# Cisco IOS Software Modularity: MPLS Layer 3 VPNs

**First Published: May 31, 2007**
**Last Updated: May 31, 2007**

In Cisco IOS Release 12.2(33)SXH, the Cisco IOS Software Modularity feature has been extended to include Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). Through software infrastructure enhancements, the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature reduces both planned and unplanned downtime and boosts operational efficiency. You can restart, upgrade, and patch modularized components and processes without interrupting service.

Identifying and fixing faults and failures is also easier, because you can isolate components and processes. The software modularity capabilities integrate with and make use of High Availability (HA) features already in place.

### Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Cisco IOS Software Modularity: MPLS Layer 3 VPNs" section on page 32.

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

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

## Contents



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

# Prerequisites for Cisco IOS Software Modularity: MPLS Layer 3 VPNs

The following are prerequisites for the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature:

- Before implementing the Cisco IOS Software Modularity: MPLS Layer 3 VPN feature, you should understand the concepts and tasks related to Cisco IOS Software Modularity. See the *Cisco IOS Software Modularity Installation and Configuration Guide*.
- The Cisco IOS Software Modularity: MPLS Layer 3: VPNs feature works with the MPLS HA features. See the following MPLS HA documentation for information about configuring MPLS HA:
  - *MPLS High Availability: Overview*
  - *NSF/SSO: MPLS VPN*
  - *NSF/SSO: MPLS LDP and LDP Graceful Restart*
  - *NSF/SSO: Any Transport over MPLS and AToM Graceful Restart*
  - *MPLS High Availability: Command Changes*
  - *Cisco Express Forwarding: Command Changes*
  - *NSF/SSO—MPLS TE and RSVP Graceful Restart*

# Restrictions for Cisco IOS Software Modularity: MPLS Layer 3 VPNs

- The software components that make up MPLS Layer 3 VPNs—that is, routing protocols, the master virtual routing and forwarding (VRF) database, and the Routing Information Bases (RIBs) for IPv4 and IPv6—were rewritten to work with the Cisco IOS software modularity infrastructure. The software modularity changes included moving the MPLS Layer 3 VPN infrastructure to the restartable routing process. However, other MPLS components, such as the MPLS Forwarding Information Base (FIB), Label Distribution Protocol (LDP), and traffic engineering (TE) have not been rewritten to conform with Cisco IOS software modularity. As a result, those components run in processes that cannot be restarted in the event of an error.
- This Cisco IOS Software Modularity: MPLS Layer 3: VPNs feature is supported on Cisco Catalyst 6500 series switches.
- You can patch and restart the MPLS Layer 3 VPN software without service disruptions. However, you cannot patch and restart without service disruption other MPLS components that are not compliant with the software modularity infrastructure.
- The Cisco IOS Software Modularity: MPLS Layer 3: VPNs feature uses 10 to 20 percent more memory than the Cisco IOS software without software modularity. For guidelines on memory requirements for modularization features, see the *Cisco IOS Software Modularity Installation and Configuration Guide*.
- The Cisco IOS Software Modularity: MPLS Layer 3: VPNs feature minimally reduces the number of targeted LDP sessions you can have. It also slightly increases tunnel setup times and marginally reduces convergence times.

For information on performance factors, see the "Best Practices for Scalability and Convergence in the Cisco IOS Software Modularity: MPLS Layer 3 VPNs Feature" section on page 7.

# Information About Cisco IOS Software Modularity: MPLS Layer 3 VPNs

To use the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature, you should understand the following concepts:



## Introduction to the Cisco IOS Software Modularity: MPLS Layer 3 VPNs Feature

Cisco IOS Software Modularity code is partitioned into multiple processes that run in their own protected memory space and that can independently restart. The control plane components for the Layer 3 VPNs moved from the tightly coupled and interdependent Cisco IOS code to the restartable routing process.

Some of the Cisco IOS modular processes that MPLS uses include:

- TCP is a separate restartable process that is important to MPLS because Border Gateway Protocol (BGP) and LDP sessions run over TCP connections.
- Routing is a restartable process that contains the following control plane components:
  - Open Shortest Path First (OSPF)
  - Intermediate System-to-Intermediate System (IS-IS)
  - BGP
  - RIB
  - Layer 3 VPN control plane components
- User Datagram Protocol (UDP) is a restartable process that is important for MPLS because LDP hello messages are transmitted in UDP packets. Further, MPLS embedded management applications may use UDP packets to transmit data.

Cisco IOS software includes more than 37 other modular processes so that restarts in the control plane components do not affect the transmission of data in the forwarding plane.

MPLS components that have not been made modular include:

- IP FIB
- MPLS Forwarding Infrastructure (MFI)

- Other MPLS control plane components, including LDP, Resource Reservation Protocol-traffic engineering (RSVP-TE), and IP Rewrite Manager (IPRM).

If an error occurs in one of those software components, the transmission of data is interrupted.

# Cisco IOS Software Modularity and High Availability

Unplanned downtime can be caused by software or hardware faults, such as control plane errors, control processor or line card failures. Most unplanned down time is caused by software faults related to the control plane.

To reduce unplanned downtime, Cisco IOS HA, nonstop forwarding (NSF) and stateful switchover (SSO) features work with routers that have primary and backup Route Processors (RPs). The following MPLS features are highly available through NSF and SSO:

- MPLS VPNs
- MPLS LDP
- MPLS TE and RSVP

With NSF and SSO, the primary and backup RPs keep identical copies of the label and state information by checkpointing. Checkpointing is a function that copies state information from the active RP to the backup RP, thereby ensuring that the backup has the latest information. If a control plane error causes the primary RP to fail, the backup RP takes over without disrupting the forwarding plane. This enables MPLS VPN, LDP, and TE features to keep running during a switchover.

Cisco IOS software modularity improves on the HA functionality by applying NSF and SSO to individual processes running within the Cisco IOS software. Cisco IOS software modularity provides the following improvements:

- For routers with a single RP, Cisco IOS software modularity enables individual processes to restart. If a process restarts successfully, it recovers its state either from a neighboring router that has Graceful Restart or from a database that checkpointed the state information. The process resumes normal operation without interrupting the forwarding plane. If the process cannot restart, the process is declared dead and the RP must be restarted.
- For routers with primary and backup RPs, Cisco IOS software modularity enables individual processes to restart. If the process cannot restart and is a mandatory process, the router switches to a backup RP, which takes over the processing without interruption.

To reduce unplanned downtime, enable the following HA features on the routers with Cisco IOS software modularity installed:

- SSO for routers with primary and backup RPs
- NSF for all supported routing protocols, that is, BGP, Enhanced Interior Routeway Gating Protocol (EIGRP), OSPF, and IS-IS
- GR for all MPLS features, that is, MPLS VPNs, MPLS LDP, MPLS TE, and RSVP

# How Cisco IOS Software Modularity Processes Work with Software That Is Not Modular

The processes that have been made modular through Cisco IOS software modularity can fail and restart without interrupting the transmission of data in the forwarding plane. These modular processes are used within MPLS applications that have not been made modular, such as MPLS LDP and MPLS TE. The following sections explain the interactions between the MPLS applications and the modular processes.

## MPLS LDP

MPLS LDP uses UDP to transmit LDP hello messages to discover neighbors and uses TCP to establish LDP sessions and exchange LDP label-binding information. Both TCP and UDP are modular processes.

If LDP is protected by GR functionality, when a TCP process fails the following events occur:

1. TCP is disconnected.
2. The LDP session is terminated.
3. LDP GR initiates and does the following:
   - Saves LDP session information and marks it stale.
   - Starts the reconnect timer, which indicates how long it will wait for the neighbor to reconnect.
   - After the neighbor reconnects, it starts the recovery timer, which indicates how long it will wait for the neighbor to readvertise label-binding information.
4. If the TCP process restarts before the reconnect timer expires and LDP can establish a new session and complete an information exchange before the respective timer expires, the LDP GR process completes successfully.

   If the TCP process does not restart before the reconnect timer expires, a restart of the RP is necessary.

If an LDP session has been protected by GR functionality, when a UDP process fails the following events occur:

1. If the UDP process restarts and LDP starts to exchange hello messages with neighbors before the LDP discovery hold timer expires, the LDP session continues without interruption.
2. If the UDP process does not restart before the LDP discovery hold timer expires, the LDP hello adjacency with the neighbor is torn down, which terminates the LDP session.
3. When the LDP session terminates, LDP GR initiates.

**Note** The MPLS LDP Session Protection feature works with the Cisco IOS Software Modularity feature, but cannot protect an LDP session if a UDP process fails.

## MPLS Traffic Engineering

If you ensure that MPLS TE is configured with the NSF/SSO: MPLS TE and RSVP GR feature, MPLS TE can recover from a failure without disrupting the forwarding plane. See *NSF/SSO: MPLS TE and RSVP Graceful Restart* for more information.

The recovery behaviors of the failing RP and its neighboring RPs depend on the versions of Cisco IOS software running on the routers:

- Cisco IOS Release 12.0(29)S introduced the MPLS TE: RSVP GR feature, which allowed a router to assist a neighboring router that has SSO/NSF support and GR to recover gracefully from an interruption in service. In Cisco IOS Release 12.0(29)S, RSVP GR operates strictly in helper mode, which means it can help only other routers that are enabled with MPLS SSO/NSF and GR to recover. If the router running 12.0(29)S (or later 12.0S release) with RSVP GR fails, its peer routers cannot help it recover.
- Cisco IOS Release 12.2(33)SRA and later releases introduced SSO/NSF support for MPLS TE so that an RP can use failover techniques to recover from a disruption in control plane service without losing its MPLS forwarding state. The feature is called NSF/SSO: MPLS TE and RSVP GR.
- Cisco IOS Release 12.2(33)SXH also supports the NSF/SSO: MPLS TE and RSVP GR feature. Enabling this feature in the MPLS Cisco IOS software modularity environment ensures that MPLS TE can recover gracefully from control plane faults.

Routers running Cisco IOS Releases 12.2(33)SXH or 12.2(33)SRA or a later require the NSF/SSO: MPLS TE and RSVP GR feature to recover from a process restart or an SSO failover without disruption. All LSPs remain intact. If you do not enable the NSF/SSO: MPLS TE and RSVP GR feature, MPLS TE may encounter the following conditions:

- During an IP process restart, packets may be lost.
- During an SSO failover, the neighboring router tears down the LSPs to and through the router that has the SSO event.

Routers running the RSVP GR feature in Cisco IOS Release 12.0(29)S or later cannot exchange GR hello messages with routers running the NSF/SSO: MPLS TE and RSVP GR feature in Cisco IOS Releases 12.2(33)SXH, 12.2(33)SRA, or later releases. Those routers cannot assist a neighboring router during a process restart or SSO failover.

### MPLS Traffic Engineering and RSVP-TE Messages

MPLS TE uses RSVP-TE extensions to explicitly route traffic over label switched paths. The RSVP-TE signaling protocol runs over IP. During an IP process restart, RSVP-TE messages can be dropped.

## How Processes Are Restarted on Cisco IOS Software Modularity: MPLS Layer 3 VPNs

The restarting capability of the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature allows the restarting of any modular process, such as the IP routing process, while the rest of the system continues to operate normally.

The following sequence shows how a system can recover without any user interaction:

**Note** Assume that all routing protocols (control plane) have converged and that the forwarding plane is forwarding traffic. The routing protocols have been configured for NSF.

- The IP routing process fails.
- The routing protocols that have been configured with NSF reestablish sessions and exchange routing information as the IP routing process restarts. The forwarding plane continues to forward traffic without interruption.
- The IP routing process recovers and sends an NSF message to its neighbors indicating that it is recovering.

- NSF-aware neighbors keep the entries they learned from the recovering system in their tables and send their information back to the recovering system.
- When the control plane has processed all routing updates it received from its neighbors, it programs the changes to the data plane.

Forwarding on the data plane is being performed at all times during this sequence.

Generally users do not need to restart processes. The integrated HA constantly monitors all processes and automatically initiates a restart when needed.

# How Patching Works on Cisco IOS Software Modularity: MPLS Layer 3 VPNs

The Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature allows you to do selective system maintenance with individual patches. You can download, verify, install, and activate a patch for a component without restarting an entire system. Because patches affect only the component they are required to fix, they need less code-certification time than if an entire system had to be verified. You have to verify only the portion of software associated with the fix.

# Best Practice for IP Routing Process Restarts with the Cisco IOS Software Modularity: MPLS Layer 3 VPNs Feature

Restarting the IP routing process restarts all the routing protocols and causes MPLS LDP to invoke the graceful restart routine. Wait until all the routing protocols have converged and LDP is back to a normal state before restarting the IP routing process again. Otherwise, traffic could be lost.

# Best Practice for SSO/NSF on Peer Route Processors with Cisco IOS Software Modularity: MPLS Layer 3 VPNs Feature

See the *NSF/SSO-MPLS VPN Guide* for information on configuring MPLS VPN GR on peer RPs to ensure that routing and forwarding is not disrupted if there is a hardware failure on the primary RP.

# Best Practices for Scalability and Convergence in the Cisco IOS Software Modularity: MPLS Layer 3 VPNs Feature

The Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature is designed to have LDP and TE scalability and overall convergence values that are within 20 percent of comparable values in nonmodularized images. Routers that have enough memory to cover some 10 to 20 percent greater memory usage should not experience diminished performance.

See the *Cisco IOS Software Modularity Installation and Configuration Guide*, for guidelines on memory requirements for software modularization.

The following are the LDP and TE scalability and convergence effects:

- LDP scalability:
  - The Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature is very effective in reducing link flaps in link sessions.

  - Images with the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature can scale to up to 900 targeted LDP sessions, compared to 1200 sessions on nonmodularized images.
- TE scalability:
  - Tunnel setup times are longer and setup times increase as the number of tunnels increases but both times are within 20 percent of those on nonmodularized images.
- Convergence:
  - Convergence times on images with the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature are within 20 percent of those on nonmodularized images.

# CLI Changes Due to the Cisco IOS Software Modularity: Layer 3 VPNs Feature

The Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature introduces the following two new commands:

- **debug mpls traffic-eng process-restart**
- **show mpls traffic-eng process-restart iprouting**

It modifies the following four commands.

- **show ip route**
- **show mpls forwarding-table**
- **show mpls traffic-eng link-management advertisements**
- **show mpls traffic-eng link-management summary**

## New Commands

The **show mpls traffic-eng process-restart iprouting** command displays statistics about the resynchronization of the information shared between TE and the Internet Gateway Protocols after an IP routing process restart.

The **debug mpls traffic-eng process-restart** command displays messages related to the transfer of information between TE and the IGPs, and the resynchronization of this information, including the flushing of any stale information, after an IP Routing process restart.

See "Command Reference" section on page 10 for more information on the new commands.

## Modified Commands

The output of the **show mpls traffic-eng link-management summary** and the **show mpls traffic-eng link-management advertisements** commands are enhanced to show when an IP routing process restart is in progress.

The detailed output of the **show ip route** command (when you specify a prefix or mask) is enhanced to show remote label information and MPLS flags for prefixes that have a remote label stored in RIB. Remote MPLS labels used for forwarding that were formerly stored in IPRM working with BGP are now stored in RIB. This enhanced output can be used for troubleshooting.

The output of the **show mpls forwarding-table** command is enhanced to display troubleshooting information in the first column, Local Label, as follows:

- An [H] notation indicates local labels that are temporarily in holddown, that is, the application that requested the labels no longer needs them and stops advertising them to its labeling peers.

- A [T] notation indicates forwarding through a label switched path (LSP).
- An [HT] notation indicates that both conditions apply.

These outputs are shown whether or not users specify the **detail** or the **internal** keywords. You can use the **detail** or the **internal** keyword to display more information.

See the "Command Reference" section on page 10 for more information on the modified commands.

# Additional References

The following sections provide references related to the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature.

## Related Documents

| Related Topic | Document Title |
|---|---|
| Installing the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature | *Cisco IOS Software Modularity Installation and Configuration Guide* |
| High availability | *MPLS High Availability: Overview* |
| Nonstop forwarding | *NSF/SSO: MPLS VPN* |
| High availability | *MPLS High Availability: Command Changes* |
| Graceful restart | *NSF/SSO: MPLS LDP and LDP Graceful Restart*<br>*NSF/SSO—MPLS TE and RSVP Graceful Restart*<br>*NSF/SSO: Any Transport over MPLS and AToM Graceful Restart* |
| Express forwarding | *Cisco Express Forwarding: 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 | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

## RFCs

| RFC | Title |
|---|---|
| RFC 1163 | A Border Gateway Protocol |
| RFC 1164 | Application of the Border Gateway Protocol in the Internet |
| RFC 2283 | Multiprotocol Extensions for BGP-4 |
| RFC 2547 | BGP/MPLS VPNs |

## Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com. | http://www.cisco.com/techsupport |

# Command Reference

This section documents new and modified commands only.

### New Commands

- **debug mpls traffic-eng process-restart**
- **show mpls traffic-eng process-restart iprouting**

### Modified Commands

- **show ip route vrf**
- **show mpls forwarding-table**
- **show mpls traffic-eng link-management advertisements**
- **show mpls traffic-eng link-management summary**

# debug mpls traffic-eng process-restart

To display information about process restarts for reporting to your technical support representative, use the **debug mpls traffic-eng process-restart** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug mpls traffic-eng process-restart**

**no debug mpls traffic-eng process-restart**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXH | This command was introduced. |

## Usage Guidelines

If you report a problem and the **show mpls traffic-eng process-restart iprouting** displays abnormal results, your technical support representative might ask you to issue the **debug mpls traffic-eng process-restart** command, then perform an IP routing process restart and capture the output for analysis.

## Examples

The following example shows partial output from an IP routing process restart:

```
Router# debug mpls traffic-eng process-restart

02:24:22: SM: ---TE ION Process Restart 0x78EF9050: process restart (3)
02:24:22: SM:    NORM (1) --> AWAIT-CFG (3)
02:24:22: TE ION Restart timer started, proc_idx:0 delay:120000
02:24:22: SM: ---TE ION Process Restart 0x78EF9050: process cfg replay start (4)
02:24:22: SM:    AWAIT-CFG (3) --> CFG (4)
02:24:22: TE ION Restart timer started, proc_idx:0 delay:300000
02:24:22: SM: ---TE ION Process Restart 0x78EF9050: reg invoke succeeded (2)
02:24:22: SM:    CFG (4) --> CFG (4)
02:24:22: SM: ---TE ION Process Restart 0x78EF9050: process cfg replay done (5)
02:24:22: SM:    CFG (4) --> SYNC (5)
02:24:22: TE ION Restart timer started, proc_idx:0 delay:900000
```

The output shows typical process restart information that your technical support representative might request if you report a problem after an IP process restart. The information displayed can vary, depending on the conditions that caused the restart.

## Related Commands

| Command | Description |
|---|---|
| **show mpls traffic-eng process-restart iprouting** | Displays the status of IP routing and MPLS traffic engineering synchronization after an IP routing process restarts. |

# show ip route vrf

To display the IP routing table associated with a Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **show ip route vrf** command in user EXEC or privileged EXEC mode.

**show ip route vrf** *vrf-name* [**connected**] [*protocol* [*as-number*] [*tag*] [*output-modifiers*]] [*ip-prefix*] [**list** *number* [*output-modifiers*]] [**profile**] [**static** [*output-modifiers*]] [**summary** [*output-modifiers*]] [**supernets-only** [*output-modifiers*]]

## Syntax Description

| | |
|---|---|
| *vrf-name* | Name assigned to the VRF. |
| **connected** | (Optional) Displays all connected routes in a VRF. |
| *protocol* | (Optional) To specify a routing protocol, use one of the following keywords: **bgp**, **egp**, **eigrp**, **hello**, **igrp**, **isis**, **ospf**, or **rip**. |
| *as-number* | (Optional) Autonomous system number. |
| *tag* | (Optional) Cisco IOS routing area label. |
| *output-modifiers* | (Optional) For a list of associated keywords and arguments, use context-sensitive help. |
| *ip-prefix* | (Optional) Specifies a network to display. |
| **list** *number* | (Optional) Specifies the IP access list to display. |
| **profile** | (Optional) Displays the IP routing table profile. |
| **static** | (Optional) Displays static routes. |
| **summary** | (Optional) Displays a summary of routes. |
| **supernets-only** | (Optional) Displays supernet entries only. |

## Command Modes

User EXEC
Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |
| 12.2(2)T | The *ip-prefix* argument was added. The output from the **show ip route vrf** *vrf-name ip-prefix* command was enhanced to display information on the multipaths to the specified network. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.0(22)S | Enhanced Interior Gateway Routing Protocol (EIGRP) VRF support was added. |
| 12.2(15)T | EIGRP VRF support was integrated into Cisco IOS Release 12.2(15)T. |
| 12.2(18)S | EIGRP VRF support was integrated into Cisco IOS Release 12.2(18)S. |
| 12.2(27)SBC | This command was integrated into Cisco IOS Release 12.2(27)SBC. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | The output was enhanced to display remote label information and corresponding MPLS flags for prefixes that have remote labels stored in the Routing Information Base (RIB). |

## Usage Guidelines

This command displays specified information from the IP routing table of a VRF.

## Examples

This example shows the IP routing table associated with the VRF named vrf1:

```
Router# show ip route vrf vrf1

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR
       T - traffic engineered route

Gateway of last resort is not set

B    10.0.0.0/8 [200/0] via 10.13.13.13, 00:24:19
C    10.0.0.0/8 is directly connected, Ethernet1/3
B    10.0.0.0/8 [20/0] via 10.0.0.1, 02:10:22
B    10.0.0.0/8 [200/0] via 10.13.13.13, 00:24:20
```

This example shows BGP entries in the IP routing table associated with the VRF named vrf1:

```
Router# show ip route vrf vrf1 bgp

B  10.0.0.0/8 [200/0] via 10.13.13.13, 03:44:14
B  10.0.0.0/8 [20/0] via 10.0.0.1, 03:44:12
B  10.0.0.0/8 [200/0] via 10.13.13.13, 03:43:14
```

This example shows the IP routing table associated with a VRF named PATH and network 10.22.22.0:

```
Router# show ip route vrf PATH 10.22.22.0

Routing entry for 10.22.22.0/24
  Known via "bgp 1", distance 200, metric 0
  Tag 22, type internal
  Last update from 10.22.5.10 00:01:07 ago
  Routing Descriptor Blocks:
  * 10.22.7.8 (Default-IP-Routing-Table), from 10.11.3.4, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.22.1.9 (Default-IP-Routing-Table), from 10.11.1.2, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.22.6.10 (Default-IP-Routing-Table), from 10.11.6.7, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.22.4.10 (Default-IP-Routing-Table), from 10.11.4.5, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.22.5.10 (Default-IP-Routing-Table), from 10.11.5.6, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
```

Table 1 describes the significant fields shown when the **show ip route vrf** *vrf-name ip-prefix* command is used.

*Table 1 show ip route vrf Field Descriptions*

| Field | Description |
|---|---|
| Routing entry for 10.22.22.0/24 | Network number. |
| Known via ... | Indicates how the route was derived. |
| distance | Administrative distance of the information source. |
| metric | The metric to reach the destination network. |
| Tag | Integer that is used to implement the route. |
| type | Indicates that the route is an L1 type or L2 type route. |
| Last update from 10.22.5.10 | Indicates the IP address of a router that is the next hop to the remote network and the router interface on which the last update arrived. |
| *hh*:*mm*:*ss* ago | Specifies the last time the route was updated (in hours:minutes:seconds). |
| Routing Descriptor Blocks: | Displays the next hop IP address followed by the information source. |
| *ip-address*, from *ip-address*, *hh*:*mm*:*ss* ago | Indicates the next hop address, the address of the gateway that sent the update, and the time that has elapsed since this update was received (in hours:minutes:seconds). |
| Route metric | This value is the best metric for this routing descriptor block. |
| traffic share count | Number of uses for this routing descriptor block. |
| AS Hops | Number of hops to the destination or to the router where the route first enters internal BGP (iBGP). |

### Example of Output Using the Cisco IOS Software Modularity for Layer 3 VPNs Feature

The following is sample output from the **show ip route vrf** command on routers using the Cisco IOS Software Modularity for Layer 3 VPNs feature. The output includes remote label information and corresponding MPLS flags for prefixes that have remote labels stored in the RIB, if BGP is the label distribution protocol:

```
Router# show ip route vrf v2 10.2.2.2

Routing entry for 10.2.2.2/32
  Known via "bgp 1", distance 200, metric 0, type internal
  Redistributing via ospf 2
  Advertised by ospf 2 subnets
  Last update from 10.0.0.4 00:22:59 ago
  Routing Descriptor Blocks:
  * 10.0.0.4 (Default-IP-Routing-Table), from 10.0.0.31, 00:22:59 ago
      Route metric is 0, traffic share count is 1
      AS Hops 0
      MPLS label: 1300
      MPLS Flags: MPLS Required
```

Table 2 describes the significant fields shown in the display.

*Table 2 show ip route vrf Field Descriptions*

| Field | Description |
|---|---|
| MPLS label | Displays the BGP prefix from the BGP peer. The output shows one of the following values:<br>• A label value (16 - 1048575)<br>• A reserved label value, such as explicit-null or implicit-null<br>• The word "none" if no label is received from the peer<br>The MPLS label field does not display if any of the following conditions is true:<br>• BGP is not the LDP. However, OSPF prefixes learned via sham link display an MPLS label.<br>• MPLS is not supported.<br>• The prefix was imported from another VRF, where the prefix was an IGP prefix and LDP provided the remote label for it. |
| MPLS Flags | The name of one of the following MPLS flags is displayed if any is set:<br>• MPLS Required—Packets are forwarded to this prefix because the MPLS label stack is present. If MPLS is disabled in the outgoing interface, the packets are dropped.<br>• No Global—MPLS packets for this prefix are forwarded from the VRF interface, not from the interface in global table. Using the VRF interface prevents loops in scenarios that use ieBGP multipath.<br>• NSF—The prefix is from an NSF-aware neighbor. If the routing information temporarily disappears due to a disruption in the control plane, packets for this prefix are preserved. |

## Related Commands

| Command | Description |
|---|---|
| **show ip cache** | Displays the Cisco Express forwarding table associated with a VRF. |
| **show ip vrf** | Displays the set of defined VRFs and associated interfaces. |

# show mpls forwarding-table

To display the contents of the Multiprotocol Label Switching (MPLS) Label Forwarding Information Base (LFIB), use the **show mpls forwarding-table** command in privileged EXEC mode.

**show mpls forwarding-table** [*network* {*mask* | *length*} | **labels** *label* [**-** *label*] | **interface** *interface* | **next-hop** *address* | **lsp-tunnel** [*tunnel-id*]] [**vrf** *vrf-name*] [**detail**]

## Syntax Description

| | |
|---|---|
| *network* | (Optional) Destination network number. |
| *mask* | IP address of the destination mask whose entry is to be shown. |
| *length* | Number of bits in the mask of the destination. |
| **labels** *label* **-** *label* | (Optional) Displays only entries with the specified local labels. |
| **interface** *interface* | (Optional) Displays only entries with the specified outgoing interface. |
| **next-hop** *address* | (Optional) Displays only entries with the specified neighbor as the next hop. |
| **lsp-tunnel** | (Optional) Displays only entries with the specified label switched path (LSP) tunnel, or with all LSP tunnel entries. |
| *tunnel-id* | (Optional) Specifies the LSP tunnel for which to display entries. |
| **vrf** *vrf-name* | (Optional) Displays only entries with the specified VPN routing and forwarding (VRF) instance. |
| **detail** | (Optional) Displays information in long form (includes length of encapsulation, length of MAC string, maximum transmission unit (MTU), and all labels). |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 11.1CT | This command was introduced. |
| 12.1(3)T | This command was updated with MPLS terminology and command syntax. |
| 12.2(8)T | The command was modified to accommodate use of the MPLS experimental (EXP) level as a selection criterion for packet forwarding. The output display was modified to include a bundle adjacency field and exp (vcd) values when the optional **detail** keyword is specified. |
| 12.0(22)S | IPv6 MPLS aggregate label and prefix information was added to the display. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.0(27)S | The command output was modified to include explicit-null label information. |
| 12.2(25)S | The output was changed in the following ways:<br>• The term “tag” was replaced with the term “label.”<br>• The term “untagged” was replaced with the term “no label.” |
| 12.0(29)S | This command was integrated into Cisco IOS Release 12.0(29)S. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers. |

| Release | Modification |
|---|---|
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | The command output was modified for the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature to show the status of local labels in holdown. The status indicator showing that traffic is forwarded through an LSP tunnel is moved to the local label. |

## Examples

The following is sample output from the **show mpls forwarding-table** command:

```
Router# show mpls forwarding-table

Local Outgoing      Prefix            Bytes label Outgoing       Next Hop
Label Label or VC   or Tunnel Id      switched  interface
26    No Label      10.253.0.0/16     0         Et4/0/0       10.27.32.4
28    1/33          10.15.0.0/16      0         AT0/0.1       point2point
29    Pop Label     10.91.0.0/16      0         Hs5/0         point2point
      1/36          10.91.0.0/16      0         AT0/0.1       point2point
30    32            10.250.0.97/32    0         Et4/0/2       10.92.0.7
      32            10.250.0.97/32    0         Hs5/0         point2point
34    26            10.77.0.0/24      0         Et4/0/2       10.92.0.7
      26            10.77.0.0/24      0         Hs5/0         point2point
35    No Label[T]   10.100.100.101/32 0         Tu301         point2point
36    Pop Label     10.1.0.0/16       0         Hs5/0         point2point
      1/37          10.1.0.0/16       0         AT0/0.1       point2point

[T]     Forwarding through a TSP tunnel.
        View additional labeling info with the 'detail' option
```

The following is sample output from the **show mpls forwarding-table** command when the IPv6 Provider Edge Router over MPLS feature is configured to allow IPv6 traffic to be transported across an IPv4 MPLS backbone. The labels are aggregated because there are several prefixes for one local label, and the prefix column contains “IPv6” instead of a target prefix.

```
Router# show mpls forwarding-table

Local Outgoing      Prefix            Bytes label Outgoing       Next Hop
Label Label or VC   or Tunnel Id      switched  interface
16    Aggregate     IPv6              0
17    Aggregate     IPv6              0
18    Aggregate     IPv6              0
19    Pop Label     192.168.99.64/30  0         Se0/0         point2point
20    Pop Label     192.168.99.70/32  0         Se0/0         point2point
21    Pop Label     192.168.99.200/32 0         Se0/0         point2point
22    Aggregate     IPv6              5424
23    Aggregate     IPv6              3576
24    Aggregate     IPv6              2600
```

The following is sample output from the **show mpls forwarding-table** command when you specify the **detail** keyword. If the MPLS EXP level is used as a selection criterion for packet forwarding, a bundle adjacency exp (vcd) field is included in the display. This field includes the EXP value and the corresponding virtual circuit descriptor (VCD) in parentheses. The line in the output that reads “No output feature configured” indicates that the MPLS egress NetFlow accounting feature is not enabled on the outgoing interface for this prefix.

```
Router# show mpls forwarding-table detail

Local Outgoing      Prefix            Bytes label Outgoing       Next Hop
label   label or VC     or Tunnel Id      switched  interface
16    Pop label       10.0.0.6/32       0         AT1/0.1       point2point
```

```
      Bundle adjacency exp(vcd)
      0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
      MAC/Encaps=12/12, MTU=4474, label Stack{}
      00010000AAAA030000008847
      No output feature configured
17    18            10.0.0.9/32        0         AT1/0.1       point2point
      Bundle adjacency exp(vcd)
      0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
      MAC/Encaps=12/16, MTU=4470, label Stack{18}
      00010000AAAA030000008847 00012000
      No output feature configured
18    19            10.0.0.10/32        0        AT1/0.1       point2point
      Bundle adjacency exp(vcd)
      0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
      MAC/Encaps=12/16, MTU=4470, label Stack{19}
      00010000AAAA030000008847 00013000
      No output feature configured
19    17            10.0.0.0/8         0        AT1/0.1       point2point
      Bundle adjacency exp(vcd)
      0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
      MAC/Encaps=12/16, MTU=4470, label Stack{17}
      00010000AAAA030000008847 00011000
      No output feature configured
20    20            10.0.0.0/8         0        AT1/0.1       point2point
      Bundle adjacency exp(vcd)
      0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
      MAC/Encaps=12/16, MTU=4470, label Stack{20}
      00010000AAAA030000008847 00014000
      No output feature configured
21    Pop label       10.0.0.0/24        0        AT1/0.1       point2point
      Bundle adjacency exp(vcd)
      0(1) 1(1) 2(1) 3(1) 4(1) 5(1) 6(1) 7(1)
      MAC/Encaps=12/12, MTU=4474, label Stack{}
      00010000AAAA030000008847
      No output feature configured
22    Pop label       10.0.0.4/32         0        Et2/3         10.0.0.4
      MAC/Encaps=14/14, MTU=1504, label Stack{}
      000427AD10430005DDFE043B8847
      No output feature configured
```

The following is sample output from the **show mpls forwarding-table** command when you use the **detail** keyword. In this example, the MPLS egress NetFlow accounting feature is enabled on the first three prefixes, as indicated by the line in the output that reads “Feature Quick flag set.”

```
Router# show mpls forwarding-table detail

Local  Outgoing    Prefix            Bytes label  Outgoing   Next Hop
label    label or VC   or Tunnel Id      switched   interface
16     Aggregate   10.0.0.0/8[V]     0
        MAC/Encaps=0/0, MTU=0, label Stack{}
        VPN route: vpn1
        Feature Quick flag set
Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
17     No label    10.0.0.0/8[V]      0          Et0/0/2    10.0.0.1
        MAC/Encaps=0/0, MTU=1500, label Stack{}
        VPN route: vpn1
        Feature Quick flag set
Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
18     No label    10.42.42.42/32[V] 4185       Et0/0/2    10.0.0.1
        MAC/Encaps=0/0, MTU=1500, label Stack{}
        VPN route: vpn1
        Feature Quick flag set
Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
19     2/33        10.41.41.41/32    0          AT1/0/0.1  point2point
```

```
        MAC/Encaps=4/8, MTU=4470, label Stack{2/33(vcd=2)}
        00028847 00002000
        No output feature configured
```

### Cisco 10000 Series Examples

The following is sample output from the **show mpls forwarding-table** command:

```
Router# show mpls forwarding-table

Local   Outgoing      Prefix            Bytes Label   Outgoing   Next Hop
Label   Label or VC   or Tunnel Id      Switched      interface
16      Pop Label     10.0.0.0/8        0             Fa1/0/0    10.0.0.2
        Pop Label     10.0.0.0/8        0             Fa1/1/0    10.0.0.2
17      Aggregate     10.0.0.0/8[V]     570           vpn2
21      Pop Label     10.11.11.11/32    0             Fa1/0/0    10.0.0.2
22      Pop Label     10.12.12.12/32    0             Fa1/1/0    10.0.0.2
23      No Label      10.3.0.0/16[V]     0             Fa4/1/0   10.0.0.2
```

The following is Cisco 10000 series sample output from the **show mpls forwarding-table** command when you specify the **detail** keyword:

```
Router# show mpls forwarding-table detail

Local   Outgoing      Prefix            Bytes Label   Outgoing   Next Hop
Label   Label or VC   or Tunnel Id      Switched      interface
16      Pop Label     10.0.0.0/8        0             Fa1/0/0    10.0.0.2
        MAC/Encaps=14/14, MRU=1500, Label Stack{}
        000B45C93889000B45C930218847
        No output feature configured
        Pop Label     10.0.0.0/8        0             Fa1/1/0     10.0.0.2
        MAC/Encaps=14/14, MRU=1500, Label Stack{}
        000B45C92881000B45C930288847
        No output feature configured
17      Aggregate    10.0.0.0/8[V]      570           vpn2
        MAC/Encaps=0/0, MRU=0, Label Stack{}
        VPN route: vpn2
        No output feature configured
21      Pop Label     10.11.11.11/32     0            Fa1/0/0     10.0.0.2
        MAC/Encaps=14/14, MRU=1500, Label Stack{}
       000B45C93889000B45C930218847
       No output feature configured
```

Table 3 describes the significant fields shown in the displays.

***Table 3 show mpls forwarding-table Field Descriptions***

| Field | Description |
|---|---|
| Local label | Label assigned by this router. |

*Table 3 show mpls forwarding-table Field Descriptions (continued)*

| Field | Description |
|---|---|
| Outgoing Label or VC<br>**Note** This field is not supported on the Cisco 10000 series routers. | Label assigned by the next hop or virtual path identifier (VPI)/virtual channel identifier (VCI) used to get to next hop. The entries in this column are the following:<br>• [T]—Means forwarding through an LSP tunnel.<br>• No Label—Means that there is no label for the destination from the next hop or that label switching is not enabled on the outgoing interface.<br>• Pop Label—Means that the next hop advertised an implicit NULL label for the destination and that the router removed the top label.<br>• Aggregate—Means there are several prefixes for one local label. This entry is used when IPv6 is configured on edge routers to transport IPv6 traffic over an IPv4 MPLS network. |
| Prefix or Tunnel Id | Address or tunnel to which packets with this label are sent.<br>**Note** If IPv6 is configured on edge routers to transport IPv6 traffic over an IPv4 MPLS network, "IPv6" is displayed here.<br>[V]—means that the corresponding prefix is in a VRF. |
| Bytes label switched | Number of bytes switched with this incoming label. This includes the outgoing label and Layer 2 header. |
| Outgoing interface | Interface through which packets with this label are sent. |
| Next Hop | IP address of the neighbor that assigned the outgoing label. |
| Bundle adjacency exp(vcd) | Bundle adjacency information. Includes the MPLS EXP value and the corresponding VCD. |
| MAC/Encaps | Length in bytes of the Layer 2 header and length in bytes of the packet encapsulation, including the Layer 2 header and label header. |
| MTU | MTU of the labeled packet. |
| label Stack | All the outgoing labels. If the outgoing interface is transmission convergence (TC)-ATM, the VCD is also shown.<br>**Note** TC-ATM is not supported on Cisco 10000 series routers. |
| 00010000AAAA030000008847<br>00013000 | The actual encapsulation in hexadecimal form. A space is shown between Layer 2 and the label header. |

### Explicit-Null Label Example

The following example shows output, including the explicit-null label = 0 (commented in bold), from the **show mpls forwarding-table** command on a CSC-PE router:

```
Router# show mpls forwarding-table

Local  Outgoing      Prefix           Bytes label  Outgoing   Next Hop
```

```
label  label or VC   or Tunnel Id      switched     interface
17     Pop label     10.10.0.0/32      0            Et2/0      10.10.0.1
18     Pop label     10.10.10.0/24     0            Et2/0      10.10.0.1
19     Aggregate     10.10.20.0/24[V]  0
20     Pop label     10.10.200.1/32[V] 0            Et2/1      10.10.10.1
21     Aggregate     10.10.1.1/32[V]   0
22     0             192.168.101.101/32[V]   \
                                       0            Et2/1      192.168.101.101
23     0             192.168.101.100/32[V]   \
                                       0            Et2/1      192.168.101.100
25     0             192.168.102.125/32[V] 0        Et2/1      192.168.102.125 !outlabel
value 0
```

Table 4 describes the significant fields shown in the display.

***Table 4 show mpls forwarding-table Field Descriptions***

| Field | Description |
|---|---|
| Local label | Label assigned by this router. |
| Outgoing label or VC | Label assigned by the next hop or VPI/VCI used to get to next hop. The entries this column are the following:<br>• [T]—Means forwarding through an LSP tunnel.<br>• No label—Means that there is no label for the destination from the next hop or that label switching is not enabled on the outgoing interface.<br>• Pop label—Means that the next hop advertised an implicit NULL label for the destination and that this router popped the top label.<br>• Aggregate—Means there are several prefixes for one local label. This entry is used when IPv6 is configured on edge routers to transport IPv6 traffic over an IPv4 MPLS network.<br>• 0—Means the explicit null label value = 0. |
| Prefix or Tunnel Id | Address or tunnel to which packets with this label are going.<br>**Note** If IPv6 is configured on edge routers to transport IPv6 traffic over an IPv4 MPLS network, IPv6 is displayed here.<br>[V]—means that the corresponding prefix is in a VRF. |
| Bytes label switched | Number of bytes switched with this incoming label. This includes the outgoing label and Layer 2 header. |
| Outgoing interface | Interface through which packets with this label are sent. |
| Next Hop | IP address of the neighbor that assigned the outgoing label. |

### Cisco IOS Software Modularity: MPLS Layer 3 VPNs Example

The following is sample output from the **show mpls forwarding-table** command.

```
Router# show mpls forwarding-table

Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         Pop Label  IPv4 VRF[V]      62951000      aggregate/v1
17    [H]  No Label   10.1.1.0/24      0             AT1/0/0.1 point2point
           No Label   10.1.1.0/24      0             PO3/1/0 point2point
      [T]  No Label   10.1.1.0/24      0             Tu1 point2point
```

```
18     [HT] Pop Label  10.0.0.3/32      0            Tu1 point2point
19     [H]  No Label   10.0.0.0/8       0            AT1/0/0.1 point2point
            No Label   10.0.0.0/8       0            PO3/1/0 point2point
20     [H]  No Label   10.0.0.0/8       0            AT1/0/0.1 point2point
            No Label   10.0.0.0/8       0            PO3/1/0 point2point
21     [H]  No Label   10.0.0.1/32      812          AT1/0/0.1 point2point
            No Label   10.0.0.1/32      0            PO3/1/0 point2point
22     [H]  No Label   10.1.14.0/24     0            AT1/0/0.1 point2point
            No Label   10.1.14.0/24     0            PO3/1/0 point2point
23     [HT] 16         172.1.1.0/24[V]  0            Tu1 point2point
24     [HT] 24         10.0.0.1/32[V]   0            Tu1 point2point
25     [H]  No Label   10.0.0.0/8[V]    0            AT1/1/0.1 point2point
26     [HT] 16         10.0.0.3/32[V]   0            Tu1 point2point
27          No Label   10.0.0.1/32[V]   0            AT1/1/0.1 point2point

[T]     Forwarding through a TSP tunnel.
        View additional labelling info with the 'detail' option
[H]     Local label is being held down temporarily.
```

Table 5 describes the field relating to the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature that is shown in the display.

***Table 5 show mpls forwarding-table Field Descriptions***

| Field | Description |
|---|---|
| Local label | Label assigned by this router.<br>• [H]—Local labels are in holddown, which means that the application that requested the labels no longer needs them and stops advertising them to its labeling peers.<br>The label's forwarding-table entry is deleted after a short, application-specific time.<br>If any application starts advertising a held-down label to its labeling peers, the label could come out of holddown.<br>**Note** [H] is not shown if labels are held down globally.<br>A label enters global holddown after a stateful switchover or a restart of certain processes in a Cisco IOS modularity environment.<br>• [T]—The label is forwarded through an LSP tunnel.<br>**Note** Although [T] is still a property of the outgoing interface, it is shown in the Local label column.<br>• [HT]—Both conditions apply. |

## Related Commands

| Command | Description |
|---|---|
| **neighbor send-label** | Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router. |
| **neighbor send-label explicit-null** | Enables a BGP router to send MPLS labels with explicit-null information for a CSC-CE router and BGP routes to a neighboring CSC-PE router. |

# show mpls traffic-eng link-management advertisements

To display local link information that Multiprotocol Label Switching (MPLS) traffic engineering link management is currently flooding into the global traffic engineering topology, use the **show mpls traffic-eng link-management advertisements** command in user EXEC or privileged EXEC mode.

**show mpls traffic-eng link-management advertisements**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

User EXEC
Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(5)S | This command was introduced. |
| 12.1(3)T | The command output was modified. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | The output was enhanced to show Internet Gateway Protocol (IGP) recovery status provided by the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature. |

## Examples

The following is sample output from the **show mpls traffic-eng link-management advertisements** command:

```
Router# show mpls traffic-eng link-management advertisements

Flooding Status:     ready
Configured Areas:    1
IGP Area[1] ID:: isis level-1
  System Information::
    Flooding Protocol:   ISIS
  Header Information::
    IGP System ID:       0001.0000.0001.00
    MPLS TE Router ID:   10.106.0.6
    Flooded Links:       1
  Link ID:: 0
    Link IP Address:     10.1.0.6
    IGP Neighbor:        ID 0001.0000.0001.02
    Admin. Weight:       10
    Physical Bandwidth:  10000 kbits/sec
    Max Reservable BW:   5000 kbits/sec
    Downstream::
      Reservable Bandwidth[0]:       5000 kbits/sec
      Reservable Bandwidth[1]:       2000 kbits/sec
      Reservable Bandwidth[2]:       2000 kbits/sec
      Reservable Bandwidth[3]:       2000 kbits/sec
      Reservable Bandwidth[4]:       2000 kbits/sec
      Reservable Bandwidth[5]:       2000 kbits/sec
      Reservable Bandwidth[6]:       2000 kbits/sec
      Reservable Bandwidth[7]:       2000 kbits/sec
```

```
    Attribute Flags:     0x00000000
```

Table 6 describes the significant fields shown in the display.

***Table 6 show mpls traffic-eng link-management advertisements Field Descriptions***

| Field | Description |
|---|---|
| Flooding Status | Status of the link management flooding system. |
| Configured Areas | Number of the IGP areas configured. |
| IGP Area [1] ID | Name of the first IGP area. |
| Flooding Protocol | IGP that is flooding information for this area. |
| IGP System ID | Identification that IGP flooding uses in this area to identify this node. |
| MPLS TE Router ID | MPLS traffic engineering router ID. |
| Flooded Links | Number of links that are flooded in this area. |
| Link ID | Index of the link that is being described. |
| Link IP Address | Local IP address of this link. |
| IGP Neighbor | IGP neighbor on this link. |
| Admin. Weight | Administrative weight associated with this link. |
| Physical Bandwidth | Link bandwidth capacity (in kBps). |
| Max Reservable BW | Amount of reservable bandwidth (in kBps) on this link. |
| Reservable Bandwidth | Amount of bandwidth (in kBps) that is available for reservation. |
| Attribute Flags | Attribute flags of the link are being flooded. |

The following is sample output from the **show mpls traffic-eng link-management advertisements** command with the enhanced output, which shows the “IGP recovering” status, from the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature:

```
Router# show mpls traffic-eng link-management advertisements

show mpls traffic-eng link-management advertisements
Flooding Status:      ready (IGP recovering)
Configured Areas:     1
IGP Area[1] ID::  ospf  area nil
  System Information::
    Flooding Protocol:    OSPF
  Header Information::
```

Table 7 describes the significant fields shown in the display.

***Table 7 show mpls traffic-eng link-management advertisements Field Descriptions***

| Field | Description |
|---|---|
| Flooding Status | Status of the link management flooding system.<br>The notation (IGP recovering) indicates that flooding cannot be determined because an IP routing process restart is in progress. |
| Configured Areas | Number of the IGP areas configured. |

**Related Commands**

| Command | Description |
|---|---|
| **show mpls traffic-eng link-management bandwidth-allocation** | Displays current local link information. |
| **show mpls traffic-eng link-management igp-neighbors** | Displays IGP neighbors. |
| **show mpls traffic-eng link-management interfaces** | Displays per-interface resource and configuration information. |
| **show mpls traffic-eng link-management summary** | Displays a summary of link management information. |

# show mpls traffic-eng link-management summary

To display a summary of link management information, use the **show mpls traffic-eng link-management summary** command in user EXEC or privileged EXEC mode.

**show mpls traffic-eng link-management summary** [*interface-name*]

## Syntax Description

| | |
|---|---|
| *interface-name* | Specific interface for which information will be displayed. |

## Command Modes

User EXEC
Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(5)S | This command was introduced. |
| 12.1(3)T | The command output was modified. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | The output was enhanced to display Internet Gateway Protocol (IGP) recovery status provided by the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature. |

## Examples

The following is sample output from the **show mpls traffic-eng link-management summary** command:

```
Router# show mpls traffic-eng link-management summary

System Information::
    Links Count:         2
    Flooding System:     enabled
IGP Area ID:: isis level-1
    Flooding Protocol:   ISIS
    Flooding Status:     data flooded
    Periodic Flooding:   enabled (every 180 seconds)
    Flooded Links:       1
    IGP System ID:       0001.0000.0001.00
    MPLS TE Router ID:   10.106.0.6
    IGP Neighbors:       1
Link ID:: Et4/0/1 (10.1.0.6)
    Link Status:
      Physical Bandwidth:  10000 kbits/sec
      Max Reservable BW:   5000 kbits/sec (reserved:0% in, 60% out)
      MPLS TE Link State:  MPLS TE on, RSVP on, admin-up, flooded
      Inbound Admission:   reject-huge
      Outbound Admission:  allow-if-room
      Admin. Weight:       10 (IGP)
      IGP Neighbor Count:  1
Link ID:: AT0/0.2 (10.42.0.6)
    Link Status:
      Physical Bandwidth:  155520 kbits/sec
      Max Reservable BW:   5000 kbits/sec (reserved:0% in, 0% out)
      MPLS TE Link State:  MPLS TE on, RSVP on
```

```
    Inbound Admission:   allow-all
    Outbound Admission:  allow-if-room
    Admin. Weight:       10 (IGP)
    IGP Neighbor Count:  0
```

Table 8 describes the significant fields shown in the display.

***Table 8 show mpls traffic-eng link-management summary Field Descriptions***

| Field | Description |
|---|---|
| Links Count | Number of links configured for Multiprotocol Label Switching (MPLS) traffic engineering. |
| Flooding System | Enable status of the MPLS traffic engineering flooding system. |
| IGP Area ID | Name of the IGP area being described. |
| Flooding Protocol | IGP being used to flood information for this area. |
| Flooding Status | Status of flooding for this area. |
| Periodic Flooding | Status of periodic flooding for this area. |
| Flooded Links | Number of links that were flooded. |
| IGP System ID | IGP for this node associated with this area. |
| MPLS TE Router ID | MPLS traffic engineering router ID for this node. |
| IGP Neighbors | Number of reachable IGP neighbors associated with this area. |
| Link ID | Interface name and IP address of the link being described. |
| Physical Bandwidth | Link bandwidth capacity (in kBps). |
| Max Reservable BW | Amount of reservable bandwidth (in kBps) on this link. |
| MPLS TE Link State | Status of the link's MPLS traffic engineering-related functions. |
| Inbound Admission | Link admission policy for incoming tunnels. |
| Outbound Admission | Link admission policy for outgoing tunnels. |
| Admin. Weight | Link administrative weight. |
| IGP Neighbor Count | List of the IGP neighbors directly reachable over this link. |

The following is sample output from the **show mpls traffic-eng link-management summary** command with the enhanced output, which shows the "IGP recovering" status, from the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature:

```
Router# show mpls traffic-eng link-management summary

System Information::
    Links Count:          3
    Flooding System:      enabled (IGP recovering)
IGP Area ID::  ospf  area nil
    Flooding Protocol:    OSPF
    Flooding Status:      data flooded
    Periodic Flooding:    enabled (every 180 seconds)
    Flooded Links:        0
```

Table 7 describes the significant fields shown in the display.

***Table 9 show mpls traffic-eng link-management summary Field Descriptions***

| Field | Description |
|---|---|
| Links Count | Number of links configured for MPLS traffic engineering. |
| Flooding System | Status of the MPLS traffic engineering flooding system.<br>The notation (IGP recovering) indicates that status cannot be determined because an IP routing process restart is in progress. |
| IGP Area ID | Name of the IGP area being described. |
| Flooding Protocol | IGP being used to flood information for this area. |
| Flooding Status | Status of flooding for this area. |
| Periodic Flooding | Status of periodic flooding for this area. |
| Flooded Links | Number of links that were flooded. |

## Related Commands

| Command | Description |
|---|---|
| **show mpls traffic-eng link-management advertisements** | Displays local link information currently being flooded by MPLS traffic engineering link management into the global traffic engineering topology. |
| **show mpls traffic-eng link-management bandwidth-allocation** | Displays current local link information. |
| **show mpls traffic-eng link-management igp-neighbors** | Displays IGP neighbors. |
| **show mpls traffic-eng link-management interfaces** | Displays per-interface resource and configuration information. |

# show mpls traffic-eng process-restart iprouting

To display the status of IP routing and Multiprotocol Label Switching (MPLS) traffic engineering synchronization after an IP routing process restart, use the **show mpls traffic-eng process-restart iprouting** command in user EXEC or privileged EXEC mode.

**show mpls traffic-eng process-restart iprouting**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

User EXEC
Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXH | This command was introduced. |

## Usage Guidelines

This command displays information about the synchronization between the IP routing process and MPLS TE that you can provide to your technical support representative when you are reporting a problem.

All counters are set to zero when the system process initializes and are not reset no matter how often the IP routing process restarts.

The following is sample output from the **show mpls traffic-eng process-restart iprouting** command when an IP routing process has restarted normally:

```
Router# show mpls traffic-eng process-restart iprouting

IP Routing Restart Statistics:
  Current State: NORM
  Flushing State: IDLE

State Entered       Count     Timestamp            Timestamp            Timestamp
INIT                1         05/10/06-13:07:01
NORM                3         05/10/06-13:07:10    05/10/06-13:10:45   05/10/06-13:11:5
NORM-SPCT           0
AWAIT-CFG           2         05/10/06-13:10:32    05/10/06-13:11:45
CFG                 2         05/10/06-13:10:32    05/10/06-13:11:45
CMPL-FLSH           0
NCMPL-FLSH          2         05/10/06-13:10:32    05/10/06-13:11:45
NCMPL-FLSHD         2         05/10/06-13:10:32     05/10/06-13:11:45

Stuck State         Count     Timestamp             Timestamp          Timestamp
No Stuck states encountered

Counter             Count     Timestamp             Timestamp          Timestamp
Reg Succeed         40       05/10/06-13:11:51      05/10/06-13:11:45  05/10/06-13:11:45
Reg Fail             0
Incarnation          5       05/10/06-13:11:45      05/10/06-13:11:45  05/10/06-13:10:37
Flushing             2        05/10/06-13:10:32      05/10/06-13:11:45
```

Table 10 describes the normal output of the significant fields shown in the display. You should contact your technical support representative if your display has values other than those described in the table.

*Table 10 show mpls traffic-eng process-restart iprouting Field Descriptions*

| Field | Description |
|---|---|
| Current State | This indicates the restart status. NORM indicates that routing convergence has occurred and that TE and the Internet Gateway Protocols (IGPs) have synchronized. |
| Flushing State | This indicates the flushing state. It should indicate IDLE. |
| Stuck State | This indicates the stuck state. The Count column should indicate that no stuck state has been encountered. |
| Reg Fail | This indicates a registry failure. The Count column should indicate 0. |

**Related Commands**

| Command | Description |
|---|---|
| **debug mpls traffic-eng process-restart** | Displays information about process restarts for reporting to your technical support representative. |

# Feature Information for Cisco IOS Software Modularity: MPLS Layer 3 VPNs

Table 11 lists the release history for this feature.

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

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

**Note** Table 11 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

*Table 11 Feature Information for Cisoc IOS Software Modularity: MPLS Layer 3 VPNs*

| Feature Name | Releases | Feature Information |
|---|---|---|
| Cisco IOS Software Modularity: MPLS Layer 3 VPNs | 12.2(33)SXH | This feature extends software modularity to MPLS VPNs. |