



## **MPLS Basic MPLS Configuration Guide, Cisco IOS Release 12.2SR**

### **Americas Headquarters**

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2011 Cisco Systems, Inc. All rights reserved.



## CONTENTS

### **MPLS Transport Profile 1**

Finding Feature Information 1

Restrictions for MPLS-TP 1

Information About MPLS-TP 2

How MPLS-TP Works 3

MPLS-TP Path Protection 3

Bidirectional LSPs 3

MPLS-TP OAM Support 3

MPLS-TP Static and Dynamic Multisegment Pseudowires 4

MPLS-TP L2VPN Pseudowire Redundancy for Static and Dynamic Multisegment Pseudowires 4

MPLS-TP OAM Status for Static and Dynamic Multisegment Pseudowires 5

MPLS-TP Links and Physical Interfaces 5

Tunnel Midpoints 5

How to Configure MPLS-TP 6

Configuring the MPLS Label Range 6

Configuring the Router ID and Global ID 7

Configuring Bidirectional Forwarding Detection Templates 8

Configuring Pseudowire OAM Attributes 9

Configuring the Pseudowire Class 10

Configuring the Pseudowire 12

Configuring the MPLS-TP Tunnel 13

Configuring MPLS-TP LSPs at Midpoints 17

Configuring MPLS-TP Links and Physical Interfaces 19

Configuring Static-to-Static Multisegment Pseudowires for MPLS-TP 21

Configuring a Template with Pseudowire Type-Length-Value Parameters 23

Configuring Static-to-Dynamic Multisegment Pseudowires for MPLS-TP 23

Example 27

Configuring the L2VPN Pseudowire Redundancy for Static Multisegment Pseudowires 27

Example 29

Verifying the MPLS-TP Configuration	30
Additional References	30
Feature Information for MPLS-TP	31
<b>MPLS Static Labels</b>	<b>35</b>
Finding Feature Information	35
Restrictions for MPLS Static Labels	35
Prerequisites for MPLS Static Labels	36
Information About MPLS Static Labels	36
MPLS Static Labels Overview	36
Benefits of MPLS Static Labels	36
How to Configure MPLS Static Labels	36
Configuring MPLS Static Prefix Label Bindings	37
Verifying MPLS Static Prefix Label Bindings	38
Configuring MPLS Static Crossconnects	39
Verifying MPLS Static Crossconnect Configuration	40
Monitoring and Maintaining MPLS Static Labels	40
Configuration Examples for MPLS Static Labels	41
Example Configuring MPLS Static Prefixes Labels	41
Example Configuring MPLS Static Crossconnects	42
Additional References	43
Feature Information for MPLS Static Labels	44
Glossary	44
<b>NetFlow MPLS Label Export</b>	<b>47</b>
Finding Feature Information	47
Prerequisites for NetFlow MPLS Label Export	47
Restrictions for NetFlow MPLS Label Export	48
Information About NetFlow MPLS Label Export	48
MPLS Label Information Gathering and Exporting	48
Labels Allocated by VPNs BGP IPv4 or BGP VPNv4 in the MPLS PAL Table	49
MPLS PAL Table Record Export	50
MPLS PAL and NetFlow Statistics Correlation on a NetFlow Collector	52
MPLS Label Mapping on a Line Card	52
How to Configure NetFlow MPLS Label Export	52
Configuring NetFlow MPLS Label Export and MPLS PAL Table Export	53
Displaying Information About the MPLS PAL Table	54

Configuring the Export of MPLS VPN Version 4 Label Information from the MPLS PAL Table to a NetFlow Collector	56
Configuration Examples for NetFlow MPLS Label Export	58
Configuring NetFlow MPLS Prefix Application Label Table Export Examples	58
Configuring the Export of MPLS VPNv4 Label Information from the MPLS PAL Table Example	59
Additional References	59
Command Reference	60
Feature Information for NetFlow MPLS Label Export	61
Glossary	61
<b>ATM PVC Bundle Enhancement MPLS EXP-Based PVC Selection</b>	<b>65</b>
Finding Feature Information	65
Feature Overview	65
VC Bundle Support and Bundle Management	66
Benefits	67
Restrictions	68
Related Features and Technologies	68
Related Documents	68
Supported Platforms	68
Supported Standards MIBs and RFCs	69
Configuration Tasks	69
Enabling MPLS	70
Creating a VC Bundle	70
Applying Parameters to Bundles	70
Configuring Bundle-Level Parameters	70
Configuring a VC Bundle Member Directly	71
Configuring VC Class Parameters to Apply to a Bundle	71
Attaching a Class to a Bundle	72
Verifying the Configuration	72
Configuration Examples	72
Example VC Bundle Configuration Using a VC Class	72
Bundle-Class Class	73
Control-Class Class	73
Premium-Class Class	73
Priority-Class Class	74

Basic-Class Class **74**  
new-york Bundle **74**  
san-francisco Bundle **75**  
los-angeles Bundle **75**  
Command Reference **76**



# MPLS Transport Profile

---

The Multiprotocol Label Switching (MPLS) Transport Profile (TP) enables you to create tunnels that provide the transport network service layer over which IP and MPLS traffic traverse. MPLS-TP tunnels enable a transition from Synchronous Optical Networking (SONET) and Synchronous Digital Hierarchy (SDH) time-division multiplexing (TDM) technologies to packet switching to support services with high bandwidth requirements, such as video.

- [Finding Feature Information, page 1](#)
- [Restrictions for MPLS-TP, page 1](#)
- [Information About MPLS-TP, page 2](#)
- [How to Configure MPLS-TP, page 6](#)
- [Additional References, page 30](#)
- [Feature Information for MPLS-TP, page 31](#)

## Finding Feature Information

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

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

## Restrictions for MPLS-TP

- MPLS-TPpenultimate hop popping is not supported. Only ultimate hop popping is supported, because label mappings are configured at the MPLS-TP endpoints.
- Ethernet subinterfaces are not supported.
- IPV6 addressing is not supported.

### L2VPN Restrictions

- L2VPN interworking is not supported.
- Local switching with AToM pseudowire as a backup is not supported.
- L2VPN pseudowire redundancy to an AToM pseudowire by one or more attachment circuits is not supported.

- PW ID Forward Equivalence Class (FEC) (type 128) is supported, but generalized ID FEC (type 129) is not supported.
- Static Pseudowire Operations, Administration, and Maintenance (OAM) protocol and BFD VCCV attachment circuit (AC) status signaling are mutually exclusive protocols. BFD VCCV in failure detection mode can be used with Static Pseudowire OAM protocol.
- BFD VCCV AC status signaling cannot be used in pseudowire redundancy configurations. You can use Static Pseudowire OAM instead.

### Ping and Trace Restrictions

- Ping for Static Pseudowires over MPLS-TP tunnels is not supported.
- Pseudowire ping and traceroute functionality for multisegment pseudowires that have one or more static pseudowire segments is not supported.
- The following packet format is supported:
  - A labeled packet with Generic Associated Channel Label (GAL) at the bottom of the label stack.
  - ACH channel is IP (0x21).
  - RFC 4379-based IP, UDP packet payload with valid source.
  - Destination IP address and UDP port 3503.
- Default reply mode for (1) is 4—Reply via application level control channel. An echo reply consists of the following elements:
  - A labeled packet with a GAL label at the bottom of the label stack.
  - ACH channel is IP (0x21).
  - RFC 4379-based IP, UDP packet payload with valid source.
  - Destination IP address and UDP port 3503.
- The optional “do not reply” mode may be set.
- The following reply modes are not allowed and are disabled in CLI:
  - 2—Reply via an IPv4/IPv6 UDP packet
  - 3—Reply via an IPv4/IPv6 UDP packet with Router Alert
- Force-explicit-null is not supported with ping and trace.
- Optional Reverse Path Connectivity verification is not supported. See *LSP-Ping Extensions for MPLS-TP* (draft-nitinb-mpls-tp-lsp-ping-extensions-01.txt).

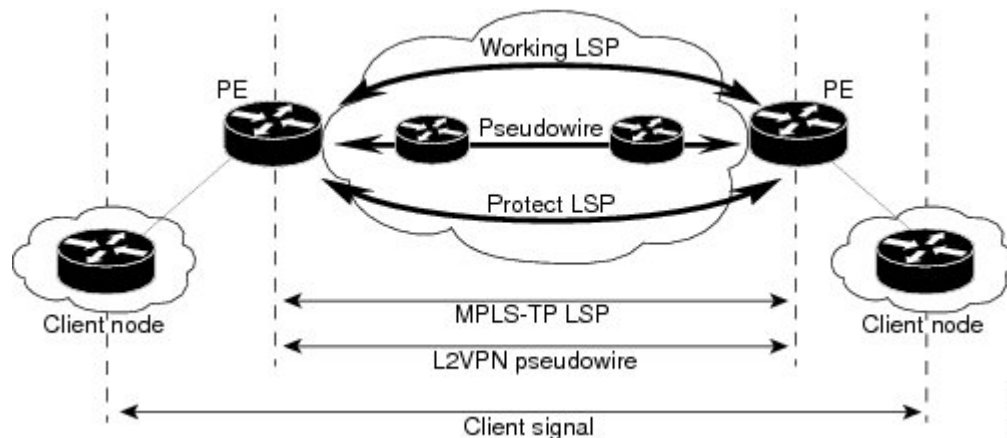
## Information About MPLS-TP

- [How MPLS-TP Works, page 3](#)
- [MPLS-TP Path Protection, page 3](#)
- [Bidirectional LSPs, page 3](#)
- [MPLS-TP OAM Support, page 3](#)
- [MPLS-TP Static and Dynamic Multisegment Pseudowires, page 4](#)
- [MPLS-TP L2VPN Pseudowire Redundancy for Static and Dynamic Multisegment Pseudowires, page 4](#)
- [MPLS-TP OAM Status for Static and Dynamic Multisegment Pseudowires, page 5](#)
- [MPLS-TP Links and Physical Interfaces, page 5](#)
- [Tunnel Midpoints, page 5](#)



## How MPLS-TP Works

MPLS-TP tunnels provide the transport network service layer over which IP and MPLS traffic traverse. MPLS-TP tunnels help transition from SONET/SDH TDM technologies to packet switching to support services with high bandwidth utilization and lower cost. Transport networks are connection oriented, statically provisioned, and have long-lived connections. Transport networks usually avoid control protocols that change identifiers (like labels). MPLS-TP tunnels provide this functionality through statically provisioned bidirectional label switched paths (LSPs), as shown in the figure below.



## MPLS-TP Path Protection

MPLS-TP LSPs support 1-to-1 path protection. You can configure the working and protect LSPs as part of configuring the MPLS-TP tunnel. The working LSP is the primary LSP used to route traffic. The protect LSP is a backup for a working LSP. If the working LSP fails, traffic is switched to the protect LSP until the working LSP is restored, at which time forwarding reverts back to the working LSP.

## Bidirectional LSPs

MPLS-TP LSPs are bidirectional and co-routed and are comprised of two unidirectional LSPs that are supported by the MPLS forwarding infrastructure. A TP tunnel consists of a pair of unidirectional tunnels providing a bidirectional LSP. Each unidirectional tunnel can optionally be protected with a protect LSP that activates automatically upon failure conditions.

## MPLS-TP OAM Support

Several OAM protocols and messages support the provisioning and maintenance of MPLS-TP tunnels and bidirectional LSPs:

- **MPLS-TP OAM: GACH:** Generic Associated Channel (G-ACh) is the control channel mechanism associated with MPLS LSPs in addition to MPLS pseudowire. The G-ACh Label (GAL) (Label 13) is a generic alert label to identify the presence of the G-ACh in the label packet. It is taken from the reserved MPLS label space.

G-ACh/GAL is used to support in-band OAMs of MPLS LSPs and PWs. The OAM messages are used for fault management, connection verification, continuity check and other functions.

The following OAM messages are forwarded along the specified MPLS LSP:

- ◦ OAM Fault Management: AIS, LDI and LKR messages. (GAL with fault-OAM channel)
- ◦ OAM Connection Verification: ping and traceroute messages. (GAL with IP channel by default)
- ◦ OAM Continuity Check: BFD (non-IP BFD and IP BFD) messages. (GAL with BFD channel or IP channel depending on message format)

The following messages are forwarded along the specified PW:

- ◦ Static PW OAM messages (static PW status)
  - PW ping and traceroute messages
  - PW BFD messages
- MPLS-TP OAM: Fault Management: Link Down Indication (LDI), Alarm Indication Signal (AIS), and Lock Report (LKR) messages. LDI messages are generated at midpoint nodes when a failure is detected. At the midpoint, an LDI message will be sent to the endpoint that is reachable with the existing failure. Similarly, LKR messages will be sent from a midpoint node to the reachable endpoint when an interface is administratively shut. AIS messages are not generated by Cisco, but are processed if received. By default, reception of LDI and LKR on the active LSP at an endpoint will cause a path protection switchover, while AIS will not.
- MPLS-TP OAM: Fault Management: Emulated Protection Switching for LSP Lockout. Cisco implements a form of Emulated Protection Switching in support of LSP Lockout using customized Fault messages. When a Cisco Lockout message is sent, it does not cause the LSP to be administratively down. The Cisco Lockout message causes a path protection switchover and prevents data traffic from using the LSP. The LSP remains up so that BFD and other OAM messages can continue to traverse it. Maintenance of the LSP can take place (such as reconfiguring or replacing a midpoint LSR). The LSP is shown as UP and OAM can verify connectivity before the LSP is put back into service by removing the lockout. Lockout of the working LSP is not allowed if no protect LSP is configured. Alternatively, lockout of the protect LSP is allowed if no working LSP is configured.
- LSP ping and trace: For MPLS-TP connectivity verification, you can use **ping mpls tp** and **trace mpls tp** commands. You can specify that the echo requests be sent along either the working LSP, the protect LSP, or the active LSP. You can also specify that the echo request be sent on a locked out MPLS-TP tunnel LSP (either working or protect) if the working or protect LSP is explicitly specified.
- MPLS-TP OAM: Continuity Check via BFD: You can configure BFD sessions running over MPLS-TP LSPs. BFD sessions run on both the working LSP and the protect LSP. In order to perform a path protection switchover within 60 msec on an MPLS-TP endpoint, the BFD Hardware Offload feature enables the router hardware to construct and send BFD messages, which removes the task from the software path. You do not need to configure the BFD Hardware Offload feature. It works automatically on supported platforms. You must enable BFD.

## MPLS-TP Static and Dynamic Multisegment Pseudowires

MPLS-TP supports the following combinations of static and dynamic multisegment pseudowires:

- Static-static
- Static-dynamic
- Dynamic-static

## MPLS-TP L2VPN Pseudowire Redundancy for Static and Dynamic Multisegment Pseudowires

MPLS-TP supports one-to-one L2VPN pseudowire redundancy for the following combinations of static and dynamic pseudowires:

- Static pseudowire with a static backup pseudowire
- Static pseudowire with a dynamic backup pseudowire
- Dynamic pseudowire with a static backup pseudowire

## MPLS-TP OAM Status for Static and Dynamic Multisegment Pseudowires

With static pseudowires, status notifications can be provided by BFD over VCCV or static pseudowire OAM protocol. However, BFD over VCCV sends only attachment circuit status code notifications. Hop-by-hop notifications of other pseudowire status codes are not supported. Therefore, static pseudowire OAM protocol is preferred. You can acquire per pseudowire OAM for attachment circuit/pseudowire notification over VCCV channel with or without the control word.

## MPLS-TP Links and Physical Interfaces

MPLS-TP link numbers may be assigned to physical interfaces only. Bundled interfaces and virtual interfaces are not supported for MPLS-TP link numbers.

The MPLS-TP link is used to create a level of indirection between the MPLS-TP tunnel and midpoint LSP configuration and the physical interface. The **mpls tp link** command is used to associate an MPLS-TP link number with a physical interface and next-hop node. On point-to-point interfaces or Ethernet interfaces designated as point-to-point using the **medium p2p** command, the next-hop can be implicit, so the **mpls tp link** command just associates a link number to the interface.

Multiple tunnels and LSPs may then refer to the MPLS-TP link to indicate they are traversing that interface. You can move the MPLS-TP link from one interface to another without reconfiguring all the MPLS-TP tunnels and LSPs that refer to the link.

Link numbers must be unique on the router or node.

See [Configuring MPLS-TP Links and Physical Interfaces](#), page 19 for more information.

## Tunnel Midpoints

Tunnel LSPs, whether endpoint or midpoint, use the same identifying information. However, it is entered differently.

- At the midpoint, all the information for the LSP is specified with the **mpls tp lsp** command, which enters the submode for configuring forward and reverse information for forwarding.
- At the midpoint, determining which end is source and which is destination is arbitrary. That is, if you are configuring a tunnel between your router and a coworker's router, then your router is the source. However, your coworker considers his or her router to be the source. At the midpoint, either router could be considered the source. At the midpoint, the forward direction is from source to destination, and the reverse direction is from destination to source.
- At the endpoint, the local information (source) either comes from the global router ID and global ID, or from locally configured information using the **tp source** command after you enter the command **interface tunnel-tp number** command, where *number* is the local/source tunnel-number.
- At the endpoint, the remote information (destination) is configured using the **tp destination** command after you enter the command **interface tunnel-tp number**. The **tp destination** command includes the destination node ID, optionally the global ID, and optionally the destination tunnel number. If you do not specify the destination tunnel number, the source tunnel number is used.
- At the endpoint, the LSP number is configured in working-lsp or protect-lsp submode. The default is 0 for the working LSP and 1 for the protect LSP.

- When configuring the LSPs at the midpoint routers, make that the configuration does not reflect traffic back to the originating node.

## How to Configure MPLS-TP

- [Configuring the MPLS Label Range, page 6](#)
- [Configuring the Router ID and Global ID, page 7](#)
- [Configuring Bidirectional Forwarding Detection Templates, page 8](#)
- [Configuring Pseudowire OAM Attributes, page 9](#)
- [Configuring the Pseudowire Class, page 10](#)
- [Configuring the Pseudowire, page 12](#)
- [Configuring the MPLS-TP Tunnel, page 13](#)
- [Configuring MPLS-TP LSPs at Midpoints, page 17](#)
- [Configuring MPLS-TP Links and Physical Interfaces, page 19](#)
- [Configuring Static-to-Static Multisegment Pseudowires for MPLS-TP, page 21](#)
- [Configuring a Template with Pseudowire Type-Length-Value Parameters, page 23](#)
- [Configuring Static-to-Dynamic Multisegment Pseudowires for MPLS-TP, page 23](#)
- [Configuring the L2VPN Pseudowire Redundancy for Static Multisegment Pseudowires, page 27](#)
- [Verifying the MPLS-TP Configuration, page 30](#)

## Configuring the MPLS Label Range

You must specify a static range of MPLS labels using the **mpls label range** command with the **static** keyword.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls label range** *minimum-value maximum-value* {**static** *minimum-static-value maximum-static-value*}

### DETAILED STEPS

Command or Action	Purpose
<p><b>Step 1</b> <b>enable</b></p> <p><b>Example:</b></p> <pre>Router&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<p><b>Step 2</b> <b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>

Command or Action	Purpose
<p><b>Step 3</b> <code>mpls label range</code> <i>minimum-value maximum-value</i> {<code>static</code> <i>minimum-static-value maximum-static-value</i>}</p> <p><b>Example:</b></p> <pre>Router(config)# mpls label range 1001 1003 static 10000 25000</pre>	Specifies a static range of MPLS labels

## Configuring the Router ID and Global ID

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `mpls tp`
4. `router-id` *node-id*
5. `global-id` *num*

### DETAILED STEPS

Command or Action	Purpose
<p><b>Step 1</b> <code>enable</code></p> <p><b>Example:</b></p> <pre>Router&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<p><b>Step 2</b> <code>configure terminal</code></p> <p><b>Example:</b></p> <pre>Router# configure terminal</pre>	Enters global configuration mode.
<p><b>Step 3</b> <code>mpls tp</code></p> <p><b>Example:</b></p> <pre>Router(config)# mpls tp</pre>	Enters MPLS-TP configuration mode, from which you can configure MPLS-TP parameters for the router.

Command or Action	Purpose
<b>Step 4</b> <code>router-id node-id</code>  <b>Example:</b>  <pre>Router(config-mpls-tp)# router-id 10.10.10.10</pre>	Specifies the default MPLS-TP router ID, which is used as the default source node ID for all MPLS-TP tunnels configured on the router.
<b>Step 5</b> <code>global-id num</code>  <b>Example:</b>  <pre>Router(config-mpls-tp)# global-id 1</pre>	<p>(Optional) Specifies the default global ID used for all endpoints and midpoints. This command makes the router ID globally unique in a multiprovider tunnel. Otherwise, the router ID is only locally meaningful. The global ID is an autonomous system number, which is a controlled number space by which providers can identify each other.</p> <p>The router ID and global ID are also included in fault messages by routers at tunnel midpoints to help isolate the location of faults.</p>

## Configuring Bidirectional Forwarding Detection Templates

The **bfd-template** command allows you to create a BFD template and enter BFD configuration mode. The template can be used to specify a set of BFD interval values. You invoke the template as part of the MPLS-TP tunnel. On platforms that support the BFD Hardware Offload feature and can provide 60-ms cutover for MPLS-TP tunnels, it is recommended to use the higher resolution timers in the BFD template.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bfd-template single-hop *template-name***
4. **interval [microseconds] {both *time*| min-tx *time* min-rx *time*} [**multiplier** *multiplier-value*]**

### DETAILED STEPS

Command or Action	Purpose
<b>Step 1</b> <code>enable</code>  <b>Example:</b>  <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b> <code>configure terminal</code>  <b>Example:</b>  <pre>Router# configure terminal</pre>	Enters global configuration mode.

Command or Action	Purpose
<b>Step 3</b> <code>bfd-template single-hop <i>template-name</i></code>  <b>Example:</b> <pre>Router(config)# bfd-template single-hop mpls-bfd-1</pre>	Creates a BFD template and enter BFD configuration mode.
<b>Step 4</b> <code>interval [microseconds] {both <i>time</i> min-tx <i>time</i> min-rx <i>time</i>} [<i>multiplier multiplier-value</i>]</code>  <b>Example:</b> <pre>Router(config-bfd)# interval min-tx 99 min-rx 99 multiplier 3</pre>	Specifies a set of BFD interval values.

## Configuring Pseudowire OAM Attributes

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `pseudowire-static-oam class class-name`
4. `timeout refresh send seconds`

### DETAILED STEPS

Command or Action	Purpose
<b>Step 1</b> <code>enable</code>  <b>Example:</b> <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b> <code>configure terminal</code>  <b>Example:</b> <pre>Router# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b> <code>pseudowire-static-oam class <i>class-name</i></code>  <b>Example:</b> <pre>Router(config)# pseudowire-static-oam class oam-class1</pre>	Creates a pseudowire OAM class and enters pseudowire OAM class configuration mode.

Command or Action	Purpose
<b>Step 4</b> <code>timeout refresh send <i>seconds</i></code>  <b>Example:</b>  <pre>Router(config-st-pw-oam-class)# timeout refresh send 20</pre>	Specifies the OAM timeout refresh intervals.

## Configuring the Pseudowire Class

When you create the pseudowire class, you specify the parameters of the pseudowire, such as the use of the control word, preferred path, OAM class, and VCCV BFD template.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `pseudowire-class class-name`
4. `encapsulation mpls`
5. `control-word`
6. `protocol {l2tpv2 | l2tpv3 | none} [l2tp-class-name]`
7. `preferred-path {interface tunnel tunnel-number | peer {ip-address | host-name}} [disable-fallback]`
8. `status protocol notification static class-name`
9. `vccv bfd template name [udp | raw-bfd]`

### DETAILED STEPS

Command or Action	Purpose
<b>Step 1</b> <code>enable</code>  <b>Example:</b>  <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b> <code>configure terminal</code>  <b>Example:</b>  <pre>Router# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b> <code>pseudowire-class <i>class-name</i></code>  <b>Example:</b>  <pre>Router(config)# pseudowire-class mpls-tp-class1</pre>	Creates a pseudowire class and enters pseudowire class configuration mode.



Command or Action	Purpose
<p><b>Step 4</b> <b>encapsulation mpls</b></p> <p><b>Example:</b></p> <pre>Router(config-pw-class)# encapsulation mpls</pre>	Specifies the encapsulation type.
<p><b>Step 5</b> <b>control-word</b></p> <p><b>Example:</b></p> <pre>Router(config-pw-class)# control-word</pre>	Enables the use of the control word.
<p><b>Step 6</b> <b>protocol {l2tpv2   l2tpv3   none} [l2tp-class-name]</b></p> <p><b>Example:</b></p> <pre>Router(config-pw-class)# protocol none</pre>	Specifies the type of protocol.
<p><b>Step 7</b> <b>preferred-path {interface tunnel tunnel-number   peer {ip-address   host-name}} [disable-fallback]</b></p> <p><b>Example:</b></p> <pre>Router(config-pw-class)# preferred-path interface tunnel-tp2</pre>	Specifies the tunnel to use as the preferred path.
<p><b>Step 8</b> <b>status protocol notification static class-name</b></p> <p><b>Example:</b></p> <pre>Router(config-pw-class)# status protocol notification static oam-class1</pre>	Specifies the OAM class to use.
<p><b>Step 9</b> <b>vccv bfd template name [udp   raw-bfd]</b></p> <p><b>Example:</b></p> <pre>Router(config-pw-class)# vccv bfd template bfd-templ raw-bfd</pre>	Specifies the VCCV BFD template to use.

## Configuring the Pseudowire

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **xconnect** *peer-ip-address vc-id* {**encapsulation** {**l2tpv3** [**manual**] | **mpls** [**manual**]} | **pw-class** *pw-class-name*} [**pw-class** *pw-class-name*] [**sequencing** {**transmit** | **receive** | **both**}]
5. **mpls label** *local-pseudowire-label remote-pseudowire-label*
6. **mpls control-word**
7. **backup delay** {*enable-delay-period* | **never**} {*disable-delay-period* | **never**}
8. **backup peer** *peer-router-ip-addr vcid* [**pw-class** *pw-class-name*] [**priority** *value*]

### DETAILED STEPS

Command or Action	Purpose
<b>Step 1</b> <b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b> <b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b> <b>interface</b> <i>type number</i>  <b>Example:</b> Router(config)# interface Ethernet 1/0	Specifies the interface and enters interface configuration mode.
<b>Step 4</b> <b>xconnect</b> <i>peer-ip-address vc-id</i> { <b>encapsulation</b> { <b>l2tpv3</b> [ <b>manual</b> ]   <b>mpls</b> [ <b>manual</b> ]}   <b>pw-class</b> <i>pw-class-name</i> } [ <b>pw-class</b> <i>pw-class-name</i> ] [ <b>sequencing</b> { <b>transmit</b>   <b>receive</b>   <b>both</b> }]  <b>Example:</b> Router(config-if)# xconnect 10.131.191.251 100 encapsulation mpls manual pw-class mpls-tp-class1	Binds the attachment circuit to a pseudowire VC and enters xconnect interface configuration mode.

Command or Action	Purpose
<p><b>Step 5</b> <code>mpls label local-pseudowire-label remote-pseudowire-label</code></p> <p><b>Example:</b></p> <pre>Router(config-if-xconn)# mpls label 100 150</pre>	<p>Configures the static pseudowire connection by defining local and remote circuit labels.</p>
<p><b>Step 6</b> <code>mpls control-word</code></p> <p><b>Example:</b></p> <pre>Router(config-if-xconn)# no mpls control-word</pre>	<p>Specifies the control word.</p>
<p><b>Step 7</b> <code>backup delay {enable-delay-period   never} {disable-delay-period   never}</code></p> <p><b>Example:</b></p> <pre>Router(config-if-xconn)# backup delay 0 never</pre>	<p>Specifies how long a backup pseudowire virtual circuit (VC) should wait before resuming operation after the primary pseudowire VC goes down.</p>
<p><b>Step 8</b> <code>backup peer peer-router-ip-addr vcid [pw-class pw-class-name] [priority value]</code></p> <p><b>Example:</b></p> <pre>Router(config-if-xconn)# backup peer 10.0.0.2 50</pre>	<p>Specifies a redundant peer for a pseudowire virtual circuit (VC).</p>

## Configuring the MPLS-TP Tunnel

On the endpoint routers, create an MPLS TP tunnel and configure its parameters. See the `interface tunnel-tp` command for information on the parameters.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **interface tunnel-tp** *number*
4. **description** *tunnel-description*
5. **tp tunnel-name** *name*
6. **tp bandwidth** *num*
7. **tp source** *node-id* [*global-id num*]
8. **tp destination** *node-id* [[**tunnel-tp** *num*] **global-id** *num*]
9. **bfd** *bfd-template*
10. **working-lsp**
11. **in-label** *num*
12. **out-label** *num out-link num*
13. **exit**
14. **protect-lsp**
15. **in-label** *num*
16. **out-label** *num out-link num*
17. **exit**

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>interface tunnel-tp</b> <i>number</i>  <b>Example:</b> Router(config)# <b>interface tunnel-tp</b> 2	Enters tunnel interface configuration mode. Tunnel numbers from 0 to 999 are supported.

	Command or Action	Purpose
Step 4	<p><b>description</b> <i>tunnel-description</i></p> <p><b>Example:</b></p> <pre>Router(config-if)# <b>description</b> headend tunnel</pre>	(Optional) Specifies a tunnel description.
Step 5	<p><b>tp tunnel-name</b> <i>name</i></p> <p><b>Example:</b></p> <pre>Router(config-if)# <b>tp tunnel-name</b> tunnel22</pre>	Specifies the name of the MPLS-TP tunnel. The TP tunnel name is displayed in the <b>show mpls tp tunnel</b> command output. This command is useful for consistently identifying the tunnel at all endpoints and midpoints.
Step 6	<p><b>tp bandwidth</b> <i>num</i></p> <p><b>Example:</b></p> <pre>Router(config-if)# <b>tp bandwidth</b> 10000</pre>	Specifies the tunnel bandwidth.
Step 7	<p><b>tp source</b> <i>node-id</i> [<i>global-id num</i>]</p> <p><b>Example:</b></p> <pre>Router(config-if)# <b>tp source</b> 10.10.11.11 <b>global-id</b> 10</pre>	(Optional) Specifies the tunnel source and endpoint. This command is and not typically used, because the global router ID and global ID can be used to identify the tunnel source at the endpoint. All tunnels on the router generally use the same (globally specified) source information.
Step 8	<p><b>tp destination</b> <i>node-id</i> [[<b>tunnel-tp</b> <i>num</i>] <b>global-id</b> <i>num</i>]</p> <p><b>Example:</b></p> <pre>Router(config-if)# <b>tp destination</b> 10.10.10.10</pre>	Specifies the destination node of the tunnel.
Step 9	<p><b>bfd</b> <i>bfd-template</i></p> <p><b>Example:</b></p> <pre>Router(config-if)# <b>bfd</b> mpls-tp-bfd-2</pre>	Specifies the BFD template.
Step 10	<p><b>working-lsp</b></p> <p><b>Example:</b></p> <pre>Router(config-if)# <b>working-lsp</b></pre>	Specifies a working LSP, also known as the primary LSP. This LSP is used to route traffic. This command enters working LSP interface configuration mode (config-if-working).

Command or Action	Purpose
<p><b>Step 11</b> <code>in-label num</code></p> <p><b>Example:</b></p> <pre>Router(config-if-working)# in-label 111</pre>	Specifies the in label.
<p><b>Step 12</b> <code>out-label num out-link num</code></p> <p><b>Example:</b></p> <pre>Router(config-if-working)# out-label 112 out-link 1</pre>	Specifies the out label and out link.
<p><b>Step 13</b> <code>exit</code></p> <p><b>Example:</b></p> <pre>Router(config-if-working)# exit</pre>	Exits from working LSP interface configuration mode.
<p><b>Step 14</b> <code>protect-lsp</code></p> <p><b>Example:</b></p> <pre>Router(config-if)# protect-lsp</pre>	Specifies a backup for a working LSP. If the working LSP fails, traffic is switched to the protect LSP until the working LSP is restored, at which time forwarding reverts back to the working LSP. This command enters protect LSP interface configuration mode (config-if-protect).
<p><b>Step 15</b> <code>in-label num</code></p> <p><b>Example:</b></p> <pre>Router(config-if-protect)# in-label 100</pre>	Specifies the in label.
<p><b>Step 16</b> <code>out-label num out-link num</code></p> <p><b>Example:</b></p> <pre>Router(config-if-protect)# out-label 113 out-link 2</pre>	Specifies the out label and out link.
<p><b>Step 17</b> <code>exit</code></p> <p><b>Example:</b></p> <pre>Router(config-if-protect)# exit</pre>	Exits from protect LSP interface configuration mode.

# Configuring MPLS-TP LSPs at Midpoints



**Note**

When configuring the LSPs at the midpoint routers, make that the configuration does not reflect traffic back to the originating node.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls tp lsp source** *node-id* [**global-id** *num*] **tunnel-tp** *num* **lsp**{*lsp-num* | **protect** | **working**} **destination** *node-id* [**global-id** *num*] **tunnel-tp** *num*
4. **forward-lsp**
5. **bandwidth** *num*
6. **in-label** *num* **out-label** *num* **out-link** *num*
7. **exit**
8. **reverse-lsp**
9. **bandwidth** *num*
10. **in-label** *num* **out-label** *num* **out-link** *num*

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b></p> <pre>Router&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
Step 3	<p><b>mpls tp lsp source</b> <i>node-id</i> [<b>global-id</b> <i>num</i>] <b>tunnel-tp</b> <i>num</i> <b>lsp</b>{<i>lsp-num</i>   <b>protect</b>   <b>working</b>} <b>destination</b> <i>node-id</i> [<b>global-id</b> <i>num</i>] <b>tunnel-tp</b> <i>num</i></p> <p><b>Example:</b></p> <pre>Router(config)# mpls tp lsp source 10.10.10.10 global-id 2 tunnel-tp 4 lsp protect destination 10.11.11.11 global-id 11 tunnel-tp 12</pre>	<p>Enables MPLS-TP midpoint connectivity and enters MPLS TP LSP configuration mode.</p>

Command or Action	Purpose
<p><b>Step 4</b> <code>forward-lsp</code></p> <p><b>Example:</b></p> <pre>Router(config-mpls-tp-lsp)# forward-lsp</pre>	<p>Enters MPLS-TP LSP forward LSP configuration mode.</p>
<p><b>Step 5</b> <code>bandwidth num</code></p> <p><b>Example:</b></p> <pre>Router(config-mpls-tp-lsp-forw)# bandwidth 100</pre>	<p>Specifies the bandwidth.</p>
<p><b>Step 6</b> <code>in-label num out-label num out-link num</code></p> <p><b>Example:</b></p> <pre>Router(config-mpls-tp-lsp-forw)# in-label 53 out-label 43 out-link 41</pre>	<p>Specifies the in label, out label, and out link numbers.</p>
<p><b>Step 7</b> <code>exit</code></p> <p><b>Example:</b></p> <pre>Router(config-mpls-tp-lsp-forw)# exit</pre>	<p>Exits MPLS-TP LSP forward LSP configuration mode.</p>
<p><b>Step 8</b> <code>reverse-lsp</code></p> <p><b>Example:</b></p> <pre>Router(config-mpls-tp-lsp)# reverse-lsp</pre>	<p>Enters MPLS-TP LSP reverse LSP configuration mode.</p>
<p><b>Step 9</b> <code>bandwidth num</code></p> <p><b>Example:</b></p> <pre>Router(config-mpls-tp-lsp-rev)# bandwidth 100</pre>	<p>Specifies the bandwidth.</p>
<p><b>Step 10</b> <code>in-label num out-label num out-link num</code></p> <p><b>Example:</b></p> <pre>Router(config-mpls-tp-lsp-rev)# in-label 33 out-label 23 out-link 44</pre>	<p>Specifies the in label, out label, and out link numbers.</p>



## Configuring MPLS-TP Links and Physical Interfaces

MPLS-TP link numbers may be assigned to physical interfaces only. Bundled interfaces and virtual interfaces are not supported for MPLS-TP link numbers.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type/num*
4. **ip address** *ip-address mask*
5. **mpls tp link** *link-num* {**ipv4** *ip-address* / **tx-mac** *mac-address*} **rx-mac** *mac-address*
6. **ip rsvp bandwidth** [**rdm** [**bc0** *interface-bandwidth*] [[*single-flow-bandwidth* [**bc1** *bandwidth* | **sub-pool** *bandwidth*]]] [*interface-bandwidth* [*single-flow-bandwidth* [**bc1** *bandwidth* | **sub-pool** *bandwidth*]] | **mam max-reservable-bw** [*interface-bandwidth* [*single-flow-bandwidth*] [**bc0** *interface-bandwidth* [**bc1** *bandwidth*]]] | **percent** *percent-bandwidth* [*single-flow-bandwidth*]]]
7. **exit**
8. **exit**
9. **show mpls tp link-numbers**

### DETAILED STEPS

Command or Action	Purpose
<b>Step 1</b> <b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b> <b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b> <b>interface</b> <i>type/num</i>  <b>Example:</b> Router(config)# interface ethernet 1/0	Specifies the interface and enters interface configuration mode.

Command or Action	Purpose
<p><b>Step 4</b> <code>ip address ip-address mask</code></p> <p><b>Example:</b></p> <pre>Router(config-if)# ip address 10.10.10.10 255.255.255.0</pre>	<p>Assigns an IP address to the interface.</p>
<p><b>Step 5</b> <code>mpls tp link link-num {ipv4 ip-address / tx-mac mac-address} rx-mac mac-address</code></p> <p><b>Example:</b></p> <pre>Router(config-if)# mpls tp link 1 ipv4 10.0.0.2</pre>	<p>Associates an MPLS-TP link number with a physical interface and next-hop node. On point-to-point interfaces or Ethernet interfaces designated as point-to-point using the <b>medium p2p</b> command, the next-hop can be implicit, so the <b>mpls tp link</b> command just associates a link number to the interface.</p> <p>Multiple tunnels and LSPs can refer to the MPLS-TP link to indicate they are traversing that interface. You can move the MPLS-TP link from one interface to another without reconfiguring all the MPLS-TP tunnels and LSPs that refer to the link.</p> <p>Link numbers must be unique on the router or node.</p>
<p><b>Step 6</b> <code>ip rsvp bandwidth [rdm [bc0 interface-bandwidth] [[single-flow-bandwidth [bc1 bandwidth   sub-pool bandwidth]]] [interface-bandwidth [single-flow-bandwidth [bc1 bandwidth   sub-pool bandwidth]]]   mam max-reservable-bw [interface-bandwidth [single-flow-bandwidth] [bc0 interface-bandwidth [bc1 bandwidth]]]   percent percent-bandwidth [single-flow-bandwidth]]</code></p> <p><b>Example:</b></p> <pre>Router(config-if)# ip rsvp bandwidth 1158 100</pre>	<p>Enables Resource Reservation Protocol (RSVP) bandwidth for IP on an interface.</p> <p>For the Cisco 7600 platform, if you configure non-zero bandwidth for the TP tunnel or at a midpoint LSP, make sure that the interface to which the output link is attached has enough bandwidth available. For example, if three tunnel LSPs run over link 1 and each LSP was assigned 1000 with the <b>tp bandwidth</b> command, the interface associated with link 1 needs bandwidth of 3000 with the <b>ip rsvp bandwidth</b> command.</p>
<p><b>Step 7</b> <code>exit</code></p> <p><b>Example:</b></p> <pre>Router(config-if)# exit</pre>	<p>Exits interface configuration mode.</p>
<p><b>Step 8</b> <code>exit</code></p> <p><b>Example:</b></p> <pre>Router(config)# exit</pre>	<p>Exits global configuration mode.</p>

Command or Action	Purpose
<b>Step 9</b> <code>show mpls tp link-numbers</code>  <b>Example:</b>  Router# <code>show mpls tp link-numbers</code>	Displays the configured links.

## Configuring Static-to-Static Multisegment Pseudowires for MPLS-TP

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `l2 vfi name point-to-point`
4. `neighbor ip-address vc-id {encapsulation mpls | pw-class pw-class-name}`
5. `mpls label local-pseudowire-label remote-pseudowire-label`
6. `mpls control-word`
7. `neighbor ip-address vc-id {encapsulation mpls | pw-class pw-class-name}`
8. `mpls label local-pseudowire-label remote-pseudowire-label`
9. `mpls control-word`

### DETAILED STEPS

Command or Action	Purpose
<b>Step 1</b> <code>enable</code>  <b>Example:</b>  Router> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b> <code>configure terminal</code>  <b>Example:</b>  Router# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 3</b> <code>l2 vfi name point-to-point</code>  <b>Example:</b>  Router(config)# <code>l2 vfi atom point-to-point</code>	Creates a point-to-point Layer 2 virtual forwarding interface (VFI) and enters VFI configuration mode.

Command or Action	Purpose
<p><b>Step 4</b> <code>neighbor ip-address vc-id {encapsulation mpls   pw-class pw-class-name}</code></p> <p><b>Example:</b></p> <pre>Router(config-vfi)# neighbor 10.111.111.111 123 pw-class atom</pre>	<p>Sets up an emulated VC. Specify the IP address and the VC ID of the remote router. Also specify the pseudowire class to use for the emulated VC.</p> <p>Note: Only two <b>neighbor</b> commands are allowed for each I2 vfi point-to-point command.</p>
<p><b>Step 5</b> <code>mpls label local-pseudowire-label remote-pseudowire-label</code></p> <p><b>Example:</b></p> <pre>Router(config-vfi)# mpls label 101 201</pre>	<p>Configures the static pseudowire connection by defining local and remote circuit labels.</p>
<p><b>Step 6</b> <code>mpls control-word</code></p> <p><b>Example:</b></p> <pre>Router(config-vfi)# mpls control-word</pre>	<p>Specifies the control word.</p>
<p><b>Step 7</b> <code>neighbor ip-address vc-id {encapsulation mpls   pw-class pw-class-name}</code></p> <p><b>Example:</b></p> <pre>Router(config-vfi)#</pre>	<p>Sets up an emulated VC. Specify the IP address and the VC ID of the remote router. Also specify the pseudowire class to use for the emulated VC.</p>
<p><b>Step 8</b> <code>mpls label local-pseudowire-label remote-pseudowire-label</code></p> <p><b>Example:</b></p> <pre>Router(config-vfi)# Router(config-vfi)# mpls label 102 202</pre>	<p>Configures the static pseudowire connection by defining local and remote circuit labels.</p>
<p><b>Step 9</b> <code>mpls control-word</code></p> <p><b>Example:</b></p> <pre>Router(config-vfi)# mpls control-word</pre>	<p>Specifies the control word.</p>

## Configuring a Template with Pseudowire Type-Length-Value Parameters

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pseudowire-tlv template *template-name***
4. **tlv [*type-name*] *type-value length* [**dec** | **hexstr** | **str**] *value***

### DETAILED STEPS

Command or Action	Purpose
<b>Step 1</b> <b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b> <b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b> <b>pseudowire-tlv template <i>template-name</i></b>  <b>Example:</b> Router(config)# pseudowire-tlv template statictemp	Creates a template of pseudowire type-length-value (TLV) parameters
<b>Step 4</b> <b>tlv [<i>type-name</i>] <i>type-value length</i> [<b>dec</b>   <b>hexstr</b>   <b>str</b>] <i>value</i></b>  <b>Example:</b> Router(config-pw-tlv-template)# tlv statictemp 2 4 hexstr 1	Specifies the TLV parameters.

## Configuring Static-to-Dynamic Multisegment Pseudowires for MPLS-TP

When you configure static-to-dynamic pseudowires, you configure the static pseudowire class with the **protocol none** command, create a dynamic pseudowire class, then invoke those pseudowire classes with the **neighbor** commands.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **pseudowire-class** *class-name*
4. **encapsulation mpls**
5. **control-word**
6. **protocol** {l2tpv2 | l2tpv3 | none} [*l2tp-class-name*]
7. **exit**
8. **pseudowire-class** *class-name*
9. **encapsulation mpls**
10. **exit**
11. **l2 vfi** *name* **point-to-point**
12. **neighbor** *ip-address* *vc-id* {**encapsulation mpls** | **pw-class** *pw-class-name*}
13. **neighbor** *ip-address* *vc-id* {**encapsulation mpls** | **pw-class** *pw-class-name*}
14. **mpls label** *local-pseudowire-label* *remote-pseudowire-label*
15. **mpls control-word**
16. **local interface** *pseudowire-type*
17. Do one of the following:
  - **tlv** [*type-name*] *type-value* *length* [**dec** | **hexstr** | **str**] *value*
  - 
  - **tlv template** *template-name*

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>pseudowire-class</b> <i>class-name</i>  <b>Example:</b> Router(config)# pseudowire-class mpls-tp-class1	Creates a pseudowire class and enters pseudowire class configuration mode.

	Command or Action	Purpose
Step 4	<p><b>encapsulation mpls</b></p> <p><b>Example:</b></p> <pre>Router(config-pw-class)# encapsulation mpls</pre>	Specifies the encapsulation type.
Step 5	<p><b>control-word</b></p> <p><b>Example:</b></p> <pre>Router(config-pw-class)# control-word</pre>	Enables the use of the control word.
Step 6	<p><b>protocol {l2tpv2   l2tpv3   none} [l2tp-class-name]</b></p> <p><b>Example:</b></p> <pre>Router(config-pw-class)# protocol none</pre>	Specifies the type of protocol. Use the <b>protocol none</b> command to specify a static pseudowire.
Step 7	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>Router(config-pw-class)# exit</pre>	Exits pseudowire class configuration mode.
Step 8	<p><b>pseudowire-class class-name</b></p> <p><b>Example:</b></p> <pre>Router(config)# pseudowire-class mpls-tp-class1</pre>	Creates a pseudowire class and enters pseudowire class configuration mode.
Step 9	<p><b>encapsulation mpls</b></p> <p><b>Example:</b></p> <pre>Router(config-pw-class)# encapsulation mpls</pre>	Specifies the encapsulation type.
Step 10	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>Router(config-pw-class)# exit</pre>	Exits pseudowire class configuration mode.

Command or Action	Purpose
<p><b>Step 11</b> <code>l2 vfi name point-to-point</code></p> <p><b>Example:</b></p> <pre>Router(config)# l2 vfi atom point-to-point</pre>	<p>Creates a point-to-point Layer 2 virtual forwarding interface (VFI) and enters VFI configuration mode.</p>
<p><b>Step 12</b> <code>neighbor ip-address vc-id {encapsulation mpls   pw-class pw-class-name}</code></p> <p><b>Example:</b></p> <pre>Router(config-vfi)# neighbor 10.111.111.111 123 pw-class atom</pre>	<p>Sets up an emulated VC. Specify the IP address and the VC ID of the remote router. Also specify the pseudowire class to use for the emulated VC. Enters config-vfi-neighbor command mode.</p> <p>Note: Only two <b>neighbor</b> commands are allowed for each l2 vfi point-to-point command.</p>
<p><b>Step 13</b> <code>neighbor ip-address vc-id {encapsulation mpls   pw-class pw-class-name}</code></p> <p><b>Example:</b></p> <pre>Router(config-vfi-neighbor)# neighbor 10.111.111.111 123 pw-class atom</pre>	<p>Sets up an emulated VC. Specify the IP address and the VC ID of the remote router. Also specify the pseudowire class to use for the emulated VC.</p> <p>Note: Only two <b>neighbor</b> commands are allowed for each l2 vfi point-to-point command.</p>
<p><b>Step 14</b> <code>mpls label local-pseudowire-label remote-pseudowire-label</code></p> <p><b>Example:</b></p> <pre>Router(config-vfi-neighbor)# mpls label 101 201</pre>	<p>Configures the static pseudowire connection by defining local and remote circuit labels.</p>
<p><b>Step 15</b> <code>mpls control-word</code></p> <p><b>Example:</b></p> <pre>Router(config-vfi-neighbor)# mpls control-word</pre>	<p>Specifies the control word.</p>
<p><b>Step 16</b> <code>local interface pseudowire-type</code></p> <p><b>Example:</b></p> <pre>Router(config-vfi-neighbor)# local interface 4</pre>	<p>Specifies the pseudowire type and enters VFI neighbor interface configuration mode.</p>



Command or Action	Purpose
<p><b>Step 17</b> Do one of the following:</p> <ul style="list-style-type: none"> <li>• <code>tlv [type-name] type-value length [dec   hexstr   str] value</code></li> <li>• <code>tlv template template-name</code></li> </ul> <p><b>Example:</b></p> <pre>Router(config-vfi-neighbor)# tlv statictemp 2 4 hexstr 1</pre>	Specifies the TLV parameters or invokes a previously configured TLV template.

- [Example, page 27](#)

## Example

```
12 vfi atom point-to-point (static-dynamic MSPW)
neighbor 10.116.116.116 4294967295 pw-class dypw (dynamic)
neighbor 10.111.111.111 123 pw-class stpw (static)
mpls label 101 201
mpls control-word
local interface 4
tlv mtu 1 4 1500
tlv description 3 6 str abcd
tlv descr C 4 hexstr 0505
```

## Configuring the L2VPN Pseudowire Redundancy for Static Multisegment Pseudowires

Perform the following steps to configure the L2VPN pseudowire redundancy for static multisegment pseudowires that are backed up with static or dynamic multisegment pseudowires.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface ethernet** *type/num*
4. **service instance** *id ethernet*
5. **encapsulation dot1q** *vlan-id*
6. **xconnect** *peer-ip-address vc-id* { **encapsulation** { **l2tpv3** [ **manual** ] | **mpls** [ **manual** ] } | **pw-class** *pw-class-name* } [ **pw-class** *pw-class-name* ] [ **sequencing** { **transmit** | **receive** | **both** } ]
7. **mpls label** *local-pseudowire-label remote-pseudowire-label*
8. **mpls control-word**
9. **backup delay** { *enable-delay-period* | **never** } { *disable-delay-period* | **never** }
10. **backup peer** *peer-router-ip-addr vcid* [ **pw-class** *pw-class-name* ] [ **priority** *value* ]
11. **mpls label** *local-pseudowire-label remote-pseudowire-label*
12. **mpls control-word**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b></p> <pre>Router&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
Step 3	<p><b>interface ethernet <i>type/num</i></b></p> <p><b>Example:</b></p> <pre>Router(config)# interface ethernet 1/0</pre>	<p>Specifies the interfaces and enters interface configuration mode.</p>
Step 4	<p><b>service instance <i>id</i> ethernet</b></p> <p><b>Example:</b></p> <pre>Router(config-if)# service instance 1 ethernet</pre>	<p>Specifies the service instance and enters service instance interface configuration mode.</p>
Step 5	<p><b>encapsulation dot1q <i>vlan-id</i></b></p> <p><b>Example:</b></p> <pre>Router(config-if-srv)# encapsulation dot1q 10</pre>	<p>Enables the interface to accept 802.1Q VLAN packets.</p>
Step 6	<p><b>xconnect <i>peer-ip-address</i> <i>vc-id</i> {encapsulation {12tpv3 [manual]   mpls [manual]}   pw-class <i>pw-class-name</i>} [pw-class <i>pw-class-name</i>] [sequencing {transmit   receive   both}]</b></p> <p><b>Example:</b></p> <pre>Router(config-if-srv)# xconnect 10.109.10.10 123encapsulation mpls manual pw-class stpw</pre>	<p>Binds the attachment circuit to a pseudowire VC and enters xconnect configuration mode.</p>
Step 7	<p><b>mpls label <i>local-pseudowire-label</i> <i>remote-pseudowire-label</i></b></p> <p><b>Example:</b></p> <pre>Router(cfg-if-ether-vc-xconn)# mpls label 100 150</pre>	<p>Configures the static pseudowire connection by defining local and remote circuit labels.</p>

	Command or Action	Purpose
Step 8	<b>mpls control-word</b>  <b>Example:</b> Router(cfg-if-ether-vc-xconn)# no mpls control-word	Specifies the control word.
Step 9	<b>backup delay</b> { <i>enable-delay-period</i>   <b>never</b> } { <i>disable-delay-period</i>   <b>never</b> }  <b>Example:</b> Router(cfg-if-ether-vc-xconn)# backup delay 0 never	Specifies how long a backup pseudowire virtual circuit (VC) should wait before resuming operation after the primary pseudowire VC goes down.
Step 10	<b>backup peer</b> <i>peer-router-ip-addr</i> <i>vcid</i> [ <b>pw-class</b> <i>pw-class-name</i> ] [ <i>priority value</i> ]  <b>Example:</b> Router(cfg-if-ether-vc-xconn)# backup peer 10.0.0.2 50	Specifies a redundant peer for a pseudowire virtual circuit (VC). Enters backup xconnect configuration mode.
Step 11	<b>mpls label</b> <i>local-pseudowire-label</i> <i>remote-pseudowire-label</i>  <b>Example:</b> Router(cfg-if-ether-vc-xconn-bkup)# mpls label 100 150	Configures the static pseudowire connection by defining local and remote circuit labels.
Step 12	<b>mpls control-word</b>  <b>Example:</b> Router(cfg-if-ether-vc-xconn-bkup)# no mpls control-word	Specifies the control word.

- [Example, page 29](#)

## Example

```
interface Ethernet1/0
  no ip address
  no shutdown
  service instance 1 ethernet
  encapsulation dot1q 10
  xconnect 10.113.113.113 123 encapsulation mpls manual pw-class stpw
  mpls label 0 101
  mpls control-word
  backup peer 1 0.120.120.120 124 pw-class stpw
  mpls label 0 105
  mpls control-word
```

## Verifying the MPLS-TP Configuration

When the entire tunnel is programmed, use the following commands to verify and help troubleshoot the configuration:

- **show mpls tp tunnel-tp lsps:** To ensure that both LSPs are up and working from a tunnel endpoint.
- **show mpls tp tunnel-tp *number* detail :** To help determine the cause if the tunnel is not up and working.
- **show bfd neighbors mpls-tp:** To display the state of BFD, which must be up for the endpoint LSPs to be up.
- **trace mpls tp** and **ping mpls tp:** To help isolate any connectivity issues.
- **debug mpls tp :** To enable the display of MPLS-TP error messages.
- **logging (MPLS-TP):** To enable the display of logging messages related to configuration changes or state changes.
- **show mpls l2transport static-oam:** To enable the display of MPLS-TP messages related to pseudowires.

## Additional References

### Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="#">Cisco IOS Master Commands List, All Releases</a>
MPLS commands	Cisco IOS MPLS Command Reference

### Standards

Standard	Title
draft-ietf-mpls-tp-gach-gal-xx	<i>MPLS Generic Associated Channel</i>

### MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

**RFCs**

<b>RFC</b>	<b>Title</b>
RFC 5921	<i>A Framework for MPLS in Transport Networks</i>
RFC 5885	<i>Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)</i>
RFC 5586	<i>MPLS Generic Associated Channel</i>

**Technical Assistance**

<b>Description</b>	<b>Link</b>
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.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## Feature Information for MPLS-TP

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 1**      **Feature Information for MPLS-TP**

Feature Name	Releases	Feature Information
MPLS Transport Profile	15.1(1)SA 15.3(1)S Cisco IOS XE Release 3.5S	<p>MPLS Transport Profile (TP) enables you to create tunnels that provide the transport network service layer over which IP and MPLS traffic traverse. MPLS-TP tunnels enable a transition from Synchronous Optical Networking (SONET) and Synchronous Digital Hierarchy (SDH) time-division multiplexing (TDM) technologies to packet switching to support services with high bandwidth requirements, such as video.</p> <p>In Cisco IOS XE Release 3.5S, support was added for the Cisco ASR 903 Router.</p> <p>The following commands were introduced or modified:</p> <p><b>debug mpls l2transport static-oam, debug mpls tp, interface tunnel-tp interval local interface logging (MPLS-TP) medium p2p mpls tp mpls tp link mpls tp lsp ping mpls tp pseudowire-static-oam class pseudowire-tlv template show mpls l2transport static-oam show mpls tp status protocol notification static timeout refresh tlv tlv template trace mpls tp</b></p>
L2VPN Static to Dynamic PW Interconnection & PW Preferred Path for MPLS-TP Tunnels	Cisco IOS XE Release 3.5S	In Cisco IOS XE Release 3.5S, support was added for the Cisco ASR 903 Router.
MPLS-TP: PW Redundancy for Static PWs	Cisco IOS XE Release 3.5S	In Cisco IOS XE Release 3.5S, support was added for the Cisco ASR 903 Router.
Bidirectional MPLS-TP LSP	Cisco IOS XE Release 3.5S	In Cisco IOS XE Release 3.5S, support was added for the Cisco ASR 903 Router.

Feature Name	Releases	Feature Information
MPLS-TP Path Protection	Cisco IOS XE Release 3.5S	In Cisco IOS XE Release 3.5S, support was added for the Cisco ASR 903 Router.
MPLS-TP OAM: GACH	Cisco IOS XE Release 3.5S	In Cisco IOS XE Release 3.5S, support was added for the Cisco ASR 903 Router.
MPLS-TP OAM: Continuity Check via BFD	Cisco IOS XE Release 3.5S	In Cisco IOS XE Release 3.5S, support was added for the Cisco ASR 903 Router.
MPLS-TP OAM: Ping/Trace	Cisco IOS XE Release 3.5S	In Cisco IOS XE Release 3.5S, support was added for the Cisco ASR 903 Router.
MPLS-TP OAM: Fault Management	Cisco IOS XE Release 3.5S	In Cisco IOS XE Release 3.5S, support was added for the Cisco ASR 903 Router.
MPLS TP: IP-less configuration of MPLS TP tunnels	Cisco IOS XE Release 3.5S	In Cisco IOS XE Release 3.5S, support was added for the Cisco ASR 903 Router.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.







## MPLS Static Labels

---

This document describes the Cisco MPLS Static Labels feature. The MPLS Static Labels feature provides the means to configure statically:

- The binding between a label and an IPv4 prefix
- The contents of an LFIB crossconnect entry
- [Finding Feature Information, page 35](#)
- [Restrictions for MPLS Static Labels, page 35](#)
- [Prerequisites for MPLS Static Labels, page 36](#)
- [Information About MPLS Static Labels, page 36](#)
- [How to Configure MPLS Static Labels, page 36](#)
- [Configuration Examples for MPLS Static Labels, page 41](#)
- [Additional References, page 43](#)
- [Feature Information for MPLS Static Labels, page 44](#)
- [Glossary, page 44](#)

## Finding Feature Information

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

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

## Restrictions for MPLS Static Labels

- The trouble shooting process for MPLS static labels is complex.
- On a provider edge (PE) router for MPLS VPNs, there is no mechanism for statically binding a label to a customer network prefix (VPN IPv4 prefix).
- MPLS static crossconnect labels remain in the LFIB even if the router to which the entry points goes down.
- MPLS static crossconnect mappings remain in effect even with topology changes.
- MPLS static labels are not supported for label-controlled Asynchronous Transfer Mode (lc-atm).
- MPLS static bindings are not supported for local prefixes.

## Prerequisites for MPLS Static Labels

The network must support the following Cisco IOS features before you enable MPLS static labels:

- Multiprotocol Label Switching (MPLS)
- Cisco Express Forwarding

## Information About MPLS Static Labels

- [MPLS Static Labels Overview, page 36](#)
- [Benefits of MPLS Static Labels, page 36](#)

## MPLS Static Labels Overview

Generally, label switching routers (LSRs) dynamically learn the labels they should use to label-switch packets by means of label distribution protocols that include:

- Label Distribution Protocol (LDP), the Internet Engineering Task Force (IETF) standard, used to bind labels to network addresses
- Resource Reservation Protocol (RSVP) used to distribute labels for traffic engineering (TE)
- Border Gateway Protocol (BGP) used to distribute labels for Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs)

To use a learned label to label-switch packets, an LSR installs the label into its Label Forwarding Information Base (LFIB).

The MPLS Static Labels feature provides the means to configure statically:

- The binding between a label and an IPv4 prefix
- The contents of an LFIB crossconnect entry

## Benefits of MPLS Static Labels

### Static Bindings Between Labels and IPv4 Prefixes

Static bindings between labels and IPv4 prefixes can be configured to support MPLS hop-by-hop forwarding through neighbor routers that do not implement LDP label distribution.

### Static Crossconnects

Static crossconnects can be configured to support MPLS Label Switched Path (LSP) midpoints when neighbor routers do not implement either the LDP or RSVP label distribution, but do implement an MPLS forwarding path.

## How to Configure MPLS Static Labels

- [Configuring MPLS Static Prefix Label Bindings, page 37](#)

- [Verifying MPLS Static Prefix Label Bindings, page 38](#)
- [Configuring MPLS Static Crossconnects, page 39](#)
- [Verifying MPLS Static Crossconnect Configuration, page 40](#)
- [Monitoring and Maintaining MPLS Static Labels, page 40](#)

## Configuring MPLS Static Prefix Label Bindings

To configure MPLS static prefix/label bindings, use the following commands beginning in global configuration mode:

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls label range** *min-label max-label* [**static** *min-static-label max-static-label*]
4. **mpls static binding ipv4** *prefix mask* [**input**| **output** *nexthop*] *label*

### DETAILED STEPS

Command or Action	Purpose
<p><b>Step 1</b> <b>enable</b></p> <p><b>Example:</b></p> <pre>Router&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<p><b>Step 2</b> <b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
<p><b>Step 3</b> <b>mpls label range</b> <i>min-label max-label</i> [<b>static</b> <i>min-static-label max-static-label</i>]</p> <p><b>Example:</b></p> <pre>Router(config)# mpls label range 200 100000 static 16 199</pre>	<p>Specifies a range of labels for use with MPLS Static Labels feature.</p> <p>(Default is no labels reserved for static assignment.)</p>
<p><b>Step 4</b> <b>mpls static binding ipv4</b> <i>prefix mask</i> [<b>input</b>  <b>output</b> <i>nexthop</i>] <i>label</i></p> <p><b>Example:</b></p> <pre>Router(config)# mpls static binding ipv4 10.0.0.0 255.0.0.0 55</pre>	<p>Specifies static binding of labels to IPv4 prefixes.</p> <p>Bindings specified are installed automatically in the MPLS forwarding table as routing demands.</p>

## Verifying MPLS Static Prefix Label Bindings

To verify the configuration for MPLS static prefix/label bindings, use this procedure:

### SUMMARY STEPS

1. Enter **show mpls label range** command. The output shows that the new label ranges do not take effect until a reload occurs:
2. Enter the **show mpls static binding ipv4** command to show the configured static prefix/label bindings:
3. Use the **show mpls forwarding-table** command to determine which static prefix/label bindings are currently in use for MPLS forwarding.

### DETAILED STEPS

**Step 1** Enter **show mpls label range** command. The output shows that the new label ranges do not take effect until a reload occurs:

#### Example:

```
Router# show mpls label range

Downstream label pool: Min/Max label: 16/100000
 [Configured range for next reload: Min/Max label: 200/100000]
Range for static labels: Min/Max/Number: 16/199
```

The following output from the **show mpls label range** command, executed after a reload, indicates that the new label ranges are in effect:

#### Example:

```
Router# show mpls label range

Downstream label pool: Min/Max label: 200/100000
Range for static labels: Min/Max/Number: 16/199
```

**Step 2** Enter the **show mpls static binding ipv4** command to show the configured static prefix/label bindings:

#### Example:

```
Router# show mpls static binding ipv4
10.17.17.17/32: Incoming label: 251 (in LIB)
  Outgoing labels:
    10.0.0.1          18
10.18.18.18/32: Incoming label: 201 (in LIB)
  Outgoing labels:
    10.0.0.1    implicit-null
```

**Step 3** Use the **show mpls forwarding-table** command to determine which static prefix/label bindings are currently in use for MPLS forwarding.

#### Example:

```
Router# show mpls forwarding-table
```

Local tag	Outgoing tag or VC Pop tag	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
201	2/35	10.18.18.18/32	0	PO1/1/0	point2point
251	18	10.18.18.18/32	0	AT4/1/0.1	point2point
		10.17.17.17/32	0	PO1/1/0	point2point

## Configuring MPLS Static Crossconnects

To configure MPLS static crossconnects, use the following command beginning in global configuration mode:

### SUMMARY STEPS

1. enable
2. configure terminal
3. `mpls label range min-label max-label [static min-static-label max-static-label]`
4. `mpls static binding ipv4 prefix mask [input| output nexthop] label`

### DETAILED STEPS

Command or Action	Purpose
<p><b>Step 1</b> enable</p> <p><b>Example:</b></p> <pre>Router&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<p><b>Step 2</b> configure terminal</p> <p><b>Example:</b></p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
<p><b>Step 3</b> <code>mpls label range min-label max-label [static min-static-label max-static-label]</code></p> <p><b>Example:</b></p> <pre>Router(config)# mpls label range 200 100000 static 16 199</pre>	<p>Specifies a range of labels for use with MPLS Static Labels feature.</p> <p>(Default is no labels reserved for static assignment.)</p>

Command or Action	Purpose
<p><b>Step 4</b> <code>mpls static binding ipv4 prefix mask [input  output nexthop] label</code></p> <p><b>Example:</b></p> <pre>Router(config)# Router(config)# mpls static binding ipv4 10.0.0.0 255.0.0.0 55</pre>	<p>Specifies static binding of labels to IPv4 prefixes.</p> <p>Bindings specified are installed automatically in the MPLS forwarding table as routing demands.</p>

## Verifying MPLS Static Crossconnect Configuration

To verify the configuration for MPLS static crossconnects, use this procedure:

### SUMMARY STEPS

1. Use the `show mpls static crossconnect` command to display information about crossconnects that have been configured:

### DETAILED STEPS

---

Use the `show mpls static crossconnect` command to display information about crossconnects that have been configured:

**Example:**

```
Router# show mpls static crossconnect
Local   Outgoing   Outgoing   Next Hop
label   label      interface
34      22         pos3/0/0   point2point (in LFIB)
```

---

## Monitoring and Maintaining MPLS Static Labels

To monitor and maintain MPLS static labels, use one or more of the following commands:

### SUMMARY STEPS

1. `enable`
2. `show mpls forwarding-table`
3. `show mpls label range`
4. `show mpls static binding ipv4`
5. `show mpls static crossconnect`

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b></p> <pre>Router&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<p><b>show mpls forwarding-table</b></p> <p><b>Example:</b></p> <pre>Router# show mpls forwarding-table</pre>	<p>Displays the contents of the MPLS LFIB.</p>
Step 3	<p><b>show mpls label range</b></p> <p><b>Example:</b></p> <pre>Router# show mpls label range</pre>	<p>Displays information about the static label range.</p>
Step 4	<p><b>show mpls static binding ipv4</b></p> <p><b>Example:</b></p> <pre>Router# show mpls static binding ipv4</pre>	<p>Displays information about the configured static prefix/label bindings.</p>
Step 5	<p><b>show mpls static crossconnect</b></p> <p><b>Example:</b></p> <pre>Router# show mpls static crossconnect</pre>	<p>Displays information about the configured crossconnects.</p>

## Configuration Examples for MPLS Static Labels

- [Example Configuring MPLS Static Prefixes Labels, page 41](#)
- [Example Configuring MPLS Static Crossconnects, page 42](#)

### Example Configuring MPLS Static Prefixes Labels

In the following output, the **mpls label range** command reconfigures the range used for dynamically assigned labels from 16 to 100000 to 200 to 100000 and configures a static label range of 16 to 199.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# mpls label range 200 100000 static 16 199
```

```
% Label range changes take effect at the next reload.
Router(config)# end
```

In the following output, the **show mpls label range** command indicates that the new label ranges do not take effect until a reload occurs:

```
Router# show mpls label range

Downstream label pool: Min/Max label: 16/100000
 [Configured range for next reload: Min/Max label: 200/100000]
Range for static labels: Min/Max/Number: 16/199
```

In the following output, the **show mpls label range** command, executed after a reload, indicates that the new label ranges are in effect:

```
Router# show mpls label range

Downstream label pool: Min/Max label: 200/100000
Range for static labels: Min/Max/Number: 16/199
```

In the following output, the **mpls static binding ipv4** commands configure static prefix/label bindings. They also configure input (local) and output (remote) labels for various prefixes:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# mpls static binding ipv4 10.0.0.0 255.0.0.0 55
Router(config)# mpls static binding ipv4 10.0.0.0 255.0.0.0 output 10.0.0.66 2607
Router(config)# mpls static binding ipv4 10.6.0.0 255.255.0.0 input 17
Router(config)# mpls static binding ipv4 10.0.0.0 255.0.0.0 output 10.13.0.8 explicit-null
Router(config)# end
```

In the following output, the **show mpls static binding ipv4** command displays the configured static prefix/label bindings:

```
Router# show mpls static binding ipv4

10.0.0.0/8: Incoming label: none;
  Outgoing labels:
10.13.0.8      explicit-null
10.0.0.0/8: Incoming label: 55 (in LIB)
  Outgoing labels:
    10.0.0.66      2607
10.66.0.0/16: Incoming label: 17 (in LIB)
  Outgoing labels: None
```

## Example Configuring MPLS Static Crossconnects

In the following output, the **mpls static crossconnect** command configures a crossconnect from incoming label 34 to outgoing label 22 out interface pos3/0/0:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# mpls static crossconnect 34 pos3/0/0 22
Router(config)# end
```

In the following output, the **show mpls static crossconnect** command displays the configured crossconnect:

```
Router# show mpls static crossconnect
Local  Outgoing  Outgoing  Next Hop
label label      interface
34     22         pos3/0/0  point2point (in LFIB)
```



# Additional References

## Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="#">Cisco IOS Master Commands List, All Releases</a>
MPLS commands	<i>Multiprotocol Label Switching Command Reference</i>

## Standards

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

## MIBs

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

## 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 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.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## Feature Information for MPLS Static Labels

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 2** Feature Information for MPLS Static Labels

Feature Name	Releases	Feature Information
MPLS Static Labels	12.0(23)S 12.2(33)SRA 12.2(33)SXH	<p>The MPLS Static Labels feature provides the means to configure the following items statically:</p> <ul style="list-style-type: none"> <li>The binding between a label and an IPv4 prefix</li> <li>The contents of an LFIB crossconnect entry</li> </ul> <p>The following commands were introduced or modified: <b>debug mpls static binding</b>, <b>mpls label range</b>, <b>mpls static binding ipv4</b>, <b>mpls static crossconnect</b>, <b>show mpls label range</b>, <b>show mpls static binding ipv4</b>, <b>show mpls static crossconnect</b></p>

## Glossary

**BGP** --Border Gateway Protocol. The predominant interdomain routing protocol used in IP networks.

**Border Gateway Protocol** --See BGP.

**FIB** --Forwarding Information Base. A table that contains a copy of the forwarding information in the IP routing table.

**Forwarding Information Base** --See FIB.

**label** --A short, fixed-length identifier that tells switching nodes how the data (packets or cells) should be forwarded.

**label binding** --An association between a label and a set of packets, which can be advertised to neighbors so that a label switched path can be established.

**Label Distribution Protocol** --See LDP.

**Label Forwarding Information Base** --See LFIB.

**label imposition** --The act of putting the first label on a packet.

**label switching router** --See LSR.

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

**LFIB** --Label Forwarding Information Base. A data structure in which destinations and incoming labels are associated with outgoing interfaces and labels.

**LSR** --label switching router. A Layer 3 router that forwards a packet based on the value of an identifier encapsulated in the packet.

**MPLS** --Multiprotocol Label Switching. An industry standard on which label switching is based.

**MPLS hop-by-hop forwarding** --The forwarding of packets along normally routed paths using MPLS forwarding mechanisms.

**Multiprotocol Label Switching** --See MPLS.

**Resource Reservation Protocol** --See RSVP.

**RIB** --Routing Information Base. A common database containing all the routing protocols running on a router.

**Routing Information Base** --See RIB.

**RSVP** --Resource Reservation Protocol. A protocol for reserving network resources to provide quality of service guarantees to application flows.

**traffic engineering** --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 were used.

**Virtual Private Network** --See VPN.

**VPN** --Virtual Private Network. A network that enables IP traffic to use tunneling to travel securely over a public TCP/IP network.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams,

and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.



## NetFlow MPLS Label Export

---

The NetFlow MPLS Label Export feature allows a label switch router (LSR) to collect and export Multiprotocol Label Switching (MPLS) labels allocated by the LSR when an adjacent router pushes that label on the top of the label stack of a transit packet. At the same time, the LSR collects the prefix associated with the MPLS label and the application that allocated the label. The router collects the information in a table called the MPLS Prefix/Application/Label (PAL) table and exports this data to a NetFlow collector as the label is allocated or, if so configured, periodically exports the full MPLS PAL table.

You can use this information to create a provider edge (PE)-to-PE matrix, which is useful for network traffic planning and billing. To realize this benefit, you must export the MPLS label information to a NetFlow collector for analysis. This feature also provides information that a NetFlow collector can use to create a Virtual Private Network (VPN) routing and forwarding instance (VRF)-to-PE and PE-to-VRF matrix.

- [Finding Feature Information, page 47](#)
- [Prerequisites for NetFlow MPLS Label Export, page 47](#)
- [Restrictions for NetFlow MPLS Label Export, page 48](#)
- [Information About NetFlow MPLS Label Export, page 48](#)
- [How to Configure NetFlow MPLS Label Export, page 52](#)
- [Configuration Examples for NetFlow MPLS Label Export, page 58](#)
- [Additional References, page 59](#)
- [Command Reference, page 60](#)
- [Feature Information for NetFlow MPLS Label Export, page 61](#)
- [Glossary, page 61](#)

## Finding Feature Information

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

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

## Prerequisites for NetFlow MPLS Label Export

The NetFlow MPLS Label Export feature requires the following:

- NetFlow configured on the LSR
- MPLS enabled on the LSR

If you are exporting data to a Cisco NetFlow collector, the following requirements apply:

- NetFlow Version 9 export format configured on the LSR
- NetFlow collector and analyzer that can use MPLS PAL records exported in NetFlow Version 9 format

## Restrictions for NetFlow MPLS Label Export

The following restrictions apply to the NetFlow MPLS Label Export feature for Cisco IOS 12.2S releases and Cisco IOS Release 12.5(1):

- The MPLS PAL table does not support the export of information for the following:
  - IP Version 6 (IPv6) labels
  - IP Multicast labels
  - Quality of service (QoS) labels
  - Traffic engineering (TE) tunnel headend labels
- The ability to create a VRF-to-VRF traffic matrix is not supported.
- If one application deallocates a label and a second application soon reallocates the same label, the NetFlow collector might not be able to determine how many packets flowed while the label was owned by each application.
- In MPLS PAL table records, for labels allocated by VPNs, Border Gateway Protocol (BGP) IPv4, or BGP VPN Version 4 (VPNv4), the stored prefix can be either 0.0.0.0 or a route distinguisher (RD)-specific address:
  - If you do not configure the **mplsexportvpn4prefixes** command, VPN prefixes are not tracked in the MPLS PAL table. These prefixes are displayed by the **showmplsflowmappings** command as 0.0.0.0.
  - If you configure the **mplsexportvpn4prefixes** command, VPN prefixes are tracked and RD-specific addresses are displayed by the **showmplsflowmappings** command.

## Information About NetFlow MPLS Label Export

The following sections contain useful information for understanding how to configure and use the NetFlow MPLS Label Export feature:

- [MPLS Label Information Gathering and Exporting, page 48](#)
- [Labels Allocated by VPNs BGP IPv4 or BGP VPNv4 in the MPLS PAL Table, page 49](#)
- [MPLS PAL Table Record Export, page 50](#)
- [MPLS PAL and NetFlow Statistics Correlation on a NetFlow Collector, page 52](#)
- [MPLS Label Mapping on a Line Card, page 52](#)

## MPLS Label Information Gathering and Exporting

In a Cisco IOS 12.0S, 12.3T, or 12.4T release that supports the MPLS-Aware NetFlow feature, the mapping of the MPLS label to a prefix and an MPLS application is achieved through the use of the Label

Forwarding Information Base (LFIB). You can display this information with the **showipcacheverboseflow** command. These releases do not support the NetFlow MPLS Label Export feature.

In a Cisco IOS 12.2(28)SB release or later release that supports the NetFlow MPLS Label Export feature, the mapping of the MPLS label to a destination prefix or Forwarding Equivalence Class (FEC) and to the MPLS application currently using the label is achieved through the use of an MPLS PAL table. Each supported MPLS application on the router where the NetFlow MPLS Label Export feature is configured registers its label values, prefixes, and owning applications as the labels are allocated. This label-tracking functionality operates on the Route Processor (RP) software.

The MPLS label information (label to prefix and application) mapping is exported to a NetFlow collector at the time when the label is allocated. You can configure periodic export of the full MPLS PAL table to a collector for further processing and analysis through the use of the **mplsexportinterval** command.

An *interval* argument to the **mplsexportinterval** command controls the time in minutes between full MPLS PAL table exports to the NetFlow collector. You can configure an interval in the range of 0 to 10080 (1 week) minutes:

- If you want to export MPLS PAL table information only when the label is allocated, then configure this command with a 0 time interval with the **mplsexportinterval0** command.
- If you want to trigger an immediate export of the full MPLS PAL table, reconfigure the command with an *interval* argument that is different from the interval that is configured. For example, if you have configured the **mplsexportinterval1440** command, reconfigure the command with any nonzero number except 1440.
- If you have a complex network that generates a large amount of traffic, configure a large interval between MPLS PAL table exports. You might want to configure an interval from 6 to 12 hours (360 and 720 minutes).

The *interval* argument that you specify is the least amount of time that passes before another export of the MPLS PAL table occurs. The system could delay the MPLS PAL table export for 10 minutes if the PAL export queue already contains a large number of entries. This could happen if the export occurred at a time when thousands of routes just came up, or if NetFlow did not have the time to clear the export queue from either a previous export of the full table or a previous time when thousands of routes came up in a brief period of time.

After you have entered the **mplsexportinterval** command, you can use the **showmplsflowmappings** command to display MPLS PAL table entries. To display information about the number of MPLS PAL records exported to the collector, use the **showipflowexportverbose** command.

## Labels Allocated by VPNs BGP IPv4 or BGP VPNv4 in the MPLS PAL Table

If you want to see VPN prefix information, that is, labels allocated by VPN, BGP IPv4, or BGP VPNv4, you need to configure the **mplsexportvpnv4prefixes** command. If you do not configure the **mplsexportvpnv4prefixes** command, MPLS PAL stores labels allocated by these application as prefix 0.0.0.0.

After you configure the **mplsexportvpnv4prefixes** command, the VPN prefix and the associated RD are stored in the MPLS PAL table. VPN addresses are made unique by adding an RD to the front of the address. The RD removes any ambiguity when the same VPN prefix is used for more than one VRF.

**Note**

To export VPN prefixes and associated RDs from the MPLS PAL table, the first time you configure the **mplsexportvpnv4prefixes** command you need to save the configuration and reboot the router or clear all routes from the table.

To display the VPN prefix entries in the MPLS PAL table, use the **showmplsflowmappings** command.

With the **mplsexportvpnv4prefixes** command configured, a line of the output might look like this:

```
Router# show mpls flow mappings
Label      Owner      Route-Distinguisher Prefix          Allocated
.
.
.
27         BGP        100:1          10.34.0.0      00:57:48
```

The format of the Route-Distinguisher field in the output depends on how the RD was configured. The RD can be configured in the as-number:network number (ASN:nn) format, as shown in the example, or it can be configured in the IP address:network number format (IP-address:nn).

If you did not configure the **mplsexportvpnv4prefixes** command, a line of the output looks like this:

```
Router# show mpls flow mappings
.
.
.
Label      Owner      Route-Distinguisher Prefix          Allocated
21         BGP        .              0.0.0.0        00:52:18
```

The Route-Distinguisher field is not populated and the Prefix is displayed as 0.0.0.0.

If the MPLS PAL table tracks a per-VRF aggregate label and you configured the **mplsexportvpnv4prefixes** command, the **showmplsflowmappings** command displays the RD associated with the per-VRF aggregate label, but the prefix for the per-VRF aggregate label is reported as 0.0.0.0. If the **mplsexportvpnv4prefixes** command is not configured, the per-VRF aggregate label is reported with no RD and prefix 0.0.0.0, and you cannot distinguish the per-VRF aggregate label from a normal BGP label.

## MPLS PAL Table Record Export

In Cisco IOS Release 12.0S and later releases, the export of MPLS-Aware NetFlow cache records makes use of the NetFlow Version 9 export format data and template. The export of MPLS PAL table entries also uses the NetFlow Version 9 export format. MPLS PAL packets are exported as NetFlow options packets rather than NetFlow data packets. NetFlow options packets are defined in *Cisco Systems NetFlow Services Export Version 9*, Request for Comments (RFC) 3954.

The RP on the PE router learns and queues the MPLS PAL table records for export. The RP can combine large numbers of PAL table entries in a single Version 9 record and send the record to the NetFlow collector. The information exported by the RP contains instances of the following for each tracked label:

Label, allocating-application (Owner), Route-Distinguisher, Prefix, time stamp (Allocated)

Because the mapping may change as labels expire and are reused, each PAL record contains a time stamp indicating the system uptime at which the label was allocated.

### NetFlow Export Template Format Used for MPLS PAL Entries

This is the NetFlow Version 9 export template format used for MPLS PAL entries:

MPLS label: 3 bytes

MPLS label application type: 1 byte



MPLS label IP prefix: 4 bytes  
 MPLS VPN prefix RD: 8 bytes  
 MPLS label allocation time: 4 bytes

**MPLS Application Types Exported**

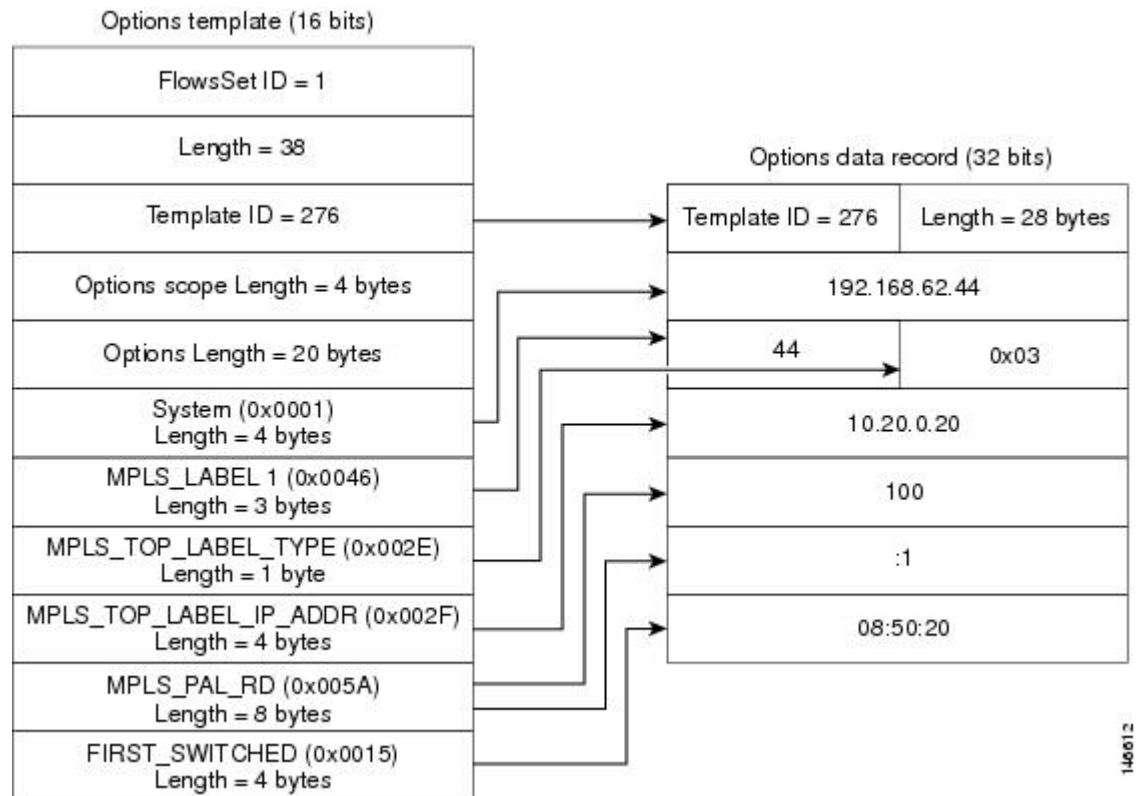
The following MPLS application types are exported in the MPLS label application type field:

- TE = 1
- ATOM = 2
- VPN = 3
- BGP = 4
- LDP = 5

**Options Template and Options Data Record for MPLS PAL Record Export**

The figure below shows an example of the options template and options data record for MPLS PAL record export. This example shows that MPLS label 44 was allocated by a VPN 0x03 at 08:50:20 and is associated with the IP address 10.20.0.20 and with RD 100:1.

**Figure 1 MPLS PAL Export Format Record**



146012

## MPLS PAL and NetFlow Statistics Correlation on a NetFlow Collector

A NetFlow collector can gather the PAL NetFlow packets from a PE router and correlate the label mappings with the recent NetFlow records from adjacent provider core (P) routers.

For example, the MPLS PAL export packet contains MPLS label mappings over a period of time, as each label is allocated and reallocated on the PE router. The packet might contain the following information:

```
label 5, prefix 10.0.0.0, type LDP, 12:00:00
label 4, prefix 10.10.0.0, type LDP, 13:00:00
label 5, prefix 10.9.0.0, type VPN, 14:00:00
```

The NetFlow collector then receives a NetFlow packet from the adjacent P router indicating the following:

```
label 5, 123 packets, 9876 bytes, time 12:22:15.
```

The collector would match the time range known from the PAL packets with the line card (LC) packet time stamp. This would result in the correct mapping for label 5 at time 12:22:15, as follows:

```
label 5, application LDP, prefix 10.0.0.0.
```

The NetFlow collector needs to be able to handle relative differences in the time stamps caused by different reboot times of the P and PE routers.

To implement the offline label mapping checks in the NetFlow collector, the collector needs to maintain a history of label mappings obtained from the MPLS PAL NetFlow packets sent by the RP. If a label is deallocated and reallocated, the collector should track both the old and the new MPLS PAL information for the label.



### Note

On a rare occasion, the collector might not be able to accurately track how many packets flowed for a label that has been deallocated by one application and soon reallocated by another application.

## MPLS Label Mapping on a Line Card

Label to prefix and application mapping is registered and exported from the router RP. This functionality does not occur on the line card. If you want to see the mapping for a particular label on a line card and the label of interest is tracked by the MPLS PAL table, then you can do the following:

- Enter the **showmplsforwarding** command on the line card.
- Enter the **showmplsflowmappings** on the RP.
- Compare the output of the two commands.

You might find the **include** keyword to the commands useful in this case. For example, You could enter the **showmplsflowmappings include 777** command to see the information for any label with substring 777.

## How to Configure NetFlow MPLS Label Export

Perform the following tasks to configure the NetFlow MPLS Label Export feature on an LSR. This feature provides the label, prefix, and application mapping through the MPLS PAL table that collects and exports the data to a NetFlow collector.

- [Configuring NetFlow MPLS Label Export and MPLS PAL Table Export, page 53](#)
- [Displaying Information About the MPLS PAL Table, page 54](#)

- [Configuring the Export of MPLS VPN Version 4 Label Information from the MPLS PAL Table to a NetFlow Collector, page 56](#)

## Configuring NetFlow MPLS Label Export and MPLS PAL Table Export

Perform this task to configure the NetFlow MPLS Label Export feature and MPLS PAL table export to a NetFlow collector. You can use the information generated for network traffic planning and billing.

The following task must be completed before MPLS labels are allocated by the router for the MPLS PAL table to be exported to a NetFlow collector.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls export interval** *interval*
4. **end**
5. **copy running-config startup-config**
6. **exit**
7. Reboot the router.

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.

Command or Action	Purpose
<p><b>Step 3</b> <code>mpls export interval interval</code></p> <p><b>Example:</b></p> <pre>Router(config)# mpls export interval 360</pre> <p><b>Example:</b></p>	<p>Configures a periodic time interval for the export of the entire MPLS PAL table to a NetFlow collector.</p> <ul style="list-style-type: none"> <li>The <i>interval</i> argument specifies the time in minutes between full PAL table exports. The range of valid time intervals is 0 to 10,080 minutes.</li> <li>We recommend that you select a time interval from 360 minutes (6 hours) to 1440 minutes (24 hours) depending on the size of your network and how often the NetFlow collector might be restarted.</li> <li>If you enter an interval of 0, full PAL table exports are disabled. PAL information is exported only as labels are allocated.</li> <li>If you need to restart your NetFlow collector and want to learn PAL information immediately, you can change the <i>interval</i> argument. When you change the time interval, the application exports the full PAL table.</li> </ul> <p><b>Note</b> Allocated labels are tracked only after you enter the <code>mplsexportinterval</code> command. Any labels allocated before you enter this command are not tracked.</p>
<p><b>Step 4</b> <code>end</code></p> <p><b>Example:</b></p> <pre>Router(config)# end</pre>	<p>Exits to privileged EXEC mode.</p>
<p><b>Step 5</b> <code>copy running-config startup-config</code></p> <p><b>Example:</b></p> <pre>Router# copy running-config startup-config</pre>	<p>Copies the modified configuration into router NVRAM, permanently saving the settings.</p> <p>The next time the router is reloaded or rebooted the NetFlow MPLS Label Export feature is already part of the configuration.</p>
<p><b>Step 6</b> <code>exit</code></p> <p><b>Example:</b></p> <pre>Router# exit</pre>	<p>Exits to user EXEC mode.</p>
<p><b>Step 7</b> Reboot the router.</p>	<p>(Optional) Saves the configuration and reboots the router to ensure that the information collected by this feature is complete.</p>

## Displaying Information About the MPLS PAL Table

Perform this task to display information about the MPLS PAL table. The information displayed includes the label, the application that allocated the label, an RD and destination prefix associated with the label, and the time the label was allocated by the application.

**SUMMARY STEPS**

1. **enable**
2. **show mpls flow mappings**
3. **show ip flow export verbose | include PAL**
4. **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 flow mappings**

Use this command to display entries in the MPLS PAL table. For example:

**Example:**

```
Router# show mpls flow mappings
Label  Owner  Route-Distinguisher Prefix           Allocated
18     LDP    10.0.0.5           10.0.0.5        00:52:10
21     BGP    0.0.0.0            0.0.0.0        00:52:18
22     BGP    0.0.0.0            0.0.0.0        00:52:18
25     BGP    0.0.0.0            0.0.0.0        00:51:44
26     LDP    10.32.0.0          10.32.0.0      00:52:10
27     TE-MIDPT 10.30.0.2          10.30.0.2      00:52:06
28     LDP    10.33.0.0          10.33.0.0      00:52:10
29     LDP    10.0.0.1            10.0.0.1      00:52:10
30     LDP    10.0.0.3            10.0.0.3      00:52:10
```

In this example, the **mplsexportvpnv4prefixes** command was not configured. Therefore, the MPLS PAL functionality did not export an RD for the BGP application, and the associated prefix is exported as 0.0.0.0.

The following shows sample output from the **showmplsflowmappings** command if you previously entered the **mplsexportvpnv4prefixes** command:

**Example:**

```
Router# show mpls flow mappings
Label  Owner  Route-Distinguisher Prefix           Allocated
16     LDP    10.0.0.3           10.0.0.3        00:58:03
17     LDP    10.33.0.0          10.33.0.0      00:58:03
19     TE-MIDPT 10.30.0.2          10.30.0.2      00:58:06
20     LDP    10.0.0.5           10.0.0.5        00:58:03
23     LDP    10.0.0.1            10.0.0.1      00:58:03
24     LDP    10.32.0.0          10.32.0.0      00:58:03
27     BGP    100:1              10.34.0.0      00:57:48
31     BGP    100:1              10.0.0.9        00:58:21
32     BGP    100:1              10.3.3.0        00:58:21
```

**Step 3****show ip flow export verbose | include PAL**

Use this command to display the number of MPLS PAL records that were exported to the NetFlow collector. For example:

**Example:**

```
Router# show ip flow verbose | include PAL
6 MPLS PAL records exported
```

When you specify the **verbose** keyword and MPLS PAL records have been exported using NetFlow Version 9 data format, the command output contains an additional line that precedes the “x records exported in y UDP datagrams” line.

**Step 4****exit**

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

**Example:**

```
Router# exit
Router>
```

---

## Configuring the Export of MPLS VPN Version 4 Label Information from the MPLS PAL Table to a NetFlow Collector

Perform the following task to configure the export of VPNv4 label information from the MPLS PAL table to a NetFlow collector.

This allows you to track VPN prefix information for MPLS labels allocated by VPNs, BGP IPv4, and BGP VPNv4. You can use the data analyzed by the collector to assist in network traffic planning and billing.

A VRF must be configured on the router.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **mpls export interval** *interval*
4. **mpls export vpnv4 prefixes**
5. **end**
6. **copy running-config startup-config**
7. **exit**
8. Reboot the router.
9. **enable**
10. **show mpls flow mappings**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b></p> <pre>Router&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
Step 3	<p><b>mpls export interval <i>interval</i></b></p> <p><b>Example:</b></p> <pre>Router(config)# mpls export interval 1440</pre>	<p>Configures the collection and export of MPLS PAL information to a NetFlow collector.</p> <ul style="list-style-type: none"> <li>The <i>interval</i> argument specifies the time in minutes between full PAL table exports. The range of valid time intervals is 0 to 10,080 minutes.</li> <li>We recommend that you select a time interval of 6 hours (360 minutes) to 24 hours (1440 minutes) depending on the size of your network.</li> <li>If you enter an interval of 0, full PAL table exports are disabled. PAL information is exported only as labels are allocated.</li> <li>If you need to restart your NetFlow collector and want to learn PAL information immediately, you can change the <i>interval</i> argument. When you change the time interval, the application exports the full PAL table.</li> </ul>
Step 4	<p><b>mpls export vpnv4 prefixes</b></p> <p><b>Example:</b></p> <pre>Router(config)# mpls export vpnv4 prefixes</pre>	<p>Configures the tracking and export of VPNv4 label information from the MPLS PAL table to a NetFlow collector.</p>
Step 5	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Router(config)# end</pre>	<p>Exits to privileged EXEC mode.</p>
Step 6	<p><b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>Router# copy running-config startup-config</pre>	<p>Copies the modified configuration into router NVRAM, permanently saving the settings.</p> <p>The next time the router is rebooted the tracking and export of VPNv4 label information from the MPLS PAL table to a NetFlow collector is already part of the configuration.</p>

	Command or Action	Purpose
Step 7	<b>exit</b>  <b>Example:</b> Router# exit	Exits to user EXEC mode.
Step 8	<b>Reboot the router.</b>	(Optional) Saves the configuration and reboots the router to ensure that the information collected by this feature is complete.
Step 9	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 10	<b>show mpls flow mappings</b>  <b>Example:</b> Router# show mpls flow mappings	Displays MPLS PAL table entries that include VPNv4 prefixes and VPN RDs.

## Configuration Examples for NetFlow MPLS Label Export

- [Configuring NetFlow MPLS Prefix Application Label Table Export Examples, page 58](#)
- [Configuring the Export of MPLS VPNv4 Label Information from the MPLS PAL Table Example, page 59](#)

## Configuring NetFlow MPLS Prefix Application Label Table Export Examples

The following examples show how to configure NetFlow MPLS PAL table export on a PE router.

This example shows how to configure the export of the full MPLS PAL table every 480 minutes (8 hours):

```
configure terminal
!
mpls export interval 480
end
copy running-config startup-config
exit
```

This example shows how to configure MPLS PAL information export only as the labels are allocated:

```
configure terminal
!
mpls export interval 0
end
copy running-config startup-config
exit
```

In this example, the full MPLS PAL table is not exported repeatedly.



## Configuring the Export of MPLS VPNv4 Label Information from the MPLS PAL Table Example

The following example shows how to configure the export of MPLS VPNv4 label information from the MPLS PAL table:

```
configure terminal
!
mpls export interval 720
mpls export vpnv4 prefixes
end
copy running-config startup-config
exit
```

The full MPLS PAL table with MPLS VPNv4 label information is configured to export to the NetFlow collector every 720 minutes (12 hours).

## Additional References

The following sections provide references related to the NetFlow MPLS Label Export feature.

### Related Documents

Related Topic	Document Title
Tasks for configuring MPLS-aware NetFlow	Configuring MPLS-aware NetFlow
Overview of the NetFlow application and advanced NetFlow features and services	Cisco IOS NetFlow Overview
Tasks for configuring NetFlow to capture and export network traffic data	Configuring NetFlow and NetFlow Data Export
Tasks for configuring MPLS egress NetFlow accounting	Configuring MPLS Egress NetFlow Accounting
Detailed information about the fields available in Version 9 export format and about export format architecture	<a href="#">Cisco IOS NetFlow Version 9 Flow-Record Format</a>

### 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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

**RFCs**

RFC	Title
RFC 3954	<a href="#">Cisco Systems NetFlow Services Export Version 9</a>
RFC 2547	<a href="#">BGP/MPLS VPNs</a>

**Technical Assistance**

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List* .

- **mpls export interval**
- **mpls export vpnv4 prefixes**
- **show ip flow export**
- **show mpls flow mappings**

## Feature Information for NetFlow MPLS Label Export

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 3** Feature Information for NetFlow MPLS Label Export

Feature Name	Releases	Feature Information
NetFlow MPLS Label Export	12.2(28)SB 12.2(33)SRA	<p>The NetFlow MPLS Label Export feature provides the label switch router (LSR) with the capability of collecting and exporting the top label in the MPLS label stack along with its prefix or Forwarding Equivalence Class (FEC) and the application allocating the label to a NetFlow collector for supported MPLS applications.</p> <p>In 12.2(28)SB, this feature was introduced.</p> <p>In 12.2(33)SRA, this feature was integrated into a 12.2SRA release.</p>

## Glossary

**BGP** --Border Gateway Protocol. An interdomain routing protocol that replaces Exterior Gateway Protocol (EGP). A BGP system exchanges reachability information with other BGP systems. It is defined by RFC 1163.

**export packet** --A type of packet built by a device (for example, a router) with NetFlow services enabled. The packet is addressed to another device (for example, the NetFlow Collection Engine). The packet contains NetFlow statistics. The other device processes the packet (parses, aggregates, and stores information on IP flows).

**FEC** --Forward Equivalency Class. A set of packets that can be handled equivalently for the purpose of forwarding and thus is suitable for binding to a single label. The set of packets destined for an address prefix is one example of an FEC. A flow is another example

**flow** --A unidirectional stream of packets between a given source and destination--each of which is defined by a network-layer IP address and transport-layer source and destination port numbers. A unique flow is defined as the combination of the following key fields: source IP address, destination IP address, source port number, destination port number, Layer 3 protocol type, type of service (ToS), and input logical interface.

**flowset** --A collection of flow records that follow the packet header in an export packet. A flowset contains information that must be parsed and interpreted by the NetFlow Collection Engine. There are two different types of flowsets: template flowsets and data flowsets. An export packet contains one or more flowsets, and both template and data flowsets can be mixed in the same export packet.

**IPv6** --IP Version 6. Replacement for IP Version 4 (IPv4). IPv6 includes support for flow ID in the packet header, which can be used to identify flows. Formerly called IPng (next generation).

**label** --A short, fixed-length identifier that tells switching nodes how the data (packets or cells) should be forwarded.

**LDP** --Label Distribution Protocol. A standard protocol that operates between Multiprotocol Label Switching (MPLS)-enabled routers to negotiate the labels (addresses) used to forward packets. The Cisco proprietary version of this protocol is the Tag Distribution Protocol (TDP).

**LFIB** --Label Forwarding Information Base. A data structure and way of managing forwarding in which destinations and incoming labels are associated with outgoing interfaces and labels.

**LSR** --label switch router. A router that forwards packets in a Multiprotocol Label Switching (MPLS) network by looking only at the fixed-length label.

**MPLS** --Multiprotocol Label Switching. A switching method in which IP traffic is forwarded through use of a label. This label instructs the routers and the switches in the network where to forward the packets. The forwarding of MPLS packets is based on preestablished IP routing information.

**NetFlow** --A Cisco IOS application that provides statistics on packets flowing through the router. It is emerging as a primary network accounting and security technology.

**NetFlow Collection Engine** (formerly NetFlow FlowCollector)--A Cisco application that is used with NetFlow on Cisco routers and Catalyst series switches. The NetFlow Collection Engine collects packets from the router that is running NetFlow and decodes, aggregates, and stores them. You can generate reports on various aggregations that can be set up on the NetFlow Collection Engine.

**NetFlow v9** --NetFlow export format Version 9. A flexible and extensible means of carrying NetFlow records from a network node to a collector. NetFlow Version 9 has definable record types and is self-describing for easier NetFlow Collection Engine configuration.

**network byte order** --Internet-standard ordering of the bytes corresponding to numeric values.

**options data record** --Special type of data record that is used in the NetFlow process. It is based on an options template and has a reserved template ID that provides information about the NetFlow process itself.

**options template** --A type of template record that the router uses to communicate the format of NetFlow-related data to the NetFlow collector.

**P router** --provider core or backbone router. A router that is part of a service provider's core or backbone network and is connected to the provider edge (PE) routers.

**packet header** --First part of an export packet. It provides basic information about the packet (such as the NetFlow version, number of records contained in the packet, and sequence numbering) so that lost packets can be detected.

**PAL table** --Prefix/Application/Label table. A data structure that collects and exports the prefix, application, and time stamp for a specific label.

**PE router** --provider edge router. A router that is part of a service provider's network connected to a customer edge (CE) router. All Virtual Private Network (VPN) processing occurs in the PE router.

**RD** --route distinguisher. An 8-byte value that is concatenated with an IPv4 prefix to create a unique VPN IPv4 prefix.

There are two formats for configuring the route distinguisher argument. It can be configured in the as-number:network number (ASN:nn) format or it can be configured in the IP address:network number format (IP-address:nn).

**RP** --Route Processor. A processor module in the Cisco 7000 series routers that contains the CPU, system software, and most of the memory components that are used in the router. Sometimes called a Supervisory Processor.

**TE** --traffic engineering. Techniques and processes that cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods were used.

**TE tunnel** --traffic engineering tunnel. A label-switched tunnel that is used for traffic engineering. Such a tunnel is set up through means other than normal Layer 3 routing; it is used to direct traffic over a path.

**template flowset** --A collection of template records that are grouped in an export packet.

**template ID** --A unique number that distinguishes a template record produced by an export device from other template records produced by the same export device. A NetFlow Collection Engine application can receive export packets from several devices. You should be aware that uniqueness is not guaranteed across export devices. Thus, you should configure the NetFlow Collection Engine to cache the address of the export device that produced the template ID in order to enforce uniqueness.

**VPN** --Virtual Private Network. A secure IP-based network that shares resources on one or more physical networks. A VPN contains geographically dispersed sites that can communicate securely over a shared backbone.

**VPNv4 prefix** --IPv4 prefix preceded by an 8-byte route distinguisher. The VPN addresses are made unique by adding a route distinguisher to the front of the address.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.





# ATM PVC Bundle Enhancement MPLS EXP-Based PVC Selection

## Feature History

Release	Modification
12.2(8)T	This feature was introduced.

This module describes the ATM PVC Bundle Enhancement MPLS EXP-Based PVC Selection feature in Cisco IOS Release 12.2(8)T. It includes the following sections:

- [Finding Feature Information, page 65](#)
- [Feature Overview, page 65](#)
- [Supported Platforms, page 68](#)
- [Supported Standards MIBs and RFCs, page 69](#)
- [Configuration Tasks, page 69](#)
- [Configuration Examples, page 72](#)
- [Command Reference, page 76](#)

## Finding Feature Information

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

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

## Feature Overview

The ATM PVC Bundle Enhancement MPLS EXP-Based PVC Selection feature is an extension to the IP to ATM Class of Service feature suite. The IP to ATM Class of Service feature suite, using virtual circuit (VC) support and bundle management, maps quality of service (QoS) characteristics between IP and ATM. It provides customers who have multiple VCs (with varying qualities of service to the same destination) the ability to build a QoS differentiated network.

The IP to ATM Class of Service feature suite allowed customers to use IP precedence level as the selection criteria for packet forwarding. This new feature now gives customers the option of using the Multiprotocol

Label Switching (MPLS) experimental (EXP) level as an additional selection criteria for packet forwarding.

**Note**

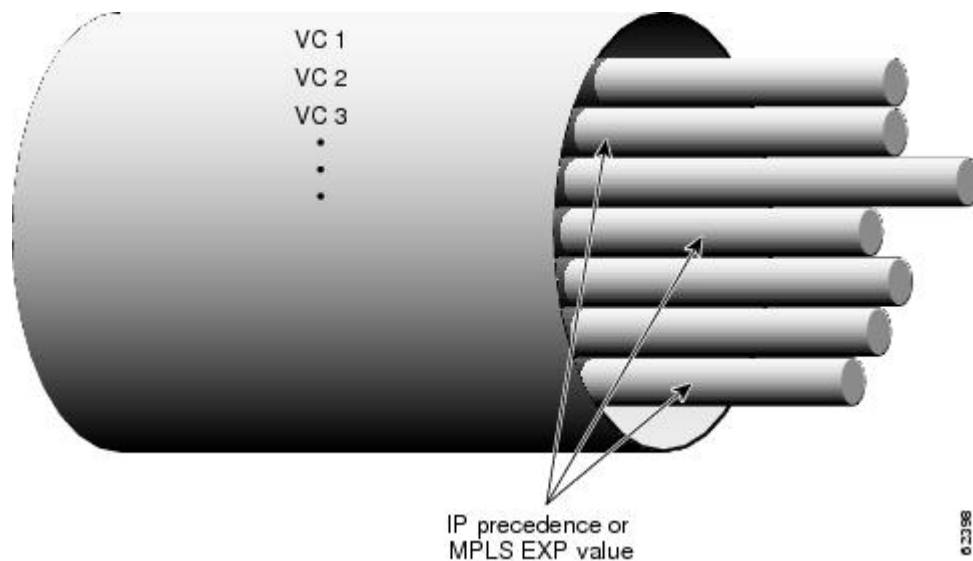
If a selection criteria for packet forwarding is not selected (that is, if the packet is unlabeled), this new feature uses the IP precedence level as the default selection criteria.

- [VC Bundle Support and Bundle Management, page 66](#)
- [Benefits, page 67](#)
- [Restrictions, page 68](#)
- [Related Features and Technologies, page 68](#)
- [Related Documents, page 68](#)

## VC Bundle Support and Bundle Management

ATM VC bundle management allows you to configure multiple VCs that have different QoS characteristics between any pair of ATM-connected routers. As shown in the figure below, these VCs are grouped in a bundle and are referred to as bundle members.

**Figure 2**      **ATM VC Bundle**



ATM VC bundle management allows you to define an ATM VC bundle and add VCs to it. Each VC of a bundle has its own ATM traffic class and ATM traffic parameters. You can apply attributes and characteristics to discrete VC bundle members, or you can apply them collectively at the bundle level.

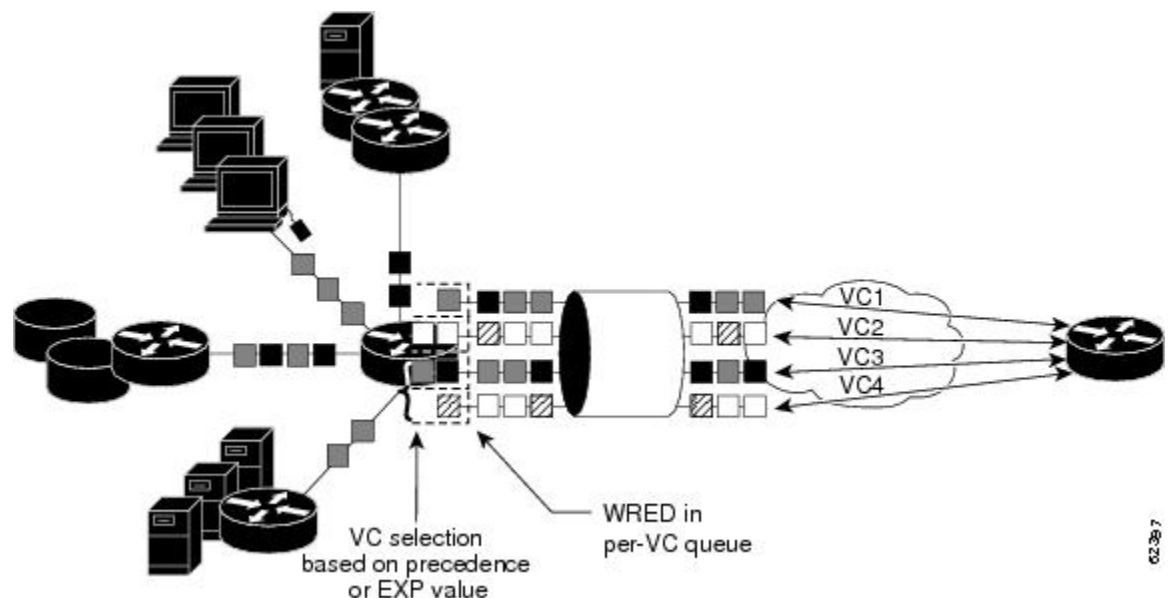
Using VC bundles, you can create differentiated service by flexibly distributing MPLS EXP levels over the different VC bundle members. You can map a single MPLS EXP level, or a range of these levels, to each discrete VC in the bundle, thereby enabling individual VCs in the bundle to carry packets marked with different MPLS EXP levels. You can use Weighted Random Early Detection (WRED) or distributed WRED (dWRED) to further differentiate service across traffic that has different MPLS EXP levels.

To determine which VC in the bundle to use to forward a packet to its destination, the ATM VC bundle management software matches MPLS EXP levels between packets and VCs (see the figure below). IP



traffic is sent to the next hop address for the bundle because all VCs in a bundle share the same destination, but the VC used to carry a packet depends on the value set for that packet in the MPLS EXP level of the type of service (ToS) byte of its header. The ATM VC bundle management software matches the MPLS EXP level of the packet to the MPLS EXP levels assigned to a VC, sending the packet out on the appropriate VC. Moreover, the ATM VC bundle management software allows you to configure how traffic will be redirected when the VC to which the packet was initially directed goes down. The figure below illustrates how the ATM VC bundle management software determines which permanent virtual circuit (PVC) bundle member to use to carry a packet and how WRED (or dWRED) is used to differentiate traffic on the same VC.

**Figure 3** ATM VC Bundle PVC Selection for Packet Transfer



The support of multiple parallel ATM VCs allows you to create stronger service differentiation at the IP layer. For instance, you might want to configure the network to provide IP traffic belonging to real-time class of service (CoS) (such as Voice over IP traffic) on an ATM VC with strict constraints (constant bit rate (CBR) or variable bit rate real-time (VBR-rt), for example), while also allowing the network to transport nonreal-time traffic over a more elastic ATM unspecified bit rate (UBR) PVC. UBR is effectively the ATM version of best-effort service. Using a configuration such as this would allow you to make full use of your network capacity.

## Benefits

### Improved System Performance

This feature is designed to provide a true working solution to class-based services, without the investment of new ATM network infrastructures. Now networks can offer different service classes (sometimes termed *differential service classes*) across the entire WAN, not just the routed portion. Mission-critical applications can be given exceptional service during periods of high network usage and congestion. In addition, noncritical traffic can be restricted in its network usage, ensuring greater QoS for more important traffic and user types.

### Additional Selection Criteria

This new feature now gives customers the option of using the MPLS EXP level, in addition to IP precedence, as a selection criteria for packet forwarding.

## Restrictions

- This feature requires ATM PVC management, as well as Forwarding Information Base (FIB) and Tag Forwarding Information Base (TFIB) switching functionality.
- This feature is not supported on either the ATM interface processor (AIP) or the ATM Lite port adapter (PA-A1).
- The router at the remote end of the network must be using a version of Cisco IOS that supports MPLS and ATM PVC management.

## Related Features and Technologies

This feature is similar to the IP to ATM Class of Service feature suite, which is documented in the "Configuring IP to ATM Class of Service" module.

## Related Documents

- Cisco IOS Quality of Service Solutions Command Reference
- Cisco IOS Switching Services Command Reference
- "Frame Relay PVC Bundles with QoS Support for IP and MPLS " module
- Cisco IOS Wide-Area Networking Command Reference
- "IP to ATM SVC Bundles for Class of Service (CoS) Mapping " module
- "MPLS Label Distribution Protocol (LDP) Overview " module

## Supported Platforms

- Cisco 3600 series

The ATM Adapter PA-A3 is not supported on either the Cisco 3620 router or the Cisco 3640 router. Because certain QoS features (for example, WRED) require the ATM Adapter PA-A3, specific limitations may apply. For more information about platform and feature support, refer to Cisco Feature Navigator (described below).

- Cisco 3725
- Cisco 3745
- Cisco 7200 series
- Cisco 7500 series

### Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS

image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

## Supported Standards MIBs and RFCs

### Standards

No new or modified standards are supported by this feature.

### MIBs

No new or modified MIBs are supported by this feature.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

### RFCs

No new or modified RFCs are supported by this feature.

## Configuration Tasks

See the following sections for configuration tasks for the ATM PVC Bundle Enhancement MPLS EXP-Based PVC Selection feature. Each task in the list is identified as either required or optional.

- [Enabling MPLS, page 70](#)
- [Creating a VC Bundle, page 70](#)
- [Applying Parameters to Bundles, page 70](#)
- [Verifying the Configuration, page 72](#)

## Enabling MPLS

### SUMMARY STEPS

1. Router(config)# **ip cef**
2. Router(config)# **mpls label protocol ldp**
3. Router(config)# **interface** *type number* [*name-tag*]
4. Router(config-if)# **mpls ip**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	Router(config)# <b>ip cef</b>	Enables Cisco Express Forwarding (CEF) on the Route Processor (RP) card. An optional keyword <b>distributed</b> can be used with this command to enable distributed CEF (dCEF) for the Versatile Interface Processor (VIP)-based platforms.
<b>Step 2</b>	Router(config)# <b>mpls label protocol ldp</b>	Specifies the default label distribution protocol for a platform.
<b>Step 3</b>	Router(config)# <b>interface</b> <i>type number</i> [ <i>name-tag</i> ]	Configures an interface type and enters interface configuration mode.
<b>Step 4</b>	Router(config-if)# <b>mpls ip</b>	Enables MPLS forwarding of IPv4 packets along normally routed paths for the platform.

## Creating a VC Bundle

Command	Purpose
Router(config-if)# <b>bundle</b> <i>bundle-name</i>	Creates the specified bundle and enters bundle configuration mode.

## Applying Parameters to Bundles

- [Configuring Bundle-Level Parameters, page 70](#)
- [Configuring a VC Bundle Member Directly, page 71](#)
- [Configuring VC Class Parameters to Apply to a Bundle, page 71](#)
- [Attaching a Class to a Bundle, page 72](#)

## Configuring Bundle-Level Parameters

Command	Purpose
Router(config-if-atm-bundle)# <b>protocol</b> <i>protocol</i> { <i>protocol-address</i>   <b>inarp</b> } [[ <b>no</b> ] <b>broadcast</b> ]	Configures a static map or enables Inverse Address Resolution Protocol (Inverse ARP) or Inverse ARP broadcasts for the bundle.  <b>Note</b> Note that some parameters applied through a VC class or directly to the bundle can be superseded by commands that you directly apply to individual VCs in bundle-vc configuration mode.
Router(config-if-atm-bundle)# <b>encapsulation</b> <i>aal-encap</i>	Configures the ATM adaptation layer (AAL) and encapsulation type for the bundle.

## Configuring a VC Bundle Member Directly

Command	Purpose
Router(config-if-atm-member)# <b>ubr</b> <i>output-pcr</i> [ <i>input-pcr</i> ]	Configures the VC for UBR QoS and specifies the output peak cell rate (PCR) for it.
Router(config-if-atm-member)# <b>vbr-nrt</b> <i>output-pcr output-scr output-mbs</i> [ <i>input-pcr</i> ] [ <i>input-scr</i> ] [ <i>input-mbs</i> ]	Configures the VC for variable bit rate nonreal-time (VBR-nrt) QoS and specifies the output PCR, output sustainable cell rate, and output maximum burst cell size for it.
Router(config-if-atm-member)# <b>mpls</b> <b>experimental</b> [ <b>other</b>   <i>range</i> ]	Configures the MPLS EXP levels for the VC.
Router(config-if-atm-member)# <b>bump</b> { <b>implicit</b>   <b>explicit</b> <i>precedence-level</i>   <b>traffic</b> }	Configures the bumping rules for the VC.
Router(config-if-atm-member)# <b>protect</b> { <b>group</b>   <b>vc</b> }	Configures the VC to belong to the protected group of the bundle or to be an individually protected VC bundle member.

## Configuring VC Class Parameters to Apply to a Bundle

Command	Purpose
Router(config-vc-class)# <b>oam-bundle</b> [ <b>manage</b> ] [ <i>frequency</i> ]	Enables end-to-end F5 Operation, Administration, and Maintenance (OAM) loopback cell generation and OAM management for all VCs in the bundle.  <b>Note</b> If you are using a VC class to configure the bundle, you must attach the VC class to the bundle. To do this, complete the procedure in the section " <a href="#">Attaching a Class to a Bundle</a> , page 72."

## Attaching a Class to a Bundle

Command	Purpose
Router(config-if-atm-bundle)# <b>class-bundle</b> <i>vc-class-name</i>	Configures a bundle with the bundle-level commands contained in the specified VC class.

## Verifying the Configuration

Command	Purpose
Router# <b>debug atm bundle error</b>	Displays debug messages for PVC bundle errors.
Router# <b>debug atm bundle events</b>	Displays PVC bundle events.
Router# <b>show atm map</b>	Displays the list of all configured ATM static maps to remote hosts on an ATM network.
Router# <b>show atm bundle</b> <i>bundle-name</i>	Displays the bundle attributes assigned to each VC member and the current working status of the VC members.
Router# <b>show mpls forwarding-table</b>	Displays the contents of the MPLS FIB.

## Configuration Examples

- [Example VC Bundle Configuration Using a VC Class](#), page 72

### Example VC Bundle Configuration Using a VC Class

This example configures VC bundle management on a router that uses Intermediate System-to-Intermediate System (IS-IS) as its IP routing protocol.

- [Bundle-Class Class](#), page 73

- [Control-Class Class, page 73](#)
- [Premium-Class Class, page 73](#)
- [Priority-Class Class, page 74](#)
- [Basic-Class Class, page 74](#)
- [new-york Bundle, page 74](#)
- [san-francisco Bundle, page 75](#)
- [los-angeles Bundle, page 75](#)

## Bundle-Class Class

At the outset, this configuration defines a VC class called "bundle-class," which includes commands that set VC parameters. When the class bundle-class is applied at the bundle level, these parameters are applied to all VCs that belong to the bundle. Note that any commands applied directly to an individual VC of a bundle in bundle-vc mode take precedence over commands applied globally at the bundle level. Taking into account hierarchy precedence rules, VCs belonging to any bundle to which the class bundle-class is applied will be characterized by the following parameters: aal5snap encapsulation, broadcast on, use of Inverse ARP to resolve IP addresses, and OAM enabled.

```
router isis
 net 49.0000.0000.0000.1111.00
vc-class atm bundle-class
 encapsulation aal5snap
 broadcast
 protocol ip inarp
 oam-bundle manage 3
 oam 4 3 10
```

The following four sections of the configuration define specific VC classes. Each of these classes contains commands used to specify parameters that can then be applied to individual VCs in a bundle by assigning the class to that VC.

## Control-Class Class

When the class called "control-class" is applied to a VC, the VC carries traffic whose MPLS EXP level is 7. When the VC to which this class is assigned goes down, it takes the bundle down with it because this class makes the VC a protected one. The QoS type of a VC using this class is vbr-nrt.

```
vc-class atm control-class
 mpls experimental 7
 protect vc
 vbr-nrt 1000 5000 32
```

## Premium-Class Class

When the class called "premium-class" is applied to a VC, the VC carries traffic whose MPLS EXP levels are 6 and 5. The VC does not allow other traffic to be bumped onto it. When the VC to which this class is applied goes down, its bumped traffic will be redirected to a VC whose MPLS EXP level is 7. This class makes a VC a member of the protected group of the bundle. When all members of a protected group go down, the bundle goes down. The QoS type of a VC using this class is vbr-nrt.

```
vc-class atm premium-class
 mpls experimental 6-5
 no bump traffic
 protect group
 bump explicitly 7
 vbr-nrt 20000 10000 32
```

## Priority-Class Class

When the class called "priority-class" is applied to a VC, the VC is configured to carry traffic with an MPLS EXP level in the 4 - 2 range. The VC uses the implicit bumping rule, it allows traffic to be bumped, and it belongs to the protected group of the bundle. The QoS type of a VC using this class is ubr+.

```
vc-class atm priority-class
mpls experimental 4-2
protect group
ubr+ 10000 3000
```

## Basic-Class Class

When the class called "basic-class" is applied to a VC, the VC is configured through the **mpls experimental other** command to carry traffic with MPLS EXP levels not specified in the profile. The VC using this class belongs to the protected group of the bundle. The QoS type of a VC using this class is ubr.

```
vc-class atm basic-class
mpls experimental other
protect group
ubr 10000
```

The following sets of commands configure three bundles that the router subinterface uses to connect to three of its neighbors. These bundles are called "new-york," "san-francisco," and "los-angeles." Bundle new-york has four VC members, bundle san-francisco has four VC members, and bundle los-angeles has three VC members.

## new-york Bundle

The first part of this example specifies the IP address of the subinterface, the router protocol--the router uses IS-IS as an IP routing protocol--and it creates the first bundle called "new-york" and enters bundle configuration mode:

```
interface al/0.1 multipoint
ip address 10.0.0.1 255.255.255.0
ip router isis
bundle new-york
```

From within bundle configuration mode, the next portion of the configuration uses two protocol commands to enable IP and Open Systems Interconnect (OSI) traffic flows in the bundle. The OSI routing packets will use the highest MPLS EXP VC in the bundle. The OSI data packets, if any, will use the lowest MPLS EXP VC in the bundle. If configured, other protocols, such as Internet Packet Exchange (IPX) or AppleTalk, will always use the lowest MPLS EXP VC in the bundle.

As the indentation levels of the preceding and following commands suggest, subordinate to bundle new-york is a command that configures its protocol and a command that applies the class called "bundle-class" to it.

```
    protocol ip 1.1.1.2 broadcast
    protocol clns 49.0000.0000.2222.00 broadcast
    class-bundle bundle-class
```

The class called "bundle-class," which is applied to the bundle new-york, includes a **protocol ip inarp** command. According to inheritance rules, **protocol ip**, configured at the bundle level, takes precedence over **protocol ip inarp** specified in the class bundle-class.

The next set of commands beginning with **pvc-bundle ny-control 207**, which are further subordinate, add four VCs (called "ny-control," "ny-premium," "ny-priority," and "ny-basic") to the bundle new-york. A



particular class--that is, one of the classes predefined in this configuration example--is applied to each VC to configure it with parameters specified by commands included in the class.

As is the case for this configuration, to configure individual VCs belonging to a bundle, the router must be in bundle mode for the mother bundle. For each VC belonging to the bundle, the subordinate mode is pvc-mode for the specific VC.

The following commands configure the individual VCs for the bundle new-york:

```
pvc-bundle ny-control 207
  class-vc control-class
pvc-bundle ny-premium 206
  class-vc premium-class
pvc-bundle ny-priority 204
  class-vc priority-class
pvc-bundle ny-basic 201
  class-vc basic-class
```

## san-francisco Bundle

The following set of commands create and configure a bundle called "san-francisco." At the bundle configuration level, the configuration commands included in the class bundle-class are ascribed to the bundle san-francisco and to the individual VCs that belong to the bundle. Then, the **pvc-bundle** command is executed for each individual VC to add it to the bundle. After a VC is added and bundle-vc configuration mode is entered, a particular, preconfigured class is assigned to the VC. The configuration commands comprising that class are used to configure the VC. Rules of hierarchy apply at this point. Command parameters contained in the applied class are superseded by the same parameters applied at the bundle configuration level, which are superseded by the same parameters applied directly to a VC.

```
bundle san-francisco
  protocol clns 49.0000.0000.0000.333.00 broadcast
  inarp 1
  class-bundle bundle-class
pvc-bundle sf-control 307
  class-vc control-class
pvc-bundle sf-premium 306
  class-vc premium-class
pvc-bundle sf-priority 304
  class-vc priority-class
pvc-bundle sf-basic 301
  class-vc basic-class
```

## los-angeles Bundle

The following set of commands create and configure a bundle called "los-angeles." At the bundle configuration level, the configuration commands included in the class bundle-class are ascribed to the bundle los-angeles and to the individual VCs that belong to the bundle. Then, the **pvc-bundle** command is executed for each individual VC to add it to the bundle. After a VC is added and bundle-vc configuration mode is entered, the MPLS EXP level is set for the VC, and the VC is either configured as a member of a protected group (protect group) or as an individually protected VC. A particular class is then assigned to each VC to further characterize it. Rules of hierarchy apply. Parameters of commands applied directly and discretely to a VC take precedence over the same parameters applied within a class to the VC at the bundle-vc configuration level, which take precedence over the same parameters applied to the entire bundle at the bundle configuration level.

```
bundle los-angeles
  protocol ip 1.1.1.4 broadcast
  protocol clns 49.0000.0000.4444.00 broadcast
  inarp 1
  class-bundle bundle-class
```

```
pvc-bundle la-high 407
  mpls experimental 7-5
  protect vc
  class-vc premium-class
pvc-bundle la-mid 404
  mpls experimental 4-2
  protect group
  class-vc priority-class
pvc-bundle la-low 401
  mpls experimental other
  protect group
  class-vc basic-class
```

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Quality of Service Solutions Command Reference* at [http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos\\_book.html](http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_book.html) . For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or a Cisco IOS master commands list.

### New Commands

- **mpls experimental**

### Modified Commands

- **show mpls forwarding-table**

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.