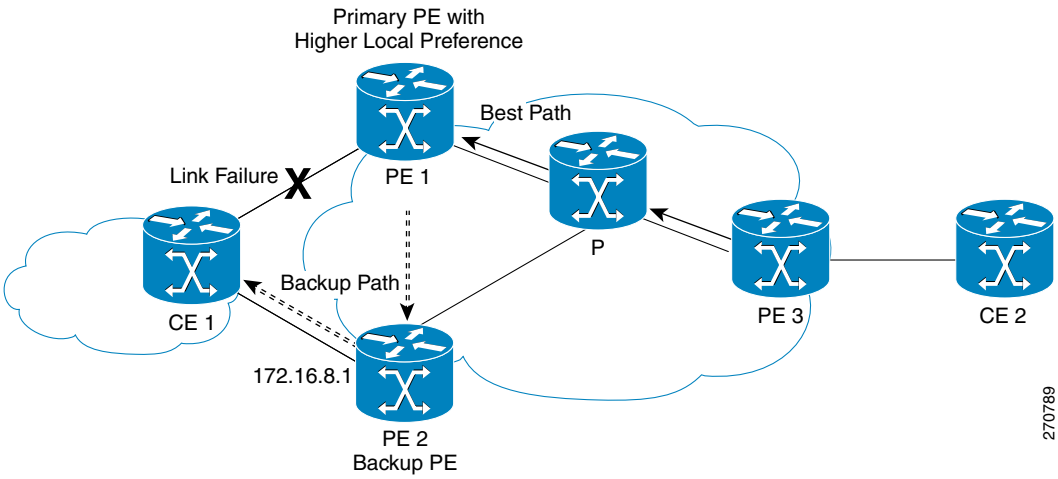
Figure 1 Network Configured with Primary and Backup Paths



The MPLS VPN—BGP Local Convergence feature reduces LoC time by sending the broken link's traffic over a backup path (as shown in Figure 2) instead of waiting for total network convergence. The local label is maintained for 5 minutes while prefixes switch from the failing local path to the backup path. Because the label is not freed as had been the usual practice, forwarding continues to take place.

The best-path algorithm selects the backup path. Thus, the local label has been applied in place of the failed BGP best-path label (which is sometimes called "label swapping"). Traffic is restored locally while the network propagation of the BGP withdrawal messages takes place. Eventually, the egress PE router converges and bypasses the local repair.

Figure 2 Network Using the Backup Path After a PE-CE Link Failure on the Primary Path



Note After the 5-minute label preservation, the local labels are freed. Any BGP prefix that is remote and is not part of a Carrier Supporting Carrier network does not have a local label and is removed. The delay in local label deletion does not modify normal BGP addition and deletion of BGP paths. Rather, BGP reprograms the new backup best-path into forwarding as usual.

How Link Failures Are Detected

Local protection relies on BGP being notified of the interface failure. Detection can occur using either the interface drivers or the routing tables. If an interface or route goes down, the corresponding path in the routing table is removed and BGP will be notified using the routing application programming interfaces (APIs).

However, when the routing table cannot detect the failure (as when a Layer 2 switch goes down), BGP determines that a neighbor is down through use of its hold-down timer. However, that determination can be extremely slow because of the 3-minute default for BGP session timeout.

You can reduce the detection delay by either reducing the BGP session timeout interval (as described in the *Configuring Internal BGP Features* document) or by enabling the Bidirectional Forwarding Detection protocol (BFD) within eBGP between the PE and CE. For complete instructions to enable BFD, see the *Bidirectional Forwarding Detection* document.

How to Enable MPLS VPN—BGP Local Convergence

This section contains the following tasks:

Configuring MPLS VPN—BGP Local Convergence with IPv4

Perform the following steps to configure MPLS VPN to BGP local convergence for IPv4 MPLS VPNs.

Note To configure a Virtual Private Network (VPN) routing and forwarding (VRF) instance for IPv4 and IPv6 VPNs or to upgrade your existing single-protocol IPv4-only VRF to a multiprotocol VRF configuration, see *MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs*.

Prerequisite

Ensure that the CE is already connected to the PE by a minimum of two paths.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **protection local-prefixes**
6. **do show ip vrf detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip vrf** *vrf-name* **Example:** `Router(config)# ip vrf vpn1`	Enters VRF configuration mode. • If no VRF routing table and Cisco Express Forwarding table had been previously created for this named VRF, then this command also creates them, giving both tables the specified *vrf-name* (in this example, the name is vpn1).

	Command or Action	Purpose
Step 4	**rd** *route-distinguisher* **Example:** `Router(config-vrf)# rd 100:3`	(Optional) Establishes the route distinguisher for the named VRF. • If no route distinguisher had been previously established for the named VRF, then it is necessary to enter this command. • The route distinguisher value can be either an: – Autonomous system number followed by a colon and an arbitrary number (for example, 100:3) or – IP address followed by a colon and an arbitrary number (for example, 192.168.122.15:1).
Step 5	**protection local-prefixes** **Example:** `Router(config-vrf)# protection local-prefixes`	Allows a preconfigured backup path to carry traffic if the PE-CE link breaks by preserving the local prefixes while BGP reconverges.
Step 6	**do show ip vrf detail** **Example:** `Router(config-vrf)# do show ip vrf detail`	(Optional) Verifies that MPLS VPN—BGP local convergence has been configured.

Configuring MPLS VPN—BGP Local Convergence with IPv6

Perform the following steps to configure MPLS VPN to BGP local convergence for IPv6 MPLS VPNs.

Prerequisite

Ensure that the CE is already connected to the PE by a minimum of two paths.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **rd** *route-distinguisher*
5. **address-family** [**ipv4** | **ipv6**]
6. **protection local-prefixes**
7. **do show ip vrf detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vrf definition** *vrf-name* **Example:** `Router(config)# vrf definition vrf2`	Enters VRF definition configuration mode. If no VRF routing table and Cisco Express Forwarding (CEF) table had been previously created for this named VRF, then this command also creates them, giving both tables the specified *vrf-name* (in this example, the name is `vrf2`).
Step 4	**rd** *route-distinguisher* **Example:** `Router(config-vrf)# rd 200:4`	(Optional) Establishes the route distinguisher for the named VRF. • If no route distinguisher had been previously established for the named VRF, then it is necessary to enter this command. • The route distinguisher value can be either an: – Autonomous system number followed by a colon and an arbitrary number (for example, 100:3) or – IP address followed by a colon and an arbitrary number (for example, 192.168.122.15:1).
Step 5	**address-family** [**ipv4** | **ipv6**] **Example:** `Router(config-vrf)# address-family ipv6`	Enters address family configuration mode and specifies the IPv4 or IPv6 protocol.
Step 6	**protection local-prefixes** **Example:** `Router(config-vrf-af)# protection local-prefixes`	Allows a preconfigured backup path to carry traffic if the PE-CE link breaks by preserving the local prefixes while BGP reconverges.
Step 7	**do show ip vrf detail** **Example:** `Router(config-vrf-af)# do show ip vrf detail`	(Optional) Verifies that MPLS VPN to BGP Local Convergence has been configured.

Examples

To verify that local link protection has been enabled, enter the VRF detail command **show ip vrf detail**. If the protection is enabled, the status message "`Local prefix protection enabled`" will be shown in the display:

```
Router# show ip vrf detail

VRF vpn1 (VRF Id = 1); default RD 100:1; default VPNID <not set>
  Interfaces:
    AT1/0/1.1
VRF Table ID = 1
  Export VPN route-target communities
    RT:100:1
  Import VPN route-target communities
    RT:100:1                 RT:100:2
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
     Local prefix protection enabled
```

Troubleshooting Tips

- Ensure that a minimum of two paths are present for the protected prefix *w.x.y.z* in BGP in steady state condition on the PE. The path using the protected PE should be the BGP best-path before failover occurs. To display the configuration, enter the **show ip bgp vpnv4 vrf** *vpn w.x.y.z* command.
- Ensure that local protection has been enabled in the protected PE by entering the **show ip vrf detail** command, as shown in the "Examples" section on page 8.
- When route reflectors exist in the topology, ensure that each VRF has a unique route distinguisher.

Configuration Examples for MPLS VPN—BGP Local Convergence

This section contains the following examples:

Configuration Examples for MPLS VPN—BGP Local Convergence

The following examples show how MPLS VPN—BGP local convergence can prevent traffic loss after a link failure. You can display a detailed view of local link protection before, during, and after BGP convergence by using the **show bgp vpnv4** and **show mpls forwarding-table vrf** commands as shown in the following three-stage example.

Note The **show bgp vpnv4 unicast** command is equivalent to the **show ip bgp vpnv4** command.

Example 1: Before the Link Failure

Both a primary path and a backup path have been configured:

```
Router# show bgp vpnv4 unicast all 172.16.0.1

BGP routing table entry for 100:1:172.16.0.1/32, version 2
Paths: (2 available, best #2, table v1)
Flag: 0x820
  Advertised to update-groups:
     1
  100, imported path from 100:2:172.16.0.1/32
    172.16.0.6 (metric 21) from 172.16.0.7 (172.16.0.7)
      Origin incomplete, metric 0, localpref 100, valid, internal
      Extended Community: RT:100:0
      Originator: 172.16.0.6, Cluster list: 172.16.0.7
      mpls labels in/out 16/17
  100
    172.16.1.1 from 172.16.1.1 (172.16.0.1)
      Origin incomplete, metric 0, localpref 100, valid, external, best
      Extended Community: RT:100:0
      mpls labels in/out 16/nolabel
BGP routing table entry for 100:2:172.16.0.1/32, version 9
Paths: (1 available, best #1, no table)
Flag: 0x820
  Not advertised to any peer
  100
    172.16.0.6 (metric 21) from 172.16.0.7 (172.16.0.7)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:100:0
      Originator: 172.16.0.6, Cluster list: 172.16.0.7
      mpls labels in/out nolabel/17
```

Label information for both paths can be displayed:

```
Router1# show bgp vpnv4 unicast all labels

Network          Next Hop      In label/Out label
Route Distinguisher: 100:1 (v1)
   172.16.0.1/32    172.16.0.6      16/17
                    172.16.1.1      16/nolabel
   172.16.0.5/32    172.16.0.4      nolabel/23
   172.16.0.22/32   0.0.0.0         17/nolabel(v1)
   172.16.0.44/32   172.16.0.4      nolabel/24
   172.16.0.66/32   172.16.0.6      nolabel/21
   172.16.1.0/24    172.16.1.1      18/nolabel
                    0.0.0.0         18/nolabel(v1)
   172.16.5.0/24    172.16.0.4      nolabel/25
   172.16.8.0/24    172.16.0.6      19/23
                    172.16.1.1      19/nolabel
Route Distinguisher: 100:2
   172.16.0.1/32    172.16.0.6      nolabel/17
   172.16.0.66/32   172.16.0.6      nolabel/21
   172.16.8.0/24    172.16.0.6      nolabel/23
```

The PE1 (see Figure 1 on page 3) forwarding table contains BGP best-path information:

```
Router1# show mpls forwarding-table vrf v1 172.16.0.1 detail

Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         No Label   172.16.0.1/32[V] 570           Et0/0      172.16.1.1
        MAC/Encaps=14/14, MRU=1504, Label Stack{}
        AABBCC000B00AABBCC000C000800
        VPN route: v1
        No output feature configured
```

Example 2: After the Link Failure and Before BGP Convergence

After the link failure on only one path, the backup path remains available (see Figure 2 on page 4):

```
Router1# show bgp vpnv4 unicast all 172.16.0.1

BGP routing table entry for 100:1:172.16.0.1/32, version 19
Paths: (1 available, best #1, table v1)
  Not advertised to any peer
  100, imported path from 100:2:172.16.0.1/32
    172.16.0.6 (metric 21) from 172.16.0.7 (172.16.0.7)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:100:0
      Originator: 172.16.0.6, Cluster list: 172.16.0.7
      mpls labels in/out 16/17
BGP routing table entry for 100:2:172.16.0.1/32, version 9
Paths: (1 available, best #1, no table)
  Not advertised to any peer
  100
    172.16.0.6 (metric 21) from 172.16.0.7 (172.16.0.7)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:100:0
      Originator: 172.16.0.6, Cluster list: 172.16.0.7
      mpls labels in/out nolabel/17
```

The label information for the backup path label can be displayed:

```
Router1# show bgp vpnv4 unicast all labels

Network          Next Hop      In label/Out label
Route Distinguisher: 100:1 (v1)
   172.16.0.1/32    172.16.0.6      16/17
   172.16.0.5/32    172.16.0.4      nolabel/23
   172.16.0.22/32   0.0.0.0         17/nolabel(v1)
   172.16.0.44/32   172.16.0.4      nolabel/24
   172.16.0.66/32   172.16.0.6      nolabel/21
   172.16.1.0/24    172.16.0.6      nolabel/22
   172.16.5.0/24    172.16.0.4      nolabel/25
   172.16.8.0/24    172.16.0.6      19/23
Route Distinguisher: 100:2
   172.16.0.1/32    172.16.0.6      nolabel/17
   172.16.0.66/32   172.16.0.6      nolabel/21
   172.16.1.0/24    172.16.0.6      nolabel/22
   172.16.8.0/24    172.16.0.6      nolabel/23
```

The PE1 (see Figure 1 on page 3) forwarding table contains new label and next-hop information to direct traffic onto the backup path:

```
Router1# show mpls forwarding-table vrf v1 172.16.0.1 detail

Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         17         172.16.0.1/32[V] 0             Et1/0      172.16.3.2
```

```
        MAC/Encaps=14/22, MRU=1496, Label Stack{21 17}
        AABBCC000D00AABBCC000C018847 0001500000011000
        VPN route: v1
        No output feature configured
```

Example 3: After Local Label Expiration and BGP Reconvergence

Because the local label preservation window has expired, the replacement local label is now gone from the PE1 forwarding table information:

```
Router1# show mpls forwarding-table vrf v1 172.16.0.1 detail

Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
None       17         172.16.0.1/32[V] 0             Et1/0      172.16.3.2
        MAC/Encaps=14/22, MRU=1496, Label Stack{21 17}
        AABBCC000D00AABBCC000C018847 0001500000011000
        VPN route: v1
        No output feature configured
```

The new BGP information reverts to the configuration shown in Figure 1 on page 3:

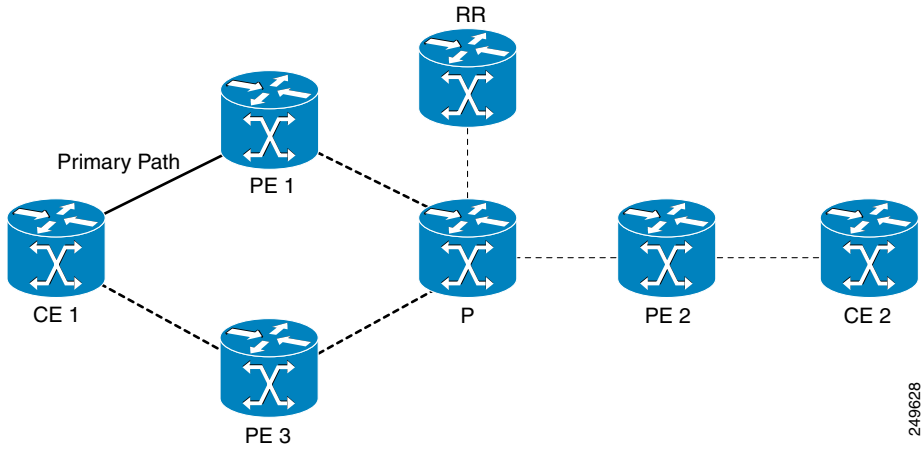
```
Router1# show bgp vpnv4 unicast all 172.16.0.1

BGP routing table entry for 100:1:172.16.0.1/32, version 23
Paths: (1 available, best #1, table v1)
  Not advertised to any peer
  100, imported path from 100:2:172.16.0.1/32
    172.16.0.6 (metric 21) from 172.16.0.7 (172.16.0.7)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:100:0
      Originator: 172.16.0.6, Cluster list: 172.16.0.7
      mpls labels in/out nolabel/17
BGP routing table entry for 100:2:172.16.0.1/32, version 9
Paths: (1 available, best #1, no table)
  Not advertised to any peer
  100
    172.16.0.6 (metric 21) from 172.16.0.7 (172.16.0.7)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:100:0
      Originator: 172.16.0.6, Cluster list: 172.16.0.7
      mpls labels in/out nolabel/17

Router1# show bgp vpnv4 unicast all labels

Network          Next Hop      In label/Out label
Route Distinguisher: 100:1 (v1)
   172.16.0.1/32    172.16.0.6      nolabel/17
   172.16.0.5/32    172.16.0.4      nolabel/23
   172.16.0.22/32   0.0.0.0         17/nolabel(v1)
   172.16.0.44/32   172.16.0.4      nolabel/24
   172.16.0.66/32   172.16.0.6      nolabel/21
   172.16.1.0/24    172.16.0.6      nolabel/22
   172.16.5.0/24    172.16.0.4      nolabel/25
   172.16.8.0/24    172.16.0.6      nolabel/23
Route Distinguisher: 100:2
   172.16.0.1/32    172.16.0.6      nolabel/17
   172.16.0.66/32   172.16.0.6      nolabel/21
   172.16.1.0/24    172.16.0.6      nolabel/22
   172.16.8.0/24    172.16.0.6      nolabel/23
```

Configuration Examples for MPLS VPN—BGP Local Convergence for 6VPE/6PE

You can display a detailed view of local link protection before, during, and after BGP local convergence for Cisco IOS VPN IPv6 provider edge routers (6VPE) and Cisco IOS IPv6 provider edge routers (6PE) over MPLS by using the **show bgp vpnv6** and **show mpls forwarding-table vrf** commands as shown in the following three-stage example.

Figure 3 shows an MPLS VPN with BGP local convergence configured. The PE to CE routing protocol is eBGP, and the PE to route reflector (RR) sessions are BGP VPNv6. The protected prefix is the CE1 loopback (2001:0DB8::/128). The primary path is from PE1 to CE1. The secondary path is from PE1, through P and PE3, to CE1.

Figure 3 MPLS VPN BGP Local Convergence



Example 1: Before the Link Failure

Both a primary path and a backup path have been configured for the prefix 2001:0DB8::/128. The inlabel/outlabel settings for the two paths are 28/28 and 28/nolabel.

```
Router1# show bgp vpnv6 unicast all 2001:0DB8::/128

BGP routing table entry for [1:1]2001:0DB8::/128, version 5
Paths: (2 available, best #2, table v1)
 Advertised to update-groups:
     2
  100, imported path from [2:2]2001:0DB8::/128
    ::FFFF:10.6.6.6 (metric 21) from 10.7.7.7 (10.7.7.7)
      Origin incomplete, metric 0, localpref 100, valid, internal
      Extended Community: RT:1:1
      Originator: 10.6.6.6, Cluster list: 10.7.7.7
      mpls labels in/out 28/28
  100
    2001:0DB8:0:ABCD::1 (FE80::A8BB:CCFF:FE00:B00) from 2001:0DB8:0:ABCD::1 (10.1.1.1)
      Origin incomplete, metric 0, localpref 100, valid, external, best

      Extended Community: RT:1:1
      mpls labels in/out 28/nolabel
BGP routing table entry for [2:2]2001:0DB8::/128, version 11
Paths: (1 available, best #1, no table)
  Not advertised to any peer
  100
    ::FFFF:10.6.6.6 (metric 21) from 10.7.7.7 (10.7.7.7)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
```

```
      Extended Community: RT:1:1
      Originator: 10.6.6.6, Cluster list: 10.7.7.7
      mpls labels in/out nolabel/28
```

The PE1 forwarding table contains new label and next-hop information to direct traffic onto the backup path:

```
Router1# show mpls forwarding-table vrf v1 2001:0DB8::/128 detail

Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
28         No Label   2001:0DB8::/128[V]     804           Et0/0
FE80::A8BB:CCFF:FE00:B00
        MAC/Encaps=14/14, MRU=1504, Label Stack{}
        AABBCC000B00AABBCC000C0086DD
        VPN route: v1
        No output feature configured
```

Example 2: After the Link Failure

After the link failure, the backup path is still available, the original path is removed from BGP, and the backup path is activated:

```
Router1#show mpls forwarding-table vrf v1 2001:0DB8::/128 detail

Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
28         28         2001:0DB8::/128[V]     0             Et1/0      10.3.0.2
        MAC/Encaps=14/22, MRU=1496, Label Stack{23 28}
        AABBCC000D00AABBCC000C018847 000170000001C000
        VPN route: v1
        No output feature configured
```

After a configured length of time, the local label expires. The output from the **show mpls forwarding-table** command also verifies that the local label has expired:

```
Router1#show mpls forwarding-table vrf v1 2001:0DB8::/128 detail

Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
None       28         2001:0DB8::/128[V]     0             Et1/0      10.3.0.2
        MAC/Encaps=14/22, MRU=1496, Label Stack{23 28}
        AABBCC000D00AABBCC000C018847 000170000001C000
        VPN route: v1
        No output feature configured
```

Example 3: After the Link Is Restored

When the link is restored the original path is added to BGP and the traffic switches back to this path:

```
Router1# show bgp vpnv6 unicast all 2001:0DB8::/128

BGP routing table entry for [1:1]2001:0DB8::/128, version 28
Paths: (2 available, best #1, table v1)
  Advertised to update-groups:
     2
  100
    2001:0DB8:0:ABCD::1 (FE80::A8BB:CCFF:FE00:B00) from 2001:0DB8:0:ABCD::1 (10.1.1.1)
      Origin incomplete, metric 0, localpref 100, valid, external, best
      Extended Community: RT:1:1
      mpls labels in/out 16/nolabel
  100, imported path from [2:2]2001:0DB8::/128
    ::FFFF:10.6.6.6 (metric 21) from 10.7.7.7 (10.7.7.7)
      Origin incomplete, metric 0, localpref 100, valid, internal
```

```
      Extended Community: RT:1:1
      Originator: 10.6.6.6, Cluster list: 10.7.7.7
      mpls labels in/out 16/28
BGP routing table entry for [2:2]2001:0DB8::/128, version 11
Paths: (1 available, best #1, no table)
  Not advertised to any peer
  100
    ::FFFF:10.6.6.6 (metric 21) from 10.7.7.7 (10.7.7.7)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:1:1
      Originator: 10.6.6.6, Cluster list: 10.7.7.7
      mpls labels in/out nolabel/28

Router1#show mpls for vrf v1 2001:0DB8::/128 detail

Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         No Label   2001:0DB8::/128[V] 0         Et0/0      FE80::A8BB:CCFF:FE00:B00
        MAC/Encaps=14/14, MRU=1504, Label Stack{}
        AABBCC000B00AABBCC000C0086DD
        VPN route: v1
        No output feature configured
```

Additional References

The following sections provide references related to the MPLS VPN—BGP Local Convergence feature.

Related Documents

Related Topic	Document Title
BGP configuration	*Configuring a Basic BGP Network*
Configuration of BGP PIC Edge for IP and MPLS-VPN	*BGP PIC Edge for IP and MPLS-VPN*
Configuration of internal BGP features	*Configuring Internal BGP Features*
Configuration of VPN routing and forwarding (VRF) instance for IPv4 and IPv6 VPNs	*MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs*
Protocol for quickly detecting failed forwarding paths	*Bidirectional Forwarding Detection*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2547	*BGP/MPLS VPNs*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for MPLS VPN—BGP Local Convergence

Table 1lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 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.

Table 1 Feature Information for MPLS VPN—BGP Local Convergence

Feature Name	Releases	Feature Information
MPLS VPN—BGP Local Convergence	12.2(33)SRC 12.2(33)SB 15.0(1)M	This feature reduces the downtime of a PE-CE link failure by rerouting PE-egress traffic onto a backup path to the CE before BGP has reconverged. In 12.2(33)SRC, this feature was introduced on the Cisco 7200 and the Cisco 7600. In 12.2(33)SB, this feature became available on the Cisco 7300 series and the Cisco 10000 series routers. This feature was integrated into Cisco IOS Release 15.0(1)M. The following command was introduced: **protection local-prefixes**.
MPLS VPN—BGP Local Convergence for 6VPE/6PE	15.0(1)S	This feature implements MPLS VPN—BGP local convergence for Cisco IOS 6VPE and Cisco IOS 6PE over MPLS. The following command was modified: **protection local-prefixes**.