NSF/SSO—MPLS VPN

First Published: August 11, 2004
Last Updated: August 21, 2007

The NSF/SSO—MPLS VPN feature allows a provider edge (PE) router or Autonomous System Border Router (ASBR) (with redundant Route Processors) to preserve data forwarding information in a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) when the primary Route Processor (RP) restarts. This feature module describes how to enable Nonstop Forwarding in MPLS VPN networks, including the following types of VPNs:

- Basic MPLS VPNs
- MPLS VPN—Carrier Supporting Carrier
- MPLS VPN—Carrier Supporting Carrier—IPv4 BGP Label Distribution
- MPLS VPN—Interautonomous Systems
- MPLS VPN—Inter-AS—IPv4 BGP Label Distribution

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for NSF/SSO—MPLS VPN" section on page 65.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS 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

- Prerequisites for NSF/SSO—MPLS VPN, page 2
- Restrictions for NSF/SSO—MPLS VPN, page 2
- Information About NSF/SSO—MPLS VPN, page 3
- How to Configure NSF/SSO—MPLS VPN, page 4

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

- Configuration Examples for NSF/SSO—MPLS VPN, page 9
- Additional References, page 50
- Command Reference, page 52
- Feature Information for NSF/SSO—MPLS VPN, page 65

Prerequisites for NSF/SSO—MPLS VPN

The NSF/SSO—MPLS VPN feature has the following prerequisites:

For information about supported hardware, see the following documents:

- For Cisco IOS Release 12.2(25)S, see the *Cross-Platform Release Notes for Cisco IOS Release 12.2S.*
- For Cisco IOS Release 12.2(28)SB, see the *Cross-Platform Release Notes for Cisco IOS Release 12.2SB.*
- For Cisco IOS Release 12.2(33)SRA, see the *Release Notes for Cisco IOS Release 12.2SR for the Cisco 7600 Series Routers*
- For Cisco IOS Release 12.2(33)SXH, see the following documents:
  - *Release Notes for Cisco IOS Release 12.2SX on the Catalyst 6500 Series MSFC*
  - *Release Notes for Cisco IOS Release 12.2SX on the Supervisor Engine 720, Supervisor Engine 32, and Supervisor Engine 2*

Before enabling Stateful Switchover (SSO), you must enable MPLS Label Distrbution Protocol (LDP) Graceful Restart if you use LDP in the core or in the MPLS VPN routing and forwarding instance in an MPLS VPN Carrier Supporting Carrier configuration. See the *NSF/SSO-MPLS LDP and MPLS LDP Graceful Restart* feature module for more information.

You must enable NSF on the routing protocols running between the provider (P) routers , PE routers, and customer edge (CE) routers. The routing protocols are:

- Border Gateway Protocol (BGP)
- Open Shortest Path First (OSPF)
- Intermediate System-to-Intermediate System (IS-IS)

Cisco nonstop forwarding support must be configured on the routers for Cisco Express Forwarding. See the *Cisco Nonstop Forwarding* feature module for more information.

Before enabling the NSF/SSO—MPLS VPN feature, you must have a supported MPLS VPN network configuration. Configuration information is included in the “Part 4: MPLS Virtual Private Networks” module in the *Cisco IOS Multiprotocol Label Switching Configuration Guide*, Release 12.4.

Restrictions for NSF/SSO—MPLS VPN

The NSF/SSO—MPLS VPN feature has the following restrictions:

- Tag Distribution Protocol (TDP) sessions are not supported. Only LDP sessions are supported.
- The NSF/SSO—MPLS VPN feature requires that neighbor networking devices be NSF-aware. Peer routers must support the graceful restart of the protocol used to communicate with the NSF/SSO—MPLS VPN-capable router.

- The NSF/SSO—MPLS VPN feature cannot be configured on label-controlled ATM (LC-ATM) interfaces.

Information About NSF/SSO—MPLS VPN

To configure NSF/SSO—MPLS VPN, you need to understand the following concepts:

- Elements That Enable NSF/SSO—MPLS VPN to Work, page 3
- How VPN Prefix Information Is Checkpointed to the Backup Route Processor, page 3
- How BGP Graceful Restart Preserves Prefix Information During a Restart, page 4
- What Happens If a Router Does Not Have NSF/SSO—MPLS VPN Enabled, page 4

Elements That Enable NSF/SSO—MPLS VPN to Work

VPN NSF requires several elements to work:

- VPN NSF uses the BGP Graceful Restart mechanisms defined in the Graceful Restart Internet Engineering Task Force (IETF) specifications and in the *Cisco Nonstop Forwarding* feature module. BGP Graceful Restart allows a router to create MPLS forwarding entries for VPNv4 prefixes in NSF mode. The forwarding entries are preserved during a restart. BGP also saves prefix and corresponding label information and recovers the information after a restart.
- The NSF/SSO—MPLS VPN feature also uses NSF for the label distribution protocol in the core network (either MPLS Label Distribution Protocol, traffic engineering, or static labeling).
- The NSF/SSO—MPLS VPN feature uses NSF for the Interior Gateway Protocol (IGP) used in the core (OSPF or IS-IS).
- The NSF/SSO—MPLS VPN feature uses NSF for the routing protocols between the PE and customer CE routers.

How VPN Prefix Information Is Checkpointed to the Backup Route Processor

When BGP allocates local labels for prefixes, it checkpoints the local label binding in the backup Route Processor. The checkpointing function copies state information from the active Route Processor to the backup Route Processor, thereby ensuring that the backup Route Processor has an identical copy of the latest information. If the active Route Processor fails, the backup Route Processor can take over with no interruption in service. Checkpointing begins when the active Route Processor does a bulk synchronization, which copies all of the local label bindings to the backup Route Processor. After that, the active Route Processor dynamically checkpoints individual prefix label bindings when a label is allocated or freed. This allows forwarding of labeled packets to continue before BGP reconverges.

How BGP Graceful Restart Preserves Prefix Information During a Restart

When a router that is capable of BGP Graceful Restart loses connectivity, the following happens to the restarting router:

1. The router establishes BGP sessions with other routers and relearns the BGP routes from other routers that are also capable of Graceful Restart. The restarting router waits to receive updates from the neighboring routers. When the neighboring routers send end-of-Routing Information Base (RIB) markers to indicate that they are done sending updates, the restarting router starts sending its own updates.
2. The restarting router accesses the checkpoint database to find the label that was assigned for each prefix. If it finds the label, it advertises it to the neighboring router. If it does not find the label, it allocates a new label and advertises it.
3. The restarting router removes any stale prefixes after a timer for stale entries expires.

When a peer router that is capable of BGP Graceful Restart encounters a restarting router, it does the following:

1. The peer router sends all of the routing updates to the restarting router. When it has finished sending updates, the peer router sends an end-of RIB marker to the restarting router.
2. The peer router does not immediately remove the BGP routes learned from the restarting router from its BGP routing table. As it learns the prefixes from the restarting router, the peer refreshes the stale routes if the new prefix and label information matches the old information.

What Happens If a Router Does Not Have NSF/SSO—MPLS VPN Enabled

If a router is not configured for the NSF/SSO—MPLS VPN feature and it attempts to establish a BGP session with a router that is configured with the NSF/SSO—MPLS VPN feature, the two routers create a normal BGP session but do not have the ability to perform the NSF/SSO—MPLS VPN feature.

How to Configure NSF/SSO—MPLS VPN

This section contains the following procedures:

- Configuring NSF Support for Basic VPNs, page 4 (required)
- Configuring NSF Support for MPLS VPN Interfaces That Use BGP as the Label Distribution Protocol, page 6 (required)
- Verifying the NSF/SSO—MPLS VPN Configuration, page 7 (optional)

Configuring NSF Support for Basic VPNs

Perform this task to configure NSF support for basic VPNs.

Prerequisites

Route Processors must be configured for SSO. See the *Stateful Switchover* feature module for more information.

If you use LDP in the core or in the virtual routing and forwarding (VRF) instances for MPLS VPN Carrier Supporting Carrier configurations, you must enable the MPLS LDP: NSF/SSO Support and Graceful Restart feature. See the *NSF/SSO-MPLS LDP and MPLS LDP Graceful Restart* feature module for more information.

You must enable Nonstop Forwarding on the routing protocols running between the P, PE, and CE routers. The routing protocols are OSPF, IS-IS, and BGP. See the *Cisco Nonstop Forwarding* feature module for more information.

Before enabling the NSF/SSO—MPLS VPN feature, you must have a supported MPLS VPN network configuration. Configuration information is included in the "Part 4: MPLS Virtual Private Networks" module in the *Cisco IOS Multiprotocol Label Switching Configuration Guide*, Release 12.4, at the following URL:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef** [**distributed**]
4. **router bgp** *as-number*
5. **bgp graceful-restart restart-time** *secs*
6. **bgp graceful-restart stalepath-time** *secs*
7. **bgp graceful-restart**
8. **end**

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 cef** [**distributed**] **Example:** `Router(config)# ip cef distributed`	Enables Cisco Express Forwarding • Use this command if Cisco Express Forwarding is not enabled by default on the router.

	Command or Action	Purpose
Step 4	**router bgp** *as-number* **Example:** `Router(config)# router bgp 1`	Configures a BGP routing process and enters router configuration mode. • The *as-number* argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.
Step 5	**bgp graceful-restart restart-time** *secs* **Example:** `Router(config-router)# bgp graceful-restart restart-time 200`	(Optional) Specifies the maximum time to wait for a graceful-restart-capable neighbor to come back up after a restart. The default is 120 seconds. The valid range is from 1 to 3600 seconds.
Step 6	**bgp graceful-restart stalepath-time** *secs* **Example:** `Router(config-router)# bgp graceful-restart stalepath-time 400`	(Optional) Specifies the maximum time to hold on to the stale paths of a gracefully restarted peer. All stale paths are deleted after the expiration of this timer. The default is 360 seconds. The valid range is from 1 to 3600 seconds.
Step 7	**bgp graceful-restart** **Example:** `Router(config-router)# bgp graceful-restart`	Enables BGP Graceful Restart on the router. See *Cisco Nonstop Forwarding* for more information about the **bgp graceful-restart** command.
Step 8	**end** **Example:** `Router(config-router)# end`	(Optional) Exits to privileged EXEC mode.

Configuring NSF Support for MPLS VPN Interfaces That Use BGP as the Label Distribution Protocol

The following VPN features require special configuration for the NSF/SSO—MPLS VPN feature:

- MPLS VPN—Carrier Supporting Carrier—IPv4 BGP Label Distribution
- MPLS VPN—Inter-AS—IPv4 BGP Label Distribution

You must issue an extra command, **mpls forwarding bgp**, on the interfaces that use BGP to distribute MPLS labels and routes. Use the following procedure to configure the NSF/SSO—MPLS VPN feature in these MPLS VPNs.

Prerequisites

- Make sure your MPLS VPN is configured for Carrier Supporting Carrier (CSC) or Inter-AS with BGP as the label distribution protocol.
- Configure NSF/SSO—MPLS VPN first, as described in "Configuring NSF Support for Basic VPNs" section on page 4.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef** [**distributed**]
4. **interface** *slot/port*
5. **mpls forwarding bgp**

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 cef** [**distributed**] **Example:** `Router(config)# ip cef distributed`	Enables Cisco Express Forwarding. • Use this command if Cisco Express Forwarding is not enabled by default on the router.
Step 4	**interface** *slot/port* **Example:** `Router(config)# interface POS1/0/0`	Defines the interface and enters interface configuration mode.
Step 5	**mpls forwarding bgp** **Example:** `Router(config-if)# mpls forwarding bgp`	Enables the interface to exchange BGP labels. You need to issue this command on any interface configured to use BGP to forward MPLS labels and routes.

Verifying the NSF/SSO—MPLS VPN Configuration

This section explains how to verify a configuratin that has the the NSF/SSO—MPLS VPN feature.

- See the *Cisco Nonstop Forwarding* feature module for verification procedures for BGP, OSPF, and IS-IS.
- See the *NSF/SSO-MPLS LDP and MPLS LDP Graceful Restart* feature module for verification procedures for the MPLS LDP: NSF/SSO feature
- See the verification information included in the “Part 4: MPLS Virtual Private Networks” module in the *Cisco IOS Multiprotocol Label Switching Configuration Guide*, Release 12.4

SUMMARY STEPS

1. **show ip bgp vpnv4 all labels**
2. **show ip bgp vpnv4 all neighbors**
3. **show ip bgp labels**
4. **show ip bgp neighbors**

DETAILED STEPS

Step 1 show ip bgp vpnv4 all labels

This command displays incoming and outgoing BGP labels for each route distinguisher. The following is sample output from the command:

```
Router# show ip bgp vpnv4 all labels

Network          Next Hop      In label/Out label
Route Distinguisher: 100:1 (vpn1)
   10.3.0.0/16      10.0.0.5        25/20
                    10.0.0.1        25/23
                    10.0.0.2        25/imp-null
   10.0.0.9/32      10.0.0.1        24/22
                    10.0.0.2        24/imp-null
```

Step 2 show ip bgp vpnv4 all neighbors

This command displays whether the BGP peers are capable of Graceful Restart. The following is sample output from the command:

```
Router# show ip bgp vpnv4 all neighbors

BGP neighbor is 10.0.0.1,  remote AS 100, internal link
  BGP version 4, remote router ID 10.0.0.1
  BGP state = Established, up for 02:49:47
  Last read 00:00:47, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family VPNv4 Unicast: advertised and received
    Graceful Restart Capabilty: advertised and received
      Remote Restart timer is 120 seconds
      Address families preserved by peer:
        VPNv4 Unicast
        .
        .
        .
```

Step 3 show ip bgp labels

This command displays information about MPLS labels in the Exterior Border Gateway Protocol (EBGP) route table. The following is sample output from the command:

```
Router# show ip bgp labels

   Network          Next Hop      In label/Out label
   10.3.0.0/16      10.0.0.1        imp-null/imp-null
                    0.0.0.0         imp-null/nolabel
   10.0.0.9/32      10.0.0.1        21/29
   10.0.0.11/32     10.0.0.1        24/38
   10.0.0.13/32     0.0.0.0         imp-null/nolabel
   10.0.0.15/32     10.0.0.1        29/nolabel
                    10.0.0.1        29/21
```

Step 4 **show ip bgp neighbors**

This command displays whether the BGP peers are capable of Graceful Restart. The following is sample output from the command:

```
Router# show ip bgp neighbors

BGP neighbor is 10.0.0.1,  remote AS 100, external link
  BGP version 4, remote router ID 10.0.0.5
  BGP state = Established, up for 02:54:19
  Last read 00:00:18, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
    ipv4 MPLS Label capability: advertised and received
    Graceful Restart Capabilty: advertised and received
      Remote Restart timer is 120 seconds
      Address families preserved by peer:
        IPv4 Unicast
       .
       .
       .
```

Configuration Examples for NSF/SSO—MPLS VPN

This section includes six configuration examples. The first configuration example shows the most simple configuration, a basic VPN configuration. The second, third, and fourth examples show different CSC VPN configurations. The fourth example hows a CSC VPN configuration that uses BGP as the MPLS label distribution method and therefore requires the **mpls forwarding bgp** command. The last two examples show Inter-AS configurations.

- NSF/SSO—MPLS VPN for a Basic MPLS VPN: Example, page 9
- NSF/SSO—MPLS VPN for a CSC Network with a Customer Carrier Who Is an ISP: Example, page 13
- NSF/SSO—MPLS VPN for a CSC Network with a Customer Who Is an MPLS VPN Provider: Example, page 18
- NSF/SSO—MPLS VPN for a CSC Network That Uses BGP to Distribute MPLS Labels: Example, page 27
- NSF/SSO—MPLS VPN for an Inter-AS Network Using BGP to Distribute Routes and MPLS Labels: Example, page 35
- NSF/SSO—MPLS VPN for an Inter-AS Network That Uses BGP to Distribute Routes and MPLS Labels over a Non-MPLS VPN Service Provider: Example, page 40

NSF/SSO—MPLS VPN for a Basic MPLS VPN: Example

In this example, the NSF/SSO—MPLS VPN feature is enabled on the existing MPLS VPN configuration.

Enabling SSO on a Cisco 7500 Series Router

The following commands are used to enable SSO on the Cisco 7500 series routers:

- **hw-module slot**

- **redundancy**
- **mode sso**

The configuration examples are the same for both platforms with the exception that the following configuration boot commands are seen in the beginning of a Cisco 7500 series router configuration (and not in a Cisco 10000 series router configuration):

```
boot system slot0:rsp-pv-mz
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz
```

Enabling SSO on a Cisco 10000 Series Router

The SSO mode is enabled by default.

Enabling NSF on Both the Cisco 7500 Series and Cisco 10000 Series Routers

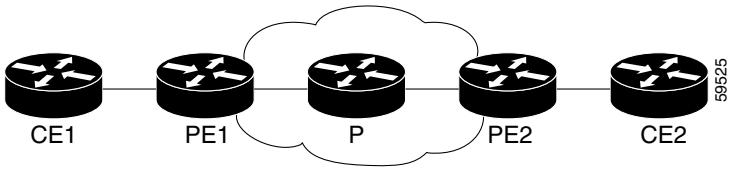
The following commands are used to enable NSF for the routing protocols, such as BGP and OSPF, and for the label distribution protocols, such as BGP and LDP:

- **bgp graceful-restart restart-time**
- **bgp graceful-restart stalepath-time**
- **bgp graceful-restart**
- **nsf enforce global**

Note In the configuration example, the NSF/SSO commands are bold-faced and any platform-specific commands are highlighted by arrows.

Figure 1 shows the configuration of the NSF/SSO—MPLS VPN feature on the PE and CE routers.

Figure 1 MPLS VPN Configuration with MPLS VPN: NSF/SSO



Note LDP is the default MPLS label protocol.

The following configuration examples show the configuration of the NSF/SSO—MPLS VPN feature on the CE and PE routers.

CE1 Router

```
ip cef
no ip domain-lookup
!
interface Loopback0
 ip address 10.10.10.10 255.255.255.255
!
interface Ethernet4
 ip address 10.0.0.1 255.0.0.0
 media-type 10BaseT
```

```
!
router ospf 100
 redistribute bgp 101
 nsf enforce global
 passive-interface Ethernet4
 network 10.0.0.0 0.255.255.255 area 100
!
router bgp 101
 no synchronization
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart network 10.0.0.0
 network 10.0.0.0
 neighbor 10.0.0.2 remote-as 100
```

PE1 Router

```
redundancy
    mode sso
!
ip cef distributed
mpls ldp graceful-restart
mpls label protocol ldp

ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
no mpls aggregate-statistics
!
interface Loopback0
 ip address 10.12.12.12 255.255.255.255
!
interface Ethernet1/4    =====> interface FastEthernet1/1/4 on a Cisco 10000 series router
 ip vrf forwarding vpn1
 ip address 10.0.0.2 255.0.0.0
 !
 mpls ip

interface ATM3/0              =====> interface ATM3/0/0 on a Cisco 10000 series router
 no ip address
!
interface ATM3/0.1 point-to-point ==> interface ATM3/0/0.1 point-to-point on a Cisco 10000
 ip unnumbered Loopback0
 mpls ip
!
router ospf 100
 passive-interface Ethernet1/4   ===> passive-interface FastEthernet1/1/4 on a Cisco 10000
 nsf enforce global
 network 10.0.0.0 0.255.255.255 area 100
!
router bgp 100
 no synchronization
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart

 no bgp default ipv4-unicast
 neighbor 10.14.14.14 remote-as 100
 neighbor 10.14.14.14 update-source Loopback0
!
 address-family ipv4 vrf vpn1
```

```
 neighbor 10.0.0.1 remote-as 101
 neighbor 10.0.0.1 activate
 exit-address-family
!
 address-family vpnv4
 neighbor 10.14.14.14 activate
 neighbor 10.14.14.14 send-community extended
 exit-address-family
```

PE2 Router

```
redundancy
    mode sso
!
ip cef distributed
mpls ldp graceful-restart
mpls label protocol ldp
!
ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
no mpls aggregate-statistics
!
!
interface Loopback0
 ip address 10.14.14.14 255.255.255.255
!
interface ATM1/0              =====> interface ATM1/0/0 on a Cisco 10000 series router
 no ip address
!
interface ATM1/0.1 point-to-point ==> interface ATM1/0/0.1 point-to-point on a Cisco 10000
 ip unnumbered Loopback0
 mpls ip
!
interface FastEthernet3/0/0
 ip vrf forwarding vpn1
 ip address 10.0.0.1 255.0.0.0
 ip route-cache distributed
 mpls ip
!
router ospf 100
 nsf enforce global
 passive-interface FastEthernet3/0/0
 network 10.0.0.0 0.255.255.255 area 100
!
router bgp 100
 no synchronization
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 no bgp default ipv4-unicast
 neighbor 10.12.12.12 remote-as 100
 neighbor 10.12.12.12 update-source Loopback0
!
address-family ipv4 vrf vpn1
 neighbor 10.0.0.2 remote-as 102
 neighbor 10.0.0.2 activate
 exit-address-family
!
address-family vpnv4
```

```
 neighbor 10.12.12.12 activate
 neighbor 10.12.12.12 send-community extended
 exit-address-family
```

CE2 Router

```
ip cef
!
interface Loopback0
 ip address 10.13.13.13 255.255.255.255
!
interface FastEthernet0
 ip address 10.0.0.2 255.0.0.0
 no ip mroute-cache
!
router ospf 100
 redistribute bgp 102
 nsf enforce global
 passive-interface FastEthernet0
 network 10.0.0.0 0.255.255.255 area 100
!
router bgp 102
 no synchronization
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart

 network 10.0.0.0
 network 10.0.0.0
 neighbor 10.0.0.1 remote-as 100
```

NSF/SSO—MPLS VPN for a CSC Network with a Customer Carrier Who Is an ISP: Example

In this example, MPLS VPN SSO and NSF are configured on the existing MPLS CSC VPN configuration. In the CSC network configuration, the customer carrier is an Internet Service Provider (ISP), as shown in Figure 2.

Enabling SSO on a Cisco 7500 Series Router

The following commands are used to enable SSO on the Cisco 7500 series routers:

- **hw-module slot**
- **redundancy**
- **mode sso**

The configuration examples are the same for both platforms with the exception that the following configuration boot commands are seen in the beginning of a Cisco 7500 series router configuration (and not in a Cisco 10000 series router configuration):

```
boot system slot0:rsp-pv-mz
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz
```

Enabling SSO on a Cisco 10000 Series Router

The SSO mode is enabled by default.

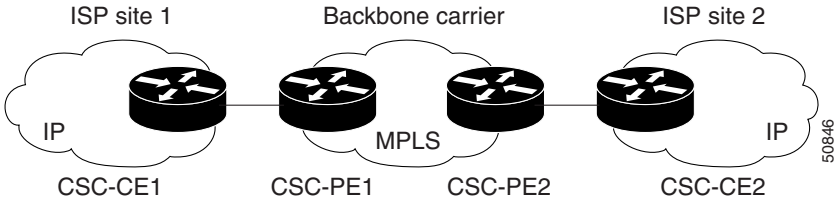
Enabling NSF on Both the Cisco 7500 Series and Cisco 10000 Series Routers

The following commands are used to enable NSF for the routing protocols, such as BGP and OSPF, and for the label distribution protocols, such as BGP and LDP:

- **bgp graceful-restart restart-time**
- **bgp graceful-restart stalepath-time**
- **bgp graceful-restart**
- **nsf enforce global**

Note In the configuration example, the NSF/SSO commands are bold-faced and any platform-specific commands are highlighted by arrows.

Figure 2 MPLS VPN CSC Configuration with MPLS VPN: NSF and SSO



CSC-CE1 Configuration

```
mpls ldp graceful-restart
mpls label protocol ldp
!
interface Loopback0
ip address 10.14.14.14 255.255.255.255
!
no ip route-cache
no ip mroute-cache
!
interface ATM1/0
no ip address
!
interface ATM1/0.1 point-to-point
ip address 10.0.0.2 255.0.0.0
!
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
interface ATM2/0
no ip address
!
interface ATM2/0.1 point-to-point
ip address 10.0.0.2 255.0.0.0
!
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
```

```
!
router ospf 200
log-adjacency-changes
redistribute connected subnets
 nsf enforce global
network 10.14.14.14 0.0.0.0 area 200
network 10.0.0.0 0.255.255.255 area 200
network 10.0.0.0 0.255.255.255 area 200
```

CSC-PE1 Configuration

```
redundancy
    mode sso
ip cef distributed
mpls ldp graceful-restart
mpls label protocol ldp

!
ip vrf vpn1
rd 100:0
route-target export 100:0
route-target import 100:0
no mpls aggregate-statistics
!
interface Loopback0
ip address 10.11.11.11 255.255.255.255
!
no ip route-cache
no ip mroute-cache
!
interface Loopback100
ip vrf forwarding vpn1
ip address 10.19.19.19 255.255.255.255
!
interface ATM1/1/0
no ip address
!
interface ATM1/1/0.1 point-to-point
ip address 10.0.0.1 255.0.0.0
!
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
interface ATM3/0/0
no ip address
!
interface ATM3/0/0.1 point-to-point
ip vrf forwarding vpn1
ip address 10.0.0.1 255.0.0.0
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
router ospf 100
log-adjacency-changes
nsf enforce global
passive-interface ATM3/0/0.1
passive-interface Loopback100
network 10.11.11.11 0.0.0.0 area 100
```

```
network 10.0.0.0 0.255.255.255 area 100
!
router ospf 200 vrf vpn1
log-adjacency-changes
nsf enforce global
redistribute bgp 100 metric-type 1 subnets
network 10.19.19.19 0.0.0.0 area 200
network 10.0.0.0 0.255.255.255 area 200
!
router bgp 100
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart

timers bgp 10 30
neighbor 10.12.12.12 remote-as 100
neighbor 10.12.12.12 update-source Loopback0
!
address-family ipv4
neighbor 10.12.12.12 activate
neighbor 10.12.12.12 send-community extended
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 10.12.12.12 activate
neighbor 10.12.12.12 send-community extended
exit-address-family
!
address-family ipv4 vrf vpn1
redistribute ospf 200 match internal external 1 external 2
no auto-summary
no synchronization
exit-address-family
```

CSC-PE2 Configuration

```
redundancy
    mode sso
ip cef distributed
!
ip vrf vpn1
rd 100:0
route-target export 100:0
route-target import 100:0
mpls ldp graceful-restart
mpls label protocol ldp
no mpls aggregate-statistics
!
interface Loopback0
ip address 10.12.12.12 255.255.255.255
no ip route-cache
no ip mroute-cache
!
interface Loopback100
ip vrf forwarding vpn1
ip address 10.20.20.20 255.255.255.255
!
interface ATM0/1/0
no ip address
!
```

```
interface ATM0/1/0.1 point-to-point
ip address 10.0.0.2 255.0.0.0
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
interface ATM3/0/0
no ip address
!
interface ATM3/0/0.1 point-to-point
ip vrf forwarding vpn1
ip address 10.0.0.1 255.0.0.0
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
router ospf 100
log-adjacency-changes
nsf enforce global
passive-interface ATM3/0/0.1
passive-interface Loopback100
network 10.12.12.12 0.0.0.0 area 100
network 10.0.0.0 0.255.255.255 area 100
!
router ospf 200 vrf vpn1
log-adjacency-changes
nsf enforce global
redistribute bgp 100 metric-type 1 subnets
network 10.20.20.20 0.0.0.0 area 200
network 10.0.0.0 0.255.255.255 area 200
!
router bgp 100
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor 10.11.11.11 remote-as 100
neighbor 10.11.11.11 update-source Loopback0
!
address-family ipv4
neighbor 10.11.11.11 activate
neighbor 10.11.11.11 send-community extended
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 10.11.11.11 activate
neighbor 10.11.11.11 send-community extended
exit-address-family
!
address-family ipv4 vrf vpn1
redistribute ospf 200 match internal external 1 external 2
no auto-summary
no synchronization
exit-address-family
```

CSC-CE2 Configuration

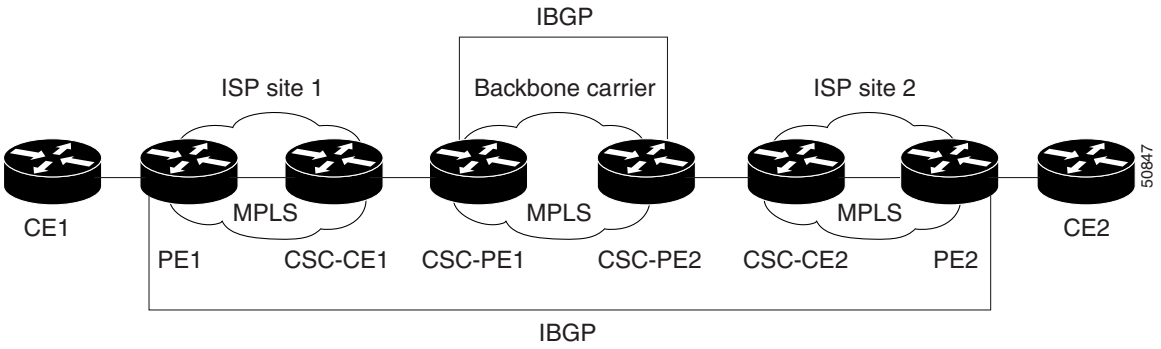
```
ip cef
```

```
!
mpls label protocol ldp
mpls ldp graceful-restart
!
interface Loopback0
ip address 10.16.16.16 255.255.255.255
no ip route-cache
no ip mroute-cache
!
interface ATM1/0
no ip address
!
interface ATM1/0.1 point-to-point
ip address 10.0.0.2 255.0.0.0
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
interface ATM5/0
no ip address
!
interface ATM5/0.1 point-to-point
ip address 10.0.0.2 255.0.0.0
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
router ospf 200
log-adjacency-changes
nsf enforce global
redistribute connected subnets
network 10.16.16.16 0.0.0.0 area 200
network 10.0.0.0 0.255.255.255 area 200
network 10.0.0.0 0.255.255.255 area 200
```

NSF/SSO—MPLS VPN for a CSC Network with a Customer Who Is an MPLS VPN Provider: Example

In the CSC network configuration shown in Figure 3, the customer carrier is an MPLS VPN provider. The customer carrier has two sites. The backbone carrier and the customer carrier use MPLS. The internal BGP (iBGP) sessions exchange the external routing information of the ISP.

Figure 3 MPLS VPN CSC Configuration 2 with MPLS VPN: NSF and SSO



The following configuration example shows the configuration of each router in the CSC network. OSPF is the protocol used to connect the customer carrier to the backbone carrier. The NSF/SSO—MPLS VPN feature is enabled on the existing MPLS VPN configuration.

Enabling SSO on a Cisco 7500 Series Router

The following commands are used to enable SSO on the routers:

- **hw-module slot**
- **redundancy**
- **mode sso**

The configuration examples are the same for both platforms with the exception that the following configuration boot commands are seen in the beginning of a Cisco 7500 series router configuration (and not in a Cisco 10000 series router configuration):

```
boot system slot0:rsp-pv-mz
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz
```

Enabling SSO on a Cisco 10000 Series Router

The SSO mode is enabled by default.

Enabling NSF on Both the Cisco 7500 Series and Cisco 10000 Series Routers

The following commands are used to enable NSF for the routing protocols, such as BGP and OSPF, and for the label distribution protocols, such as BGP and LDP:

- **bgp graceful-restart restart-time**
- **bgp graceful-restart stalepath-time**
- **bgp graceful-restart**
- **nsf enforce global**

Note In the configuration examples, the NSF/SSO commands are bold-faced and any platform-specific commands are highlighted with arrows.

CE1 Configuration

```
ip cef
!
interface Loopback0
ip address 10.17.17.17 255.255.255.255
!
interface Ethernet0/1
ip address 10.0.0.2 255.0.0.0
!
router ospf 300
log-adjacency-changes
nsf enforce global
redistribute bgp 300 subnets
passive-interface Ethernet0/1
network 10.17.17.17 0.0.0.0 area 300
!
router bgp 300
no synchronization
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
redistribute connected
redistribute ospf 300 match internal external 1 external 2
neighbor 10.0.0.1 remote-as 200
neighbor 10.0.0.1 advertisement-interval 5
no auto-summary
```

PE1 Configuration

```
redundancy
    mode sso
ip cef distributed
mpls ldp graceful-restart
mpls label protocol ldp
!
ip vrf vpn2
rd 200:1
route-target export 200:1
route-target import 200:1
!
interface Loopback0
ip address 10.13.13.13 255.255.255.255
!
interface ATM1/0              =====> interface ATM1/0/0 on a Cisco 10000 series router
no ip address
!
interface ATM1/0.1 point-to-point  ===> interface ATM1/0/0 point-to-point on a Cisco 10000
ip address 10.0.0.1 255.0.0.0
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
interface Ethernet3/0    =====> interface FastEthernet3/0/0 on a Cisco 10000 series router
ip vrf forwarding vpn2
ip address 10.0.0.1 255.0.0.0
no ip mroute-cache
!
router ospf 200
```

```
log-adjacency-changes
redistribute connected subnets
nsf enforce global
passive-interface Ethernet3/0    ===> passive-interface FastEthernet3/0/0 on a Cisco 10000

network 10.13.13.13 0.0.0.0 area 200
network 10.0.0.0 0.255.255.255 area 200
!
router bgp 200
no bgp default ipv4-unicast
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor 10.15.15.15 remote-as 200
neighbor 10.15.15.15 update-source Loopback0
!
address-family ipv4
neighbor 10.15.15.15 activate
neighbor 10.15.15.15 send-community extended
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 10.15.15.15 activate
neighbor 10.15.15.15 send-community extended
exit-address-family
!
address-family ipv4 vrf vpn2
neighbor 10.0.0.2 remote-as 300
neighbor 10.0.0.2 activate
neighbor 10.0.0.2 as-override
neighbor 10.0.0.2 advertisement-interval 5
no auto-summary
no synchronization
exit-address-family
```

CSC-CE1 Configuration

```
mpls label protocol ldp
mpls ldp graceful-restart
!
interface Loopback0
ip address 10.14.14.14 255.255.255.255
no ip route-cache
no ip mroute-cache
!
interface ATM1/0
no ip address
!
interface ATM1/0.1 point-to-point
ip address 10.0.0.2 255.0.0.0
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
interface ATM2/0
no ip address
!
```

```
interface ATM2/0.1 point-to-point
ip address 10.0.0.2 255.0.0.0
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
router ospf 200
log-adjacency-changes
redistribute connected subnets
nsf enforce global
network 10.14.14.14 0.0.0.0 area 200
network 10.0.0.0 0.255.255.255 area 200
network 10.0.0.0 0.255.255.255 area 200
```

CSC-PE1 Configuration

```
redundancy
    mode sso
ip cef distributed
!
ip vrf vpn1
rd 100:0
route-target export 100:0
route-target import 100:0
mpls label protocol ldp
mpls ldp graceful-restart
no mpls aggregate-statistics
!
interface Loopback0
ip address 10.11.11.11 255.255.255.255
no ip route-cache
no ip mroute-cache
!
interface Loopback100
ip vrf forwarding vpn1
ip address 10.19.19.19 255.255.255.255
!
interface ATM1/1/0
no ip address
!
interface ATM1/1/0.1 point-to-point
ip address 10.0.0.1 255.0.0.0
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
interface ATM3/0/0
no ip address
!
interface ATM3/0/0.1 point-to-point
ip vrf forwarding vpn1
ip address 10.0.0.1 255.0.0.0
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
router ospf 100
log-adjacency-changes
passive-interface ATM3/0/0.1
```

```
nsf enforce global
passive-interface Loopback100
network 10.11.11.11 0.0.0.0 area 100
network 10.0.0.0 0.255.255.255 area 100
!
router ospf 200 vrf vpn1
log-adjacency-changes
nsf enforce global
redistribute bgp 100 metric-type 1 subnets
network 10.19.19.19 0.0.0.0 area 200
network 10.0.0.0 0.255.255.255 area 200
!
router bgp 100
bgp log-neighbor-changes
timers bgp 10 30
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
neighbor 10.12.12.12 remote-as 100
neighbor 10.12.12.12 update-source Loopback0
!
address-family ipv4
neighbor 10.12.12.12 activate
neighbor 10.12.12.12 send-community extended
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 10.12.12.12 activate
neighbor 10.12.12.12 send-community extended
exit-address-family
!
address-family ipv4 vrf vpn1
redistribute ospf 200 match internal external 1 external 2
no auto-summary
no synchronization
exit-address-family
```

CSC-PE2 Configuration

```
redundancy
   mode sso
ip cef distributed
!
ip vrf vpn1
rd 100:0
route-target export 100:0
route-target import 100:0
mpls label protocol ldp
mpls ldp graceful-restart
no mpls aggregate-statistics
!
interface Loopback0
ip address 10.12.12.12 255.255.255.255
no ip route-cache
no ip mroute-cache
!
interface Loopback100
ip vrf forwarding vpn1
ip address 10.20.20.20 255.255.255.255
!
interface ATM0/1/0
```

```
no ip address
!
interface ATM0/1/0.1 point-to-point
ip address 10.0.0.2 255.0.0.0
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
interface ATM3/0/0
no ip address
!
interface ATM3/0/0.1 point-to-point
ip vrf forwarding vpn1
ip address 10.0.0.1 255.0.0.0
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
router ospf 100
log-adjacency-changes
nsf enforce global
passive-interface ATM3/0/0.1
passive-interface Loopback100
network 10.12.12.12 0.0.0.0 area 100
network 10.0.0.0 0.255.255.255 area 100
!
router ospf 200 vrf vpn1
log-adjacency-changes
nsf enforce global
redistribute bgp 100 metric-type 1 subnets
network 10.20.20.20 0.0.0.0 area 200
network 10.0.0.0 0.255.255.255 area 200
!
router bgp 100
bgp log-neighbor-changes
timers bgp 10 30
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
neighbor 10.11.11.11 remote-as 100
neighbor 10.11.11.11 update-source Loopback0
!
address-family ipv4
neighbor 10.11.11.11 activate
neighbor 10.11.11.11 send-community extended
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 10.11.11.11 activate
neighbor 10.11.11.11 send-community extended
exit-address-family
!
address-family ipv4 vrf vpn1
redistribute ospf 200 match internal external 1 external 2
no auto-summary
no synchronization
exit-address-family
```

CSC-CE2 Configuration

```
ip cef
!
mpls ldp graceful-restart
mpls label protocol ldp
!
interface Loopback0
ip address 10.16.16.16 255.255.255.255
no ip route-cache
no ip mroute-cache
!
interface ATM1/0
no ip address
!
interface ATM1/0.1 point-to-point
ip address 10.0.0.2 255.0.0.0
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
interface ATM5/0
no ip address
!
interface ATM5/0.1 point-to-point
ip address 10.0.0.2 255.0.0.0
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
router ospf 200
log-adjacency-changes
redistribute connected subnets
nsf enforce global
network 10.16.16.16 0.0.0.0 area 200
network 10.0.0.0 0.255.255.255 area 200
network 10.0.0.0 0.255.255.255 area 200
```

PE2 Configuration

```
redundancy
    mode sso
ip cef distributed
ip cef accounting non-recursive
!
ip vrf vpn2
rd 200:1
route-target export 200:1
route-target import 200:1
mpls ldp graceful-restart
mpls label protocol ldp
!
interface Loopback0
ip address 10.15.15.15 255.255.255.255
!
interface Ethernet3/0    =====> interface FastEthernet3/0/0 on a Cisco 10000 series router
ip vrf forwarding vpn2
ip address 10.0.0.1 255.0.0.0
!
interface ATM5/0            =====> interface ATM5/0/0 on a Cisco 10000 series router
```

```
no ip address
!
interface ATM5/0.1 point-to-point ==> interface ATM5/0/0.1 point-to-point on a Cisco 10000
ip address 10.0.0.1 255.0.0.0
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
router ospf 200
log-adjacency-changes
redistribute connected subnets
nsf enforce global
passive-interface Ethernet3/0   ===> passive-interface FastEthernet3/0/0 on a Cisco 10000
network 10.15.15.15 0.0.0.0 area 200
network 10.0.0.0 0.255.255.255 area 200
!
router bgp 200
no bgp default ipv4-unicast
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor 10.13.13.13 remote-as 200
neighbor 10.13.13.13 update-source Loopback0
!
address-family ipv4
neighbor 10.13.13.13 activate
neighbor 10.13.13.13 send-community extended
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 10.13.13.13 activate
neighbor 10.13.13.13 send-community extended
exit-address-family
!
address-family ipv4 vrf vpn2
neighbor 10.0.0.2 remote-as 300
neighbor 10.0.0.2 activate
neighbor 10.0.0.2 as-override
neighbor 10.0.0.2 advertisement-interval 5
no auto-summary
no synchronization
exit-address-family
```

CE2 Configuration

```
ip cef
!
interface Loopback0
ip address 10.18.18.18 255.255.255.255
!
interface Ethernet0/1
ip address 10.0.0.2 255.0.0.0
!
router ospf 300
log-adjacency-changes
nsf enforce global
redistribute bgp 300 subnets
passive-interface Ethernet0/1
```

```
network 10.18.18.18 0.0.0.0 area 300
!
router bgp 300
no synchronization
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
redistribute connected
redistribute ospf 300 match internal external 1 external 2
neighbor 10.0.0.1 remote-as 200
neighbor 10.0.0.1 advertisement-interval 5
no auto-summary
```

NSF/SSO—MPLS VPN for a CSC Network That Uses BGP to Distribute MPLS Labels: Example

In the following example and in Figure 4, the NSF/SSO—MPLS VPN feature is configured on an existing MPLS VPN.

Enabling SSO on a Cisco 7500 Series Router

The following commands are used to enable SSO on the routers:

- **hw-module slot**
- **redundancy**
- **mode sso**

The configuration examples are the same for both platforms with the exception that the following configuration boot commands are seen in the beginning of a Cisco 7500 series router configuration (and not in a Cisco 10000 series router configuration):

```
boot system slot0:rsp-pv-mz
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz
```

Enabling SSO on a Cisco 10000 Series Router

The SSO mode is enabled by default.

Enabling NSF on Both the Cisco 7500 Series and Cisco 10000 Series Routers

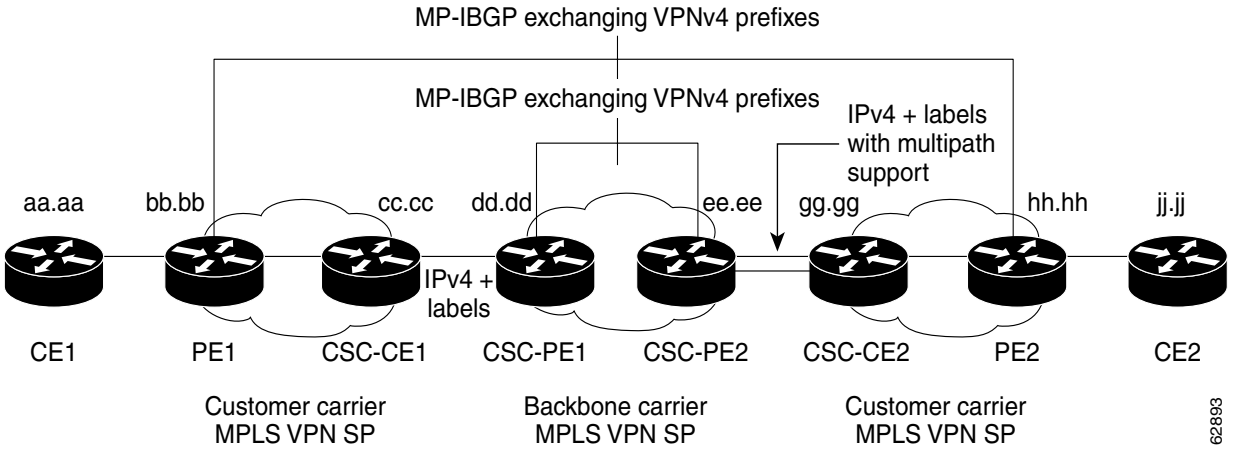
The following commands are used to enable NSF for the routing protocols, such as BGP and OSPF, and for the label distribution protocols, such as BGP and LDP:

- **bgp graceful-restart restart-time**
- **bgp graceful-restart stalepath-time**
- **bgp graceful-restart**
- **nsf enforce global**
- **mpls forwarding bgp**

Note In the configuration examples, the NSF/SSO commands are bold-faced and arrows highlight any platform-specific commands.

This section and Figure 4 provide an example of a backbone carrier and a customer carrier who are both BGP/MPLS VPN service providers. The example shows how BGP is enabled to distribute routes and MPLS labels between PE and CE routers.

Figure 4 MPLS VPN CSC Configuration 3 with MPLS VPN: NSF and SSO



In Figure 4, the subnet mask is 255.255.255.252.

The routers have the following characteristics:

- CE1 and CE2 belong to an end customer. CE1 and CE2 routers exchange routes learned from PE routers. The end customer is purchasing VPN services from a customer carrier.
- PE1 and PE2 are part of a customer carrier network that is configured to provide MPLS VPN services. PE1 and PE2 are peering with a VPNv4 IBGP session to form an MPLS VPN network.
- CSC-CE1 and CSC-CE2 are part of a customer carrier network. CSC-CE1 and CSC-CE2 routers exchange IPv4 BGP updates with MPLS labels and redistribute PE loopback addressees that are sent to and received from the IGP (OSPF in this example). The customer carrier is purchasing Carrier Supporting Carrier VPN services from a backbone carrier.
- CSC-PE1 and CSC-PE2 are part of the backbone carrier's network configured to provide Carrier Supporting Carrier VPN services. CSC-PE1 and CSC-PE2 peer with a VPNv4 IP BGP session to form the MPLS VPN network. In the VRF, CSC-PE1 and CSC-PE2 peer with the CSC-CE routers, which are configured to carry MPLS labels with the routes, within an IPv4 EBGP session.

CE1 Configuration

```
ip cef
interface Loopback0
ip address aa.aa.aa.aa 255.255.255.255
!
interface Ethernet3/3
ip address mm.0.0.1 255.0.0.0
!
router bgp 300
no synchronization
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
```

```
timers bgp 10 30
redistribute connected !Exchange routes
neighbor mm.0.0.2 remote-as 200 !learned from PE1.
neighbor mm.0.0.2 advertisement-interval 5
no auto-summary
```

PE1 Configuration

```
redundancy
   mode sso
ip cef distributed
!
ip vrf vpn2
rd 200:1
route-target export 200:1
route-target import 200:1
mpls ldp graceful-restart
mpls label protocol ldp
!
interface Loopback0
ip address bb.bb.bb.bb 255.255.255.255
!
interface Ethernet3/0    =====> interface FastEthernet3/0/0 on a Cisco 10000 series router
ip address nn.0.0.1 255.0.0.0
no ip mroute-cache
mpls label protocol ldp
mpls ip
!
interface Ethernet3/3    =====> interface FastEthernet3/0/3 on a Cisco 10000 series router
ip vrf forwarding vpn2
ip address mm.0.0.2 255.0.0.0
no ip mroute-cache
!
router ospf 200
log-adjacency-changes
auto-cost reference-bandwidth 1000
nsf enforce global
redistribute connected subnets
passive-interface Ethernet3/3   ===> passive-interface FastEthernet3/0/3 on a Cisco 10000
network bb.bb.bb.bb 0.0.0.0 area 200
network nn.0.0.0 0.255.255.255 area 200
!
router bgp 200
no bgp default ipv4-unicast
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor hh.hh.hh.hh remote-as 200
neighbor hh.hh.hh.hh update-source Loopback0
!
address-family vpnv4 !VPNv4 session with PE2.
neighbor hh.hh.hh.hh activate
neighbor hh.hh.hh.hh send-community extended
bgp dampening 30
exit-address-family
!
address-family ipv4 vrf vpn2
neighbor mm.0.0.1 remote-as 300
neighbor mm.0.0.1 activate
neighbor mm.0.0.1 as-override
```

```
neighbor mm.0.0.1 advertisement-interval 5
no auto-summary
no synchronization
bgp dampening 30
exit-address-family
```

CSC-CE1 Configuration

```
ip cef
!
mpls ldp graceful-restart
mpls label protocol ldp
!
interface Loopback0
ip address cc.cc.cc.cc 255.255.255.255
!
interface Ethernet3/0
ip address pp.0.0.1 255.0.0.0
mpls forwarding bgp
!
interface Ethernet4/0
ip address nn.0.0.2 255.0.0.0
no ip mroute-cache
mpls label protocol ldp
mpls ip
!
router ospf 200
log-adjacency-changes
auto-cost reference-bandwidth 1000
nsf enforce global
redistribute connected subnets !Exchange routes
redistribute bgp 200 metric 3 subnets !learned from PE1.
passive-interface ATM1/0
passive-interface Ethernet3/0
network cc.cc.cc.cc 0.0.0.0 area 200
network nn.0.0.0 0.255.255.255 area 200
!
router bgp 200
no bgp default ipv4-unicast
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor pp.0.0.2 remote-as 100
neighbor pp.0.0.2 update-source Ethernet3/0
no auto-summary
!
address-family ipv4
redistribute connected
redistribute ospf 200 metric 4 match internal
neighbor pp.0.0.2 activate
neighbor pp.0.0.2 send-label
no auto-summary
no synchronization
bgp dampening 30
exit-address-family
```

CSC-PE1 Configuration

```
redundancy
```

```
    mode sso
ip cef distributed
!
ip vrf vpn1
rd 100:1
route-target export 100:1
route-target import 100:1
mpls ldp graceful-restart
mpls label protocol ldp
!
interface Loopback0
    ip address dd.dd.dd.dd 255.255.255.255
!
interface Ethernet3/1    =====> interface FastEthernet3/0/1 on a Cisco 10000 series router
    ip vrf forwarding vpn1
    ip address pp.0.0.2 255.0.0.0
    mpls forwarding bgp
!
interface ATM0/1/0
    no ip address
!
interface ATM0/1/0.1 point-to-point
    ip unnumbered Loopback0
    no atm enable-ilmi-trap
    mpls label protocol ldp
    mpls ip
!
router ospf 100
    log-adjacency-changes
    auto-cost reference-bandwidth 1000
    nsf enforce global
    redistribute connected subnets
    passive-interface Ethernet3/1
    network dd.dd.dd.dd 0.0.0.0 area 100
!
router bgp 100
    no bgp default ipv4-unicast
    bgp log-neighbor-changes
    bgp graceful-restart restart-time 120
    bgp graceful-restart stalepath-time 360
    bgp graceful-restart
    timers bgp 10 30
    neighbor ee.ee.ee.ee remote-as 100
    neighbor ee.ee.ee.ee update-source Loopback0
!
address-family vpnv4 !VPNv4 session with CSC-PE2.
    neighbor ee.ee.ee.ee activate
    neighbor ee.ee.ee.ee send-community extended
    bgp dampening 30
    exit-address-family
!
address-family ipv4 vrf vpn1
    neighbor pp.0.0.1 remote-as 200
    neighbor pp.0.0.1 activate
    neighbor pp.0.0.1 as-override
    neighbor pp.0.0.1 advertisement-interval 5
    neighbor pp.0.0.1 send-label
    no auto-summary
    no synchronization
    bgp dampening 30
    exit-address-family
```

CSC-PE2 Configuration

```
redundancy
    mode sso
ip cef distributed
!
ip vrf vpn1
rd 100:1
route-target export 100:1
route-target import 100:1
mpls ldp graceful-restart
mpls label protocol ldp
!
interface Loopback0
    ip address ee.ee.ee.ee 255.255.255.255
!
interface Ethernet5/0    =====> interface FastEthernet5/0/0 on a Cisco 10000 series router
    ip vrf forwarding vpn1
    ip address ss.0.0.2 255.0.0.0
    mpls forwarding bgp
    no ip route-cache distributed
    clock source internal
!
interface ATM2/1/0
    no ip address
!
interface ATM2/1/0.1 point-to-point
    ip unnumbered Loopback0
    no atm enable-ilmi-trap
    mpls label protocol ldp
    mpls ip
!
router ospf 100
log-adjacency-changes
auto-cost reference-bandwidth 1000
nsf enforce global
redistribute connected subnets
passive-interface Ethernet5/0   ====> passive-interface FastEthernet5/0/0 on a Cisco 10000
passive-interface ATM3/0/0
network ee.ee.ee.ee 0.0.0.0 area 100
!
router bgp 100
no bgp default ipv4-unicast
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor dd.dd.dd.dd remote-as 100
neighbor dd.dd.dd.dd update-source Loopback0
!
address-family vpnv4 !VPNv4 session with CSC-PE1.
    neighbor dd.dd.dd.dd activate
    neighbor dd.dd.dd.dd send-community extended
    bgp dampening 30
    exit-address-family
!
address-family ipv4 vrf vpn1
    neighbor ss.0.0.1 remote-as 200
    neighbor ss.0.0.1 activate
    neighbor ss.0.0.1 as-override
    neighbor ss.0.0.1 advertisement-interval 5
    neighbor ss.0.0.1 send-label
```

```
    no auto-summary
    no synchronization
    bgp dampening 30
    exit-address-family
```

CSC-CE2 Configuration

```
ip cef
!
mpls ldp graceful-restart
mpls label protocol ldp
!
interface Loopback0
    ip address gg.gg.gg.gg 255.255.255.255
!
interface Ethernet2/2
    ip address ss.0.0.2 255.0.0.0
    no ip mroute-cache
    mpls forwarding bgp
!
interface ATM3/1/0.1 point-to-point
    ip address yy.0.0.1 255.0.0.0
    mpls label protocol ldp
    mpls ip
!
router ospf 200
log-adjacency-changes
auto-cost reference-bandwidth 1000
nsf enforce global
redistribute connected subnets !Exchange routes
redistribute bgp 200 metric 3 subnets !learned from PE2.
passive-interface ATM3/1/0.1
network gg.gg.gg.gg 0.0.0.0 area 200
network ss.0.0.0 0.255.255.255 area 200
!
router bgp 200
no bgp default ipv4-unicast
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor yy.0.0.2 remote-as 100
neighbor yy.0.0.2 update-source ATM3/1/0.1
no auto-summary
!
address-family ipv4
redistribute connected
redistribute ospf 200 metric 4 match internal
neighbor yy.0.0.2 activate
neighbor yy.0.0.2 send-label
no auto-summary
no synchronization
bgp dampening 30
exit-address-family
```

PE2 Configuration

```
redundancy
    mode sso
ip cef distributed
```

```
!
ip vrf vpn2
rd 200:1
route-target export 200:1
route-target import 200:1
!
mpls ldp graceful-restart
mpls label protocol ldp
!
interface Loopback0
    ip address hh.hh.hh.hh 255.255.255.255
!
interface Ethernet3/6    =====> interface FastEthernet3/0/6 on a Cisco 10000 series router
    ip vrf forwarding vpn2
    ip address tt.0.0.2 255.0.0.0
!
interface ATM5/0.1 point2point
    ip address qq.0.0.1 255.0.0.0
    no atm enable-ilmi-trap
    no ip mroute-cache
    mpls label protocol ldp
    mpls ip
!
router bgp 200
no bgp default ipv4-unicast
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor bb.bb.bb.bb remote-as 200
neighbor bb.bb.bb.bb update-source Loopback0
!
address-family vpnv4 !VPNv4 session with PE1.
    neighbor bb.bb.bb.bb activate
    neighbor bb.bb.bb.bb send-community extended
    bgp dampening 30
    exit-address-family
!
address-family ipv4 vrf vpn2
    neighbor tt.0.0.1 remote-as 300
    neighbor tt.0.0.1 activate
    neighbor tt.0.0.1 as-override
    neighbor tt.0.0.1 advertisement-interval 5
    no auto-summary
    no synchronization
    bgp dampening 30
    exit-address-family
```

CE2 Configuration

```
ip cef
!
interface Loopback0
    ip address jj.jj.jj.jj 255.255.255.255
!
interface Ethernet3/6
    ip address tt.0.0.1 255.0.0.0
!
router bgp 300
bgp graceful-restart restart-time 120
```

```
bgp graceful-restart stalepath-time 360
bgp graceful-restart
no synchronization
bgp log-neighbor-changes
timers bgp 10 30 !Exchange routes
redistribute connected !learned from PE2.
redistribute ospf 300 match internal external 1 external 2
neighbor tt.0.0.2 remote-as 200
neighbor tt.0.0.2 advertisement-interval 5
no auto-summary
```

NSF/SSO—MPLS VPN for an Inter-AS Network Using BGP to Distribute Routes and MPLS Labels: Example

In Figure 5 and in the following example, the NSF/SSO—MPLS VPN feature is configured on the existing MPLS VPN Inter-AS configuration.

Enabling SSO on a Cisco 7500 Series Router

The following commands are used to enable SSO on the routers:

- **hw-module slot**
- **redundancy**
- **mode sso**

The configuration examples are the same for both platforms with the exception that the following configuration boot commands are seen in the beginning of a Cisco 7500 series router configuration (and not in a Cisco 10000 series router configuration):

```
boot system slot0:rsp-pv-mz
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz
```

Enabling SSO on a Cisco 10000 Series Router

The SSO mode is enabled by default.

Enabling NSF on Both the Cisco 7500 Series and Cisco 10000 Series Routers

The following commands are used to enable NSF for the routing protocols, such as BGP and OSPF, and for the label distribution protocols, such as BGP and LDP:

- **bgp graceful-restart restart-time**
- **bgp graceful-restart stalepath-time**
- **bgp graceful-restart**
- **nsf enforce global**
- **mpls forwarding bgp**

Inter-AS with IPv4 BGP Label Distribution enables you to set up a VPN so that the ASBRs exchange IPv4 routes with MPLS labels of the PE routers. Route reflectors (RRs) exchange VPNv4 routes by using Multihop, Multiprotocol EBGP. This configuration saves the ASBRs from having to store all of the VPNv4 routes. Using the RRs to store the VPNv4 routes and forward them to the PE routers improves scalability.

Figure 5 shows two MPLS VPN service providers. They distribute VPNv4 addresses between the RRs and IPv4 routes and MPLS labels between ASBRs.

Figure 5 MPLS VPN Inter-AS Configuration with MPLS VPN: NSF/SSO

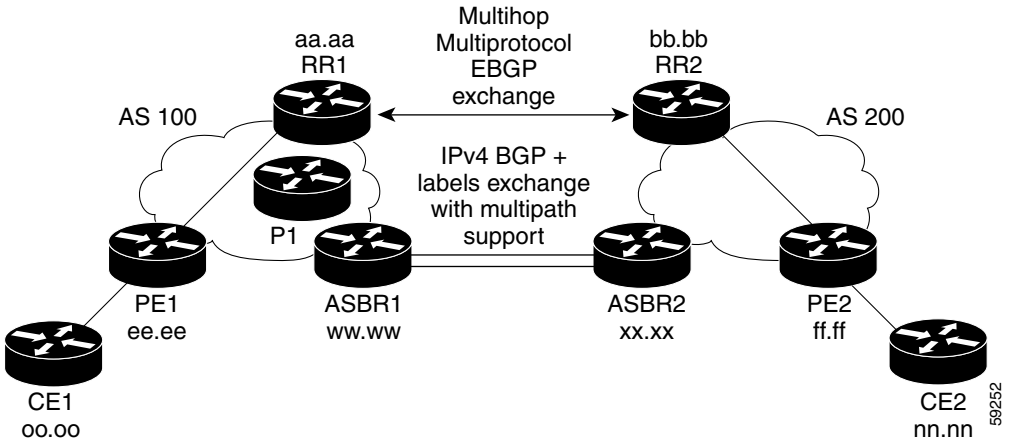


Figure 5 shows the two techniques you can use to distribute the VPNv4 routes and the IPv4 routes and MPLS labels of remote PEs and RRs to local PEs and RRs:

- AS 100 uses the route reflectors to distribute the IPv4 routes and MPLS labels and the VPNv4 routes from the ASBR to the PE.
- In AS 200, the IPv4 routes that ASBR2 learned are redistributed into IGP.

Note In the configuration examples, the NSF/SSO commands are bold-faced and arrows highlight any platform-specific commands.

RR1 Configuration

The configuration example for RR1 specifies the following:

- RR1 exchanges VPNv4 routes with RR2, using Multihop, Multiprotocol EBGP.
- The VPNv4 next hop information and the VPN label are preserved across the autonomous systems.
- RR1 reflects to PE1 the VPNv4 routes learned from RR2 and the IPv4 routes and MPLS labels learned from ASBR1.

```
redundancy
    mode sso
ip subnet-zero
ip cef distributed

!
interface Loopback0
    ip address aa.aa.aa.aa 255.255.255.255
!
interface Serial1/2                    =======> Serial1/0/2 on a Cisco 10000 series router
    ip address dd.0.0.2 255.0.0.0
    clockrate 124061
!
router ospf 10
log-adjacency-changes
auto-cost reference-bandwidth 1000
network aa.aa.aa.aa 0.0.0.0 area 100
network dd.0.0.0 0.255.255.255 area 100
!
```

```
router bgp 100
bgp cluster-id 1
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor ee.ee.ee.ee remote-as 100
neighbor ee.ee.ee.ee update-source Loopback0
neighbor ww.ww.ww.ww remote-as 100
neighbor ww.ww.ww.ww update-source Loopback0
neighbor bb.bb.bb.bb remote-as 200
neighbor bb.bb.bb.bb ebgp-multihop 255
neighbor bb.bb.bb.bb update-source Loopback0
no auto-summary
!
address-family ipv4
    neighbor ee.ee.ee.ee activate
    neighbor ee.ee.ee.ee route-reflector-client !IPv4+labels session to PE1
    neighbor ee.ee.ee.ee send-label
    neighbor ww.ww.ww.ww activate
    neighbor ww.ww.ww.ww route-reflector-client !IPv4+labels session to ASBR1
    neighbor ww.ww.ww.ww send-label
    no neighbor bb.bb.bb.bb activate
    no auto-summary
    no synchronization
    exit-address-family
!
address-family vpnv4
    neighbor ee.ee.ee.ee activate
    neighbor ee.ee.ee.ee route-reflector-client !VPNv4 session with PE1
    neighbor ee.ee.ee.ee send-community extended
    neighbor bb.bb.bb.bb activate
    neighbor bb.bb.bb.bb next-hop-unchanged
    !MH-VPNv4 session with RR2 with next hop unchanged
    neighbor bb.bb.bb.bb send-community extended
    exit-address-family
!
ip default-gateway 10.3.0.1
no ip classless
!
end
```

ASBR1 Configuration

ASBR1 exchanges IPv4 routes and MPLS labels with ASBR2.

```
redundancy
    mode sso
ip cef distributed
ip subnet-zero
mpls ldp graceful-restart
mpls label protocol ldp
!
interface Loopback0
    ip address ww.ww.ww.ww 255.255.255.255
    no ip route-cache
    no ip mroute-cache
!
interface Ethernet0/2    =====> interface FastEthernet1/0/2 on a Cisco 10000 series router
    ip address hh.0.0.2 255.0.0.0
    no ip mroute-cache
    mpls forwarding bgp
```

```
!
interface Ethernet0/3    =====> interface FastEthernet1/0/3 on a Cisco 10000 series router
    ip address dd.0.0.1 255.0.0.0
    no ip mroute-cache
    mpls label protocol ldp
    mpls ip
!
router ospf 10
log-adjacency-changes
auto-cost reference-bandwidth 1000
nsf enforce global
redistribute connected subnets
passive-interface Ethernet0/2  =====> passive-interface FastEthernet1/0/2 on a Cisco 10000
network ww.ww.ww.ww 0.0.0.0 area 100
network dd.0.0.0 0.255.255.255 area 100
!
router bgp 100
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor aa.aa.aa.aa remote-as 100
neighbor aa.aa.aa.aa update-source Loopback0
neighbor hh.0.0.1 remote-as 200
no auto-summary
! Redistributing IGP into BGP
! so that PE1 & RR1 loopbacks
! get into the BGP table.
address-family ipv4
redistribute ospf 10
neighbor aa.aa.aa.aa activate
neighbor aa.aa.aa.aa send-label
neighbor hh.0.0.1 activate
neighbor hh.0.0.1 advertisement-interval 5
neighbor hh.0.0.1 send-label
no auto-summary
no synchronization
exit-address-family
!
ip default-gateway 10.3.0.1
ip classless
end
```

RR2 Configuration

RR2 exchanges VPNv4 routes with RR1 through Multihop, Multiprotocol EBGP. In this configuration, the next hop information and the VPN label are preserved across the autonomous systems.

```
ip subnet-zero
ip cef
!
interface Loopback0
    ip address bb.bb.bb.bb 255.255.255.255
!
interface Serial1/1
    ip address ii.0.0.2 255.0.0.0
    no ip mroute-cache
!
router ospf 20
log-adjacency-changes
```

```
network bb.bb.bb.bb 0.0.0.0 area 200
network ii.0.0.0 0.255.255.255 area 200
!
router bgp 200
bgp cluster-id 1
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor aa.aa.aa.aa remote-as 100
neighbor aa.aa.aa.aa ebgp-multihop 255
neighbor aa.aa.aa.aa update-source Loopback0
neighbor ff.ff.ff.ff remote-as 200
neighbor ff.ff.ff.ff update-source Loopback0
no auto-summary
!
address-family vpnv4
    neighbor aa.aa.aa.aa activate
    neighbor aa.aa.aa.aa next-hop-unchanged
    !Multihop VPNv4 session with RR1 with next-hop unchanged
    neighbor aa.aa.aa.aa send-community extended
    neighbor ff.ff.ff.ff activate
    neighbor ff.ff.ff.ff route-reflector-client !VPNv4 session with PE2
    neighbor ff.ff.ff.ff send-community extended
    exit-address-family
!
ip default-gateway 10.3.0.1
no ip classless
end
```

ASBR2 Configuration

ASBR2 exchanges IPv4 routes and MPLS labels with ASBR1. However, in contrast to ASBR1, ASBR2 does not use the RR to reflect IPv4 routes and MPLS labels to PE2. ASBR2 redistributes the IPv4 routes and MPLS labels learned from ASBR1 into IGP. PE2 can reach these prefixes.

```
ip subnet-zero
ip cef
!
mpls ldp graceful-restart
mpls label protocol ldp
!
interface Loopback0
    ip address xx.xx.xx.xx 255.255.255.255
!
interface Ethernet1/0
    ip address hh.0.0.1 255.0.0.0
    no ip mroute-cache
    mpls forwarding bgp
!
interface Ethernet1/2
    ip address jj.0.0.1 255.0.0.0
    no ip mroute-cache
    mpls label protocol ldp
    mpls ip
!
router ospf 20
log-adjacency-changes
auto-cost reference-bandwidth 1000
nsf enforce global
redistribute connected subnets
```

```
redistribute bgp 200 subnets
passive-interface Ethernet1/0
! redistributing the routes learned from ASBR1
!(EBGP+labels session) into IGP so that PE2
! will learn them
network xx.xx.xx.xx 0.0.0.0 area 200
network jj..0.0 0.255.255.255 area 200
!
router bgp 200
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor bb.bb.bb.bb remote-as 200
neighbor bb.bb.bb.bb update-source Loopback0
neighbor hh.0.0.2 remote-as 100
no auto-summary
!
address-family ipv4
    redistribute ospf 20
    ! Redistributing IGP into BGP
    ! so that PE2 & RR2 loopbacks
    ! will get into the BGP-4 table
    neighbor hh.0.0.2 activate
    neighbor hh.0.0.2 advertisement-interval 5
    neighbor hh.0.0.2 send-label
    no auto-summary
    no synchronization
    exit-address-family
!
address-family vpnv4
    neighbor bb.bb.bb.bb activate
    neighbor bb.bb.bb.bb send-community extended
    exit-address-family
!
ip default-gateway 10.3.0.1
ip classless
!
end
```

NSF/SSO—MPLS VPN for an Inter-AS Network That Uses BGP to Distribute Routes and MPLS Labels over a Non-MPLS VPN Service Provider: Example

In this example, the NSF/SSO—MPLS VPN feature is configured on an existing MPLS VPN.

Enabling SSO on a Cisco 7500 Series Router

The following commands are used to enable SSO on the routers:

- **hw-module slot**
- **redundancy**
- **mode sso**

The configuration examples are the same for both platforms with the exception that the following configuration boot commands are seen in the beginning of a Cisco 7500 series router configuration (and not in a Cisco 10000 series router configuration):

```
boot system slot0:rsp-pv-mz
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz
```

Enabling SSO on a Cisco 10000 Series Router

The SSO mode is enabled by default.

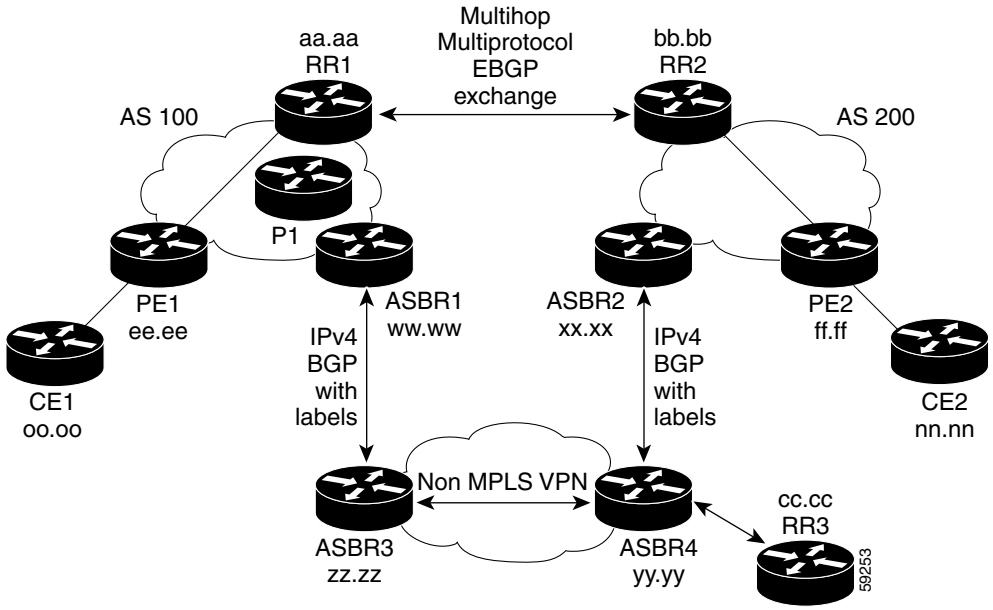
Enabling NSF on Both the Cisco 7500 Series and Cisco 10000 Series Routers

The following commands are used to enable NSF for the routing protocols, such as BGP and OSPF, and for the label distribution protocols, such as BGP and LDP:

- **bgp graceful-restart restart-time**
- **bgp graceful-restart stalepath-time**
- **bgp graceful-restart**
- **nsf enforce global**
- **mpls forwarding bgp**

Figure 6 shows two MPLS VPN service providers that are connected through a non-MPLS VPN service provider. The autonomous system in the middle of the network is configured as a backbone autonomous system that uses LDP to distribute MPLS labels. You can also use traffic engineering tunnels instead of LDP to build the LSP across the non-MPLS VPN service provider.

Figure 6 MPLS VPN Inter-AS Configuration 2 with MPLS VPN: NSF/SSO



Note In the configuration examples, the NSF/SSO commands are bold-faced and arrows highlight any platform-specific commands.

RR1 Configuration

The configuration example for RR1 specifies the following:

- RR1 exchanges VPNv4 routes with RR2, using Multihop, Multiprotocol EBGP.
- The VPNv4 next hop information and the VPN label are preserved across the autonomous systems.
- RR1 reflects to PE1 the VPNv4 routes learned from RR2 and the IPv4 routes and MPLS labels learned from ASBR1.

```
ip subnet-zero
ip cef
!
interface Loopback0
    ip address aa.aa.aa.aa 255.255.255.255
!
interface Serial1/2
    ip address dd.0.0.2 255.0.0.0
    clockrate 124061
!
router ospf 10
log-adjacency-changes
auto-cost reference-bandwidth 1000
network aa.aa.aa.aa 0.0.0.0 area 100
network dd.dd.0.0.0 0.255.255.255 area 100
!
router bgp 100
bgp cluster-id 1
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor ee.ee.ee.ee remote-as 100
neighbor ee.ee.ee.ee update-source Loopback0
neighbor ww.ww.ww.ww remote-as 100
neighbor ww.ww.ww.ww update-source Loopback0
neighbor bb.bb.bb.bb remote-as 200
neighbor bb.bb.bb.bb ebgp-multihop 255
neighbor bb.bb.bb.bb update-source Loopback0
no auto-summary
!
address-family ipv4
    neighbor ee.ee.ee.ee activate
    neighbor ee.ee.ee.ee route-reflector-client !IPv4+labels session to PE1
    neighbor ee.ee.ee.ee send-label
    neighbor ww.ww.ww.ww activate
    neighbor ww.ww.ww.ww route-reflector-client !IPv4+labels session to ASBR1
    neighbor ww.ww.ww.ww send-label
    no neighbor bb.bb.bb.bb activate
    no auto-summary
    no synchronization
    exit-address-family
!
address-family vpnv4
    neighbor ee.ee.ee.ee activate
    neighbor ee.ee.ee.ee route-reflector-client !VPNv4 session with PE1
    neighbor ee.ee.ee.ee send-community extended
    neighbor bb.bb.bb.bb activate
    neighbor bb.bb.bb.bb next-hop-unchanged
    !MH-VPNv4 session with RR2 with next-hop-unchanged
    neighbor bb.bb.bb.bb send-community extended
    exit-address-family
```

```
!
ip default-gateway 10.3.0.1
no ip classless
!
snmp-server engineID local 00000009020000D0584B25C0
snmp-server community public RO
snmp-server community write RW
no snmp-server ifindex persist
snmp-server packetsize 2048
!
end
```

ASBR1 Configuration

ASBR1 exchanges IPv4 routes and MPLS labels with ASBR2.

```
redundancy
    mode sso

ip subnet-zero
ip cef distributed
mpls ldp graceful-restart
mpls label protocol ldp
!
interface Loopback0
    ip address ww.ww.ww.ww 255.255.255.255
    no ip route-cache
    no ip mroute-cache
!
interface Serial3/0/0
    ip address kk.0.0.2 255.0.0.0
    mpls forwarding bgp
    ip route-cache distributed
!
interface Ethernet0/3
    ip address dd.0.0.1 255.0.0.0
    no ip mroute-cache
    mpls label protocol ldp
    mpls ip
!
router ospf 10
log-adjacency-changes
nsf enforce global
auto-cost reference-bandwidth 1000
redistribute connected subnets
passive-interface Serial3/0/0
network ww.ww.ww.ww 0.0.0.0 area 100
network dd.0.0.0 0.255.255.255 area 100
!
router bgp 100
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor aa.aa.aa.aa remote-as 100
neighbor aa.aa.aa.aa update-source Loopback0
neighbor kk.0.0.1 remote-as 200
no auto-summary
!
address-family ipv4
    redistribute ospf 10 ! Redistributing IGP into BGP
    neighbor aa.aa.aa.aa activate ! so that PE1 & RR1 loopbacks
```

```
    neighbor aa.aa.aa.aa send-label ! get into BGP table
    neighbor kk.0.0.1 activate
    neighbor kk.0.0.1 advertisement-interval 5
    neighbor kk.0.0.1 send-label
    no auto-summary
    no synchronization
    exit-address-family
!
ip default-gateway 10.3.0.1
ip classless
!
end
```

RR2 Configuration

RR2 exchanges VPNv4 routes with RR1, using Multihop, Multiprotocol EBGP. This configuration also preserves the next hop information and the VPN label across the autonomous systems.

```
ip subnet-zero
ip cef
!
interface Loopback0
    ip address bb.bb.bb.bb 255.255.255.255
!
interface Serial1/1
    ip address ii.0.0.2 255.0.0.0
    no ip mroute-cache
!
router ospf 20
log-adjacency-changes
network bb.bb.bb.bb 0.0.0.0 area 200
network ii.0.0.0 0.255.255.255 area 200
!
router bgp 200
bgp cluster-id 1
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor aa.aa.aa.aa remote-as 100
neighbor aa.aa.aa.aa ebgp-multihop 255
neighbor aa.aa.aa.aa update-source Loopback0
neighbor ff.ff.ff.ff remote-as 200
neighbor ff.ff.ff.ff update-source Loopback0
no auto-summary
!
address-family vpnv4
    neighbor aa.aa.aa.aa activate
    neighbor aa.aa.aa.aa next-hop-unchanged
    !MH Vpnv4 session with RR1 with next-hop-unchanged
    neighbor aa.aa.aa.aa send-community extended
    neighbor ff.ff.ff.ff activate
    neighbor ff.ff.ff.ff route-reflector-client !Vpnv4 session with PE2
    neighbor ff.ff.ff.ff send-community extended
    exit-address-family
!
ip default-gateway 10.3.0.1
no ip classless
!
end
```

ASBR2 Configuration

ASBR2 exchanges IPv4 routes and MPLS labels with ASBR1. However, in contrast to ASBR1, ASBR2 does not use the RR to reflect IPv4 routes and MPLS labels to PE2. Instead, ASBR2 redistributes the IPv4 routes and MPLS labels learned from ASBR1 into IGP. PE2 can now reach these prefixes.

```
redundancy
    mode sso
ip subnet-zero
ip cef distributed
!
mpls ldp graceful-restart
mpls label protocol ldp
!
interface Loopback0
    ip address xx.xx.xx.xx 255.255.255.255
!
interface Ethernet0/1    =====> interface FastEthernet1/0/1 on a Cisco 10000 series router
    ip address qq.0.0.2 255.0.0.0
    mpls forwarding bgp
!
interface Ethernet1/2    =====> interface FastEthernet1/1/2 on a Cisco 10000 series router
    ip address jj.0.0.1 255.0.0.0
    no ip mroute-cache
    mpls label protocol ldp
    mpls ip
!
router ospf 20
log-adjacency-changes
auto-cost reference-bandwidth 1000
nsf enforce global
redistribute connected subnets
redistribute bgp 200 subnets
!redistributing the routes learned from ASBR4
!(EBGP+labels session) into IGP so that PE2
!will learn them
passive-interface Ethernet0/1   ====> passive-interface FastEthernet1/0/1 on a Cisco 10000
network xx.xx.xx.xx 0.0.0.0 area 200
network jj.0.0.0 0.255.255.255 area 200
!
router bgp 200
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor bb.bb.bb.bb remote-as 200
neighbor bb.bb.bb.bb update-source Loopback0
neighbor qq.0.0.1 remote-as 100
no auto-summary
!
address-family ipv4
! Redistributing IGP into BGP redistribute ospf 20
! so that PE2 & RR2 loopbacks
! will get into the BGP-4 table
neighbor qq.0.0.1 activate
neighbor qq.0.0.1 advertisement-interval 5
neighbor qq.0.0.1 send-label
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
```

```
neighbor bb.bb.bb.bb activate
neighbor bb.bb.bb.bb send-community extended
exit-address-family
!
ip default-gateway 10.3.0.1
ip classless
!
end
```

ASBR3 Configuration

ASBR3 belongs to a non-MPLS VPN service provider. ASBR3 exchanges IPv4 routes and MPLS labels with ASBR1. ASBR3 also passes the routes learned from ASBR1 to ASBR3 through RR3.

Note Do not redistribute EBGP routes learned into internal BGP if you are using IBGP to distribute the routes and labels. This is not a supported configuration.

```
ip subnet-zero
ip cef
!
interface Loopback0
    ip address yy.yy.yy.yy 255.255.255.255
    no ip route-cache
    no ip mroute-cache
!
interface Hssi4/0                          ========> only on a Cisco 7500 series router
    ip address mm.0.0.0.1 255.0.0.0        ========> only on a Cisco 7500 series router
    no ip mroute-cache                     ========> only on a Cisco 7500 series router
    mpls ip                                ========> only on a Cisco 7500 series router
    hssi internal-clock                    ========> only on a Cisco 7500 series router
!
interface Serial5/0                      ========> Serial5/0/0 on a Cisco 10000 series router
    ip address kk.0.0.1 255.0.0.0
    no ip mroute-cache
    load-interval 30
    clockrate 124061
    mpls forwarding bgp
!
router ospf 30
log-adjacency-changes
auto-cost reference-bandwidth 1000
redistribute connected subnets
network yy.yy.yy.yy 0.0.0.0 area 300
network mm.0.0.0 0.255.255.255 area 300   ========> only on a Cisco 7500 series router
!
router bgp 300
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor cc.cc.cc.cc remote-as 300
neighbor cc.cc.cc.cc update-source Loopback0
neighbor kk.0.0.2 remote-as 100
no auto-summary
!
address-family ipv4
    neighbor cc.cc.cc.cc activate ! IBGP+labels session with RR3
    neighbor cc.cc.cc.cc send-label
    neighbor kk.0.0.2 activate ! EBGP+labels session with ASBR1
```

```
    neighbor kk.0.0.2 advertisement-interval 5
    neighbor kk.0.0.2 send-label
    no auto-summary
    no synchronization
    exit-address-family
!
end
```

RR3 Configuration

RR3 is a non-MPLS VPN RR that reflects IPv4 routes with MPLS labels to ASBR3 and ASBR4.

```
ip subnet-zero
!
interface Loopback0
    ip address cc.cc.cc.cc 255.255.255.255
!
interface POS0/2              ==========> interface POS1/0/2 on a Cisco 10000 series router
    ip address pp.0.0.1 255.0.0.0
    no ip route-cache cef
    no ip route-cache
    no ip mroute-cache
    crc 16
    clock source internal
!
router ospf 30
log-adjacency-changes
network cc.cc.cc.cc 0.0.0.0 area 300
network pp.0.0.0 0.255.255.255 area 300
!
router bgp 300
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
neighbor zz.zz.zz.zz remote-as 300
neighbor zz.zz.zz.zz update-source Loopback0
neighbor yy.yy.yy.yy remote-as 300
neighbor yy.yy.yy.yy update-source Loopback0
no auto-summary
!
address-family ipv4
    neighbor zz.zz.zz.zz activate
    neighbor zz.zz.zz.zz route-reflector-client
    neighbor zz.zz.zz.zz send-label ! IBGP+labels session with ASBR3
    neighbor yy.yy.yy.yy activate
    neighbor yy.yy.yy.yy route-reflector-client
    neighbor yy.yy.yy.yy send-label ! IBGP+labels session with ASBR4
    no auto-summary
    no synchronization
    exit-address-family
!
ip default-gateway 10.3.0.1
ip classless
!
end
```

ASBR4 Configuration

ASBR4 belongs to a non-MPLS VPN service provider. ASBR4 and ASBR3 exchange IPv4 routes and MPLS labels by means of RR3.

Note If you use IBGP to distribute the routes and labels, do not redistribute EBGP learned routes into IBGP. This is not a supported configuration.

```
redundancy
    mode sso
mpls ldp graceful-restart
ip subnet-zero
ip cef distributed
!
interface Loopback0
    ip address zz.zz.zz.zz 255.255.255.255
    no ip route-cache
    no ip mroute-cache
!
interface Ethernet0/2    =====> interface FastEthernet1/0/2 on a Cisco 10000 series router
    ip address qq.0.0.1 255.0.0.0
    no ip mroute-cache
    mpls forwarding bgp
!
interface POS1/1/0
    ip address pp.0.0.2 255.0.0.0
    ip route-cache distributed
!
interface Hssi2/1/1                         ========> only on a Cisco 7500 series router
    ip address mm.0.0.2 255.0.0.0           ========> only on a Cisco 7500 series router
    ip route-cache distributed       ========> only on a Cisco 7500 series router
    no ip mroute-cache               ========> only on a Cisco 7500 series router
    mpls label protocol ldp          ========> only on a Cisco 7500 series router
    mpls ip                          ========> only on a Cisco 7500 series router
    hssi internal-clock              ========> only on a Cisco 7500 series router
!
router ospf 30
log-adjacency-changes
nsf enforce global
auto-cost reference-bandwidth 1000
redistribute connected subnets
passive-interface Ethernet0/2   ====> passive-interface FastEthernet1/0/2 on a Cisco 10000
network zz.zz.zz.zz 0.0.0.0 area 300
network pp.0.0.0 0.255.255.255 area 300
network mm.0.0.0 0.255.255.255 area 300
!
router bgp 300
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor cc.cc.cc.cc remote-as 300
neighbor cc.cc.cc.cc update-source Loopback0
neighbor qq.0.0.2 remote-as 200
no auto-summary
!
address-family ipv4
    neighbor cc.cc.cc.cc activate
    neighbor cc.cc.cc.cc send-label
    neighbor qq.0.0.2 activate
```

```
    neighbor qq.0.0.2 advertisement-interval 5
    neighbor qq.0.0.2 send-label
    no auto-summary
    no synchronization
    exit-address-family
!
ip classless
end
```

Additional References

The following sections provide additional information related to the NSF/SSO—MPLS VPN feature.

Related Documents

Related Topic	Document Title
Nonstop forwarding and BGP Graceful Restart	*Cisco Nonstop Forwarding*
Stateful awitchover	*Stateful Switchover*
Basic VPNs, MPLS VPN interautonomous systems, MPLS VPN Carrier Supporting Carrier	"Part 4: MPLS Virtual Private Networks" module in the *Cisco IOS Multiprotocol Label Switching Configuration Guide*, Release 12.4

Standards

Standards	Title
draft-ietf-mpls-bgp-mpls-restart.txt	*Graceful Restart Mechanism for BGP with MPLS*
draft-ietf-mpls-idr-restart.txt	*Graceful Restart Mechanism for BGP*

MIBs

MIBs	MIBs Link
MPLS VPN MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 1163	*A Border Gateway Protocol*
RFC 1164	*Application of the Border Gateway Protocol in the Internet*
RFC 2283	*Multiprotocol Extensions for BGP-4*
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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Command Reference

This section documents only new and modified commands.

- **mpls forwarding bgp**
- **show ip bgp labels**
- **show ip bgp vpnv4**

mpls forwarding bgp

To enable Multiprotocol Label Switching (MPLS) nonstop forwarding on an interface that uses Border Gateway Protocol (BGP) as the label distribution protocol, use the **mpls forwarding bgp** command in interface configuration mode. To disable MPLS nonstop forwarding on the interface, use the **no** form of this command.

mpls forwarding bgp

no mpls forwarding bgp

Syntax Description

This command has no arguments or keywords.

Defaults

MPLS nonstop forwarding is not enabled on the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series router.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Configure this command on the interfaces of the BGP peers that send and receive labels. If this command is not configured on an interface and a stateful switchover occurs, packets received from an interface are dropped until the BGP session is established in the new route processor.

Issue this command to enable nonstop forwarding on interfaces that use BGP to distribute labels for the following types of VPNs:

- MPLS VPN—Carrier Supporting Carrier—IPv4 BGP Label Distribution
- MPLS VPN—Inter-AS—IPv4 BGP Label Distribution

Examples

In the following examples, an interface is configured to save BGP labels in the event of a stateful switchover:

Cisco 7000 Series Example

```
Router(config)# interface Pos1/0
Router(config-if)# mpls forwarding bgp
```

Cisco 10000 Series Example

```
Router(config)# interface Pos1/0/0
```

```
Router(config-if)# mpls forwarding bgp
```

Related Commands

Command	Description
bgp graceful-restart	Enables BGP Graceful Restart on the router.

show ip bgp labels

To display information about Multiprotocol Label Switching (MPLS) labels from the external Border Gateway Protocol (eBGP) route table, use the **show ip bgp labels** command in privileged EXEC mode.

show ip bgp labels

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series router.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use this command to display eBGP labels associated with an Autonomous System Boundary Router (ASBR).

This command displays labels for BGP routes in the default table only. To display labels in the Virtual Private Network (VPN) routing and forwarding (VRF) tables, use the **show ip bgp vpnv4** {**all** | **vrf** *vrf-name*} command with the optional **labels** keyword.

Examples

The following example shows output for an ASBR using BGP as a label distribution protocol:

```
Router# show ip bgp labels

Network          Next Hop         In Label/Out Label
10.3.0.0/16       0.0.0.0          imp-null/exp-null
10.15.15.15/32   10.15.15.15      18/exp-null
10.16.16.16/32   0.0.0.0          imp-null/exp-null
10.17.17.17/32   10.0.0.1         20/exp-null
10.18.18.18/32   10.0.0.1         24/31
10.18.18.18/32   10.0.0.1         24/33
```

Table 1 describes the significant fields shown in the display.

Table 1 show ip bgp labels Field Descriptions

Field	Description
Network	Displays the network address from the eGBP table.
Next Hop	Specifies the eBGP next hop address.
In Label	Displays the label (if any) assigned by this router.
Out Label	Displays the label assigned by the BGP next hop router.

Related Commands

Command	Description
show ip bgp vpnv4	Displays VPN address information from the BGP table.

show ip bgp vpnv4

To display Virtual Private Network Version 4 (VPNv4) address information from the Border Gateway Protocol (BGP) table, use the **show ip bgp vpnv4** command in user EXEC or privileged EXEC mode.

show ip bgp vpnv4 {**all** | **rd** *route-distinguisher* | **vrf** *vrf-name*} [**rib-failure**] [*ip-prefix/length* [**longer-prefixes**]] [*network-address* [*mask*] [**longer-prefixes**]] [**cidr-only**] [**community**] [**community-list**] [**dampened-paths**] [**filter-list**] [**flap-statistics**] [**inconsistent-as**] [**neighbors**] [**paths** [*line*]] [**peer-group**] [**quote-regexp**] [**regexp**] [**summary**] [**labels**]

Syntax Description

all	Displays the complete VPNv4 database.
rd *route-distinguisher*	Displays Network Layer Reachability Information (NLRI) prefixes that match the named route distinguisher.
vrf *vrf-name*	Displays NLRI prefixes associated with the named VPN routing and forwarding (VRF) instance.
rib-failure	(Optional) Displays BGP routes that failed to install in the VRF table.
ip-prefix/length	(Optional) The IP prefix address (in dotted decimal format) and the length of the mask (0 to 32). The slash mark must be included.
longer-prefixes	(Optional) Displays the entry, if any, that exactly matches the specified prefix parameter and all entries that match the prefix in a "longest-match" sense. That is, prefixes for which the specified prefix is an initial substring.
network-address	(Optional) The IP address of a network in the BGP routing table.
mask	(Optional) The mask of the network address, in dotted decimal format.
cidr-only	(Optional) Displays only routes that have nonclassful net masks.
community	(Optional) Displays routes that match this community.
community-list	(Optional) Displays routes that match this community list.
dampened-paths	(Optional) Displays paths suppressed because of dampening (BGP route from peer is up and down).
filter-list	(Optional) Displays routes that conform to the filter list.
flap-statistics	(Optional) Displays flap statistics of routes.
inconsistent-as	(Optional) Displays only routes that have inconsistent autonomous systems of origin.
neighbors	(Optional) Displays details about TCP and BGP neighbor connections.
paths	(Optional) Displays path information.
line	(Optional) A regular expression to match the BGP autonomous system paths.
peer-group	(Optional) Displays information about peer groups.
quote-regexp	(Optional) Displays routes that match the autonomous system path regular expression.
regexp	(Optional) Displays routes that match the autonomous system path regular expression.

summary	(Optional) Displays BGP neighbor status.
labels	(Optional) Displays incoming and outgoing BGP labels for each NLRI prefix.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(2)T	The output of the **show ip bgp vpnv4 all** *ip-prefix* command was enhanced to display attributes including multipaths and a best path to the specified network.
12.0(21)ST	The **tags** keyword was replaced by the **labels** keyword to conform to the MPLS guidelines. This command was integrated into Cisco IOS Release 12.0(21)ST.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.0(27)S	The output of the **show ip bgp vpnv4 all labels** command was enhanced to display explicit-null label information.
12.3	The **rib-failure** keyword was added for VRFs.
12.2(22)S	The output of the **show ip bgp vpnv4 vrf** *vrf-name* **labels** command was modified so that directly connected VRF networks no longer display as aggregate; no label appears instead.
12.2(25)S	This command was updated to display MPLS VPN nonstop forwarding information.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series router. The display output was modified to indicate whether BGP Nonstop Routing (NSR) with stateful switchover (SSO) is enabled and the reason the last BGP lost SSO capability.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA, and the output was modified to support per-VRF assignment of the BGP router ID.
12.2(31)SB2	The output was modified to support per-VRF assignment of the BGP router ID.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH. **Note** In Cisco IOS Release 12.2(33)SXH, the command output does not display on the standby route processor in NSF/SSO mode.

Usage Guidelines

Use this command to display VPNv4 information from the BGP database. The **show ip bgp vpnv4 all** command displays all available VPNv4 information. The **show ip bgp vpnv4 summary** command displays BGP neighbor status. The **show ip bgp vpnv4 all labels** command displays explicit-null label information.

Examples

The following example shows output for all available VPNv4 information in a BGP routing table:

```
Router# show ip bgp vpnv4 all

BGP table version is 18, local router ID is 10.14.14.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP,? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:101 (default for vrf vpn1)
*>i10.6.6.6/32      10.0.0.21               11    100      0 ?
*> 10.7.7.7/32      10.150.0.2              11         32768 ?
*>i10.69.0.0/30     10.0.0.21                0    100      0 ?
*> 10.150.0.0/24    0.0.0.0                  0         32768 ?
```

Table 2 describes the significant fields shown in the display.

Table 2 show ip bgp vpnv4 all Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Displays the address of the BGP next hop.
Metric	Displays the BGP metric.
LocPrf	Displays the local preference.
Weight	Displays the BGP weight.
Path	Displays the BGP path per route.

The following example shows how to display a table of labels for NLRI prefixes that have a route distinguisher value of 100:1.

```
Router# show ip bgp vpnv4 rd 100:1 labels

Network            Next Hop       In label/Out label
Route Distinguisher: 100:1 (vrf1)
   10.0.0.0         10.20.0.60      34/nolabel
   10.0.0.0         10.20.0.60      35/nolabel
   10.0.0.0         10.20.0.60      26/nolabel
                    10.20.0.60      26/nolabel
   10.0.0.0         10.15.0.15      nolabel/26
```

Table 3 describes the significant fields shown in the display.

Table 3 show ip bgp vpnv4 rd labels Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Specifies the BGP next hop address.
In label	Displays the label (if any) assigned by this router.
Out label	Displays the label assigned by the BGP next hop router.

The following example shows VPNv4 routing entries for the VRF named vpn1:

```
Router# show ip bgp vpnv4 vrf vpn1

BGP table version is 18, local router ID is 10.14.14.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP,? - incomplete

Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:101 (default for vrf vpn1)
*>i10.6.6.6/32       10.0.0.21               11    100      0 ?
*> 10.7.7.7/32       10.150.0.2              11         32768 ?
*>i10.69.0.0/30      10.0.0.21                0    100      0 ?
*> 10.150.0.0/24      0.0.0.0                 0         32768 ?
*> 10.0.0.1/32       10.150.0.2              11         32768 ?
*>i10.0.0.3/32       10.0.0.21               11    100      0 ?
```

Table 4 describes the significant fields shown in the display.

Table 4 show ip bgp vpnv4 vrf Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Displays the address of the BGP next hop.
Metric	Displays the BGP metric.
LocPrf	Displays the local preference.
Weight	Displays the BGP weight.
Path	Displays the BGP path per route.

The following example shows attributes for network 10.22.22.0 that include multipaths and a best path:

```
Router# show ip bgp vpnv4 all 10.22.22.0

BGP routing table entry for 10:1:10.22.22.0/24, version 50
Paths:(6 available, best #1)
Multipath:iBGP
  Advertised to non peer-group peers:
  10.1.12.12
  22
    10.22.7.8 (metric 11) from 10.11.3.4 (10.0.0.8)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath, best
      Extended Community:RT:100:1
      Originator:10.0.0.8, Cluster list:10.1.1.44
  22
    10.22.1.9 (metric 11) from 10.11.1.2 (10.0.0.9)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath
      Extended Community:RT:100:1
      Originator:10.0.0.9, Cluster list:10.1.1.22
```

Table 5 describes the significant fields shown in the display.

Table 5 show ip bgp vpnv4 all network-address Field Descriptions

Field	Description
BGP routing table entry for ... version	Internal version number of the table. This number is incremented whenever the table changes.
Paths	Number of autonomous system paths to the specified network. If multiple paths exist, one of the multipaths is designated the best path.
Multipath	Indicates the maximum paths configured (iBGP or eBGP).
Advertised to non peer-group peers	IP address of the BGP peers to which the specified route is advertised.
10.22.7.8 (metric 11) from 10.11.3.4 (10.0.0.8)	Indicates the next hop address and the address of the gateway that sent the update.
Origin	Indicates the origin of the entry. It can be one of the following values: • IGP—Entry originated from Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • incomplete—Entry originated from other than an IGP or Exterior Gateway Protocol (EGP) and was advertised with the **redistribute** router configuration command. • EGP—Entry originated from an EGP.
metric	If shown, the value of the interautonomous system metric.
localpref	Local preference value as set with the **set local-preference route-map** configuration command. The default value is 100.
valid	Indicates that the route is usable and has a valid set of attributes.
internal/external	The field is *internal* if the path is learned via iBGP. The field is *external* if the path is learned via eBGP.
multipath	One of multiple paths to the specified network.
best	If multiple paths exist, one of the multipaths is designated the best path and this path is advertised to neighbors.
Extended Community	Route Target value associated with the specified route.
Originator	The router ID of the router from which the route originated when route reflector is used.
Cluster list	The router ID of all the route reflectors that the specified route has passed through.

The following example shows routes that BGP could not install in the VRF table:

```
Router# show ip bgp vpnv4 vrf xyz rib-failure

Network            Next Hop                      RIB-failure   RIB-NH Matches
Route Distinguisher: 2:2 (default for vrf bar)
10.1.1.2/32        10.100.100.100      Higher admin distance              No
10.111.111.112/32  10.9.9.9            Higher admin distance             Yes
```

Table 6 describes the significant fields shown in the display.

Table 6 show ip bgp vpnv4 vrf rib-failure Field Descriptions

Field	Description
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
RIB-failure	Cause of the Routing Information Base (RIB) failure. Higher admin distance means that a route with a better (lower) administrative distance, such as a static route, already exists in the IP routing table.
RIB-NH Matches	Route status that applies only when Higher admin distance appears in the RIB-failure column and the **bgp suppress-inactive** command is configured for the address family being used. There are three choices: • Yes—Means that the route in the RIB has the same next hop as the BGP route or that the next hop recurses down to the same adjacency as the BGP next hop. • No—Means that the next hop in the RIB recurses down differently from the next hop of the BGP route. • n/a—Means that the **bgp suppress-inactive** command is not configured for the address family being used.

The following example shows the information displayed on the active and standby Route Processors when they are configured for NSF/SSO: MPLS VPN.

Note In Cisco IOS Release 12.2(33)SXH, the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature incurred various infrastructure changes. The result of those changes affect the output of this command on the standby route processor. In Cisco IOS Release 12.2(33)SXH, the standby route processor does not display any output from the **show ip bgp vpnv4** commands.

Active Route Processor

```
Router# show ip bgp vpnv4 all labels

Network          Next Hop    In label/Out label
Route Distinguisher: 100:1 (vpn1)
10.12.12.12/32   0.0.0.0     16/aggregate(vpn1)
10.0.0.0/8       0.0.0.0     17/aggregate(vpn1)
Route Distinguisher: 609:1 (vpn0)
10.13.13.13/32   0.0.0.0     18/aggregate(vpn0)

Router# show ip bgp vpnv4 vrf vpn1 labels

Network           Next Hop    In label/Out label
Route Distinguisher: 100:1 (vpn1)
10.12.12.12/32    0.0.0.0     16/aggregate(vpn1)
10.0.0.0/8        0.0.0.0     17/aggregate(vpn1)
```

Standby Route Processor

```
Router# show ip bgp vpnv4 all labels
```

```
Network       Masklen   In label
Route Distinguisher: 100:1
10.12.12.12   /32       16
10.0.0.0      /8        17
Route Distinguisher: 609:1
10.13.13.13   /32       18

Router# show ip bgp vpnv4 vrf vpn1 labels

Network        Masklen   In label
Route Distinguisher: 100:1
10.12.12.12    /32       16
10.0.0.0       /8        17
```

Table 7 describes the significant fields shown in the display.

Table 7 show ip bgp vpn4 labels Field Descriptions

Field	Description
Network	The network address from the BGP table.
Next Hop	The BGP next hop address.
In label	The label (if any) assigned by this router.
Out label	The label assigned by the BGP next hop router.
Masklen	The mask length of the network address.

The following example displays output, including the explicit-null label, from the **show ip bgp vpnv4 all labels** command on a CSC-PE router:

```
Router# show ip bgp vpnv4 all labels

   Network          Next Hop      In label/Out label
Route Distinguisher: 100:1 (v1)
   10.0.0.0/24      10.0.0.0        19/aggregate(v1)
   10.0.0.1/32      10.0.0.0        20/nolabel
   10.1.1.1/32      10.0.0.0        21/aggregate(v1)
   10.10.10.10/32   10.0.0.1        25/exp-null
   10.168.100.100/32
                    10.0.0.1        23/exp-null
   10.168.101.101/32
                    10.0.0.1        22/exp-null
```

Table 8 describes the significant fields shown in the display.

Table 8 show ip bgp vpnv4 all labels Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Displays the address of the BGP next hop.
In label	Displays the label (if any) assigned by this router.
Out label	Displays the label assigned by the BGP next hop router.
Route Distinguisher	Displays an 8-byte value added to an IPv4 prefix to create a VPN IPv4 prefix.

The following example displays separate router IDs for each VRF in the output from an image in Cisco IOS Release 12.2(33)SRA, 12.2(31)SB2, and later releases with the Per-VRF Assignment of BGP Router ID feature configured. The router ID is shown next to the VRF name.

```
Router# show ip bgp vpnv4 all

BGP table version is 5, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf vrf_trans) VRF Router ID 10.99.1.2
*> 192.168.4.0      0.0.0.0                  0         32768 ?
Route Distinguisher: 42:1 (default for vrf vrf_user) VRF Router ID 10.99.1.1
*> 192.168.5.0      0.0.0.0                  0         32768 ?
```

Table 9 describes the significant fields shown in the display.

Table 9 show ip bgp vpnv4 all (VRF Router ID) Field Descriptions

Field	Description
Route Distinguisher	Displays an 8-byte value added to an IPv4 prefix to create a VPN IPv4 prefix.
vrf	Name of the VRF.
VRF Router ID	Router ID for the VRF.

Related Commands

Command	Description
show ip vrf	Displays the set of defined VRFs and associated interfaces.

Feature Information for NSF/SSO—MPLS VPN

Table 10 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note Table 10 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 10 Feature Information for NSF/SSO—MPLS VPN

Feature Name	Releases	Feature Information
NSF/SSO—MPLS VPN	12.2(25)S 12.2(28)SB 12.2(33)SRA 12.2(33)SXH	This feature allows a provider edge (PE) router or Autonomous System Border Router (ASBR) (with redundant Route Processors) to preserve data forwarding information in a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) when the primary Route Processor restarts. In 12.2(25)S, this feature was introduced on the Cisco 7500 series router. In 12.2(28)SB, support was added for the Cisco 10000 series routers. In 12.2(33)SRA, support was added for the Cisco 7600 series routers. In 12.2(33)SXH, this feature was integrated into this release.