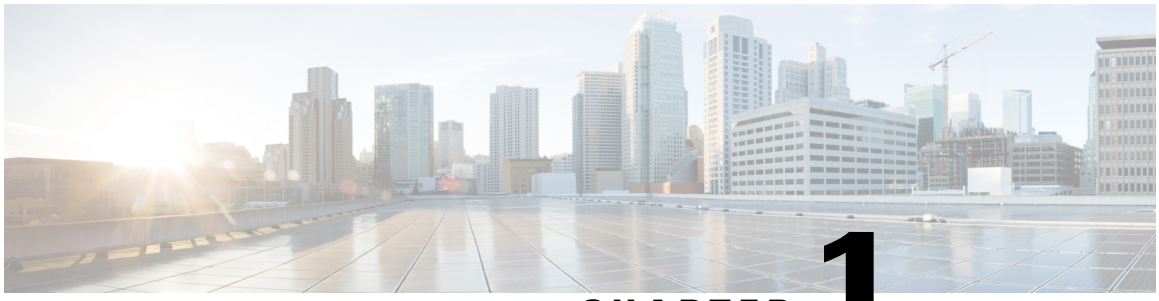
MPLS High Availability Configuration Guide, Cisco IOS XE Release 3S

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



CHAPTER 1

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. 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 the router recover.

For brevity, the following are used in this document:

- MPLS LDP SSO/NSF Support and Graceful Restart is called LDP SSO/NSF.
- 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 caveats and feature information, see Bug Search Tool and 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 module.

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 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.

Restrictions for MPLS LDP Graceful Restart

- MPLS LDP GR is supported in strict helper mode.
- MPLS LDP GR cannot be configured on label-controlled ATM (LC-ATM) interfaces.

Information About MPLS LDP Graceful Restart

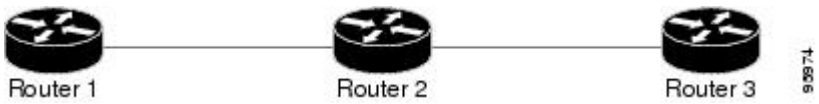
How MPLS LDP Graceful Restart Works

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 MPLS 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 **showmplsldpneighbor** 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 **showmplsforwarding-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 (RP) that is configured to perform MPLS LDP GR includes the Fault Tolerant (FT) Type Length Value (TLV) in the LDP initialization message. The RP 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 MPLS 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

To configure MPLS LDP Graceful Restart, perform the following task.

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.

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef distributed**
4. **mpls ldp graceful-restart**
5. **interface** *type slot* / *subslot* / *port* [**.** *subinterface-number*]
6. **mpls ip**
7. **mpls label protocol ldp**
8. **exit**
9. **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.

	Command or Action	Purpose
Step 3	**ip cef distributed** **Example:** `Router(config)# ip cef distributed`	Enables distributed 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.
Step 5	**interface** *type slot* / *subslot* / *port* [**.** *subinterface-number*] **Example:** `Router(config)# interface pos 0/3/0`	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** **Example:** `Router(config-if)# mpls label protocol ldp`	Configures the use of LDP for an interface.
Step 8	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 9	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Verifying the MPLS LDP Graceful Restart Configuration

To verify that MPLS LDP Graceful Restart is configured correctly, perform the following task.

SUMMARY STEPS

1. **enable**
2. **show mpls ldp neighbor graceful restart**
3. **show mpls ldp graceful-restart**
4. **exit**

DETAILED STEPS

Step 1 **enable**

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

Example:

```
Router>? enable
Router#
```

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

Use this command to display graceful restart information for LDP sessions. For example:

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 graceful-restart**

Use this command to display graceful restart sessions and session parameters. For example:

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 4 **exit**

Use this command to exit to user EXEC mode. For example:

Example:

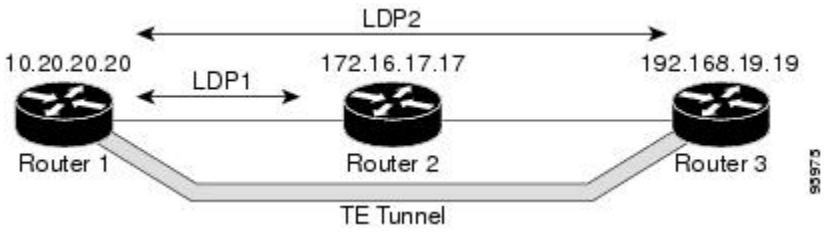
```
Router# exit
Router>
```

Configuration Examples for MPLS LDP Graceful Restart

Configuring MPLS LDP Graceful Restart Example

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.

Figure 2: MPLS LDP Graceful Restart Configuration Example



Router 1 configured with LDP GR:

```
!
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 10.12.0.2 255.0.0.0
 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 10.12.0.0 0.255.255.255 area 100
 network 10.20.20.20 0.0.0.0 area 100
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 100
```

Router 2 configured with LDP SSO/NSF:

```
!
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 10.17.17.17 255.255.255.255
 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 10.12.0.1 255.0.0.0
 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 10.11.0.1 255.0.0.0
 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 10.11.0.0 0.255.255.255 area 100
 network 10.12.0.0 0.255.255.255 area 100
 network 10.17.17.17 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:

```
!
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 10.19.19.19 255.255.255.255
 no ip directed-broadcast
!
interface POS1/0
 ip address 10.11.0.2 255.0.0.0
 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 10.11.0.0 0.255.255.255 area 100
network 10.19.19.19 0.0.0.0 area 100
mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 100
!
ip classless
```

Additional References

The following sections provide references related to MPLS LDP GR.

Related Documents

Related Topic	Document Title
MPLS Label Distribution Protocol	MPLS Label Distribution Protocol (LDP)
LDP commands	*Cisco IOS Multiprotocol Label Switching Command Reference*

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 XE 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 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

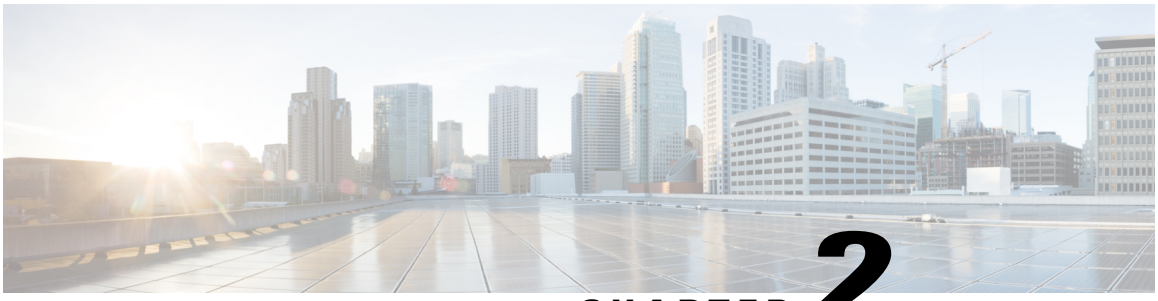
Feature Information for MPLS LDP Graceful Restart

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.

Table 1: Feature Information for MPLS LDP Graceful Restart

Feature Name	Releases	Feature Information
MPLS LDP Graceful Restart	Cisco IOS XE Release 2.1	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. 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 the router recover. In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced or modified: **debugmplsldpgraceful-restart**, **mplsldpgraceful-restart**, **mplsldpgraceful-restarttimersmax-recovery**, **mplsldpgraceful-restarttimersneighbor-liveness**, **showmplsipbinding**, **showmplsldpbindings**, **showmplsldpgraceful-restart**, **showmplsldpneighbor**.



CHAPTER 2

NSF SSO--MPLS LDP and LDP Graceful Restart

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.

Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) uses SSO, NSF, and graceful restart to allow a Route Processor (RP) 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

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 module.

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 LDP and LDP Graceful Restart

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

To perform LDP NSF, RPs 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 restriction:

- LDP NSF cannot be configured on label-controlled ATM (LC-ATM) interfaces.

Information About NSF SSO--MPLS LDP and LDP Graceful Restart

How NSF SSO--MPLS LDP and LDP Graceful Restart Works

LDP NSF allows an RP 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 RPs are configured with LDP NSF, the backup RP retains the MPLS forwarding state and reestablishes communication with the LDP neighbors. Then the RP 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 RP is configured with MPLS LDP NSF support and graceful restart, the RP 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

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 an RP 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 enter a **showmplsldpgraceful-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 enter a **showmplsldpneighbor**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 **showmplsforwarding-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

An RP that is configured to perform LDP NSF includes the Fault Tolerant (FT) Type Length Value (TLV) in the LDP initialization message. The RP 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 RP 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

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

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

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

Checkpointing for NSF SSO--MPLS LDP and LDP Graceful Restart

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.

For the LDP NSF feature, the checkpointing function copies the active RP's LDP local label bindings to the backup RP. The active RP sends updates to the backup RP 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 RP.

To check that the active and backup RPs 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 RPs. This command displays the local label bindings that have been saved. The active RP and the backup RP should have the same local label bindings.

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

To configure MPLS LDP Graceful Restart, perform the following task. 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.

Before You Begin

- RPs 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* / *subslot* / *port* [**.** *subinterface-number*
6. **mpls ip**
7. **mpls label protocol ldp**
8. **exit**
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• 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	**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* / *subslot* / *port* [**.** *subinterface-number* **Example:** `Router(config)# interface pos 0/3/0`	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** **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.
Step 8	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 9	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Verifying the MPLS LDP Graceful Restart Configuration

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

SUMMARY STEPS

1. **enable**
2. **show mpls ldp graceful-restart**
3. **show mpls ldp neighbor graceful restart**
4. **show mpls ldp checkpoint**
5. **exit**

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 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 3 **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 4 **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
```

Step 5 **exit**

Use this command to return to user EXEC mode. For example:

Example:

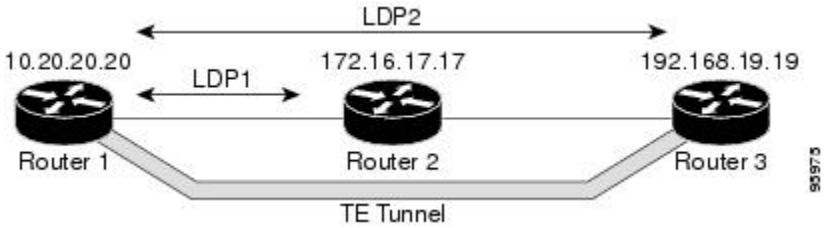
```
Router# exit
Router>
```

Configuration Examples for NSF SSO--MPLS LDP and LDP Graceful Restart

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

```
redundancy
mode sso
ip subnet-zero
ip cef distributed
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 ATM0/1/0
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
```

```
interface ATM0/1/0.5 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

```
redundancy
mode sso
!
ip cef distributed
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 ATM0/3/0
 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 ATM0/3/0.5 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 POS0/1/0
 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

```
redundancy
mode sso
!
ip subnet-zero
ip cef distributed
!
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 POS1/1/0
 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
```

Additional References

The following sections provide references related to the NSF/SSO--MPLS LDP and LDP Graceful Restart feature.

Related Documents

Related Topic	Document Title
Stateful switchover	Stateful Switchover
MPLS Label Distribution Protocol	MPLS Label Distribution Protocol (LDP)
MPLS LDP commands	*Cisco IOS Multiprotocol Label Switching Command Reference*
Cisco nonstop forwarding	Cisco Nonstop Forwarding
High availability commands	*Cisco IOS High Availability Command Reference*

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 XE software 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 Distributio* n

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

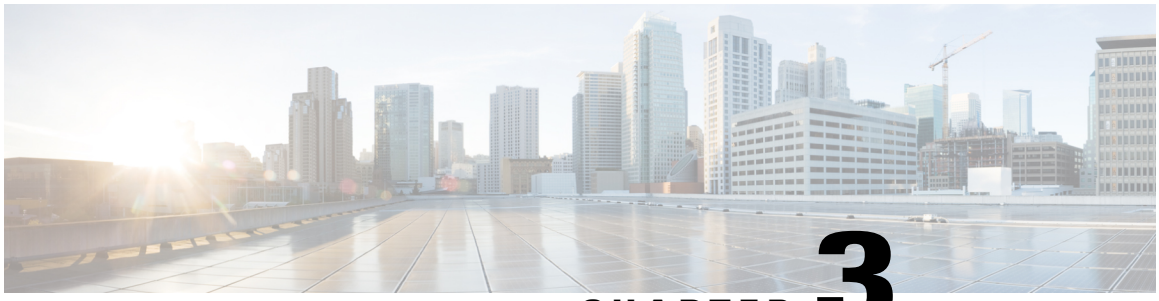
Feature Information for NSF SSO--MPLS LDP and LDP Graceful Restart

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.

Table 2: Feature Information for NSF/SSO--MPLS LDP and LDP Graceful Restart

Feature Name	Releases	Feature Information
NSF/SSO--MPLS LDP and MPLS LDP Graceful Restart	Cisco IOS XE Release 2.1	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. Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) uses SSO, NSF, and graceful restart to allow a Route Processor (RP) 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). In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced or modified: **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**.



CHAPTER 3

ISSU MPLS Clients

MPLS applications can be upgraded using the In Service Software Upgrade (ISSU) process. Thus, MPLS applications are considered ISSU's MPLS clients. The ISSU process allows Cisco IOS XE software to be updated or otherwise modified while packet forwarding continues.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 module.

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, on page 32 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 3: 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

Information About ISSU MPLS Clients

Before examining ISSU coordination of MPLS clients, you should understand the following concepts:

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

For more information on the ISSU procedure, see Cisco IOS XE In Service Software Upgrade Process document and see the Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide .

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 aggregation protocol (PagP) and Link Aggregation 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)

Note For a complete list of ISSU- compliant protocols and applications that are supported for the Cisco ASR Series Routers for your release, see the Release Notes for Cisco ASR Series Aggregation Services Routers .

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”
- 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

Note For the complete task sequence that accomplishes ISSU see theCisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide .

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.

Before You Begin

Ensure that you have successfully loaded new Cisco IOS XE software onto the standby processor as described in the Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide.

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.
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.

	Command or Action	Purpose
Step 3	**show issu sessions** *clientID* **Example:** `Router# show issu sessions 2002`	Displays detailed information about a particular ISSU client that includes 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, 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

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

The following sections provide references related to the ISSU MPLS Clients feature.

Related Documents

Related Topic	Document Title
ISSU process	• Cisco IOS XE In Service Software Upgrade Process • Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide
High availability commands	*Cisco IOS High Availability Command Reference*

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 XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature	--

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 4: Feature Information for ISSU MPLS Clients

Feature Name	Releases	Feature Information
ISSU MPLS--LDP	Cisco IOS XE Release 2.1	This feature allows In Service Software Upgrade (ISSU) support for the Label Distribution Protocol (LDP) and Multiprotocol Label Switching (MPLS) Forwarding. MPLS applications can be upgraded using the In Service Software Upgrade (ISSU) process. Thus, MPLS applications are considered ISSU's MPLS clients. The ISSU process allows Cisco IOS XE software to be updated or otherwise modified while packet forwarding continues. In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers.

Feature Name	Releases	Feature Information
		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.**
ISSU--MPLS VPN (Support for IPv4 VPNs)	Cisco IOS XE Release 2.1	This feature supports In Service Software Upgrade (ISSU) for Multiprotocol Label Switching (MPLS) Virtual Private networks (VPNs) for IPv4 address families only. In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. No commands were introduced or modified for this feature.
ISSU--MPLS TE	Cisco IOS XE Release 2.3	This feature allows upgrade or downgrade of compatible Cisco IOS XE software images on the back up Route Processor (RP) while the device is operational and passing traffic on Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnels. In Cisco IOS XE Release 2.3, this feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. No commands were introduced or modified for this feature.

Glossary

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.

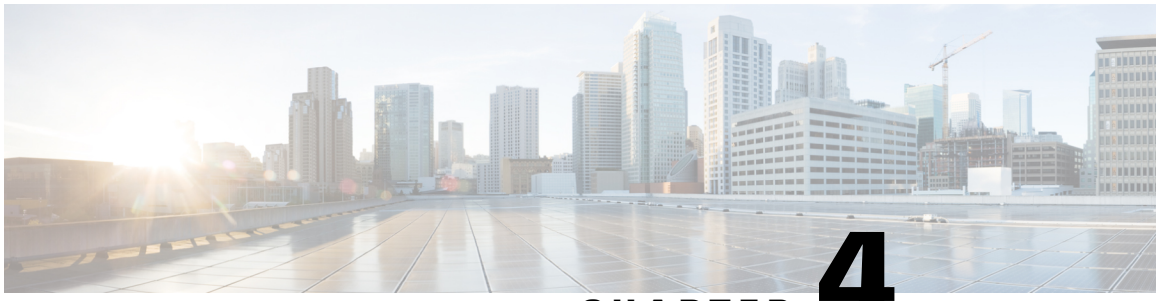
RP--Route Processor.

RSVP GR--Resource Reservation Protocol graceful restart.

TE--traffic engineering.

VPN--Virtual Private Network.

VRF--virtual routing and forwarding.



CHAPTER 4

MPLSTrafficEngineering--RSVPGracefulRestart

The MPLS Traffic Engineering--RSVP Graceful Restart feature allows a neighboring Route Processor (RP) to recover from disruption in control plane service (specifically, the Label Distribution Protocol [LDP] component) without losing its Multiprotocol Label Switching (MPLS) forwarding state.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 module.

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 MPLS TE--RSVP Graceful Restart

Perform the following tasks on routers before configuring the MPLS Traffic Engineering--RSVP Graceful Restart feature:

- Configure the Resource Reservation Protocol (RSVP).

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

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*.

Restrictions for MPLS TE--RSVP Graceful Restart

- Graceful restart supports node failure only.
- Graceful restart does not support restart or recovery on Cisco nodes, but helps in recovering a neighbor that is restart capable. Cisco routers advertise a restart time of 5 milliseconds (ms) and a recovery time of 0 in hello messages.
- Unnumbered interfaces are not supported.

Information About MPLS TE--RSVP Graceful Restart

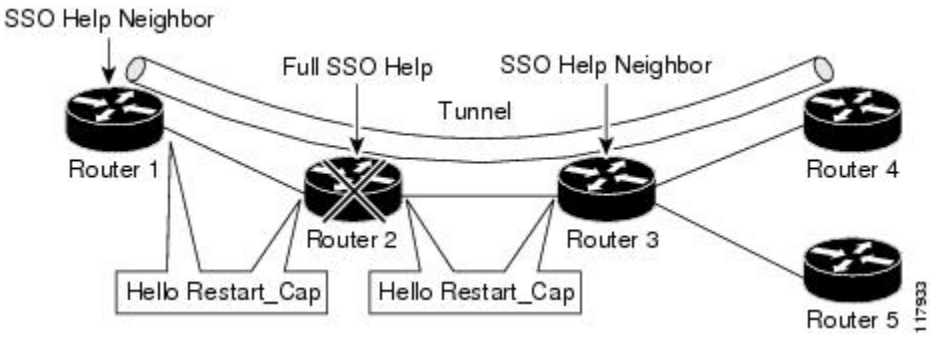
Graceful Restart

Graceful restart allows RSVP TE enabled nodes to start 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 as far as the RSVP state is concerned.

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

Graceful restart depends on RSVP hello messages that include Hello Request or Hello Acknowledgment (ACK) objects between two neighbors.

The figure below shows the graceful restart extension to these messages that an object called Restart_Cap, which tells neighbors that a node, may be capable of restarting if a failure occurs. The time-to-live (TTL) in these messages is set to 255 so that adjacencies can be maintained through alternate paths even if the link between two neighbors goes down.



The 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, graceful restart is enabled on Router 1, Router 2, Router 3, and Router 4. For simplicity, assume that all routers are restart capable. A TE label switched path (LSP) is signaled from Router 1 to Router 4.

Router 2 and Router 3 exchange periodic graceful restart hello messages every 10,000 ms (10 seconds), and so do Router 2 and Router 1 and Router 3 and Router 4. Assume that Router 2 advertises its restart time as 60,000 ms (60 seconds) and its recovery time as 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
```

Note The restart and recovery time are shown in **bold** in the last entry.

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 Route Processor 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 four ACK messages are missed from Router 2 (40 seconds), Router 3 declares communication with Router 2 lost "indicated by LOST" and starts the restart time to wait for the duration advertised in Router 2's restart time previously and recorded (60 seconds). Router 1 and Router 2 suppress all RSVP messages to Router 3 except hellos. Router 3 keeps sending the RSVP Path and Resv refresh messages to Router 4 and Router 5 so that they do not expire the state for the LSP; however, Router 3 suppresses these messages for Router 2.

Note A node restarts if it misses four ACKs or its hello src_instance (last source instance sent to its neighbor) changes so that its restart time = 0.

Before the restart time expires, Router 2 restarts and loads its configuration and graceful restart makes the configuration of router 2 send the hello messages with a new source instance to all the data links attached. However, because Router 2 has lost the neighbor states, it does not know what destination instance it should use in those messages; therefore, all destination instances are set to 0.

When Router 3 sees the hello from Router 2, Router 3 stops the restart time for Router 2 and sends an ACK message back. When Router 3 sees a new source instance value in Router 2's hello message, Router 3 knows that Router 2 had a control plane failure. Router 2 gets Router 3's source instance value and uses it as the destination instance going forward.

Router 3 also checks the recovery time value in the hello message from Router 2. If the recovery time is 0, Router 3 knows that Router 2 was not able to preserve its forwarding information and Router 3 deletes all RSVP state that it 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.

Graceful Restart Benefits

- Graceful restart allows a node to recover state information from its neighbor when there is an RP failure or the device has undergone a stateful switchover (SSO).
- Graceful restart allows session information recovery with minimal disruption to the network.
- A node can perform a graceful restart to help a neighbor recover its state by keeping the label bindings and state information to provide a quick recovery of the failed node and not affect the traffic that is currently forwarded.

How to Configure MPLS TE--RSVP Graceful Restart

Enabling Graceful Restart

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• 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** **Example:** `Router(config)# ip rsvp signalling hello graceful-restart mode help-neighbor`	Sets the number of DSCP hello messages on a neighboring router with restart capability.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits to privileged EXEC mode.

What to Do Next

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
```

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

Setting a DSCP Value on a Router for MPLS TE Graceful Restart

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 the number of DSCP hello messages on a graceful restart-enabled router.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits to privileged EXEC mode.

Setting a Hello Refresh Interval for MPLS TE Graceful Restart

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.

	Command or Action	Purpose
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 a hello refresh interval on a router with graceful restart enabled.
Step 4	**exit** **Example:** `Router(config)# end`	Exits to privileged EXEC mode.

Setting a Missed Refresh Limit for MPLS TE Graceful Restart

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.

	Command or Action	Purpose
Step 3	**ip rsvp signalling hello graceful-restart refresh misses** *msg-count* **Example:** `Router(config)# ip rsvp signalling hello graceful-restart refresh misses 5`	Sets a refresh limit on a router with graceful restart enabled.
Step 4	**exit** **Example:** `Router(config)# end`	Exits to privileged EXEC mode.

Verifying Graceful Restart Configuration

SUMMARY STEPS

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

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 rsvp hello graceful-restart**
Use this command to display information about the status of graceful restart and related parameters. For example:

Example:

```
Router# show ip rsvp hello graceful-restart
Graceful Restart:Enabled (help-neighbor only)
  Refresh interval:10000 msecs
  Refresh misses:4
  DSCP:0x30
  Advertised restart time:0 secs
```

```
  Advertised recovery time:0 secs
  Maximum wait for recovery:3600000 secs
```

Step 3 **exit**

Use this command to exit to user EXEC mode. For example:

Example:

```
Router# exit
Router>
```

Configuration Examples for MPLS TE--RSVP Graceful Restart

Example MPLS TE--RSVP Graceful Restart

In the following example, graceful restart is enabled, and related parameters, including a DSCP value, a refresh interval, and a missed refresh limit are set:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip rsvp signalling hello graceful-restart mode help-neighbor
Router(config)# ip rsvp signalling hello graceful-restart dscp 30
Router(config)# ip rsvp signalling hello graceful-restart refresh interval 10000
Router(config)# ip rsvp signalling hello graceful-restart refresh misses 4
Router(config)# end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
RSVP commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
Quality of service (QoS) features including signaling, classification, and congestion management	*Cisco IOS XE Quality of Service Solutions Configuration Guide*, Release 2
Stateful switchover	Stateful Switchover
MPLS Label Distribution Protocol	MPLS Label Distribution Protocol (LDP)
Cisco nonstop forwarding	Cisco Nonstop Forwarding

Related Topic	Document Title
Information on stateful switchover, Cisco nonstop forwarding, graceful restart	MPLS LDP: SSO/NSF Support and Graceful Restart
Hellos for state timeout	MPLS TE--RSVP Hello State Timer

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

RFCs

RFCs	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 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 MPLS Traffic Engineering--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 5: Feature Information for MPLS Traffic Engineering--RSVP Graceful Restart

Feature Name	Releases	Feature Information
MPLS Traffic Engineering--RSVP Graceful Restart	Cisco IOS XE Release 2.3	The MPLS TE--RSVP Graceful Restart feature allows a neighboring Route Processor (RP) to recover from disruption in control plane service (specifically, the Label Distribution Protocol (LDP) component) without losing its MPLS forwarding state. In Cisco IOS XE Release 2.3, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced or modified: **ip rsvp signalling hello graceful-restart dscp**, **ip rsvp signalling hello graceful-restart mode help-neighbor**, **ip rsvp signalling hello graceful-restart refresh interval**, **ip rsvp signalling hello graceful-restart refresh misses**, **show ip rsvp counters**, **show ip rsvp counters state teardown**, **show ip rsvp hello**, **show ip rsvp hello client lsp detail**, **show ip rsvp hello client lsp summary**, **show ip rsvp hello client neighbor detail**, **show ip rsvp hello client neighbor summary**, **show ip rsvp hello graceful-restart**, **show ip rsvp hello instance detail**, **show ip rsvp hello instance summary**.

Glossary

autonomous system --A collection of networks that share the same routing protocol and that are under the same system administration.

ASBR --Autonomous System Boundary Router. A router that connects and exchanges information between two or more autonomous systems.

backup tunnel --A Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnel used to protect other (primary) tunnels' traffic when a link or node failure occurs.

DSCP --differentiated services code point. Six bits in the IP header, as defined by the Internet Engineering Task Force (IETF). These bits determine the class of service provided to the IP packet.

Fast Reroute --A mechanism for protecting Multiprotocol Label Switching (MPLS) traffic engineering (TE) label switched paths (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. Fast Reroute (FRR) locally repairs the protected LSPs by rerouting them over backup tunnels that bypass failed links or nodes.

graceful restart --A process for helping a neighboring Route Processor (RP) restart after a node failure has occurred.

headend --The router that originates and maintains a given label switched path (LSP). This is the first router in the LSP's path.

IGP --Interior Gateway Protocol. Internet protocol used to exchange routing information within an autonomous system. Examples of common Internet IGPs include Interior Gateway Routing Protocol (IGRP), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP).

instance --A mechanism that implements the Resource Reservation Protocol. (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 label switched paths (LSPs) crossing this neighbor to be fast rerouted.

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

LDP --Label Distribution Protocol. The protocol that supports Multiprotocol Label Switching (MPLS) hop-by-hop forwarding by distributing bindings between labels and network prefixes.

LSP --label switched path. A configured connection between two routers, in which Multiprotocol Label Switching (MPLS) is used to carry packets. A path created by the concatenation of one or more label switched hops, allowing a packet to be forwarded by swapping labels from an MPLS node to another MPLS node.

merge point --The tail of the backup tunnel.

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.

PLR --point of local repair. The headend of the backup tunnel.

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.

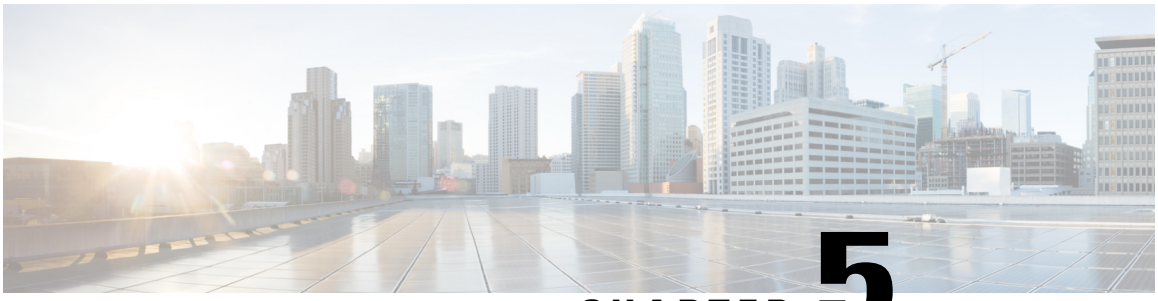
state --Information that a router must maintain about each label switched path (LSP). The information is used for rerouting tunnels.

tailend --The router upon which an label switched path (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.

topology --The physical arrangement of network nodes and media within an enterprise networking structure.

tunnel --Secure communications path between two peers, such as two routers.



CHAPTER 5

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.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 module.

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.
- Configure RSVP graceful restart on all interfaces of the neighbor that you want to be restart-capable.
- Configure the redundancy mode as SSO. See the Stateful Switchover feature module for more information.
- 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)

See the Cisco Nonstop Forwarding feature module for more information.

- 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.
- 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.
- 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.

Information About NSF SSO--MPLS TE and RSVP Graceful Restart

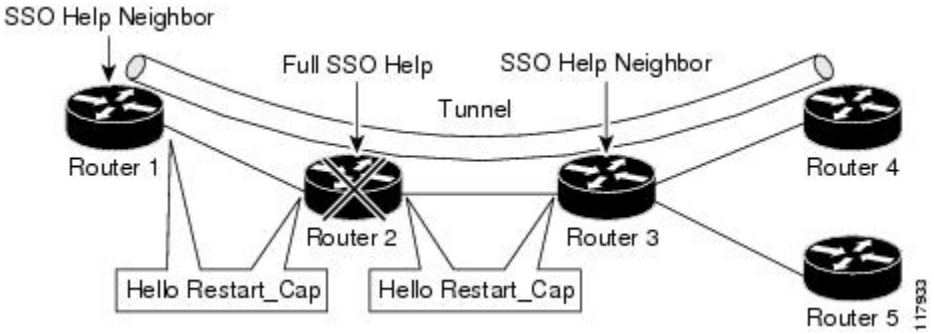
Overview of MPLS TE and RSVP Graceful Restart

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.

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.

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.

Enabling RSVP Graceful Restart on an Interface

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *subslot* / *port* [**.** *subinterface-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**
8. **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 slot* / *subslot* / *port* [**.** *subinterface-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.
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.

	Command or Action	Purpose
Step 7	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 8	**exit** **Example:** `Router(config)# exit`	(Optional) Exits global configuration mode and returns to privileged EXEC mode.

Setting a DSCP Value for RSVP Graceful Restart

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 Refresh Interval for RSVP Hello Messages

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 for RSVP Graceful Restart Hello Acknowledgements

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**

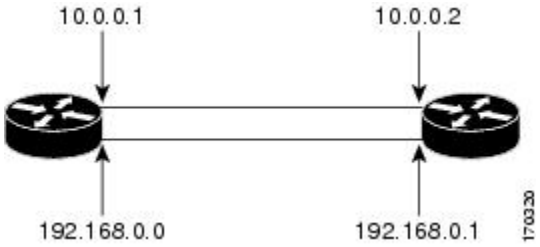
DETAILED STEPS

	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

Example Configuring NSF SSO--MPLS TE and RSVP Graceful Restart

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
```

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

```
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
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
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
Stateful switchover	Stateful Switchover
Cisco nonstop forwarding	Information about Cisco Nonstop Forwarding
RSVP hello state timer	MPLS Traffic Engineering: RSVP Hello State Timer

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

RFCs

RFCs	Title
RFC 3209	*RSVP-TE: Extensions to RSVP for LSP Tunnels*

RFCs	Title
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 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 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 6: Feature Information for NSF/SSO--MPLS TE and RSVP Graceful Restart

Feature Name	Releases	Feature Information
NSF/SSO--MPLS TE and RSVP Graceful Restart	Cisco IOS XE Release 3.1S Cisco IOS XE Release 3.5S	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 XE Release 3.1S, this feature was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Feature Name	Releases	Feature Information
		The following commands were introduced or modified: **clear ip rsvp high-availability counters**, **debug ip rsvp high-availability**, **debug ip rsvp sso**, **debug mpls traffic-eng ha sso**, **ip rsvp signalling hello graceful-restart dscp**, **ip rsvp signalling hello graceful-restart mode**, **ip rsvp signalling hello graceful-restart mode help-neighbor**, **ip rsvp signalling hello graceful-restart neighbor**, **ip rsvp signalling hello graceful-restart refresh interval**, **ip rsvp signalling hello graceful-restart refresh misses**, **show ip rsvp counters**, **show ip rsvp counters state teardown**, **show ip rsvp hello**, **show ip rsvp hello client lsp detail**, **show ip rsvp hello client lsp summary**, **show ip rsvp hello client neighbor detail**, **show ip rsvp hello client neighbor summary**, **show ip rsvp hello graceful-restart**, **show ip rsvp hello instance detail**, **show ip rsvp hello instance summary**, **show ip rsvp high-availability counters**, **show ip rsvp high-availability database**, **show ip rsvp high-availability summary**.
MPLS TE--RSVP Graceful Restart 12.0S--12.2S Interop	Cisco IOS XE Release 3.5S	In Cisco IOS XE Release 3.5S, this feature was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.
MPLS TE— Autotunnel/Automesh SSO Coexistence	Cisco IOS XE Release 3.5S	In Cisco IOS XE Release 3.5S, this feature was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Glossary

DSCP --differentiated services code point. Six bits in the IP header, as defined by the Internet Engineering Task Force (IETF). These bits determine the class of service provided to the IP packet.

Fast Reroute --A mechanism for protecting Multiprotocol Label Switching (MPLS) traffic engineering (TE) label switched paths (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. Fast reroute (FRR) locally repairs the protected LSPs by rerouting them over backup tunnels that bypass failed links or nodes.

graceful restart --A process for helping a Route Processor (RP) restart after a node failure has occurred.

headend --The router that originates and maintains a given label switched path (LSP). This is the first router in the LSP's path.

hello instance --A mechanism that implements the Resource Reservation Protocol (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 Interior Gateway Routing Protocol (IGRP), Open Shortest Path First (OSPF), and Routing Information Protocol (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 Multiprotocol Label Switching (MPLS) is used to carry packets.

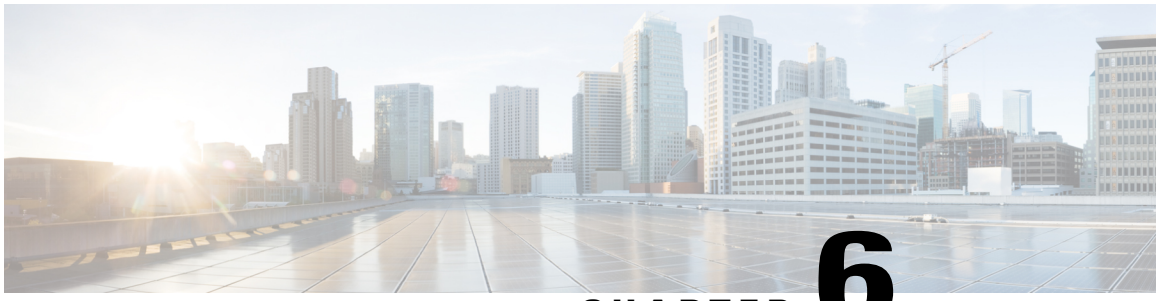
MPLS --Multiprotocol Label Switching. A method for forwarding packets (frames) through a network. MPLS enables routers at the edge of a network to apply labels to packets (frames). ATM switches or existing routers in the network core can switch packets according to the labels.

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 label switched path (LSP). The information is used for rerouting tunnels.

tailend --The router upon which a label switched path (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.



CHAPTER 6

AToM Graceful Restart

The AToM Graceful Restart feature assists neighboring devices that have nonstop forwarding (NSF), stateful switchover (SSO), and graceful restart (GR) for Any Transport over Multiprotocol Label Switching (AToM) to recover gracefully from an interruption in service. AToM GR functions strictly in helper mode, which means it helps other devices that are enabled with the NSF/SSO—Any Transport over MPLS and AToM Graceful Restart feature to recover. If the device 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.
- 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 caveats and feature information, see Bug Search Tool and 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 module.

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 Graceful Restart

Any Transport over Multiprotocol Label Switching (AToM) must be configured.

Restrictions for AToM Graceful Restart

- Any Transport over Multiprotocol Label Switching (AToM) graceful restart (GR) is supported in strict helper mode.
- MPLS Label Distribution Protocol (LDP) GR cannot be configured on label-controlled ATM (LC-ATM) interfaces.
- On some hardware platforms, Tag Distribution Protocol (TDP) sessions are not supported. Only LDP sessions are supported.

Information About AToM Graceful Restart

How AToM Graceful Restart Works

Any Transport over Multiprotocol Label Switching Graceful Restart (AToM GR) works in strict helper mode, which means it helps a neighboring Route Processor (RP) that has AToM nonstop forwarding (NSF) and stateful switchover (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 SSO of an RP. AToM GR is based on the MPLS Label Distribution Protocol (LDP) Graceful Restart feature, which preserves forwarding information for AToM circuits during an LDP session interruption. When the neighboring device establishes a new session, the LDP bindings and MPLS forwarding state are recovered.

How to Configure AToM Graceful Restart

Configuring AToM Graceful Restart

There is no Any Transport over Multiprotocol Label Switching (AToM)-specific configuration for AToM Graceful Restart (GR). You enable the Label Distribution Protocol (LDP) GR to assist a neighboring device configured with AToM nonstop forwarding (NSF) and stateful switchover (SSO) to maintain its forwarding state while the LDP session is disrupted.

SUMMARY STEPS

1. enable
2. configure terminal
3. ip cef distributed
4. mpls ldp graceful-restart
5. exit
6. show mpls l2transport vc detail

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip cef distributed** **Example:** `Device(config)# ip cef distributed`	Enables distributed Cisco Express Forwarding.
Step 4	**mpls ldp graceful-restart** **Example:** `Device(config)# mpls ldp graceful-restart`	Enables the device 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.
Step 5	**exit** **Example:** `Device(config)# exit`	Exits to privileged EXEC mode.
Step 6	**show mpls l2transport vc detail** **Example:** `Device# show mpls l2transport vc detail`	Displays detailed information about AToM virtual circuits (VCs).

Configuration Examples for AToM Graceful Restart

Example: Configuring AToM Graceful Restart

The following example shows a Fast Ethernet VLAN over Multiprotocol Label Switching (MPLS) configuration. PE1 is configured with Any Transport over MPLS Graceful Restart (AToM GR). PE2 is configured with AToM nonstop forwarding (NSF) and stateful switchover (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 distributed ! 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 FastEthernet2/1/1 no ip address ! interface FastEthernet2/1/1.2 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 distributed ! 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 FastEthernet0/3/2 no ip address ! interface FastEthernet0/3/2.2 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 cisco 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

Examples: Verifying AToM Graceful Restart Recovery from an LDP Session Disruption

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

The following example shows the status of the virtual circuit (VC) on PE1 with Any Transport over Multiprotocol Label Switching Graceful Restart (AToM GR) during normal operation:

```
Device# show mpls l2transport vc

Local intf     Local circuit        Dest address    VC ID      Status
-------------  -------------------- --------------- ---------- ----------
Fa2/1/1.2      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.

```
Device# show mpls l2transport vc

Local intf     Local circuit        Dest address    VC ID      Status
-------------  -------------------- --------------- ---------- ----------
Fa2/1/1.2      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.

```
Device# show mpls l2transport vc

Local intf     Local circuit        Dest address    VC ID      Status
-------------  -------------------- --------------- ---------- ----------
Fa2/1/1.2      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:

```
Device# show mpls l2transport vc detail

Local interface: Fa2/1/1.2 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: Se2/0/2, 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.

```
Device# show mpls l2transport vc detail

Local interface: Fa2/1/1.2 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: Se2/0/2, 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

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
MPLS AToM and LDP commands	Cisco IOS Multiprotocol Label Switching Command Reference
MPLS LDP graceful restart	"MPLS LDP Graceful Restart" module in the *MPLS: High Availability Configuration Guide* (part of the *Multiprotocol Label Switching Configuration Guide Library*)
Configuring AToM	"Any Transport over MPLS" module in the *MPLS: Layer 2 VPNs Configuration Guide* (part of the *Multiprotocol Label Switching Configuration Guide Library*)
Nonstop forwarding and stateful switchover for AToM	"NSF SSO Any Transport over MPLS and AToM Graceful Restart" module in the *MPLS: High Availability Configuration Guide* (part of the *Multiprotocol Label Switching Configuration Guide Library*)
High availability commands	*Cisco IOS High Availability Command Reference*

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/mib

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

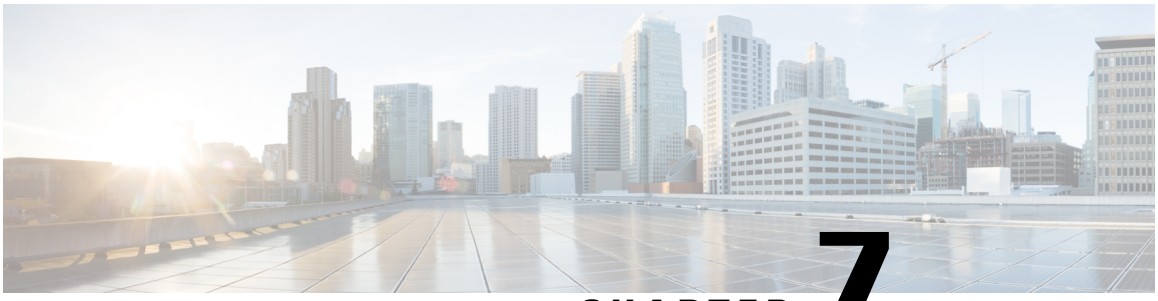
Feature Information for AToM Graceful Restart

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 7: Feature Information for AToM Graceful Restart

Feature Name	Releases	Feature Information
AToM Graceful Restart	12.0(29)S 12.2(33)SRA 12.2(33)SXH 12.4(11)T Cisco IOS XE Release 2.3	The AToM Graceful Restart feature assists neighboring devices that have nonstop forwarding (NSF), stateful switchover (SSO), and graceful restart (GR) for Any Transport over Multiprotocol Label Switching (AToM) to recover gracefully from an interruption in service. AToM GR functions strictly in helper mode, which means it helps other devices that are enabled with the NSF/SSO—Any Transport over MPLS and AToM Graceful Restart feature to recover. If the device with AToM GR fails, its peers cannot help it recover. AToM GR is based on the MPLS Label Distribution Protocol (LDP) Graceful Restart feature. In Cisco IOS Release 12.0(29)S, this feature was introduced. In Cisco IOS Release 12.2(33)SRA, support was added for the Cisco 7600 series routers. In Cisco IOS Release 12.2(33)SXH, this feature was integrated into the release. In Cisco IOS Release 12.4(11)T, this feature was integrated into the release. In Cisco IOS Release XE 2.3, this feature was implemented on the Cisco ASR 1000 Series Aggregation Services Routers. This feature uses no new or modified commands.



CHAPTER 7

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 allow 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 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 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.

In Cisco IOS XE software, AToM NSF supports the following attachment circuits:

- ATM
- Ethernet to Ethernet VLAN interworking

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 module.

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 can configure AToM NSF, make sure the following tasks have been completed:

- AToM virtual circuits (VCs) have been configured on the router. See the Any Transport over MPLS for information on configuring AToM. For configuring L2VPN Interworking, see the L2VPN Interworking feature module.
- SSO has been configured on the RPs. See the Stateful Switchover feature module for configuration information.
- Nonstop forwarding has been configured on the routers. You must enable nonstop forwarding on the routing protocols running between the P routers, PE routers, and CE routers. The routing protocols are the following:
  - Open Shortest Path First (OSPF),
  - Intermediate System-to-Intermediate System (IS-IS), and
  - Border Gateway Protocol (BGP).

See the Cisco Nonstop Forwarding feature module for configuration information.

- AToM NSF requires that neighbor networking devices be able to perform AToM GR.

Restrictions for AToM NSF

- AToM NSF cannot be configured on label-controlled ATM (LC-ATM) interfaces.
- AToM NSF supports AToM Layer 2 Virtual Private Network (L2VPN) Interworking. However, Layer 2 Tunnel Protocol Version 3 (L2TPv3) Interworking is not supported.
- AToM NSF interoperates with Layer 2 local switching. However, AToM NSF has no effect on interfaces configured for local switching.
- To allow distributed Cisco Express Forwarding to work on the interfaces, disable fair queueing on serial interfaces.

Information About AToM NSF

How AToM NSF Works

AToM NSF improves the availability of a service provider's network that uses AToM to provide Layer 2 VPN services to its customers. 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.

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, issue 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 for AToM NSF

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 **show acircuit checkpoint** command to display the 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.

NSF SSO Support for Ethernet to Ethernet VLAN Interworking

The NSF/SS0--Ethernet to Ethernet VLAN Interworking features enables SSO and NSF capabilities for Ethernet to VLAN attachment circuits. Changes in the learned MAC address for interworking are reflected on the standby RP so that identical values exist on the active and standby RPs.

ISSU Support for AToM NSF

AToM NSF supports 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 XE 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.

How to Configure AToM NSF

There is no AToM-specific configuration for AToM NSF. Before you configure AToM NSF, you need to configure MPLS LDP Graceful Restart. You enable MPLS LDP Graceful Restart to assist a neighboring router configured with AToM NSF to maintain its forwarding state while the LDP session is disrupted. See the LDP Graceful Restart document for information about how MPLS LDP Graceful Restart works and how you can customize it for your network.

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

This section contains the following task:

Configuring MPLS LDP Graceful Restart

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef distributed**
4. **mpls ldp graceful-restart**
5. **interface** *type slot / subslot / port* [**.** *subinterface-number*]
6. **mpls ip**
7. **mpls label protocol ldp**
8. **exit**
9. **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 distributed 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 the LDP bindings and MPLS forwarding state during a disruption in service.
Step 5	**interface** *type slot / subslot / port* [**.** *subinterface-number*] **Example:** `Router(config)# interface pos 0/3/0`	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** **Example:** `Router(config-if)# mpls label protocol ldp`	Configures the use of LDP for an interface. • 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 and returns to global configuration mode.
Step 9	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuration Examples for AToM NSF

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 POS0/1/0
 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 10.19.1.1 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 FastEthernet0/3/0
 ip route-cache cef
!
interface FastEthernet0/3/0.3
 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
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
MPLS AToM and LDP commands	*Cisco IOS Multiprotocol Label Switching Command Reference*
High availability commands	*Cisco IOS High Availability Command Reference*

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

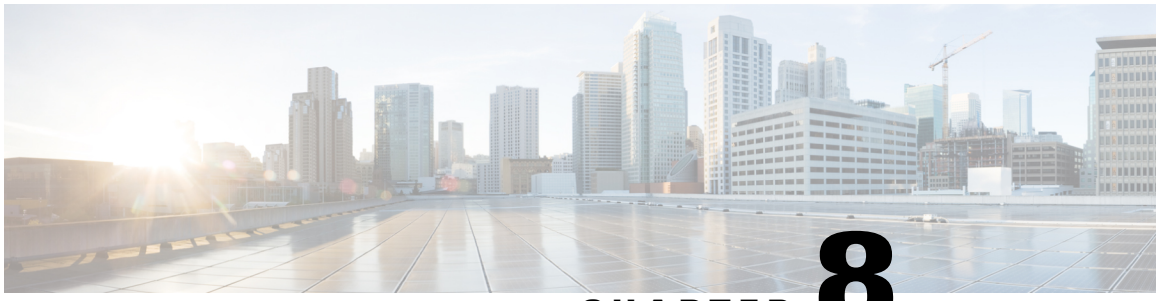
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train 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 8: Feature Information for AToM NSF Any Transport over MPLS and AToM Graceful Restart

Feature Name	Releases	Feature Information
NSF/SSO--AToM ATM Attachment Circuit	Cisco IOS XE Release 2.3	This feature provides support for AToM NSF/SSO support for ATM over MPLS (ATMoMPLS), which allows ATMoMPLS to use Cisco nonstop forwarding (NSF), stateful switchover (SSO), and Graceful Restart (GR) to allow a Route Processor (RP) to recover from a disruption in control plane service without losing its Multiprotocol Label Switching (MPLS) forwarding state. In Cisco IOS XE Release 2.3, this feature was implemented on the Cisco ASR 1000 Series Aggregation Services Routers. 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**.
ISSU--AToM ATM Attachment Circuit	Cisco IOS XE Release 2.3	This feature supports 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 XE 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. In Cisco IOS XE Release 2.3, this feature was implemented on the Cisco ASR 1000 Series Aggregation Services Routers. No commands were introduced or modified for this feature.

Feature Name	Releases	Feature Information
NSF/SSO--Ethernet to Ethernet VLAN Interworking	Cisco IOS XE Release 2.4	The NSF/SS0--Ethernet to Ethernet VLAN Interworking features enables stateful switchover (SSO) and nonstop forwarding (NSF) capabilities for Ethernet to VLAN attachment circuits. Changes in the learned MAC address for interworking are reflected on the standby RP so that identical values exist on the Active and Standby RPs. In Cisco IOS XE Release 2.4, this feature was introduced on the Cisco ASR 1000 Series Aggregation Routers. No commands were introduced or modified for this feature.



CHAPTER 8

Configuring NSF SSO--MPLS VPN

The NSF/SSO--MPLS VPN feature allows a provider edge (PE) router to preserve data forwarding information in a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) when the primary Route Processor (RP) restarts. This module describes how to enable nonstop forwarding (NSF) in a basic MPLS VPN network.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 module.

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

- You must have a supported MPLS VPN network configuration. See Configuring MPLS VPNs for more information.
- The networking device that is to be configured for NSF must first be configured for stateful switchover (SSO). See Stateful Switchover for more information

- You must enable NSF on the routing protocols running between the provider (P) routers, provider edge (PE) routers, and customer edge (CE) routers. The supported routing protocols are Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), and Intermediate System-to-Intermediate System (IS-IS). See Configuring Nonstop Forwarding for more information.
- You must configure Cisco NSF support on the routers for Cisco Express Forwarding. See Configuring Nonstop Forwarding for more information.
- All neighbor networking devices must be NSF-aware. Peer routers must support the graceful restart of the protocol used to communicate with the NSF/SSO--MPLS VPN-capable router.

Restrictions for NSF SSO--MPLS VPN

- Tag Distribution Protocol (TDP) sessions are not supported. Only Label Distribution Protocol (LDP) sessions are supported.
- 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

VPN NSF requires several elements in order to work:

- VPN NSF uses the BGP Graceful Restart mechanisms to create MPLS forwarding entries for VPNv4 prefixes in NSF mode. The forwarding entries are preserved during a restart. BGP also saves prefix and corresponding label information and recovers the information after a restart.
- The NSF/SSO--MPLS VPN feature also uses NSF for the label distribution protocol in the core network (either MPLS Label Distribution Protocol, traffic engineering, or static labeling).
- The NSF/SSO--MPLS VPN feature uses NSF for the Interior Gateway Protocol (IGP) used in the core (OSPF or IS-IS).
- The NSF/SSO--MPLS VPN feature uses NSF for the routing protocols between the PE and 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 RP. The checkpointing function copies state information from the active RP to the backup RP, thereby ensuring that the backup RP has an identical copy of the latest information. If the active RP fails, the backup RP can take over with no interruption in service. Checkpointing begins when the active RP does a bulk synchronization, which copies all of the local label bindings to the backup RP. After that, the active RP 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 BGP Graceful Restart-capable router loses connectivity, it performs the following actions as the restarting router:

1. The restarting 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.

A BGP Graceful Restart-capable peer router performs the following actions when it encounters a restarting router:

1. The peer router sends all 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.

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip cef** [**distributed**] **Example:** `Router(config)# ip cef distributed`	Enables Cisco Express Forwarding. • Use this command if Cisco Express Forwarding is not enabled by default on the router.
Step 4	**router bgp** *autonomous-system-number* **Example:** `Router(config)# router bgp 1`	Configures a BGP routing process and enters router configuration mode.
Step 5	**bgp graceful-restart** **Example:** `Router(config-router)# bgp graceful-restart`	Enables BGP Graceful Restart on the router.
Step 6	**bgp graceful-restart restart-time** *seconds* **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.
Step 7	**bgp graceful-restart stalepath-time** *seconds* **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.
Step 8	**end** **Example:** `Router(config-router)# end`	Exits to privileged EXEC mode.

Verifying the Configuration

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

Example NSF SSO--MPLS VPN for a Basic MPLS VPN

The following sample output shows the configuration of the NSF/SSO--MPLS VPN feature on the CE and PE routers. SSO is enabled by default, and LDP is the default MPLS label protocol.

CE1 Router

```
ip cef
no ip domain-lookup
!
interface Loopback0
 ip address 10.10.10.10 255.255.255.255
!
```

```
interface GigabitEthernet1/0/4
 ip address 10.0.0.1 255.0.0.0
 media-type 10BaseT
!
router ospf 100
 redistribute bgp 101
 nsf enforce global
 passive-interface GigabitEthernet1/0/4
 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 GigabitEthernet1/0/4
 ip vrf forwarding vpn1
 ip address 10.0.0.2 255.0.0.0
 !
 mpls ip
interface ATM3/0/0
 no ip address
!
interface ATM3/0/0.1 point-to-point
 ip unnumbered Loopback0
 mpls ip
!
router ospf 100
 passive-interface GigabitEthernet1/0/4
 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
 no ip address
!
interface ATM1/0.1 point-to-point
 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
!
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 FastEthernet0/1
 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 FastEthernet0/1
```

```
 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
```

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

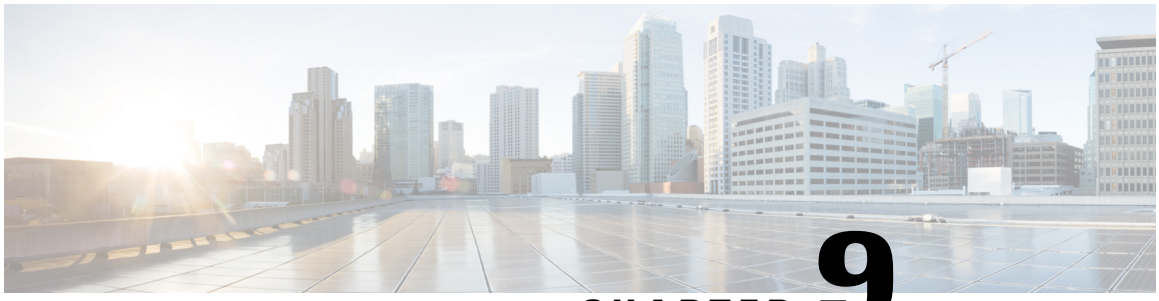
Feature Information for NSF SSO--MPLS VPN

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 9: Feature Information for NSF/SSO--MPLS VPN

Feature Name	Releases	Feature Information
NSF/SSO--MPLS VPN	Cisco IOS XE Release 2.1	This feature allows a provider edge router to preserve data forwarding information in a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) when the primary Route Processor restarts.



CHAPTER 9

SSO and ISSU--MPLS VPN 6VPE and 6PE Support

This document provides information about configuring stateful switchover (SSO) and In Service Software Upgrade (ISSU) support for Cisco IOS XE VPN IPv6 provider edge (6VPE) and Cisco IOS XE IPv6 provider edge (6PE) routers over Multiprotocol Label Switching (MPLS).

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 module.

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 SSO and ISSU--MPLS VPN 6VPE and 6PE Support

- Your networking device must be running Cisco IOS XE 3.2S or a later release.
- Your network must be configured for a supported MPLS VPN. For information, see Configuring MPLS Layer 3 VPNs and Implementing IPv6 VPN over MPLS.
- SSO must be configured on the Route Processor (RP). For information, see Stateful Switchover.
- Your networking device must support the following:
  - IPv6 Cisco Express Forwarding (CEF)
  - IPv6 nonstop forwarding (NSF)
  - Label Distribution Protocol (LDP) Graceful Restart
- NSF must be enabled on the Border Gateway Protocol (BGP) and static routes that run between the provider (P), PE, and the customer edge (CE) routers. For configuration information, see Cisco Nonstop Forwarding.
- LDP Graceful Restart must be enabled if LDP is the protocol used in the MPLS core. For configuration information, see NSF/SSO-MPLS LDP and MPLS LDP Graceful Restart.

Restrictions for SSO and ISSU--MPLS VPN 6VPE and 6PE Support

- 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.

Information About SSO and ISSU--MPLS VPN 6VPE and 6PE Support

Elements Supporting SSO and ISSU--MPLS VPN 6VPE and 6PE Support Features

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

- MPLS VPN--Forwards IP traffic using a VPN label that instructs the routers and switches in the network where to forward the packets based on preestablished IP routing information.

- 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 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--CEF and the MPLS Forwarding Infrastructure (MFI) are responsible for preserving forwarding entries and local labels across RP switchover.

Note If a router does not support the SSO and ISSU--MPLS VPN 6VPE and 6PE Support 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 can cause the loss of some network traffic.

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, such as IPv4/VPNv4 and IPv6/VPNv6 address families.

Both BGP peers must agree on a Graceful Restart timer. After a BGP session comes up and finishes sending initial updates, each BGP peer sends an end-of-Routing Information Base (RIB) marker.

The SSO and ISSU--MPLS VPN 6VPE and 6PE Support features use the mechanisms defined in RFC 4724, *Graceful Restart Mechanism for BGP*.

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 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

The ISSU process allows Cisco IOS XE 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 XE 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.

SSO Support for MPLS VPN 6VPE and 6PE

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

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-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 fail and lose 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 must 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 and BGP then 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

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 stale 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 stale 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. The PE router begins to calculate the best path and send out initial updates only after receiving an end-of-RIB marker from all BGP capable peers.

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.

How to Configure SSO and ISSU--MPLS VPN 6VPE and 6PE Support

Note Unlike SSO, which is a mode of operation for the device and a prerequisite for performing ISSU, the ISSU process is a series of steps performed while the router or switch is in operation. For information on performing ISSU upgrades on the Cisco ASR 1000 Series Aggregation Services Router, see the "In Service Software Upgrade (ISSU)" module in the *Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*.

Configuring SSO for a Basic MPLS 6VPE and 6PE Setup

Perform this task to configure SSO for a basic MPLS 6VPE and 6PE setup.

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.
Step 5	**ipv6 cef distributed** **Example:** `Router(config)# ipv6 cef distributed`	Enables distributed Cisco Express Forwarding for IPv6.

	Command or Action	Purpose
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.
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 and 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.
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 and sets the maximum time period that the local router will hold stale paths for a restarting peer.
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 SSO and ISSU Support for 6VPE and 6PE

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

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 stale 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 stale 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             FEt1/0/0      10.2.3.3
19         Pop Label      10.3.4.0/24      0             FEt1/0/0      10.2.3.3
20         17             10.4.4.4/32      0             FEt1/0/0      10.2.3.3
21         Pop Label      10.1.2.1/32[V]   0             FEt0/0/0      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             FEt0/0/0      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             FEt0/0/0
FE80::A8BB:CCFF:FE03:2101
27         26             10.4.5.5/32[V]   0             FEt1/0/0      10.2.3.3
28         25             10.4.5.0/24[V]   0             FEt1/0/0      10.2.3.3
29         22             A::4:5:5/128[V]  0             FEt1/0/0      10.2.3.3
30         21             A::4:5:0/112[V]  0             FEt1/0/0      10.2.3.3
31         23             A::4:5:4/128[V]  0             FEt1/0/0      10.2.3.3
32         24             A::5/128[V]      0             FEt1/0/0      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             FEt0/0/0      10.1.2.1
35         27             10.4.5.4/32[V]   0             FEt1/0/0      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             FEt1/0/0      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             FEt1/0/0      10.2.3.3
19         Pop Label      10.3.4.0/24      0             FEt1/0/0      10.2.3.3
20         17             10.4.4.4/32      0             FEt1/0/0      10.2.3.3
21         Pop Label      10.1.2.1/32[V]   0             FEt0/0/0      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             FEt0/0/0      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             FEt0/0/0
FE80::A8BB:CCFF:FE03:2101
27         26             10.4.5.5/32[V]   0             FEt1/0/0      10.2.3.3
28         25             10.4.5.0/24[V]   0             FEt1/0/0      10.2.3.3
29         22             A::4:5:5/128[V]  0             FEt1/0/0      10.2.3.3
30         21             A::4:5:0/112[V]  0             FEt1/0/0      10.2.3.3
31         23             A::4:5:4/128[V]  0             FEt1/0/0      10.2.3.3
32         24             A::5/128[V]      0             FEt1/0/0      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             FEt0/0/0      10.1.2.1
35         27             10.4.5.4/32[V]   0             FEt1/0/0      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             FEt1/0/0      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 FastEthernet0/0/0 label 18
A::5/128
  nexthop 10.2.3.3 FastEthernet1/0/0 label 17 24
A::1:2:0/112
  attached to FastEthernet0/0/0
A::1:2:1/128
  attached to FastEthernet0/0/0
A::1:2:2/128
  receive for FastEthernet0/0/0
A::4:5:0/112
  nexthop 10.2.3.3 FastEthernet1/0/0 label 17 21
A::4:5:4/128
  nexthop 10.2.3.3 FastEthernet1/0/0 label 17 23
A::4:5:5/128
  nexthop 10.2.3.3 FastEthernet1/0/0 label 17 22
FE80::/10
```

Following is sample output from the standby router:

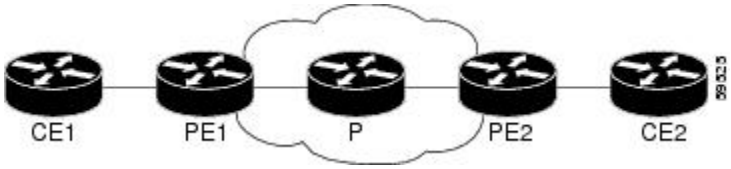
Example:

```
Standby-Router# show ipv6 cef vrf vrf1
::/0
  no route
::/127
  discard
A::1/128
  nexthop FE80::A8BB:CCFF:FE03:2101 FastEthernet0/0/0 label 18
A::5/128
  nexthop 10.2.3.3 FastEthernet1/0/0 label 17 24
A::1:2:0/112
  attached to FastEthernet0/0/0
A::1:2:1/128
  attached to FastEthernet0/0/0
A::1:2:2/128
  receive for FastEthernet0/0/0
A::4:5:0/112
  nexthop 10.2.3.3 FastEthernet1/0/0 label 17 21
A::4:5:4/128
  nexthop 10.2.3.3 FastEthernet1/0/0 label 17 23
A::4:5:5/128
  nexthop 10.2.3.3 FastEthernet1/0/0 label 17 22
FE80::/10
```

Configuration Examples for Configuring SSO and ISSU--MPLS VPN 6VPE and 6PE Support

The figure below illustrates a basic 6VPE or 6PE network configuration.

Figure 5: Sample Basic 6VPE/6PE Network Configuration



This section provides the following configuration examples for PE1 routers in a basic 6VPE or 6PE network configuration:

Example Configuring SSO for a Basic 6VPE Setup

The following is a configuration example for a PE1 router in a basic 6VPE setup (see the figure above) 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 FastEthernet0/0/0
 vrf forwarding vpn1
 ip address 10.1.2.2 255.255.255.0
 ipv6 address A::1:2:2/112
!interface FastEthernet1/0/0
 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 FastEthernet0/0/0
  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 FastEthernet0/0/0
  neighbor A::1:2:1 activate
 exit-address-family
```

Example Configuring SSO for a Basic 6PE Setup

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

```
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 FastEthernet0/0/0
 ip address 10.50.1.2 255.255.255.0
 ipv6 address 4000::72B/64
 ipv6 address 8008::72B/64
!
interface FastEthernet1/0/0
 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

Related Documents

Related Topic	Document Title
6VPE over MPLS	Implementing IPv6 VPN over MPLS

Related Topic	Document Title
6PE over MPLS	Implementing IPv6 over MPLS
Cisco IOS XE commands	Cisco IOS Master Command List, All Releases
Cisco IOS XE MPLS commands	*Cisco IOS Multiprotocol Label Switching Command Reference*
Cisco nonstop forwarding	Cisco Nonstop Forwarding
ISSU	• Cisco IOS XE In Service Software Upgrade Process • "In Service Software Upgrade (ISSU)" module in the *Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*
MPLS LDP NSF/SSO and Graceful Restart	NSF/SSO-MPLS LDP and MPLS LDP Graceful Restart
MPLS VPNs	Configuring MPLS Layer 3 VPNs
NFS/SSO for MPLS VPN	NSF/SSO--MPLS VPN
SSO	Stateful Switchover

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 SSO and ISSU--MPLS VPN 6VPE and 6PE Support

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 SSO and ISSU--MPLS VPN 6VPE and 6PE Support

Feature Name	Releases	Feature Information
ISSU--MPLS VPN 6VPE and 6PE ISSU Support	Cisco IOS XE 3.2S	This feature provides ISSU support for Cisco IOS XE VPN IPv6 provider edge router (6VPE) over MPLS and Cisco IOS XE IPv6 provider edge router (6PE) over MPLS. In Cisco IOS XE 3.2S, this feature was introduced for Cisco ASR 1000 Series Aggregation Services Routers. This feature introduced no new or modified commands.
SSO--MPLS VPN 6VPE and 6PE SSO Support	Cisco IOS XE 3.2S	This feature provides SSO support for Cisco IOS XE VPN IPv6 provider edge router (6VPE) over MPLS and Cisco IOS XE IPv6 provider edge router (6PE) over MPLS. In Cisco IOS XE 3.2S, this feature was introduced for Cisco ASR 1000 Series Aggregation Services Routers. 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.

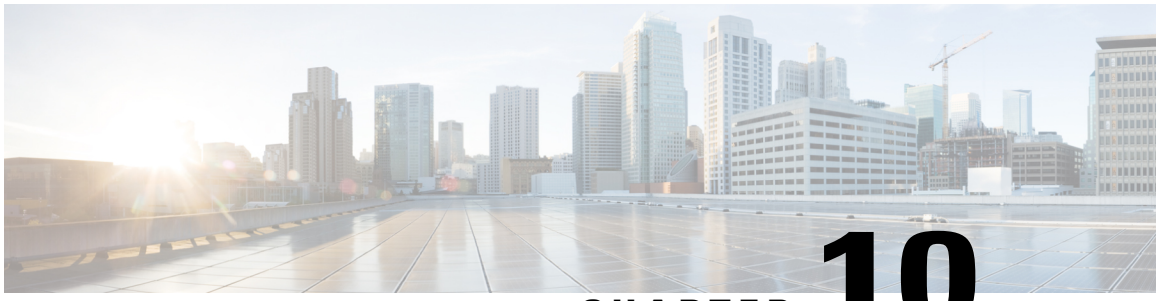
PE router --provider edge router. The PE router is the entry point into the service provider network. The PE router is typically deployed on the edge of the network and is administered by the service provider. The PE router is the redistribution point between EIGRP and BGP in PE to CE networking.

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

SSO --stateful switchover. SSO refers to the implementation of Cisco IOS XE 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 --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.



CHAPTER 10

SSO Support for MPLS TE Autotunnel and Automesh

The SSO Support for MPLS TE Autotunnel and Automesh feature provides full stateful switchover (SSO), Cisco nonstop forwarding (NSF), and In Service Software Upgrade (ISSU) support for autotunnel primary and backup TE tunnels feature and for autotunnel mesh group TE tunnels feature.

The 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 during a critical failure in the primary processor. SSO synchronizes the network state information between the primary and the secondary processor.

Note For brevity in this document, the Autotunnel Primary and Backup feature is called Autotunnel. The Autotunnel Mesh Groups feature is called Automesh.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 module.

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 SSO Support for MPLS TE Autotunnel and Automesh

- The MPLS TE RSVP Graceful Restart feature must be enabled on the stateful switchover (SSO) device and its neighbor devices.
- NSF must be configured on the IGP that is configured for TE. You must specify either the **nsf cisco** or the **nsf ietf** router configuration command or the recovery of TE tunnels might fail.
- The MPLS TE Autotunnel feature must be configured.
- The MPLS TE Automesh feature must be configured.

Note The SSO Support for MPLS TE Autotunnel and Automesh feature obsoletes the MPLS TE Autotunnel and SSO Coexistence feature available with the MPLS TE Autotunnel feature and the MPLS TE Automesh feature.

Restrictions for SSO Support for MPLS TE Autotunnel and Automesh

- The SSO Support for MPLS TE Autotunnel and Automesh feature is supported only on hardware platforms with dual Route Processors (RPs) that support SSO and Cisco NSF.
- SSO and Fast Reroute (FRR) double failure cases are not supported.
- To keep the Autotunnel and Automesh configurations synchronized between the active and standby RPs, you can no longer modify an existing Autotunnel or Automesh interface by using the **interface tunnel** command. This action is prohibited by the software.
- You can no longer use the following commands as a way for disabling the Autotunnel or the Automesh feature:
  - **clear mpls traffic-eng auto-tunnel primary**
  - **clear mpls traffic-eng auto-tunnel backup**
  - **clear mpls traffic-eng auto-tunnel mesh**

  Instead, use the **no** form of these commands:
  - **no mpls traffic-eng auto-tunnel primary onehop**
  - **no mpls traffic-eng auto-tunnel backup**
  - **no mpls traffic-eng auto-tunnel mesh**

Information About SSO Support for MPLS TE Autotunnel and Automesh

Overview of SSO Support for MPLS TE Autotunnel and Automesh

With the SSO Support for MPLS TE Autotunnel and Automesh feature, once you enable the device for the Autotunnel feature or for the Automesh feature by using the **mpls traffic-eng auto-tunnel primary onehop**, **mpls traffic-eng auto-tunnel backup**, or the **mpls traffic-eng auto-tunnel mesh** commands, the device starts creating the specified type of autotunnel on both the active and standby RPs. No additional configuration is needed to implement the SSO Support for MPLS TE Autotunnel and Automesh feature.

When the **no** form of these commands is executed, the SSO feature is disabled on both the active and the standby RPs.

The Autotunnel feature enables a device to dynamically build backup tunnels and to dynamically create one-hop primary tunnels on all interfaces that have been configured with MPLS TE tunnels.

The Automesh feature allows a network administrator to configure TE label switched paths (LSPs). In a network topology where edge label switch routers (LSRs) are connected by core LSRs, the Automesh feature automatically constructs a mesh of TE LSPs among the provider edge (PE) devices.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Commands List, All Releases
MPLS traffic engineering commands	*Multiprotocol Label Switching Command Reference*
MPLS traffic engineering—Autotunnel Mesh Groups feature	*MPLS Traffic Engineering Path Calculation and Setup Configuration Guide*
MPLS traffic engineering—Autotunnel Primary and Backup feature	*MPLS Traffic Engineering Path Link and Node Protection Configuration Guide*

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 SSO Support for MPLS TE Autotunnel and Automesh

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 SSO Support for MPLS TE Autotunnel and Automesh

Feature Name	Releases	Feature Information
SSO Support for MPLS TE Autotunnel and Automesh	15.2(2)S Cisco IOS XE Release 3.6S	The SSO Support for MPLS TE Autotunnel and Automesh feature provides full stateful switchover (SSO), Cisco nonstop forwarding (NSF), and In Service Software Upgrade (ISSU) support for the autotunnel primary and backup TE tunnels and for the autotunnel mesh group TE tunnels. The following commands were introduced or modified: **clear mpls traffic-eng auto-tunnel backup tunnel**, **clear mpls traffic-eng auto-tunnel mesh tunnel**, **clear mpls traffic-eng auto-tunnel primary tunnel**, **debug mpls traffic-eng auto-tunnel backup**, **debug mpls traffic-eng auto-tunnel primary**, **debug mpls traffic-eng ha sso**, **mpls traffic-eng auto-tunnel backup**, **mpls traffic-eng auto-tunnel mesh**, **mpls traffic-eng auto-tunnel primary onehop**, **show ip rsvp high-availability counters**, **show ip rsvp high-availability database**, **show ip rsvp high-availability database summary**, **show ip rsvp high-availability summary**, **show mpls traffic-eng auto-tunnel primary**.

Glossary

backup tunnel—An MPLS traffic engineering tunnel used to protect another (primary) tunnel's traffic when a link or node failure occurs.

Fast Reroute—Fast Reroute (FRR) is a mechanism for protecting MPLS traffic engineering 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 devices 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.

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

LSP—label switched path. A path that a labeled packet follows over several hops, starting at an ingress LSR and ending at an egress LSR.

LSR—label switch router. A Layer 3 device that forwards a packet based on the value of a label encapsulated in the packet.

mesh group—A set of label switch routers (LSRs) that are members of a full or partial network of traffic engineering label switched paths (LSPs).

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

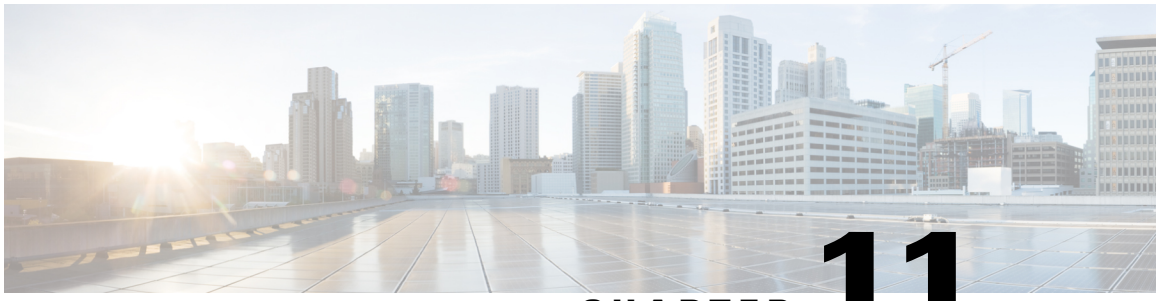
NSF—nonstop forwarding. The ability of a device to continue to forward traffic to a device that may be recovering from a failure. Also, the ability of a device recovering from a failure to continue to correctly forward traffic sent to it by a peer.

primary tunnel—An MPLS tunnel whose LSP can be fast-rerouted if there is a failure.

SSO—stateful switchover. SSO refers to the implementation of Cisco 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.

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.

tunnel—A secure communication path between two peers. A traffic engineering tunnel is a label switched tunnel that is used for traffic engineering. Such a tunnel is set up through means other than a normal Layer 3 device.



CHAPTER 11

NSR LDP Support

The NSR LDP Support feature allows the Label Distribution Protocol (LDP) to continue to operate across a node failure without losing peer sessions. Before the introduction of nonstop routing (NSR), LDP sessions with peers reset if a Route Processor (RP) failover or a Cisco In-Service Software Upgrade (ISSU) occurred. When peers reset, traffic is lost while the session is down. Protocol reconvergence occurs after the session is reestablished.

When NSR is enabled, RP failover and Cisco ISSU events are not visible to the peer device, and the LDP sessions that were established prior to failover do not flap. The protocol state learned from the peers persists across an RP failover or Cisco ISSU event and does not need to be relearned.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 module.

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 NSR LDP Support

The Label Distribution Protocol (LDP) must be up and running on the standby Route Processor (RP) for NSR LDP Support to work.

Information About NSR LDP Support

Roles of the Standby Route Processor and Standby LDP

For the NSR LDP Support feature to work, the Label Distribution Protocol (LDP) must be up and running on the standby Route Processor (RP). The LDP component running on the active RP is called the active LDP, and the LDP component running on the standby RP is called the standby LDP.

When nonstop routing (NSR) is enabled, the standby LDP runs independently from the active LDP, but with the assistance of some software components. The standby LDP maintains LDP session states and database information, ready to take over for the active LDP if the failover occurs.

Standby LDP maintains its local database by querying or receiving notifications of interface status change, configuration changes from the CLI, and checkpoints from the active LDP for other information that is not directly available on the standby RP.

To keep the protocol and session-state information synchronized with the active LDP, the standby LDP depends on TCP to replicate all LDP messages on the active RP to the standby RP. The standby LDP processes all received messages, updates its state, but does not send any responses to its neighbors.

The standby LDP performs the following tasks:

- Processes LDP configuration on startup and during steady state
- Processes active LDP checkpoints of state and session information such as LDP adjacencies, remote addresses, remote bindings, and so forth
- Builds its database of local interfaces
- Processes interface change events
- Receives and processes all LDP messages replicated by TCP
- Updates remote address and label databases

After a switchover and notification that the RP has become active, the standby LDP takes over the role of the active LDP and performs the following tasks:

- Sends hello messages immediately to prevent neighbors from reaching the discovery timeout and bringing down the session
- Retransmits any protocol-level response that has not been sent by the previous active LDP
- Readvertises label bindings
- Refreshes all forwarding entries
- Processes and responds to any LDP message from its neighbor

When the NSR LDP Support feature is disabled, the active LDP performs the following tasks:

- Stops checkpointing to the standby LDP
- Continues to manage all existing sessions

The standby LDP performs the following tasks:

- Cleans up all session-state information
- Reverses to the behavior before NSR is enabled

LDP Operating States

When the NSR LDP Support feature is enabled, the Label Distribution Protocol (LDP) operates in the following states:

Initial State

In the initial state, the active Label Distribution Protocol (LDP) process sets up the standby LDP to be ready to support nonstop routing (NSR). The active LDP performs the following tasks:

- Replicates all TCP sessions used by LDP with the standby LDP
- Synchronizes all existing session-state information with the standby LDP
- Synchronizes the LDP database with the standby LDP

LDP could be in the initial state because of one of these conditions:

- NSR is enabled
- NSR was enabled and the standby Route Processor (RP) starts up (asymmetric startup)
- System boots up and NSR is configured (symmetric startup)

Steady State

In the steady state, the active and standby Label Distribution Protocol (LDP) databases are synchronized. The active and standby LDP process the same LDP messages and update their states independently. The standby LDP is ready to take over the active LDP role in a switchover event.

On the active Route Processor (RP), the active LDP performs the following tasks:

- Continues to manage all existing sessions and checkpoints any significant session event to the standby LDP (such as adjacency delete, session shutdown, timers)
- Notifies the standby LDP of new adjacencies and neighbors

On the standby RP, the standby LDP performs these tasks:

- Processes all received messages but does not send any messages to its neighbor
- Processes checkpoint information from the active LDP

- Manages session keepalive timers but does not bring down the session if a keepalive timer times out

Post Switchover

In the post switchover state, the standby Label Distribution Protocol (LDP) process takes over the active LDP role while the active Route Processor (RP) is reloading.

Supported NSR Scenarios

The NSR LDP Support feature is supported under the following scenarios:

- Route Processor (RP) failover or node failure

  The Label Distribution Protocol (LDP) keeps the session up during an RP or node failover because the LDP adjacency and session-state information between LDP on the active and standby RPs are synchronized. As sessions are created on the active RP, new adjacencies are synchronized to the standby RP. If a standby RP is brought online after sessions are already up (asymmetric startup), LDP synchronizes the existing session-state information from the active to the standby RP.

- Cisco In-Service Software Upgrade (ISSU)

  LDP supports Cisco ISSU negotiation between RPs when a standby RP comes online for the MPLS LDP IGP Synchronization feature. Current Cisco ISSU negotiation is not impacted by NSR. For NSR, LDP negotiates messages specific to NSR, which are checkpointed during initial synchronization (adjacency and session-state information).

How to Configure NSR LDP Support

Enabling NSR LDP Support

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ldp nsr**
4. **exit**
5. **show mpls ldp nsr**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mpls ldp nsr** **Example:** `Device(config)# mpls ldp nsr`	Enables nonstop routing (NSR) for all Label Distribution Protocol (LDP) sessions for both link and targeted.
Step 4	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.
Step 5	**show mpls ldp nsr** **Example:** `Device# show mpls ldp nsr`	Displays whether NSR is enabled.

Troubleshooting Tips for NSR LDP Support

Use the **debug mpls ldp nsr** command to enable the display of Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) nonstop routing (NSR) debugging events for all NSR sessions or for the specified peer.

Configuration Examples for NSR LDP Support

Example: NSR LDP Configuration

Device 1 Configured with NSR LDP Support

```
!
mpls label range 16 100000 static 100001 1048575
mpls label protocol ldp
mpls ldp nsr
mpls ldp graceful-restart
```

```
!
interface Loopback0
ip address 20.20.20.20 255.255.255.255
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 10.12.0.2 255.255.0.0
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
nsr
nsf cisco enforce global
redistribute connected subnets
network 20.20.20.20 0.0.0.0 area 0
network 10.12.0.0 0.0.255.255 area 0
!
mpls ldp router-id Loopback0 force
```

Device 2 Configured without NSR LDP Support

```
mpls label range 16 100000 static 100001 1048575
mpls label protocol ldp
mpls ldp graceful-restart
!
interface Loopback0
ip address 10.17.17.17 255.255.255.255
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 10.12.0.1 255.255.0.0
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 10.11.0.1 255.255.0.0
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
```

```
nsr
nsf enforce global
redistribute connected
network 10.11.0.0 0.0.255.255 area 0
network 10.12.0.0 0.0.255.255 area 0
network 10.17.17.17 0.0.0.0 area 0
!
mpls ldp router-id Loopback0 force
```

Additional References for NSR LDP Support

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
MPLS commands	Cisco IOS Multiprotocol Label Switching Command Reference
LDP configuration tasks	*MPLS Label Distribution Protocol Configuration Guide*

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 NSR LDP Support

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 NSR LDP Support

Feature Name	Releases	Feature Information
NSR LDP Support	Cisco IOS XE Release 3.9S	The NSR LDP Support feature allows the Label Distribution Protocol (LDP) to continue to operate across a node failure without losing peer sessions. Before the introduction of nonstop routing (NSR), LDP sessions with peers reset if a Route Processor (RP) failover or an Cisco In-Service Software Upgrade (ISSU) occurred. When peers reset, traffic is lost while the session is down. Protocol reconvergence occurs after the session is reestablished. In Cisco IOS XE Release 3.9S, this feature was introduced and implemented on Cisco ASR 1000 Series Routers. The following commands were introduced or modified: **clear mpls ldp nsr statistics**, **debug mpls ldp nsr**, **mpls ldp nsr**, **show mpls ldp nsr**, **show mpls ldp neighbor**, **show mpls ldp parameters**.