MPLS High Availability Configuration Guide, Cisco IOS Release 12.2SR

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

MPLS High Availability Overview

This document provides an overview of the Multiprotocol Label Switching (MPLS) high availability (HA) features. MPLS HA provides full nonstop forwarding (NSF) and stateful switchover (SSO) capability to the MPLS Label Distribution Protocol (LDP) and MPLS Virtual Private Networks (VPNs) features.

Finding Feature Information

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

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

Restrictions for MPLS High Availability

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 12.2SB, 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 Release Notes for Cisco IOS Release 12.2SX on the Catalyst 6500 Series MSFC

Information About MPLS High Availability

- MPLS Applications That Coexist with SSO, page 5

MPLS High Availability Overview

MPLS HA features provide SSO and NSF capability to the MPLS Label Distribution Protocol (LDP) and MPLS Virtual Private Network (VPN) features. MPLS HA includes the following new features:

- NSF SSO—MPLS VPN, page 3
- NSF SSO - MPLS LDP and LDP Graceful Restart, page 3
- NSF SSO Any Transport over MPLS and Graceful Restart, page 3

In addition, the MIBs for MPLS VPNs and MPLS LDP have been enhanced to work in the MPLS HA environment.

The following features have been changed or created to work in the MPLS HA environment:

- MPLS High Availability Infrastructure Changes, page 4
- Cisco Express Forwarding Scalability Enhancements, page 4

The following features perform normally in an NSF/SSO environment. They can exist with SSO and NSF but do not have the ability to keep duplicate information in a backup Route Processor (RP) on the Cisco 7500 series router and in a backup Performance Routing Engine2 (PRE2) on the Cisco 10000 series router.

- MPLS Traffic Engineering, page 5
- MPLSQualityofServiceApplications, page 5
- IPv6 over MPLS, page 6 (not supported on the Cisco 10000 series router)
- MPLS Label Switching Router MIB, page 6
- MPLS TE MIB, page 6
- MPLS Enhancements to Interfaces MIB, page 6

The following sections explain these features in more detail.

MPLS High Availability Features

The following MPLS HA features have the ability to continue forwarding data following an RP switchover on the Cisco 7500 series router or PRE2 switchover on the Cisco 10000 series router:

- MPLS Label Distribution Protocol (LDP)
- MPLS Virtual Private Networks (VPNs)
- Any Transport over MPLS (AToM)

Note In Cisco IOS Release 12.2(28)SB, AToM is not enabled for high availability on the Cisco 10000 series router. However, AToM coexists with SSO. This means that AToM functions normally in an SSO environment but because state information is not maintained on the standby RP, a switchover can partially disrupt operations

When you enable MPLS HA, you get the benefit of allowing an RP on the Cisco 7500 series router or PRE2 on the Cisco 10000 series router to recover from disruption in service without losing its LDP bindings, MPLS forwarding state, and VPN prefix information.

- NSF SSO—MPLS VPN, page 3
- NSF SSO - MPLS LDP and LDP Graceful Restart, page 3

- NSF SSO Any Transport over MPLS and Graceful Restart, page 3

NSF SSO—MPLS VPN

The MPLS High Availability feature allows a router to recover from a disruption in service without losing its VPN prefix information. The MPLS High Availability feature works with the BGP Graceful Restart mechanisms defined in the Graceful Restart Internet Engineering Task Force (IETF) specifications and in the Cisco Nonstop Forwarding feature module. The BGP Graceful Restart feature supports the VPNv4 VRFs, which allows the routers running BGP Graceful Restart to preserve VPN prefix information when a router restarts.

For information about configuring the MPLS High Availability feature, see the following feature module: NSF/SSO—MPLS VPN.

- NSF SSO MPLS VPN MIB, page 3

NSF SSO MPLS VPN MIB

The MPLS High Availability feature works with the MPLS VPN MIB. For information about configuring the MPLS VPN MIB, see the following feature module: MPLS VPN: SNMP MIB Support.

NSF SSO - MPLS LDP and LDP Graceful Restart

MPLS LDP uses SSO, NSF, and Graceful Restart to allow an RP on the Cisco 7500 series router or PRE2 on the Cisco 10000 series router to recover from disruption in the LDP components of the control plane service without losing its MPLS forwarding state. The NSF/SSO--MPLS LDP and LDP Graceful Restart feature works with LDP sessions between directly connected peers as well as with peers that are not directly connected (targeted sessions).

For information about configuring the NSF/SSO MPLS LDP and LDP Graceful Restart feature, see the following feature module: *NSF/SSO—MPLS LDP and LDP Graceful Restart.*

- NSF SSO MPLS LDP MIB, page 3

NSF SSO MPLS LDP MIB

The MPLS LDP MIB with the IETF Version 8 Upgrade is supported with NSF/SSO MPLS LDP and LDP Graceful Restart. For information about configuring the MPLS LDP MIB, see the following feature module: MPLS Label Distribution Protocol MIB Version 8 Upgrade.

NSF SSO Any Transport over MPLS and Graceful Restart

AToM uses SSO, NSF, and Graceful Restart to allow an RP to recover from disruption in the LDP components of the control plane service without losing its MPLS forwarding state.

Note In Cisco IOS Release 12.2(28)SB, AToM is not enabled for high availability on the Cisco 10000 series router. However, AToM coexists with SSO. This means that AToM functions normally in an SSO environment but because state information is not maintained on the standby RP, a switchover can partially disrupt operations.

For information about configuring AToM NSF/SSO Support and Graceful Restart, see NSF/SSO: Any Transport over MPLS and Graceful Restart.

MPLS High Availability Infrastructure Changes

The MPLS control plane software has been enhanced to work in an HA environment. The changes made the control plane software more modular, which helps MPLS support newer applications. Some of the control plane software changes made MPLS more scalable and flexible. See the Cisco Express Forwarding Scalability Enhancements, page 4 for more information.

Changes to the MPLS Forwarding Infrastructure (MFI) and the Cisco Express Forwarding component introduced new commands and changed other existing commands.

MFI replaced the Label Forwarding Information Base (LFIB) and is responsible for managing MPLS data structures used for forwarding. For information about the MPLS command changes related to the MFI, see the following document: MPLS High Availability: Command Changes.

Note The MFI and LFIB do not coexist in the same image. Users must use MFI starting with Cisco IOS Release 12.2(25)S and later releases.

MPLS High Availability introduces the MPLS IP Rewrite Manager (IPRM), which manages the interactions between Cisco Express Forwarding, the IP Label Distribution Modules (LDMs), and the MFI. MPLS IPRM is enabled by default. You do not need to configure or customize the IPRM. See the Feature Information for MPLS High Availability Overview, page 8 for show and debug commands related to IPRM.

- Cisco Express Forwarding Scalability Enhancements, page 4

Cisco Express Forwarding Scalability Enhancements

Cisco Express Forwarding provides a forwarding path and maintains a complete forwarding and adjacency table for both the software and hardware forwarding engines.

With MPLS High Availability, Cisco Express Forwarding supports new features and new hardware. The Cisco Express Forwarding improvements enable Cisco Express Forwarding to work with the MPLS HA applications and the MFI infrastructure. Cisco Express Forwarding improvements increase scalability, which are outlined in the table below.

Table 1 Cisco Express Forwarding Scalability Enhancements

For the Cisco 7500 Series Router	For the Cisco 10000 Series Router
Up to 512,000 prefixes	Up to 1 million prefixes
Up to 128,000 adjacencies	Up to 1 million adjacencies
4000 VPNs	4000 VPNs
Arbitrary prefix path counts from the Routing Information Base (RIB)	Arbitrary prefix path counts from the RIB
16 paths per prefix for forwarding	8 paths per prefix for forwarding
64 Cisco Express Forwarding instances (such as line cards or redundant RPs)	NA

Cisco Express Forwarding makes the following enhancements:

- Improves memory use
- Reduces large peak memory use
- Reduces route convergence times for the Cisco 7500 series router.

For information about the Cisco Express Forwarding command changes, see Cisco Express Forwarding: Command Changes.

MPLS Applications That Coexist with SSO

The following sections list the MPLS features that maintain, either partially or completely, undisturbed operation through an RP switchover on the Cisco 7500 series router or PRE2 switchover on the Cisco 10000 series router.

- MPLS Traffic Engineering, page 5
- MPLSQualityofServiceApplications, page 5
- IPv6 over MPLS, page 6
- MPLS Label Switching Router MIB, page 6
- MPLS TE MIB, page 6
- MPLS Enhancements to Interfaces MIB, page 6

MPLS Traffic Engineering

The MPLS Traffic Engineering (TE) features work with the new Cisco Express Forwarding and MFI modules. TE is SSO coexistent, which means it maintains, either partially or completely, undisturbed operation through an RP switchover on the Cisco 7500 series router or PRE2 switchover on the Cisco 10000 series router. No additional capabilities have been introduced with MPLS High Availability. The **debug mpls traffic-eng lsd-client**command is introduced with the MPLS High Availability features.

MPLSQualityofServiceApplications

Cisco IOS MPLS supports the IETF DiffServ architecture by enabling the quality of service (QoS) functions listed in the table below to act on the MPLS packets.

Table 2 MPLS QoS Support

Category	Related MPLS QoS Features
Traffic classification	Access Control List matching
Traffic marking	Differentiated services code point (DSCP) MPLS Experimental (EXP) field
Congestion management	Low latency queueing (LLQ) Class-based weighted fair queueing (CBWFQ)
Congestion avoidance	Weighted Random Early Detection (WRED)
Traffic conditioning	Shaping and policing

IPv6 over MPLS

The IPv6 over MPLS application works with the new Cisco Express Forwarding and MFI modules. IPv6 over MPLS is SSO coexistent, which means it maintains, either partially or completely, undisturbed operation through an RP switchover.

Note The Cisco 10000 series router does not support the IPv6 over MPLS application.

Command changes are documented in the Cisco IOS IPv6 Command Reference.

MPLS Label Switching Router MIB

The MPLS Label Switching Router (LSR) MIB works in the MPLS HA environment. Two indexes in the LSR MIB were changed to provide well-defined and ordered values:

- mplsXCIndex
- mplsOutSegmentIndex

This benefits the MPLS LSR MIB in the following ways:

- The MIB walk-through has a consistent and logical order.
- The same index values are maintained after a switchover.

For information about the MPLS LSR MIB, see the MPLS Label Switching Router MIB.

MPLS TE MIB

The MPLS TE MIB works in the MPLS HA environment. For information about the MPLS TE MIB, see the MPLS Traffic Engineering (TE) MIB.

Note After an RP switchover on the Cisco 7500 series router or PRE2 switchover on the Cisco 10000 series router, the value of mplsTunnelCreationTime in the TE MIB does not correctly reflect the time when the tunnel was created. After an RP or PRE2 switchover, the tunnel gets a new time stamp.

MPLS Enhancements to Interfaces MIB

The MPLS Enhancements to Interfaces MIB works in the MPLS HA environment. For information about the MPLS Enhancements to Interfaces MIB, see the MPLS Enhancements to Interfaces MIB.

Additional References

The following sections provide references related to the MPLS High Availability feature.

Related Documents

Related Topic	Document Title
MPLS VPNs Non Stop Forwarding	NSF/SSO—MPLS VPN
MPLS LDP Non Stop Forwarding	*NSF/SSO—MPLS LDP and LDP Graceful Restart*
AToM Non Stop Forwarding	NSF/SSO: Any Transport over MPLS and Graceful Restart
Cisco Express Forwarding	Cisco Express Forwarding: Command Changes
MIBs	• MPLS VPN: SNMP MIB Support • MPLS Label Distribution Protocol MIB Version 8 Upgrade • MPLS Label Switching Router MIB • MPLS Enhancements to Interfaces MIB • MPLS Traffic Engineering (TE) MIB
NSF/SSO	Cisco Nonstop Forwarding MPLS High Availability: Command Changes

Standards

Standard	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

MIB	MIBs Link
• MPLS VPN MIB • MPLS Label Distribution Protocol MIB Version 8 Upgrade	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

RFC	Title
RFC 3478	Graceful Restart Mechanism for Label Distribution

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

Feature Information for MPLS High Availability Overview

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

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

Table 3 Feature Information for MPLS High Availability: Overview

Feature Name	Releases	Feature Information
MPLS High Availability: Overview	12.2(25)S 12.2(28)SB 12.2(33)SRA 12.2(33)SXH	This feature provides an overview of the Multiprotocol Label Switching (MPLS) high availability (HA) features. 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. In 12.2(33)SRA, support was added for the Cisco 7600 series routers. In 12.2(33)SXH, this feature was integrated into Cisco IOS Release 12.2(33)SXH.

MPLS High Availability Command Changes

This feature module details changes to commands that are required to support updates to the Multiprotocol Label Switching (MPLS) High Availability (HA) feature.

In Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, and 12.2(33)SXH, the MPLS control plane software is enhanced to work in MPLS HA environments. The changes made the control plane software more modular, which helps MPLS support MPLS HA applications. Some of the control plane software changes also made MPLS more scalable and flexible.

Changes to the MPLS Forwarding Infrastructure (MFI) and the Cisco Express Forwarding component introduced new commands and changed other existing commands. MFI replaced the Label Forwarding Information Base (LFIB) and is responsible for managing MPLS data structures used for forwarding.

Finding Feature Information

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

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

Information About MPLS High Availability Command Changes

MPLS Replacement Commands for Tag-Switching Commands

Starting with Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA and 12.2(33)SXH, all tag-switching commands are obsoleted and are replaced with MPLS command versions. When you enter an obsolte tag-switching command, such as **tag-switching ip**, you receive the following message:

```
% Command accepted but obsolete, unreleased, or unsupported; see documentation
```

Use the MPLS version of the command instead, such as **mpls ip.**

Support for the tag-switching versions of commands will cease in a future release.

Configuration files that use the tag-switching version of the commands continue to operate. However, running configurations will display the new MPLS versions of the commands.

New Command Defaults

Starting with Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA and 12.2(33)SXH, Label Distribution Protocol (LDP) is the default protocol. In other releases and trains, the default label distribution protocol is Tag Distribution Protocol (TDP). See the **mpls label protocol**(global configuration) command in the NSF/SSO—MPLS LDP and MPLS LDP Graceful Restart feature for more information.

MPLS MTU Command Changes

The **mpls mtu** command has changed over the course of the several releases, starting in Cisco IOS Release 12.2(25)S. This section documents the changes implemented in Cisco IOS Release 12.2(25)S. For information about the changes implemented in Cisco IOS Releases 12.2(27)SBC and later releases, see the MPLS MTU Command Changes feature.

In Cisco IOS Release 12.2(25)S, if the interface MTU is less than 1524 bytes, you can set the maximum MPLS MTU to 24 bytes more than the interface MTU. For example, if the interface MTU is set to 1510 bytes, then you can set the maximum MPLS MTU to 1534 bytes (1510 + 24).

Note Although you can set the MPLS MTU to a value greater than the MPLS MTU, it is recommended that you keep the MPLS MTU less than or equal to the interface MTU to prevent the hardware from dropping packets. A best practice is to set the interface MTU of the core-facing interface to a value greater than either the IP MTU or interface MTU of the edge-facing interface.

If the interface MTU is greater than or equal to 1524 bytes, then you can set the maximum MPLS MTU as high as the interface MTU. For example, if the interface MTU is set to 1600 bytes, then you can set the MPLS MTU to a maximum of 1600 bytes. If you set the MPLS MTU higher than the interface MTU, traffic is dropped.

For interfaces that do not allow you to configure the interface MTU value and the interface MTU is 1500 bytes, the MPLS MTU range is 64 to 1524 bytes.

If you upgrade to Cisco IOS Release 12.2(25)S from an earlier release and you have an MPLS MTU setting that does not conform to these guidelines, the MPLS MTU setting is not accepted by the system. If this happens, reconfigure the MPLS MTU setting to conform to the guidelines.

Deleted Commands

The following commands are no longer available in Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, and 12.2(33)SXH:

- **debug mpls adjacency**
- **debug mpls lfib cef**
- **debug mpls lfib enc**
- **debug mpls lfib lsp**
- **debug mpls lfib state**
- **debug mpls lfib struct**
- **debug mpls lfib fast-reroute**

Replaced Commands

The first table below lists the commands that use the term tag-switching. Starting with Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, and 12.2(33)SXH, these commands have been updated with MPLS terminology. Although the tag-switching versions of the commands are obsoleted, the tag-switching commands continue to work, but are not documented.

Please use the MPLS versions of the commands. If you issue a tag-switching command, you receive the following error:

```
% Command accepted but obsolete, unreleased, or unsupported; see documentation
```

For information about any of the MPLS commands in the two tables below, see the Cisco IOS Multiprotocol Label Switching Command Reference.

The table below alphabetically lists the MPLS commands used by the Cisco 7500 series routers that replaced the tag-switching commands.

Table 4 Cisco 7500 Series—MPLS Commands That Replaced Tag-Switching Commands

This MPLS Command Replaces	This Tag-Switching Command
debug mpls atm-cos	debug tag-switching atm-cos
debug mpls atm-ldp api	debug tag-switching atm-tdp api
debug mpls atm-ldp routes	debug tag-switching atm-tdp routes
debug mpls atm-ldp states	debug tag-switching atm-tdp states
debug mpls events	debug tag-switching events
debug mpls ldp advertisements	debug tag-switching tdp advertisements
debug mpls ldp bindings	debug tag-switching tdp bindings
debug mpls ldp messages	debug tag-switching tdp pies
debug mpls ldp peer state-machine	debug tag-switching tdp peer state-machine

This MPLS Command Replaces	This Tag-Switching Command
debug mpls ldp session io	debug tag-switching tdp session io
debug mpls ldp session state-machine	debug tag-switching tdp session state-machine
debug mpls ldp targeted-neighbors	debug tag-switching tdp directed-neighbors
debug mpls ldp transport connections	debug tag-switching tdp transport connections
debug mpls ldp transport events	debug tag-switching tdp transport events
debug mpls traffic-eng tunnels events	debug tag-switching tsp-tunnels events
debug mpls traffic-eng tunnels labels	debug tag-switching tsp-tunnels tagging
debug mpls traffic-eng tunnels signalling	debug tag-switching tsp-tunnels signalling
debug mpls xtagatm cross-connect	debug tag-switching xtagatm cross-connect
debug mpls xtagatm errors	debug tag-switching xtagatm errors
debug mpls xtagatm events	debug tag-switching xtagatm events
debug mpls xtagatm vc	debug tag-switching xtagatm vc
mpls atm control-vc	tag-switching atm control-vc
mpls atm cos	tag-switching atm cos
mpls atm disable-headend-vc	tag-switching atm disable-headend-vc
mpls atm multi-vc	tag-switching atm multi-vc
mpls atm vpi	tag-switching atm vpi
mpls atm vp-tunnel	tag-switching atm vp-tunnel
mpls cos-map	tag-switching cos-map
mpls ip (global configuration)	tag-switching ip (global configuration)
mpls ip (interface configuration)	tag-switching ip (interface configuration)
mpls ip default-route	tag-switching ip default-route
mpls ip propagate-ttl	tag-switching ip propagate-ttl
mpls label range	tag-switching tag-range downstream
mpls ldp advertise-labels	tag-switching advertise-tags
mpls ldp atm control-mode	tag-switching atm allocation-mode
mpls ldp atm vc-merge	tag-switching atm vc-merge
mpls ldp discovery	tag-switching tdp discovery

This MPLS Command Replaces	This Tag-Switching Command
mpls ldp holdtime	tag-switching tdp holdtime
mpls ldp maxhops	tag-switching atm maxhops
mpls mtu	tag-switching mtu
mpls prefix-map	tag-switching prefix-map
mpls request-labels for	tag-switching request-tags for
mpls traffic-eng tunnels	tag-switching tsp-tunnels
show mpls atm-ldp bindings	show tag-switching atm-tdp bindings
show mpls atm-ldp bindwait	show tag-switching atm-tdp bindwait
show mpls atm-ldp capability	show tag-switching atm-tdp capability
show mpls atm-ldp summary	show tag-switching atm-tdp summary
show mpls cos-map	show tag-switching cos-map
show mpls forwarding-table	show tag-switching forwarding-table show tag-switching forwarding vrf
show mpls interfaces	show tag-switching interfaces
show mpls ldp bindings	show tag-switching tdp bindings
show mpls ldp discovery	show tag-switching tdp discovery
show mpls ldp neighbors	show tag-switching tdp neighbors
show mpls ldp parameters	show tag-switching tdp parameters
show mpls prefix-map	show tag-switching prefix-map
show mpls traffic-eng tunnels	show tag-switching tsp-tunnels
tunnel mode mpls traffic-eng	tunnel mode tag-switching

The table below alphabetically lists the MPLS commands used by the Cisco 10000 series routers that replaced the tag-switching commands.

Table 5 Cisco 10000 Series—MPLS Commands That Replaced Tag-Switching Commands

This MPLS Command Replaces	This Tag-Switching Command
debug mpls events	debug tag-switching events
debug mpls ldp advertisements	debug tag-switching tdp advertisements
debug mpls ldp bindings	debug tag-switching tdp bindings

This MPLS Command Replaces	This Tag-Switching Command
debug mpls ldp messages	debug tag-switching tdp pies
debug mpls ldp peer state-machine	debug tag-switching tdp peer state-machine
debug mpls ldp session io	debug tag-switching tdp session io
debug mpls ldp session state-machine	debug tag-switching tdp session state-machine
debug mpls ldp targeted-neighbors	debug tag-switching tdp directed-neighbors
debug mpls ldp transport connections	debug tag-switching tdp transport connections
debug mpls ldp transport events	debug tag-switching tdp transport events
debug mpls traffic-eng tunnels events	debug tag-switching tsp-tunnels events
debug mpls traffic-eng tunnels labels	debug tag-switching tsp-tunnels tagging
debug mpls traffic-eng tunnels signalling	debug tag-switching tsp-tunnels signalling
mpls ip (global configuration)	tag-switching ip (global configuration)
mpls ip (interface configuration)	tag-switching ip (interface configuration)
mpls ip default-route	tag-switching ip default-route
mpls ip propagate-ttl	tag-switching ip propagate-ttl
mpls label range	tag-switching tag-range downstream
mpls ldp advertise-labels	tag-switching advertise-tags
mpls ldp discovery	tag-switching tdp discovery
mpls ldp holdtime	tag-switching tdp holdtime
mpls ldp maxhops	tag-switching atm maxhops
mpls mtu	tag-switching mtu
mpls prefix-map	tag-switching prefix-map
mpls request-labels for	tag-switching request-tags for
mpls traffic-eng tunnels	tag-switching tsp-tunnels
show mpls forwarding-table	show tag-switching forwarding-table show tag-switching forwarding vrf
show mpls interfaces	show tag-switching interfaces
show mpls ldp bindings	show tag-switching tdp bindings
show mpls ldp discovery	show tag-switching tdp discovery

This MPLS Command Replaces	This Tag-Switching Command
show mpls ldp neighbors	show tag-switching tdp neighbors
show mpls ldp parameters	show tag-switching tdp parameters
show mpls prefix-map	show tag-switching prefix-map
show mpls traffic-eng tunnels	show tag-switching tsp-tunnels
tunnel mode mpls traffic-eng	tunnel mode tag-switching

How to Configure MPLS High Availability Command Changes

There are no cofiguration tasks for this feature.

Configuration Examples for MPLS High Availability Command Changes

There are no configuration examples for this feature.

Additional References

The following sections provide references related to the MPLS High Availability feature.

Related Documents

Related Topic	Document Title
MPLS HA for VPNS	NSF/SSO-MPLS VPN
MPLS HA for LDP	NSF/SSO-MPLS LDP and MPLS LDP Graceful Restart
MPLS HA and other applications	MPLS High Availability: Overview
Stateful switchover	Stateful Switchover
MPLS Label Distribution Protocol	MPLS Label Distribution Protocol (LDP)
Cisco nonstop forwarding	Cisco Nonstop Forwarding
MPLS MTU command changes implemented in Cisco IOS Releases 12.2(27)SBC and later releases.	MPLS MTU Command Changes
Cisco IOS Release 12.4 commands	*Cisco IOS Multiprotocol Label Switching Command Reference*

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

RFC	Title
None	—

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

Feature Information for MPLS High Availability Command Changes

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

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

Table 6 Feature Information for MPLS High Availability: Command Changes

Feature Name	Releases	Feature Information
MPLS High Availability: Command Changes	12.2(25)S 12.2(28)SB 12.2(33)SRA 12.2(33)SXH	This feature explains the MPLS commands that have been modified for the MPLS High Availability feature. 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 router. In 12.2(33)SRA, support was added for the Cisco 7600 series router. In 12.2(33)SXH, this feature was integrated into Cisco IOS Release 12.2(33)SXH.

MPLS LDP Graceful Restart

When a router is configured with Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) Graceful Restart (GR), it assists a neighboring router that has MPLS LDP Stateful Switchover/Nonstop Forwarding (SSO/NSF) Support and Graceful Restart to recover gracefully from an interruption in service. In this Cisco IOS release, MPLS LDP GR functions strictly in helper mode, which means it can only help other routers that are enabled with MPLS SSO/NSF and GR to recover. If the router with LDP GR fails, its peer routers cannot help it recover.

Notes:

- MPLS LDP SSO/NSF Support and Graceful Restart is supported in Cisco IOS Release 12.2(25)S. For brevity, this feature is called LDP SSO/NSF in this document.
- The MPLS LDP GR feature described in this document refers to helper mode.

When you enable MPLS LDP GR on a router that peers with an MPLS LDP SSO/NSF-enabled router, the SSO/NSF-enabled router can maintain its forwarding state when the LDP session between them is interrupted. While the SSO/NSF-enabled router recovers, the peer router forwards packets using stale information. This enables the SSO/NSF-enabled router to become operational more quickly.

Finding Feature Information

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

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

Restrictions

- MPLS LDP GR is supported in strict helper mode.
- Tag Distribution Protocol (TDP) sessions are not supported. Only LDP sessions are supported.
- MPLS LDP GR cannot be configured on label-controlled ATM (LC-ATM) interfaces.
- MPLS LDP SSO/NSF is supported in IOS Release 12.2(25)S. It is not supported in this release.

Information About MPLS LDP Graceful Restart

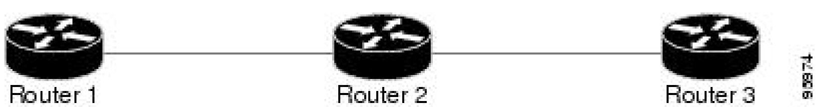
How MPLS LDP Graceful Restart Works

MPLS LDP GR works in strict helper mode, which means it helps a neighboring route processor that has MPLS LDP SSO/NSF to recover from disruption in service without losing its MPLS forwarding state. The disruption in service could be the result of a TCP or UDP event or the stateful switchover of a route processor. When the neighboring router establishes a new session, the LDP bindings and MPLS forwarding states are recovered.

In the topology shown in the figure below, the following elements have been configured:

- LDP sessions are established between Router 1 and Router 2, as well as between Router 2 and Router 3.
- Router 2 has been configured with MPLS LDP SSO/NSF. Routers 1 and 3 have been configured with MPLS LDP GR.
- A label switched path (LSP) has been established between Router 1 and Router 3.

Figure 1 Example of a Network Using LDP Graceful Restart



The following process shows how Routers 1 and 3, which have been configured with LDP GR help Router 2, which has been configured with LDP SSO/NSF recover from a disruption in service:

1. Router 1 notices an interruption in service with Router 2. (Router 3 also performs the same actions in this process.)
2. Router 1 marks all the label bindings from Router 2 as stale, but it continues to use the bindings for MPLS forwarding.

Router 1 reestablishes an LDP session with Router 2, but keeps its stale label bindings. If you issue a **show mpls ldp neighbor** command with the **graceful-restart** keyword, the command output displays the recovering LDP sessions.

1. Both routers readvertise their label binding information. If Router 1 relearns a label from Router 2 after the session has been established, the stale flags are removed. The **show mpls forwarding-table**command displays the information in the MPLS forwarding table, including the local label, outgoing label or VC, prefix, label-switched bytes, outgoing interface, and next hop.

You can set various graceful restart timers. See the following commands for more information:

- **mpls ldp graceful-restart timers neighbor-liveness**
- **mpls ldp graceful-restart timers max-recovery**

How a Route Processor Advertises That It Supports MPLS LDP Graceful Restart

A route processor that is configured to perform MPLS LDP GR includes the Fault Tolerant (FT) Type Length Value (TLV) in the LDP initialization message. The route processor sends the LDP initialization message to a neighbor to establish an LDP session.

The FT session TLV includes the following information:

- The Learn from Network (L) flag is set to 1, which indicates that the route processor is configured to perform MPLS LDP GR.
- The Reconnect Timeout field shows the time (in milliseconds) that the neighbor should wait for a reconnection if the LDP session is lost. In this release, the timer is set to 0, which indicates that if the local router fails, its peers should not wait for it to recover. The timer setting indicates that the local router is working in helper mode.
- The Recovery Time field shows the time (in milliseconds) that the neighbor should retain the MPLS forwarding state during a recovery. If a neighbor did not preserve the MPLS forwarding state before the restart of the control plane, the neighbor sets the recovery time to 0.

What Happens If a Route Processor Does Not Have LDP Graceful Restart

If two route processors establish an LDP session and one route processor is not configured for MPLS LDP GR, the two route processors create a normal LDP session but do not have the ability to perform MPLS LDP GR. Both route processors must be configured for MPLS LDP GR.

How to Configure MPLS LDP Graceful Restart

- Configuring MPLS LDP Graceful Restart, page 23
- Verifying the Configuration, page 25

Configuring MPLS LDP Graceful Restart

You must enable MPLS LDP GR on all route processors for an LDP session to be preserved during an interruption in service.

MPLS LDP GR is enabled globally. When you enable MPLS LDP GR, it has no effect on existing LDP sessions. New LDP sessions that are established can perform MPLS LDP GR.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef** [**distributed**]
4. **mpls ldp graceful-restart**
5. **interface** *type slot/port*
6. **mpls ip**
7. **mpls label protocol** {**ldp**| **tdp**| **both**}

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 (CEF).
Step 4	**mpls ldp graceful-restart** **Example:** `Router(config)# mpls ldp graceful-restart`	Enables the router to protect the LDP bindings and MPLS forwarding state during a disruption in service.
Step 5	**interface** *type slot/port* **Example:** `Router(config)# interface pos 3/0`	Specifies an interface and enters interface configuration mode.

	Command or Action	Purpose
Step 6	**mpls ip** **Example:** `Router(config-if)# mpls ip`	Configures MPLS hop-by-hop forwarding for an interface.
Step 7	**mpls label protocol** {**ldp**| **tdp**| **both**} **Example:** `Router(config-if)# mpls label protocol ldp`	Configures the use of LDP for an interface. You must use LDP.

Note You can also issue the **mpls label protocol ldp** command in global configuration mode, which enables LDP on all interfaces configured for MPLS.

Verifying the Configuration

The following commands help verify that MPLS LDP GR has been configured correctly:

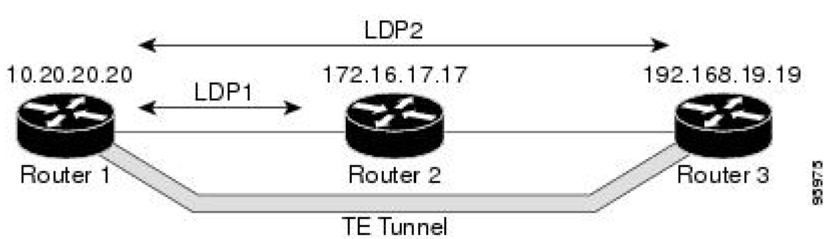
show mpls ldp neighbor with the **graceful-restart** keyword	Displays the Graceful Restart information for LDP sessions.
show mpls ldp graceful-restart	Displays Graceful Restart sessions and session parameters.

Configuration Example for MPLS LDP Graceful Restart

The figure below shows a configuration where MPLS LDP GR is enabled on Router 1 and MPLS LDP SSO/NSF is enabled on Routers 2 and 3. In this configuration example, Router 1 creates an LDP session with Router 2. Router 1 also creates a targeted session with Router 3 through a traffic engineering tunnel using Router 2.

Note MPLS LDP SSO/NSF is supported in Cisco IOS Release 12.2(25)S. It is not supported in this release.

Figure 2 ***MPLS LDP Graceful Restart Configuration Example***



Router 1 configured with LDP GR:

```
boot system slot0:rsp-pv-mz
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz
!
ip subnet-zero
ip cef
mpls label range 16 10000 static 10001 1048575
mpls label protocol ldp
mpls ldp logging neighbor-changes
mpls ldp graceful-restart
mpls traffic-eng tunnels
no mpls traffic-eng auto-bw timers frequency 0
mpls ldp router-id Loopback0 force
!
interface Loopback0
 ip address 20.20.20.20 255.255.255.255
 no ip directed-broadcast
 no ip mroute-cache
!
interface Tunnel1
 ip unnumbered Loopback0
 no ip directed-broadcast
 mpls label protocol ldp
 mpls ip
 tunnel destination 19.19.19.19
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth  500
 tunnel mpls traffic-eng path-option 1 dynamic
!
interface ATM5/1/0
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM5/1/0.5 point-to-point
 ip address 12.0.0.2 255.0.0.0
 no ip directed-broadcast
 no atm enable-ilmi-trap
 pvc 6/100
  encapsulation aal5snap
mpls label protocol ldp
mpls traffic-eng tunnels
mpls ip
ip rsvp bandwidth 1000
!
router ospf 100
 log-adjacency-changes
 redistribute connected
     network 12.0.0.0 0.255.255.255 area 100
 network 20.20.20.20 0.0.0.0 area 100
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 100
```

Router 2 configured with LDP SSO/NSF:

```
boot system slot0:rsp-pv-mz
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz
redundancy
  mode sso
!
ip cef
no ip domain-lookup
mpls label range 17 10000 static 10001 1048575
mpls label protocol ldp
```

```
mpls ldp logging neighbor-changes
mpls ldp graceful-restart
mpls traffic-eng tunnels
no mpls traffic-eng auto-bw timers frequency 0
no mpls advertise-labels
mpls ldp router-id Loopback0 force
!
interface Loopback0
 ip address 17.17.17.17 255.255.255.255
 no ip directed-broadcast
!
interface ATM4/0/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM4/0/0.5 point-to-point
 ip address 12.0.0.1 255.0.0.0
 no ip directed-broadcast
 no atm enable-ilmi-trap
 pvc 6/100
  encapsulation aal5snap
mpls label protocol ldp
mpls traffic-eng tunnels
mpls ip
ip rsvp bandwidth 1000
!
interface POS5/1/0
 ip address 11.0.0.1 255.0.0.0
 no ip directed-broadcast
 encapsulation ppp
 mpls label protocol ldp
 mpls traffic-eng tunnels
 mpls ip
 no peer neighbor-route
 clock source internal
 ip rsvp bandwidth 1000
!
router ospf 100
 log-adjacency-changes
 redistribute connected
 nsf enforce global
 network 11.0.0.0 0.255.255.255 area 100
 network 12.0.0.0 0.255.255.255 area 100
 network 17.17.17.17 0.0.0.0 area 100
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 100
!
ip classless
```

Router 3 configured with LDP SSO/NSF:

```
boot system slot0:rsp-pv-mz
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz
redundancy
  mode sso
!
ip subnet-zero
ip cef
!
no ip finger
no ip domain-lookup
mpls label protocol ldp
mpls ldp neighbor 11.11.11.11 targeted ldp
mpls ldp logging neighbor-changes
mpls ldp graceful-restart
mpls traffic-eng tunnels
```

```
no mpls traffic-eng auto-bw timers frequency 0
mpls ldp discovery directed-hello interval 12
mpls ldp discovery directed-hello holdtime 130
mpls ldp discovery directed-hello accept
mpls ldp router-id Loopback0 force
!
interface Loopback0
 ip address 19.19.19.19 255.255.255.255
 no ip directed-broadcast
!
interface POS1/0
 ip address 11.0.0.2 255.0.0.0
 no ip directed-broadcast
 encapsulation ppp
 mpls label protocol ldp
 mpls traffic-eng tunnels
 mpls ip
 no peer neighbor-route
 clock source internal
 ip rsvp bandwidth 1000
!
router ospf 100
 log-adjacency-changes
 redistribute connected
 nsf enforce global
network 11.0.0.0 0.255.255.255 area 100
network 19.19.19.19 0.0.0.0 area 100
mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 100
!
ip classless
```

Additional References

Related Documents

Related Topic	Document Title
MPLS Label Distribution Protocol	MPLS Label Distribution Protocol (LDP)

Standards

Standards	Title
None	—

MIBs

MIBs[1]	MIBs Link
• MPLS Label Distribution Protocol MIB Version 8 Upgrade	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

1 Not all supported MIBs are listed.

RFCs

RFCs[2]	Title
RFC 3036	*LDP Specification*
RFC 3478	*Graceful Restart Mechanism for Label Distribution*

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for MPLS LDP Graceful Restart

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

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

2 **Not all supported RFCs are listed.**

Table 7 Feature Information for MPLS LDP Graceful Restart

Feature Name	Releases	Feature Information
MPLS LDP Graceful Restart	12.0(29)S 12.3(14)T 12.2(33)SRA	MPLS LDP Graceful Restart assists a neighboring router that has MPLS LDP Stateful Switchover/Nonstop Forwarding (SSO/NSF) Support and Graceful Restart to recover gracefully from an interruption in service. In Cisco IOS Release 12.0(29)S, this feature was introduced. This feature was integrated into Cisco IOS Release 12.3(14)T. This feature was integrated into Cisco IOS Release 12.2(33)SRA. The following sections provide information about this feature: The following commands were introduced or modified: • **debug mpls ldp graceful-restart** • **mpls ldp graceful-restart** • **mpls ldp graceful-restart timers max-recovery** • **mpls ldp graceful-restart timers neighbor-liveness** • **show mpls ip binding** • **show mpls ldp bindings** • **show mpls ldp graceful-restart** • **show mpls ldp neighbor**

NSF SSO - MPLS LDP and LDP Graceful Restart

Cisco Nonstop Forwarding with Stateful Switchover provides continuous packet forwarding, even during a network processor hardware or software failure. In a redundant system, the secondary processor recovers control plane service during a critical failure in the primary processor. SSO synchronizes the network state information between the primary and the secondary processor.

Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) uses SSO, NSF, and graceful restart to allow a Route Processor to recover from disruption in control plane service (specifically, the LDP component) without losing its MPLS forwarding state. LDP NSF works with LDP sessions between directly connected peers and with peers that are not directly connected (targeted sessions).

Note In this document, the NSF/SSO - MPLS LDP and LDP Graceful Restart feature is called LDP NSF for brevity.

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 LDP and LDP Graceful Restart, page 43.

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.

Prerequisites for NSF SSO - MPLS LDP and LDP Graceful Restart

For information about supported hardware, see the release notes for your platform.

MPLS high availability (HA) requires that neighbor networking devices be NSF-aware.

To perform LDP NSF, Route Processors must be configured for SSO. See the Stateful Switchover feature module for more information:

You must enable nonstop forwarding on the routing protocols running between the provider (P) routers, provider edge (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)

See the Cisco Nonstop Forwarding feature module for more information.

Restrictions for NSF SSO - MPLS LDP and LDP Graceful Restart

LDP NSF has the following restrictions:

- Tag Distribution Protocol (TDP) sessions are not supported. Only LDP sessions are supported.
- LDP NSF cannot be configured on label-controlled ATM (LC-ATM) interfaces.

Information About NSF SSO - MPLS LDP and LDP Graceful Restart

To configure LDP NSF, you need to understand the following concepts:

- How NSF SSO - MPLS LDP and LDP Graceful Restart Works, page 32
- How a Route Processor Advertises That It Supports NSF SSO - MPLS LDP and LDP Graceful Restart, page 34
- Checkpointing, page 34

How NSF SSO - MPLS LDP and LDP Graceful Restart Works

LDP NSF allows a Route Processor to recover from disruption in service without losing its MPLS forwarding state. LDP NSF works under the following circumstances:

- LDP restart—An LDP Restart occurs after an SSO event interrupts LDP communication with all LDP neighbors. If the Route Processors are configured with LDP NSF, the backup Route Processor retains the MPLS forwarding state and reestablishes communication with the LDP neighbors. Then the Route Processor ensures that the MPLS forwarding state is recovered.
- LDP session reset—An LDP session reset occurs after an individual LDP session has been interrupted, but the interruption is not due to an SSO event. The LDP session might have been interrupted due to a

TCP or UDP communication problem. If the Route Processor is configured with MPLS LDP NSF support and graceful restart, the Route Processor associates a new session with the previously interrupted session. The LDP bindings and MPLS forwarding states are recovered when the new session is established.

If an SSO event occurs on an LSR, that LSR performs an LDP restart. The adjacent LSRs perform an LDP session reset.

See the following section for more information about LDP restart and reset.

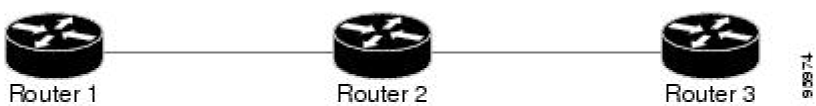
- What Happens During an LDP Restart and an LDP Session Reset, page 33

What Happens During an LDP Restart and an LDP Session Reset

In the topology shown in the figure below, the following elements have been configured:

- LDP sessions are established between Router 1 and Router 2, as well as between Router 2 and Router 3.
- A label switched path (LSP) has been established between Router 1 and Router 3.
- The routers have been configured with LDP NSF.

Figure 3 Example of a Network Using LDP Graceful Restart



The following process shows how LDP recovers when one of the routers fails:

1. When a Route Processor fails on Router 2, communications between the routers is interrupted.
2. Router 1 and Router 3 mark all the label bindings from Router 2 as stale, but they continue to use the bindings for MPLS forwarding.
3. Router 1 and Router 3 attempt to reestablish an LDP session with Router 2.
4. Router 2 restarts and marks all of its forwarding entries as stale. If you issue a **show mpls ldp graceful-restart** command, the command output includes the following line:

```
LDP is restarting gracefully.
```

1. Router 1 and Router 3 reestablish LDP sessions with Router 2, but they keep their stale label bindings. If you issue a show mpls ldp neighbor command with the **graceful-restart** keyword, the command output displays the recovering LDP sessions.
2. All three routers readvertise their label binding information. If a label has been relearned after the session has been established, the stale flags are removed. The **show mpls forwarding-table**command displays the information in the MPLS forwarding table, including the local label, outgoing label or VC, prefix, label-switched bytes, outgoing interface, and next hop.

You can set various timers to limit how long the routers wait for an LDP session to be reestablished before restarting the router. See the following commands for more information:

- **mpls ldp graceful-restart timers forwarding-holding**
- **mpls ldp graceful-restart timers max-recovery**
- **mpls ldp graceful-restart timers neighbor-liveness**

How a Route Processor Advertises That It Supports NSF SSO - MPLS LDP and LDP Graceful Restart

A Route Processor that is configured to perform LDP NSF includes the Fault Tolerant (FT) Type Length Value (TLV) in the LDP initialization message. The Route Processor sends the LDP initialization message to a neighbor to establish an LDP session.

The FT session TLV includes the following information:

- The Learn from Network (L) flag is set to 1, which indicates that the Route Processor is configured to perform LDP Graceful Restart.
- The Reconnect Timeout field shows the time (in milliseconds) that the neighbor should wait for a reconnection if the LDP session is lost. This field is set to 120 seconds and cannot be configured.
- The Recovery Time field shows the time (in milliseconds) that the neighbor should retain the MPLS forwarding state during a recovery. If a neighbor did not preserve the MPLS forwarding state before the restart of the control plane, the neighbor sets the recovery time to 0.

- What Happens if a Route Processor Does Not Have LDP Graceful Restart, page 34

What Happens if a Route Processor Does Not Have LDP Graceful Restart

If a Route Processor is not configured for MPLS LDP Graceful Restart and it attempts to establish an LDP session with a Route Processor that is configured with LDP Graceful Restart, the following events occur:

1. The Route Processor that is configured with MPLS LDP Graceful Restart sends an initialization message that includes the FT session TLV value to the Route Processor that is not configured with MPLS LDP Graceful Restart.
2. The Route Processor that is not configured for MPLS LDP Graceful Restart receives the LDP initialization message and discards the FT session TLV.
3. The two Route Processors create a normal LDP session but do not have the ability to perform MPLS LDP Graceful Restart.

You must enable all Route Processors with MPLS LDP Graceful Restart for an LDP session to be preserved during an interruption in service.

Checkpointing

Checkpointing is a function that copies state information from the active Route Processor to the backup Route Processor, thereby ensuring that the backup Route Processor has the latest information. If the active Route Processor fails, the backup Route Processor can take over.

For the LDP NSF feature, the checkpointing function copies the active Route Processor's LDP local label bindings to the backup Route Processor. The active Route Processor sends updates to the backup Route Processor when local label bindings are modified as a result of routing changes.

Note Local label bindings that are allocated by BGP and null local label bindings are not included in the checkpointing operation.

The checkpointing function is enabled by default.

To display checkpointing data, issue the **show mpls ldp graceful-restart** command on the active Route Processor.

To check that the active and backup Route Processors have identical copies of the local label bindings, you can issue the **show mpls ldp bindings** command with the **detail** keyword on the active and backup Route Processors. This command displays the local label bindings that have been saved. The active Route Processor and the backup Route Processor should have the same local label bindings.

- Troubleshooting Tips, page 35

Troubleshooting Tips

You can use the **debug mpls ldp graceful-restart** command to enable the display of MPLS LDP checkpoint events and errors.

How to Configure and Use NSF SSO - MPLS LDP and LDP Graceful Restart

- Configuring MPLS LDP Graceful Restart, page 35
- Verifying the Configuration, page 37

Configuring MPLS LDP Graceful Restart

MPLS LDP Graceful Restart (GR) is enabled globally. When you enable LDP GR, it has no effect on existing LDP sessions. LDP GR is enabled for new sessions that are established after the feature has been globally enabled.

- Route Processors must be configured for SSO. See the Stateful Switchover feature module for more information:
- You must enable Nonstop Forwarding on the routing protocols running between the P, PE, routers, and CE routers. See the Cisco Nonstop Forwarding feature module for more information.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef** [**distributed**]
4. **mpls ldp graceful-restart**
5. **interface** *type slot /port*
6. **mpls ip**
7. **mpls label protocol** {**ldp** | **tdp** | **both**}

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 distributed Cisco Express Forwarding on Cisco 7500 series routers. Distributes Cisco Express Forwarding information to line cards. **Note** For the Cisco 10000 series routers, IP Cisco Express Forwarding is on by default and it cannot be disabled.
Step 4	**mpls ldp graceful-restart** **Example:** `Router (config)# mpls ldp graceful-restart`	Enables the router to protect the LDP bindings and MPLS forwarding state during a disruption in service.
Step 5	**interface** *type slot /port* **Example:** `Router(config)# interface pos 3/0`	Specifies an interface and enters interface configuration mode.
Step 6	**mpls ip** **Example:** `Router(config-if)# mpls ip`	Configures MPLS hop-by-hop forwarding for an interface.
Step 7	**mpls label protocol** {**ldp** | **tdp** | **both**} **Example:** `Router(config-if)# mpls label protocol ldp`	Configures the use of LDP for an interface. You must use LDP. You can also issue the **mpls label protocol ldp** command in global configuration mode, which enables LDP on all interfaces configured for MPLS.

Verifying the Configuration

Use the following procedure to verify that MPLS LDP Graceful Restart has been configured correctly.

SUMMARY STEPS

1. **show mpls ldp graceful-restart**
2. **show mpls ldp neighbor graceful restart**
3. **show mpls ldp checkpoint**

DETAILED STEPS

Step 1 **show mpls ldp graceful-restart**

The command output displays Graceful Restart sessions and session parameters:

Example:

```
Router# show mpls ldp graceful-restart
LDP Graceful Restart is enabled
Neighbor Liveness Timer: 5 seconds
Max Recovery Time: 200 seconds
Down Neighbor Database (0 records):
Graceful Restart-enabled Sessions:
VRF default:
    Peer LDP Ident: 10.18.18.18:0, State: estab
    Peer LDP Ident: 10.17.17.17:0, State: estab
```

Step 2 **show mpls ldp neighbor graceful restart**

The command output displays the Graceful Restart information for LDP sessions:

Example:

```
Router# show mpls ldp neighbor graceful-restart
Peer LDP Ident: 10.20.20.20:0; Local LDP Ident 10.17.17.17:0
  TCP connection: 10.20.20.20.16510 - 10.17.17.17.646
  State: Oper; Msgs sent/rcvd: 8/18; Downstream
  Up time: 00:04:39
  Graceful Restart enabled; Peer reconnect time (msecs): 120000
Peer LDP Ident: 10.19.19.19:0; Local LDP Ident 10.17.17.17:0
  TCP connection: 10.19.19.19.11007 - 10.17.17.17.646
  State: Oper; Msgs sent/rcvd: 8/38; Downstream
  Up time: 00:04:30
  Graceful Restart enabled; Peer reconnect time (msecs): 120000
```

Step 3 **show mpls ldp checkpoint**

The command output displays the summary of the checkpoint information:

Example:

```
Router# show mpls ldp checkpoint
Checkpoint status: dynamic-sync
Checkpoint resend timer: not running
5 local bindings in add-skipped
9 local bindings in added
1 of 15+ local bindings in none
```

Configuration Examples for LDP NSF

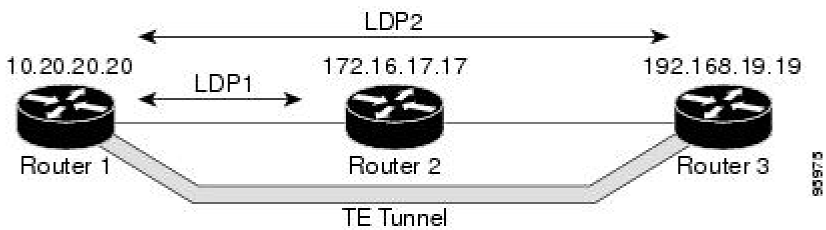
This section contains the following examples:

- Configuring NSF SSO - MPLS LDP and LDP Graceful Restart Example, page 38

Configuring NSF SSO - MPLS LDP and LDP Graceful Restart Example

The following configuration example shows the LDP NSF feature configured on three routers. (See the figure below.) In this configuration example, Router 1 creates an LDP session with Router 2. Router 1 also creates a targeted session with Router 3 through a TE tunnel using Router 2.

Figure 4 MPLS LDP: NSF/SSO Support and Graceful Restart Configuration Example



Router 1—Cisco 7500 Series

```
boot system slot0:rsp-pv-mz
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz
redundancy
mode sso
ip subnet-zero
ip cef
mpls label range 16 10000 static 10001 1048575
mpls label protocol ldp
mpls ldp logging neighbor-changes
mpls ldp graceful-restart
mpls traffic-eng tunnels
no mpls traffic-eng auto-bw timers frequency 0
mpls ldp router-id Loopback0 force
!
interface Loopback0
 ip address 172.20.20.20 255.255.255.255
 no ip directed-broadcast
 no ip mroute-cache
!
interface Tunnel1
 ip unnumbered Loopback0
 no ip directed-broadcast
 mpls label protocol ldp
 mpls ip
 tunnel destination 10.19.19.19
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth  500
 tunnel mpls traffic-eng path-option 1 dynamic
!
interface ATM5/1/0
```

```
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM5/1/0.5 point-to-point
 ip address 172.17.0.2 255.255.0.0
 no ip directed-broadcast
 no atm enable-ilmi-trap
 pvc 6/100
  encapsulation aal5snap
mpls label protocol ldp
mpls traffic-eng tunnels
mpls ip
ip rsvp bandwidth 1000
!
router ospf 100
 log-adjacency-changes
 redistribute connected
     nsf enforce global
     network 172.17.0.0 0.255.255.255 area 100
 network 172.20.20.20 0.0.0.0 area 100
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 100
```

Router 2—Cisco 7500 Series

```
boot system slot0:rsp-pv-mz
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz
redundancy
mode sso
!
ip cef
no ip domain-lookup
mpls label range 17 10000 static 10001 1048575
mpls label protocol ldp
mpls ldp logging neighbor-changes
mpls ldp graceful-restart
mpls traffic-eng tunnels
no mpls traffic-eng auto-bw timers frequency 0
no mpls advertise-labels
mpls ldp router-id Loopback0 force
!
interface Loopback0
 ip address 172.18.17.17 255.255.255.255
 no ip directed-broadcast
!
interface ATM4/0/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM4/0/0.5 point-to-point
 ip address 172.17.0.1 255.255.0.0
 no ip directed-broadcast
 no atm enable-ilmi-trap
 pvc 6/100
  encapsulation aal5snap
mpls label protocol ldp
mpls traffic-eng tunnels
mpls ip
ip rsvp bandwidth 1000
!
interface POS5/1/0
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
```

```
 encapsulation ppp
 mpls label protocol ldp
 mpls traffic-eng tunnels
 mpls ip
 no peer neighbor-route
 clock source internal
 ip rsvp bandwidth 1000
!
router ospf 100
 log-adjacency-changes
     nsf enforce global
 redistribute connected
 network 10.0.0.0 0.255.255.255 area 100
 network 172.17.0.0 0.255.255.255 area 100
 network 172.18.17.17 0.0.0.0 area 100
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 100
!
ip classless
```

Router 3—Cisco 7500 Series

```
boot system slot0:rsp-pv-mz
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz
redundancy
mode sso
!
ip subnet-zero
ip cef
!
no ip finger
no ip domain-lookup
mpls label protocol ldp
mpls ldp neighbor 10.11.11.11 targeted ldp
mpls ldp logging neighbor-changes
mpls ldp graceful-restart
mpls traffic-eng tunnels
no mpls traffic-eng auto-bw timers frequency 0
mpls ldp discovery directed-hello interval 12
mpls ldp discovery directed-hello holdtime 130
mpls ldp discovery directed-hello accept
mpls ldp router-id Loopback0 force
!
interface Loopback0
 ip address 172.19.19.19 255.255.255.255
 no ip directed-broadcast
!
interface POS1/0
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 encapsulation ppp
 mpls label protocol ldp
 mpls traffic-eng tunnels
 mpls ip
 no peer neighbor-route
 clock source internal
 ip rsvp bandwidth 1000
!
router ospf 100
 log-adjacency-changes
     nsf enforce global
 redistribute connected
 network 10.0.0.0 0.255.255.255 area 100
 network 172.19.19.19 0.0.0.0 area 100
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 100
!
ip classless
```

Router 1—Cisco 10000 Series

```
boot system flash:c10k2-p11-mz
redundancy
mode sso
ip subnet-zero
ip cef
mpls label protocol ldp
mpls ldp logging neighbor-changes
mpls ldp graceful-restart
no mpls traffic-eng auto-bw timers frequency 0
mpls ldp router-id Loopback0 force
!
interface Loopback0
 ip address 172.20.20.20 255.255.255.255
 no ip directed-broadcast
 no ip mroute-cache
!
interface ATM5/1/0
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM5/1/0.5 point-to-point
 ip address 172.18.0.2 255.255.0.0
 no ip directed-broadcast
 no atm enable-ilmi-trap
 pvc 6/100
  encapsulation aal5snap
mpls label protocol ldp
mpls ip
!
router ospf 100
 log-adjacency-changes
 redistribute connected
     nsf enforce global
     network 172.18.0.0 0.255.255.255 area 100
 network 172.20.20.20 0.0.0.0 area 100
```

Router 2—Cisco 10000 Series

```
boot system flash:c10k2-p11-mz
redundancy
mode sso
!
ip cef
no ip domain-lookup
mpls label protocol ldp
mpls ldp logging neighbor-changes
mpls ldp graceful-restart
no mpls traffic-eng auto-bw timers frequency 0
mpls ldp router-id Loopback0 force
!
interface Loopback0
 ip address 172.17.17.17 255.255.255.255
 no ip directed-broadcast
!
interface ATM4/0/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM4/0/0.5 point-to-point
 ip address 172.18.0.1 255.255.0.0
 no ip directed-broadcast
```

```
 no atm enable-ilmi-trap
 pvc 6/100
  encapsulation aal5snap
mpls label protocol ldp
mpls ip
!
interface POS5/1/0
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 encapsulation ppp
 mpls label protocol ldp
 mpls ip
 no peer neighbor-route
 clock source internal
!
router ospf 100
 log-adjacency-changes
     nsf enforce global
 redistribute connected
 network 10.0.0.0 0.255.255.255 area 100
 network 172.18.0.0 0.255.255.255 area 100
 network 172.17.17.17 0.0.0.0 area 100
 mpls traffic-eng router-id Loopback0
!
ip classless
```

Router 3—Cisco 10000 Series

```
boot system flash:c10k2-p11-mz
redundancy
mode sso
!
ip subnet-zero
ip cef
!
no ip finger
no ip domain-lookup
mpls label protocol ldp
mpls ldp logging neighbor-changes
mpls ldp graceful-restart
no mpls traffic-eng auto-bw timers frequency 0
mpls ldp router-id Loopback0 force
!
interface Loopback0
 ip address 172.19.19.19 255.255.255.255
 no ip directed-broadcast
!
interface POS1/0
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 encapsulation ppp
 mpls label protocol ldp
 mpls ip
 no peer neighbor-route
 clock source internal
!
router ospf 100
 log-adjacency-changes
     nsf enforce global
 redistribute connected
 network 10.0.0.0 0.255.255.255 area 100
 network 172.19.19.19 0.0.0.0 area 100
 mpls traffic-eng router-id Loopback0
!
ip classless
```

Additional References

Related Documents

Related Topic	Document Title
Stateful switchover	Stateful Switchover
MPLS Label Distribution Protocol	MPLS Label Distribution Protocol (LDP)
Cisco nonstop forwarding	Cisco Nonstop Forwarding

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
MPLS Label Distribution Protocol MIB Version 8 Upgrade	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

RFC	Title
RFC 3036	LDP Specification
RFC 3478	Graceful Restart Mechanism for Label Distribution

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

Feature Information for NSF SSO - MPLS LDP and LDP Graceful Restart

The table below 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.

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

Note The table below 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 8 Feature Information for NSF/SSO - MPLS LDP and LDP Graceful Restart

Feature Name	Releases	Feature Information
NSF/SSO - MPLS LDP and LDP Graceful Restart	12.2(25)S 12.2(28)SB 12.2(33)SRA 12.2(33)SXH	LDP NSF allows a Route Processor to recover from disruption in service without losing its MPLS forwarding state. In 12.2(25)S, this feature was introduced on Cisco 7500 series routers. In 12.2(28)SB, this feature was integrated into Cisco IOS Release 12.2(28)SB and implemented on Cisco 10000 series routers. In 12.2(33)SRA, this feature was integrated into Cisco IOS Release 12.2(33)SRA. In 12.2(33)SXH, this feature was integrated into Cisco IOS Release 12.2(33)SXH. The following commands are introduced or modified in the feature or features documented in this module. • **debug mpls ldp graceful-restart** • **mpls label protocol (global configuration)** • **mpls ldp graceful-restart** • **mpls ldp graceful-restart timers forwarding-holding** • **mpls ldp graceful-restart timers max-recovery** • **mpls ldp graceful-restart timers neighbor-liveness** • **show mpls ip binding** • **show mpls ldp bindings** • **show mpls ldp checkpoint** • **show mpls ldp graceful-restart** • **show mpls ldp neighbor**

AToM Graceful Restart

The AToM Graceful Restart feature assists neighboring routers that have nonstop forwarding (NSF), stateful switchover (SSO) and graceful restart (GR) for Any Transport over MPLS (AToM) to recover gracefully from an interruption in service. AToM GR functions strictly in helper mode, which means it helps other routers that are enabled with the NSF/SSO: Any Transport over MPLS and AToM Graceful Restart feature to recover. If the router with AToM GR fails, its peers cannot help it recover. AToM GR is based on the MPLS Label Distribution Protocol (LDP) Graceful Restart feature.

Keep the following points in mind when reading this document:

- The AToM GR feature described in this document refers to helper mode.
- The NSF/SSO: Any Transport over MPLS and AToM Graceful Restart feature is supported in Cisco IOS Releases 12.2(25)S and 12.2(33)SRA. For brevity, the NSF/SSO: Any Transport over MPLS and AToM Graceful Restart feature is called AToM SSO/NSF in this document.

Finding Feature Information

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

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

Information About AToM Graceful Restart

How AToM Graceful Restart Works

AToM GR works in strict helper mode, which means it helps a neighboring route processor that has AToM NSF/SSO to recover from a disruption in service without losing its MPLS forwarding state. The disruption in service could result from a TCP or User Datagram Protocol (UDP) event or the stateful switchover of a route processor. AToM GR is based on the MPLS LDP Graceful Restart feature, which preserves forwarding information for AToM circuits during an LDP session interruption. When the neighboring router establishes a new session, the LDP bindings and MPLS forwarding state are recovered. For more information related to how the LDP Graceful Restart feature works, see the MPLS LDP Graceful Restart feature module.

How to Configure AToM Graceful Restart

- Configuring AToM Graceful Restart, page 48

Configuring AToM Graceful Restart

There is no AToM-specific configuration for AToM GR. You enable LDP GR to assist a neighboring router configured with AToM NSF/SSO to maintain its forwarding state while the LDP session is disrupted.

- See the MPLS LDP Graceful Restart document for information about how LDP GR works and how you can customize it for your network.
- Configure AToM. For information about setting up or configuring AToM, see the Any Transport over MPLS document.

Note

- AToM GR is supported in strict helper mode.
- AToM NSF/SSO is supported in Cisco IOS Release 12.2(25)S and 12.2(33)SRA.
- Tag Distribution Protocol (TDP) sessions are not supported. Only LDP sessions are supported.
- MPLS LDP GR cannot be configured on label-controlled ATM (LC-ATM) interfaces.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef** [**distributed**]
4. **mpls ldp graceful-restart**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
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.
Step 4	**mpls ldp graceful-restart** **Example:** `Router(config)# mpls ldp graceful-restart`	Enables the router to protect the LDP bindings and MPLS forwarding state during a disruption in service. AToM GR is enabled globally. When you enable AToM GR, it has no effect on existing LDP sessions. New LDP sessions that are established can perform AToM GR.

Configuration Examples for AToM Graceful Restart

- AToM Graceful Restart Configuration Example, page 49
- AToM Graceful Restart Recovering from an LDP Session Disruption Example, page 50

AToM Graceful Restart Configuration Example

The following example shows an Ethernet VLAN over MPLS configuration. PE1 is configured with AToM Graceful Restart. PE2 is configured with AToM NSF/SSO. The commands for configuring AToM GR and NSF/SSO are shown in bold.

PE1 with AToM GR	PE2 with AToM NSF/SSO
ip cef ! mpls label protocol ldp **mpls ldp graceful-restart** mpls ldp router-id Loopback0 ! pseudowire-class atom encapsulation mpls ! interface Loopback0 ip address 10.1.1.2 255.255.255.255 ! interface FastEthernet5/1/1 no ip address ! interface FastEthernet5/1/1.2 description “xconnect to PE2” encapsulation dot1Q 2 native xconnect 10.2.2.2 1002 pw-class mpls ! ! IGP for MPLS router ospf 10 log-adjacency-changes auto-cost reference-bandwidth 1000 network 10.1.1.2 10.0.0.0 area 0 network 10.1.1.0 10.0.0.255 area 0	**redundancy** **mode sso** ip cef ! mpls label protocol ldp **mpls ldp graceful-restart** mpls ldp router-id Loopback0 ! pseudowire-class atom encapsulation mpls ! interface Loopback0 ip address 10.2.2.2 255.255.255.255 ! interface Ethernet3/3 no ip address ! interface Ethernet3/3.2 description “xconnect to PE1” encapsulation dot1Q 2 xconnect 10.1.1.2 1002 pw-class mpls ! ! IGP for MPLS router ospf 10 log-adjacency-changes **nsf enforce global** auto-cost reference-bandwidth 1000 network 10.2.2.2 10.0.0.0 area 0 network 10.1.1.0 10.0.0.255 area 0

AToM Graceful Restart Recovering from an LDP Session Disruption Example

The following examples show the output of the **show mpls l2transport vc**command during normal operation and when an LDP session is recovering from a disruption.

The following example shows the status of the VC on PE1 with AToM GR during normal operation:

```
Router# show mpls l2transport vc
Local intf     Local circuit        Dest address    VC ID      Status
-------------  -------------------- --------------- ---------- ----------
Fa5/1/1.2      Eth VLAN 2           10.2.2.2         1002       UP
```

The following example shows the status of the VC on PE1 with AToM GR while the VC is recovering from an LDP session disruption. The forwarding state for the circuit remains as it was before the disruption.

```
Router# show mpls l2transport vc
Local intf     Local circuit        Dest address    VC ID      Status
-------------  -------------------- --------------- ---------- ----------
Fa5/1/1.2      Eth VLAN 2           10.2.2.2         1002       RECOVERING
```

The following example shows the status of the VC on PE1 with AToM GR after the LDP session disruption was cleared. The AToM label bindings were advertised within the allotted time and the status returned to UP.

```
Router# show mpls l2transport vc
Local intf     Local circuit        Dest address    VC ID      Status
-------------  -------------------- --------------- ---------- ----------
Fa5/1/1.2      Eth VLAN 2           10.2.2.2         1002       UP
```

The following example shows the detailed status of the VC on PE1 with AToM GR during normal operation:

```
Router# show mpls l2transport vc detail
```

```
Local interface: Fa5/1/1.2 up, line protocol up, Eth VLAN 2 up
  Destination address: 10.2.2.2, VC ID: 1002, VC status: up
    Preferred path: not configured
    Default path: active
    Tunnel label: imp-null, next hop point2point
    Output interface: Se4/0/3, imposed label stack {16}
  Create time: 1d00h, last status change time: 1d00h
  Signaling protocol: LDP, peer 10.2.2.2:0 up
    MPLS VC labels: local 21, remote 16
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description: "xconnect to PE2"
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 3466, send 12286
    byte totals:   receive 4322368, send 5040220
    packet drops:  receive 0, send 0
```

The following example shows the detailed status of the VC on PE1 with AToM GR while the VC is recovering.

```
Router# show mpls l2transport vc detail
Local interface: Fa5/1/1.2 up, line protocol up, Eth VLAN 2 up
  Destination address: 10.2.2.2, VC ID: 1002, VC status: recovering
    Preferred path: not configured
    Default path: active
    Tunnel label: imp-null, next hop point2point
    Output interface: Se4/0/3, imposed label stack {16}
  Create time: 1d00h, last status change time: 00:00:03
  Signaling protocol: LDP, peer 10.2.2.2:0 down
    MPLS VC labels: local 21, remote 16
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description: "xconnect to PE2"
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 20040, send 28879
    byte totals:   receive 25073016, send 25992388
    packet drops:  receive 0, send 0
```

Additional References

The following sections provide references related to AToM GR.

Related Documents

Related Topic	Document Title
MPLS LDP graceful restart	MPLS LDP Graceful Restart
Configuring AToM	Any Transport over MPLS
Nonstop forwarding and stateful switchover for AToM	NSF/SSO—Any Transport over MPLS and AToM Graceful Restart

Standards

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

MIBs

MIBs	MIBs Link
MPLS Label Distribution Protocol MIB Version 8 Upgrade	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 3036	*LDP Specification*
RFC 3478	*Graceful Restart Mechanism for Label Distribution*

Technical Assistance

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

Feature Information for AToM Graceful Restart

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

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

Table 9 Feature Information for AToM Graceful Restart

Feature Name	Releases	Feature Information
AToM Graceful Restart	12.0(29)S 12.2(33)SRA 12.4(11)T 12.2(33)SXH	In 12.0(29)S, this feature was introduced. In 12.2(33)SRA, support was added for the Cisco 7600 series routers. In 12.4(11)T, this feature was integrated into the release. In 12.2(33)SXH, this feature was integrated into the release.

NSF SSO—Any Transport over MPLS and AToM Graceful Restart

The NSF/SSO—Any Transport over MPLS and AToM Graceful Restart feature allows Any Transport over MPLS (AToM) to use Cisco nonstop forwarding (NSF), stateful switchover (SSO), and Graceful Restart (GR) to facilitate a Route Processor (RP) to recover from a disruption in control plane service without losing its Multiprotocol Label Switching (MPLS) forwarding state.

NSF with SSO is effective at increasing the availability of network services. Cisco NSF with SSO provides continuous packet forwarding, even during a network processor hardware or software failure. In a redundant system, the secondary processor recovers the control plane service during a critical failure in the primary processor. SSO synchronizes the network state information between the primary and the secondary processor.

Note In this document, the NSF/SSO—Any Transport over MPLS and AToM Graceful Restart feature is referred to as AToM NSF for brevity.

Finding Feature Information

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

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

Prerequisites for AToM NSF

Before you configure AToM NSF, ensure the following tasks are completed:

- AToM virtual circuits (VCs) are configured on the router. For information on configuring AToM, see the Any Transport over MPLS feature module. For configuring L2VPN Interworking, see the L2VPN Interworking feature module.
- SSO is configured on the Route Processors. For configuration information, see the Stateful Switchover feature module.
- Nonstop forwarding is configured on the routers. You must enable nonstop forwarding on the routing protocols running between the provider edge (PE) and customer edge (CE) routers. The routing protocols are Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS), and Border Gateway Protocol (BGP). For configuring nonstop forwarding, see the Cisco Nonstop Forwarding feature module.
- The routers must be configured to detect and interact with the neighbor routers in the MPLS high availibility (HA) environment. AToM NSF requires that neighbor networking devices be able to perform AToM GR. In Cisco IOS Releases 12.2(25)S and 12.2(28)SB, the Cisco 7200 and Cisco 7500 routers support AToM GR and can be used as neighbor networking devices. In Cisco IOS Release 12.2(33)SRC, the Cisco 7600 routers support AToM high availability HA and MPLS Label Distribution Protocol (LDP) GR.
- The Route Processors for SSO and GR are configured. For more information, see the Stateful Switchover feature module.
- NSF on the routing protocols running between the PE, and CE routers must be enabled. The routing protocols are as follows:
    - BGP
    - IS-IS
    - OSPF

For more information, see the Cisco Nonstop Forwarding feature module.

- Supported Hardware, page 56

Supported Hardware

For hardware requirements for this feature, see the following documents:

- For Cisco IOS Release 12.2(25)S, see the “Supported Hardware” section of the Cross-Platform Release Notes for Cisco IOS Release 12.2S.
- For Cisco IOS Release 12.2(28)SB, see the “Supported Hardware” section of the Cross-Platform Release Notes for Cisco IOS Release 12.2SB.
- For Cisco IOS Release 12.2(33)SRC, see the “Supported Hardware” section of the Release Notes for Cisco IOS Release 12.2SR for the Cisco 7600 Series Routers.

Restrictions for AToM NSF

- Tag Distribution Protocol (TDP) sessions are not supported. Only LDP sessions are supported.
- AToM NSF cannot be configured on label-controlled ATM (LC-ATM) interfaces.

- AToM NSF does not support Layer 2 Tunnel Protocol Version 3 (L2TPv3) Interworking; only AToM Layer 2 Virtual Private Network (L2VPN) Interworking is supported.
- AToM NSF interoperates with Layer 2 local switching. However, AToM NSF has no effect on interfaces configured for local switching.
- You must disable fair queueing on serial interfaces to allow distributed Cisco Express Forwarding to work on the interfaces.
- On Cisco 7500 series routers, distributed Cisco Express Forwarding is needed to support AToM NSF.
- The Cisco 7500 router does not support AToM Ethernet-VLAN interworking IP; however, AToM Ethernet-VLAN interworking Ethernet is supported.

Information About AToM NSF

How AToM NSF Works

AToM NSF improves the availability of the network of the service provider that uses AToM to provide Layer 2 VPN services. HA provides the ability to detect failures and handle them with minimal disruption to the service being provided. AToM NSF is achieved by SSO and NSF mechanisms. A standby RP provides control-plane redundancy. The control plane state and data plane provisioning information for the attachment circuits (ACs) and AToM pseudowires (PWs) are checkpointed to the standby RP to provide NSF for AToM L2VPNs.

AToM Information Checkpointing

Checkpointing is a function that copies state information from the active RP to the backup RP, thereby ensuring that the backup RP has the latest information. If the active RP fails, the backup RP can take over the copying of state information.

For the AToM NSF feature, the checkpointing function copies the active RP's information bindings to the backup RP. The active RP sends updates to the backup RP when information is modified.

To display checkpointing data, use the **show acircuit checkpoint**command on the active and backup RPs. The active and backup RPs have identical copies of the information.

Checkpointing Troubleshooting Tips

To help troubleshoot checkpointing errors, use the following commands:

- Use the **debug acircuit checkpoint** command to enable checkpointing debug messages for ACs.
- Use the **debug mpls l2transport checkpoint** command to enable checkpointing debug messages for AToM.
- Use the **debug vfi checkpoint** command to debug virtual forwarding instance (VFI) checkpointing events and errors.
- Use the **show acircuit checkpoint** command to display AC checkpoint information.

- Use the **show mpls l2transport checkpoint** command to display whether checkpointing is allowed, how many AToM VCs were bulk-synchronized (on the active RP), and how many AToM VCs have checkpoint data (on the standby RP).
- Use the **show mpls l2transport vc detail** command to display details of VC checkpointed information.
- Use the **show vfi checkpoint** command to display checkpointing information on a VFI.

ISSU Support

Beginning with Cisco IOS Release 12.2(33)SRC, AToM NSF supports the In Service Software Upgrade (ISSU) capability. Virtual Private LAN Services (VPLS) NSF/SSO and HA with ISSU work together to enable upgrades or downgrades of a Cisco IOS image without control and data plane outages. With ISSU, all message data structures that are used for checkpointing and exchanges between the active RP and standby RP are versioned.

The maximum transmission length (MTU) of checkpoint messages can be negotiated. The VPLS ISSU client transforms checkpoint messages by converting Source Specific Multicast (SSM) IDs and VFI IDs of an individual VFI to AC and PW, respectively.

Configuring MPLS LDP Graceful Restart

Before you configure AToM NSF, you need to configure MPLS LDP Graceful Restart.

MPLS LDP GR is enabled globally. When you enable LDP GR, it has no effect on existing LDP sessions. LDP GR is enabled for new sessions that are established after the feature has been globally enabled.

Perform this task to configure MPLS LDP GR.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef** [**distributed**]
4. **mpls ldp graceful-restart**
5. **interface** *type slot* / *port*
6. **mpls ip**
7. **mpls label protocol** {**ldp** | **tdp** | **both**}
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
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. **Note** In Cisco ASR 1000 Series Aggregation Services Routers, the **distributed** keyword is mandatory.
Step 4	**mpls ldp graceful-restart** **Example:** `Router(config)# mpls ldp graceful-restart`	Enables the router to protect LDP bindings and the MPLS forwarding state during service disruption.
Step 5	**interface** *type slot* / *port* **Example:** `Router(config)# interface pos 3/0`	Specifies an interface and enters interface configuration mode.
Step 6	**mpls ip** **Example:** `Router(config-if)# mpls ip`	Configures MPLS hop-by-hop forwarding for an interface.
Step 7	**mpls label protocol** {**ldp** | **tdp** | **both**} **Example:** `Router(config-if)# mpls label protocol ldp`	Configures the LDP on an interface. • You must use LDP, because TDP sessions are not supported. • You can also issue the **mpls label protocol ldp** command in global configuration mode, which enables LDP on all interfaces configured for MPLS.
Step 8	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.

Configuration Examples for AToM NSF

- Example Ethernet to VLAN Interworking with AToM NSF, page 60

Example Ethernet to VLAN Interworking with AToM NSF

The following example shows how to configure AToM NSF on two PE routers:

PE1

```
ip cef distributed
!
redundancy
mode sso
!
boot system flash disk2:rsp-pv-mz
!
mpls ldp graceful-restart
mpls ip
mpls label protocol ldp
mpls ldp router-id Loopback0 force
mpls ldp advertise-labels
!
pseudowire-class atom-eth
 encapsulation mpls
 interworking ethernet
!
interface Loopback0
 ip address 10.8.8.8 255.255.255.255
!
interface FastEthernet1/1/0
 xconnect 10.9.9.9 123 encap mpls pw-class
atom-eth
interface POS6/1/0
 ip address 10.1.1.1 255.255.255.0
 mpls ip
 mpls label protocol ldp
 clock source internal
 crc 32
!
interface Loopback0
 ip address 10.8.8.8 255.255.255.255
 no shutdown
!
router ospf 10
 nsf
 network 10.8.8.8 0.0.0.0 area 0
 network 19.1.1.1 0.0.0.0 area 0
```

PE2

```
ip cef distributed
!
redundancy
mode sso
!
boot system flash disk2:rsp-pv-mz
mpls ldp graceful-restart
mpls ip
mpls label protocol ldp
mpls ldp router-id Loopback0 force
mpls ldp advertise-labels
!
pseudowire-class atom-eth
 encapsulation mpls
 interworking eth
!
interface Loopback0
 ip address 10.9.9.9 255.255.255.255
!
interface FastEthernet3/0/0
 ip route-cache cef
!
interface FastEthernet3/0/0.3
 encapsulation dot1Q 10
 xconnect 10.8.8.8 123 encap mpls pw-class
atom-eth
interface POS1/0/0
 ip address 10.1.1.2 255.255.255.0
 mpls ip
 mpls label protocol ldp
 clock source internal
 crc 32
!
interface Loopback0
 ip address 10.9.9.9 255.255.255.255
!
router ospf 10
 nsf
 network 10.9.9.9 0.0.0.0 area 0
 network 10.1.1.2 0.0.0.0 area 0
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco IOS Multiprotocol Label Switching Command Reference	*Cisco IOS Multiprotocol Label Switching Command Reference*
Stateful switchover	Stateful Switchover
MPLS Label Distribution Protocol	MPLS Label Distribution Protocol (LDP)
Cisco nonstop forwarding	Cisco Nonstop Forwarding
Any Transport over MPLS	Any Transport over MPLS
L2VPN Interworking configuration	L2VPN Interworking

Standards

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

MIBs

MIBs	MIBs Link
MPLS Label Distribution Protocol MIB Version 8 Upgrade	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 3036	*LDP Specification*
RFC 3478	*Graceful Restart Mechanism for Label Distribution*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for AToM NSF

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

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

Table 10 Feature Information for AToM NSF Any Transport over MPLS and AToM Graceful Restart

Feature Name	Releases	Feature Information
AToM NSF	12.2(25)S 12.2(28)SB 12.2(33)SRC	This feature uses NSF, SSO, and Graceful Restart to allow a Route Processor to recover from a disruption in control plane service without losing its MPLS forwarding state. In 12.2(25)S, this feature was introduced on the Cisco 7500 series router. In 12.2(28)SB, this feature was integrated into the release. In 12.2(33)SRC, this feature was integrated into the release for the Cisco 7600 router. Support for ISSU was added. The following commands were introduced or modified: **debug acircuit checkpoint, debug mpls l2transport checkpoint, show acircuit checkpoint, show mpls l2transport checkpoint, show mpls l2transport vc.**
AToM over MPLS	12.2(50)SY	The HA capabilities such as SSO and Non-Stop Forwarding to MPLS over AToM were added to the feature. The following commands were introduced or modified: **debug vfi checkpoint, show vfi checkpoint.**

NSF SSO - MPLS VPN

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

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

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

Prerequisites for NSF SSO - MPLS VPN

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

For information about supported hardware, see the release notes for your platform.

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 Configuring MPLS VPNs feature module.

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

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 (LDP) 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

Configuring NSF Support for Basic VPNs

Perform this task to configure NSF support for basic VPNs.

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 Configuring MPLS VPNs feature module.

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.

	Command or Action	Purpose
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	**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 Interfaces That Use BGP as the LDP

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.

- 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, page 68.

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.

	Command or Action	Purpose
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 and 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 Configuring MPLS VPNs feature module.

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:

Example:

```
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:

Example:

```
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:

Example:

```
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:

Example:

```
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 73
- NSF SSO - MPLS VPN for a CSC Network with a Customer ISP as Carrier Example, page 76
- NSF SSO - MPLS VPN for a CSC Network with a MPLS VPN Provider Example, page 81
- NSF SSO - MPLS VPN for a CSC Network with BGP to Distribute MPLS Labels Example, page 89
- NSF SSO - MPLS VPN for an Inter-AS Network with BGP to Distribute Routes and MPLS Labels Example, page 96
- NSF SSO - MPLS VPN for an Inter-AS Network That Uses BGP over a Non-MPLS VPN Service Provider Example, page 101

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.

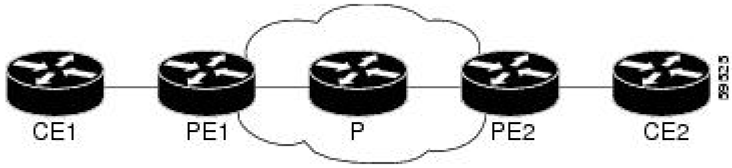
Enabling NSF on Both the Cisco 7500 Series and Cisco 10000 Series Routers

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.

The figure below shows the configuration of the NSF/SSO - MPLS VPN feature on the PE and CE routers.



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, page 74
- PE1 Router, page 74
- PE2 Router, page 75
- CE2 Router, page 76

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 ISP as Carrier 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 the figure below.

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

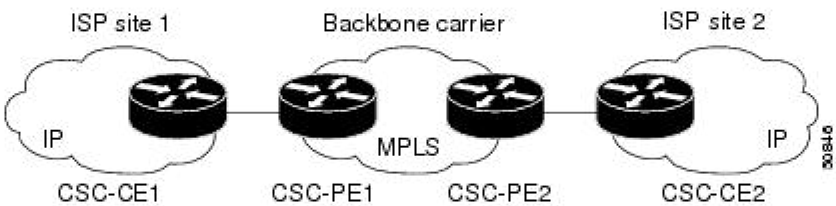
The SSO mode is enabled by default.

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.



- CSC-CE1 Configuration, page 77
- CSC-PE1 Configuration, page 78
- CSC-PE2 Configuration, page 79
- CSC-CE2 Configuration, page 80

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
```

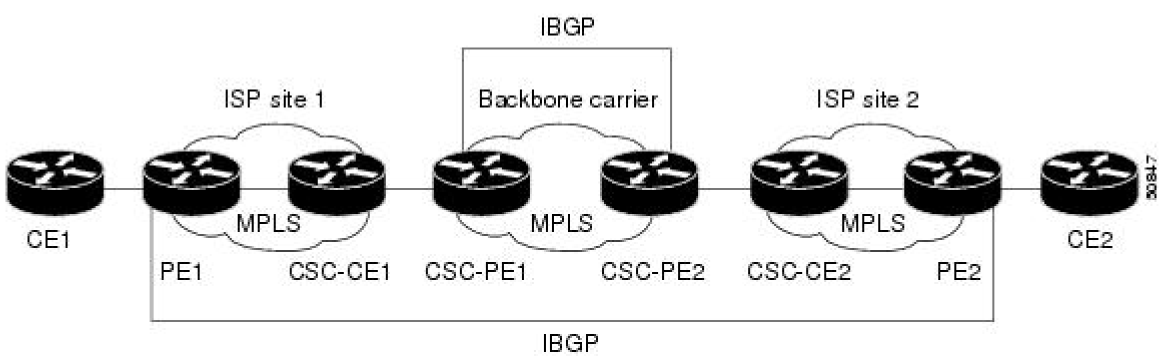
CSC-CE2 Configuration

```
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 MPLS VPN Provider Example

In the CSC network configuration shown in the figure below, 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.



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, page 82
- PE1 Configuration, page 83
- CSC-CE1 Configuration, page 84
- CSC-PE1 Configuration, page 84
- CSC-PE2 Configuration, page 85
- CSC-CE2 Configuration, page 87
- PE2 Configuration, page 87
- CE2 Configuration, page 88

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 with BGP to Distribute MPLS Labels Example

In the following example and in the figure below, 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

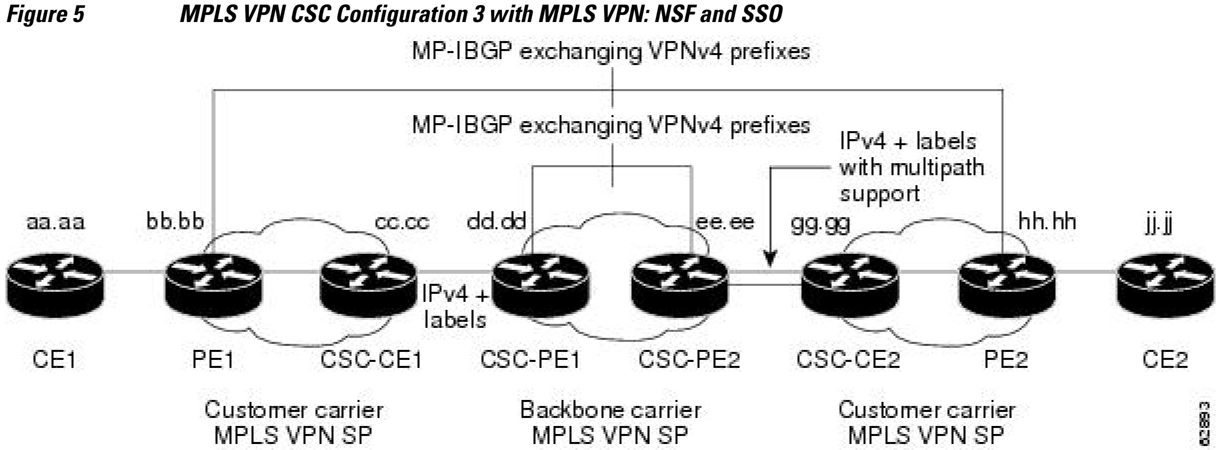
The following commands are used to enable NSF for the routing protocols, such as BGP and OSPF, and for the label distribution protocols, such as BGP and LDP:

- 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 the figure below 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 5 MPLS VPN CSC Configuration 3 with MPLS VPN: NSF and SSO



In the figure above, 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, page 90
- PE1 Configuration, page 90
- CSC-CE1 Configuration, page 91
- CSC-PE1 Configuration, page 92
- CSC-PE2 Configuration, page 93
- CSC-CE2 Configuration, page 94
- PE2 Configuration, page 95
- CE2 Configuration, page 95

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 with BGP to Distribute Routes and MPLS Labels Example

In the figure below 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.

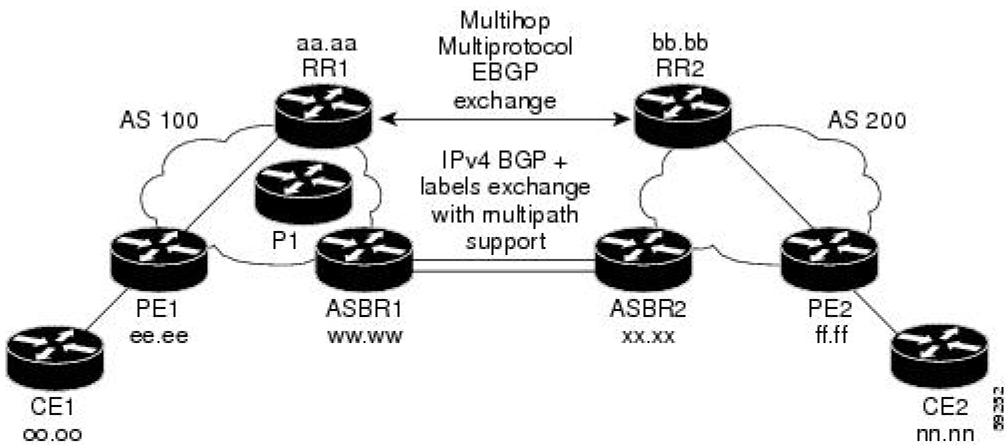
Enabling NSF on Both the Cisco 7500 Series and Cisco 10000 Series Routers

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.

The figure below shows two MPLS VPN service providers. They distribute VPNv4 addresses between the RRs and IPv4 routes and MPLS labels between ASBRs.



The figure above 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, page 97
- ASBR1 Configuration, page 98
- RR2 Configuration, page 99
- ASBR2 Configuration, page 100

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 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

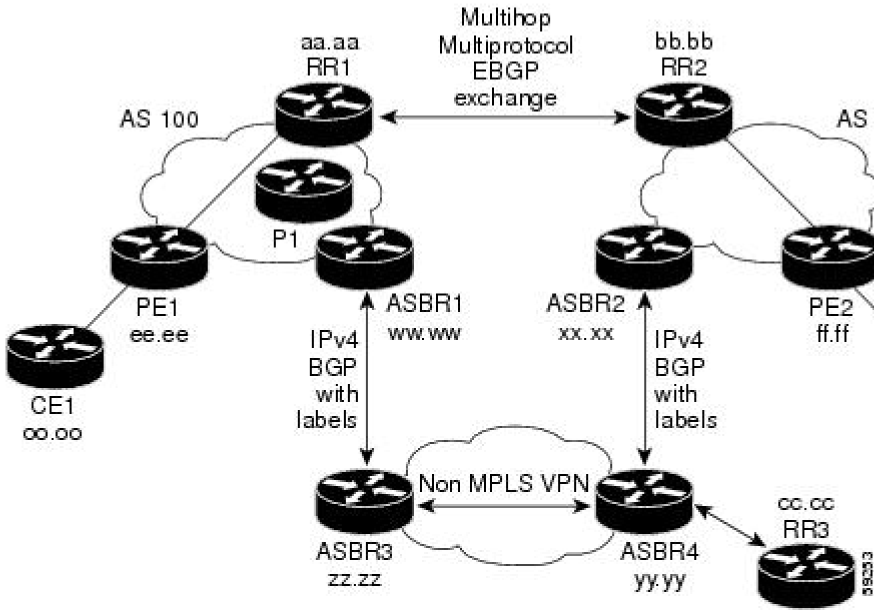
The SSO mode is enabled by default.

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

The figure below 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.



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
Nonstop forwarding for MPLS LDP	NSF/SSO-MPLS LDP and MPLS LDP Graceful Restart
Stateful awitchover	Stateful Switchover
Basic VPNs, MPLS VPN interautonomous systems, MPLS VPN Carrier Supporting Carrier	Configuring MPLS VPNs

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

Feature Information for NSF SSO - MPLS VPN

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

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

Table 11 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.

NSF SSO—MPLS TE and RSVP Graceful Restart

The NSF/SSO—MPLS TE and RSVP Graceful Restart feature allows a Route Processor (RP) to recover from disruption in control plane service without losing its Multiprotocol Label Switching (MPLS) forwarding state.

Cisco nonstop forwarding (NSF) with stateful switchover (SSO) provides continuous packet forwarding, even during a network processor hardware or software failure. In a redundant system, the secondary processor recovers control plane service during a critical failure in the primary processor. SSO synchronizes the network state information between the primary and the secondary processor.

In Cisco IOS Release 12.2(33)SRE, SSO can co-exist with traffic engineering (TE) primary tunnels, backup tunnels, and automesh tunnels.

Finding Feature Information

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

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

Prerequisites for NSF SSO—MPLS TE and RSVP Graceful Restart

- Configure Resource Reservation Protocol (RSVP) graceful restart in full mode.

If you have many tunnels/LSPs (100 or more) or if you have a large-scale network, the following configuration is recommended:

```
ip rsvp signalling refresh reduction
ip rsvp signalling rate-limit period 50 burst 16 maxsize 3000 limit 37
ip rsvp signalling patherr state-removal
ip rsvp signalling initial-retransmit-delay 15000
```

Additional info about these RSVP commands can be found in the Cisco IOS Quality of Service Command Reference .

- Configure RSVP graceful restart on all interfaces of the neighbor that you want to be restart-capable.
- Configure the redundancy mode as SSO. See Stateful Switchover .
- Enable NSF on the routing protocols running among the provider routers (P), provider edge (PE) routers, and customer edge (CE) routers. The routing protocols are as follows:
    - Border Gateway Protocol (BGP)
    - Open Shortest Path First (OSPF)
    - Intermediate System-to-Intermediate System (IS-IS)

For more information, see Information about Cisco Nonstop Forwarding .

- Enable MPLS.
- Configure traffic engineering (TE).

Restrictions for NSF SSO—MPLS TE and RSVP Graceful Restart

- RSVP graceful restart supports node failure only.
- Unnumbered interfaces are not supported.
- You cannot enable RSVP fast reroute (FRR) hello messages and RSVP graceful restart on the same router.
- Configure this feature on Cisco 7600 series routers with dual RPs only.
- For releases prior to Cisco IOS Release 12.2(33)SRE, you cannot enable primary one-hop autotunnels, backup autotunnels, or autotunnel mesh groups on a router that is also configured with SSO and Route Processor Redundancy Plus (RPR+). This restriction does not prevent an MPLS TE tunnel that is automatically configured by TE autotunnel from being successfully recovered if any midpoint router along the label-switched path (LSP) of the router experiences an SSO. For Cisco IOS Release 12.2(33)SRE, go to the MPLS TE Autotunnel and SSO Coexistence, page 117.
- MPLS TE LSPs that are fast reroutable cannot be successfully recovered if the LSPs are FRR active and the Point of Local Repair (PLR) router experiences an SSO.
- When you configure RSVP graceful restart, you must use the neighbor's interface IP address.
- When SSO (stateful switchover) occurs on a router, the switchover process must complete before FRR (fast reroute) can complete successfully. In a testing environment, allow approximately 2 minutes for

TE SSO recovery to complete before manually triggering FRR. To check the TE SSO status, use the **show ip rsvp high-availability summary** command. Note the status of the HA state field.

- When SSO is in the process of completing, this field will display 'Recovering'.
- When the SSO process has completed, this field will display 'Active'.

Information About NSF SSO—MPLS TE and RSVP Graceful Restart

Overview of MPLS TE and RSVP Graceful Restart

RSVP graceful restart allows RSVP TE-enabled nodes to recover gracefully following a node failure in the network such that the RSVP state after the failure is restored as quickly as possible. The node failure may be completely transparent to other nodes in the network.

RSVP graceful restart preserves the label values and forwarding information and works with third-party or Cisco routers seamlessly.

RSVP graceful restart depends on RSVP hello messages to detect that a neighbor went down. Hello messages include Hello Request or Hello Acknowledgment (ACK) objects between two neighbors.

A node hello is transmitted when Graceful Restart is globally configured and the first LSP to the neighbor is created.

Interface Hello is an optional configuration. If the Graceful Restart Hello command is configured on an interface, the interface hello is considered to be an additional hello instance with the neighbor.

An interface hello for Graceful Restart is transmitted when all of the following conditions are met:

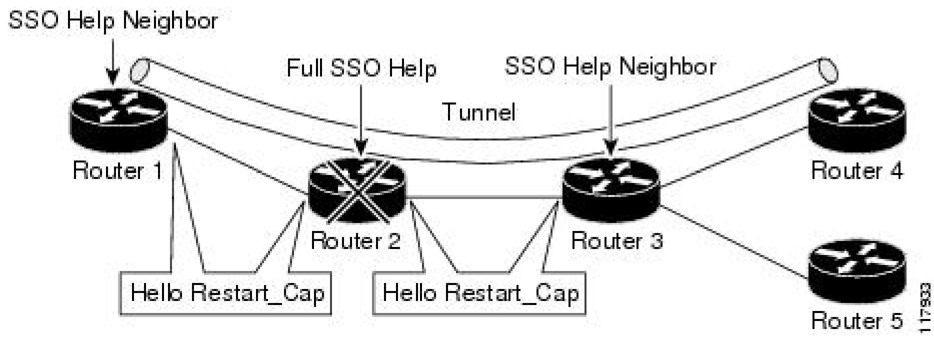
- Graceful Restart is configured globally.
- Graceful restart is configured on the interface.
- An LSP to the neighbor is created and goes over the interface.

Cisco recommends that you use node hellos if the neighbor supports node hellos, and configure interface hellos only if the neighbor router does not support node hellos.

Interface hellos differ from node hellos. as follows:

- **Interface hello** —The source address in the IP header of the hello message has an IP address that matches the interface that the Hello message sent out. The destination address in the IP header is the interface address of the neighbor on the other side of the link. A TTL of 1 is used for per-interface hellos as it is destined for the directly-connected neighbor.
- **Node hello** —The source address in the IP header of the Hello message includes the TE router ID of the sending router. The destination address of the IP header has the router ID of the neighbor to which this message is sent. A TTL of more than 1 is used.

As shown in the figure below, the RSVP graceful restart extension to these messages adds an object called Hello Restart_Cap, which tells neighbors that a node may be capable of recovering if a failure occurs.



The Hello Restart_Cap object has two values: the restart time, which is the sender's time to restart the RSVP_TE component and exchange hello messages after a failure; and the recovery time, which is the desired time that the sender wants the receiver to synchronize the RSVP and MPLS databases.

In the figure above, RSVP graceful restart help neighbor support is enabled on Routers 1 and 3 so that they can help a neighbor recover after a failure, but they cannot perform self recovery. Router 2 has full SSO help support enabled, meaning it can perform self recovery after a failure or help its neighbor to recover. Router 2 has two RPs, one that is active and one that is standby (backup). A TE LSP is signaled from Router 1 to Router 4.

Router 2 performs checkpointing; that is, it copies state information from the active RP to the standby RP, thereby ensuring that the standby RP has the latest information. If an active RP fails, the standby RP can take over.

Routers 2 and 3 exchange periodic graceful restart hello messages every 10,000 milliseconds (ms) (10 seconds), and so do Routers 2 and 1 and Routers 3 and 4. Assume that Router 2 advertises its restart time = 60,000 ms (60 seconds) and its recovery time = 60,000 ms (60 seconds) as shown in the following example:

```
23:33:36: Outgoing Hello:
23:33:36:   version:1 flags:0000 cksum:883C ttl:255 reserved:0 length:32
23:33:36:  HELLO                type HELLO REQUEST length 12:
23:33:36:   Src_Instance: 0x6EDA8BD7, Dst_Instance: 0x00000000
23:33:36:  RESTART_CAP          type 1 length 12:
23:33:36:   Restart_Time: 0x0000EA60, Recovery_Time: 0x0000EA60
```

Router 3 records this into its database. Also, both neighbors maintain the neighbor status as UP. However, Router 3's control plane fails at some point (for example, a primary RP failure). As a result, RSVP and TE lose their signaling information and states although data packets continue to be forwarded by the line cards.

When Router 3 declares communication with Router 2 lost, Router 3 starts the restart time to wait for the duration advertised in Router 2's restart time previously recorded (60 seconds). Routers 1 and 2 suppress all RSVP messages to Router 3 except hellos. Router 3 keeps sending the RSVP PATH and RESV refresh messages to Routers 4 and 5 so that they do not expire the state for the LSP; however, Routers 1 and 3 suppress these messages for Router 2.

When Routers 1 and 3 receive the hello message from Router 2, Routers 1 and 3 check the recovery time value in the message. If the recovery time is 0, Router 3 knows that Router 2 was not able to preserve its forwarding information, and Routers 1 and 3 delete all RSVP state that they had with Router 2.

If the recovery time is greater than 0, Router 1 sends Router 2 PATH messages for each LSP that it had previously sent through Router 2. If these messages were previously refreshed in summary messages, they are sent individually during the recovery time. Each of these PATH messages includes a Recovery_Label object containing the label value received from Router 2 before the failure.

When Router 3 receives a PATH message from Router 2, Router 3 sends a RESV message upstream. However, Router 3 suppresses the RESV message until it receives a PATH message. When Router 2 receives the RESV message, it installs the RSVP state and reprograms the forwarding entry for the LSP.

MPLS TE Autotunnel and SSO Coexistence

In Cisco IOS 12.2(33)SRE and later releases, MPLS TE primary tunnels, backup tunnels, and automesh tunnels can coexist with SSO; that is, they can be configured together. However, there are the following functional differences:

- Headend autotunnels created on the active RP are not checkpointed and created on the standby RP.
- After the SSO switchover, the new active RP recreates all the headend autotunnels and signals their LSPs. The LSP ID is different from the LSP ID used before the SSO switchover. Tunnel traffic may be dropped during the signaling of new autotunnel LSPs.
- SSO coexistence does not affect TE autotunnels in the midpoint or tailend routers along the LSPs from being checkpointed and recovered.

Benefits of MPLS TE and RSVP Graceful Restart

State Information Recovery

RSVP graceful restart allows a node to perform self recovery or to help its neighbor recover state information when there is an RP failure or the device has undergone an SSO.

Session Information Recovery

RSVP graceful restart allows session information recovery with minimal disruption to the network.

Increased Availability of Network Services

A node can perform a graceful restart to help itself or a neighbor recover its state by keeping the label bindings and state information, thereby providing a faster recovery of the failed node and not affecting currently forwarded traffic.

How to Configure NSF SSO—MPLS TE and RSVP Graceful Restart

Enabling RSVP Graceful Restart Globally

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rsvp signalling hello graceful-restart mode** (**help-neighbor**| **full**)
4. **exit**

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 rsvp signalling hello graceful-restart mode** (**help-neighbor**| **full**) **Example:** `Router(config)# ip rsvp signalling hello graceful-restart mode full`	Enables RSVP TE graceful restart capability on an RP. • Enter the **help-neighbor** keyword to enable a neighboring router to restart after a failure. • Enter the **full**keyword to enable a router to perform self recovery or to help a neighbor recover after a failure.
Step 4	**exit** **Example:** `Router(config)# exit`	(Optional) Returns to privileged EXEC mode.

Note

If you have many tunnels/LSPs (100 or more) or if you have a large-scale network, the following configuration is recommended:

```
ip rsvp signalling refresh reduction
ip rsvp signalling rate-limit period 50 burst 16 maxsize 3000 limit 37
ip rsvp signalling patherr state-removal
ip rsvp signalling initial-retransmit-delay 15000
```

Enabling RSVP Graceful Restart on an Interface

Note You must repeat this procedure for each of the neighbor router's interfaces.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. Repeat Step 3 as needed to configure additional interfaces.
5. **ip rsvp signalling hello graceful-restart neighbor** *ip-address*
6. Repeat Step 5 as needed to configure additional IP addresses on a neighbor router's interfaces.
7. **exit**

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	**interface** *type number* **Example:** `Router(config)# interface POS 1/0/0`	Configures the interface type and number and enters interface configuration mode.
Step 4	Repeat Step 3 as needed to configure additional interfaces.	(Optional) Configures additional interfaces.
Step 5	**ip rsvp signalling hello graceful-restart neighbor** *ip-address* **Example:** `Router(config-if)# ip rsvp signalling hello graceful-restart neighbor 10.0.0.0`	Enables support for RSVP graceful restart on routers helping their neighbors recover TE tunnels following SSO. **Note** The IP address must be that of the neighbor's interface.

	Command or Action	Purpose
Step 6	Repeat Step 5 as needed to configure additional IP addresses on a neighbor router's interfaces.	(Optional) Configures additional IP addresses on a neighbor router's interfaces.
Step 7	**exit** **Example:** `Router(config-if)# exit`	(Optional) Returns to privileged EXEC mode.

Setting a DSCP Value

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rsvp signalling hello graceful-restart dscp num**
4. **exit**

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 rsvp signalling hello graceful-restart dscp num** **Example:** `Router(config)# ip rsvp signalling hello graceful-restart dscp 30`	Sets a DSCP value on a router with RSVP graceful restart enabled.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Router(config)# exit`	(Optional) Returns to privileged EXEC mode.

Setting a Value to Control the Hello Refresh Interval

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rsvp signalling hello graceful-restart refresh interval** *interval-value*
4. **exit**

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 rsvp signalling hello graceful-restart refresh interval** *interval-value* **Example:** `Router(config)#` **ip rsvp signalling hello graceful-restart refresh interval** *5000*	Sets the value to control the request interval in graceful restart hello messages. This interval represents the frequency at which RSVP hello messages are sent to a neighbor; for example, one hello message is sent per each interval. **Note** If you change the default value for this command and you also changed the RSVP refresh interval using the **ip rsvp signalling refresh interval** command, ensure that the value for the **ip rsvp signalling hello graceful-restart refresh interval**command **is less than the value for the ip rsvp signalling hello refresh interval** command. Otherwise, some or all of the label-switched paths (LSPs) may not be recovered after an SSO has occurred.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Router(config)# exit`	(Optional) Returns to privileged EXEC mode.

Setting a Value to Control the Missed Refresh Limit

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rsvp signalling hello graceful-restart refresh misses** *msg-count*
4. **exit**

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 rsvp signalling hello graceful-restart refresh misses** *msg-count* **Example:** `Router(config)#` **ip rsvp signalling hello graceful-restart refresh misses** *5*	Specifies how many sequential RSVP TE graceful restart hello acknowledgments (ACKs) a node can miss before the node considers communication with its neighbor lost. **Note** If you change the default value for this command and you are also using the **ip rsvp signalling hello refresh misses**command, ensure that the value for the **ip rsvp signalling hello graceful-restart refresh misses**command **is less than the value for the ip rsvp signalling hello refresh misses** command. Otherwise, some or all of the LSPs may not be recovered after an SSO has occurred.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Router(config)# exit`	(Optional) Returns to privileged EXEC mode.

Verifying the RSVP Graceful Restart Configuration

SUMMARY STEPS

1. **enable**
2. **show ip rsvp hello graceful-restart**
3. **exit**

DETAILED STEPS

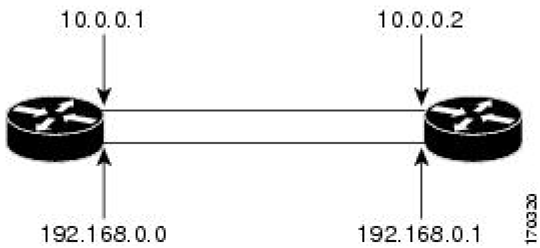
	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Optional) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip rsvp hello graceful-restart** **Example:** `Router#` **show ip rsvp hello graceful-restart**	Displays information about the status of RSVP graceful restart and related parameters.
Step 3	**exit** **Example:** `Router# exit`	(Optional) Returns to user EXEC mode.

Configuration Examples for NSF SSO—MPLS TE and RSVP Graceful Restart

- Configuring NSF SSO—MPLS TE and RSVP Graceful Restart Example, page 124
- Verifying the NSF SSO—MPLS TE and RSVP Graceful Restart Configuration Example, page 124

Configuring NSF SSO—MPLS TE and RSVP Graceful Restart Example

In the following example, RSVP graceful restart is enabled globally and on a neighbor router's interfaces as shown in the figure below. Related parameters, including a DSCP value, a refresh interval, and a missed refresh limit are set.




```
enable
configure terminal
ip rsvp signalling hello graceful-restart mode full
interface POS 1/0/0
 ip rsvp signalling hello graceful-restart neighbor 10.0.0.1
 ip rsvp signalling hello graceful-restart neighbor 10.0.0.2
 exit
ip rsvp signalling hello graceful-restart dscp 30
ip rsvp signalling hello graceful-restart refresh interval 50000
ip rsvp signalling hello graceful-restart refresh misses 5
exit
```

Verifying the NSF SSO—MPLS TE and RSVP Graceful Restart Configuration Example

The following example verifies the status of RSVP graceful restart and the configured parameters:

```
Router# show ip rsvp hello graceful-restart
Graceful Restart: Enabled (full mode)
  Refresh interval: 10000 msecs
  Refresh misses: 4
  DSCP:0x30
  Advertised restart time: 30000 msecs
  Advertised recovery time: 120000 msecs
  Maximum wait for recovery: 3600000 msecs
```

Additional References

Related Documents

Related Topic	Document Title
RSVP commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
Quality of service (QoS) classification	Classification Overview

Related Topic	Document Title
QoS signalling	Signalling Overview
QoS congestion management	Congestion Management Overview
Stateful switchover	Stateful Switchover
Cisco nonstop forwarding	Information about Cisco Nonstop Forwarding
RSVP hello state timer	MPLS Traffic Engineering: RSVP Hello State Timer

Standards

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

MIBs

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

RFCs

RFC	Title
RFC 3209	RSVP-TE: Extensions to RSVP for LSP Tunnels
RFC 3473	*Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions*
RFC 4558	Node-ID Based Resource Reservation Protocol (RSVP) Hello: A Clarification Statement

Technical Assistance

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

Feature Information for NSF SSO—MPLS TE and RSVP Graceful Restart

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

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

Table 12 Feature Information for NSF/SSO—MPLS TE and RSVP Graceful Restart

Feature Name	Releases	Feature Information
NSF/SSO—MPLS TE and RSVP Graceful Restart	12.0(29)S 12.2(33)SRA 12.2(33)SRB 12.2(33)SXH 12.2(33)SRE	The NSF/SSO—MPLS TE and RSVP Graceful Restart feature allows an RP or its neighbor to recover from disruption in control plane service without losing its MPLS forwarding state. In Cisco IOS Release 12.0(29)S, this feature was introduced as MPLS Traffic Engineering—RSVP Graceful Restart and allowed a neighboring RP to recover from disruption in control plane service without losing its MPLS forwarding state. In Cisco IOS Release 12.2(33)SRA, this feature was integrated and new commands were added. In Cisco IOS Release 12.2(33)SRB, support was added for ISSU and SSO recovery of LSPs that include loose hops. In Cisco IOS Release 12.2(33)SXH, this feature was integrated. In Cisco IOS Release 12.2(33)SRE, SSO can coexist with primary tunnels, backup tunnels, and mesh tunnels.
MPLS TE— RSVP Graceful Restart and 12.0S—12.2S Interop	15.2(1)S	In Cisco IOS Release 15.2(1)S, this feature was integrated.
MPLS TE— Autotunnel/ Automesh SSO Coexistence	15.2(1)S	In Cisco IOS Release 15.2(1)S, this feature was integrated.

Glossary

DSCP —differentiated services code point. Six bits in the IP header, as defined by the IETF. These bits determine the class of service provided to the IP packet.

Fast Reroute —A mechanism for protecting MPLS traffic engineering (TE) LSPs from link and node failure by locally repairing the LSPs at the point of failure, allowing data to continue to flow on them while their headend routers attempt to establish end-to-end LSPs to replace them. FRR locally repairs the protected LSPs by rerouting them over backup tunnels that bypass failed links or nodes.

graceful restart —A process for helping an RP restart after a node failure has occurred.

headend —The router that originates and maintains a given LSP. This is the first router in the LSP's path.

hello instance —A mechanism that implements the RSVP hello extensions for a given router interface address and remote IP address. Active hello instances periodically send hello request messages, expecting Hello ACK messages in response. If the expected ACK message is not received, the active hello instance declares that the neighbor (remote IP address) is unreachable (that is, it is lost). This can cause LSPs crossing this neighbor to be fast rerouted.

IGP —Interior Gateway Protocol. Internet protocol used to exchange routing information within an autonomous system. Examples of common Internet IGPs include IGRP, OSPF, and RIP.

ISSU —In Service Software Upgrade. Software upgrade without service interruption.

label —A short, fixed-length data identifier that tells switching nodes how to forward data (packets or cells).

LSP —label switched path. A configured connection between two routers, in which MPLS is used to carry packets.

MPLS —Multiprotocol Label Switching. A method for forwarding packets (frames) through a network. MPLS enables routers at the edge of a network to apply labels to packets (frames). ATM switches or existing routers in the network core can switch packets according to the labels.

RSVP —Resource Reservation Protocol. A protocol that supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature (bandwidth, jitter, maximum burst, and so on) of the packet streams they want to receive.

state —Information that a router must maintain about each LSP. The information is used for rerouting tunnels.

tailend —The router upon which an LSP is terminated. This is the last router in the LSP's path.

TE —traffic engineering. The techniques and processes used to cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods had been used.

ISSU MPLS Clients

MPLS applications can be upgraded using the In Service Software Upgrade (ISSU) process and the enhanced Fast Software Upgrade (eFSU) process. Thus, MPLS applications are considered ISSU's MPLS clients. The ISSU process allows Cisco IOS software *at the router level* to be updated or otherwise modified while packet forwarding continues. *At the line-card level* , the eFSU process minimizes line-card downtime during such upgrades to between 30 and 90 seconds, by loading the new line-card image before the ISSU switchover occurs from the active to the standby Route Processor (RP).

Finding Feature Information

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

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

Prerequisites for ISSU MPLS Clients

Before you perform an upgrade, you need to verify that the clients you are concerned about are compatible with the intended switchover. Use the commands listed in the Verifying the ISSU Process for an MPLS Client, page 133 to determine compatibility.

The success performance of some clients in the upgraded network will depend upon their compatibility with other clients as described in the table below.

Table 13 MPLS Client Interdependencies

This client . . .	...can only work when this client is shown to be compatible
MPLS VPN	LSD Label Manager High Availability
LDP	LSD Label Manager High Availability
VRF (“Table ID”)	LSD Label Manager High Availability
LSD Label Manager High Availability	Base clients: Checkpointing and Redundancy Facility
MFI Pull	XDR
MFI Push	XDR
LSPV Push within OAM	XDR
TE	Base clients: • Checkpointing and Redundancy Facility • MPLS TE High Availability

Restrictions for ISSU MPLS Clients

Because line cards in the Cisco series 7600 routers do not support Minimum Disruption Restart (MDR), they reset when eFSU is performed. That causes IGP adjacencies to flap (adjacent routes are advertised as unavailable and then available again in quick sequence), bringing down the MPLS traffic engineering (TE) tunnels. Therefore, after an eFSU operation, it may take as long as two minutes for TE tunnels to be resignaled and reestablished.

For this reason, we recommend that before you begin eFSU you first disable Resource Reservation Protocol Graceful Restart (RSVP GR) full mode. If this mode is not disabled, RSVP can inadvertently delay the reestablishment of TE tunnels while it waits for the recovery of the preexisting TE tunnel state.

To see how long each line card will be placed out of service during the eFSU process, use the **show issu outage slot all** command as described in the Determining Impending Line-Card Outage Periods During an ISSU, page 132.

Information About ISSU MPLS Clients

This section provides information about upgrading MPLS-related applications through ISSU and eFSU. Those MPLS applications are considered ISSU’s MPLS “clients.”

For information on the entire ISSU and eFSU procedure, please see the document, Cisco IOS In Service Software Upgrade and Enhanced Fast Software Upgrade Process.

For information specific to eFSU on the Cisco 7600 series router, please refer to the “ISSU and eFSU on Cisco 7600 Series Routers” chapter in the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide*, Release 12.2SR.

• ISSU-Capable Protocols and Applications Clients, page 131

- ISSU-Capable MPLS Feature Sets, page 131

ISSU-Capable Protocols and Applications Clients

Protocols and applications that can be upgraded through the ISSU process are considered clients of ISSU. These include at least the following:

- Address Resolution Protocol (ARP)
- Asynchronous Transfer Mode (ATM)
- Cisco Express Forwarding
- Dynamic Host Configuration Protocol (DHCP)
- EtherChannel—port aggregration protocol (PagP) and Link Aggregration Control Protocol (LACP)
- Frame Relay (FR)
- Gateway Load Balancing Protocol (GLBP)
- High-Level Data Link Control (HDLC)
- Hot Standby Router Protocol (HSRP)
- IEEE 802.1x and 802.3af
- Internet Group Management Protocol (IGMP) snooping
- IP host
- Intermediate System-to-Intermediate System (IS-IS)
- Multiprotocol Label Switching (MPLS)
- PPP and Multilink PPP
- Port security
- Quality of service (QoS)
- Remote File System (RFS) versioning
- Simple Network Management Protocol (SNMP)
- Spanning Tree Protocol (STP)

ISSU-Capable MPLS Feature Sets

Within the MPLS technology, ISSU supports the following feature sets as clients:

- Label Distribution Protocol (LDP)
- MPLS Virtual Private Network (MPLS VPN)
- VPN routing and forwarding (VRF), also called the “Table ID” client
- Label Switching Database Label Manager for high availability, usually called “LSD Label Manager for HA”
- MPLS Forwarding Infrastructure Pull, called “MFI Pull”
- MPLS Forwarding Infrastructure Push, called “MFI Push”

Beginning with Cisco IOS Release 12.2(33)SRB1, the following MPLS features are also supported as ISSU clients:

- Label Switched Path Verification Push within Operation, Administration, and Management (OAM), called “LSPV Push”
- TE

How to Verify that an MPLS Client Can Support an In Service Software Upgrade

Determining Impending Line-Card Outage Periods During an ISSU

Perform this task to determining impending line-card outage periods during an ISSU.

During an ISSU, the router preloads line-card software onto line cards that support enhanced Fast Service Upgrade (eFSU). Then, when the switchover occurs between active and standby processors, the line cards that support eFSU are restarted with the new, preloaded software, which helps to minimize outage time during the upgrade. Line cards that do not support eFSU undergo a hard reset at switchover, and the software image is loaded after the line card is restarted.

Note For the complete task sequence that accomplishes ISSU and eFSU, please see the document entitled, Cisco IOS In Service Software Upgrade and Enhanced Fast Software Upgrade Process.

Ensure that you have successfully loaded new Cisco IOS software onto the standby processor as described in Cisco IOS In Service Software Upgrade and Enhanced Fast Software Upgrade Process.

SUMMARY STEPS

1. **enable**
2. **show issu outage slot** *all*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show issu outage slot** *all* **Example:** `Router# show issu outage slot all` **Example:**	Determines the maximum length of time each line card could be down when use of the **issu runversion** command will trigger eFSU.

- Examples, page 133

Examples

The following is sample output from the **show issu outage**command:

```
Router# show issu outage slot all

Slot # Card Type                              MDR Mode         Max Outage Time
------ ------------------------------------   -----------      ---------------
     1 CEF720 24 port 1000mb SFP              WARM_RELOAD       300 secs
     2 1-subslot SPA Interface Processor-600  WARM_RELOAD       300 secs
     3 4-subslot SPA Interface Processor-400  WARM_RELOAD       300 secs
```

4 2+4 port GE-WAN RELOAD 360 secs

The column “Max Outage Time” shows the longest downtime that should be expected for each of the four listed line card types:

Note When there is no eFSU to be performed, and only ISSU will result from the use of the **issu runversion**command, the MDR Mode column in this display shows “NSF_RELOAD” for each line card, to indicate that the line card will not be restarted during the upgrade and therefore will not experience any downtime.

If you happen to enter the **show issu outage**command outside of the ISSU command sequence, the MDR Mode column in this display shows “INVALID”.

Verifying the ISSU Process for an MPLS Client

Perform this task to verify that a particular MPLS client can be upgraded successfully during a particular ISSU session. The commands in this task also can be used to display other details about the ISSU MPLS clients, and should be entered in the order described.

SUMMARY STEPS

1. **enable**
2. **show issu clients**
3. **show issu sessions** *clientID*
4. **show issu negotiated version** *sessionID*
5. **show issu negotiated capability** *sessionID*
6. **show issu message types** *clientID*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show issu clients** **Example:** `Router# show issu clients`	Lists network applications and protocols currently supported by ISSU. You can use this command to discover the client ID that you will need to enter in Steps 3 and 6.
Step 3	**show issu sessions** *clientID* **Example:** `Router# show issu sessions 2002`	Tells whether a particular client is compatible with the intended upgrade. You can use this command to discover the session ID that you will need to enter in Steps 4 and 5.

Step 4	**show issu negotiated version** *sessionID*
	
	Example:
	
	`Router#`
	`show issu negotiated version 33`
		Displays details of the session's negotiated message version.

Step 5	**show issu negotiated capability** *sessionID*
	
	Example:
	
	`Router#`
	`show issu negotiated capability 33`
		Displays results of a negotiation about the client application's capabilities.

Step 6	**show issu message types** *clientID* **Example:** `Router# show issu message types 2002`	Displays the message formats ("types") and versions supported by the specified client.

Configuration Examples for ISSU MPLS Clients

To examine any ISSU client, you must specify its unique client ID when entering the **show issu sessions** command. If you do not already know that client ID, enter the **show issu clients**command in user EXEC or privileged EXEC mode. Each ISSU client on the network will then be listed, with its client ID and client name on the same line, as shown in the following example:

```
Router# show issu clients
Client_ID = 2,  Client_Name = ISSU Proto client,  Entity_Count = 1
Client_ID = 3,  Client_Name = ISSU RF,  Entity_Count = 1
Client_ID = 4,  Client_Name = ISSU CF client,  Entity_Count = 1
Client_ID = 5,  Client_Name = ISSU Network RF client,  Entity_Count = 1
Client_ID = 7,  Client_Name = ISSU CONFIG SYNC,  Entity_Count = 1
Client_ID = 8,  Client_Name = ISSU ifIndex sync,  Entity_Count = 1
Client_ID = 9,  Client_Name = ISSU IPC client,  Entity_Count = 1
Client_ID = 10,  Client_Name = ISSU IPC Server client,  Entity_Count = 1
```

```
Client_ID = 11,  Client_Name = ISSU Red Mode Client,  Entity_Count = 1
Client_ID = 12,  Client_Name = ISSU EHSA services client,  Entity_Count = 1
Client_ID = 100,  Client_Name = ISSU rfs client,  Entity_Count = 1
Client_ID = 110,  Client_Name = ISSU ifs client,  Entity_Count = 1
Client_ID = 1001,  Client_Name = OC3POS-6,  Entity_Count = 4
Client_ID = 1002,  Client_Name = C10K ATM,  Entity_Count = 1
Client_ID = 1003,  Client_Name = C10K CHSTM1,  Entity_Count = 1
Client_ID = 1004,  Client_Name = C10K CT3,  Entity_Count = 1
Client_ID = 1005,  Client_Name = C10K GE,  Entity_Count = 1
Client_ID = 1006,  Client_Name = C10K ET,  Entity_Count = 1
Client_ID = 1007,  Client_Name = C10K CHE1T1,  Entity_Count = 1
Client_ID = 1009,  Client_Name = C10K MFE,  Entity_Count = 1
Client_ID = 1010,  Client_Name = C10K APS,  Entity_Count = 1
Client_ID = 1013,  Client_Name = C10K CARD OIR,  Entity_Count = 1
Client_ID = 2002,  Client_Name = CEF Push ISSU client,  Entity_Count = 1
Client_ID = 2003,  Client_Name = ISSU XDR client,  Entity_Count = 1
Client_ID = 2004,  Client_Name = ISSU SNMP client,  Entity_Count = 1
Client_ID = 2005,  Client_Name = ISSU HDLC Client,  Entity_Count = 1
Client_ID = 2006,  Client_Name = ISSU QoS client,  Entity_Count = 1
Client_ID = 2007,  Client_Name = ISSU LSD Label Mgr HA Client,  Entity_Count = 1
Client_ID = 2008,  Client_Name = ISSU Tableid Client,  Entity_Count = 1
Client_ID = 2009,  Client_Name = ISSU MPLS VPN Client,  Entity_Count = 1
Client_ID = 2010,  Client_Name = ARP HA,  Entity_Count = 1
Client_ID = 2011,  Client_Name = ISSU LDP Client,  Entity_Count = 1
Client_ID = 2012,  Client_Name = ISSU HSRP Client,  Entity_Count = 1
Client_ID = 2013,  Client_Name = ISSU ATM Client,  Entity_Count = 1
Client_ID = 2014,  Client_Name = ISSU FR Client,  Entity_Count = 1
Client_ID = 2015,  Client_Name = ISSU REDSSOC client,  Entity_Count = 1
Client_ID = 2019,  Client_Name = ISSU TCP client,  Entity_Count = 1
Client_ID = 2020,  Client_Name = ISSU BGP client,  Entity_Count = 1
Client_ID = 2021,  Client_Name = XDR Int Priority ISSU client,  Entity_Count = 1
Client_ID = 2022,  Client_Name = XDR Proc Priority ISSU client,  Entity_Count = 1
Client_ID = 2023,  Client_Name = FIB HWIDB ISSU client,  Entity_Count = 1
Client_ID = 2024,  Client_Name = FIB IDB ISSU client,  Entity_Count = 1
Client_ID = 2025,  Client_Name = FIB HW subblock ISSU client,  Entity_Count = 1
Client_ID = 2026,  Client_Name = FIB SW subblock ISSU client,  Entity_Count = 1
Client_ID = 2027,  Client_Name = Adjacency ISSU client,  Entity_Count = 1
Client_ID = 2028,  Client_Name = FIB IPV4 ISSU client,  Entity_Count = 1
Client_ID = 2030,  Client_Name = MFI Pull ISSU client,  Entity_Count = 1
Client_ID = 2031,  Client_Name = MFI Push ISSU client,  Entity_Count = 1
Client_ID = 2051,  Client_Name = ISSU CCM Client,  Entity_Count = 1
Client_ID = 2052,  Client_Name = ISSU PPP SIP CCM Client,  Entity_Count = 1
Client_ID = 2053,  Client_Name = ISSU MPLS TE Client,  Entity_Count = 1
Client_ID = 2054,  Client_Name = ISSU process client,  Entity_Count = 1
Client_ID = 2089,  Client_Name = MPLS LSPV Push client,  Entity_Count = 1
.
.
.
.
Base Clients:
 Client_Name = ISSU Proto client
 Client_Name = ISSU RF
 Client_Name = ISSU CF client
 Client_Name = ISSU Network RF client
 Client_Name = ISSU CONFIG SYNC
 Client_Name = ISSU ifIndex sync
 Client_Name = ISSU IPC client
 Client_Name = ISSU IPC Server client
 Client_Name = ISSU Red Mode Client
 Client_Name = ISSU EHSA services client
 Client_Name = ISSU rfs client
Client_Name = ISSU ifs client
 Client_Name = ISSU EM client
 Client_Name = ISSU Platform Medialayer Client
 Client_Name = ISSU FM Client
 Client_Name = ISSU TCAM Manager Client
 Client_Name = ISSU L2 Cmn Client
 Client_Name = ISSU L3 Manager HA Client
 Client_Name = ISSU L3 Manager Client
 Client_Name = ISSU CFIB BASE Client
 Client_Name = ISSU PF CONFIG SYNC Client
 Client_Name = ISSU MLS CEF Client
 Client_Name = ISSU Cat6k Logger Client
```

Verifying the ISSU Process for an MPLS LDP Client Example

This example shows how to verify the ISSU process for an LDP client.

The first command shows you whether the LDP client's old and new software versions are compatible, and therefore are able to make use of the ISSU opportunity:

```
Router# show issu sessions 2011
---------------------------------------------------------------------
 Client_ID = 2011,  Entity_ID = 1 :
 *** Session_ID = 46,  Session_Name = LDP Session :
    Peer   Peer  Negotiate  Negotiated   Cap      Msg     Session
  UniqueID  Sid    Role       Result   GroupID  GroupID  Signature
     4       34   PRIMARY   COMPATIBLE    1        1         0
                           (no policy)
    Negotiation Session Info for This Message Session:
         Nego_Session_ID = 46
         Nego_Session_Name = LDP Session
         Transport_Mtu = 3948
```

Now you can take the session ID displayed in the previous command's output and enter it into the next command, in order to see the negotiated message version:

```
Router# show issu negotiated version 46
 Session_ID = 46 :
     Message_Type = 1,  Negotiated_Version = 2,  Message_MTU = 20
     Message_Type = 2,  Negotiated_Version = 2,  Message_MTU = 20
     Message_Type = 3,  Negotiated_Version = 2,  Message_MTU = 4
```

Next you can enter the same session ID into the following command to display the capability negotiation result:

```
Router# show issu negotiated capability 46
 Session_ID = 46 :
     Negotiated_Cap_Entry = 1
```

Finally, to see which message types and versions are supported by this particular client, you enter the client ID into the following command:

```
Router# show issu message types 2011
---------------------------------------------------------------------
 Client_ID = 2011,  Entity_ID = 1 :
    Message_Type = 1,  Version_Range = 2 ~ 2
          Message_Ver = 2,    Message_Mtu = 20
    Message_Type = 2,  Version_Range = 2 ~ 2
          Message_Ver = 2,    Message_Mtu = 20
    Message_Type = 3,  Version_Range = 2 ~ 2
          Message_Ver = 2,    Message_Mtu = 4
```

Verifying the ISSU Process for an MPLS VPN Client Example

This example shows how to verify the ISSU process for an MPLS VPN client.

The first command shows you whether the VPN client's old and new software versions are compatible, and therefore are able to make use of the ISSU opportunity:

```
Router# show issu sessions 2009
--------------------------------------------------------------------
Client_ID = 2009,  Entity_ID = 1 :
*** Session_ID = 39,  Session_Name = MPLS VPN ISSU Session :
   Peer   Peer  Negotiate  Negotiated   Cap      Msg     Session
 UniqueID  Sid    Role       Result   GroupID  GroupID  Signature
    3       33   PASSIVE   COMPATIBLE    1        1         0
                          (no policy)
   Negotiation Session Info for This Message Session:
        Nego_Session_ID = 39
        Nego_Session_Name = MPLS VPN ISSU Session
        Transport_Mtu = 3980
```

Now you can take the session ID displayed in the previous command's output and enter it into the next command, in order to see the negotiated message version:

```
Router# show issu negotiated version 39
Session_ID = 39 :
    Message_Type = 1,  Negotiated_Version = 1,  Message_MTU = 32
```

Next you can enter the same session ID into the following command to display the capability negotiation result:

```
Router# show issu negotiated capability 39
Session_ID = 39 :
Negotiated_Cap_Entry = 1
```

Finally,= to see which message types and versions are supported by this particular client, you enter the client ID into the following command:

```
Router# show issu message types 2009
--------------------------------------------------------------------
Client_ID = 2009,  Entity_ID = 1 :
   Message_Type = 1,  Version_Range = 1 ~ 1
         Message_Ver = 1,    Message_Mtu = 32
```

Verifying the ISSU Process for an MPLS VRF ("Table ID") Client Example

This example shows how to verify the ISSU process for an MPLS VRF ("Table ID") client.

The first command shows you whether the VRF client's old and new software versions are compatible, and therefore are able to make use of the ISSU opportunity:

```
Router# show issu sessions 2008
--------------------------------------------------------------------
 Client_ID = 2008,  Entity_ID = 1 :
 *** Session_ID = 19,  Session_Name = TABLEID ISSU CF :
    Peer   Peer  Negotiate  Negotiated   Cap      Msg     Session
  UniqueID  Sid    Role       Result   GroupID  GroupID  Signature
     4       13   PRIMARY   COMPATIBLE    1        1         0
                           (no policy)
    Negotiation Session Info for This Message Session:
         Nego_Session_ID = 19
         Nego_Session_Name = TABLEID ISSU CF
         Transport_Mtu = 3948
```

Now you can take the session ID displayed in the previous command's output and enter it into the next command, in order to see the negotiated message version:

```
Router# show issu negotiated version 19
 Session_ID = 19 :
```

```
     Message_Type = 1,  Negotiated_Version = 1,  Message_MTU = 44
     Message_Type = 2,  Negotiated_Version = 1,  Message_MTU = 4
```

Next you can enter the same session ID into the following command to display the capability negotiation result:

```
Router# show issu negotiated capability 19
Session_ID = 19 :
Negotiated_Cap_Entry = 1
```

Finally, to see which message types and versions are supported by this particular client, you enter the client ID into the following command:

```
Router# show issu message types 2008
---------------------------------------------------------------------
 Client_ID = 2008,  Entity_ID = 1 :
    Message_Type = 1,  Version_Range = 1 ~ 1
          Message_Ver = 1,    Message_Mtu = 44
    Message_Type = 2,  Version_Range = 1 ~ 1
          Message_Ver = 1,    Message_Mtu = 4
```

Verifying the ISSU Process for an MPLS LSD Label Manager HA Client Example

This example shows how to verify the ISSU process for an MPLS LSD Label Manager HA client.

The first command shows you whether the LSD client's old and new software versions are compatible, and therefore are able to make use of the ISSU opportunity:

```
Router# show issu sessions 2007
---------------------------------------------------------------------
 Client_ID = 2007,  Entity_ID = 1 :
 *** Session_ID = 40,  Session_Name = lsd_ha :
    Peer   Peer  Negotiate  Negotiated   Cap      Msg     Session
  UniqueID  Sid    Role       Result   GroupID  GroupID  Signature
     4       30   PRIMARY   COMPATIBLE    1        1         0
                              (policy)
    Negotiation Session Info for This Message Session:
         Nego_Session_ID = 40
         Nego_Session_Name = lsd_ha
         Transport_Mtu = 3948
         Compat_Result: raw_result = COMPATIBLE,  policy_result = COMPATIBLE
```

Now you can take the session ID displayed in the previous command's output and enter it into the next command, in order to see the negotiated message version:

```
Router# show issu negotiated version 40
Session_ID = 40 :
     Message_Type = 1,  Negotiated_Version = 2,  Message_MTU = 8
```

Next you can enter the same session ID into the following command to display the capability negotiation result:

```
Router# show issu negotiated capability 40
---------------------------------------------------
  Client_ID = 2007,  Entity_ID = 1,  Session_ID = 40 :
      Negotiated_Cap_Entry = 1
```

Finally, to see which message types and versions are supported by this particular client, you enter the client ID into the following command:

```
Router# show issu message types 2007
---------------------------------------------------------------------
```

```
 Client_ID = 2007,  Entity_ID = 1 :
    Message_Type = 1,  Version_Range = 1 ~ 2
          Message_Ver = 1,    Message_Mtu = 12
          Message_Ver = 2,    Message_Mtu = 8
```

Verifying the ISSU Process for an MPLS MFI Pull Client Example

This example shows how to verify the ISSU process for an MPLS MFI Pull client.

The first command shows you whether the MFI Pull client's old and new software versions are compatible, and therefore are able to make use of the ISSU opportunity:

```
Router# show issu sessions 2030
---------------------------------------------------------------------
Client_ID = 2030,  Entity_ID = 1 :
*** Session_ID = 131073,  Session_Name = MFI
Pull                                                         (6):
    Peer   Peer  Negotiate  Negotiated   Cap      Msg     Session
  UniqueID  Sid    Role       Result   GroupID  GroupID  Signature
    7         35     PRIMARY   COMPATIBLE     1        1         0
                              (no policy)
    Negotiation Session Info for This Message Session:
         Nego_Session_ID = 131073
         Nego_Session_Name = MFI
Pull                                                        (6)
         Transport_Mtu = 4056
```

Now you can take the session ID displayed in the previous command's output and enter it into the next command, in order to see the negotiated message version:

```
Router# show issu negotiated version 131073
    Session_ID = 131073:
     Message_Type = 1006,  Negotiated_Version = 1,  Message_MTU = 4
    Message_Type = 3003,  Negotiated_Version = 1,  Message_MTU = 12
```

Next you can enter the same session ID into the following command to display the capability negotiation result:

```
Router# show issu negotiated capability 131073
    Session_ID = 131073 :
      Negotiated_Cap_Entry = 1
```

Finally to see which message types and versions are supported by this particular client, you enter the client ID into the following command:

```
Router# show issu message types 2030
---------------------------------------------------------------------
    Client_ID = 2030,  Entity_ID = 1 :
    Message_Type = 1006,  Version_Range = 1 ~ 1
          Message_Ver = 1,    Message_Mtu = 4
    Message_Type = 2004,  Version_Range = 1 ~ 1
          Message_Ver = 1,    Message_Mtu = 12
```

Verifying the ISSU Process for an MPLS MFI Push Client Example

This example shows how to verify the ISSU process for an MPLS MFI Push client.

The first command shows you whether the MFI Push client's old and new software versions are compatible, and therefore are able to make use of the ISSU opportunity:

```
Router# show issu sessions 2031
---------------------------------------------------------------------
Client_ID = 2031,  Entity_ID = 1 :
*** Session_ID = 196646,  Session_Name = MFI
Push                                                         (6):
```

```
    Peer   Peer  Negotiate  Negotiated   Cap      Msg     Session
  UniqueID  Sid    Role       Result   GroupID  GroupID  Signature
    7         36          PRIMARY   COMPATIBLE                          1        1         0
                               (no policy)
    Negotiation Session Info for This Message Session:
         Nego_Session_ID = 196646
         Nego_Session_Name = MFI
Push                                                        (6)
         Transport_Mtu = 4056
```

Now you can take the session ID displayed in the previous command's output and enter it into the next command, in order to see the negotiated message version:

```
Router# show issu negotiated version 196646
Session_ID = 196646:
     Message_Type = 101,  Negotiated_Version = 1,  Message_MTU = 17
    Message_Type = 105,  Negotiated_Version = 1,  Message_MTU = 31
```

Next you can enter the same session ID into the following command to display the capability negotiation result:

```
Router# show issu negotiated capability 196646
Session_ID = 196646 :
      Negotiated_Cap_Entry = 1
```

Finally to see which message types and versions are supported by this particular client, you enter the client ID into the following command:

```
Router# show issu message types 2031
---------------------------------------------------------------------
    Client_ID = 2031,  Entity_ID = 1 :
    Message_Type = 5002,  Version_Range = 1 ~ 2
          Message_Ver = 1,    Message_Mtu = 10
    Message_Type = 5018,  Version_Range = 1 ~ 1
          Message_Ver = 1,    Message_Mtu = 39
```

Verifying the ISSU Process for an MPLS LSPV Push Client Example

This example shows how to verify the ISSU process for an MPLS LSVP Push client.

The first command shows you whether the LSPV Push client's old and new software versions are compatible, and therefore are able to make use of the ISSU opportunity:

```
Router# show issu sessions 2089
---------------------------------------------------------------------
 Client_ID = 2089,  Entity_ID = 1 :
 *** Session_ID = 45,  Session_Name = MPLS LSPV Push (6 ):
    Peer   Peer  Negotiate  Negotiated   Cap      Msg     Session
  UniqueID  Sid    Role       Result   GroupID  GroupID  Signature
     7        36         PRIMARY   COMPATIBLE    1       1         0
                            (no policy)
    Negotiation Session Info for This Message Session:
         Nego_Session_ID = 45
         Nego_Session_Name = MPLS LSPV Push ( 6)
         Transport_Mtu = 1438
```

Now you can take the session ID displayed in the previous command's output and enter it into the next command, in order to see the negotiated message version:

```
Router# show issu negotiated version 45
 Session_ID = 45:
    Message_Type = 0,  Negotiated_Version = 1,  Message_MTU = 74
    Message_Type = 1,  Negotiated_Version = 1,  Message_MTU = 120
    Message_Type = 2,  Negotiated_Version = 1,  Message_MTU = 120
    Message_Type = 3,  Negotiated_Version = 1,  Message_MTU = 5122
    Message_Type = 4,  Negotiated_Version = 1,  Message_MTU = 6
```

Next you can enter the same session ID into the following command to display the capability negotiation result:

```
Router# show issu negotiated capability 45
Session_ID = 45:
Cap_Type = 0                Cap_Result = 1                   No cap value assigned
```

Finally to see which message types and versions are supported by this particular client, you enter the client ID into the following command:

```
Router# show issu message types 2089
---------------------------------------------------------------------
 Client_ID = 2089,  Entity_ID = 1 :
    Message_Type = 0,  Version_Range = 1 ~ 1
          Message_Ver = 1,    Message_Mtu = 74
    Message_Type = 1,  Version_Range = 1 ~ 1
          Message_Ver = 1,    Message_Mtu = 120
    Message_Type = 2,  Version_Range = 1 ~ 1
          Message_Ver = 1,    Message_Mtu = 120
    Message_Type = 3,  Version_Range = 1 ~ 1
          Message_Ver = 1,    Message_Mtu = 5122
    Message_Type = 4,  Version_Range = 1 ~ 1
          Message_Ver = 1,    Message_Mtu = 6
```

Verifying the ISSU Process for an MPLS TE Client Example

This example shows how to verify the ISSU process for an MPLS TE client.

The first command shows you whether the TE client’s old and new software versions are compatible, and therefore are able to make use of the ISSU opportunity:

```
Router# show issu sessions 2053
---------------------------------------------------------------------
 Client_ID = 2053,  Entity_ID = 1 :
 *** Session_ID = 84,  Session_Name = RSVP HA Session :
    Peer   Peer  Negotiate  Negotiated   Cap      Msg     Session
  UniqueID  Sid    Role       Result   GroupID  GroupID  Signature
    22       94   PRIMARY   COMPATIBLE    1        1         0
                           (no policy)
    Negotiation Session Info for This Message Session:
         Nego_Session_ID = 84
         Nego_Session_Name = RSVP HA Session
         Transport_Mtu = 1392
```

Now you can take the session ID displayed in the previous command’s output and enter it into the next command, in order to see the negotiated message version:

```
Router# show issu negotiated version 84
Session_ID = 84 :
     Message_Type = 1,  Negotiated_Version = 2,  Message_MTU = 1024
```

Next you can enter the same session ID into the following command to display the capability negotiation result:

```
Router# show issu negotiated capability 84
Session_ID = 84 :
     Cap_Type = 0,     Cap_Result = 1     No cap value assigned
```

Finally to see which message types and versions are supported by this particular client, you enter the client ID into the following command:

```
Router# show issu message types 2053
---------------------------------------------------------------------
 Client_ID = 2053,  Entity_ID = 1 :
```

```
Message_Type = 1,  Version_Range = 1 ~ 2
      Message_Ver = 1,    Message_Mtu = 1024
      Message_Ver = 2,    Message_Mtu = 1024
```

Additional References

Related Documents

Related Topic	Document Title
ISSU and eFSU procedure	Cisco IOS In Service Software Upgrade and Enhanced Fast Software Upgrade Process
I SSU and eFSU on Cisco 7600 series routers	*Cisco 7600 Series Router Cisco IOS Software Configuration Guide*

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	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

RFC	Title
None	—

Technical Assistance

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

Feature Information for ISSU MPLS Clients

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

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

Table 14 Feature Information for ISSU MPLS Clients

Feature Name	Releases	Feature Information
ISSU MPLS Clients	12.2(28)SB 12.2(33) SRB-1	MPLS applications can be upgrading using the In Service Software Upgrade (ISSU) process and the enhanced Fast Software Upgrade (eFSU) process. Thus, MPLS applications are considered ISSU's MPLS clients. The ISSU process allows Cisco IOS software *at the router level* to be updated or otherwise modified while packet forwarding continues. *At the line-card level* , the eFSU process minimizes line-card downtime during such upgrades to between 30 and 90 seconds, by loading the new line-card image before the ISSU switchover occurs from the active to the standby Route Processor (RP). In 12.2(28)SB, the ISSU feature was introduced. In 12.2(33)SRB-1, the LSPV Push and TE clients and the eFSU functionality were added. The following commands were introduced or modified: **show issu clients, show issu entities, show issu message types, show issu negotiated, show issu outage, show issu sessions**.

Glossary

eFSU—enhanced Fast Software Upgrade.

IS —intermediate system.

ISSU —In Service Software Upgrade.

LACP —Link Aggregration Control Protocol.

LDP —Label Distribution Protocol.

MFI —Multiprotocol Label Switching Forwarding Infrastructure.

MPLS —Multiprotocol Label Switching.

OAM —Operation, Administration, and Management.

PagP —port aggregation Protocol.

PPP —Point to Point protocol.

RP —Route Processor.

RSVP GR —Resource Reservation Protocol graceful restart.

TE —traffic engineering.

VPN —Virtual Private Network.

VRF —virtual routing and forwarding.

NSF SSO ISSU Support for VPLS

Virtual Private LAN Services (VPLS), with nonstop forwarding (NSF), stateful switchover (SSO), and in service software upgrade (ISSU) support, improves the availability of service provider networks that use VPLS for multipoint Layer 2 virtual private network (VPN) services. Cisco NSF with SSO is effective at increasing availability of network services. Cisco NSF with SSO provides continuous packet forwarding, even during a network processor hardware or software failure. In a redundant system, the secondary processor recovers control plane service in the event of a critical failure in the primary processor, while SSO synchronizes the network state information between the primary and the secondary processor.

In conjunction with VPLS NSF/SSO, VPLS High Availability (HA) features include the ISSU capability. Working together, ISSU and NSF/SSO enable upgrades or downgrades of a Cisco IOS image without control and data plane outages.

Finding Feature Information

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

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

Prerequisites for NSF SSO ISSU Support for VPLS

This section lists the following prerequisites that are required to use the NSF/SSO/ISSU Support for VPLS feature.

You must configure the following features on your network:

- VPLS (see the “Virtual Private LAN Services on the Optical Services Modules” chapter in the Cisco 7600 Series Router Cisco IOS Software Configuration Guide , Release 12.2SR)
- VPLS Autodiscovery (see VPLS Autodiscovery: BGP Based and BGP Support for the L2VPN Address Family)
- NSF/SSO: Any Transport over MPLS (see NSF/SSO—Any Transport over MPLS and AToM Graceful Restart)
- NSF/SSO router support on the 7600 router (see the “Configuring NSF with SSO Supervisor Engine Redundancy” chapter in the Cisco 7600 Series Cisco IOS Software Configuration Guide , Release 12.2SR)
- ISSU router support on the 7600 router (see the “ISSU and eFSU on Cisco 7600 Series Routers” chapter in the Cisco 7600 Series Cisco IOS Software Configuration Guide , Release 12.2SR)

Restrictions for NSF SSO ISSU Support for VPLS

The NSF/SSO/ISSU Support for VPLS feature has the following restrictions:

- NSF/SSO/ISSU support for VPLS does not include support for PWs to auto discovered neighbors via Border Gateway Protocol (BGP). Statically configured neighbors are supported.
- For supported hardware, see the Cisco Release 12.2SR Release Notes.
- NSF/SSO/ISSU support for VPLS does not include support for line cards that do not support Minimal Disruptive Restart (MDR) or pre downloading of firmware or driver code.

Information About NSF SSO ISSU Support for VPLS

How NSF SSO Works with VPLS

VPLS with NSF/SSO support improves the availability of service provider networks that use VPLS for multipoint Layer 2 VPN services. HA minimizes service disruptions that can occur if a system failure occurs. To address failures, VPLS HA includes SSO and NSF mechanisms using a standby Route Processor (RP) to provide control-plane redundancy. VPLS NSF is achieved by SSO and NSF mechanisms.

While the standby RP transitions to the active RP, packet forwarding either continues forwarding on line card(s) or packet forwarding is switched over (switchover) to other hardware devices associated with the newly active RP.

How ISSU Works with VPLS

In conjunction with VPLS NSF/SSO, VPLS HA includes ISSU, a comprehensive in-service upgrade solution for the IP/MPLS edge. ISSU minimizes network downtime due to software upgrades and maintenance activities. ISSU allows upgrades or downgrades to Cisco IOS software images with no effect on the control plane and minimal effect on system packet forwarding. With ISSU, all message data structures used for checkpointing, and exchanges between the active RP and standby RP are versioned.

To perform an in-service upgrade, the standby RP in a dual RP-based platform (such as the Cisco 7600 router) is first loaded with the desired Cisco IOS software release. The standby RP then comes up as a hot-standby RP with an upgraded version of the software, and a switchover is performed to transfer control to the standby RP and run the upgraded image.

During the ISSU procedure, supported SSO protocols and features maintain their session states with no disruption of the Layer 2 protocol sessions. Cisco NSF technology is used to continue packet forwarding during the software upgrade procedure while the routing information is re-created on the newly active RP. The result is a seamless software upgrade for an IP/MPLS provider edge router with no disruptions to Layer 2 protocol sessions and minimal effect on packet forwarding.

Benefits

Primary benefits for ISSU are:

- Rapid, nondisruptive feature deployment—By preserving user sessions and minimizing packet loss during software upgrades, ISSU helps enable rapid, nondisruptive deployments for new features and services at the IP/MPLS provider edge.
- Comprehensive solution for planned downtime—ISSU addresses the entire spectrum of software upgrade needs, from applying caveat fixes to deploying new features and services, and delivers a comprehensive solution for addressing planned network downtime.
- Increased operational efficiencies—ISSU minimizes and streamlines planned downtime and helps enable operational process changes for software deployment, significantly decreasing planned downtime effort and expenses and increasing operational efficiency.

How to Configure NSF SSO ISSU Support for VPLS

Configuring VPLS

VPLS must be configured on the router. See the “Virtual Private LAN Services on the Optical Services Modules” chapter in the Cisco 7600 Series Router Cisco IOS Software Configuration Guide , Release 12.2SR for information on configuring VPLS.

Configuring NSF SSO Any Transport over MPLS

You must configure the NSF/SSO: Any Transport over MPLS feature on the router. See the NSF/SSO—Any Transport over MPLS and AToM Graceful Restart feature module for information on configuring the NSF/SSO: Any Transport over MPLS feature.

Configuring NSF SSO Router support

You must configure NSF/SSO router support on the Cisco 7600 router. See the “Configuring NSF with SSO Supervisor Engine Redundancy” chapter in the Cisco 7600 Series Cisco IOS Software Configuration Guide , Release 12.2SR for information on configuring the NSF with SSO Supervisor Engine Redundancy feature.

Configuring ISSU Router Support

You must configure ISSU router support on the Cisco 7600 router.

- See the "ISSU and eFSU on Cisco 7600 Series Routers" chapter in the Cisco 7600 Series Cisco IOS Software Configuration Guide , Release 12.2SR for information on configuring ISSU and Enhanced Fast Software Upgrade (eFSU) on Cisco 7600 series routers.

Verifying and Troubleshooting NSF SSO ISSU Support for VPLS

To verify the NSF/SSO/ISSU Support for VPLS configuration, use the following show and debug commands:

1 **show checkpoint clients**
2 **show vfi [name** *vfi-name* **] checkpoint [summary]**
3 **debug cwan atom**
4 **debug cwan ltl**
5 **debug issu client negotiation**
6 **debug issu client registration**
7 **debug issu client transform**
8 **debug vfi checkpoint**

SUMMARY STEPS

1. **show checkpoint clients**
2. **show vfi [name** *vfi-name* **] checkpoint [summary]**
3. **debug cwan atom**
4. **debug cwan ltl**
5. **debug issu client negotiation**
6. **debug issu client registration**
7. **debug issu client transform** [**clientID** *client-id*]
8. **debug vfi checkpoint**

DETAILED STEPS

Step 1 **show checkpoint clients**
Use this command to display information about checkpoint clients:

Example:

```
Router# show checkpoint clients
                         Check Point List of Clients
 CHKPT on ACTIVE server.
--------------------------------------------------------------------------------
Client Name         Client  Entity  Bundle
                        ID      ID    Mode
--------------------------------------------------------------------------------
CHKPT Test client        1     --     On
  Total API Messages Sent:             0
  Total IPC Sent:                      0
```

```
  Total Message Len:                   0
  Total Bytes Allocated:               0
  Buffers Held:                        0
  IPC Frag Count:                      0
  IPC HW mark:                         0
  IPC Sends w/Flow Off:                0
  Send Errs:                           0
  Send Peer Errs:                      0
  Rcv Xform Errs:                      0
  Xmit Xform Errs:                     0
  Incompatible Messages:               0
--------------------------------------------------------------------------------
Client Name         Client  Entity  Bundle
                        ID      ID    Mode
--------------------------------------------------------------------------------
Network RF Client        3     --    Off
  Total API Messages Sent:            10
  Total IPC Sent:                     10
  Total Message Len:                2144
  Total Bytes Allocated:            2904
  Buffers Held:                        0
  IPC Frag Count:                      0
  IPC HW mark:                         0
  IPC Sends w/Flow Off:                0
  Send Errs:                           0
  Send Peer Errs:                      0
  Rcv Xform Errs:                      0
  Xmit Xform Errs:                     0
  Incompatible Messages:               0
--------------------------------------------------------------------------------
Client Name         Client  Entity  Bundle
                        ID      ID    Mode
 --More--
.
.
.
```

Step 2 **show vfi [name *vfi-name*] checkpoint [summary]**

Use this command to display checkpoint information related to a specific virtual forwarding instance (VFI) named H-VPLS-A-VFI:

Example:

```
Router# show vfi name H-VPLS-A-VFI checkpoint
VFI Active RP
 Checkpointing: Allowed
 ISSU Client id: 2092, Session id: 65543, Compatible with peer
                                VFI      VFI AC      VFI PW
 Bulk-sync                        1           1           3
 Checkpoint failures:             0           3          21
 Recovered at switchover:         0           0           0
 Recovery failures:               0           0           0
Legend: C=Checkpointed
VFI name: H-VPLS-A-VFI, state: up, type: multipoint
  VPN ID: 12, Internal ID 1 C
  Local attachment circuits:
    Vlan200  16387 / 8195  C
Neighbors connected via pseudowires:
    Peer ID         VC ID              SSM IDs
    10.0.0.12      12                4096 / 12292       C
    10.0.0.15      12                8193 / 16389       C
    10.0.0.14      12                12290 / 20486      C
```

Step 3 **debug cwan atom**

Use this command to enable debugging of Any Transport over MPLS (AToM) platform events.

The following example shows debug message output that appears when debugging is enabled and a PW port is configured and then unconfigured:

Example:

```
Router# debug cwan atom
ConstWan Generic AToM debugging is on
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router#(config)# l2 vfi VPLS-2000 manual
Router#(config-vfi)# vpn id 2000

Router#(config-vfi)# neighbor 10.1.1.1 encapsulation mpls
Router#(config-vfi)#
01:16:36: cwan_rp_vfi_atom_provision_vlan PROV[VFI-ATOM]: plat_index(0xC7D00084) vlanid(2000)
pseudo_port(0x84) vfi_plat_index(0xC7D00084) seginfo(0x53D38220) segtype(25) seghandle(0x53AEE074)
split-horizon(On) cwan_atom_intfs(3) vfi_vcs(3) spoke_vcs(0)
Router#(config-vfi)# end
Router# debug cwan atom
ConstWan Generic AToM debugging is on
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# l2 vfi VPLS-2000
Router(config-vfi)# no neighbor 10.1.1.1 encapsulation mpls
Router(config-vfi)#
01:27:18: cwan_rp_vfi_atom_unprovision_vlan: UNPROV[VFI-ATOM]: circ_index(0xC7D00084) is_vfi(1)
vlan(2000) vfi_vcs(3) spoke_vcs(0) split_horizon(On)
01:27:18: cwan_atom_vlan_remove_rp: Vlan2000 ip_iw(0) ip_enabled(0)
Router#(config-vfi)# end
```

Step 4 **debug cwan ltl**

Use this command to enable debugging of Local Target Manager (LTL) debugging events and errors.

The following example shows debug message outputs that appear when debugging is enabled and a PW port is configured and then unconfigured:

Example:

```
Router# debug cwan ltl
ConstWan LTL manager debugging is on
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router#(config)# l2 vfi VPLS-2000 manual
Router#(config-vfi)# vpn id 2000
Router#(config-vfi)# neighbor 10.1.1.1 encapsulation mpls
Router#(config-vfi)#
01:17:35: CWAN LTL MGR: Port 133 is free to use for VPLS with vlan 2000 - tx_tvc(0x9F404)
Router#(config-vfi)# end
Router# debug cwan ltl
ConstWan LTL manager debugging is on
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# l2 vfi VPLS-2000 manual

Router(config-vfi)# no neighbor 10.1.1.1 encapsulation mpls
Router(config-vfi)#
01:29:05: CWAN LTL MGR: DELETE VPLS PW vlan(2000) pseudo_slotunit(133)
Router(config-vfi)# end
```

Step 5 **debug issu client negotiation**

Use this command to enable debugging of ISSU client negotiation events and errors:

Example:

```
Router# debug issu client negotiation
*Jun  5 22:41:47.332: VFI ISSU: Negotiation rc ISSU_RC_NEGO_DONE, compatible
*Jun  5 22:41:47.332: AToM HA: CID 84 Seq 230 Event RF_PROG_STANDBY_CONFIG Op 0 State ACTIVE Peer
STANDBY COLD-CONFIG
*Jun  5 22:41:47.432: ATOM ISSU: Propose L2HW cap 0xFFF rc 0
```

```
*Jun  5 22:41:47.532: ATOM ISSU: Active negotiator, accept compatible L2HW cap 0xFFF
*Jun  5 22:41:48.232: ATOM ISSU: Negotiation rc ISSU_RC_NEGO_DONE, compatible
*Jun  5 22:41:50.836: cwan_atom_issu_start_nego_session: Start session negotiation
*Jun  5 22:41:50.836: cwan_atom_issu_start_nego_session: Started nego successfully,
rc=ISSU_RC_NEGO_NOT_DONE
*Jun  5 22:41:50.836: cwan_atom_issu_receive_nego_msg: Start, cwan_atom_issu_nego_done=0
*Jun  5 22:41:50.840: cwan_atom_issu_receive_nego_msg: issu_receive_nego_msg
rc=ISSU_RC_NEGO_NOT_DONE
*Jun  5 22:41:50.940: cwan_atom_issu_receive_nego_msg: Start, cwan_atom_issu_nego_done=0
*Jun  5 22:41:50.940: cwan_atom_issu_receive_nego_msg: issu_receive_nego_msg
rc=ISSU_RC_NEGO_NOT_DONE
*Jun  5 22:41:51.040: cwan_atom_issu_receive_nego_msg: Start, cwan_atom_issu_nego_done=0
*Jun  5 22:41:51.040: cwan_atom_issu_receive_nego_msg: issu_receive_nego_msg
rc=ISSU_RC_NEGO_NOT_DONE
*Jun  5 22:41:51.140: cwan_atom_issu_receive_nego_msg: Start, cwan_atom_issu_nego_done=0
*Jun  5 22:41:51.140: cwan_atom_issu_receive_nego_msg: issu_receive_nego_msg
rc=ISSU_RC_NEGO_NOT_DONE
*Jun  5 22:41:51.240: cwan_atom_issu_receive_nego_msg: Start, cwan_atom_issu_nego_done=0
*Jun  5 22:41:51.240: cwan_atom_issu_receive_nego_msg: issu_receive_nego_msg
rc=ISSU_RC_NEGO_NOT_DONE
*Jun  5 22:41:51.340: cwan_atom_issu_receive_nego_msg: Start, cwan_atom_issu_nego_done=0
*Jun  5 22:50:40.156: VFI ISSU: Negotiation rc ISSU_RC_NEGO_DONE, compatible
*Jun  5 22:50:40.156: AToM HA: CID 84 Seq 230 Event RF_PROG_STANDBY_CONFIG Op 0 State ACTIVE Peer
STANDBY COLD-CONFIG
*Jun  5 22:50:40.256: ATOM ISSU: Passive negotiator, accept compatible L2HW cap 0xFFF
*Jun  5 22:50:40.964: ATOM ISSU: Negotiation rc ISSU_RC_NEGO_DONE, compatible
*Jun  5 22:50:43.516: cwan_atom_issu_start_nego_session: Start session negotiation
*Jun  5 22:50:43.516: cwan_atom_issu_start_nego_session: Started nego successfully,
rc=ISSU_RC_NEGO_NOT_DONE
*Jun  5 22:50:43.520: cwan_atom_issu_receive_nego_msg: Start, cwan_atom_issu_nego_done=0
*Jun  5 22:50:43.520: cwan_atom_issu_receive_nego_msg: issu_receive_nego_msg
rc=ISSU_RC_NEGO_NOT_DONE
*Jun  5 22:50:43.620: cwan_atom_issu_receive_nego_msg: Start, cwan_atom_issu_nego_done=0
*Jun  5 22:50:43.620: cwan_atom_issu_receive_nego_msg: issu_receive_nego_msg
rc=ISSU_RC_NEGO_NOT_DONE
*Jun  5 22:50:43.720: cwan_atom_issu_receive_nego_msg: Start, cwan_atom_issu_nego_done=0
*Jun  5 22:50:43.720: cwan_atom_issu_receive_nego_msg: issu_receive_nego_msg
rc=ISSU_RC_NEGO_NOT_DONE
*Jun  5 22:50:43.820: cwan_atom_issu_receive_nego_msg: Start, cwan_atom_issu_nego_done=0
*Jun  5 22:50:43.820: cwan_atom_issu_receive_nego_msg: issu_receive_nego_msg
rc=ISSU_RC_NEGO_NOT_DONE
*Jun  5 22:50:43.920: cwan_atom_issu_receive_nego_msg: Start, cwan_atom_issu_nego_done=0
*Jun  5 22:50:43.920: cwan_atom_issu_receive_nego_msg: issu_receive_nego_msg
rc=ISSU_RC_NEGO_NOT_DONE
*Jun  5 22:50:44.020: cwan_atom_issu_receive_nego_msg: Start, cwan_atom_issu_nego_done=0
```

Step 6 **debug issu client registration**

Use this command to enable debugging of ISSU client registration events and errors.

After the peer router reloads, the following debug messages appear:

Example:

```
Router# debug issu client registration
Router#
00:42:21: VFI ISSU: Unregistered ISSU session 0, ISSU_RC_OK
00:42:21: %LINK-3-UPDOWN: Interface GigabitEthernet6/2, changed state to down
00:42:21: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet6/2, changed state to down
00:42:21: %LINK-3-UPDOWN: Interface Vlan2000, changed state to down
00:42:21: %LINK-3-UPDOWN: Interface Vlan2001, changed state to down
00:42:21: %LINK-3-UPDOWN: Interface Vlan2002, changed state to down
Router#
00:42:21: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2000, changed state to down
00:42:21: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2001, changed state to down
00:42:21: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2002, changed state to down
Router#
00:49:01: %LINK-3-UPDOWN: Interface GigabitEthernet6/2, changed state to down
00:49:02: %LINK-3-UPDOWN: Interface GigabitEthernet6/2, changed state to up
PE-3#
00:49:05: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet6/2, changed state to up
```

```
Router#
00:49:35: %LINK-3-UPDOWN: Interface Vlan2000, changed state to up
00:49:35: %LINK-3-UPDOWN: Interface Vlan2001, changed state to up
00:49:35: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2000, changed state to up
00:49:35: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2001, changed state to up
00:49:35: %LINK-3-UPDOWN: Interface Vlan2002, changed state to up
Router#
00:49:35: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2002, changed state to up
Router#
00:49:48: VFI ISSU: Registered session 131171, ISSU_RC_OK
Router#
00:50:08: %HA_CONFIG_SYNC-6-BULK_CFGSYNC_SUCCEED: Bulk Sync succeeded
Router#
```

Step 7 **debug issu client transform** [**clientID** *client-id*]

Use this command to enable debugging of ISSU client transform events and errors.

The following command example enables debug output for a specific ISSU client (clientID 2092**)**. After the peer router reloads, the following debug messages appear:

Example:

```
Router# debug issu client transform clientID 2092
Router#
05:35:15: %LINK-3-UPDOWN: Interface GigabitEthernet6/2, changed state to down
05:35:15: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet6/2, changed state to down
05:35:15: %LINK-3-UPDOWN: Interface Vlan2000, changed state to down
05:35:15: %LINK-3-UPDOWN: Interface Vlan2001, changed state to down
05:35:15: %LINK-3-UPDOWN: Interface Vlan2002, changed state to down
Router#
05:35:15: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2000, changed state to down
05:35:15: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2001, changed state to down
05:35:15: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2002, changed state to down
Router#
05:41:55: %LINK-3-UPDOWN: Interface GigabitEthernet6/2, changed state to down
05:41:56: %LINK-3-UPDOWN: Interface GigabitEthernet6/2, changed state to up
.
.
.
05:43:02: VFI ISSU: Xmit transform message 5, rc ISSU_RC_OK
05:43:02: ISSU Buffer dump @ 0x0817EC7C
05:43:02:     00 00 00 00
05:43:02: VFI ISSU: Xmit transform message 1, rc ISSU_RC_OK
05:43:02: %HA_CONFIG_SYNC-6-BULK_CFGSYNC_SUCCEED succeeded
Router#
```

Step 8 **debug vfi checkpoint**

Use this command to enable debugging VFI checkpointing events and errors:

Example:

```
Router# debug vfi checkpoint
Router# $may24_v1  6 slavedisk0:s72033-adventerprisek9_wan-mz.cflow_may24_v1
Router#
*Jun  5 22:37:17.268: AToM HA: CF status 3 not processed
*Jun  5 22:37:17.268: VFI HA: CF status 3 not processed
*Jun  5 22:37:17.296: AC HA RF: CId:83, Seq:228, Sta:RF_STATUS_PEER_COMM, Opr:0, St:ACTIVE,
PSt:STANDBY HOT
*Jun  5 22:37:17.296: VFI HA: CID 145, Seq 229, Status RF_STATUS_PEER_COMM, Op 0, State ACTIVE,
Peer STANDBY HOT
*Jun  5 22:37:17.296: AToM HA: CID 84, Seq 230, Status RF_STATUS_PEER_COMM, Op 0, State ACTIVE,
Peer STANDBY HOT
*Jun  5 22:37:17.444: AToM HA: CF status 3 not processed
*Jun  5 22:37:17.444: VFI HA: CF status 3 not processed
*Jun  5 22:37:17.268: %OIR-SP-3-PWRCYCLE: Card in module 6, is being power-cycled (RF request)
*Jun  5 22:37:17.792: AC HA RF: CId:83, Seq:228, Sta:RF_STATUS_PEER_PRESENCE, Opr:0, St:ACTIVE,
PSt:DISABLED
```

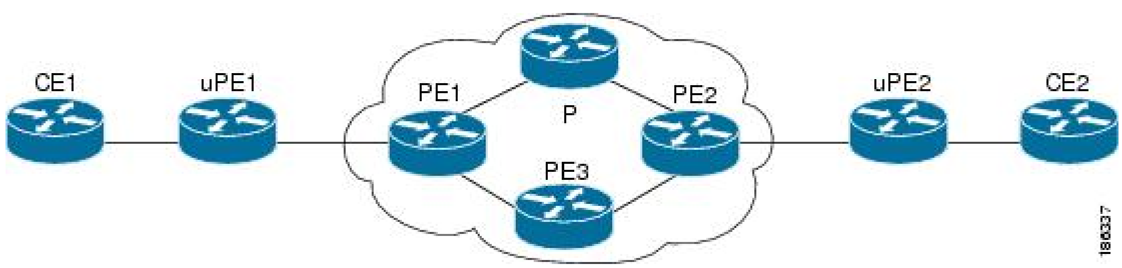
```
*Jun  5 22:37:17.792: VFI HA: CID 145, Seq 229, Status RF_STATUS_PEER_PRESENCE, Op 0, State
ACTIVE, Peer DISABLED
*Jun  5 22:40:40.244: SP-STDBY: SP: Currently running ROMMON from S (Gold) region
*Jun  5 22:40:45.028: %DIAG-SP-STDBY-6-RUN_MINIMUM: Module 6: Running Minimal Diagnostics...
*Jun  5 22:40:56.492: %DIAG-SP-STDBY-6-DIAG_OK: Module 6: Passed Online Diagnostics
*Jun  5 22:41:53.436: %SYS-SP-STDBY-5-RESTART: System restarted --
*Jun  5 22:42:12.760: VFI HA: CID 145 Seq 229 Event RF_PROG_STANDBY_BULK Op 0 State ACTIVE Peer
STANDBY COLD-BULK
*Jun  5 22:42:12.764: VFI HA: Ignore RF progression event, VFI Mgr process is not running, skipped
bulk sync
.
.
.
*Jun  5 22:42:16.948: %ISSU_PROCESS-SP-7-DEBUG: Peer state is [ STANDBY HOT ]; Please issue the
runversion command
*Jun  5 22:42:15.928: %PFREDUN-SP-STDBY-6-STANDBY: Ready for SSO mode
*Jun  5 22:42:16.956: %RF-SP-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)
*Jun  5 22:42:16.112: %SYS-SP-STDBY-3-LOGGER_FLUSHED: System was paused for 00:00:00 to ensure
console debugging output.
Router#
```

Configuration Examples for NSF SSO ISSU Support for VPLS

NSF SSO ISSU VPLS Example

The figure below shows a basic configuration of NSF/SSO/ISSU VPLS.

Figure 6 Basic NSF/SSO/ISSU VPLS Configuration



CE1

```
CE1_7206#
!
hostname CE1_7206
!
ip cef
!
interface Loopback0
 description - FULL MESH VPN
 ip address 10.0.0.0 10.255.255.255
!
interface FastEthernet0/0
 ip address 10.0.57.100 255.255.255.0
 no ip mroute-cache
```

```
 duplex half
 no cdp enable
!
interface FastEthernet1/0
 description - H-VPLS VPN to uPE1
 no ip address
 no ip mroute-cache
 duplex auto
 speed auto
!
interface FastEthernet1/0.1
 description - H-VPLS VPN to uPE1
 encapsulation dot1Q 121
 ip address 10.1.1.120 255.255.255.0
!
interface FastEthernet4/1
 description - FULL MESH VPN to PE1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet4/1.1
 description - FULL MESH VPN to PE1
 encapsulation dot1Q 120
 ip address 10.1.1.120 255.255.255.0
!
interface FastEthernet6/1
 description - VPWS VPN to PE1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet6/1.1
 description - VPWS VPN to PE1
 encapsulation dot1Q 122
 ip address 10.1.1.120 255.255.255.0
!
router ospf 10
 log-adjacency-changes
 network 10.1.1.0 0.0.0.255 area 0
 network 10.120.120.120 0.0.0.0 area 0
 network 10.1.1.0 0.0.0.255 area 0
!
ip default-gateway 10.0.57.1
!
end
```

uPE1

```
uPE1_7609#
!
upgrade fpd auto
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
service internal
!
hostname uPE1_7609
!
boot-start-marker
boot system flash disk0:s72033-adventerprisek9_wan_dbg-mz.xx
boot-end-marker
!
no aaa new-model
!
no ip domain lookup
ip host lab24 172.16.0.0
ip host dirt 172.16.0.19
!
vtp mode transparent
!
multilink bundle-name authenticated
```

```
mpls ldp graceful-restart
mpls ldp discovery targeted-hello accept
mpls label protocol ldp
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
!
vlan internal allocation policy ascending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
vlan 100
!
interface Loopback0
 description - H-VPLS
 ip address 10.0.0.0 255.255.255.255
!
interface GigabitEthernet1/1
 description - H-VPLS to CE1
 switchport
 switchport trunk allowed vlan 10-1000
 switchport mode trunk
!
interface GigabitEthernet5/2
 ip address 10.0.0.0 255.255.255.0
 media-type rj45
 no cdp enable
!
interface GigabitEthernet9/0/0
 description - H-VPLS to PE1
 ip address 10.0.0.1 255.255.255.0
 negotiation auto
 mpls label protocol ldp
 mpls ip
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 10
 log-adjacency-changes
 passive-interface Loopback0
 network 10.0.5.0 0.0.0.255 area 0
 network 10.0.0.8 0.0.0.0 area 0
!
ip route 172.16.17.19 255.255.255.255 10.0.57.1
ip route 172.16.0.0 255.255.255.255 10.0.57.1
!
mpls ldp router-id Loopback0 force
!
control-plane
!
end
```

PE1

```
PE1_7613#
!
upgrade fpd auto
service internal
!
hostname PE1_7613
!
boot-start-marker
boot system flash disk0:s72033-adventerprisek9_wan_dbg-mz.xxx
boot-end-marker
```

```
!
no aaa new-model
ip subnet-zero
!
!
no ip domain lookup
ip host dirt 172.16.0.0
ip host lab24 172.16.0.01
!
ipv6 mfib hardware-switching replication-mode ingress
!
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
no mls acl tcam share-global
mls cef error action freeze
multilink bundle-name authenticated
mpls ldp discovery targeted-hello accept
mpls label protocol ldp
!
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
!
vlan internal allocation policy ascending
vlan dot1q tag native
vlan access-log ratelimit 2000
l2 vfi vpls_auto autodiscovery
 vpn id 1
!
l2 vfi vpls_man manual
 vpn id 10
 neighbor 10.0.0.12 encapsulation mpls
 neighbor 10.0.0.11 encapsulation mpls
!
interface Loopback0
 description - FULL MESH
 ip address 10.0.0.9 255.255.255.255
!
interface Loopback1
 description - VPWS
 ip address 172.16.0.0 255.255.255.255
!
interface Loopback2
 description - H-VPLS
 ip address 10.0.0.0 255.255.255.255
!
interface GigabitEthernet7/2
 ip address 10.0.0.01 255.255.255.0
 media-type rj45
 no cdp enable
!
interface GigabitEthernet10/1
 description - FULL MESH to CE1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10-1000
 switchport mode trunk
!
interface GigabitEthernet10/2
 description - VPWS to CE1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10-1000
 switchport mode trunk
!
interface GigabitEthernet12/0/0
```

```
 description - H-VPLS to uPE1
 ip address 10.0.0.3 255.255.255.0
 negotiation auto
 mpls label protocol ldp
 mpls ip
!
interface GigabitEthernet12/0/1
 description - H-VPLS to nPE2
 ip address 10.0.0.1 255.255.255.0
 negotiation auto
 mpls label protocol ldp
 mpls ip
!
interface GigabitEthernet12/1/0
 description - VPWS to P
 ip address 10.0.0.3 255.255.255.0
 negotiation auto
 mpls label protocol ldp
 mpls ip
!
interface GigabitEthernet12/1/1
 description - FULL MESH to P
 ip address 10.0.2.0 255.255.255.0
 negotiation auto
 mpls label protocol ldp
 mpls ip
!
interface GigabitEthernet12/2/0
 description - FULL MESH to PE3
 ip address 10.1.0.3 255.255.255.0
 negotiation auto
 mpls label protocol ldp
 mpls ip
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 no ip address
 xconnect vfi vpls_auto
!
router ospf 10
 ! for FULL MESH
 log-adjacency-changes
 passive-interface Loopback0
 network 10.1.1.0 0.0.0.255 area 0
 network 10.2.2.0 0.0.0.255 area 0
 network 10.5.5.0 0.0.0.255 area 0
 network 10.9.9.9 0.0.0.0 area 0
 network 10.0.0.02 0.0.0.255 area 0
 network 10.0.0.04 0.0.0.0 area 0
 network 10.0.0.5 0.0.0.0 area 0
!
router ospf 20
 ! for VPWS
 log-adjacency-changes
 passive-interface Loopback1
 network 10.0.20.0 0.0.0.255 area 0
 network 10.0.0.9 0.0.0.0 area 0
!
router bgp 1
 bgp log-neighbor-changes
 neighbor 10.0.11.0 remote-as 1
 neighbor 10.0.10.0 update-source Loopback0
 neighbor 10.0.12.0 remote-as 1
 neighbor 10.0.0.12 update-source Loopback0
 neighbor 10.0.0.32 remote-as 1
 neighbor 10.0.0.31 update-source Loopback2
 !
 address-family ipv4
  no synchronization
  neighbor 10.0.11.0 activate
```

```
  neighbor 10.12.0.0 activate
  neighbor 10.0.32.0 activate
  no auto-summary
 exit-address-family
 !
 address-family l2vpn vpls
  neighbor 10.0.0.11 activate
  neighbor 10.0.11.0 send-community both
  neighbor 10.12.0.0 activate
  neighbor 10.0.0.12 send-community both
  neighbor 10.0.0.32 activate
  neighbor 10.0.32.0 send-community both
 exit-address-family
!
ip default-gateway 10.0.57.1
ip route 172.16.0.0 255.255.255.255 10.0.57.1
ip route 172.16.0.2 255.255.255.255 10.0.57.1
!
mpls ldp router-id Loopback0 force
!
end
```

P

```
P_7206_g1#
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname P_7206_g1
!
ip cef
ip host lab24 172.16.0.254
ip host dirt 172.16.0.129
!
mpls label protocol ldp
mpls ldp graceful-restart
mpls ldp discovery targeted-hello accept
!
interface Loopback0
 description - FULL MESH
 ip address 10.0.0.10 255.255.255.255
!
interface Loopback1
 description - VPWS
 ip address 10.0.0.1 255.255.255.255
!
!
interface GigabitEthernet1/0
 description - VPWS to PE1
 ip address 10.0.20.6 255.255.255.0
 negotiation auto
 mpls label protocol ldp
 mpls ip
!
interface GigabitEthernet2/0
 description - FULL MESH to PE1
 ip address 10.0.2.6 255.255.255.0
 negotiation auto
 mpls label protocol ldp
 mpls ip
!
interface GigabitEthernet3/0
 description - VPWS to PE2
 ip address 10.0.0.6 255.255.255.0
 negotiation auto
 mpls label protocol ldp
 mpls ip
!
interface GigabitEthernet4/0
```

```
 description - FULL MESH to PE2
 ip address 10.0.3.6 255.255.255.0
 negotiation auto
 mpls label protocol ldp
 mpls ip
!
router ospf 10
 ! for FULL MESH
 log-adjacency-changes
 passive-interface Loopback0
 network 10.0.2.6 0.0.0.0 area 0
 network 10.0.2.0 0.0.0.255 area 0
 network 10.0.3.6 0.0.0.0 area 0
 network 10.0.3.0 0.0.0.255 area 0
 network 10.0.0.0 0.0.0.255 area 0
!
router ospf 20
 ! for VPWS
 log-adjacency-changes
 passive-interface Loopback1
 network 10.0.20.0 0.0.0.255 area 0
 network 10.21.0.0 0.0.0.255 area 0
 network 10.0.10.0 0.0.0.0 area 0
!
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.0.9.9 remote-as 1
 neighbor 10.9.0.9 update-source Loopback0
 neighbor 10.11.0.11 remote-as 1
 neighbor 10.0.11.0 update-source Loopback0
 no auto-summary
!
ip default-gateway 10.0.0.0
!
mpls ldp router-id Loopback0 force
!
```

PE2

```
PE2_7606#
!
upgrade fpd auto
!
service internal
service counters max age 10
!
hostname PE2_7606
!
boot-start-marker
boot system flash disk0:s72033-adventerprisek9_wan_dbg-mz.xx
boot-end-marker
!
no aaa new-model
!
ipv6 mfib hardware-switching replication-mode ingress
!
mls ip multicast flow-stat-timer 9
!
multilink bundle-name authenticated
mpls ldp graceful-restart
mpls ldp discovery targeted-hello accept
mpls label protocol ldp
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
!
redundancy
 mode sso
 main-cpu
```

```
  auto-sync running-config
!
vlan internal allocation policy ascending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
l2 vfi vpls_auto autodiscovery
 vpn id 1
!
l2 vfi vpls_manual manual
 vpn id 10
 neighbor 10.0.0.9 encapsulation mpls
 neighbor 10.0.0.11 encapsulation mpls
!
interface Loopback0
 description - FULL MESH
 ip address 10.0.0.12 255.255.255.255
!
interface Loopback1
 description - VPWS
 ip address 10.0.0.112 255.255.255.255
!
interface Loopback2
 description - H-VPLS
 ip address 10.0.32.0 255.255.255.255
!
interface GigabitEthernet2/1
 description - FULL MESH to CE2
 switchport
 switchport trunk allowed vlan 10-1000
 switchport mode trunk
!
interface GigabitEthernet4/0/0
 description - FULL MESH to PE3
 ip address 10.0.4.0 255.255.255.0
 negotiation auto
 mpls label protocol ldp
 mpls ip
!
interface GigabitEthernet4/1/0
 description - VPWS to P
 ip address 10.0.21.0 255.255.255.0
 negotiation auto
 mpls label protocol ldp
 mpls ip
!
interface GigabitEthernet4/1/1
 description - FULL MESH to P
 ip address 10.0.3.4 255.255.255.0
 negotiation auto
 mpls label protocol ldp
 mpls ip
!
interface GigabitEthernet4/3/0
 description - VPWS to CE2
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet4/3/1
 description - H-VPLS to nPE1
 ip address 10.0.0.3 255.255.255.0
 negotiation auto
 mpls label protocol ldp
 mpls ip
!
interface GigabitEthernet5/2
 ip address 10.0.5.0 255.255.255.0
 media-type rj45
 no cdp enable
!
interface Vlan1
 no ip address
```

```
 shutdown
!
interface Vlan10
 no ip address
 shutdown
 xconnect vfi vpls_auto
!
router ospf 10
 log-adjacency-changes
 passive-interface Loopback0
 network 10.0.3.4 0.0.0.0 area 0
 network 10.0.4.0 0.0.0.255 area 0
 network 10.0.6.4 0.0.0.0 area 0
 network 10.0.0.5 0.0.0.255 area 0
 network 10.0.0.12 0.0.0.0 area 0
 network 10.0.32.0 0.0.0.0 area 0
 network 10.0.1.0 0.0.0.0 area 0
!
router bgp 1
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 bgp update-delay 1
 neighbor 10.0.0.9 remote-as 1
 neighbor 10.0.9.0 update-source Loopback0
 neighbor 10.0.11.0 remote-as 1
 neighbor 10.0.0.11 update-source Loopback0
 neighbor 10.0.29.0 remote-as 1
 neighbor 10.0.0.29 update-source Loopback2
 !
 address-family ipv4
  no synchronization
  no auto-summary
 exit-address-family
 !
 address-family l2vpn vpls
  neighbor 10.0.0.9 activate
  neighbor 10.0.9.0 send-community both
  neighbor 10.0.11.0 activate
  neighbor 10.0.0.11 send-community both
  neighbor 10.0.0.2 activate
  neighbor 10.0.0.3 send-community both
 exit-address-family
!
ip default-gateway 10.0.0.1
ip route 172.16.0.0 255.255.255.255 10.0.57.1
ip route 172.16.0.254 255.255.255.255 10.0.57.1
!
mpls ldp router-id Loopback0 force
!
end
```

uPE2

```
uPE2_7606#
!
upgrade fpd auto
version 12.2
service timestamps debug uptime
service timestamps log uptime
service internal
!
hostname uPE2_7606
!
boot-start-marker
boot system flash disk0:s72033-adventerprisek9_wan_dbg-mz.xx
boot-end-marker
!
ipv6 mfib hardware-switching replication-mode ingress
!
multilink bundle-name authenticated
mpls ldp graceful-restart
mpls ldp discovery targeted-hello accept
```

```
mpls label protocol ldp
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
power redundancy-mode combined
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
!
vlan internal allocation policy ascending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
interface Loopback0
 description - H-VPLS
 ip address 10.0.0.13 255.255.255.255
!
interface FastEthernet3/1
 description - H-VPLS to CE2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10-1000
 switchport mode trunk
!
interface GigabitEthernet4/0/0
 description - H-VPLS to uPE2
 ip address 10.0.0.2 255.255.255.0
 negotiation auto
 mpls label protocol ldp
 mpls ip
!
interface GigabitEthernet5/2
 ip address 10.0.0.11 255.255.255.0
 media-type rj45
 no cdp enable
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 10
 log-adjacency-changes
 passive-interface Loopback0
 network 10.0.6.0 0.0.0.255 area 0
 network 10.0.0.13 0.0.0.0 area 0
!
ip default-gateway 10.0.0.1
ip route 172.16.1.129 255.255.255.255 10.0.57.1
ip route 172.16.192.254 255.255.255.255 10.0.57.1
!
mpls ldp router-id Loopback0 force
!
control-plane
!
end
```

CE2

```
CE2_7206#
!
hostname CE2_7206
!
ip cef
!
interface Loopback0
 ip address 10.0.0.123 255.255.255.255
!
interface FastEthernet1/0
```

```
 description - H-VPLS VPN to uPE2
 no ip address
 no ip mroute-cache
 duplex auto
 speed auto
!
interface FastEthernet1/0.1
 description - H-VPLS VPN to uPE2
 encapsulation dot1Q 10
 ip address 10.0.0.121 255.255.255.0
!
interface Ethernet2/0
 ip address 10.0.0.97 255.255.255.0
 no ip mroute-cache
 duplex half
 no cdp enable
!
interface FastEthernet4/0
 description - FULL MESH VPN to PE2
 no ip address
 no ip mroute-cache
 duplex auto
 speed auto
!
interface FastEthernet4/0.1
 description - FULL MESH VPN to PE2
 encapsulation dot1Q 10
 ip address 10.0.0.121 255.255.255.0
!
interface GigabitEthernet5/0
 description - VPWS VPN to PE2
 no ip address
 no ip mroute-cache
 no negotiation auto
!
interface GigabitEthernet5/0.1
 description - VPWS VPN to PE2
 encapsulation dot1Q 10
 ip address 10.0.0.121 255.255.255.0
!
router ospf 10
 log-adjacency-changes
 network 10.0.1.0 0.0.0.255 area 0
 network 10.0.0.1 0.0.0.255 area 0
 network 10.0.0.123 0.0.0.0 area 0
!
ip default-gateway 10.0.0.4
!
end
```

PE3

```
PE3_7606#
!
upgrade fpd auto
version 12.2
service timestamps debug uptime
service timestamps log uptime
service internal
!
hostname PE3_7606
!
boot-start-marker
boot system flash disk0:s72033-adventerprisek9_wan_dbg-mz.xx
boot-end-marker
!
ipv6 mfib hardware-switching replication-mode ingress
!
multilink bundle-name authenticated
mpls ldp graceful-restart
mpls ldp discovery targeted-hello accept
mpls label protocol ldp
```

```
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
!
vlan internal allocation policy ascending
vlan dot1q tag native
vlan access-log ratelimit 2000
l2 vfi vpls_auto autodiscovery
 vpn id 1
!
l2 vfi vpls_manual manual
 vpn id 10
 neighbor 10.0.9.9 encapsulation mpls
 neighbor 10.0.0.12 encapsulation mpls
!
interface Loopback0
 description - FULL MESH
 ip address 10.0.0.11 255.255.255.255
!
interface Loopback1
 description - H-VPLS
 ip address 10.0.0.31 255.255.255.255
!
interface GigabitEthernet3/2/1
 description - FULL MESH to PE1
 ip address 10.0.0.5 255.255.255.0
 negotiation auto
 mpls label protocol ldp
 mpls ip
!
interface GigabitEthernet5/2
 ip address 10.0.0.115 255.255.255.0
 media-type rj45
 no cdp enable
!
interface GigabitEthernet6/2
 description - FULL MESH to CE3
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10-1000
 switchport mode trunk
 no cdp enable
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 10
 log-adjacency-changes
 passive-interface Loopback0
 network 10.0.4.0 0.0.0.255 area 0
 network 10.0.0.11 0.0.0.0 area 0
 network 10.0.31.0 0.0.0.0 area 0
!
router bgp 1
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 bgp update-delay 1
 neighbor 10.0.0.9 remote-as 1
 neighbor 10.0.9.0 update-source Loopback0
 neighbor 10.0.12.0 remote-as 1
 neighbor 10.0.0.12 update-source Loopback0
 !
 address-family ipv4
  no synchronization
  no auto-summary
 exit-address-family
```

```
 !
 address-family l2vpn vpls
  neighbor 10.0.9.0 activate
  neighbor 10.0.0.9 send-community both
  neighbor 10.0.0.12 activate
  neighbor 10.0.12.0 send-community both
 exit-address-family
!
ip default-gateway 10.0.57.1
ip route 172.16.0.129 255.255.255.255 10.0.57.1
ip route 172.16.0.254 255.255.255.255 10.0.57.1
!
mpls ldp router-id Loopback0 force
!
end
```

Additional References

The following sections provide references related to the NSF/SSO/ISSU Support for VPLS feature.

Related Documents

Related Topic	Document Title
Stateful switchover	Stateful Switchover
MPLS Label Distribution Protocol	MPLS Label Distribution Protocol (LDP)
Cisco nonstop forwarding	Cisco Nonstop Forwarding
Any Transport over MPLS	Any Transport over MPLS
NSF/SSO: Any Transport over MPLS	NSF/SSO—Any Transport over MPLS and AToM Graceful Restart
L2VPN Interworking configuration	L2VPN Interworking
VPLS	See the "Virtual Private LAN Services on the Optical Services Modules" chapter in the Cisco 7600 Series Router Cisco IOS Software Configuration Guide , Release 12.2SR)
VPLS Autodiscovery	See VPLS Autodiscovery: BGP Based and BGP Support for the L2VPN Address Family
NSF/SSO router support on the 7600 router	See the "Configuring NSF with SSO Supervisor Engine Redundancy" chapter in the Cisco 7600 Series Cisco IOS Software Configuration Guide , Release 12.2SR
ISSU router support on the 7600 router	See the "ISSU and eFSU on Cisco 7600 Series Routers" chapter in the Cisco 7600 Series Cisco IOS Software Configuration Guide , Release 12.2SR

Standards

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

MIBs

MIB	MIBs Link
MPLS Label Distribution Protocol MIB Version 8 Upgrade	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

RFC	Title
RFC 3036	*LDP Specification*
RFC 3478	*Graceful Restart Mechanism for Label Distribution*

Technical Assistance

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

Feature Information for NSF SSO ISSU Support for VPLS

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

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

Table 15 Feature Information for NSF/SSO/ISSU Support for VPLS

Feature Name	Releases	Feature Information
NSF/SSO/ISSU Support for VPLS	12.2(33)SRC	Virtual Private LAN Services (VPLS), with NSF/SSO/ISSU support, improves the availability of service provider networks that use VPLS for multipoint Layer 2 VPN services. Cisco nonstop forwarding (NSF) with stateful switchover (SSO) is effective at increasing availability of network services. In 12.2(33)SRC, this feature was introduced on the Cisco 7600 router.

NSF SSO and ISSU—MPLS VPN 6VPE and 6PE

This document provides information about configuring nonstop forwarding (NSF), stateful switchover (SSO), and In Service Software Upgrade (ISSU) support for Cisco IOS Virtual Private Network (VPN) IPv6 provider edge router (6VPE) and Cisco IOS IPv6 provider edge router (6PE) over Multiprotocol Label Switching (MPLS).

Finding Feature Information

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

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

Prerequisites for NSF SSO and ISSU—MPLS VPN 6VPE and 6PE

Ensure that the following are supported for the NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE feature to work:

- IPv6 NSF
- IPv6 Cisco Express Forwarding
- Label Distribution Protocol (LDP) Graceful Restart

LDP Graceful Restart should be enabled if LDP is the protocol used in the MPLS core

You must enable NSF on the following routing protocol that run between the provider (P) routers, PE routers, and the customer edge (CE) routers:

- Border Gateway Protocol (BGP)
- Static routes

Before enabling the NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE feature, you must have a supported MPLS VPN network configuration. See 1the configuration information included in the following modules: Configuring MPLS Layer 3 VPNs , Implementing IPv6 over MPLS , and Implementing IPv6 VPN over MPLS .

Restrictions for NSF SSO and ISSU—MPLS VPN 6VPE and 6PE

The NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE feature has the following restrictions:

- Tag Distribution Protocol (TDP) sessions are not supported. Only LDP sessions are supported.
- MPLS VPN 6VPE and 6PE Carrier Supporting Carrier (CSC) VPNs support only BGP. CSC configurations that use LDP are not supported.
- Only BGP and static routes are supported for 6VPE and 6PE in Cisco IOS Release 12.2(33)SRE.

Information About NSF SSO and ISSU—MPLS VPN 6VPE and 6PE

Elements Supporting NSF SSO and ISSU—MPLS VPN 6VPE and 6PE Features

The major elements supporting the functionality of the NSF/SSO and ISSU for Cisco IOS VPN 6vPE and 6PE feature are the following:

- MPLS VPN—A supported MPLS VPN network must be configured before you enable the NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE feature
- BGP Graceful Restart—The BGP Graceful Restart feature is responsible for negotiating graceful restart capabilities, exchanging forwarding preservation states, and coordinating advertisements after session restarts. MPLS VPNs interact with BGP to exchange Virtual Private Network (VPN) routing and forwarding (VRF) routes and labels.

- IPv6 NSF—IPv6 NSF support enables IPv6 cache rebuilds during switchover using checkpointed Cisco Express Forwarding adjacencies.
- CEF/MFI—Cisco Express Forwarding and the MPLS Forwarding Infrastructure are responsible for preserving forwarding entries and local labels across Route Processor (RP) switchover.

How BGP Graceful Restart Works for MPLS VPN 6vPE and 6PE

BGP Graceful Restart behavior for IPv6 and VPNv6 is essentially the same as Graceful Restart behavior for IPv4 and VPNv4; the only difference is the addition of support for IPv6 and VPNv6 address families.

When you configure BGP Graceful Restart, BGP includes the Graceful Restart capability and negotiates the preservation states of address families, that is, IPv4/VPNv4 and IPv6/VPNv6 address families.

Both BGP peers must agree on a Graceful Restart timer, which you can set with the **bgp graceful-restart restart-timer** *seconds* command. After a BGP session comes up and finishes sending initial updates, each BGP peer sends an end-of-Routing Information Base (RIB) marker.

The NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE feature uses the mechanisms defined in the RFC 4724, Graceful Restart Mechanism for BGP , and in the Cisco Nonstop Forwarding feature module.

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-RIB markers to indicate that they are done sending updates, the restarting router starts sending its own updates.
2. The restarting router recovers labels from the MPLS Forwarding Infrastructure (MFI) database for each prefix. If the router finds the label, it advertises the label to the neighboring router. If the router does not find the label, it allocates a new label from the database 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.

ISSU Support for MPLS VPN 6vPE and 6PE

In Cisco IOS Release 12.2(33)SRE and future releases, ISSU supports MPLS VPN 6vPE and 6PE. The Cisco IOS ISSU process allows Cisco IOS software to be updated or otherwise modified while packet forwarding continues. In most networks, planned software upgrades are a significant cause of downtime. ISSU allows Cisco IOS software to be modified while packet forwarding continues, which increases network availability and reduces downtime caused by planned software upgrades.

ISSU support for MPLS 6vPE and 6PE relies on 6vPE and 6PE NFS/SSO capability on the platform to minimize disruption on the forwarding plane.

For more information about ISSU, see Cisco IOS In Service Software Upgrade Process .

NSF SSO Support for MPLS VPN 6VPE and 6PE

In Cisco IOS Release 12.2(33)SRE and future releases, NFS/SSO supports MPLS VPN 6vPE and 6PE.

NSF/SSO for 6VPE and 6PE supports the following configurations:

- NSF/SSO for IPv4 and VPNv4 coexistence
- Basic 6VPE and 6PE over MPLS core technology
- BGP multipath configuration

NSF/SSO for 6VPE supports the following configurations:

- Per-VRF label configuration
- Interautonomous systems (Inter-AS) topologies, including options B and C
- CSC when IPv6 + labels is configured on the PE-customer edge (CE) link

Because the SSO feature maintains stateful protocol and application information, user session information is maintained during a switchover, and line cards continue to forward network traffic with no loss of sessions, providing improved network availability. SSO initializes and configures the standby RP and synchronizes state information, which can reduce the time required for routing protocols to converge. Network stability may be improved with the reduction in the number of route flaps created when routers in the network failed and lost their routing tables.

When RP switchover happens, forwarding information is preserved by MFI and Cisco Express Forwarding on both line cards and the standby RP. VPNv6 prefix and local label mapping is preserved in the forwarding database. When the standby RP becomes the new active RP, 6PE and 6vPE traffic continues to be forwarded with minimal interruption.

When a BGP session restarts on the new active RP, the new active RP does not have any prior state information about prefixes or labels. The new active RP will have to relearn VPNv6 prefixes from its peers. As the new active RP learns the VPNv6 prefixes, it tries to get new local labels the same way it does when it first comes up. If the MFI database has the preserved copy of the local label for a prefix, the MFI database gives the local label to BGP. Then, BGP maintains the same local label. If the MFI database does not have a preserved local label for the prefix, MFI allocates a new one.

BGP Graceful Restart Support for MPLS VPN Configurations

The section describes BGP Graceful Restart support for a basic 6VPE setup and for a CSC setup and interautonomous system setup.

- Graceful Restart Support for a Basic 6VPE Setup, page 174
- Graceful Restart for 6VPE in Carrier Supporting Carrier and Interautonomous System Setups, page 175

Graceful Restart Support for a Basic 6VPE Setup

For PE- to-CE external BGP (eBGP), Graceful Restart capability is supported for IPv6 address families. For PE-to-PE interior BGP (iBGP) sessions with or without a route reflector (RR) in the core, BGP Graceful Restart capability supports VPNv6 address families.

When the PE router resets, the connected CE router retains IPv6 prefixes that it received from the PE router and marks the prefixes as stale. If the eBGP session does not reestablish within the specified restart time or the session reestablishes, but does not set the restart or forwarding state bit, the CE router removes the staled IPv6 routes. If the eBGP session reestablishes within the specified restart time and has both the forwarding and restart bits set, the CE router removes the stale state from the IPv6 routes when it receives the updates from PE router. After the CE router receives the end-of-RIB marker, it removes or withdraws the rest of the staled information, if any exists.

The restarting PE router waits for an end-of-RIB marker from all BGP-capable peers including iBGP peers and eBGP peers. Only after receiving an end-of-RIB marker from all BGP capable peers will the PE router start to calculate the best path and send out initial updates.

Graceful Restart for 6VPE in Carrier Supporting Carrier and Interautonomous System Setups

The same Graceful Restart capabilities for route preservation that apply to a basic 6VPE setup apply to a CSC and Inter-AS setup. IPv6 or VPNv6 routes and labels are preserved during switchover.

In a CSC configuration, when send-labels are configured between a CSC-PE and CSC-CE eBGP connection, labels are preserved along with IPv6 BGP routes when one of the peers restarts.

In Inter-AS option B and options C setups, VPNv6 routes and labels are preserved on an Autonomous System Border Router (ASBR) or route reflector when the VPNv6 peer restarts.

What Happens If a Router Does Not Support NSF SSO and ISSU—MPLS VPN 6VPE and 6PE

If a router does not support the NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE feature, prefix and label information is not preserved. After a switchover, BGP has to restart, relearn all routes, and install labels in the forwarding database. This might result in the loss of some network traffic.

How to Configure NSF SSO and ISSU—MPLS VPN 6VPE and 6PE

For information on how to configure ISSU, see the Cisco IOS In Service Software Upgrade Process module.

- Configuring NSF SSO for Basic MPLS 6VPEs and 6PEs, page 175
- Verifying NSF SSO and ISSU Support for MPLS VPN 6VPE and 6PE, page 178

Configuring NSF SSO for Basic MPLS 6VPEs and 6PEs

Perform this task to configure NSF/SSO for basic MPLS 6VPE and 6PEs.

Note You can use the **bgp graceful-restart** command to configure BGP Graceful Restart for all available address families.

Route Processors must be configured for SSO. See Stateful Switchover for more information.

If you use LDP in the core, you must enable the MPLS LDP: NSF/SSO Support and Graceful Restart feature. See NSF/SSO-MPLS LDP and MPLS LDP Graceful Restart for more information.

You must enable nonstop forwarding on the routing protocols running between the P, PE, and CE routers. The routing protocols between the CE router and the PE router are Static and BGP. See Cisco Nonstop Forwarding for more information.

Before enabling the NSF/SSO—MPLS VPN feature, you must have a supported MPLS VPN network configuration. See configuration information included in the following: Configuring MPLS Layer 3 VPNs , Implementing IPv6 over MPLS , and Implementing IPv6 VPN over MPLS .

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef distributed**
4. **ipv6 unicast-routing**
5. **ipv6 cef distributed**
6. **redundancy**
7. **mode sso**
8. **exit**
9. **router bgp** *autonomous-system-number*
10. **bgp graceful-restart restart-time** *seconds*
11. **bgp graceful-restart stalepath-time** *seconds*
12. **bgp graceful-restart**
13. 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 distributed Cisco Express Forwarding.
Step 4	**ipv6 unicast-routing** **Example:** `Router(config)# ipv6 unicast-routing`	Enables the forwarding of IPv6 unicast datagrams.

	Command or Action	Purpose
Step 5	**ipv6 cef distributed** **Example:** `Router(config)# ipv6 cef distributed`	Enables distributed Cisco Express Forwarding for IPv6.
Step 6	**redundancy** **Example:** `Router(config)# redundancy`	Enters redundancy configuration mode.
Step 7	**mode sso** **Example:** `Router(red-config)# mode sso`	Sets the redundancy configuration mode to SSO.
Step 8	**exit** **Example:** `Router(red-config)# exit`	Exits to global configuration mode.
Step 9	**router bgp** *autonomous-system-number* **Example:** `Router(config)# router bgp 1000`	Enters router configuration mode and configures the BGP routing process. • The *autonomous-system-number*argument is the number of an autonomous system that identifies the router to other BGP routers and tags the routing information that is passed along. Number is in the range from 1 to 65535.
Step 10	**bgp graceful-restart restart-time** *seconds* **Example:** `Router(config-router)# bgp graceful-restart restart-time 180`	Enables the BGP graceful restart timer capability globally for all BGP neighbors. • The **restart-time** *seconds* keyword and argument sets the maximum time period that the local router will wait for a graceful-restart-capable neighbor to return to normal operation after a restart event occurs. The default value for the *seconds* argument is 120. The configurable range of values is from 1 to 3600.

	Command or Action	Purpose
Step 11	**bgp graceful-restart stalepath-time** *seconds* **Example:** `Router(config-router)# bgp graceful-restart stalepath-time 420`	Enables the BGP graceful restart stale path timer capability globally for all BGP neighbors. • The **stalepath-time** *seconds* keyword and argument sets the maximum time period that the local router will hold stale paths for a restarting peer. All stale paths are deleted after this timer expires. The default value for the *seconds* argument is 360. The configurable range of values is from 1 to 3600.
Step 12	**bgp graceful-restart** **Example:** `Router(config-router)# bgp graceful-restart`	Enables the BGP graceful restart capability globally for all BGP neighbors.
Step 13	end **Example:** `Router(config-router)# end`	Exits to privileged EXEC mode.

Verifying NSF SSO and ISSU Support for MPLS VPN 6VPE and 6PE

Perform this task to verify NSF/SSO and ISSU support for 6VPE and 6PE.

SUMMARY STEPS

1. **enable**
2. **show ip bgp neighbor**
3. **show ip bgp vpnv6 unicast vrf** *vrf-name*
4. **show ip bgp ipv6 unicast**
5. **show mpls forwarding**
6. **show ipv6 cef vrf** *vrf-name*

DETAILED STEPS

Step 1 **enable**

Use this command to enable privileged EXEC mode. Enter your password if prompted. For example:

Example:

```
Router> enable
Router#
```

Step 2 **show ip bgp neighbor**

Use this command to verify that the IPv6 address family and VPNv6 address family entries are preserved. For example:

Example:

```
Router# show ip bgp neighbor
BGP neighbor is 10.2.2.2, remote AS 100, internal link
  BGP version 4, remote router ID 10.2.2.2
  BGP state = Established, up for 00:02:42
  Last read 00:00:36, last write 00:00:36, hold time is 180, keepalive
.
.
.
  Neighbor capabilities:
.
.
.
    Graceful Restart Capability: advertised and received
      Remote Restart timer is 120 seconds
      Address families advertised by peer:
        IPv6 Unicast (was preserved), VPNv6 Unicast (was preserved)
```

IPv6 Unicast (was preserved), VPNv6 Unicast (was preserved) is displayed in the Graceful Restart Capability section of the output only after the peer restarts.

Step 3 **show ip bgp vpnv6 unicast vrf** *vrf-name*

Use this command to verify that VPNv6 entries are marked as staled during switchover. For example:

Example:

```
Router# show ip bgp vpnv6 unicast vrf vpn1
BGP table version is 10, local router ID is 10.4.4.4
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 vpn1)
S>iA::1/128         ::FFFF:10.2.2.2         0    100      0 200 ?
*> A::5/128         A::4:5:5                0             0 200 ?
S>iA::1:2:0/112     ::FFFF:10.2.2.2         0    100      0 ?
*  A::4:5:0/112     A::4:5:5                0             0 200 ?
```

Step 4 **show ip bgp ipv6 unicast**

Use this command to verify that VPNv6 entries are marked as staled during switchover. For example:

Example:

```
Router# show ip bgp ipv6 unicast
BGP table version is 9, local router ID is 10.1.1.1
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
*> A::1/128         ::                       0         32768 ?
S  A::1:2:0/112     A::1:2:2                 0             0 100 ?
*>                  ::                       0         32768 ?
S> A::4:5:0/112     A::1:2:2                               0 100 ?
Router#
```

Step 5 **show mpls forwarding**

Use this command to show preserved forwarding entries for IPv6 and VPNv6 prefixes. The sample output is from a PE router in a CSC configuration. Enter the command on the active and the standby router. Compare the sample output from the active router with the sample output from the standby router. Following is sample output from the active router;

Example:

```
Router# show mpls forwarding
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
18         Pop Label      10.3.3.3/32      0             Et1/0      10.2.3.3
19         Pop Label      10.3.4.0/24      0             Et1/0      10.2.3.3
20         17             10.4.4.4/32      0             Et1/0      10.2.3.3
21         Pop Label      10.1.2.1/32[V]   0             Et0/0      10.1.2.1
22         Pop Label      A::1:2:0/112[V]  0             aggregate/vpn1
23         Pop Label      A::1:2:1/128[V]  0             Et0/0      A::1:2:1
24         Pop Label      10.1.2.0/24[V]   0             aggregate/vpn1
25         Pop Label      A::1:2:2/128[V]  0             aggregate/vpn1
26         18             A::1/128[V]      0             Et0/0
FE80::A8BB:CCFF:FE03:2101
27         26             10.4.5.5/32[V]   0             Et1/0      10.2.3.3
28         25             10.4.5.0/24[V]   0             Et1/0      10.2.3.3
29         22             A::4:5:5/128[V]  0             Et1/0      10.2.3.3
30         21             A::4:5:0/112[V]  0             Et1/0      10.2.3.3
31         23             A::4:5:4/128[V]  0             Et1/0      10.2.3.3
32         24             A::5/128[V]      0             Et1/0      10.2.3.3
33         Pop Label      10.1.2.2/32[V]   0             aggregate/vpn1
34         Pop Label      10.1.1.1/32[V]   0             Et0/0      10.1.2.1
35         27             10.4.5.4/32[V]   0             Et1/0      10.2.3.3
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
36         28             10.5.5.5/32[V]   0             Et1/0      10.2.3.3
```

Following is sample output from the standby router:

Example:

```
Standby-Router# show mpls forwarding
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
18         Pop Label      10.3.3.3/32      0             Et1/0      10.2.3.3
19         Pop Label      10.3.4.0/24      0             Et1/0      10.2.3.3
20         17             10.4.4.4/32      0             Et1/0      10.2.3.3
21         Pop Label      10.1.2.1/32[V]   0             Et0/0      10.1.2.1
22         Pop Label      A::1:2:0/112[V]  0             aggregate/vpn1
23         Pop Label      A::1:2:1/128[V]  0             Et0/0      A::1:2:1
24         Pop Label      10.1.2.0/24[V]   0             aggregate/vpn1
25         Pop Label      A::1:2:2/128[V]  0             aggregate/vpn1
26         18             A::1/128[V]      0             Et0/0
FE80::A8BB:CCFF:FE03:2101
27         26             10.4.5.5/32[V]   0             Et1/0      10.2.3.3
28         25             10.4.5.0/24[V]   0             Et1/0      10.2.3.3
29         22             A::4:5:5/128[V]  0             Et1/0      10.2.3.3
30         21             A::4:5:0/112[V]  0             Et1/0      10.2.3.3
31         23             A::4:5:4/128[V]  0             Et1/0      10.2.3.3
32         24             A::5/128[V]      0             Et1/0      10.2.3.3
33         Pop Label      10.1.2.2/32[V]   0             aggregate/vpn1
34         Pop Label      10.1.1.1/32[V]   0             Et0/0      10.1.2.1
35         27             10.4.5.4/32[V]   0             Et1/0      10.2.3.3
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
36         28             10.5.5.5/32[V]   0             Et1/0      10.2.3.3
```

Step 6 **show ipv6 cef vrf** *vrf-name*

Use this command to show preserved forwarding entries for IPv6 and VPNv6 prefixes. This sample output is also from a PE router in a CSC configuration. Enter the command on the active and the standby router. Compare the sample output from the active router with the sample output from the standby router. Following is the output from the active router:

Example:

```
Router# show ipv6 cef vrf vrf1
::/0
  no route
::/127
  discard
A::1/128
  nexthop FE80::A8BB:CCFF:FE03:2101 Ethernet0/0 label 18
A::5/128
  nexthop 10.2.3.3 Ethernet1/0 label 17 24
A::1:2:0/112
  attached to Ethernet0/0
A::1:2:1/128
  attached to Ethernet0/0
A::1:2:2/128
  receive for Ethernet0/0
A::4:5:0/112
  nexthop 10.2.3.3 Ethernet1/0 label 17 21
A::4:5:4/128
  nexthop 10.2.3.3 Ethernet1/0 label 17 23
A::4:5:5/128
  nexthop 10.2.3.3 Ethernet1/0 label 17 22
FE80::/10
```

Following is sample output from the standby router:

Example:

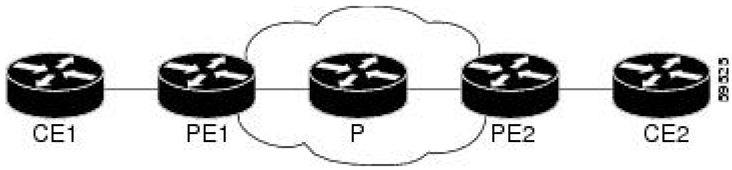
```
Standby-Router# show ipv6 cef vrf vrf1
::/0
  no route
::/127
  discard
A::1/128
  nexthop FE80::A8BB:CCFF:FE03:2101 Ethernet0/0 label 18
A::5/128
  nexthop 10.2.3.3 Ethernet1/0 label 17 24
A::1:2:0/112
  attached to Ethernet0/0
A::1:2:1/128
  attached to Ethernet0/0
A::1:2:2/128
  receive for Ethernet0/0
A::4:5:0/112
  nexthop 10.2.3.3 Ethernet1/0 label 17 21
A::4:5:4/128
  nexthop 10.2.3.3 Ethernet1/0 label 17 23
A::4:5:5/128
  nexthop 10.2.3.3 Ethernet1/0 label 17 22
FE80::/10
```

Configuration Examples for Configuring NSF SSO and ISSU—MPLS VPN 6VPE and 6PE

Configuring NSF SSO for a Basic 6VPE Setup Example

This section shows the NSF/SSO configuration for a basic 6VPE setup. The figure below show a sample basic 6VPE network configuration.

Figure 7 Sample Basic 6VPE Network Configuration



• PE1 Configuration in a Basic 6VPE Setup, page 182

PE1 Configuration in a Basic 6VPE Setup

Following is a configuration example for a PE1 router (see the figure above) in a basic 6VPE setup that includes VPNv6 and VPNv6 address families:

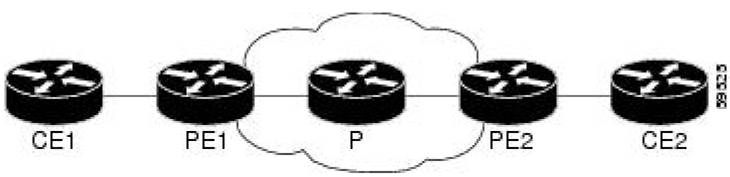
```
vrf definition vpn1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
!
ip cef distributed
!
ipv6 unicast-routing
ipv6 cef distributed
mpls ldp graceful-restart ! <==+ Command to configure LDP Graceful Restart
mpls label protocol ldp
redundancy
 mode sso
interface Loopback0
 ip address 10.2.2.2 255.255.255.255
 ipv6 address A::2/128
!
interface Ethernet0/0
 vrf forwarding vpn1
 ip address 10.1.2.2 255.255.255.0
 ipv6 address A::1:2:2/112
!interface Ethernet1/0
 ip address 10.2.3.2 255.255.255.0
 mpls label protocol ldp
 mpls ip
!router ospf 10
 log-adjacency-changes
 nsf
 network 0.0.0.0 255.255.255.255 area 0
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120      ! <=== This command,
 bgp graceful-restart stalepath-time 360    ! <=== this command, and
 bgp graceful-restart            ! <=== this command configures NFS/SSO for a 6VPE router.
```

```
neighbor 10.4.4.4 remote-as 100
neighbor 10.4.4.4 update-source Loopback0
no auto-summary
!
address-family vpnv4
 neighbor 10.4.4.4 activate
 neighbor 10.4.4.4 send-community extended
exit-address-family
!
address-family vpnv6
 neighbor 10.4.4.4 activate
 neighbor 10.4.4.4 send-community extended
exit-address-family
!
address-family ipv4 vrf vpn1
 no synchronization
 redistribute connected
 redistribute static
 neighbor 10.1.2.1 remote-as 200
 neighbor 10.1.2.1 update-source Ethernet0/0
 neighbor 10.1.2.1 activate
exit-address-family
!
address-family ipv6 vrf vpn1
 redistribute connected
 redistribute static
 no synchronization
 neighbor A::1:2:1 remote-as 200
 neighbor A::1:2:1 update-source Ethernet0/0
 neighbor A::1:2:1 activate
exit-address-family
```

Configuring NSF SSO for a Basic 6PE Setup Example

This section shows the NSF/SSO configuration for a basic 6PE setup. The figure below shows a sample basic 6PE network configuration.

Figure 8 Sample Basic 6PE Network Configuration



- PE1 Configuration in a Basic 6PE Setup, page 183

PE1 Configuration in a Basic 6PE Setup

Following is a configuration example for the PE1 router (see the figure above) in a basic 6PE setup:

```
ip cef distributed
!
ipv6 unicast-routing
ipv6 cef distributed
mpls ldp graceful-restart ! <=== Command to configure LDP Graceful Restart
mpls label protocol ldp
redundancy
 mode sso
interface Loopback0
 ip address 10.11.11.1 255.255.255.255
 ipv6 address BEEF:11::1/64
interface Ethernet0/0
 ip address 10.50.1.2 255.255.255.0
```

```
 ipv6 address 4000::72B/64
 ipv6 address 8008::72B/64
!
interface Ethernet1/0
 ip address 10.40.1.2 255.255.255.0
 mpls ip
!
router ospf
nsf
network 0.0.0.0 0.0.0.0 area 0
!
router bgp 100
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120               ! <=== This command,
 bgp graceful-restart stalepath-time 360             ! <=== this command, and
 bgp graceful-restart             ! <=== this command configures NFS/SSO for a 6PE
router.
 neighbor 8008::72A remote-as 200
 neighbor 10.10.10.1 remote-as 100
 neighbor 10.10.10.1 update-source Loopback0
 !
 address-family ipv4
  no synchronization
  redistribute connected
  no neighbor 8008::72A activate
  neighbor 10.10.10.1 activate
  no auto-summary
 exit-address-family
 !
 address-family ipv6
  redistribute connected
  no synchronization
  neighbor 8008::72A activate
  neighbor 10.10.10.1 activate
  neighbor 10.10.10.1 send-label
 exit-address-family
```

Additional References

The following sections provide references related to the NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE feature.

Related Documents

Related Topic	Document Title
Information about NFS/SSO for MPLS VPN	NSF/SSO—MPLS VPN
Information about and configuration tasks for Cisco nonstop forwarding	Cisco Nonstop Forwarding
Information about and configuration tasks for MPLS VPNs	Configuring MPLS Layer 3 VPNs
Information about and configuration tasks for 6VPE over MPLS	Implementing IPv6 VPN over MPLS
Information about and configuration tasks for 6PE over MPLS	Implementing IPv6 over MPLS
Information about and configuration tasks for ISSU	Cisco IOS In Service Software Upgrade Process

Related Topic	Document Title
Information about and configuration tasks for SSO	Stateful Switchover
Information about and configuration tasks for MPLS LDP NSF/SSO and Graceful Restart	NSF/SSO-MPLS LDP and MPLS LDP Graceful Restart

Standards

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

MIBs

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

RFCs

RFC	Title
RFC 4659	BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN
RFC 4724	Graceful Restart Mechanism for BGP
RFC 4781	Graceful Restart Mechanism for BGP with MPLS
FRC 4798	Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)

Technical Assistance

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

Feature Information for NSF SSO and ISSU—MPLS VPN 6VPE and 6PE

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

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

Table 16 Feature Information for NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE

Feature Name	Releases	Feature Information
ISSU—MPLS VPN 6VPE and 6PE ISSU Support	12.2(33)SRE 12.2(33)XNE 15.0(1)SY	This feature provides In Service Software Upgrade (ISSU) support for Cisco IOS Virtual Private Network (VPN) IPv6 provider edge router (6VPE) over Multiprotocol Label Switching (MPLS) and Cisco IOS IPv6 provider edge router (6PE) over MPLS. In 12.2(33)SRE, this feature was introduced on the Cisco 7600 series routers. The following sections provide information about this feature: This feature introduced no new or modified commands.
SSO—MPLS VPN 6VPE and 6PE SSO Support	12.2(33)SRE 12.2(33)XNE 15.0(1)SY	This feature provides stateful switchover (SSO) support for Cisco IOS Virtual Private Network (VPN) IPv6 provider edge router (6VPE) over Multiprotocol Label Switching (MPLS) and Cisco IOS IPv6 provider edge router (6PE) over MPLS. In 12.2(33)SRE, this feature was introduced on the Cisco 7600 series routers. The following sections provide information about this feature: This feature introduced no new or modified commands.

Glossary

6PE router —IPv6 provider edge (PE) router. A router running a Border Gateway Protocol (BGP)-based mechanism to interconnect IPv6 islands over a Multiprotocol Label Switching (MPLS)-enabled IPv4 cloud.

6VPE router —Provider edge router providing Border Gateway Protocol (BGP)-Multiprotocol Label Switching (MPLS) IPv6 Virtual Private Network (VPN) service over an IPv4-based MPLS core. It is a IPv6 VPN provider edge (PE), dual-stack router that implements 6PE concepts on the core-facing interfaces.

BGP —Border Gateway Protocol. An interdomain routing protocol designed for the global Internet. Exterior Border Gateway Protocols (eBGPs) communicate among different autonomous systems. Interior Border Gateway Protocols (iBGPs) communicate among routers within a single autonomous system.

CE router —customer edge router. A router that is part of a customer network and interfaces to a provider edge (PE) router.

Cisco Express Forwarding —An advanced Layer 3 IP switching technology. It optimizes network performance and scalability for all kinds of networks.

eBGP —external Border Gateway Protocol.

graceful restart —A process for helping an RP restart after a node failure has occurred.

iBGP —Interior Border Gateway Protocol.

ISSU —In Service Software Upgrade. Software upgrade without service interruption.

LDP —Label Distribution Protocol. A standard protocol between Multiprotocol Label Switching (MPLS)-enabled routers to negotiate the labels (addresses) used to forward packets.

MPLS —Multiprotocol Label Switching. A switching method that forwards IP traffic using a label. This label instructs the routers and switches in the network where to forward the packets based on preestablished IP routing information.

NSF —nonstop forwarding. The ability of a router to continue to forward traffic to a router that may be recovering from a failure. Also, the ability of a router recovering from a failure to continue to correctly forward traffic sent to it by a peer.

PE router —provider edge router. The PE router is the entry point into the service provider network. The PE router is typically deployed on the edge of the network and is administered by the service provider. The PE router is the redistribution point between EIGRP and BGP in PE to CE networking.

RIB —Routing Information Base. Also called the routing table.

SSO —stateful switchover. SSO refers to the implementation of Cisco IOS software that allows applications and features to maintain a defined state between an active and standby RP. When a switchover occurs, forwarding and sessions are maintained. Along with NSF, SSO makes an RP failure undetectable to the network.

VPN —Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting traffic from one network to another. A VPN uses tunneling to encrypt all information at the IP level.

VRF —Virtual Private Network (VPN) routing and forwarding instance. A VRF consists of an IP routing table, a derived routing table, a set of interfaces that use the forwarding table. and a set of rules and routing information that defines a customer VPN site that is attached to a provider edge (PE) router.