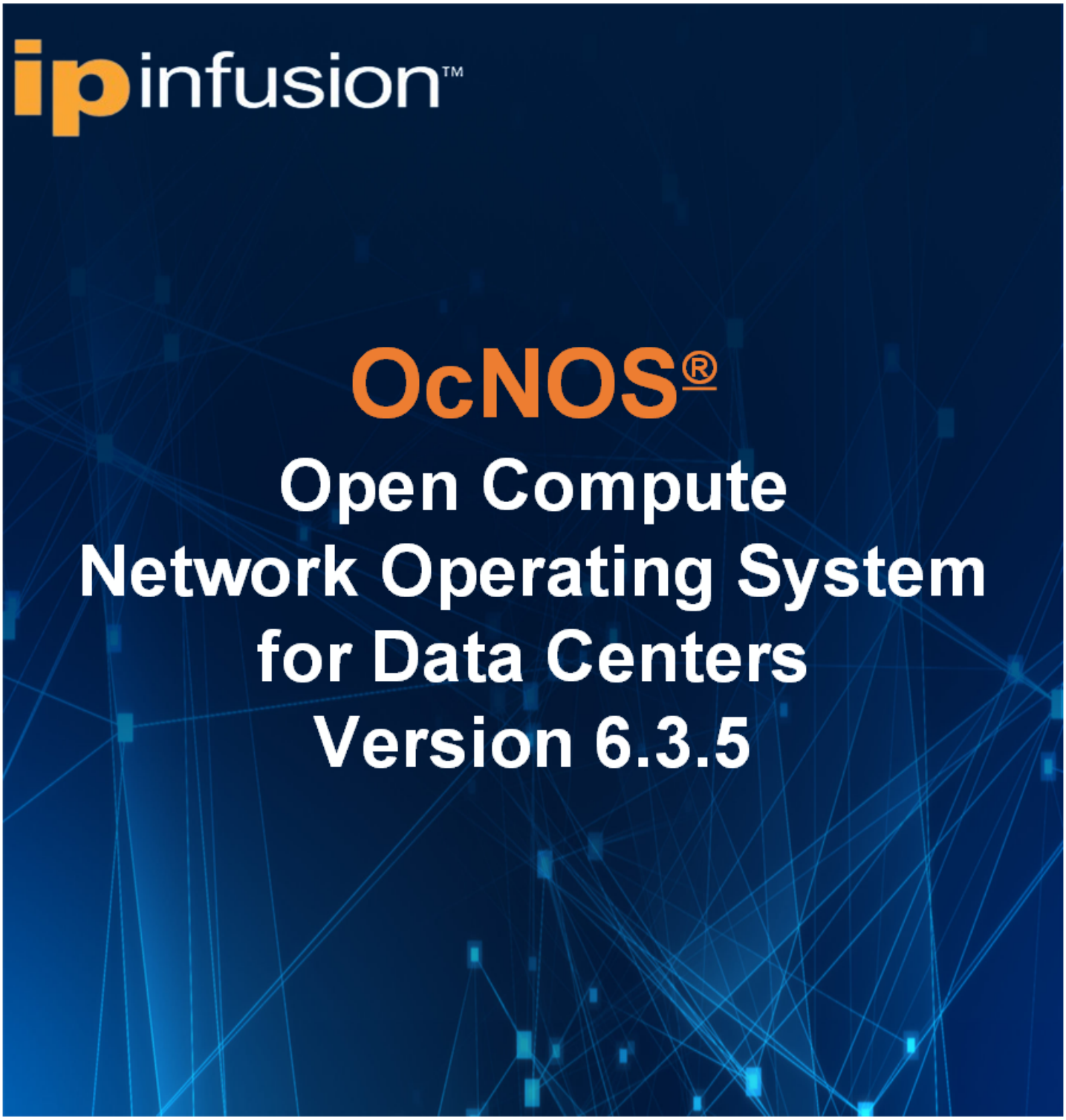


Multi-Protocol Label Switching Guide

June 2024

IP Infusion Inc.

3965 Freedom Circle, Suite 200

Santa Clara, CA 95054

+1 408-400-1900

http://www.ipinfusion.com/

For support, questions, or comments via E-mail, contact:

support@ipinfusion.com

Contents

Preface

This guide describes how to configure MPLS for OcNOS.

IP Maestro Support

Monitor devices running OcNOS Release 6.3.4-70 and above using IP Maestro software.

Audience

This guide is intended for network administrators and other engineering professionals who configure MPLS for OcNOS.

Conventions

Table P-1 shows the conventions used in this guide.

Table P-1: Conventions

Convention	Description
Italics	Emphasized terms; titles of books
Note:	Special instructions, suggestions, or warnings
`monospaced type`	Code elements such as commands, parameters, files, and directories

Chapter Organization

The chapters in command references are organized as described in Command Description Format.

The chapters in configuration guides are organized into these major sections:

- An overview that explains a configuration in words
- Topology with a diagram that shows the devices and connections used in the configuration
- Configuration steps in a table for each device where the left-hand side shows the commands you enter and the right-hand side explains the actions that the commands perform
- Validation which shows commands and their output that verify the configuration

Related Documentation

For information about installing OcNOS, see the *Installation Guide* for your platform.

Feature Availability

The features described in this document are available depending upon the OcNOS SKU that you purchased. See the *Feature Matrix* for a description of the OcNOS SKUs.

Support

For support-related questions, contact support@ipinfusion.com.

Comments

If you have comments, or need to report a problem with the content, contact techpubs@ipinfusion.com.

Command Line Interface

This chapter introduces the OcNOS Command Line Interface (CLI) and how to use its features.

Overview

You use the CLI to configure, monitor, and maintain OcNOS devices. The CLI is text-based and each command is usually associated with a specific task.

You can give the commands described in this manual locally from the console of a device running OcNOS or remotely from a terminal emulator such as `putty` or `xterm`. You can also use the commands in scripts to automate configuration tasks.

Command Line Interface Help

You access the CLI help by entering a full or partial command string and a question mark “?”. The CLI displays the command keywords or parameters along with a short description. For example, at the CLI command prompt, type:

```
> show ?
```

The CLI displays this keyword list with short descriptions for each keyword:

```
show ?
  application-priority            Application Priority
  arp                             Internet Protocol (IP)
  bfd                             Bidirectional Forwarding Detection (BFD)
  bgp                             Border Gateway Protocol (BGP)
  bi-lsp                          Bi-directional lsp status and configuration
  bridge                          Bridge group commands
  ce-vlan                         COS Preservation for Customer Edge VLAN
  class-map                       Class map entry
  cli                             Show CLI tree of current mode
  clns                            Connectionless-Mode Network Service (CLNS)
  control-adjacency               Control Adjacency status and configuration
  control-channel                 Control Channel status and configuration
  cspf                            CSPF Information
  customer                        Display Customer spanning-tree
  cvlan                           Display CVLAN information
  debugging                       Debugging functions (see also 'undebug')
  etherchannel                    LACP etherchannel
  ethernet                        Layer-2
...
```

If you type the ? in the middle of a keyword, the CLI displays help for that keyword only.

```
> show de?
debugging  Debugging functions (see also 'undebug')
```

If you type the ? in the middle of a keyword, but the incomplete keyword matches several other keywords, OcNOS displays help for all matching keywords.

```
> show i? (CLI does not display the question mark).
interface  Interface status and configuration
ip         IP information
isis       ISIS information
```

Command Completion

The CLI can complete the spelling of a command or a parameter. Begin typing the command or parameter and then press the tab key. For example, at the CLI command prompt type `sh`:

```
> sh
```

Press the tab key. The CLI displays:

```
> show
```

If the spelling of a command or parameter is ambiguous, the CLI displays the choices that match the abbreviation. Type `show i` and press the tab key. The CLI displays:

```
> show i
  interface  ip          ipv6       isis
> show i
```

The CLI displays the `interface` and `ip` keywords. Type `n` to select `interface` and press the tab key. The CLI displays:

```
> show in
> show interface
```

Type ? and the CLI displays the list of parameters for the `show interface` command.

```
> show interface
  IFNAME  Interface name
  |       Output modifiers
  >       Output redirection
  <cr>
```

The CLI displays the only parameter associated with this command, the `IFNAME` parameter.

Command Abbreviations

The CLI accepts abbreviations that uniquely identify a keyword in commands. For example:

```
> sh int xe0
```

is an abbreviation for:

```
> show interface xe0
```

Command Line Errors

Any unknown spelling causes the CLI to display the error `Unrecognized command` in response to the ?. The CLI displays the command again as last entered.

```
> show dd?
% Unrecognized command
> show dd
```

When you press the Enter key after typing an invalid command, the CLI displays:

```
(config)#router ospf here
                        ^
% Invalid input detected at '^' marker.
```

where the ^ points to the first character in error in the command.

If a command is incomplete, the CLI displays the following message:

```
> show
% Incomplete command.
```

Some commands are too long for the display line and can wrap mid-parameter or mid-keyword, as shown below. This does *not* cause an error and the command performs as expected:

```
area 10.10.0.18 virtual-link 10.10.0.19 authent
ication-key 57393
```

Command Negation

Many commands have a `no` form that resets a feature to its default value or disables the feature. For example:

- The `ip address` command assigns an IPv4 address to an interface
- The `no ip address` command removes an IPv4 address from an interface

Syntax Conventions

Table P-2 describes the conventions used to represent command syntax in this reference.

Table P-2: Syntax conventions

Convention	Description	Example
`monospaced font`	Command strings entered on a command line	`show ip ospf`
`lowercase`	Keywords that you enter exactly as shown in the command syntax.	`show ip ospf`
`UPPERCASE`	See Variable Placeholders	`IFNAME`
`()`	Optional parameters, from which you must select one. Vertical bars delimit the selections. Do not enter the parentheses or vertical bars as part of the command.	`(A.B.C.D|<0-4294967295>)`
`()`	Optional parameters, from which you select one or none. Vertical bars delimit the selections. Do not enter the parentheses or vertical bars as part of the command.	`(A.B.C.D|<0-4294967295>|)`
`()`	Optional parameter which you can specify or omit. Do not enter the parentheses or vertical bar as part of the command.	`(IFNAME|)`
`{}`	Optional parameters, from which you must select one or more. Vertical bars delimit the selections. Do not enter the braces or vertical bars as part of the command.	`{intra-area <1-255>|inter-area <1-255>|external <1-255>}`

Table P-2: Syntax conventions (Continued)

Convention	Description	Example
`[]`	Optional parameters, from which you select zero or more. Vertical bars delimit the selections. Do not enter the brackets or vertical bars as part of the command.	`[<1-65535>|AA:NN|internet|local-AS|no-advertise|no-export]`
`?`	Nonrepeatable parameter. The parameter that follows a question mark can only appear once in a command string. Do not enter the question mark as part of the command.	`?route-map WORD`
`.`	Repeatable parameter. The parameter that follows a period can be repeated more than once. Do not enter the period as part of the command.	`set as-path prepend .<1-65535>`

Variable Placeholders

Table P-3 shows the tokens used in command syntax use to represent variables for which you supply a value.

Table P-3: Variable placeholders

Token	Description
`WORD`	A contiguous text string (excluding spaces)
`LINE`	A text string, including spaces; no other parameters can follow this parameter
`IFNAME`	Interface name whose format varies depending on the platform; examples are: `eth0`, `Ethernet0`, `ethernet0`, `xe0`
`A.B.C.D`	IPv4 address
`A.B.C.D/M`	IPv4 address and mask/prefix
`X:X::X:X`	IPv6 address
`X:X::X:X/M`	IPv6 address and mask/prefix
`HH:MM:SS`	Time format
`AA:NN`	BGP community value
`XX:XX:XX:XX:XX:XX`	MAC address

`<1-5>`
`<1-65535>`
`<0-2147483647>`
`<0-4294967295>`
	Numeric range

Command Description Format

Table P-4 explains the sections used to describe each command in this reference.

Table P-4: Command descriptions

Section	Description
Command Name	The name of the command, followed by what the command does and when should it be used
Command Syntax	The syntax of the command
Parameters	Parameters and options for the command
Default	The state before the command is executed
Command Mode	The mode in which the command runs; see Command Modes
Example	An example of the command being executed

Keyboard Operations

Table P-5 lists the operations you can perform from the keyboard.

Table P-5: Keyboard operations

Key combination	Operation
Left arrow or Ctrl+b	Moves one character to the left. When a command extends beyond a single line, you can press left arrow or Ctrl+b repeatedly to scroll toward the beginning of the line, or you can press Ctrl+a to go directly to the beginning of the line.
Right arrow or Ctrl-f	Moves one character to the right. When a command extends beyond a single line, you can press right arrow or Ctrl+f repeatedly to scroll toward the end of the line, or you can press Ctrl+e to go directly to the end of the line.
Esc, b	Moves back one word
Esc, f	Moves forward one word
Ctrl+e	Moves to end of the line
Ctrl+a	Moves to the beginning of the line
Ctrl+u	Deletes the line
Ctrl+w	Deletes from the cursor to the previous whitespace
Alt+d	Deletes the current word
Ctrl+k	Deletes from the cursor to the end of line
Ctrl+y	Pastes text previously deleted with Ctrl+k, Alt+d, Ctrl+w, or Ctrl+u at the cursor

Table P-5: Keyboard operations (Continued)

Key combination	Operation
Ctrl+t	Transposes the current character with the previous character
Ctrl+c	Ignores the current line and redisplays the command prompt
Ctrl+z	Ends configuration mode and returns to exec mode
Ctrl+l	Clears the screen
Up Arrow or Ctrl+p	Scroll backward through command history
Down Arrow or Ctrl+n	Scroll forward through command history

Show Command Modifiers

You can use two tokens to modify the output of a `show` command. Enter a question mark to display these tokens:

```
# show users ?
  | Output modifiers
  > Output redirection
```

You can type the | (vertical bar character) to use output modifiers. For example:

```
> show rsvp | ?
  begin     Begin with the line that matches
  exclude   Exclude lines that match
  include   Include lines that match
  last      Last few lines
  redirect  Redirect output
```

Begin Modifier

The `begin` modifier displays the output beginning with the first line that contains the input string (everything typed after the `begin` keyword). For example:

```
# show running-config | begin xe1
...skipping
interface xe1
 ipv6 address fe80::204:75ff:fee6:5393/64
!
interface xe2
 ipv6 address fe80::20d:56ff:fe96:725a/64
!
line con 0
 login
!
end
```

You can specify a regular expression after the `begin` keyword, This example begins the output at a line with either “xe2” or “xe4”:

```
# show running-config | begin xe[3-4]

...skipping
```

```
interface xe3
 shutdown
!
interface xe4
 shutdown
!
interface svlan0.1
 no shutdown
!
route-map myroute permit 3
!
route-map mymap1 permit 10
!
route-map rmap1 permit 3
!
line con 0
 login
line vty 0 4
 login
!
end
```

Include Modifier

The `include` modifier includes only those lines of output that contain the input string. In the output below, all lines containing the word “input” are included:

```
# show interface xe1 | include input
    input packets 80434552, bytes 2147483647, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 1, missed 0
```

You can specify a regular expression after the `include` keyword. This examples includes all lines with “input” or “output”:

```
#show interface xe0 | include (in|out)put
    input packets 597058, bytes 338081476, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 613147, bytes 126055987, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
```

Exclude Modifier

The `exclude` modifier excludes all lines of output that contain the input string. In the following output example, all lines containing the word “input” are excluded:

```
# show interface xe1 | exclude input
Interface xe1
  Scope: both
  Hardware is Ethernet, address is 0004.75e6.5393
  index 3 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Administrative Group(s): None
  DSTE Bandwidth Constraint Mode is MAM
  inet6 fe80::204:75ff:fee6:5393/64
    output packets 4438, bytes 394940, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
```

You can specify a regular expression after the `exclude` keyword. This example excludes lines with “output” or “input”:

```
# show interface xe0 | exclude (in|out)put
Interface xe0
  Scope: both
  Hardware is Ethernet  Current HW addr: 001b.2139.6c4a
  Physical:001b.2139.6c4a  Logical:(not set)
  index 2 metric 1 mtu 1500 duplex-full arp ageing timeout 3000
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Bandwidth 100m
  DHCP client is disabled.
  inet 10.1.2.173/24 broadcast 10.1.2.255
  VRRP Master of :  VRRP is not configured on this interface.
  inet6 fe80::21b:21ff:fe39:6c4a/64
    collisions 0
```

Redirect Modifier

The `redirect` modifier writes the output into a file. The output is not displayed.

```
# show cli history | redirect /var/frame.txt
```

The output redirection token (>) does the same thing:

```
# show cli history >/var/frame.txt
```

Last Modifier

The `last` modifier displays the output of last few number of lines (As per the user input). The last number ranges from 1 to 9999.

For example:

```
#show running-config | last 10
```

String Parameters

The restrictions in Table P-6 apply for all string parameters used in OcNOS commands, unless some other restrictions are noted for a particular command.

Table P-6: String parameter restrictions

Restriction	Description
Input length	1965 characters or less
Restricted special characters	“?”, “,”, “>”, “|”, and “=” The “|” is allowed only for `description` CLI in interface mode.

Command Modes

Commands are grouped into modes arranged in a hierarchy. Each mode has its own set of commands. Table P-7 lists the command modes common to all protocols.

Table P-7: Common command modes

Name	Description
Executive mode	Also called *view* mode, this is the first mode to appear after you start the CLI. It is a base mode from where you can perform basic commands such as `show`, `exit`, `quit`, `help`, and `enable`.
Privileged executive mode	Also called *enable* mode, in this mode you can run additional basic commands such as `debug`, `write`, and `show`.
Configure mode	Also called *configure terminal* mode, in this mode you can run configuration commands and go into other modes such as interface, router, route map, key chain, and address family. Configure mode is single user. Only one user at a time can be in configure mode.
Interface mode	In this mode you can configure protocol-specific settings for a particular interface. Any setting you configure in this mode overrides a setting configured in router mode.
Router mode	This mode is used to configure router-specific settings for a protocol such as BGP or OSPF.

Command Mode Tree

The diagram below shows the common command mode hierarchy.

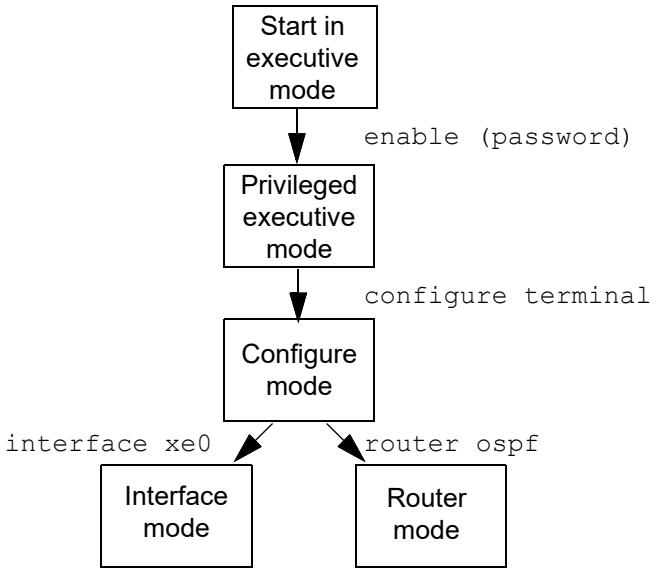


Figure P-1: Common command modes

To change modes:

1. Enter privileged executive mode by entering `enable` in Executive mode.
2. Enter configure mode by entering `configure terminal` in Privileged Executive mode.

The example below shows moving from executive mode to privileged executive mode to configure mode and finally to router mode:

```
> enable mypassword
# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)# router ospf
(config-router)#
```

Note: Each protocol can have modes in addition to the common command modes. See the command reference for the respective protocol for details.

Transaction-based Command-line Interface

The OcNOS command line interface is transaction based:

- Any changes done in configure mode are stored in a separate *candidate* configuration that you can view with the show transaction current command.
- When a configuration is complete, apply the candidate configuration to the running configuration with the commit command.
- If a commit fails, no configuration is applied as the entire transaction is considered failed. You can continue to change the candidate configuration and then retry the commit.
- Discard the candidate configuration with the abort transaction command.
- Check the last aborted transaction with the show transaction last-aborted command.

Multi-Protocol Label Switching Configuration Guide

CHAPTER 1 Understanding Label Space

This chapter contains configurations for Label Space. It also provides an overview of Label Space concepts.

Overview

The Label space refers to the scope of labels in a given LSR. It determines assignment and distribution of labels to a given peer. During data flow, it decides the key for looking up MPLS table and takes appropriate action based on the entry. Label space is designated either as platform label space or per-interface label space.

Per-platform label space

In this implementation, a label must be unique for the entire platform. A label will be interpreted the same way at all the interfaces. The FIB entry in the router does not contain incoming interface related information. Thus the incoming traffic will be matched only with the label.

Per-interface label space

In this implementation, a label must be unique for a given input interface. A label will be interpreted Uniquely at different interface which allows us to re-use label for different entries. The FIB entry in router must contain incoming interface information along with label. Thus the incoming traffic will be matched with label and incoming interface.

Topology

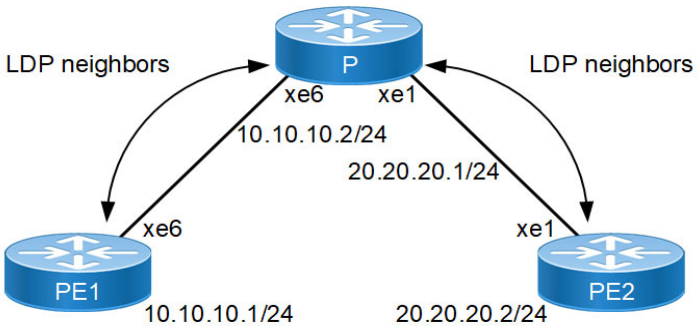


Figure 1-1: LDP Topology

Configuration

Per-Platform Label Space

PE1

`PE1#configure terminal`	Enter configure mode
`PE1(config)#interface lo`	Enter interface mode.
`PE1(config-if)#ip address 1.1.1.1/32`	Configure IP address for the loopback address

`PE1(config-if)#exit`	Exit interface mode
`PE1(config)#interface xe6`	Specify the interface `(xe6)` to be configured
`PE1(config-if)#ip address 10.10.10.1/24`	Configure IP address for the interface
`PE1(config-if)#no shutdown`	Administratively bringing up the interface
`PE1(config-if)#exit`	Exit interface mode
`PE1(config)#router ospf 100`	Configure the routing process and specify the Process ID (100)
`PE1(config-router)#network 10.10.10.0/24 area 0` `PE1(config-router)#network 1.1.1.1/32 area 0`	Define the interface on which OSPF runs and associate the area ID `(0)` with the interface
`PE1(config-router)#exit`	Exit configure mode
`PE1(config)#router ldp`	Enter router mode for LDP
`PE1(config-router)#exit`	Exit router mode for LDP
`PE1(config)#interface xe6`	Specify the interface (xe6)to be configured
`PE1(config-if)#label-switching`	Enabling label switching capability on router
`PE1(config-if)#enable-ldp ipv4`	Enabling ldp on interface
`PE1(config-if)#exit`	Exit interface mode
`PE1(config)#exit`	Exit configure mode

P

`P#configure terminal`	Enter configure mode.
`P(config)#interface lo`	Enter interface mode.
`P(config-if)#ip address 2.2.2.2/32`	Configure IP address for the loopback address
`P(config-if)#exit`	Exit interface mode
`P(config)#interface xe6`	Specify the interface `(xe6)` to be configured
`P(config-if)#ip address 10.10.10.2/24`	Configure IP address for the interface
`P(config-if)#no shutdown`	Administratively bringing up the interface
`P(config)#interface xe1`	Specify the interface `(xe1)` to be configured
`P(config-if)#ip address 20.20.20.1/24`	Configure IP address for the interface
`P(config)#router ospf 100`	Configure the routing process and specify the Process ID (100)

`P(config-router)#network 10.10.10.0/24 area 0`
`P(config-router)#network 20.20.20.0/24 area 0`
`P(config-router)#network 2.2.2.2/32 area 0`
	Define the interface on which OSPF runs and associate the area ID `(0)` with the interface

`P(config-router)#exit`	Exit router mode
`P(config)#router ldp`	Enter router mode for LDP
`P(config-router)#exit`	Exit router mode for LDP
`P(config)#mpls min-label-value 1000 max-label-value 50000 label-space 0`	Configure the minimum label value and maximum label value to be used by Platform label space (Label space 0)
`P(config)#interface xe6`	Specify the interface (xe6)to be configured
`P(config-if)#label-switching`	Enabling label switching capability on router

P(config-if)#enable-ldp ipv4	Enabling ldp on interface
P(config-if)#exit	Exit interface mode
P(config)#interface xe1	Specify the interface (xe1)to be configured
P(config-if)#label-switching	Enabling label switching capability on router
P(config-if)#enable-ldp ipv4	Enabling ldp on interface
P(config-if)#exit	Exit interface mode
P(config)#exit	Exit configure mode

PE2

PE2#configure terminal	Enter configure mode.
PE2(config)#interface lo	Enter interface mode.
PE2(config-if)#ip address 3.3.3.3/32	Configure IP address for the loopback address
PE2(config-if)#exit	Exit interface mode
PE2(config)#interface xe1	Specify the interface (xe1) to be configured
PE2(config-if)#ip address 20.20.20.2/24	Configure IP address for the interface
PE2(config-if)#no shutdown	Administratively bringing up the interface
PE2(config-if)#exit	Exit interface mode
PE2(config)#router ospf 100	Configure the routing process and specify the Process ID (100)
PE2(config-router)#network 20.20.20.0/24 area 0 PE2(config-router)#network 3.3.3.3/32 area 0	Define the interface on which OSPF runs and associate the area ID (0) with the interface
PE2(config-router)#exit	Exit router mode
PE2(config)#router ldp	Enter router mode for LDP
PE2(config-router)#exit	Exit router mode for LDP
PE2(config)#interface xe1	Specify the interface (xe1)to be configured
PE2(config-if)#label-switching	Enabling label switching capability on router
PE2(config-if)#enable-ldp ipv4	Enabling ldp on interface
PE2(config-if)#exit	Exit interface mode

Validation

```
P#sh ldp
Router ID                : 2.2.2.2
LDP Version              : 1
Global Merge Capability  : Merge Capable
Label Advertisement Mode : Downstream Unsolicited
Label Retention Mode     : Liberal
Label Control Mode       : Independent
Instance Loop Detection  : Off
Request Retry            : Off
Propagate Release        : Disabled
Graceful Restart         : Disabled
```

```
Hello Interval           : 5
Targeted Hello Interval  : 15
Hold time                : 15
Targeted Hold time       : 45
Keepalive Interval       : 10
Keepalive Timeout        : 30
Request retry Timeout    : 5
Transport Address data   :
  Labelspace 0           : 2.2.2.2 (in use)
Import BGP routes        : No

P#show mpls label-space 0
 Min-label-value : 1000
 Max-label-value : 50000

 module-static   min-label-value  : 1000
                 max-label-value  : 15999
 module-srgb     min-label-value  : 16000
                 max-label-value  : 24319
 module-rsvp     min-label-value  : 0
                 max-label-value  : 0
 module-ldp      min-label-value  : 0
                 max-label-value  : 0
 module-bgp      min-label-value  : 0
                 max-label-value  : 0
 module-ospf     min-label-value  : 0
                 max-label-value  : 0
P#sh mpls ilm-table
Codes: > - selected ILM, p - stale ILM, K - CLI ILM, T - MPLS-TP

Code  FEC                ILM-ID      In-Label    Out-Label   In-Intf   Out-Intf
Nexthop                      LSP-Type
  >   1.1.1.1/32          1           3840         3          N/A      eth1
172.168.25.56                LSP_DEFAULT
  >   3.3.3.3/32          2           3841         3          N/A      eth2
10.10.20.51                  LSP_DEFAULT
```

Per-Interface Label Space

PE1

`PE1#configure terminal`	Enter configure mode
`PE1(config)#interface lo`	Enter interface mode.
`PE1(config-if)#ip address 1.1.1.1/32`	Configure IP address for the loopback address
`PE1(config-if)#exit`	Exit interface mode
`PE1(config)#interface xe6`	Specify the interface `(xe6)` to be configured
`PE1(config-if)#ip address 10.10.10.1/24`	Configure IP address for the interface
`PE1(config-if)#no shutdown`	Administratively bringing up the interface

`PE1(config-if)#exit`	Exit interface mode
`PE1(config)#router ospf 100`	Configure the routing process and specify the Process ID (100)
`PE1(config-router)#network 10.10.10.0/24 area 0` `PE1(config-router)#network 1.1.1.1/32 area 0`	Define the interface on which OSPF runs and associate the area ID `(0)` with the interface
`PE1(config-router)#exit`	Exit configure mode
`PE1(config)#router ldp`	Enter router mode for LDP
`PE1(config-router)#exit`	Exit router mode for LDP
`PE1(config)#mpls min-label-value 60000 max-label-value 80000 label-space 1`	Configure the minimum label value and maximum label value to be used by interface label space (Label space 1 in this case)
`PE1(config)#interface xe6`	Specify the interface (xe6)to be configured
`PE1(config-if)#label-switching`	Enabling label switching capability on router
`PE1(config-if)#enable-ldp ipv4`	Enabling ldp on interface
`PE1(config-if)#exit`	Exit interface mode
`PE1(config)#exit`	Exit configure mode

P

`P#configure terminal`	Enter configure mode.
`P(config)#interface lo`	Enter interface mode.
`P(config-if)#ip address 2.2.2.2/32`	Configure IP address for the loopback address
`P(config-if)#exit`	Exit interface mode
`P(config)#interface xe6`	Specify the interface `(xe6)` to be configured
`P(config-if)#ip address 10.10.10.2/24`	Configure IP address for the interface
`P(config-if)#no shutdown`	Administratively bringing up the interface
`P(config)#interface xe1`	Specify the interface `(xe1)` to be configured
`P(config-if)#ip address 20.20.20.1/24`	Configure IP address for the interface
`P(config)#router ospf 100`	Configure the routing process and specify the Process ID (100)

`P(config-router)#network 10.10.10.0/24 area 0`
`P(config-router)#network 20.20.20.0/24 area 0`
`P(config-router)#network 2.2.2.2/32 area 0`
	Define the interface on which OSPF runs and associate the area ID `(0)` with the interface

`P(config-router)#exit`	Exit router mode
`P(config)#router ldp`	Enter router mode for LDP
`P(config-router)#exit`	Exit router mode for LDP
`P(config)#mpls min-label-value 60000 max-label-value 80000 label-space 1`	Configure the minimum label value and maximum label value to be used by Interface label space (Label space 1)
`P(config)#interface xe6`	Specify the interface (xe6)to be configured
`P(config-if)#label-switching 1`	Enabling label switching capability on router
`P(config-if)#enable-ldp ipv4`	Enabling ldp on interface

`P(config)#interface xe1`	Specify the interface (xe1)to be configured
`P(config-if)#label-switching 1`	Enabling label switching capability on router
`P(config-if)#enable-ldp ipv4`	Enabling ldp on interface
`P(config-if)#exit`	Exit interface mode
`P(config)#exit`	Exit configure mode

PE2

`PE2#configure terminal`	Enter configure mode.
`PE2(config)#interface lo`	Enter interface mode.
`PE2(config-if)#ip address 3.3.3.3/32`	Configure IP address for the loopback address
`PE2(config-if)#exit`	Exit interface mode
`PE2(config)#interface xe1`	Specify the interface `(xe1)` to be configured
`PE2(config-if)#ip address 20.20.20.2/24`	Configure IP address for the interface
`PE2(config-if)#no shutdown`	Administratively bringing up the interface
`PE2(config-if)#exit`	Exit interface mode
`PE2(config)#router ospf 100`	Configure the routing process and specify the Process ID (100)
`PE2(config-router)#network 20.20.20.0/24 area 0` `PE2(config-router)#network 3.3.3.3/32 area 0`	Define the interface on which OSPF runs and associate the area ID `(0)` with the interface
`PE2(config-router)#exit`	Exit router mode
`PE2(config)#router ldp`	Enter router mode for LDP
`PE2(config-router)#exit`	Exit router mode for LDP
`PE2(config)#mpls min-label-value 60000 max-label-value 80000 label-space 1`	Configure the minimum label value and maximum label value to be used by interface label space (Label space 1)
`PE2(config)#interface xe1`	Specify the interface (xe1)to be configured
`PE2(config-if)#label-switching`	Enabling label switching capability on router
`PE2(config-if)#enable-ldp ipv4`	Enabling ldp on interface
`PE2(config-if)#exit`	Exit interface mode

Validation

```
P#show ldp

Router ID                : 2.2.2.2
LDP Version              : 1
Global Merge Capability  : Merge Capable
Label Advertisement Mode : Downstream Unsolicited
Label Retention Mode     : Liberal
Label Control Mode       : Independent
Instance Loop Detection  : Off
Request Retry            : Off
```

```
Propagate Release        : Disabled
Graceful Restart         : Disabled
Hello Interval           : 5
Targeted Hello Interval  : 15
Hold time                : 15
Targeted Hold time       : 45
Keepalive Interval       : 10
Keepalive Timeout        : 30
Request retry Timeout    : 5
Transport Address data   :
  Labelspace 1           : 2.2.2.2 (in use)
Import BGP routes        : No

P#show mpls label-space 1
 Min-label-value : 60000
 Max-label-value : 80000

 module-static   min-label-value  : 60000
                 max-label-value  : 61000
 module-rsvp     min-label-value  : 0
                 max-label-value  : 0
 module-ldp      min-label-value  : 0
                 max-label-value  : 0
 module-bgp      min-label-value  : 0
                 max-label-value  : 0
 module-ospf     min-label-value  : 0
                 max-label-value  : 0
P#sh mpls ilm
Codes: > - selected ILM, p - stale ILM, K - CLI ILM, T - MPLS-TP

Code  FEC                ILM-ID      In-Label    Out-Label   In-Intf   Out-Intf
Nexthop                      LSP-Type
  >   3.3.3.3/32          3           61441        3          eth1     eth2
10.10.20.51                   LSP_DEFAULT
  >   1.1.1.1/32          4           61440        3          eth2     eth1
172.168.25.56                 LSP_DEFAULT
```

CHAPTER 2 Understanding MPLS TTL Processing

This chapter contains configurations for MPLS-TTL-Processing. It also provides an overview of MPLS-TTL-Processing concepts.

Overview

This feature performs 'Time To Live' (TTL) processing for Multi-Protocol Label Switching (MPLS) packets. The TTL processing is decided by the model chosen by you. This feature provides TTL processing of MPLS packets on ingress, egress, and intermediate routers. TTL processing is compliant with RFC 3443.

The details of TTL processing vary with the tunnel model that is configured for TTL processing. The incoming and outgoing TTL of the packet is determined by the configured tunnel model. Two Models are supported, pipe model and uniform model. Pipe model is default model, where MPLS header TTL Value wont get propagated to IP header.

To know more about uniform model and pipe model, refer chapter MPLS DiffServ Configuration.

Topology

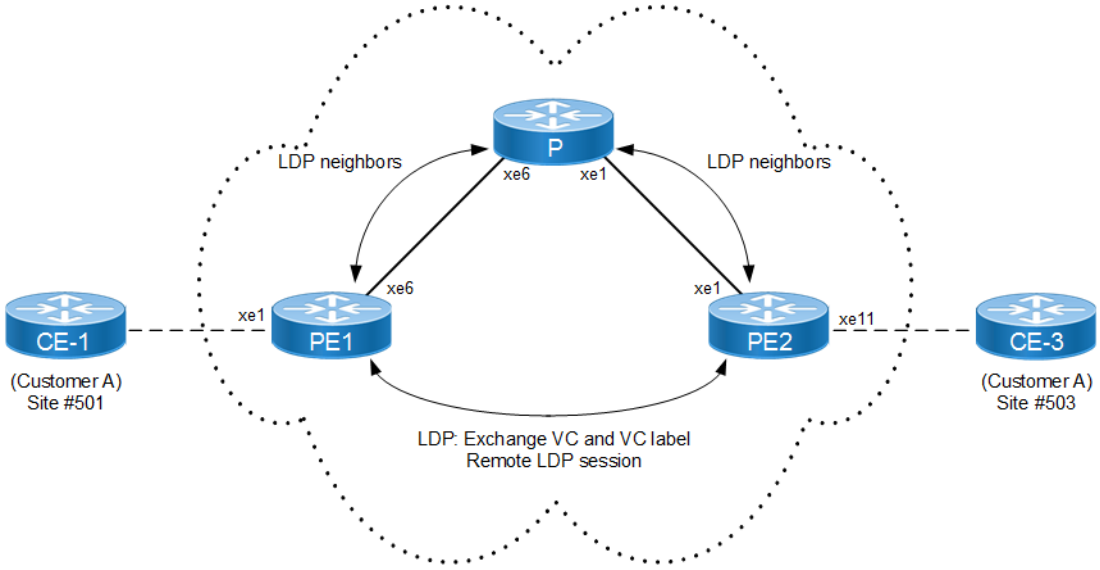


Figure 2-2: TTL Processing Topology

Configuration

PE1

`PE1#configure terminal`	Enter configure mode
`PE1(config)#interface lo`	Enter interface mode.
`PE1(config-if)#ip address 1.1.1.1/32`	Configure IP address for the loopback address
`PE1(config-if)#exit`	Exit interface mode
`PE1(config)#mpls lsp-model pipe`	Configure Lsp-Model as Pipe
`PE1(config)#interface xe6`	Specify the interface `(xe6)` to be configured

`PE1(config-if)#ip address 10.10.10.1/24`	Configure IP address for the interface
`PE1(config-if)#no shutdown`	Administratively bringing up the interface
`PE1(config-if)#exit`	Exit interface mode
`PE1(config)#router ospf 100`	Configure the routing process and specify the Process ID (100)
`PE1(config-router)#network 10.10.10.0/24 area 0` `PE1(config-router)#network 1.1.1.1/32 area 0`	Define the interface on which OSPF runs and associate the area ID `(0)` with the interface
`PE1(config-router)#exit`	Exit configure mode
`PE1(config)#router ldp`	Enter router mode for LDP
`PE1(config-router)#exit`	Exit router mode for LDP
`PE1(config)#interface xe6`	Specify the interface (xe6)to be configured
`PE1(config-if)#label-switching`	Enabling label switching capability on router
`PE1(config-if)#enable-ldp ipv4`	Enabling ldp on interface
`PE1(config-if)#exit`	Exit interface mode
`PE1(config)#exit`	Exit configure mode

P

`P#configure terminal`	Enter configure mode.
`P(config)#interface lo`	Enter interface mode.
`P(config-if)#ip address 2.2.2.2/32`	Configure IP address for the loopback address
`P(config-if)#exit`	Exit interface mode
`P(config)#interface xe6`	Specify the interface `(xe6)` to be configured
`P(config-if)#ip address 10.10.10.2/24`	Configure IP address for the interface
`P(config-if)#no shutdown`	Administratively bringing up the interface
`P(config)#interface xe1`	Specify the interface `(xe1)` to be configured
`P(config-if)#ip address 20.20.20.1/24`	Configure IP address for the interface
`P(config)#router ospf 100`	Configure the routing process and specify the Process ID (100)

`P(config-router)#network 10.10.10.0/24 area 0`
`P(config-router)#network 20.20.20.0/24 area 0`
`P(config-router)#network 2.2.2.2/32 area 0`
	Define the interface on which OSPF runs and associate the area ID `(0)` with the interface

`P(config-router)#exit`	Exit router mode
`P(config)#router ldp`	Enter router mode for LDP
`P(config-router)#exit`	Exit router mode for LDP
`P(config)#interface xe6`	Specify the interface (xe6)to be configured
`P(config-if)#label-switching`	Enabling label switching capability on router
`P(config-if)#enable-ldp ipv4`	Enabling ldp on interface
`P(config)#interface xe1`	Specify the interface (xe1)to be configured
`P(config-if)#label-switching`	Enabling label switching capability on router
`P(config-if)#enable-ldp ipv4`	Enabling ldp on interface

`P(config-if)#exit`	Exit interface mode
`P(config)#exit`	Exit configure mode

PE2

`PE2#configure terminal`	Enter configure mode.
`PE2(config)#interface lo`	Enter interface mode.
`PE2(config-if)#ip address 3.3.3.3/32`	Configure IP address for the loopback address
`PE2(config-if)#exit`	Exit interface mode
`PE2(config)#interface xe1`	Specify the interface `(xe1)` to be configured
`PE2(config-if)#ip address 20.20.20.2/24`	Configure IP address for the interface
`PE2(config-if)#no shutdown`	Administratively bringing up the interface
`PE2(config-if)#exit`	Exit interface mode
`PE2(config)#router ospf 100`	Configure the routing process and specify the Process ID (100)
`PE2(config-router)#network 20.20.20.0/24 area 0` `PE2(config-router)#network 3.3.3.3/32 area 0`	Define the interface on which OSPF runs and associate the area ID `(0)` with the interface
`PE2(config)#router ldp`	Enter router mode for LDP
`PE2(config-router)#exit`	Exit router mode for LDP
`PE2(config)#interface xe1`	Specify the interface (xe1)to be configured
`PE2(config-if)#label-switching`	Enabling label switching capability on router
`PE2(config-if)#enable-ldp ipv4`	Enabling ldp on interface
`PE2(config-if)#exit`	Exit interface mode

CHAPTER 3 Virtual Private Wire Service Configuration

This chapter shows configurations for Virtual Private Wire Service (VPWS), where a point-to-point Layer 2 VPN service interconnects multiple Ethernet LANs across an MPLS backbone.

Overview

An MPLS Layer 2 Virtual Circuit (VC) is a point-to-point Layer 2 connection transported via MPLS on the service provider's network. The Layer 2 circuit is transported over a single Label Switched Path (LSP) tunnel between two Provider Edge (PE) routers.

The following diagram illustrates the configuration steps in this section. In this sample, the VC host devices, Host1 and Host2, are connected to the Provider Edge (PE) router PE-1; and Host3 and Host4 are connected to PE-2. The VC is established between PE-1 and PE-2. Interface eth2, on PE-1 and PE-2, is connected to the customer network; eth1, on PE-1 and PE-2, is connected to the MPLS cloud.

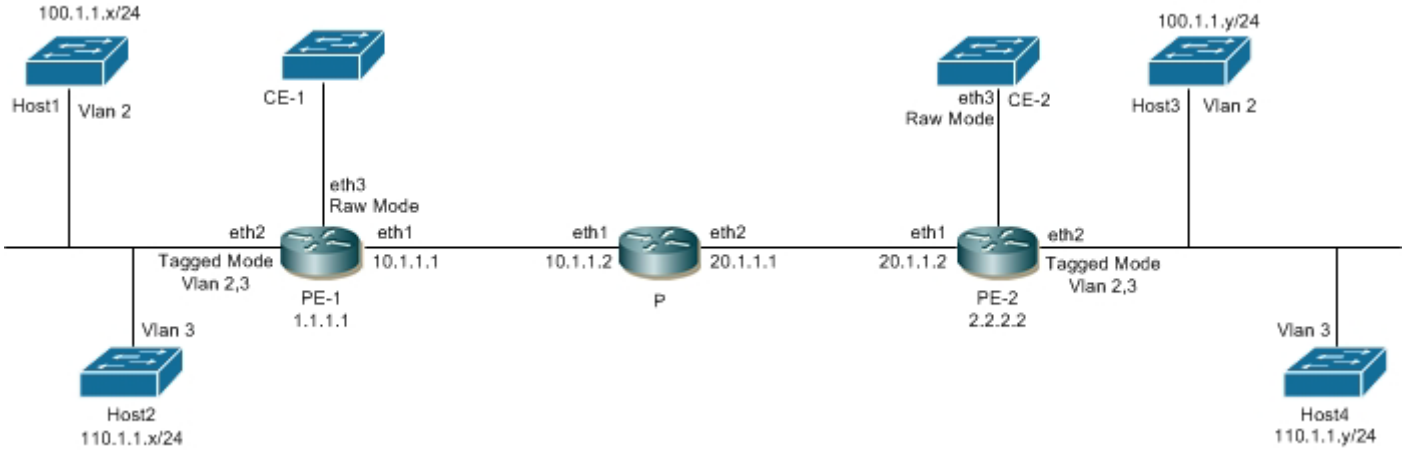


Figure 3-3: MPLS Layer 2 Virtual Circuit

The VC configuration process can be divided into the following steps:

Note: Loopback addresses being used should be advertised through OSPF, or should be statically routed.

1. Configure the IP address and OSPF for the PE-1, P (Provider), and PE-2 routers.
2. Configure MPLS and LDP on PE-1, P, and PE-2, and LDP targeted peer for the PE-1 and PE-2 routers. (If RSVP is used for configuring trunks, LDP must be configured on PE-1 and PE-2, and RSVP must be configured on PE-1, P, and PE-2.)
3. Configure the VC.
4. Bind the customer interface to the VC.

Configure IP Address and OSPF on Routers

Configure the IP addresses and OSPF on the PE-1, P, and PE-2 routers.

PE-1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Specify the loopback interface `(lo0)` to be configured.
`(config-if)#ip address 1.1.1.1/32 secondary`	Set the IP address of the loopback interface to `1.1.1.1/32`.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth1`	Specify the interface `(eth1)` to be configured.
`(config-if)#ip address 10.1.1.1/24`	Set the IP address of the interface to `10.1.1.1/24`.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 100`	Configure the routing process and specify the Process ID (100). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.1.1.0/24 area 0` `(config-router)#network 1.1.1.1/32 area 0`	Define the interface on which OSPF runs and associate the area ID `(0)` with the interface.

P

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Specify the loopback interface `(lo0)` to be configured.
`(config-if)#ip address 9.9.9.9/32 secondary`	Set the IP address of the loopback interface to `9.9.9.9/32`.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth1`	Specify the interface `(eth1)` to be configured.
`(config-if)#ip address 10.1.1.2/24`	Set the IP address of the interface to `10.1.1.2/24`.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Specify the interface `(eth2)` to be configured.
`(config-if)#ip address 20.1.1.1/24`	Set the IP address of the interface to `20.1.1.1/24`.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 100`	Configure the routing process and specify the Process ID (100). The Process ID should be a unique positive integer identifying the routing process.

`(config-router)#network 10.1.1.0/24 area 0`
`(config-router)#network 20.1.1.0/24 area 0`
`(config-router)#network 9.9.9.9/32 area 0`
	Define the interface on which OSPF runs and associate the area ID `(0)` with the interface.

PE-2

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Specify the loopback interface `(lo0)` to be configured.
`(config-if)#ip address 2.2.2.2/32 secondary`	Set the IP address of the loopback interface to `2.2.2.2/32`.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth1`	Specify the interface `(eth1)` to be configured.
`(config-if)#ip address 20.1.1.2/24`	Set the IP address of the interface to `20.1.1.2/24`.

`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 100`	Configure the routing process and specify the Process ID (100). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 20.1.1.0/24 area 0` `(config-router)#network 2.2.2.2/32 area 0`	Define the interface on which OSPF runs, and associate the area ID `(0)` with the interface.

Configure MPLS, LDP, and LDP Targeted Peer on Routers

Configure MPLS and LDP on PE-1, P, and PE-2, and LDP targeted peers on PE-1 and PE-2.

Note: If RSVP is used for configuring trunks, LDP must be configured on PE-1 and PE-2, and RSVP must be configured on PE-1, P, and PE-2,

PE-1

`#configure terminal`	Enter configure mode.
`(config)#router ldp`	Enter the `Router` mode.
`(config-router)#transport-address ipv4 1.1.1.1`	Configure the transport address to be used for a TCP session over which LDP will run on an IPv4 interface.
`(config-router)#targeted-peer ipv4 2.2.2.2`	Specify the targeted LDP peer on PE-1.
`(config-router-targeted-peer)# exit`	Exit the Router targeted peer mode.
`(config-router)#exit`	Exit the `Router` mode.
`(config)#interface eth1`	Specify the interface `(eth1)` to be configured.
`(config-if)#label-switching`	Enable label switching on interface `eth1`.
`(config-if)#enable-ldp ipv4`	Enable LDP on interface `eth1`.

P

`#configure terminal`	Enter configure mode.
`(config)#router ldp`	Enter the `Router` mode.
`(config-router)#transport-address ipv4 9.9.9.9`	Configure the transport address to be used for a TCP session over which LDP will run on an IPv4 interface.
`(config-router)#exit`	Exit the `Router` mode.
`(config)#interface eth1`	Specify the interface `(eth1)` to be configured.
`(config-if)#label-switching`	Enable label switching on interface `eth2`.
`(config-if)#enable-ldp ipv4`	Enable LDP on interface `eth2`.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Specify the interface `(eth2)` to be configured.
`(config-if)#label-switching`	Enable label switching on interface `eth2`.
`(config-if)#enable-ldp ipv4`	Enable LDP on interface `eth2`.

PE-2

`#configure terminal`	Enter configure mode.
`(config)#router ldp`	Enter the Router mode.
`(config-router)#transport-address ipv4 2.2.2.2`	Configure the transport address to be used for a TCP session over which LDP will run on an IPv4 interface.
`(config-router)#targeted-peer ipv4 1.1.1.1`	Specify the targeted LDP peer on PE-2.
`(config-router-targeted-peer)# exit`	Exit the Router targeted peer mode.
`(config-router)#exit`	Exit the Router mode.
`(config)#interface eth1`	Specify the interface(eth1) to be configured.
`(config-if)#label-switching`	Enable label switching on interface eth1.
`(config-if)#enable-ldp ipv4`	Enable LDP on interface eth1.

Configure VC

Configure the VC. Each VC ID uniquely identifies the Layer-2 circuit among all the Layer-2 circuits.

Note: Both PE routers (endpoints) must be configured with the same VC-ID (`100` in this example).

PE-1

`#configure terminal`	Enter configure mode.
`(config)#mpls l2-circuit t1 100 2.2.2.2`	Configure the VC for PE-2. In this example, `t1` is the VC name, `100` is the VC ID, and `2.2.2.2` is the VC endpoint IP address.

PE-2

`#configure terminal`	Enter configure mode.
`(config)#mpls l2-circuit t1 100 1.1.1.1`	Configure the VC for PE-1. In this example, `t1` is the VC name, `100` is the VC ID, and `1.1.1.1` is the VC endpoint IP address.

Bind Customer Interface to VC

Bind the customer interface to the VC using one of the two procedures described below: Layer-2 untagged traffic or Layer-2 tagged traffic.

Note: Layer 2 VCs can only be bound to Layer 2 interfaces. The VC encapsulation method should be Ethernet (default), VLAN.

Layer 2 Untagged Traffic

Use Access mode for Layer 2 untagged traffic.

PE-1

`#configure terminal`	Enter configure mode.
`(config)#service-template SUT1`	Create a service template SUT1
`(config-svc)#match untagged`	Allow untagged traffic.
`(config-svc)#exit`	Exit the service template mode
`(config)#interface eth3`	Specify the interface (eth3) to be configured.
`(config-if)#switchport`	Switch to Layer-2 mode.
`(config-if)#mpls-l2-circuit t1 service-template SUT1`	Bind the interface to the VC with service template.

PE-2

`#configure terminal`	Enter configure mode.
`(config)#service-template SUT1`	Create a service template SUT1
`(config-svc)#match untagged`	Allow untagged traffic.
`(config-svc)#exit`	Exit the service template mode
`(config)#interface eth3`	Specify the interface (eth3) to be configured.
`(config-if)#switchport`	Switch to Layer-2 mode.
`(config-if)#mpls-l2-circuit t1 service-template SUT1`	Bind the interface to the VC with service template.

Layer 2 Tagged Traffic

Use Trunk mode for Layer-2 tagged traffic. The following configuration allows only VLAN 2 and 3 traffic.

PE-1

`#configure terminal`	Enter configure mode.
`(config)#mpls l2-circuit t2 200 2.2.2.2`	Configure the VC for PE-2. In this example, t2 is the VC name, 200 is the VC ID, and 2.2.2.2 is the VC endpoint IP address.
`(config-pseudowire)#exit`	Exit pseudowire config mode.
`(config)#service-template ST1`	Create a service template ST1
`(config-svc)#match outer-vlan 2`	Allow VLAN 2 traffic on this VC.
`(config-svc)#match outer-vlan 3`	Allow VLAN 3 traffic on this VC.
`(config-svc)#exit`	Exit the service template mode
`(config)#interface eth2`	Specify the interface (eth2) to be configured.
`(config-if)#switchport`	Switch to Layer-2 mode.
`(config-if)#mpls-l2-circuit t2 service-template ST1`	Bind the interface to the VC with service template.

PE-2

`#configure terminal`	Enter configure mode.
`(config)#mpls l2-circuit t2 200 1.1.1.1`	Configure the VC for PE-2. In this example, t2 is the VC name, 200 is the VC ID, and 1.1.1.1 is the VC endpoint IP address.
`(config-pseudowire)#exit`	Exit pseudowire config mode.
`(config)#service-template ST1`	Create a service template ST1
`(config-svc)#match outer-vlan 2`	Allow VLAN 2 traffic on this VC.
`(config-svc)#match outer-vlan 3`	Allow VLAN 3 traffic on this VC.
`(config-svc)#exit`	Exit the service template mode
`(config)#interface eth2`	Specify the interface (eth2) to be configured.
`(config-if)#switchport`	Switch to Layer-2 mode.
`(config-if)#mpls-l2-circuit t2 service-template ST1`	Bind the interface to the VC with service template.

Validation

Use the show ldp mpls-l2-circuit (Control Plane) command, and the show mpls vc-table (Forwarding Plane) command, to display complete information about the Layer 2 VC.

If the VC State is UP in the output from the show ldp mpls-l2 circuit command, and the Status is Active in the output of the show mpls vc-table command, a ping from CE1 to CE2 should be successful.

```
#show ldp mpls-l2-circuit
Transport    Client       VC       Trans    Local       Remote        Destination
VC ID        Binding      State    Type     VC Label    VC Label      Address
100          eth3         UP   Ethernet VLAN 24320       24321         2.2.2.2
200          eth2         UP   Ethernet VLAN 24321       24322         2.2.2.2


#show mpls vc-table
VC-ID      Vlan-ID  Inner-Vlan-ID  Access-Intf   Network-Intf  Out Label  Tunnel-Label
Nexthop         Status
100         N/A      N/A           eth3          eth6          24321      24320
2.2.2.2         Active
200         N/A      N/A           eth2          eth6          24322      24320
2.2.2.2         Active
#
```

These additional commands can also be used to display information about the Layer 2 virtual circuits.

```
show ldp mpls-l2-circuit detail
show ldp mpls-l2-circuit VC-ID
show ldp mpls-l2-circuit VC-ID detail
show mpls l2-circuit
```

Configure a Static Layer-2 VC

For a static MPLS Layer 2 VC configuration:

1. Configure the VC with the manual option
2. Configure the VC FIB entry
3. Bind the VC; all steps are in the configurations that follow.

PE-1

`#configure terminal`	Enter configure mode.
`PE1(config)#mpls l2-circuit t3 300 2.2.2.2 manual`	Configure the VC ID with the manual option (no signaling used).
`PE1(config-pseuodwire)#manual-pseudowire`	Configure pseudowire manual (no signaling)
`PE1(config-pseudowire)#exit`	Exit pseudowire config mode.
`PE1(config)#service-template ST3`	Create a service template ST3
`PE1(config-svc)#exit`	Exit the service template mode
`PE1(config)#interface eth2`	Add an FTN entry; where 1000 is the incoming label, 2000 is the outgoing label, 2.2.2.2 is the endpoint, eth1 is the incoming interface name, and eth2 is outgoing interface name.
`PE1(config-if)#mpls-l2-circuit t2 service-template ST3`	Bind the interface to the VC with service template.
`PE1(config-if)#exit`	Exit interface mode
`PE1(config)#mpls l2-circuit-fib-entry 300 1000 2000 2.2.2.2 eth1 eth2`	Configure the VC ID with the manual option (no signaling used).

PE-2

`#configure terminal`	Enter configure mode.
`PE2(config)#mpls l2-circuit t3 300 1.1.1.1 manual`	Configure the VC ID with the manual option (no signaling used).
`PE2(config-pseuodwire)#manual-pseudowire`	Configure pseudowire manual (no signaling)
`PE2(config-pseudowire)#exit`	Exit pseudowire config mode.
`PE2(config)#service-template ST3`	Create a service template ST3
`(config-svc)#exit`	Exit the service template mode
`PE2(config)#interface eth2`	Add an FTN entry; where 2000 is the incoming label, 1000 is the outgoing label, 1.1.1.1 is the endpoint, eth1 is the incoming interface name, and eth 2 is outgoing interface name.
`PE2(config-if)#mpls-l2-circuit t2 service-template ST3`	Bind the interface to the VC with service template.
`PE2(config-if)#exit`	Exit interface mode.
`PE2(config)#mpls l2-circuit-fib-entry 300 2000 1000 1.1.1.1 eth1 eth2`	Configure the VC ID with the manual option (no signaling used).
`PE2(config)#end`	Exit configure mode

Validation

This example shows number of configured VCs and its status.

```
#show mpls vc-table count
 -------------------------------
  Num PWs      : 3
  Active PWs   : 3
  OAM-only PWs : 0
  Inactive PWs : 0
 -------------------------------

 #show ldp mpls-l2-circuit count
 ------------------------------------------------
 Num Signaled PWs: 3        [UP: 3]
 ------------------------------------------------
```

Service template Configuration

PE-1

`#configure terminal`	Enter configure mode.
`(config)#mpls l2-circuit vc1 10 2.2.2.2`	Configure the VC
`(config-pseudowire)#service-tpid dot1.ad`	Configure Service-TPID as dot1.ad (0x88a8)
`(config-pseudowire)#exit`	Exit pseudowire config mode.
`(config)# service-template template1`	Configure the service template.
`(config-svc)# match double-tag outer-vlan 204 inner-vlan 203`	Matching criteria for service template.
`(config-svc)#rewrite ingress pop outgoing-tpid dot1.ad`	Action performed for service template.
`(config-svc)#exit`	Exit configure SVC mode
`(config)#interface eth2`	Specify the interface `(eth2)` to be configured.
`(config-if)#switchport`	Switch to Layer-2 mode.
`(config-if)#switchport dot1q ethertype 0x88a8`	Configure interface ethertype as dot1.ad (0x88a8)
`(config-if)#mpls-l2-circuit vc1 service-template template1`	Bind the interface to the VC with service template.
`(config-if)#exit`	End of Interface and configurations mode.

PE-2

`(config)#mpls l2-circuit vc1 10 1.1.1.1`	Configure the VC.
`(config-pseudowire)#service-tpid dot1.ad`	Configure Service-TPID as dot1.ad (0x88a8)
`(config-pseudowire)#exit`	Exit pseudowire config mode.
`(config)# service-template template1`	Configure the service template.
`(config-svc)# match double-tag outer-vlan 204 inner-vlan 203`	Matching criteria for service template.
`(config-svc)# rewrite ingress pop outgoing-tpid dot1.ad`	Action performed for service template.
`(config-svc)#exit`	Exit configure SVC mode

`(config)#interface eth2`	Specify the interface `(eth2)` to be configured.
`(config-if)#switchport`	Switch to Layer-2 mode.
`(config-if)#switchport dot1q ethertype 0x88a8`	Configure interface ethertype as dot1.ad (0x88a8)
`(config-if)#mpls-l2-circuit vc1 service-template template1`	Bind the interface to the VC with service template.
`(config-if)#exit`	End of interface and configurations mode.

Validation

PE1

```
PE1#sh ldp mpls-l2-circuit detail
PW ID: 10, VC state is up
Access IF: eth2,up,AC state is up
Session IF: eth1, state is up
Destination: 2.2.2.2, Peer LDP Ident: 2.2.2.2
Local vctype: vlan, remote vctype :vlan
Local groupid: 0, remote groupid: 0
Local label: 24322, remote label: 52482
Local MTU: 1500, Remote MTU: 1500
Local Control Word: disabled  Remote Control Word: Not-Applicable  Current
use: disabled
Local PW Status Capability : disabled
Remote PW Status Capability : disabled
Current PW Status TLV : disabled


PE1#sh mpls l2-circuit detail
MPLS Layer-2 Virtual Circuit: vc1, id: 10  PW-INDEX: 1 service-tpid: dot1.ad
 Endpoint: 2.2.2.2
 Control Word: 0
 MPLS Layer-2 Virtual Circuit Group: none
 Bound to interface: eth2
 Virtual Circuit Type: Ethernet VLAN
 Virtual Circuit is configured as Primary
 Virtual Circuit is configured as Active
 Virtual Circuit is active
 Service-template : template1
  Match criteria : 204/203
  Action type : Pop
  Outgoing tpid : dot1.ad


PE1#sh mpls vc-table
VC-ID       Vlan-ID  Inner-Vlan-ID  Access-Intf   Network-Intf  Out Label
Tunnel-Label  Nexthop         Status
10          N/A      N/A           eth2          eth1           52482
52480         2.2.2.2         Active
```

Service-template with multiple match support

This is to validate the multiple match criteria support in a service template. When multiple match statements are configured only rewrite push is supported, rewrite translate and pop are not supported.

PE-1

`#configure terminal`	Enter configure mode.
`(config)#mpls l2-circuit t4 400 2.2.2.2`	Configure the VC for PE-1. In this example, t4 is the VC name, 400 is the VC ID, and 2.2.2.2 is the VC endpoint IP address.
`(config-pseudowire)#exit`	Exit pseudowire config mode.
`(config)#service-template template4`	Template configuration
`(config-svc)# match outer-vlan 700`	Allow VLAN 700 traffic on this VC
`(config-svc)# match double-tag outer-vlan 1200 inner-vlan 3200`	Allow double tag match with s+c tags
`(config-svc)# match untagged`	Allow untagged traffic
`(config-svc)# rewrite ingress push 300`	Push Action performed for service template
`(config)#interface eth2`	Specify the interface (eth2) to be configured.
`(config-if)#switchport`	Switch to Layer-2 mode.
`(config-if)#mpls-l2-circuit t4 service-template template4`	Bind the interface to the VC with service template.

PE-2

`#configure terminal`	Enter configure mode.
`(config)#mpls l2-circuit t4 400 1.1.1.1`	Configure the VC for PE-2. In this example, t4 is the VC name, 400 is the VC ID, and 1.1.1.1 is the VC endpoint IP address.
`(config-pseudowire)#exit`	Exit pseudowire config mode.
`(config)#service-template template4`	Template configuration
`(config-svc)# match outer-vlan 700`	Allow VLAN 700 traffic on this VC
`(config-svc)# match double-tag outer-vlan 1200 inner-vlan 3200`	Allow double tag match with s+c tags
`(config-svc)# match untagged`	Allow untagged traffic
`(config-svc)# rewrite ingress push 300`	Push Action performed for service template
`(config)#interface eth2`	Specify the interface (eth2) to be configured.
`(config-if)#switchport`	Switch to Layer-2 mode.
`(config-if)#mpls-l2-circuit t4 service-template template4`	Bind the interface to the VC with service template.

Validation

```
PE1#sh ldp mpls-l2-circuit detail
PW ID: 400, VC state is up
Access IF: eth2,up,AC state is up
Session IF: eth1, state is up
```

```
Destination: 2.2.2.2, Peer LDP Ident: 2.2.2.2
Local vctype: vlan, remote vctype :vlan
Local groupid: 0, remote groupid: 0
Local label: 24324, remote label: 52485
Local MTU: 1500, Remote MTU: 1500
Local Control Word: disabled  Remote Control Word: Not-Applicable  Current use: disabled
Local PW Status Capability : disabled
Remote PW Status Capability : disabled
Current PW Status TLV : disabled


PE1#sh mpls l2-circuit detail
MPLS Layer-2 Virtual Circuit: t4, id: 400  PW-INDEX: 4 service-tpid: dot1.q

 Endpoint: 2.2.2.2
 Control Word: 0
 MPLS Layer-2 Virtual Circuit Group: none
 Bound to interface: eth2
 Virtual Circuit Type: Ethernet VLAN
 Virtual Circuit is configured as Primary
 Virtual Circuit is configured as Active
 Virtual Circuit is active
 Service-template : template4
  Match criteria : 700
 1200/3200
  untagged
  Action type : Push
  Action value : 300

PE1#show mpls vc-table
VC-ID       Vlan-ID  Inner-Vlan-ID  Access-Intf   Network-Intf  Out Label  Tunnel-Label  Nexthop         Status     Ecmp-Group
400         N/A      N/A            eth2           eth1          24322      24320         2.2.2.2           Active     N/A


PE2#show mpls vc-table
VC-ID       Vlan-ID  Inner-Vlan-ID  Access-Intf   Network-Intf  Out Label  Tunnel-Label  Nexthop         Status     Ecmp-Group
400         N/A      N/A            eth2           eth1          24321      24325         1.1.1.1           Active     N/A
```

CHAPTER 4 MPLS Layer-3 VPN Configurations

This chapter contains configurations for MPLS Layer-3 Virtual Private Networks (VPNs).

Overview

The MPLS Layer-3 VPN solution provides address space and routing separation via the use of per-VPN Routing and Forwarding tables (VRFs), and MPLS switching in the core and at the edge of the network. VPN customer routing data is imported into the VRFs utilizing the Route Target BGP extended community. This routing data is identified by a Route Distinguisher (RD) and is distributed among Provider Edge (PE) routers using Multi-Protocol BGP extensions.

Terminology

The following illustrates a Virtual Private Network in a CConnect Service Provider Network. This illustration corresponds to the terms defined in this subsection.

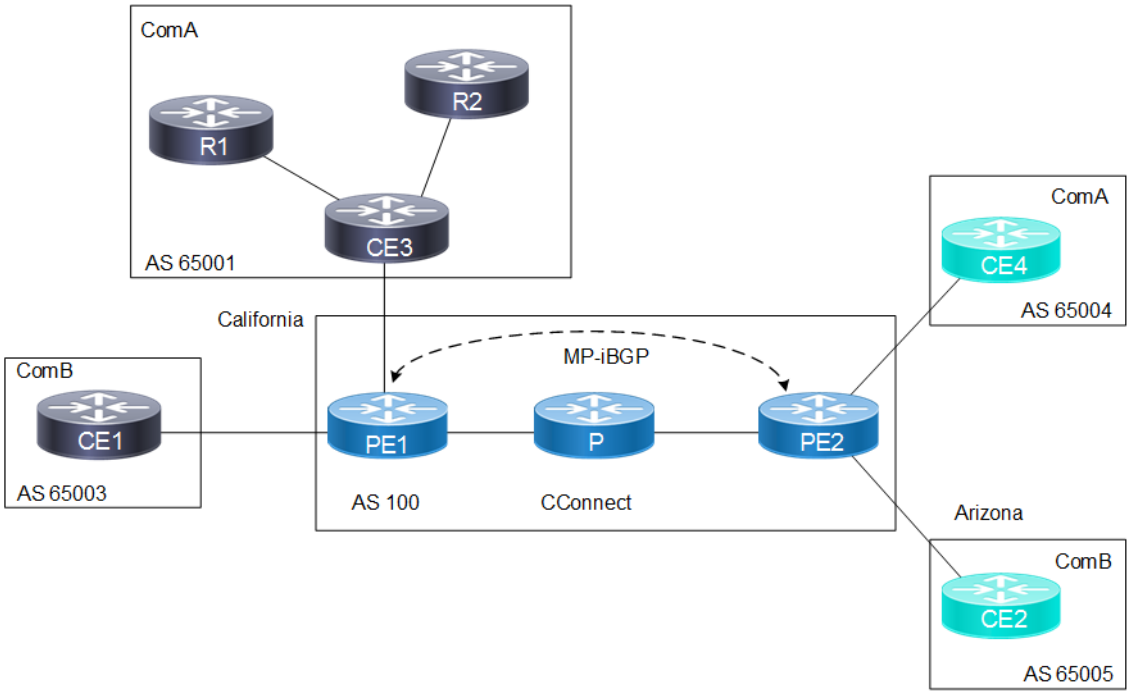


Figure 4-4: CConnect Provider with ComA and ComB Customers

Service Provider. The organization that owns the infrastructure that provides leased lines to customers, offering them. a Virtual Private Network Service. In the above illustration, CConnect is the service provider providing services to clients ComA and ComB.

Customer Edge (CE) Router. A router at a customer's site that connects to the Service Provider via one or more . Provider Edge routers. In the above illustration, CE1, CE2, CE3 and CE4 are all CE routers connected directly to the CConnect network.

Provider Edge (PE) Router. A provider's router connected to a CE router through a leased line or dial-up connection.. In the above illustration, PE1 and PE2 are the PE routers, because they link the CConnect service provider to its clients.

Provider Core Router (P). The devices in the core of the service provider network, which are generally not Provider Edge routers. In the above illustration, the P router is the Provider device, not connected to any customer, and is the core of the CConnect network.

Site. A contiguous part of the customer network. A site connects to the provider network through transmission lines, using a CE and PE router. In the above illustration, R1, R2 and CE3 comprise a Customer network, and are seen as a single site by the CConnect network.

Customer Router. In the illustration above, R1 and R2 are the Customer routers, and are not directly connected to the CConnect network.

The VPN Routing Process

The OcNOS MPLS-VPN Routing process follows these steps:

1. Service Providers provide VPN services from PE routers that communicate directly with CE routers via an Ethernet Link.
2. Each PE router maintains a Routing and Forwarding table (VRF) for each customer. This guarantees isolation, and allows the usage of uncoordinated private addresses. When a packet is received from the CE, the VRF that is mapped to that site is used to determine the routing for the data. If a PE has multiple connections to the same site, a single VRF is mapped to all of those connections.
3. After the PE router learns of the IP prefix, it converts it into a VPN-IPv4 prefix by prepending it with an 8-byte Route Distinguisher (RD). The RD ensures that even if two customers have the same address, two separate routes to that address can be maintained. These VPN-IPv4 addresses are exchanged between the PE routers through MP-BGP.
4. A unique Router ID (usually the loopback address) is used to allocate a label, and enable VPN packet forwarding across the backbone.
5. Based on routing information stored in the VRF table, packets are forwarded to their destination using MPLS. Each PE router allocates a unique label to every route in each VRF (even if they have the same next hop), and propagates these labels, together with 12-byte VPN-IPv4 addresses, through Multi-Protocol BGP.
6. Ingress PE routers prepend a two-level label stack to the VPN packet, which is forwarded across the Provider network. This label stack contains a BGP-specific label from the VRF table (associated with the incoming interface), specifying the BGP next hop and an LDP-specific label from the global FTN table, specifying the IP next hop.
7. The Provider router in the network switches the VPN packet, based on the top label or the LDP-specific label in the stack. This top label is used as the key to lookup in the incoming interface's Incoming Labels Mapping table (ILM). If there is an outbound label, the label is swapped, and the packet is forwarded to the next hop; if not, the router is the penultimate router, and it pops the LDP-specific label, and forwards the packet with only the BGP-specific label to the egress PE router.
8. The egress PE router pops the BGP-specific label, performs a single label lookup in the outbound interface, and sends the packet to the appropriate CE router.

Configure MPLS Layer-3 VPN

The MPLS Layer-3 VPN configuration process can be divided into the following tasks

1. Establish connection between PE routers.
2. Configure PE1 and PE2 as iBGP neighbors.

3. Create VRF.
4. Associate interfaces to VRFs.
5. Configure VRF Route Destination and Route Targets.
6. Configure CE neighbor for the VPN.
7. Verify the MPLS to VPN configuration.

Topology

In this example, the CConnect MPLS-VPN backbone has two customers — ComA and ComB. Both customers have sites in California and Arizona. The following topology shows BGP4 address assignment between PE and CE routers. The steps that follow provision a customer VPN service across the MPLS-VPN backbone.

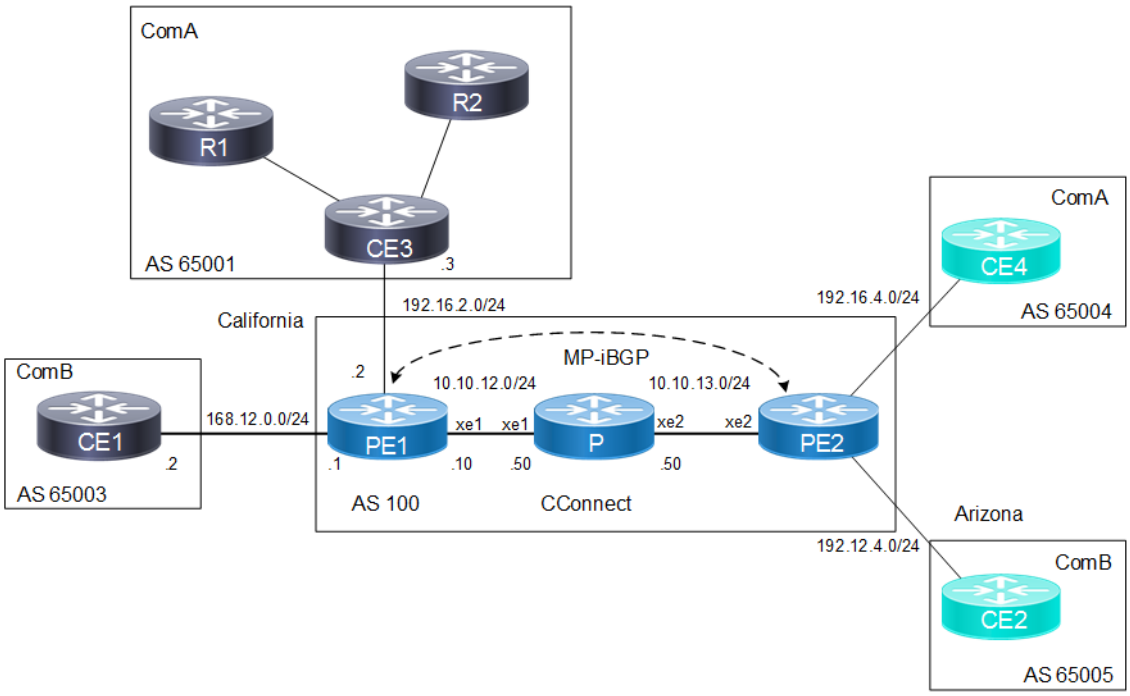


Figure 4-5: Connect Sample Topology

To establish this connection involves three steps:

1. Enable Label Switching

   This is a sample configuration to enable label switching for the Labeled Switched Path (LSP) between PE1 and PE2 (refer to Figure 4).

PE1

```
PE1(config)#interface xe1
PE1(config-if)#label-switching
!
```

P

```
P(config)#interface xe1
P(config-if)#label-switching
!
```

```
P(config)#interface xe2
P(config-if)#label-switching
!
```

PE2

```
PE2(config)#interface xe2
PE2(config-if)#label-switching
!
```

2. Enable IGP

   What follows is a sample configuration to establish connections between the two Provider Edge routers PE1 and PE2.

PE1

```
PE1(config)#router ospf 100
PE1(config-router)#network 10.10.12.0/24 area 0
!
```

P

```
P(config)#router ospf 100
P(config-router)#network 10.10.12.0/24 area 0
P(config-router)#network 10.10.13.0/24 area 0
!
```

PE2

```
PE2(config)#router ospf 100
PE2(config-router)#network 10.10.13.0/24 area 0
!
```

3. Enable Label Switching Protocol

   Label switching protocols are used to set up a Label-Switched Path (LSP) between PE routers. OcNOS supports LDP and RSVP-TE protocols for label switching. Enable either LDP or RSVP-TE.

   a. LDP

      This is a sample configuration to enable LDP on the whole path between PE1 and PE2 (see Figure 4-5).

PE1

```
PE1(config)#interface xe1
PE1(config-if)#enable-ldp ipv4
PE1(config-if)#exit
PE1(config)#ip prefix-list permit-any
PE1(config-ip-prefix-list)#seq 5 permit any
PE1(config-ip-prefix-list)#exit
PE1(config)#router ldp
PE1(config-router)#request-labels-for prefix-list-ipv4 permit-any
PE1(config-router)#advertisement-mode downstream-on-demand
PE1(config-router)#multicast-hellos
```

P

```
P(config)#interface xe1
P(config-if)#enable-ldp ipv4
P(config)#interface xe2
P(config-if)#enable-ldp
P(config-if)#exit
```

```
P(config)#ip prefix-list permit-any
P(config-ip-prefix-list)#seq 5 permit any
P(config-ip-prefix-list)#exit
P(config)#router ldp
P(config-router)#request-labels-for prefix-list-ipv4 permit-any
P(config-router)#advertisement-mode downstream-on-demand
P(config-router)#multicast-hellos
```

PE2

```
PE2(config)#interface xe2
PE2(config-if)#enable-ldp ipv4
PE2(config-if)#exit
PE2(config)#ip prefix-list permit-any
PE2(config-ip-prefix-list)#seq 5 permit any
PE2(config-ip-prefix-list)#exit
PE2(config)#router ldp
PE2(config-router)#request-labels-for prefix-list-ipv4 permit-any
PE2(config-router)#advertisement-mode downstream-on-demand
```

b. RSVP-TE

This is a sample configuration to enable RSVP-TE along the entire path between PE1 and PE2 (see Figure 4-5).

PE1

```
PE1(config)#router rsvp
!
PE1(config)#rsvp-path p1 mpls
PE1(config-path)#10.10.12.50 loose
!
PE1(config)#rsvp-trunk t1
PE1(config-rsvp)#primary path p1
PE1(config-rsvp)#from 2.2.2.2
PE1(config-rsvp)#to 3.3.3.3
!
PE1(config)#interface eth1
PE1(config-if)#enable-rsvp
```

P

```
P(config)#router rsvp
!
P(config)#interface xe1
P(config-if)#enable-rsvp
!
P(config)#interface xe2
P(config-if)#enable-rsvp
!
```

PE2

```
PE2(config)#router rsvp
!
PE2(config)#rsvp-trunk t1
PE2(config-rsvp)#from 3.3.3.3
PE2(config-rsvp)#to 2.2.2.2
!
```

```
PE2(config)#interface xe2
PE2(config-if)#enable-rsvp
```

Configure PEs as BGP Neighbors

BGP is the preferred protocol to transport VPN routes because of its multiprotocol capability and its scalability. Its ability to exchange information between indirectly connected routers supports keeping VPN routing information out of the Provider (P) routers. The P routers carry information as an optional BGP attribute. Additional attributes are transparently forwarded by any P router. The MPLS-VPN forwarding model does not require the P routers to make routing decisions based on VPN addresses: They forward packets based on the label value attached to the packet. The P routers do not require a VPN configuration in order to carry this information.

PE1

```
PE1(config)#interface lo
PE1(config-if)#ip address 2.2.2.2/32 secondary
```

PE2

```
PE2(config)#interface lo
PE2(config-if)#ip address 3.3.3.3/32 secondary
!
```

PE1

```
PE1#configure terminal
PE1(config)#router bgp 100
PE1(config-router)#neighbor 3.3.3.3 remote-as 100
PE1(config-router)#neighbor 3.3.3.3 update-source 2.2.2.2
!
PE1(config-router)#address-family vpnv4 unicast
PE1(config-router-af)#neighbor 3.3.3.3 activate
!
```

PE2

```
PE2(config)#router bgp 100
PE2(config-router)#neighbor 2.2.2.2 remote-as 100
PE2(config-router)#neighbor 2.2.2.2 update-source 3.3.3.3
!
!
PE2(config-router)#address-family vpnv4 unicast
PE2(config-router-af)#neighbor 2.2.2.2 activate
!
```

Create VRF

Each PE router in the MPLS-VPN backbone is attached to a site that receives routes from a specific VPN, so the PE router must have the relevant Virtual Routing and Forwarding (VRF) configuration for that VPN.

This command creates a VRF RIB (Routing Information Base), assigns a VRF-ID, and switches the command mode to `vrf` mode. The following example creates a VRF named `ComB`.

```
(config)#ip vrf ComB
(config-vrf)#
```

Associate Interfaces to VRFs

After the VRFs are defined on the PE router, the PE router needs to recognize which interfaces belong to which VRF. The VRF is populated with routes from connected sites. More than one interface can belong to the same VRF.

In the following example, interface `eth1` is associated with the VRF named `ComB`.

```
(config)#interface eth1
(config-if)#ip vrf forwarding ComB
```

Configure VRF—RD and Route Targets

After the VRF is created, configure Router Distinguishers and the Route Targets.

Configure Route Distinguishers

Route Distinguishers (RDs) make all customer routes unique. The routes must be unique, so that Multi-Protocol BGP treats the same prefix from two different VPNs as non-comparable routes. To configure RDs, a sequence of 64 bits is prepended to the IPv4 address in the Multi-Protocol BGP update. BGP considers two IPv4 addresses with different RDs as non-comparable, even if they have the same address and mask.

Assign a particular value to the RD for each VRF on the PE router. To display the routing table for a VRF, use the `show ip route vrf` command.

The following example shows adding an RD:

```
(config)#ip vrf ComB
(config-vrf)#rd 1:1
```

Configure Route Targets

Any routes learned from customers are advertised across the network through Multi-Protocol BGP, and any routes learned through Multi-Protocol BGP are added into the appropriate VRFs. The route target helps PE routers identify which VRFs should receive the routes.

The `route-target` command creates lists of import and export route-target extended communities for the VRF. It specifies a target VPN extended community. Execute the command once for each community. All routes with the specific route-target extended community are imported into all VRFs with the same extended community as an import route-target.

The following example demonstrates the route-target configuration for `ComB`.

```
bgpd(config)#ip vrf ComB
bgpd(config-vrf)#route-target both 100:1
```

Configure CE Neighbor for the VPN (Using BGP/ OSPF)

To provide a VPN service, the PE-router must be configured so that any routing information learned from a VPN customer interface can be associated with a particular VRF. This is achieved using any standard routing protocol process (OSPF, BGP or static routes etc). Use any one of the following configurations (BGP, or OSPF) to configure the CE neighbor.

Using BGP

The BGP sessions between PE and CE routers can carry different types of routes (VPN-IPv4, IPv4 routes). Address families are used to control the type of BGP session. Configure a BGP address family for each VRF on the PE-router, and a separate address family to carry VPN-IPv4 routes between PE routers. All non-VPN BGP neighbors are defined using the `IPv4 address` mode. Each VPN BGP neighbor is defined under its associated address family mode.

A separate address family entry is used for every VRF, and each address family entry can have multiple CE routers within the VRF.

The PE and CE routers must be directly connected for BGP4 sessions; BGP multihop is not supported between PE and CE routers.

The following example places the router in address family mode, and specifies company names, `ComA` and `ComB`, as the names of the VRF instance to associate with subsequent IPv4 address family configuration mode commands. This configuration is used when BGP is used for PE and CE.

PE1

```
PE1(config)#router bgp 100
PE1(config-router)#address-family ipv4 vrf ComA
PE1(config-router-af)#redistribute connected
PE1(config-router-af)#neighbor 192.16.2.3 remote-as 65001
PE1(config-router-af)#neighbor 192.16.2.3 activate
PE1(config-router-af)#exit-address-family
!
PE1(config-router)#address-family ipv4 vrf ComB
PE1(config-router-af)#neighbor 168.12.0.2 remote-as 65003
PE1(config-router-af)#neighbor 168.12.0.2 activate
```

PE2

```
PE2(config)#interface xe2
PE2(config-if)#ip address 25.25.25.1/24 secondary
PE2(config)#router bgp 100
PE2(config-router)#address-family ipv4 vrf ComA
PE2(config-router-af)#redistribute connected
PE2(config-router-af)#neighbor 192.16.4.3 remote-as 65004
PE2(config-router-af)#neighbor 192.16.4.3 activate
PE2(config-router-af)#exit-address-family
!
PE2(config-router)# address-family ipv4 vrf ComB
PE2(config-router-af)#neighbor 192.12.4.1 remote-as 65005
PE2(config-router-af)#neighbor 192.12.4.1 activate
```

CE1

BGP configuration on CE1

`configure terminal`	Enter configure mode
`(config)#interface xe48`	Enter interface mode for xe48
`(config-if)#exit`	Exit interface mode
`(config)#router bgp 65003`	Enter BGP router mode
`(config-router)#neighbor 168.12.0.1 remote-as 100`	Specify the neighbor of this device

CE2

BGP configuration on CE2

`configure terminal`	Enter configure mode
`(config)#interface xe23`	Enter interface mode for xe48

`(config-if)#exit`	Exit interface mode
`(config)#router bgp 65005`	Enter BGP router mode
`(config-router)#neighbor 192.12.4.1/24 remote-as 100`	Specify the neighbor of this device

Using OSPF

Unlike BGP, OSPF does not run different routing contexts within one process. Thus, for running OSPF between the PE and CE routers, configure a separate OSPF process for each VRF that receives VPN routes through OSPF. The PE router distinguishes routers belonging to a specific VRF, by associating a particular customer interface to a specific VRF and to a particular OSPF process.

To redistribute VRF OSPF routes into BGP, redistribute OSPF under the BGP VRF address family submode.

PE1

```
PE1(config)#router ospf 101 comA
PE1(config-router)#network 192.16.3.0/24 area 0
PE1(config-router)#redistribute bgp

PE1(config)#router ospf 102 comB
PE1(config-router)#network 168.12.0.2/24 area 0
PE1(config-router)#redistribute bgp

PE1(config)#router bgp 100
PE1(config-router)#address-family ipv4 vrf ComA
PE1(config-router-af)#redistribute ospf
!
PE1(config-router)#address-family ipv4 vrf ComB
PE1(config-router-af)#redistribute ospf
PE1(config-router-af)#redistribute rip
```

Verify the MPLS-VPN Configuration

Use the show ip bgp neighbor command to validate the neighbor session between the CE and the PE routers. Use the `show ip bgp vpnv4 all` command to display all the VRFs and the routes associated with them. The following is sample output for the above commands for the PE1, CE1 and PE2 routers (based on the topology in Figure 4-5).

```
PE1#show ip bgp neighbors
BGP neighbor is 3.3.3.3, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 2.2.2.2, remote router ID 3.3.3.3
  BGP state = Established, up for 00:03:17
  Last read 00:00:17, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family VPNv4 Unicast: advertised and received
  Received 96 messages, 1 notifications, 0 in queue
  Sent 97 messages, 1 notifications, 0 in queue
  Route refresh request: received 0, sent 1
  Minimum time between advertisement runs is 5 seconds
  Update source is 2.2.2.2
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
```

```
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 For address family: VPNv4 Unicast
  BGP table version 4, neighbor version 4
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  2 accepted prefixes
  1 announced prefixes

 Connections established 3; dropped 2
Local host: 2.2.2.2, Local port: 54005
Foreign host: 3.3.3.3, Foreign port: 179
Nexthop: 2.2.2.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:03:42, due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)

BGP neighbor is 168.12.0.2, vrf ComB, remote AS 65003, local AS 100, external
link
  BGP version 4, local router ID 168.12.0.1, remote router ID 168.12.0.2
  BGP state = Established, up for 00:33:42
  Last read 00:00:12, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 70 messages, 1 notifications, 0 in queue
  Sent 75 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (standard)
  0 accepted prefixes
  3 announced prefixes

 Connections established 1; dropped 0
Local host: 168.12.0.1, Local port: 48102
Foreign host: 168.12.0.2, Foreign port: 179
Nexthop: 168.12.0.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:33:47, due to BGP Notification received
Notification Error Message: (OPEN Message Error/Bad BGP Identifier.)


CE1#show ip bgp neighbors
BGP neighbor is 168.12.0.1, remote AS 100, local AS 65003, external link
  BGP version 4, local router ID 168.12.0.2, remote router ID 168.12.0.1
  BGP state = Established, up for 00:34:03
  Last read 00:00:03, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
```

```
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 75 messages, 0 notifications, 0 in queue
  Sent 125 messages, 1 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 5, neighbor version 5
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  3 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 168.12.0.2, Local port: 179
Foreign host: 168.12.0.1, Foreign port: 48102
Nexthop: 168.12.0.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:34:03, due to BGP Notification sent
Notification Error Message: (OPEN Message Error/Bad BGP Identifier.)


PE1#show ip bgp vpnv4 all
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf      Weight Path
Route Distinguisher: 1:1 (Default for VRF ComB)
*>i  25.25.25.0/24    3.3.3.3              0         100           0        ?
*>   168.12.0.0/24    0.0.0.0             0         100          32768    ?
*>i  192.12.4.0       3.3.3.3              0         100           0        ?
 Announced routes count = 1
 Accepted routes count = 2
Route Distinguisher: 1:1
*>i  25.25.25.0/24    3.3.3.3              0         100           0        ?
*>i  192.12.4.0       3.3.3.3              0         100           0        ?
 Announced routes count = 0
 Accepted routes count = 2


PE2#show ip bgp vpnv4 all
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf      Weight Path
Route Distinguisher: 1:1 (Default for VRF ComB)
*>   25.25.25.0/24    0.0.0.0             0         100          32768    ?
*>i  168.12.0.0/24    2.2.2.2              0         100           0        ?
*>   192.12.4.0       0.0.0.0             0         100          32768    ?
 Announced routes count = 2
 Accepted routes count = 1
```

```
Route Distinguisher: 1:1
*>i  168.12.0.0/24    2.2.2.2              0         100           0        ?
 Announced routes count = 0
 Accepted routes count = 1
PE2#


CE1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
B     25.25.25.0/24 [20/0] via 168.12.0.1, xe48, 00:12:45
C     127.0.0.0/8 is directly connected, lo, 02:43:20
C     168.12.0.0/24 is directly connected, xe48, 02:18:21
B     192.12.4.0/24 [20/0] via 168.12.0.1, xe48, 00:12:45

Gateway of last resort is not set
```

Verify MPLS-L3 VPN VRF Ping and Traceroute

Use the `ping mpls l3vpn` command for the below requirements:

- PE to PE L3VPN ping via VRF
- PE to remote CE Ping via the VRF
- CE to remote PE ping (to the VRF interface facing its customer edge).
- Trace route from PE to PE via VRF
- Trace route from PE to remote CE via VRF
- Commands for ipv6 ping and trace route

1. PE to PE L3VPN Ping via VRF:

```
PE2#ping 168.12.0.1 vrf ComB
Press CTRL+C to exit
PING 168.12.0.1 (168.12.0.1) 56(84) bytes of data.
64 bytes from 168.12.0.1: icmp_seq=1 ttl=64 time=0.695 ms

#
```

2. PE to remote CE Ping via VRF:

```
PE2#ping 168.12.0.2 vrf ComB
Press CTRL+C to exit
PING 168.12.0.2 (168.12.0.2) 56(84) bytes of data.
64 bytes from 168.12.0.2: icmp_seq=1 ttl=63 time=0.776 ms

--- 168.12.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.776/0.776/0.776/0.000 ms
PE2#
```

```
PE2
```

3. CE to remote PE ping:

```
CE1#ping 168.12.0.1
Press CTRL+C to exit
PING 168.12.0.1 (168.12.0.1) 56(84) bytes of data.
64 bytes from 168.12.0.1: icmp_seq=160 ttl=254 time=0.606 ms
64 bytes from 168.12.0.1: icmp_seq=161 ttl=254 time=0.558 ms
64 bytes from 168.12.0.1: icmp_seq=162 ttl=254 time=0.568 ms
64 bytes from 168.12.0.1: icmp_seq=163 ttl=254 time=0.574 ms
64 bytes from 168.12.0.1: icmp_seq=164 ttl=254 time=0.609 ms

--- 168.12.0.2 ping statistics ---
5 packets transmitted, 5 received, 0 errors, 0% packet loss, time 163002ms
```

4. Trace Route from PE to PE via VRF

```
PE2#traceroute ip 168.12.0.1 vrf ComB
traceroute to 168.12.0.1 (168.12.0.1), 30 hops max, 60 byte packets
1168.12.0.1 (168.12.0.1)  0.706 ms  0.743 ms  0.989 ms
```

5. Trace Route from PE to Remote CE via VRF

```
PE2#traceroute ip 168.12.0.2 vrf ComB
traceroute to 168.12.0.2 (168.12.0.2), 30 hops max, 60 byte packets
 1  168.12.0.1 (168.12.0.1)  0.871 ms  1.006 ms  1.055 ms
2168.12.0.2 (168.12.0.2)  1.965 ms  2.045 ms  2.256 ms
```

6. Ping and Traceroute commands for ipv6

```
PE2#ping ipv6 <ipv6-addr> vrf ComB
      PE2#traceroute ipv6 <ipv6-addr> vrf ComB
```

CHAPTER 5 L3VPN GR Configuration

Using BGP graceful restart, the data-forwarding plane of a router can continue to process and forward packets even if the control plane - which is responsible for determining best paths - fails. Graceful restart also reduces routing flaps, which stabilizes the network and reduces the consumption of control-plane resources.

When the initial BGP connection is established then both the restarting router and its peers indicate their understanding of the BGP graceful restart mechanism by exchanging a new BGP capability (BGP capability code 64) in the initial BGP open messages that establish the session. The restarting router also provides to its peers a list of supported address-families (VPNv4, IPv4, IPV6) for which it has the capability to maintain forwarding state across a BGP restart.

When the router restarts its BGP process, the TCP connection to the peer router might be cleared. Under normal circumstances, this would cause the peer router to clear all routes associated with the restarting router. This does not occur with BGP graceful restart, however. Instead, the peer router marks all routes as "stale," but continues to use them to forward packets based on the expectation that the restarting router will re-establish the BGP session shortly. Likewise, the restarting router also continues forwarding packets in the interim.

When the restarting router opens the new BGP session, it will again send BGP capability 64 to its peers. But this time, flags will be set in the graceful restart capabilities exchange to let the peer router know that the BGP process has restarted.

BGP graceful restart was developed to minimize the duration and reach of an outage associated with a failed BGP process. To do so, the software extensions must be deployed on the router restarting the BGP process and on that router's BGP peers. The peers help the BGP process regain lost forwarding information and also help isolate failures from the rest of the network.

While continuing to forward packets, the peer router will refresh the restarting router with any relevant BGP routing information base (RIB) updates. The peer signals that it has finished sending the updates with an "End-of-RIB" (EOR) marker - an "empty" BGP update message. EOR markers help speed convergence because once the restarting router has received them from all peers; it knows it can begin best-path selection again using the new routing information. Similarly, the restarting router then sends any updates to its peer routers and uses the EOR marker to indicate the completion of the process.

As part of this feature, we will be extending the feature for VPNv4 AF.

Topology

In the below example shows to configure bgp vpnv4 neighborship between PE1 and PE2.

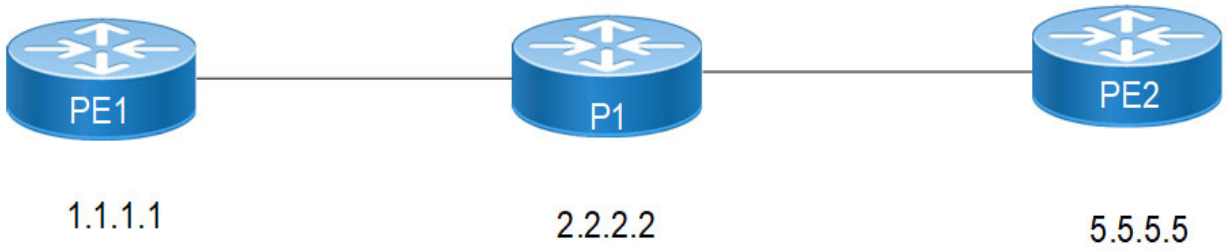


Figure 5-6: L3VPN GR Topology

L3VPN GR Configuration

Configuration

Below are the configurations and validations of L3VPN GR with OSPF as IGP. We can also configure ISIS as IGP and LDP/RSVP as transport.

PE1

`#configure terminal`	Enter configuration mode.
`(config)#interface lo`	Specify the loopback (lo) interface to be configured.
`(config-if)#ip address 1.1.1.1/32 secondary`	Set the IP address of the loopback interface to 1.1.1.1/32
`(config-if)#exit`	Exit interface mode.
`(config)#ip vrf l3vpn`	Ip vrf l3vpn
`(config-vrf)#rd 1:300`	Enter RD value
`(config-vrf)#route-target both 300:400`	Enter RT value
`(config-vrf)#exit`	Exiting from vrf mode
`(config)#router ldp`	Enter router mode for LDP.
`(config-router)#router-id 1.1.1.1`	Set the router ID to IP address 1.1.1.1
`(config-router)#exit`	Exit router mode
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip address 10.10.10.1/24`	Configure IPv4 address for eth1.
`(config-if)#label-switching`	Enable label switching on interface eth1.
`(config-if)#enable-ldp ipv4`	Enable LDP for IPv4 on eth1.
`(config-if)#exit`	Exit interface mode
`(config)#router ospf 1`	Configure the routing process and specify the Process ID 100. The Process ID should be a unique positive integer identifying the routing process.
`(config)#ospf router-id 1.1.1.1`	Configure OSPF router-ID same as loopback interface IP address
`(config-router) #network 1.1.1.1/32 area 0`	Define the interface on which OSPF runs and associate the area ID (0) with the interface
`(config-router) #network 10.10.10.0/24 area 0`	Define the interface on which OSPF runs and associate the area ID (0) with the interface
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 100`	Enter router bgp mode
`(config-router)#bgp router-id 1.1.1.1`	Configuring the bgp router id 1.1.1.1
`(config-router)# bgp graceful-restart restart-time 100`	Enable BGP GR with restart timer 100
`(config-router)# neighbor 5.5.5.5 remote-as 100`	Configure neighbor 5.5.5.5

(config-router)#neighbor 5.5.5.5 update-source lo	Update source lo for neighbor 5.5.5.5
(config-router)#address-family vpnv4 unicast	Entering Address family vpnv4 unicast
(config-router-af)# neighbor 5.5.5.5 activate	Activate the neighbor 5.5.5.5
(config-router-af)# neighbor 5.5.5.5 capability graceful-restart	Activate capability graceful restart for neighbor 5.5.5.5
(config-router-af)# exit-address-family	Exit address family
(config-router)# address-family ipv4 vrf l3vpn	Entering address family
(config-router-af)# redistribute connected	Redistribute connected
(config-router-af)#commit	Commit all the transactions

P1

#configure terminal	Enter configuration mode.
(config)#interface lo	Specify the loopback (lo) interface to be configured.
(config-if)#ip address 2.2.2.2/32 secondary	Set the IP address of the loopback interface to 2.2.2.2/32
(config-if)#exit	Exit interface mode.
(config)#router ldp	Enter router mode for LDP.
(config-router)#router-id 2.2.2.2	Set the router ID to IP address 2.2.2.2
(config-router)#transport-address ipv4 2.2.2.2 0	Configure the transport address for IPV4 (for IPV6 use ipv6) to be used for a TCP session over which LDP will run. Note: It is preferable to use the loopback address as the transport address.
(config-router)#exit	Exit-targeted-peer-mode
(config-if)#exit	Exit router mode
(config)#interface eth1	Enter interface mode.
(config-if)#ip address 10.10.10.2/24	Configure IPv4 address for eth1.
(config-if)#label-switching	Enable label switching on interface eth1.
(config-if)#enable-ldp ipv4	Enable LDP for IPv4 on eth1.
(config-if)#exit	Exit interface mode
(config)#interface eth2	Enter interface mode.
(config-if)#ip address 40.40.40.1/24	Configure IPv4 address for eth2
(config-if)#label-switching	Enable label switching on interface eth2.
(config-if)#enable-ldp ipv4	Enable LDP for IPv4 on eth2.
(config-if)#exit	Exit interface mode
(config)#router ospf 1	Configure the routing process and specify the Process ID • The Process ID should be a unique positive integer identifying the routing process.
(config)#ospf router-id 2.2.2.2	Configure OSPF router-ID same as loopback interface IP address

(config-router) #network 2.2.2.2/32 area 0	Define the interface on which OSPF runs and associate the area ID (0) with the interface
(config-router) #network 10.10.10.0/24 area 0	Define the interface on which OSPF runs and associate the area ID (0) with the interface
(config-router)#network 40.40.40.0/24 area 0	Define the interface on which OSPF runs and associate the area ID (0) with the interface
(config-router)#bfd all-interfaces	Enable the OSPF enabled interfaces with bfd
(config-if)#exit	Exit interface mode.

PE-2

#configure terminal	Enter configuration mode.
(config)#interface lo	Specify the loopback (lo) interface to be configured.
(config)#ip vrf l3vpn	Ip vrf l3vpn
(config-vrf)#rd 1:300	Enter RD value
(config-vrf)#route-target both 300:400	Enter RT value
(config-vrf)#exit	Exiting from vrf mode
(config-if)#ip address 5.5.5.5/32 secondary	Set the IP address of the loopback interface to 5.5.5.5/32
(config-if)#exit	Exit interface mode.
(config)#router ldp	Enter router mode for LDP.
(config-router)#router-id 5.5.5.5	Set the router ID to IP address 5.5.5.5
(config-router)#exit	Exit router mode
(config)#interface eth1	Enter interface mode.
(config-if)#ip address 40.40.40.2/24	Configure IPv4 address for eth1.
(config-if)#label-switching	Enable label switching on interface eth1.
(config-if)#enable-ldp ipv4	Enable LDP for IPv4 on eth1.
(config-if)#exit	Exit interface mode
(config-if)#exit	Exit interface mode
(config)#router ospf 1	Configure the routing process and specify the Process ID • The Process ID should be a unique positive integer identifying the routing process.
(config)#ospf router-id 5.5.5.5	Configure OSPF router-ID same as loopback interface IP address
(config-router) #network 5.5.5.5/32 area 0	Define the interface on which OSPF runs and associate the area ID (0) with the interface.
(config-router) #network 40.40.40.0/24 area 0	Define the interface on which OSPF runs and associate the area ID (0) with the interface.
(config-if)#exit	Exit interface mode.
(config)#router bgp 100	Enter router bgp mode
(config-router)#bgp router-id 5.5.5.5	Configuring the bgp router id 1.1.1.1
(config-router)# bgp graceful-restart restart-time 100	Enable BGP GR with restart timer 100

(config-router)# neighbor 1.1.1.1 remote-as 100	Configure neighbor 1.1.1.1
(config-router)#neighbor 1.1.1.1 update-source lo	Update source lo for neighbor 1.1.1.1
(config-router)#address-family vpnv4 unicast	Entering Address family vpnv4 unicast
(config-router-af)# neighbor 1.1.1.1 activate	Activate the neighbor 1.1.1.1
(config-router-af)# neighbor 1.1.1.1 capability graceful-restart	Activate capability graceful restart for neighbor 1.1.1.1
(config-router-af)# exit-address-family	Exit address family
(config-router)# address-family ipv4 vrf l3vpn	Entering address family
(config-router-af)# redistribute connected	Redistribute connected
(config-router-af)#commit	Commit all the transactions

Validation

Restart bgp gracefully:

PE1:

```
PE1#restart bgp graceful
%Warning : BGP process will stop and needs to restart manually,
You may lose bgp configuration,if not saved
Proceed for graceful restart? (y/n):y
%% Managed module is down or crashed

R1#sh mpls ilm-table
Codes: > - installed ILM, * - selected ILM, p - stale ILM
      K - CLI ILM, T - MPLS-TP, s - Stitched ILM
       S - SNMP, L - LDP, R - RSVP, C - CRLDP
       B - BGP , K - CLI , V - LDP_VC, I - IGP_SHORTCUT
       O - OSPF/OSPF6 SR, i - ISIS SR, k - SR CLI
       P - SR Policy, U - unknown

Code    FEC/VRF/L2CKT    ILM-ID     In-Label    Out-Label   In-Intf    Out-Intf/VRF
Nexthop                    LSP-Type
                          LSP_DEFAULT
   B> p 77.77.80.0/24      7          24323       Nolabel     N/A        l3vpn
N/A                        LSP_DEFAULT
   B> p 77.77.78.0/24      5          24321       Nolabel     N/A        l3vpn
N/A                        LSP_DEFAULT
   B> p 77.77.77.0/24      4          24320       Nolabel     N/A        l3vpn
N/A                        LSP_DEFAULT
   B> p 77.77.79.0/24      6          24322       Nolabel     N/A        l3vpn
N/A                        LSP_DEFAULT
   B> p 77.77.81.0/24      8          24324       Nolabel     N/A        l3vpn
N/A                        LSP_DEFAULT
   B> p 172.168.25.0/24    9          24325       Nolabel     N/A        l3vpn
N/A                        LSP_DEFAULT
```

```
   V    l2ckt:900         1          24960      Nolabel     po1        xe1             N/
A                      LSP_DEFAULT

PE1#sh mpls vrf-forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN, B - BGP FTN
(m) - Service mapped over multipath transport

Code    FEC                 FTN-ID    Tunnel-id   Pri   LSP-Type     Out-Label    Out-
Intf     Nexthop

  B> p 88.88.88.0/24      1        0          Yes   LSP_DEFAULT  24321       -
5.5.5.5
  B>p 88.88.89.0/24      2        0          Yes   LSP_DEFAULT  24321       -
5.5.5.5
   B> p 88.88.90.0/24      3        0          Yes   LSP_DEFAULT  24321       -
5.5.5.5
   B >p 88.88.91.0/24      4        0          Yes   LSP_DEFAULT  24321       -
5.5.5.5
   B >p 88.88.92.0/24      5        0          Yes   LSP_DEFAULT  24321       -
5.5.5.5
   B> p 172.168.26.0/24    6        0          Yes   LSP_DEFAULT  24321       -
5.5.5.5

PE1#sh nsm forwarding-timer
Protocol-Name  GR-State  Time Remaining (sec)   Disconnected-time
     BGP        ACTIVE            74           2022/01/13 16:33:43

PE# sh run bgp
!
PE1#sh ip bgp vpnv4 all
```

PE2:

```
PE2#sh ip bgp vpnv4 all
Status codes: s suppressed, d damped, h history, a add-path, * valid, > best, i -
internal, l - labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf      Weight Path
Route Distinguisher: 1:300 (Default for VRF l3vpn)
*>i  77.77.77.0/24    1.1.1.1              0        100       0   600 i
*>i  77.77.78.0/24    1.1.1.1              0        100       0   600 i
*>i  77.77.79.0/24    1.1.1.1              0        100       0   600 i
*>i  77.77.80.0/24    1.1.1.1              0        100       0   600 i
*>i  77.77.81.0/24    1.1.1.1              0        100       0   600 i
*> l 88.88.88.0/24    172.168.26.1         0        100       0   700 i
*> l 88.88.89.0/24    172.168.26.1         0        100       0   700 i
*> l 88.88.90.0/24    172.168.26.1         0        100       0   700 i
*> l 88.88.91.0/24    172.168.26.1         0        100       0   700 i
*> l 88.88.92.0/24    172.168.26.1         0        100       0   700 i
*>i  172.168.25.0/24  1.1.1.1              0        100       0    ?
```

```
*> l 172.168.26.0/24  0.0.0.0              0        100       32768  ?
 Announced routes count = 6
 Accepted routes count = 6
Route Distinguisher: 1:300
S>i  77.77.77.0/24    1.1.1.1              0        100       0   600 i
S>i  77.77.78.0/24    1.1.1.1              0        100       0   600 i
S>i  77.77.79.0/24    1.1.1.1              0        100       0   600 i
S>i  77.77.80.0/24    1.1.1.1              0        100       0   600 i
S>i  77.77.81.0/24    1.1.1.1              0        100       0   600 i
S>i  172.168.25.0/24  1.1.1.1              0        100       0    ?
 Announced routes count = 0
```

After restarting the bgp manually:

PE1:

```
PE1#start-shell
bash-5.0$ su
Password:
root@PE1:/home/ocnos# cd /usr/local/sbin/
root@PE1:/usr/local/sbin# ./bgpd -d

PE1#sh mpls ilm-table
Codes: > - installed ILM, * - selected ILM, p - stale ILM
      K - CLI ILM, T - MPLS-TP, s - Stitched ILM
       S - SNMP, L - LDP, R - RSVP, C - CRLDP
       B - BGP , K - CLI , V - LDP_VC, I - IGP_SHORTCUT
       O - OSPF/OSPF6 SR, i - ISIS SR, k - SR CLI
       P - SR Policy, U - unknown

Code    FEC/VRF/L2CKT    ILM-ID     In-Label    Out-Label   In-Intf    Out-Intf/VRF
Nexthop                    LSP-Type
   B> 77.77.80.0/24      7          24323       Nolabel     N/A        l3vpn           N/
A                        LSP_DEFAULT
   B> 77.77.78.0/24      5          24321       Nolabel     N/A        l3vpn           N/
A                        LSP_DEFAULT
   B> 77.77.77.0/24      4          24320       Nolabel     N/A        l3vpn           N/
A                        LSP_DEFAULT
   B> 77.77.79.0/24      6          24322       Nolabel     N/A        l3vpn           N/
A                        LSP_DEFAULT
   B> 77.77.81.0/24      8          24324       Nolabel     N/A        l3vpn           N/
A                        LSP_DEFAULT
   B> 172.168.25.0/24    9          24325       Nolabel     N/A        l3vpn           N/
A                        LSP_DEFAULT
   V    l2ckt:900         1          24960       Nolabel     po1        xe1             N/
A                        LSP_DEFAULT

PE1#sh mpls vrf-forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN, B - BGP FTN
(m) - Service mapped over multipath transport
```

```
Code    FEC                 FTN-ID    Tunnel-id   Pri   LSP-Type     Out-Label    Out-
Intf     Nexthop

  B>88.88.88.0/24       1         0          Yes   LSP_DEFAULT  24321        -
5.5.5.5
  B>88.88.89.0/24       2         0          Yes   LSP_DEFAULT  24321        -
5.5.5.5
   B>88.88.90.0/24       3         0          Yes   LSP_DEFAULT  24321        -
5.5.5.5
   B>88.88.91.0/24       4         0          Yes   LSP_DEFAULT  24321        -
5.5.5.5
   B>88.88.92.0/24       5         0          Yes   LSP_DEFAULT  24321        -
5.5.5.5
   B> 172.168.26.0/24     6         0          Yes   LSP_DEFAULT  24321        -
5.5.5.5
```

PE2:

```
PE2#sh ip bgp vpnv4 all
Status codes: s suppressed, d damped, h history, a add-path, * valid, > best, i -
internal, l - labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf      Weight Path
Route Distinguisher: 1:300 (Default for VRF l3vpn)
*>i 77.77.77.0/24    1.1.1.1               0        100        0   600 i
*>i 77.77.78.0/24    1.1.1.1               0        100        0   600 i
*>i 77.77.79.0/24    1.1.1.1               0        100        0   600 i
*>i 77.77.80.0/24    1.1.1.1               0        100        0   600 i
*>i 77.77.81.0/24    1.1.1.1               0        100        0   600 i
*> l 88.88.88.0/24    172.168.26.1          0        100        0   700 i
*> l 88.88.89.0/24    172.168.26.1          0        100        0   700 i
*> l 88.88.90.0/24    172.168.26.1          0        100        0   700 i
*> l 88.88.91.0/24    172.168.26.1          0        100        0   700 i
*> l 88.88.92.0/24    172.168.26.1          0        100        0   700 i
*>i 172.168.25.0/24 1.1.1.1              0        100        0  ?
*> l 172.168.26.0/24 0.0.0.0              0        100        32768 ?
 Announced routes count = 6
 Accepted routes count = 6
Route Distinguisher: 1:300
>i 77.77.77.0/24    1.1.1.1               0        100        0   600 i
>i 77.77.78.0/24    1.1.1.1               0        100        0   600 i
>i 77.77.79.0/24    1.1.1.1               0        100        0   600 i
>i 77.77.80.0/24    1.1.1.1               0        100        0   600 i
>i 77.77.81.0/24    1.1.1.1               0        100        0   600 i
>i 172.168.25.0/24 1.1.1.1              0        100        0    ?
 Announced routes count = 0
```

CHAPTER 6 6PE Configuration

This chapter explains about IPv6 islands over IPv4 MPLS using IPv6 Provider Edge Routers (6PE). With this technique, IPv6 islands are connected to each other across an IPv4 backbone enabled with MPLS label stacking while MP-BGP is used to announce the IPv6 routes across these MPLS tunnels. This feature can be implemented with label-switched paths (LSPs) using the Label Distribution Protocol (LDP) or Resource Reservation Protocol (RSVP).

This feature offers the following options to the service providers:

- Connect to other IPv6 networks accessible across the MPLS core.
- Provide access to IPv6 services and resources that service provider provides.
- Provide IPv6 VPN services without going for complete overhaul of existing MPLS/IPv4 core.

The 6PE uses the existing IPv4 MPLS core infrastructure for IPv6 transport. It enables IPv6 sites to communicate with each other over an IPv4 MPLS core network using MPLS label switched paths (LSPs). This feature relies heavily on multiprotocol Border Gateway Protocol (BGP) extensions in the IPv4 network configuration on the provider edge (PE) router to exchange IPv6 reachability information (in addition to an MPLS label) for each IPv6 address prefix. Edge routers are configured as dual-stack, running both IPv4 and IPv6, and use the IPv4 mapped IPv6 address for IPv6 prefix reachability exchange.

Benefits of 6PE

6PE offers the following benefits to service providers:

- Minimal operational cost and risk - No impact on existing IPv4 and MPLS services.
- Only provider edge routers require upgrade - A 6PE router can be an existing PE router or a new one dedicated to IPv6 traffic.
- No impact on IPv6 customer edge (CE) routers - The ISP can connect to any CE router running Static, IGP or EGP.
- Production services ready - An ISP can delegate IPv6 prefixes.
- IPv6 introduction into an existing MPLS service - 6PE routers can be added at any time.

IPv6 on Provider Edge Routers

The 6PE is a technique that provides global IPv6 reachability over IPv4 MPLS. It allows one shared routing table for all other devices. 6PE allows IPv6 domains to communicate with one another over the IPv4 without an explicit tunnel setup, requiring only one IPv4 address per IPv6 domain. While implementing 6PE, the provider edge routers are upgraded to support 6PE, while the rest of the core network is not touched (IPv6 unaware).

This implementation requires no re-configuration of core routers because forwarding is based on labels rather than on the IP header itself. This provides a cost-effective strategy for deploying IPv6.The IPv6 reachability information is exchanged by PE routers using multi-protocol Border Gateway Protocol (mp-iBGP) extensions. 6PE relies on mp-iBGP extensions in the IPv4 network configuration on the PE router to exchange IPv6 reachability information in addition to an MPLS label for each IPv6 address prefix to be advertised. PE routers are configured as dual stacks, running both IPv4 and IPv6, and use the IPv4 mapped IPv6 address for IPv6 prefix reachability exchange. The next hop advertised by the PE router for 6PE prefixes is still the IPv4 address that is used for IPv4 L3 VPN routes.

The following figure illustrates the 6PE topology.

Topology

As shown in Figure 6-7:

- CE1 and CE2 are customer edge routers
- 6PE1 and 6PE2 are IPv6 Provider Edge routers
- P is the router at the core of the IPv4 MPLS provider network

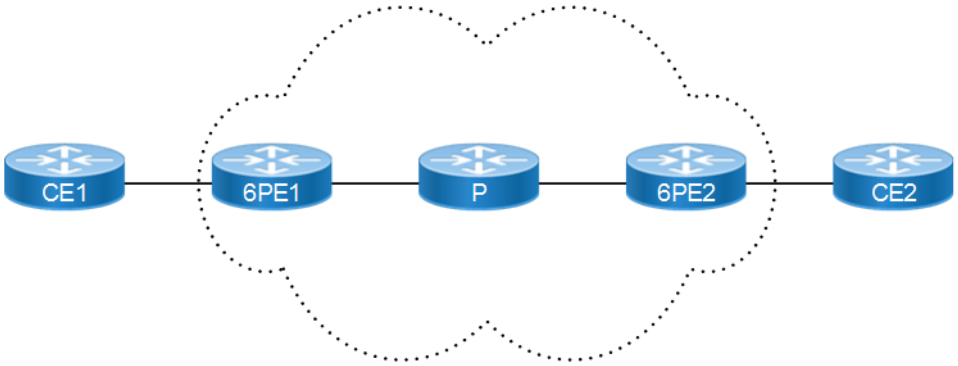


Figure 6-7: 6PE Configuration

Configuration

CE1

`#configure terminal`	Enter configure mode
`(config)#interface lo`	Enter interface mode
`(config-if)#ip address 44.44.44.44/32 secondary`	Assign the IPv4 address
`(config-if)#exit`	Exit interface mode
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 address 2001::2/64`	Assign the IPv6 address.
`(config-if)#exit`	Exit interface mode.
`(config)#router bgp 200`	Enter router BGP mode.
`(config-router)#bgp router-id 44.44.44.44`	Assign router ID
`(config-router)#neighbor 2001::1 remote-as 100`	Configure 6PE1 as an eBGP4+ neighbor.
`(config-router)#address-family ipv6 unicast`	Enter Address-Family IPv6 unicast mode
`(config-router-af)#redistribute static`	Redistribute static routes
`(config-router-af)# neighbor 2001::1 activate`	Activate the neighbor in the IPv6 address family
`(config-router-af)# exit-address-family`	Exit address family
`(config-router)#exit`	Exit BGP router mode
`(config)#ipv6 route 2ffe::/64 eth1`	Configure IPV6 static route

CE2

`#configure terminal`	Enter configure mode
`(config)#interface lo`	Enter interface mode

(config-if)#ip address 66.66.66.66/32 secondary	Assign the IPv4 address
(config-if)#exit	Exit interface mode
(config)#interface eth1	Enter Interface mode
(config-if)#ipv6 address 3002::2/64	Assign IPv6 address
(config-if)#exit	Exit interface mode
(config)#router bgp 300	Enter BGP configure mode
(config-router)#bgp router-id 66.66.66.66	Assign router ID
(config-router)# neighbor 3002::1 remote-as 100	Configure 6PE2 as an eBGP4+ neighbor.
(config-router)#address-family ipv6 unicast	Enter Address-Family IPv6 unicast mode
(config-router-af)#redistribute static	Redistribute static routes
(config-router-af)# neighbor 3002::1 activate	Activate the neighbor in the IPv6 address family.
(config-router-af)# exit-address-family	Exit address family
(config-router)#exit	Exit BGP router mode
(config)#ipv6 route 3ffe::/64 eth1	Configure IPV6 static route

PE1

#configure terminal	Enter configure mode
(config)#interface eth1	Enter Interface mode
(config-if)#ipv6 address 2001::1/64	Assign IPv6 address
(config-if)#exit	Exit interface mode
(config)#interface lo	Enter Interface mode
(config-if)#ip address 1.1.1.1/32 secondary	Assign the IP address to loopback interface
(config-if)#exit	Exit interface mode.
(config)#router ldp	Enter router ldp mode.
(config-router)#router-id 1.1.1.1	Configure router-id
(config-router)#explicit-null	Configure explicit-null.
(config-router)#exit	Exit LDP mode
(config)#interface eth2	Enter Interface mode
(config-if)# ip address 20.1.1.1/24	Assign IPv4 address
(config-if)#label-switching	Enable label switching in interface.
(config-if)#enable-ldp ipv4	Enable ldp in interface.
(config-if)#exit	Exit interface mode
(config)#router ospf	Enter router ospf mode.
(config-router)#ospf router-id 1.1.1.1	Configure ospf router id same as loopback ip address.
(config-router)#network 1.1.1.1/32 area 0 (config-router)#network 20.1.1.0/24 area 0	Define the network on which OSPF runs and associate area id.
(config-router)#exit	Exit from router ospf mode.
(config)#mpls label mode 6pe per-prefix	Change label mode to per-prefix, default is per VRF
(config)#router bgp 100	Enter BGP Configure mode.
(config-router)# bgp router-id 1.1.1.1	Configure BGP router-id

`(config-router)#neighbor 3.3.3.3 remote-as 100`	Configure 6PE2 as an iBGP peer.
`(config-router)#neighbor 3.3.3.3 update-source lo`	Update the source as loopback for iBGP peering with the remote 6PE router.
`(config-router)#neighbor 2001::2 remote-as 200`	Configure CE1 as eBGP peer
`(config-router)#address-family ipv4 unicast`	Enter address family mode
`(config-router-af)#neighbor 3.3.3.3 activate`	Activate neighbor
`(config-router-af)#exit`	Exit address family mode
`(config-router)#address-family ipv6 labeled-unicast`	Enter IPv6 labeled-unicast Address Family mode.
`(config-router-af)#neighbor 3.3.3.3 activate`	Activate the 6PE neighbor
`(config-router-af)#exit-address-family`	Exit IPv6 LU Address Family mode.
`(config-router)#address-family ipv6 unicast`	Enter the IPv6 address family
`(config-router-af)#neighbor 2001::2 activate`	Activate CE inside IPv6 address family
`(config-router-af)#redistribute connected`	Redistribute the connected routes
`(config-router-af)#exit-address-family`	Exit IPv6 Address Family mode.
`(config-router)#exit`	Exit Router mode.

P1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode
`(config-if)#ip address 2.2.2.2/32 secondary`	Assign the IP address to loopback interface
`(config-if)#exit`	Exit interface mode
`(config)#router ldp`	Enter router ldp mode.
`(config-router)#router-id 2.2.2.2`	Configure router-id
`(config-router)#exit`	Exit router ldp mode.
`(config)#router ospf`	Enter router ospf mode.
`(config-router)#ospf router-id 2.2.2.2`	Configure ospf router id same as loopback ip address.

`(config-router)#network 2.2.2.2/32 area 0`
`(config-router)#network 20.1.1.2/24 area 0`
`(config-router)#network 30.1.1.1/24 area 0`
	Define the network on which OSPF runs and associate area id.

`(config-router)#exit`	Exit from router ospf mode.
`(config)#interface eth1`	Enter Interface mode
`(config-if)# ip address 30.1.1.1/24`	Assign IPv4 address
`(config-if)#label-switching`	Enable label switching in interface.
`(config-if)#enable-ldp ipv4`	Enable ldp in interface.
`(config-if)#exit`	Exit interface mode
`(config)#interface eth2`	Enter Interface mode
`(config-if)# ip address 20.1.1.2/24`	Assign IPv4 address
`(config-if)#label-switching`	Enable label switching in interface.
`(config-if)#enable-ldp ipv4`	Enable ldp in interface.
`(config-if)#exit`	Exit interface mode

PE2

`#configure terminal`	Enter configure mode
`(config)#interface eth2`	Enter Interface mode
`(config-if)#ipv6 address 3002::1/64`	Assign IPv6 address
`(config-if)#exit`	Exit interface mode
`(config)#interface lo`	Enter Interface mode
`(config-if)#ip address 3.3.3.3/32 secondary`	Assign the IP address to loopback interface
`(config-if)#exit`	Exit interface mode.
`(config)#router ldp`	Enter router ldp mode.
`(config-router)#router-id 3.3.3.3`	Configure router-id
`(config-router)#explicit-null`	Configure explicit-null.
`(config-router)#exit`	Exit LDP mode
`(config)#interface eth1`	Enter Interface mode
`(config-if)# ip address 30.1.1.2/24`	Assign IPv4 address
`(config-if)#label-switching`	Enable label switching in interface.
`(config-if)#enable-ldp ipv4`	Enable ldp in interface.
`(config-if)#exit`	Exit interface mode
`(config)#mpls label mode 6pe per-prefix`	Change label mode to per-prefix, default is per VRF
`(config)#router bgp 100`	Enter router BGP mode.
`(config-router)#bgp router-id 3.3.3.3`	Configure BGP router id
`(config-router)#neighbor 1.1.1.1 remote-as 100`	Configure 6VPE2 as an iBGP peer.
`(config-router)#neighbor 1.1.1.1 update-source lo`	Update the source as loopback for iBGP peering with the remote 6VPE router.
`(config-router)#address-family ipv4 unicast`	Enter address family mode
`(config-router-af)#neighbor 1.1.1.1 activate`	Activate neighbor
`(config-router-af)#exit`	Exit address family mode
`(config-router)#neighbor 3002::2 remote-as 300`	Configure CE1 as eBGP peer
`(config-router)#address-family ipv6 labeled-unicast`	Enter IPv6 labeled-unicast Address Family mode.
`(config-router-af)#neighbor 1.1.1.1 activate`	Activate the 6PE neighbor
`(config-router-af)#exit-address-family`	Exit IPv6 LU Address Family mode.
`(config-router)#address-family ipv6 unicast`	Enter the IPv6 address family
`(config-router-af)#neighbor 3002::2 activate`	Activate CE inside IPv6 address family
`(config-router-af)#redistribute connected`	Redistribute the connected routes
`(config-router-af)#exit-address-family`	Exit IPv6 Address Family mode.
`(config-router)#exit`	Exit Router mode.
`(config)#router ospf`	Enter OSPF router mode
`(config-router)#network 3.3.3.3/32 area 0`	Enable OSPF with specified area ID on interfaces with IP address that matches the specified network address

(config-router)#network 30.1.1.0/24 area 0	Enable OSPF with specified area ID on interfaces with IP address that matches the specified network address
(config-router)#exit	Exit OSPF router mode

Validation

CE1

```
CE1#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, D- DHCP, R - RIP,
       O - OSPF, IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, i - IS-IS, B - BGP,
       v - vrf leaked
Timers: Uptime

IP Route Table for VRF "default"
C       ::1/128 via ::, lo, 01:10:32
C       2001::/64 via ::, eth1, 00:46:49
S       2ffe::/64 [1/0] via ::, eth1, 00:35:20
B       3002::/64 [20/0] via fe80::5054:ff:fe29:189d, eth1, 00:02:12
B       3ffe::/64 [20/0] via fe80::5054:ff:fe29:189d, eth1, 00:02:36
C       fe80::/64 via ::, eth3, 01:10:32
#

CE1#show ipv6 bgp summary
BGP router identifier 44.44.44.44, local AS number 200
BGP table version is 8
3 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
2001::1                  4   100   80        83      8      0      0  00:01:45
3

Total number of neighbors 1

Total number of Established sessions 1
```

PE1

```
PE1#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, D- DHCP, R - RIP,
       O - OSPF, IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, i - IS-IS, B - BGP,
       v - vrf leaked
Timers: Uptime
```

```
IP Route Table for VRF "default"
C       ::1/128 via ::, lo, 01:17:11
C       2001::/64 via ::, eth1, 00:40:22
B       2ffe::/64 [20/0] via fe80::5054:ff:fe60:f4e5, eth1, 00:02:37
B       3002::/64 [200/0] via ::ffff:3.3.3.3, 00:03:10
B       3ffe::/64 [200/0] via ::ffff:3.3.3.3, 00:01:07
C       fe80::/64 via ::, eth2, 01:17:11

PE1#show bgp ipv6
BGP table version is 5, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, a add-path, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop                    Metric    LocPrf     Weight Path
*> l 2001::/64        ::                             0        100      32768  ?
*> l 2ffe::/64        2001::2(fe80::5054:ff:fe60:f4e5)
                                                     0        100      0    200 ?
*>i  3002::/64        ::ffff:3.3.3.3                 0        100      0     ?
*>i  3ffe::/64        ::ffff:3.3.3.3                 0        100      0    300 ?

Total number of prefixes 4

PE1#show mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN,
       B - BGP FTN, K - CLI FTN, t - tunnel, P - SR Policy FTN,
       L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, I - IGP-Shortcut,
       U - unknown FTN, O - SR-OSPF FTN, i - SR-ISIS FTN, k - SR-CLI FTN

Code    FEC               FTN-ID    Nhlfe-ID  Tunnel-id   Pri   LSP-Type     Out-Label
Out-Intf    ELC   Nexthop
   L>   2.2.2.2/32          3         3         -           -     LSP_DEFAULT  3
eth2        No    20.1.1.2
   L>   3.3.3.3/32          4         4         -           -     LSP_DEFAULT  24321
eth2        No    20.1.1.2
   L>   30.1.1.0/24         5         3         -           -     LSP_DEFAULT  3
eth2        No    20.1.1.2
   B>   3002::/64           2         2         0           Yes   LSP_DEFAULT  24960
-           No    3.3.3.3
   B>   3ffe::/64           1         1         0           Yes   LSP_DEFAULT  24961
-           No    3.3.3.3

PE1#show ldp session
Peer IP Address           IF Name    My Role    State      KeepAlive  UpTime
30.1.1.1                  ce46       Passive   OPERATIONAL   30    00:10:11

PE1#show mpls ftn-table
 Primary FTN entry with FEC: 2.2.2.2/32, id: 3, row status: Active, Tunnel-Policy: N/A
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
```

```
    Matched bytes:0, pkts:0, TX bytes:0, Pushed pkts:0
     Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 3
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 3, owner: N/A, Stale: NO, out intf: eth2, out label: 3
    Nexthop addr: 20.1.1.2        cross connect ix: 4, op code: Push


 Primary FTN entry with FEC: 3.3.3.3/32, id: 4, row status: Active, Tunnel-Policy: N/A
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
    Matched bytes:0, pkts:0, TX bytes:0, Pushed pkts:0
     Cross connect ix: 5, in intf: - in label: 0 out-segment ix: 4
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 4, owner: LDP, Stale: NO, out intf: eth2, out label: 24321
    Nexthop addr: 20.1.1.2        cross connect ix: 5, op code: Push


 Primary FTN entry with FEC: 30.1.1.0/24, id: 5, row status: Active, Tunnel-Policy: N/A
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
    Matched bytes:0, pkts:0, TX bytes:0, Pushed pkts:0
     Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 3
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 3, owner: N/A, Stale: NO, out intf: eth2, out label: 3
    Nexthop addr: 20.1.1.2        cross connect ix: 4, op code: Push


 Primary FTN entry with FEC: 3002::/64, id: 2, row status: Active, Tunnel-Policy: N/A
  Owner: BGP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Transport Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
    Matched bytes:0, pkts:0, TX bytes:0, Pushed pkts:0
     Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
      Owner: BGP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: BGP, Stale: NO, BGP out intf: eth2, transport out
intf: eth2, out label: 24960
    Nexthop addr: 3.3.3.3        cross connect ix: 2, op code: Push and Lookup


 Primary FTN entry with FEC: 3ffe::/64, id: 1, row status: Active, Tunnel-Policy: N/A
  Owner: BGP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Transport Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
    Matched bytes:0, pkts:0, TX bytes:0, Pushed pkts:0
     Cross connect ix: 1, in intf: - in label: 0 out-segment ix: 1
      Owner: BGP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 1, owner: BGP, Stale: NO, BGP out intf: eth2, transport out
intf: eth2, out label: 24961
    Nexthop addr: 3.3.3.3        cross connect ix: 1, op code: Push and Lookup
```

```
PE1#show mpls ilm-table
Codes: > - installed ILM, * - selected ILM, p - stale ILM
        K - CLI ILM, T - MPLS-TP, s - Stitched ILM
       S - SNMP, L - LDP, R - RSVP, C - CRLDP
       B - BGP , K - CLI , V - LDP_VC, I - IGP_SHORTCUT
       O - OSPF/OSPF6 SR, i - ISIS SR, k - SR CLI
       P - SR Policy, U - unknown

Code    FEC/VRF/L2CKT    ILM-ID     In-Label    Out-Label   In-Intf    Out-Intf/VRF
Nexthop                  LSP-Type
   B>   2001::/64         3          24960       Nolabel     N/A        N/A
127.0.0.1                LSP_DEFAULT
   B>   2ffe::/64         4          24961       Nolabel     N/A        N/A
127.0.0.1                LSP_DEFAULT
#

PE1#show ip bgp summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 1
3 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
3.3.3.3                 4   100   42        43      1      0      0  00:08:40
0

Total number of neighbors 1

Total number of Established sessions 1

PE1#sh ipv6 bgp summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 5
3 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
2001::2                 4   200   93        98      5      0      0  00:08:33
1

Total number of neighbors 1

Total number of Established sessions 1

PE1#sh ip bgp neighbors
BGP neighbor is 3.3.3.3, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 1.1.1.1, remote router ID 3.3.3.3
  BGP state = Established, up for 00:08:55
  Last read 00:00:21, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
```

```
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv6 Labeled Unicast: advertised and received
  Received 42 messages, 0 notifications, 0 in queue
  Sent 43 messages, 1 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
  Update source is lo
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 For address family: IPv6 Labeled-Unicast
  BGP table version 6, neighbor version 6
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  2 accepted prefixes
  2 announced prefixes

 Connections established 2; dropped 1
Local host: 1.1.1.1, Local port: 34293
Foreign host: 3.3.3.3, Foreign port: 179
Nexthop: 1.1.1.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:09:51, due to Administratively Reset (Cease Notification sent)
Notification Error Message: (Cease/Administratively Reset.)

BGP neighbor is 2001::2, remote AS 200, local AS 100, external link
  BGP version 4, local router ID 1.1.1.1, remote router ID 44.44.44.44
  BGP state = Established, up for 00:08:45
  Last read 00:00:16, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv6 Unicast: advertised and received
  Received 92 messages, 1 notifications, 0 in queue
  Sent 97 messages, 1 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv6 Unicast
  BGP table version 5, neighbor version 5
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  3 announced prefixes
```

```
 Connections established 3; dropped 2
Local host: 2001::1, Local port: 179
Foreign host: 2001::2, Foreign port: 40980
Nexthop: 1.1.1.1
Nexthop global: 2001::1
Nexthop local: fe80::5054:ff:fe29:189d
BGP connection: shared network
Last Reset: 00:08:50, due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)
```

P1

```
P1#show ldp session
Peer IP Address           IF Name    My Role    State      KeepAlive  UpTime
3.3.3.3                   eth1       Passive   OPERATIONAL   30    00:10:11
1.1.1.1                   eth2       Active    OPERATIONAL   30    00:09:21

P1#show mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN,
       B - BGP FTN, K - CLI FTN, t - tunnel, P - SR Policy FTN,
       L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, I - IGP-Shortcut,
       U - unknown FTN, O - SR-OSPF FTN, i - SR-ISIS FTN, k - SR-CLI FTN

Code    FEC               FTN-ID    Nhlfe-ID  Tunnel-id   Pri   LSP-Type     Out-Label
Out-Intf    ELC   Nexthop
   L>   1.1.1.1/32          2         2         -           -     LSP_DEFAULT  0
eth2        No    20.1.1.1
   L>   3.3.3.3/32          1         1         -           -     LSP_DEFAULT  0
eth1        No    30.1.1.2

P1#show mpls ilm-table
Codes: > - installed ILM, * - selected ILM, p - stale ILM
        K - CLI ILM, T - MPLS-TP, s - Stitched ILM
       S - SNMP, L - LDP, R - RSVP, C - CRLDP
       B - BGP , K - CLI , V - LDP_VC, I - IGP_SHORTCUT
       O - OSPF/OSPF6 SR, i - ISIS SR, k - SR CLI
       P - SR Policy, U - unknown

Code    FEC/VRF/L2CKT    ILM-ID     In-Label    Out-Label   In-Intf    Out-Intf/VRF
Nexthop                  LSP-Type
   L>   3.3.3.3/32        2          24321       0           N/A        eth1
30.1.1.2                 LSP_DEFAULT
   L>   1.1.1.1/32        1          24320       0           N/A        eth2
20.1.1.1                 LSP_DEFAULT
```

PE2

```
PE2#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, D- DHCP, R - RIP,
       O - OSPF, IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, i - IS-IS, B - BGP,
       v - vrf leaked
```

```
Timers: Uptime

IP Route Table for VRF "default"
C       ::1/128 via ::, lo, 01:24:48
B       2001::/64 [200/0] via ::ffff:1.1.1.1, 00:11:08
B       2ffe::/64 [200/0] via ::ffff:1.1.1.1, 00:10:34
C       3002::/64 via ::, eth2, 00:24:41
B       3ffe::/64 [20/0] via fe80::5054:ff:fef6:c35d, eth2, 00:09:07
C       fe80::/64 via ::, eth3, 01:24:48

PE2#show mpls ilm-table
Codes: > - installed ILM, * - selected ILM, p - stale ILM
        K - CLI ILM, T - MPLS-TP, s - Stitched ILM
       S - SNMP, L - LDP, R - RSVP, C - CRLDP
       B - BGP , K - CLI , V - LDP_VC, I - IGP_SHORTCUT
       O - OSPF/OSPF6 SR, i - ISIS SR, k - SR CLI
       P - SR Policy, U - unknown

Code    FEC/VRF/L2CKT    ILM-ID     In-Label    Out-Label   In-Intf    Out-Intf/VRF
Nexthop                  LSP-Type
   B>   3002::/64         3          24960       Nolabel     N/A        N/A
127.0.0.1                LSP_DEFAULT
   B>   3ffe::/64         4          24961       Nolabel     N/A        N/A
127.0.0.1                LSP_DEFAULT

PE2#show mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN,
       B - BGP FTN, K - CLI FTN, t - tunnel, P - SR Policy FTN,
       L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, I - IGP-Shortcut,
       U - unknown FTN, O - SR-OSPF FTN, i - SR-ISIS FTN, k - SR-CLI FTN

Code    FEC               FTN-ID    Nhlfe-ID  Tunnel-id   Pri   LSP-Type     Out-Label
Out-Intf    ELC   Nexthop
   L>   1.1.1.1/32         3         2         -           -     LSP_DEFAULT  24320
eth1        No    30.1.1.1
   L>   2.2.2.2/32         1         1         -           -     LSP_DEFAULT  3
eth1        No    30.1.1.1
   L>   20.1.1.0/24        2         1         -           -     LSP_DEFAULT  3
eth1        No    30.1.1.1
   B>   2001::/64          4         3         0           Yes   LSP_DEFAULT  24960
-           No    1.1.1.1
   B>   2ffe::/64          5         4         0           Yes   LSP_DEFAULT  24961
-           No    1.1.1.1

PE2#show mpls ftn-table
 Primary FTN entry with FEC: 1.1.1.1/32, id: 3, row status: Active, Tunnel-Policy: N/A
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
    Matched bytes:0, pkts:0, TX bytes:0, Pushed pkts:0
     Cross connect ix: 3, in intf: - in label: 0 out-segment ix: 2
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: LDP, Stale: NO, out intf: eth1, out label: 24320
```

```
    Nexthop addr: 30.1.1.1        cross connect ix: 3, op code: Push


 Primary FTN entry with FEC: 2.2.2.2/32, id: 1, row status: Active, Tunnel-Policy: N/A
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
    Matched bytes:0, pkts:0, TX bytes:0, Pushed pkts:0
     Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 1
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 1, owner: N/A, Stale: NO, out intf: eth1, out label: 3
    Nexthop addr: 30.1.1.1        cross connect ix: 2, op code: Push


 Primary FTN entry with FEC: 20.1.1.0/24, id: 2, row status: Active, Tunnel-Policy: N/A
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
    Matched bytes:0, pkts:0, TX bytes:0, Pushed pkts:0
     Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 1
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 1, owner: N/A, Stale: NO, out intf: eth1, out label: 3
    Nexthop addr: 30.1.1.1        cross connect ix: 2, op code: Push


 Primary FTN entry with FEC: 2001::/64, id: 4, row status: Active, Tunnel-Policy: N/A
  Owner: BGP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Transport Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
    Matched bytes:0, pkts:0, TX bytes:0, Pushed pkts:0
     Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 3
      Owner: BGP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 3, owner: BGP, Stale: NO, BGP out intf: eth1, transport out
intf: eth1, out label: 24960
    Nexthop addr: 1.1.1.1        cross connect ix: 4, op code: Push and Lookup


 Primary FTN entry with FEC: 2ffe::/64, id: 5, row status: Active, Tunnel-Policy: N/A
  Owner: BGP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Transport Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
    Matched bytes:0, pkts:0, TX bytes:0, Pushed pkts:0
     Cross connect ix: 5, in intf: - in label: 0 out-segment ix: 4
      Owner: BGP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 4, owner: BGP, Stale: NO, BGP out intf: eth1, transport out
intf: eth1, out label: 24961
    Nexthop addr: 1.1.1.1        cross connect ix: 5, op code: Push and Lookup

PE2# show ldp session
Peer IP Address           IF Name    My Role    State      KeepAlive  UpTime
2.2.2.2                   eth1       Active    OPERATIONAL   30    00:12:01
```

```
PE2#show bgp ipv6
BGP table version is 5, local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, a add-path, * valid, > best, i -
internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop                    Metric    LocPrf     Weight Path
*>i  2001::/64        ::ffff:1.1.1.1                 0        100       0    ?
*>i  2ffe::/64        ::ffff:1.1.1.1                 0        100       0   200 ?
*> l 3002::/64        ::                             0        100       32768  ?
*> l 3ffe::/64        3002::2(fe80::5054:ff:fef6:c35d)
                                                     0        100       0   300 ?

Total number of prefixes 4

PE2#show ip bgp neighbors
BGP neighbor is 1.1.1.1, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 3.3.3.3, remote router ID 1.1.1.1
  BGP state = Established, up for 00:11:54
  Last read 00:00:06, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv6 Labeled Unicast: advertised and received
  Received 50 messages, 0 notifications, 0 in queue
  Sent 50 messages, 1 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
  Update source is lo
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 For address family: IPv6 Labeled-Unicast
  BGP table version 5, neighbor version 5
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  2 accepted prefixes
  2 announced prefixes

 Connections established 2; dropped 1
Local host: 3.3.3.3, Local port: 179
Foreign host: 1.1.1.1, Foreign port: 34293
Nexthop: 3.3.3.3
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
```

```
Last Reset: 00:12:28, due to Administratively Reset (Cease Notification sent)
Notification Error Message: (Cease/Administratively Reset.)

BGP neighbor is 3002::2, remote AS 300, local AS 100, external link
  BGP version 4, local router ID 3.3.3.3, remote router ID 66.66.66.66
  BGP state = Established, up for 00:10:17
  Last read 00:00:25, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv6 Unicast: advertised and received
  Received 61 messages, 2 notifications, 0 in queue
  Sent 68 messages, 2 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv6 Unicast
  BGP table version 5, neighbor version 5
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  3 announced prefixes

 Connections established 3; dropped 2
Local host: 3002::1, Local port: 52758
Foreign host: 3002::2, Foreign port: 179
Nexthop: 3.3.3.3
Nexthop global: 3002::1
Nexthop local: fe80::5054:ff:fe2b:8d4f
BGP connection: shared network
Last Reset: 00:10:22, due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)

PE2# show ip bgp summary
BGP router identifier 3.3.3.3, local AS number 100
BGP table version is 1
3 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
1.1.1.1                 4   100   50        52      1      0      0  00:12:06
0

Total number of neighbors 1

Total number of Established sessions 1

PE2#sh ipv6 bgp summary
BGP router identifier 3.3.3.3, local AS number 100
BGP table version is 5
3 BGP AS-PATH entries
0 BGP community entries
```

```
Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
3002::2                  4   300   64        70       5      0      0  00:10:31
1

Total number of neighbors 1

Total number of Established sessions 1
```

CE2

```
CE2#sh ipv6 bgp summary
BGP router identifier 66.66.66.66, local AS number 300
BGP table version is 9
3 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
3002::1                  4   100   70        67       9      0      0  00:11:35
3

Total number of neighbors 1

Total number of Established sessions 1

CE2#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, D- DHCP, R - RIP,
       O - OSPF, IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, i - IS-IS, B - BGP,
       v - vrf leaked
Timers: Uptime

IP Route Table for VRF "default"
C       ::1/128 via ::, lo, 01:26:48
B       2001::/64 [20/0] via fe80::5054:ff:fe2b:8d4f, eth2, 00:11:43
B       2ffe::/64 [20/0] via fe80::5054:ff:fe2b:8d4f, eth2, 00:11:43
C       3002::/64 via ::, eth2, 00:24:47
S       3ffe::/64 [1/0] via ::, eth2, 00:24:05
C       fe80::/64 via ::, eth2, 01:26:48
```

CHAPTER 7 6VPE Configuration

This chapter explains how 6VPE (IPv6 on VPN Provider Edge Routers) can interconnect IPv6 islands over an MPLS-enabled IPv4 cloud. 6VPE enables IPv6 sites to communicate with each other over an MPLS/IPv4 core network using MPLS LSPs. The 6VPE routers exchange IPv6 reachability information over the core using Multi-Protocol Border Gateway Protocol (MP-BGP) over IPv4.

Topology

As shown in Figure 7-8:

- CE1 and CE2 are customer edge routers
- 6VPE1 and 6VPE2 are IPv6 Provider Edge routers
- P is the router at the core of the IPv4 MPLS provider network.

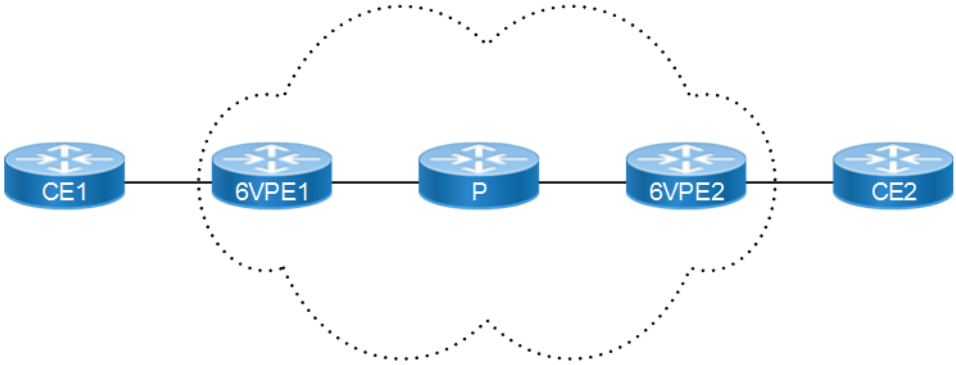


Figure 7-8: 6VPE Configuration

Configuration

CE1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode
`(config-if)#ip address 44.44.44.44/32 secondary`	Assign the IPv4 addres
`(config-if)#exit`	Exit interface mode
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 address 2001::2/64`	Assign the IPv6 address.
`(config-if)#exit`	Exit interface mode.
`(config)#ipv6 route 2ffe::/64 eth1`	Advertise IPv6 static route.
`(config)#router bgp 200`	Enter BGP router mode.
`(config-router)#bgp router-id 44.44.44.44`	Configure bgp router-id
`(config-router)#neighbor 2001::1 remote-as 100`	Configure 6VPE1 as an eBGP4+ neighbor.
`(config-router)#address-family ipv6 unicast`	Enter address-family IPv6 unicast mode.

(config-router-af)#neighbor 2001::1 activate	Activate the neighbor in the IPv6 address family.
(config-router-af)#redistribute connected	Redistribute the connected route under address family IPv6 unicast.
(config-router-af)#redistribute static	Redistribute static routes
(config-router-af)#exit	Exit twice.

CE2

#configure terminal	Enter configure mode
(config)#interface lo	Enter interface mode
(config-if)#ip address 66.66.66.66/32 secondary	Assign the IPv4 address
(config-if)#exit	Exit interface mode
(config)#interface eth1	Enter interface mode.
(config-if)#ipv6 address 3001::2/64	Assign the IPv6 address.
(config-if)#exit	Exit interface mode.
(config)#ipv6 route 3ffe::/64 eth1	Configure IPV6 static route
(config)#router bgp 300	Enter BGP router mode.
(config-router)# bgp router-id 66.66.66.66	Configure BGP router-id
(config-router)#neighbor 3001::1 remote-as 100	Configure 6VPE1 as an eBGP4+ neighbor.
(config-router)#address-family ipv6 unicast	Enter address-family IPv6 unicast mode.
(config-router-af)#neighbor 3001::1 activate	Activate the neighbor in the IPv6 address family.
(config-router-af)#redistribute connected	Redistribute the connected route under address family IPv6 unicast.
(config-router-af)#redistribute static	Redistribute static routes
(config-router-af)#exit	Exit twice.

PE1

#configure terminal	Enter configure mode.
(config)#ip vrf IPI	Create a new VRF named IPI.
(config-vrf)#rd 1:100	Assign the route distinguisher (RD) value as 1:100.
(config-vrf)#route-target both 100:200	Import routes between route target (RT) ext-communities 100 and 200.
(config-vrf)#router-id 77.77.77.77	Configure router-id for VRF
(config-vrf)#exit	Exit VRF mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ip vrf forwarding IPI	Bind the interface connected to the CE router with VRF IPI.
(config-if)#ipv6 address 2001::1/64	Assign the IPv6 address.
(config-if)#exit	Exit interface mode.
(config)#router bgp 100	Enter BGP router mode.
(config-router)#bgp router-id 1.1.1.1	Configure BGP router-id

(config-router)#neighbor 3.3.3.3 remote-as 100	Configure 6VPE2 as an iBGP peer.
(config-router)#neighbor 3.3.3.3 update-source lo	Update the source as loopback for iBGP peering with the remote 6VPE router.
(config-router)#address-family ipv4 unicast	Enter address family mode
(config-router-af)#neighbor 3.3.3.3 activate	Activate the neighbor
(config-router-af)#exit-address-family	Exit address family mode
(config-router)#address-family vpnv6 unicast	Enter VPNv6 address family mode.
(config-router-af)#neighbor 3.3.3.3 activate	Activate the 6VPE neighbor so that it can accept VPN IPv6 routes.
(config-router-af)#exit-address-family	Exit VPNv6 address family mode.
(config-router)#address-family ipv6 vrf IPI	Enter the IPv6 address family for VRF IPI.
(config-router-af)#neighbor 2001::2 remote-as 200	Activate CE inside IPv6 address family for vrf IPI.
(config-router-af)#neighbor 2001::2 activate	Activate the 6VPE neighbor so that it can accept VPN IPv6 routes.
(config-router-af)#redistribute connected	Redistribute the connected route under address family IPv6 for VRF IPI.
(config-router-af)#exit-address-family	Exit IPv6 Address Family mode.
(config-router)#exit	Exit router mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 1.1.1.1/32 secondary	Assign the IP address to loopback interface.
(config-if)#exit	Exit interface mode.
(config)#router ldp	Enter router LDP mode.
(config-router)#transport-address ipv4 1.1.1.1	Configure transport address as loopback address.
(config-router)#exit	Exit router LDP mode.
(config)#router rsvp	Enter RSVP router mode.
(config-router)#exit	Exit router mode.
(config)#interface eth2	Enter interface mode.
(config-if)#label-switching	Enable label switching in interface.
(config-if)#enable-rsvp	Enable RSVP in interface.
(config-if)#enable-ldp ipv4	Enable LDP in interface.
(config-if)#ip address 20.10.10.1/24	Assign IP address to interface.
(config-if)#exit	Exit interface mode.
(config)#router ospf 100	Enter OSPF router mode.
(config-router)#ospf router-id 1.1.1.1	Configure OSPF router id same as loopback ip address.
(config-router)#network 1.1.1.1/32 area 0 (config-router)#network 20.10.10.1/24 area 0	Define the network on which OSPF runs and associate area id.
(config-router)#exit	Exit OSPF router mode.
(config)#rsvp-trunk toPE2	Enter the trunk mode for RSVP.
(config-trunk)#to 3.3.3.3	Specify IPv4 Egress for the LSP.
(config-trunk)#exit	Exit twice.

P1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode.
`(config-if)#ip address 2.2.2.2/32 secondary`	Assign the IP address to loopback interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router ldp`	Enter router LDP mode.
`(config-router)#transport-address ipv4 2.2.2.2`	Configure transport address as loopback address.
`(config-router)#exit`	Exit router mode.
`(config)#router rsvp`	Enter RSVP router mode.
`(config-router)#exit`	Exit router mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#label-switching`	Enable label switching in interface.
`(config-if)#enable-rsvp`	Enable RSVP in interface.
`(config-if)#enable-ldp ipv4`	Enable LDP in interface.
`(config-if)#ip address 20.10.10.2/24`	Assign IP address to interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#label-switching`	Enable label switching in interface.
`(config-if)#enable-rsvp`	Enable RSVP in interface.
`(config-if)#enable-ldp ipv4`	Enable ldp in interface.
`(config-if)#ip address 20.10.20.1/24`	Assign IP address to interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 100`	Enter OSPF router mode.
`(config-router)#ospf router-id 2.2.2.2`	Configure OSPF router id same as loopback ip address..=

`(config-router)#network 2.2.2.2/32 area 0`
`(config-router)#network 20.10.20.1/24 area 0`
`(config-router)#network 20.10.10.2/24 area 0`
	Define the network on which OSPF runs and associate area id.

`(config-router)#exit`	Exit twice.

PE2

`#configure terminal`	Enter configure mode.
`(config)#ip vrf IPI`	Create a new VRF named IPI.
`(config-vrf)#rd 1:101`	Assign the route distinguisher (RD) value as 1:100.
`(config-vrf)#route-target both 100:200`	Import routes between route target (RT) ext-communities 100 and 200.
`(config-vrf)#router-id 55.55.55.55`	Configure Router-id for VRF
`(config-vrf)#exit`	Exit VRF mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip vrf forwarding IPI`	Bind the interface connected to the CE router with VRF IPI.

(config-if)#ipv6 address 3001::1/64	Assign the IPv6 address.
(config-if)#exit	Exit interface mode.
(config)#router bgp 100	Enter BGP router mode.
(config-router)#bgp router-id 3.3.3.3	Configure BGP router-id
(config-router)#neighbor 1.1.1.1 remote-as 100	Configure 6VPE2 as an iBGP peer.
(config-router)#neighbor 1.1.1.1 update-source lo	Update the source as loopback for iBGP peering with the remote 6VPE router.
(config-router)#address-family ipv4 unicast	Enter address family mode
(config-router-af)#neighbor 1.1.1.1 activate	Activate the neighbor
(config-router-af)#exit-address-family	Exit address family mode
(config-router)#address-family vpnv6 unicast	Enter VPNv6 address family mode.
(config-router-af)#neighbor 1.1.1.1 activate	Activate the 6VPE neighbor so that it can accept VPN IPv6 routes.
(config-router-af)#exit-address-family	Exit VPNv6 address family mode.
(config-router)#address-family ipv6 vrf IPI	Enter the IPv6 address family for VRF IPI.
(config-router-af)#neighbor 3001::2 remote-as 300	Activate CE inside IPv6 address family for vrf IPI.
(config-router-af)#neighbor 3001::2 activate	Activate the neighbor
(config-router-af)#redistribute connected	Redistribute the connected route under address family IPv6 for VRF IPI.
(config-router-af)#exit-address-family	Exit IPv6 Address Family mode.
(config-router)#exit	Exit router mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 3.3.3.3/32 secondary	Assign the IP address to loopback interface.
(config-if)#exit	Exit interface mode.
(config)#router ldp	Enter router LDP mode.
(config-router)#transport-address ipv4 3.3.3.3	Configure transport address as loopback address.
(config-router)#exit	Exit router mode
(config)#router rsvp	Enter RSVP router mode.
(config-router)#exit	Exit router mode.
(config)#interface eth1	Enter interface mode.
(config-if)#label-switching	Enable label switching in interface
(config-if)#enable-rsvp	Enable RSVP in interface.
(config-if)#enable-ldp ipv4	Enable LDP in interface.
(config-if)#ip address 20.10.20.2/24	Assign IP address to interface.
(config-if)#exit	Exit interface mode.
(config)#router ospf 100	Enter OSPF router mode.
(config-router)#ospf router-id 3.3.3.3	Configure OSPF router id same as loopback ip address.
(config-router)#network 3.3.3.3/32 area 0 (config-router)#network 20.10.20.2/24 area 0	Define the network on which OSPF runs and associate area id.
(config-router)#exit	Exit OSPF router mode.
(config)#rsvp-trunk toPE1	Enter the trunk mode for RSVP.

(config-trunk)#to 1.1.1.1	Specify IPv4 Egress for the LSP.
(config-trunk)#exit	Exit twice.

Validation

CE1

```
CE1#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, D- DHCP, R - RIP,
       O - OSPF, IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, i - IS-IS, B - BGP,
       v - vrf leaked
Timers: Uptime

IP Route Table for VRF "default"
C       ::1/128 via ::, lo, 01:38:28
C       2001::/64 via ::, eth1, 01:20:30
S       2ffe::/64 [1/0] via ::, eth1, 00:01:27
B       3001::/64 [20/0] via fe80::5054:ff:fe29:189d, eth1, 00:06:40
B       3ffe::/64 [20/0] via fe80::5054:ff:fe29:189d, eth1, 00:02:24
C       fe80::/64 via ::, eth3, 01:38:28
CE1#show ipv6 bgp summary vrf all
BGP router identifier 44.44.44.44, local AS number 200
BGP table version is 4
3 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
2001::1                 4   100 1167      1522       4     0      0  00:13:23
3

Total number of neighbors 1

Total number of Established sessions 1
```

PE1

```
PE1#show ipv6 route vrf IPI
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, D- DHCP, R - RIP,
       O - OSPF, IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, i - IS-IS, B - BGP,
       v - vrf leaked
Timers: Uptime

IP Route Table for VRF "IPI"
C       2001::/64 via ::, eth1, 01:12:03
```

```
B       2ffe::/64 [20/0] via fe80::5054:ff:fe60:f4e5, eth1, 00:02:05
B       3001::/64 [200/0] via ::ffff:3.3.3.3, 00:08:02
B       3ffe::/64 [200/0] via ::ffff:3.3.3.3, 00:03:33
C       fe80::/64 via ::, eth1, 01:12:32
PE1#show ip bgp summary vrf all
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 1
3 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
3.3.3.3                 4   100   23        23      1      0      0  00:08:12
0

Total number of neighbors 1

Total number of Established sessions 1
PE1#show ipv6 bgp v
PE1#show ipv6 bgp summary vrf all
BGP router identifier 77.77.77.77, local AS number 100
BGP VRF IPI Route Distinguisher: 1:100
BGP table version is 1
3 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
2001::2                 4   200   38        38      1      0      0  00:14:50
2

Total number of neighbors 1

Total number of Established sessions 1
PE1#show mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN,
       B - BGP FTN, K - CLI FTN, t - tunnel, P - SR Policy FTN,
       L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, I - IGP-Shortcut,
       U - unknown FTN, O - SR-OSPF FTN, i - SR-ISIS FTN, k - SR-CLI FTN

Code    FEC               FTN-ID    Nhlfe-ID  Tunnel-id   Pri   LSP-Type     Out-Label
Out-Intf    ELC   Nexthop
   L>   2.2.2.2/32          1         1         -           -     LSP_DEFAULT  3
eth2        No    20.10.10.2
R(t)>   3.3.3.3/32          4         4         5001        Yes   LSP_DEFAULT  24320
eth2        No    20.10.10.2
   L    3.3.3.3/32          3         2         -           -     LSP_DEFAULT  24960
eth2        No    20.10.10.2
   L>   20.10.20.0/24       2         1         -           -     LSP_DEFAULT  3
eth2        No    20.10.10.2
PE1#show rsvp session
Type  : PRI - Primary, SEC - Secondary, DTR - Detour, BPS - Bypass
```

```
State : UP - Up, DN - Down, BU - Backup in Use, SU - Secondary in Use, FS - Forced to
Secondary
* indicates the session is active with local repair at one or more nodes
(P) indicates the secondary-priority session is acting as primary

Ingress RSVP:
To              From            Type    LSPName                         State Uptime    Rt
Style  Labelin  Labelout  DSType
3.3.3.3         1.1.1.1          PRI     toPE2-Primary                      UP    00:08:44
1 1 SE     -         24320     DEFAULT
Total 1 displayed, Up 1, Down 0.

Egress RSVP:
To              From            Type    LSPName                         State Uptime    Rt
Style  Labelin  Labelout  DSType
1.1.1.1         3.3.3.3          PRI     toPE1-Primary                      UP    00:08:39
1 1 SE     24960     -         ELSP_CON
Total 1 displayed, Up 1, Down 0.

PE1#show mpls ilm-table
Codes: > - installed ILM, * - selected ILM, p - stale ILM
        K - CLI ILM, T - MPLS-TP, s - Stitched ILM
       S - SNMP, L - LDP, R - RSVP, C - CRLDP
       B - BGP , K - CLI , V - LDP_VC, I - IGP_SHORTCUT
       O - OSPF/OSPF6 SR, i - ISIS SR, k - SR CLI
       P - SR Policy, U - unknown

Code    FEC/VRF/L2CKT    ILM-ID     In-Label    Out-Label   In-Intf    Out-Intf/VRF
Nexthop                  LSP-Type
   B>   IPI              1          24320       Nolabel     N/A        IPI             N/
A                        LSP_DEFAU
LT
   R>   1.1.1.1/32        2          24960       Nolabel     N/A        N/A
127.0.0.1                ELSP_CONF
IG
PE1#show mpls vrf-table
Output for IPv6 VRF table with id: 2
 Primary FTN entry with FEC: 3001::/64, id: 1, row status: Active, Tunnel-Policy: N/A
  Owner: BGP, distance: 0, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming
DSCP: none
  Transport Tunnel id: 5001, Protected LSP id: 2201, QoS Resource id: 0, Description: N/
A, Color: 0
    Matched bytes:0, pkts:0, TX bytes:0, Pushed pkts:0
     Cross connect ix: 5, in intf: - in label: 0 out-segment ix: 5
      Owner: BGP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 5, owner: BGP, Stale: NO, BGP out intf: eth2, transport out
intf: eth2, out label: 24320
    Nexthop addr: 3.3.3.3        cross connect ix: 5, op code: Push and Lookup


 Primary FTN entry with FEC: 3ffe::/64, id: 2, row status: Active, Tunnel-Policy: N/A
  Owner: BGP, distance: 0, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming
DSCP: none
```

```
  Transport Tunnel id: 5001, Protected LSP id: 2201, QoS Resource id: 0, Description: N/
A, Color: 0
    Matched bytes:0, pkts:0, TX bytes:0, Pushed pkts:0
     Cross connect ix: 5, in intf: - in label: 0 out-segment ix: 5
      Owner: BGP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 5, owner: BGP, Stale: NO, BGP out intf: eth2, transport out
intf: eth2, out label: 24320
    Nexthop addr: 3.3.3.3        cross connect ix: 5, op code: Push and Lookup


PE1#show mpls ftn-table
 Primary FTN entry with FEC: 2.2.2.2/32, id: 1, row status: Active, Tunnel-Policy: N/A
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
    Matched bytes:0, pkts:0, TX bytes:0, Pushed pkts:0
     Cross connect ix: 1, in intf: - in label: 0 out-segment ix: 1
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 1, owner: N/A, Stale: NO, out intf: eth2, out label: 3
    Nexthop addr: 20.10.10.2        cross connect ix: 1, op code: Push


 Primary FTN entry with FEC: 3.3.3.3/32, id: 4, row status: Active, Tunnel-Policy: N/A
  Owner: RSVP, distance: 0, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming
DSCP: none
  Tunnel id: 5001, Protected LSP id: 2201, QoS Resource id: 2, Description: toPE2,
Color: 0
    Matched bytes:0, pkts:0, TX bytes:0, Pushed pkts:0
     Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 4
      Owner: RSVP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 4, owner: RSVP, Stale: NO, out intf: eth2, out label: 24320
    Nexthop addr: 20.10.10.2        cross connect ix: 4, op code: Push


 Primary FTN entry with FEC: 3.3.3.3/32, id: 3, row status: Active, Tunnel-Policy: N/A
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
    Matched bytes:0, pkts:0, TX bytes:0, Pushed pkts:0
     Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
      Owner: LDP, Persistent: No, Admin Status: Down, Oper Status: Down
       Out-segment with ix: 2, owner: LDP, Stale: NO, out intf: eth2, out label: 24960
    Nexthop addr: 20.10.10.2        cross connect ix: 2, op code: Push


 Primary FTN entry with FEC: 20.10.20.0/24, id: 2, row status: Active, Tunnel-Policy: N/
A
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
    Matched bytes:0, pkts:0, TX bytes:0, Pushed pkts:0
     Cross connect ix: 1, in intf: - in label: 0 out-segment ix: 1
```

```
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 1, owner: N/A, Stale: NO, out intf: eth2, out label: 3
    Nexthop addr: 20.10.10.2        cross connect ix: 1, op code: Push


PE1#show ip bgp vpnv6 all
Status codes: s suppressed, d damped, h history, a add-path, * valid, > best, i -
internal, l - labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

     Network          Next Hop                    Metric    LocPrf      Weight       Path
Route Distinguisher: 1:100 (Default for VRF IPI)
*> l 2001::/64        ::                               0        100       32768  ?
*    2001::/64        2001::2(fe80::5054:ff:fe60:f4e5)
                                                      0        100       0   200 ?
*> l 2ffe::/64        2001::2(fe80::5054:ff:fe60:f4e5)
                                                      0        100       0   200 ?
*>i  3001::/64        ::ffff:3.3.3.3                  0        100       0    ?
*>i  3ffe::/64        ::ffff:3.3.3.3                  0        100       0   300 ?
 Announced routes count = 3
 Accepted routes count = 2
Route Distinguisher: 1:101
*>i  3001::/64        ::ffff:3.3.3.3                  0        100       0    ?
*>i  3ffe::/64        ::ffff:3.3.3.3                  0        100       0   300 ?
 Announced routes count = 0
 Accepted routes count = 2
PE1#show ip bgp neighbors i
PE1#show ip bgp neighbors
BGP neighbor is 3.3.3.3, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 1.1.1.1, remote router ID 3.3.3.3
  BGP state = Established, up for 00:09:55
  Last read 00:00:21, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family VPNv6 Unicast: advertised and received
  Received 27 messages, 0 notifications, 0 in queue
  Sent 27 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
  Update source is lo
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 For address family: VPNv6 Unicast
  BGP table version 3, neighbor version 3
```



```
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  2 accepted prefixes
  2 announced prefixes

 Connections established 1; dropped 0
Local host: 1.1.1.1, Local port: 33537
Foreign host: 3.3.3.3, Foreign port: 179
Nexthop: 1.1.1.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 2001::2, vrf IPI, remote AS 200, local AS 100, external link
  BGP version 4, local router ID 77.77.77.77, remote router ID 44.44.44.44
  BGP state = Established, up for 00:16:19
  Last read 00:00:10, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv6 Unicast: advertised and received
  Received 42 messages, 0 notifications, 0 in queue
  Sent 42 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv6 Unicast
  BGP table version 1, neighbor version 1
  Index 0, Offset 0, Mask 0x1
  Community attribute sent to this neighbor (standard)
  2 accepted prefixes
  3 announced prefixes

 Connections established 1; dropped 0
Local host: 2001::1, Local port: 34776
Foreign host: 2001::2, Foreign port: 179
Nexthop: 77.77.77.77
Nexthop global: 2001::1
Nexthop local: fe80::5054:ff:fe29:189d
BGP connection: shared network
```

P1

```
P1#show mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN,
       B - BGP FTN, K - CLI FTN, t - tunnel
       L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, I - IGP-Shortcut,
       U - unknown FTN, O - SR-OSPF FTN, i - SR-ISIS FTN, k - SR-CLI FTN

Code    FEC                FTN-ID    Tunnel-id   Pri   LSP-Type        Out-Label    Out-
Intf       Nexthop
   L>   1.1.1.1/32        1       0         Yes   LSP_DEFAULT    3          ce46
20.10.10.1
```

```
   L>    3.3.3.3/32         2       0          Yes   LSP_DEFAULT    3           ce44
20.10.20.2
P1#
P1#show mpls ilm-table
Codes: > - installed ILM, * - selected ILM, p - stale ILM
        K - CLI ILM, T - MPLS-TP, S - Stitched ILM
       S - SNMP, L - LDP, R - RSVP, C - CRLDP
       B - BGP , K - CLI , V - LDP_VC, I - IGP_SHORTCUT
       O - OSPF/OSPF6 SR, i - ISIS SR, k - SR CLI
       U - unknown

Code    FEC/VRF          ILM-ID      In-Label    Out-Label   In-Intf    Out-Intf
Nexthop                 LSP-Type
   R>   1.1.1.1/32          2           24321       24960       N/A        ce46
20.10.10.1             ELSP_CONFIG
   R>   3.3.3.3/32          1           24320       24960       N/A        ce44
20.10.20.2             ELSP_CONFIG
   L>   1.1.1.1/32          4           24961       3           N/A        ce46
20.10.10.1             LSP_DEFAULT
   L>   3.3.3.3/32          5           24960       3           N/A        ce44
20.10.20.2             LSP_DEFAULT
P1#show ip ospf neighbor

Total number of full neighbors: 2
OSPF process 100 VRF(default):
Neighbor ID     Pri   State            Dead Time   Address         Interface
Instance ID
1.1.1.1           1   Full/Backup      00:00:31    20.10.10.1      ce46                  0
3.3.3.3           1   Full/DR          00:00:32    20.10.20.2      ce44                  0
```

PE2

```
PE2#show ipv6 route vrf IPI
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "IPI"
C      ::1/128 via ::, lo.IPI, 00:24:23
C      3001::/64 via ::, ce43, 00:24:22
B      3ffe::/64 [20/0] via fe80::3617:ebff:fe0e:1201, ce43, 00:05:28
C      fe80::/64 via ::, ce43, 00:24:22

PE2# show ip bgp summary vrf all
BGP router identifier 55.55.55.55, local AS number 100
BGP VRF IPI Route Distinguisher: 1:100
BGP table version is 1
3 BGP AS-PATH entries
0 BGP community entries
```

```
Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
3001::2                 4   300  116       181      1      0      0  00:22:05
0

Total number of neighbors 1

Total number of Established sessions 1
BGP router identifier 3.3.3.3, local AS number 100
BGP table version is 1
3 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
1.1.1.1                 4   100   65        66      1      0      0  00:26:21
0

Total number of neighbors 1

Total number of Established sessions 1

PE2#show mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN,
       B - BGP FTN, K - CLI FTN, t - tunnel
       L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, I - IGP-Shortcut,
       U - unknown FTN, O - SR-OSPF FTN, i - SR-ISIS FTN, k - SR-CLI FTN

Code    FEC                FTN-ID    Tunnel-id   Pri   LSP-Type        Out-Label    Out-
Intf       Nexthop
R(t)>   1.1.1.1/32         1       5001       Yes   LSP_DEFAULT    24321       ce44
20.10.20.1
  L     1.1.1.1/32         2       0          Yes   LSP_DEFAULT    24961       ce44
20.10.20.1
  L>    2.2.2.2/32         3       0          Yes   LSP_DEFAULT    3           ce44
20.10.20.1
  L>    20.10.10.0/24      4       0          Yes   LSP_DEFAULT    3           ce44
20.10.20.1
PE2#show rsvp session
Type  : PRI - Primary, SEC - Secondary, DTR - Detour, BPS - Bypass
State : UP - Up, DN - Down, BU - Backup in Use, SU - Secondary in Use, FS - Forced to
Secondary
* indicates the session is active with local repair at one or more nodes

Ingress RSVP:
To              From            Type  LSPName                          State Uptime    Rt
Style  Labelin  Labelout  DSType
1.1.1.1         3.3.3.3          PRI   toPE1-Primary                      UP    00:23:21  1
1 SE     -        24321     DEFAULT
Total 1 displayed, Up 1, Down 0.

Egress RSVP:
```

```
To              From            Type  LSPName                          State Uptime    Rt
Style  Labelin  Labelout  DSType
3.3.3.3         1.1.1.1          PRI   toPE2-Primary                      UP    00:23:33  1
1 SE     24960    -         ELSP_CON
Total 1 displayed, Up 1, Down 0.

PE2#show mpls ilm-table
Codes: > - installed ILM, * - selected ILM, p - stale ILM
        K - CLI ILM, T - MPLS-TP, S - Stitched ILM
       S - SNMP, L - LDP, R - RSVP, C - CRLDP
       B - BGP , K - CLI , V - LDP_VC, I - IGP_SHORTCUT
       O - OSPF/OSPF6 SR, i - ISIS SR, k - SR CLI
       U - unknown

Code    FEC/VRF          ILM-ID      In-Label    Out-Label   In-Intf    Out-Intf
Nexthop                 LSP-Type
   B>   3ffe::/64          3           24321       N/A         N/A        ce43
fe80::3617:ebff:fe0e:1201  LSP_DEFAULT
  B>  3001::/64       2        24320     N/A       N/A      ce43       ::
LSP_DEFAULT
   R>   3.3.3.3/32         1           24960       N/A         N/A        N/A
127.0.0.1             ELSP_CONFIG

PE2#show ip bgp neighbors
BGP neighbor is 1.1.1.1, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 3.3.3.3, remote router ID 1.1.1.1
  BGP state = Established, up for 00:23:39
  Last read 00:00:27, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family VPNv6 Unicast: advertised and received
  Received 58 messages, 0 notifications, 0 in queue
  Sent 60 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
  Update source is lo
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 For address family: VPNv6 Unicast
  BGP table version 4, neighbor version 4
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  2 accepted prefixes
  2 announced prefixes

 Connections established 1; dropped 0
```

```
Local host: 3.3.3.3, Local port: 37145
Foreign host: 1.1.1.1, Foreign port: 179
Nexthop: 3.3.3.3
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 3001::2, vrf IPI, remote AS 300, local AS 100, external link
  BGP version 4, local router ID 55.55.55.55, remote router ID 66.66.66.66
  BGP state = Established, up for 00:19:23
  Last read 00:00:05, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv6 Unicast: advertised and received
  Received 110 messages, 0 notifications, 0 in queue
  Sent 113 messages, 62 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (standard)
  0 accepted prefixes
  0 announced prefixes

 For address family: IPv6 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (standard)
  2 accepted prefixes
  3 announced prefixes

 Connections established 1; dropped 0
Local host: 3001::1, Local port: 179
Foreign host: 3001::2, Foreign port: 58741
Nexthop: 55.55.55.55
Nexthop global: 3001::1
Nexthop local: fe80::da9e:f3ff:fec9:65a1
BGP connection: shared network
Last Reset: 00:19:28, due to OPEN Message Error (Notification sent)
Notification Error Message: (OPEN Message Error/Bad BGP Identifier.)

PE2#show ip bgp vpnv6 all
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, l -
labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf      Weight Path
Route Distinguisher: 1:100 (Default for VRF IPI)
```

```
*>i  2001::/64       ::ffff:101:101                      0        100          0
?
*>i  2ffe::/64       ::ffff:101:101                       0        100          0
200 ?
*> l 3001::/64        ::                     0         100           32768    ?
*    3001::/64        3001::2(fe80::3617:ebff:fe0e:1201)
                                    0         100           0       300 ?
*> l 3ffe::/64        3001::2(fe80::3617:ebff:fe0e:1201)
                                    0         100           0       300 ?
 Announced routes count = 3
 Accepted routes count = 2
Route Distinguisher: 1:100
*>i  2001::/64       ::ffff:101:101                      0        100          0
?
*>i  2ffe::/64       ::ffff:101:101                       0        100          0
200 ?
 Announced routes count = 0
 Accepted routes count = 2

PE2#show mpls ftn-table
 Primary FTN entry with FEC: 1.1.1.1/32, id: 1, row status: Active
  Owner: RSVP, distance: 0, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming
DSCP: none
  Tunnel id: 5001,   Protected LSP id: 2201, QoS Resource id: 2, Description: toPE1
     Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 3
      Owner: RSVP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 3, owner: RSVP, out intf: ce44, out label: 24321
    Nexthop addr: 20.10.20.1        cross connect ix: 4, op code: Push


 Primary FTN entry with FEC: 1.1.1.1/32, id: 2, row status: Active
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 5, in intf: - in label: 0 out-segment ix: 4
      Owner: LDP, Persistent: No, Admin Status: Down, Oper Status: Down
       Out-segment with ix: 4, owner: LDP, out intf: ce44, out label: 24961
    Nexthop addr: 20.10.20.1        cross connect ix: 5, op code: Push


 Primary FTN entry with FEC: 2.2.2.2/32, id: 3, row status: Active
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 6, in intf: - in label: 0 out-segment ix: 5
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 5, owner: LDP, out intf: ce44, out label: 3
    Nexthop addr: 20.10.20.1        cross connect ix: 6, op code: Push


 Primary FTN entry with FEC: 20.10.10.0/24, id: 4, row status: Active
```

```
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0,   Protected LSP id: 0, Description: N/A
     Cross connect ix: 6, in intf: - in label: 0 out-segment ix: 5
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 5, owner: LDP, out intf: ce44, out label: 3
    Nexthop addr: 20.10.20.1        cross connect ix: 6, op code: Push


PE2#show mpls vrf-table
Output for IPv6 VRF table with id: 2
 Primary FTN entry with FEC: 2001::/64, id: 1, row status: Active
  Owner: BGP, distance: 0, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming
DSCP: none
  Tunnel id: 5001,   Protected LSP id: 2201, QoS Resource id: 0, Description: N/A
     Cross connect ix: 3, in intf: - in label: 0 out-segment ix: 2
      Owner: BGP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: BGP, out intf: N/A, out label: 24320
    Nexthop addr: 1.1.1.1        cross connect ix: 3, op code: Push and Lookup


 Primary FTN entry with FEC: 2ffe::/64, id: 2, row status: Active
  Owner: BGP, distance: 0, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming
DSCP: none
  Tunnel id: 5001,   Protected LSP id: 2201, QoS Resource id: 0, Description: N/A
     Cross connect ix: 7, in intf: - in label: 0 out-segment ix: 6
      Owner: BGP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 6, owner: BGP, out intf: N/A, out label: 24321
    Nexthop addr: 1.1.1.1        cross connect ix: 7, op code: Push and Lookup
```

CE2

```
CE2#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 00:37:26
B      2001::/64 [20/0] via fe80::da9e:f3ff:fec9:65a1, ce43, 00:20:44
B      2ffe::/64 [20/0] via fe80::da9e:f3ff:fec9:65a1, ce43, 00:09:52
C      3001::/64 via ::, ce43, 00:27:07
S      3ffe::/64 [1/0] via ::, ce43, 00:07:31
C      fe80::/64 via ::, ce47, 00:37:26

CE2#show ip bgp summary vrf all
BGP router identifier 66.66.66.66, local AS number 300
BGP table version is 1
3 BGP AS-PATH entries
```

```
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
3001::1                  4   100  178       176       1     0     0  00:20:51
0

Total number of neighbors 1

Total number of Established sessions 1
```

CHAPTER 8 RSVP-TE Configuration

This chapter contains configurations for Resource Reservation Protocol - Traffic Engineering (RSVP-TE).

RSVP-TE Overview

RSVP-TE is a signaling protocol that supports explicit routing capabilities, To do this, an Explicit Route (ER) object is incorporated into RSVP PATH messages. This object encapsulates a sequence of hops that constitute the explicitly-routed path. Using the ER object, the paths taken by label-switched RSVP-MPLS flows can be pre-determined without conventional IP routing. An ER path can be administratively specified or computed based on CSPF and any policy requirements dictated by the operator through the trunk node, taking the current network state into consideration. A useful application of explicit routing is Traffic Engineering (TE). Using explicitly-routed LSPs, an ingress node can control the path through which traffic flows from itself, through the MPLS network, to the egress node. Explicit routing is therefore useful for the optimization of network resources and an increase in the quality of traffic-oriented performance.

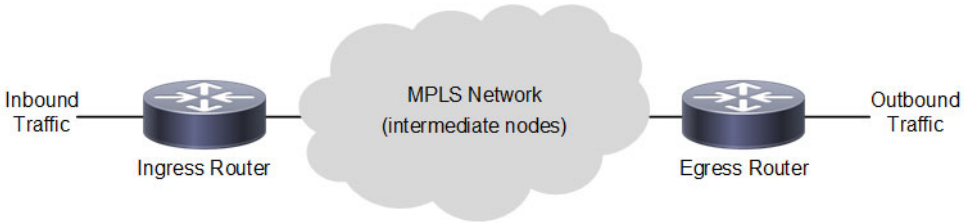


Figure 8-9: Basic RSVP-TE Topology

RSVP-TE Architecture

RSVP-TE is a signaling protocol that supports explicit routing capabilities to establish LSPs in a MPLS network. OcNOS RSVP-TE:

- creates explicitly-routed paths, which might not agree with the route suggested by the IGP (OSPF, RIP) being used. Explicitly-routed LSPs, by definition, do not follow the paths suggested by IGPs.
- queries CSPF for a complete, end-to-end, explicit route based on constraints specified by the operator using RSVP commands.
- performs make-before-break type re-routing of tunnels. (Make-before-break is the creation of a new LSP before the old one is torn down).
- exchanges Hello messages to make node failures easier to detect. This means when there is no hello exchange between routers, then other node is assumed dead or offline (except in the case when the peer is known to not support Hellos).
- provides statistical information of RSVP messages exchanged.

In addition, OcNOS RSVP-TE may be used in unison with BGP to generate MPLS/BGP VPNs, and in unison with LDP to generate Layer-2 Virtual Circuits.

Configure RSVP-TE

Note: The following configuration for establishing a trunk is required on all routers participating in label-switching. Based on the assumption that minimal configurations exist on all participating routers, other examples do not repeat this configuration.

Enable Label Switching - Minimal Configuration

To establish a trunk on a system:

1. Enable label-switching and RSVP-TE on all participating interfaces.
2. Configure a trunk on the ingress router to use the best available IGP path.

   In this example, the Label Switched Path (LSP) is configured using minimal configuration and is setup using the best IP nexthop available. Each router along the path is chosen by the previous router by looking up the best nexthop available in its IP routing table.

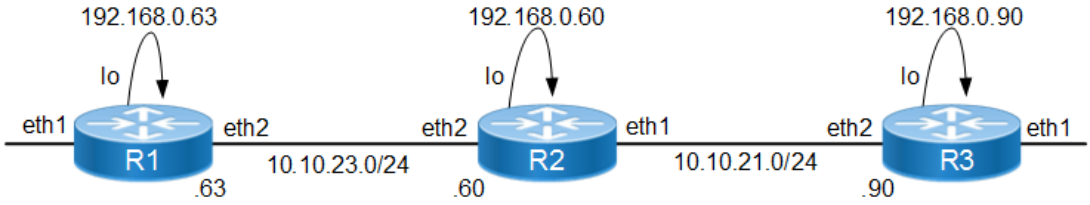


Figure 8-10: Topology for Minimal Configuration

R1

NSM

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode.
`(config-if)#ip address 192.168.0.63/32 secondary`	Set the IP address for the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip address 10.10.23.63/24`	Set the IP address for the interface.
`(config-if)#label-switching`	Enable label switching on interface `eth0`.
`(config-if)#exit`	Exit interface mode.

RSVP-TE

`(config)#router rsvp`	Enter `Configure Router` mode.
`(config-router)#exit`	Exit `Router` mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#enable-rsvp`	Enable RSVP message exchange on this interface.
`(config-if)#exit`	Exit interface mode.

OSPF

`#configure terminal`	Enter configure mode.
`(config)#router ospf 100`	Configure the Routing process and specify the Process ID `(100)`. The Process ID should be a unique positive integer identifying the routing process.

(config-router)#router-id 192.168.0.63	Configure OSPF router-ID same as loopback interface IP address
(config-router)#network 10.10.23.0/24 area 0	Define the network (10.10.23.0/24) on which OSPF runs and associate the area ID (0).
(config-router)#network 192.168.0.63/32 area 0	Set the IP address of the loopback interface to 192.168.0.63/32.
(config-router)#exit	Exit Router mode.

R2

NSM

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 192.168.0.60/32 secondary	Set the IP address for the interface.
(config-if)#exit	Enable label switching on interface lo.
(config)#interface eth2	Enter interface mode.
(config-if)#ip address 10.10.23.60/24	Set the IP address for the interface.
(config-if)#label-switching	Enable label switching on interface eth2.
(config-if)#exit	Exit interface mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ip address 10.10.21.60/24	Set the IP address for the interface.
(config-if)#label-switching	Enable label switching on interface eth1.
(config-if)#exit	Exit interface mode.

RSVP-TE

(config)#router rsvp	Enter Configure Router mode.
(config-router)#exit	Exit Router mode.
(config)#interface eth2	Enter interface mode.
(config-if)#enable-rsvp	Enable RSVP message exchange on this interface.
(config-if)#exit	Exit interface mode.
(config)#interface eth1	Enter interface mode.
(config-if)#enable-rsvp	Enable RSVP message exchange on this interface.
(config-if)#exit	Exit interface mode.

OSPF

#configure terminal	Enter configure mode.
(config)#router ospf 100	Configure the Routing process and specify the Process ID (100). The Process ID should be a unique positive integer identifying the routing process.
(config-router)#router-id 192.168.0.60	Configure OSPF router-ID same as loopback interface IP address

(config-router)#network 10.10.23.0/24 area 0	Define the first network (10.10.23.0/24) on which OSPF runs and associate the area ID (0).
(config-router)#network 10.10.21.0/24 area 0	Define the second network (10.10.21.0/24) on which OSPF runs and associate the area ID (0).
(config-router)#network 192.168.0.60/32 area 0	Set the IP address of the loopback interface to 192.168.0.63/32.
(config-router)#exit	Exit Router mode.

R3

NSM

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 192.168.0.90/32 secondary	Set the IP address for the interface.
(config-if)#exit	Exit interface mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ip address 10.10.21.90/24	Set the IP address for the interface.
(config-if)#label-switching	Enable label switching on interface eth0.
(config-if)#exit	Exit interface mode.

RSVP-TE

(config)#router rsvp	Enter Configure Router mode.
(config-router)#exit	Exit Router mode.
(config)#interface eth1	Enter interface mode.
(config-if)#enable-rsvp	Enable RSVP message exchange on this interface.
(config-if)#exit	Exit interface mode.

OSPF

#configure terminal	Enter configure mode.
(config)#router ospf 100	Configure the Routing process and specify the Process ID (100). The Process ID should be a unique positive integer identifying the routing process.
(config-router)#router-id 192.168.0.90	Configure OSPF router-ID same as loopback interface IP address
(config-router)#network 10.10.21.0/24 area 0	Define the network (10.10.21.0/24) on which OSPF runs and associate the area ID (0).
(config-router)#network 192.168.0.90/32 area 0	Set the IP address of the loopback interface to 192.168.0.63/32.
(config-router)#exit	Exit Router mode.

Establish a Trunk with CSPF Disabled

OcNOS, Constrained Shortest Path First (CSPF) calculation is enabled by default.Typically, CSPF is disabled when all of the participating nodes do not support the required traffic engineering extensions and LSPs are configured manually to use an explicit path. In this case, an LSP is established only along the path specified by the operator.

Note: This example is based on the assumption that a minimal configuration exists on all participating routers as described in Enable Label Switching - Minimal Configuration.

Topology

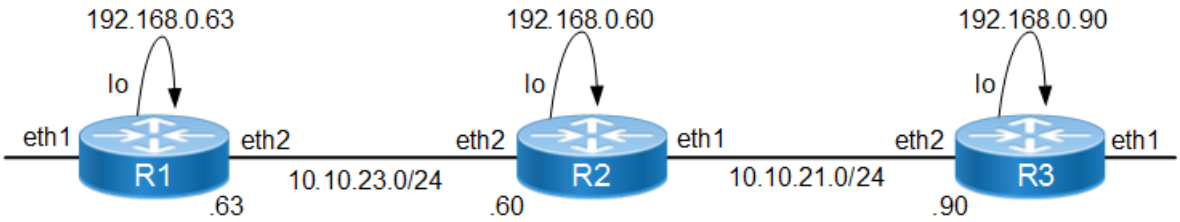


Figure 8-11: Basic Topology

R1 - RSVP-TE

`#configure terminal`	Enter configure mode.
`(config)#rsvp-trunk T1`	Create an RSVP trunk `T1` and enter the Trunk mode.
`(config-trunk)#no primary cspf`	Specify `no primary cspf` since CSPF is enabled by default.
`(config-trunk)#to 192.168.0.90`	Specify the IPv4 egress (destination point) for the LSP.

Establish a Trunk Using CSPF

The RSVP trunk can be configured using CSPF (Constraint-based Shortest Path First). In this case, the RSVP daemon (rsvpd) sends a request to the CSPF server to compute a path through the network to reach the destination. CSPF returns a hop-by-hop path called the Explicit Route to the RSVP daemon to be used in the Explicit Route Object (ERO). Each router along the path sends a `Path` message only to the nexthop specified in the ERO. In the OcNOS implementation, CSPF is enabled by default and if `no cspf` is not specified, the trunk is CSPF enabled automatically.

Note: This example is based on the assumption that a minimal configuration exists on all participating routers as described in Enable Label Switching - Minimal Configuration.

R1 (RSVP Daemon)

`#configure terminal`	Enter configure mode.
`(config)#rsvp-trunk T1`	Create an RSVP trunk `T1` and enter the Trunk mode.
`(config-trunk)#to 192.168.0.90`	Specify the IPv4 egress (destination point) for the LSP.

Mapping a Route to a Trunk

In the OcNOS implementation, a network can be mapped to a particular trunk using map-route configuration.

Note: This example is based on the assumption that a minimal configuration exists on all participating routers. For configuration details, refer to the “Establishing a Trunk - Minimal Configuration” section.

Topology

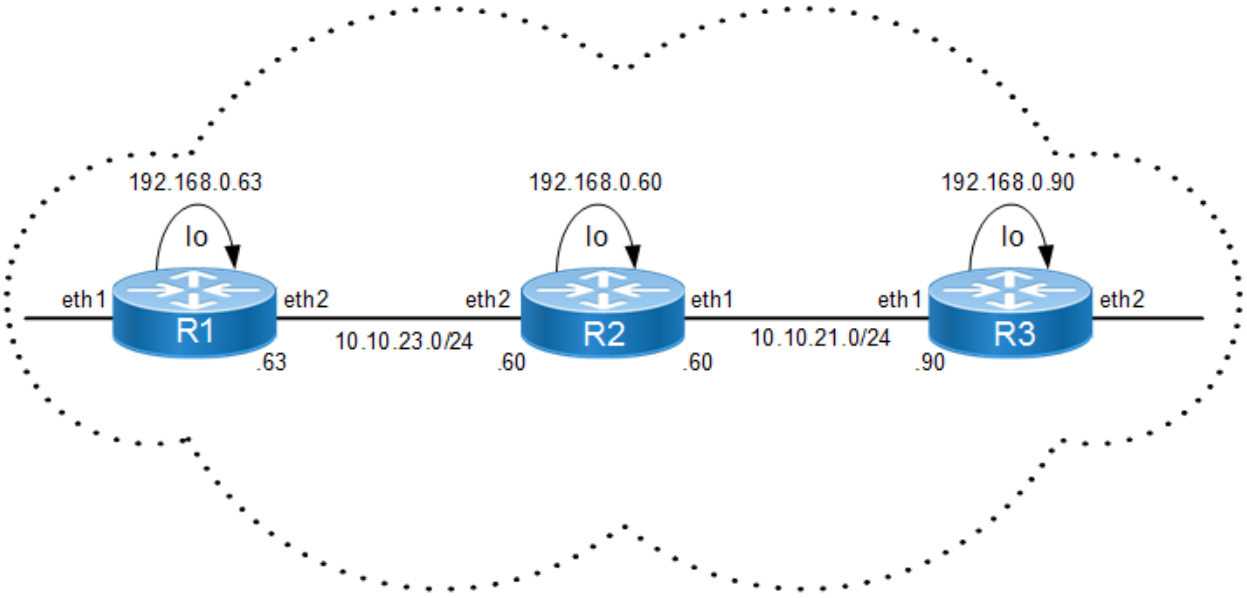


Figure 8-12: Topology for route mapping

R1 - RSVP-TE

`#configure terminal`	Enter configure mode.
`(config)#rsvp-trunk T1`	Create an RSVP trunk T1 and enter the Trunk mode.
`(config-trunk)#map-route 90.90.90.0/24`	Specify the destination prefix that needs to mapped to this trunk.
`(config-trunk)#to 192.168.0.90`	Specify the IPv4 egress (destination point) for the LSP.

Establish a Trunk Using Explicitly-Defined Path

Explicit Route hops can be configured manually in the trunk configuration. In this case, the RSVP daemon uses the configured hops as Explicit Route Objects (ERO). It sets up the LSP using specified hops only.

An ERO is composed of IP addresses called hops. An ERO hop can be defined as loose or strict. A loose hop can be reached by any available route. A strict hop must be reached via a direct link and cannot be routed over any alternate routers in between. In this example, since R3 is defined as loose hop, R2 can use R4 as an intermediate hop to reach R3. However, if it was a strict hop, then R2 would have to use interface `eth1` to reach R3 directly.

Note: This example is based on the assumption that a minimal configuration exists on all participating routers as described in Enable Label Switching - Minimal Configuration.

Topology

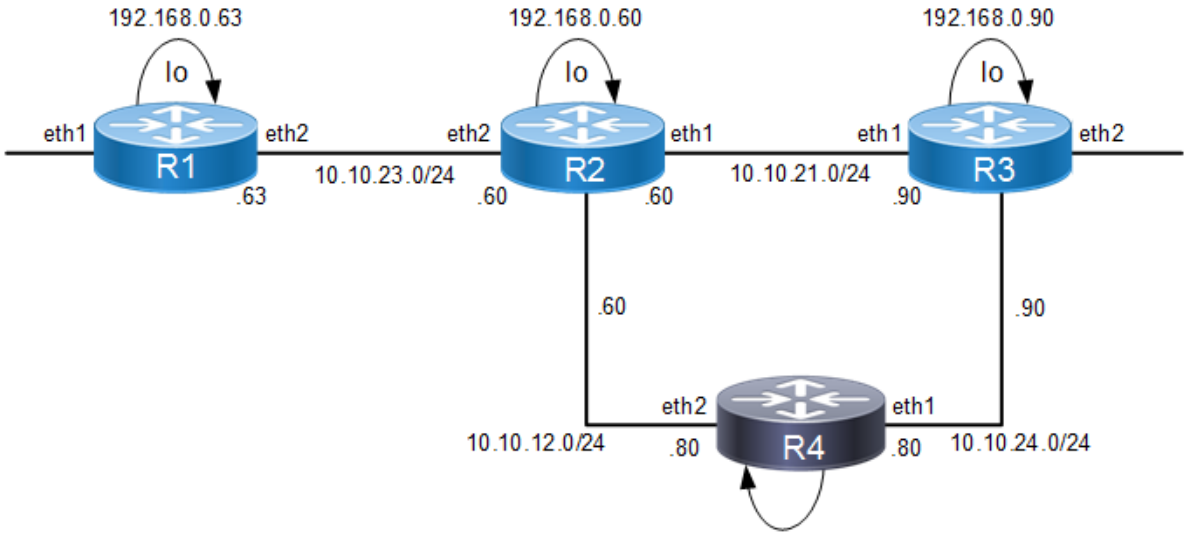


Figure 8-13: Topology for Explicitly Defined Path

R1 - RSVP-Path

`#configure terminal`	Enter configure mode.
`(config)#rsvp-path P1`	Create an RSVP Path `P1` and enter the `Path` mode.
`(config-path)#10.10.23.60 strict`	Configure this explicit route path as a `strict` hop.
`(config-path)#10.10.21.90 loose`	Configure this explicit route path as a `loose` hop.
`(config-path)#exit`	Exit `Path` mode.
`#configure terminal`	Enter configure mode.
`(config)#rsvp-trunk T1`	Create an RSVP trunk `T1` and enter the Trunk mode.
`(config-trunk)#no primary cspf`	Since CSPF is enabled by default, specify `no primary cspf` if CSPF is not required.
`(config-trunk)#primary path P1`	Configure trunk `T1` to use the defined path.
`(config-trunk)#to 192.168.0.90`	Specify the IPv4 egress (destination point) for the LSP.
`(config-trunk)#exit`	Exit `Trunk` mode.

Validation

```
R1#show rsvp session
Ingress RSVP:
To            From            State                Pri Rt  Style Labelin Labelout
LSPName                         Uptime  Est.time     DSType

192.168.0.90    192.168.0.63    Up                   Yes 1 2 SE    -       24321    T1-
Primary                        00:09:21 0s 3ms   DEFAULT
                      00:09:21 0s 3ms   DEFAULT
```

Add a Secondary LSP to the Trunk

Although the attributes of a Secondary LSP are independent of the Primary LSP, a Secondary LSP cannot be configured without first configuring a Primary LSP. In addition to information on how to configure a secondary LSP, this example illustrates how to define a non-default setup and the hold priority for an LSP. Setup and hold priorities are used to determine which LSP should be given a preference when competing for resources. Specifically, the setup priority of an un-established LSP is compared to the hold priorities of established LSPs, and the numerically lower one is given a preference. However, once the LSP is established, its setup priority is never used until it is pre-empted or reset and is being brought up again.

Note: This example is based on the assumption that a minimal configuration exists on all participating routers as described in Enable Label Switching - Minimal Configuration.

Note: If user provides the RSVP path option for secondary, the primary path exclusion logic gets disabled. User needs to keep primary and secondary path mutually exclusive. Else, RSVP-Primary LSP and RSVP-Secondary LSP may select the same next hop, when RSVP is configured with "loose". Hence RSVP-Path first next-hop should be "strict".

R1 - RSVP-TE

`#configure terminal`	Enter configure mode.
`(config)#rsvp-path myPath`	Specify an RSVP path to be used.
`(config-path)#10.10.23.60 strict`	Configure this explicit route path as a `strict` hop.
`(config-path)#exit`	Exit Path mode.
`(config)#rsvp-path myPath2`	Specify an RSVP path to be used.
`(config-path)#10.10.23.60 loose`	Configure this explicit route path as a `loose` hop.
`(config-path)#exit`	Exit Path mode.
`(config)#rsvp-trunk T1`	Create an RSVP trunk `T1` and enter the Trunk mode.
`(config-trunk)#no secondary cspf`	Since CSPF is enabled by default, specify `no secondary cspf` if CSPF is not required.
`(config-trunk)#primary path myPath`	Specify an RSVP path to be used.
`(config-trunk)#no secondary cspf`	Specify the `no secondary cspf` option for the Secondary LSP.
`(config-trunk)#secondary path myPath2`	Specify an RSVP path to be used.
`(config-trunk)#to 192.168.0.90`	Specify the IPv4 egress (destination point) for the LSP.
`(config-trunk)#exit`	Exit `Trunk` mode.

Validation

This example shows the number of configured RSVP sessions in a router.

R1

```
#show rsvp session count
Total configured: 50000, Up 50000, Down 0

Total ingress sessions: 50000, Up 50000, Down 0
Total transit sessions: 0, Up 0, Down 0
Total egress sessions: 0, Up 0, Down 0
```

Add Multiple Secondary LSP to the trunk

RSVP Multiple Secondary feature tries to provide continuous protection when multiple failures happen. In majority scenarios, feature tries to provide seamless protection. This is a proprietary feature where user can configure multiple secondary sessions in a rsvp-trunk. Each secondary will be associated with a priority. Priority secondary sessions must be programmed with a predefined path. User can configure a maximum of five priority levels. Lowest priority number corresponds to highest priority. Highest priority session will be signaled to be programmed as secondary session. If highest priority session cannot come up, then next available secondary will be selected based on polling. During primary session fail-over, programmed secondary priority session will protect the primary and then goes for an MBB update to act as the primary session until primary comes up. Once the highest priority session comes up as acting primary session, next available secondary priority session will be programmed to signal and come up secondary. Re-optimization timer executed once in every 5 minutes to ensure the best priority session serves as secondary. Configuration updates on secondary priority configurations doesn't trigger MBB and session will be restarted. This example illustrates how to create SVI, enable IGP protocols and RSVP on SVI.

Note: Ensure that the VLAN is configured before creating SVI.

Topology

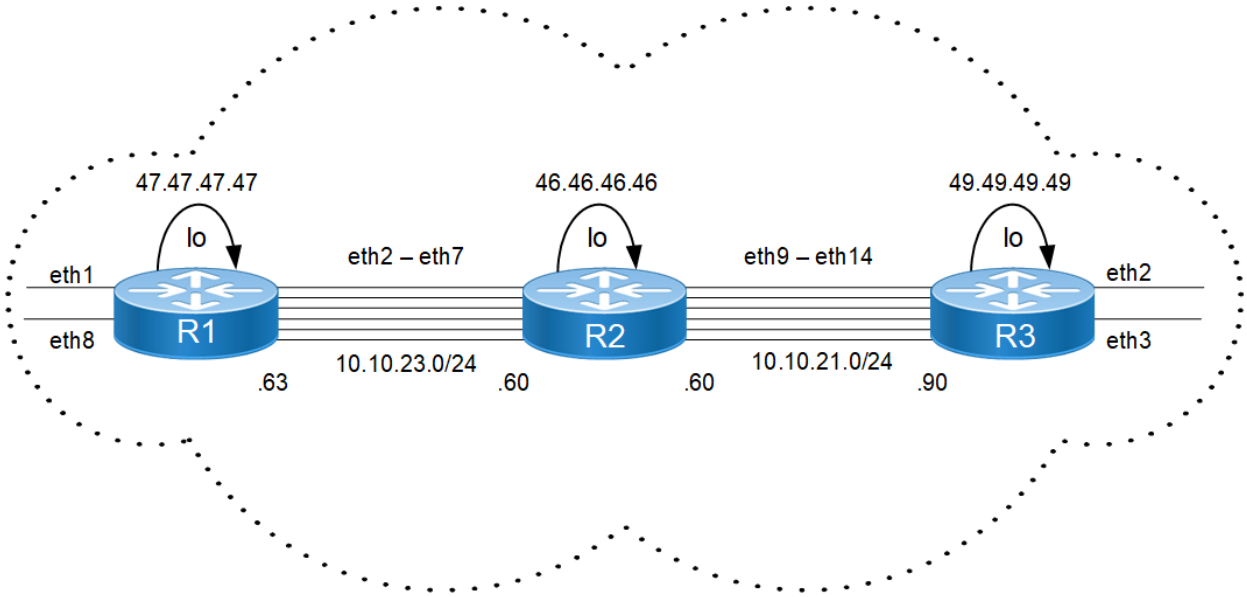


Figure 8-14: Topology for Multiple Secondary Protection

Bridge Configuration

bridge 1 protocol ieee vlan-bridge

no bridge 1 spanning-tree enable bridge-forward

VLAN creation

vlan database

vlan 2-7 bridge 1 state enable

vlan 501-506 bridge 1 state enable

R1

`#configure terminal`	Enter configure mode.
`(config)#router rsvp`	Enable RSVP globally.
`(config-router)#exit`	Exit RSVP mode.
`(config)#interface vlan1.2`	Enter the interface mode.
`(config-if)#ip address 10.10.23.1/24`	Configure the IP Address
`(config-if)#mtu 1600`	Configure MTU size.
`(config-if)#label-switching`	Enable MPLS.
`(config-if)#ip ospf network point-to-point`	Enable OSPF point-to-point network type.
`(config-if)#enable-rsvp`	Enable RSVP at the interface level.
`(config-if)#exit`	Exit the interface mode.
`(config)#interface vlan1.3`	Enter the interface mode.
`(config-if)#ip address 10.10.24.1/24`	Configure the IP Address
`(config-if)#mtu 1600`	Configure MTU size.
`(config-if)#label-switching`	Enable MPLS.
`(config-if)#ip ospf network point-to-point`	Enable OSPF point-to-point network type.
`(config-if)#enable-rsvp`	Enable RSVP at the interface level.
`(config-if)#exit`	Exit the interface mode.
`(config)#interface vlan1.4`	Enter the interface mode.
`(config-if)#ip address 10.10.25.1/24`	Configure the IP Address
`(config-if)#mtu 1600`	Configure MTU size.
`(config-if)#label-switching`	Enable MPLS.
`(config-if)#ip ospf network point-to-point`	Enable OSPF point-to-point network type.
`(config-if)#enable-rsvp`	Enable RSVP at the interface level.
`(config-if)#exit`	Exit the interface mode.
`(config)#interface vlan1.5`	Enter the interface mode.
`(config-if)#ip address 10.10.26.1/24`	Configure the IP Address
`(config-if)#mtu 1600`	Configure MTU size.
`(config-if)#label-switching`	Enable MPLS.
`(config-if)#ip ospf network point-to-point`	Enable OSPF point-to-point network type.
`(config-if)#enable-rsvp`	Enable RSVP at the interface level.
`(config-if)#exit`	Exit the interface mode.
`(config)#interface vlan1.6`	Enter the interface mode.
`(config-if)#ip address 10.10.27.1/24`	Configure the IP Address
`(config-if)#mtu 1600`	Configure MTU size.
`(config-if)#label-switching`	Enable MPLS.
`(config-if)#ip ospf network point-to-point`	Enable OSPF point-to-point network type.
`(config-if)#enable-rsvp`	Enable RSVP at the interface level.
`(config-if)#exit`	Exit the interface mode.
`(config)#interface vlan1.7`	Enter the interface mode.

(config-if)#ip address 10.10.28.1/24	Configure the IP Address
(config-if)#mtu 1600	Configure MTU size.
(config-if)#label-switching	Enable MPLS.
(config-if)#ip ospf network point-to-point	Enable OSPF point-to-point network type.
(config-if)#enable-rsvp	Enable RSVP at the interface level.
(config-if)#exit	Exit the interface mode.
(config)#interface eth2	Enter the interface mode.
(config-if)#switchport	Configure Switchport
(config-if)#bridge-group 1	Assign a Bridge ID to the port channel
(config-if)#switchport mode trunk	Configure trunk
(config-if)#switchport trunk allowed vlan add 2,501	Configure allowed VLANs
(config-if)#switchport trunk native vlan 501	Configure native VLAN.
(config-if)# load-interval 30	Set load interval
(config-if)# mtu 9192	Configure the MTU Size.
(config-if)#exit	Exit the interface mode.
(config)#interface eth3	Enter the interface mode.
(config-if)#switchport	Configure Switchport
(config-if)#bridge-group 1	Assign a Bridge ID to the port channel
(config-if)#switchport mode trunk	Configure trunk
(config-if)#switchport trunk allowed vlan add 3,502	Configure allowed VLANs
(config-if)#switchport trunk native vlan 502	Configure native VLAN.
(config-if)# load-interval 30	Set load interval
(config-if)# mtu 9192	Configure the MTU Size.
(config-if)#exit	Exit the interface mode.
(config)#interface eth4	Enter the interface mode.
(config-if)#switchport	Configure Switchport
(config-if)#bridge-group 1	Assign a Bridge ID to the port channel
(config-if)#switchport mode trunk	Configure trunk
(config-if)#switchport trunk allowed vlan add 4,503	Configure allowed VLANs
(config-if)#switchport trunk native vlan 503	Configure native VLAN.
(config-if)# load-interval 30	Set load interval
(config-if)# mtu 9192	Configure the MTU Size.
(config-if)#exit	Exit the interface mode.
(config)#interface eth5	Enter the interface mode.
(config-if)#switchport	Configure Switchport
(config-if)#bridge-group 1	Assign a Bridge ID to the port channel
(config-if)#switchport mode trunk	Configure trunk
(config-if)#switchport trunk allowed vlan add 5,504	Configure allowed VLANs

(config-if)#switchport trunk native vlan 504	Configure native VLAN.
(config-if)# load-interval 30	Set load interval
(config-if)# mtu 9192	Configure the MTU Size.
(config-if)#exit	Exit the interface mode.
(config)#interface eth6	Enter the interface mode.
(config-if)#switchport	Configure Switchport
(config-if)#bridge-group 1	Assign a Bridge ID to the port channel
(config-if)#switchport mode trunk	Configure trunk
(config-if)#switchport trunk allowed vlan add 6,505	Configure allowed VLANs
(config-if)#switchport trunk native vlan 505	Configure native VLAN.
(config-if)# load-interval 30	Set load interval
(config-if)# mtu 9192	Configure the MTU Size.
(config-if)#exit	Exit the interface mode.
(config)#interface eth7	Enter the interface mode.
(config-if)#switchport	Configure Switchport
(config-if)#bridge-group 1	Assign a Bridge ID to the port channel
(config-if)#switchport mode trunk	Configure trunk
(config-if)#switchport trunk allowed vlan add 7,506	Configure allowed VLANs
(config-if)#switchport trunk native vlan 506	Configure native VLAN.
(config-if)# load-interval 30	Set load interval
(config-if)# mtu 9192	Configure the MTU Size.
(config-if)#exit	Exit the interface mode.
(conf)#rsvp-path p1-r1-r3 mpls	Create RSVP path
(conf-path)# 10.10.23.2 strict	Configure nexthop
(conf-path)# 10.10.21.2 strict	Configure nexthop
(conf)#rsvp-path sp1-r1-r3 mpls	Create RSVP path
(conf-path)#10.10.24.2 strict	Configure nexthop
(conf-path)#10.10.22.2 strict	Configure nexthop
(conf)#rsvp-path sp2-r1-r3 mpls	Create RSVP path
(conf-path)#10.10.25.2 strict	Configure nexthop
(conf-path)# 10.10.29.2 strict	Configure nexthop
(conf)#rsvp-path sp3-r1-r3 mpls	Create RSVP path
(conf-path)#10.10.26.2 strict	Configure nexthop
(conf-path)# 10.10.30.2 strict	Configure nexthop
(conf)#rsvp-path sp4-r1-r3 mpls	Create RSVP path
(conf-path)#10.10.27.2 strict	Configure nexthop
(conf-path)# 10.10.31.2 strict	Configure nexthop
(conf)#rsvp-path sp5-r1-r3 mpls	Create RSVP path
(conf-path)# 10.10.28.2 strict	Configure nexthop

(conf-path)#10.10.32.2 strict	Configure nexthop
(conf)#rsvp-trunk 47-49-test ipv4	Create a RSVP trunk link
(conf-trunk)#primary path p1-r1-r3	Configure primary path for trunk link
(conf-trunk)# secondary-priority 1 path sp1-r1-r3	Configure secondary link for trunk link
(conf-trunk)#secondary-priority 2 path sp2-r1-r3	Configure secondary link for trunk link
(conf-trunk)#secondary-priority 3 path sp3-r1-r3	Configure secondary link for trunk link
(conf-trunk)#secondary-priority 4 path sp4-r1-r3	Configure secondary link for trunk link
(conf-trunk)#secondary-priority 5 path sp5-r1-r3	Configure secondary link for trunk link
(conf-trunk)#to 49.49.49.49	Configure remote node for the LSP

Validation

This example shows the number of configured RSVP sessions in a router.

R1

```
 # show rsvp session
Type  : PRI - Primary, SEC - Secondary, DTR - Detour, BPS - Bypass
State : UP - Up, DN - Down, BU - Backup in Use, SU - Secondary in Use, FS - Forced to Secondary
* indicates the session is active with local repair at one or more nodes
(P) indicates the secondary-priority session is acting as primary

Ingress RSVP:
To              From            Type    LSPName                          State Uptime    Rt Style  Labelin  Labelout  DSType
49.49.49.49     47.47.47.47      PRI     47-49-test-Primary               UP    00:32:35 1 1 SE     -         24961     DEFAULT
49.49.49.49     47.47.47.47      SEC     47-49-test-Secondary-Priority-1 UP    00:32:35 1 1 SE     -         24962     DEFAULT
Total 2 displayed, Up 2, Down 0.

Egress RSVP:
To              From            Type    LSPName                          State Uptime    Rt Style  Labelin  Labelout  DSType
47.47.47.47     49.49.49.49      PRI     49-47-test-Primary               UP    00:32:53 1 1 SE     24964     -         ELSP_CON
47.47.47.47     49.49.49.49      PRI     49-47-test-Secondary-Priority-1 UP    00:32:47 1 1 SE     24962     -         ELSP_CON
Total 2 displayed, Up 2, Down 0.

# show rsvp trunk multi-sec-detail
Ingress (Secondary-Priority1)
49.49.49.49
  From: 47.47.47.47, LSPstate: Up, LSPname: 47-49-test-Secondary-Priority-1
  Ingress FSM state: Operational
  Establishment Time: 0s 253ms
```

```
  Setup priority: 7, Hold priority: 0
  CSPF usage: Enabled, CSPF Retry Count: 0, CSPF Retry Interval: 30 seconds
  LSP Re-Optimization: Disabled, Re-Optimization Timer: NA, Cspf Client: OSPF
  IGP-Shortcut: Disabled, LSP metric: 3
  LSP Protection: None
  Label in: -,  Label out:    24962,
  Tspec rate: 0, Fspec rate: 0
  Policer: Not Configured
  Tunnel Id: 5001, LSP Id: 2219, Ext-Tunnel Id: 47.47.47.47
  Downstream: 47.46.3.2, vlan1.1003
  Path refresh: 30 seconds (RR enabled) (due in 27970 seconds)
  Resv lifetime: 157 seconds (due in 138 seconds)
  Retry count: 0, intrvl: 30 seconds
  RRO re-use as ERO: Disabled
  Label Recording: Disabled
  Admin Groups: none
  Configured Path: SP1-47-49 (in use)
  Configured Explicit Route Detail :
   47.46.3.2/32 strict
   46.45.9.2/32 strict
   45.49.24.2/32 strict
  Session Explicit Route Detail :
   47.46.3.2/32 strict
   46.45.9.2/32 strict
   45.49.24.2/32 strict
  Record route:
   ----------------------------------------------------------------
   IP Address        Label
   ----------------------------------------------------------------
   <self>
   47.46.3.2
   46.45.9.2
   45.49.24.2
  Style: Shared Explicit Filter
  Traffic type: controlled-load
  Minimum Path MTU: 9216
  Last Recorded Error Code: None
  Last Recorded Error Value: None
  Node where Last Recorded Error originated: None
  Trunk Type: mpls
Ingress (Secondary-Priority2)
49.49.49.49
  From: 47.47.47.47, LSPstate: Dn, LSPname: 47-49-test-Secondary-Priority-2
  Ingress FSM state: Idle
  Setup priority: 7, Hold priority: 0
  CSPF usage: Enabled, CSPF Retry Count: 0, CSPF Retry Interval: 30 seconds
  LSP Re-Optimization: Disabled, Re-Optimization Timer: NA, Cspf Client: NA
  IGP-Shortcut: Disabled, LSP metric: 3
  LSP Protection: None
  Label in: -,  Label out: -,
```

```
  Tspec rate: 0, Fspec rate: 0
  Policer: Not Configured
  Tunnel Id: 5001, LSP Id: 2223, Ext-Tunnel Id: 47.47.47.47
  Last Recorded Error Code: None
  Last Recorded Error Value: None
  Node where Last Recorded Error originated: None
  Trunk Type: mpls
Ingress (Secondary-Priority3)
49.49.49.49
  From: 47.47.47.47, LSPstate: Dn, LSPname: 47-49-test-Secondary-Priority-3
  Ingress FSM state: Idle
  Setup priority: 7, Hold priority: 0
  CSPF usage: Enabled, CSPF Retry Count: 0, CSPF Retry Interval: 30 seconds
  LSP Re-Optimization: Disabled, Re-Optimization Timer: NA, Cspf Client: NA
  IGP-Shortcut: Disabled, LSP metric: 65
  LSP Protection: None
  Label in: -,  Label out: -,
  Tspec rate: 0, Fspec rate: 0
  Policer: Not Configured
  Tunnel Id: 5001, LSP Id: 2219, Ext-Tunnel Id: 47.47.47.47
  Last Recorded Error Code: Routing Problem (24)
  Last Recorded Error Value: No route available toward destination (5)
  Node where Last Recorded Error originated: None
  Trunk Type: mpls
Ingress (Secondary-Priority4)
49.49.49.49
  From: 47.47.47.47, LSPstate: Dn, LSPname: 47-49-test-Secondary-Priority-4
  Ingress FSM state: Idle
  Setup priority: 7, Hold priority: 0
  CSPF usage: Enabled, CSPF Retry Count: 0, CSPF Retry Interval: 30 seconds
  LSP Re-Optimization: Disabled, Re-Optimization Timer: NA, Cspf Client: NA
  IGP-Shortcut: Disabled, LSP metric: 65
  LSP Protection: None
  Label in: -,  Label out: -,
  Tspec rate: 0, Fspec rate: 0
  Policer: Not Configured
  Tunnel Id: 5001, LSP Id: 2219, Ext-Tunnel Id: 47.47.47.47
  Last Recorded Error Code: Routing Problem (24)
  Last Recorded Error Value: No route available toward destination (5)
  Node where Last Recorded Error originated: None
  Trunk Type: mpls
Ingress (Secondary-Priority5)
49.49.49.49
  From: 47.47.47.47, LSPstate: Dn, LSPname: 47-49-test-Secondary-Priority-5
  Ingress FSM state: Idle
  Setup priority: 7, Hold priority: 0
  CSPF usage: Enabled, CSPF Retry Count: 0, CSPF Retry Interval: 30 seconds
  LSP Re-Optimization: Disabled, Re-Optimization Timer: NA, Cspf Client: NA
  IGP-Shortcut: Disabled, LSP metric: 65
  LSP Protection: None
```

```
Label in: -,  Label out: -,
Tspec rate: 0, Fspec rate: 0
Policer: Not Configured
Tunnel Id: 5001, LSP Id: 2219, Ext-Tunnel Id: 47.47.47.47
Last Recorded Error Code: Routing Problem (24)
Last Recorded Error Value: No route available toward destination (5)
Node where Last Recorded Error originated: None
Trunk Type: mpls
```

R2

Bridge Configuration

bridge 1 protocol ieee vlan-bridge

no bridge 1 spanning-tree enable bridge-forward

VLAN creation (Peer configuration for R1)

vlan database

vlan 2-7 bridge 1 state enable

vlan 507-5012 bridge 1 state enable

VLAN creation (Peer configuration for R3)

vlan database

vlan 9-14 bridge 1 state enable

vlan 513-518 bridge 1 state enable

`#configure terminal`	Enter configure mode.
`(config)#router rsvp`	Enable RSVP globally.
`(config-router)#exit`	Exit RSVP mode.
`(config)#interface vlan1.2`	Enter the interface mode.
`(config-if)#ip address 10.10.23.2/24`	Configure the IP Address
`(config-if)#mtu 1600`	Configure MTU size.
`(config-if)#label-switching`	Enable MPLS.
`(config-if)#ip ospf network point-to-point`	Enable OSPF point-to-point network type.
`(config-if)#enable-rsvp`	Enable RSVP at the interface level.
`(config-if)#exit`	Exit the interface mode.
`(config)#interface vlan1.3`	Enter the interface mode.
`(config-if)#ip address 10.10.24.2/24`	Configure the IP Address
`(config-if)#mtu 1600`	Configure MTU size.
`(config-if)#label-switching`	Enable MPLS.

(config-if)#ip ospf network point-to-point	Enable OSPF point-to-point network type.
(config-if)#enable-rsvp	Enable RSVP at the interface level.
(config-if)#exit	Exit the interface mode.
(config)#interface vlan1.4	Enter the interface mode.
(config-if)#ip address 10.10.25.2/24	Configure the IP Address
(config-if)#mtu 1600	Configure MTU size.
(config-if)#label-switching	Enable MPLS.
(config-if)#ip ospf network point-to-point	Enable OSPF point-to-point network type.
(config-if)#enable-rsvp	Enable RSVP at the interface level.
(config-if)#exit	Exit the interface mode.
(config)#interface vlan1.5	Enter the interface mode.
(config-if)#ip address 10.10.26.2/24	Configure the IP Address
(config-if)#mtu 1600	Configure MTU size.
(config-if)#label-switching	Enable MPLS.
(config-if)#ip ospf network point-to-point	Enable OSPF point-to-point network type.
(config-if)#enable-rsvp	Enable RSVP at the interface level.
(config-if)#exit	Exit the interface mode.
(config)#interface vlan1.6	Enter the interface mode.
(config-if)#ip address 10.10.27.2/24	Configure the IP Address
(config-if)#mtu 1600	Configure MTU size.
(config-if)#label-switching	Enable MPLS.
(config-if)#ip ospf network point-to-point	Enable OSPF point-to-point network type.
(config-if)#enable-rsvp	Enable RSVP at the interface level.
(config-if)#exit	Exit the interface mode.
(config)#interface vlan1.7	Enter the interface mode.
(config-if)#ip address 10.10.28.2/24	Configure the IP Address
(config-if)#mtu 1600	Configure MTU size.
(config-if)#label-switching	Enable MPLS.
(config-if)#ip ospf network point-to-point	Enable OSPF point-to-point network type.
(config-if)#enable-rsvp	Enable RSVP at the interface level.
(config-if)#exit	Exit the interface mode.
(config)#interface vlan1.9	Enter the interface mode.
(config-if)#ip address 10.10.21.1/24	Configure the IP Address
(config-if)#mtu 1600	Configure MTU size.
(config-if)#label-switching	Enable MPLS.
(config-if)#ip ospf network point-to-point	Enable OSPF point-to-point network type.
(config-if)#enable-rsvp	Enable RSVP at the interface level.
(config-if)#exit	Exit the interface mode.
(config)#interface vlan1.10	Enter the interface mode.
(config-if)#ip address 10.10.22.1/24	Configure the IP Address
(config-if)#mtu 1600	Configure MTU size.

(config-if)#label-switching	Enable MPLS.
(config-if)#ip ospf network point-to-point	Enable OSPF point-to-point network type.
(config-if)#enable-rsvp	Enable RSVP at the interface level.
(config-if)#exit	Exit the interface mode.
(config)#interface vlan1.11	Enter the interface mode.
(config-if)#ip address 10.10.29.1/24	Configure the IP Address
(config-if)#mtu 1600	Configure MTU size.
(config-if)#label-switching	Enable MPLS.
(config-if)#ip ospf network point-to-point	Enable OSPF point-to-point network type.
(config-if)#enable-rsvp	Enable RSVP at the interface level.
(config-if)#exit	Exit the interface mode.
(config)#interface vlan1.12	Enter the interface mode.
(config-if)#ip address 10.10.30.1/24	Configure the IP Address
(config-if)#mtu 1600	Configure MTU size.
(config-if)#label-switching	Enable MPLS.
(config-if)#ip ospf network point-to-point	Enable OSPF point-to-point network type.
(config-if)#enable-rsvp	Enable RSVP at the interface level.
(config-if)#exit	Exit the interface mode.
(config)#interface vlan1.13	Enter the interface mode.
(config-if)#ip address 10.10.31.1/24	Configure the IP Address
(config-if)#mtu 1600	Configure MTU size.
(config-if)#label-switching	Enable MPLS.
(config-if)#ip ospf network point-to-point	Enable OSPF point-to-point network type.
(config-if)#enable-rsvp	Enable RSVP at the interface level.
(config-if)#exit	Exit the interface mode.
(config)#interface vlan1.14	Enter the interface mode.
(config-if)#ip address 10.10.32.1/24	Configure the IP Address
(config-if)#mtu 1600	Configure MTU size.
(config-if)#label-switching	Enable MPLS.
(config-if)#ip ospf network point-to-point	Enable OSPF point-to-point network type.
(config-if)#enable-rsvp	Enable RSVP at the interface level.
(config-if)#exit	Exit the interface mode.
(config)#interface eth2	Enter the interface mode.
(config-if)#switchport	Configure Switchport
(config-if)#bridge-group 1	Assign a Bridge ID to the port channel
(config-if)#switchport mode trunk	Configure trunk
(config-if)#switchport trunk allowed vlan add 2,507	Configure allowed VLANs
(config-if)#switchport trunk native vlan 507	Configure native VLAN.
(config-if)# load-interval 30	Set load interval
(config-if)# mtu 9192	Configure the MTU Size.

(config-if)#exit	Exit the interface mode.
(config)#interface eth3	Enter the interface mode.
(config-if)#switchport	Configure Switchport
(config-if)#bridge-group 1	Assign a Bridge ID to the port channel
(config-if)#switchport mode trunk	Configure trunk
(config-if)#switchport trunk allowed vlan add 3,508	Configure allowed VLANs
(config-if)#switchport trunk native vlan 508	Configure native VLAN.
(config-if)# load-interval 30	Set load interval
(config-if)# mtu 9192	Configure the MTU Size.
(config-if)#exit	Exit the interface mode.
(config)#interface eth4	Enter the interface mode.
(config-if)#switchport	Configure Switchport
(config-if)#bridge-group 1	Assign a Bridge ID to the port channel
(config-if)#switchport mode trunk	Configure trunk
(config-if)#switchport trunk allowed vlan add 4,509	Configure allowed VLANs
(config-if)#switchport trunk native vlan 509	Configure native VLAN.
(config-if)# load-interval 30	Set load interval
(config-if)# mtu 9192	Configure the MTU Size.
(config-if)#exit	Exit the interface mode.
(config)#interface eth5	Enter the interface mode.
(config-if)#switchport	Configure Switchport
(config-if)#bridge-group 1	Assign a Bridge ID to the port channel
(config-if)#switchport mode trunk	Configure trunk
(config-if)#switchport trunk allowed vlan add 5,510	Configure allowed VLANs
(config-if)#switchport trunk native vlan 510	Configure native VLAN.
(config-if)# load-interval 30	Set load interval
(config-if)# mtu 9192	Configure the MTU Size.
(config-if)#exit	Exit the interface mode.
(config)#interface eth6	Enter the interface mode.
(config-if)#switchport	Configure Switchport
(config-if)#bridge-group 1	Assign a Bridge ID to the port channel
(config-if)#switchport mode trunk	Configure trunk
(config-if)#switchport trunk allowed vlan add 6,511	Configure allowed VLANs
(config-if)#switchport trunk native vlan 511	Configure native VLAN.
(config-if)# load-interval 30	Set load interval
(config-if)# mtu 9192	Configure the MTU Size.
(config-if)#exit	Exit the interface mode.
(config)#interface eth7	Enter the interface mode.

(config-if)#switchport	Configure Switchport
(config-if)#bridge-group 1	Assign a Bridge ID to the port channel
(config-if)#switchport mode trunk	Configure trunk
(config-if)#switchport trunk allowed vlan add 7,512	Configure allowed VLANs
(config-if)#switchport trunk native vlan 512	Configure native VLAN.
(config-if)# load-interval 30	Set load interval
(config-if)# mtu 9192	Configure the MTU Size.
(config-if)#exit	Exit the interface mode.
(config)#interface eth9	Enter the interface mode.
(config-if)#switchport	Configure Switchport
(config-if)#bridge-group 1	Assign a Bridge ID to the port channel
(config-if)#switchport mode trunk	Configure trunk
(config-if)#switchport trunk allowed vlan add 9,513	Configure allowed VLANs
(config-if)#switchport trunk native vlan 513	Configure native VLAN.
(config-if)# load-interval 30	Set load interval
(config-if)# mtu 9192	Configure the MTU Size.
(config-if)#exit	Exit the interface mode.
(config)#interface eth10	Enter the interface mode.
(config-if)#switchport	Configure Switchport
(config-if)#bridge-group 1	Assign a Bridge ID to the port channel
(config-if)#switchport mode trunk	Configure trunk
(config-if)#switchport trunk allowed vlan add 10,514	Configure allowed VLANs
(config-if)#switchport trunk native vlan 514	Configure native VLAN.
(config-if)# load-interval 30	Set load interval
(config-if)# mtu 9192	Configure the MTU Size.
(config-if)#exit	Exit the interface mode.
(config)#interface eth11	Enter the interface mode.
(config-if)#switchport	Configure Switchport
(config-if)#bridge-group 1	Assign a Bridge ID to the port channel
(config-if)#switchport mode trunk	Configure trunk
(config-if)#switchport trunk allowed vlan add 11,515	Configure allowed VLANs
(config-if)#switchport trunk native vlan 515	Configure native VLAN.
(config-if)# load-interval 30	Set load interval
(config-if)# mtu 9192	Configure the MTU Size.
(config-if)#exit	Exit the interface mode.
(config)#interface eth12	Enter the interface mode.
(config-if)#switchport	Configure Switchport
(config-if)#bridge-group 1	Assign a Bridge ID to the port channel

(config-if)#switchport mode trunk	Configure trunk
(config-if)#switchport trunk allowed vlan add 12,516	Configure allowed VLANs
(config-if)#switchport trunk native vlan 516	Configure native VLAN.
(config-if)# load-interval 30	Set load interval
(config-if)# mtu 9192	Configure the MTU Size.
(config-if)#exit	Exit the interface mode.
(config)#interface eth13	Enter the interface mode.
(config-if)#switchport	Configure Switchport
(config-if)#bridge-group 1	Assign a Bridge ID to the port channel
(config-if)#switchport mode trunk	Configure trunk
(config-if)#switchport trunk allowed vlan add 13,517	Configure allowed VLANs
(config-if)#switchport trunk native vlan 517	Configure native VLAN.
(config-if)# load-interval 30	Set load interval
(config-if)# mtu 9192	Configure the MTU Size.
(config-if)#exit	Exit the interface mode.
(config)#interface eth14	Enter the interface mode.
(config-if)#switchport	Configure Switchport
(config-if)#bridge-group 1	Assign a Bridge ID to the port channel
(config-if)#switchport mode trunk	Configure trunk
(config-if)#switchport trunk allowed vlan add 14,518	Configure allowed VLANs
(config-if)#switchport trunk native vlan 518	Configure native VLAN.
(config-if)# load-interval 30	Set load interval
(config-if)# mtu 9192	Configure the MTU Size.
(config-if)#exit	Exit the interface mode.

R3

Bridge Configuration

bridge 1 protocol ieee vlan-bridge

no bridge 1 spanning-tree enable bridge-forward

VLAN creation

vlan database

vlan 9-14 bridge 1 state enable

vlan 519-524 bridge 1 state enable

#configure terminal	Enter configure mode.
(config)#router rsvp	Enable RSVP globally.
(config-router)#exit	Exit RSVP mode.

(config)#interface vlan1.9	Enter the interface mode.
(config-if)#ip address 10.10.21.2/24	Configure the IP Address
(config-if)#mtu 1600	Configure MTU size.
(config-if)#label-switching	Enable MPLS.
(config-if)#ip ospf network point-to-point	Enable OSPF point-to-point network type.
(config-if)#enable-rsvp	Enable RSVP at the interface level.
(config-if)#exit	Exit the interface mode.
(config)#interface vlan1.10	Enter the interface mode.
(config-if)#ip address 10.10.22.2/24	Configure the IP Address
(config-if)#mtu 1600	Configure MTU size.
(config-if)#label-switching	Enable MPLS.
(config-if)#ip ospf network point-to-point	Enable OSPF point-to-point network type.
(config-if)#enable-rsvp	Enable RSVP at the interface level.
(config-if)#exit	Exit the interface mode.
(config)#interface vlan1.11	Enter the interface mode.
(config-if)#ip address 10.10.29.2/24	Configure the IP Address
(config-if)#mtu 1600	Configure MTU size.
(config-if)#label-switching	Enable MPLS.
(config-if)#ip ospf network point-to-point	Enable OSPF point-to-point network type.
(config-if)#enable-rsvp	Enable RSVP at the interface level.
(config-if)#exit	Exit the interface mode.
(config)#interface vlan1.12	Enter the interface mode.
(config-if)#ip address 10.10.30.2/24	Configure the IP Address
(config-if)#mtu 1600	Configure MTU size.
(config-if)#label-switching	Enable MPLS.
(config-if)#ip ospf network point-to-point	Enable OSPF point-to-point network type.
(config-if)#enable-rsvp	Enable RSVP at the interface level.
(config-if)#exit	Exit the interface mode.
(config)#interface vlan1.13	Enter the interface mode.
(config-if)#ip address 10.10.31.2/24	Configure the IP Address
(config-if)#mtu 1600	Configure MTU size.
(config-if)#label-switching	Enable MPLS.
(config-if)#ip ospf network point-to-point	Enable OSPF point-to-point network type.
(config-if)#enable-rsvp	Enable RSVP at the interface level.
(config-if)#exit	Exit the interface mode.
(config)#interface vlan1.14	Enter the interface mode.
(config-if)#ip address 10.10.32.2/24	Configure the IP Address
(config-if)#mtu 1600	Configure MTU size.
(config-if)#label-switching	Enable MPLS.
(config-if)#ip ospf network point-to-point	Enable OSPF point-to-point network type.
(config-if)#enable-rsvp	Enable RSVP at the interface level.

(config-if)#exit	Exit the interface mode.
(config)#interface eth9	Enter the interface mode.
(config-if)#switchport	Configure Switchport
(config-if)#bridge-group 1	Assign a Bridge ID to the port channel
(config-if)#switchport mode trunk	Configure trunk
(config-if)#switchport trunk allowed vlan add 9,519	Configure allowed VLANs
(config-if)#switchport trunk native vlan 519	Configure native VLAN.
(config-if)# load-interval 30	Set load interval
(config-if)# mtu 9192	Configure the MTU Size.
(config-if)#exit	Exit the interface mode.
(config)#interface eth10	Enter the interface mode.
(config-if)#switchport	Configure Switchport
(config-if)#bridge-group 1	Assign a Bridge ID to the port channel
(config-if)#switchport mode trunk	Configure trunk
(config-if)#switchport trunk allowed vlan add 10,520	Configure allowed VLANs
(config-if)#switchport trunk native vlan 520	Configure native VLAN.
(config-if)# load-interval 30	Set load interval
(config-if)# mtu 9192	Configure the MTU Size.
(config-if)#exit	Exit the interface mode.
(config)#interface eth11	Enter the interface mode.
(config-if)#switchport	Configure Switchport
(config-if)#bridge-group 1	Assign a Bridge ID to the port channel
(config-if)#switchport mode trunk	Configure trunk
(config-if)#switchport trunk allowed vlan add 11,521	Configure allowed VLANs
(config-if)#switchport trunk native vlan 521	Configure native VLAN.
(config-if)# load-interval 30	Set load interval
(config-if)# mtu 9192	Configure the MTU Size.
(config-if)#exit	Exit the interface mode.
(config)#interface eth12	Enter the interface mode.
(config-if)#switchport	Configure Switchport
(config-if)#bridge-group 1	Assign a Bridge ID to the port channel
(config-if)#switchport mode trunk	Configure trunk
(config-if)#switchport trunk allowed vlan add 12,522	Configure allowed VLANs
(config-if)#switchport trunk native vlan 522	Configure native VLAN.
(config-if)# load-interval 30	Set load interval
(config-if)# mtu 9192	Configure the MTU Size.
(config-if)#exit	Exit the interface mode.
(config)#interface eth13	Enter the interface mode.

(config-if)#switchport	Configure Switchport
(config-if)#bridge-group 1	Assign a Bridge ID to the port channel
(config-if)#switchport mode trunk	Configure trunk
(config-if)#switchport trunk allowed vlan add 13,523	Configure allowed VLANs
(config-if)#switchport trunk native vlan 523	Configure native VLAN.
(config-if)# load-interval 30	Set load interval
(config-if)# mtu 9192	Configure the MTU Size.
(config-if)#exit	Exit the interface mode.
(config)#interface eth14	Enter the interface mode.
(config-if)#switchport	Configure Switchport
(config-if)#bridge-group 1	Assign a Bridge ID to the port channel
(config-if)#switchport mode trunk	Configure trunk
(config-if)#switchport trunk allowed vlan add 14,524	Configure allowed VLANs
(config-if)#switchport trunk native vlan 524	Configure native VLAN.
(config-if)# load-interval 30	Set load interval
(config-if)# mtu 9192	Configure the MTU Size.
(config-if)#exit	Exit the interface mode.
(conf)#rsvp-path sp1-r3-r1 mpls	Create RSVP path
(conf-path)# 10.10.21.1 strict	Configure nexthop
(conf-path)# 10.10.23.1 strict	Configure nexthop
(conf)#rsvp-path sp2-r3-r1 mpls	Create RSVP path
(conf-path)#10.10.22.1 strict	Configure nexthop
(conf-path)#10.10.24.1 strict	Configure nexthop
(conf)#rsvp-path sp2-r3-r1 mpls	Create RSVP path
(conf-path)#10.10.29.2 strict	Configure nexthop
(conf-path)# 10.10.25.1 strict	Configure nexthop
(conf)#rsvp-path sp3-r3-r1 mpls	Create RSVP path
(conf-path)#10.10.30.1 strict	Configure nexthop
(conf-path)# 10.10.26.1 strict	Configure nexthop
(conf)#rsvp-path sp4-r3-r1 mpls	Create RSVP path
(conf-path)#10.10.31.1 strict	Configure nexthop
(conf-path)# 10.10.27.1 strict	Configure nexthop
(conf)#rsvp-path sp5-r3-r1 mpls	Create RSVP path
(conf-path)# 10.10.32.1 strict	Configure nexthop
(conf-path)#10.10.28.1 strict	Configure nexthop
(conf)#rsvp-trunk 49-47-test ipv4	Create a RSVP trunk link
(conf-trunk)#primary path p1-r3-r1	Configure primary path for trunk link
(conf-trunk)# secondary-priority 1 path sp1-r3-r1	Configure secondary link for trunk link

(conf-trunk)#secondary-priority 2 path sp2-r3-r1	Configure secondary link for trunk link
(conf-trunk)#secondary-priority 3 path sp3-r3-r1	Configure secondary link for trunk link
(conf-trunk)#secondary-priority 4 path sp4-r3-r1	Configure secondary link for trunk link
(conf-trunk)#secondary-priority 5 path sp5-r3-r1	Configure secondary link for trunk link
(conf-trunk)#to 47.47.47.47	Configure remote node for the LSP

Validation

This example shows the number of configured RSVP sessions in a router.

R3

```
 # show rsvp session
Type  : PRI - Primary, SEC - Secondary, DTR - Detour, BPS - Bypass
State : UP - Up, DN - Down, BU - Backup in Use, SU - Secondary in Use, FS - Forced to Secondary
* indicates the session is active with local repair at one or more nodes
(P) indicates the secondary-priority session is acting as primary

Ingress RSVP:
To              From            Type    LSPName                          State Uptime    Rt Style  Labelin  Labelout  DSType
47.47.47.47     49.49.49.49      PRI     49-47-test-Primary               UP    00:34:57 1 1 SE     -         24970     DEFAULT
47.47.47.47     49.49.49.49      SEC     49-47-test-Secondary-Priority-1 UP    00:34:56 1 1 SE     -         24968     DEFAULT
Total 2 displayed, Up 2, Down 0.

Egress RSVP:
To              From            Type    LSPName                          State Uptime    Rt Style  Labelin  Labelout  DSType
49.49.49.49     47.47.47.47      PRI     47-49-test-Primary               UP    00:34:45 1 1 SE     31364     -         ELSP_CON
49.49.49.49     47.47.47.47      PRI     47-49-test-Secondary-Priority-1 UP    00:34:44 1 1 SE     31360     -         ELSP_CON
Total 2 displayed, Up 2, Down 0.

# show rsvp trunk multi-sec-detail
Ingress (Secondary-Priority1)
47.47.47.47
  From: 49.49.49.49, LSPstate: Up, LSPname: 49-47-test-Secondary-Priority-1
  Ingress FSM state: Operational
  Establishment Time: 1s 71ms
  Setup priority: 7, Hold priority: 0
  CSPF usage: Enabled, CSPF Retry Count: 0, CSPF Retry Interval: 30 seconds
  LSP Re-Optimization: Disabled, Re-Optimization Timer: NA, Cspf Client: OSPF
  IGP-Shortcut: Disabled, LSP metric: 3
  LSP Protection: None
```

```
  Label in: -,  Label out:    24968,
  Tspec rate: 0, Fspec rate: 0
  Policer: Not Configured
  Tunnel Id: 5001, LSP Id: 2214, Ext-Tunnel Id: 49.49.49.49
  Downstream: 45.49.24.1, vlan1.1024
  Path refresh: 30 seconds (RR enabled) (due in 27829 seconds)
  Resv lifetime: 157 seconds (due in 145 seconds)
  Retry count: 0, intrvl: 30 seconds
  RRO re-use as ERO: Disabled
  Label Recording: Disabled
  Admin Groups: none
  Configured Path: SP1-49-47 (in use)
  Configured Explicit Route Detail :
   45.49.24.1/32 strict
   46.45.9.1/32 strict
   47.46.3.1/32 strict
  Session Explicit Route Detail :
   45.49.24.1/32 strict
   46.45.9.1/32 strict
   47.46.3.1/32 strict
  Record route:
   ----------------------------------------------------------------
   IP Address        Label
   ----------------------------------------------------------------
   <self>
   45.49.24.1
   46.45.9.1
   47.46.3.1
  Style: Shared Explicit Filter
  Traffic type: controlled-load
  Minimum Path MTU: 9216
  Last Recorded Error Code: None
  Last Recorded Error Value: None
  Node where Last Recorded Error originated: None
  Trunk Type: mpls
Ingress (Secondary-Priority2)
47.47.47.47
  From: 49.49.49.49, LSPstate: Dn, LSPname: 49-47-test-Secondary-Priority-2
  Ingress FSM state: Idle
  Setup priority: 7, Hold priority: 0
  CSPF usage: Enabled, CSPF Retry Count: 0, CSPF Retry Interval: 30 seconds
  LSP Re-Optimization: Disabled, Re-Optimization Timer: NA, Cspf Client: NA
  IGP-Shortcut: Disabled, LSP metric: 3
  LSP Protection: None
  Label in: -,  Label out: -,
  Tspec rate: 0, Fspec rate: 0
  Policer: Not Configured
  Tunnel Id: 5001, LSP Id: 2215, Ext-Tunnel Id: 49.49.49.49
  Last Recorded Error Code: None
  Last Recorded Error Value: None
```

```
  Node where Last Recorded Error originated: None
  Trunk Type: mpls
Ingress (Secondary-Priority3)
47.47.47.47
  From: 49.49.49.49, LSPstate: Dn, LSPname: 49-47-test-Secondary-Priority-3
  Ingress FSM state: Idle
  Setup priority: 7, Hold priority: 0
  CSPF usage: Enabled, CSPF Retry Count: 0, CSPF Retry Interval: 30 seconds
  LSP Re-Optimization: Disabled, Re-Optimization Timer: NA, Cspf Client: NA
  IGP-Shortcut: Disabled, LSP metric: 65
  LSP Protection: None
  Label in: -,  Label out: -,
  Tspec rate: 0, Fspec rate: 0
  Policer: Not Configured
  Tunnel Id: 5001, LSP Id: 2213, Ext-Tunnel Id: 49.49.49.49
  Last Recorded Error Code: Routing Problem (24)
  Last Recorded Error Value: No route available toward destination (5)
  Node where Last Recorded Error originated: None
  Trunk Type: mpls
Ingress (Secondary-Priority4)
47.47.47.47
  From: 49.49.49.49, LSPstate: Dn, LSPname: 49-47-test-Secondary-Priority-4
  Ingress FSM state: Idle
  Setup priority: 7, Hold priority: 0
  CSPF usage: Enabled, CSPF Retry Count: 0, CSPF Retry Interval: 30 seconds
  LSP Re-Optimization: Disabled, Re-Optimization Timer: NA, Cspf Client: NA
  IGP-Shortcut: Disabled, LSP metric: 65
  LSP Protection: None
  Label in: -,  Label out: -,
  Tspec rate: 0, Fspec rate: 0
  Policer: Not Configured
  Tunnel Id: 5001, LSP Id: 2213, Ext-Tunnel Id: 49.49.49.49
  Last Recorded Error Code: Routing Problem (24)
  Last Recorded Error Value: No route available toward destination (5)
  Node where Last Recorded Error originated: None
  Trunk Type: mpls
Ingress (Secondary-Priority5)
47.47.47.47
  From: 49.49.49.49, LSPstate: Dn, LSPname: 49-47-test-Secondary-Priority-5
  Ingress FSM state: Idle
  Setup priority: 7, Hold priority: 0
  CSPF usage: Enabled, CSPF Retry Count: 0, CSPF Retry Interval: 30 seconds
  LSP Re-Optimization: Disabled, Re-Optimization Timer: NA, Cspf Client: NA
  IGP-Shortcut: Disabled, LSP metric: 65
  LSP Protection: None
  Label in: -,  Label out: -,
  Tspec rate: 0, Fspec rate: 0
  Policer: Not Configured
  Tunnel Id: 5001, LSP Id: 2213, Ext-Tunnel Id: 49.49.49.49
  Last Recorded Error Code: Routing Problem (24)
```

```
Last Recorded Error Value: No route available toward destination (5)
Node where Last Recorded Error originated: None
Trunk Type: mpls
```

Add Administrative Group Constraints to an LSP

To add administrative group constraints (also known as color constraints) to an LSP:

- Configure support for required administrative groups in NSM on all participating routers
- Configure required administrative groups on all participating interfaces

The configuration in this example forces the primary LSP to be setup through links that belong either to administrative group A or C. A link that does not belong to either of these administrative groups will not be used for setting up the LSP.

Note: This example is based on the assumption that a minimal configuration exists on all participating routers as described in Enable Label Switching - Minimal Configuration.

R1 - NSM

`#configure terminal`	Enter configure mode.
`(config)#mpls admin-group A 0`	Add new administrative groups, specify their names and assign bit values to them.
`(config)#mpls admin-group B 1`	
`(config)#mpls admin-group C 2`	
`(config)#mpls admin-group D 3`	
`(config)#mpls admin-group E 4`	
`(config)#interface eth0`	Enter interface mode.
`(config-if)#admin-group A`	Add administrative groups to the links. When used in the interface mode, this command adds a link between an interface and a group. The name is the name of the group previously configured. You can have multiple groups per interface.
`(config-if)#admin-group B`	
`(config-if)#admin-group C`	
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#admin-group E`	Add administrative groups to the links. When used in the interface mode, this command adds a link between an interface and a group. The name is the name of the group previously configured. You can have multiple groups per interface.
`(config-if)#admin-group D`	
`(config-if)#exit`	Exit interface mode.

R2 - NSM

`#configure terminal`	Enter configure mode.
`(config)#mpls admin-group A 0`	Add new administrative groups and specify their names and assign bit values to them.
`(config)#mpls admin-group C 2`	
`(config)#interface eth2`	Enter interface mode

(config-if)#admin-group A	Add administrative groups to the links. When used in the interface mode, this command adds a link between an interface and a group. The name is the name of the group previously configured. You can have multiple groups per interface.
(config-if)#admin-group C	
(config-if)#exit	Exit interface mode.

R1 - RSVP-TE

#configure terminal	Enter configure mode.
(config)#rsvp-trunk T1	Create an RSVP trunk T1 and enter the Trunk mode.
(config-trunk)#no primary cspf	Since CSPF is enabled by default, specify no primary cspf if CSPF is not required.
(config-trunk)#primary path P1	Specify an RSVP primary path to be used.
(config-trunk)#no primary cspf	Specify the no primary cspf option for the LSP.
(config-trunk)#primary include-any A	Set up the LSP with admin group constraint A.
(config-trunk)#primary include-any C	Set up the LSP with admin group constraint C.
(config-trunk)#to 192.168.0.90	Specify the IPv4 egress (destination point) for the LSP.

Configure Global Parameters

Some common parameters can be configured in the Router mode on the RSVP-TE daemon. These parameters are global and affect all LSPs. In the following example the interval between two consecutive hello messages is set. The neighbor is defined by the neighbor command. Hello exchanges are enabled only between explicitly configured neighbors (configure this router as a neighbor on R2 (IP address 10.10.23.60).

Note: This example is based on the assumption that a minimal configuration exists on all participating routers as described in Enable Label Switching - Minimal Configuration.

R1 - RSVP-TE

#configure terminal	Enter configure mode.
(config)#router rsvp	Enter the router mode for RSVP.
(config-router)#hello-interval 10	Set the hello-interval (in seconds) between hello packets.
(config-router)#hello-timeout 35	Set the hello-timeout value. If an LSR has not received a Hello message from a peer within this period, all sessions shared with this peer are reset.
(config-router)#neighbor 10.10.23.60	Explicitly specify the neighbor to exchange Hello messages with.

R2 - RSVP-TE

#configure terminal	Enter configure mode.
(config)#router rsvp	Enter the router mode for RSVP.
(config-router)#hello-interval 10	Set the hello-interval (in seconds) between hello packets.

`(config-router)#hello-timeout 35`	Set the `hello-timeout value`. If an LSR has not received a Hello message from a peer within this period, all sessions shared with this peer are reset.
`(config-router)#neighbor 10.10.23.63`	Explicitly specify the neighbor to exchange Hello messages with.

Fast Reroute Configuration (one-to-one method)

The Fast Reroute (FRR) configuration is a MPLS resiliency technology that provides fast traffic recovery when there is a link or router failure on mission critical services. These mechanisms enable the re-direction of traffic onto backup LSP tunnels in tens of milliseconds, in the event of a failure. The one-to-one backup method creates detour LSPs for each protected LSP at each potential point of local repair. This method is used to protect links and nodes during network failure.

In the below configurations each FRR trunk is mapped to VPWS,VPLS and L3 VPN services.So it includes configurations of VPWS,VPLS and L3 VPN also.

Figure 8-15 is a simple topology example for FRR:

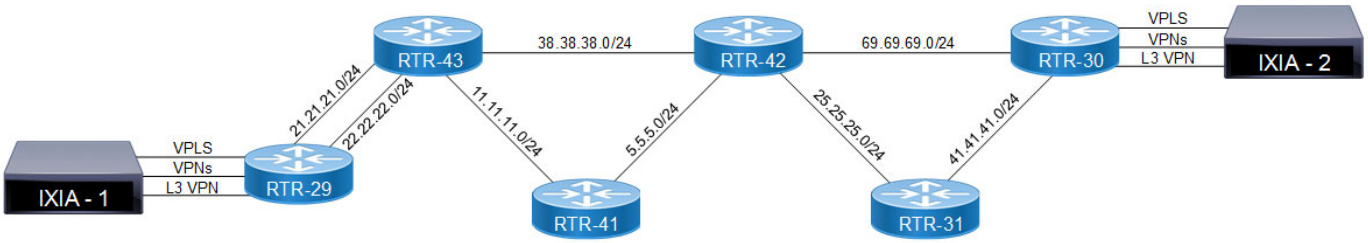


Figure 8-15: Topology Example for Fast Reroute

RTR-29

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode.
`(config-if)#ip address 29.29.29.29/32 secondary`	Set a secondary IP address of the interface
`(config-if)#no shutdown`	Administratively bring the interface up.
`(config-if)#exit`	Exit interface mode.
`(config)#router-id 29.29.29.29`	Configure the router ID.
`(config)#router rsvp`	Enter to router rsvp mode.
`(config-router)#no php`	Disable PHP
`(config-router)#exit`	Exit the router mode
`(config)#router ldp`	Enter to router LDP mode.
`(config-router)# targeted-peer ipv4 30.30.30.30`	Configure targeted peer.
`(config-router-targeted-peer)# exit-targeted-peer-mode`	Exit-targeted-peer-mode
`(config-router)#exit`	Exit router mode
`(config)#interface xe21`	Enter interface mode.

(config-if)#label-switching	Enable label switching on interface.
(config-if)#ip address 21.21.21.29/24	Set an IP address of the interface.
(config-if)#no shutdown	Administratively no shutdown the interface.
(config-if)#enable-rsvp	Enable RSVP message exchange on this interface.
(config-if)#enable-ldp ipv4	Enable LDP on this interface
(config-if)#exit	Exit interface mode.
(config)#interface xe22	Enter interface mode.
(config-if)#label-switching	Enable label switching on interface
(config-if)#enable-ldp ipv4	Enable LDP on this interface
(config-if)#ip address 22.22.22.29/24	Set an IP address of the interface.
(config-if)#no shutdown	Administratively no shutdown the interface.
(config-if)#enable-rsvp	Enable RSVP message exchange on this interface.
(config-if)#exit	Exit interface mode.
(config)#router ospf	Enter the router configure mode for OSPF.
(config-router)#router-id 29.29.29.29	Configure OSPF router-ID same as loopback interface IP address
(config-router)#network 21.21.21.0/24 area 0 (config-router)#network 22.22.22.0/24 area 0 (config-router)#network 29.29.29.29/32 area 0	Define the network on which OSPF runs and associate the area ID
(config-router)#exit	Exit the router configure mode.
(config)#rsvp-path p21	Enter the path mode for RSVP pt1.
(config-path)# 21.21.21.43 strict	Configure this explicit route path as a strict hop.
(config-path)# 38.38.38.42 strict	Configure this explicit route path as a strict hop.
(config-path)#69.69.69.30 strict	Configure this explicit route path as a strict hop.
(config)#exit	Exit the path mode.
(config)#rsvp-trunk to_30 ipv4	Enter the trunk mode for RSVP.
(config-trunk)#primary fast-reroute protection one-to-one	Configure primary fast-reroute protection facility for a trunk.
(config-trunk)# primary fast-reroute node-protection	Configure primary fast-reroute node protection for the trunk
(config-trunk)#primary path p21	Configure trunk to 30 to use the defined path.
(config-trunk)#to 30.30.30.30	Specify the IPv4 egress (destination point) for the LSP.
(config-trunk)#exit	Exit from trunk mode.
(config)#ip vrf vrf1	Configure VRF instance
(config-vrf)# rd 100:1	Configure Router Distinguisher value
(config-vrf)# route-target both 100:1	Configure route-target as both
(config-vrf)#exit	Exit the path mode.
(config)#interface xe43	Enter to the interface mode
(config-if)#ip vrf forwarding vrf1	Bind the VRF instance to the interface
(config-if)#ip address 43.43.43.29/24	Configure IP address
(config-if)#exit	Exit interface mode.
(config)# router bgp 100	Configure BGP router instance

(config-router)#neighbor 30.30.30.30 remote-as 100	Configure neighbor with remote-as
(config-router)#neighbor 30.30.30.30 update-source 29.29.29.29	Configure update source as loopback address
(config-router)#address-family vpnv4 unicast	Configure VPNv4 address family
(config-router-af)#neighbor 30.30.30.30 activate	Activate the VPN neighbor
(config-router-af)#exit-address-family	Exit the VPN address family
(config-router)#address-family ipv4 vrf vrf1	Configure VRF address family
(config-router-af)redistribute connected	Redistribute connected route
(config-router-af)exit-address-family	Exit VRF address family
(config-router)#exit	Exit router mode
(config)#mpls l2-circuit vlan10 10 30.30.30.30	Configure Virtual circuit.
(config-pseudowire)#exit	Exit pseudowire config mode.
(config)#service-template st1	Template configuration
(config-svc)#match outer-vlan 10	Match criteria under template configuration
(config-svc)#exit	Exit service template mode
(config)#service-template st2	Template configuration
(config-svc)#match outer-vlan 30	Match criteria under template configuration
(config-svc)#exit	Exit service template mode
(config)#interface xe44	Enter interface configuration mode
(config-if)#switchport	Configure interface as switch port
(config-if)#mpls-l2-circuit t1 service-template st1	Bind the interface to the VC with service template
(config-if)#exit	Exit interface configuration mode
(config)#mpls vpls vpls30 30	Configure VPLS instance
(config-vpls)#signaling ldp	Configure VPLS signaling as LDP
(config-vpls-sig)#vpls-type vlan	Configure VPLS type as VLAN encapsulation
(config-vpls-sig)#vpls-peer 30.30.30.30	Configure VPLS peer
(config-vpls-sig)#exit-signaling	Exit VPLS configuration mode
(config)#interface xe45	Enter interface configuration mode
(config-if)#switchport	Configure interface as switch port
(config-if)#mpls-vpls vpls30 service-template st2	Bind the VPLS instance to the interface
(config-if-vpls)#exit	Exit VPLS attachment-circuit mode
(config-if)#exit	Exit the interface and configure mode

RTR-43

(config)#interface lo	Enter interface mode.
(config-if)#ip address 43.43.43.43/32 secondary	Set a secondary IP address of the interface
(config-if)#no shutdown	Administratively shutdown the interface.

(config-if)#exit	Exit interface mode.
(config)#router-id 43.43.43.43	Configure the router ID.
(config)#router rsvp	Enter to router RSVP mode.
(config-router)#no php	Disable PHP
(config-router)#exit	Exit the router mode
(config)#interface xe5/1	Enter interface mode.
(config-if)#label-switching	Enable label switching on interface.
(config-if)#ip address 11.11.11.43/24	Set an IP address of the interface.
(config-if)#no shutdown	Administratively no shutdown the interface.
(config-if)#enable-rsvp	Enable RSVP message exchange on this interface.
(config-if)#exit	Exit interface mode.
(config)#interface xe9/1	Enter interface mode.
(config-if)#label-switching	Enable label switching on interface
(config-if)#ip address 21.21.21.43/24	Set an IP address of the interface.
(config-if)#no shutdown	Administratively no shutdown the interface.
(config-if)#enable-rsvp	Enable RSVP message exchange on this interface.
(config-if)#exit	Exit interface mode.
(config)#interface xe9/2	Enter interface mode.
(config-if)#label-switching	Enable label switching on interface.
(config-if)#ip address 22.22.22.43/24	Set an IP address of the interface.
(config-if)#no shutdown	Administratively no shutdown the interface.
(config-if)#enable-rsvp	Enable RSVP message exchange on this interface.
(config-if)#exit	Exit interface mode.
(config)#interface xe13/2	Enter interface mode.
(config-if)#label-switching	Enable label switching on interface
(config-if)#ip address 38.38.38.43/24	Set an IP address of the interface.
(config-if)#no shutdown	Administratively no shutdown the interface.
(config-if)#enable-rsvp	Enable RSVP message exchange on this interface.
(config-if)#exit	Exit interface mode.
(config)#router ospf	Enter the router configure mode for OSPF.
(config-router)#router-id 43.43.43.43	Configure OSPF router-ID same as loopback interface IP address
(config-router)#network 11.11.11.0/24 area 0 (config-router)#network 22.22.22.0/24 area 0 (config-router)#network 21.21.21.0/24 area 0 (config-router)#network 38.38.38.0/24 area 0 (config-router)#network 43.43.43.43/32 area 0	Define the network on which OSPF runs and associate the area ID
(config-router)#end	Exit the router and configure mode.

RTR-42

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode.
`(config-if)#ip address 42.42.42.42/32 secondary`	Set a secondary IP address of the interface
`(config-if)#no shutdown`	Administratively shutdown the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router-id 42.42.42.42`	Configure the router ID.
`(config)#router rsvp`	Enter to router RSVP mode.
`(config-router)#no php`	Disable PHP
`(config-router)#exit`	Exit the router mode
`(config)#interface xe2`	Enter interface mode.
`(config-if)#label-switching`	Enable label switching on interface.
`(config-if)#ip address 5.5.5.42/24`	Set an IP address of the interface.
`(config-if)#no shutdown`	Administratively no shutdown the interface.
`(config-if)#enable-rsvp`	Enable RSVP message exchange on this interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe10/1`	Enter interface mode.
`(config-if)#label-switching`	Enable label switching on interface
`(config-if)#ip address 25.25.25.42/24`	Set an IP address of the interface.
`(config-if)#no shutdown`	Administratively no shutdown the interface.
`(config-if)#enable-rsvp`	Enable RSVP message exchange on this interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe3`	Enter interface mode.
`(config-if)#label-switching`	Enable label switching on interface.
`(config-if)#ip address 38.38.38.42/24`	Set an IP address of the interface.
`(config-if)#no shutdown`	Administratively no shutdown the interface.
`(config-if)#enable-rsvp`	Enable RSVP message exchange on this interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe4`	Enter interface mode
`(config-if)#label-switching`	Enable label switching on interface
`(config-if)#ip address 69.69.69.42/24`	Specify an IP address for the interface
`(config-if)#no shutdown`	Administratively no shutdown the interface
`(config-if)#enable-rsvp`	Enable RSVP message exchange on this interface
`(config-if)#exit`	Exit interface mode
`(config)#router ospf`	Enter the router configure mode for OSPF.
`(config-router)#router-id 42.42.42.42`	Configure OSPF router-ID same as loopback interface IP address

(config-router)#network 5.5.5.0/24 area 0 (config-router)#network 25.25.25.0/24 area 0 (config-router)#network 69.69.69.0/24 area 0 (config-router)#network 38.38.38.0/24 area 0 (config-router)#network 42.42.42.42/32 area 0	Define the network on which OSPF runs and associate the area ID
(config-router)#end	Exit the router and configure mode.

RTR-41

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 44.44.44.44/32 secondary	Set a secondary IP address of the interface
(config-if)#no shutdown	Administratively no shutdown the interface.
(config-if)#exit	Exit interface mode.
(config)#router-id 44.44.44.44	Configure the router ID.
(config)#router rsvp	Enter to router RSVP mode.
(config-router)#no php	Disable PHP
(config-router)#exit	Exit the router mode
(config)#interface xe1/1	Enter interface mode.
(config-if)#label-switching	Enable label switching on interface.
(config-if)#ip address 1.1.1.41/24	Set an IP address of the interface.
(config-if)#no shutdown	Administratively no shutdown the interface.
(config-if)#enable-rsvp	Enable RSVP message exchange on this interface.
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#label-switching	Enable label switching on interface
(config-if)#ip address 5.5.5.41/24	Set an IP address of the interface.
(config-if)#no shutdown	Administratively no shutdown the interface.
(config-if)#enable-rsvp	Enable RSVP message exchange on this interface.
(config-if)#exit	Exit interface mode.
(config)#interface xe5/1	Enter interface mode.
(config-if)#label-switching	Enable label switching on interface.
(config-if)#ip address 11.11.11.41/24	Set an IP address of the interface.
(config-if)#no shutdown	Administratively no shutdown the interface.
(config-if)#enable-rsvp	Enable RSVP message exchange on this interface.
(config-if)#exit	Exit interface mode.
(config)#router ospf	Enter the router configure mode for OSPF.
(config-router)#router-id 44.44.44.44	Configure OSPF router-ID same as loopback interface IP address

(config-router)#network 5.5.5.0/24 area 0 (config-router)#network 1.1.1.0/24 area 0 (config-router)#network 11.11.11.0/24 area 0 (config-router)#network 44.44.44.44/32 area 0	Define the network on which OSPF runs and associate the area ID
(config-router)#end	Exit the router and configure mode.

RTR-31

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 31.31.31.31/32 secondary	Set a secondary IP address of the interface
(config-if)#no shutdown	Administratively shutdown the interface.
(config-if)#exit	Exit interface mode.
(config)#router-id 31.31.31.31	Configure the router ID.
(config)#router rsvp	Enter to router RSVP mode.
(config-router)#no php	Disable PHP
(config-router)#exit	Exit the router mode
(config)#interface xe1	Enter interface mode.
(config-if)#label-switching	Enable label switching on interface.
(config-if)#ip address 1.1.1.31/24	Set an IP address of the interface.
(config-if)#no shutdown	Administratively no shutdown the interface.
(config-if)#enable-rsvp	Enable RSVP message exchange on this interface.
(config-if)#exit	Exit interface mode.
(config)#interface xe25	Enter interface mode.
(config-if)#label-switching	Enable label switching on interface
(config-if)#ip address 25.25.25.31/24	Set an IP address of the interface.
(config-if)#no shutdown	Administratively no shutdown the interface.
(config-if)#enable-rsvp	Enable RSVP message exchange on this interface.
(config-if)#exit	Exit interface mode.
(config)#interface xe41	Enter interface mode.
(config-if)#label-switching	Enable label switching on interface.
(config-if)#ip address 41.41.41.31/24	Set an IP address of the interface.
(config-if)#no shutdown	Administratively no shutdown the interface.
(config-if)#enable-rsvp	Enable RSVP message exchange on this interface.
(config-if)#exit	Exit interface mode.
(config)#router ospf	Enter the router configure mode for OSPF.
(config-router)#router-id 31.31.31.31	Configure OSPF router-ID same as loopback interface IP address

(config-router)#network 1.1.1.0/24 area 0 (config-router)#network 25.25.25.0/24 area 0 (config-router)#network 41.41.41.0/24 area 0 (config-router)#network 31.31.31.31/32 area 0	Define the network on which OSPF runs and associate the area ID
(config-router)#end	Exit the router and configure mode.

RTR-30

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 30.30.30.30/32 secondary	Set a secondary IP address of the interface
(config-if)#no shutdown	Administratively shutdown the interface.
(config-if)#exit	Exit interface mode.
(config)#router-id 30.30.30.30	Configure the router ID.
(config)#router rsvp	Enter to router RSVP mode.
(config-router)#no php	Disable PHP
(config-router)#exit	Exit the router mode
(config)#router ldp	Enter to router LDP mode.
(config-router)# targeted-peer ipv4 29.29.29.29	Configure targeted peer.
(config-router-targeted-peer)# exit-targeted-peer-mode	Exit-targeted-peer-mode
(config-router)#exit	Exit router mode
(config)#interface xe41	Enter interface mode.
(config-if)#label-switching	Enable label switching on interface.
(config-if)#ip address 41.41.41.30/24	Set an IP address of the interface.
(config-if)#no shutdown	Administratively no shutdown the interface.
(config-if)#enable-rsvp	Enable RSVP message exchange on this interface.
(config-if)#enable-ldp ipv4	Enable LDP on this interface
(config-if)#exit	Exit interface mode.
(config)#interface xe54/1	Enter interface mode.
(config-if)#label-switching	Enable label switching on interface
(config-if)#enable-ldp ipv4	Enable LDP on this interface
(config-if)#ip address 69.69.69.30/24	Set an IP address of the interface.
(config-if)#no shutdown	Administratively no shutdown the interface.
(config-if)#enable-rsvp	Enable RSVP message exchange on this interface.
(config-if)#exit	Exit interface mode.
(config)#router ospf	Enter the router configure mode for OSPF.
(config-router)#router-id 30.30.30.30	Configure OSPF router-ID same as loopback interface IP address

(config-router)#network 41.41.41.0/24 area 0 (config-router)#network 69.69.69.0/24 area 0 (config-router)#network 30.30.30.30/32 area 0	Define the network on which OSPF runs and associate the area ID
(config-router)#exit	Exit the router configure mode.
(config)#rsvp-path p41	Enter the path mode for RSVP pt1.
(config-path)# 41.41.41.31 strict	Configure this explicit route path as a strict hop.
(config-path)# 1.1.1.41 strict	Configure this explicit route path as a strict hop.
(config-path)#11.11.11.43 strict	Configure this explicit route path as a strict hop.
(config)#exit	Exit the path mode.
(config)#rsvp-trunk to_29 ipv4	Enter the trunk mode for rsvp.
(config-trunk)#primary fast-reroute protection one-to-one	Configure primary fast-reroute protection facility for a trunk.
(config-trunk)# primary fast-reroute node-protection	Configure primary fast-reroute node protection for the trunk
(config-trunk)#primary path p41	Configure trunk to_29 to use the defined path.
(config-trunk)#to 29.29.29.29	Specify the IPv4 egress (destination point) for the LSP.
(config-trunk)#exit	Exit from trunk mode.
(config)#ip vrf vrf1	Configure VRF instance
(config-vrf)# rd 100:1	Configure Router Distinguisher value
(config-vrf)# route-target both 100:1	Configure route-target as both
(config-vrf)#exit	Exit the path mode.
(config)#interface xe23	Enter to the interface mode
(config-if)#ip vrf forwarding vrf1	Bind the VRF instance to the interface
(config-if)#ip address 23.23.23.29/24	Configure IP address
(config-if)#exit	Exit interface mode.
(config)# router bgp 100	Configure BGP router instance
(config-router)#neighbor 29.29.29.29 remote-as 100	Configure neighbor with remote-as
(config-router)#neighbor 29.29.29.29 update-source 30.30.30.30	Configure update source as loopback address
(config-router)#address-family vpnv4 unicast	Configure VPNv4 address family
(config-router-af)#neighbor 29.29.29.29 activate	Activate the VPN neighbor
(config-router-af)#exit-address-family	Exit the VPN address family
(config-router)#address-family ipv4 vrf vrf1	Configure VRF address family
(config-router-af)redistribute connected	Redistribute connected route
(config-router-af)exit-address-family	Exit VRF address family
(config-router)#exit	Exit router mode
(config)#mpls l2-circuit vlan10 10 29.29.29.29	Configure Virtual circuit.
(config-pseudowire)#exit	Exit pseudowire config mode.
(config)#service-template st1	Template configuration
(config-svc)#match outer-vlan 10	Match criteria under template configuration

(config-svc)#exit	Exit service template mode
(config)#service-template st2	Template configuration
(config-svc)#match outer-vlan 30	Match criteria under template configuration
(config-svc)#exit	Exit service template mode
(config)#interface xe24	Enter interface configuration mode
(config-if)#switchport	Configure interface as switch port
(config-if)#mpls-l2-circuit vlan10 service-template st1	Bind the interface to the VC with service template
(config-if)#exit	Exit interface configuration mode
(config)#mpls vpls vpls30 30	Configure VPLS instance
(config-vpls)#signaling ldp	Configure VPLS signaling as LDP
(config-vpls-sig)#vpls-type vlan	Configure VPLS type as VLAN encapsulation
(config-vpls-sig)#vpls-peer 29.29.29.29	Configure VPLS peer
(config-vpls-sig)#exit-signaling	Exit VPLS configuration mode
(config)#interface xe25	Enter interface configuration mode
(config-if)#switchport	Configure interface as switch port
(config-if)#mpls-vpls vpls30 service-template st2	Bind the VPLS instance to the interface
(config-if-vpls)#exit	Exit VPLS attachment-circuit mode
(config-if)#exit	Exit the interface and configure mode

Validation

```
RTR-30#show rsvp session
Ingress RSVP:
To              From            State               Pri Rt  Style Labelin
Labelout LSPName                          Uptime  Est.time   D
SType
29.29.29.29     30.30.30.30     Up                  Yes 1 1 SE    -
24322    to_29-Primary                    00:07:53 0s 118ms  D
EFAULT
29.29.29.29     69.69.69.30     Up                  No  1 1 SE    -
24322    to_29-Detour                     00:07:53 0s 4ms  DEF
AULT
Total 2 displayed, Up 2, Down 0.

Egress RSVP:
To              From            State               Pri Rt  Style Labelin
Labelout LSPName                          Uptime  Est.time   D
SType
30.30.30.30     29.29.29.29     Up                  Yes 1 1 SE    24960   -
to_30-Primary                     00:07:57 N/A    ELSP
_CON
30.30.30.30     25.25.25.42     Up                  Yes 1 1 SE    24961   -
to_30-Detour                      00:07:57 N/A    ELSP
_CON
Total 2 displayed, Up 2, Down 0.


RTR-30#show mpls forwarding-table
```

```
Codes: > - installed FTN, * - selected FTN, p - stale FTN,
       B - BGP FTN, K - CLI FTN, t - tunnel
       L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, I - IGP-Shortcut,
       U - unknown FTN, O - SR-OSPF FTN, i - SR-ISIS FTN, k - SR-CLI FTN

Code    FEC                FTN-ID    Tunnel-id   Pri   LSP-Type        Out-
Label    Out-Intf       Nexthop
R(t)>   29.29.29.29/32     1       5001       Yes   LSP_DEFAULT    24322
eth2          41.41.41.31
R(t)>   29.29.29.29/32     2       5001       No    LSP_DEFAULT    24322
eth1          69.69.69.42
RTR-30#

RTR-30#show mpls vrf-table
Output for IPv4 VRF table with id: 2
 Primary FTN entry with FEC: 43.43.43.0/24, id: 1, row status: Active
  Owner: BGP, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 5001,   Protected LSP id: 0, QoS Resource id: 0, Description: N/A
    Matched bytes:0, pkts:0, TX bytes:0, Pushed pkts:0
     Cross connect ix: 7, in intf: - in label: 0 out-segment ix: 6
      Owner: BGP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 6, owner: BGP, out intf: eth1, out label: 25602
    Nexthop addr: 29.29.29.29        cross connect ix: 7, op code: Push and
Lookup


Link 41.41.41.0/24 Goes down. Interface xe41 on router 30 is admistratively
disabled with the "shutdown command".

RTR-30#

RTR-30#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RTR-30(config)#in xe41
RTR-30(config-if)#shutdown
RTR-30(config-if)#


RTR-30#show rsvp session
Ingress RSVP:
To              From            State               Pri Rt  Style Labelin
Labelout LSPName                          Uptime  Est.time   D
SType
29.29.29.29     30.30.30.30     Using Backup        Yes 0 0 SE    -       -
to_29-Primary                  N/A    DEFAULT
29.29.29.29     30.30.30.30      Dn                 Yes 0 0 SE    -       -
to_29-Primary                  N/A    DEFAULT
29.29.29.29      69.69.69.30      Up                   No  1 1 SE    -
24322    to_29-Detour                    00:10:53 0s 4ms  DEF
AULT
Total 3 displayed, Up 1, Down 2.

Egress RSVP:
To              From            State               Pri Rt  Style Labelin
Labelout LSPName                          Uptime  Est.time   D
SType
30.30.30.30     29.29.29.29     Up                  Yes 1 1 SE    24960   -
to_30-Primary                    00:10:57 N/A    ELSP
```

```
_CON
Total 1 displayed, Up 1, Down 0.


RTR-30#show mpls vc-table
VC-ID       Vlan-ID  Inner-Vlan-ID  Access-Intf   Network-Intf  Out Label
Tunnel-Label  Nexthop         Status
10          N/A      N/A            eth4          eth1          24321
24322         29.29.29.29     Active
RTR-30#


RTR-30#show mpls vpls mesh
VPLS-ID    Peer Addr         Tunnel-Label  In-Label   Network-Intf   Out-Label
Lkps/St   PW-INDEX  SIG-Protocol  Status
30          29.29.29.29       24322         24320      xe41           24320
2/Up      2         LDP           Active



Link 41.41.41.0/24 is reestablished. Interfce xe41 is administrativly re-
enabled.


RTR-30#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RTR-30(config)#in xe41
RTR-30(config-if)#no shutdown
RTR-30(config-if)#
RTR-30#


RTR-30#show rsvp session
Ingress RSVP:
To              From            State                Pri Rt  Style Labelin
Labelout LSPName                          Uptime  Est.time   D
SType
29.29.29.29     30.30.30.30     Up                   Yes 1 1 SE    -
24322    to_29-Primary                    00:00:01 0s 8ms  DEF
AULT
29.29.29.29     69.69.69.30     Up                   No  1 1 SE    -
24322    to_29-Detour                     00:00:01 0s 8ms  DEF
AULT
Total 2 displayed, Up 2, Down 0.

Egress RSVP:
To              From            State                Pri Rt  Style Labelin
Labelout LSPName                          Uptime  Est.time   D
SType
30.30.30.30     29.29.29.29     Up                   Yes 1 1 SE    24960   -
to_30-Primary                     00:13:22 N/A    ELSP
_CON
30.30.30.30     25.25.25.42     Up                   Yes 1 1 SE    24961   -
to_30-Detour                      00:00:08 N/A    ELSP
_CON
Total 2 displayed, Up 2, Down 0.


RTR-30#show mpls forwarding-table
```

```
Codes: > - installed FTN, * - selected FTN, p - stale FTN,
       B - BGP FTN, K - CLI FTN, t - tunnel
       L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, I - IGP-Shortcut,
       U - unknown FTN, O - SR-OSPF FTN, i - SR-ISIS FTN, k - SR-CLI FTN

Code    FEC                FTN-ID    Tunnel-id   Pri   LSP-Type        Out-
Label    Out-Intf       Nexthop
R(t)>   29.29.29.29/32     1       5001       Yes   LSP_DEFAULT    24322
xe41          41.41.41.31
R(t)>   29.29.29.29/32     2       5001       No    LSP_DEFAULT    24322
xe54/1          69.69.69.42
```

Note: The primary LSP, which is in using backup state shall continue to use backup path in case where secondary is provisioned after the LSP state is changed to switch to backup.

MPLS RSVP PING and TRACEROUTE

This example shows MPLS ping and trace route for RSVP

```
#ping mpls rsvp tunnel-name to_30 detail
Sending 5 MPLS Echos to  to_30 , timeout is 5 seconds
Codes:
'!' - Success, 'Q' - request not sent, '.' - timeout,
'x' - Retcode 0, 'M' - Malformed Request, 'm' - Errored TLV,
'N' - LBL Mapping Err, 'D' - DS Mismatch,
'U' - Unknown Interface, 'R' - Transit (LBL Switched),
'B' - IP Forwarded, 'F' No FEC Found, 'f' - FEC Mismatch,
'P' - Protocol Error, 'X' - Unknown code,
'Z' - Reverse FEC Validation Failed
Type 'Ctrl+C' to abort
! seq_num = 1 30.30.30.30 0.28 ms
! seq_num = 2 30.30.30.30 0.24 ms
! seq_num = 3 30.30.30.30 0.22 ms
! seq_num = 4 30.30.30.30 0.22 ms
! seq_num = 5 30.30.30.30 0.22 ms

Success Rate is 100.00 percent (5/5)
round-trip min/avg/max = 0.22/0.25/0.28


RTR-29#trace mpls rsvp tunnel-name to_30 detail
Tracing MPLS Label Switched Path to  to_30 , timeout is 5 seconds

Codes:
'!' - Success, 'Q' - request not sent, '.' - timeout,
'x' - Retcode 0, 'M' - Malformed Request, 'm' - Errored TLV,
'N' - LBL Mapping Err, 'D' - DS Mismatch,
'U' - Unknown Interface, 'R' - Transit (LBL Switched),
'B' - IP Forwarded, 'F' No FEC Found, 'f' - FEC Mismatch,
'P' - Protocol Error, 'X' - Unknown code,
'Z' - Reverse FEC Validation Failed

 Type 'Ctrl+C' to abort

  0 21.21.21.29 [Labels:  24320]
```

```
R 1 43.43.43.43 [Labels:  24320] 123.22 ms
R 2 42.42.42.42 [Labels:  24960] 1.60 ms
! 3 30.30.30.30 1.62 ms
```

MPLS RSVP LSP Re-optimization

Follow these steps to configure RSVP LSP Re-optimization.

`#configure terminal`	Enter configure mode.
`(config)#rsvp-trunk T1`	Create an RSVP trunk T1 and enter the Trunk mode.
`(config-trunk)#reoptimize`	Enable re-optimization of the session.

`#configure terminal`	Enter configure mode.
`(config)#router rsvp`	Enter RSVP mode
`(config-router)#lsp-reoptimization-timer 5`	Sets the re-optimization timer for the session.

Follow these steps to force the LSP to be re-optimized.

`(config)#rsvp-trunk t1 force-reoptimize`	Re-optimize the LSP forcefully

CHAPTER 9 RSVP-TE Facility Backup (Facility Bypass)

RSVP supports multiple path protection mechanisms and facility backup is one of them. With facility backup protection, N number of LSPs sharing the common path can be protected using one bypass tunnel which leads to resource utilization.

Note: Do not configure a facility backup trunk with the same transit node as that of the primary trunk.

Topology

As shown in Figure 9-16, we have four routers R1, R2, R3, and R4.

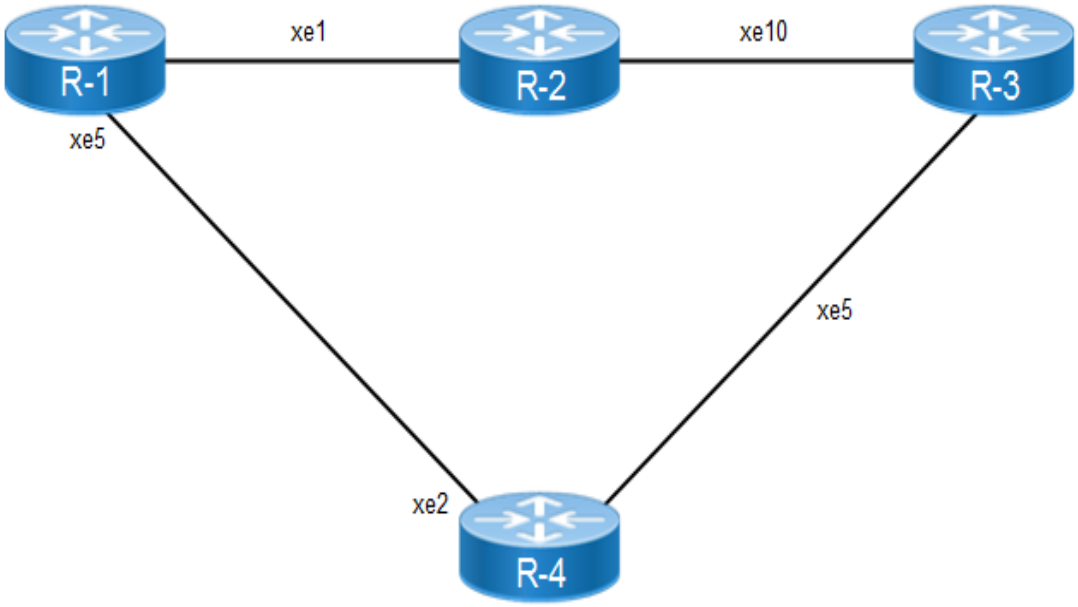


Figure 9-16: RSVP facility backup

Configuration

PE1

`#configure terminal`	Enter configuration mode
`(config)#interface lo`	Specify interface loopback for configuration
`(config-if)#ip address 1.1.1.1/32 secondary`	Configure ip address of loopback
`(config-if)#exit`	Exit interface configuration mode
`(config)#interface xe1`	Specify interface xe1 for configuration
`(config-if)#ip address 10.1.2.12/24`	Configure ip address of interface
`(config)#exit`	Exit interface configuration mode

(config-if)#int xe5	Specify interface xe1 for configuration
(config-if)#ip address 10.1.4.14/24	Configure ip address of loopback
(config-if)#exit	Exit configuration mode
(config)#router ospf 1	Configure the router OSPF with process id
(config-router)#router-id 1.1.1.1	Configure OSPF router-id
(config-router)#network 1.1.1.1/32 area 1	Define the network of the interface with area 0
(config-router)#network 10.1.2.0/24 area 1	Define the network of the interface with area 0
(config-router)#network 10.1.4.0/24 area 1	Define the network of the interface with area 0
(config-router)#exit	Exit the configure mode
(config)#bfd interval 3 minrx 3 multiplier 3	Configure BFD interval
(config)#exit	Exit the configure mode
(config)#router ospf 1	Enter router OSPF mode with process id
(config-router)#bfd all-interfaces	Enable the OSPF enabled interfaces with bfd
(config-router)#exit	Exit the router mode
(config)#router rsvp	Enter router RSVP
(config-router)#exit	Exit the router configuration mode
(config)#interface xe1	Enter the interface mode
(config-if)#enable-rsvp	Enable RSVP
(config-if)#label-switching	Enable label-switching
(config-if)#exit	Exit the interface configuration mode
(config)#interface xe5	Enter the interface mode
(config-if)#enable-rsvp	Enable RSVP
(config-if)#label-switching	Enable label-switching
(config-if)#commit	Commit the transaction.

P1

(config)#interface lo	Specify the interface (lo)
(config-if)#ip address 2.2.2.2/32 secondary	Enter the loopback ip address as secondary
(config-if)#exit	Exit the interface configure mode
(config-if)#int xe1	Specify the interface(xe1)
(config-if)#ip address 10.1.2.21/24	Configure the IP address for the interface
(config-if)#exit	Exit the interface mode
(config-if)#int xe10	Specify the interface(xe1)
(config-if)#ip address 10.2.3.23/24	Configure the IP address for the interface
(config-if)#exit	Exit the configuration mode
(config)#router ospf 1	Configure OSPF router-id
(config-router)#router-id 2.2.2.2	Configure the router id
(config-router)#network 2.2.2.2/32 area 1	Define the network of the interface with area 0
(config-router)#network 10.1.2.0/24 area 1	Define the network of the interface with area 0
(config-router)#network 10.2.3.0/24 area 1	Define the network of the interface with area 0

(config-router)#exit	Exit the configure mode
(config)#bfd interval 3 minrx 3 multiplier 3	Configure BFD interval
(config)#exit	Exit the configure mode
(config)#router ospf 1	Enter router OSPF mode with process id
(config-router)#bfd all-interfaces	Enable the OSPF enabled interfaces with bfd
(config-router)#exit	Exit the router mode
(config)#router rsvp	Enter router RSVP
(config-router)#exit	Exit the router configuration mode
(config)#interface xe1	Enter the interface mode
(config-if)#enable-rsvp	Enable RSVP
(config-if)#label-switching	Enable label-switching
(config-if)#exit	Exit the interface configuration mode
(config)#interface xe10	Enter the interface mode
(config-if)#enable-rsvp	Enable RSVP
(config-if)#label-switching	Enable label-switching
(config-if)#commit	Commit the transaction.

P2

(config)#interface lo	Specify the interface (lo)
(config-if)#ip address 3.3.3.3/32 secondary	Enter the loopback ip address as secondary
(config-if)#exit	Exit the interface configuration mode
(config-if)#int xe10	Specify the interface(xe1)
(config-if)#ip address 10.2.3.32/24	Configure the IP address for the interface
(config-if)#exit	Exit the interface mode
(config-if)#interface xe5	Specify the interface(xe1)
(config-if)#ip address 10.3.4.34/24	Configure the IP address for the interface
(config-if)#exit	Exit the configuration mode
(config)#router ospf 1	Configure OSPF router-id
(config-router)#router-id 3.3.3.3	Configure the router id
(config-router)#network 3.3.3.3/32 area 1	Define the network of the interface with area 0
(config-router)#network 10.3.4.0/24 area 1	Define the network of the interface with area 0
(config-router)#network 10.2.3.0/24 area 1	Define the network of the interface with area 0
(config-router)#exit	Exit the configure mode
(config)#bfd interval 3 minrx 3 multiplier 3	Configure BFD interval
(config)#exit	Exit the configure mode
(config)#router ospf 1	Enter router OSPF mode with process id
(config-router)#bfd all-interfaces	Enable the OSPF enabled interfaces with bfd
(config-router)#exit	Exit the router mode
(config)#router rsvp	Enter router RSVP
(config-router)#exit	Exit the router configuration mode

(config)#interface xe10	Enter the interface mode
(config-if)#enable-rsvp	Enable RSVP
(config-if)#label-switching	Enable label-switching
(config-if)#exit	Exit the interface configuration mode
(config)#interface xe5	Enter the interface mode
(config-if)#enable-rsvp	Enable RSVP
(config-if)#label-switching	Enable label-switching
(config-if)#commit	Commit the transaction.

PE2

(config)#interface lo	Specify the interface (lo)
(config-if)#ip address 4.4.4.4/32 secondary	Enter the loopback IP address as secondary
(config-if)#exit	Exit the interface configuration mode
(config-if)#interface xe2	Specify the interface(xe1)
(config-if)#ip address 10.1.4.41/24	Configure the ip address for the interface
(config-if)#exit	Exit the interface mode
(config-if)#int xe5	Specify the interface(xe1)
(config-if)#ip address 10.3.4.43/24	Configure the ip address for the interface
(config-if)#exit	Exit the configuration mode
(config)#router ospf 1	Configure ospf router-id
(config-router)#router-id 4.4.4.4	Configure the router id
(config-router)#network 4.4.4.4/32 area 1	Define the network of the interface with area 0
(config-router)#network 10.1.4.0/24 area 1	Define the network of the interface with area 0
(config-router)#network 10.3.4.0/24 area 1	Define the network of the interface with area 0
(config-router)#exit	Exit the configure mode
(config)#bfd interval 3 minrx 3 multiplier 3	Configure BFD interval
(config)#exit	Exit the configuration mode
(config)#router ospf 1	Exit the router OSPF mode with process id
(config-router)#bfd all-interfaces	Enable the OSPF enabled interfaces with bfd
(config-router)#exit	Exit the router mode
(config)#router rsvp	Enter router RSVP
(config-router)#exit	Exit the router configuration mode
(config)#interface xe1	Enter the interface mode
(config-if)#enable-rsvp	Enable RSVP
(config-if)#label-switching	Enable label-switching
(config-if)#exit	Exit the interface configuration mode
(config)#interface xe5	Enter the interface mode
(config-if)#enable-rsvp	Enable RSVP
(config-if)#label-switching	Enable label-switching
(config-if)#commit	Commit the transaction.

RSVP Path on PE1

(config)#rsvp-path primary_1	Enter the rsvp-path configuration mode with name
(config-path)#10.1.2.21 strict	Specify the first next-hop ip address
(config-path)#10.2.3.32 strict	Specify the second next-hop ip address
(config-path)#exit	Exit the rsvp-path configuration mode
#configure terminal	Enter the configuration mode
(config)#rsvp-path bypass_1	Enter the rsvp-path configuration mode with name
(config-path)#10.1.4.41 strict	Specify the first next-hop ip address
(config-path)#10.3.4.34 strict	Specify the second next-hop ip address
(config-path)#exit	Exit the rsvp-path configuration mode
#configure terminal	Enter the configuration mode
(config)#rsvp-trunk R1-R3	Enter the rsvp trunk to be created with name
(config-trunk)#primary path primary_1	Configure primary path for the trunk
(config-trunk)#to 3.3.3.3	Enter the destination ip
(config-trunk)# primary fast-reroute protection facility	Configure facility backup protection for the trunk
(config-trunk)#exit	Exit the configuration mode
(config)#rsvp-bypass B1-B8	Enter the rsvp bypass to be created with name
(config-trunk)#path bypass_1	Configure primary path for the trunk
(config-trunk)#to 3.3.3.3	Enter the destination IP
(config-if)#commit	Commit the transaction.

Validation

OSPF Neighborship

PE1

```
#show ip ospf neighbor

Total number of full neighbors: 2
OSPF process 1 VRF(default):
Neighbor ID     Pri   State            Dead Time   Address         Interface
Instance ID
2.2.2.2         1   Full/Backup     00:00:38   10.1.2.21             xe1
0
4.4.4.4         1   Full/DR          00:00:33   10.1.4.41             xe5
0
```

P1

```
#show ip ospf neighbor

Total number of full neighbors: 2
OSPF process 1 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address     Interface    Instance ID
```

```
1.1.1.1          1    Full/DR         00:00:35    10.1.2.12       xe1           0
3.3.3.3          1    Full/Backup     00:00:34    10.2.3.32       xe10          0
```

P2

```
#show ip ospf neighbor

Total number of full neighbors: 2
OSPF process 1 VRF(default):
Neighbor ID     Pri   State     Dead Time   Address     Interface         Instance ID
2.2.2.2          1   Full/DR     00:00:37     10.2.3.23     xe10              0
4.4.4.4          1   Full/Backup 00:00:39     10.3.4.43     xe5               0
```

PE2

```
#show ip ospf neighbor

Total number of full neighbors: 2
OSPF process 1 VRF(default):
Neighbor ID    Pri   State          Dead Time   Address         Interface     Instance ID
1.1.1.1        1   Full/Backup      00:00:38      10.1.4.14      xe2           0
3.3.3.3        1    Full/DR         00:00:36      10.3.4.34      xe5           0
```

RSVP Session

PE1

```
#show rsvp session
Type  : PRI - Primary, SEC - Secondary, DTR - Detour, BPS - Bypass
State : UP - Up, DN - Down, BU - Backup in Use, SU - Secondary in Use, FS - Forced to
Secondary
* indicates the session is active with local repair at one or more nodes

Ingress RSVP:
To              From           Type  LSPName                          State Uptime    Rt
Style  Labelin  Labelout  DSType
3.3.3.3         1.1.1.1         PRI   R1-R3-Primary                      UP    00:54:48  1
1 SE     -        24321     DEFAULT
3.3.3.3         1.1.1.1         BPS   B1-B4-Bypass                       UP    01:08:32  1
1 SE     -        24321     DEFAULT
Total 2 displayed, Up 2, Down 0.
#show rsvp bypass
Ingress RSVP:
To              From           LSPName                          State Uptime    Rt  Style
Labelin  Labelout  DSType
3.3.3.3         1.1.1.1         B1-B4-Bypass                       UP    01:09:17  1 1 SE
-        24321     DEFAULT


#show rsvp bypass protected-lsp-list
Bypass trunk: B1-B4
Bypass trunk bandwidth type: best-effort
List of LSP's Protected:
Tunnel-id     Lsp Id     Lsp Name                 Role     Ext_tnl_id     Ingress
Egress
```



```
5001        2202      R1-R3-Primary             Ingress   1.1.1.1       1.1.1.1
3.3.3.3
Total LSP protected : 1
 Bandwidth in use : 0


#show rsvp bypass B1-B4 protected-lsp-list
Bypass trunk: B1-B4
Bypass trunk bandwidth type: best-effort
List of LSP's Protected:
Tunnel-id     Lsp Id     Lsp Name                  Role     Ext_tnl_id     Ingress
Egress
5001        2202      R1-R3-Primary             Ingress   1.1.1.1       1.1.1.1
3.3.3.3
Total LSP protected : 1
 Bandwidth in use : 0


#show rsvp session detail
Ingress (Primary)
3.3.3.3
  From: 1.1.1.1, LSPstate: Up, LSPname: R1-R3-Primary
  Ingress FSM state: Operational
  Establishment Time: 0s 8ms
  Setup priority: 7, Hold priority: 0
  CSPF usage: Enabled, CSPF Retry Count: 0, CSPF Retry Interval: 30 seconds
  IGP-Shortcut: Disabled, LSP metric: 2
  LSP Protection: facility
  Fast-Reroute bandwidth : 0
  Protection type desired: Link
  Fast-Reroute Setup priority: 7, Hold priority: 0
  Bypass trunk: B1-B4,  Merge Point: 10.2.3.32,  MP Label: 3
    Bypass OutLabel: 24321,  OutIntf: xe5
    Protection provided -> Type: Link, BW: Best-effort
  Label in: -,  Label out:    24321
  Tspec rate: 0, Fspec rate: 0
  Policer: Not Configured
  Tunnel Id: 5001, LSP Id: 2202, Ext-Tunnel Id: 1.1.1.1
  Downstream: 10.1.2.21, xe1
  Path refresh: 30 seconds (RR enabled) (due in 26564 seconds)
  Resv refresh: 0 seconds (due in 0 seconds)
  Resv lifetime: 157 seconds (due in 150 seconds)
  Retry count: 0, intrvl: 30 seconds
  RRO re-use as ERO: Disabled
  Label Recording: Enabled
  Admin Groups: none
  Configured Path: primary_1 (in use)
  Configured Explicit Route Detail :
   10.1.2.21/32 strict
   10.2.3.32/32 strict
  Session Explicit Route Detail :
```

```
   10.1.2.21/32 strict
   10.2.3.32/32 strict
  Record route:
   LP = 1 -> PLR's Downstream link is protected      PU = 1 -> Protection is in use on
PLR
   NP = 1 -> PLR's Downstream neighbor is protected  BP = 1 -> BW protection available
at PLR
   ---------------------------------------------------------------
   IP Address        Label     (LP, PU, NP, BP)
   ---------------------------------------------------------------
   <self>
   10.1.2.21         24321     ( 0,  0,  0,  0)
   10.2.3.32         3         ( 0,  0,  0,  0)
  Style: Shared Explicit Filter
  Traffic type: controlled-load
  Minimum Path MTU: 1500
  Last Recorded Error Code: None
  Last Recorded Error Value: None
  Node where Last Recorded Error originated: None
  Trunk Type: mpls
Ingress (Bypass)
3.3.3.3
  From: 1.1.1.1, LSPstate: Up, LSPname: B1-B4-Bypass
  Ingress FSM state: Operational
  Establishment Time: 0s 14ms
  Setup priority: 7, Hold priority: 0
  CSPF usage: Enabled, CSPF Retry Count: 0, CSPF Retry Interval: 30 seconds
  IGP-Shortcut: Disabled, LSP metric: 2
  LSP Protection: None
  Bypass trunk bandwidth type: Best-effort
   Label in: -,  Label out:    24321
  Tspec rate: 0, Fspec rate: 0
  Policer: Not Configured
  Tunnel Id: 5002, LSP Id: 2203, Ext-Tunnel Id: 1.1.1.1
  Downstream: 10.1.4.41, xe5
  Path refresh: 30 seconds (RR enabled) (due in 25747 seconds)
  Resv lifetime: 157 seconds (due in 139 seconds)
  Retry count: 0, intrvl: 30 seconds
  RRO re-use as ERO: Disabled
  Label Recording: Disabled
  Admin Groups: none
  Configured Path: bypass_1 (in use)
  Configured Explicit Route Detail :
   10.1.4.41/32 strict
   10.3.4.34/32 strict
  Session Explicit Route Detail :
   10.1.4.41/32 strict
   10.3.4.34/32 strict
  Record route:
   ---------------------------------------------------------------
   IP Address        Label
```

```
   ------------------------------------------------------------
   <self>
   10.1.4.41
   10.3.4.34
  Style: Shared Explicit Filter
  Traffic type: controlled-load
  Minimum Path MTU: 1500
  Last Recorded Error Code: None
  Last Recorded Error Value: None
  Node where Last Recorded Error originated: None
  Trunk Type: mpls
  Total LSP protected : 1, Bandwidth in use : 0
```

P1

```
#show rsvp session
Type  : PRI - Primary, SEC - Secondary, DTR - Detour, BPS - Bypass
State : UP - Up, DN - Down, BU - Backup in Use, SU - Secondary in Use, FS - Forced to
Secondary
* indicates the session is active with local repair at one or more nodes

Transit RSVP:
To              From            Type  LSPName                          State Uptime    Rt
Style  Labelin  Labelout  DSType
3.3.3.3         1.1.1.1          PRI   R1-R3-Primary                      UP    00:57:44  1
1 SE     24321    3          ELSP_CON
Total 1 displayed, Up 1, Down 0.

#show rsvp session de
Transit
3.3.3.3
  From: 1.1.1.1, LSPstate: Up, LSPname: R1-R3-Primary
  Transit upstream state: Operational, downstream state: Operational
  Setup priority: 7, Hold priority: 0
  IGP-Shortcut: Disabled, LSP metric: 65
  LSP Protection: facility
  Fast-Reroute bandwidth : 0
  Protection type desired: Link
  Fast-Reroute Setup priority: 7, Hold priority: 0
  Label in:    24321,  Label out:        3
  Tspec rate: 0, Fspec rate: 0
  Tunnel Id: 5001, LSP Id: 2202, Ext-Tunnel Id: 1.1.1.1
  Downstream: 10.2.3.32, xe10   Upstream: 10.1.2.12, xe1
  Path refresh: 30 seconds (RR enabled) (due in 26500 seconds)
  Path lifetime: 157 seconds (due in 126 seconds)
  Resv refresh: 30 seconds (RR enabled) (due in 20926 seconds)
  Resv lifetime: 157 seconds (due in 151 seconds)
  RRO re-use as ERO: Disabled
  Label Recording: Enabled
  Admin Groups:   Received Explicit Route Detail :
   10.1.2.21/32 strict
   10.2.3.32/32 strict
```

```
  Session Explicit Route Detail :
   10.2.3.32/32 strict
  Record route:
   ----------------------------------------------------------------
   IP Address        Label
   ----------------------------------------------------------------
   10.1.2.12         24321
   <self>
   10.2.3.32         3
  Style: Shared Explicit Filter
  Traffic type: controlled-load
  Minimum Path MTU: 1500
  LSP Type:  ELSP_CONFIG
  CLASS    DSCP_value     EXP_value
  Last Recorded Error Code: None
  Last Recorded Error Value: None
  Node where Last Recorded Error originated: None
  Trunk Type: mpls
```

P2

```
#show rsvp session
Type  : PRI - Primary, SEC - Secondary, DTR - Detour, BPS - Bypass
State : UP - Up, DN - Down, BU - Backup in Use, SU - Secondary in Use, FS - Forced to
Secondary
* indicates the session is active with local repair at one or more nodes

Egress RSVP:
To              From            Type  LSPName                          State Uptime    Rt
Style  Labelin  Labelout  DSType
3.3.3.3         1.1.1.1          PRI   R1-R3-Primary                      UP    00:58:47  1
1 SE     3        -          ELSP_CON
3.3.3.3         1.1.1.1          PRI   B1-B4-Bypass                       UP    01:12:30  1
1 SE     3        -          ELSP_CON
Total 2 displayed, Up 2, Down 0

#show rsvp session detail
Egress
3.3.3.3
  From: 1.1.1.1, LSPstate: Up, LSPname: R1-R3-Primary
  Egress FSM state: Operational
  Setup priority: 7, Hold priority: 0
  IGP-Shortcut: Disabled, LSP metric: 65
  LSP Protection: facility
  Fast-Reroute bandwidth : 0
  Protection type desired: Link
  Fast-Reroute Setup priority: 7, Hold priority: 0
  Label in:        3,  Label out: -
  Tspec rate: 0, Fspec rate: 0
  Tunnel Id: 5001, LSP Id: 2202, Ext-Tunnel Id: 1.1.1.1
  Upstream: 10.2.3.23, xe10
  Path lifetime: 157 seconds (due in 140 seconds)
```

```
  Resv refresh: 30 seconds (RR enabled) (due in 37780 seconds)
  RRO re-use as ERO: Disabled
  Label Recording: Enabled
  Admin Groups:   Received Explicit Route Detail :
   10.2.3.32/32 strict
  Record route:
   ----------------------------------------------------------------
   IP Address        Label
   ----------------------------------------------------------------
   10.1.2.12         24321
   10.2.3.23         3
   <self>
  Style: Shared Explicit Filter
  Traffic type: controlled-load
  Minimum Path MTU: 1500
  LSP Type:  ELSP_CONFIG
  CLASS    DSCP_value     EXP_value
  Last Recorded Error Code: None
  Last Recorded Error Value: None
  Node where Last Recorded Error originated: None
  Trunk Type: mpls
Egress
3.3.3.3
  From: 1.1.1.1, LSPstate: Up, LSPname: B1-B4-Bypass
  Egress FSM state: Operational
  Setup priority: 7, Hold priority: 0
  IGP-Shortcut: Disabled, LSP metric: 65
  LSP Protection: None
  Label in:        3,  Label out: -
  Tspec rate: 0, Fspec rate: 0
  Tunnel Id: 5002, LSP Id: 2203, Ext-Tunnel Id: 1.1.1.1
  Upstream: 10.3.4.43, xe5
  Path lifetime: 157 seconds (due in 134 seconds)
  Resv refresh: 30 seconds (RR enabled) (due in 29222 seconds)
  RRO re-use as ERO: Disabled
  Label Recording: Disabled
  Admin Groups:   Received Explicit Route Detail :
   10.3.4.34/32 strict
  Record route:
   ----------------------------------------------------------------
   IP Address        Label
   ----------------------------------------------------------------
   10.1.4.14
   10.3.4.43
   <self>
  Style: Shared Explicit Filter
  Traffic type: controlled-load
  Minimum Path MTU: 1500
  LSP Type:  ELSP_CONFIG
  CLASS    DSCP_value     EXP_value
```

```
  Last Recorded Error Code: None
  Last Recorded Error Value: None
  Node where Last Recorded Error originated: None
  Trunk Type: mpls.
```

PE2

```
#show rsvp session
Type  : PRI - Primary, SEC - Secondary, DTR - Detour, BPS - Bypass
State : UP - Up, DN - Down, BU - Backup in Use, SU - Secondary in Use, FS - Forced to
Secondary
* indicates the session is active with local repair at one or more nodes

Transit RSVP:
To              From            Type  LSPName                          State Uptime    Rt
Style  Labelin  Labelout  DSType
3.3.3.3         1.1.1.1          PRI   B1-B4-Bypass                       UP    01:14:12  1
1 SE     24321    3         ELSP_CON
Total 1 displayed, Up 1, Down 0.


#show rsvp session de
Transit
3.3.3.3
  From: 1.1.1.1, LSPstate: Up, LSPname: B1-B4-Bypass
  Transit upstream state: Operational, downstream state: Operational
  Setup priority: 7, Hold priority: 0
  IGP-Shortcut: Disabled, LSP metric: 65
  LSP Protection: None
  Label in:    24321,  Label out:        3
  Tspec rate: 0, Fspec rate: 0
  Tunnel Id: 5002, LSP Id: 2203, Ext-Tunnel Id: 1.1.1.1
  Downstream: 10.3.4.34, xe5   Upstream: 10.1.4.14, xe2
  Path refresh: 30 seconds (RR enabled) (due in 25543 seconds)
  Path lifetime: 157 seconds (due in 146 seconds)
  Resv refresh: 30 seconds (RR enabled) (due in 17729 seconds)
  Resv lifetime: 157 seconds (due in 135 seconds)
  RRO re-use as ERO: Disabled
  Label Recording: Disabled
  Admin Groups:   Received Explicit Route Detail :
   10.1.4.41/32 strict
   10.3.4.34/32 strict
  Session Explicit Route Detail :
   10.3.4.34/32 strict
  Record route:
   ----------------------------------------------------------------
   IP Address        Label
   ----------------------------------------------------------------
   10.1.4.14
   <self>
   10.3.4.34
  Style: Shared Explicit Filter
```

```
Traffic type: controlled-load
Minimum Path MTU: 1500
LSP Type:  ELSP_CONFIG
CLASS    DSCP_value     EXP_value
Last Recorded Error Code: None
Last Recorded Error Value: None
Node where Last Recorded Error originated: None
Trunk Type: mpls
```

Limitations

Dedicated Bypass Bandwidth

Refer the topology defined above.

Suppose we have two primary tunnels P1 (100mbps) and P2(20mbps) ingressing from R1 and egressing at R3 (path R1->R2>R3) and asking for BW protection and we have two Bypass tunnels bp1 (120mbps) and bp2(80mbps) type dedicated with same ingress and egress router taking Path R1->R4->R3. Below are the two cases defined in which we can observe different kinds of behavior.

1. Let the primary P1 and P2 come up.

CASE 1:

i) If the bypass bp1 (120mbps) comes up first it will give protection to both the primaries P1 and P2. bp2 should remain idle and will not give protection if there are no other primary tunnels asking for it.

CASE 2:

i) If the bypass bp2 (80mbps) comes up first it will give protection to only the primary P2 (20mbps) that will have satisfied protection which will not be changed until the bypass will go down.

ii) After that if bp1 (120mbps) comes it will provide protection to primary P1 (100mbps).

So in the CASE 1 after the protection has been provided to both the primary tunnels P1 and P2 by bypass bp1 if new primary tunnel P3 comes up with BW protection of 80mbps it would be given by bp2 (80mbps).

But in the CASE 2 as bp2 has only 60mbps left (20mbps is being used by P2) and it would not give protection to P3 tunnel and it will remain unprotected. To get the protection new tunnel has to have setup and hold priorities higher than other tunnels which are already been served with the bypass protection.

Secondary Tunnel

Suppose we have primary tunnel P1 (100mbps) ingressing from R1 and egressing at R3 (path R1->R2>R3) and asking for BW protection and we have Bypass tunnel bp1 (120mbps) type dedicated with same ingress and egress router taking Path R1->R4->R3. Then Bypass will start providing protection to primary P1.

If the primary went down it will start using the local protection.

After that if the secondary tunnel is provisioned, primary LSP, which is in using backup state shall continue to use backup path and will not shift over to secondary path.

Facility Bypass with Ring Topology Configuration

This section contains a complete Facility Bypass with Ring Topology configuration.

During facility bypass integration to OcNOS SP, few issues were reported when upstream and downstream interfaces of a session happens to be same (i.e. protection path is same as upstream path) and also CSPF most likely had some issues where LSP path used to formed by crossing the head node of the path.

Considering the information available in RSVP to impose restriction, bypass tunnel path crossing primary LSP node anywhere in between merge point were not considered for mapping.

Below assumption point was added in ERD and documents were updated on the line.

If protection is requested by primary session, then initial bypass matching criteria will be to ensure egress (merge point) node of bypass will be one of the nodes of primary LSP and bypass never intersect any node of primary LSP until the merge point.

The facility bypass method takes advantage of the MPLS label stack. Instead of creating a separate LSP for every backed-up LSP, a single LSP is created that serves to back up a set of LSPs. We call such an LSP tunnel a bypass tunnel. The bypass tunnel must intersect the path of the original LSP(s) somewhere downstream of the PLR. Naturally, this constrains the set of LSPs being backed up via that bypass tunnel to those that pass through some common downstream node. All LSPs that pass through the point of local repair and through this common node that do not also use the facilities involved in the bypass tunnel are candidates for this set of LSPs.

By multiple facility bypass tunnels, we mean that multiple facility bypass tunnels can be created to the same egress/ MP. For a protected LSP there could be multiple candidates available. The mapping of the LSP to one of the backup tunnels has to be efficiently done so that we can extract the maximum benefit out of those backup tunnels available

Topology

Figure 9-17 displays a sample Facility Bypass with Ring topology.

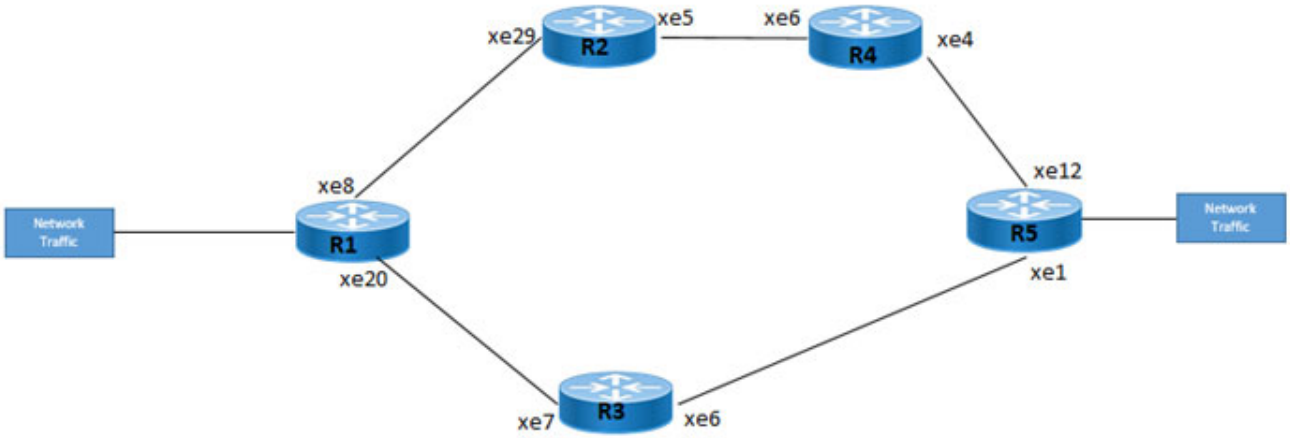


Figure 9-17: Facility Bypass with Ring Topology

Configurations

All configuration commands in the table below should be followed for each router.

R1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode.
`(config-if)#ip address 1.1.1.1/32 secondary`	Configure IP address for the loopback interface.

(config-if)# ip router isis ISIS-IGP	Enable IS-IS routing on an interface
(config-if)#exit	Exit interface mode.
(config)#bfd interval 3 minrx 3 multiplier	Configure BFD interval
(config)# router-id 1.1.1.1	Assigning router-id
(config)#router rsvp	Enter router mode for RSVP.
(config-router)#exit	Exit router configuration mode.
(config)#interface xe8	Specify the Interface to be configured.
(config-if)#ip address 10.1.1.1/24	Configure IP address for the interface.
(config-if)#no shutdown	Administratively bringing up the interface.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# isis network point-to-point	Configure the ISIS interface network type as point to point
(config-if)# ip router isis ISIS-IGP	Enable IS-IS routing on an interface
(config-if)# enable-rsvp	Enable rsvp configuration on interface
(config-if)#exit	Exit interface mode.
(config)#interface xe20	Specify the Interface to be configured
(config-if)#ip address 12.1.1.1/24	Configure IP address for the interface.
(config-if)#no shutdown	Administratively bringing up the interface.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# isis network point-to-point	Configure the ISIS interface network type as point to point
(config-if)# ip router isis ISIS-IGP	Enable IS-IS routing on an interface
(config-if)# enable-rsvp	Enable rsvp configuration on interface
(config-if)#exit	Exit interface mode.
(config)# router isis ISIS-IGP	Create an IS-IS routing instance
(config-router)# is-type level-1	Configure instance as level-1only routing.
(config-router)# metric-style wide	Configure the new style of metric type as wide.
(config-router)# mpls traffic-eng router-id 1.1.1.1	Configure MPLS-TE unique router-id TLV.
(config-router)# mpls traffic-eng level-1	Enable MPLS-TE in is-type Level-1
(config-router)# capability cspf	Enable CSPF feature for ISIS instance.
(config-router)# dynamic-hostname	Configure the hostname to be advertised for an ISIS instance
(config-router)# bfd all-interfaces	Enable BFD for all neighbors.
(config-router)# net 49.0000.0000.0001.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#exit	Exit router mode.
(config)# rsvp-path R1-R5-PRI-001	Create a rsvp path
(config-path)# 10.1.1.2 strict	Configure this explicit router path as a strict hop
(config-path)# 14.1.1.3 strict	Configure this explicit router path as a strict hop
(config-path)# 17.1.1.3 strict	Configure this explicit router path as a strict hop
(config-path)# exit	Exit the rsvp-path mode
(config)# rsvp-path R1-R5-BPS-001	Create a rsvp path
(config-path)# 12.1.1.2 strict	Configure this explicit router path as a strict hop

(config-path)# 15.1.1.3 strict	Configure this explicit router path as a strict hop
(config-path)# exit	Exit the rsvp-path mode
(config)#rsvp-trunk R1-R5-PRI-001	Enter the trunk mode for RSVP
(config-trunk)#primary fast-reroute protection facility	Configure primary fast-reroute protection facility for a trunk.
(config-trunk)#primary fast-reroute node-protection	Configure primary fast-reroute node protection for a trunk.
(config-trunk)#primary path R1-R5-PRI-001	Configure trunk to use the defined path.
(config-trunk)#to 5.5.5.5	Specify the IPv4 egress (destination point) for the LSP
(config-path)# exit	Exit the rsvp-trunk mode
(config)#rsvp-bypass R1-R5-BPS-001	Enter the bypass mode for RSVP
(config-trunk)#path R1-R5-BPS-001	Configure path for bypass tunnel
(config-trunk)#to 5.5.5.5	Specify the IPv4 egress (destination point) for the LSP
(config-path)# exit	Exit the rsvp-bypass mode
(config)#commit	Commit the transaction.

R2

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 2.2.2.2/32 secondary	Configure IP address for the loopback interface.
(config-if)# ip router isis ISIS-IGP	Enable IS-IS routing on an interface
(config-if)#exit	Exit interface mode.
(config)# router-id 2.2.2.2	Assigning router-id
(config)#bfd interval 3 minrx 3 multiplier	Configure BFD interval
(config)#router rsvp	Enter router mode for RSVP.
(config-router)#exit	Exit router configuration mode.
(config)#interface xe29	Specify the Interface to be configured.
(config-if)#ip address 10.1.1.2/24	Configure IP address for the interface.
(config-if)#no shutdown	Administratively bringing up the interface.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# isis network point-to-point	Configure the ISIS interface network type as point to point
(config-if)# ip router isis ISIS-IGP	Enable IS-IS routing on an interface
(config-if)# enable-rsvp	Enable rsvp configuration on interface
(config-if)#exit	Exit interface mode.
(config)#interface xe5	Specify the Interface to be configured
(config-if)#ip address 14.1.1.2/24	Configure IP address for the interface.
(config-if)#no shutdown	Administratively bringing up the interface.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# isis network point-to-point	Configure the ISIS interface network type as point to point
(config-if)# ip router isis ISIS-IGP	Enable IS-IS routing on an interface
(config-if)# enable-rsvp	Enable rsvp configuration on interface

(config-if)#exit	Exit interface mode.
(config)# router isis ISIS-IGP	Create an IS-IS routing instance
(config-router)# is-type level-1	Configure instance as level-1only routing.
(config-router)# metric-style wide	Configure the new style of metric type as wide.
(config-router)# mpls traffic-eng router-id 2.2.2.2	Configure MPLS-TE unique router-id TLV.
(config-router)# mpls traffic-eng level-1	Enable MPLS-TE in is-type Level-1
(config-router)# capability cspf	Enable CSPF feature for ISIS instance.
(config-router)# dynamic-hostname	Configure the hostname to be advertised for an ISIS instance
(config-router)# bfd all-interfaces	Enable BFD for all neighbors.
(config-router)# net 49.0000.0000.0002.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#exit	Exit router mode.
(config)#commit	Commit the transaction.

R3

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 3.3.3.3/32 secondary	Configure IP address for the loopback interface.
(config-if)# ip router isis ISIS-IGP	Enable IS-IS routing on an interface
(config-if)#exit	Exit interface mode.
(config)# router-id 3.3.3.3	Assigning router-id
(config)#bfd interval 3 minrx 3 multiplier	Configure BFD interval
(config)#router rsvp	Enter router mode for RSVP.
(config-router)#exit	Exit router configuration mode.
(config)#interface xe7	Specify the Interface to be configured.
(config-if)#ip address 12.1.1.2/24	Configure IP address for the interface.
(config-if)#no shutdown	Administratively bringing up the interface.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# isis network point-to-point	Configure the ISIS interface network type as point to point
(config-if)# ip router isis ISIS-IGP	Enable IS-IS routing on an interface
(config-if)# enable-rsvp	Enable rsvp configuration on interface
(config-if)#exit	Exit interface mode.
(config)#interface xe6	Specify the Interface to be configured
(config-if)#ip address 15.1.1.2/24	Configure IP address for the interface.
(config-if)#no shutdown	Administratively bringing up the interface.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# isis network point-to-point	Configure the ISIS interface network type as point to point
(config-if)# ip router isis ISIS-IGP	Enable IS-IS routing on an interface
(config-if)# enable-rsvp	Enable rsvp configuration on interface
(config-if)#exit	Exit interface mode.

(config)# router isis ISIS-IGP	Create an IS-IS routing instance
(config-router)# is-type level-1	Configure instance as level-1only routing.
(config-router)# metric-style wide	Configure the new style of metric type as wide.
(config-router)# mpls traffic-eng router-id 3.3.3.3	Configure MPLS-TE unique router-id TLV.
(config-router)# mpls traffic-eng level-1	Enable MPLS-TE in is-type Level-1
(config-router)# capability cspf	Enable CSPF feature for ISIS instance.
(config-router)# dynamic-hostname	Configure the hostname to be advertised for an ISIS instance
(config-router)# bfd all-interfaces	Enable BFD for all neighbors.
(config-router)# net 49.0000.0000.0003.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#exit	Exit router mode.
(config)#commit	Commit the transaction.

R4

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 4.4.4.4/32 secondary	Configure IP address for the loopback interface.
(config-if)# ip router isis ISIS-IGP	Enable IS-IS routing on an interface
(config-if)#exit	Exit interface mode.
(config)# router-id 4.4.4.4	Assigning router-id
(config)#bfd interval 3 minrx 3 multiplier	Configure BFD interval
(config)#router rsvp	Enter router mode for RSVP.
(config-router)#exit	Exit router configuration mode.
(config)#interface xe4	Specify the Interface to be configured.
(config-if)#ip address 17.1.1.2/24	Configure IP address for the interface.
(config-if)#no shutdown	Administratively bringing up the interface.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# isis network point-to-point	Configure the ISIS interface network type as point to point
(config-if)# ip router isis ISIS-IGP	Enable IS-IS routing on an interface
(config-if)# enable-rsvp	Enable rsvp configuration on interface
(config-if)#exit	Exit interface mode.
(config)#interface xe6	Specify the Interface to be configured
(config-if)#ip address 14.1.1.3/24	Configure IP address for the interface.
(config-if)#no shutdown	Administratively bringing up the interface.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# isis network point-to-point	Configure the ISIS interface network type as point to point
(config-if)# ip router isis ISIS-IGP	Enable IS-IS routing on an interface
(config-if)# enable-rsvp	Enable rsvp configuration on interface
(config-if)#exit	Exit interface mode.
(config)# router isis ISIS-IGP	Create an IS-IS routing instance

(config-router)# is-type level-1	Configure instance as level-1only routing.
(config-router)# metric-style wide	Configure the new style of metric type as wide.
(config-router)# mpls traffic-eng router-id 4.4.4.4	Configure MPLS-TE unique router-id TLV.
(config-router)# mpls traffic-eng level-1	Enable MPLS-TE in is-type Level-1
(config-router)# capability cspf	Enable CSPF feature for ISIS instance.
(config-router)# dynamic-hostname	Configure the hostname to be advertised for an ISIS instance
(config-router)# bfd all-interfaces	Enable BFD for all neighbors.
(config-router)# net 49.0000.0000.0004.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#exit	Exit router mode.
(config)#commit	Commit the transaction.

R5

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 5.5.5.5/32 secondary	Configure IP address for the loopback interface.
(config-if)# ip router isis ISIS-IGP	Enable IS-IS routing on an interface
(config-if)#exit	Exit interface mode.
(config)# router-id 5.5.5.5	Assigning router-id
(config)#bfd interval 3 minrx 3 multiplier	Configure BFD interval
(config)#router rsvp	Enter router mode for RSVP.
(config-router)#exit	Exit router configuration mode.
(config)#interface xe12	Specify the Interface to be configured.
(config-if)#ip address 17.1.1.3/24	Configure IP address for the interface.
(config-if)#no shutdown	Administratively bringing up the interface.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# isis network point-to-point	Configure the ISIS interface network type as point to point
(config-if)# ip router isis ISIS-IGP	Enable IS-IS routing on an interface
(config-if)# enable-rsvp	Enable rsvp configuration on interface
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Specify the Interface to be configured
(config-if)#ip address 15.1.1.3/24	Configure IP address for the interface.
(config-if)#no shutdown	Administratively bringing up the interface.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# isis network point-to-point	Configure the ISIS interface network type as point to point
(config-if)# ip router isis ISIS-IGP	Enable IS-IS routing on an interface
(config-if)# enable-rsvp	Enable rsvp configuration on interface
(config-if)#exit	Exit interface mode.
(config)# router isis ISIS-IGP	Create an IS-IS routing instance
(config-router)# is-type level-1	Configure instance as level-1only routing.

(config-router)# metric-style wide	Configure the new style of metric type as wide.
(config-router)# mpls traffic-eng router-id 5.5.5.5	Configure MPLS-TE unique router-id TLV.
(config-router)# mpls traffic-eng level-1	Enable MPLS-TE in is-type Level-1
(config-router)# capability cspf	Enable CSPF feature for ISIS instance.
(config-router)# dynamic-hostname	Configure the hostname to be advertised for an ISIS instance
(config-router)# bfd all-interfaces	Enable BFD for all neighbors.
(config-router)# net 49.0000.0000.0005.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#exit	Exit router mode.
(config)#commit	Commit the transaction.

Validation

RSVP Session

Validate that the RSVP Session is up.

R1:

```
R1#show rsvp session
Type  : PRI - Primary, SEC - Secondary, DTR - Detour, BPS - Bypass
State : UP - Up, DN - Down, BU - Backup in Use, SU - Secondary in Use, FS - Forced to
Secondary
* indicates the session is active with local repair at one or more nodes
(P) indicates the secondary-priority session is acting as primary

Ingress RSVP:
To              From            Type    LSPName                          State Uptime    Rt
Style  Labelin  Labelout  DSType
5.5.5.5         1.1.1.1           PRI     R1-R5-PRI-001-Primary            UP    00:49:18
1 1 SE     -        52480     DEFAULT
5.5.5.5         1.1.1.1           BPS     R1-R5-BPS-001-Bypass             UP    05:24:23
1 1 SE     -        25600     DEFAULT
Total 2 displayed, Up 2, Down 0.

R1#show rsvp session detail
Ingress (Primary)
5.5.5.5
  From: 1.1.1.1, LSPstate: Up, LSPname: R1-R5-PRI-001-Primary
  Ingress FSM state: Operational
  Establishment Time: 322s 925ms
  Setup priority: 7, Hold priority: 0
  CSPF usage: Enabled, CSPF Retry Count: 0, CSPF Retry Interval: 30 seconds
  LSP Re-Optimization: Disabled, Re-Optimization Timer: NA, Cspf Client: ISIS
  IGP-Shortcut: Disabled, LSP metric: 30
  LSP Protection: facility
  Fast-Reroute bandwidth : 0
  Protection type desired: Node
  Fast-Reroute Hop limit: 255
```

```
  Fast-Reroute Setup priority: 7, Hold priority: 0
  Bypass trunk: R1-R5-BPS-001,  Merge Point: 17.1.1.3,  MP Label: 25600
    Bypass OutLabel: 25600,  OutIntf: xe20
    Protection provided -> Type: Node, BW: Best-effort
  Label in: -,  Label out:    52480,
  Tspec rate: 0, Fspec rate: 0
  Policer: Not Configured
  Tunnel Id: 5001, LSP Id: 2201, Ext-Tunnel Id: 1.1.1.1
  Bind value: 0, Oper state: NA, Alloc mode: NA
  Downstream: 10.1.1.2, xe8
  Path refresh: 30 seconds (RR enabled) (due in 27023 seconds)
  Resv refresh: 0 seconds (due in 0 seconds)
  Resv lifetime: 157 seconds (due in 128 seconds)
  Retry count: 0, intrvl: 30 seconds
  RRO re-use as ERO: Disabled
  Label Recording: Enabled
  Admin Groups: none
  Configured Path: R1-R5-PRI-001 (in use)
  Configured Explicit Route Detail :
   10.1.1.2/32 strict
   14.1.1.3/32 strict
   17.1.1.3/32 strict
  Session Explicit Route Detail :
   10.1.1.2/32 strict
   14.1.1.3/32 strict
   17.1.1.3/32 strict
  Record route:
   LP = 1 -> PLR's Downstream link is protected      PU = 1 -> Protection is in use on
PLR
   NP = 1 -> PLR's Downstream neighbor is protected  BP = 1 -> BW protection available
at PLR
   ---------------------------------------------------------------
   IP Address        Label     (LP, PU, NP, BP)
   ---------------------------------------------------------------
   <self>
   10.1.1.2          52480     ( 0,  0,  0,  0)
   14.1.1.3          52480     ( 0,  0,  0,  0)
   17.1.1.3          25600     ( 0,  0,  0,  0)
  Style: Shared Explicit Filter
  Traffic type: controlled-load
  Minimum Path MTU: 9216
Recorded Time : N/A
  Current Error:
    Code : None, Value : None
    Originated Node : None, Recorded Time : N/A
  Last Signaled Error:
    Code : None, Value : None
    Originated Node : None, Recorded Time : N/A
  Trunk Type: mpls
Ingress (Bypass)
5.5.5.5
```

```
  From: 1.1.1.1, LSPstate: Up, LSPname: R1-R5-BPS-001-Bypass
  Ingress FSM state: Operational
  Establishment Time: 0s 4ms
  Setup priority: 7, Hold priority: 0
  CSPF usage: Enabled, CSPF Retry Count: 0, CSPF Retry Interval: 30 seconds
  LSP Re-Optimization: Disabled, Re-Optimization Timer: NA, Cspf Client: ISIS
  IGP-Shortcut: Disabled, LSP metric: 20
  LSP Protection: None
  Bypass trunk bandwidth type: Best-effort
   Label in: -,  Label out:    25600,
  Tspec rate: 0, Fspec rate: 0
  Policer: Not Configured
  Tunnel Id: 5002, LSP Id: 2205, Ext-Tunnel Id: 1.1.1.1
  Bind value: 0, Oper state: NA, Alloc mode: NA
  Downstream: 12.1.1.2, xe20
  Path refresh: 30 seconds (RR enabled) (due in 10514 seconds)
  Resv lifetime: 157 seconds (due in 141 seconds)
  Retry count: 0, intrvl: 30 seconds
  RRO re-use as ERO: Disabled
  Label Recording: Disabled
  Admin Groups: none
  Configured Path: R1-R5-BPS-001 (in use)
  Configured Explicit Route Detail :
   12.1.1.2/32 strict
   15.1.1.3/32 strict
  Session Explicit Route Detail :
   12.1.1.2/32 strict
   15.1.1.3/32 strict
  Record route:
   ----------------------------------------------------------------
   IP Address        Label
   ----------------------------------------------------------------
   <self>
   12.1.1.2
   15.1.1.3
  Style: Shared Explicit Filter
  Traffic type: controlled-load
  Minimum Path MTU: 9216
Recorded Time : N/A
  Current Error:
    Code : None, Value : None
    Originated Node : None, Recorded Time : N/A
  Last Signaled Error:
    Code : RSVP System error (23), Value : N/A (0)
    Originated Node : 15.1.1.3, Recorded Time : 2023 May 16 08:52:51
  Trunk Type: mpls
  Total LSP protected : 1, Bandwidth in use : 0
```

R2:

```
R2#show rsvp session
```

```
Type  : PRI - Primary, SEC - Secondary, DTR - Detour, BPS - Bypass
State : UP - Up, DN - Down, BU - Backup in Use, SU - Secondary in Use, FS - Forced to
Secondary
* indicates the session is active with local repair at one or more nodes
(P) indicates the secondary-priority session is acting as primary

Transit RSVP:
To              From            Type    LSPName                          State Uptime    Rt
Style  Labelin  Labelout  DSType
5.5.5.5          1.1.1.1          PRI     R1-R5-PRI-001-Primary            UP    00:49:59
1 1 SE     52480    52480     ELSP_CON
Total 1 displayed, Up 1, Down 0.

R2#
R2#
R2#show rsvp session detail
Transit
5.5.5.5
  From: 1.1.1.1, LSPstate: Up, LSPname: R1-R5-PRI-001-Primary
  Transit upstream state: Operational, downstream state: Operational
  Setup priority: 7, Hold priority: 0
  IGP-Shortcut: Disabled, LSP metric: 65
  LSP Protection: facility
  Fast-Reroute bandwidth : 0
  Protection type desired: Node
  Fast-Reroute Hop limit: 255
  Fast-Reroute Setup priority: 7, Hold priority: 0
  Label in:    52480,  Label out:    52480,
  Tspec rate: 0, Fspec rate: 0
  Tunnel Id: 5001, LSP Id: 2201, Ext-Tunnel Id: 1.1.1.1
  Bind value: 0, Oper state: NA, Alloc mode: NA
  Downstream: 14.1.1.3, xe5   Upstream: 10.1.1.1, xe29
  Path refresh: 30 seconds (RR enabled) (due in 27004 seconds)
  Path lifetime: 157 seconds (due in 130 seconds)
  Resv refresh: 30 seconds (RR enabled) (due in 19943 seconds)
  Resv lifetime: 157 seconds (due in 141 seconds)
  RRO re-use as ERO: Disabled
  Label Recording: Enabled
  Admin Groups:   Received Explicit Route Detail :
   10.1.1.2/32 strict
   14.1.1.3/32 strict
   17.1.1.3/32 strict
  Session Explicit Route Detail :
   14.1.1.3/32 strict
   17.1.1.3/32 strict
  Record route:
   ----------------------------------------------------------------
   IP Address        Label
   ----------------------------------------------------------------
   10.1.1.1          52480
   <self>
```

```
   14.1.1.3          52480
   17.1.1.3          25600
  Style: Shared Explicit Filter
  Traffic type: controlled-load
  Minimum Path MTU: 9216
  LSP Type:  ELSP_CONFIG
  CLASS    DSCP_value     EXP_value
  Current Error:
    Code : None, Value : None
    Originated Node : None, Recorded Time : N/A
  Trunk Type: mpls
```

R3:

```
R3#show rsvp session
Type  : PRI - Primary, SEC - Secondary, DTR - Detour, BPS - Bypass
State : UP - Up, DN - Down, BU - Backup in Use, SU - Secondary in Use, FS - Forced to
Secondary
* indicates the session is active with local repair at one or more nodes
(P) indicates the secondary-priority session is acting as primary

Transit RSVP:
To              From           Type    LSPName                          State Uptime    Rt
Style  Labelin  Labelout  DSType
5.5.5.5         1.1.1.1         PRI     R1-R5-BPS-001-Bypass             UP    05:25:48
1 1 SE     25600    3         ELSP_CON
Total 1 displayed, Up 1, Down 0.

R3#show rsvp session detail
Transit
5.5.5.5
  From: 1.1.1.1, LSPstate: Up, LSPname: R1-R5-BPS-001-Bypass
  Transit upstream state: Operational, downstream state: Operational
  Setup priority: 7, Hold priority: 0
  IGP-Shortcut: Disabled, LSP metric: 65
  LSP Protection: None
  Label in:    25600,  Label out:        3,
  Tspec rate: 0, Fspec rate: 0
  Tunnel Id: 5002, LSP Id: 2205, Ext-Tunnel Id: 1.1.1.1
  Bind value: 0, Oper state: NA, Alloc mode: NA
  Downstream: 15.1.1.3, xe6   Upstream: 12.1.1.1, xe7
  Path refresh: 30 seconds (RR enabled) (due in 10445 seconds)
  Path lifetime: 157 seconds (due in 155 seconds)
  Resv refresh: 30 seconds (RR enabled) (due in 24008 seconds)
  Resv lifetime: 157 seconds (due in 140 seconds)
  RRO re-use as ERO: Disabled
  Label Recording: Disabled
  Admin Groups:   Received Explicit Route Detail :
   12.1.1.2/32 strict
   15.1.1.3/32 strict
  Session Explicit Route Detail :
   15.1.1.3/32 strict
```

```
  Record route:
   ----------------------------------------------------------------
   IP Address        Label
   ----------------------------------------------------------------
   12.1.1.1
   <self>
   15.1.1.3
  Style: Shared Explicit Filter
  Traffic type: controlled-load
  Minimum Path MTU: 9216
  LSP Type:  ELSP_CONFIG
  CLASS    DSCP_value     EXP_value
Recorded Time : N/A
  Current Error:
    Code : None, Value : None
    Originated Node : None, Recorded Time : N/A
  Trunk Type: mpls
R3#
```

R4:

```
R4#show rsvp session
Type  : PRI - Primary, SEC - Secondary, DTR - Detour, BPS - Bypass
State : UP - Up, DN - Down, BU - Backup in Use, SU - Secondary in Use, FS - Forced to
Secondary
* indicates the session is active with local repair at one or more nodes
(P) indicates the secondary-priority session is acting as primary

Transit RSVP:
To              From           Type    LSPName                          State Uptime    Rt
Style  Labelin  Labelout  DSType
5.5.5.5         1.1.1.1          PRI     R1-R5-PRI-001-Primary            UP    00:51:13
1 1 SE     52480    25600     ELSP_CON
Total 1 displayed, Up 1, Down 0.

R4#
R4#
R4#show rsvp session detail
Transit
5.5.5.5
  From: 1.1.1.1, LSPstate: Up, LSPname: R1-R5-PRI-001-Primary
  Transit upstream state: Operational, downstream state: Operational
  Setup priority: 7, Hold priority: 0
  IGP-Shortcut: Disabled, LSP metric: 65
  LSP Protection: facility
  Fast-Reroute bandwidth : 0
  Protection type desired: Node
  Fast-Reroute Hop limit: 255
  Fast-Reroute Setup priority: 7, Hold priority: 0
  Label in:    52480,  Label out:    25600,
  Tspec rate: 0, Fspec rate: 0
  Tunnel Id: 5001, LSP Id: 2201, Ext-Tunnel Id: 1.1.1.1
```

```
  Bind value: 0, Oper state: NA, Alloc mode: NA
  Downstream: 17.1.1.3, xe4   Upstream: 14.1.1.2, xe6
  Path refresh: 30 seconds (RR enabled) (due in 26908 seconds)
  Path lifetime: 157 seconds (due in 148 seconds)
  Resv refresh: 30 seconds (RR enabled) (due in 37164 seconds)
  Resv lifetime: 157 seconds (due in 144 seconds)
  RRO re-use as ERO: Disabled
  Label Recording: Enabled
  Admin Groups:   Received Explicit Route Detail :
   14.1.1.3/32 strict
   17.1.1.3/32 strict
  Session Explicit Route Detail :
   17.1.1.3/32 strict
  Record route:
   ------------------------------------------------------------
   IP Address        Label
   ------------------------------------------------------------
   10.1.1.1          52480
   14.1.1.2          52480
   <self>
   17.1.1.3          25600
  Style: Shared Explicit Filter
  Traffic type: controlled-load
  Minimum Path MTU: 9216
  LSP Type:  ELSP_CONFIG
  CLASS    DSCP_value     EXP_value
  Current Error:
    Code : None, Value : None
    Originated Node : None, Recorded Time : N/A
  Trunk Type: mpls
```

R5:

```
R5#show rsvp session
Type  : PRI - Primary, SEC - Secondary, DTR - Detour, BPS - Bypass
State : UP - Up, DN - Down, BU - Backup in Use, SU - Secondary in Use, FS - Forced to
Secondary
* indicates the session is active with local repair at one or more nodes
(P) indicates the secondary-priority session is acting as primary

Egress RSVP:
To              From           Type    LSPName                          State Uptime    Rt
Style  Labelin  Labelout  DSType
5.5.5.5         1.1.1.1          PRI     R1-R5-PRI-001-Primary            UP    00:51:45
1 1 SE     25600    -         ELSP_CON
5.5.5.5         1.1.1.1          PRI     R1-R5-BPS-001-Bypass             UP    05:26:50
1 1 SE     3        -         ELSP_CON
Total 2 displayed, Up 2, Down 0.

R5#show rsvp session detail
Egress
5.5.5.5
```

```
  From: 1.1.1.1, LSPstate: Up, LSPname: R1-R5-PRI-001-Primary
  Egress FSM state: Operational
  Setup priority: 7, Hold priority: 0
  IGP-Shortcut: Disabled, LSP metric: 65
  LSP Protection: facility
  Fast-Reroute bandwidth : 0
  Protection type desired: Node
  Fast-Reroute Hop limit: 255
  Fast-Reroute Setup priority: 7, Hold priority: 0
  Label in:    25600,  Label out: -,
  Tspec rate: 0, Fspec rate: 0
  Tunnel Id: 5001, LSP Id: 2201, Ext-Tunnel Id: 1.1.1.1
  Bind value: 0, Oper state: NA, Alloc mode: NA
  Upstream: 17.1.1.2, xe12
  Path lifetime: 157 seconds (due in 126 seconds)
  Resv refresh: 30 seconds (RR enabled) (due in 28434 seconds)
  RRO re-use as ERO: Disabled
  Label Recording: Enabled
  Admin Groups:   Received Explicit Route Detail :
   17.1.1.3/32 strict
  Record route:
   ----------------------------------------------------------------
   IP Address        Label
   ----------------------------------------------------------------
   10.1.1.1          52480
   14.1.1.2          52480
   17.1.1.2          25600
   <self>
  Style: Shared Explicit Filter
  Traffic type: controlled-load
  Minimum Path MTU: 9216
  LSP Type:  ELSP_CONFIG
  CLASS    DSCP_value     EXP_value
Recorded Time : N/A
  Current Error:
    Code : None, Value : None
    Originated Node : None, Recorded Time : N/A
  Trunk Type: mpls
Egress
5.5.5.5
  From: 1.1.1.1, LSPstate: Up, LSPname: R1-R5-BPS-001-Bypass
  Egress FSM state: Operational
  Setup priority: 7, Hold priority: 0
  IGP-Shortcut: Disabled, LSP metric: 65
  LSP Protection: None
  Label in:        3,  Label out: -,
  Tspec rate: 0, Fspec rate: 0
  Tunnel Id: 5002, LSP Id: 2205, Ext-Tunnel Id: 1.1.1.1
  Bind value: 0, Oper state: NA, Alloc mode: NA
  Upstream: 15.1.1.2, xe1
```

```
  Path lifetime: 157 seconds (due in 141 seconds)
  Resv refresh: 30 seconds (RR enabled) (due in 927 seconds)
  RRO re-use as ERO: Disabled
  Label Recording: Disabled
  Admin Groups:   Received Explicit Route Detail :
   15.1.1.3/32 strict
  Record route:
   ----------------------------------------------------------------
   IP Address        Label
   ----------------------------------------------------------------
   12.1.1.1
   15.1.1.2
   <self>
  Style: Shared Explicit Filter
  Traffic type: controlled-load
  Minimum Path MTU: 9216
  LSP Type:  ELSP_CONFIG
  CLASS    DSCP_value     EXP_value
Recorded Time : N/A
  Current Error:
    Code : None, Value : None
    Originated Node : None, Recorded Time : N/A
  Trunk Type: mpls
```

RSVP Bypass

Validate that the RSVP bypass session is up.

R1:

```
R1#   show rsvp bypass
Ingress RSVP:
To              From            LSPName                          State Uptime    Rt  Style
Labelin  Labelout  DSType
5.5.5.5         1.1.1.1         R1-R5-BPS-001-Bypass              UP    05:27:41  1 1 SE
-        25600     DEFAULT
To validate RSVP bypass session details
R1#   show rsvp bypass detail
Ingress (Bypass)
5.5.5.5
  From: 1.1.1.1, LSPstate: Up, LSPname: R1-R5-BPS-001-Bypass
  Ingress FSM state: Operational
  Establishment Time: 0s 4ms
  Setup priority: 7, Hold priority: 0
  CSPF usage: Enabled, CSPF Retry Count: 0, CSPF Retry Interval: 30 seconds
  LSP Re-Optimization: Disabled, Re-Optimization Timer: NA, Cspf Client: ISIS
  IGP-Shortcut: Disabled, LSP metric: 20
  LSP Protection: None
  Bypass trunk bandwidth type: Best-effort
   Label in: -,  Label out:    25600,
  Tspec rate: 0, Fspec rate: 0
  Policer: Not Configured
  Tunnel Id: 5002, LSP Id: 2205, Ext-Tunnel Id: 1.1.1.1
```

```
  Bind value: 0, Oper state: NA, Alloc mode: NA
  Downstream: 12.1.1.2, xe20
  Path refresh: 30 seconds (RR enabled) (due in 10319 seconds)
  Resv lifetime: 157 seconds (due in 126 seconds)
  Retry count: 0, intrvl: 30 seconds
  RRO re-use as ERO: Disabled
  Label Recording: Disabled
  Admin Groups: none
  Configured Path: R1-R5-BPS-001 (in use)
  Configured Explicit Route Detail :
   12.1.1.2/32 strict
   15.1.1.3/32 strict
  Session Explicit Route Detail :
   12.1.1.2/32 strict
   15.1.1.3/32 strict
  Record route:
   ----------------------------------------------------------
   IP Address        Label
   ----------------------------------------------------------
   <self>
   12.1.1.2
   15.1.1.3
  Style: Shared Explicit Filter
  Traffic type: controlled-load
  Minimum Path MTU: 9216
Recorded Time : N/A
  Current Error:
    Code : None, Value : None
    Originated Node : None, Recorded Time : N/A
  Last Signaled Error:
    Code : RSVP System error (23), Value : N/A (0)
    Originated Node : 15.1.1.3, Recorded Time : 2023 May 16 08:52:51
  Trunk Type: mpls
  Total LSP protected : 1, Bandwidth in use : 0
To validate RSVP bypass Protected-lsp-list
R1#   show rsvp bypass protected-lsp-list
Bypass trunk: R1-R5-BPS-001
Bypass trunk bandwidth type: best-effort
List of LSP's Protected:
Tunnel-id     Lsp Id     Lsp Name                  Role     Ext_tnl_id     Ingress
Egress
5001         2201      R1-R5-PRI-001-Primary       Ingress   1.1.1.1       1.1.1.1
5.5.5.5
Total LSP protected : 1
 Bandwidth in use : 0
```

CHAPTER 10 LDP Configuration

This chapter contains LDP (Label Distribution Protocol) configuration examples.

Label Distribution Protocol Overview

The Label Distribution Protocol (LDP) is a routing protocol used in MPLS technology. The LDP daemon (`ldpd`) uses NSM services to obtain routing information. Routers send Hello packets to establish Hello Adjacencies with other nearby routers. This opens the way for sessions between routers to be established during which routers exchange labels in preparation for forwarding packets.

LDP generates labels for and exchanges labels between peer routers. It works in with other routing protocols (RIP, OSPF and BGP) to create label-switched paths (LSP) used when forwarding packets. A label-switched path is the path taken by all packets that belong to the Forwarding Equivalence Class (FEC) corresponding to that LSP. This is analogous to establishing a virtual circuit in ATM (Asynchronous Transfer Mechanism). In this way, OcNOS LDP assigns labels to every destination address and destination prefix provided by OcNOS. The LDP interface to the MPLS forwarder adds labels to, and deletes labels from, the forwarding tables.

LDP Adjacencies

LDP defines a mechanism for discovering adjacent, LDP capable Label Switching Routers (LSR) that participate in label switching (adjacencies). Whenever a new router comes up it sends out a hello packet to a specified, multicast address announcing itself to the network. Every router directly connected to the network receives the packet. Receipt of a hello packet from another LSR creates a *Hello Adjacency* with that LSR. To create a Hello Adjacency with an LSR that cannot send/receive multicast packets, LDP allows a router to be manually configured to send unicast Hello packets to non-multicast LSRs . This non-multicast LSR is a *targeted peer*. Adjacencies are maintained by sending out periodic Hello packets to the multicast group and to all targeted peers. Hello packets are sent using UDP.

LDP Session

LDP capable LSRs establish a session before exchanging label information. All the session messages are sent using TCP to ensure reliable delivery. After the LSRs establish a session and negotiate options, a given pair of routers may exchange label information. The labels exchanged over a session are valid only during the lifetime of the session and routers release them when session is closed.

Forwarding Equivalence Class

A Forwarding Equivalence Class (FEC) section defines a set of packets that are forwarded on the same path by the MPLS network. Two common methods to define FEC are by advertising the IPv4 routes using:

- **Host Address** The LSR uses the address of the destination host to create this FEC. This means that all the packets going to this destination will take the same LSP.
- **Prefix** The LSR uses destination prefix to create this FEC. This means that all the packets take the LSP corresponding to the longest matching prefix.

Label Generation

An LDP Label is a 20-bit number the LSR uses to forward a packet to its destination. When an LSR creates a new FEC, the router generates new labels and distributes them to its peers. A router keeps both incoming and outgoing labels in its database.

Label Distribution Modes

The OcNOS LDP implementation supports two label distribution modes:

- **Downstream Unsolicited** In this mode, next hop LSRs distribute labels to peers without waiting for a label request.
- **Downstream on Demand** In this mode, a LSR distributes a label to a peer only if there is a pending label request from the peer.

Label Retention Mode

The OcNOS LDP implementation supports two label retention modes:

- **Liberal Retention Mode** In this mode, the LSR retains all labels received from all sources. This mode helps in fast LSP setup in case of a change in next hop.
- **Conservative Retention Mode** In this mode, the LSR retains only those labels received from peers that are the next hop for a given FEC. This mode is used by LSRs that have a constraint on the number of labels that it can retain at any given time.

LSP Control

LSPs can be set up in the following two ways:

- **Ordered Control** In this mode, an LSR distributes a label for a FEC to its peer only if it has a corresponding label from its next hop or it is the egress node.
- **Independent Control** In this mode, an LSR may distribute a label to its peers without waiting for a corresponding label from its next hop.

Loop Detection

Loop detection can be enabled to detect routing loops in LSPs. There are two methods supported for the loop detection mechanism:

- **Hop Count** During setup of an LSP, the LSP passes hop count with the LSP setup messages. This hop count is incriminated by each node router participating in LSP establishment. If the hop count exceeds the maximum configured value, the LSP setup process is stopped and a notification message is passed back to the message originator.
- **Path Vector** A path vector contains a list of LSR identifiers. This is passed as a part of LSP setup messages. Each LSR participating in the LSP establishment adds its own LSR identifier to the path vector. If an LSR finds its own identifier in the path vector, it drops the message and sends a message back to the originator.

The use of these messages ensures that a loop is detected while establishing a label switched path and before any data is passed over that LSP.

Configure LDP

The `enable-ldp ipv4` command is used to enable LDP for IPv4, on a specified interface, as follows:

- `enable-ldp ipv4` enables only IPv4 on the interface

For the examples covered in this section, the command `enable-ldp ipv4` is used.

Enable Label Switching

Running LDP on a system requires the following tasks:

1. Enabling label-switching on the interface on NSM.
2. Enabling LDP on an interface in the LDP daemon.
3. Running an IGP (Internal Gateway Protocol), for example, OSPF, to distribute reachability information within the MPLS cloud.
4. Configuring the transport address.

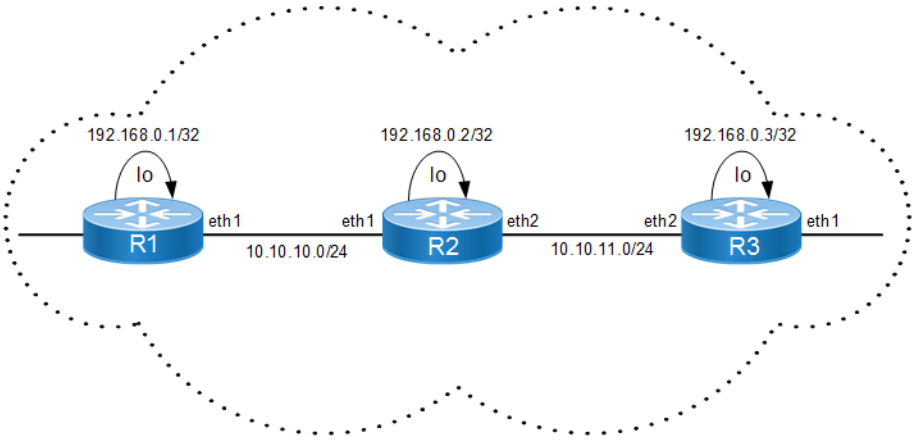


Figure 10-18: Basic LDP Topology

R1

NSM

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Specify the interface `(eth1)` to be configured.
`(config-if)#label-switching`	Enable label switching on interface `eth1`.
`(config-if)#exit`	Exit interface mode.
`(config)#interface lo`	Specify the loopback (`lo`) interface to be configured.
`(config-if)#ip address 192.168.0.1/32`	Set the IP address of the loopback interface to `192.168.0.1/32`.

LDP

`(config)#router ldp`	Enter `Router` mode for LDP.
`(config-router)#router-id 192.168.0.1`	Set the router ID to IP address `192.168.0.1`.
`(config-router)#transport-address ipv4 192.168.0.1`	Configure the transport address to be used for a TCP session over which LDP will run on an IPv4 interface. **Note**: It is preferable to use the loopback address as transport address. In addition, use the parameter “ipv6” if you are configuring an IPv6 interface.
`(config-router)#exit`	Exit the `Router` mode and return to the `Configure` mode.

(config)#interface eth1	Enter interface mode.
(config-if)#enable-ldp ipv4	Enable LDP on eth1.
(config-if)#exit	Exit interface mode.

OSPF

(config)#router ospf 100	Configure the routing process and specify the Process ID (100). The Process ID should be a unique positive integer identifying the routing process.
(config-router)#network 10.10.10.0/24 area 0 (config-router)#network 192.168.0.1/32 area 0	Define the interface on which OSPF runs and associate the area ID (0) with the interface.

R2

NSM

#configure terminal	Enter configure mode.
(config)#interface lo	Specify the loopback (lo) interface to be configured.
(config-if)#ip address 192.168.0.2/32	Set the IP address of the loopback interface to 192.168.0.2/32.
(config-if)#exit	Exit interface mode.
(config)#interface eth1	Specify the interface (eth1) to be configured.
(config-if)#label-switching	Enable label switching on interface eth1.
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Specify the interface (eth2) to be configured.
(config-if)#label-switching	Enable label switching on interface eth2.
(config-if)#exit	Exit interface mode.

LDP

(config)#router ldp	Enter Router mode.
(config-router)#router-id 192.168.0.2	Set the router ID to IP address 192.168.0.2.
(config-router)#transport-address ipv4 192.168.0.2	Configure the transport address to be used for a TCP session over which LDP will run on an IPv4 interface. **Note**: It is preferable to use the loopback address as transport address. In addition, use the parameter “ipv6” if you are configuring an IPv6 interface.
(config-router)#exit	Exit Router mode and return to Configure mode.
(config)#interface eth1	Specify the interface (eth1) to be configured.
(config-if)#enable-ldp ipv4	Enable LDP on a specified interface (eth1).
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Specify the interface (eth2) to be configured.

(config-if)#enable-ldp ipv4	Enable LDP on a specified interface (eth2).
(config-if)#exit	Exit interface mode.

OSPF

(config)#router ospf 100	Configure the routing process and specify the Process ID (100). The Process ID should be a unique positive integer identifying the routing process.
(config-router)#network 10.10.10.0/24 area 0 (config-router)#network 10.10.11.0/24 area 0 (config-router)#network 192.168.0.2/32 area 0	Define the interfaces on which OSPF runs and associate the area ID (0) with them.

R3

NSM

#configure terminal	Enter configure mode.
(config)#interface lo	Specify the loopback (lo) interface to be configured.
(config-if)#ip address 192.168.0.3/32	Set the IP address of the loopback interface to 192.168.0.3/32.
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Specify the interface (eth2) to be configured.
(config-if)#label-switching	Enable label switching on interface eth2.
(config-if)#exit	Exit interface mode.

LDP

(config)#router ldp	Enter Router mode.
(config-router)#router-id 192.168.0.3	Set the router ID for IP address 192.168.0.3.
(config-router)#transport-address ipv4 192.168.0.3	Configure the transport address to be used for a TCP session over which LDP will run on an IPv4 interface. **Note**: It is preferable to use the loopback address as transport address. In addition, use the parameter “ipv6” if you are configuring an IPv6 interface.
(config-router)#exit	Exit the Router mode and return to the Configure mode.
(config)#interface eth2	Enter interface mode.
(config-if)#enable-ldp ipv4	Enable LDP on eth2.
(config-if)#exit	Exit interface mode.

OSPF

`(config)#router ospf 100`	Configure the routing process and specify the Process ID (100). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.11.0/24 area 0` `(config-router)#network 192.168.0.3/32 area 0`	Define the interfaces on which OSPF runs and associate the area ID `(0)` with them.

LDP MD5 Authentication

LDP MD5 configuration enables LDP MD5 password authentication on a per-peer basis.

Direct LDP Session

In this example, MD5 authentication is configured for a direct LDP session.

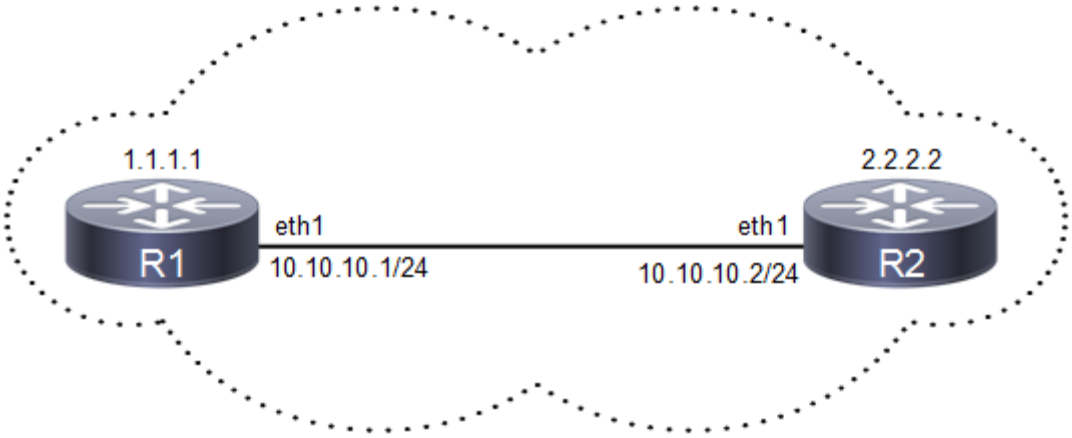


Figure 10-19: Topology for Direct Session MD5

R1

`#configure terminal`	Enter configure mode.
`(config)#router ldp`	Enter `Router` mode.
`(config-router)#neighbor 10.10.10.2 auth md5 password 0 pwd1`	Configure the MD5 authentication and password, `pwd1`, for the neighbor, `10.10.10.2`.
`(config-router)#exit`	Exit the `Router` mode and return to the `Configure` mode.
`(config)#interface eth1`	Specify the interface `(eth1)` to be configured.
`(config-if)#label-switching`	Enable label switching on interface `eth1`.
`(config-if)#enable-ldp ipv4`	Enable LDP on interface `eth1`.
`(config-if)#exit`	Exit interface mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#router ldp`	Enter `Router` mode.
`(config-router)#neighbor 10.10.10.1 auth md5 password 0 pwd1`	Configure the MD5 authentication and password, `pwd1`, for the neighbor, `10.10.10.1`.
`(config-router)#exit`	Exit the `Router` mode and return to the `Configure` mode.
`(config)#interface eth1`	Specify the interface `(eth1)` to be configured.
`(config-if)#label-switching`	Enable label switching on interface `eth1`.
`(config-if)#enable-ldp ipv4`	Enable LDP on interface `eth1`.
`(config-if)#exit`	Exit interface mode.

Configure LDP MD5 for Targeted LDP Session

In this example, MD5 authentication is configured for the targeted LDP session established between R1 and R3.

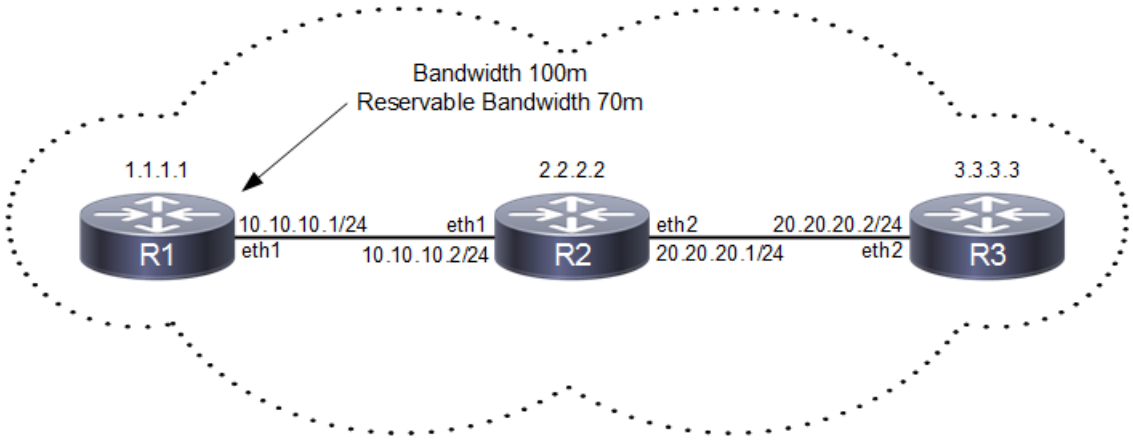


Figure 10-20: Topology for Targeted Session MD5

R1

`#configure terminal`	Enter configure mode.
`(config)#router ldp`	Enter `Router` mode.
`(config-router)#neighbor 10.10.10.2 auth md5 password 0 pwd1`	Configure the MD5 authentication and password, `pwd1`, for the neighbor, `10.10.10.2`.
`(config-router)#targeted-peer ipv4 3.3.3.3`	Configure the targeted peer IP address (R3 loopback address).
(config-router-targeted-peer)#exit	Exit targeted peer mode.
`(config-router)#neighbor 3.3.3.3 auth md5 password 0 pwd2`	Configure the MD5 authentication and password, `pwd2`, for the targeted peer, `3.3.3.3`.
`(config-router)#exit`	Exit the `Router` mode and return to the `Configure` mode.
`(config)#interface eth1`	Specify the interface `(eth1)` to be configured.

(config-if)#label-switching	Enable label switching on interface eth1.
(config-if)#enable-ldp ipv4	Enable LDP on interface eth1.
(config-if)#exit	Exit interface mode.

R2

#configure terminal	Enter configure mode.
(config)#router ldp	Enter Router mode to enable LDP.
(config-router)#exit	Exit the Router mode and return to the Configure mode.
(config)#interface eth1	Specify the interface (eth1) to be configured.
(config-if)#label-switching	Enable label switching on interface eth1.
(config-if)#enable-ldp ipv4	Enable LDP on interface eth1.
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Specify the interface (eth2) to be configured.
(config-if)#label-switching	Enable label switching on interface eth2.
(config-if)#enable-ldp ipv4	Enable LDP on interface eth2.
(config-if)#exit	Exit interface mode.

R3

#configure terminal	Enter configure mode.
(config)#router ldp	Enter Router mode.
(config-router)#targeted-peer ipv4 1.1.1.1	Configure the targeted peer IP address (R1 loopback address).
(config-router-targeted-peer)#exit	Exit targeted peer mode.
(config-router)#neighbor 1.1.1.1 auth md5 password 0 pwd2	Configure the MD5 authentication and password, pwd2, for the targeted peer, 1.1.1.1.
(config-router)#exit	Exit the Router mode and return to the Configure mode.
(config)#interface eth1	Specify the interface (eth1) to be configured.
(config-if)#label-switching	Enable label switching on interface eth1.
(config-if)#enable-ldp ipv4	Enable LDP on interface eth1.
(config-if)#exit	Exit interface mode.

Removing MD5 Authentication for LDP Session

This example shows removing the MD5 authentication configuration from an LDP session.

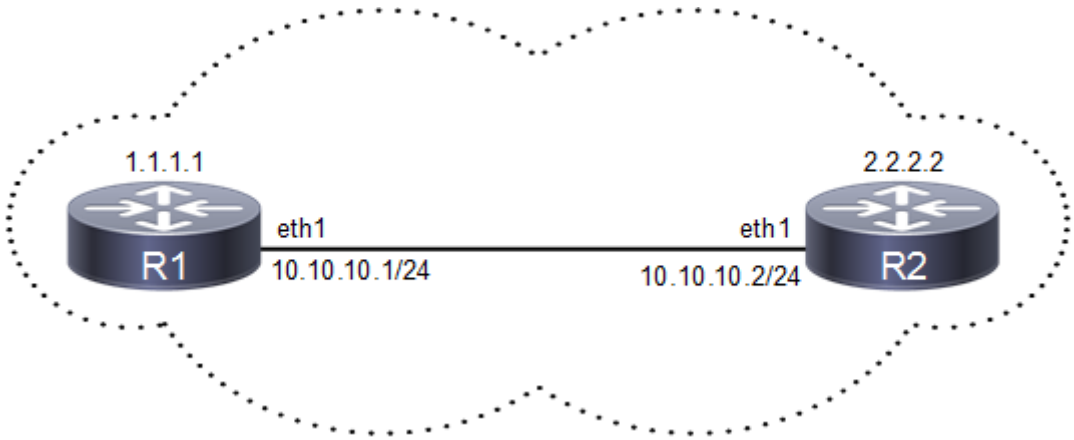


Figure 10-21: LDP Session Topology

R1

`#configure terminal`	Enter configure mode.
`(config)#router ldp`	Enter `Router` mode.
`(config-router)#no neighbor 10.10.10.2 auth md5 password 0`	Remove MD5 authentication for the neighbor, `10.10.10.2`.
`(config-router)#exit`	Exit the `Router` mode and return to the `Configure` mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#router ldp`	Enter `Router` mode.
`(config-router)#no neighbor 10.10.10.1 auth md5 password 0`	Remove MD5 authentication for the neighbor, `10.10.10.1`.
`(config-router)#exit`	Exit the `Router` mode and return to the `Configure` mode.

Validation for LDP Session Count

This example shows the number of configured LDP basic neighbors and targeted neighbors count.

```
 #show ldp session count
 ------------------------------------------
 Multicast Peers      : 1          [UP: 1]
 Targeted Peers       : 1          [UP: 1]
 Total Sessions       : 2          [UP: 2]
------------------------------------------

 #show ldp targeted-peer count
 ------------------------------------------------
 Num Targeted Peers: 500          [UP: 500]
 ------------------------------------------------
```

Validation for FTN, SWAP, and POP Entries

This example shows forwarding table entries, SWAP entries and POP entries for IPV4 and IPV6 prefixes.

```
#show mpls forwarding-table count
-------------------------------------------
Num FTNs            : 3          [UP: 3, INSTALLED: 3]
Primary FTNs        : 3          [UP: 3, INSTALLED: 3]
Secondary FTNs      : 0          [UP: 0, INSTALLED: 0]
-------------------------------------------
-------------------------------------------
Num IPV6 FTNs       : 0          [UP: 0, INSTALLED: 0]
Primary IPV6 FTNs   : 0          [UP: 0, INSTALLED: 0]
Secondary IPV6 FTNs : 0          [UP: 0, INSTALLED: 0]
-------------------------------------------

#show mpls ilm-table count
-------------------------------------------
Num ILMs         : 0          [UP: 0, INSTALL: 0]
  Swap Entries   : 0          [UP: 0, INSTALL: 0]
  Pop Entries    : 0          [UP: 0, INSTALL: 0]
  VC Pop Entries : 0          [UP: 0]
-------------------------------------------
```

MPLS LDP PING and TRACEROUTE

This example shows MPLS ping and trace route for LDP

```
#show ip ospf neighbor
Total number of full neighbors: 1
OSPF process 0 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address
Interface           Instance ID
43.43.43.43       1   Full/DR         00:00:33    21.21.21.43
xe21                  0
RTR-29#show ldp session
Peer IP Address           IF Name    My Role    State      KeepAlive
43.43.43.43               xe21       Passive   OPERATIONAL   30

#show mpls  forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN,
       B - BGP FTN, K - CLI FTN, t - tunnel, P - SR Policy FTN,
       L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, I - IGP-Shortcut,
       U - unknown FTN, O - SR-OSPF FTN, i - SR-ISIS FTN, k - SR-CLI FTN

Code    FEC                FTN-ID    Nhlfe-ID  Tunnel-id   Pri   LSP-Type
Out-Label    Out-Intf    ELC   Nexthop
   L>   13.1.1.1/32         1         1         -           -     LSP_DEFAULT
3            xe13        No    20.20.20.12
   L>   20.1.1.1/32         2         2         -           -     LSP_DEFAULT
24320        xe13        No    20.20.20.12
   L>   20.20.20.10/31      3         1         -           -     LSP_DEFAULT
3            xe13        No    20.20.20.12
```

```
#ping mpls ldp 43.43.43.43/32 detail
Sending 5 MPLS Echos to 43.43.43.43, timeout is 5 seconds

Codes:
'!' - Success, 'Q' - request not sent, '.' - timeout,
'x' - Retcode 0, 'M' - Malformed Request, 'm' - Errored TLV,
'N' - LBL Mapping Err, 'D' - DS Mismatch,
'U' - Unknown Interface, 'R' - Transit (LBL Switched),
'B' - IP Forwarded, 'F' No FEC Found, 'f' - FEC Mismatch,
'P' - Protocol Error, 'X' - Unknown code,
'Z' - Reverse FEC Validation Failed

Type 'Ctrl+C' to abort
! seq_num = 1 43.43.43.43 1.73 ms
! seq_num = 2 43.43.43.43 1.46 ms
! seq_num = 3 43.43.43.43 0.64 ms
! seq_num = 4 43.43.43.43 0.65 ms
! seq_num = 5 43.43.43.43 0.62 ms

Success Rate is 100.00 percent (5/5)
round-trip min/avg/max = 0.62/1.18/1.73

#trace mpls ldp 43.43.43.43/32 detail
Tracing MPLS Label Switched Path to 43.43.43.43, timeout is 5 seconds
Codes:
'!' - Success, 'Q' - request not sent, '.' - timeout,
'x' - Retcode 0, 'M' - Malformed Request, 'm' - Errored TLV,
'N' - LBL Mapping Err, 'D' - DS Mismatch,
'U' - Unknown Interface, 'R' - Transit (LBL Switched),
'B' - IP Forwarded, 'F' No FEC Found, 'f' - FEC Mismatch,
'P' - Protocol Error, 'X' - Unknown code,
'Z' - Reverse FEC Validation Failed
Type 'Ctrl+C' to abort
  0 21.21.21.29 [Labels:  0]
! 1 43.43.43.43 0.69 ms

#ping mpls ldp 43.43.43.43/32 detail interval 5000 rep
reply-mode  repeat
#ping mpls ldp 43.43.43.43/32 detail interval 5000 repeat 50
Sending 50 MPLS Echos to 43.43.43.43, timeout is 5 seconds

Codes:
'!' - Success, 'Q' - request not sent, '.' - timeout,
'x' - Retcode 0, 'M' - Malformed Request, 'm' - Errored TLV,
'N' - LBL Mapping Err, 'D' - DS Mismatch,
'U' - Unknown Interface, 'R' - Transit (LBL Switched),
'B' - IP Forwarded, 'F' No FEC Found, 'f' - FEC Mismatch,
'P' - Protocol Error, 'X' - Unknown code,
'Z' - Reverse FEC Validation Failed

Type 'Ctrl+C' to abort

! seq_num = 1 43.43.43.43 0.70 ms
! seq_num = 2 43.43.43.43 0.73 ms
! seq_num = 3 43.43.43.43 0.71 ms
Success Rate is 100.00 percent (3/3)
round-trip min/avg/max = 0.70/0.71/0.73
```

LDP Session Protection

LDP Session Protection is an optimization feature. It is used when directly connected LDP peer sessions (via multicast) become unavailable but still have IP reachability over a different path. LDP bindings are kept in the LIB to save time from full synchronization when the direct connections comes back up.

There are two types of LDP connections:

- Direct LDP Session - directly connected LSR, one hop away.
- Targeted LDP Session - not directly connected LSR, multiple hops away.

By default if the directly connected LDP session loses connectivity to its peer, all bindings are flushed from the LIB. When interfaces come up and LDP sessions are re-established, LDP has to synchronize its label bindings.

LDP Session Protection is an optimization, when enabled, will not flush the LIB when direct LDP sessions go down. As long as there exists another path to the LDP Peer, it will maintain the LIB synchronized using Targeted LDP Session. IGP will cause a reroute, but the label bindings will still be present from the old peer. When interfaces come back up, LDP will not need to synchronize since it maintains the state using the targeted sessions.

1. Running LDP Session Protection on a system requires the following tasks:
2. Enabling label-switching on the interface on NSM.
3. Enabling LDP on an interface in the LDP daemon.
4. Running an IGP (Internal Gateway Protocol), for example, OSPF, to distribute reachability information within the MPLS cloud.
5. Configuring the transport address.
6. Configuring LDP Session Protection.

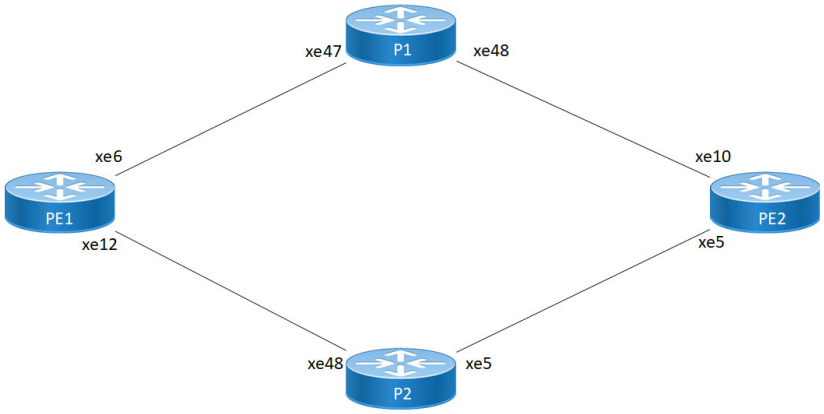


Figure 10-22: Basic LDP Topology

PE1

NSM:

`#configure terminal`	Enter configure mode.
`(config)#interface xe6`	Specify the interface (xe6) to be configured.
`(config-if)#ip address 10.10.10.1/24`	Configure IPv4 address for xe6
`(config-if)#label-switching`	Enable label switching on interface xe6.

(config)#interface xe12	Specify the interface (xe12) to be configured.
(config-if)#ip address 30.30.30.1/24	Configure IPv4 address for xe12
(config-if)#label-switching	Enable label switching on interface xe12.
(config-if)#exit	Exit interface mode.
(config)#interface lo	Specify the loopback (lo) interface to be configured.
(config-if)#ip address 1.1.1.1/32	Set the IP address of the loopback interface to 1.1.1.1/32.
(config-if)#commit	Commit the transaction.

LDP:

(config)#router ldp	Enter Router mode for LDP.
(config-router)#router-id 1.1.1.1	Set the router ID to IP address 1.1.1.1
(config-router)#transport-address ipv4 1.1.1.1	Configure the transport address to be used for a TCP session over which LDP will run on an IPv4 interface. Note: It is preferable to use the loopback address as transport address. In addition, use the parameter "ipv6" if you are configuring an IPv6 interface.
(config-router)#exit	Exit the Router mode and return to the Configure mode.
(config)#interface xe6	Enter interface mode.
(config-if)#enable-ldp ipv4	Enable LDP on xe6.
(config)#interface xe12	Enter interface mode.
(config-if)#enable-ldp ipv4	Enable LDP on xe12.
(config-if)#commit	Commit the transaction.

OSPF:

(config)#router ospf 1	Configure the routing process and specify the Process ID (1). The Process ID should be a unique positive integer identifying the routing process.
(config-router)#ospf router-id 1.1.1.1	Configure Router ID
(config-router)#network 1.1.1.1/32 area 0	Define the interface on which OSPF runs and associate the area ID (0) with the interface.
(config-router)#network 10.10.10.1/24 area 0	Define the interface on which OSPF runs and associate the area ID (0) with the interface.
(config-router)#network 30.30.30.1/24 area 0	Define the interface on which OSPF runs and associate the area ID (0) with the interface.
(config-router)#commit	Commit the transaction.

P1

NSM:

#configure terminal	Enter configure mode.
(config)#interface xe47	Specify the interface (xe47) to be configured.
(config-if)#ip address 10.10.10.2/24	Configure IPv4 address for xe47
(config-if)#label-switching	Enable label switching on interface xe47.

(config)#interface xe48	Specify the interface (xe48) to be configured.
(config-if)#ip address 20.20.20.1/24	Configure IPv4 address for xe48
(config-if)#label-switching	Enable label switching on interface xe48.
(config-if)#exit	Exit interface mode.
(config)#interface lo	Specify the loopback (lo) interface to be configured.
(config-if)#ip address 2.2.2.2/32	Set the IP address of the loopback interface to 2.2.2.2/32.
(config-if)#commit	Commit the transaction.

LDP:

(config)#router ldp	Enter Router mode for LDP.
(config-router)#router-id 2.2.2.2	Set the router ID to IP address 2.2.2.2
(config-router)#transport-address ipv4 2.2.2.2	Configure the transport address to be used for a TCP session over which LDP will run on an IPv4 interface. Note: It is preferable to use the loopback address as transport address. In addition, use the parameter "ipv6" if you are configuring an IPv6 interface.
(config-router)#exit	Exit the Router mode and return to the Configure mode.
(config)#interface xe47	Enter interface mode.
(config-if)#enable-ldp ipv4	Enable LDP on xe47.
(config)#interface xe48	Enter interface mode.
(config-if)#enable-ldp ipv4	Enable LDP on xe48.
(config-if)#commit	Commit the transaction.

OSPF:

(config)#router ospf 1	Configure the routing process and specify the Process ID (1). The Process ID should be a unique positive integer identifying the routing process.
(config-router)#ospf router-id 2.2.2.2	Configure Router ID
(config-router)#network 2.2.2.2/32 area 0	Define the interface on which OSPF runs and associate the area ID (0) with the interface.
(config-router)#network 10.10.10.2/24 area 0	Define the interface on which OSPF runs and associate the area ID (0) with the interface.
(config-router)#network 20.20.20.1/24 area 0	Define the interface on which OSPF runs and associate the area ID (0) with the interface.
(config-router)#commit	Commit the transaction.

P2

NSM:

#configure terminal	Enter configure mode.
(config)#interface xe48	Specify the interface (xe48) to be configured.
(config-if)#ip address 30.30.30.2/24	Configure IPv4 address for xe48

(config-if)#label-switching	Enable label switching on interface xe48.
(config)#interface xe5	Specify the interface (xe5) to be configured.
(config-if)#ip address 40.40.40.1/24	Configure IPv4 address for xe5
(config-if)#label-switching	Enable label switching on interface xe5.
(config-if)#exit	Exit interface mode.
(config)#interface lo	Specify the loopback (lo) interface to be configured.
(config-if)#ip address 4.4.4.4/32	Set the IP address of the loopback interface to 4.4.4.4/32.
(config-if)#commit	Commit the transaction.

LDP:

(config)#router ldp	Enter Router mode for LDP.
(config-router)#router-id 4.4.4.4	Set the router ID to IP address 4.4.4.4
(config-router)#transport-address ipv4 4.4.4.4	Configure the transport address to be used for a TCP session over which LDP will run on an IPv4 interface. Note: It is preferable to use the loopback address as transport address. In addition, use the parameter "ipv6" if you are configuring an IPv6 interface.
(config-router)#exit	Exit the Router mode and return to the Configure mode.
(config)#interface xe48	Enter interface mode.
(config-if)#enable-ldp ipv4	Enable LDP on xe48.
(config)#interface xe5	Enter interface mode.
(config-if)#enable-ldp ipv4	Enable LDP on xe5.
(config-if)#commit	Commit the transaction.

OSPF:

(config)#router ospf 1	Configure the routing process and specify the Process ID (1). The Process ID should be a unique positive integer identifying the routing process.
(config-router)#ospf router-id 4.4.4.4	Configure Router ID
(config-router)#network 4.4.4.4/32 area 0	Define the interface on which OSPF runs and associate the area ID (0) with the interface.
(config-router)#network 20.20.20.2/24 area 0	Define the interface on which OSPF runs and associate the area ID (0) with the interface.
(config-router)#network 30.30.30.1/24 area 0	Define the interface on which OSPF runs and associate the area ID (0) with the interface.
(config-router)#commit	Commit the transaction.

PE2

NSM:

#configure terminal	Enter configure mode.
(config)#interface xe10	Specify the interface (xe10) to be configured.

`(config-if)#ip address 20.20.20.2/24`	Configure IPv4 address for xe10
`(config-if)#label-switching`	Enable label switching on interface xe10.
`(config)#interface xe5`	Specify the interface (xe5) to be configured.
`(config-if)#ip address 40.40.40.2/24`	Configure IPv4 address for xe5
`(config-if)#label-switching`	Enable label switching on interface xe5.
`(config-if)#exit`	Exit interface mode.
`(config)#interface lo`	Specify the loopback (lo) interface to be configured.
`(config-if)#ip address 3.3.3.3/32`	Set the IP address of the loopback interface to 3.3.3.3/32.
`(config-if)#commit`	Commit the transaction.

LDP:

`(config)#router ldp`	Enter Router mode for LDP.
`(config-router)#router-id 3.3.3.3`	Set the router ID to IP address 3.3.3.3
`(config-router)#transport-address ipv4 3.3.3.3`	Configure the transport address to be used for a TCP session over which LDP will run on an IPv4 interface. Note: It is preferable to use the loopback address as transport address. In addition, use the parameter "ipv6" if you are configuring an IPv6 interface.
`(config-router)#exit`	Exit the Router mode and return to the Configure mode.
`(config)#interface xe10`	Enter interface mode.
`(config-if)#enable-ldp ipv4`	Enable LDP on xe10.
`(config)#interface xe5`	Enter interface mode.
`(config-if)#enable-ldp ipv4`	Enable LDP on xe5.
`(config-if)#commit`	Commit the transaction.

OSPF:

`(config)#router ospf 1`	Configure the routing process and specify the Process ID (1). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#ospf router-id 3.3.3.3`	Configure Router ID
`(config-router)#network 3.3.3.3/32 area 0`	Define the interface on which OSPF runs and associate the area ID (0) with the interface.
`(config-router)#network 20.20.20.2/24 area 0`	Define the interface on which OSPF runs and associate the area ID (0) with the interface.
`(config-router)#network 40.40.40.2/24 area 0`	Define the interface on which OSPF runs and associate the area ID (0) with the interface.
`(config-router)#commit`	Commit the transaction.

Validation

Without session protection Enabled

Verify that session protection status is not shown when session protection not enabled.

```
PE1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
C            1.1.1.1/32 is directly connected, lo, 00:04:22
O            2.2.2.2/32 [110/2] via 10.10.10.2, xe12, 00:03:03
O            3.3.3.3/32 [110/3] via 10.10.10.2, xe12, 00:02:49
O            4.4.4.4/32 [110/31] via 30.30.30.2, xe6, 00:02:17
C            10.10.10.0/24 is directly connected, xe12, 00:03:48
O            20.20.20.0/24 [110/2] via 10.10.10.2, xe12, 00:03:03
C            30.30.30.0/24 is directly connected, xe6, 00:03:02
O            40.40.40.0/24 [110/31] via 30.30.30.2, xe6, 00:02:17
C            127.0.0.0/8 is directly connected, lo, 00:04:22

Gateway of last resort is not set

PE1#show ldp session
Peer IP Address           IF Name    My Role    State      KeepAlive  UpTime
4.4.4.4                   xe6        Passive   OPERATIONAL   30    00:02:25
2.2.2.2                   xe12       Passive   OPERATIONAL   30    00:03:11
PE1#show ldp targeted-peers
PE1#show ldp session 2.2.2.2
Session state         : OPERATIONAL
Session role          : Passive
TCP Connection        : Established
IP Address for TCP    : 2.2.2.2
Interface being used  : xe12
Peer LDP ID           : 2.2.2.2:0
Peer LDP Password     : Not Set
Adjacencies           : 10.10.10.2
Advertisement mode    : Downstream Unsolicited
Label retention mode  : Liberal
Graceful Restart      : Not Capable
Keepalive Timeout     : 30
Reconnect Interval    : 15
Address List received : 2.2.2.2
                        10.10.10.2
                        20.20.20.1
                        254.128.0.0
Received Labels :       Fec             Label           Maps To
                IPV4:3.3.3.3/32         52480           24963
                IPV4:20.20.20.0/24      impl-null       24964
                IPV4:10.10.10.0/24      impl-null       none
```

```
                IPV4:2.2.2.2/32         impl-null       24962
Sent Labels :   Fec                     Label           Maps To
                IPV4:40.40.40.0/24      24961           impl-null
                IPV4:4.4.4.4/32         24960           impl-null
                IPV4:30.30.30.0/24      impl-null       none
                IPV4:10.10.10.0/24      impl-null       none
                IPV4:1.1.1.1/32         impl-null       none
PE1#show mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN,
       B - BGP FTN, K - CLI FTN, t - tunnel, P - SR Policy FTN,
       L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, I - IGP-Shortcut,
       U - unknown FTN, O - SR-OSPF FTN, i - SR-ISIS FTN, k - SR-CLI FTN
(m) - FTN mapped over multipath transport

Code    FEC               FTN-ID    Nhlfe-ID  Tunnel-id   Pri   LSP-Type     Out-Label
Out-Intf    ELC   Nexthop
   L>   2.2.2.2/32          1         2         -           Yes   LSP_DEFAULT  3
xe12        No    10.10.10.2
   L>   3.3.3.3/32          3         5         -           Yes   LSP_DEFAULT  52480
xe12        No    10.10.10.2
   L>   4.4.4.4/32          4         7         -           Yes   LSP_DEFAULT  3
xe6         No    30.30.30.2
   L>   20.20.20.0/24       2         3         -           Yes   LSP_DEFAULT  3
xe12        No    10.10.10.2
   L>   40.40.40.0/24       5         8         -           Yes   LSP_DEFAULT  3
xe6         No    30.30.30.2

PE1#show mpls ftn-table
 Primary FTN entry with FEC: 2.2.2.2/32, id: 1, row status: Active, Tunnel-Policy: N/A
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
     Cross connect ix: 1, in intf: - in label: 0 out-segment ix: 1
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 1, owner: N/A, Stale: NO, out intf: xe12, out label: 3
    Nexthop addr: 10.10.10.2        cross connect ix: 1, op code: Push


 Primary FTN entry with FEC: 3.3.3.3/32, id: 3, row status: Active, Tunnel-Policy: N/A
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
     Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 4
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 4, owner: LDP, Stale: NO, out intf: xe12, out label: 52480
    Nexthop addr: 10.10.10.2        cross connect ix: 2, op code: Push


 Primary FTN entry with FEC: 4.4.4.4/32, id: 4, row status: Active, Tunnel-Policy: N/A
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
```

```
     Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 6
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 6, owner: N/A, Stale: NO, out intf: xe6, out label: 3
    Nexthop addr: 30.30.30.2        cross connect ix: 4, op code: Push


 Primary FTN entry with FEC: 20.20.20.0/24, id: 2, row status: Active, Tunnel-Policy: N/
A
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
     Cross connect ix: 1, in intf: - in label: 0 out-segment ix: 1
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 1, owner: N/A, Stale: NO, out intf: xe12, out label: 3
    Nexthop addr: 10.10.10.2        cross connect ix: 1, op code: Push


 Primary FTN entry with FEC: 40.40.40.0/24, id: 5, row status: Active, Tunnel-Policy: N/
A
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
     Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 6
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 6, owner: N/A, Stale: NO, out intf: xe6, out label: 3
    Nexthop addr: 30.30.30.2        cross connect ix: 4, op code: Push


PE1#show mpls ilm-table
Codes: > - installed ILM, * - selected ILM, p - stale ILM
        K - CLI ILM, T - MPLS-TP, s - Stitched ILM
       S - SNMP, L - LDP, R - RSVP, C - CRLDP
       B - BGP , K - CLI , V - LDP_VC, I - IGP_SHORTCUT
       O - OSPF/OSPF6 SR, i - ISIS SR, k - SR CLI
       P - SR Policy, U - unknown

Code    FEC/VRF/L2CKT    ILM-ID     In-Label    Out-Label   In-Intf    Out-Intf/VRF
Nexthop                    LSP-Type
   L>   3.3.3.3/32         4          24963       52480       N/A        xe12
10.10.10.2                 LSP_DEFAULT
   L>   40.40.40.0/24      2          24961       3           N/A        xe6
30.30.30.2                 LSP_DEFAULT
   L>   4.4.4.4/32         1          24960       3           N/A        xe6
30.30.30.2                 LSP_DEFAULT
   L>   2.2.2.2/32         3          24962       3           N/A        xe12
10.10.10.2                 LSP_DEFAULT
   L>   20.20.20.0/24      5          24964       3           N/A        xe12
10.10.10.2                 LSP_DEFAULT

PE1#show ldp fec
LSR codes    : E/N - LSR is egress/non-egress for this FEC,
               L - LSR received a label for this FEC,
               > - LSR will use this route for the FEC
```

```
FEC                 Code    Session             Out Label   ELC   Nexthop Addr
1.1.1.1/32          E >     non-existent        none        No    connected
2.2.2.2/32          NL>     2.2.2.2             impl-null   No    10.10.10.2
3.3.3.3/32          NL      4.4.4.4             24325       No    no nexthop
                    NL>     2.2.2.2             52480       No    10.10.10.2
4.4.4.4/32          NL>     4.4.4.4             impl-null   No    30.30.30.2
10.10.10.0/24       NL      2.2.2.2             impl-null   No    connected
                    E >     non-existent        none        No    connected
20.20.20.0/24       NL      4.4.4.4             24326       No    no nexthop
                    NL>     2.2.2.2             impl-null   No    10.10.10.2
30.30.30.0/24       NL      4.4.4.4             impl-null   No    connected
                    E >     non-existent        none        No    connected
40.40.40.0/24       NL>     4.4.4.4             impl-null   No    30.30.30.2
```

Configure Session Protection:

Note: Recommended to configure both ends.

Configure session protection under LDP in both nodes.

PE1

`(config)#router ldp`	Enter Router mode for LDP.
`(config-router)# session-protection`	Session-protection protect label indefinitely if no timer mentioned.
`(config-router)# commit`	Commit and exit

P1

`(config)#router ldp`	Enter Router mode for LDP.
`(config-router)# session-protection`	Session-protection protect label indefinitely if no timer mentioned.
`(config-router)# commit`	Commit and exit

Validation

After session protection command Enabled

Verify that session protection status shown once session protection enabled in both peer nodes.

```
PE1#show ldp session
Peer IP Address           IF Name    My Role    State      KeepAlive  UpTime
4.4.4.4                   xe6        Passive   OPERATIONAL   30    00:05:46
2.2.2.2                   xe12       Passive   OPERATIONAL   30    00:06:32
PE1#show ldp targeted-peers
IP Address          Interface
2.2.2.2             xe12
4.4.4.4             xe6
PE1#show ldp session 2.2.2.2
```

```
Session state         : OPERATIONAL
Session role          : Passive
TCP Connection        : Established
IP Address for TCP    : 2.2.2.2
Interface being used  : xe12
Peer LDP ID           : 2.2.2.2:0
Peer LDP Password     : Not Set
Adjacencies           : 10.10.10.2
                        2.2.2.2
Advertisement mode    : Downstream Unsolicited
Label retention mode  : Liberal
Graceful Restart      : Not Capable
Keepalive Timeout     : 30
Reconnect Interval    : 15
Session protection    : Ready
Address List received : 2.2.2.2
                        10.10.10.2
                        20.20.20.1
                        254.128.0.0
Received Labels :       Fec             Label           Maps To
                IPV4:3.3.3.3/32         52480           24963
                IPV4:20.20.20.0/24      impl-null       24964
                IPV4:10.10.10.0/24      impl-null       none
                IPV4:2.2.2.2/32         impl-null       24962
Sent Labels :   Fec                     Label           Maps To
                IPV4:40.40.40.0/24      24961           impl-null
                IPV4:4.4.4.4/32         24960           impl-null
                IPV4:30.30.30.0/24      impl-null       none
                IPV4:10.10.10.0/24      impl-null       none
                IPV4:1.1.1.1/32         impl-null       none
PE1#show mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN,
       B - BGP FTN, K - CLI FTN, t - tunnel, P - SR Policy FTN,
       L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, I - IGP-Shortcut,
       U - unknown FTN, O - SR-OSPF FTN, i - SR-ISIS FTN, k - SR-CLI FTN
(m) - FTN mapped over multipath transport

Code    FEC               FTN-ID    Nhlfe-ID  Tunnel-id   Pri   LSP-Type     Out-Label
Out-Intf    ELC   Nexthop
   L>   2.2.2.2/32         1         2         -           Yes   LSP_DEFAULT  3
xe12        No    10.10.10.2
   L>   3.3.3.3/32         3         5         -           Yes   LSP_DEFAULT  52480
xe12        No    10.10.10.2
   L>   4.4.4.4/32         4         7         -           Yes   LSP_DEFAULT  3
xe6         No    30.30.30.2
   L>   20.20.20.0/24       2         3         -           Yes   LSP_DEFAULT  3
xe12        No    10.10.10.2
   L>   40.40.40.0/24       5         8         -           Yes   LSP_DEFAULT  3
xe6         No    30.30.30.2
PE1#show mpls ilm-table
Codes: > - installed ILM, * - selected ILM, p - stale ILM
        K - CLI ILM, T - MPLS-TP, s - Stitched ILM
```

```
       S - SNMP, L - LDP, R - RSVP, C - CRLDP
       B - BGP , K - CLI , V - LDP_VC, I - IGP_SHORTCUT
       O - OSPF/OSPF6 SR, i - ISIS SR, k - SR CLI
       P - SR Policy, U - unknown

Code    FEC/VRF/L2CKT    ILM-ID     In-Label    Out-Label   In-Intf    Out-Intf/VRF
Nexthop                    LSP-Type
   L>   3.3.3.3/32         4          24963       52480       N/A        xe12
10.10.10.2                 LSP_DEFAULT
   L>   40.40.40.0/24      2          24961       3           N/A        xe6
30.30.30.2                 LSP_DEFAULT
   L>   4.4.4.4/32         1          24960       3           N/A        xe6
30.30.30.2                 LSP_DEFAULT
   L>   2.2.2.2/32         3          24962       3           N/A        xe12
10.10.10.2                 LSP_DEFAULT
   L>   20.20.20.0/24      5          24964       3           N/A        xe12
10.10.10.2                 LSP_DEFAULT
PE1#show mpls ftn-table
 Primary FTN entry with FEC: 2.2.2.2/32, id: 1, row status: Active, Tunnel-Policy: N/A
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
     Cross connect ix: 1, in intf: - in label: 0 out-segment ix: 1
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 1, owner: N/A, Stale: NO, out intf: xe12, out label: 3
    Nexthop addr: 10.10.10.2        cross connect ix: 1, op code: Push


 Primary FTN entry with FEC: 3.3.3.3/32, id: 3, row status: Active, Tunnel-Policy: N/A
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
     Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 4
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 4, owner: LDP, Stale: NO, out intf: xe12, out label: 52480
    Nexthop addr: 10.10.10.2        cross connect ix: 2, op code: Push


 Primary FTN entry with FEC: 4.4.4.4/32, id: 4, row status: Active, Tunnel-Policy: N/A
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
     Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 6
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 6, owner: N/A, Stale: NO, out intf: xe6, out label: 3
    Nexthop addr: 30.30.30.2        cross connect ix: 4, op code: Push


 Primary FTN entry with FEC: 20.20.20.0/24, id: 2, row status: Active, Tunnel-Policy: N/
A
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
```



```
     Cross connect ix: 1, in intf: - in label: 0 out-segment ix: 1
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 1, owner: N/A, Stale: NO, out intf: xe12, out label: 3
    Nexthop addr: 10.10.10.2        cross connect ix: 1, op code: Push


 Primary FTN entry with FEC: 40.40.40.0/24, id: 5, row status: Active, Tunnel-Policy: N/
A
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
     Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 6
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 6, owner: N/A, Stale: NO, out intf: xe6, out label: 3
    Nexthop addr: 30.30.30.2        cross connect ix: 4, op code: Push


PE1#show ldp fec
LSR codes    : E/N - LSR is egress/non-egress for this FEC,
               L - LSR received a label for this FEC,
               > - LSR will use this route for the FEC
FEC                 Code    Session             Out Label   ELC   Nexthop Addr
1.1.1.1/32          E >     non-existent        none        No    connected
2.2.2.2/32          NL>     2.2.2.2             impl-null   No    10.10.10.2
3.3.3.3/32          NL      4.4.4.4             24325       No    no nexthop
                    NL>     2.2.2.2             52480       No    10.10.10.2
4.4.4.4/32          NL>     4.4.4.4             impl-null   No    30.30.30.2
10.10.10.0/24       NL      2.2.2.2             impl-null   No    connected
                    E >     non-existent        none        No    connected
20.20.20.0/24       NL      4.4.4.4             24326       No    no nexthop
                    NL>     2.2.2.2             impl-null   No    10.10.10.2
30.30.30.0/24       NL      4.4.4.4             impl-null   No    connected
                    E >     non-existent        none        No    connected
40.40.40.0/24       NL>     4.4.4.4             impl-null   No    30.30.30.2


P1#show ldp session
Peer IP Address           IF Name    My Role    State      KeepAlive  UpTime
3.3.3.3                   xe5        Passive   OPERATIONAL   30    00:05:40
1.1.1.1                   xe48       Active    OPERATIONAL   30    00:06:43
P1#show ldp targeted-peers
IP Address          Interface
1.1.1.1             xe48
3.3.3.3             xe5

P1#show ldp session 1.1.1.1
Session state         : OPERATIONAL
Session role          : Active
TCP Connection        : Established
IP Address for TCP    : 1.1.1.1
Interface being used  : xe48
```

```
Peer LDP ID           : 1.1.1.1:0
Peer LDP Password     : Not Set
Adjacencies           : 10.10.10.1
                        1.1.1.1
Advertisement mode    : Downstream Unsolicited
Label retention mode  : Liberal
Graceful Restart      : Not Capable
Keepalive Timeout     : 30
Reconnect Interval    : 15
Session protection    : Ready
Address List received : 1.1.1.1
                        10.10.10.1
                        30.30.30.1
                        254.128.0.0
Received Labels :       Fec             Label           Maps To
                IPV4:4.4.4.4/32         24960           52482
                IPV4:40.40.40.0/24      24961           52484
                IPV4:30.30.30.0/24      impl-null       52483
                IPV4:10.10.10.0/24      impl-null       none
                IPV4:1.1.1.1/32         impl-null       52481
Sent Labels :   Fec                     Label           Maps To
                IPV4:3.3.3.3/32         52480           impl-null
                IPV4:20.20.20.0/24      impl-null       none
                IPV4:10.10.10.0/24      impl-null       none
                IPV4:2.2.2.2/32         impl-null       none

P1#show mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN,
       B - BGP FTN, K - CLI FTN, t - tunnel,
       L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, I - IGP-Shortcut,
       U - unknown FTN

Code    FEC               FTN-ID    Nhlfe-ID  Tunnel-id   Pri   LSP-Type     Out-Label
Out-Intf    ELC   Nexthop
   L>   1.1.1.1/32          1         2         -          Yes   LSP_DEFAULT  3
xe48        No    10.10.10.1
   L>   3.3.3.3/32          5         9         -          Yes   LSP_DEFAULT  3
xe5         No    20.20.20.2
   L>   4.4.4.4/32          3         5         -          Yes   LSP_DEFAULT  24960
xe48        No    10.10.10.1
   L>   30.30.30.0/24       2         3         -          Yes   LSP_DEFAULT  3
xe48        No    10.10.10.1
   L>   40.40.40.0/24       4         7         -          Yes   LSP_DEFAULT  24961
xe48        No    10.10.10.1


P1#show mpls ilm-table
Codes: > - installed ILM, * - selected ILM, p - stale ILM
        K - CLI ILM, T - MPLS-TP, s - Stitched ILM
       S - SNMP, L - LDP, R - RSVP, C - CRLDP
       B - BGP , K - CLI , V - LDP_VC, I - IGP_SHORTCUT
       U - unknown
```

```
Code    FEC/VRF/L2CKT    ILM-ID      In-Label    Out-Label   In-Intf    Out-Intf/VRF
Nexthop                    LSP-Type
   L>   30.30.30.0/24      4           52483       3           N/A        xe48
10.10.10.1                 LSP_DEFAULT
   L>   1.1.1.1/32         2           52481       3           N/A        xe48
10.10.10.1                 LSP_DEFAULT
   L>   3.3.3.3/32         1           52480       3           N/A        xe5
20.20.20.2                 LSP_DEFAULT
   L>   4.4.4.4/32         3           52482       24960       N/A        xe48
10.10.10.1                 LSP_DEFAULT
   L>   40.40.40.0/24      5           52484       24961       N/A        xe48
10.10.10.1                 LSP_DEFAULT
P1#show mpls ftn-table
 Primary FTN entry with FEC: 1.1.1.1/32, id: 1, row status: Active
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A
     Cross connect ix: 1, in intf: - in label: 0 out-segment ix: 1
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 1, owner: N/A, Stale: NO, out intf: xe48, out label: 3
    Nexthop addr: 10.10.10.1        cross connect ix: 1, op code: Push


 Primary FTN entry with FEC: 3.3.3.3/32, id: 5, row status: Active
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A
     Cross connect ix: 5, in intf: - in label: 0 out-segment ix: 8
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 8, owner: N/A, Stale: NO, out intf: xe5, out label: 3
    Nexthop addr: 20.20.20.2        cross connect ix: 5, op code: Push


 Primary FTN entry with FEC: 4.4.4.4/32, id: 3, row status: Active
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A
     Cross connect ix: 3, in intf: - in label: 0 out-segment ix: 4
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 4, owner: LDP, Stale: NO, out intf: xe48, out label: 24960
    Nexthop addr: 10.10.10.1        cross connect ix: 3, op code: Push


 Primary FTN entry with FEC: 30.30.30.0/24, id: 2, row status: Active
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A
     Cross connect ix: 1, in intf: - in label: 0 out-segment ix: 1
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 1, owner: N/A, Stale: NO, out intf: xe48, out label: 3
    Nexthop addr: 10.10.10.1        cross connect ix: 1, op code: Push
```

```
 Primary FTN entry with FEC: 40.40.40.0/24, id: 4, row status: Active
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A
     Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 6
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 6, owner: LDP, Stale: NO, out intf: xe48, out label: 24961
    Nexthop addr: 10.10.10.1        cross connect ix: 4, op code: Push


P1#show ldp fec
LSR codes    : E/N - LSR is egress/non-egress for this FEC,
               L - LSR received a label for this FEC,
               > - LSR will use this route for the FEC
FEC                 Code    Session             Out Label   ELC   Nexthop Addr
1.1.1.1/32          NL>     1.1.1.1             impl-null   No    10.10.10.1
2.2.2.2/32          E >     non-existent        none        No    connected
3.3.3.3/32          NL>     3.3.3.3             impl-null   No    20.20.20.2
4.4.4.4/32          NL>     1.1.1.1             24960       No    10.10.10.1
10.10.10.0/24       NL      1.1.1.1             impl-null   No    connected
                    E >     non-existent        none        No    connected
20.20.20.0/24       NL      3.3.3.3             impl-null   No    connected
                    E >     non-existent        none        No    connected
30.30.30.0/24       NL>     1.1.1.1             impl-null   No    10.10.10.1
40.40.40.0/24       NL      3.3.3.3             impl-null   No    no nexthop
                    NL>     1.1.1.1             24961       No    10.10.10.1
```

Perform Link failure and check labels are retained until peer is reachable through alternate path.

`(config)#interface xe12`	Enter interface mode.
`(config-if)#shutdown`	Shutdown the link.
`(config)#commit`	commit.

Validation

After link down

```
PE1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
```

```
C            1.1.1.1/32 is directly connected, lo, 00:14:17
O            2.2.2.2/32 [110/33] via 30.30.30.2, xe6, 00:03:38
O            3.3.3.3/32 [110/32] via 30.30.30.2, xe6, 00:03:38
O            4.4.4.4/32 [110/31] via 30.30.30.2, xe6, 00:12:12
O            20.20.20.0/24 [110/32] via 30.30.30.2, xe6, 00:03:38
C            30.30.30.0/24 is directly connected, xe6, 00:12:57
O            40.40.40.0/24 [110/31] via 30.30.30.2, xe6, 00:12:12
    C           127.0.0.0/8 is directly connected, lo, 00:14:17
PE1#show ldp session
Peer IP Address           IF Name    My Role    State      KeepAlive  UpTime
4.4.4.4                   xe6        Passive   OPERATIONAL   30    00:10:10
2.2.2.2                   xe6        Passive   OPERATIONAL   30    00:10:56
PE1#show ldp targeted-peers
IP Address          Interface
2.2.2.2             xe6
4.4.4.4             xe6/
PE1#show ldp session 2.2.2.2
Session state         : OPERATIONAL
Session role          : Passive
TCP Connection        : Established
IP Address for TCP    : 2.2.2.2
Interface being used  : xe6
Peer LDP ID           : 2.2.2.2:0
Peer LDP Password     : Not Set
Adjacencies           : 2.2.2.2
Advertisement mode    : Downstream Unsolicited
Label retention mode  : Liberal
Graceful Restart      : Not Capable
Keepalive Timeout     : 30
Reconnect Interval    : 15
Session protection    : Protecting
Address List received : 2.2.2.2
                        20.20.20.1
                        254.128.0.0
Received Labels :       Fec             Label           Maps To
                IPV4:3.3.3.3/32         52480           none
                IPV4:20.20.20.0/24      impl-null       none
                IPV4:10.10.10.0/24      impl-null       none
                IPV4:2.2.2.2/32         impl-null       none
Sent Labels :   Fec                     Label           Maps To
                IPV4:40.40.40.0/24      24961           impl-null
                IPV4:4.4.4.4/32         24960           impl-null
                IPV4:30.30.30.0/24      impl-null       none
                IPV4:10.10.10.0/24      impl-null       none
                    IPV4:1.1.1.1/32         impl-null       none

PE1#show mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN,
       B - BGP FTN, K - CLI FTN, t - tunnel, P - SR Policy FTN,
       L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, I - IGP-Shortcut,
```

```
       U - unknown FTN, O - SR-OSPF FTN, i - SR-ISIS FTN, k - SR-CLI FTN
(m) - FTN mapped over multipath transport

Code    FEC               FTN-ID    Nhlfe-ID  Tunnel-id   Pri   LSP-Type     Out-Label
Out-Intf    ELC   Nexthop
   L>   2.2.2.2/32         3         9         -           Yes   LSP_DEFAULT  24321
xe6         No    30.30.30.2
   L>   3.3.3.3/32         1         2         -           Yes   LSP_DEFAULT  24325
xe6         No    30.30.30.2
   L>   4.4.4.4/32         4         7         -           Yes   LSP_DEFAULT  3
xe6         No    30.30.30.2
   L>   20.20.20.0/24       2         4         -           Yes   LSP_DEFAULT  24326
xe6         No    30.30.30.2
   L>   40.40.40.0/24       5         8         -           Yes   LSP_DEFAULT  3
xe6         No    30.30.30.2

PE1#show mpls ftn-table
 Primary FTN entry with FEC: 2.2.2.2/32, id: 3, row status: Active, Tunnel-Policy: N/A
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
     Cross connect ix: 3, in intf: - in label: 0 out-segment ix: 5
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 5, owner: LDP, Stale: NO, out intf: xe6, out label: 24321
    Nexthop addr: 30.30.30.2        cross connect ix: 3, op code: Push


 Primary FTN entry with FEC: 3.3.3.3/32, id: 1, row status: Active, Tunnel-Policy: N/A
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
     Cross connect ix: 1, in intf: - in label: 0 out-segment ix: 1
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 1, owner: LDP, Stale: NO, out intf: xe6, out label: 24325
    Nexthop addr: 30.30.30.2        cross connect ix: 1, op code: Push


 Primary FTN entry with FEC: 4.4.4.4/32, id: 4, row status: Active, Tunnel-Policy: N/A
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
     Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 6
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 6, owner: N/A, Stale: NO, out intf: xe6, out label: 3
    Nexthop addr: 30.30.30.2        cross connect ix: 4, op code: Push


 Primary FTN entry with FEC: 20.20.20.0/24, id: 2, row status: Active, Tunnel-Policy: N/
A
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
     Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 3
```

```
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 3, owner: LDP, Stale: NO, out intf: xe6, out label: 24326
    Nexthop addr: 30.30.30.2        cross connect ix: 2, op code: Push


 Primary FTN entry with FEC: 40.40.40.0/24, id: 5, row status: Active, Tunnel-Policy: N/
A
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
     Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 6
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 6, owner: N/A, Stale: NO, out intf: xe6, out label: 3
    Nexthop addr: 30.30.30.2        cross connect ix: 4, op code: Push


PE1#show mpls ilm-table
Codes: > - installed ILM, * - selected ILM, p - stale ILM
        K - CLI ILM, T - MPLS-TP, s - Stitched ILM
       S - SNMP, L - LDP, R - RSVP, C - CRLDP
       B - BGP , K - CLI , V - LDP_VC, I - IGP_SHORTCUT
       O - OSPF/OSPF6 SR, i - ISIS SR, k - SR CLI
       P - SR Policy, U - unknown

Code    FEC/VRF/L2CKT    ILM-ID     In-Label    Out-Label   In-Intf    Out-Intf/VRF
Nexthop                    LSP-Type
   L>   40.40.40.0/24      2          24961       3           N/A        xe6
30.30.30.2                 LSP_DEFAULT
   L>   4.4.4.4/32         1          24960       3           N/A        xe6
30.30.30.2                 LSP_DEFAULT

P1#show ldp session
Peer IP Address           IF Name    My Role    State      KeepAlive  UpTime
3.3.3.3                   xe5        Passive   OPERATIONAL   30    00:11:12
1.1.1.1                   xe5        Active    OPERATIONAL   30    00:12:15
P1#show ldp targeted-peers
IP Address          Interface
1.1.1.1             xe5
    3.3.3.3             xe5

P1#show ldp session 1.1.1.1
Session state         : OPERATIONAL
Session role          : Active
TCP Connection        : Established
IP Address for TCP    : 1.1.1.1
Interface being used  : xe5
Peer LDP ID           : 1.1.1.1:0
Peer LDP Password     : Not Set
Adjacencies           : 1.1.1.1
Advertisement mode    : Downstream Unsolicited
Label retention mode  : Liberal
```

```
Graceful Restart      : Not Capable
Keepalive Timeout     : 30
Reconnect Interval    : 15
Session protection    : Protecting
Address List received : 1.1.1.1
                        30.30.30.1
                        254.128.0.0
Received Labels :       Fec             Label           Maps To
                IPV4:4.4.4.4/32         24960           52482
                IPV4:40.40.40.0/24      24961           52484
                IPV4:30.30.30.0/24      impl-null       52483
                IPV4:10.10.10.0/24      impl-null       none
                IPV4:1.1.1.1/32         impl-null       52481
Sent Labels :   Fec                     Label           Maps To
                IPV4:3.3.3.3/32         52480           impl-null
                IPV4:20.20.20.0/24      impl-null       none
                IPV4:10.10.10.0/24      impl-null       none
                    IPV4:2.2.2.2/32         impl-null       none

P1#show mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN,
       B - BGP FTN, K - CLI FTN, t - tunnel,
       L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, I - IGP-Shortcut,
       U - unknown FTN

Code    FEC               FTN-ID    Nhlfe-ID  Tunnel-id   Pri   LSP-Type     Out-Label
Out-Intf    ELC   Nexthop
   L>   1.1.1.1/32          2         3         -          Yes   LSP_DEFAULT  24965
xe5         No    20.20.20.2
   L>   3.3.3.3/32          5         9         -          Yes   LSP_DEFAULT  3
xe5         No    20.20.20.2
   L>   4.4.4.4/32          3         5         -          Yes   LSP_DEFAULT  24966
xe5         No    20.20.20.2
   L>   30.30.30.0/24       4         7         -          Yes   LSP_DEFAULT  24967
xe5         No    20.20.20.2
   L>   40.40.40.0/24       1         1         -          Yes   LSP_DEFAULT  3
xe5         No    20.20.20.2
P1#show mpls ilm-table
Codes: > - installed ILM, * - selected ILM, p - stale ILM
        K - CLI ILM, T - MPLS-TP, s - Stitched ILM
       S - SNMP, L - LDP, R - RSVP, C - CRLDP
       B - BGP , K - CLI , V - LDP_VC, I - IGP_SHORTCUT
       U - unknown

Code    FEC/VRF/L2CKT    ILM-ID     In-Label    Out-Label   In-Intf    Out-Intf/VRF
Nexthop                  LSP-Type
   L>   4.4.4.4/32        3          52482       Nolabel     N/A        N/A
127.0.0.1                LSP_DEFAULT
   L>   3.3.3.3/32        1          52480       3           N/A        xe5
20.20.20.2               LSP_DEFAULT
   L>   1.1.1.1/32        2          52481       Nolabel     N/A        N/A
127.0.0.1                LSP_DEFAULT
```

```
   L>   30.30.30.0/24      4          52483       Nolabel     N/A        N/A
127.0.0.1                 LSP_DEFAULT
   L>   40.40.40.0/24      5          52484       Nolabel     N/A        N/A
127.0.0.1                 LSP_DEFAULT
P1#
P1#show mpls ftn-table
 Primary FTN entry with FEC: 1.1.1.1/32, id: 2, row status: Active
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A
     Cross connect ix: 1, in intf: - in label: 0 out-segment ix: 2
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: LDP, Stale: NO, out intf: xe5, out label: 24965
    Nexthop addr: 20.20.20.2        cross connect ix: 1, op code: Push


 Primary FTN entry with FEC: 3.3.3.3/32, id: 5, row status: Active
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A
     Cross connect ix: 5, in intf: - in label: 0 out-segment ix: 8
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 8, owner: N/A, Stale: NO, out intf: xe5, out label: 3
    Nexthop addr: 20.20.20.2        cross connect ix: 5, op code: Push


 Primary FTN entry with FEC: 4.4.4.4/32, id: 3, row status: Active
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A
     Cross connect ix: 3, in intf: - in label: 0 out-segment ix: 4
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 4, owner: LDP, Stale: NO, out intf: xe5, out label: 24966
    Nexthop addr: 20.20.20.2        cross connect ix: 3, op code: Push


 Primary FTN entry with FEC: 30.30.30.0/24, id: 4, row status: Active
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A
     Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 6
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 6, owner: LDP, Stale: NO, out intf: xe5, out label: 24967
    Nexthop addr: 20.20.20.2        cross connect ix: 4, op code: Push


 Primary FTN entry with FEC: 40.40.40.0/24, id: 1, row status: Active
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A
     Cross connect ix: 5, in intf: - in label: 0 out-segment ix: 8
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
```

```
       Out-segment with ix: 8, owner: N/A, Stale: NO, out intf: xe5, out label: 3
    Nexthop addr: 20.20.20.2        cross connect ix: 5, op code: Push


P1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
O            1.1.1.1/32 [110/53] via 20.20.20.2, xe5, 00:03:44
C            2.2.2.2/32 is directly connected, lo, 00:14:13
O            3.3.3.3/32 [110/2] via 20.20.20.2, xe5, 00:12:51
O            4.4.4.4/32 [110/52] via 20.20.20.2, xe5, 00:03:44
C            20.20.20.0/24 is directly connected, xe5, 00:13:46
O            30.30.30.0/24 [110/52] via 20.20.20.2, xe5, 00:03:44
O            40.40.40.0/24 [110/51] via 20.20.20.2, xe5, 00:03:44
C            127.0.0.0/8 is directly connected, lo, 00:14:13
```

Bring up the link and check same labels reused.

`(config)#interface xe12`	Enter interface mode.
`(config-if)#no shutdown`	Shutdown the link.
`(config)#commit`	Commit.

Validation

```
PE1#show ldp session
Peer IP Address           IF Name    My Role    State      KeepAlive  UpTime
4.4.4.4                   xe6        Passive   OPERATIONAL   30    00:14:55
2.2.2.2                   xe12       Passive   OPERATIONAL   30    00:15:41
PE1#show ldp targeted-peers
IP Address          Interface
2.2.2.2             xe12
4.4.4.4             xe6

PE1#show ldp session 2.2.2.2
Session state         : OPERATIONAL
Session role          : Passive
TCP Connection        : Established
IP Address for TCP    : 2.2.2.2
Interface being used  : xe12
Peer LDP ID           : 2.2.2.2:0
```

```
Peer LDP Password     : Not Set
Adjacencies           : 10.10.10.2
                        2.2.2.2
Advertisement mode    : Downstream Unsolicited
Label retention mode  : Liberal
Graceful Restart      : Not Capable
Keepalive Timeout     : 30
Reconnect Interval    : 15
Session protection    : Ready
Address List received : 2.2.2.2
                        10.10.10.2
                        20.20.20.1
                        254.128.0.0
Received Labels :       Fec             Label           Maps To
                IPV4:3.3.3.3/32         52480           24966
                IPV4:20.20.20.0/24      impl-null       24967
                IPV4:10.10.10.0/24      impl-null       none
                IPV4:2.2.2.2/32         impl-null       24965
Sent Labels :   Fec                     Label           Maps To
                IPV4:40.40.40.0/24      24961           impl-null
                IPV4:4.4.4.4/32         24960           impl-null
                IPV4:30.30.30.0/24      impl-null       none
                IPV4:10.10.10.0/24      impl-null       none
                IPV4:1.1.1.1/32         impl-null       none

PE1#show mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN,
       B - BGP FTN, K - CLI FTN, t - tunnel, P - SR Policy FTN,
       L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, I - IGP-Shortcut,
       U - unknown FTN, O - SR-OSPF FTN, i - SR-ISIS FTN, k - SR-CLI FTN
(m) - FTN mapped over multipath transport

Code    FEC               FTN-ID    Nhlfe-ID  Tunnel-id   Pri   LSP-Type     Out-Label
Out-Intf    ELC   Nexthop
   L>   2.2.2.2/32         3         9         -           Yes   LSP_DEFAULT  3
xe12        No    10.10.10.2
   L>   3.3.3.3/32         1         2         -           Yes   LSP_DEFAULT  52480
xe12        No    10.10.10.2
   L>   4.4.4.4/32         4         7         -           Yes   LSP_DEFAULT  3
xe6         No    30.30.30.2
   L>   20.20.20.0/24      2         4         -           Yes   LSP_DEFAULT  3
xe12        No    10.10.10.2
   L>   40.40.40.0/24      5         8         -           Yes   LSP_DEFAULT  3
xe6         No    30.30.30.2
PE1#
PE1#show mpls ilm-table
Codes: > - installed ILM, * - selected ILM, p - stale ILM
        K - CLI ILM, T - MPLS-TP, s - Stitched ILM
       S - SNMP, L - LDP, R - RSVP, C - CRLDP
       B - BGP , K - CLI , V - LDP_VC, I - IGP_SHORTCUT
       O - OSPF/OSPF6 SR, i - ISIS SR, k - SR CLI
       P - SR Policy, U - unknown
```

```
Code    FEC/VRF/L2CKT    ILM-ID     In-Label    Out-Label   In-Intf    Out-Intf/VRF
Nexthop                    LSP-Type
   L>   2.2.2.2/32         9          24965       3           N/A        xe12
10.10.10.2                 LSP_DEFAULT
   L>   40.40.40.0/24      2          24961       3           N/A        xe6
30.30.30.2                 LSP_DEFAULT
   L>   4.4.4.4/32         1          24960       3           N/A        xe6
30.30.30.2                 LSP_DEFAULT
   L>   3.3.3.3/32         10         24966       52480       N/A        xe12
10.10.10.2                 LSP_DEFAULT
   L>   20.20.20.0/24      11         24967       3           N/A        xe12
10.10.10.2                 LSP_DEFAULT
PE1#show mpls ftn-table
 Primary FTN entry with FEC: 2.2.2.2/32, id: 3, row status: Active, Tunnel-Policy: N/A
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
     Cross connect ix: 5, in intf: - in label: 0 out-segment ix: 10
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 10, owner: N/A, Stale: NO, out intf: xe12, out label: 3
    Nexthop addr: 10.10.10.2        cross connect ix: 5, op code: Push


 Primary FTN entry with FEC: 3.3.3.3/32, id: 1, row status: Active, Tunnel-Policy: N/A
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
     Cross connect ix: 6, in intf: - in label: 0 out-segment ix: 11
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 11, owner: LDP, Stale: NO, out intf: xe12, out label: 52480
    Nexthop addr: 10.10.10.2        cross connect ix: 6, op code: Push


 Primary FTN entry with FEC: 4.4.4.4/32, id: 4, row status: Active, Tunnel-Policy: N/A
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
     Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 6
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 6, owner: N/A, Stale: NO, out intf: xe6, out label: 3
    Nexthop addr: 30.30.30.2        cross connect ix: 4, op code: Push


 Primary FTN entry with FEC: 20.20.20.0/24, id: 2, row status: Active, Tunnel-Policy: N/
A
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
     Cross connect ix: 5, in intf: - in label: 0 out-segment ix: 10
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 10, owner: N/A, Stale: NO, out intf: xe12, out label: 3
    Nexthop addr: 10.10.10.2        cross connect ix: 5, op code: Push
```

```
 Primary FTN entry with FEC: 40.40.40.0/24, id: 5, row status: Active, Tunnel-Policy: N/
A
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A, Color: 0
     Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 6
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 6, owner: N/A, Stale: NO, out intf: xe6, out label: 3
    Nexthop addr: 30.30.30.2        cross connect ix: 4, op code: Push


P1#show ldp session
Peer IP Address           IF Name    My Role    State      KeepAlive  UpTime
3.3.3.3                   xe5        Passive   OPERATIONAL   30    00:15:30
    1.1.1.1                   xe48       Active    OPERATIONAL   30    00:16:33

P1#show ldp targeted-peers
IP Address          Interface
1.1.1.1             xe48
3.3.3.3             xe5

P1#show ldp session 1.1.1.1
Session state         : OPERATIONAL
Session role          : Active
TCP Connection        : Established
IP Address for TCP    : 1.1.1.1
Interface being used  : xe48
Peer LDP ID           : 1.1.1.1:0
Peer LDP Password     : Not Set
Adjacencies           : 10.10.10.1
                        1.1.1.1
Advertisement mode    : Downstream Unsolicited
Label retention mode  : Liberal
Graceful Restart      : Not Capable
Keepalive Timeout     : 30
Reconnect Interval    : 15
Session protection    : Ready
Address List received : 1.1.1.1
                        10.10.10.1
                        30.30.30.1
                        254.128.0.0
Received Labels :       Fec             Label           Maps To
                IPV4:4.4.4.4/32         24960           52482
                IPV4:40.40.40.0/24      24961           52484
                IPV4:30.30.30.0/24      impl-null       52483
                IPV4:10.10.10.0/24      impl-null       none
                IPV4:1.1.1.1/32         impl-null       52481
Sent Labels :   Fec                     Label           Maps To
                IPV4:3.3.3.3/32         52480           impl-null
```

```
                IPV4:20.20.20.0/24      impl-null       none
                IPV4:10.10.10.0/24      impl-null       none
                    IPV4:2.2.2.2/32         impl-null       none

P1#show mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN,
       B - BGP FTN, K - CLI FTN, t - tunnel,
       L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, I - IGP-Shortcut,
       U - unknown FTN

Code    FEC               FTN-ID    Nhlfe-ID  Tunnel-id   Pri   LSP-Type     Out-Label
Out-Intf    ELC   Nexthop
   L>   1.1.1.1/32          2         3         -           Yes   LSP_DEFAULT  3
xe48        No    10.10.10.1
   L>   3.3.3.3/32          5         9         -           Yes   LSP_DEFAULT  3
xe5         No    20.20.20.2
   L>   4.4.4.4/32          3         5         -           Yes   LSP_DEFAULT  24960
xe48        No    10.10.10.1
   L>   30.30.30.0/24       4         7         -           Yes   LSP_DEFAULT  3
xe48        No    10.10.10.1
   L>   40.40.40.0/24       1         1         -           Yes   LSP_DEFAULT  24961
xe48        No    10.10.10.1
P1#
P1#show mpls ilm-table
Codes: > - installed ILM, * - selected ILM, p - stale ILM
        K - CLI ILM, T - MPLS-TP, s - Stitched ILM
       S - SNMP, L - LDP, R - RSVP, C - CRLDP
       B - BGP , K - CLI , V - LDP_VC, I - IGP_SHORTCUT
       U - unknown

Code    FEC/VRF/L2CKT    ILM-ID     In-Label    Out-Label   In-Intf    Out-Intf/VRF
Nexthop                  LSP-Type
   L>   4.4.4.4/32        3          52482       24960       N/A        xe48
10.10.10.1               LSP_DEFAULT
   L>   1.1.1.1/32        2          52481       3           N/A        xe48
10.10.10.1               LSP_DEFAULT
   L>   3.3.3.3/32        1          52480       3           N/A        xe5
20.20.20.2               LSP_DEFAULT
   L>   40.40.40.0/24     5          52484       24961       N/A        xe48
10.10.10.1               LSP_DEFAULT
   L>   30.30.30.0/24     4          52483       3           N/A        xe48
10.10.10.1               LSP_DEFAULT

P1#show mpls ftn-table
 Primary FTN entry with FEC: 1.1.1.1/32, id: 2, row status: Active
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A
     Cross connect ix: 6, in intf: - in label: 0 out-segment ix: 10
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 10, owner: N/A, Stale: NO, out intf: xe48, out label: 3
    Nexthop addr: 10.10.10.1        cross connect ix: 6, op code: Push
```

```
 Primary FTN entry with FEC: 3.3.3.3/32, id: 5, row status: Active
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A
     Cross connect ix: 5, in intf: - in label: 0 out-segment ix: 8
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 8, owner: N/A, Stale: NO, out intf: xe5, out label: 3
    Nexthop addr: 20.20.20.2        cross connect ix: 5, op code: Push


 Primary FTN entry with FEC: 4.4.4.4/32, id: 3, row status: Active
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A
     Cross connect ix: 7, in intf: - in label: 0 out-segment ix: 11
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 11, owner: LDP, Stale: NO, out intf: xe48, out label: 24960
    Nexthop addr: 10.10.10.1        cross connect ix: 7, op code: Push


 Primary FTN entry with FEC: 30.30.30.0/24, id: 4, row status: Active
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A
     Cross connect ix: 6, in intf: - in label: 0 out-segment ix: 10
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 10, owner: N/A, Stale: NO, out intf: xe48, out label: 3
    Nexthop addr: 10.10.10.1        cross connect ix: 6, op code: Push


 Primary FTN entry with FEC: 40.40.40.0/24, id: 1, row status: Active
  Owner: LDP, distance: 0, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0, Protected LSP id: 0, Description: N/A
     Cross connect ix: 8, in intf: - in label: 0 out-segment ix: 12
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 12, owner: LDP, Stale: NO, out intf: xe48, out label: 24961
    Nexthop addr: 10.10.10.1        cross connect ix: 8, op code: Push
```

CHAPTER 11 MPLS LDP-IGP Synchronization

This chapter contains configurations for MPLS LDP-IGP Synchronization.

Overview

Multi-Protocol Label Switching (MPLS) Label Distribution Protocol (LDP) Interior Gateway Protocol (IGP) Synchronization ensures that LDP is fully established before the IGP path is used for switching. In certain networks, there is dependency on the edge-to-edge Label Switched Paths (LSPs) setup by the Label Distribution Protocol (LDP), e.g., networks that are used for Multi-Protocol Label Switching (MPLS) Virtual Private Network (VPN) applications. For such applications, it is not possible to rely on Internet Protocol (IP) forwarding if the MPLS LSP is not operating appropriately. Labelled traffic can be dropped due to presence of black holes in situations where the Interior Gateway Protocol (IGP) is operational on a link but LDP sessions are not up as the label distribution is not completed. While the link could still be used for IP forwarding, it is not useful for MPLS forwarding, for example, MPLS VPN applications or Border Gateway Protocol (BGP) route-free cores.

The MPLS LDP-IGP Synchronization feature ensures that the Label Distribution Protocol (LDP) is fully established before the Interior Gateway Protocol (IGP) path is used for packet forwarding. It is useful for cases in which the router is the ingress and the decision of whether to take the MPLS LSP or IGP path is decided there.

LDP-IGP synchronization is an interface level feature. It can be selectively enabled in the required interfaces. For each interface there are two commands available for synchronization, one each for IS-IS. Once configured the IGP saves the required information, and also notifies LDP. In between the IGP increases the link cost to maximum and sends advertisements to its peer. This discourages its peers from taking routes that pass via it.

When all LDP sessions hosted on the interface become operational, it sends a notification to the IGP. This is termed as LDP convergence. The IGP then advertises normal cost, so that all traffic now coming to the interface takes the MPLS LSP path established by LDP and not be IP routed.

Prerequisites

Only interfaces that are running Open Shortest Path First (OSPF) or Intermediate System-to-Intermediate System (IS-IS) processes are capable of LDP-IGP synchronization. The router must also be running LDP.

Topology

The sample topology diagram is applicable to all configurations in this chapter.

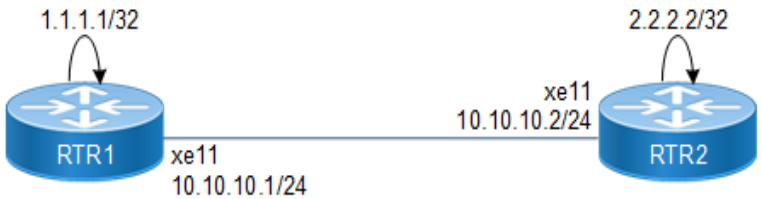


Figure 11-23: Sample Topology for LDP-IGP Synchronization

LDP-IGP Synchronization with OSPF

When IGP synchronization is enabled on OSPF-enabled interfaces, OSPF sends Maximum/Normal cost based on LDP session Down or Up state messages to interfaces until the hold-down-timer expires or synchronization is achieved.

Before configuring LDP-IGP synchronization, the NSM, OSPF and LDP configurations must be completed. The tables below contain examples of how this is done.

RTR1-NSM

`#configure terminal`	Enter configuration mode.
`(config)#interface xe11`	Enter interface mode.
`(config-if)#ip address 10.10.10.1/24`	Configure IPv4 address for xe11.
`(config-if)#label-switching`	Enable label switching on interface xe11.
`(config-if)#exit`	Exit interface mode.
`(config)#interface lo`	Specify the loopback (lo) interface to be configured.
`(config-if)#ip address 1.1.1.1/32 secondary`	Set the IP address of the loopback interface to 1.1.1.1/32.

RTR1-OSPF

`(config)#router ospf 100`	Configure the routing process and specify the Process ID 100. The Process ID should be a unique positive integer identifying the routing process.
`(config-router)# router-id 1.1.1.1`	Configure router id for OSPF
`(config-router)#network 10.10.10.0/24 area 0` `(config-router)#network 1.1.1.1/32 area 0`	Define the interface on which OSPF runs and associate the area ID (0) with the interface.

RTR1-LDP

`(config)#router ldp`	Enter router mode for LDP.
`(config-router)#router-id 1.1.1.1`	Set the router ID to IP address 1.1.1.1.
`(config-router)#transport-address ipv4 1.1.1.1`	Configure the transport address for IPV4 (for IPV6 use ipv6) to be used for a TCP session over which LDP will run. Note: It is preferable to use the loopback address as the transport address.
`(config-router)#exit`	Exit router mode.
`(config)#interface xe11`	Enter interface mode.
`(config-if)#enable-ldp ipv4`	Enable LDP for IPv4 on xe11.
`(config-if)#exit`	Exit interface mode.

RTR2-NSM

`#configure terminal`	Enter configuration mode.
`(config)#interface xe11`	Enter interface mode.
`(config-if)#ip address 10.10.10.2/24`	Configure IPv4 address for xe11.
`(config-if)#label-switching`	Enable label switching on interface xe11.
`(config-if)#exit`	Exit interface mode.
`(config)#interface lo`	Specify the loopback (lo) interface to be configured.
`(config-if)#ip address 2.2.2.2/32 secondary`	Set the IP address of the loopback interface to 2.2.2.2/32.

RTR2-OSPF

`(config)#router ospf 100`	Configure the routing process and specify the Process ID 100. The Process ID should be a unique positive integer identifying the routing process.
`(config-router)# router-id 2.2.2.2`	Configure router id for OSPF
`(config-router)#network 10.10.10.0/24 area 0` `(config-router)#network 2.2.2.2/32 area 0`	Define the interface on which OSPF runs and associate the area ID (0) with the interface.

RTR2-LDP

`(config)#router ldp`	Enter Router mode for LDP.
`(config-router)#router-id 2.2.2.2`	Set the router ID to IP address 2.2.2.2.
`(config-router)#transport-address ipv4 2.2.2.2`	Configure the transport address for IPV4 (for IPV6 use ipv6) to be used for a TCP session over which LDP will run. Note: It is preferable to use the loopback address as transport address.
`(config-router)#exit`	Exit the Router mode and return to the Configure mode.
`(config)#interface xe11`	Enter interface mode.
`(config-if)#enable-ldp ipv4`	Enable LDP for IPv4 on xe11.
`(config-if)#exit`	Exit interface mode.

Validation

```
R1#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
2.2.2.2           1   Full/DR         00:00:33    10.10.10.2      xe11
0

R2#show ip ospf neighbor
```

```
Total number of full neighbors: 1
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
1.1.1.1         1   Full/Backup     00:00:31    10.10.10.1      xe11
0
R2#

R1#show ldp session
Peer IP Address           IF Name    My Role    State      KeepAlive  UpTime
2.2.2.2                   xe11       Passive    OPERATIONAL   30    00:06:03

R2#show ldp session
Peer IP Address           IF Name    My Role    State      KeepAlive  UpTime
1.1.1.1                   xe11       Active     OPERATIONAL   30    00:06:31

R1#show ldp adjacency
IP Address      Mode          Intf Name    Holdtime   LDP-Identifier
10.10.10.2      Interface     xe11         15         2.2.2.2:0


R2#show ldp adjacency
IP Address      Mode          Intf Name    Holdtime   LDP-Identifier
10.10.10.1      Interface     xe11         15         1.1.1.1:0

R1#show ip ospf interface
lo is up, line protocol is up
  Internet Address 1.1.1.1/32, Area 0.0.0.0, MTU 16436
  Process ID 100, VRF (default), Router ID 1.1.1.1, Network Type LOOPBACK,
Cost: 1
  Transmit Delay is 1 sec,  State Loopback, TE Metric 1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
xe11 is up, line protocol is up
  Internet Address 10.10.10.1/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 1.1.1.1, Network Type BROADCAST,
Cost: 1
  Transmit Delay is 1 sec,  State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 2.2.2.2, Interface Address 10.10.10.2
  Backup Designated Router (ID) 1.1.1.1, Interface Address 10.10.10.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Neighbor Count is 1, Adjacent neighbor count is 1
  Hello received 61 sent 62, DD received 3 sent 6
  LS-Req received 1 sent 1, LS-Upd received 4 sent 5
  LS-Ack received 4 sent 3, Discarded 0
  No authentication

R2#sh ip ospf interface
lo is up, line protocol is up
  Internet Address 2.2.2.2/32, Area 0.0.0.0, MTU 16436
  Process ID 100, VRF (default), Router ID 2.2.2.2, Network Type LOOPBACK,
Cost: 1
  Transmit Delay is 1 sec,  State Loopback, TE Metric 1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
xe11 is up, line protocol is up
  Internet Address 10.10.10.2/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 2.2.2.2, Network Type BROADCAST,
Cost: 1
```

```
  Transmit Delay is 1 sec,  State DR, Priority 1, TE Metric 1
  Designated Router (ID) 2.2.2.2, Interface Address 10.10.10.2
  Backup Designated Router (ID) 1.1.1.1, Interface Address 10.10.10.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Neighbor Count is 1, Adjacent neighbor count is 1
  Hello received 62 sent 63, DD received 6 sent 3
  LS-Req received 1 sent 1, LS-Upd received 5 sent 4
  LS-Ack received 3 sent 4, Discarded 0
  No authentication

R1#show mpls ldp igp sync
R1#

R2#show mpls ldp igp sync
R2#
```

LDP-IGP Synchronization

Now that NSM, OSPF and LDP are all enabled, the LDP-IGP synchronization can be configured.

RTR1

`(config)#interface xe11`	Enter interface mode.
`(config-if)#mpls ldp-igp sync ospf holddown-timer 500`	Enable LDP-IGP Synchronization for xe11 belonging to an OSPF process and 500 seconds is holddown-timer value for IGP to wait until LDP converges. **OSPF:** This command is part of OSPF Process. Note: Holddown-timer range is 1 to 2147483 seconds. If holddown timer is not configured, IGP waits indefinitely for LDP to converge. Use the command mpls ldp-igp sync ospf to configure without a holddown-timer.
`(config-if)#mpls ldp-igp sync-delay 60`	Configure time delay in seconds for notification of LDP convergence to IGP. This is not applicable for notification of non-convergence. Range is 5 to 60 seconds. This command is optional. **LDP:** This command is part of LDP Process. **Default:** If not configured the delay is 0 seconds.
`(config-if)#exit`	Exit interface mode.

RTR2

`(config)#interface xe11`	Enter interface mode.
`(config-if)#mpls ldp-igp sync ospf holddown-timer 500`	Enable LDP-IGP Synchronization for interfaces (xe11) belonging to an OSPF process.and 500 secs is Holddown-timer value for IGP to wait until LDP Converge. **OSPF:** This command is part of the OSPF Process.vNote: Holddown-timer range is <1-2147483> seconds. If holddown timer is not configured, IGP waits indefinitely for LDP to converge. Use command mpls ldp-igp sync ospf to configure without a holddown-timer.

`(config-if)#mpls ldp-igp sync-delay 60`	Configure the time delay in seconds for the notification of LDP convergence to IGP. (This is not applicable for notification of non-convergence.) Range is 5 to 60 seconds. This command is optional. **LDP:** This command is part of LDP Process. **Default:** If not configured the delay is 0 seconds.
`(config-if)#exit`	Exit interface mode.

RTR1 Validation

When LDP IGP SYNC is Configured with hold-down and sync-delay timer

```
R1#show ip ospf interface
lo is up, line protocol is up
  Internet Address 1.1.1.1/32, Area 0.0.0.0, MTU 16436
  Process ID 100, VRF (default), Router ID 1.1.1.1, Network Type LOOPBACK,
Cost:
 1
  Transmit Delay is 1 sec,  State Loopback, TE Metric 1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
xe11 is up, line protocol is up
  Internet Address 10.10.10.1/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 1.1.1.1, Network Type BROADCAST,
Cost
: 1
  Transmit Delay is 1 sec,  State Backup, Priority 1, TE Metric 1
  LDP-OSPF Sync configured
    Holddown timer : 500 seconds, Remaining time = 0 seconds
  Designated Router (ID) 2.2.2.2, Interface Address 10.10.10.2
  Backup Designated Router (ID) 1.1.1.1, Interface Address 10.10.10.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Neighbor Count is 1, Adjacent neighbor count is 1
  Hello received 178 sent 179, DD received 3 sent 6
  LS-Req received 1 sent 1, LS-Upd received 5 sent 6
  LS-Ack received 5 sent 4, Discarded 0
  No authentication
R1#

R1#show mpls ldp igp sync
xe11 is up, line protocol is up
  LDP configured; LDP-IGP Synchronization enabled.
  Session IP Address : 2.2.2.2
    Sync status: Achieved
    Delay timer: Configured, 60 seconds, Not Running
```

RTR2 Validation

```
R2#show ip ospf interface
lo is up, line protocol is up
  Internet Address 2.2.2.2/32, Area 0.0.0.0, MTU 16436
  Process ID 100, VRF (default), Router ID 2.2.2.2, Network Type LOOPBACK,
Cost:
 1
  Transmit Delay is 1 sec,  State Loopback, TE Metric 1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

```
xe11 is up, line protocol is up
  Internet Address 10.10.10.2/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 2.2.2.2, Network Type BROADCAST,
Cost
: 1
  Transmit Delay is 1 sec,  State DR, Priority 1, TE Metric 1
  LDP-OSPF Sync configured
    Holddown timer : 500 seconds, Remaining time = 0 seconds
  Designated Router (ID) 2.2.2.2, Interface Address 10.10.10.2
  Backup Designated Router (ID) 1.1.1.1, Interface Address 10.10.10.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Neighbor Count is 1, Adjacent neighbor count is 1
  Hello received 211 sent 211, DD received 6 sent 3
  LS-Req received 1 sent 1, LS-Upd received 8 sent 7
  LS-Ack received 6 sent 7, Discarded 0
  No authentication
R2#

R2#show mpls ldp igp sync
xe11 is up, line protocol is up
  LDP configured; LDP-IGP Synchronization enabled.
  Session IP Address : 1.1.1.1
    Sync status: Achieved
    Delay timer: Configured, 60 seconds, Not Running
```

LDP-IGP Synchronization with IS-IS

When IGP synchronization is enabled on an IS-IS enabled interfaces, IS-IS sends Maximum/Normal cost based on LDP session or Up state on interfaces until hold-down-timer expires or synchronization is achieved.

Before configuring LDP-IGP synchronization, the NSM, IS-IS and LDP configurations must be completed. The tables below contain examples of how this is done.

RTR1-NSM

`#configure terminal`	Enter configuration mode.
`(config)#interface xe11`	Enter interface mode.
`(config-if)#ip address 10.10.10.1/24`	Set the IP address of the xe11 to 10.10.10.1/24.
`(config-if)#label-switching`	Enable label switching on xe11.
`(config-if)#exit`	Exit interface mode.
`(config)#interface lo`	Specify the loopback (lo) interface to be configured.
`(config-if)#ip address 1.1.1.1/32 secondary`	Set the IP address of the loopback interface to 1.1.1.1/32.
`(config-if)#exit`	Exit interface mode.

RTR1-IS-IS

`(config)#router isis 1`	Configure the IS-IS routing instance and specify the TAG (1). The TAG should be a WORD - ISO routing area tag.
`(config-router)#is-type level-1`	Define the IS to the specified level of routing for router.

`(config-router)#net 49.0001.0000.0000.0001.00`	Configure the Network Entity Title (NET) for the instance.
`(config-router)#exit`	Exit the Router mode and return to the Configure mode.
`(config)#interface xe11`	Enter interface mode.
`(config-if)#ip router isis 1`	Configure IS-IS IPv4 routing on the interface with IS-IS tag instance 1.
`(config-if)#exit`	Exit interface mode.
`(config)#interface lo`	Enter interface mode for the loopback interface (lo).
`(config-if)#ip router isis 1`	Configure IS-IS IPv4 routing on the interface with IS-IS tag instance 1.
`(config-if)#exit`	Exit interface mode.

RTR1-LDP

`(config)#router ldp`	Enter Router mode for LDP.
`(config-router)#router-id 1.1.1.1`	Set the router ID to IP address 1.1.1.1.
`(config-router)#transport-address ipv4 1.1.1.1`	Configure the transport address for IPV4 (for IPv6 use an IPv6 address) to use for a TCP session over which LDP will run. Note: It is preferable to use the loopback address as transport address.
`(config-router)#exit`	Exit the Router mode and return to the Configure mode.
`(config)#interface xe11`	Enter interface mode.
`(config-if)#enable-ldp ipv4`	Enable LDP for IPv4 on xe11.
`(config-if)#exit`	Exit interface mode.

RTR2-NSM

`#configure terminal`	Enter configuration mode
`(config)#interface xe11`	Enter interface mode.
`(config-if)#ip address 10.10.10.2/24`	Set the IP address of xe11 to 10.10.10.2/24
`(config-if)#label-switching`	Enable label switching on interface xe11.
`(config-if)#exit`	Exit interface mode.
`(config)#interface lo`	Specify the loopback (lo) interface to be configured.
`(config-if)#ip address 2.2.2.2/32 secondary`	Set the IP address of the loopback interface to 2.2.2.2/32.
`(config-if)#exit`	Exit interface mode.

RTR2-IS-IS

`(config)#router isis 1`	Configure the IS-IS routing instance and specify the TAG as 1. The TAG should be a WORD - ISO routing area tag.
`(config-router)#is-type level-1`	Define the IS to the specified level of routing for router.
`(config-router)#net 49.0001.0000.0000.0002.00`	Configure the Network Entity Title (NET) for the instance.
`(config-router)#exit`	Exit the Router mode and return to the Configure mode.
`(config)#interface xe11`	Enter interface mode.

(config-if)#ip router isis 1	Configure IS-IS IPv4 routing on the interface with is-is tag instance 1.
(config-if)#exit	Exit interface mode.
(config)#interface lo	Enter interface mode for the loopback (lo) interface.
(config-if)#ip router isis 1	Configure IS-IS IPv4 routing on the interface with IS-IS tag instance 1.
(config-if)#exit	Exit interface mode.

RTR2-LDP

(config)#router ldp	Enter Router mode for LDP.
(config-router)#router-id 2.2.2.2	Set the router ID to IP address 2.2.2.2.
(config-router)#transport-address ipv4 2.2.2.2	Configure the transport address for IPv4 (for IPv6 use an IPv6 address) to use for a TCP session over which LDP will run. Note: It is preferable to use the loopback address as transport address.
(config-router)#exit	Exit the Router mode and return to the Configure mode.
(config)#interface xe11	Enter interface mode.
(config-if)#enable-ldp ipv4	Enable LDP for IPv4 on xe11.
(config-if)#exit	Exit interface mode.

Validation

```
R1#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 0
Total number of adjacencies: 1
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0002 xe11        6cb9.c5cf.da69      Up     24        L1   IS-IS

R2#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 0
Total number of adjacencies: 1
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0001 xe11        b86a.97d1.24d1      Up     9         L1   IS-IS

R1#show clns is-neighbors

Tag 1:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id
0000.0000.0002 xe11        Up     L1   64        0000.0000.0001.01

R2#show clns is-neighbors

Tag 1:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id
```

```
0000.0000.0001 xe11        Up     L1   64         0000.0000.0001.01

R1#show ldp session
Peer IP Address           IF Name    My Role    State      KeepAlive  UpTime
2.2.2.2                   xe11       Passive   OPERATIONAL   30    00:08:08

R1#show ldp adjacency
IP Address      Mode          Intf Name    Holdtime   LDP-Identifier
10.10.10.2      Interface     xe11        15         2.2.2.2:0

R2#show ldp session
Peer IP Address           IF Name    My Role    State      KeepAlive  UpTime
1.1.1.1                   xe11       Active    OPERATIONAL   30    00:08:24

R2#show ldp adjacency
IP Address      Mode          Intf Name    Holdtime   LDP-Identifier
10.10.10.1      Interface     xe11        15         1.1.1.1:0

R1#show isis interface xe11
xe11 is up, line protocol is up
  Routing Protocol: IS-IS (1)
    Network Type: Broadcast
    Circuit Type: level-1
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x0000271C
    Local SNPA: b86a.97d1.24d1
    IP interface address:
      10.10.10.1/24
    IPv6 interface address:
      fe80::ba6a:97ff:fed1:24d1/64
    Level-1 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0001.01
    Number of active level-1 adjacencies: 1
    Level-1 LSP MTU: 1492
    Next IS-IS LAN Level-1 Hello in 792 milliseconds

R2#show isis interface xe11
xe11 is up, line protocol is up
  Routing Protocol: IS-IS (1)
    Network Type: Broadcast
    Circuit Type: level-1
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x0000271B
    Local SNPA: 6cb9.c5cf.da69
    IP interface address:
      10.10.10.2/24
    IPv6 interface address:
      fe80::6eb9:c5ff:fecf:da69/64
    Level-1 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0001.01
    Number of active level-1 adjacencies: 1
    Level-1 LSP MTU: 1492
    Next IS-IS LAN Level-1 Hello in 1 seconds


R1#show isis database detail
Tag 1:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
```

```
0000.0000.0001.00-00* 0x00000002   0xB193        516               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   10.10.10.1
  Metric:   10         IS 0000.0000.0001.01
  Metric:   10         IP 10.10.10.0 255.255.255.0
  Metric:   10         IP 1.1.1.1 255.255.255.255
0000.0000.0001.01-00* 0x00000001   0x1FBD        516               0/0/0
  Metric:   0          IS 0000.0000.0001.00
  Metric:   0          IS 0000.0000.0002.00
0000.0000.0002.00-00  0x00000002   0x84BA        519               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   10.10.10.2
  Metric:   10         IS 0000.0000.0001.01
  Metric:   10         IP 10.10.10.0 255.255.255.0
  Metric:   10         IP 2.2.2.2 255.255.255.255

R2#show isis database detail
Tag 1:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00  0x00000002   0xB193        521               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   10.10.10.1
  Metric:   10         IS 0000.0000.0001.01
  Metric:   10         IP 10.10.10.0 255.255.255.0
  Metric:   10         IP 1.1.1.1 255.255.255.255
0000.0000.0001.01-00  0x00000001   0x1FBD        521               0/0/0
  Metric:   0          IS 0000.0000.0001.00
  Metric:   0          IS 0000.0000.0002.00
0000.0000.0002.00-00* 0x00000002   0x84BA        526               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  IP Address:   10.10.10.2
  Metric:   10         IS 0000.0000.0001.01
  Metric:   10         IP 10.10.10.0 255.255.255.0
  Metric:   10         IP 2.2.2.2 255.255.255.255



R1#show mpls ldp igp sync
R1#

R2#show mpls ldp igp sync
R2#
```

LDP-IGP SYNC Configuration

Now that NSM, IS-IS and LDP are all enabled, the LDP-IGP synchronization can be configured.

RTR1

`(config)#interface xe11`	Enter interface mode.
`(config-if)#mpls ldp-igp sync isis level-1 holddown-timer 700`	Configure LDP-IGP Synchronization for interface xe11 belonging to an IS-IS process with corresponding IS-IS level.700 seconds is the holddown-timer value for IGP to wait until LDP converges. The values level-1|level-2-only|level-1-2 identify the IS-IS level instance. The interface can be acting on any level, but the sync is applicable only when it matches with the level given in IGP sync command. **IS-IS:** This command is part of ISIS Process. **Default:** Mandatory configuration. No default option. Note: The holddown-timer Range is 1 to 2147483 seconds. If no holddown timer is configured, IGP waits indefinitely for LDP to Converge. Use the command mpls ldp-igp sync is-is <level-type> to configure without a holddown-timer.
`(config-if)#mpls ldp-igp sync-delay 55`	Set the time delay in seconds for the notification of LDP convergence to IGP. This is not applicable for notification of non-convergence. Range is 5 to 60 seconds. This command is optional. **LDP:** This command is part of LDP Process. **Default:** If not configured, the delay is 0 seconds.
`(config-if)#exit`	Exit interface mode.

LDP-IGP SYNC Configuration

Now that NSM, IS-IS and LDP are all enabled, the LDP-IGP synchronization can be configured.

RTR2

`(config)#interface xe11`	Enter interface mode.
`(config-if)#mpls ldp-igp sync isis level-1 holddown-timer 700`	Configure LDP-IGP Synchronization for interface xe11 belonging to an IS-IS process with corresponding IS-IS level.700 secs is the holddown-timer value for IGP to wait until LDP converges. The parameters level-1|level-2-only|level-1-2 identify the IS-IS instance level. The interface can be acting on any level, but sync is applicable only when it matches with the level given in IGP sync command. **IS-IS:** This command is part of IS-IS Process. **Default:** Mandatory configuration. No default option. Note: The holddown-timer Range is 1 to 2147483 seconds. If no holddown timer is configured, IGP waits indefinitely for LDP to Converge. Use command mpls ldp-igp sync is-is <level-type> to configure without a holddown-timer.

`(config-if)#mpls ldp-igp sync-delay 55`	Set the time delay in seconds for notification of LDP convergence to IGP. This is not applicable for notification of non-convergence. Range is 5 to 60 seconds. This command is optional. **LDP:** This command is part of LDP Process. **Default:** If not configured, the delay is 0 seconds.
`(config-if)#exit`	Exit interface mode.

RTR1 Validation

When LDP IGP SYNC is Configured with hold-down and sync-delay timer

```
R1#show isis interface xe11
xe11 is up, line protocol is up
  Routing Protocol: IS-IS (1)
    Network Type: Broadcast
    Circuit Type: level-1
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x0000271C
    Local SNPA: b86a.97d1.24d1
    IP interface address:
      10.10.10.1/24
    IPv6 interface address:
      fe80::ba6a:97ff:fed1:24d1/64
    LDP-ISIS Sync Configured
      Holddown timer = 700 seconds, Remaining time = 0 seconds
    Level-1 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0001.01
    Number of active level-1 adjacencies: 1
    Level-1 LSP MTU: 1492
    Next IS-IS LAN Level-1 Hello in 420 milliseconds
R1#

R1#show mpls ldp igp sync
xe11 is up, line protocol is up
  LDP configured; LDP-IGP Synchronization enabled.
  Session IP Address : 2.2.2.2
    Sync status: Achieved
    Delay timer: Configured, 55 seconds, Not Running
R1#
```

RTR2 Validation

```
R2#show  isis interface xe11
xe11 is up, line protocol is up
  Routing Protocol: IS-IS (1)
    Network Type: Broadcast
    Circuit Type: level-1
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x0000271B
    Local SNPA: 6cb9.c5cf.da69
    IP interface address:
      10.10.10.2/24
    IPv6 interface address:
      fe80::6eb9:c5ff:fecf:da69/64
```

```
    LDP-ISIS Sync Configured
      Holddown timer = 700 seconds, Remaining time = 0 seconds
    Level-1 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0001.01
    Number of active level-1 adjacencies: 1
    Level-1 LSP MTU: 1492
    Next IS-IS LAN Level-1 Hello in 4 seconds
R2#
R2#show mpls ldp igp sync
xe11 is up, line protocol is up
  LDP configured; LDP-IGP Synchronization enabled.
  Session IP Address : 1.1.1.1
    Sync status: Achieved
    Delay timer: Configured, 55 seconds, Not Running
```

CHAPTER 12 MPLS DiffServ Configuration

This chapter contains an overview of MPLS DiffServ functionality and terminology, MPLS DiffServ configuration example for a relevant scenario, configuration guidelines, and sample procedures for enabling and configuring MPLS DiffServ.

MPLS Diff-Serv Overview

The initial efforts to provide quality of service (QoS) in IP networks were based on a per application-Flow model (IntServ), in which individual applications requested QoS. With large number of flows traversing IP networks, this approach proved to be un-scalable and overly complex, and a more “coarse-grained” model was developed in the form of DiffServ. DiffServ approaches the problem of QoS by dividing traffic into a small number of classes and allocating network resources on a per-class basis. DiffServ provides differential forwarding treatment to traffic, thus enforcing QoS for different traffic flows. It is a scalable solution that does not require per flow signalling and state maintenance in the core. However, it cannot guarantee QoS if the path followed by the traffic does not have adequate resources to meet the QoS requirements.

DiffServ Tunnelling modes:

RFC 3270 has recommended three QoS models for DiffServ tunneled traffic in MPLS networks:

OcNOS supports two models:

- Pipe model (default mode): With the Pipe Model, MPLS tunnels (aka LSPs) are used to hide the intermediate MPLS nodes between LSP Ingress and Egress from the Diff-Serv perspective. In this model, tunneled packets must convey two meaningful pieces of Diff-Serv information:
  - The Diff-Serv information which is meaningful to intermediate nodes along the LSP span including the LSP Egress (which we refer to as the “LSP Diff-Serv Information”).This LSP Diff-Serv Information is not meaningful beyond the LSP Egress: Whether Traffic Conditioning at intermediate nodes on the LSP span affects the LSP Diff-Serv information or not, this updated Diff-Serv information is not considered meaningful beyond the LSP Egress and is ignored.
  - The Diff-Serv information which is meaningful beyond the LSP Egress (which we refer to as the “Tunneled Diff-Serv Information”).This information is to be conveyed by the LSP Ingress to the LSP Egress.This Diff-Serv information is not meaningful to the intermediate nodes on the LSP span.
- Uniform model: With the Uniform Model, MPLS tunnels (aka LSPs) are viewed as artifacts of the end-to-end path from the Diff-Serv standpoint. MPLS Tunnels may be used for forwarding purposes but have no significant impact on Diff-Serv. In this model, any packet contains exactly one piece of Diff-Serv information which is meaningful and is always encoded in the outer most label entry (or in the IP DSCP where the IP packet is transmitted unlabeled for instance at the egress of the LSP). Any Diff-Serv information encoded somewhere else (e.g., in deeper label entries) is of no significance to intermediate nodes or to the tunnel egress and is ignored. If Traffic Conditioning at intermediate nodes on the LSP span affects the “outer” Diff-Serv information, the updated Diff-Serv information is the one considered meaningful at the egress of the LSP.
  - The Uniform Model for Diff-Serv over MPLS is such that, from the Diff-Serv perspective, operations are exactly identical to the operations if MPLS was not used. In other words, MPLS is entirely transparent to the Diff-Serv operations.
  - Use of the Uniform Model allows LSPs to span Diff-Serv domain boundaries without any other measure in place than an inter-domain Traffic Conditioning Agreement at the physical boundary between the Diff-Serv domains and operating exclusively on the “outer” header, since the meaningful Diff-Serv information is always visible and modifiable in the outmost label entry.

Terminology

Following is a brief description of terms and concepts used to describe MPLS Diffserv.

EXP Value

The MPLS experimental bits (EXP) field is a 3-bit field in the MPLS header that you can use to define the QoS treatment (per-hop behavior) that a node should give to a packet. In an IP network, the DiffServ Code Point (DSCP) (a 6-bit field) defines a class and drop precedence. The EXP bits can be used to carry some of the information encoded in the IP DSCP and can also be used to encode the dropping precedence.

By default, OcNOS copies the three most significant bits of the DSCP or the IP precedence of the IP packet to the EXP field in the MPLS header. This action happens when the MPLS header is initially imposed on the IP packet. However, you can also set the EXP field by defining a mapping between the DSCP or IP precedence and the EXP bits. This mapping is configured using the set mpls class command in pmap-class mode or qos map class exp in global mode. For more information, see the “Remarking” section.

DSCP Value

Differentiated Services Code Point (DSCP) is a 6-bit value used to classify the priority of Layer-3 packets upon entry into a network. DSCP values range from 0 to 63, 63 being the highest priority, 0 being best-effort traffic.

Classification

Traffic classification allows the network to recognize traffic as it falls into classes that you have configured. Network traffic must be classified to apply specific QoS to it. Classification can be inclusive (for example, all of the traffic passing through an interface) or classification can be very specific (for example, you can use a class map with match commands that recognize specific aspects of the traffic). You can classify and apply QoS (for example, marking) and then, on another interface or network device, classify again based on the marked value and apply other QoS.

Policing

Policing determines whether a packet is in or out of profile by comparing the internal DSCP to the configured policer. Policer limits the bandwidth consumed by a traffic flow with the results given to the marker.

Policing and policers have the following attributes:

- Policers can occur only on a physical port basis.
- Policing can occur on ingress interfaces.
- Only one policer can be applied to a packet per direction.

Marking

Marking determines how to handle a packet when it is out of profile. It assesses the policer and the configuration data to determine the action required for the packet, and then handles the packet using one of the following methods:

- Let the packet through without modification
- Drop the packet

Marking can occur on ingress and egress interfaces.

Class Map

A class map names and isolates specific traffic from other traffic. The class map defines the criteria used to match against a specific traffic flow to classify it further. The criteria can include:

- Matching the access group defined by the ACL
- Matching a specific list of DSCP values

If there is more than one type of traffic to be classified, another class map can be created under a different name. After a packet is matched against the class-map criteria, it is further classified using a policy map.

Policy Map

A policy map specifies on which traffic class to act. This can be implemented as follows:

- Set a specific CoS or DSCP value in the traffic class.
- Specify the traffic bandwidth limitations for each matched traffic class (policer) and the action to take (marking) when the traffic is out of profile.

Policy maps have the following attributes:

- A policy map can contain multiple class statements, each with different match criteria and policers.
- A separate policy-map class can exist for each type of traffic received through an interface.
- There can be only one policy map per interface per direction. The same policy map can be applied to multiple interfaces and directions.
- Before a policy map can be effective, it must be attached to an interface.

MPLS Class

MPLS class or class specifies the class of the frames, for example frames with DSCP 0-7 belongs to class 0, DSCP 8-15 belongs to Class 1, and so on.

In OcNOS, there are 8 classes varying form 0-7. By default, EXP to class is mapped one-to-one.

For more, see Table 12-1

For MPLS Diff-Serv to work, QoS must be enabled at the global level. By default QoS is disabled.

Table 12-1: EXP to class mapping

CoS	DSCP	EXP	Class	Queue
0	0-7	0	0	0
1	8-15	1	1	1
2	16-23	2	2	2
3	24-31	3	3	3
4	32-39	4	4	4
5	40-47	5	5	5
6	48-55	6	6	6
7	56-63	7	7	7

CHAPTER 13 Remarking Configuration

This chapter contains a complete sample of configuring Remarking of EXP bits on interface and global level along with LDP LSP for Pipe model and Uniform model.

Configuration

Configuring Remarking for MPLS EXP bits require following configurations:

- Enabling label-switching on the interface on NSM.
- Configuring LSP (Using LDP, Static or RSVP-TE, in this example we are using LDP for setting UP LSP).
- Running an IGP (Internal Gateway Protocol), for example, OSPF, to distribute reachability information within the MPLS cloud.
- Enable QoS, Configuring Remarking on interface and Global Level.

Topology

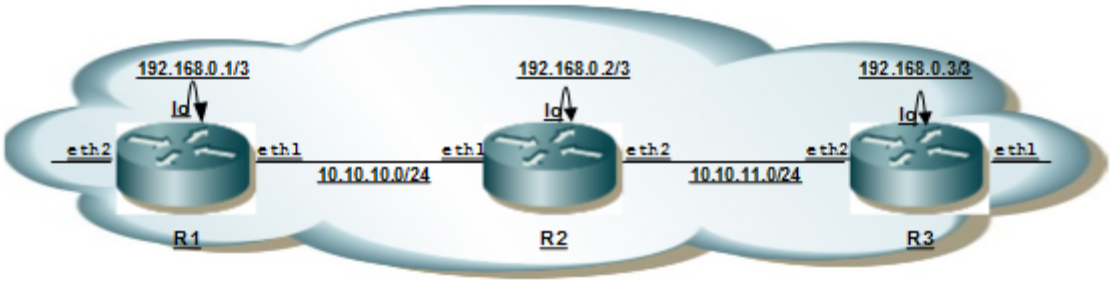


Figure 13-24: Basic LDP Topology

OSPF and LDP Configuration for R1, R2 and R3

R1

NSM

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Specify the interface `(eth1)` to be configured.
`(config-if)#ip address 10.10.10.1/24`	Configure IP address for the interface
`(config-if)#label-switching`	Enable label switching on interface `eth1`.
`(config-if)#exit`	Exit interface mode.
`(config)#interface lo`	Specify the loopback (`lo`) interface to be configured.
`(config-if)#ip address 192.168.0.1/32`	Set the IP address of the loopback interface to `192.168.0.1/32`

OSPF

`#configure terminal`	Enter configure mode.
`(config)#router ospf 100`	Configure the routing process and specify the Process ID (100). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0` `(config-router)#network 192.168.0.1/32 area 0`	Define the interface on which OSPF runs and associate the area ID (0) with the interface.
`(config-router)#exit`	Exit from router mode

LDP

`#configure terminal`	Enter configure mode.
`(config)#router ldp`	Enter Router mode for LDP.
`(config-router)#router-id 192.168.0.1`	Set the router ID to IP address 192.168.0.1.
`(config-router)#transport-address ipv4 192.168.0.1`	Configure the transport address to be used for a TCP session over which LDP will run on an IPv4 interface. Note: It is preferable to use the loopback address as transport address.
`(config-router)#exit`	Exit router mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#enable-ldp ipv4`	Enable LDP on eth1.
`(config-if)#exit`	Exit interface mode.

R2

NSM

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Specify the interface `(eth1)` to be configured.
`(config-if)#ip address 10.10.10.2/24`	Configure IP address for the interface
`(config-if)#label-switching`	Enable label switching on interface `eth1`.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Specify the interface `(eth2)` to be configured.
`(config-if)#ip address 10.10.11.1/24`	Configure IP address for the interface
`(config-if)#label-switching`	Enable label switching on interface `eth1`.
`(config-if)#exit`	Exit interface mode.
`(config)#interface lo`	Specify the loopback (`lo`) interface to be configured.
`(config-if)#ip address 192.168.0.2/32`	Set the IP address of the loopback interface to `192.168.0.2/32`
`(config-if)#exit`	Exit interface mode.

OSPF

`#configure terminal`	Enter configure mode.
`(config)#router ospf 100`	Configure the routing process and specify the Process ID (100). The Process ID should be a unique positive integer identifying the routing process.

`(config-router)#network 10.10.10.0/24 area 0`
`(config-router)#network 10.10.11.0/24 area 0`
`(config-router)#network 192.168.0.2/32 area 0`
	Define the interface on which OSPF runs and associate the area ID (0) with the interface.

`(config-router)#exit`	Exit from router mode

LDP

`#configure terminal`	Enter configure mode.
`(config)#router ldp`	Enter Router mode for LDP.
`(config-router)#router-id 192.168.0.2`	Set the router ID to IP address 192.168.0.2.
`(config-router)#transport-address ipv4 192.168.0.2`	Configure the transport address to be used for a TCP session over which LDP will run on an IPv4 interface. Note: It is preferable to use the loopback address as transport address.
`(config-router)#exit`	Exit router mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#enable-ldp ipv4`	Enable LDP on eth1.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#enable-ldp ipv4`	Enable LDP on eth2.
`(config-if)#exit`	Exit interface mode.

R3

NSM

`#configure terminal`	Enter configure mode.
`(config)#interface eth2`	Specify the interface `(eth2)` to be configured.
`(config-if)#ip address 10.10.11.2/24`	Configure IP address for the interface
`(config-if)#label-switching`	Enable label switching on interface `eth1`.
`(config-if)#exit`	Exit interface mode.
`(config)#interface lo`	Specify the loopback (`lo`) interface to be configured.
`(config-if)#ip address 192.168.0.3/32`	Set the IP address of the loopback interface to `192.168.0.3/32`

OSPF

`#configure terminal`	Enter configure mode.
`(config)#router ospf 100`	Configure the routing process and specify the Process ID (100). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.11.0/24 area 0` `(config-router)#network 192.168.0.3/32 area 0`	Define the interface on which OSPF runs and associate the area ID (0) with the interface.
`(config-router)#exit`	Exit from router mode

LDP

`#configure terminal`	Enter configure mode.
`(config)#router ldp`	Enter Router mode for LDP.
`(config-router)#router-id 192.168.0.3`	Set the router ID to IP address 192.168.0.3.
`(config-router)#explicit-null`	To disable PHP.
`(config-router)#transport-address ipv4 192.168.0.3`	Configure the transport address to be used for a TCP session over which LDP will run on an IPv4 interface. Note: It is preferable to use the loopback address as transport address.
`(config-router)#exit`	Exit `router` mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#enable-ldp ipv4`	Enable LDP on eth2.
`(config-if)#exit`	Exit interface mode.

Configuration of Marking or Remarking

Marking/Remarking can be done in Global level and in Interface level. Both methods are shown in the following sample configurations.

Global level configuration for R2

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QOS.
`(config)#qos statistics`	Enable QOS statistics.
`(config)#qos map exp 5 class 7`	Map exp value 5 to Class 7.

Validation

R2:

```
#show mpls diffserv
```

```
MPLS Differentiated Services EXP to CLASS mapping data:
 exp 0 class 0
 exp 1 class 1
 exp 2 class 2
 exp 3 class 3
 exp 4 class 4
 exp 5 class 7
 exp 6 class 6
 exp 7 class 7

MPLS Differentiated Services CLASS to EXP mapping data:
 class 0 exp 0
 class 1 exp 1
 class 2 exp 2
 class 3 exp 3
 class 4 exp 4
 class 5 exp 5
 class 6 exp 6
 class 7 exp 7
```

Interface level configuration for R2

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QOS.
`(config)#qos statistics`	Enable QOS statistics.
`(config)#mpls lsp-model uniform`	To change the lsp model to Uniform.
`(config)#class-map cmap2`	Enter Class-map mode
`(config-class-qos)#match mpls experimental topmost 5`	Configure match EXP as EXP with Value 5
`(config-class-qos)#exit`	Exit Class-map mode
`(config)#policy-map pmap2`	Enter policy-map mode
`(config-pmap-qos)#class cmap2`	Assign Class cmap1 to Policy-map pmap1
`(config-pmap-c-qos)#set mpls class 7`	Remark EXP from EXP 2 to class 7
`(config-pmap-c-qos)#exit`	Exit out of policy-class-map mode
`(config-pmap-qos)#exit`	Exit out of Policy-map mode
`(config)#interface eth1`	Enter eth1 interface
`(config-if)#service-policy type qos input pmap2`	Assign service-policy to interface on in-direction
`(config-if)#exit`	Exit interface mode.

Validation:

```
R2#show class-map

  Type qos class-maps
  ===================
```

```
        class-map type qos match-any class-default

        class-map cmap2
           match mpls experimental topmost 5

  Type queuing class-maps
  =======================
        class-map match-any q0

        class-map match-any q1

        class-map match-any q2

        class-map match-any q3

        class-map match-any q4

        class-map match-any q5

        class-map match-any q6

        class-map match-any q7

  Type Vlan-Queuing class-maps
  ============================

R2#show policy-map

Type qos policy-maps
====================

policy-map pmap2
 class cmap2
  set mpls class 7
  exit


Type queuing policy-maps
========================

policy-map type queuing default default-out-policy
 class type queuing default q0
  priority level 1
  exit
 class type queuing default q1
  priority level 1
  exit
 class type queuing default q2
  priority level 1
  exit
 class type queuing default q3
  priority level 1
  exit
 class type queuing default q4
  priority level 1
  exit
 class type queuing default q5
```

```
  priority level 1
  exit
 class type queuing default q6
  priority level 1
  exit
 class type queuing default q7
  priority level 1
  exit


R2#show running-config qos
qos enable
!
qos map exp 5 class 7
qos statistics
!
class-map cmap2
 match mpls experimental topmost 5
!
policy-map pmap2
 class cmap2
  set mpls class 7
  exit
!
interface ce10/1
 service-policy type qos input pmap2
!

#show mpls diffserv

MPLS Differentiated Services EXP to CLASS mapping data:
 exp 0 class 0
 exp 1 class 1
 exp 2 class 2
 exp 3 class 3
 exp 4 class 4
 exp 5 class 7
 exp 6 class 6
 exp 7 class 7

MPLS Differentiated Services CLASS to EXP mapping data:
 class 0 exp 0
 class 1 exp 1
 class 2 exp 2
 class 3 exp 3
 class 4 exp 4
 class 5 exp 5
 class 6 exp 6
 class 7 exp 7

R2# show policy-map interface eth2

Global statistics status : enabled

Service-policy (queuing) output: default-out-policy
-----------------------------------
Class-map (queuing): q0
```

```
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q1
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q2
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q3
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q4
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q5
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q6
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q7
 priority level 1
      output       : 22993 packets, 1563572 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
```

```
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 35 packets, 2872 bytes
      dropped      : 0 packets, 0 bytes

Wred Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets


R2#
```

CHAPTER 14 Policing Configuration

This chapter contains a complete sample of configuration of Policing for Pipe and Uniform models.This example shows configurations using LDP.

Configuration

Configuring Remarking for MPLS EXP bits require following configurations:

- Enabling label-switching on the interface on NSM.
- Configuring LSP (Using LDP, Static or RSVP-TE, in this example we are using LDP for setting UP LSP).
- Running an IGP (Internal Gateway Protocol), for example, OSPF, to distribute reachability information within the MPLS cloud.
- Enable QoS, Configuring Policing on interface Level.

Topology

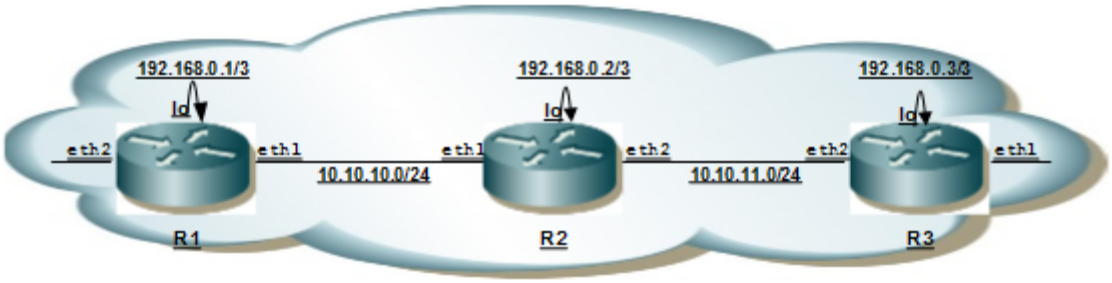


Figure 14-25: Basic Policing Topology

R1

The following steps describes how to configure Policing.

Note: Basic configuration for Policing is same as that of the configurations given in Remarking chapter

`(config)#class-map cmap1`	Enter Class-map mode
`(config-cmap-qos)#match dscp 2`	Configure match criteria as DSCP with Value 2
`(config-cmap-qos)#exit`	Exit Class-map mode
`(config)#policy-map pmap1`	Enter policy-map mode
`(config-pmap-qos)#class cmap1`	Assign Class cmap1 to Policy-map pmap1
`(config-pmap-c-qos)#police cir 1 mbps conform set-mpls-class 6 violate drop`	Police DSCP 2 packets @ Committed information rate 1 mbps, and map DSCP 2 to class 6.
`(config-pmap-c-qos)#exit`	Exit out of policy-class-map mode
`(config-pmap-qos)#exit`	Exit out of Policy-map mode
`(config)#interface eth2`	Enter eth0 interface
`(config-if)#service-policy type qos input pmap1`	Assign service-policy to interface on in-direction
`(config-if)#exit`	Exit interface mode.

Validation

```
R1#show class-map

  Type qos class-maps
  ===================
      class-map type qos match-any class-default

      class-map cmap1
         match dscp 2


  Type queuing class-maps
  =======================
      class-map match-any q0

      class-map match-any q1

      class-map match-any q2

      class-map match-any q3

      class-map match-any q4

      class-map match-any q5

      class-map match-any q6

      class-map match-any q7


  Type Vlan-Queuing class-maps
  ============================


#show running-config qos
qos enable
!
qos statistics
!
class-map cmap1
 match dscp 2
!
policy-map pmap1
 class cmap1
  police cir 1 mbps conform set-mpls-class 6 violate drop
  exit
!
interface eth2
 service-policy type qos input pmap1 exit
#

#show policy-map

Type qos policy-maps
====================
```

```
policy-map pmap1
 class cmap1
  police cir 1 mbps conform set-mpls-class 6 violate drop
  exit


Type queuing policy-maps
========================

policy-map type queuing default default-out-policy
 class type queuing default q0
  priority level 1
  exit
 class type queuing default q1
  priority level 1
  exit
 class type queuing default q2
  priority level 1
  exit
 class type queuing default q3
  priority level 1
  exit
 class type queuing default q4
  priority level 1
  exit
 class type queuing default q5
  priority level 1
  exit
 class type queuing default q6
  priority level 1
  exit
 class type queuing default q7
  priority level 1
  exit


#show policy-map interface eth1

Interface eth1
Global statistics status : enabled

Service-policy (queuing) output: default-out-policy
---------------------------------
Class-map (queuing): q0
 priority level 1
      output       : 5 packets, 340 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q1
 priority level 1
      output       : 25 packets, 2208 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q2
 priority level 1
      output       : 0 packets, 0 bytes
```

```
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q3
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q4
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q5
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q6
 priority level 1
      output       : 46337 packets, 3150916 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q7
 priority level 1
      output       : 346 packets, 25193 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 808 packets, 67946 bytes
```

```
      dropped      : 0 packets, 0 bytes

Wred Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets
```

CHAPTER 15 MPLS Statistics Configuration

This chapter provides the configuration required for configuring MPLS LSPs and verifying the statistics of packets captured at the supported interfaces, in terms of both packet count and bytes, when traffic is sent.

Configure LDP-LSP

Topology

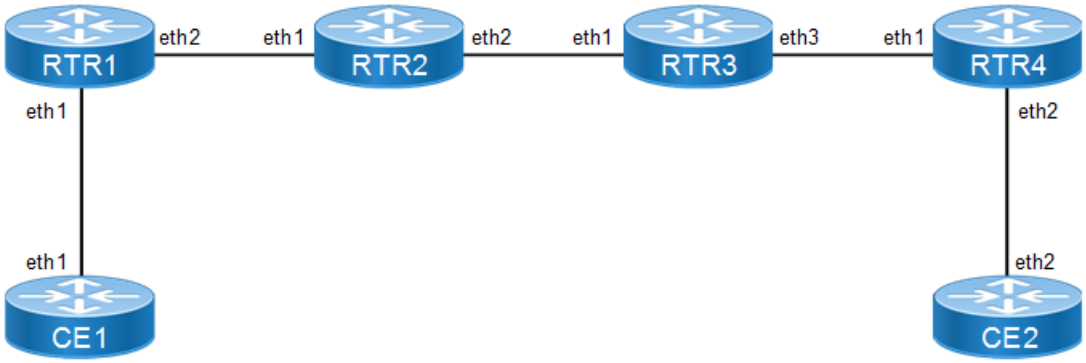


Figure 15-26: MPLS Statistics Topology

RTR1

Loopback Interface configuration

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Specify the interface `(lo)` to be configured.
`(config-if)#ip address 11.11.11.11/32 secondary`	Configure IP address on loopback interface
`(config-if)#exit`	Exit interface mode.

Global LDP configuration

`(config)#router ldp`	Enter `Router` mode for LDP.
`(config-router)#transport-address ipv4 11.11.11.11`	Configure the loopback address as transport-address
`(config-router)#targeted-peer ipv4 44.44.44.44`	Configure the loopback address of RTR4 as targeted peer.
`(config-router-targeted-peer)#exit`	Exit router-targeted-peer mode and enter config-router mode
`(config-router)#end`	Exit router and configure mode

Enabling LDP and label switching on interface

`#configure terminal`	Enter configure mode.
`(config)#interface eth2`	Enter interface mode for eth2.
`(config-if)#enable-ldp ipv4`	Enable LDP on the interface.
`(config-if)#label-switching`	Enable Label switching on the interface.
`(config-if)#ip address 10.10.10.1/24`	Configure IP address on the interface.
`(config-if)#exit`	Exit interface mode.

Global OSPF configuration

`(config)#router ospf 100`	Enter the Router OSPF mode.
`(config-router)#network 11.11.11.11/32 area 0`	Advertise loopback address in OSPF.
`(config-router)#network 10.10.10.0/24 area 0`	Advertise network address (eth2) in OSPF.
`(config-router)#exit`	Exit Router OSPF mode and return to Configure mode.

RTR2

Loopback Interface configuration

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Specify the interface `(lo)` to be configured.
`(config-if)#ip address 22.22.22.22/32 secondary`	Configure IP address on loopback interface
`(config-if)#exit`	Exit interface mode.

Global LDP configuration

`(config)#router ldp`	Enter `Router` mode for LDP.
`(config-router)#transport-address ipv4 22.22.22.22`	Configure the loopback address as transport-address
`(config-router)#end`	Exit router and configure mode

Enabling LDP and label switching on interface

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode for eth1.
`(config-if)#enable-ldp ipv4`	Enable LDP on the interface.
`(config-if)#label-switching`	Enable Label switching on the interface.
`(config-if)#ip address 10.10.10.2/24`	Configure IP address on the interface.
`(config-if)#exit`	Exit interface mode.

(config)#interface eth2	Enter interface mode for eth2.
(config-if)#enable-ldp ipv4	Enable LDP on the interface.
(config-if)#label-switching	Enable Label switching on the interface.
(config-if)#ip address 20.20.20.1/24	Configure IP address on the interface.
(config-if)#exit	Exit interface mode.

OSPF Configuration

(config)#router ospf 100	Enter the Router OSPF mode
(config-router)#network 22.22.22.22/32 area 0.0.0.0	Advertise loopback address in OSPF
(config-router)#network 10.10.10.2/24 area 0.0.0.0	Advertise network address (eth1) in OSPF.
(config-router)#network 20.20.20.1/24 area 0.0.0.0	Advertise network address (eth2) in OSPF.
(config-router)#exit	Exit OSPF router configuration mode.

RTR3

Loopback Interface configuration

#configure terminal	Enter configure mode.
(config)#interface lo	Specify the interface (lo) to be configured.
(config-if)#ip address 33.33.33.33/32 secondary	Configure IP address on loopback interface
(config-if)#exit	Exit interface mode.

Global LDP configuration

(config)#router ldp	Enter Router mode for LDP.
(config-router)#transport-address ipv4 33.33.33.33	Configure the loopback address as transport-address
(config-router)#end	Exit router and configure mode

Enabling LDP and label switching on interface

#configure terminal	Enter configure mode.
(config)#interface eth1	Enter interface mode for eth1.
(config-if)#enable-ldp ipv4	Enable LDP on the interface.
(config-if)#label-switching	Enable Label switching on the interface.
(config-if)#ip address 20.20.20.2/24	Configure IP address on the interface.
(config-if)#exit	Exit interface mode.

(config)#interface eth2	Enter interface mode for eth2.
(config-if)#enable-ldp ipv4	Enable LDP on the interface.
(config-if)#label-switching	Enable Label switching on the interface.
(config-if)#ip address 30.30.30.1/24	Configure IP address on the interface.
(config-if)#exit	Exit interface mode.

OSPF Configuration

(config)#router ospf 100	Enter the Router OSPF mode
(config-router)#network 33.33.33.33/32 area 0.0.0.0	Advertise loopback address in OSPF
(config-router)#network 20.20.20.2/24 area 0.0.0.0	Advertise network address (eth1) in OSPF.
(config-router)#network 30.30.30.1/24 area 0.0.0.0	Advertise network address (eth2) in OSPF.
(config-router)#exit	Exit OSPF router configuration mode.

RTR4

Loopback Interface configuration

#configure terminal	Enter configure mode.
(config)#interface lo	Specify the interface (lo) to be configured.
(config-if)#ip address 44.44.44.44/32 secondary	Configure IP address on loopback interface
(config-if)#exit	Exit interface mode.

Global LDP configuration

(config)#router ldp	Enter Router mode for LDP.
(config-router)#transport-address ipv4 44.44.44.44	Configure the loopback address as transport-address
(config-router)#targeted-peer ipv4 11.11.11.11	Configure the loopback address of RTR1 as targeted peer.
(config-router-targeted-peer)#exit	Exit router-targeted-peer mode and enter config-router mode
(config-router)#end	Exit router and configure mode

Enabling LDP and label switching on interface

#configure terminal	Enter configure mode.
(config)#interface eth1	Enter interface mode for eth1.

(config-if)#enable-ldp ipv4	Enable LDP on the interface.
(config-if)#label-switching	Enable Label switching on the interface.
(config-if)#ip address 30.30.30.2/24	Configure IP address on the interface.
(config-if)#exit	Exit interface mode.

Global OSPF Configuration

(config)#router ospf 100	Enter the Router OSPF mode
(config-router)#network 44.44.44.44/32 area 0.0.0.0	Advertise loopback address in OSPF
(config-router)#network 30.30.30.2/24 area 0.0.0.0	Advertise network address (eth1) in OSPF.
(config-router)#exit	Exit OSPF router configuration mode.

Virtual Circuit Configuration

RTR1

Global VC Configuration

(config)#mpls l2-circuit t1 100 44.44.44.44	Enter the VC configuration command in router mode.
(config)#bridge 1 protocol ieee vlan-bridge	Creating a VLAN-bridge in router mode.

Interface Configuration

(config)#service-template st1	Template configuration
(config-svc)#exit	Exit service template configuration
(config)#interface eth1	Enter interface mode for eth1.
(config-if)#switchport	Enable switchport on the interface.
(config-if)#mpls-l2-circuit t1 service-template st1	Bind the interface to VC created in ethernet mode.
(config-if)#exit	Exit interface mode.

RTR4

Global VC Configuration

(config)#mpls l2-circuit t1 100 11.11.11.11	Enter the VC configuration command in router mode.
(config)#bridge 1 protocol ieee vlan-bridge	Creating a VLAN-bridge in router mode.

Interface Configuration

(config)#service-template st1	Template configuration
(config-svc)#exit	Exit service template mode
(config)#interface eth2	Enter interface mode for eth2.

(config-if)#switchport	Enable switchport on the interface.
(config-if)#mpls-l2-circuit t1 service-template st1	Bind the interface to VC created in ethernet mode.
(config-if)#exit	Exit interface mode.

Configure Static-LSP

RTR1

Global Static configuration

(config)#mpls ftn-entry 44.44.44.44/32 100 10.10.10.2 eth2	Configure FTN entry for rtr4 loopback.
(config)#mpls ilm-entry 900 pop	Pop the incoming label

Enabling label switching on interface

(config)#interface eth2	Enter interface mode for eth2.
(config-if)#label-switching	Enable Label switching on the interface.
(config-if)#exit	Exit interface mode.

RTR2

Global Static configuration

mpls ilm-entry 100 swap 200 eth2 20.20.20.2 44.44.44.44/32	Swap the incoming label
mpls ilm-entry 800 swap 900 eth1 10.10.10.1 11.11.11.11/32	Swap the incoming label

Enabling label switching on interface

(config)#interface eth1	Enter interface mode for eth1.
(config-if)#label-switching	Enable Label switching on the interface.
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode for eth2.
(config-if)#label-switching	Enable Label switching on the interface.
(config-if)#exit	Exit interface mode.

RTR3

Global Static configuration

(config)#mpls ilm-entry 200 swap 300 eth2 30.30.30.2 44.44.44.44/32	Swap the incoming label
(config)#mpls ilm-entry 700 swap 800 eth1 20.20.20.1 11.11.11.11/32	Swap the incoming label

Enabling label switching on interface

(config)#interface eth1	Enter interface mode for eth1.
(config-if)#label-switching	Enable Label switching on the interface.
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode for eth2.
(config-if)#label-switching	Enable Label switching on the interface.
(config-if)#exit	Exit interface mode.

RTR4

Global Static configuration

(config)#mpls ftn-entry 11.11.11.11/32 700 30.30.30.1 eth1	Configure FTN entry for RTR1 loopback.
(config)mpls ilm-entry 300 pop	Pop the incoming label.

Enabling label switching on interface

(config)#interface eth1	Enter interface mode for eth1.
(config-if)#label-switching	Enable Label switching on the interface.
(config-if)#exit	Exit interface mode.

Validation

Here, 1000 packets are transmitted between the PE nodes and the output of counters at each node is mentioned below.

For Static-LSP

```
RTR1#show mpls counters static
[FTN statistics]
+------------------+-----------+--------------------+--------------------+
|       FEC        | out-label |     Tx packets     |      Tx bytes      |
+------------------+-----------+--------------------+--------------------+
 44.44.44.44/32     100         49939                807798
[ILM statistics]
+------------------+-----------+-----------+--------------------+-------------
-------+--------------------+--------------------+
|       FEC        | in-label  | out-label |     Rx packets     |      Rx
bytes      |     Tx packets     |      Tx bytes      |
```

```
+------------------+-----------+-----------+--------------------+------------
-------+--------------------+--------------------+
 0.0.0.0/0         900         n/a         40546               3486956
n/a                  n/a
RTR1#


RTR2#show mpls counters static
[FTN statistics]
+------------------+-----------+--------------------+--------------------+
|       FEC        | out-label |     Tx packets     |      Tx bytes      |
+------------------+-----------+--------------------+--------------------+

[ILM statistics]
+------------------+-----------+-----------+--------------------+------------
--
-----+--------------------+--------------------+
|       FEC        | in-label  | out-label |     Rx packets     |      Rx
bytes
     |     Tx packets     |      Tx bytes      |
+------------------+-----------+-----------+--------------------+------------
--
-----+--------------------+--------------------+
 44.44.44.44/32     100         200         9393                 807798
      9393                 807798
 11.11.11.11/32     800         900         40546                3486956
      40546                3486956
RTR2#


RTR3#show mpls counters static
[FTN statistics]
+------------------+-----------+--------------------+--------------------+
|       FEC        | out-label |     Tx packets     |      Tx bytes      |
+------------------+-----------+--------------------+--------------------+

[ILM statistics]
+------------------+-----------+-----------+--------------------+------------
-------+--------------------+--------------------+
|       FEC        | in-label  | out-label |     Rx packets     |      Rx
bytes      |     Tx packets     |      Tx bytes      |
+------------------+-----------+-----------+--------------------+------------
-------+--------------------+--------------------+
 44.44.44.44/32     200         300         9393                 807798
9393                   807798
 11.11.11.11/32     700         800         40546                3486956
40546                  3486956
RTR3#


RTR4#show mpls counters static
[FTN statistics]
+------------------+-----------+--------------------+--------------------+
|       FEC        | out-label |     Tx packets     |      Tx bytes      |
+------------------+-----------+--------------------+--------------------+
 11.11.11.11/32     700         49939                3486956

[ILM statistics]
```

```
+------------------+-----------+-----------+--------------------+------------
--
-----+--------------------+--------------------+
|       FEC        | in-label  | out-label |     Rx packets     |      Rx
bytes
     |     Tx packets     |      Tx bytes      |
+------------------+-----------+-----------+--------------------+------------
--
-----+--------------------+--------------------+
 0.0.0.0/0          300         n/a         9393                  807798
      n/a                  n/a
RTR4#
```

For LDP-LSP

```
RTR1#show mpls counters ldp
[FTN statistics]
+------------------+-----------+--------------------+--------------------+
|       FEC          | out-label |   Tx packets     |      Tx bytes      |
+------------------+-------------+------------------+--------------------+
 44.44.44.44/32     52483          1000                1004000
[ILM statistics]
+-----+---------+-----------+------------+---------+-----------+---------+
| FEC |in-label | out-label | Rx packets | Rx bytes| Tx packets| Tx bytes|
+-----+---------+-----------+------------+---------+-----------+---------+

RTR2#show mpls counters ldp
[FTN statistics]
+------------------+-----------+--------------------+--------------------+
|       FEC        | out-label |     Tx packets     |      Tx bytes      |
+------------------+-----------+--------------------+--------------------+
[ILM statistics]
+-----+----------+-----------+------------+----------+------------+----------+
| FEC | in-label | out-label | Rx packets | Rx bytes | Tx packets | Tx bytes |
+-----+----------+-----------+------------+----------+------------+----------+
44.44.44.44/32     52483   52483  1000        1004000   1000         1004000
```

For LDP-VC

```
R1#show mpls l2-circuit t1 statistics
MPLS Layer-2 Virtual Circuit: t1, id 100
 Access port statistics:
   RX:  Input packets  : 0
        Input bytes    : 0
   TX:  Output packets : 4642811
        Output bytes   : 297139904

 Network port statistics:
   RX:  Input packets  : 4642804
        Input bytes    : 399281144
   TX:  Output packets : 0
        Output bytes   : 0


R4#show mpls l2-circuit t1 statistics
MPLS Layer-2 Virtual Circuit: t1, id 100
```

```
Access port statistics:
  RX:  Input packets  : 4633957
       Input bytes    : 296573248
  TX:  Output packets : 0
       Output bytes   : 0

Network port statistics:
  RX:  Input packets  : 0
       Input bytes    : 0
  TX:  Output packets : 4633960
       Output bytes   : 398520560
```

CHAPTER 16 Inter-AS VPN Configuration Overview

MPLS VPN architecture typically runs within an AS. Routes of any VPN can be flooded within the AS, but not to other ASs. To implement the exchange of VPN routes between different ASs, the inter-AS MPLS VPN model is used. The inter-AS MPLS VPN model is an extension to MPLS VPN framework. Route prefixes and labels can be advertised over links between different carrier networks through the inter-AS MPLS model.

The MPLS VPN solution serves an increasing number of users across many applications. A site at one geographical location often needs to connect to an ISP network at another geographical location. In this situation, for example, inter-AS issues may arise for operators who manage different metropolitan area networks (MANs) or backbone networks that span different autonomous systems (AS).

Types of Inter-AS VPN

1. Inter-AS VPN Option A: Autonomous system boundary routers (ASBRs) manage VPN routes for in-ter-AS VPNs through dedicated interfaces.
2. Inter-AS VPN Option B: ASBRs advertise labeled VPN-IPv4 routes to each other through MP-EBGP.
3. Inter-AS VPN Option C: PE devices advertise labeled VPN-IPv4 routes to each other through Mul-ti-hop MP-EBGP.

CHAPTER 17 Inter-AS VPN Option-A Configuration

This chapter explain about Inter-AS VPN Option-A. Option A is the simplest of the options to inter-connect the ASBRs Option A has the following characteristics:

- Each customer VRF requires either a physical interface or more likely a subinterface.
- Each ASBR thinks the other is a CE.
- One logical interface per VPN.
- Link may use any supported PE-CE protocol.
- Packets are sent unlabelled between the ASBRs.
- The most secure and easy option to provision.
- Does not scale well to a large number of VPNs.

Topology

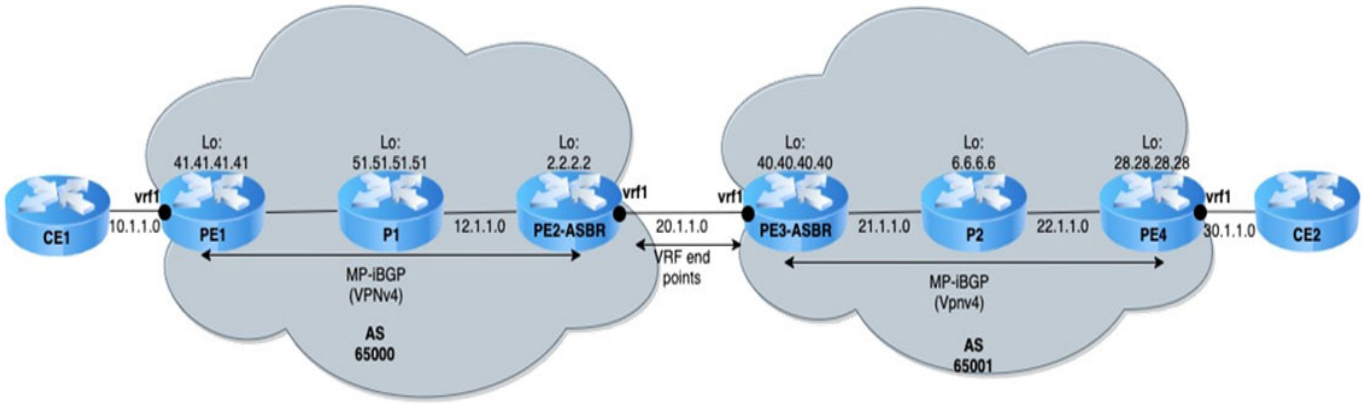


Figure 17-27: InterAS-VPN Option-A

PE1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode.
`(config-if)#ip address 2.2.2.2/32 secondary`	Assign the IPv4 address.
`(config-if)#exit`	Exit interface mode.
`(config)#ip vrf vrf1`	Create a new VRF named vrf1.
`(config-vrf)#rd 1:1`	Assign the route distinguisher (RD) value as 1:1.
`(config-vrf)#route-target both 1:1`	Import routes between route target (RT) ext-communities.
`(config-vrf)#exit`	Exit interface mode.
`(config)#interface xe22`	Enter interface mode.

(config-if)#ip vrf forwarding vrf1	Bind the interface connected to the CE router with VRF vrf1
(config-if)#ip address 10.1.1.2/24	Assign the IPv4 address.
(config-if)#exit	Exit interface mode
(config)#interface xe20	Enter interface mode
(config-if)#ip address 11.1.1.2/24	Assign the IPv4 address.
(config-if)#exit	Exit interface mode
(config)#router ospf 1	Enter router OSPF mode.
(config-router)#ospf router-id 2.2.2.2	Configure OSPF router id same as loopback ip address.
(config-router)#network 2.2.2.2/32 area 0	Define the network on which OSPF runs and associate area id.
(config-router)#network 11.1.1.0/24 area 0	Define the network on which OSPF runs and associate area id.
(config-router)#exit	Exit OSPF router mode.
(config)#router ldp	Enter router LDP mode.
(config-router)#transport-address ipv4 2.2.2.2	Configure LDP transport address same as loopback address.
(config-router)#exit	Exit LDP mode.
(config)#interface xe20	Enter interface mode.
(config-if)#label-switching	Enable label switching in interface.
(config-if)#enable-ldp ipv4	Enable LDP in interface.
(config-if)#exit	Exit interface mode.
(config)#router bgp 65000	Enter BGP router mode.
(config-router)#bgp router-id 2.2.2.2	Configure BGP router-id.
(config-router)#neighbor 41.41.41.41 remote-as 65000	Configure PE2-ASBR1 as an iBGP peer.
(config-router)#neighbor 41.41.41.41 update-source lo	Update the source as loopback for iBGP peering with the remote PE2 router.
(config-router)#address-family vpnv4	Enter VPNv4 address family mode.
(config-router-af)#neighbor 41.41.41.41 activate	Activate the PE neighbor so that it can accept VPN IPv4 routes.
(config-router-af)#exit-address-family	Exit VPNv4 address family mode.
(config-router)#address-family ipv4 vrf vrf1	Enter the IPv4 address family for VRF vrf1.
(config-router-af)#redistribute connected	Redistribute connected route.
(config-router-af)#exit-address-family	Exit IPv4 VRF Address Family mode.

P1 Configuration

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 31.31.31.31/32 secondary	Assign the IPv4 address.
(config-if)#exit	Exit interface mode.
(config)#interface xe21	Enter interface mode.
(config-if)#ip address 11.1.1.31/24	Assign the IPv4 address.

(config-if)#exit	Exit interface mode.
(config)#interface xe15	Enter interface mode.
(config-if)#ip address 12.1.1.31/24	Assign the IPv4 address.
(config-if)#exit	Exit interface mode.
(config)#router ospf 1	Enter router OSPF mode.
(config-router)#ospf router-id 31.31.31.31	Configure OSPF router id same as loopback ip address.
(config-router)#network 31.31.31.31/32 area 0	Define the network on which OSPF runs and associate area id.
(config-router)#network 11.1.1.0/24 area 0	Define the network on which OSPF runs and associate area id.
(config-router)#network 12.1.1.0/24 area 0	Define the network on which OSPF runs and associate area id.
(config-router)#exit	Exit OSPF router mode.
(config)#router ldp	Enter router LDP mode.
(config-router)#transport-address ipv4 31.31.31.31	Configure LDP transport address same as loopback address.
(config-router)#exit	Exit LDP mode.
(config)#interface xe21	Enter interface mode.
(config-if)#label-switching	Enable label switching in interface.
(config-if)#enable-ldp ipv4	Enable LDP in interface.
(config-router)#exit	Exit interface mode.
(config)#interface xe15	Enter interface mode.
(config-if)#label-switching	Enable label switching in interface.
(config-if)#enable-ldp ipv4	Enable LDP in interface.
(config-router)#exit	Exit interface mode.

PE2-ASBR1

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 41.41.41.41/32 secondary	Assign the IPv4 address.
(config-if)#exit	Exit interface mode.
(config)#ip vrf vrf1	Create a new VRF named vrf1.
(config-vrf)#rd 1:1	Assign the route distinguisher (RD) value as 1:1.
(config-vrf)#route-target both 1:1	Import routes between route target (RT) ext-communities.
(config-vrf)#exit	Exit interface mode.
(config)#interface xe21	Enter interface mode.
(config-if)#ip vrf forwarding vrf1	Bind the interface connected to the CE router with VRF vrf1.
(config-if)#ip address 20.1.1.41/24	Assign the IPv4 address.
(config-if)#exit	Exit interface mode.
(config)#interface xe15	Enter interface mode.
(config-if)#ip address 12.1.1.41/24	Assign the IPv4 address.

(config-if)#	Exit interface mode.
(config)#router ospf 1	Enter router OSPF mode.
(config-router)#ospf router-id 41.41.41.41	Configure OSPF router id same as loopback ip address.
(config-router)#network 41.41.41.41/32 area 0	Define the network on which OSPF runs and associate area id.
(config-router)#network 12.1.1.0/24 area 0	Define the network on which OSPF runs and associate area id.
(config-router)#exit	Exit OSPF router mode.
(config)#router ldp	Enter router LDP mode.
(config-router)#transport-address ipv4 41.41.41.41	Configure LDP transport address same as loopback address.
(config-router)#exit	Exit LDP mode.
(config)#interface xe15	Enter interface mode.
(config-if)#label-switching	Enable label switching in interface.
(config-if)#enable-ldp ipv4	Enable LDP in interface.
(config-router)#exit	Exit interface mode.
(config)#router bgp 65000	Enter BGP router mode.
(config-router)#bgp router-id 41.41.41.41	Configure BGP router-id.
(config-router)#neighbor 2.2.2.2 remote-as 65000	Configure PE1 as an iBGP peer.
(config-router)#neighbor 2.2.2.2 update-source lo	Update the source as loopback for iBGP peering with the remote PE2 router.
(config-router)#address-family vpnv4	Enter VPNv4 address family mode.
(config-router-af)#neighbor 2.2.2.2 activate	Activate the PE neighbor so that it can accept VPN IPv4 routes.
(config-router-af)#exit-address-family	Exit VPNv4 address family mode.
(config-router)#address-family ipv4 vrf vrf1	Enter the IPv4 address family for VRF vrf1.
(config-router-af)#neighbor 20.1.1.3 remote-as 65001	Configure eBGP neighbor.
(config-router-af)#redistribute connected	Redistribute connected route.
(config-router-af)#exit-address-family	Exit IPv4 VRF Address Family mode.

PE3-ASBR2

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 3.3.3.3/32 secondary	Assign the IPv4 address.
(config-if)#exit	Exit interface mode.
(config)#ip vrf vrf1	Create a new VRF named vrf1.
(config-vrf)#rd 1:1	Assign the route distinguisher (RD) value as 1:1.
(config-vrf)#route-target both 1:1	Import routes between route target (RT) ext-communities.
(config-vrf)#exit	Exit interface mode.
(config)#interface xe21	Enter interface mode.
(config-if)#ip vrf forwarding vrf1	Bind the interface connected to the CE router with VRF vrf1.

(config-if)#ip address 20.1.1.3/24	Assign the IPv4 address.
(config-if)#exit	Exit interface mode.
(config)#interface xe15	Enter interface mode.
(config-if)#ip address 21.1.1.3/24	Assign the IPv4 address.
(config-if)#exit	Exit interface mode
(config)#router ospf 1	Enter router OSPF mode.
(config-router)#ospf router-id 3.3.3.3	Configure OSPF router id same as loopback ip address.
(config-router)#network 3.3.3.3/32 area 0	Define the network on which OSPF runs and associate area id.
(config-router)#network 21.1.1.0/24 area 0	Define the network on which OSPF runs and associate area id.
(config-router)#exit	Exit OSPF router mode.
(config)#router ldp	Enter router LDP mode.
(config-router)#transport-address ipv4 3.3.3.3	Configure LDP transport address same as loopback address.
(config-router)#exit	Exit LDP mode.
(config)#interface xe15	Enter interface mode.
(config-if)#label-switching	Enable label switching in interface.
(config-if)#enable-ldp ipv4	Enable LDP in interface.
(config-router)#exit	Exit interface mode.
(config)#rsvp-trunk lsp1	Create an RSVP trunk lsp1 and enter the Trunk mode.
(config-trunk)#to 5.5.5.5	Specify the IPv4 egress (destination point-PE4 loopback address) for the LSP.
(config-trunk)#exit	Exit interface mode.
(config)#router bgp 65001	Enter BGP router mode.
(config-router)#bgp router-id 3.3.3.3	Configure BGP router-id.
(config-router)#neighbor 5.5.5.5 remote-as 65001	Configure PE4 as an iBGP peer.
(config-router)#neighbor 5.5.5.5 update-source lo	Update the source as loopback for iBGP peering with the remote PE2 router.
(config-router)#address-family vpnv4	Enter VPNv4 address family mode.
(config-router-af)#neighbor 5.5.5.5 activate	Activate the PE neighbor so that it can accept VPN IPv4 routes.
(config-router-af)#exit-address-family	Exit VPNv4 address family mode.
(config-router)#address-family ipv4 vrf vrf1	Enter the IPv4 address family for VRF vrf1.
(config-router-af)#neighbor 20.1.1.41 remote-as 65000	Configure eBGP neighbor.
(config-router-af)#neighbor 20.1.1.41 activate	Activate the eBGP neighbor under address family.
(config-router-af)#redistribute connected	Redistribute connected route.
(config-router-af)#exit-address-family	Exit IPv4 VRF Address Family mode.

P2

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode.
`(config-if)#ip address 40.40.40.40/32 secondary`	Assign the IPv4 address.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe21`	Enter interface mode.
`(config-if)#ip address 21.1.1.40/24`	Assign the IPv4 address.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe15`	Enter interface mode.
`(config-if)#ip address 22.1.1.40/24`	Assign the IPv4 address.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 1`	Enter router OSPF mode.
`(config-router)#ospf router-id 40.40.40.40`	Configure OSPF router id same as loopback ip address.
`(config-router)#network 40.40.40.40/32 area 0`	Define the network on which OSPF runs and associate area id.
`(config-router)#network 21.1.1.0/24 area 0`	Define the network on which OSPF runs and associate area id.
`(config-router)#network 22.1.1.0/24 area 0`	Define the network on which OSPF runs and associate area id.
`(config-router)#exit`	Exit OSPF router mode
`(config)#router ldp`	Enter router LDP mode.
`(config-router)#transport-address ipv4 40.40.40.40`	Configure LDP transport address same as loopback address.
`(config-router)#exit`	Exit LDP mode.
`(config)#interface xe21`	Enter interface mode.
`(config-if)#label-switching`	Enable label switching in interface.
`(config-if)#enable-ldp ipv4`	Enable LDP in interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe15`	Enter interface mode.
`(config-if)#label-switching`	Enable label switching in interface.
`(config-if)#enable-ldp ipv4`	Enable LDP in interface.
`(config-if)#exit`	Exit interface mode.

PE4

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode.
`(config-if)#ip address 5.5.5.5/32 secondary`	Assign the IPv4 address.
`(config-if)#exit`	Exit interface mode.
`(config)#ip vrf vrf1`	Create a new VRF named vrf1.
`(config-vrf)#rd 1:1`	Assign the route distinguisher (RD) value as 1:1.

(config-vrf)#route-target both 1:1	Import routes between route target (RT) ext-communities.
(config-vrf)#exit	Exit VRF mode.
(config)#interface xe22	Enter interface mode.
(config-if)#ip vrf forwarding vrf1	Bind the interface connected to the CE router with VRF vrf1.
(config-if)#ip address 30.1.1.5/24	Assign the IPv4 address.
(config-if)#exit	Exit interface mode.
(config)#interface xe15	Enter interface mode.
(config-if)#ip address 22.1.1.5/24	Assign the IPv4 address.
(config-if)#exit	Exit interface mode.
(config)#router ospf 1	Enter router OSPF mode.
(config-router)#ospf router-id 5.5.5.5	Configure OSPF router id same as loopback ip address.
config-router)#network 5.5.5.5/32 area 0	Define the network on which OSPF runs and associate area id.
(config-router)#network 22.1.1.0/24 area 0	Define the network on which OSPF runs and associate area id.
(config-router)#exit	Exit router OSPF mode.
(config)#router ldp	Enter router LDP mode.
(config-router)#transport-address ipv4 5.5.5.5	Configure LDP transport address same as loopback address.
(config-router)#exit	Exit LDP mode.
(config)#interface xe15	Enter interface mode.
(config-if)#label-switching	Enable label switching in interface.
(config-if)#enable-ldp ipv4	Enable LDP in interface.
(config-if)#exit	Exit interface mode.
(config)#router bgp 65001	Enter BGP router mode.
(config-router)#bgp router-id 5.5.5.5	Configure BGP router-id.
(config-router)#neighbor 3.3.3.3 remote-as 65001	Configure PE2-ASBR1 as an iBGP peer.
(config-router)#neighbor 3.3.3.3 update-source lo	Update the source as loopback for iBGP peering with the remote PE2 router.
(config-router)#address-family vpnv4	Enter VPNv4 address family mode.
(config-router-af)#neighbor 3.3.3.3 activate	Activate neighbor.
(config-router-af)#exit-address-family	Exit VPNv4 Address Family mode.
(config-router)#address-family ipv4 vrf vrf1	Enter IPv4 VRF Address Family mode.
(config-router-af)#redistribute connected	Redistribute connected route.
(config-router-af)#exit-address-family	Exit Ipv4 Address Family mode.

Validation

PE1

```
#show ip route vrf vrf1 database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
```

```
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       > - selected route, * - FIB route, p - stale info

IP Route Table for VRF "vrf1"
C    *>  10.1.1.0/24 is directly connected, xe22, 01:05:28
B    *>  20.1.1.0/24 [200/0] via 41.41.41.41, 00:01:18
B    *>  30.1.1.0/24 [200/0] via 41.41.41.41, 00:00:24
C    *>  127.0.0.0/8 is directly connected, lo.vrf1, 01:06:20

Gateway of last resort is not set
#show ip bgp vpnv4 all
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf      Weight Path
Route Distinguisher: 1:1 (Default for VRF vrf1)
*> l 10.1.1.0/24      0.0.0.0               0         100           32768    ?
*>i  20.1.1.0/24      41.41.41.41           0         100           0        ?
*>i  30.1.1.0/24      41.41.41.41           0         100           0
65001 ?
 Announced routes count = 1
 Accepted routes count = 2
Route Distinguisher: 1:1
*>i  20.1.1.0/24      41.41.41.41           0         100           0        ?
*>i  30.1.1.0/24      41.41.41.41           0         100           0
65001 ?
 Announced routes count = 0
 Accepted routes count = 2
```

PE2-ASBR1

```
#show ip route vrf vrf1 database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       > - selected route, * - FIB route, p - stale info

IP Route Table for VRF "vrf1"
C    *>  20.1.1.0/24 is directly connected, xe22, 01:05:28
B    *>  10.1.1.0/24 [200/0] via 2.2.2.2, 00:01:18
B    *>  30.1.1.0/24 [20/0] via 20.1.1.3, xe2, 00:54:13
C    *>  127.0.0.0/8 is directly connected, lo.vrf1, 01:06:20

Gateway of last resort is not set

#show ip bgp vpnv4 all
```

```
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf      Weight Path
Route Distinguisher: 1:1 (Default for VRF vrf1)
*>i  10.1.1.0/24      2.2.2.2              0         100           0        ?
*> l 20.1.1.0/24      0.0.0.0              0         100           32768    ?
*    20.1.1.0/24      20.1.1.3             0         100           0
65001 ?
*> l 30.1.1.0/24      20.1.1.3             0         100           0
65001 ?
 Announced routes count = 3
 Accepted routes count = 1
Route Distinguisher: 1:1
*>i  10.1.1.0/24      2.2.2.2              0         100           0        ?
 Announced routes count = 0
 Accepted routes count = 1
```

PE3-ASBR2

```
#show ip route vrf vrf1 database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       > - selected route, * - FIB route, p - stale info

IP Route Table for VRF "vrf1"
B    *>  10.1.1.0/24 [20/0] via 20.1.1.41, xe22, 00:55:54
C    *>  20.1.1.0/24 is directly connected, xe22, 01:05:28
B    *>  30.1.1.0/24 [200/0] via 5.5.5.5, 00:01:18
C    *>  127.0.0.0/8 is directly connected, lo.vrf1, 01:06:20

Gateway of last resort is not set
#show ip bgp vpnv4 all
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf      Weight Path
Route Distinguisher: 1:1 (Default for VRF vrf1)
*> l 10.1.1.0/24      20.1.1.41            0         100           0
65000 ?
*> l 20.1.1.0/24      0.0.0.0              0         100           32768    ?
*    20.1.1.0/24      20.1.1.41            0         100           0
65000 ?
*>i  30.1.1.0/24      5.5.5.5              0         100           0        ?
 Announced routes count = 3
 Accepted routes count = 1
Route Distinguisher: 1:1
*>i  30.1.1.0/24      5.5.5.5              0         100           0        ?
 Announced routes count = 0
```

```
 Accepted routes count = 1
```

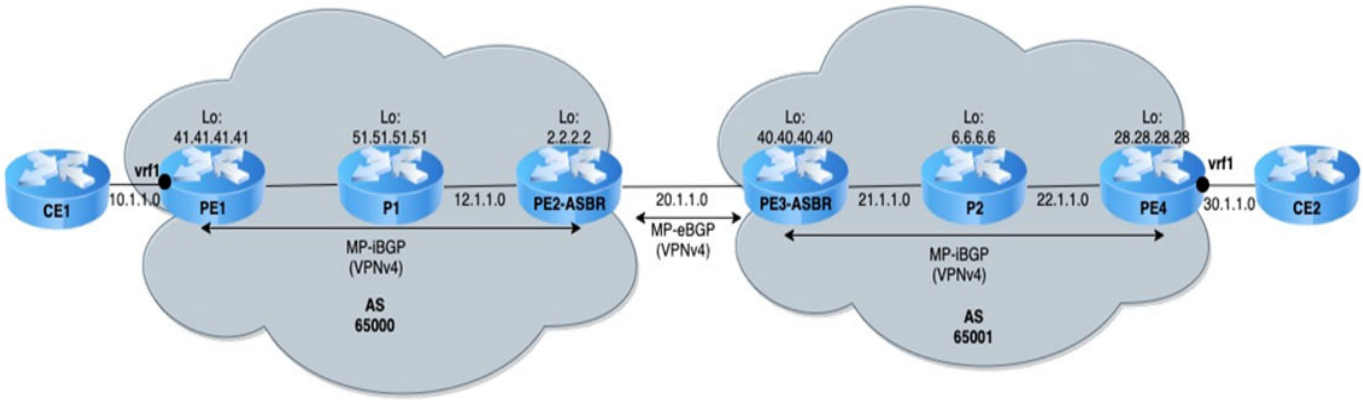
PE4

```
#show ip route vrf vrf1 database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       > - selected route, * - FIB route, p - stale info

IP Route Table for VRF "vrf1"
B    *>  10.1.1.0/24 [200/0] via 3.3.3.3, 00:00:08
B    *>  20.1.1.0/24 [200/0] via 3.3.3.3, 00:02:45
C    *>  30.1.1.0/24 is directly connected, xe18, 01:02:20
C    *>  127.0.0.0/8 is directly connected, lo.vrf1, 01:05:36

Gateway of last resort is not set

#show ip bgp vpnv4 all
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf      Weight Path
Route Distinguisher: 1:1 (Default for VRF vrf1)
*>i  10.1.1.0/24      3.3.3.3              0         100           0
65000 ?
*>i  20.1.1.0/24      3.3.3.3              0         100           0        ?
*> l 30.1.1.0/24      0.0.0.0              0         100           32768    ?
 Announced routes count = 1
 Accepted routes count = 2
Route Distinguisher: 1:1
*>i  10.1.1.0/24      3.3.3.3              0         100           0
65000 ?
*>i  20.1.1.0/24      3.3.3.3              0         100           0        ?
 Announced routes count = 0
 Accepted routes count = 2
```

CHAPTER 18 Inter-AS VPN Option-B Configuration

- Inter-AS Option B is a more scalable solution compared to Option A. It does not require any VRFs on the ASBRs, it uses VPNv4 eBGP to exchange VPNv4 updates.
- Single interface to connect the ASBRs.
- Packets are sent labelled between the ASBRs.
- No need for VRFs on the ASBR.
- ASBRs must be directly connected.
- Scales better than Option A.

Topology



PE1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode.
`(config-if)#ip address 2.2.2.2/32 secondary`	Assign the IPv4 address.
`(config-if)#exit`	Exit interface mode.
`(config)#ip vrf vrf1`	Create a new VRF named vrf1.
`(config-vrf)#rd 1:1`	Assign the route distinguisher (RD) value as 1:1.
`(config-vrf)#route-target both 1:1`	Import routes between route target (RT) ext-communities.
`(config-vrf)#exit`	Exit VRF mode.
`(config)#interface xe22`	Enter interface mode.
`(config-if)#ip vrf forwarding vrf1`	Bind the interface connected to the CE router with VRF vrf1.
`(config-if)#ip address 10.1.1.2/24`	Assign the IPv4 address.
`(config-if)#exit`	Exit interface mode.

(config)#interface xe20	Enter interface mode.
(config-if)#ip address 11.1.1.2/24	Assign the IPv4 address.
(config-if)#exit	Exit interface mode.
(config)#router ospf 1	Enter router OSPF mode.
(config-router)#ospf router-id 2.2.2.2	Configure OSPF router id same as loopback ip address.
(config-router)#network 2.2.2.2/32 area 0	Define the network on which OSPF runs and associate area id.
(config-router)#network 11.1.1.0/24 area 0	Define the network on which OSPF runs and associate area id.
(config-router)#exit	Exit OSPF router mode.
(config)#router ldp	Enter router LDP mode.
(config-router)#transport-address ipv4 2.2.2.2	Configure LDP transport address same as loopback address.
(config-router)#exit	Exit LDP mode.
(config)#interface xe20	Enter interface mode.
(config-if)#label-switching	Enable label switching in interface.
(config-if)#enable-ldp ipv4	Enable LDP in interface.
(config-if)#exit	Exit interface mode.
(config)#router bgp 65000	Enter BGP router mode.
(config-router)#bgp router-id 2.2.2.2	Configure BGP router-id.
(config-router)#neighbor 41.41.41.41 remote-as 65000	Configure PE2-ASBR1 as an iBGP peer.
(config-router)#neighbor 41.41.41.41 update-source lo	Update the source as loopback for iBGP peering with the remote PE2 router.
(config-router)#address-family vpnv4	Enter VPNv4 address family mode.
(config-router-af)#neighbor 41.41.41.41 activate	Activate the PE neighbor so that it can accept VPN IPv4 routes.
(config-router-af)#exit-address-family	Exit VPNv4 address family mode.
(config-router)#address-family ipv4 vrf vrf1	Enter the IPv4 address family for VRF vrf1.
(config-router-af)#redistribute connected	Redistribute connected route.
(config-router-af)#exit-address-family	Exit IPv4 VRF Address Family mode.

P1

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 31.31.31.31/32 secondary	Assign the IPv4 address.
(config-if)#exit	Exit interface mode.
(config)#interface xe21	Enter interface mode.
(config-if)#ip address 11.1.1.31/24	Assign the IPv4 address.
(config-if)#exit	Exit interface mode.
(config)#interface xe15	Enter interface mode.

(config-if)#ip address 12.1.1.31/24	Assign the IPv4 address.
(config-if)#exit	Exit interface mode.
(config)#router ospf 1	Enter router OSPF mode.
(config-router)#ospf router-id 31.31.31.31	Configure OSPF router id same as loopback ip address.
(config-router)#network 31.31.31.31/32 area 0	Define the network on which OSPF runs and associate area id.
(config-router)#network 11.1.1.0/24 area 0	Define the network on which OSPF runs and associate area id.
(config-router)#network 12.1.1.0/24 area 0	Define the network on which OSPF runs and associate area id.
(config-router)#exit	Exit OSPF router mode.
(config)#router ldp	Enter router LDP mode.
(config-router)#transport-address ipv4 31.31.31.31	Configure LDP transport address same as loopback address.
(config-router)#exit	Exit LDP mode.
(config)#interface xe21	Enter interface mode.
(config-if)#label-switching	Enable label switching in interface.
(config-if)#enable-ldp ipv4	Enable LDP in interface.
(config-if)#exit	Exit interface mode.
(config)#interface xe15	Enter interface mode.
(config-if)#label-switching	Enable label switching in interface.
(config-if)#enable-ldp ipv4	Enable LDP in interface.
(config-router)#exit	Exit interface mode.

PE2-ASBR1

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 41.41.41.41/32 secondary	Assign the IPv4 address.
(config-if)#exit	Exit interface mode.
(config)#interface xe21	Enter interface mode.
(config-if)#ip address 20.1.1.41/24	Assign the IPv4 address.
(config-if)#exit	Exit interface mode.
(config)#interface xe15	Enter interface mode.
(config-if)#ip address 12.1.1.41/24	Assign ipv4 address.
(config-if)#exit	Exit interface mode.
(config)#router ospf 1	Enter router OSPF mode.
(config-router)#ospf router-id 41.41.41.41	Configure OSPF router id same as loopback ip address.
(config-router)#network 41.41.41.41/32 area 0	Define the network on which OSPF runs and associate area id.
(config-router)#network 12.1.1.0/24 area 0	Define the network on which OSPF runs and associate area id.
(config-router)#exit	Exit OSPF router mode.

(config)#router ldp	Enter router LDP mode.
(config-router)#transport-address ipv4 41.41.41.41	Configure LDP transport address same as loopback address.
(config-router)#exit	Exit LDP mode.
(config)#interface xe15	Enter interface mode.
(config-if)#label-switching	Enable label switching in interface.
(config-if)#enable-ldp ipv4	Enable LDP in interface.
(config-if)#exit	Exit interface mode.
(config)#interface xe21	Enter interface mode.
(config-if)#label-switching	Enable label switching in interface.
(config-if)#exit	Exit interface mode.
(config)#router bgp 65000	Enter BGP router mode.
(config-router)#bgp router-id 41.41.41.41	Configure BGP router-id.
(config-router)#no bgp inbound-route-filter	Disable inbound route filter.
(config-router)#neighbor 2.2.2.2 remote-as 65000	Configure PE1 as an iBGP peer.
(config-router)#neighbor 2.2.2.2 update-source lo	Update the source as loopback for iBGP peering with the remote PE1 router.
(config-router)#neighbor 20.1.1.3 remote-as 65001	Configure eBGP neighbor with ASBR2.
(config-router)#address-family vpnv4	Enter VPNv4 address family mode.
(config-router-af)#neighbor 2.2.2.2 activate	Activate the PE neighbor so that it can accept VPN IPv4 routes.
(config-router-af)#neighbor 2.2.2.2 next-hop-self	Configure this to make the router the next hop for a BGP neighbor.
(config-router-af)#neighbor 20.1.1.3 allow-ebgp-vpn	Configure this to allow exchange of VPN updates between eBGP peers.
(config-router-af)#neighbor 20.1.1.3 activate	Activate the ASBR eBGP neighbor.
(config-router-af)#exit-address-family	Exit VPNv4 address family mode.

PE3-ASBR2

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 3.3.3.3/32 secondary	Assign the IPv4 address.
(config-if)#exit	Exit interface mode.
(config)#interface xe21	Enter interface mode.
(config-if)#ip address 20.1.1.3/24	Assign the IPv4 address.
(config-if)#exit	Exit interface mode.
(config)#interface xe15	Enter interface mode.
(config-if)#ip address 21.1.1.3/24	Assign the IPv4 address.

(config-if)#exit	Exit interface mode.
(config)#router ospf 1	Enter router OSPF mode.
(config-router)#ospf router-id 3.3.3.3	Configure OSPF router id same as loopback ip address.
(config-router)#network 3.3.3.3/32 area 0	Define the network on which OSPF runs and associate area id.
(config-router)#network 21.1.1.0/24 area 0	Define the network on which OSPF runs and associate area id.
(config-router)#exit	Exit OSPF router mode.
(config)#router ldp	Enter router ldp mode.
(config-router)#transport-address ipv4 3.3.3.3	Configure LDP transport address same as loopback address
(config-router)#exit	Exit LDP mode.
(config)#interface xe15	Enter interface mode.
(config-if)#label-switching	Enable label switching in interface.
(config-if)#enable-ldp ipv4	Enable LDP in interface.
(config-router)#exit	Exit LDP mode.
(config)#interface xe21	Enter interface mode.
(config-if)#label-switching	Enable label switching in interface.
(config-if)#exit	Exit interface mode.
(config)#router bgp 65001	Enter BGP router mode.
(config-router)#bgp router-id 3.3.3.3	Configure BGP router-id.
(config-router)#no bgp inbound-route-filter	Disable inbound route filter.
(config-router)#neighbor 5.5.5.5 remote-as 65001	Configure PE4 as an iBGP peer.
(config-router)#neighbor 5.5.5.5 update-source lo	Update the source as loopback for iBGP peering with the remote PE1 router.
(config-router)#neighbor 20.1.1.41 remote-as 65000	Configure eBGP neighbor with PE4.
(config-router)#address-family vpnv4	Enter VPNv4 address family mode.
(config-router-af)#neighbor 5.5.5.5 activate	Activate the PE neighbor so that it can accept VPN IPv4 routes.
(config-router-af)#neighbor 5.5.5.5 next-hop-self	Configure this to make the router the next hop for a BGP neighbor.
(config-router-af)#neighbor 20.1.1.41 allow-ebgp-vpn	Configure this to allow exchange of vpn updates between eBGP peers.
(config-router-af)#neighbor 20.1.1.41 activate	Activate the ASBR eBGP neighbor.
(config-router-af)#exit-address-family	Exit VPNv4 address family mode.

P2

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 40.40.40.40/32 secondary	Assign the IPv4 address.

`(config-if)#exit`	Exit interface mode.
`(config)#interface xe21`	Enter interface mode.
`(config-if)#ip address 21.1.1.40/24`	Assign the IPv4 address.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe15`	Enter interface mode.
`(config-if)#ip address 22.1.1.40/24`	Assign the IPv4 address.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 1`	Enter router OSPF mode.
`(config-router)#ospf router-id 40.40.40.40`	Configure OSPF router id same as loopback ip address.
`(config-router)#network 40.40.40.40/32 area 0`	Define the network on which OSPF runs and associate area id.
`(config-router)#network 21.1.1.0/24 area 0`	Define the network on which OSPF runs and associate area id.
`(config-router)#network 22.1.1.0/24 area 0`	Define the network on which OSPF runs and associate area id.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#router ldp`	Enter router LDP mode.
`(config-router)#transport-address ipv4 40.40.40.40`	Configure LDP transport address same as loopback address.
`(config-router)#exit`	Exit LDP mode.
`(config)#interface xe21`	Enter interface mode.
`(config-if)#label-switching`	Enable label switching in interface.
`(config-if)#enable-ldp ipv4`	Enable ldp in interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe15`	Enter interface mode.
`(config-if)#label-switching`	Enable label switching in interface.
`(config-if)#enable-ldp ipv4`	Enable LDP in interface.
`(config-if)#exit`	Exit interface mode.

PE4 Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode.
`(config-if)#ip address 5.5.5.5/32 secondary`	Assign the IPv4 address.
`(config-if)#exit`	Exit interface mode.
`(config)#ip vrf vrf1`	Create a new VRF named vrf1.
`(config-vrf)#rd 1:1`	Assign the route distinguisher (RD) value as 1:1.
`(config-vrf)#route-target both 1:1`	Import routes between route target (RT) ext-communities.
`(config-vrf)#exit`	Exit VRF mode.
`(config)#interface xe22`	Enter interface mode.

(config-if)#ip vrf forwarding vrf1	Bind the interface connected to the CE router with VRF vrf1.
(config-if)#ip address 30.1.1.5/24	Assign the IPv4 address.
(config-if)#exit	Exit interface mode.
(config)#interface xe15	Enter interface mode.
(config-if)#ip address 22.1.1.5/24	Assign the IPv4 address.
(config-if)#exit	Exit interface mode.
(config)#router ospf 1	Enter router OSPF mode.
(config-router)#ospf router-id 5.5.5.5	Configure OSPF router id same as loopback ip address.
(config-router)#network 5.5.5.5/32 area 0	Define the network on which OSPF runs and associate area id.
(config-router)#network 22.1.1.0/24 area 0	Define the network on which OSPF runs and associate area id.
(config-router)#exit	Exit OSPF router mode.
(config)#router ldp	Enter router LDP mode.
(config-router)#transport-address ipv4 5.5.5.5	Configure LDP transport address same as loopback address.
(config-router)#exit	Exit LDP mode.
(config)#interface xe15	Enter interface mode.
(config-if)#label-switching	Enable label switching in interface.
(config-if)#enable-ldp ipv4	Enable LDP in interface.
(config-if)#exit	Exit interface mode.
(config)#router bgp 65001	Enter BGP router mode.
(config-router)#bgp router-id 5.5.5.5	Configure BGP router-id.
(config-router)#neighbor 3.3.3.3 remote-as 65001	Configure PE2-ASBR1 as an iBGP peer.
(config-router)#neighbor 3.3.3.3 update-source lo	Update the source as loopback for iBGP peering with the remote PE2 router.
(config-router)#address-family vpnv4	Enter VPNv4 address family mode.
(config-router-af)#neighbor 3.3.3.3 activate	Activate the PE neighbor so that it can accept VPN IPv4 routes.
(config-router-af)#exit-address-family	Exit VPNv4 address family mode.
(config-router)#address-family ipv4 vrf vrf1	Enter the IPv4 address family for VRF vrf1.
(config-router-af)#redistribute connected	Redistribute connected route.
(config-router-af)#exit-address-family	Exit IPv4 VRF Address Family mode.

Validation

PE1

```
#show ip route vrf vrf1 database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, E - EVPN,
       v - vrf leaked
       > - selected route, * - FIB route, p - stale info

IP Route Table for VRF "vrf1"
C    *>  10.1.1.0/24 is directly connected, xe22, 03:49:26
B    *>  30.1.1.0/24 [200/0] via 41.41.41.41, 00:00:41
C    *>  127.0.0.0/8 is directly connected, lo.vrf1, 03:50:18

PE1#show ip bgp vpnv4 all
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf      Weight Path
Route Distinguisher: 1:1 (Default for VRF vrf1)
*> l 10.1.1.0/24      0.0.0.0              0         100           32768    ?
*>i  30.1.1.0/24      41.41.41.41          0         100           0
65001 ?
 Announced routes count = 1
 Accepted routes count = 1
Route Distinguisher: 1:1
*>i  30.1.1.0/24      41.41.41.41          0         100           0
65001 ?
 Announced routes count = 0
 Accepted routes count = 1
```

PE2-ASBR1

```
#show ip bgp vpnv4 all
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf      Weight Path
Route Distinguisher: 1:1
*>il 10.1.1.0/24      2.2.2.2              0         100           0        ?
*> l 30.1.1.0/24      20.1.1.3             0         100           0
65001 ?
 Announced routes count = 0
 Accepted routes count = 2

#show ip bgp vpnv4 all summary
BGP router identifier 41.41.41.41, local AS number 65000
BGP table version is 4
2 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
2.2.2.2                  4 65000  168        171       4      0      0
00:29:03              1
20.1.1.3                 4 65001  111        119       4      0      0
00:42:51              1

Total number of neighbors 2
```

```
Total number of Established sessions 2
```

PE3-ASBR2

```
#show ip bgp vpnv4 all
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf      Weight Path
Route Distinguisher: 1:1
*> l 10.1.1.0/24      20.1.1.41             0         100           0
65000 ?
*>il 30.1.1.0/24      5.5.5.5               0         100           0        ?
 Announced routes count = 0
 Accepted routes count = 2

#show ip bgp vpnv4 all summary
BGP router identifier 3.3.3.3, local AS number 65001
BGP table version is 4
2 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
5.5.5.5                  4 65001   41         45       4      0      0
00:15:59              1
20.1.1.41                4 65000  115        118       4      0      0
00:43:58              1

Total number of neighbors 2

Total number of Established sessions 2
```

PE4

```
#show ip bgp vpnv4 all
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf      Weight Path
Route Distinguisher: 1:1 (Default for VRF vrf1)
*>i  10.1.1.0/24      3.3.3.3               0         100           0
65000 ?
*> l 30.1.1.0/24      0.0.0.0               0         100           32768    ?
 Announced routes count = 1
 Accepted routes count = 1
Route Distinguisher: 1:1
*>i  10.1.1.0/24      3.3.3.3               0         100           0
65000 ?
 Announced routes count = 0
 Accepted routes count = 1

#show ip route vrf vrf1 database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
```

```
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
        ia - IS-IS inter area, E - EVPN,
        v - vrf leaked
        > - selected route, * - FIB route, p - stale info

IP Route Table for VRF "vrf1"
B    *>  10.1.1.0/24 [200/0] via 3.3.3.3, 00:00:48
C    *>  30.1.1.0/24 is directly connected, xe22, 03:46:38
C    *>  127.0.0.0/8 is directly connected, lo.vrf1, 03:49:54

Gateway of last resort is not set
```

CHAPTER 17 Mapping RSVP Tunnel Name to L2VPN Service

This chapter shows configurations of mapping of rsvp tunnel-name to L2VPN service.

An MPLS Layer 2 Virtual Circuit (VC) is a point-to-point Layer 2 connection transported via MPLS on the service provider's network. The Layer 2 circuit is transported over a single Label Switched Path (LSP) tunnel between two Provider Edge (PE) routers

Virtual Private LAN Service (VPLS) is a way to provide Ethernet-based multipoint-to-multipoint communication over IP-MPLS networks. It allows geographically-dispersed sites to share an Ethernet broadcast domain by connecting sites through pseudowires. A set of Martini circuits is grouped by a common VPLS identifier to achieve this service objective

Overview

This topology will be applicable for both VPWS and VPLS services.

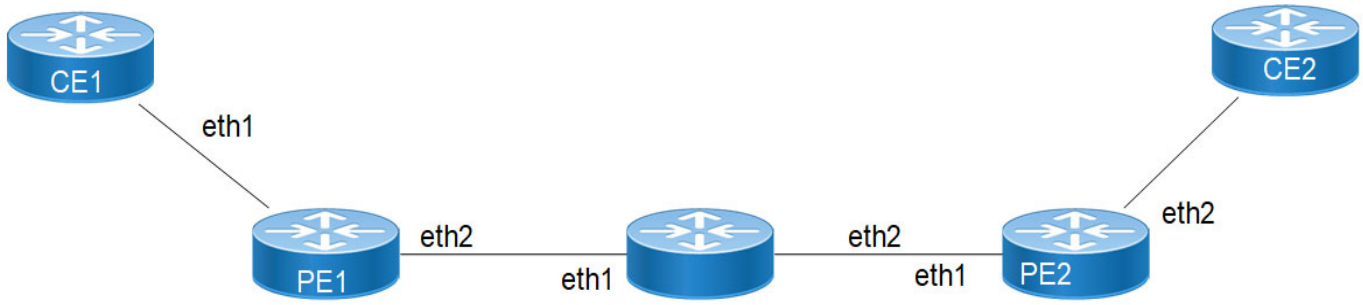


Figure 17-28: Mapping of RSVP Tunnel-name to L2VPN services

Configuring the VC:

Note: Loopback addresses being used should be advertised through OSPF, or should be statically routed.

1. Configure the IP address and OSPF for the PE-1, P (Provider), and PE-2 routers.
2. Configure MPLS and LDP on PE-1, P, and PE-2, and LDP targeted peer for the PE-1 and PE-2 routers. (If RSVP is used for configuring trunks, LDP must be configured on PE-1 and PE-2, and RSVP must be configured on PE-1, P, and PE-2).
3. Configure the VC with trunk-name.
4. Bind the customer interface to the VC.

Configure IP Address and OSPF on Routers

Configure the IP addresses and OSPF on the PE-1, P, and PE-2 routers.

PE-1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Specify the loopback interface (lo0) to be configured.
`(config-if)#ip address 1.1.1.1/32 secondary`	Set the IP address of the loopback interface to 1.1.1.1/32.

(config-if)#exit	Exit interface mode.
(config)#interface xe1	Specify the interface (xe1) to be configured.
(config-if)#label-switching	Enable label switching on interface xe1.
(config-if)#ip address 10.1.1.1/24	Set the IP address of the interface to 10.1.1.1/24.
(config-if)#exit	Exit interface mode.
(config)#router ospf 100	Configure the routing process and specify the Process ID (100). The Process ID should be a unique positive integer identifying the routing process.
(config-router)#network 10.1.1.0/24 area 0	Define the interface on which OSPF runs and associate the area ID (0) with the interface.
(config-router)#network 1.1.1.1/32 area 0	Define the interface on which OSPF runs and associate the area ID (0) with the interface.

P

#configure terminal	Enter configure mode.
(config)#interface lo	Specify the loopback interface (lo0) to be configured.
(config-if)#ip address 9.9.9.9/32 secondary	Set the IP address of the loopback interface to 9.9.9.9/32.
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Specify the interface (xe1) to be configured.
(config-if)#label-switching	Enable label switching on interface xe1.
(config-if)#ip address 10.1.1.2/24	Set the IP address of the interface to 10.1.1.2/24.
(config-if)#exit	Exit interface mode.
(config)#interface xe13	Specify the interface (xe13) to be configured.
(config-if)#label-switching	Enable label switching on interface xe13.
(config-if)#ip address 20.1.1.1/24	Set the IP address of the interface to 20.1.1.1/24.
(config-if)#exit	Exit interface mode.
(config)#router ospf 100	Configure the routing process and specify the Process ID (100). The Process ID should be a unique positive integer identifying the routing process.
(config-router)#network 10.1.1.0/24 area 0	Define the interface on which OSPF runs and associate the area ID (0) with the interface.
(config-router)#network 20.1.1.0/24 area 0	Define the interface on which OSPF runs and associate the area ID (0) with the interface.
(config-router)#network 9.9.9.9/32 area 0	Define the interface on which OSPF runs and associate the area ID (0) with the interface.

PE-2

#configure terminal	Enter configure mode.
(config)#interface lo	Specify the loopback interface (lo0) to be configured.
(config-if)#ip address 2.2.2.2/32 secondary	Set the IP address of the loopback interface to 2.2.2.2/32.
(config-if)#exit	Exit interface mode.
(config)#interface xe13	Specify the interface (xe13) to be configured.
(config-if)#label-switching	Enable label switching on interface xe13.

(config-if)#ip address 20.1.1.2/24	Set the IP address of the interface to 20.1.1.2/24.
(config-if)#exit	Exit interface mode.
(config)#router ospf 100	Configure the routing process and specify the Process ID (100). The Process ID should be a unique positive integer identifying the routing process.
(config-router)#network 20.1.1.0/24 area 0	Define the interface on which OSPF runs, and associate the area ID (0) with the interface.
(config-router)#network 2.2.2.2/32 area 0	Define the interface on which OSPF runs, and associate the area ID (0) with the interface.

Configure MPLS, RSVP, and LDP Targeted Peer on Routers

Configure MPLS and LDP on PE-1, P, and PE-2, and LDP targeted peers on PE-1 and PE-2.

Note: If RSVP is used for configuring trunks, LDP must be configured on PE-1 and PE-2, and RSVP must be configured on PE-1, P, and PE-2.

PE-1

#configure terminal	Enter configure mode.
(config)#router ldp	Enter the Router mode.
(config-router)#transport-address ipv4 1.1.1.1	Configure the transport address to be used for a TCP session over which LDP will run on an IPv4 interface.
(config-router)#targeted-peer ipv4 2.2.2.2	Specify the targeted LDP peer on PE-1.
(config-router-targeted-peer)# exit	Exit the Router targeted peer mode.
(config-router)#exit	Exit the Router mode.
(config)#router rsvp	Enter RSVP configuration mode for the router.
(config-router)#exit	Exit configuration mode of the router.
(config)#interface xe1	Specify the interface (xe1) to be configured.
(config-if)#enable-ldp ipv4	Enable LDP on interface xe1.
(config-if)#enable-rsvp	Enable RSVP on the interface.
(config-if)#exit	Exit interface mode.
(config)#rsvp-trunk t2	Configure RSVP trunk t2
(config-trunk)#to 2.2.2.2	Configure PE2 as the end of trunk
(config-trunk)#end	Exit configuration mode

P

#configure terminal	Enter configure mode.
(config)#router rsvp	Enter RSVP configuration mode for the router.
(config-router)#exit	Exit configuration mode of the router.
(config)#interface xe1	Specify the interface (xe1) to be configured.
(config-if)#enable-rsvp	Enable RSVP on the interface.
(config-if)#exit	Exit interface mode.

(config)#interface xe13	Specify the interface (xe13) to be configured.
(config-if)#enable-rsvp	Enable RSVP on the interface.
(config-if)#exit	Exit interface mode.
(config)#rsvp-trunk t5	Configure RSVP trunk t5
(config-trunk)#to 2.2.2.2	Configure PE2 as the end of trunk
(config-trunk)#exit	Exit configuration mode
(config)#rsvp-trunk t6	Configure RSVP trunk t6
(config-trunk)#to 1.1.1.1	Configure PE2 as the end of trunk
(config-trunk)#exit	Exit configuration mode

PE-2

#configure terminal	Enter configure mode.
(config)#router ldp	Enter the Router mode.
(config-router)#transport-address ipv4 2.2.2.2	Configure the transport address to be used for a TCP session over which LDP will run on an IPv4 interface.
(config-router)#targeted-peer ipv4 1.1.1.1	Specify the targeted LDP peer on PE-2.
(config-router-targeted-peer)# exit	Exit the Router targeted peer mode.
(config-router)#exit	Exit the Router mode.
(config)#router rsvp	Enter RSVP configuration mode for the router.
(config-router)#exit	Exit configuration mode of the router.
(config)#interface xe13	Specify the interface(xe13) to be configured.
(config-if)#enable-ldp ipv4	Enable LDP on interface xe13.
(config-if)#enable-rsvp	Enable RSVP on the interface.
(config-if)#exit	Exit interface mode.
(config)#rsvp-trunk t3	Configure RSVP trunk t3
(config-trunk)#to 1.1.1.1	Configure PE1 as the end of trunk
(config-trunk)#exit	Exit configuration mode

Configure VC

Configure the VC. Each VC ID uniquely identifies the Layer-2 circuit among all the Layer-2 circuits.

Note: Both PE routers (endpoints) must be configured with the same VC-ID (100 in this example).

PE-1

#configure terminal	Enter configure mode.
(config)#mpls l2-circuit t2 100 2.2.2.2	Configure the VC for PE-2. In this example, t2 is the VC name, 200 is the VC ID, and 2.2.2.2 is the VC endpoint IP address
(config-pseudowire)#tunnel-name t2	Configure the RSVP Trunk name as t2
(config-pseudowire)#exit	Exit pseudowire config mode.

`(config)#mpls l2-circuit t3 300 2.2.2.2 mode raw`	Configure the VC for PE-2. In this example, t3 is the VC-name, 300 is the VC ID and 2.2.2.2 is the VC endpoint IP address
`(config-pseudowire)#tunnel-name t2`	Configure RSVP Trunk name as t2
`(config-pseudowire)#exit`	Exit pseudowire config mode.

PE-2

`#configure terminal`	Enter configure mode.
`(config)#mpls l2-circuit t2 100 1.1.1.1`	Configure the VC for PE-1. In this example, t2 is the VC name, 200 is the VC ID, and 1.1.1.1 is the VC endpoint IP address
`(config-pseudowire)#tunnel-name t2`	Configure RSVP Tunnel name as t2
`(config-pseudowire)#exit`	Exit pseudowire config mode.
`(config)#mpls l2-circuit t3 300 1.1.1.1 mode raw`	Configure the VC for PE-1. In this example, t3 is the VC name, 300 is the VC ID, and 1.1.1.1 is the VC endpoint IP address
`(config-pseudowire)#tunnel-name t3`	Configure RSVP Tunnel name as t3
`(config-pseudowire)#exit`	Exit pseudowire config mode.

Bind Customer Interface to VC

The following configuration allows only VLAN 2 and 3 traffic.

PE-1

`(config)#service-template ST1`	Create a service template ST1
`(config-svc)#match outer-vlan 2`	Allow VLAN 2 traffic on this VC.
`(config-svc)#exit`	Exit the service template mode
`(config)#service-template ST2`	Create a service template ST2
`(config-svc)#match outer-vlan 3`	Allow VLAN 3 traffic on this VC.
`(config-svc)#exit`	Exit the service template mode
`(config)#interface xe15`	Specify the interface (xe15) to be configured.
`(config-if)#switchport`	Switch to Layer-2 mode.
`(config-if)#mpls-l2-circuit t2 service-template ST1`	Bind the interface to the VC with service template.
`(config-if)#mpls-l2-circuit t3 service-template ST2`	Bind the interface to the VC with service template.

PE-2

`(config)#service-template ST1`	Create a service template ST1
`(config-svc)#match outer-vlan 2`	Allow VLAN 2 traffic on this VC.
`(config-svc)#exit`	Exit the service template mode

`(config)#service-template ST2`	Create a service template ST2
`(config-svc)#match outer-vlan 3`	Allow VLAN 3 traffic on this VC.
`(config-svc)#exit`	Exit the service template mode
`(config)#interface xe12`	Specify the interface (xe12) to be configured.
`(config-if)#switchport`	Switch to Layer-2 mode.
`(config-if)#mpls-l2-circuit t2 service-template ST1`	Bind the interface to the VC with service template.
`(config-if)#mpls-l2-circuit t3 service-template ST2`	Bind the interface to the VC with service template.

Validation

Use the show ldp mpls-l2-circuit (Control Plane) command, and the show mpls vc-table (Forwarding Plane) command, to display complete information about the Layer 2 VC.

If the VC State is UP in the output from the show ldp mpls-l2 circuit command, and the Status is Active in the output of the show mpls vc-table command, a ping from CE1 to CE2 should be successful.

Below are the sample output for VPWS service with Tunnel name:

```
PE1#sh mpls vc-table
VC-ID       Vlan-ID  Inner-Vlan-ID  Access-Intf   Network-Intf  Out Label  Tunnel-Label  Nexthop         Status
100         N/A      N/A            xe15          xe1           24320      24321         2.2.2.2         Active
300         N/A      N/A            xe15          xe1           24321      24321         2.2.2.2         Active
PE1#

PE1#sh ldp mpls-l2-circuit
Transport     Client     VC     VC            Local       Remote      Destination
VC ID         Binding    State  Type          VC Label    VC Label    Address
300           xe15       UP     Ethernet      24321       24321       2.2.2.2
100           xe15       UP     Ethernet VLAN 24320       24320       2.2.2.2
PE1#

PE1#sh mpls l2-circuit
MPLS Layer-2 Virtual Circuit: t2, id: 100  PW-INDEX: 1 Tunnel-Name: t2
 Endpoint: 2.2.2.2
 Control Word: 0
 MPLS Layer-2 Virtual Circuit Group: none
 Bound to interface: xe15
 Virtual Circuit Type: Ethernet VLAN
 Virtual Circuit is configured as Primary
 Virtual Circuit is configured as Active
 Virtual Circuit is active
 Service-template : ST1
  Match criteria : 2


MPLS Layer-2 Virtual Circuit: t3, id: 300  PW-INDEX: 2 Tunnel-Name: t2
 Operating mode: Raw
 Endpoint: 2.2.2.2
 Control Word: 0
 MPLS Layer-2 Virtual Circuit Group: none
 Bound to interface: xe15
 Virtual Circuit Type: Ethernet
 Virtual Circuit is configured as Primary
 Virtual Circuit is configured as Active
 Virtual Circuit is active
 Service-template : ST2
  Match criteria : 3


These additional commands can also be used to display information about the Layer 2 virtual circuits.
show ldp mpls-l2-circuit detail
show ldp mpls-l2-circuit VC-ID
show ldp mpls-l2-circuit VC-ID detail
```

```
show mpls l2-circuit
```

Configuring a MPLS Static Layer-2 VC

1. Configure the VC with the manual option using tunnel name
2. Configure the VC FIB entry.
3. Bind the VC; all steps are in the configurations that follow.

PE-1

`#configure terminal`	Enter configure mode.
`PE1(config)#mpls l2-circuit t5 500 2.2.2.2`	Configure the VC for PE1
`PE1(config-pseudowire)#tunnel-name t2`	Configure the RSVP Tunnel name as t2
`PE1(config-pseudowire)#manual-pseudowire`	Configure the VC as manual (no signaling is used)
`PE1(config-pseudowire)#exit`	Exit pseudowire config mode.
`PE1(config)#service-template ST5`	Create a service template ST5
`PE1(config-svc)#match outer-vlan 5`	Configure single match criteria vlan 5
`PE1(config-svc)#exit`	Exit the service template mode
`PE1(config)#interface xe15`	Access interface xe15
`(config-if)#switchport`	Switch to Layer-2 mode.
`PE1(config-if)#mpls-l2-circuit t5 service-template ST5`	Bind the interface to the VC with service template.
`PE1(config-if)#exit`	Exit interface mode
`PE1(config)#mpls l2-circuit-fib-entry 500 1000 2000 2.2.2.2 xe1 xe15`	Add an FTN entry; where 1000 is the incoming label, 2000 is the outgoing label, 2.2.2.2 is the endpoint, xe1 is the Provider facing interface name, and xe15 is access interface name

PE-2

`#configure terminal`	Enter configure mode.
`PE2(config)#mpls l2-circuit t5 500 1.1.1.1`	Configure the VC for PE2
`PE2(config-pseudowire)#tunnel-name t3`	Configure RSVP Tunnel name as t3
`PE2(config-pseudowire)#manual-pseudowire`	Configure VC as manual (no signaling used)
`PE2(config-pseudowire)#exit`	Exit pseudowire config mode.
`PE2(config)#service-template ST5`	Create a service template ST5
`PE2(config-svc)#match outer-vlan 5`	Configure single match criteria vlan 5
`PE2(config-svc)#exit`	Exit the service template mode
`PE2(config)#interface xe12`	Access interface xe12
`(config-if)#switchport`	Switch to Layer-2 mode.
`PE2(config-if)#mpls-l2-circuit t5 service-template ST5`	Bind the interface to the VC with service template.
`PE2(config-if)#exit`	Exit interface mode.

`PE1(config)#mpls l2-circuit-fib-entry 500 2000 1000 1.1.1.1 xe13 xe12`	Add an FTN entry; where 2000 is the incoming label, 1000 is the outgoing label, 1.1.1.1 is the endpoint, xe12 is the Provider facing interface name, and xe13 access interface name
`PE2(config)#exit`	Exit configure mode

Validation

This example shows number of configured VCs and its status.

```
PE1#sh mpls vc-table
VC-ID       Vlan-ID  Inner-Vlan-ID  Access-Intf   Network-Intf  Out Label  Tunnel-Label  Nexthop         Status
100         N/A      N/A            xe15          xe1           24320      24321         2.2.2.2         Active
300         N/A      N/A            xe15          xe1           24321      24321         2.2.2.2         Active
500         N/A      N/A            xe15          xe1           2000       24321         2.2.2.2         Active
PE1#

PE1#sh mpls l2-circuit
MPLS Layer-2 Virtual Circuit: t2, id: 100  PW-INDEX: 1 Tunnel-Name: t2
 Endpoint: 2.2.2.2
 Control Word: 0
 MPLS Layer-2 Virtual Circuit Group: none
 Bound to interface: xe15
 Virtual Circuit Type: Ethernet VLAN
 Virtual Circuit is configured as Primary
 Virtual Circuit is configured as Active
 Virtual Circuit is active
 Service-template : ST1
  Match criteria : 2


MPLS Layer-2 Virtual Circuit: t3, id: 300  PW-INDEX: 2 Tunnel-Name: t2
 Operating mode: Raw
 Endpoint: 2.2.2.2
 Control Word: 0
 MPLS Layer-2 Virtual Circuit Group: none
 Bound to interface: xe15
 Virtual Circuit Type: Ethernet
 Virtual Circuit is configured as Primary
 Virtual Circuit is configured as Active
 Virtual Circuit is active
 Service-template : ST2
  Match criteria : 3


MPLS Layer-2 Virtual Circuit: t5, id: 500  PW-INDEX: 3 Tunnel-Name: t2
 Endpoint: 2.2.2.2
 Control Word: 0
 MPLS Layer-2 Virtual Circuit Group: none
 Bound to interface: xe15
 Virtual Circuit Type: Ethernet VLAN
 Virtual Circuit is configured as Primary
 Virtual Circuit is configured as Active
 Virtual Circuit is active
 Service-template : ST5
  Match criteria : 5


PE1#
These additional commands can also be used to display information about the Layer 2 virtual circuits.
show ldp mpls-l2-circuit detail
show ldp mpls-l2-circuit VC-ID
show ldp mpls-l2-circuit VC-ID detail
show mpls l2-circuit
```

Configure Dynamic VPLS

PE1

LDP VPLS Configuration:

`(config)#mpls vpls v1 25`	Enter VPLS config mode
`(config-vpls)#service-tpid dot1.ad`	Service tp-id configuration.
`(config-vpls)#signaling ldp`	Define Signaling as LDP
`(config-vpls-sig)#vpls-type vlan`	Type VLAN configuration for VPLS
`(config-vpls-sig)#vpls-peer 2.2.2.2 tunnel-name t2`	Configure VPLS Peer with trunk-name t2
`(config-vpls-sig)#exit-signaling`	Exit Signaling LDP mode
`(config-vpls)#exit`	Exit VPLS mode
`(config)#mpls vpls v2 26`	Enter VPLS config mode
`(config-vpls)#service-tpid dot1.ad`	Service tp-id configuration.
`(config-vpls)#signaling ldp`	Define Signaling as LDP
`(config-vpls-sig)#vpls-type ethernet`	Type ethernet configuration for VPLS
`(config-vpls-sig)#vpls-peer 2.2.2.2 tunnel-name t2`	Configure VPLS Peer
`(config-vpls-sig)#exit-signaling`	Exit Signaling LDP mode
`(config-vpls)#exit`	Exit VPLS mode

PE2

LDP VPLS Configuration:

`(config)#mpls vpls v1 25`	Enter VPLS config mode
`(config-vpls)#service-tpid dot1.ad`	Service tp-id configuration.
`(config-vpls)#signaling ldp`	Define Signaling as LDP
`(config-vpls-sig)#vpls-type vlan`	Type VLAN configuration for VPLS
`(config-vpls-sig)#vpls-peer 1.1.1.1 tunnel-name t3`	Configure VPLS Peer
`(config-vpls-sig)# exit-signaling`	Exit Signaling LDP mode
`(config-vpls)#exit`	Exit VPLS mode
`(config)#mpls vpls v2 26`	Enter VPLS config mode
`(config-vpls)#service-tpid dot1.ad`	Service tp-id configuration.
`(config-vpls)#signaling ldp`	Define Signaling as LDP
`(config-vpls-sig)#vpls-type ethernet`	Type ethernet configuration for VPLS
`(config-vpls-sig)#vpls-peer 1.1.1.1 tunnel-name t3`	Configure VPLS Peer with tunnel-name t2
`(config-vpls-sig)#exit-signaling`	Exit Signaling LDP mode
`(config-vpls)#exit`	Exit VPLS mode

LDP VPLS Service Mapping Configuration

PE1

`#configure terminal`	Configure mode
`(config)#service-template template1`	Template configuration
`(config-svc)# match double-tag outer-vlan 2024 inner-vlan 2023`	Match criteria under template configuration
`(config-svc)# rewrite ingress pop outgoing-tpid dot1.q`	Action to be performed for the match.
`(config-svc)#exit`	Exit template configuration mode
`(config)#service-template template4`	Template configuration
`(config-svc)# match outer-vlan 700`	Allow VLAN 700 traffic on this VC
`(config-svc)# match double-tag outer-vlan 1200 inner-vlan 3200`	Allow double tag match with s+c tags
`(config-svc)# match untagged`	Allow untagged traffic
`(config-svc)# rewrite ingress push 300`	Push Action performed for service template
`(config-svc)#exit`	Exit configure SVC mode

Access port Configuration:

`(config)#interface xe15`	Enter the access interface xe15.
`(config-if)#switchport`	Configure interface as a layer 2 port.
`(config-if)#mpls-vpls v1 service-template template1`	Bind the VPLS to the Access Interface.
`(config-if-vpls)#exit-if-vpls`	Exit VPLS attachment-circuit mode
`(config-if)#mpls-vpls v2 service-template template4`	Bind the VPLS to the Access Interface.
`(config-if-vpls)# exit-if-vpls`	Exit VPLS attachment-circuit mode
`(config-if)#exit`	Exit Interface mode and return to Configure mode.

PE2

`#configure terminal`	Configure mode
`(config)#service-template template1`	Template configuration
`(config-svc)# match double-tag outer-vlan 2024 inner-vlan 2023`	Match criteria under template configuration
`(config-svc)# rewrite ingress pop outgoing-tpid dot1.q`	Action to be performed for the match.
`(config-svc)#exit`	Exit template configuration mode
`(config)#service-template template4`	Template configuration
`(config-svc)# match outer-vlan 700`	Allow VLAN 700 traffic on this VC
`(config-svc)# match double-tag outer-vlan 1200 inner-vlan 3200`	Allow double tag match with s+c tags

`(config-svc)# match untagged`	Allow untagged traffic
`(config-svc)# rewrite ingress push 300`	Push Action performed for service template
`(config-svc)#exit`	Exit configure SVC mode

Access port Configuration:

`(config)#interface xe12`	Enter access Interface xe12
`(config-if)#switchport`	Configure interface as a layer 2 port.
`(config-if)#mpls-vpls v1 service-template template1`	Bind the VPLS to the Access Interface.
`(config-if-vpls)#exit-if-vpls`	Exit VPLS attachment-circuit mode
`(config-if)#mpls-vpls v2 service-template template4`	Bind the VPLS to the Access Interface.
`(config-if-vpls)#exit-if-vpls`	Exit VPLS attachment-circuit mode
`(config-if)#exit`	Exit Interface mode and return to Configure mode.

Validation

Below are the example outputs of mpls vpls with tunnel-name

```
PE1#sh mpls vpls mesh
VPLS-ID    Peer Addr         Tunnel-Label  In-Label   Network-Intf   Out-Label  Lkps/St   PW-INDEX SIG-Protocol  Status
25         2.2.2.2           24321         24322      xe1            24322      2/Up      4         LDP           Active
26         2.2.2.2           24321         24323      xe1            24323      2/Up      5         LDP           Active
PE1#

PE1#sh mpls vpls detail
Virtual Private LAN Service Instance: v1, ID: 25
 SIG-Protocol: LDP
 Attachment-Circuit :UP
 Learning: Enabled
 Control-Word: Disabled
 Group ID: 0, VPLS Type: Ethernet VLAN, Configured MTU: 1500
 Description: none
 service-tpid: dot1.ad
 Operating mode: Tagged
 Svlan Id: 0
 Svlan Tpid: 88a8
 Configured interfaces:
  Interface: xe15
 Service-template : template1
  Match criteria : 2024/2023
  Action type : Pop
  Outgoing tpid : dot1.q

 Mesh Peers:
   2.2.2.2 (Up)
   Tunnel-Name: t2


Virtual Private LAN Service Instance: v2, ID: 26
 SIG-Protocol: LDP
 Attachment-Circuit :UP
 Learning: Enabled
 Control-Word: Disabled
 Group ID: 0, VPLS Type: Ethernet, Configured MTU: 1500
 Description: none
 service-tpid: dot1.ad
 Operating mode: Raw
 Configured interfaces:
```

```
  Interface: xe15
 Service-template : template4
  Match criteria : 700,
 1200/3200,
 Untagged
  Action type : Push
  Action value : 300

 Mesh Peers:
   2.2.2.2 (Up)
   Tunnel-Name: t2


PE1#
```

Configure Static VPLS

PE1

LDP VPLS Configuration:

`(config)#mpls vpls v3 27`	Enter VPLS config mode
`(config-vpls)#vpls-peer 2.2.2.2 tunnel-name t2 manual`	Configure VPLS Peer with trunk-name t2 with manual option
`(config-vpls)#exit`	Exit VPLS mode
`(config)#service-template vpls1`	Template configuration
`(config-svc)# match outer-vlan 1000`	Allow VLAN 1000 traffic on this VC
`(config-svc)#exit`	Exit service template mode

Access port Configuration:

`(config)#interface xe15`	Enter the access Interface xe15
`(config-if)#switchport`	Configure interface as a layer 2 port.
`(config-if)#mpls-vpls v3 service-template vpls1`	Bind the VPLS to the Access Interface.
`(config-if-vpls)#exit-if-vpls`	Exit VPLS attachment-circuit mode
`(config-if)#exit`	Exit from the interface mode
`(config)#vpls fib-entry 27 peer 2.2.2.2 3000 xe1 4000`	Configure VPLS FIB entry for VPLS peer PE-2

PE2

LDP VPLS Configuration:

`(config)#mpls vpls v3 27`	Enter VPLS config mode
`(config-vpls)#vpls-peer 1.1.1.1 tunnel-name t3 manual`	Configure static VPLS Peer with tunnel-name t3
`(config-vpls)#exit`	Exit VPLS mode
`(config)#service-template vpls1`	Template configuration

`(config-svc)# match outer-vlan 1000`	Allow VLAN 1000 traffic on this VC
`(config-svc)#exit`	Exit service template mode

Access port Configuration:

`(config)#interface xe12`	Enter the access interface xe12
`(config-if)#switchport`	Configure interface as a layer 2 port.
`(config-if)#mpls-vpls v3 service-template vpls1`	Bind the VPLS to the Access Interface.
`(config-if-vpls)#exit-if-vpls`	Exit VPLS attachment-circuit mode
`(config-if)#exit`	Exit interface mode.
`(config)#vpls fib-entry 27 peer 1.1.1.1 4000 xe13 3000`	Configure VPLS FIB entry for VPLS peer PE-1.

Validation

```
PE1#sh mpls vpls mesh
VPLS-ID    Peer Addr         Tunnel-Label  In-Label   Network-Intf   Out-Label  Lkps/St   PW-INDEX SIG-Protocol  Status
25         2.2.2.2           24321         24322      xe1            24322      2/Up      4         LDP           Active
26         2.2.2.2           24321         24323      xe1            24323      2/Up      5         LDP           Active
27         2.2.2.2           24321         3000       xe1            4000       2/Up      6         STATIC        Active
PE1#

PE1#sh mpls vpls v3 detail
Virtual Private LAN Service Instance: v3, ID: 27
 SIG-Protocol: STATIC
 Attachment-Circuit :UP
 Learning: Enabled
 Control-Word: Disabled
 Group ID: 0, Configured MTU: 1500
 Description: none
 service-tpid: dot1.q
 Operating mode: Raw
 Configured interfaces:
  Interface: xe15
 Service-template : vpls1
  Match criteria : 1000

 Mesh Peers:
   2.2.2.2 (Up)
   Tunnel-Name: t2

PE1#
```

\

CHAPTER 18 Signaled LLSP Configuration

This chapter contains a complete sample of configuring Signaled LLSP Configuration.

Note: Signaled LLSP is only supported in RSVP-TE.

Configure Signaled LLSP Using RSVP-TE

Note: The following configuration for establishing a trunk is required on all routers participating in label-switching. Based on the assumption that minimal configurations exist on all participating routers, other examples do not repeat this configuration

Enable Label Switching - Minimal Configuration

To establish a Signaled LLSP trunk on a system:

- Enable QoS on All LSR's.
- Configure llsp-signal map under Router RSVP on ingress LSR.
- Enable label-switching and RSVP-TE on all participating interfaces.
- Configure a trunk on the ingress router to use the best available IGP path.

Topology

In this example, the Label Switched Path (LSP) is configured using minimal configuration and is setup using the best IP nexthop available. Each router along the path is chosen by the previous router by looking up the best nexthop available in its IP routing table.

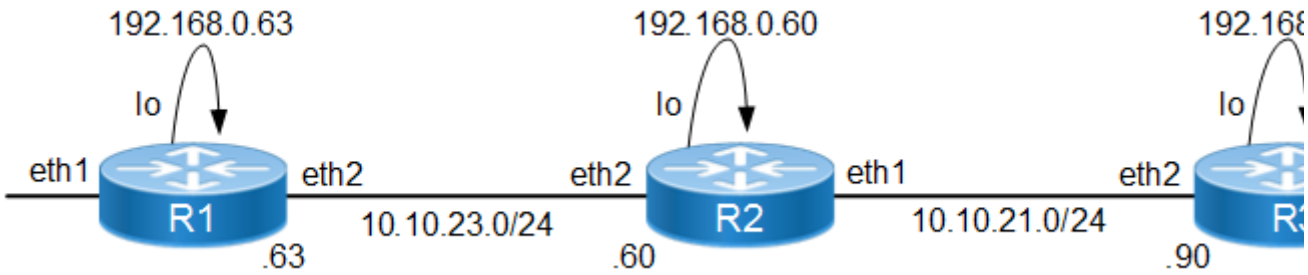


Figure 18-29: Minimal configuration Topology

R1

NSM

`#configure terminal`	Enter configure mode.
`(config)#interface eth2`	Specify the interface `(eth2)` to be configured.
`(config-if)#ip address 10.10.23.63/24`	Configure IP address for the interface
`(config-if)#label-switching`	Enable label switching on interface `eth2`.

(config-if)#exit	Exit interface mode.
(config)#interface lo	Specify the loopback (lo) interface to be configured.
(config-if)#ip address 192.168.0.63/32 secondary	Set the IP address of the loopback interface to 192.168.0.63/32
(config-if)#exit	Exit interface mode.
(config)#qos enable	Enable QoS
(config)#qos statistics	Enable QoS statistics

OSPF

#configure terminal	Enter configure mode.
(config)#router ospf 100	Configure the routing process and specify the Process ID (100). The Process ID should be a unique positive integer identifying the routing process.
(config-router)#network 10.10.23.0/24 area 0 (config-router)#network 192.168.0.63/32 area 0	Define the interface on which OSPF runs and associate the area ID (0) with the interface.
(config-router)#exit	Exit from router mode

RSVP-TE

#configure terminal	Enter configure mode.
(config)#router rsvp	Enter Configure Router mode.
(config-router)#elsp-signal-map class 1 exp 0	Enabling ELSP
(config-router)#exit	Exit Router Mode
(config)#interface eth2	Enter interface mode.
(config-if)#enable-rsvp	Enable RSVP message exchange on this interface.
(config-if)#exit	Exit interface mode.
(config)#rsvp-trunk T1	Create an RSVP trunk T1 and enter the Trunk mode.
(config-trunk)# map-route 90.90.90.0/24	Specify the destination prefix that needs to mapped to this trunk
(config-trunk)#to 192.168.0.90	Specify the IPv4 egress (destination point) for the LSP.
(config-trunk)#primary llsp class	Enable LLSP-Signaling for this trunk

DiffServ Traffic Engineering

(

config)#dste enable	Enable DSTE
(config)#mpls class-type ct0 def	Configure class-type ct0 with name default
(config)#mpls class-type ct1 voice	Configure class-type ct1 with name voice
(config)#mpls te-class te1 voice 6	Configure te-class te1 with name voice

Trunk Configuration

(config-trunk)#primary setup-priority 6	Setup priority value for a trunk
(config-trunk)#primary hold-priority 6	Configure hold priority value for the selected trunk
(config-trunk)# primary class-type voice	Configure a primary Class-Type

R2

NSM

#configure terminal	Enter configure mode.
(config)#interface eth2	Specify the interface (eth2) to be configured.
(config-if)#ip address 10.10.23.60/24	Configure IP address for the interface
(config-if)#label-switching	Enable label switching on interface eth2.
(config-if)#exit	Exit interface mode.
(config)#interface eth1	Specify the interface (eth1) to be configured.
(config-if)#ip address 10.10.21.60/24	Configure IP address for the interface
(config-if)#label-switching	Enable label switching on interface eth1.
(config-if)#exit	Exit interface mode.
(config)#interface lo	Specify the loopback (lo) interface to be configured.
(config-if)#ip address 192.168.0.60/32 secondary	Set the IP address of the loopback interface to 192.168.0.60/32
(config-if)#exit	Exit interface mode.
(config)#qos enable	Enable QoS
(config)#qos statistics	Enable QoS statistics

RSVP-TE

#configure terminal	Enter configure mode.
(config)#router rsvp	Enter Configure Router mode.
(config-router)#elsp-signal-map class 1 exp 0	Enabling ELSP
(config-router)#exit	Exit Router mode.
(config)#interface eth2	Enter interface mode.
(config-if)#enable-rsvp	Enable RSVP message exchange on this interface.
(config-if)#exit	Exit interface mode.
(config)#interface eth1	Enter interface mode.
(config-if)#enable-rsvp	Enable RSVP message exchange on this interface.
(config-if)#exit	Exit interface mode.

OSPF

`#configure terminal`	Enter configure mode.
`(config)#router ospf 100`	Configure the routing process and specify the Process ID (100). The Process ID should be a unique positive integer identifying the routing process.

`(config-router)#network 10.10.23.0/24 area 0`
`(config-router)#network 192.168.0.63/32 area 0`
`(config-router)#network 10.10.21.0/24 area 0`
	Define the interface on which OSPF runs and associate the area ID (0) with the interface.

`(config-router)#exit`	Exit from router mode

DiffServ Traffic Engineering

(

`config)#dste enable`	Enable DSTE
`(config)#mpls class-type ct0 def`	Configure class-type ct0 with name default
`(config)#mpls class-type ct1 voice`	Configure class-type ct1 with name voice
`(config)#mpls te-class te1 voice 6`	Configure te-class te1 with name voice

Trunk Configuration

`(config-trunk)#primary setup-priority 6`	Setup priority value for a trunk
`(config-trunk)#primary hold-priority 6`	Configure hold priority value for the selected trunk
`(config-trunk)# primary class-type voice`	Configure a primary Class-Type

R3

NSM

`#configure terminal`	Enter configure mode.
`(config)#interface eth2`	Specify the interface `(eth2)` to be configured.
`(config-if)#ip address 10.10.21.90/24`	Configure IP address for the interface
`(config-if)#label-switching`	Enable label switching on interface `eth2`.
`(config-if)#exit`	Exit interface mode.
`(config)#interface lo`	Specify the loopback (`lo`) interface to be configured.
`(config-if)#ip address 192.168.0.90/32 secondary`	Set the IP address of the loopback interface to `192.168.0.90/32`
`(config-if)#exit`	Exit interface mode.
`(config)#qos enable`	Enable QoS
`(config)#qos statistics`	Enable QoS statistics

RSVP-TE

`#configure terminal`	Enter configure mode.
`(config)#router rsvp`	Enter Configure Router mode.
`(config-router)#elsp-signal-map class 1 exp 0`	Enabling ELSP
`(config-router)#exit`	Exit `Router` mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#enable-rsvp`	Enable RSVP message exchange on this interface.
`(config-if)#exit`	Exit interface mode.

OSPF

`#configure terminal`	Enter configure mode.
`(config)#router ospf 100`	Configure the routing process and specify the Process ID (100). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 192.168.0.90/32 area 0` `(config-router)#network 10.10.21.0/24 area 0`	Define the interface on which OSPF runs and associate the area ID (0) with the interface.
`(config-router)#exit`	Exit from router mode

DiffServ Traffic Engineering

(

`config)#dste enable`	Enable DSTE
`(config)#mpls class-type ct0 def`	Configure class-type ct0 with name default
`(config)#mpls class-type ct1 voice`	Configure class-type ct1 with name voice
`(config)#mpls te-class te1 voice 6`	Configure te-class te1 with name voice

Trunk Configuration

`(config-trunk)#primary setup-priority 6`	Setup priority value for a trunk
`(config-trunk)#primary hold-priority 6`	Configure hold priority value for the selected trunk
`(config-trunk)# primary class-type voice`	Configure a primary Class-Type

Validation

```
#show rsvp session
Ingress RSVP:
To              From            State               Pri Rt  Style Labelin
Labelout LSPName                            Uptime  Est.time   DSType
192.168.0.90    192.168.0.63    Up                  Yes 1 1 SE    -
24321    T1-Primary                         00:11:41 0s 5ms  LLSP
Total 1 displayed, Up 1, Down 0.
```

```
#show rsvp session detail
Ingress (Primary)
192.168.0.90
  From: 192.168.0.63, LSPstate: Up, LSPname: T1-Primary
  Ingress FSM state: Operational
  Setup priority: 6, Hold priority: 6
  CSPF usage: Enabled, CSPF Retry Count: 0, CSPF Retry Interval: 30 seconds
  IGP-Shortcut: Disabled, LSP metric: 2
  LSP Protection: None
  Label in: -,  Label out:    24321
  Tspec rate: 0, Fspec rate: 0
  Policer: Not Configured
  Tunnel Id: 5001, LSP Id: 2201, Ext-Tunnel Id: 192.168.0.63
  Downstream: 10.10.23.60, xe10/1
  Path refresh: 30 seconds (RR enabled) (due in 29 seconds)
  Resv lifetime: 157 seconds (due in 143 seconds)
  Retry count: 0, intrvl: 30 seconds
  RRO re-use as ERO: Disabled
  Label Recording: Disabled
  Admin Groups: none
  Configured Path: none
  Session Explicit Route Detail :
   10.10.23.60/32 strict
   10.10.21.90/32 strict
  Record route: <self> 10.10.23.60 10.10.21.90
  Style: Shared Explicit Filter
  Traffic type: controlled-load
  Minimum Path MTU: 1500
  LSP Type:  L-LSP
  LLSP CLASS: 6
  DSTE Class Type Number: 1, Class Type name: voice
  Last Recorded Error Code: None
  Last Recorded Error Value: None
  Node where Last Recorded Error originated: None
  Trunk Type: mpls


#show policy-map in eth2

Interface eth2
Global statistics status : enabled

Service-policy (queuing) output: default-out-policy
-----------------------------------
Class-map (queuing): q0
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q1
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q2
 priority level 1
      output       : 0 packets, 0 bytes
```

```
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q3
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q4
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q5
 priority level 1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q6
 priority level 1
      output       : 530026 packets, 33921664 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): q7
 priority level 1
      output       : 17 packets, 1088 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q0
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q1
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q2
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q3
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q4
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q5
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q6
      output       : 0 packets, 0 bytes
      dropped      : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output       : 25 packets, 2146 bytes
```

```
      dropped      : 0 packets, 0 bytes

Wred Drop Statistics :
----------------------
 green  : 0 packets
 yellow : 0 packets
 red    : 0 packets
```

CHAPTER 19 Virtual Private LAN Service Configuration

This chapter contains configurations for Virtual Private LAN Service (VPLS).

VPLS Raw Mode

The examples show the minimum configuration required for enabling a VPLS Mesh peer between PE-1, PE-2, and PE-3 in raw mode.

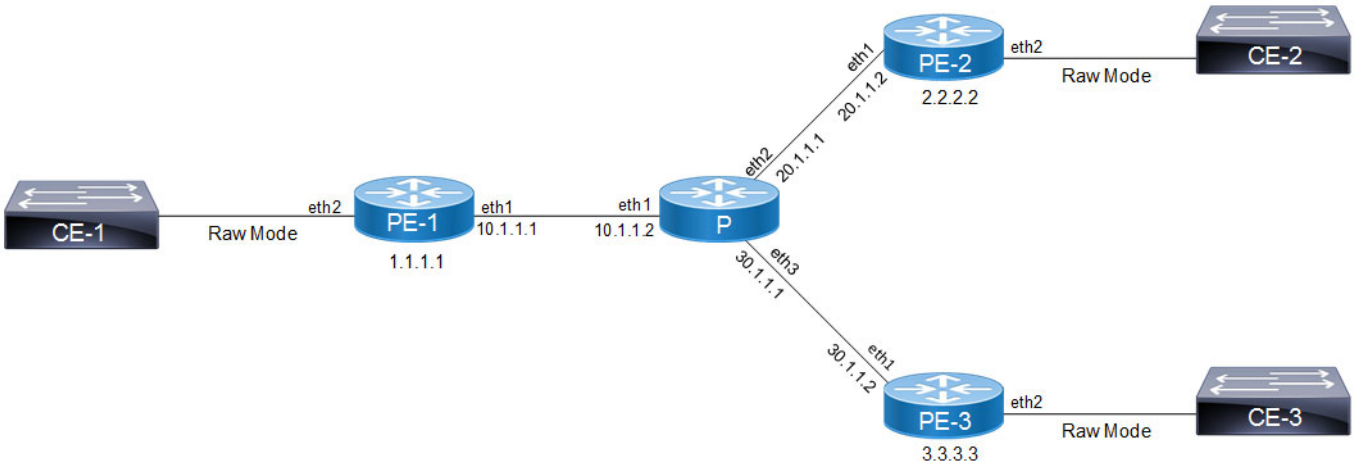


Figure 19-30: VPLS Mesh Peers Raw Mode

Configuration

PE-1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode.
`(config-if)#ip address 1.1.1.1/32 secondary`	Configure IP address for the loopback interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth1`	Specify the Interface (eth1) to be configured.
`(config-if)#ip address 10.10.1.1/24`	Configure IP address for the interface.
`(config-if)#no shutdown`	Administratively brining up the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 100`	Configure the routing process and specify the routing process ID(100).
`(config-router)#network 10.1.1.0/24 area 0` `(config-router)#network 1.1.1.1/32 area 0`	Define the interface address on which the OSPF runs and associate an area ID(0) with the interface address.
`(config-router)#exit`	Exit router mode.

(config)#router ldp	Enter router mode for LDP.
(config-router)#targeted-peer ipv4 2.2.2.2	Configuring targeted LDP sessions to PE-2
(config-router-targeted-peer)#exi	Exit config-router-targeted-peer mode
(config-router)#targeted-peer ipv4 3.3.3.3	Enter targeted-peer-mode and PE-3
(config-router-targeted-peer)#exit	Exit config-router-targeted-peer mode
(config-router)#exit	Exit router configuration mode.
(config)#interface eth1	Enter interface mode.
(config-if)#label-switching	Enable label switching capability on the interface.
(config-if)#enable-ldp ipv4	Enabling LDP on the interface.
(config-if)#exit	Exit interface mode.
(config)#mpls vpls VPLS1 100	Configuring VPLS instance with name and VPLS ID.
(config-vpls)#signaling ldp	Enabling LDP signaling for the VPLS instance.
(config-vpls-sig)#vpls-peer 2.2.2.2 (config-vpls-sig)#vpls-peer 3.3.3.3	Configuring VPLS mesh peers.
(config-vpls-sig)#exit-signaling	Exit from VPLS signaling mode.
(config-vpls)#exit	Exit from VPLS Mode.
(config)#service-template st1	Template configuration
(config-svc)# exit	Exit service template mode
(config)#interface eth2	Specify the attachment circuit interface.
(config-if)#switchport	Configuring the attachment circuit interface as Layer-2.
(config-if)mpls-vpls VPLS1 service-template st1	Associating the VPLS Instance to the attachment circuit interface.
(config-if-vpls)#exit	Exit VPLS attachment-circuit mode
(config-if)exit	Exit interface mode.
(config)#exit	Exit configure mode.
#copy running-config startup-config	Save the configuration.

P

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 9.9.9.9/32 secondary	Configure IP address for the loopback interface.

(config-if)#exit	Exit interface mode.
(config)#interface eth1	Specify the interface to be configured.
(config-if)#ip address 10.10.1.2/24	Configure IP address for the interface.
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode.
(config-if)#ip address 20.20.1.2/24	Configure IP address for the interface.
(config-if)#exit	Exit interface mode.
(config)#interface eth3	Enter interface mode.
(config-if)#ip address 30.30.1.2/24	Configure IP address for the interface.
(config-if)#exit	Exit interface mode.
(config)#router ospf 100	Configure the routing process and specify the routing process ID(100).
(config-router)#network 10.1.1.0/24 area 0 (config-router)#network 20.20.1.0/24 area 0 (config-router)#network 30.30.1.0/24 area 0 (config-router)#network 9.9.9.9/32 area 0	Define the interface address on which the OSPF runs and associate an area ID(0) with the Interface address.
(config-router)#exit	Exit router mode.
(config)#router ldp	Enter router mode for LDP.
(config-router)#exit	Exit router mode.
(config)#interface eth1	Enter interface mode.
(config-if)#label-switching	Enable label switching capability on the interface.
(config-if)#enable-ldp ipv4	Enabling LDP on the interface.
(congig-if)#exit	Exit interface configuration mode.
(config)#interface eth2	Specify the interface to be configured.
(config-if)#label-switching	Enable label switching capability on the interface.
(config-if)#enable-ldp ipv4	Enabling LDP on the interface.
(congig-if)#exit	Exit interface mode.
(config)#interface eth3	Enter interface mode.
(config-if)#label-switching	Enable label switching capability on the interface.
(config-if)#enable-ldp ipv4	Enabling LDP on the interface.
(congig-if)#exit	Exit interface mode.
(config)#exit	Exit configure mode.
#copy running-config startup-config	Save the configuration.

PE-2

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 2.2.2.2/32 secondary	Configure IP address for the loopback interface.

`(config-if)#exit`	Exit interface mode.
`(config)#interface eth1`	Specify the Interface (eth1) to be configured.
`(config-if)#ip address 20.20.1.1/24`	Configure IP address for the interface.
`(config-if)#no shutdown`	Administratively brining up the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 100`	Configure the routing process and specify the routing process ID(100).
`(config-router)#network 20.20.1.0/24 area 0` `(config-router)#network 2.2.2.2/32 area 0`	Define the interface address on which the OSPF runs and associate an area ID(0) with the interface address.
`(config-router)#exit`	Exit router mode.
`(config)#router ldp`	Enter router mode for LDP.
`(config-router)#targeted-peer ipv4 1.1.1.1`	Configuring targeted LDP sessions to PE-2.
`(config-router-targeted-peer)#exit`	Exit targeted-peer-mode
`(config-router)#targeted-peer ipv4 3.3.3.3`	Configuring targeted LDP sessions to PE-3
`(config-router-targeted-peer)#exit`	Exit targeted-peer-mode
`(config-router)#exit`	Exit router configuration mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#label-switching`	Enable label switching capability on the interface.
`(config-if)#enable-ldp ipv4`	Enabling LDP on the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#mpls vpls VPLS1 100`	Configuring VPLS instance with name and VPLS ID.
`(config-vpls)#signaling ldp`	Enabling LDP signaling for the VPLS instance.
`(config-vpls-sig)#vpls-peer 1.1.1.1` `(config-vpls-sig)#vpls-peer 3.3.3.3`	Configuring VPLS mesh peers.
`(config-vpls-sig)#exit-signaling`	Exit from VPLS signaling mode.
`(config-vpls)#exit`	Exit from VPLS Mode.
`(config)#service-template st1`	Template configuration.
`(config-svc)# exit`	Exit service template mode.
`(config)#interface eth2`	Specify the attachment circuit interface.
`(config-if)#switchport`	Configuring the attachment circuit interface as Layer-2.
`(config-if)mpls-vpls VPLS1 service-template st1`	Associating the VPLS Instance to the attachment circuit interface.

(config-if-vpls)#exit	Exit VPLS attachment-circuit mode
(config-if)exit	Exit interface mode.
(config)#exit	Exit configure mode.
#copy running-config startup-config	Save the configuration.

PE-3

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 3.3.3.3/32 secondary	Configure IP address for the loopback interface.
(config-if)#exit	Exit interface mode.
(config)#interface eth1	Specify the Interface (eth1) to be configured.
(config-if)#ip address 30.30.1.1/24	Configure IP address for the interface.
(config-if)#no shutdown	Administratively brining up the interface.
(config-if)#exit	Exit interface mode.
(config)#router ospf 100	Configure the routing process and specify the routing process ID(100).
(config-router)#network 30.30.1.0/24 area 0 (config-router)#network 3.3.3.3/32 area 0	Define the interface address on which the OSPF runs and associate an area ID(0) with the interface address.
(config-router)#exit	Exit router mode.
(config)#router ldp	Enter router mode for LDP.
(config-router)#targeted-peer ipv4 1.1.1.1	Configuring targeted LDP sessions to PE-2
(config-router-targeted-peer)#exit	Exit targeted-peer-mode
(config-router)#targeted-peer ipv4 2.2.2.2	Configuring targeted LDP sessions to PE-3
(config-router-targeted-peer)#exit	Exit targeted-peer-mode
(config-router)#exit	Exit router configuration mode.
(config)#interface eth1	Enter interface mode.
(config-if)#label-switching	Enable label switching capability on the interface.
(config-if)#enable-ldp ipv4	Enabling LDP on the interface.
(config-if)#exit	Exit interface mode.
(config)#mpls vpls VPLS1 100	Configuring VPLS instance with name and VPLS ID.

(config-vpls)#signaling ldp	Enabling LDP signaling for the VPLS instance.
(config-vpls-sig)#vpls-peer 1.1.1.1 (config-vpls-sig)#vpls-peer 2.2.2.2	Configuring VPLS mesh peers.
(config-vpls-sig)#exit-signaling	Exit from VPLS signaling mode.
(config-vpls)#exit	Exit from VPLS Mode.
(config)#service-template st1	Template configuration.
(config-svc)# exit	Exit service template mode.
(config)#interface eth2	Specify the attachment circuit interface.
(config-if)#switchport	Configuring the attachment circuit interface as Layer-2.
(config-if)mpls-vpls VPLS1 service-template st1	Associating the VPLS Instance to the attachment circuit interface.
(config-if-vpls)#exit	Exit VPLS attachment-circuit mode
(config-if)exit	Exit interface mode.
(config)#exit	Exit configure mode.
#copy running-config startup-config	Save the configuration.

Validation

PE-1

Verify VPLS Session

```
PE1#show mpls vpls detail
Virtual Private LAN Service Instance: VPLS1, ID: 100
 SIG-Protocol: LDP
 Attachment-Circuit :UP
 Learning: Enabled
 Group ID: 0, VPLS Type: Ethernet, Configured MTU: 1500
 Description: none
 service-tpid: dot1.q
 Operating mode: Raw
 Configured interfaces:
  Interface: xe17
 Service-template : s1
  Match criteria : Accept all

 Mesh Peers:
   2.2.2.2 (Up)
   3.3.3.3 (Up)

PE1#
```

Verify VPLS Mesh Peer

```
PE1#sh mpls vpls mesh

VPLS-ID       Peer Addr         Tunnel-Label  In-Label   Network-Intf   Out-Label  Lkps/
St   PW-INDEX  SIG-Protocol   Status   Ecmp-Group100           1.1.1.1
```

```
301          4000       eth6                    3000       2/Up              1
STATIC          Active      N/A100                2.2.2.2                    302
4500       eth6                    3500       2/Up              2             STATIC
Active       N/A
```

VPLS Tagged Mode

The examples show the minimum configuration required for enabling a VPLS Mesh peer between PE-1, PE-2, and PE-3 in Tagged Mode. In the below example PE-1 and PE-2 uses VLAN 10 for binding the VPLS instance to the attachment circuit and PE-3 used VLAN 20 where it shows that VLAN swapping is supported.

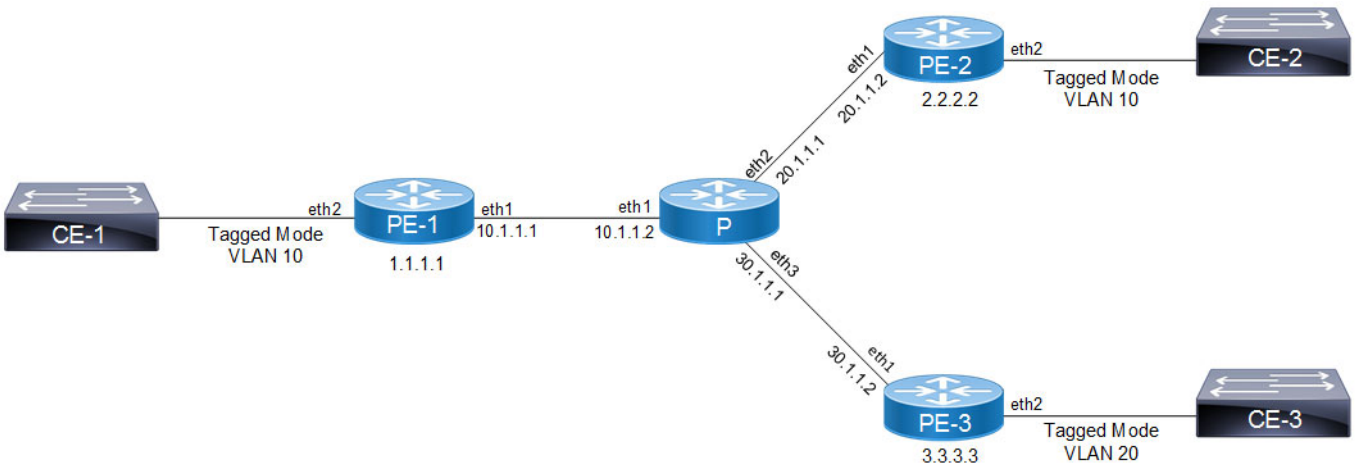


Figure 19-31: VPLS Mesh Peers Tagged Mode

Configuration

PE-1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode.
`(config-if)#ip address 1.1.1.1/32 secondary`	Configure IP address for the loopback interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth1`	Specify the Interface (eth1) to be configured.
`(config-if)#ip address 10.10.1.1/24`	Configure IP address for the interface.
`(config-if)#no shutdown`	Administratively brining up the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 100`	Configure the routing process and specify the routing process ID(100).

(config-router)#network 10.1.1.0/24 area 0 (config-router)#network 1.1.1.1/32 area 0	Define the interface address on which the OSPF runs and associate an area ID(0) with the interface address.
(config-router)#exit	Exit router mode.
(config)#router ldp	Enter router mode for LDP.
(config-router)#targeted-peer ipv4 2.2.2.2	Configuring targeted LDP sessions to PE-2
(config-router-targeted-peer)#exit	Exit targeted peer mode
(config-router-targeted-peer)#targeted-peer ipv4 3.3.3.3	Configuring targeted LDP sessions to PE-3
(config-router-targeted-peer)#exit	Exit targeted peer mode
(config-router)#exit	Exit router configuration mode
(config)#interface eth1	Enter interface mode
(config-if)#label-switching	Enable label switching capability on the interface.
(config-if)#enable-ldp ipv4	Enabling LDP on the interface.
(config-if)#exit	Exit interface mode.
(config)#mpls vpls VPLS1 100	Configuring VPLS instance with name and VPLS ID.
(config-vpls)#signaling ldp	Enabling LDP signaling for the VPLS instance.
(config-vpls-sig)#vpls-type vlan	Configuring VPLS type as VLAN mode.
(config-vpls-sig)#vpls-peer 2.2.2.2 (config-vpls-sig)#vpls-peer 3.3.3.3	Configuring VPLS mesh peers.
(config-vpls-sig)#exit-signaling	Exit from VPLS signaling mode.
(config-vpls)#exit	Exit from VPLS Mode.
(config)#mpls vpls v4 28	Enter VPLS config mode
(config-vpls)#signaling ldp	Define Signaling as LDP
(config-vpls-sig)#vpls-type vlan	Type VLAN configuration for VPLS
(config-vpls-sig)#vpls-peer 2.2.2.2	Configure VPLS Peers
config-vpls-sig)#vpls-peer 3.3.3.3	Configure VPLS Peers
(config-vpls-sig)# exit-signaling	Exit Signaling LDP mode
(config-vpls)#exit	Exit VPLS mode
(config)#service-template st1	Template configuration.
(config-svc)# match outer-vlan 10	Match criteria under template configuration
(config-svc)# exit	Exit service template mode.
(config)#interface eth2	Specify the attachment circuit interface.
(config-if)#switchport	Configuring the attachment circuit interface as Layer-2.

(config-if)mpls-vpls VPLS1 service-template st1	Associating the VPLS Instance to the attachment circuit interface to match service template st1.
(config-if-vpls)#exit	Exit VPLS attachment-circuit mode
(config-if)exit	Exit interface mode.
(config)#exit	Exit configure mode.
#copy running-config startup-config	Save the configuration.

service-template with multiple match support

This is to validate the multiple match criteria support in a service template. When multiple match statements are configured only rewrite push is supported, rewrite translate and pop are not supported.

(config)#service-template template4	Template configuration
(config-svc)# match outer-vlan 700	Allow VLAN 700 traffic on this VC
(config-svc)# match double-tag outer-vlan 1200 inner-vlan 3200	Allow double tag match with s+c tags
(config-svc)# match untagged	Allow untagged traffic
(config-svc)# rewrite ingress push 300	Push Action performed for service template
(config-svc)#exit	Exit configure SVC mode
(config)#interface eth2	Specify the attachment circuit interface.
(config-if)#switchport	Configuring the attachment circuit interface as Layer-2.
(config-if)mpls-vpls v4 service-template template4	Associating the VPLS Instance to the attachment circuit interface.
(config-if-vpls)#exit	Exit VPLS attachment-circuit mode

P

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 9.9.9.9/32 secondary	Configure IP address for the loopback interface.
(config-if)#exit	Exit interface mode.
(config)#interface eth1	Specify the interface to be configured.
(config-if)#ip address 10.10.1.2/24	Configure IP address for the interface.
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode.
(config-if)#ip address 20.20.1.2/24	Configure IP address for the interface.
(config-if)#exit	Exit interface mode.
(config)#interface eth3	Enter interface mode.
(config-if)#ip address 30.30.1.2/24	Configure IP address for the interface.
(config-if)#exit	Exit interface mode.

(config)#router ospf 100	Configure the routing process and specify the routing process ID(100).
(config-router)#network 10.1.1.0/24 area 0 (config-router)#network 20.20.1.0/24 area 0 (config-router)#network 30.30.1.0/24 area 0 (config-router)#network 9.9.9.9/32 area 0	Define the interface address on which the OSPF runs and associate an area ID(0) with the Interface address.
(config-router)#exit	Exit router mode.
(config)#router ldp	Enter router mode for LDP.
(config-router)#exit	Exit router mode.
(config)#interface eth1	Enter interface mode.
(config-if)#label-switching	Enable label switching capability on the interface.
(config-if)#enable-ldp ipv4	Enabling LDP on the interface.
(congig-if)#exit	Exit interface configuration mode.
(config)#interface eth2	Specify the interface to be configured.
(config-if)#label-switching	Enable label switching capability on the interface.
(config-if)#enable-ldp ipv4	Enabling LDP on the interface.
(congig-if)#exit	Exit interface mode.
(config)#interface eth3	Enter interface mode.
(config-if)#label-switching	Enable label switching capability on the interface.
(config-if)#enable-ldp ipv4	Enabling LDP on the interface.
(congig-if)#exit	Exit interface mode.
(config)#exit	Exit configure mode.
#copy running-config startup-config	Save the configuration.

PE-2

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 2.2.2.2/32 secondary	Configure IP address for the loopback interface.
(config-if)#exit	Exit interface mode.
(config)#interface eth1	Specify the Interface (eth1) to be configured.
(config-if)#ip address 20.20.1.1/24	Configure IP address for the interface.
(config-if)#no shutdown	Administratively brining up the interface.
(config-if)#exit	Exit interface mode.
(config)#router ospf 100	Configure the routing process and specify the routing process ID(100).
(config-router)#network 20.20.1.0/24 area 0 (config-router)#network 2.2.2.2/32 area 0	Define the interface address on which the OSPF runs and associate an area ID(0) with the interface address.
(config-router)#exit	Exit router mode.

(config)#router ldp	Enter router mode for LDP.
(config-router)#targeted-peer ipv4 1.1.1.1	Configuring targeted LDP sessions to PE-2
(config-router-targeted-peer)#exit	Exit targeted peer mode
(config-router-targeted-peer)#targeted-peer ipv4 3.3.3.3	Configuring targeted LDP sessions to PE-3
(config-router-targeted-peer)#exit	Exit targeted peer mode
(config-router-targeted-peer)#exit-targeted-peer-mode	Exit targeted peer mode.
(config-router)#exit	Exit router configuration mode.
(config)#interface eth1	Enter interface mode.
(config-if)#label-switching	Enable label switching capability on the interface.
(config-if)#enable-ldp ipv4	Enabling LDP on the interface.
(config-if)#exit	Exit interface mode.
(config)#mpls vpls VPLS1 100	Configuring VPLS instance with name and VPLS ID.
(config-vpls)#signaling ldp	Enabling LDP signaling for the VPLS instance.
(config-vpls-sig)#vpls-type vlan	Configuring VPLS type as VLAN mode.
(config-vpls-sig)#vpls-peer 1.1.1.1 (config-vpls-sig)#vpls-peer 3.3.3.3	Configuring VPLS mesh peers.
(config-vpls-sig)#exit-signaling	Exit from VPLS signaling mode.
(config-vpls)#exit	Exit from VPLS Mode.
(config)#mpls vpls v4 28	Enter VPLS config mode
(config-vpls)#signaling ldp	Define Signaling as LDP
(config-vpls-sig)#vpls-type vlan	Type VLAN configuration for VPLS
(config-vpls-sig)#vpls-peer 1.1.1.1	Configure VPLS Peers
config-vpls-sig)#vpls-peer 3.3.33	Configure VPLS Peers
(config-vpls-sig)# exit-signaling	Exit Signaling LDP mode
(config-vpls)#exit	Exit VPLS mode
(config)#service-template st1	Template configuration.
(config-svc)#match outer-vlan 10	Match criteria under template configuration
(config-svc)#exit	Exit service template mode.
(config)#service-template template4	Template configuration
(config-svc)#match outer-vlan 700	Allow VLAN 700 traffic on this VC
(config-svc)#match double-tag outer-vlan 1200 inner-vlan 3200	Allow double tag match with s+c tags
(config-svc)#match untagged	Allow untagged traffic

(config-svc)# rewrite ingress push 300	Push Action performed for service template
(config-svc)#exit	Exit configure SVC mode
(config)#interface eth2	Specify the attachment circuit interface.
(config-if)#switchport	Configuring the attachment circuit interface as Layer-2.
(config-if)mpls-vpls VPLS1 service-template st1	Associating the VPLS Instance to the attachment circuit interface to match service template st1.
(config-if)mpls-vpls v4 service-template template4	Associating the VPLS Instance to the attachment circuit interface.
(config-if-vpls)#exit	Exit VPLS attachment-circuit mode
(config-if)exit	Exit interface mode.
(config)#exit	Exit configure mode.
#copy running-config startup-config	Save the configuration.

PE-3

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 3.3.3.3/32 secondary	Configure IP address for the loopback interface.
(config-if)#exit	Exit interface mode.
(config)#interface eth1	Specify the Interface (eth1) to be configured.
(config-if)#ip address 30.30.1.1/24	Configure IP address for the interface.
(config-if)#no shutdown	Administratively brining up the interface.
(config-if)#exit	Exit interface mode.
(config)#router ospf 100	Configure the routing process and specify the routing process ID(100).
(config-router)#network 30.30.1.0/24 area 0 (config-router)#network 3.3.3.3/32 area 0	Define the interface address on which the OSPF runs and associate an area ID(0) with the interface address.
(config-router)#exit	Exit router mode.
(config)#router ldp	Enter router mode for LDP.
(config-router)#targeted-peer ipv4 1.1.1.1	Configuring targeted LDP sessions to PE-2
(config-router-targeted-peer)#exit	Exit targeted peer mode
(config-router-targeted-peer)#targeted-peer ipv4 2.2.2.2	Configuring targeted LDP sessions to PE-3
config-router-targeted-peer)#exit	Exit targeted peer mode
(config-router)#exit	Exit router configuration mode.

(config)#interface eth1	Enter interface mode.
(config-if)#label-switching	Enable label switching capability on the interface.
(config-if)#enable-ldp ipv4	Enabling LDP on the interface.
(config-if)#exit	Exit interface mode.
(config)#mpls vpls VPLS1 100	Configuring VPLS instance with name and VPLS ID.
(config-vpls)#signaling ldp	Enabling LDP signaling for the VPLS instance.
(config-vpls-sig)#vpls-type vlan	Configuring VPLS type as VLAN mode.
(config-vpls-sig)#vpls-peer 1.1.1.1 (config-vpls-sig)#vpls-peer 2.2.2.2	Configuring VPLS mesh peers.
(config-vpls-sig)#exit-signaling	Exit from VPLS signaling mode.
(config-vpls)#exit	Exit from VPLS Mode.
(config)#mpls vpls v4 28	Enter VPLS config mode
(config-vpls)#signaling ldp	Define Signaling as LDP
(config-vpls-sig)#vpls-type vlan	Type VLAN configuration for VPLS
(config-vpls-sig)#vpls-peer 1.1.1.1	Configure VPLS Peers
(config-vpls-sig)#vpls-peer 2.2.2.2	Configure VPLS Peers
(config-vpls-sig)#exit-signaling	Exit from VPLS signaling mode.
(config-vpls)#exit	Exit from VPLS Mode.
(config)#service-template st1	Template configuration.
(config-svc)# match outer-vlan 20	Match criteria under template configuration
(config-svc)# exit	Exit service template mode.
(config)#service-template template4	Template configuration
(config-svc)# match outer-vlan 700	Allow VLAN 700 traffic on this VC
(config-svc)# match double-tag outer-vlan 1200 inner-vlan 3200	Allow double tag match with s+c tags
(config-svc)# match untagged	Allow untagged traffic
(config-svc)# rewrite ingress push 300	Push Action performed for service template
(config-svc)#exit	Exit configure SVC mode
(config)#interface eth2	Specify the attachment circuit interface.
(config-if)#switchport	Configuring the attachment circuit interface as Layer-2.
(config-if)mpls-vpls VPLS1 service-template st1	Associating the VPLS Instance to the attachment circuit interface to match service template st1.
(config-if-vpls)#exit	Exit VPLS attachment-circuit mode
(config-if)exit	Exit interface mode.
(config)#exit	Exit configure mode.
#copy running-config startup-config	Save the configuration.

Validation

PE-1

Verify VPLS Session

```
PE1#sh mpls vpls detail
Virtual Private LAN Service Instance: VPLS1, ID: 100
 SIG-Protocol: LDP
 Attachment-Circuit :UP
 Learning: Enabled
 Group ID: 0, VPLS Type: Ethernet VLAN, Configured MTU: 1500
 Description: none
 service-tpid: dot1.q
 Operating mode: Tagged
 Svlan Id: 0
 Svlan Tpid: 8100
 Configured interfaces:
  Interface: eth2
 Service-template : s1
  Match criteria : 10

 Mesh Peers:
   2.2.2.2 (Up)
   3.3.3.3 (Up)
PE1#
Virtual Private LAN Service Instance: v4, ID: 28
 SIG-Protocol: LDP
 Attachment-Circuit :UP
 Learning: Enabled
 Group ID: 0, VPLS Type: Ethernet VLAN, Configured MTU: 1500
 Description: none
 service-tpid: dot1.q
 Operating mode: Tagged
 Svlan Id: 0
 Svlan Tpid: 8100
 Configured interfaces:
  Interface: eth2
 Service-template : template4
     Match criteria : 700
    1200/3200
    Untagged
    Action type : Push
    Action value : 300


 Mesh Peers:
   2.2.2.2 (Up)
   3.3.3.3 (Up)
PE1#
```

Verify VPLS Mesh Peer

```
PE1#sh mpls vpls mesh
```

```
VPLS-ID       Peer Addr         Tunnel-Label  In-Label   Network-Intf   Out-
Label  Lkps/St   PW-INDEX  SIG-Protocol   Status   Ecmp-Group100
100         2.2.2.2       24320         24322      eth2           24321
2/Up      1         LDP           Active      N/A
100         3.3.3.3       24325         24321      eth2           24323
2/Up      1         LDP           Active      N/A
28          2.2.2.2       24327         24324      eth2           24325      2/
Up      1         LDP           Active      N/A
28          3.3.3.3       24345         24325      eth2           24324      2/
Up      1         LDP           Active      N/A
```

Validation for the Number of Configured VPLS Instances

This example below shows number of configured VPLS instances.

```
PE-1#show mpls vpls count
------------------------------
Total VPLS instances    : 2
Active VPLS instances   : 2
Inactive VPLS instances : 2
------------------------------
```

The example below shows the Count of VPLS from LDP standpoint

```
.
PE-1#show ldp vpls count
------------------------------
Total VPLS instances    : 2
Active VPLS instances   : 2
Inactive VPLS instances : 0
------------------------------
```

The example below shows the number of MAC addresses learnt by the VPLS.

```
PE-1#show mpls vpls mac-address count
Total no of MAC addresses learnt :6
```

CHAPTER 20 Static VPLS Configuration

This chapter includes step-by-step configurations for Static VPLS. It also contains an overview of the concepts of Static VPLS.

Overview

Virtual Private LAN Service (VPLS) is a way to provide Ethernet-based multipoint-to-multipoint communication over IP-MPLS networks. It allows geographically-dispersed sites to share an Ethernet broadcast domain by connecting sites through pseudowires. A set of Martini circuits is grouped by a common VPLS identifier to achieve this service objective.

The VPLS identifier is exchanged with the labels, so that both PWs can be linked and be associated with a particular VPLS instance.

Configure Static VPLS

In the following examples, VPLS (v1) is configured on PE-2 with Static VPLS-Peers PE-1 and PE-3 using static LSPs.

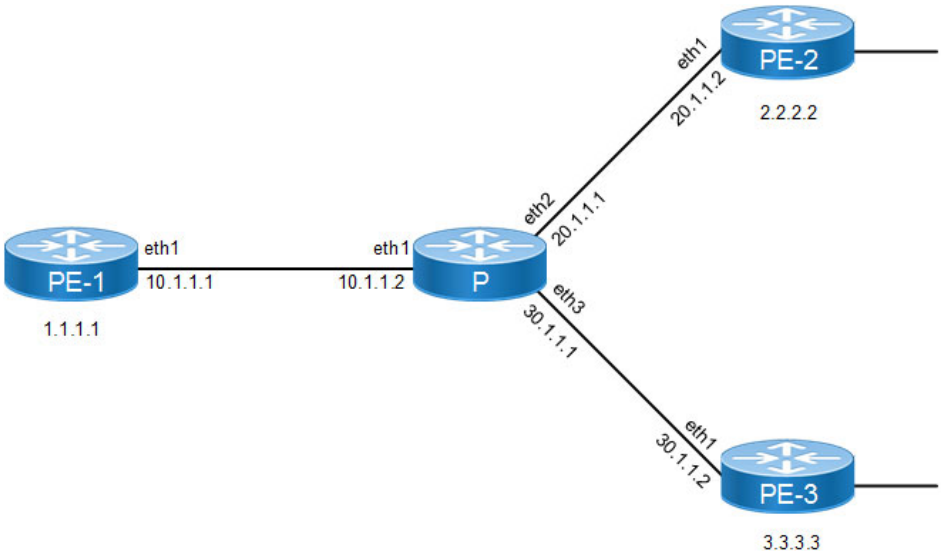


Figure 20-32: Static Virtual Private LAN Service Topology

PE-1

`#configure terminal`	Enter configure mode.
`(config)#mpls ftn-entry tunnel-id 11 2.2.2.2/32 102 10.10.1.2 eth1 primary`	Configure MPLS FTN entry for the creation of a static LSP to PE-2.
`(config)#mpls ftn-entry tunnel-id 22 3.3.3.3/32 103 10.10.1.2 eth1 primary`	Configure MPLS FTN entry for the creation of a static LSP to PE-3.
`(config)#mpls ilm-entry 201 pop`	Configure MPLS ILM entry for the creation of a static LSP to PE-2.
`(config)#mpls ilm-entry 301 pop`	Configure MPLS ILM entry for the creation of a static LSP to PE-3.

(config)#mpls vpls v1 100	Configure VPLS v1 with ID 100 on PE-1.
(config-vpls)#vpls-peer 2.2.2.2 tunnel-id 11 manual	Configure PE-2 as a manual VPLS peer using the static LSP tunnel ID 11
(config-vpls)#vpls-peer 3.3.3.3 tunnel-id 22 manual	Configure PE-3 as a manual VPLS peer using the static LSP tunnel ID 22.
(config-vpls)#exit	Exit Configure VPLS mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ip address 10.10.1.1/24	Configure IP address for the interface.
(config-if)#label-switching	Enable label switching capability on the interface.
(config-if)#exit	Exit interface mode
(config)#interface lo	Enter interface mode
(config-if)#ip address 1.1.1.1/32 secondary	Configure IP address for the loopback interface.
(config-if)#exit	Exit interface mode
(config)#router ospf 100	Configure the routing process and specify the routing process ID(100).
(config-router)#network 10.10.1.0/24 area 0	Define the interface address on which the OSPF runs and associate an area ID(0) with the interface address.
(config-router)#network 1.1.1.1/32 area 0	Define the interface address on which the OSPF runs and associate an area ID(0) with the interface address.
(config-router)#exit	Exit router mode
(config-if)#label-switching	Configure label switching
(config-if)#exit	Exit interface mode.
(config)#service-template st1	Template configuration
(config-svc)#exit	Exit service template mode
(config)#interface eth2	Enter interface mode.
(config-if)#switchport	Switch to Layer-2 mode.
(config-if)#mpls-vpls v1 service-template st1	Bind the VPLS to the Access Interface.
(config-if-vpls)#exit	Exit VPLS attachment-circuit mode
(config-if)#exit	Exit interface mode.
(config)#vpls fib-entry 100 peer 2.2.2.2 1000 eth1 2000	Configure VPLS FIB entry for VPLS peer PE-2.
(config)#vpls fib-entry 100 peer 3.3.3.3 3000 eth1 4000	Configure VPLS FIB entry for VPLS peer PE-3.

P

#configure terminal	Enter configure mode
(config)#interface lo	Enter interface mode
(config-if)#ip address 9.9.9.9/32 secondary	Configure IP address for the loopback interface.
(config-if)#exit	Exit interface mode
(config)#interface eth1	Specify the interface to be configured.
(config-if)#ip address 10.10.1.2/24	Configure IP address for the interface.
(config-if)#label-switching	Enable label switching capability on the interface.

(config-if)#exit	Exit interface mode
(config)#interface eth2	Enter interface mode
(config-if)#ip address 20.20.1.2/24	Configure IP address for the interface.
(config-if)#label-switching	Enable label switching capability on the interface.
(config-if)#exit	Exit interface mode
(config)#interface eth3	Enter interface mode
(config-if)#ip address 30.30.1.2/24	Configure IP address for the interface.
(config-if)#label-switching	Enable label switching capability on the interface.
(config-if)#exit Exit	interface mode
(config)#router ospf 100	Configure the routing process and specify the routing process ID(100).
(config-router)#network 10.1.1.0/24 area 0	Define the interface address on which the OSPF runs and associate an area ID(0) with the Interface address.
(config-router)#network 20.20.1.0/24 area 0	Define the interface address on which the OSPF runs and associate an area ID(0) with the Interface address.
(config-router)#network 30.30.1.0/24 area 0	Define the interface address on which the OSPF runs and associate an area ID(0) with the Interface address.
(config-router)#network 9.9.9.9/32 area 0	Define the interface address on which the OSPF runs and associate an area ID(0) with the Interface address.
(config-router)#exit	Exit router mode

PE-2

#configure terminal	Enter Configure mode
(config)# mpls ftn-entry tunnel-id 11 1.1.1.1/32 201 20.20.1.2 eth1 primary	Configure MPLS FTN entry for the creation of a static LSP to PE-1, and designate eth1 as primary.
(config)# mpls ftn-entry tunnel-id 33 3.3.3.3/32 301 20.20.1.2 eth1 primary	Configure MPLS FTN entry for the creation of a static LSP to PE-3, and designate eth1 as primary.
(config)#mpls ilm-entry 102 pop	Configure MPLS ILM entry for the creation of a static LSP to PE-1.
(config)#mpls ilm-entry 302 pop	Configure MPLS ILM entry for the creation of a static LSP to PE-3
(config)#mpls vpls v1 100	Configure VPLS v1 with ID 100 on PE-2.
(config-vpls)#vpls-peer 1.1.1.1 tunnel-id 11 manual	Configure PE-1 as a manual VPLS peer using static LSP tunnel ID
(config-vpls)#vpls-peer 3.3.3.3 tunnel-id 33 manual	Configure PE-3 as a manual VPLS peer using static LSP tunnel ID
(config-vpls)#exit	Exit Configure VPLS mode
(config)#interface lo	Enter interface mode
(config-if)#ip address 2.2.2.2/32 secondary	Configure IP address for the loopback interface.
(config-if)#exit	Exit interface mode
(config)#interface eth1	Enter interface mode
(config-if)#ip address 20.20.1.1/24	Configure IP address for the interface
(config-if)#label-switching	Configure label switching
(config-if)#exit	Exit interface mode

(config)#service-template st1	Template configuration
(config-svc)#exit	Exit service template mode
(config)#interface eth2	Enter interface mode
(config-if)#switchport Switch to Layer-2 mode	Make port Layer-2
(config-if)#mpls-vpls v1 service-template st1	Bind the VPLS to the Access Interface
(config-if-vpls)#exit	Exit VPLS attachment-circuit mode
(config-if)#exit	Exit interface mode
(config)# vpls fib-entry 100 peer 1.1.1.1 2500 eth1 1500	Configure VPLS FIB entry for VPLS peer PE-1.
(config)# vpls fib-entry 100 peer 3.3.3.3 3500 eth1 4500	Configure VPLS FIB entry for VPLS peer PE-3.
(config)#router ospf 100	Configure the routing process and specify the routing process ID(100).
(config-router)#network 20.20.1.0/24 area 0	Define the interface address on which the OSPF runs and associate an area ID(0) with the interface address.
(config-router)#network 2.2.2.2/32 area 0	Define the interface address on which the OSPF runs and associate an area ID(0) with the interface address.
(config-router)#exit	Exit router mode
(config)#exit	Exit configure mode

PE-3

#configure terminal	Enter Configure mode
(config)#mpls ftn-entry tunnel-id 11 1.1.1.1/32 301 30.30.1.2 eth1 primary	Configure MPLS FTN entry for the creation of a static LSP to PE-1.
(config)# mpls ftn-entry tunnel-id 22 2.2.2.2/32 302 30.30.1.2 eth1 primary	Configure MPLS FTN entry for the creation of a static LSP to PE-2.
(config)#mpls ilm-entry 103 pop	Configure MPLS ILM entry for the creation of a static LSP to PE-1.
(config)#mpls ilm-entry 203 pop	Configure MPLS ILM entry for the creation of a static LSP to PE-2.
(config)#mpls vpls v1 100	Configure VPLS v1 with ID 100 on PE-3.
(config-vpls)#vpls-peer 1.1.1.1 tunnel-id 11 manual	Configure PE-1 as a manual VPLS peer using static LSP tunnel ID 11.
(config-vpls)#vpls-peer 2.2.2.2 tunnel-id 22 manual	Configure PE-2 as a manual VPLS peer using static LSP tunnel ID 22.
(config-vpls)#exit	Exit Configure VPLS mode
(config)#interface lo	Enter interface mode
(config-if)#ip address 3.3.3.3/32 secondary	Configure IP address for the loopback interface.
(config-if)#exit	Exit interface mode
(config)#interface eth1	Enter interface mode
(config-if)#ip address 30.30.1.1/24	Configure IP address for the interface
(config-if)#label-switching	Configure label switching
(config-if)#exit	Exit interface mode

(config)#service-template st1	Template configuration
(config-svc)#exit	Exit service template mode
(config)#interface eth2	Enter interface mode
(config-if)#switchport	Switch to Layer-2 mode
(config-if)#mpls-vpls v1 service-template st1	Bind the VPLS to the Access Interface.
(config-if-vpls)#exit	Exit VPLS attachment-circuit mode
(config-if)#exit	Exit interface mode.
(config)#vpls fib-entry 100 peer 1.1.1.1 4000 eth1 3000	Configure VPLS FIB entry for VPLS peer PE-1.
(config)#vpls fib-entry 100 peer 2.2.2.2 4500 eth1 3500	Configure VPLS FIB entry for VPLS peer PE-2.
(config)#router ospf 100	Configure the routing process and specify the routing process ID(100).
(config-router)#network 30.30.1.0/24 area 0	Define the interface address on which the OSPF runs and associate an area ID(0) with the interface address.
(config-router)#network 3.3.3.3/32 area 0	Define the interface address on which the OSPF runs and associate an area ID(0) with the interface address.
(config-router)#exit	Exit router mode

Validation

Enter the commands listed in the sections below to confirm the configurations.

Verify VPLS Session on PE-1

```
#show mpls vpls detail
Virtual Private LAN Service Instance: vpls3100, ID: 3100
SIG-Protocol: BGP
Route-Distinguisher :65010:3100
Route-Target :65010:3100
VE-ID :31
Attachment-Circuit :UP
Learning: Enabled
Group ID: 0, Configured MTU: 9216
Description: none
service-tpid: dot1.q
Operating mode: Raw
Configured interfaces:
Interface: xe26
Service-template : vpls3100_3100_13100
Match criteria : 3100
Action type : Translate
Action value : 4075
Outgoing tpid : dot1.q

 Mesh Peers:
   2.2.2.2 (Up)
 Mesh Peers:
```

```
   3.3.3.3 (Up)
PE1#
```

Verify VPLS Peer

```
#show mpls vpls mesh
VPLS-ID    Peer Addr         Tunnel-Label  In-Label   Network-Intf   Out-Label  Lkps/St
PW-INDEX  SIG-Protocol  Status  Ecmp-Group
100        2.2.2.2           24320         24320      eth1           24321      2/Up
1         LDP           Active    N/A
100        3.3.3.3           24321         24321      eth1           24320      2/Up
2         LDP           Active    N/A
PE1#
```

Remove Configurations

Follow these steps to remove VPLS peer and VPLS spoke FIB entries from router PE-2.

`#configure terminal`	Enter configure mode
`(config)#no vpls fib-entry 100 peer 1.1.1.1`	Remove VPLS FIB for VPLS peer PE-1.
`(config)#no vpls fib-entry 100 peer 3.3.3.3`	Remove VPLS FIB for VPLS peer PE-3.
`(config)#exit`	Exit Configure mode

CHAPTER 21 BGP-VPLS Configuration

This chapter contains configurations for VPLS with Border Gateway Protocol Signaling.

Overview

Virtual Private LAN Service (VPLS) is a way to provide Ethernet-based multipoint-to-multipoint communication over IP/MPLS networks. It allows geographically-dispersed sites to share an Ethernet broadcast domain by connecting sites through pseudowires. A set of Kompella circuits is grouped by a common VPLS identifier to achieve this service objective.

A Pseudowire (PW) consists of a pair of point-to-point, single-hop unidirectional LSPs in opposite directions, each identified by a PW label, also called a Virtual Connection (VC) label.

The Border Gateway Protocol (BGP) is used to signaling VCs and for auto-discovery of neighbors. A service provider may use either LDP or RSVP-TE or add static provisioning to set up LSP tunnels to transport data through virtual circuits.

The VPLS identifier is exchanged with the labels, so that both PWs can be linked and associated with a particular VPLS instance.

Note: In Inter-AS, OcNOS accepts information from any other AS but the same VPN-ID/VPLS-ID (*: VPLS-ID). OcNOS does not have explicit RD/RT (import/export) support for BGP VPLS. RD/RT are automatically generated based on the configured BGP AS number and VPN-ID/VPLS-ID as (AS-number: VPN-ID).

Topology

The diagram depicts the topology for the configuration examples that follow.

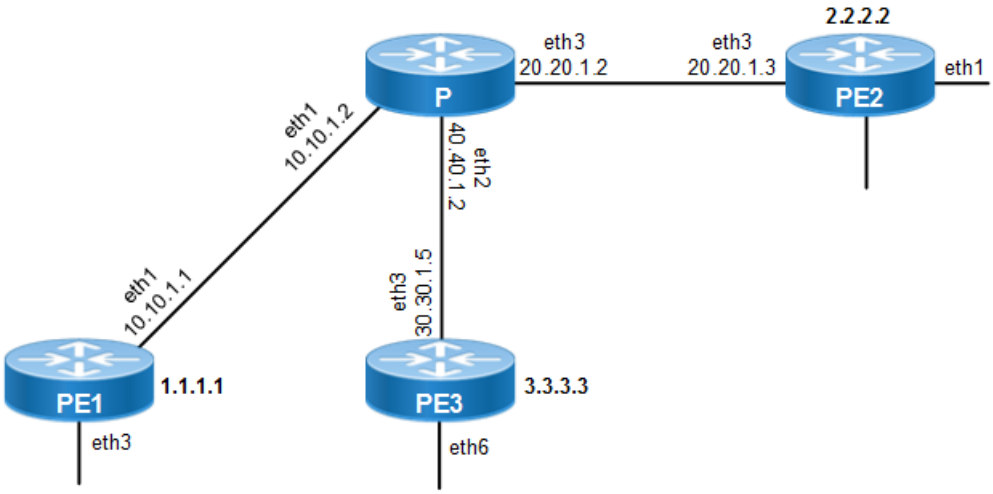


Figure 21-33: Sample Topology for VPLS with BGP Signaling

BGP-VPLS Configuration

PE-1

`#configure terminal`	Enter configuration mode.
`(config)#interface eth1`	Specify the interface `(eth1)` to be configured.
`(config-if)#ip address 10.10.1.1/24`	Set the IP address of the interface to `10.10.1.1/24`.
`(config-if)#label-switching`	Enable label switching on interface `eth1`.
`(config-if)#exit`	Exit interface mode.
`(config)#interface lo`	Specify the loopback address.
`(config-if)#ip address 1.1.1.1/32`	Set the IP address of the loopback interface to `1.1.1.1/32`.
`(config-if)#exit`	Exit interface mode
`(config)#mpls vpls v1 25`	Create an instance of VPLS, and switch to the VPLS command mode, by specifying the VPLS name (v1) and VPLS ID (`25`).
`(config-vpls)#vpls-mtu 1400`	Configure the MTU for the VPLS. (Default is 1500; range is <576 - 65535>.
`(config-vpls)#signaling bgp`	Enter the Signaling bgp mode for BGP VPLS.
`(config-vpls-sig)#ve-id 1`	Configure VE ID, which is mandatory for BGP VPLS, otherwise, Signaling does not take place. VE ID should be unique per VPLS instance.
`(config-vpls-sig)#exit`	Exit is a mandatory command for signaling BGP configuration to take affect. If exit is not given BGP signaling does not take place.
`(config-vpls)#exit`	Exit VPLS mode.
`(config)#service-template v1`	Configure service template
`(config-svc)#match all`	Configure the match condition
`(config-svc)#exit`	Exit interface mode
`(config)#interface eth3`	Specify the interface `(eth3)` to be configured.
`(config-if)#switchport`	Switch to Layer-2 mode. (VPLS can be bound only on the Layer-2 port.)
`(config-if)#mpls-vpls v1 service-template v1`	Bind the VPLS to the Access Interface.
`(config-if-vpls)#exit`	Exit VPLS attachment-circuit mode
`(config-if)#exit`	Exit interface mode.

Note: VE IDs range is from 1 to 64. Administrator should configure the VE ID's accordingly in their Network.

PE1 - LDP

`#configure terminal`	Enter configuration mode
`(config)#router ldp`	Enter Router LDP mode.

(config-router)#transport-address ipv4 1.1.1.1	Configure the transport address for a label space by binding the address to a loopback address.
(config-router)#exit	Exit Router mode.
(config)#interface eth1	Specify the interface (eth1) to be configured.
(config-if)#enable-ldp ipv4	Enable LDP on interface eth1.
(config-if)#exit	Exit interface mode.

PE1 - OSPF

#configure terminal	Enter configure mode
(config)#router ospf 1	Configure the OSPF routing process, and specify the process ID.
(config-router)#network 10.10.1.0/24 area 0	Define the interfaces on which OSPF runs, and specify the backbone area 0.
(config-router)#network 1.1.1.1/32 area 0	
(config-router)#exit	Exit Router mode.

PE1 - BGP

#configure terminal	Enter configuration mode.
(config)#router bgp 100	Enter BGP Configure mode.
(config-router)#neighbor 2.2.2.2 remote-as 100	Configure PE2 as an iBGP peer.
(config-router)#neighbor 2.2.2.2 update-source lo	Update the source as loopback for iBGP peering with the remote PE2 router.
(config-router)#neighbor 3.3.3.3 remote-as 100	Configure PE3 as an iBGP peer.
(config-router)#neighbor 3.3.3.3 update-source lo	Update the source as loopback for iBGP peering with the remote PE3 router
(config-router)#address-family l2vpn vpls	Configure address-family l2vpn vpls.
(config-router-af)#neighbor 2.2.2.2 activate	Activate PE2 in the VPLS address family.
(config-router-af)#neighbor 3.3.3.3 activate	Activate PE3 in the VPLS address family.

PE2

#configure terminal	Enter configuration mode.
(config)#interface eth3	Specify the interface (eth3) to be configured.
(config-if)#ip address 20.20.1.3/24	Set the IP address of the interface to 20.20.1.3/24.
(config-if)#label-switching	Enable label switching on interface eth3.
(config-if)#exit	Exit interface mode.
(config)#interface lo	Specify the loopback address.
(config-if)#ip address 2.2.2.2/32	Set the IP address of the loopback interface to 2.2.2.2/32.

(config-if)#exit	Exit interface mode.
(config)#mpls vpls v1 25	Create an instance of VPLS, and switch to the VPLS command mode, by specifying the VPLS name (v1) and VPLS ID (25).
(config-vpls)#vpls-mtu 1400	Configure the MTU for the VPLS. (Default is 1500; range is <576 - 65535>.)
(config-vpls)#signaling bgp	Enter the Signaling BGP mode for BGP VPLS.
(config-vpls-sig)#ve-id 2	Configure ve-id, which is mandatory for BGP VPLS. Without a ve-id Signaling does not take place. VE ID should be unique per VPLS instance.
(config-vpls-sig)#exit	Exit is a mandatory command for signaling BGP configuration to take affect. If exit is done, BGP signaling does not take place.
(config-vpls)#exit	Exit VPLS mode.
(config)#service-template v1	Configure service template
(config-svc)#match all	Configure the match condition
(config-svc)#exit	Exit interface mode
(config)#interface eth1	Specify the interface (eth1) to be configured.
(config-if)#switchport	Switch to Layer-2 mode. (VPLS can only be bound on the Layer-2 port.)
(config-if)#mpls-vpls service-template v1	Bind the VPLS to the Access Interface.
(config-if-vpls)#exit	Exit VPLS attachment-circuit mode
(config-if)#exit	Exit interface mode.

Note: VE ID's range is from 1 to 64. Administrator should configure the VE ID's accordingly in their Network.

PE2 - LDP

#configure terminal	Enter configuration mode
(config)#router ldp	Enter Router LDP mode.
(config-router)#transport-address ipv4 2.2.2.2	Configure the transport address for a label space by binding the address to a loopback address.
(config-router)#exit	Exit Router mode.
(config)#interface eth3	Specify the interface (eth3) to be configured.
(config-if)#enable-ldp ipv4	Enable LDP on the specified interface (eth3).
(config-if)#exit	Exit interface mode.

PE2 - OSPF

#configure terminal	Enter configuration mode.
(config)#router ospf 1	Configure the OSPF routing process, and specify the process ID.

(config-router)#network 20.20.1.0/24 area 0	Define the interfaces on which OSPF runs, and specify the backbone area 0.
(config-router)#network 2.2.2.2/32 area 0	
(config-router)#exit	Exit Router mode.

PE2 - BGP

#configure terminal	Enter configuration mode.
(config)#router bgp 100	Enter BGP router mode.
(config-router)#neighbor 1.1.1.1 remote-as 100	Configure PE1 as an iBGP peer.
(config-router)#neighbor 1.1.1.1 update-source lo	Update the source as loopback for iBGP peering with the remote PE1 router.
(config-router)#neighbor 3.3.3.3 remote-as 100	Configure PE3 as an iBGP peer.
(config-router)#neighbor 3.3.3.3 update-source lo	Update the source as loopback for iBGP peering with the remote PE3 router.
(config-router)#address-family l2vpn vpls	Configure address-family l2vpn vpls.
(config-router-af)#neighbor 1.1.1.1 activate	Activate PE1 in the VPLS address family.
(config-router-af)#neighbor 3.3.3.3 activate	Activate PE3 in the VPLS address family.

PE3

#configure terminal	Enter configuration mode.
(config)#interface eth3	Specify the interface (eth3) to be configured.
(config-if)#ip address 40.40.1.5/24	Set the IP address of the interface to 40.40.1.5/24.
(config-if)#label-switching	Enable label switching on interface eth3.
(config-if)#exit	Exit interface mode.
(config)#interface lo	Specify the loopback address.
(config-if)#ip address 3.3.3.3/32	Set the IP address of the loopback interface to 3.3.3.3/32.
(config-if)#exit	Exit interface mode.
(config)#mpls vpls v1 25	Create an instance of VPLS, and switch to the VPLS command mode, by indicating the VPLS name (v1) and VPLS ID (25).
(config-vpls)#vpls-mtu 1400	Configure the MTU for the VPLS. Default is 1500; range is <576 - 65535>.
(config-vpls)#signaling bgp	Enter the Signaling BGP mode, for BGP VPLS.
(config-vpls-sig)#exit	Exit is a mandatory command for signaling BGP configuration to take affect. If exit is not done, BGP signaling does not take place.
(config-vpls)#exit	Exit VPLS mode.
(config)#service-template v1	Configure service template
(config-svc)#match all	Configure the match condition

(config-svc)#exit	Exit interface mode
(config)#interface eth6	Specify the interface (eth6) to be configured.
(config-if)#switchport	Switch to Layer-2 mode. (VPLS can be bound only on the Layer-2 port.)
(config-if)#mpls-vpls v1 service-template v1	Bind the VPLS to the Access Interface.
(config-if-vpls)#exit	Exit VPLS attachment-circuit mode
(config-if)#exit	Exit interface mode.

Note: VE ID's range is from 1 to 64. Administrator should configure the VE ID's accordingly in their Network.

PE3 - LDP

#configure terminal	Enter configuration mode.
(config)#router ldp	Enter Router LDP mode.
(config-router)#transport-address ipv4 3.3.3.3	Configure the transport address for a label space by binding the address to a loopback address.
(config-router)#exit	Exit Router mode.
(config)#interface eth3	Specify the interface (eth3) to be configured.
(config-if)#enable-ldp ipv4	Enable LDP on the interface.
(config-if)#exit	Exit interface mode.

PE3 - OSPF

#configure terminal	Enter configuration mode.
(config)#router ospf 1	Configure the OSPF routing process, and specify the process ID.
(config-router)#network 40.40.1.0/24 area 0	Define the interfaces on which OSPF runs, and specify the backbone area 0.
(config-router)#network 3.3.3.3/32 area 0	
(config-router)#exit	Exit Router mode.

PE3 - BGP

#configure terminal	Enter configuration mode.
(config)#router bgp 100	Enter BGP Router mode.
(config-router)#neighbor 1.1.1.1 remote-as 100	Configure PE1 as an iBGP peer.
(config-router)#neighbor 1.1.1.1 update-source lo	Update the source as loopback for iBGP peering with the remote PE1 router.
(config-router)#neighbor 2.2.2.2 remote-as 100	Configure PE2 as an iBGP peer.
(config-router)#neighbor 2.2.2.2 update-source lo	Update the source as loopback for iBGP peering with the remote PE2 router.
(config-router)#address-family l2vpn vpls	Configure address-family l2vpn vpls.

(config-router-af)#neighbor 1.1.1.1 activate	Activate PE1 in the VPLS address family.
(config-router-af)#neighbor 2.2.2.2 activate	Activate PE2 in the VPLS address family.

P

#configure terminal	Enter configuration mode.
(config)#interface eth1	Specify the interface (eth1) to be configured.
(config-if)#ip address 10.10.1.2/24	Set the IP address of the interface to 10.10.1.2/24.
(config-if)#label-switching	Enable label switching on interface eth1.
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Specify the interface (eth2) to be configured.
(config-if)#ip address 40.40.1.2/24	Set the IP address of the interface to 40.40.1.2/24.
(config-if)#label-switching	Enable label switching on interface eth2.
(config-if)#exit	Exit interface mode.
(config)#interface eth3	Specify the interface (eth3) to be configured.
(config-if)#ip address 20.20.1.2/24	Set the IP address of the loopback interface to 20.20.1.2/24.
(config-if)#label-switching	Enable label switching on interface eth3.
(config-if)#exit	Exit interface mode.

P - LDP

#configure terminal	Enter configuration mode.
(config)#router ldp	Enter Router LDP mode.
(config-router)#exit	Exit Router mode.
(config)#interface eth1	Specify the interface (eth1) to be configured.
(config-if)#enable-ldp ipv4	Enable LDP on the interface.
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Specify the interface (eth2) to be configured.
(config-if)#enable-ldp ipv4	Enable LDP on the interface.
(config-if)#exit	Exit interface mode.
(config)#interface eth3	Specify the interface (eth3) to be configured.
(config-if)#enable-ldp ipv4	Enable LDP on the interface.
(config-if)#exit	Exit interface mode.

P - OSPF

#configure terminal	Enter configuration mode.
(config)#router ospf 1	Configure the OSPF routing process, and specify the process ID.

(config-router)#network 10.10.1.0/24 area 0	Define the interfaces on which OSPF runs, and specify the backbone area 0.
(config-router)#network 20.20.1.0/24 area 0	
(config-router)#network 40.40.1.0/24 area 0	
(config-router)#exit	Exit Router mode.

Note: BGP L2VPN VPLS Route Reflector is not supported.

Validation

PE1

```
#show mpls vpls detail
Virtual Private LAN Service Instance: v1, ID: 25
 SIG-Protocol: BGP
  Route-Distinguisher :100:25
  Route-Target :100:25
  VE-ID :1
 Attachment-Circuit :UP
 Learning: Enabled
 Group ID: 0, Configured MTU: 1400
 Description: none
 Redundancy admin role: Primary  Redundancy oper role: Primary
 Configured interfaces:   Interface: eth3      oper-state UP  Service-template
: v1  Match criteria : Accept all

 Mesh Peers:
   2.2.2.2 (Up)
   3.3.3.3 (Up)

#show mpls vpls mesh
VPLS-ID    Peer Addr    Tunnel-Label  In-Label   Network-Intf   Out-Label
Lkps/St   PW-INDEX SIG-Protocol  Status   Ecmp-Group
25       2.2.2.2      3            24969      eth1            26125      2/
Up      1298      BGP           Active      N/A
25       3.3.3.3      24677        24961      eth1            25605      2/
Up      1297      BGP           Active      N/A

#show bgp l2vpn vpls detail
VPLS ID: 25
VE-ID: 1
Discovered Peers: 2
Route-Target: 1:100
Local RD: 2:100
 Mesh Peers:
  Address:2.2.2.2, RD:2:100, VE-ID:2
  VC Details: VC-ID:610
  Remote (LB:26120,VBO:1,VBS:64)  Local (LB:24960,VBO:1,VBS:64)
  LB sent on known VEID:Yes
  In Label:24969, Out Label:26125
  PW Status:Established
  VC Installed:Yes
 All Local LB:
  LB:24960,VBO:1,VBS:64

  Address:3.3.3.3, RD:2:100, VE-ID:3
  VC Details: VC-ID:62
```

```
 Remote (LB:25600,VBO:1,VBS:64)  Local (LB:24960,VBO:1,VBS:64)
 LB sent on known VEID:Yes
 In Label:24961, Out Label:25605
 PW Status:Established
 VC Installed:Yes

#show bgp l2vpn vpls 25
VPLS ID: 25
VE-ID: 1
Discovered Peers: 2
Route-Target: 1:100
Local RD: 2:100
 Mesh Peers:
  Address:2.2.2.2, RD:2:100, VE-ID:2
  VC Details: VC-ID:610
  Remote (LB:26120,VBO:1,VBS:64)  Local (LB:24960,VBO:1,VBS:64)
  LB sent on known VEID:Yes
  In Label:24969, Out Label:26125
  PW Status:Established
  VC Installed:Yes
 All Local LB:
 LB:24960,VBO:1,VBS:64

 Address:3.3.3.3, RD:2:100, VE-ID:3
 VC Details: VC-ID:62
 Remote (LB:25600,VBO:1,VBS:64)  Local (LB:24960,VBO:1,VBS:64)
 LB sent on known VEID:Yes
 In Label:24961, Out Label:25605
 PW Status:Established
 VC Installed:Yes
```

CHAPTER 22 Static VPLS Service Mapping Configuration

Overview

This chapter includes step-by-step configurations for static VPLS. It also contains an overview of the concepts of Static VPLS. Virtual Private LAN Service (VPLS) is a way to provide Ethernet-based multipoint-to-multipoint communication over IP- MPLS networks. It allows geographically-dispersed sites to share an Ethernet broadcast domain by connecting sites through pseudowires.

Topology

The diagram depicts the topology for the configuration examples that follow.

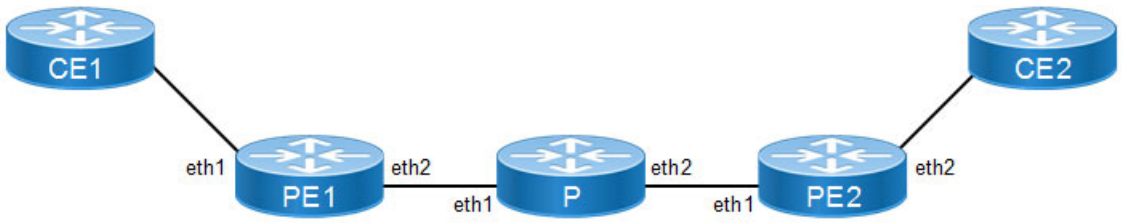


Figure 22-34: Static VPLS SM

Configuration

PE-1

Loopback Interface

`#configure terminal`	Enter configuration mode.
`(config)#interface lo`	Enter interface mode for the loopback interface.
`(config-if)#ip address 21.21.21.21/32 secondary`	Configure IP address on loopback interface.
`(config-if)#exit`	Exit interface mode

Interface Configuration

`(config)#interface eth2`	Enter interface mode for eth2.
`(config-if)#ip address 10.10.23.21/24`	Configure IP address on the interface.
`(config-if)#label-switching`	Enable label switching on the interface.
`(config-if)#exit`	Exit interface mode

Static VPLS Configuration

`(config)#mpls vpls v1 25`	Enter VPLS configuration mode
`(config-vpls)#vpls-peer 23.23.23.23 tunnel-id 1 manual`	Configure VPLS peer
`(config-vpls)#exit`	Exit from VPLS configuration mode
`(config)#mpls vpls v2 26`	Enter VPLS configuration mode
`(config-vpls)#vpls-peer 23.23.23.23 tunnel-id 1 manual`	Configure VPLS peer
`(config-vpls)#exit`	Exit from VPLS configuration mode
`(config)#mpls vpls v3 27`	Enter VPLS configuration mode
`(config-vpls)#vpls-peer 23.23.23.23 tunnel-id 1 manual`	Configure VPLS peer
`(config-vpls)#end`	Exit from VPLS configuration and configuration mode

FIB Entry Configuration

`#configure terminal`	Enter configuration mode.
`(config)#mpls ftn-entry tunnel-id 1 23.23.23.23/32 100 10.10.23.22 eth2 primary`	Configure Static LSP FTN entry
`(config)#mpls ilm-entry 250 pop`	Configure ILM entry
`(config)#exit`	Exit

P1

Loopback Interface

`#configure terminal`	Enter configuration mode.
`(config)#interface lo`	Enter interface mode for the loopback interface.
`(config-if)#ip address 22.22.22.22/32 secondary`	Configure IP address on loopback interface.
`(config-if)#exit`	Exit interface mode

Interface Configuration

`(config)#interface eth1`	Enter interface mode for eth1.
`(config-if)#ip address 10.10.23.22/24`	Configure IP address on the interface.
`(config-if)#label-switching`	Enable label switching on the interface.
`(config-if)#exit`	Exit interface mode
`(config)#interface eth2`	Enter interface mode for eth2.
`(config-if)#ip address 10.10.21.22/24`	Configure IP address on the interface.
`(config-if)#label-switching`	Enable label switching on the interface.
`(config-if)#exit`	Exit interface mode

FIB Entry Configuration

`#configure terminal`	Enter configure mode.
`(config)#mpls ilm-entry 100  swap 200 eth2 10.10.21.23 23.23.23.23/32`	Configure Static LSP ILM entry
`(config)#mpls ilm-entry 150  swap 250 eth1 10.10.23.21 21.21.21.21/32`	Configure ILM entry
`(config)#exit`	Exit

PE-2

Loopback Interface

`#configure terminal`	Enter configuration mode.
`(config)#interface lo`	Enter interface mode for the loopback interface.
`(config-if)#ip address 23.23.23.23/32 secondary`	Configure IP address on loopback interface.
`(config-if)#exit`	Exit interface mode

Interface Configuration

`(config)#interface eth1`	Enter interface mode for eth1.
`(config-if)#ip address 10.10.21.23/24`	Configure IP address on the interface.
`(config-if)#label-switching`	Enable label switching on the interface.
`(config-if)#exit`	Exit interface mode

Static VPLS Configuration

`(config)#mpls vpls v1 25`	Enter VPLS configuration mode
`(config-vpls)#vpls-peer 21.21.21.21 tunnel-id 1 manual`	Configure VPLS peer
`(config-vpls)#exit`	Exit from VPLS configuration mode
`(config)#mpls vpls v2 26`	Enter VPLS configuration mode
`(config-vpls)#vpls-peer 21.21.21.21 tunnel-id 1 manual`	Configure VPLS peer
`(config-vpls)#exit`	Exit from VPLS configuration mode
`(config)#mpls vpls v3 27`	Enter VPLS configuration mode
`(config-vpls)#vpls-peer 21.21.21.21 tunnel-id 1 manual`	Configure VPLS peer
`(config-vpls)#exit`	Exit from VPLS configuration and configuration mode
`(config)#mpls vpls v4 28`	Enter VPLS configuration mode
`(config-vpls)#vpls-peer 21.21.21.21 tunnel-id 1 manual`	Configure VPLS peer
`(config-vpls)#exit`	Exit from VPLS configuration and configuration mode

FIB Entry Configuration

`(config)#mpls ftn-entry tunnel-id 1 21.21.21.21/32 150 10.10.21.22 eth1`	Configure Static LSP FTN entry
`(config)#mpls ilm-entry 200 pop`	Configure ILM entry
`(config)#exit`	Exit

Static VPLS Service Mapping Configuration

PE-1

POP

`#configure terminal`	Enter configuration mode.
`(config)#service-template template1`	Template configuration
`(config-svc)#match double-tag outer-vlan 2024 inner-vlan 2023`	Match criteria under template configuration
`(config-svc)#rewrite ingress pop outgoing-tpid dot1.q`	Action to be performed for the match.
`(config-svc)#exit`	Exit template configuration mode

XLATE

`(config)#service-template template2`	Template configuration
`(config-svc)#match double-tag outer-vlan 2030 inner-vlan 2024`	Match criteria under template configuration
`(config-svc)#rewrite ingress translate 2026 outgoing-tpid dot1.q`	Action to be performed for the match
`(config-svc)#exit`	Exit template configuration mode

PUSH

`(config)#service-template template3`	Template configuration
`(config-svc)#rewrite ingress push 300`	Action to be performed for the default match .
`(config-svc)#exit`	Exit template configuration mode

PUSH-service-template with multiple match support

This is to validate the multiple match criteria support in a service template. When multiple match statements are configured only rewrite push is supported, rewrite translate and pop are not supported.

`(config)#service-template template4`	Template configuration
`(config-svc)# match outer-vlan 700`	Allow VLAN 700 traffic on this VC

(config-svc)# match double-tag outer-vlan 1200 inner-vlan 3200	Allow double tag match with s+c tags
(config-svc)# match untagged	Allow untagged traffic
(config-svc)# rewrite ingress push 300	Push Action performed for service template
(config-svc)#exit	Exit configure SVC mode

Access port Configuration

(config)#interface eth1	Enter the Interface mode for ethernet1.
(config-if)#switchport	Configure interface as L2 interface
(config-if)#mpls-vpls v1 service-template template1	Configure template configuration.
(config_if_vpls)#no ac-admin-status	Making Ac-admin-status Up
(config_if_vpls)#exit	Exit Interface VPLS mode and return to Interface mode.
(config-if)#mpls-vpls v2 service-template template2	Configure template configuration.
(config_if_vpls)#no ac-admin-status	Making Ac-admin-status Up
(config_if_vpls)#exit	Exit Interface VPLS mode and return to Interface mode.
(config-if)#mpls-vpls v3 service-template template3	Configure template configuration.
(config_if_vpls)#no ac-admin-status	Making Ac-admin-status Up
(config_if_vpls)#exit	Exit Interface VPLS mode and return to Interface mode.
(config-if)#mpls-vpls v4 service-template template4	Configure template configuration.
(config_if_vpls)#no ac-admin-status	Making Ac-admin-status Up
(config_if_vpls)#exit	Exit Interface mode and return to Configure mode.
(config_if)#exit	Exit interface mode.
(config)#vpls fib-entry 25 peer 23.23.23.23 1001 eth2 2001	Configure access port
(config)#vpls fib-entry 26 peer 23.23.23.23 1002 eth2 2002	Configure access port
(config)#vpls fib-entry 27 peer 23.23.23.23 1003 eth2 2003	Configure access port
(config)#vpls fib-entry 28 peer 23.23.23.23 1004 eth2 2004	Configure access port

PE-2

POP

#configure terminal	Configure mode
(config)#service-template template1	Template configuration
(config-svc)#match double-tag outer-vlan 2024 inner-vlan 2023	Match criteria under template configuration

`(config-svc)#rewrite ingress pop outgoing-tpid dot1.q`	Action to be performed for the match.
`(config-svc)#exit`	Exit template configuration mode

XLATE

`(config)#service-template template2`	Template configuration
`(config-svc)#match double-tag outer-vlan 2030 inner-vlan 2024`	Match criteria under template configuration
`(config-svc)#rewrite ingress translate 2026 outgoing-tpid dot1.q`	Action to be performed for the match
`(config-svc)#exit`	Exit template configuration mode

PUSH

`(config)#service-template template3`	Template configuration
`(config-svc)#rewrite ingress push 300`	Action to be performed for the default match .
`(config-svc)#exit`	Exit template configuration mode

PUSH-service-template with multiple match

This is to validate the multiple match criteria support in a service template. When multiple match statements are configured only rewrite push is supported, rewrite translate and pop are not supported.

`(config)#service-template template4`	Template configuration
`(config-svc)# match outer-vlan 700`	Allow VLAN 700 traffic on this VC
`(config-svc)# match double-tag outer-vlan 1200 inner-vlan 3200`	Allow double tag match with s+c tags
`(config-svc)# match untagged`	Allow untagged traffic
`(config-svc)# rewrite ingress push 300`	Push Action performed for service template
`(config-svc)#exit`	Exit configure SVC mode

Access port Configuration

`(config)#interface eth2`	Enter the Interface mode for ethernet2.
`(config-if)#switchport`	Configure interface as L2 interface
`(config-if)#mpls-vpls v1 service-template template1`	Configure template configuration.
`(config_if_vpls)#no ac-admin-status`	Making Ac-admin-status Up
`(config_if_vpls)#exit`	Exit Interface VPLS mode and return to Interface mode.
`(config-if)#mpls-vpls v2 service-template template2`	Configure template configuration.
`(config_if_vpls)#no ac-admin-status`	Making Ac-admin-status Up
`(config_if_vpls)#exit`	Exit Interface VPLS mode and return to Interface mode.
`(config-if)#mpls-vpls v3 service-template template3`	Configure template configuration.

(config_if_vpls)#no ac-admin-status	Making Ac-admin-status Up
(config_if_vpls)#exit	Exit Interface VPLS mode and return to Interface mode.
(config-if)#mpls-vpls v4 service-template template4	Configure template configuration.
(config_if_vpls)#no ac-admin-status	Making Ac-admin-status Up
(config_if_vpls)#exit	Exit Interface VPLS mode and return to Interface mode.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#vpls fib-entry 25 peer 21.21.21.21 2001 eth1 1001	Configure access port
(config)#vpls fib-entry 26 peer 21.21.21.21 2002 eth1 1002	Configure access port
(config)#vpls fib-entry 27 peer 21.21.21.21 2003 eth1 1003	Configure access port
(config)#vpls fib-entry 28 peer 21.21.21.21 2004 eth1 1004	Configure access port

Validation

```
#show mpls vpls mesh
VPLS-ID    Peer Addr         Tunnel-Label  In-Label   Network-Intf   Out-Label
Lkps/St   PW-INDEX  SIG-Protocol  Status   Ecmp-Group
25         23.23.23.23       150           1001       eth2           2001
2/Up      1          STATIC        Active   N/A
26         23.23.23.23       150           1002       eth2           2002
2/Up      2          STATIC        Active   N/A
27         23.23.23.23       150           1003       eth2           2003
2/Up      3          STATIC        Active   N/A
28         23.23.23.23       150           1004       eth2           2004
2/Up      4          STATIC        Active   N/A


#show mpls vpls detail
Virtual Private LAN Service Instance: v1, ID: 25
 SIG-Protocol: STATIC
 Attachment-Circuit :UP
 Learning: Enabled
 Group ID: 0, Configured MTU: 1500
 Description: none
 service-tpid: dot1.q
 Operating mode: Raw
 Configured interfaces:
  Interface: eth1
 Service-template : template1
  Match criteria : 2024/2023
  Action type : Pop
  Outgoing tpid : dot1.q

 Mesh Peers:
   23.23.23.23 (Up)


Virtual Private LAN Service Instance: v2, ID: 26
 SIG-Protocol: STATIC
 Attachment-Circuit :UP
```

```
 Learning: Enabled
 Group ID: 0, Configured MTU: 1500
 Description: none
 service-tpid: dot1.q
 Operating mode: Raw
 Configured interfaces:
  Interface: eth1
 Service-template : template2
  Match criteria : 2030/2024
  Action type : Translate
  Action value : 2026
  Outgoing tpid : dot1.q

 Mesh Peers:
   23.23.23.23 (Up)


Virtual Private LAN Service Instance: v3, ID: 27
 SIG-Protocol: STATIC
 Attachment-Circuit :UP
 Learning: Enabled
 Group ID: 0, Configured MTU: 1500
 Description: none
 service-tpid: dot1.q
 Operating mode: Raw
 Configured interfaces:
  Interface: eth1
 Service-template : template3
  Match criteria : Accept all
  Action type : Push
  Action value : 300

 Mesh Peers:
   23.23.23.23 (Up)

Virtual Private LAN Service Instance: v4, ID: 28
 SIG-Protocol: STATIC
 Attachment-Circuit :UP
 Learning: Enabled
 Group ID: 0, Configured MTU: 1500
 Description: none
 service-tpid: dot1.q
 Operating mode: Raw
 Configured interfaces:
  Interface: eth1
Service-template : template4
  Match criteria : 700
 1200/3200
 Untagged
  Action type : Push
  Action value : 300

 Mesh Peers:
   23.23.23.23 (Up)
```

CHAPTER 23 LDP-VPLS Service Mapping Configuration

Overview

This chapter includes step-by-step configurations for LDP VPLS. It also contains an overview of the concepts of LDP VPLS. Virtual Private LAN Service (VPLS) is a way to provide Ethernet-based multipoint-to-multipoint communication over IP- MPLS networks. It allows geographically-dispersed sites to share an Ethernet broadcast domain by connecting sites through pseudowires.

Topology

The diagram depicts the topology for the configuration examples that follow.

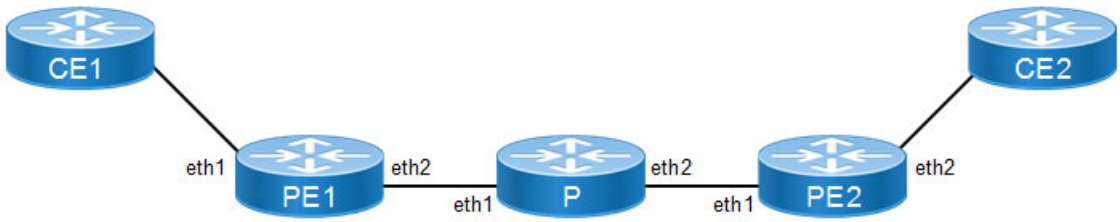


Figure 23-35: LDP-VPLS SM

Configuration

PE-1

Loopback Interface

`#configure terminal`	Enter configuration mode.
`(config)#interface lo`	Enter the Interface mode for the loopback interface.
`(config-if)#ip address 21.21.21.21/32 secondary`	Configure IP address on loopback interface.
`(config-if)#exit`	Exit interface mode

Global LDP

`(config)#router ldp`	Enter the Router LDP mode.
`(config-router)#transport-address ipv4 21.21.21.21`	Configure transport address
`(config-router)#targeted-peer ipv4 23.23.23.23`	Configure targeted peer
`(config-router-targeted-peer)#end`	Exit from router target peer and LDP mode

Interface Configuration

`(config)#interface eth2`	Enter the Interface mode for eth2.
`(config-if)# ip address 10.10.23.21/24`	Configure IP address on the interface.
`(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface
`(config-if)# label-switching`	Enable label switching on the interface.
`(config-if)#exit`	Exit interface mode

OSPF Configuration

`(config)#router ospf 100`	Enter the Router OSPF mode.
`(config-router)#ospf router-id 21.21.21.21`	Router-id configurations
`(config-router)#network 21.21.21.21/32 area 0`	Advertise loopback address in OSPF.
`(config-router)#network 10.10.23.0/24 area 0`	Advertise network address in OSPF.
`(config-router)#exit`	Exit Router OSPF mode and return to Configure mode.

LDP VPLS Configuration

`(config)#mpls vpls v1 25`	Enter VPLS config mode
`(config-vpls)#service-tpid dot1.ad`	Service tp-id configuration.
`(config-vpls)#signaling ldp`	Define Signaling as LDP
`(config-vpls-sig)#vpls-type vlan`	Type VLAN configuration for VPLS
`(config-vpls-sig)#vpls-peer 23.23.23.23`	Configure VPLS Peer
`(config-vpls-sig)#exit-signaling`	Exit Signaling LDP mode
`(config-vpls)#exit`	Exit VPLS mode
`(config)#mpls vpls v2 26`	Enter VPLS config mode
`(config-vpls)#service-tpid dot1.ad`	Service tp-id configuration.
`(config-vpls)#signaling ldp`	Define Signaling as LDP
`(config-vpls-sig)#vpls-type vlan`	Type VLAN configuration for VPLS
`(config-vpls-sig)#vpls-peer 23.23.23.23`	Configure VPLS Peer
`(config-vpls-sig)#exit-signaling`	Exit Signaling LDP mode
`(config-vpls)#exit`	Exit VPLS mode
`(config)#mpls vpls v3 27`	Enter VPLS config mode
`(config-vpls)#signaling ldp`	Define Signaling as LDP
`(config-vpls-sig)#vpls-type vlan`	Type VLAN configuration for VPLS
`(config-vpls-sig)#vpls-peer 23.23.23.23`	Configure VPLS Peer
`(config-vpls-sig)# exit-signaling`	Exit Signaling LDP mode
`(config-vpls)#exit`	Exit VPLS mode

P1

Loopback Interface

`#configure terminal`	Enter configuration mode.
`(config)#interface lo`	Enter the Interface mode for the loopback interface.
`(config-if)#ip address 22.22.22.22/32 secondary`	Configure IP address on loopback interface.
`(config-if)#exit`	Exit interface mode

Global LDP

`(config)#router ldp`	Enter the Router LDP mode.
`(config-router)#transport-address ipv4 22.22.22.22`	Configure transport address
`(config-router-targeted-peer)#end`	Exit from router target peer and LDP mode

Interface Configuration

`(config)#interface eth1`	Enter the Interface mode for eth1.
`(config-if)# ip address 10.10.23.22/24`	Configure IP address on the interface.
`(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface
`(config-if)# label-switching`	Enable label switching on the interface.
`(config-if)#exit`	Exit interface mode
`(config)#interface eth2`	Enter the Interface mode for eth2.
`(config-if)# ip address 10.10.21.22/24`	Configure IP address on the interface.
`(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface
`(config-if)# label-switching`	Enable label switching on the interface.
`(config-if)#exit`	Exit interface mode

OSPF Configuration

`(config)#router ospf 100`	Enter the Router OSPF mode.
`(config-router)#network 22.22.22.22/32 area 0`	Advertise loopback address in OSPF.
`(config-router)#network 10.10.23.0/24 area 0`	Advertise network address in OSPF.
`(config-router)#network 10.10.21.0/24 area 0`	Advertise network address in OSPF.
`(config-router)#exit`	Exit Router OSPF mode and return to Configure mode.

PE-2

Loopback Interface

`#configure terminal`	Enter configuration mode.
`(config)#interface lo`	Enter the Interface mode for the loopback interface.
`(config-if)#ip address 23.23.23.23/32 secondary`	Configure IP address on loopback interface.
`(config-if)#exit`	Exit interface mode

Global LDP

`(config)#router ldp`	Enter the Router LDP mode.
`(config-router)#transport-address ipv4 23.23.23.23`	Configure transport address
`(config-router)#targeted-peer ipv4 21.21.21.21`	Configure targeted peer
`(config-router-targeted-peer)#end`	Exit from router target peer and LDP mode

Interface Configuration

`(config)#interface eth1`	Enter the Interface mode for eth1.
`(config-if)# ip address 10.10.21.23/24`	Configure IP address on the interface.
`(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface
`(config-if)# label-switching`	Enable label switching on the interface.
`(config-if)#exit`	Exit interface mode

OSPF Configuration

`(config)#router ospf 100`	Enter the Router OSPF mode.
`(config-router)#network 23.23.23.23/32 area 0`	Advertise loopback address in OSPF.
`(config-router)#network 10.10.21.0/24 area 0`	Advertise network address in OSPF.
`(config-router)#exit`	Exit Router OSPF mode and return to Configure mode.

LDP VPLS Configuration

`(config)#mpls vpls v1 25`	Enter VPLS config mode
`(config-vpls)#service-tpid dot1.ad`	Service tp-id configuration.
`(config-vpls)#signaling ldp`	Define Signaling as LDP
`(config-vpls-sig)#vpls-type vlan`	Type VLAN configuration for VPLS
`(config-vpls-sig)#vpls-peer 21.21.21.21`	Configure VPLS Peer
`(config-vpls-sig)# exit-signaling`	Exit Signaling LDP mode
`(config-vpls)#exit`	Exit VPLS mode
`(config)#mpls vpls v2 26`	Enter VPLS config mode

(config-vpls)#service-tpid dot1.ad	Service tp-id configuration.
(config-vpls)#signaling ldp	Define Signaling as LDP
(config-vpls-sig)#vpls-type vlan	Type VLAN configuration for VPLS
(config-vpls-sig)#vpls-peer 21.21.21.21	Configure VPLS Peer
(config-vpls-sig)# exit-signaling	Exit Signaling LDP mode
(config-vpls)#exit	Exit VPLS mode
(config)#mpls vpls v3 27	Enter VPLS config mode
(config-vpls)#signaling ldp	Define Signaling as LDP
(config-vpls-sig)#vpls-type vlan	Type VLAN configuration for VPLS
(config-vpls-sig)#vpls-peer 21.21.21.21	Configure VPLS Peer
(config-vpls-sig)# exit-signaling	Exit Signaling LDP mode
(config-vpls)#exit	Exit VPLS mode

LDP VPLS Service Mapping Configuration

PE1

POP

#configure terminal	Configure mode
(config)#service-template template1	Template configuration
(config-svc)# match double-tag outer-vlan 2024 inner-vlan 2023	Match criteria under template configuration
(config-svc)# rewrite ingress pop outgoing-tpid dot1.q	Action to be performed for the match.
(config-svc)#exit	Exit template configuration mode

XLATE

(config)#service-template template2	Template configuration
(config-svc)# match double-tag outer-vlan 2030 inner-vlan 2024	Match criteria under template configuration
(config-svc)# rewrite ingress translate 2026 outgoing-tpid dot1.q	Action to be performed for the match
(config-svc)#exit	Exit template configuration mode

PUSH

(config)#service-template template3	Template configuration
(config-svc)# rewrite ingress push 300	Action to be performed for the default match .
(config-svc)#exit	Exit template configuration mode

Access port Configuration

`(config)#interface eth1`	Enter the Interface mode for ethernet1.
`(config-if)#switchport`	Configure interface as a layer 2 port.
`(config-if)#mpls-vpls v1 service-template template1`	Bind the VPLS to the Access Interface.
`(config-if-vpls)#exit`	Exit VPLS attachment-circuit mode
`(config-if)#mpls-vpls v2 service-template template2`	Bind the VPLS to the Access Interface.
`(config-if-vpls)#exit`	Exit VPLS attachment-circuit mode
`(config-if)#mpls-vpls v3 service-template template3`	Bind the VPLS to the Access Interface.
`(config-if-vpls)#exit`	Exit VPLS attachment-circuit mode
`(config-if)#exit`	Exit Interface mode and return to Configure mode.

PE2

POP

`#configure terminal`	Configure mode
`(config)#service-template template1`	Template configuration
`(config-svc)# match double-tag outer-vlan 2024 inner-vlan 2023`	Match criteria under template configuration
`(config-svc)# rewrite ingress pop outgoing-tpid dot1.q`	Action to be performed for the match.
`(config-svc)#exit`	Exit template configuration mode

XLATE

`(config)#service-template template2`	Template configuration
`(config-svc)# match double-tag outer-vlan 2030 inner-vlan 2024`	Match criteria under template configuration
`(config-svc)# rewrite ingress translate 2026 outgoing-tpid dot1.q`	Action to be performed for the match
`(config-svc)#exit`	Exit template configuration mode

PUSH

`(config)#service-template template3`	Template configuration
`(config-svc)# rewrite ingress push 300`	Action to be performed for the default match .
`(config-svc)#exit`	Exit template configuration mode

Access port Configuration

`(config)#interface eth2`	Enter the Interface mode for ethernet1.
`(config-if)#switchport`	Configure interface as a layer 2 port.
`(config-if)#mpls-vpls v1 service-template template1`	Bind the VPLS to the Access Interface.
`(config-if-vpls)#exit`	Exit VPLS attachment-circuit mode
`(config-if)#mpls-vpls v2 service-template template2`	Bind the VPLS to the Access Interface.
`(config-if-vpls)#exit`	Exit VPLS attachment-circuit mode
`(config-if)#mpls-vpls v3 service-template template3`	Bind the VPLS to the Access Interface.
`(config-if-vpls)#exit`	Exit VPLS attachment-circuit mode
`(config-if)#exit`	Exit Interface mode and return to Configure mode.

Validation

```
show mpls vpls mesh
VPLS-ID    Peer Addr         Tunnel-Label  In-Label   Network-Intf   Out-Label
Lkps/St   PW-INDEX SIG-Protocol  Status   Ecmp-Group
25         23.23.23.23       24320         24322      eth2           24320
2/Up      1          LDP           Active      N/A
26         23.23.23.23       24320         24320      eth2           24321
2/Up      2          LDP           Active      N/A
27         23.23.23.23       24320         24321      eth2           24322
2/Up      3          LDP           Active      N/A

#show ldp vpls
VPLS-ID     Peer Address      State  Type       Label-Sent   Label-Rcvd
25          23.23.23.23       Up     vlan       24322        24320
26          23.23.23.23       Up     vlan       24320        24321
27          23.23.23.23       Up     vlan       24321        24322

#show ldp vpls detail
 VPLS Identifier    : 25
 Peer IP            : 23.23.23.23
 VC State           : UP
 VC Type            : vlan
 VC Label Sent      : 24322
 VC Label Received  : 24320

 VPLS Identifier    : 26
 Peer IP            : 23.23.23.23
 VC State           : UP
 VC Type            : vlan
 VC Label Sent      : 24320
 VC Label Received  : 24321

 VPLS Identifier    : 27
 Peer IP            : 23.23.23.23
 VC State           : UP
 VC Type            : vlan
 VC Label Sent      : 24321
```

```
 VC Label Received  : 24322

#show mpls vpls detail
Virtual Private LAN Service Instance: v1, ID: 25
 SIG-Protocol: LDP
 Attachment-Circuit :UP
 Learning: Enabled
 Group ID: 0, VPLS Type: Ethernet VLAN, Configured MTU: 1500
 Description: none
 service-tpid: dot1.ad
 Operating mode: Tagged
 Svlan Id: 0
 Svlan Tpid: 88a8
 Configured interfaces:
  Interface: eth1
 Service-template : template1
  Match criteria : 2024/2023

 Mesh Peers:
   23.23.23.23 (Up)


Virtual Private LAN Service Instance: v2, ID: 26
 SIG-Protocol: LDP
 Attachment-Circuit :UP
 Learning: Enabled
 Group ID: 0, VPLS Type: Ethernet VLAN, Configured MTU: 1500
 Description: none
 service-tpid: dot1.ad
 Operating mode: Tagged
 Svlan Id: 0
 Svlan Tpid: 88a8
 Configured interfaces:
  Interface: eth1
 Service-template : template2
  Match criteria : 2030/2024
  Action type : Translate
  Action value : 2026
  Outgoing tpid : dot1.q

 Mesh Peers:
   23.23.23.23 (Up)


Virtual Private LAN Service Instance: v3, ID: 27
 SIG-Protocol: LDP
 Attachment-Circuit :UP
 Learning: Enabled
 Group ID: 0, VPLS Type: Ethernet VLAN, Configured MTU: 1500
 Description: none
 service-tpid: dot1.q
 Operating mode: Tagged
 Svlan Id: 0
 Svlan Tpid: 8100
 Configured interfaces:
  Interface: eth1
 Service-template : template3
```

```
 Match criteria : Accept all
 Action type : Push
 Action value : 300

Mesh Peers:
  23.23.23.23 (Up)
```

CHAPTER 24 BGP-VPLS Service Mapping Configuration

Overview

This chapter includes step-by-step configurations for BGP VPLS. It also contains an overview of the concepts of BGP VPLS. Virtual Private LAN Service (VPLS) is a way to provide Ethernet-based multipoint-to-multipoint communication over IP- MPLS networks. It allows geographically-dispersed sites to share an Ethernet broadcast domain by connecting sites through pseudowires

Topology

The diagram depicts the topology for the configuration examples that follow.

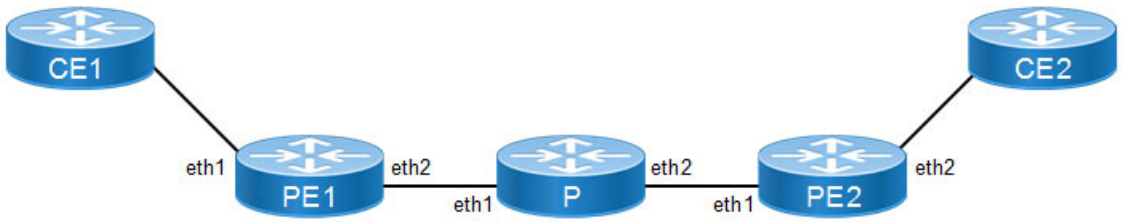


Figure 24-36: BGP-VPLS SM

Configuration

PE-1

Loopback Interface

`#configure terminal`	Enter configuration mode.
`(config)#interface lo`	Enter the Interface mode for the loopback interface.
`(config-if)#ip address 21.21.21.21/32`	Configure IP address on loopback interface.
`(config-if)#exit`	Exit interface mode

Interface Configuration

`(config)#interface eth2`	Enter the Interface mode for eth2.
`(config-if)# ip address 10.10.23.21/24`	Configure IP address on the interface.
`(config-if)#enable-rsvp`	Enable RSVP on the physical interface
`(config-if)# label-switching`	Enable label switching on the interface.
`(config-if)#exit`	Exit interface mode

OSPF Configuration

(config)#router ospf 100	Enter the Router OSPF mode.
(config-router)#ospf router-id 21.21.21.21	Router-id configurations
(config-router)#network 21.21.21.21/32 area 0	Advertise loopback address in OSPF.
(config-router)#network 10.10.23.0/24 area 0	Advertise network address in OSPF.
(config-router)#exit	Exit Router OSPF mode and return to Configure mode.

Global RSVP

(config)#router rsvp	Enter the Router OSPF mode.
(config-router)#exit	Exit Router RSVP mode and return to Configure mode.

RSVP-Trunk Configuration

(config)#rsvp-trunk 1	Enter the Trunk configuration mode
(config-trunk)#to 23.23.23.23	Configure the destination of the Trunk
(config-trunk)#exit	Exit.Trunk configuration mode

BGP Configuration

(config)# router bgp 100	Enter the BGP configuration mode.
(config-router)#neighbor 23.23.23.23 remote-as 100	Configure neighbor
(config-router)#neighbor 23.23.23.23 update-source 21.21.21.21	Update loopback address as source
(config-router)#address-family l2vpn vpls	Enter address family mode.
(config-router-af)#neighbor 23.23.23.23 activate	Activate the neighbor.
(config-router-af)#exit	Exit address family mode.
(config-router)#exit	Exit Router BGP mode

BGP VPLS Configuration

(config)#mpls vpls v1 25	Enter VPLS config mode
(config)#service-tpid dot1.ad	Service tp-id configuration.
(config-vpls)#signaling bgp	Define Signaling as BGP
(config-vpls-sig)#ve-id 1	Configure VE-ID
(config-vpls-sig)#exit	Exit Signaling BGP mode
(config-vpls)#exit	Exit VPLS mode
(config)#mpls vpls v2 26	Enter VPLS config mode
(config)#service-tpid dot1.ad	Service tp-id configuration.
(config-vpls)#signaling bgp	Define Signaling as BGP
(config-vpls-sig)#ve-id 1	Configure VE-ID

(config-vpls-sig)#exit	Exit Signaling BGP mode
(config-vpls)#exit	Exit VPLS mode
(config)#mpls vpls v3 27	Enter VPLS config mode
(config-vpls)#signaling bgp	Define Signaling as BGP
(config-vpls-sig)#ve-id 1	Configure VE-ID
(config-vpls-sig)#exit	Exit Signaling BGP mode
(config-vpls)#exit	Exit VPLS mode
(config)#mpls vpls v4 28	Enter VPLS config mode
(config-vpls)#signaling bgp	Define Signaling as BGP
(config-vpls-sig)#ve-id 1	Configure VE-ID
(config-vpls-sig)#exit	Exit Signaling BGP mode
(config-vpls)#exit	Exit VPLS mode

P1

Loopback Interface

#configure terminal	Enter configuration mode.
(config)#interface lo	Enter the Interface mode for the loopback interface.
(config-if)#ip address 22.22.22.22/32	Configure IP address on loopback interface.
(config-if)#exit	Exit interface mode

Interface Configuration

(config)#interface eth1	Enter the Interface mode for eth1
(config-if)#ip address 10.10.23.22/24	Configure IP address on the interface.
(config-if)#enable-rsvp	Enable RSVP on the physical interface
(config-if)#label-switching	Enable label switching on the interface.
(config-if)#exit	Exit interface mode
(config)#interface eth2	Enter the Interface mode for eth2
(config-if)#ip address 10.10.21.22/24	Configure IP address on the interface.
(config-if)#enable-rsvp	Enable RSVP on the physical interface
(config-if)#label-switching	Enable label switching on the interface.
(config-if)#exit	Exit interface mode

OSPF Configuration

(config)#router ospf 100	Enter the Router OSPF mode.
(config-router)#network 22.22.22.22/32 area 0	Advertise loopback address in OSPF.
(config-router)#network 10.10.23.0/24 area 0	Advertise network address in OSPF.
(config-router)#network 10.10.21.0/24 area 0	Advertise network address in OSPF.
(config-router)#exit	Exit Router OSPF mode and return to Configure mode.

Global RSVP

`(config)#router rsvp`	Enter the Router OSPF mode.
`(config-router)#exit`	Exit Router RSVP mode and return to Configure mode.

RSVP-Trunk Configuration

`(config)#rsvp-trunk 1`	Enter the Trunk configuration mode
`(config-trunk)#to 21.21.21.21`	Configure the destination of the Trunk
`(config-trunk)#exit`	Exit.Trunk configuration mode

PE-2

Loopback Interface

`#configure terminal`	Enter configuration mode.
`(config)#interface lo`	Enter the Interface mode for the loopback interface.
`(config-if)#ip address 23.23.23.23/32`	Configure IP address on loopback interface.
`(config-if)#exit`	Exit interface mode

Interface Configuration

`(config)#interface eth1`	Enter the Interface mode for eth1
`(config-if)#ip address 10.10.21.23/24`	Configure IP address on the interface.
`(config-if)#enable-rsvp`	Enable RSVP on the physical interface
`(config-if)#label-switching`	Enable label switching on the interface.
`(config-if)#exit`	Exit interface mode

OSPF Configuration

`(config)#router ospf 100`	Enter the Router OSPF mode.
`(config-router)#network 23.23.23.23/32 area 0`	Advertise loopback address in OSPF.
`(config-router)#network 10.10.23.0/24 area 0`	Advertise network address in OSPF.
`(config-router)#exit`	Exit Router OSPF mode and return to Configure mode.

Global RSVP

`(config)#router rsvp`	Enter the Router OSPF mode.
`(config-router)#exit`	Exit Router RSVP mode and return to Configure mode.

BGP Configuration

`(config)# router bgp 100`	Enter the BGP configuration mode.
`(config-router)#neighbor 21.21.21.21 remote-as 100`	Configure neighbor
`(config-router)#neighbor 21.21.21.21 update-source 21.21.21.21`	Update loopback address as source
`(config-router)#address-family l2vpn vpls`	Enter address family mode.
`(config-router-af)#neighbor 21.21.21.21 activate`	Activate the neighbor.
`(config-router-af)#exit`	Exit address family mode.
`(config-router)#exit`	Exit Router BGP mode

BGP VPLS Configuration

`(config)#mpls vpls v1 25`	Enter VPLS config mode
`(config)#service-tpid dot1.ad`	Service tp-id configuration.
`(config-vpls)#signaling bgp`	Define Signaling as BGP
`(config-vpls-sig)#ve-id 2`	Configure VE-ID
`(config-vpls-sig)#exit`	Exit Signaling BGP mode
`(config-vpls)#exit`	Exit VPLS mode
`(config)#mpls vpls v2 26`	Enter VPLS config mode
`(config)#service-tpid dot1.ad`	Service tp-id configuration.
`(config-vpls)#signaling bgp`	Define Signaling as BGP
`(config-vpls-sig)#ve-id 2`	Configure VE-ID
`(config-vpls-sig)#exit`	Exit Signaling BGP mode
`(config-vpls)#exit`	Exit VPLS mode
`(config)#mpls vpls v3 27`	Enter VPLS config mode
`(config-vpls)#signaling bgp`	Define Signaling as BGP
`(config-vpls-sig)#ve-id 2`	Configure VE-ID
`(config-vpls-sig)#exit`	Exit Signaling BGP mode
`(config-vpls)#exit`	Exit VPLS mode
`(config)#mpls vpls v4 28`	Enter VPLS config mode
`(config-vpls)#signaling bgp`	Define Signaling as BGP
`(config-vpls-sig)#ve-id 2`	Configure VE-ID
`(config-vpls-sig)#exit`	Exit Signaling BGP mode
`(config-vpls)#exit`	Exit VPLS mode

BGP VPLS Service Mapping Configuration

PE-1

POP

`(config)#configure terminal`	Configure mode
`(config)#service-template template1`	Template configuration
`(config-svc)# match double-tag outer-vlan 2024 inner-vlan 2023`	Match criteria under template configuration
`(config-svc)# rewrite ingress pop outgoing-tpid dot1.ad`	Action to be performed for the match.
`(config-svc)#exit`	Exit template configuration mode

XLATE

`(config)#service-template template2`	Template configuration
`(config-svc)# match double-tag outer-vlan 2030 inner-vlan 2024`	Match criteria under template configuration
`(config-svc)# rewrite ingress translate 2026 outgoing-tpid dot1.q`	Action to be performed for the match
`(config-svc)#exit`	Exit template configuration mode

PUSH

`(config)#service-template template3`	Template configuration
`(config-svc)# rewrite ingress push 300`	Action to be performed for the default match .
`(config-svc)#exit`	Exit template configuration mode

PUSH-service-template with multiple match

This is to validate the multiple match criteria support in a service template. When multiple match statements are configured only rewrite push is supported, rewrite translate and pop are not supported.

`(config)#service-template template4`	Template configuration
`(config-svc)# match outer-vlan 700`	Allow VLAN 700 traffic on this VC
`(config-svc)# match double-tag outer-vlan 1200 inner-vlan 3200`	Allow double tag match with s+c tags
`(config-svc)# match untagged`	Allow untagged traffic
`(config-svc)# rewrite ingress push 300`	Push Action performed for service template
`(config-svc)#exit`	Exit configure SVC mode

Access port Configuration

`(config)#interface eth1`	Enter the Interface mode for ethernet1.
`(config-if)#mpls-vpls v1 service-template template1`	Bind the VPLS to the Access Interface.
`(config-if-vpls)#exit`	Exit VPLS attachment-circuit mode
`(config-if)#mpls-vpls v2 service-template template2`	Bind the VPLS to the Access Interface.
`(config-if-vpls)#exit`	Exit VPLS attachment-circuit mode
`(config-if)#mpls-vpls v3 service-template template3`	Bind the VPLS to the Access Interface.
`(config-if-vpls)#exit`	Exit VPLS attachment-circuit mode
`(config-if)#mpls-vpls v4 service-template template4`	Bind the VPLS to the Access Interface.
`(config-if-vpls)#exit`	Exit VPLS attachment-circuit mode
`(config-if)#no ac-admin-status`	Making Ac-admin-status Up
`(config-if)#exit`	Exit Interface mode and return to Configure mode.

PE-2

POP

`(config)#configure terminal`	Configure mode
`(config)#service-template template1`	Template configuration
`(config-svc)# match double-tag outer-vlan 2024 inner-vlan 2023`	Match criteria under template configuration
`(config-svc)# rewrite ingress pop outgoing-tpid dot1.ad`	Action to be performed for the match.
`(config-svc)#exit`	Exit template configuration mode

XLATE

`(config)#service-template template2`	Template configuration
`(config-svc)# match double-tag outer-vlan 2030 inner-vlan 2024`	Match criteria under template configuration
`(config-svc)# rewrite ingress translate 2026 outgoing-tpid dot1.q`	Action to be performed for the match
`(config-svc)#exit`	Exit template configuration mode

PUSH

`(config)#service-template template3`	Template configuration
`(config-svc)# rewrite ingress push 300`	Action to be performed for the default match .
`(config-svc)#exit`	Exit template configuration mode

PUSH-service-template with multiple match

This is to validate the multiple match criteria support in a service template. When multiple match statements are configured only rewrite push is supported, rewrite translate and pop are not supported.

`(config)#service-template template4`	Template configuration
`(config-svc)# match outer-vlan 700`	Allow VLAN 700 traffic on this VC
`(config-svc)# match double-tag outer-vlan 1200 inner-vlan 3200`	Allow double tag match with s+c tags
`(config-svc)# match untagged`	Allow untagged traffic
`(config-svc)# rewrite ingress push 300`	Push Action performed for service template
`(config-svc)#exit`	Exit configure SVC mode

Access port Configuration

`(config)#interface eth2`	Enter the Interface mode for ethernet1.
`(config-if)#mpls-vpls v1 service-template template1`	Bind the VPLS to the Access Interface.
`(config-if-vpls)#exit`	Exit VPLS attachment-circuit mode
`(config-if)#mpls-vpls v2 service-template template2`	Bind the VPLS to the Access Interface.
`(config-if-vpls)#exit`	Exit VPLS attachment-circuit mode
`(config-if)#mpls-vpls v3 service-template template3`	Bind the VPLS to the Access Interface.
`(config-if-vpls)#exit`	Exit VPLS attachment-circuit mode
`(config-if)#mpls-vpls v4 service-template template4`	Bind the VPLS to the Access Interface.
`(config-if-vpls)#exit`	Exit VPLS attachment-circuit mode
`(config-if)#no ac-admin-status`	Making Ac-admin-status Up
`(config-if)#exit`	Exit Interface mode and return to Configure mode.

Validation

Router1

```
#show bgp l2vpn vpls
VPLS-ID     VE-ID    Discovered-Peers   Route-Target
25          1        1                   100:25
26          1        1                   100:26
27          1        1                   100:27
28     1        1                  100:28
#show bgp l2vpn vp
vpls  vpws

#show bgp l2vpn vpls detail

VPLS ID: 25
VE-ID: 1
Discovered Peers: 1
```

```
Route-Target: 100:25
Local RD: 100:25
 Mesh Peers:
  Address:23.23.23.23, RD:100:25, VE-ID:2
  VC Details: VC-ID:12
  Remote (LB:53120,VBO:1,VBS:64)  Local (LB:53120,VBO:1,VBS:64)
  LB sent on known VEID:Yes
  In Label:53121, Out Label:53120
  PW Status:Established


VPLS ID: 26
VE-ID: 1
Discovered Peers: 1
Route-Target: 100:26
Local RD: 100:26
 Mesh Peers:
  Address:23.23.23.23, RD:100:26, VE-ID:2
  VC Details: VC-ID:12
  Remote (LB:53120,VBO:1,VBS:64)  Local (LB:53184,VBO:1,VBS:64)
  LB sent on known VEID:Yes
  In Label:53185, Out Label:53120
  PW Status:Established


VPLS ID: 27
VE-ID: 1
Discovered Peers: 1
Route-Target: 100:27
Local RD: 100:27
 Mesh Peers:
  Address:23.23.23.23, RD:100:27, VE-ID:2
  VC Details: VC-ID:12
  Remote (LB:53184,VBO:1,VBS:64)  Local (LB:53120,VBO:1,VBS:64)
  LB sent on known VEID:Yes
  In Label:53121, Out Label:53184
  PW Status:Established

VPLS ID: 28
VE-ID: 1
Discovered Peers: 1
Route-Target: 100:28
Local RD: 100:28
 Mesh Peers:
  Address:23.23.23.23, RD:100:28, VE-ID:2
  VC Details: VC-ID:12
  Remote (LB:53184,VBO:1,VBS:64)  Local (LB:53120,VBO:1,VBS:64)
  LB sent on known VEID:Yes
  In Label:53122, Out Label:53186
  PW Status:Established

#show mpls vpls mesh
VPLS-ID    Peer Addr         Tunnel-Label  In-Label   Network-Intf   Out-Label
Lkps/St   PW-INDEX  SIG-Protocol  Status
    Ecmp-Group
25         23.23.23.23       52480         53121      eth2           53120
2/Up      1         BGP           Active
```

```
    N/A
26          23.23.23.23       52480          53185       eth2           53120
2/Up       2          BGP            Active     N/A
27          23.23.23.23       52480          53121       eth2           53184
2/Up       3          BGP            Active     N/A
28          23.23.23.23       52480          53122       eth2           53186
2/Up       3          BGP            Active     N/A

#show mpls vpls detail
Virtual Private LAN Service Instance: v1, ID: 25
 SIG-Protocol: BGP
  Route-Distinguisher :100:25
  Route-Target :100:25
  VE-ID :1
 Attachment-Circuit :UP
 Learning: Enabled
 Group ID: 0, Configured MTU: 1500
 Description: none
 service-tpid: dot1.ad
 Configured interfaces:
  Interface: eth1

 Service-template : template1
  Match criteria : 2024/2023
  Action type : Pop
  Outgoing tpid : dot1.ad

 Mesh Peers:
   23.23.23.23 (Up)

Virtual Private LAN Service Instance: v2, ID: 26
 SIG-Protocol: BGP
  Route-Distinguisher :100:26
  Route-Target :100:26
  VE-ID :1
 Attachment-Circuit :UP
 Learning: Enabled
 Group ID: 0, Configured MTU: 1500
 Description: none
 service-tpid: dot1.ad
 Configured interfaces:
  Interface: eth1

 Service-template : template2
  Match criteria : 2030/2024
  Action type : Translate
  Action value : 2026
  Outgoing tpid : dot1.q

 Mesh Peers:
   23.23.23.23 (Up)

Virtual Private LAN Service Instance: v3, ID: 27
 SIG-Protocol: BGP
  Route-Distinguisher :100:27
  Route-Target :100:27
  VE-ID :1
```

```
 Attachment-Circuit :UP
 Learning: Enabled
 Group ID: 0, Configured MTU: 1500
 Description: none
 service-tpid: dot1.q
 Configured interfaces:
  Interface: eth1

 Service-template : template3
  Match criteria : Accept all
  Action type : Push
  Action value : 300

 Mesh Peers:
   23.23.23.23 (Up)

Virtual Private LAN Service Instance: v4, ID: 28
 SIG-Protocol: BGP
  Route-Distinguisher :100:28
  Route-Target :100:28
  VE-ID :1
 Attachment-Circuit :UP
 Learning: Enabled
 Group ID: 0, Configured MTU: 1500
 Description: none
 service-tpid: dot1.q
 Configured interfaces:
  Interface: eth1

 Service-template : template4
  Match criteria : 700
 1200/3200
untagged
  Action type : Push
  Action value : 300

 Mesh Peers:
   23.23.23.23 (Up)
```

CHAPTER 25 BGP Peer Groups for Address-Family L2VPN EVPN

BGP peer groups are used to simplify configuration and to improve performance. This is achieved by assigning the same outbound policy to each of the neighbors. Because UPDATEs are generated only once per peer group rather than multiple times for each neighboring router, peer groups save processing time when building neighbor updates. It reduces the amount of system resources (CPU and memory) necessary in an update generation.

A BGP peer group reduces the load on system resources by allowing the routing table to be checked only once, and updates to be replicated to all peer group members instead of being done individually for each peer in the peer group.

Topology

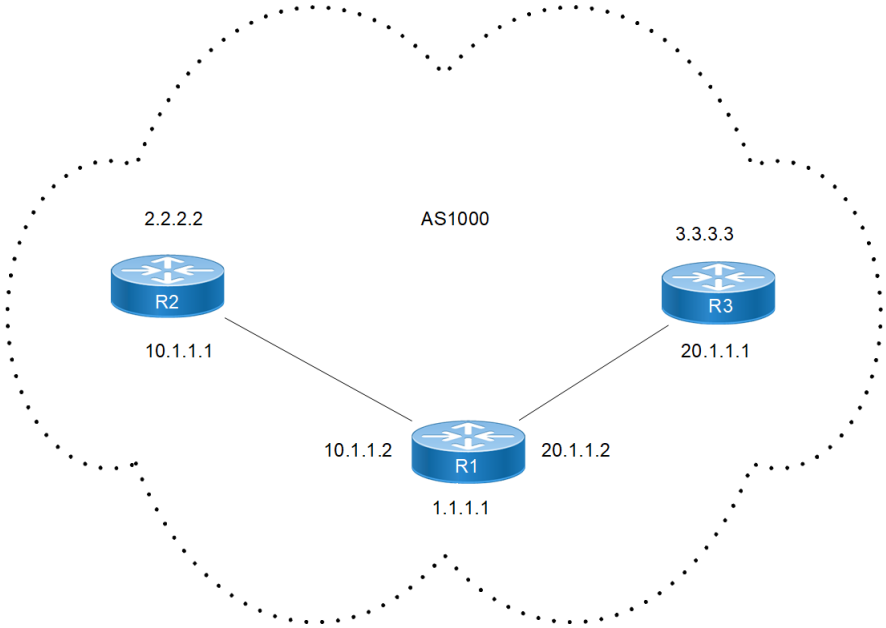


Figure 25-37: BGP Peer-Groups with L2VPN EVPN address-family

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)# interface lo`	Enter interface mode for Loopback
`(config-if)#ip address 1.1.1.1/32 secondary`	Configure ip address for Loopback interface
`(config-if)#exit`	Exit interface mode
`(config)# interface xe15`	Enter interface mode for xe15
`(config-if)#ip address 10.1.1.2/24`	Configure ip address

(config-if)#exit	Exit interface mode
(config)# interface ce0	Enter interface mode for ce0
(config-if)#ip address 20.1.1.2	Configure ip address
(config-if)#exit	Exit interface mode
(config)#router ospf 100	Configure the OSPF process (100)
(config-router)# ospf router-id 1.1.1.1	Configure OSPF router-id
(config-router)#network 1.1.1.1/32 area 0	Advertise the network in Area 0
(config-router)#network 10.1.1.0/24 area 0	Advertise the network in Area 0
(config-router)#network 20.1.1.0/24 area 0	Advertise the network in Area 0
(config-router)#exit	Exit Router mode and return to Configure mode
(config)#router bgp 100	Define the routing process. The number 100 specifies the AS number of R1.
(config-router)# bgp router-id 1.1.1.1	Configure BGP router-id
(config-router)#neighbor PG peer-group	Create a peer group named PG
(config-router)#neighbor PG remote-as 100	Assign options to the peer group named PG
(config-router)#neighbor PG update-source lo	Assign options to the peer group named PG
(config-router)#neighbor 2.2.2.2 peer-group PG	Define neighbor 2.2.2.2 (R2) as a peer group
(config-router)#neighbor 3.3.3.3 peer-group PG	Define neighbor 3.3.3.3 (R3) as a peer group member.
(config-router)#address-family l2vpn evpn	Enter address-family l2vpn evpn mode
(config-router-af)#neighbor PG activate	Activate the peer-group ABC for address-family l2vpn evpn
(config-router-af)# exit-address-family	Exit address-family ipv4 unicast mode
(config-router)#exit	Exit router bgp mode
(config)#commit	Commit the candidate configuration to the running configuration.

R2

#configure terminal	Enter configure mode.
(config)# interface lo	Enter interface mode for Loopback
(config-if)#ip address 2.2.2.2/32 secondary	Configure ip address for Loopback interface
(config-if)#exit	Exit interface mode
(config)# interface xe15	Enter interface mode for xe15
(config-if)#ip address 10.1.1.2/24	Configure ip address
(config-if)#exit	Exit interface mode
(config)# interface xe10	Enter interface mode for xe10
(config-if)#ip address 10.1.1.1/24	Configure ip address
(config-if)#exit	Exit interface mode
(config)#router ospf 100	Configure the OSPF process (100)
(config-router)# ospf router-id 2.2.2.2	Configure OSPF router-id
(config-router)#network 2.2.2.2/32 area 0	Advertise the network in Area 0
(config-router)#network 10.1.1.0/24 area 0	Advertise the network in Area 0

(config-router)#exit	Exit Router mode and return to Configure mode
(config)#router bgp 100	Define the routing process. The number 100 specifies the AS number of R1.
(config-router)# bgp router-id 2.2.2.2	Configure BGP router-id
(config-router)#neighbor PG peer-group	Create a peer group named PG
(config-router)#neighbor PG remote-as 100	Assign options to the peer group named PG
(config-router)#neighbor PG update-source lo	Assign options to the peer group named PG
(config-router)#neighbor 1.1.1.1 peer-group PG	Define neighbor 1.1.1.1 (R1) as a peer group member.
(config-router)#address-family l2vpn evpn	Enter address-family l2vpn evpn mode
(config-router-af)#neighbor PG activate	Activate the peer-group ABC for address-family l2vpn evpn
(config-router-af)# exit-address-family	Exit address-family ipv4 unicast mode
(config-router)#exit	Exit router bgp mode
(config)#commit	Commit the candidate configuration to the running configuration.

R3

#configure terminal	Enter configure mode.
(config)# interface lo	Enter interface mode for Loopback
(config-if)#ip address 3.3.3.3/32 secondary	Configure ip address for Loopback interface
(config-if)#exit	Exit interface mode
(config)# interface ce15	Enter interface mode for ce15
(config-if)#ip address 20.1.1.1/24	Configure ip address
(config-if)#exit	Exit interface mode
(config)# interface xe10	Enter interface mode for xe10
(config-if)#ip address 10.1.1.1/24	Configure ip address
(config-if)#exit	Exit interface mode
(config)#router ospf 100	Configure the OSPF process (100)
(config-router)# ospf router-id 3.3.3.3	Configure OSPF router-id
(config-router)#network 20.1.1.0/24 area 0	Advertise the network in Area 0
(config-router)#exit	Exit Router mode and return to Configure mode
(config)#router bgp 100	Define the routing process. The number 100 specifies the AS number of R1.
(config-router)# bgp router-id 3.3.3.3	Configure BGP router-id
(config-router)#neighbor PG peer-group	Create a peer group named PG
(config-router)#neighbor PG remote-as 100	Assign options to the peer group named PG
(config-router)#neighbor PG update-source lo	Assign options to the peer group named PG
(config-router)#neighbor 1.1.1.1 peer-group PG	Define neighbor 1.1.1.1 (R1) as a peer group member.
(config-router)#address-family l2vpn evpn	Enter address-family l2vpn evpn mode
(config-router-af)#neighbor PG activate	Activate the peer-group ABC for address-family l2vpn evpn
(config-router-af)# exit-address-family	Exit address-family ipv4 unicast mode

(config-router)#exit	Exit router bgp mode
(config)#commit	Commit the candidate configuration to the running configuration.

Validation

R1

```
R1#sh run bgp
!
router bgp 100
 bgp router-id 1.1.1.1
 neighbor PG peer-group
 neighbor PG remote-as 100
 neighbor PG update-source lo
 neighbor 2.2.2.2 peer-group PG
 neighbor 3.3.3.3 peer-group PG
 !
 address-family l2vpn evpn
 neighbor PG activate
 exit-address-family
R1#sh bgp neighbors
BGP neighbor is 2.2.2.2, remote AS 100, local AS 100, internal link
 Member of peer-group PG for session parameters
  BGP version 4, local router ID 1.1.1.1, remote router ID 2.2.2.2
  BGP state = Established, up for 01:20:53
  Last read 00:00:24, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family L2VPN EVPN: advertised and received
  Received 192 messages, 0 notifications, 0 in queue
  Sent 191 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
  Update source is lo
 For address family: L2VPN EVPN
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  PG peer-group member
  Community attribute sent to this neighbor (both)
  Large Community attribute sent to this neighbor
  0 accepted prefixes
  Accepted AD:0 MACIP:0 MCAST:0 ESI:0 PREFIX:0
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 1.1.1.1, Local port: 42981
Foreign host: 2.2.2.2, Foreign port: 179
```

```
Nexthop: 1.1.1.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 3.3.3.3, remote AS 100, local AS 100, internal link
 Member of peer-group PG for session parameters
  BGP version 4, local router ID 1.1.1.1, remote router ID 3.3.3.3
  BGP state = Established, up for 01:36:13
  Last read 00:00:08, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family L2VPN EVPN: advertised and received
  Received 227 messages, 0 notifications, 0 in queue
  Sent 229 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
  Update source is lo
 For address family: L2VPN EVPN
  BGP table version 1, neighbor version 1
  Index 3, Offset 0, Mask 0x8
  PG peer-group member
  Community attribute sent to this neighbor (both)
  Large Community attribute sent to this neighbor
  0 accepted prefixes
  Accepted AD:0 MACIP:0 MCAST:0 ESI:0 PREFIX:0
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 1.1.1.1, Local port: 179
Foreign host: 3.3.3.3, Foreign port: 32857
Nexthop: 1.1.1.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
R1#sh ip ospf neighbor

Total number of full neighbors: 2
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
2.2.2.2           1   Full/Backup     00:00:38    10.1.1.1        xe15                  0
3.3.3.3           1   Full/Backup     00:00:34    20.1.1.1        ce0                   0
R1#sh bgp l2vpn evpn summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd     AD  MACIP  MCAST    ESI  PREFIX-ROUTE
```

```
2.2.2.2                 4   100  193       191       1     0     0  01:21:07
0       0       0       0       0       0
3.3.3.3                 4   100  227       229       1     0     0  01:36:27
0       0       0       0       0       0

Total number of neighbors 2

Total number of Established sessions 2
```

R2

```
R2#sh run bgp
!
router bgp 100
 bgp router-id 2.2.2.2
 neighbor PG peer-group
 neighbor PG remote-as 100
 neighbor PG update-source lo
 neighbor 1.1.1.1 peer-group PG
 !
 address-family l2vpn evpn
 neighbor PG activate
 exit-address-family
!
R2#sh bgp neighbors
BGP neighbor is 1.1.1.1, remote AS 100, local AS 100, internal link
 Member of peer-group PG for session parameters
  BGP version 4, local router ID 2.2.2.2, remote router ID 1.1.1.1
  BGP state = Established, up for 01:20:42
  Last read 00:00:20, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family L2VPN EVPN: advertised and received
  Received 190 messages, 0 notifications, 0 in queue
  Sent 193 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
  Update source is lo
 For address family: L2VPN EVPN
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  PG peer-group member
  Community attribute sent to this neighbor (both)
  Large Community attribute sent to this neighbor
  0 accepted prefixes
  Accepted AD:0 MACIP:0 MCAST:0 ESI:0 PREFIX:0
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 2.2.2.2, Local port: 179
Foreign host: 1.1.1.1, Foreign port: 42981
```

```
Nexthop: 2.2.2.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

R2#sh ip ospf neighbor

Total number of full neighbors: 1
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
1.1.1.1           1   Full/DR         00:00:30    10.1.1.2        xe10                    0
R2#sh bgp l2vpn evpn summary
BGP router identifier 2.2.2.2, local AS number 100
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd     AD  MACIP  MCAST    ESI  PREFIX-ROUTE
1.1.1.1                 4   100  192       195       1     0     0  01:21:28
0      0      0      0      0      0

Total number of neighbors 1

Total number of Established sessions 1
```

R3

```
R3#sh run bgp
!
router bgp 100
 bgp router-id 3.3.3.3
 neighbor PG peer-group
 neighbor PG remote-as 100
 neighbor PG update-source lo
 neighbor 1.1.1.1 peer-group PG
 !
 address-family l2vpn evpn
 neighbor PG activate
 exit-address-family
!
R3#sh bgp neighbors
BGP neighbor is 1.1.1.1, remote AS 100, local AS 100, internal link
 Member of peer-group PG for session parameters
  BGP version 4, local router ID 3.3.3.3, remote router ID 1.1.1.1
  BGP state = Established, up for 01:36:07
  Last read 00:00:06, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family L2VPN EVPN: advertised and received
```

```
  Received 228 messages, 0 notifications, 0 in queue
  Sent 227 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
  Update source is lo
 For address family: L2VPN EVPN
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  PG peer-group member
  Community attribute sent to this neighbor (both)
  Large Community attribute sent to this neighbor
  0 accepted prefixes
  Accepted AD:0 MACIP:0 MCAST:0 ESI:0 PREFIX:0
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 3.3.3.3, Local port: 32857
Foreign host: 1.1.1.1, Foreign port: 179
Nexthop: 3.3.3.3
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
R3#sh ip os neighbor

Total number of full neighbors: 1
OSPF process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
1.1.1.1           1   Full/DR         00:00:37    20.1.1.2        ce15                  0
R3#sh bgp l2vpn evpn summary
BGP router identifier 3.3.3.3, local AS number 100
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd     AD  MACIP  MCAST    ESI  PREFIX-ROUTE
1.1.1.1                 4   100  232       231       1     0     0  01:37:55
0       0       0       0       0       0

Total number of neighbors 1

Total number of Established sessions 1
```

Multi-Protocol Label Switching Command Reference

CHAPTER 1 MPLS Commands

This chapter is a reference for the MPLS commands:

- service-template
- service-tpid
- show mpls
- show mpls admin-groups
- show mpls bandwidth-class
- show mpls counters ldp
- show mpls counters rsvp
- show mpls counters static
- show mpls cross-connect-table
- show mpls forwarding-table
- show mpls ftn-table
- show mpls ilm-table
- show mpls in-segment-table
- show mpls l2-circuit
- show mpls l2-circuit statistics
- show mpls mapped-routes
- show mpls out-segment-table
- show mpls qos-resource
- show mpls vc-table
- show mpls vrf
- show mpls vrf-forwarding-table vrf
- show running-config interface mpls
- show running-config mpls
- show running-config service-template
- show running-config vc
- show running-config vpls
- show service-template
- show vccv statistics
- srlg-disjoint
- trace mpls
- tunnel-id
- tunnel-name
- tunnel-select-policy
- vccv cc-type
- vccv cv-type

allow-l2protocol-peer

Use this command to peer L2CP packets.

Command Syntax

```
allow-l2protocol-peer
no allow-l2protocol-peer
```

Parameter

NA

Default

By default, L2CP packets are tunneled

Command Mode

Configure Pseudowire mode

Applicability

This command is introduced in OcNOS-SP version 5.0

Example

VPWS sub-mode

```
OcNOS(config)#mpls l2-circuit vc10 10 1.1.1.1
OcNOS(config-pseudowire)#allow-l2protocol-peer
OcNOS(config-pseudowire)#no allow-l2protocol-peer
```

bandwidth

Use this command to specify the maximum bandwidth to be used for a band-class. The bandwidth value is in bits.

Note: Run this command in the Bandwidth-class mode (refer to mpls bandwidth-class).

Command Syntax

```
bandwidth BANDWIDTH setup-priority <0-7> hold-priority <0-7>
```

Parameter

`BANDWIDTH`	<1-999>k for 1 to 999 kilo bits/s
	<1-999>m for 1 to 999 mega bits/s
	<1-100>g for 1 to 100 giga bits/s
`setup-priority`	Indicate the `setup-priority` parameter
`<0-7>`	The actual setup priority value
`hold-priority`	Indicate the `hold-priority` parameter
`<0-7>`	The actual hold priority value

Default

By default, bandwidth priority is 0

Command Mode

Bandwidth-class mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#mpls bandwidth-class new-BC
(config-mpls-bw)#bandwidth 100m setup-priority 1 hold-priority 1
```

clear mpls counters ldp

Use this command to clear traffic statistics for FTNs and ILMs configured by LDP.

Command Syntax

```
clear mpls counters ldp ((ftn (|A.B.C.D/M)) | (ilm (|A.B.C.D/M)) |)
```

Parameter

`ftn`	FEC-to-NHLFE map counters
`A.B.C.D/M`	FEC prefix
`ilm`	Incoming label map counters
`A.B.C.D/M`	FEC prefix

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear mpls counters ldp
```

clear mpls counters rsvp

Use this command to clear traffic statistics for LSPs configured by RSVP.

Command Syntax

```
clear mpls counters rsvp ((tunnel-name NAME) | (tunnel-id TUNNEL_ID) | (node-role
  (ingress | transit | egress)) |)
```

Parameter

NAME	RSVP tunnel name
TUNNEL_ID	RSVP tunnel identifier
ingress	LSP role is ingress
transit	LSP role is transit
egress	LSP role is egress

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear mpls counters rsvp
```

clear mpls counters static

Use this command to clear traffic statistics for statically configured FTNs and ILMs.

Command Syntax

```
clear mpls counters static ((ftn (|A.B.C.D/M)) | (ilm (|A.B.C.D/M)) |)
```

Parameter

`ftn`	FEC-to-NHLFE map counters
`A.B.C.D/M`	FEC prefix
`ilm`	Incoming label map counters
`A.B.C.D/M`	FEC prefix

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear mpls counters static
```

clear mpls l2-circuit statistics

Use this command to clear MPLS traffic statistics for l2 circuit.

Command Syntax

```
clear mpls l2-circuit NAME statistics(access-port|network-port|)
```

Parameters

`name`	Name of L2 circuit
`access-port`	Displays the access port statistics
`network-port`	Displays the network port statistics

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear mpls l2-circuit vcl statistics
```

group-id

Use this command to configure a specific group identifier to existing group with a group name in the MPLS layer-2 virtual circuit.

Use the no parameter with this command to remove group identifier from the MPLS layer-2 virtual circuit

Command Syntax

```
group-id <1-4294967295>
no group-id
```

Parameters

`<1-4294967295>` Value for group identifier

Default

By default, group-id is disabled. If group-name is configured, default group-id is the first available identifier.

Command Mode

Configure Pseudowire mode

Applicability

This command was introduced before OcNOS version 1.X

Example

```
#configure terminal
(config)#mpls l2-circuit mycircuit 45678 1.2.3.4
(config-pseudowire)#group-name group-1
(config-pseudowire)#group-id 11
```

group-name

Use this command to map the MPLS layer-2 virtual circuit with a specific group.

Use the no parameter with this command to remove group from the MPLS layer-2 virtual circuit

Command Syntax

```
group-name NAME
no group-name
```

Parameters

NAME	String identifying group NAME

Default

By default, group-name is disabled

Command Mode

Configure Pseudowire mode

Applicability

This command was introduced before OcNOS version 1.X

Example

```
#configure terminal
(config)#mpls l2-circuit mycircuit 45678 1.2.3.4
(config-pseudowire)#group-name group-1
```

control-word

Use this command to enable control word for the MPLS layer-2 virtual circuit.

Use the no parameter with this command to disable control word from the MPLS layer-2 virtual circuit.

Command Syntax:

```
control-word
no control-word
```

Parameters

NA

Default

By default, control-word is disabled

Command Mode

Configure Pseudowire mode

Applicability

This command was introduced before OcNOS version 1.X

Example

```
#configure terminal
(config)#mpls l2-circuit mycircuit 45678 1.2.3.4
(config-pseudowire)#control-word
```

label-switching

Use this command to either enable label-switching on an interface or to modify the label-space to which this interface is bound.

Use the `no` parameter and the interface is bound to the platform-wide (zero) label-space.

Note: When label-switching enabled on VLAN interface, MTU value must be manually increased by at least 20 bytes on Parent interfaces of VLAN. Example, default MTU must be set as 1520 instead of 1500 on label-switching parent interface label switched VLAN interface. (Parent Interface MTU >= label switched VLAN interface MTU + 20).

Command Syntax

```
label-switching
label-switching <0-60000>
no label-switching
```

Parameter

`<0-60000>`	Label space value in this range

Default

By default, label switching is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows the enabling of label switching on the `eth0` interface.

```
#configure terminal
(config)#interface eth0
(config-if)#label-switching 654
```

match vlan

Use this command to configure a match VLAN action for a service template.

Use the `no` parameter to remove a match VLAN action for a service template.

Command Syntax

```
match (all | double-tag outer-vlan <2-4094> inner-vlan VLAN_RANGE | outer-vlan
  VLAN_RANGE | untagged)
no match (double-tag outer-vlan <2-4094> inner-vlan VLAN_RANGE | outer-vlan
  VLAN_RANGE | untagged)
```

Parameter

`all`	Accept all matches
`double-tag`	Double tag match
`outer-vlan`	Double tag outer VLAN
`<2-4094>`	Outer VLAN identifier
`inner-vlan`	Double tag inner VLAN
`VLAN_RANGE`	VLAN identifier <2-4094> range: 2-5,10 or 2-5,7-19
`outer-vlan`	Single tag outer-VLAN
`VLAN_RANGE`	VLAN identifier <2-4094> range: 2-5,10 or 2-5,7-19
`untagged`	Match untagged. This parameter depends on the `switchport dot1q ethertype` configuration. Packets received with a TPID other than 0x8100 (default value) and the TPID value configured by `switchport dot1q ethertype` are treated as untagged. For example, if you give the command: `switchport dot1q ethertype 0x8888` then packets received with TPID 0x8100 or 0x88a8 are treated as tagged. Packets received with other TPIDs are treated as untagged.

Command Mode

MPLS SVC mode

Applicability

This command was introduced before OcNOS version 1.3 and updated in OcNOS-SP version 1.0.

The inner vlan range option added in OcNOS-SP version 4.1.

Example

```
#configure terminal
(config)#service-template C2
(config-svc)#match double-tag outer-vlan 10 inner-vlan 20
(config-svc)#exit
(config)#service-template C2
(config-svc)#no match double-tag outer-vlan 10 inner-vlan 20
(config-svc)#exit
#configure terminal
```

```
(config)#service-template C3
(config-svc)#match double-tag outer-vlan 10 inner-vlan 200-300
(config-svc)#exit
(config)#service-template C4
(config-svc)#no match double-tag outer-vlan 10 inner-vlan 200-300
(config-svc)#exit
#configure terminal
(config)#service-template t1
(config-svc)#match untagged
(config-svc)#rewrite ingress push 100
```

mpls ac-group

Use this command to create a new access circuit group for MPLS.

Use the `no` parameter with this command to remove an access circuit group.

Command Syntax

```
mpls ac-group NAME <1-4294967295>
no mpls ac-group NAME
```

Parameter

`NAME`	The name of the access circuit group
`<1-4294967295>`	The identifier for the group; used in LDP

Default

By default, mpls ac group is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mpls ac-group new-ac 123

(config)#no mpls ac-group new-ac
```

mpls admin-groups

Use this command to create a name-to-value binding for an administrative group.

Note: Only 32 administrative groups can be configured at one time.

Use the `no` parameter with this command to remove a named administrative group.

Command Syntax

```
mpls admin-group NAME <0-31>
no mpls admin-group NAME <0-31>
```

Parameters

`NAME`	Name of administrative group
`<0-31>`	The value of the administrative group

Default

By default, mpls admin group is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#mpls admin-group mygroup 3
```

mpls bandwidth-class

Use this command to create a new bandwidth class name. Using this command changes the command mode to Bandwidth-class mode.

Use the `no` parameter with this command to remove a bandwidth class name.

Command Syntax

```
mpls bandwidth-class NAME
no mpls bandwidth-class NAME
```

Parameter

`NAME`	Name of the bandwidth class

Default

By default, mpls bandwidth-class is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mpls bandwidth-class new-BC
(config-mpls-bw)#

(config)#no mpls bandwidth-class new-BC
```

mpls ftn-entry tunnel-id

This command will be used to create a static tunnel.

In hardware, it creates a logical interface to which services can be mapped.

Command Syntax

```
mpls ftn-entry tunnel-id <1-5000> A.B.C.D/M LABEL A.B.C.D IFNAME
  (primary|secondary|)
mpls ftn-entry tunnel-id <1-5000> A.B.C.D A.B.C.D LABEL A.B.C.D IFNAME
  (primary|secondary|)
mpls ftn-entry tunnel-id <1-5000> (A.B.C.D/M|A.B.C.D A.B.C.D) <16-1048575> A.B.C.D
  IFNAME ((secondary|primary)|)


no mpls ftn-entry tunnel-id <1-5000> A.B.C.D/M WORD A.B.C.D IFNAME
  (primary|secondary|)
no mpls ftn-entry tunnel-id <1-5000> A.B.C.D A.B.C.D WORD A.B.C.D IFNAME
  (primary|secondary|)
```

Command Syntax

```
mpls ftn-entry tunnel-id <1-5000> X:X::X:X/M <16-1048575> X:X::X:X IFNAME
  ((secondary|primary)|)
mpls ilm-entry <16-52443> swap <16-52443> IFNAME X:X::X:X X:X::X:X/M
mpls ilm-entry <16-52443> IFNAME swap <16-52443> IFNAME X:X::X:X X:X::X:X/M


no mpls ftn-entry tunnel-id <1-5000> X:X::X:X/M <16-1048575> X:X::X:X IFNAME
  ((secondary|primary)|)
no mpls ilm-entry <16-52443> swap <16-52443> IFNAME X:X::X:X X:X::X:X/M
no mpls ilm-entry <16-52443> IFNAME swap <16-52443> IFNAME X:X::X:X X:X::X:X/M
```

Parameters

`<1-5000>`	The tunnel ID value
`A.B.C.D/M`	Forwarding equivalence class with mask
`A.B.C.D`	Mask for forwarding equivalency class
`LABEL`	Outgoing label
`A.B.C.D`	Nexthop IPv4 address
`IFNAME`	Outgoing interface name
`INDEX`	FTN index for update

Note: When the INDEX parameter is passed, the FTN entry is updated. When INDEX is not used, a new FTN entry is created.

`primary`	The primary LSP; default is primary
`secondary`	The secondary LSP Command Mode

Default

By default, mpls ftn-entry tunnel-id are disabled

Command mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mpls ftn-entry tunnel-id 2 10.10.0.0/24 16 1.2.3.4 eth1 secondary
(config)#no mpls ftn-entry tunnel-id 2 10.10.0.0/24 16 1.2.3.4 eth1 secondary
```

mpls ftn-entry

Use this command to create a static LSP. In the hardware, this command creates an IP route with outgoing MPLS parameters.

Command Syntax

```
mpls ftn-entry (A.B.C.D/M|A.B.C.D A.B.C.D) <16-52443> A.B.C.D IFNAME
no mpls ftn-entry A.B.C.D/M LABEL A.B.C.D IFNAME
```

Parameters

A.D.C.D/M	Forwarding Equivalence Class with Mask
LABEL	Outgoing label <16-1048575>
A.B.C.D	Nexthop IPv4 address
IFNAME	Outgoing interface name
INDEX	FTN index for update

Default

By default, mpls ftn-entry are disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)# mpls ftn-entry 2.2.2.2/32 111 20.0.0.2 eth1
(config)# no mpls ftn-entry 2.2.2.2/32 111 20.0.0.2 eth1
```

mpls ilm-entry pop

Use this command to create an ILM entry in the ILM table to which a POP incoming interface is bound. Upon receipt of a labeled packet on an MPLS-enabled router, a lookup is done based on the incoming label in the ILM table. If a match is found, the packet may either be label-switched downstream, or popped and passed over IP. In a pop operation, an outgoing label is not needed as is either accepted or forwarded over IP. The nexthop option is also not mandatory because the FEC IP address could be a local IP address.

Use the `no` option with the command to delete an ILM entry. If there is no match, an error message displays.

Command Syntax

```
mpls ilm-entry LABEL IFNAME (pop)
no mpls ilm-entry LABEL IFNAME (pop)
```

Parameters

`LABEL`	Incoming label value
`IFNAME`	Incoming interface name
`pop`	Pop the incoming label

Default

By default, mpls ilm-entry are disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mpls ilm-entry 100 eth0 pop
```

mpls ilm-entry swap

Use this command to create an ILM entry in the ILM table to which a swap incoming interface is bound. Upon receipt of a labeled packet on an MPLS-enabled router, a lookup is done based on the incoming label in the ILM table. If a match is found, the packet may either be label-switched downstream, or popped and passed over IP.

Use the `no` option with the command to delete an ILM entry. If there is no match, an error message displays.

Command Syntax

```
mpls ilm-entry <16-52443> swap <16-52443> IFNAME A.B.C.D (A.B.C.D/M|A.B.C.D
  A.B.C.D)
mpls ilm-entry <16-52443> IFNAME swap <16-52443> IFNAME A.B.C.D (A.B.C.D/M|A.B.C.D
  A.B.C.D)


no mpls ilm-entry <16-52443> swap <16-52443> IFNAME A.B.C.D (A.B.C.D/M|A.B.C.D
  A.B.C.D)
no mpls ilm-entry <16-52443> IFNAME swap <16-52443> IFNAME A.B.C.D (A.B.C.D/
  M|A.B.C.D A.B.C.D)
```

Parameters

`LABEL`	Incoming label value range <16-1048575>
`IFNAME`	Incoming interface name
`swap`	Specify swap for the incoming label
`LABEL`	Configure an outgoing label with a value from <16-1048575>

Note: A value of 2 indicates explicit NULL and a value of 3 indicates implicit NULL.

`IFNAME`	Outgoing interface name
`A.B.C.D`	Nexthop IPv4 address
`A.B.C.D`	The FEC for which this ILM entry is created
`A.B.C.D/M`	The FEC for which this ILM entry is created, plus mask
`A.B.C.D`	A mask for forwarding equivalence class mask
`<1-429496725>`	ILM index update

Note: When an ILM index value is passed, the ILM entry is updated. If the ILM index is not used, then a new ILM entry is created.

Default

By default, mpls ilm-entry are disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mpls ilm-entry 16 eth1 swap 17 eth2 1.1.1.1 1.1.1.1/3 1
```

mpls ilm-entry vpnpop

Use this command to create an ILM entry in the ILM table to which a VPN POP incoming interface is bound. Upon receipt of a labeled packet on an MPLS-enabled router, a lookup is done based on the incoming label in the ILM table. If a match is found, the packet may either be label-switched downstream, or popped and passed over IP.

Use the `no` option with the command to delete an ILM entry. If there is no match, an error message displays.

Note: This command is not supported for ZebIC releases.

Command Syntax

```
mpls ilm-entry LABEL IFNAME (vpnpop) LABEL IFNAME A.B.C.D (A.B.C.D/M|A.B.C.D
  A.B.C.D) (<1-4294967295>|)
no mpls ilm-entry LABEL IFNAME (vpnpop) LABEL IFNAME A.B.C.D (A.B.C.D/M|A.B.C.D
  A.B.C.D|) (<1-4294967295>|)
```

Parameters

`LABEL`	Incoming label value
`IFNAME`	Incoming interface name
`vpnpop`	Specify pop for the incoming label
`LABEL`	Configure an outgoing label with a value from <16-1048575>

Note: A value of 0 indicates explicit NULL and a value of 3 indicates implicit NULL.

`IFNAME`	Outgoing interface name
`A.B.C.D`	Nexthop IPv4 address
`A.B.C.D`	The FEC for which this ILM entry is created
`A.B.C.D/M`	The FEC for which this ILM entry is created, plus mask
`A.B.C.D`	A mask for forwarding equivalence class mask
`<1-429496725>`	ILM index update

Note: When an ILM index value is passed, the ILM entry is updated. If the ILM index is not used, then a new ILM entry is created.

Default

By default, mpls ilm-entry are disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mpls ilm-entry 100 eth0 vpnpop 200 eth1 1.2.3.4 10.10.0.0/24
```

mpls ingress-ttl

Use this command to set a Time to Live (TTL) value for LSPs for which this LSR is the ingress.

Use the `no` parameter with this command to unset the custom TTL value being used for LSPs for which this LSR is the ingress.

Command Syntax

```
mpls ingress-ttl <0-255>
no mpls ingress-ttl
```

Parameter

`<0-255>`	Set the TTL value to use

Default

By default, mpls ingress-ttl value is 64

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#mpls ingress-ttl 3
```

mpls l2-circuit

Use this command to create an instance of an MPLS layer 2 virtual circuit, without specifying a group to which the VC belongs. Refer to group-name for information on how to create an MPLS “with” a specific group. A Layer-2 MPLS Virtual Circuit instance may be bound to any interface on the router; however, only one interface may be bound to a Layer-2 circuit at a time.

Use the `no` parameter with this command to delete an instance of an MPLS Layer-2 Virtual Circuit.

Command Syntax

```
mpls l2-circuit NAME <1-4294967295> A.B.C.D
mpls l2-circuit NAME <1-4294967295> A.B.C.D mode raw
mpls l2-circuit NAME <1-4294967295> A.B.C.D mode tagged
no mpls l2-circuit NAME <1-4294967295> A.B.C.D
```

Parameters

`NAME`	String identifying the MPLS Layer-2 virtual circuit
`<1-4294967295>`	A 32-bit identifier to which the L2 circuit name should be mapped
`A.B.C.D`	IPv4 address for the MPLS L2 virtual circuit end-point

Default

By default, mpls l2-circuit is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#mpls l2-circuit mycircuit 45678 1.2.3.4
```

mpls-l2-circuit NAME

Use this command in the Interface mode to bind an interface to a MPLS Layer-2 Virtual Circuit created in the configure mode. The qos profiles cos-to-queue and queue-color-to-cos are optional parameters and are configurable dynamically on the virtual circuit by repeating mpls-l2-circuit command along with one or both profile options. In order to dynamically unbind the profile, same command pattern should be repeated by removing the profile which needs to be unbound from the command. Refer ‘qos profile’ commands from configuration guide for more details about qos profiles.

Use the `no` parameter with this command to delete this instance.

Note: QoS profiles are supported only on vlan based virtual circuits. For port based virtual circuits (service template with match-all option), qos profiles can be bound to interface which will take effect, otherwise default qos profile will take effect. Refer ‘qos map-profile’ command for binding qos profiles on interface.

Note: For untagged traffic forwarded via port based virtual circuits (service template with match-all option), queue will be 0 by default. In order to assign a non-zero queue for untagged traffic, use ‘qos untagged-priority <0-7>’ command on the interface.

Note: QoS profile queue-color-to-cos will take effect when MPLS model is uniform. For virtual circuit without rewrite option, ‘qos remark-cos’ need to be additionally configured to update cos. For virtual circuits with rewrite action pop, cos will always be updated based on qos profile irrespective of the MPLS model.

Command Syntax

```
mpls-l2-circuit NAME service-template NAME ({cos-to-queue NAME | queue-color-to-cos
  NAME}|) ((primary|secondary)|)
no  mpls-l2-circuit NAME
```

Parameters

`NAME`	A string identifying the MPLS Layer-2 Virtual Circuit
`primary`	Identify L2 circuit as the primary link
`secondary`	Identify L2 circuit as the secondary link; the secondary link is not activated unless the primary link fails
`service-template`	Customer service template
`NAME`	Name of Customer service template
`cos-to-queue`	Profile for cos to queue map
`NAME`	Profile name for cos to queue map
`queue-color-to-cos`	Profile for queue color to cos map
`NAME`	Profile name for queue color to cos map

Default

By default, mpls l2-circuit is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal

(config)#interface eth1
(config-if)#switchport
(config-if)#mpls-l2-circuit vc1 service-template C1

(config-if)#no mpls-l2-circuit vc1

(config)#interface eth2
(config-if)#switchport
(config-if)#mpls-l2-circuit vc2 service-template C2

(config-if)#no mpls-l2-circuit vc2

(config-if)#mpls-l2-circuit vc2 service-template C2
(config-if)#no mpls-l2-circuit vc2

(config)#interface eth2
(config-if)#switchport
(config-if)#mpls-l2-circuit vc2 service-template C2

(config-if)#no mpls-l2-circuit vc2

(config-if)#mpls-l2-circuit vc2 service-template C2
(config-if)#no mpls-l2-circuit vc2
```

mpls l2-circuit-fib-entry

Use this command to add a static Layer-2 MPLS Virtual Circuit FIB entry.

Use the `no` parameter with this command to delete a Layer-2 MPLS Virtual Circuit FIB entry.

Command Syntax

```
mpls l2-circuit-fib-entry VC-ID
mpls l2-circuit-fib-entry VC-ID LABEL LABEL A.B.C.D IFNAME NAME
no mpls l2-circuit-fib-entry VC-ID
```

Parameters

`VC-ID`	Virtual Circuit ID
`LABEL`	Incoming label in the range of <16-1048575>
`LABEL`	Outgoing label in the range of <16-1048585>
`A.B.C.D`	Nexthop IPv4 address
`IFNAME`	Provider-facing interface name
`NAME`	Access interface name or VC to be stitched to.

Default

By default, mpls l2-circuit is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#mpls l2-circuit-fib-entry 10 100 200 10.10.10.10 eth1 eth2
```

mpls label mode

Use this command to configure label allocation mode for VPNv4 and/or VPNv6 routes. Label allocation mode as per-vrf is the default mode in which single mpls-label is allocated for all VPN Routes in a VRF. Label allocation mode as per-prefix will allocate unique mpls-labels per VPN route in a VRF. If allocation model is disabled using no mpls label mode configuration, the configuration reverts back to default-mode .

Label allocation mode is the local property i.e. the VRF routes are distributed to BGP-peer as per the mode configured on local node. When per-vrf mode is configured, single label for all routes in the VRF will be distributed to peer node.

Label allocation mode can be set for all VRFs or selective VRFs by these commands:

```
mpls label mode vpnv4 all-vrfs per-vrf
```

- If the admin selects the per-vrf mode for the entire system, then all VRFs switches to per-vrf allocation mode except for the VRFs that has been explicitly configured using command mpls label mode vpnv4 vrf WORD per-prefix. Label allocation mode set using specific VRF takes precedence over all-vrf command.

```
mpls label mode vpnv6 vrf WORD per-vrf
```

- If the admin selects per-vrf mode for a particular vrf say vrf1, then only vrf1 switches to per-vrf mode and rest of the vrfs will remain in default allocation mode.

Command Syntax

```
mpls label mode (vpnv4|vpnv6|all-afs) (all-vrfs|vrf WORD) (per-prefix|per-vrf)
no mpls label mode (vpnv4|vpnv6|all-afs) (all-vrfs|vrf WORD) (per-prefix)

mpls label mode 6pe per-prefix
no mpls label mode 6pe per-prefix
```

Parameters

`vrf WORD`	Enter a string to identify the VRF
`all-vrfs`	All the VRFs
`per-prefix`	Unique MPLS labels are allocated per VPN route in a VRF
`per-vrf`	Single MPLS labels are allocated for all VPN routes in a VRF
`all-afs`	All the address families

Default

By default, per-vrf is enabled.

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS-SP version 1.0.

Example

```
#configure terminal
(config)#mpls label mode all-afs all-vrfs per-vrf
```

```
(config)#no mpls label mode all-afs all-vrfs

(config)#mpls label mode 6pe per-prefix

(config)#no mpls label mode 6pe per-prefix
```

mpls local-packet-handling

Use this command to enable the labeling of locally generated TCP packets. All other locally generated packets are not looked at by the MPLS Forwarder

Use the `no` parameter with this command to disable labeling of locally generated TCP packets.

Command Syntax

```
mpls local-packet-handling
no mpls local-packet-handling
```

Default

By default, mpls local packet handling is disabled

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mpls local-packet-handling
```

mpls lsp-model

Use this command to configure the MPLS LSP model as Uniform.

Use the `no` parameter with this command to configure the MPLS LSP model as Pipe or short-pipe.

Command Syntax

```
mpls lsp-model uniform
no mpls lsp-model uniform
```

Parameter

None

Default

By default, model configuration is pipe for XGS devices.

Qumran device has following default behavior:

For L3VPN services, model is short-pipe by default and pipe model can be achieved by configuring policy-maps with match exp and set queue.

For L2VPN services, short-pipe model is not supported and default model is pipe.

For L2VPN services with rewrite action pop, cos value will always be updated from qos profile irrespective of model.

For L2VPN services without rewrite, uniform model command doesn't take effect until 'qos remark-cos' is configured on egress interface.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mpls lsp-model uniform
(config)#exit

#configure terminal
(config)#no mpls lsp-model uniform
(config)#exit
```

mpls lsp-stitching

Use this command to stitch the LSP segment for an FEC created via a different label signaling protocol.

Use the `no` form of this command to disable this configuration.

Command Syntax

```
mpls lsp-stitching
no mpls lsp-stitching
```

Parameters

None

Default

By default, MPLS LSP stitching is disabled.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS-SP version 1.0.

Command Example

```
#configure terminal
(config)#mpls lsp-stitching
```

mpls map-route

Use this command to map a prefix to an FEC.

Use the `no` parameter with this command to disable this configuration.

Command Syntax

```
mpls map-route (A.B.C.D/M|A.B.C.D A.B.C.D) (A.B.C.D/M|A.B.C.D A.B.C.D)
no mpls map-route (A.B.C.D/M|A.B.C.D A.B.C.D)
```

Parameters

`A.B.C.D`	IPv4 prefix to map
`A.B.C.D/M`	IPv4 prefix to map, plus mask
`A.B.C.D`	Mask for IPv4 prefix to map
`A.B.C.D/M`	Mask for IPv4 prefix to map, plus mask.
`A.B.C.D`	IPv4 forwarding equivalence class for route to map
`A.B.C.D`	Mask for IPv4 forwarding equivalence class

Default

By default, mpls map-route is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

In the following examples 5.6.7.8/32 is the FEC for an LSP, and 1.2.3.4 is the prefix to be mapped.

```
#configure terminal
(config)#mpls map-route 1.2.3.4/32 5.6.7.8/32

#configure terminal
(config)#mpls map-route 1.2.3.4 255.255.255.255 5.6.7.8 255.255.255.255
```

mpls min-label-value

Use this command to configure minimum and maximum label value for a label space. Use module names (rsvp | ldp | bgp) to configure minimum and maximum label value for module in a label space, minimum and maximum label space value for a module should be within the range of label space being used. After setting minimum and maximum label value for a label space, make sure to bind the label space to an interface.

Use the `no` parameter with this command to use the default minimum and maximum label value for all the label pools.

Note: The system allows label-space range (maximum and minimum label values) changes for interface-specific label spaces only. The platform-wide label-space range cannot be modified.

Note: Only label-space 0 (global) is supported. Any label-space other than 0, is not supported.

Command Syntax

```
mpls (rsvp|ldp|bgp|) min-label-value <16-1048575> max-label-value <16-1048575>
  (label-space <0-60000>|)
no mpls min-label-value max-label-value (label-space <0-60000>|)
no mpls (rsvp|ldp|bgp) (label-space <0-60000>|))
```

Parameters

`rsvp`	Label range value for RSVP
`ldp`	Label range value for LDP
`bgp`	Label range value for BGP
`min-label-value`	Specify the minimum label value
`<16-1048575>`	Minimum size to be used for label pools or protocol range
`max-label-value`	Specify the maximum label value
`<16-1048575>`	Maximum size for all label pools
`label-space`	Label space for which the minimum value needs to be modified
`<0-60000>`	Range for label space

Default

By default, mpls min-label value is 16

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mpls min-label-value 50000 max-label-value 80000 label-space 0
```

mpls propagate-ttl

Use this command to enable TTL propagation. Enabling TTL propagation causes the TTL value in the IP header to be copied onto the TTL field in the shim header, at the LSP ingress.

Use the `no` parameter with this command to disable TTL propagation.

Command Syntax

```
mpls propagate-ttl
no mpls propagate-ttl
```

Parameters

None

Default

By default, TTL propagation is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mpls propagate-ttl

#configure terminal
(config)#no mpls propagate-ttl
```

mpls traffic-eng

Use this command to configure a routing command level for MPLS Traffic Engineering (MPLS-TP).

Use the `no` parameter with this command to remove this configuration.

Command Syntax

```
mpls traffic-eng (level-1|level-2|router-id)
no mpls traffic-eng (level-1|level-2|router-id)
```

Parameters

`level-1`	Run MPLS-TE only at IS-IS level 1
`level-2`	Run MPLS-TE only at IS-IS level 2
`router-id`	Traffic Engineering stable IP address for system

Command Mode

IS-IS Router mode

Examples

```
#configure terminal
(config)#mpls traffic-eng level-1

(config-router)#no mpls traffic-eng level-1
```

mpls traffic-eng srlg

Use this command to create a Shared Risk Link Group (SRLG). An SRLG uses secondary backup LSPs or Fast Reroute bypass/detour LSPs that minimize the probability of "fate sharing" with the path of the primary LSP.

Use the `no` form of this command to remove an SRLG.

Note: An interface can be part of multiple SRLG groups upto a maximum of 255 SRLG groups.

Any addition or deletion of SRLG value on an interface will not recalculate Primary/Backup. It is advised to configure SRLG values before bringing UP rsvp sessions or clear rsvp sessions after updating SRLG values.

Command Syntax:

```
mpls traffic-eng srlg <0-4294967295>
no mpls traffic-eng srlg <0-4294967295>
```

Parameters

```
<0-4294967295> Risk group number
```

Command Mode

Interface mode

Example

```
#configure terminal
(config)#int eth1
(config-if)#mpls traffic-eng srlg 1
```

ping mpls

Use this command to start sending MPLS request packets using various parameters as defined below. Ping packets can be configured for LDP, RSVP, L2 circuit, VPLS, L3 VPN, or generic FEC types.

Command Syntax

```
ping mpls (ldp A.B.C.D/M|rsvp (tunnel-name NAME|egress A.B.C.D)|l2-circuit (vccv|)
 <1-4294967295> |vpls <1-10000> peer A.B.C.D/M|l3vpn VRFNAME A.B.C.D/M |ipv4
 A.B.C.D/M) ({reply-mode (1|2)|flags|destination A.B.C.D|source A.B.C.D|ttl <1-
 255>|timeout <1-500>|repeat <5-5000>|interval <2-20000>|force-explicit-
 null|detail}|)
ping mpls (ldp A.B.C.D/M|rsvp (tunnel-name NAME|egress A.B.C.D)|l2-circuit (vccv|)
 <1-4294967295> |vpls <1-10000> peer A.B.C.D/M|l3vpn VRFNAME A.B.C.D/M |ipv4
 A.B.C.D/M) ({reply-mode (1|2)|flags|destination A.B.C.D|source A.B.C.D|ttl <1-
 255>|timeout <1-500>|repeat <5-5000>|interval <2-20000>|force-explicit-
 null|detail}|)
ping mpls (l3vpn (VRFNAME A.B.C.D/M X:X::X:X/M source A.B.C.D destination A.B.C.D))
 ({timeout <1-500>|ttl <1-255>|repeat <5-5000>|interval <2-20000>|detail}|)
ping mpls (6pe default X:X::X:X/M source A.B.C.D destination A.B.C.D)) ({timeout
 <1-500>|ttl <1-255>|repeat <5-5000>|interval <2-20000>|detail}|)
```

Parameters

`ldp`	FEC type is LDP
`A.B.C.D/M`	LDP prefix address
`rsvp`	FEC type is RSVP
`tunnel-name`	RSVP tunnel name
`NAME`	Tunnel name string
`egress`	RSVP tunnel egress
`A.B.C.D`	RSVP tunnel egress address
`l2-circuit`	FEC type is L2 circuit
`vccv`	Virtual Circuit Connectivity Verification
`<1-4294967295>`	L2 circuit ID
`vpls`	FEC type is MPLS VPLS (L2-VPN)
`<1-10000>`	VPLS instance ID
`peer`	VPLS peer
`A.B.C.D/M`	VPLS peer address
`l3vpn`	FEC type is MPLS VPN (L3-VPN)
`VRFNAME`	VPN instance name
`A.B.C.D./M`	VPN prefix
`X:X::X:X/M`	VPNv6 prefix
`6pe`	FEC type (6PE)

default	VPN Instance Name (default)
X:X::X:X/M	6PE Prefix
ipv4	FEC type is generic; use for static/SNMP label switched paths
A.B.C.D/M	IPv4 prefix address
reply-mode	Reply mode, one of
1	Do not reply
2	Reply via UDP/IP packet (default)
flags	Validate FEC stack
destination	Destination address
A.B.C.D	IPv4 address of the destination
source	Source address
A.B.C.D	IPv4 address of the source
ttl	Trace packet Time-to-live
<1-255>	Trace packet TTL value
repeat	Repeat sending of ping packets
<5-5000>	Number of pings to send
interval	Interval between ping packets, in milliseconds
<2-20000>	Interval value
timeout	Time to wait before rejecting the probe as a failure, in seconds
<1-500>	Timeout value
force-explicit-null	Force Explicit NULL label
detail	Print detailed output of the ping

Defaults

Default TTL value is 255.

Default timeout value is 60 seconds.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#ping mpls ipv4 10.10.0.0/24 reply-mode 2 flags destination 127.1.2.3 source
10.10.0.1 ttl 226 timeout 65 repeat 6 interval 3 detail force-explicit-null

#ping mpls l2-circuit 3 reply-mode 2 flags destination 127.1.3.4 source 10.10.0.1
ttl 226 timeout 65 repeat 6 interval 3 detail force-explicit-null

#ping mpls l3vpn vrfa 10.10.0.0/24 reply-mode 2 flags destination 127.1.2.3 source
10.10.0.1 ttl 226 timeout 65 repeat 6 interval 3 detail force-explicit-null
```

```
#ping mpls ldp 10.10.0.0/24 reply-mode 2 flags destination 127.1.2.3 source
10.10.0.1 ttl 226 timeout 65 repeat 6 interval 3 detail force-explicit-null

#ping mpls rsvp egress 1.2.3.5 reply-mode 2 flags destination 127.1.2.3 source
10.10.0.1 ttl 226 timeout 65 repeat 6 interval 3 detail force-explicit-null

#ping mpls rsvp tunnel-name tun1 reply-mode 2 flags destination 127.1.2.3 source
10.10.0.1 ttl 226 timeout 65 repeat 6 interval 3 detail force-explicit-null

#ping mpls vpls 2 peer 10.10.0.0 reply-mode 2 flags destination 127.1.2.3 source
10.10.0.1 ttl 226 timeout 65 repeat 6 interval 3 detail force-explicit-null

Codes:
'!' - Success, 'Q' - request not sent, '.' - timeout,
'x' - Retcode 0, 'M' - Malformed Request, 'm' - Errored TLV,
'N' - LBL Mapping Err, 'D' - DS Mismatch,
'U' - Unknown Interface, 'R' - Transit (LBL Switched),
'B' - IP Forwarded, 'F' No FEC Found, 'f' - FEC Mismatch,
'P' - Protocol Error, 'X' - Unknown code,
'Z' - Reverse FEC Validation Failed

 Type 'Ctrl+C' to abort

! seq_num = 1 200.0.0.1 2.02 ms
! seq_num = 2 200.0.0.1 2.00 ms
! seq_num = 3 200.0.0.1 1.93 ms
! seq_num = 4 200.0.0.1 2.14 ms
! seq_num = 5 200.0.0.1 1.78 ms

Success Rate is 100.00 percent (5/5)
round-trip min/avg/max = 1.78/1.96/2.14
```

rewrite ingress

Use this command to configure a match VLAN action for a service template.

Use the `no` parameter with this command to remove a match VLAN action for a service template.

Command Syntax

```
rewrite ingress (((pop |translate <2-4094>)(|outgoing-tpid (dot1.ad |dot1.q)))|
  (push <2-4094>))
no rewrite ingress (pop |push |translate)
```

Parameters

`pop`	POP the outer VLAN identifier from ACCESS->NETWORK and PUSH the match outer VID to NETWORK->ACCESS
`translate`	Translate the outer VLAN identifier to configured action VID for ACCESS->NETWORK and translate to the match outer VID for NETWORK->ACESS
`<2-4094>`	Outer VLAN identifier
`outgoing-tpid`	Outgoing TPID, set the outer-tpid for the NETWORK->ACCESS
`dot1.ad`	Set TPID value as 0x88a8 for the traffic NETWORK->ACCESS
`dot1.q`	Set TPID value as 0x8100 for the traffic NETWORK->ACCESS
`push`	PUSH the outer VLAN identifier from ACESS->NETWORK and POP the Outer VID from NETWORK->ACCESS
`<2-4094>`	Outer VLAN identifier

Command Mode

MPLS SVC mode

Applicability

This command was introduced in OcNOS version 1.3.3, and changed in OcNOS-SP version 1.0.

Examples

```
#configure terminal
(config)#service-template C2
(config-svc)#match double-tag outer-vlan 9 inner-vlan 8
(config-svc)#rewrite ingress translate 7 outgoing-tpid dot1.ad
(config-svc)#exit

(config)#service-template C2
(config-svc)#no rewrite ingress translate
(config-svc)#exit
```

secondary srlg-disjoint

Use this command to set how to avoid the SRLGs (Shared Risk Link Groups) of a protected primary.

A fast-reroute/secondary path for an LSP that is disjoint from the primary ensures that a single point of failure on a particular link does not bring down both the primary and secondary paths in the LSP.

Note: The SRLG option configured in RSVP-TRUNK mode (this command) takes higher preference than the option configured in RSVP router mode (see 'srlg-disjoint').

Use the `no` form of this command to not avoid the SRLGs of a protected interface.

Command Syntax

```
secondary srlg-disjoint (forced|preferred)
no secondary srlg-disjoint
```

Parameters

`forced`	The router does not create the secondary/backup tunnel unless it avoids SRLGs of the primary-path/protected-interface.
`preferred`	With two explicit paths, the first explicit path tries to avoid the SRLGs of the primary-path/ protected interface. If that does not work, the secondary/backup tunne uses the second path (which ignores SRLGs).

Command Mode

RSVP -TRUNK mode

Example

```
#configure terminal
(config)#rsvp-trunk t1
(config-rsvp)# secondary srlg-disjoint forced
```

secondary-priority srlg-disjoint

Use this command to set how to avoid the SRLGs (Shared Risk Link Groups) of a protected primary.

A fast-reroute/secondary path for an LSP that is disjoint from the primary ensures that a single point of failure on a particular link does not bring down both the primary and secondary paths in the LSP.

Note: The SRLG option configured in RSVP-TRUNK mode (this command) takes higher preference than the option configured in RSVP router mode (see the srlg-disjoint command).

Use the `no` form of this command to not avoid the SRLGs of a protected interface.

Command Syntax

```
secondary-priority <1-5> srlg-disjoint (forced|preferred)
no secondary-priority <1-5> srlg-disjoint
```

Parameters

`forced`	The router does not create the secondary/backup tunnel unless it avoids SRLGs of the primary-path/protected-interface.
`preferred`	With two explicit paths, the first explicit path tries to avoid the SRLGs of the primary-path/ protected interface. If that does not work, the secondary/backup tunnel uses the second path (which ignores SRLGs).

Command Mode

RSVP -TRUNK mode

Example

```
#configure terminal
(config)#rsvp-trunk t1
(config-rsvp)# secondary-piority 1 srlg-disjoint forced
```

service-template

Use this command to configure a service template.

Use no form of this command to remove a service template.

Command Syntax

```
service-template NAME
no service-template NAME
```

Parameters

NAME	Name of the customer service template

Defaults

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 1.3.3.

Examples

```
#configure terminal
(config)#service-template C1
(config-svc)#
```

service-tpid

Use this command to configure service tpid for the MPLS layer-2 virtual circuit.

Use the no parameter with this command to delete service tpid from the MPLS layer-2 virtual circuit.

Command Syntax

```
service-tpid (dot1.q|dot1.ad|0x9100)
no service-tpid
```

Parameters

`0x9100`	Set tpid value as 0x9100
`dot1.ad`	Set tpid value as 0x88a8
`dot1.q`	Set tpid value as 0x8100

Default

By default, service-tpid is disabled

Command Mode

Configure Pseudowire mode

Applicability

This command was introduced before OcNOS version 1.X

Example

```
#configure terminal
(config)#mpls l2-circuit mycircuit 45678 1.2.3.4
(config-pseudowire)#service-tpid dot1.ad
```

show mpls

Use this command to display MPLS data.

Command Syntax

```
show mpls
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following subsection displays a variety of `show mpls` commands.

```
#show mpls
Minimum label configured: 16
 Maximum label configured: 1048575
 Per label-space information:
   Label-space 0 is using minimum label: 16 and maximum label: 1048575
   Label-space 2342 is using minimum label: 556 and maximum label: 1048575
 Custom ingress TTL configured: none
 Custom egress TTL configured: none
 Log message detail: none
 Admin group detail: none
 Packets dropped IP:115167, dropped MPLS:0 sent to IP:490943, labeled:0,
switch
d:0

MPLS Differentiated Services Supported Classes data:
CLASS       DSCP_value
  be           000000

MPLS Differentiated Services CLASS to EXP mapping data:
CLASS    DSCP_value     EXP_value
  be      000000           0
#
```

Table 1-2 explains the show command output fields.

Table 1-2: show mpls output field

Field	Description
Packets dropped IP	Displays the number of packets dropped over the internet protocol.
Dropped MPLS	Displays the number of packets dropped over the MPLS.

Table 1-2: show mpls output field

Field	Description
Sent to IP	Displays the number of packets transmitted to the internet protocol.
Labeled	Number of labeled packets in the interface. The MPLS-labeled packets are switched after a label lookup/switch instead of a lookup into the IP table. Labels of pop-and-forward mpls tunnel: P—Pop labels. D—Delegation labels.
Switch	Type of switching on the links needed for the MPLS.
Class	Creates a class map to be used for matching traffic to a specified class, and enters class-map configuration mode.
DSCP Value	The value of the DSCP and DSCP classifier is used for routing Layer 3 packets.
EXP value	Sets the value of the MPLS EXP field on all imposed label entries.

show mpls admin-groups

Use this command to display all configured administrative groups.

Command Syntax

```
show mpls admin-groups
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following sample shows the output of the `show mpls admin-group` command.

```
#show mpls admin-groups
 Admin group detail:
  Value of 0 associated with admin group 'a'
  Value of 1 associated with admin group 'b'
  Value of 2 associated with admin group 'c'
  Value of 4 associated with admin group 'd'
#
```

Table 1-3 explains the show command output fields.

Table 1-3: show mpls admin-groups output field

Field	Description
Admin group detail	Display information about configured Multi Protocol Label Switching (MPLS) administrative groups.

show mpls bandwidth-class

Use this command to view bandwidth class parameters: bandwidth class name; allocated bandwidth; setup hold priority

Command Syntax

```
show mpls bandwidth-class
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
> show mpls bandwidth-class
Bandwidth-class: BW_1
Bandwidth:  6k        Setup-priority: 1  Class-type: 1
```

Table 1-4 explains the show command output fields.

Table 1-4: show mpls bandwidth-class output field

Field	Description
Bandwidth-class	Bandwidth for each class type.
Bandwidth	Bandwidth configured for the active MPLS.
Setup-Priority	The setup priority is compared with other setup priorities for established sessions on the link to determine whether some of them should be preempted to accommodate the new session. Sessions with lower hold priorities are preempted.
Class-type	Bandwidth allocated for the specified class type.

show mpls counters ldp

Use this command to display traffic statistics for FTNs and ILMs configured by LDP.

Command Syntax

```
show mpls counters ldp ((ftn (|A.B.C.D/M)) | (ilm (|A.B.C.D/M)) |)
```

Parameter

`ftn`	FEC-to-NHLFE map counters
`A.B.C.D/M`	FEC prefix
`ilm`	Incoming label map counters
`A.B.C.D/M`	FEC prefix

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 1.3.2.

Note: For Qumran, counters are not available for transit nodes.

Examples

```
#show mpls counters ldp
[ FTN statistics ]
+------------------+-----------+--------------------+--------------------+
|       FEC        | out-label |     Tx packets     |      Tx bytes      |
+------------------+-----------+--------------------+--------------------+
 1.1.61.0/24        52480       0                    0
 1.1.62.0/24        52481       0                    0
 1.1.63.0/24        52482       0                    0
 1.1.64.0/24        52483       0                    0
 9.9.9.3/32         52485       0                    0

[ ILM statistics ]
+------------------+-----------+-----------+--------------------+--------------------+--------------------+----------------+
|       FEC        | in-label  | out-label |     Rx packets     |      Rx bytes      |     Tx packets     |      Tx bytes    |
+------------------+-----------+-----------+--------------------+--------------------+--------------------+----------------+
#
```

Table 1-5 explains the show command output fields.

Table 1-5: show mpls counters ldp output field

Field	Description
FTN statistics	Displays the statistics details of FTN.
ILM statistics	Displays the statistics details of ILM.
FEC	Displays the Forward Equivalency Class (FEC) for this entry.
In-label	Displays the ingress (incoming interface) label for this segment.

Table 1-5: show mpls counters ldp output field

Field	Description
Out-label	Displays the egress (outgoing interface) label for this segment.
Rx packets	Number of hello packets received from the neighbor.
Rx bytes	Size of hello packets received from the neighbor.
Tx packets	Number of hello packets sent to the neighbor.
Tx bytes	Size of hello packets sent to the neighbor.

show mpls counters rsvp

Use this command to display traffic statistics for LSPs configured by RSVP.

Command Syntax

```
show mpls counters rsvp ((tunnel-name NAME) | (tunnel-id TUNNEL_ID) | (node-role
  (ingress | transit | egress)) |)
```

Parameter

NAME	RSVP tunnel name
TUNNEL_ID	RSVP tunnel identifier
ingress	LSP role is ingress
transit	LSP role is transit
egress	LSP role is egress

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 1.3.2.

Note: For Qumran, counters are not available for transit nodes.

Examples

```
#show mpls counters rsvp
Tunnel-id 5001 Extended Tunnel-ID 9.9.9.1 Egress 9.9.9.2
 lsp-name : t1-Primary                                  [Ingress]
 lsp-ingress : 9.9.9.1          lsp-id : 101
 Rx pkts : 0                    Rx bytes : 0
 Tx pkts : 0                    Tx bytes : 0

 lsp-name : t1-Secondary                                [Ingress]
 lsp-ingress : 9.9.9.1          lsp-id : 102
 Rx pkts : 0                    Rx bytes : 0
 Tx pkts : 0                    Tx bytes : 0

Tunnel-id 5002 Extended Tunnel-ID 9.9.9.1 Egress 9.9.9.3
 lsp-name : t2-Primary                                  [Ingress]
 lsp-ingress : 9.9.9.1          lsp-id : 104
 Rx pkts : 0                    Rx bytes : 0
 Tx pkts : 0                    Tx bytes : 0

 lsp-name : t2-Detour                                   [Ingress]
 lsp-ingress : 1.1.49.1         lsp-id : 104
 Rx pkts : 0                    Rx bytes : 0
 Tx pkts : 0                    Tx bytes : 0
```

Table 1-6 explains the show command output fields.

Table 1-6: show mpls counters rsvp output field

Field	Description
Tunnel-id	Tunnel identifier (destination port) for the RSVP session.
Extended Tunnel-ID	Extended Tunnel identifier (destination port) for the RSVP session.
Egress	Egress router is the final MPLS device that removes the last label before packets leave the MPLS network.
lsp-name	Name of the SPRING-TE LSP.
Ingress	The router at the beginning of an LSP. This router encapsulates IP packets with an MPLS Layer 2 frame and forwards it to the next router in the path.
lsp-ingress	The router at the beginning of an LSP.
lsp-id	Specify the generic LSP identifier.
Rx packets	Number of hello packets received from the neighbor.
Rx bytes	Size of hello packets received from the neighbor.
Tx packets	Number of hello packets sent to the neighbor.
Tx bytes	Size of hello packets sent to the neighbor.

show mpls counters static

Use this command to display traffic statistics for statically configured FTNs and ILMs.

Command Syntax

```
show mpls counters static ((ftn (A.B.C.D/M|)) | (ilm (A.B.C.D/M|)) |)
```

Parameter

`ftn`	FEC-to-NHLFE map counters
`A.B.C.D/M`	FEC prefix
`ilm`	Incoming label map counters
`A.B.C.D/M`	FEC prefix

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 1.3.2.

Note: For Qumran, counters are not available for transit nodes.

Examples

```
#show mpls counters static
[ FTN statistics ]
+------------------+-----------+--------------------+--------------------+
|       FEC        | out-label |     Tx packets     |      Tx bytes      |
+------------------+-----------+--------------------+--------------------+
 192.168.1.0/24     100         0                    0
 192.168.2.0/24     200         0                    0

[ ILM statistics ]
+------------------+-----------+-----------+--------------------+--------------------+--------------------+----------------+
|       FEC        | in-label  | out-label |     Rx packets     |      Rx bytes      |     Tx packets     |      Tx bytes  |
+------------------+-----------+-----------+--------------------+--------------------+--------------------+----------------+
 0.0.0.0/0          201         n/a         0                    0                    n/a                  n/a
 0.0.0.0/0          101         n/a         0                    0                    n/a                  n/a
 192.168.3.0/24     301         302         0                    0                    0                    0
 192.168.4.0/24     401         402         0                    0                    0                    0
#
```

Table 1-7 explains the show command output fields.

Table 1-7: show mpls counters static output field

Field	Description
FTN statistics	Displays the statistics details of FTN.
ILM statistics	Displays the statistics details of ILM.
FEC	Displays the Forward Equivalency Class (FEC) for this entry.
In-label	Displays the ingress (incoming interface) label for this segment.

Table 1-7: show mpls counters static output field

Field	Description
Out-label	Displays the egress (outgoing interface) label for this segment.
Rx packets	Number of hello packets received from the neighbor.
Rx bytes	Size of hello packets received from the neighbor.
Tx packets	Number of hello packets sent to the neighbor.
Tx bytes	Size of hello packets sent to the neighbor.

show mpls cross-connect-table

Use this command to display detailed information for all entries created in the MPLS cross-connect table.

Command Syntax

```
show mpls cross-connect-table
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of the show mpls cross-connect-table

```
#show mpls cross-connect-table
  Cross connect ix: 3, in intf: -, in label: 0, out-segment ix: 3
    Owner: RSVP, Persistent: No, Admin Status: Up, Oper Status: Up
   Out-segment with ix: 3, owner: RSVP, out intf: eth1, out label: 16
    Nexthop addr: 10.10.20.80, cross connect ix: 3, op code: Push

  Cross connect ix: 6, in intf: -, in label: 0, out-segment ix: 6
    Owner: RSVP, Persistent: No, Admin Status: Up, Oper Status: Up
   Out-segment with ix: 6, owner: RSVP, out intf: eth1, out label: 17
    Nexthop addr: 10.10.20.80, cross connect ix: 6, op code: Push
#
```

Table 1-8 explains the show command output fields.

Table 1-8: show mpls cross-connect-table output field

Field	Description
Cross connect ix	Displays the table index for the cross-connect.
In intf	Installed as a result of configuring an interface.
In label	Displays the ingress (incoming interface) label for this segment.
Out-segment ix	Displays the outbound segment index.
Owner	Displays the creator of this segment, typically a protocol such as BGP.
Persistent	Displays whether the tunnel is persistent – Yes or No.
Admin Status	Indicates whether the user can administratively disable a peer while still preserving its configuration. Up = Yes, Down = No.

Table 1-8: show mpls cross-connect-table output field

Field	Description
Oper Status	Displays the current status of the cross-connect segment – Up or Down
Nexthop addr	Displays the IP address of the next hop.
Op code	PUSH = Replace the top label with another and then push one or more additional labels onto the label stack SET = Set the next hop label.

show mpls forwarding-table

Use this command to view forwarding table entries.

Command Syntax

```
show mpls forwarding-table (count|)
```

Parameters

`count`	Count of IPv4 FTNs.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
show mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN, B - BGP FTN, K - CLI FTN, t -
tunnel
L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, I - IGP-Shortcut,
U - unknown FTN, O - SR-OSPF FTN, i - SR-ISIS FTN, k - SR-CLI FTN

Code   FEC    FTN-ID   Tunnel-id  Pri  LSP-Type   Out- Label   ELC  Out-Intf  Nexthop
R(t)> 29.29.29.29/32 1  5001 Yes  LSP_DEFAULT 24322  yes
eth2  41.41.41.31
R(t)> 29.29.29.29/32 2   5001 No   LSP_DEFAULT 24322  yes
eth1  69.69.69.42

#show mpls forwarding-table count

-------------------------------------------
Num FTNs         : 3          [UP: 3, INSTALLED: 3]
  Primary FTNs   : 3          [UP: 3, INSTALLED: 3]
  Secondary FTNs : 0          [UP: 0, INSTALLED: 0]
-------------------------------------------
-------------------------------------------
Num  FTNs         : 0          [UP: 0]
  Primary  FTNs   : 0          [UP: 0]
  Secondary  FTNs : 0          [UP: 0]
-------------------------------------------
```

Table 1-9 shows the status codes displayed at the start of a route entry.

Table 1-9: status code output field

Status Code	Field	Description
P	Stale FTN	Stale marked FTN due to on-going Graceful Restart of MPLS module.
B	BGP FTN	FTN entry installed by BGP.
K	CLI FTN	Admin configured Static FTN entry.
L	LDP FTN	FTN entry installed by LDP.
R	RSVP-TE FTN	FTN entry installed by RSVP.
S	SNMP FTN	FTN entry installed via SNMP.
I	IGP-Shortcut	FTN entry installed by IGP shortcut.
U	Unknown FTN	FTN entry installed by unknown module.
O	SR-OSPF FTN	FTN entry installed by OSPF segment-Routing.
I	SR-ISIS FTN	FTN entry installed by ISIS segment-routing.
K	SR-CLI FTN	FTN entry installed by Static Segment Routing.

Table 1-10 explains the show command output fields.

Table 1-10: show mpls forwarding-table output field

Field	Description
FEC	Displays the Forward Equivalency Class (FEC) for this entry.
FTN-ID	FEC-to-NHLFE map counters identification.
Tunnel-ID	Tunnel identification to which packets with this label are going.
Pri	Primary.
LSP-Type	LSP type associated with each interface being protected.
Out-Label	Label received from downstream neighbor for route.
ELC	Whether the RSVP router has Entropy Label Capability.
Out-Intf	Short name of the physical interface through which traffic goes to the protected link.
Nexthop	Displays the IP address of the next hop.
Num FTNs	Number of FEC-to-NHLFE map counters in the interface.
Primary FTNs	Primary FEC-to-NHLFE in the interface.
Secondary FTNs	Secondary FEC-to-NHLFE in the interface.
Num FTNs	Number of FEC-to-NHLFE map counters in protocol.

Table 1-10: show mpls forwarding-table output field

Field	Description
Primary FTNs	Primary FEC-to-NHLFE map counters in protocol.
Secondary FTNs	Secondary FEC-to-NHLFE map counters in protocol.

show mpls ftn-table

Use this command to display FTN (FEC-To-NHLF) table information.

Command Syntax

```
show mpls ftn-table
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mpls ftn-table
Primary FTN entry with FEC: 5.5.5.5/32, id: 2, row status: Active
  Owner: LDP, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0,   Protected LSP id: 0, QoS Resource id: 0, Description: N/A
    Matched bytes:0, pkts:0, TX bytes:0, Pushed pkts:0
     Cross connect ix: 1, in intf: - in label: 0 out-segment ix: 1
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 1, owner: LDP, out intf: p9p1, out label: 3
    Nexthop addr: 40.0.0.2        cross connect ix: 1, op code: Push
     Cross connect ix: 3, in intf: - in label: 0 out-segment ix: 3
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 3, owner: LDP, out intf: p8p1, out label: 3
    Nexthop addr: 30.0.0.2        cross connect ix: 3, op code: Push

 Primary FTN entry with FEC: 50.0.0.0/24, id: 6, row status: Active
  Owner: LDP, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP:
none
  Tunnel id: 0,   Protected LSP id: 0, QoS Resource id: 0, Description: N/A
    Matched bytes:0, pkts:0, TX bytes:0, Pushed pkts:0
     Cross connect ix: 3, in intf: - in label: 0 out-segment ix: 3
      Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 3, owner: LDP, out intf: p8p1, out label: 3
    Nexthop addr: 30.0.0.2        cross connect ix: 3, op code: Push
```

Table 1-11 explains the show command output fields.

Table 1-11: show mpls ftn-table output field

Field	Description
Action-type	Packets flow direction in the tunnel.
Exp-bits	Experimental bits (EXP) field is a 3-bit field in the MPLS header.

Table 1-11: show mpls ftn-table output field

Field	Description
Incoming DSCP	Number of incoming packets in the DSCP.
Tunnel ID	Tunnel identifier (destination port) for the session.
Protected LSP ID	Identifier to protect the LSP in the interface.
QoS Resource ID	Resource identifier of the Quality of Service.
Description	Terms and concepts used to describe MPLS.
Matched bytes	Size of the matched packets.
Pkts	Number packets in the interface.
TX bytes	Size of the packets that transmitted to the neighbor.
Cross connect ix	Displays the table index for the cross-connect.
Pushed pkts	Number of hello packets pushed to the neighbor.
in intf	Installed as a result of configuring an interface.
in label	Displays the ingress (incoming interface) label for this segment.
out-segment ix	Displays the outbound segment index.
Persistent	Displays whether the tunnel is persistent – Yes or No.
Admin Status	Indicates whether the user can administratively disable a peer while still preserving its configuration. Up = Yes, Down = No.
Oper Status	Displays the current status of the cross-connect segment – Up or Down.
Out-Label	Label received from downstream neighbor for route.
Out-Intf	Short name of the physical interface through which traffic goes to the protected link.
Nexthop addr	Displays the IP address of the next hop.
OP code	PUSH = Replace the top label with another and then push one or more additional labels onto the label stack. SET = Set the next hop label.
Primary FTN entry with FEC	Primary FTN entry configured for the FEC.
ID	Displays the Opcode that identifies the specific PDU for this entry.
ROW status	Displays the current status of the row.

show mpls ilm-table

Use this command to view Incoming label mapping (ILM) table entries.

Command Syntax

```
show mpls ilm-table (count|)
```

Parameters

`count`	Count of entries in ILM table.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mpls ilm-table
Codes: > - installed ILM, * - selected ILM, p - stale ILM
        K - CLI ILM,T - MPLS-TP

Code  FEC                ILM-ID      In-Label    Out-Label   In-Intf   Out-
Intf     Nexthop                     LSP-Type
  >   63.63.63.63/32     151187      53121       3          N/A      xe6
6.6.6.63                     LSP_DEFAULT
  >   16.16.16.0/24      151186      53120       3          N/A      xe6
6.6.6.63                     LSP_DEFAULT
 K>   N/A                151189      500         N/A        N/A      N/A
127.0.0.1                    LSP_DEFAULT
  >   65.65.65.65/32     151188      53122       3          N/A      xe1
1.1.1.65                     LSP_DEFAULT

#show mpls ilm-table count
-------------------------------------------
Num ILMs          : 4          [UP: 4, INSTALL: 4]
  Swap Entries    : 3          [UP: 3, INSTALL: 3]
  Pop Entries     : 1          [UP: 1, INSTALL: 1]
-------------------------------------------
```

Table 1-9 shows the status codes displayed at the start of a route entry.

Table 1-12: status code output field

Status Code	Field	Description
	Installed ILM	Number of ILM entry installed.
*	Selected ILM	ILM entry selected in the interface.
P	Stale ILM	Stale marked ILM due to on-going graceful restart of MPLS module.

Table 1-12: status code output field

Status Code	Field	Description
K	CLI ILM	Admin configured static ILM entry.
T	MPLS-TP	ILM entry installed by MPLS-TP.

Table 1-2 explains the show command output fields.

Table 1-13: show mpls ilm-table output field

Field	Description
FEC	Displays the Forward Equivalency Class (FEC) for this entry.
ILM-ID	ILM identifier for the session.
LSP-Type	LSP type associated with each interface being protected.
Out-Label	Label received from downstream neighbor for route.
Out-Intf	Short name of the physical interface through which traffic goes to the protected link.
In label	Displays the ingress (incoming interface) label for this segment.
In intf	Installed as a result of configuring an interface.
Nexthop	Displays the IP address of the next hop.
Num ILMs	Number of ILMs in the session.
Swap Entries	Number of packets in the entry.
Pop Entries	Number of POP entries.

show mpls in-segment-table

Use this command to display detailed information about all entries in the Incoming Label Map (also known as in-segment) table.

Command Syntax

```
show mpls in-segment-table
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mpls in-segment-table
  Owner: RSVP,#of pops: 1, fec: 192.168.0.5/32
    RX bytes:0, pkts:0, TX bytes:0, Swapped pkts:0, Popped pkts:0
LSP Type: ELSP_CONFIG
Class_Exp mapping:
CLASS    DSCP_value     EXP_value
  be      000000           0
     Cross connect ix: 1, in intf: eth0 in label: 52480 out-segment ix: 1
      Owner: RSVP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 1, owner: RSVP, out intf: eth1, out label: 52480
        Nexthop addr: 20.30.0.3        cross connect ix: 1, op code: Swap
     Cross connect ix: 1, in intf: eth0 in label: 52480 out-segment ix: 2
      Owner: RSVP, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: RSVP, out intf: eth2, out label: 52481
        Nexthop addr: 30.30.0.3        cross connect ix: 1, op code: Swap
#
```

Table 1-14 explains the show command output fields.

Table 1-14: show mpls in-segment-table output field

Field	Description
FEC	Displays the Forward Equivalency Class (FEC) for this entry.
RX bytes	Size of hello packets received from the neighbor.
Pkts	Number packet in the interface.
TX bytes	Size of the packets that transmitted to the neighbor.
Swapped pkts	Number of swapped packets in session.

Table 1-14: show mpls in-segment-table output field

Field	Description
Popped pkts	Number of popped packets in the interface.
LSP-Type	LSP type associated with each interface being protected.
CLASS	Creates a class map to be used for matching traffic to a specified class, and enters class-map configuration mode.
DSCP value	The value of the DSCP and DSCP classifier is used for routing Layer 3 packets.
EXP value	Sets the value of the MPLS EXP field on all imposed label entries.
Cross-connect ix	Displays the table index for the cross-connect.
Out-Label	Label received from downstream neighbor for route.
Out-Intf	Short name of the physical interface through which traffic goes to the protected link.
In label	Displays the ingress (incoming interface) label for this segment.
In intf	Installed as a result of configuring an interface.
Nexthop	Displays the IP address of the next hop.
Out-segment ix	Displays the outbound segment index.
Persistent	Displays whether the tunnel is persistent – Yes or No.
Admin Status	Indicates whether the user can administratively disable a peer while still preserving its configuration. Up = Yes, Down = No.
Oper Status	Displays the current status of the cross-connect segment – Up or Down.
Op code	PUSH = Replace the top label with another and then push one or more additional labels onto the label stack. SET = Set the next hop label.

show mpls l2-circuit

Use this command to view MPLS-TP L2 circuit parameters.

Command Syntax

```
show mpls l2-circuit (detail|)
show mpls l2-circuit NAME (detail|)
```

Parameters

`detail`	Show detailed information
`NAME`	The name of the virtual circuit

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mpls l2-circuit detail
MPLS Layer-2 Virtual Circuit: vc1, id: 1 PW-INDEX: 1 service-tpid: 8100

Endpoint: 1.1.1.1
Control Word: 0
MPLS Layer-2 Virtual Circuit Group: none
Bound to interface: xe41
Virtual Circuit Type: Ethernet VLAN
Virtual Circuit is configured as Primary
Virtual Circuit is configured as Active
Virtual Circuit is active
Service-template : C1
Match criteria : 10-14, 16-20
```

Table 1-15 explains the show command output fields.

Table 1-15: show mpls l2-circuit output field

Field	Description
MPLS Layer-2 Virtual Circuit	The MPLS virtual circuit on the egress PE router or switch and the specified neighbor, testing the integrity of the Layer 2 circuit between the ingress and egress PE routers or switches.
Endpoint	Endpoint address.
Control Word	Number of control words.
MPLS Layer-2 Virtual Circuit Group	The MPLS virtual circuit group on the egress PE router or switch and the specified neighbor, testing the integrity of the Layer 2 circuit between the ingress and egress PE routers or switches.

Table 1-15: show mpls l2-circuit output field

Field	Description
Bound to interface	A bound service is the server in a client-server interface.
Virtual Circuit Type	Type of virtual circuit in the interface.
Service-template	Service Templates provides a powerful mechanism to configure advanced service-related options.
Match criteria	The match criteria under which redistribution is allowed for the current route-map.

show mpls l2-circuit statistics

Use this command to display MPLS traffic statistics for l2 circuit.

Command Syntax

```
show mpls l2-circuit NAME statistics (access-port|network-port|)
```

Parameters

`NAME`	Name of L2 circuit
`access-port`	Displays the access port statistics
`network-port`	Displays the network port statistics

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mpls l2-circuit t1 statistics
MPLS Layer-2 Virtual Circuit: t1, id 100        # Virtual circuit name and ID
Access port statistics:
   RX: Input packets : 1000
       Input bytes : 120000
   TX: Output packets : 0
       Output bytes : 0
Network port statistics:
   RX: Input packets : 0
       Input bytes : 0
   TX: Output packets : 1000
       Output bytes : 120000
```

Table 1-16 explains the show command output fields.

Table 1-16: show mpls l2-circuit statistics output field

Field	Description
MPLS Layer-2 Virtual Circuit	The MPLS virtual circuit on the egress PE router or switch and the specified neighbor, testing the integrity of the Layer 2 circuit between the ingress and egress PE routers or switches.
Virtual circuit name and ID	The MPLS virtual circuit identifier on the egress PE router or switch and the specified neighbor, testing the integrity of the Layer 2 circuit between the ingress and egress PE routers or switches.
Access port statistics	Traffic statistics on Access port of VC/VPLS.
Network port statistics	Traffic statistics on Provider port of VC/VPLS.
RX	Number of received packets.

Table 1-16: show mpls l2-circuit statistics output field

Field	Description
Input packets	Number of hello packets received from the neighbor.
Input bytes	Size of hello packets received from the neighbor.
TX	Number of packets transmitted.
Output packets	Number of hello packets sent to the neighbor.
Output bytes	Size of hello packets sent to the neighbor.

show mpls mapped-routes

Use this command to view MPLS mapped routes.

Use the `no` parameter with this command to reset this configuration.

Command Syntax

```
show mpls mapped-routes
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mpls mapped-routes

Mapped-route        IPv4 FEC            MPLS-TP Tunnel
14.1.2.3/32         N/A                 NH4
```

Table 1-17 explains the show command output fields.

Table 1-17: show mpls mapped-routes output field

Field	Description
Mapped-route	Map the route of the interface.
IPv4	IPv4 address of the neighbor interface.
FEC	Displays the Forward Equivalency Class (FEC) for this entry.
MPLS-TP Tunnel	MPLS-TP tunnel can be provisioned between two arbitrary nodes in an MPLS-TP enabled network.

show mpls out-segment-table

Use this command to display detailed information of out-segment entries (also known as NHLFE) table.

Command Syntax

```
show mpls out-segment-table
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mpls out-segment-table
       Out-segment with ix: 1, owner: RSVP, out intf: eth1, out label: 52480
        Nexthop addr: 20.30.0.3        cross connect ix: 1, op code: Swap
        TX bytes:0, pkts:0, error pkts:0, discard pkts:0

       Out-segment with ix: 2, owner: RSVP, out intf: eth2, out label: 52481
        Nexthop addr: 30.30.0.3        cross connect ix: 1, op code: Swap
        TX bytes:0, pkts:0, error pkts:0, discard pkts:0Zx
```

Table 1-18 explains the show command output fields.

Table 1-18: show mpls out-segment-table output field

Field	Description
Out-segment ix	Displays the outbound segment index.
Out-Label	Label received from downstream neighbor for route.
Out-Intf	Short name of the physical interface through which traffic goes to the protected link.
Nexthop addr	Displays the IP address of the next hop.
Cross-connect ix	Displays the table index for the cross-connect.
Op code	PUSH = Replace the top label with another and then push one or more additional labels onto the label stack. SET = Set the next hop label.
Pkts	Number packet in the interface.
TX bytes	Size of the packets that transmitted to the neighbor.

Table 1-18: show mpls out-segment-table output field

Field	Description
Error pkts	Number of error packets.
Discard pkts	Number of packets discarded in the interface.

show mpls qos-resource

Use this command to display detailed QoS resource information.

Command Syntax

```
show mpls qos-resource IFNAME
```

Parameters

IFNAME	Display the interface name for a QoS resource

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mpls qos-resource eth1
<*****************************************>
              QOS RESERVED TABLE
<*****************************************>
HOLD PRIORITY : 0

HOLD PRIORITY : 1

HOLD PRIORITY : 2

HOLD PRIORITY : 3

HOLD PRIORITY : 4

HOLD PRIORITY : 5

HOLD PRIORITY : 6

HOLD PRIORITY : 7
<*****************************************>
   QOS AWAITING TABLE (static resources)
<*****************************************>
HOLD PRIORITY : 0

HOLD PRIORITY : 1

HOLD PRIORITY : 2

HOLD PRIORITY : 3

HOLD PRIORITY : 4

HOLD PRIORITY : 5

HOLD PRIORITY : 6
```

```
    HOLD PRIORITY : 7
    TSUP-173>
```

Table 1-19 explains the show command output fields.

Table 1-19: show mpls qos-resource output fields

Field	Description
QOS RESERVED TABLE	FTM/ILM entries for which QOS is reserved.
HOLD PRIORITY	Determines the degree to which an LSP holds onto its session reservation after the LSP has been set up successfully
QOS AWAITING TABLE (static resources)	FTN/ILM entries for which QOS reservation is pending.

show mpls vc-table

Use this command view configured virtual circuit (VC) components

Command Syntax

```
show mpls vc-table
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show mpls vc-table

VC-ID Vlan-ID Inner-Vlan-ID Access-Intf Network-Intf Out Label  Tunnel-Label
Nexthop Status
500     N/A         N/A           eth2          eth1         544         57
N/A    Active
#
```

Table 1-20 explains the show command output fields.

Table 1-20: show mpls vc-table output fields

Field	Description
VC-ID	The virtual circuit ID for the Provider Edge (PE) MPLS.
Vlan-ID	Virtual LAN (VLAN) ID number.
Inner-Vlan-ID	Inner Virtual LAN (VLAN) ID number.
Access-Intf	The Interface Access page provides a method with which to control access to specific areas of the interface.
Network-Intf	A networking interface allows a computer or mobile device to connect to a local area network (LAN) using Ethernet as the transmission mechanism.
Out Label	Label received from downstream neighbor for route.
Tunnel-Label	Used to provide reachability between PE devices.
Nexthop Status	Displays the network status of the next hop.

show mpls vrf

Use this command to display detailed information of all the configured VRF entries. Specify the name of the VRF to display information about a specific VRF entry.

Command Syntax

```
show mpls vrf-table
show mpls vrf-table VRFNAME (count|)
```

Parameters

VRFNAME	Display the MPLS VRF table by its configured name
count	Display the MPLS VRF FTN's count

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show mpls vrf new_vrf count
-------------------------------------------
Num VRF-FTNs          : 1          [UP: 1, INSTALLED: 1]
-------------------------------------------
-------------------------------------------
Num  VRF-FTNs          : 0          [UP: 0]
-------------------------------------------
```

Table 1-21 explains the show command output fields.

Table 1-21: show vrf-table output fields

Field	Description
Num VRF-FTNs	Number of FEC-to-NHLFE map counters in VRF protocol.
Num VRF-FTNs	Number of VRF FEC-to-NHLFE map counters in protocol.

show mpls vrf-forwarding-table vrf

This CLI can be used to display a tabular output of the VRF forwarding entries received from the remote PE via MPBGP.

Command Syntax

```
show mpls vrf-forwarding-table vrf <VRFNAME>
```

Parameters

VRFNAME	Display the MPLS VRF table by its configured name

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.1.

Examples

```
OcNos#show mpls vrf-forwarding-table vrf BEVrf
Owner     FEC                        FTN-ID    Oper-Status    Out-Label    Tunnel-id    NHLFE-id    Out-Intf    Nexthop
BGP       10.143.73.1/32              1          Up            24320        0            19          xe25        10.143.73.1
BGP       10.143.73.10/32             6          Up            25600        0            30          xe4         10.143.73.10
BGP       10.143.169.26/31            2          Up            24320        0            19          xe25        10.143.73.1
BGP       10.143.170.26/31            3          Up            24324        0            28          xe4         10.143.73.6
```

Table 1-22 explains the show command output fields.

Table 1-22: show mpls vrf-forwarding-table vrf output fileds

Field	Description
Owner	Displays the creator of this entry, typically a protocol such as BGP.
FEC	Displays the Forward Equivalency Class (FEC) for this entry.
FTN-ID	FEC-to-NHLFE identification.
Oper-Status	Displays the current status of the entry – Up or Down. It will be “UP” if the vrf entry is installed in the forwarder and it will be in “DOWN“ state if the vrf entry is not installed in the forwarder.
Out-Label	Displays the egress label for this FTN.
Tunnel-id	Tunnel identification to which packets of this FTN are going.
NHLFE-id	Next Hop Label Forwarding Entry identification (also known as out-segment entry identification).
Out-Intf	Name of the physical interface through which traffic goes.
Nexthop	Displays the IP address of the next hop.

show running-config interface mpls

Use this command to show the running system status and configuration for an MPLS interface.

Command Syntax

```
show running-config interface IFNAME mpls
```

Parameters

IFNAME	Display information for this interface name

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config interface eth1 mpls

#
```

show running-config mpls

Use this command to show any Multi-Protocol Label Switching (MPLS) related running configuration.

Command Syntax

```
show running-config mpls
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#show running-config mpls
!
mpls propagate-ttl
!
!
!
#
```

show running-config service-template

Use this command to show service-template related running configuration.

Command Syntax

```
show running-config service-template
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.2.

Examples

```
OcNOS#sho running-config service-template
!
service-template s2
 match outer-vlan 200
!
service-template s1
 match outer-vlan 100
!
service-template s3
 match outer-vlan 300
!
service-template s4
 match outer-vlan 400
!
```

show running-config vc

Use this command to show any Virtual Private Wire Service (VPWS) related running configuration.

Command Syntax

```
show running-config vc
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.2.

Examples

```
OcNOS#show running-config vc
!
mpls l2-circuit vc1 1 2.2.2.2
!
mpls l2-circuit vc2 3 2.2.2.2
 tunnel-select-policy p1
!
!
interface xe2
 mpls-l2-circuit vc1 service-template s1 primary
 mpls-l2-circuit vc2 service-template s3 primary
!
```

show running-config vpls

Use this command to show any Virtual Private LAN Service (VPLS) related running configuration.

Command Syntax

```
show running-config vpls
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS-SP version 4.2.

Examples

```
#show running-config vpls
!
mpls vpls vpls1 2
 signaling ldp
  vpls-type vlan
  vpls-peer 2.2.2.2
  exit-signaling
 exit-vpls
!
mpls vpls vpls2 4
 signaling ldp
  vpls-type vlan
  vpls-peer 2.2.2.2 tunnel-select-policy p1
  exit-signaling
 exit-vpls
!
!
interface xe2
 mpls-vpls vpls1 service-template s2
 mpls-vpls vpls2 service-template s4
!
```

show service-template

Use this command to display information of all or particular service templates.

Command Syntax

```
show service-template (detail|)
show service-template NAME
```

Parameters

detail	Show detailed information
NAME	Name of customer service template

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 1.3.3.

Examples

```
#show service-template detail
 Service-template : C2
  Services mapped : -
  Match criteria : 9/8

 Service-template : C1
  Services mapped : -
  Match criteria : 100

 Service-template : C3
  Services mapped : -
  Match criteria : 2-5

#show service-template C1
 Service-template : C1
  Services mapped : -
  Match criteria : 100
```

Table 1-23 explains the show command output fields.

Table 1-23: show service template output fields

Field	Description
Service-template	Creates a service template and enters service template configuration mode.
Services mapped	Used to match the type of services.
Match criteria	Used to approve the identification result or dismiss it.

show vccv statistics

Use this command to display VCCV messages received prior to advertising capability.

Command Syntax

```
show vccv statistics
```

Parameters

None

Command Mode

Privileged mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following is the sample output for `show vccv statistics` command.

```
#show vccv statistics
  CC Mismatch Discards - 10
```

Table 1-24 explains the show command output fields.

Table 1-24: show vccv statistics output fields

Field	Description
CC Mismatch Discards	Number of CC mismatch packets received from neighbor discarded.

srlg-disjoint

Use this command to set how to avoid the SRLGs (Shared Risk Link Groups) of a protected primary.

A fast-reroute/secondary path for an LSP that is disjoint from the primary ensures that a single point of failure on a particular link does not bring down both the primary and secondary paths in the LSP.

Note: The SRLG option configured in RSVP-TRUNK mode (see the secondary-priority srlg-disjoint command) takes higher preference than the option configured in RSVP router mode (this command).

Use the `no` form of this command to not avoid the SRLGs of a protected interface.

Command Syntax

```
srlg-disjoint (forced|preferred)
no srlg-disjoint
```

Parameters

`forced`	The router does not create the secondary/backup tunnel unless it avoids SRLGs of the primary-path/protected-interface.
`preferred`	With two explicit paths, the first explicit path tries to avoid the SRLGs of the primary-path/protected interface. If that does not work, the secondary/backup tunnel uses the second path (which ignores SRLGs).

Command Mode

Router RSVP mode

Example

```
#configure terminal
(config)#router rsvp
(config-rsvp)# srlg-disjoint forced
```

trace mpls

Use this command to trace the route traversed by a specified echo request packet in an MPLS protocol. Trace requests can be configured for LDP, RSVP, L2 VC, VPLS, and L3 VPN label switched paths.

```
trace mpls (6pe default X:X::X:X/M|ldp A.B.C.D/M|rsvp (tunnel-name NAME|egress
  A.B.C.D)|l3vpn VRFNAME A.B.C.D/M|ipv4 A.B.C.D/M) ({reply-mode
  (2)|flags|destination A.B.C.D|source A.B.C.D|timeout <1-500>|force-explicit-
  null|detail}|)
```

Parameters

`6pe`	FEC type is 6pe
`default`	VPN Instance Name (default)
`X:X::X:X/M`	6pe prefix address
`ldp`	FEC type is LDP
`A.B.C.D/M`	LDP prefix address
`rsvp`	FEC type is RSVP
`tunnel-name`	RSVP tunnel name
`NAME`	Tunnel name string
`egress`	RSVP tunnel egress
`A.B.C.D`	RSVP tunnel egress address
`l3vpn`	FEC type is MPLS VPN (L3-VPN)
`VRFNAME`	VPN instance name
`A.B.C.D./M`	VPN prefix
`ipv4`	FEC type generic; use for static/SNMP label switched paths
`A.B.C.D/M`	IPv4 prefix address
`X:X::X:X/M`	VPNv6 prefix
`reply-mode`	Reply mode, one of
`2`	Reply via UDP/IP packet (default)
`flags`	Validate FEC stack
`destination`	Destination address
`A.B.C.D`	IPv4 address of the destination
`source`	Source address
`A.B.C.D`	IPv4 address of the source
`timeout`	Time to wait before rejecting the probe as a failure, in seconds
`<1-500>`	Timeout value
`force-explicit-null`	Force Explicit NULL label
`detail`	Print detailed output of the trace probe

Defaults

Default timeout value is 60 seconds.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#trace mpls ipv4 10.10.0.0/24 reply-mode 2 flags destination 127.1.2.3 source
10.10.0.1 timeout 65 detail force-explicit-null

#trace mpls l3vpn vrfa 10.10.0.0/24 reply-mode 2 flags destination 127.1.2.3
source 10.10.0.1 timeout 65 detail force-explicit-null

#trace mpls ldp 10.10.0.0/24 reply-mode 2 flags destination 127.1.2.3 source
10.10.0.1 timeout 65 detail force-explicit-null

#trace mpls rsvp egress 1.2.3.5 reply-mode 2 flags destination 127.1.2.3 source
10.10.0.1 timeout 65 detail force-explicit-null

#trace mpls rsvp tunnel-name tun1 reply-mode 2 flags destination 127.1.2.3 source
10.10.0.1 timeout 65 detail force-explicit-null
```

tunnel-id

Use this command to configure tunnel identifier for the MPLS transport tunnel to be used for the MPLS layer-2 virtual circuit.

Use the no parameter with this command to delete tunnel identifier from the MPLS layer-2 virtual circuit.

Command Syntax:

```
tunnel-id <1-5000>
no tunnel-id
```

Parameters

<1-5000>	Identifying value for Tunnel-id

Default

By default, tunnel-id is disabled

Command Mode

Configure Pseudowire mode

Applicability

This command was introduced before OcNOS version 1.X

Example

```
#configure terminal
(config)#mpls l2-circuit mycircuit 45678 1.2.3.4
(config-pseudowire)#tunnel-id 22
```

tunnel-name

Use this command to configure tunnel name for the MPLS transport tunnel to be used for the MPLS layer-2 virtual circuit.

Use the no parameter with this command to delete tunnel name from the MPLS layer-2 virtual circuit.

Command Syntax:

```
tunnel-name NAME
no tunnel-name
```

Parameters

NAME	Identifying name for MPLS Tunnel

Default

By default, tunnel-name is disabled

Command Mode

Configure Pseudowire mode

Applicability

This command was introduced before OcNOS version 1.X

Example

```
#configure terminal
(config)#mpls l2-circuit mycircuit 45678 1.2.3.4
(config-pseudowire)#tunnel-name pe1-to-pe2
```

tunnel-select-policy

Use this command to configure tunnel selection policy name for the MPLS transport tunnel to be used for the MPLS layer-2 virtual circuit.

Use the no parameter with this command to delete tunnel selection policy name from the MPLS layer-2 virtual circuit.

Command Syntax

```
tunnel-select-policy POLICYNAME
no tunnel-select-policy
```

Parameters

POLICYNAME	Selection policy name for MPLS Tunnel

Default

By default, tunnel-select-policy is disabled

Command Mode

Configure Pseudowire mode

Applicability

This command was introduced before OcNOS version 1.X

Example

```
#configure terminal
(config)#mpls l2-circuit mycircuit 45678 1.2.3.4
(config-pseudowire)#tunnel-select-policy policy1
```

vccv cc-type

Use this command to configure the VCCV control channel for MPLS layer-2 virtual circuit.

Use the no parameter with this command to disable control channel from MPLS layer-2 virtual circuit.

Command Syntax

```
vccv cc-type (type-1|type-2|type-3)
no vccv cc-type (type-1|type-2|type-3)
```

Parameters

`type-1`	CC Type 1 - PWE3 Control Word with 0001b as first nibble
`type-2`	CC Type 2 - MPLS Router Alert Label
`type-3`	CC Type 3 - MPLS PW Label with TTL == 1

Default

By default, vccv is disabled

Command Mode

Configure Pseudowire mode

Applicability

This command was introduced before OcNOS version 1.X

Example

```
#configure terminal
(config)#mpls l2-circuit mycircuit 45678 1.2.3.4
(config-pseudowire)# vccv cc-type type-2
```

vccv cv-type

Use this command to configure the VCCV control verification for MPLS layer-2 virtual circuit.

Use the no parameter with this command to disable control verification from MPLS layer-2 virtual circuit.

Command Syntax:

```
vccv cv-type (type-1|type-2|type-3|type-4)
no vccv cv-type (type-1|type-2|type-3|type-4)
```

Parameters

type-1	BFD IP/UDP-encapsulated for PW Fault Detection only
type-2	BFD IP/UDP-encapsulated for PW Fault Detection and AC/PW Fault Status Signalling
type-3	BFD PW-ACH-encapsulated for PW Fault Detection only
type-4	BFD PW-ACH-encapsulated for PW Fault Detection and AC/PW Fault Status Signalling

Default

By default, vccv is disabled

Command Mode

Configure Pseudowire mode

Applicability

This command was introduced before OcNOS version 1.X

Example

```
#configure terminal
(config)#mpls l2-circuit mycircuit 45678 1.2.3.4
(config-pseudowire)# vccv cv-type type-1
```

CHAPTER 2 Differentiated Services Commands

This chapter describes the RSVP Differentiated Services (DiffServ) commands.

map-route A.B.C.D

Use this command to map a IPv4 prefix route onto a trunk. This route is to be used for packets that are mapped to a specific RSVP trunk.

Use the `no` parameter with this command for unmapping routes from specified trunks.

Command Syntax

```
map-route A.B.C.D A.B.C.D
map-route A.B.C.D A.B.C.D CLASS
map-route A.B.C.D/M
map-route A.B.C.D/M CLASS
no map-route A.B.C.D A.B.C.D
no map-route A.B.C.D A.B.C.D CLASS
no map-route A.B.C.D/M
no map-route A.B.C.D/M CLASS
```

Parameters

`A.B.C.D`	Specify the IPV4 address to be mapped.
`A.B.C.D`	Specify a mask to be applied to the address being mapped.
`A.B.C.D/M`	Specify the IPV4 address to be mapped, with mask.
`CLASS`	Specify the DiffServ Class Name (for example, `be`, `ef` etc.) used for selecting incoming IP packets to be mapped to a specified RSVP trunk.

Default

By default, map route A.B.C.D is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#map-route 1.1.2.2/24 be
```

override-diffserv

Use this command to enable the Differentiated Services (Diff-Serv) override configuration.

If a Path message is received without a Diff-Serv object by a Diff-Serv enabled node, it can be interpreted either as a request for an E-LSP (EXP-Inferred-PSC LSP) or as a request for Non-Diff-Serv LSP. This command supports the override option and when configured, the LSR interprets a path message without a Diff-Serv object as a request for Non-Diff-Serv LSP.

Use the `no` parameter with this command disable this feature.

Command Syntax

```
override-diffserv
no override-diffserv
```

Parameters

None

Default

By default, override diffserv is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router rsvp
(config-router)#override-diffserv
```

primary class-to-exp-bit

Use this command to configure a primary PHB-EXP (Per-Hop Behavior-Experimental) mapping to be used by an E-LSP (EXP-Inferred-PSC LSP). This mapping is different from the node level PHB-EXP mapping.

Use the `no` parameter with this command to remove a PHB-EXP mapping configuration from current E-LSP PHB-EXP mapping.

Command Syntax

```
primary class-to-exp-bit CLASS <0-7>
no primary class-to-exp-bit CLASS <0-7>
```

Parameters

`CLASS`	Specify the DiffServ Class Name (for example, be, ef etc.) used for selecting incoming IP packets to be mapped to a specified RSVP trunk.
`<0-7>`	Exp bit which is to be mapped to this PHB.

Default

By default, primary map class is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#primary class-to-exp-bit af12 3

(config)#rsvp-trunk T1
(config-trunk)#no primary class-to-exp-bit af12 3
```

primary elsp-signaled

Use this command to configure a primary Diff-Serv (Differentiated Services) explicitly signaled E-LSP (EXP-Inferred-PSC LSP) interface.

The classes 1 to 7 are optional parameters that can be selected from node level PHB-EXP (Per-Hop Behavior) mapping as PHBs, which will then be used for an E-LSP. If you do not specify a class with this command, all classes will be selected for the E-LSP.

Use the no parameter with this command to remove the configuration.

Command Syntax

```
primary elsp-signaled
primary elsp-signaled CLASS1
primary elsp-signaled CLASS1 CLASS2
primary elsp-signaled CLASS1  CLASS2 CLASS3
primary elsp-signaled CLASS1  CLASS2 CLASS3 CLASS4
primary elsp-signaled CLASS1  CLASS2 CLASS3 CLASS4 CLASS5
primary elsp-signaled CLASS1  CLASS2 CLASS3 CLASS4 CLASS5 CLASS6
primary elsp-signaled CLASS1  CLASS2 CLASS3 CLASS4 CLASS5 CLASS6 CLASS7
no primary elsp-signaled
```

Parameter

`CLASS<0-7>`	Diffserv class alias. e.g.: be, ef, af11, etc.

Default

By default, primary elsp signaled is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#primary elsp-signaled cs2 cs5 cs6

(config)#rsvp-trunk T1
(config-trunk)#no primary elsp-signaled
```

primary llsp

Use this command to configure a primary Differentiated Services Label-Only-Inferred-PSC (Diff-Serv L-LSP) interface, which will use Diff-Serv Class as its PHB Scheduling Class (PSC).

Use the no parameter with this command to remove the Diff-Serv L-LSP configuration.

Command Syntax

```
primary llsp CLASS
no primary llsp
```

Parameters

CLASS<0-7>	Diffserv class alias. e.g: be, ef, af11, etc.

Default

By default, primary llsp is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

This command is not available on QUMRAN devices.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#primary llsp cs4

(config)#rsvp-trunk T1
(config-trunk)#no primary llsp
```

secondary map class

Use this command to configure a secondary PHB-EXP (Per-Hop Behavior-Experimental) mapping to be used by an E-LSP (EXP-Inferred-PSC LSP). This mapping is different from the node level PHB-EXP mapping.

Use the no parameter with this command to remove a PHB-EXP mapping configuration from current E-LSP PHB-EXP mapping.

Command Syntax

```
secondary map class-to-exp-bit CLASS  <0-7>
no secondary map class-to-exp-bit CLASS  <0-7>
```

Parameters

CLASS	Diff-Serv class (queue) mapped to the particular PHB. Diffserv class alias e.g: be, ef, af11, etc.
<0-7>	Exp bit that is to be mapped to this PHB.

Default

By default, secondary map class is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#secondary class-to-exp-bit cs4 3

(config)#rsvp-trunk T1
(config-trunk)#no secondary class-to-exp-bit cs4 3
```

secondary elsp-signaled

Use this command to configure a secondary Diff-Serv (Differentiated Services) explicitly signaled E-LSP (EXP-Inferred-PSC LSP) interface. The classes 1 to 7 are optional parameters can be selected from the node level PHB-EXP (Per-Hop Behavior) mapping as PHBs. They will then be used for an E-LSP. If you do not specify a class with this command, all classes will be selected for the E-LSP.

Use the no parameter with this command to remove the configuration.

Command Syntax

```
secondary elsp-signaled
secondary elsp-signaled CLASS1
secondary elsp-signaled CLASS1 CLASS2
secondary elsp-signaled CLASS1 CLASS2 CLASS3
secondary elsp-signaled  CLASS1 CLASS2 CLASS3 CLASS4
secondary elsp-signaled  CLASS1 CLASS2 CLASS3 CLASS4 CLASS5
secondary elsp-signaled CLASS1 CLASS2 CLASS3 CLASS4 CLASS5 CLASS6
secondary elsp-signaled CLASS1 CLASS2 CLASS3 CLASS4 CLASS5 CLASS6 CLASS7
no secondary elsp-signaled
```

Parameters

CLASS<0-7>	Diffserv class alias. e.g: be, ef, af11, etc.

Default

By default, secondary elsp signaled is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#secondary elsp-signaled class cs3 cs6 cs2 cs5

(config)#rsvp-trunk T1
(config-trunk)#no secondary elsp-signaled
```

secondary llsp

Use this command to configure a secondary Differentiated Services Label-Only-Inferred-PSC (Diff-Serv L-LSP) interface, which will use Diff-Serv Class as its PHB Scheduling Class (PSC).

Use the no parameter with this command to remove the Diff-Serv L-LSP configuration.

Command Syntax

```
secondary llsp CLASS
no secondary llsp
```

Parameters

CLASS<0-7>	Diffserv class alias. e.g: be, ef, af11, etc.

Default

By default, secondary llsp is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

This command is not available on QUMRAN devices.

Example

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#secondary llsp class cs5

(config)#rsvp-trunk T1
(config-trunk)#no secondary llsp
```

show rsvp diffserv-info

Use this command to display node level Differentiated Services (Diff-Serv) configuration information. This information includes the node level PHB-EXP mapping configured for ELSP-signaled LSP.

Command Syntax

```
show rsvp diffserv-info
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

Following is a sample output of the `show rsvp diffserv-info` command.

```
#show rsvp diffserv-info
CLASS-EXP mapping:
CLASS    DSCP_value
 c5  101000 0
 be  000000 1
 cs1 001000 2
 cs3 011000 3
 cs2 010000 4
 cs4 100000 5
 cs6 110000 6
 cs7 111000 7
```

Table 2-25 explains the show command output fields.

Table 2-25: show rsvp diffserv-info output fields

Field	Description
CLASS	MPLS class type that corresponds to the DiffServ traffic engineering class.
EXP_value	Exp value is initialized at the ingress routing device only and overrides the rewrite configuration established for that forwarding class.

CHAPTER 3 Virtual Private LAN Service Commands

This chapter describes each VPLS (Virtual Private LAN Service) command.

ac-admin-status

Use this command to configure the admin status of an attachment circuit specific to a VPLS instance.

Command Syntax

```
ac-admin-status down
no ac-admin-status
```

Parameter

`down`	set the admin role as DOWN

Default

By default, ac admin status is up

Command Mode

Interface VPLS

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows the configuration of admin status for attachment circuit specific to VPLS instance

```
#configure terminal
(config)#interface xe1
(config-if)#mpls-vpls vpls1 service-template st1
(config-if-vpls)#no ac-admin-status
```

ac-description

Use this command to add description for an attachment circuit specific for a VPLS instance

Use the no parameter with this command to remove the description

Command Syntax

```
ac-description LINE
```

Parameter

LINE	Characters describing this AC

Default

By default, ac description LINE is disabled

Command Mode

Interface VPLS

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows the configuration of description for attachment circuit specific to VPLS instance

```
#configure terminal
(config)#interface xe1
(config-if)#mpls-vpls vpls1 service-template st1
(config-if-vpls)#ac-description AC1_VPLS1
```

allow-l2protocol-peer

Use this command to peer L2CP packets.

Command Syntax

```
allow-l2protocol-peer
no allow-l2protocol-peer
```

Parameter

NA

Default

By default, L2CP packets are tunneled

Command Mode

Interface VPLS

Applicability

This command is introduced in OcNOS-SP version 5.0

Example

VPLS AC mode

```
OcNOS(config)#interface xe1/1
OcNOS(config-if)#mpls-vpls vpls1 service-template vc1
OcNOS(config-if-vpls)#allow-l2protocol-peer
OcNOS(config-if-vpls)#no allow-l2protocol-peer
```

clear mpls vpls

Use this command to clear VPLS data.

Command Syntax

```
clear mpls vpls (NAME |) mac-addresses
```

Parameters

`NAME`	Clear data for the VPLS instance with name given
`mac-addresses`	Flush all MAC addresses for a VPLS instance

Command Mode

Exec mode and privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear mpls vpls VPLS_123 mac-addresses
```

control-word

Use this command to enable control-word for a VPLS instance.

Use the `no` parameter with this command to disable control-word.

Command Syntax

```
control-word
no control-word
```

Parameters

None

Default

By default, control-word is disabled.

Command Mode

VPLS mode

Applicability

This command was introduced in OcNOS-SP version 4.1.

Example

```
#(config-vpls)#control-word
#(config-vpls)#no control-word
```

exit-signaling

Use this command to exit the VPLS signaling configuration mode, and start signaling. To configure signaling with LDP, see the signaling ldp command. Other VPLS signaling configuration commands include show mpls vpls, show mpls vpls, vpls-vc, vpls-ac-group, and vpls-peer.

Note: It is *critical* to give this command after all VPLS signaling configurations are complete, otherwise signaling does not start.

Command Syntax

```
exit-signaling
```

Parameters

None

Default

No default value is specified

Command Mode

VPLS Signaling mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
# configure terminal
(config)#mpls vpls test 100
(config-vpls)#signaling ldp
(config-vpls-sig)#exit-signaling
```

exit-if-vpls

Use this command to exit from Interface VPLS mode

Command Syntax

```
exit-if-vpls
```

Parameter

None

Default

No default value is specified

Command Mode

Interface VPLS

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows exiting from interface VPLS mode

```
#configure terminal
(config)#interface xe1
(config-if)#mpls-vpls vpls1 service-template st1
(config-if-vpls)#ac-description AC1_VPLS1
(config-if-vpls)#exit-if-vpls
(config-if-vpls)#exit
```

learning disable (VPLS Mode)

Use this command to disable learning for a VPLS instance.

Use the `no` form of this command to enable learning on a VPLS instance.

Note: This command disables learning on all the attachment circuits and pseudo-wires belonging to that VPLS instance.

Command Syntax

```
learning disable
no learning disable
```

Parameter

None

Default

By default, learning disable is disabled

Command Mode

VPLS mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config-vpls)#mpls vpls vpls2 vlan 3
(config-vpls)#learning disable
(config-vpls)#exit

#configure terminal
(config-vpls)#mpls vpls vpls2 vlan 3
(config-vpls)#no learning disable
(config-vpls)#exit
```

learning disable (Interface VPLS Mode)

Use this command to disable learning on a particular Attachment Circuit (AC) interface.

Use the learning enable command to enable learning on a particular AC interface.

Note: This command disables MAC learning only on that interface.

Command Syntax

```
learning disable
```

Parameter

None

Default

By default, learning disable is disabled

Command Mode

Interface VPLS mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#mpls-vpls vpls1 service-template st1
(config-if-vpls)#learning disable
(config-if-vpls)#exit
```

learning enable

Use this command to enable learning on a particular attachment circuit (AC) interface.

Use the learning disable (Interface VPLS Mode) command to disable learning on a particular AC interface.

Note: This command enables MAC learning only on that AC interface.

Command Syntax

```
learning enable
```

Parameter

None

Default

By default, learning enable is enabled

Command Mode

Interface VPLS mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#mpls-vpls vpls1 service-template st1
(config-if-vpls)#learning enable
(config-if-vpls)#exit
```

no learning

Use this command to reset learning on a particular AC-interface to the global learning configuration.

Command Syntax

```
no learning
```

Parameter

None

Default

By default, no learning is disabled

Command Mode

Interface VPLS mode and VPLS mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#mpls-vpls vpls1 service-template st1
(config-if-vpls)#no learning
(config-if-vpls)#exit
(config)#

#configure terminal
(config)#mpls vpls vpls5 vlan 34
(config-vpls)#learning limit 500
(config-vpls)#exit
(config)#
```

mac

Use this command to add static MAC address for a VPLS instance

Use the no parameter with this command to remove static MAC address

Command Syntax

```
mac XXXX.XXXX.XXXX IFNAME(|vlan <1-4094>)
no mac XXXX.XXXX.XXXX IFNAME(|vlan <1-4094>)
```

Parameter

IFNAME	Interface name
vlan	VLAN Interface
<1-4094>	VLAN ID

Default

By default, mac is disabled

Command Mode

VPLS mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mpls vpls vpls1 10
(config-vpls)#mac 0001.a001.0801 xe1 vlan 10
```

mpls vpls

Use this command to create an instance of MPLS-based Virtual Private LAN Services (VPLS).

Use the `no` parameter with this command to delete an MPLS-based VPLS instance.

Command Syntax

```
mpls vpls NAME
mpls vpls NAME <1-4294967295>
no mpls vpls NAME
```

Parameters

`NAME`	VPLS instance identifier
`<1-4294967295>`	VPLS instance identifier

Default

By default, mpls vpls is disabled

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#mpls vpls t1 6489
(config-vpls)#exit
```

mpls-vpls service-template

Use this command to bind a VPLS instance to a service template.

Use the no parameter with this command unbind the VPLS instance from service template.

Command Syntax

```
mpls-vpls VPLS_NAME service-template TEMPLATE_NAME
no mpls-vpls VPLS_NAME service-template TEMPLATE_NAME
```

Parameters

VPLS_NAME	VPLS instance name
TEMPLATE_NAME	Service template name

Default

N/A

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#switchport
(config-if)#mpls-vpls VPLS1 service-template C1
(config_if_vpls)#exit-if-vpls

(config-if)#no mpls-vpls VPLS1 service-template C1
(config_if)#exit-if-vpls
```

show bgp l2vpn vpls

This command displays details about Layer 2 Virtual Private Network (L2VPN) Virtual Private LAN Service (VPLS) for BGP VPLS Signaling.

Command Syntax

```
show bgp l2vpn vpls (rr|) (detail|)
show bgp l2vpn vpls <1-4294967295>
show bgp l2vpn vpls summary
show bgp l2vpn vpls internal
```

Parameters

`<1-4294967295>`	VPLS-ID value for VPLS
`detail`	Show detailed L2VPN information
`internal`	Internal
`rr`	Layer-2 VPN RR
`summary`	Summary of BGP VPLS neighbor status

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3 and updated in OcNOS version 6.4.0.

Examples

Using `show bgp l2vpn vpls` command without parameters displays information about all VPLS instances.

The example below displays information about the VPLS instance.

```
R1#show bgp l2vpn vpls summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor         V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ   Up/Down
2.2.2.2          4   100    3          5       1      0      0  00:00:13
3.3.3.3          4   100    2          5       1      0      0  00:00:13
4.4.4.4          4   100    3          5       1      0      0  00:00:13
5.5.5.5          4   100    3          5       1      0      0  00:00:13

Total number of neighbors 4

Total number of Established sessions 0

R1#show bgp l2vpn vpls
VPLS-ID     VE-ID    Discovered-Peers   Route-Target
```

```
11          11      4                   100:11

R1#show bgp l2vpn vpls 11

VPLS ID: 11
VE-ID: 11
Discovered Peers: 4
Route-Target: 100:11
Local RD: 100:11
All Local Label Blocks:
 [LB:25664, VBO:1, VBS:64]
 [LB:25600, VBO:65, VBS:64]
Mesh Peers:
 BGP Peer:2.2.2.2/32
  VC Nbr Address:2.2.2.2, RD:100:11, VE-ID:2
  VC Details: VC-ID:1112
  Remote (LB:25664,VBO:65,VBS:64)  Local (LB:25664,VBO:1,VBS:64)
  LB sent on known VEID:Yes
  In Label:25665, Out Label:25710
  PW Status:Established
  VC Installed:Yes
  VC Signaled Time: 00:02:49

 BGP Peer:3.3.3.3/32
  VC Nbr Address:2.2.2.2, RD:100:11, VE-ID:44
  VC Details: VC-ID:11144
  Remote (LB:26304,VBO:65,VBS:64)  Local (LB:25664,VBO:1,VBS:64)
  LB sent on known VEID:Yes
  In Label:25707, Out Label:26350
  PW Status:Established
  VC Installed:No
  VC Signaled Time:

 BGP Peer:3.3.3.3/32
  VC Nbr Address:4.4.4.4, RD:100:11, VE-ID:44
  VC Details: VC-ID:11144
  Remote (LB:26304,VBO:65,VBS:64)  Local (LB:25664,VBO:1,VBS:64)
  LB sent on known VEID:Yes
  In Label:25707, Out Label:26350
  PW Status:Established
  VC Installed:Yes
  VC Signaled Time: 00:02:53

 BGP Peer:5.5.5.5/32
  VC Nbr Address:5.5.5.5, RD:100:11, VE-ID:5
  VC Details: VC-ID:1115
  Remote (LB:25664,VBO:65,VBS:64)  Local (LB:25664,VBO:1,VBS:64)
  LB sent on known VEID:Yes
  In Label:25668, Out Label:25710
  PW Status:Established
  VC Installed:Yes
  VC Signaled Time: 00:02:49

R1#show bgp l2vpn vpls detail

VPLS ID: 11
VE-ID: 11
```

```
Discovered Peers: 4
Route-Target: 100:11
Local RD: 100:11
All Local Label Blocks:
 [LB:25664, VBO:1, VBS:64]
 [LB:25600, VBO:65, VBS:64]
Mesh Peers:
 BGP Peer:2.2.2.2/32
  VC Nbr Address:2.2.2.2, RD:100:11, VE-ID:2
  VC Details: VC-ID:1112
  Remote (LB:25664,VBO:65,VBS:64)  Local (LB:25664,VBO:1,VBS:64)
  LB sent on known VEID:Yes
  In Label:25665, Out Label:25710
  PW Status:Established
  VC Installed:Yes
  VC Signaled Time: 00:02:59

 BGP Peer:3.3.3.3/32
  VC Nbr Address:2.2.2.2, RD:100:11, VE-ID:44
  VC Details: VC-ID:11144
  Remote (LB:26304,VBO:65,VBS:64)  Local (LB:25664,VBO:1,VBS:64)
  LB sent on known VEID:Yes
  In Label:25707, Out Label:26350
  PW Status:Established
  VC Installed:No
  VC Signaled Time:

 BGP Peer:3.3.3.3/32
  VC Nbr Address:4.4.4.4, RD:100:11, VE-ID:44
  VC Details: VC-ID:11144
  Remote (LB:26304,VBO:65,VBS:64)  Local (LB:25664,VBO:1,VBS:64)
  LB sent on known VEID:Yes
  In Label:25707, Out Label:26350
  PW Status:Established
  VC Installed:Yes
  VC Signaled Time: 00:03:03

 BGP Peer:5.5.5.5/32
  VC Nbr Address:5.5.5.5, RD:100:11, VE-ID:5
  VC Details: VC-ID:1115
  Remote (LB:25664,VBO:65,VBS:64)  Local (LB:25664,VBO:1,VBS:64)
  LB sent on known VEID:Yes
  In Label:25668, Out Label:25710
  PW Status:Established
  VC Installed:Yes
  VC Signaled Time: 00:02:59

R1#show bgp l2vpn vpls rr
RD        RR-Clients     Non-Clients           Route-Target        RD_KEY
100:11     2                 3                   100:11         [11:0.0.0.0]
100:11     2                 3                   100:11         [11:2.2.2.2]
100:11     2                 3                   100:11         [11:4.4.4.4]

R1#show bgp l2vpn vpls rr detail

Route-Target: 100:11, RD_KEY: [11:0.0.0.0]
  Peer:2.2.2.2
```

```
    RR Client  : Yes
    Nbr:2.2.2.2/32
      NLRI [VEID:2,LB:25600,VBO:1,VBS:64]
      NLRI [VEID:2,LB:25664,VBO:65,VBS:64]
  Peer:5.5.5.5
    RR Client  : No
    Nbr:5.5.5.5/32
      NLRI [VEID:5,LB:25600,VBO:1,VBS:64]
      NLRI [VEID:5,LB:25664,VBO:65,VBS:64]
  Peer:3.3.3.3
    RR Client  : No
    Nbr:2.2.2.2/32
      NLRI [VEID:44,LB:26240,VBO:1,VBS:64]
      NLRI [VEID:2,LB:25600,VBO:1,VBS:64]
      NLRI [VEID:44,LB:26304,VBO:65,VBS:64]
      NLRI [VEID:2,LB:25664,VBO:65,VBS:64]
    Nbr:4.4.4.4/32
      NLRI [VEID:44,LB:26240,VBO:1,VBS:64]
      NLRI [VEID:44,LB:26304,VBO:65,VBS:64]
  Peer:Self Peer
    RR Client  : No

Route-Target: 100:11, RD_KEY: [11:2.2.2.2]
  Peer:2.2.2.2
    RR Client  : Yes
    Nbr:2.2.2.2/32
      NLRI [VEID:2,LB:25600,VBO:1,VBS:64]
      NLRI [VEID:2,LB:25664,VBO:65,VBS:64]

Route-Target: 100:11, RD_KEY: [11:4.4.4.4]
  Peer:4.4.4.4
    RR Client  : Yes
    Nbr:4.4.4.4/32
      NLRI [VEID:44,LB:26240,VBO:1,VBS:64]
      NLRI [VEID:44,LB:26304,VBO:65,VBS:64]

R1#show bgp l2vpn vpls internal
BGP Local Routes DB
-------------------------
RN:0x7f16eaeda000, Key:11 Key-Len:32 Lock: 9
  RN-INFO:0x7f16e8e0b6b8 Peer:2.2.2.2 local_ve_id:2
    VPLS:11, RT:100:11 VE-ID:11 RR_CLIENT_COUNT: 2
     Nbr:2.2.2.2/32
       NLRI [VEID:2,LB:25600,VBO:1,VBS:64]
       NLRI [VEID:2,LB:25664,VBO:65,VBS:64]
  RN-INFO:0x7f16e8e0b408 Peer:5.5.5.5 local_ve_id:5
    VPLS:11, RT:100:11 VE-ID:11 RR_CLIENT_COUNT: 2
     Nbr:5.5.5.5/32
       NLRI [VEID:5,LB:25600,VBO:1,VBS:64]
       NLRI [VEID:5,LB:25664,VBO:65,VBS:64]
  RN-INFO:0x7f16e8e0b158 Peer:3.3.3.3 local_ve_id:2
    VPLS:11, RT:100:11 VE-ID:11 RR_CLIENT_COUNT: 2
     Nbr:2.2.2.2/32
       NLRI [VEID:44,LB:26240,VBO:1,VBS:64]
       NLRI [VEID:2,LB:25600,VBO:1,VBS:64]
       NLRI [VEID:44,LB:26304,VBO:65,VBS:64]
       NLRI [VEID:2,LB:25664,VBO:65,VBS:64]
```

```
      Nbr:4.4.4.4/32
        NLRI [VEID:44,LB:26240,VBO:1,VBS:64]
        NLRI [VEID:44,LB:26304,VBO:65,VBS:64]
  RN-INFO:0x7f16e8e0b000 Peer:Self Peer local_ve_id:111
    VPLS:11, RT:100:11 VE-ID:11 RR_CLIENT_COUNT: 2

RN:0x7f16e26e90a0, Key:11 Key-Len:37 Lock: 0
  RN-INFO: NULL!!

RN:0x7f16e26e9140, Key:[11:2.2.2.2] Key-Len:64 Lock: 4
  RN-INFO:0x7f16e8e0b560 Peer:2.2.2.2 local_ve_id:2
    VPLS:11, RT:100:11 VE-ID:11 RR_CLIENT_COUNT: 2
     Nbr:2.2.2.2/32
       NLRI [VEID:2,LB:25600,VBO:1,VBS:64]
       NLRI [VEID:2,LB:25664,VBO:65,VBS:64]

RN:0x7f16e26e9000, Key:[11:4.4.4.4] Key-Len:64 Lock: 4
  RN-INFO:0x7f16e8e0b2b0 Peer:4.4.4.4 local_ve_id:44
    VPLS:11, RT:100:11 VE-ID:11 RR_CLIENT_COUNT: 2
     Nbr:4.4.4.4/32
       NLRI [VEID:44,LB:26240,VBO:1,VBS:64]
       NLRI [VEID:44,LB:26304,VBO:65,VBS:64]


BGP VPLS DB - Local/Remote
--------------------------
  VPLS: 11, RT:100:11 VE-ID:11 [Locally Configured] Lock: 1
    All Local Label Blocks:
      [LB:25664, VBO:1, VBS:64]
      [LB:25600, VBO:65, VBS:64]
    BGP Peer: 2.2.2.2/32
    VC:: Nbr:2.2.2.2, [Local VE-ID:11] [Remote VE-ID:2] Installed:Yes Lock: 1
    BGP Peer: 3.3.3.3/32
    VC:: Nbr:2.2.2.2, [Local VE-ID:11] [Remote VE-ID:44] Installed:No Lock: 2
    VC:: Nbr:4.4.4.4, [Local VE-ID:11] [Remote VE-ID:44] Installed:Yes Lock:2
    BGP Peer: 4.4.4.4/32
    VC:: Nbr:4.4.4.4, [Local VE-ID:11] [Remote VE-ID:44] Installed:No Lock: 1
    BGP Peer: 5.5.5.5/32
    VC:: Nbr:5.5.5.5, [Local VE-ID:11] [Remote VE-ID:5] Installed:Yes Lock: 1
```

show mpls vpls

Use this command to display logging information configured for MPLS.

Command Syntax

```
show mpls vpls
show mpls vpls detail
show mpls vpls mesh
show mpls vpls NAME
show mpls vpls NAME mesh
show mpls vpls NAME spoke
show mpls vpls spoke
show mpls vpls count
```

Parameters

`detail`	Display detailed VPLS information
`mesh`	Display MPLS VPLS Mesh Forwarding information. Use this parameter to display information about all core Virtual Circuit (VC) connections for all VPLS instances. Give the name of a VPLS instance to display information about that instance.
`NAME`	Display the identifying string for the VPLS domain
`spoke`	Display MPLS VPLS Spoke Forwarding information. Use this parameter to display information about all spoke VC connections for all VPLS instances. Give the name of a VPLS instance to display information about that instance.
`count`	Display the count of VPLS instances

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Examples

Using `show mpls vpls` command without parameters displays information about all VPLS instances.

The example below displays information about the VPLS instance `v1`, returned when using the `NAME` parameter.

```
#show mpls vpls t1
Virtual Private LAN Service Instance: t1, ID: 1
 Group ID: 0, VPLS Type: Ethernet VPLS, Configured MTU: 0
 Description: none
 Configured interfaces: none
 Mesh Peers: 192.168.0.80 (Up)
             192.168.0.90 (Up)
 Spoke Peers: t100 (Up)
#
```

Table 3-26 explains the show command output fields.

Table 3-26: show mpls vpls t1 output field

Field	Description
Virtual Private LAN Service Instance	Number of VPLAN service instance.
ID	VPLAN identification detail for service instance.
Group ID	Group identification detail for VLAN.
VPLS Type	Type of VPLS in the interface.
Configured MTU	Number of configured MTU in the VPLs.
Description	Details of VPLS.
Configured interfaces	Description of the configured interfaces.
Mesh Peers	Configuring the VPLS mesh peers.
Spoke Peers	Configuring the VPLS spoke peers.

The example below displays the name of the VPLS instance, its ID, they type of instance (Ethernet), the M and S peers, and the signaling protocol. For the first entry, the signaling protocol is BGP and for the second entry it is LDP.

```
#show mpls vpls
Name  VPLS-ID     Type            MPeers    SPeers    SIG-Protocol
v1    100         Ethernet        1         0         BGP
v3    300         Ethernet        1         0         LDP
```

Table 3-27 explains the show command output fields.

Table 3-27: show mpls vpls output field

Field	Description
Name	Type of the MPLS protocol.
VPLS-ID	Identification detail of VPLS.
Type	Type of VPLS in MPLS protocol.
Mesh Peers	Configuring the VPLS mesh peers.
Spoke Peers	Configuring the VPLS spoke peers.
SIG-Protocol	Type of protocol in MPLS configuration.

The example below displays the output when using the `detail` parameter. It displays information for VPLS instance `v1`, including the signaling protocol.

```
#show mpls vpls detail
Virtual Private LAN Service Instance: vpls1, ID: 10
SIG-Protocol: LDP
Attachment-Circuit :UP
Learning: Enabled
Group ID: 0, VPLS Type: Ethernet VLAN, Configured MTU: 1500
Description: none
service-tpid: dot1.q
Operating mode: Tagged
Svlan Id: 0
Svlan Tpid: 8100
Configured interfaces:
Interface: xe39

Service-template : t1
Match criteria : Accept all
Mesh Peers:
2.2.2.2 (Up)
```

Table 3-28 explains the show command output fields.

Table 3-28: show mpls vpls details output field

Field	Description
Virtual Private LAN Service Instance	Number of VPLS service instance.
ID	VPLS identification detail for service instance.
SIG-Protocol	Type of protocol in MPLS configuration.
Attachment-Circuit	Details of the attached circuit in interface.
Learning	State of the interface.
Group ID	Group identification detail for VLAN.
VPLS Type	Type of VPLS in MPLS protocol.
Configured MTU	Number of configured MTU in the VPLs.
Description	Details of VPLS.
Service-tpid	Service TP identifier configured for the VPLS PW.
Operating mode	Type of mode in the interface.
Svlan Id	Configures a specific virtual LAN (VLAN).
Svlan Tpid	Service vlan TP identifier for the VPLS PW.
Redundancy admin role	Creating a Backup Administrator Role.
Redundancy oper role	Operational Role of the VPLS instance.

Table 3-28: show mpls vpls details output field

Field	Description
Configured interfaces	Details of the configured interfaces.
Interface	Selects an interface to configure.
Oper-state	Displays the current status of the cross-connect segment – Up or Down.
Service-template	Used to configure advanced service-related option.
Match criteria	Identifies prefix characteristics (network, BGP path attribute, nexthop, and so on) for a specific sequence.
Mesh Peers	Configuring the VPLS mesh peers.
PW Status Local	Used to perform limited local configuration changes, monitor device status and utilization, and simple local troubleshooting.
Remote	PW status of Remote end.

The example below displays the output provided when using the `mesh` parameter without a specific VPLS name.

```
VPLS-ID  Peer Addr Tunnel-Label In-Label Network-Intf Out-Label Lkps/St PW-
INDEX    SIG-Protocol
100      2.2.2.2   N/A           52503    eth2           53258      0/Dn
2        BGP
300      2.2.2.2   N/A           none      N/A            none      0/Dn
1        LDP
```

Table 3-29 explains the show command output fields.

Table 3-29: show mpls vpls output field

Field	Description
VPLS-ID	Identification details of the VPLS.
Peer Addr	IP address of the peer device.
Tunnel-Label	Tunnel label used for the next segment.
In-label	Displays the ingress (incoming interface) label for this segment.
Out-Label	Label received from downstream neighbor for route.
Network-Intf	Installed as a result of configuring an interface.
Lkps/St	Opcode and Status of the VPLS PW.
PW-INDEX	Index of the VPLS entry in PW table.
SIG-Protocol	Signaling protocol used for VPLS labels advertisement.

The following is a sample output of the `show mpls vpls detail` command displaying detailed information about all configured VPLS instances.

```
#show mpls vpls detail
Virtual Private LAN Service Instance: vpls3100, ID: 3100
SIG-Protocol: BGP
Route-Distinguisher :65010:3100
Route-Target :65010:3100
VE-ID :31
Attachment-Circuit :UP
Learning: Enabled
Group ID: 0, Configured MTU: 9216
Description: none
service-tpid: dot1.q
Operating mode: Raw
Configured interfaces:
Interface: xe26
Service-template : vpls3100_3100_13100
Match criteria : 3100
Action type : Translate
Action value : 4075
Outgoing tpid : dot1.q

Mesh Peers:
2.2.2.2 (Up)
```

Table 3-30 explains the show command output fields.

Table 3-30: show mpls vpls details output field

Field	Description
Virtual Private LAN Service Instance	Number of VPLS service instance.
ID	VPLS identification detail for service instance.
SIG-Protocol	Type of protocol in MPLS configuration.
Attachment-Circuit	Details of the attached circuit in interface.
Learning	State of the interface.
Group ID	Group identification detail for VLAN.
VPLS Type	Type of VPLS in MPLS protocol.
Configured MTU	Number of configured MTU in the VPLs.
Description	Details of VPLS.
Service-tpid	Service TP identifier configured for the VPLS PW.
Operating mode	Type of mode in the interface.
Svlan Id	Configures a specific virtual LAN (VLAN).
Svlan Tpid	Service vlan TP identifier for the VPLS PW.

Table 3-30: show mpls vpls details output field

Field	Description
Redundancy admin role	Creating a Backup Administrator Role.
Redundancy oper role	Operational Role of the VPLS instance.
Configured interfaces	Details of the configured interfaces.
Interface	Selects an interface to configure.
Oper-state	Displays the current status of the cross-connect segment – Up or Down.
Service-template	Used to configure advanced service-related option.
Match criteria	Identifies prefix characteristics (network, BGP path attribute, nexthop, and so on) for a specific sequence.
Mesh Peers	Configuring the VPLS mesh peers.
PW Status Local	Used to perform limited local configuration changes, monitor device status and utilization, and simple local troubleshooting.
Remote	PW status of Remote end.

The following is a sample output of the `show mpls vpls mesh` command displaying information about all the core VC connections for all VPLS instances.

```
#show mpls vpls mesh
VPLS-ID    Peer Addr        In-Intf    In-Label   Out-Intf   Out-Label Lkps/St
PW-INDEX SIG-Protocol Status  Ecmp-Group
1           192.168.0.80     eth0       16          eth0       640         1/Up
1          BGP Active   N/A
1           192.168.0.90     eth1       18          eth1       642         1/Up
2          BGP Active   N/A
2           192.168.0.80     eth0       19          eth0       641         1/Up
1          BGP Active   N/A
2           192.168.0.90     eth1       17          eth1       643         1/Up
2          BGP Active   N/A
#
```

Table 3-31 explains the show command output fields.

Table 3-31: show mpls vpls mesh output field

Field	Description
VPLS-ID	Identification details of the VPLS.
Peer Addr	IP address of the peer device.
In-Intf	Installed as a result of configuring an interface.
In-label	Displays the ingress (incoming interface) label for this segment.
Out-Label	Label received from downstream neighbor for route.

Table 3-31: show mpls vpls mesh output field

Field	Description
Network-Intf	Installed as a result of configuring an interface.
Lkps/St	Opcode and Status of the VPLS PW.
PW-INDEX	Psuedo wire index
SIG-Protocol	Signalling protocol
Status	Status of Psuedo wire
Ecmp-Group	Equal cost multi path group

The following is a sample output of the `show mpls vpls spoke` displaying the spoke VC connection to the VPLS instance.

```
#show mpls vpls spoke
VPLS-ID    Virtual Circuit In-Intf    In-Label   Out-Intf   Out-Label Lkps/St
1          t100             eth2       20         eth2       640        1/Up
#
```

Table 3-32 explains the show command output fields.

Table 3-32: show mpls vpls spoke output field

Field	Description
VPLS-ID	Identification details of the VPLS.
Virtual Circuit	Used in transportation of data over a packet switch computer network.
In-Intf	Installed as a result of configuring an interface.
In-label	Displays the ingress (incoming interface) label for this segment.
Out-Label	Label received from downstream neighbor for route.
Network-Intf	Installed as a result of configuring an interface.
Lkps/St	Opcode and Status of the VPLS PW.

The following is a sample output of show mpls vpls count displaying information about total, active and inactive vpls instances.

```
#show mpls vpls count
------------------------------
Total VPLS instances    : 2
Active VPLS instances   : 2
Inactive VPLS instances : 0
------------------------------
```

Table 3-33 explains the show command output fields.

Table 3-33: show mpls vpls count output field

Field	Description
Total VPLS instances	Number of total VPLS instance.
Active VPLS instances	Number of active VPLS instance.
Inactive VPLS instances	Number of inactive VPLS instance.

show mpls vpls mac-address

Use this command to display retrieved VPLS learning mac-addresses on MPLS enabled node.

Command Syntax

```
show mpls vpls mac-address (name NAME |) (interface IFNAME |) (peer A.B.C.D |)
  (count |)
```

Parameters

NAME	Specify the name of the vpls instance
count	Counts the number of MAC address learned
IFNAME	Specify the name of interface
A.B.C.D	Specify the peer address

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show mpls vpls mac-address
VPLS-ID     MAC address        Learned from    Peer address
1           08:00:27:85:28:8a   eth1             1.1.1.1
1           08:00:27:99:91:1d   eth3             -


#show mpls vpls mac-address count
Total no of MAC addresses learnt :2


#show mpls vpls mac-address name vpls1
MAC address        Learned from    Peer address
08:00:27:85:28:8a   eth1             1.1.1.1
08:00:27:99:91:1d   eth3             -



#show mpls vpls mac-address name vpls1 count
Total no of MAC addresses learnt :2


#show mpls vpls mac-address interface eth1
VPLS-ID     MAC address        Learned from    Peer address
1           08:00:27:85:28:8a   eth1             1.1.1.1


#show mpls vpls mac-address interface eth1 count
Total no of MAC addresses learnt :1
```

```
#show mpls vpls mac-address name vpls1 interface eth1
MAC address        Learned from    Peer address
08:00:27:85:28:8a   eth1             1.1.1.1


#show mpls vpls mac-address name vpls1 interface eth1 count
Total no of MAC addresses learnt :1


#show mpls vpls mac-address peer 1.1.1.1
VPLS-ID     MAC address        Learned from    Peer address
1           08:00:27:85:28:8a   eth1             1.1.1.1


#show mpls vpls mac-address peer 1.1.1.1 count
Total no of MAC addresses learnt :1


#show mpls vpls mac-address name vpls1 peer 1.1.1.1
MAC address        Learned from    Peer address
08:00:27:85:28:8a   eth1             1.1.1.1


#show mpls vpls mac-address name vpls1 peer 1.1.1.1 count
Total no of MAC addresses learnt :1


#show mpls vpls mac-address interface eth1 peer 1.1.1.1
VPLS-ID     MAC address        Learned from    Peer address
1           08:00:27:85:28:8a   eth1             1.1.1.1


# show mpls vpls mac-address interface eth1 peer 1.1.1.1 count
Total no of MAC addresses learnt :1


#show mpls vpls mac-address name vpls1 interface eth1 peer 1.1.1.1
MAC address        Learned from    Peer address
08:00:27:85:28:8a   eth1             1.1.1.1


#show mpls vpls mac-address name vpls1 interface eth1 peer 1.1.1.1 count
Total no of MAC addresses learnt :1
```

Table 3-34 explains the show command output fields.

Table 3-34: show mpls vpls mac-address output field

Field	Description
MAC address	Used to forward the packet into a given VPLS instance.
Learned from	MAC addresses learned from a specific interface.
Peer address	IP address of the peer device.

show mpls vpls statistics

Use this command to display MPLS traffic statistics for VPLS network or access or all ports.

Note: Multicast traffic statistics not supported by hardware.

Command Syntax

```
show mpls vpls NAME statistics
show mpls vpls NAME statistics ((network-port ((peer A.B.C.D)|(spoke-vc VC-NAME)|))
  | (access-port (IFNAME (ethernet|(vlan <1-4094>))|)))
```

Parameters

NAME	Name of the VPLS instance
a.b.c.d	Mesh peer address of VC instance
VC-NAME	Name of the spoke VC instance
IFNAME	Name of the access-port interface
<1-4094>	VLAN ID of access-port of type VLAN

Command Mode

Exec mode and privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mpls vpls v1 statistics
Virtual Private LAN Service Instance: v1, ID: 10

 Access port statistics:
 Interface: xe3/4 VLAN ID: 2
   RX:  Input packets  : 10
        Input bytes    : 640
   TX:  Output packets : 0
        Output bytes   : 0

 Network port statistics:
 Mesh Peer: 8.8.8.8 (Up)
   RX:  Input packets  : 0
        Input bytes    : 0
   TX:  Output packets : 10
        Output bytes   : 640
```

Table 3-34 explains the show command output fields.

Table 3-35: show mpls vpls statistics output field

Field	Description
Access port statistics	Traffic statistics on Access port of VC/VPLS.
Network port statistics	Traffic statistics on Provider port of VC/VPLS.
Interface	Type of interface in the network.
VLAN ID	Identification details of the VPLS.
Mesh Peer	Configuring the VPLS mesh peers.
RX	Number of received packets.
Input packets	Number of hello packets received from the neighbor.
Input bytes	Size of hello packets received from the neighbor.
TX	Number of packets transmitted.
Output packets	Number of hello packets sent to the neighbor.
Output bytes	Size of hello packets sent to the neighbor.

signaling ldp

Use this command to establish a pseudowire connection between Provider Edge (PE) routers. Use this command to use the Label Distribution Protocol (LDP) for signaling and to support VPLS auto-discovery between VPLS instances.Using this command triggers LDP to signal a pseudowire between the configured VPLS peers in the same VPLS instance. The `vpls-peer` command is used to identify the VPLS peers that are part of a VPLS instance

Note: Issuing this command puts the router into VPLS signaling (`config-vpls-sig`) mode.

Use the `no` parameter with this command to remove (tear down) pseudowires with other PE routers.

Command Syntax

```
signaling ldp
no signaling ldp
```

Parameters

None

Default

By default, signaling ldp is disabled

Command Mode

VPLS mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)# mpls vpls test 100
(config-vpls)#signaling ldp
(config-vpls-sig)#vpls-peer 97.97.97.97
(config-vpls-sig)#exit
```

signaling bgp

Use this command to establish a pseudowire connection between Provider Edge (PE) routers. Use this command to use the Border Gateway Protocol (BGP) for signaling and to support VPLS auto-discovery between VPLS instances.Using this command triggers BGP to auto-discover VPLS peers and signal pseudowire between the VPLS peers in the same VPLS instance.

Note: Issuing this command puts the router into VPLS signaling .

Use the `no` parameter with this command to remove (tear down) pseudowires with other PE routers.

Command Syntax

```
signaling bgp
no signaling bgp
```

Parameters

None

Default

By default, signaling bgp is disabled

Command Mode

VPLS mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)# mpls vpls test 100
(config-vpls)#signaling bgp
(config-vpls-sig)#exit
```

static-mac

Use this command to add static MAC address to attachment circuit specific for a VPLS instance.

Use the `no` parameter with this command to remove static MAC address.

Note: It is not supported, if the user configures same mac address on different attachment circuits for same VPLS instance.

Command Syntax

```
static-mac XXXX.XXXX.XXXX
no static-mac XXXX.XXXX.XXXX
```

Parameter

`XXXX.XXXX.XXXX` MAC address in HHHH.HHHH.HHHH format.

Default

By default, mac is disabled

Command Mode

Interface VPLS

Applicability

This command was introduced before OcNOS-SP version 4.2.

Examples

```
(config)#interface ce11/2
(config-if)#mpls-vpls vpls2 service-template vc1
(config-if-vpls)#static-mac 0000.0400.0602
```

ve-id

Use this command to configure a VPLS Edge (VE) device. Each Provider Edge (PE) device participating in a VPLS must have at least one VE ID. When the PE is connected to several u-PEs (Layer 2 PE devices used to provide Layer 2 aggregation), there are unique VE ID's for each u-PE. The PE may also be assigned a VE ID, if it is to act as the VE for the VPLS.

Use the `no` parameter with this command to remove a VE ID.

Command Syntax

```
ve-id <1-64>
no ve-id <1-64>
```

Parameters

`<1-64>`	VE-ID's range is between 1 and 64. This should be unique among the VPLS Peers for a VPLS instance.

Default

By default, ve id is disabled

Command Mode

VPLS Signaling mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mpls vpls test 100
(config-vpls)#signaling bgp
(config-vpls-sig)#ve-id 2
(config-vpls-sig)#exit
```

vpls-ac-group

Use this command to assign an Attachment Circuit (AC) group to VPLS.

Use the `no` parameter with this command to remove an AC group.

Command Syntax

```
vpls-ac-group GROUPNAME
no vpls-ac-group
```

Parameter

`GROUPNAME`	Enter a name for the AC group

Default

By default, vpls ac group is disabled

Command Mode

VPLS mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mpls vpls test 12
(config-vpls)#vpls-ac-group new-ac
(config-vpls)#no vpls-ac-group
```

vpls-description

Use this command to add a description line for a VPLS instance.

Use the `no` parameter with this command to remove a VPLS description.

Command Syntax

```
vpls-description LINE
no vpls-description (LINE|)
```

Parameter

`LINE`	Enter a text string for the VPLS instance

Default

By default, vpls description is disabled

Command Mode

VPLS mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#mpls vpls test 34
(config-vpls)#vpls-description This is for testing
(config-vpls)#exit
```

vpls fib-entry

Use this command to create a static VPLS FIB entry. When a VPLS peer is configured manually, no signaling is done. Therefore, a VPLS static entry must be created for all manually created nodes.

Use the `no` option with this command to delete a static VPLS FIB entry.

Command Syntax

```
vpls fib-entry VPLS-ID (peer A.B.C.D| spoke-vc VC-NAME) IN-LABEL OUT-INTF OUT-LABEL
no vpls fib-entry VPLS-ID ((peer A.B.C.D)| (spoke-vc VC-NAME))
no vpls fib-entry VPLS-ID ((peer A.B.C.D)| (spoke-vc VC-NAME)) IN-LABEL OUT-INTF
  OUT-LABEL
```

Parameters

`VPLS-ID`	VPLS identifier
`peer`	Mesh peer address VPLS identifier
`A.B.C.D`	Peer IPv4 Address.
`spook-vc`	Spoke VC
`VC-NAME`	Virtual Circuit name
`IN-LABEL`	Incoming label value in the range of <16-15999>
`OUT-INTF`	Provider-facing interface
`OUT-LABEL`	Outgoing label value in the range of <16-15999>

Default

By default, vpls fib entry is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The first example shows how to configure VPLS FIB entry 100 with mesh peer 97.97.97.97 for incoming label 15999, outgoing interface eth2 with outgoing label 15999:

```
#configure terminal
(config)#vpls fib-entry 100 peer 97.97.97.97 15999 eth2 15999
```

The second example shows how to configure VPLS FIB entry 100 with spoke-vc t1 for incoming label 15999, outgoing interface eth2 with outgoing label 15999:

```
#configure terminal
(config)#vpls fib-entry 100 spoke-vc t1 15999 eth2 15999
```

vpls-mtu

Use this command to set the Maximum Transmission Unit (MTU) size for a given VPLS instance. This size is signaled to peer VPLS routers.

Use the `no` parameter with this command to remove the MTU size setting.

Command Syntax

```
vpls-mtu <576-65535>
no vpls-mtu (<576-65535>|)
```

Parameter

`<576-65535>`	Range of MTU size allowed for a VPLS instance

Default

By default, vpls mtu is 1500

Command Mode

VPLS mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#mpls vpls test 34
(config-vpls)#vpls-mtu 6506
(config-vpls)#exit
```

vpls-peer

Use this command to add a peer to a VPLS domain. This command triggers Label Distribution Protocol (LDP) signaling by default.

Use the `no` parameter to delete a VPLS virtual circuit for a specific peer.

Command Syntax

```
vpls-peer A.B.C.D ((agi NAME saii NAME taii NAME)|)   ((tunnel-id <1-65535>
  (forward|reverse|))|)
no vpls-peer A.B.C.D
```

Parameters

`A.B.C.D`	The address of a VPLS peer node to which a mesh virtual circuit is to be created
`tunnel-id`	The tunnel-identifier
`<1-65535>`	Tunnel ID within this range
`forward`	Tunnel direction - forward tunnel identifier (default setting)
`reverse`	Tunnel direction - reverse tunnel identifier
`A.B.C.D`	IPv4 Address for end-point for FEC129 MPLS Layer-2 Virtual Circuit
`agi`	Specify the value used for the AGI in FEC129 MPLS Layer-2 Virtual Circuit
`NAME`	AGI value for FEC129 MPLS Layer-2 Virtual Circuit
`saii`	Specify the value used for the SAII in FEC129 MPLS Layer-2 Virtual Circuit
`NAME`	SAII value for FEC129 MPLS Layer-2 Virtual Circuit
`taii`	Specify the value used for the TAII in FEC129 MPLS Layer-2 Virtual Circuit
`NAME`	TAII value for FEC129 MPLS Layer-2 Virtual Circuit

Default

By default, vpls peer is disabled

Command Mode

VPLS Signaling mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mpls vpls test 100
(config-vpls)#signaling ldp
(config-vpls-sig)#vpls-peer 97.97.97.97
(config-vpls-sig)#vpls-peer 97.97.97.97 tunnel-id 24
(config-vpls)#exit
(config)#exit
```

vpls-peer manual

Use this command to statically configure a VPLS peer. Because this command is not used in signaling mode, no signaling is used to set up the virtual circuit. At least one such peer configuration is required for every VPLS instance.

Use the `no` parameter with this command to remove a statically configured VPLS peer.

Command Syntax

```
vpls-peer A.B.C.D ((tunnel-id <1-65535> (forward|reverse|))|) manual
no vpls-peer A.B.C.D
```

Parameters

`A.B.C.D`	The address of a VPLS peer node to which a mesh virtual circuit is to be created
`tunnel-id`	The tunnel-identifier
`<1-65535>`	Tunnel ID within this range
`forward`	Tunnel direction - forward tunnel identifier (default setting)
`reverse`	Tunnel direction - reverse tunnel identifier

Default

By default, vpls peer A.B.C.D manual is disabled

Command Mode

VPLS mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mpls vpls test 100
(config-vpls)#vpls-peer 97.97.97.97 manual
(config-vpls)#vpls-peer 97.97.97.97 tunnel-id 24 manual
(config-vpls)#exit
(config)#exit
```

vpls-type

Use this command to assign a type (either Ethernet or VLAN) for VPLS.

Note: The default type is chosen as Ethernet.

Command Syntax

```
vpls-type (ethernet|vlan)
```

Parameter

`ethernet`	Designate Ethernet as the VPLS type
`vlan`	Designate VLAN as the VPLS type

Default

By default, vpls type is ethernet

Command Mode

signaling ldp mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mpls vpls test 100
(config-vpls)#signaling ldp
(config-vpls-sig)#vpls-type vlan
(config-vpls-sig)#vpls-peer 2.2.2.2
(config-vpls-sig)#exit
(config-vpls)#exit
```

vpls-vc

Use this command add a spoke virtual circuit to VPLS domain.

Use the `no` parameter to remove this configuration.

Command Syntax

```
vpls-vc NAME (ethernet|vlan|)
vpls-vc NAME (secondary NAME|) (ethernet|vlan|)
no vpls-vc NAME
```

Parameter

`NAME`	Enter a string that identifies the MPLS VC to add to the VPLS domain
`secondary`	Set the secondary spoke name
`NAME`	Enter a string that identifies the secondary spoke
`ethernet`	Identify the spoke type as Ethernet (default)
`vlan`	Identify the spoke type as VLAN.
`TNLNAME`	Specify the MPLS-TP tunnel-name.

Default

By default, vpls vc name is disabled

Command Mode

VPLS mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#mpls vpls test 34
(config-vpls)#vpls-vc VC1
(config-vpls)#exit
(config)#exit
```

Label Distribution Protocol Command Reference

CHAPTER 1 LDP Commands

This chapter is a reference for the LDP commands:

- ldp label-retention-mode
- ldp multicast-hellos
- ldp-optimization
- loop-detection
- loop-detection-hop-count
- loop-detection-path-vec-count
- mpls ldp-igp sync isis
- mpls ldp-igp sync ospf
- mpls ldp-igp sync-delay
- neighbor
- propagate-release
- pw-status-tlv
- request-labels-for
- request-retry
- request-retry-timeout
- restart ldp graceful
- router ldp
- router-id
- session-group
- snmp restart ldp
- targeted-peer ipv4
- targeted-peer-hello-interval
- targeted-peer-hold-time
- transport-address ipv4

advertise-labels

Use this command to prevent the distribution of any locally assigned labels.

Use the `no` parameter to enable the distribution of all locally assigned labels to all LDP neighbors.

Command Syntax

```
advertise-labels for any to none
 advertise-labels for PREFIX to (PEER|any)
no advertise-labels for any to none
no advertise-labels for PREFIX to (PEER|any)
```

Parameters

`for`	Specify the permitted destinations
`any`	Specify to permit any locally assigned labels
`PREFIX`	Specify the destinations which have labels are advertised
`to`	Specify the given neighbor
`PEER`	Specify the LDP neighbors which receive these advertisements
`none`	Specify that there are no LDP neighbors

Default

The labels of all destinations are advertised to all LDP neighbors.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ldp
(config-router)#advertise-labels for any to none

#configure terminal
(config)#router ldp
(config-router)#advertise-labels for PREFIX to any

#configure terminal
(config)#router ldp
(config-router)#advertise-labels for PREFIX to PEER
```

advertise-label-for-default-route

Use this command to enable label advertisement for default route.

Use no form to disable the label advertisement for default route.

Command Syntax

```
advertise-label-for-default-route
```

Parameters

None

Default

Disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS-OTN version 4.2.

Examples

```
#configure terminal
(config)#router ldp
(config-router)#advertise-label-for-default-route
```

advertisement-mode

Use this command to set the label advertisement mode for all the interfaces for the current LSR. Specifying `downstream-on-demand` and `downstream-unsolicited` mode affects which LSR initiates mapping requests and mapping advertisements.

This command is a global command used to set the label advertisement mode for all interfaces for the current LSR. The advertisement mode set for a specific interface overrides the value set by this command (see ldp advertisement-mode). Use this command before starting the interface as it closes and restarts all sessions.

Use the `no` parameter to revert to the default advertisement mode value.

Command Syntax

```
advertisement-mode (downstream-on-demand|downstream-unsolicited)
no advertisement-mode (downstream-on-demand|downstream-unsolicited)
```

Parameters

`downstream-on-demand`

Sends label upon request. When a users uses this mode, a router distributes a label to a peer only if there is a pending label request from a peer. The reaction of the downstream router to this request depends on the label advertising mode supported on the next hop. This mode is typically used with the conservative label retention mode.

`downstream-unsolicited`

Sends label without waiting request. This mode distributes labels to peers without waiting for a label request, and is typically used with the liberal label retention mode.

Default

By default, advertisement mode is downstream-unsolicited

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

In the following example, the LSR will use the downstream-unsolicited advertisement mode for an LDP session on its interfaces.

```
#configure terminal
(config)#router ldp
(config-router)#advertisement-mode downstream-unsolicited
```

clear ldp adjacency

Use this command to clear an adjacency with a specified peer, or to clear all adjacencies for the current LSR.

Command Syntax

```
clear ldp adjacency (A.B.C.D|*)
```

Parameters

`*`	Specify to clear all adjacencies.
`A.B.C.D`	Specify to clear IPv4 address of the peer.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ldp adjacency 123.123.123.33
```

clear ldp session

Use this command to clear a session established with a specified peer, or to clear all sessions for the current LSR.

Command Syntax

```
clear ldp session (A.B.C.D|*)
```

Parameters

`*`	Specify to clear all sessions.
`A.B.C.D`	Specify to clear IPv4 address of the peer.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ldp session 123.123.123.33
```

clear ldp statistics

Use this command to clear LDP statistics. This command clears the count per each operation filtered by an advertisement list.

Command Syntax

```
clear ldp statistics
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ldp statistics
```

clear ldp statistics advertise-labels

Use this command to clear LDP advertise-labels statistics. This command clears the count per each operation filtered by an advertisement list.

Command Syntax

```
clear ldp statistics advertise-labels
clear ldp statistics advertise-labels for PREFIX
clear ldp statistics advertise-labels for PREFIX to PEER
```

Parameters

`advertise-labels`	Specify the IP prefix list of advertise-labels.
`for`	Specify the permitted destinations.
`PREFIX`	Specify the destinations that have their labels advertised.
`to`	Specify the given neighbor.
`PEER`	Specify the LDP neighbors that receive these advertisements.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ldp statistics advertise-labels
```

control-mode

Use this command to set the control mode for label processing. Ordered processing sets the mode to strict chain-of-command; an LSR replies to a request packet from an LSR higher in the chain only after it receives a label from an LSR lower in the chain. Independent processing sets the mode to instant replies.

In independent control mode, each LSR might advertise label mappings to its neighbors at any time. In independent downstream-on-demand mode, an LSR might answer requests for label mappings immediately, without waiting for a label mapping from the next hop. In independent downstream unsolicited mode, an LSR might advertise a label mapping for an Forwarding Equivalence Class (FEC) to its neighbors whenever it is prepared to label-switch that FEC. In independent mode, an upstream label can be advertised before a downstream label is received.

In ordered control mode, an LSR may initiate the transmission of label mapping only for an FEC for which it has a label mapping for the FEC next hop, or for which the LSR is the egress. For each FEC for which the LSR is not the egress and no mapping exists, the LSR must wait until a label from a downstream LSR is received. An LSR may be an egress for some FECs and a non-egress for others. Changes in control mode only affect labels that were sent or received after the change was made.

Use the `no` parameter to revert to default control mode.

Note: Control mode "independent" is supported with advertisement mode "DU" only.
When the advertisement mode is set as "DU", control mode automatically sets to "independent".
Control mode "independent" is not supported with advertisement mode "DOD".
Control mode "ordered" is supported with advertisement mode "DOD" only.
Control mode "ordered" is not supported with advertisement mode "DU".
When the advertisement mode is set as "DOD", control mode automatically sets to "ordered".

Command Syntax

```
control-mode (ordered|independent)
no control-mode
```

Parameters

`independent`	Sets control mode to independent processing.
`ordered`	Sets control mode to ordered processing.

Command Mode

Router mode

Default

By default, control mode is independent

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ldp
(config-router)#control-mode ordered
```

debug ldp advertise-labels

Use this command to enable the debugging of LDP advertise-label events.

On using the debug command, the router continues to generate an output until the `no` parameter is used with this command. The debug output and system error messages are written on the virtual terminal. Use `log syslog` command in `configure` mode to redirect the debugging output to a file or the syslog.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ldp advertise-labels
no debug ldp advertise-labels
```

Parameters

None

Command Mode

Configure mode, Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#log syslog
(config)#debug ldp advertise-labels
```

debug ldp all

Use this command to enable the debugging of all LDP events.

On using the debug command, the router continues to generate an output until the `no` parameter is used with this command. The debug output and system error messages are written on the virtual terminal. Use the l`og syslog` command in `configure` mode to redirect the debugging output to a file or the syslog.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ldp all
no debug ldp all
no debug all
undebug all
```

Parameters

None

Command Mode

Configure mode, Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#log syslog
(config)#debug ldp all
```

debug ldp dsm

Use this command to enable the debugging of LDP DSM events.

On using the debug command, the router continues to generate an output until the `no` parameter is used with this command. The debug output and system error messages are written on the virtual terminal. Use the l`og syslog` command in `configure` mode to redirect the debugging output to a file or the syslog.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ldp dsm
```

```
no debug ldp dsm
```

Parameters

None

Command Mode

Configure mode, Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#log syslog
(config)#debug ldp dsm
```

debug ldp events

Use this command to enable the debugging of all LDP events.

On using the debug command, the router continues to generate an output until the `no` parameter is used with this command. The debug output and system error messages are written on the virtual terminal. Use the l`og syslog` command in `configure` mode to redirect the debugging output to a file or the syslog.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ldp events
```

```
no debug ldp events
```

Parameters

None

Command Mode

Configure mode, Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#log syslog
(config)#debug ldp advertise-labels
(config)#debug ldp all
(config)#debug ldp dsm
(config)#debug ldp events
```

debug ldp fsm

Use this command to enable the debugging of LDP FSM events.

On using the debug command, the router continues to generate an output until the `no` parameter is used with this command. The debug output and system error messages are written on the virtual terminal. Use the l`og syslog` command in `configure` mode to redirect the debugging output to a file or the syslog.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ldp fsm
```

```
no debug ldp fsm
```

Parameters

None

Command Mode

Configure mode, Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#log syslog
(config)#debug ldp fsm
```

debug ldp hexdump

Use this command to enable the debugging of LDP hexdump events.

On using the debug command, the router continues to generate an output until the `no` parameter is used with this command. The debug output and system error messages are written on the virtual terminal. Use the l`og syslog` command in `configure` mode to redirect the debugging output to a file or the syslog.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ldp hexdump
```

```
no debug ldp hexdump
```

Parameters

None

Command Mode

Configure mode, Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#log syslog
(config)#debug ldp hexdump
```

debug ldp inter-area

Use this command to enable the debugging of LDP inter-area events.

On using the debug command, the router continues to generate an output until the no parameter is used with this command. The debug output and system error messages are written on the virtual terminal. Use the log syslog command in configure mode to redirect the debugging output to a file or the syslog.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ldp inter-area
no debug ldp inter-area
```

Parameters

None

Command Mode

Configure mode, Privileged Exec mode

Applicability

This command was introduced before OcNOS-OTN version 4.2.

Example

```
#configure terminal
(config)#log syslog
(config)#debug ldp inter-area
```

debug ldp nsm

Use this command to enable the debugging of LDP NSM events.

On using the debug command, the router continues to generate an output until the `no` parameter is used with this command. The debug output and system error messages are written on the virtual terminal. Use the l`og syslog` command to redirect the debugging output to a file or the syslog.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ldp nsm
```

```
no debug ldp nsm
```

Parameters

None

Command Mode

Configure mode, Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#log syslog
(config)#debug ldp nsm
```

debug ldp packet

Use this command to enable the debugging of LDP packet events.

On using the debug command, the router continues to generate an output until the `no` parameter is used with this command. The debug output and system error messages are written on the virtual terminal. Use the l`og syslog` command in `configure` mode to redirect the debugging output to a file or the syslog.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ldp packet
debug ldp packet (notification|hello|initialization|keepalive|address|label)
no debug ldp packet
no debug ldp packet (notification|hello|initialization|keepalive|address|label)
```

Parameters

`notification`	Debug LDP notification packets.
`hello`	Debug LDP hello packets.
`initialization`	Debug LDP initialization packets.
`keepalive`	Debug LDP keepalive packets.
`address`	Debug LDP address (withdraw) packets.
`label`	Debug LDP address label packets.

Command Mode

Configure mode, Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#log syslog
(config)#debug ldp packet hello
```

debug ldp usm

Use this command to enable the debugging of LDP USM events.

On using the debug command, the router continues to generate an output until the `no` parameter is used with this command. The debug output and system error messages are written on the virtual terminal. Use the l`og syslog` command in `configure` mode to redirect the debugging output to a file or the syslog.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ldp usm
```

```
no debug ldp usm
```

Parameters

None

Command Mode

Configure mode, Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#log syslog
(config)#debug ldp usm
```

debug ldp vc usm

Use this command to enable the debugging of LDP VC events.

On using the debug command, the router continues to generate an output until the `no` parameter is used with this command. The debug output and system error messages are written on the virtual terminal. Use the l`og syslog` command in `configure` mode to redirect the debugging output to a file or the syslog.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
debug ldp vc dsm
debug ldp vc usm
no debug ldp vc dsm
no debug ldp vc usm
```

Parameters

`dsm`	Debug LDP downstream SM.
`usm`	Debug LDP upstream SM.

Command Mode

Configure mode, Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#log syslog
(config)#debug ldp vc dsm
(config)#debug ldp vc usm
```

disable-ldp

Use this command to disable LDP IPv4 on a specified interface.

This command disables the transmission of Hello packets through the current interface, and clears all created sessions and adjacencies for this interface. Use `disable-ldp` alone to disable only LDP IPv4 on the interface.

Command Syntax

```
disable-ldp (ipv4|)
```

Parameters

`ipv4`	Disables IPv4 on the interface.

Default

By default, disable ldp is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example disables LDP IPv4 on interface eth0.

```
#configure terminal
(config)#interface eth0
(config-if)#disable-ldp
```

The following example disables LDP IPv4 on interface eth0.

```
#configure terminal
(config)#interface eth0
(config-if)#disable-ldp ipv4
```

enable-ldp

Use this command to enable LDP IPv4 on a specified interface. This command enables the transmission of Hello packets through the current interface, so that LDP adjacencies and LDP sessions can be created.

Note: The corresponding interface must be enabled for label-switching using the label-switching command.

Command Syntax

```
enable-ldp ipv4
```

Parameters

None

Default

By default, enable ldp is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example enables LDP IPv4 on interface eth0.

```
#configure terminal
(config)#interface eth0
(config-if)#enable-ldp ipv4
```

explicit-null

Use this command to configure the router to send explicit-null labels for directly connected FECs instead of implicit-null labels. Implicit-nulls are the default labels.

This command controls the label value advertised on the egress router of an LSP. By default, implicit null label (label 3) is advertised for directly connected FECs. LDP advertises an Implicit Null label that causes the previous hop router to perform penultimate hop popping. Use the `explicit null` command to avoid the penultimate router from penultimate hop popping, and to force it to replace the incoming label with the explicit null label.

Note: Do not use this command if the LDP is concurrently used for MPLS/BGP VPNs.

Use the `no` parameter to stop sending explicit-null labels for directly connected FECs and resume sending implicit-null labels for them.

Command Syntax

```
explicit-null
no explicit-null
```

Parameters

None

Default

By default, sends implicit-null labels.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ldp
(config-router)#explicit-null
```

global-merge-capability

Use this command to override the default merge capability setting of all the interfaces for the current LSR.

The merge capability aggregates multiple incoming flows with the same destination address into a single outgoing flow. This reduces the label-space shortage by sharing labels for different flows with the same destination, or the same FEC (Forwarding Equivalence Class).

Use the `no` parameter to revert to the default merge capability settings of all the interfaces for this LSR.

Command Syntax

```
global-merge-capability (merge-capable|non-merge-capable)
no global-merge-capability
```

Parameters

`merge-capable` Maps all incoming labels that are destined for the same FEC to the same outgoing label (this is the Ethernet default.)

`non-merge-capable`

Maps all incoming labels, regardless of destination FEC to unique outgoing labels (this is the non-Ethernet default.)

Default

By default, global merge capability is merge capable.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ldp
(config-router)#global-merge-capability merge-capable
```

graceful-restart

Use this command to enable the Graceful-Restart capability for LDP.

Use the `no` parameter to disable the GR capability for LDP.

Command Syntax

```
graceful-restart full
graceful-restart helper-only
graceful-restart timers max-recovery <15-600>
graceful-restart timers neighbor-liveness <5-300>
no graceful-restart
no graceful-restart timers max-recovery
no graceful-restart timers neighbor-liveness
```

Parameters

`full`	Configuring with full enable the complete GR capability
`helper-only`	Configuring with helper-only enables only helper mode
`timers`	Used to configure the non-default recovery and reconnect timer values.
`max-recovery`	Maximum recovery time
`<15-600>`	Interval until which LDP preserves route after peer restart
`neighbor-liveness`	Neighbor Liveness Time
`<5-300>`	Set the hold timer for a targeted LDP peer

Default

GR capability is not enbabled.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS-SP version 5.0.

Examples

```
OcNOS#configure terminal
OcNOS(config)#router ldp
OcNOS(config-router)#graceful-restart full
OcNOS(config-router)#graceful-restart helper-only
OcNOS(config-router)#graceful-restart timers max-recovery 100
OcNOS(config-router)#graceful-restart timers neighbor-liveness 200
```

hello-interval

Use this command to set the interval after which `hello` packets are sent out.

LDP defines a mechanism for discovering adjacent Label Switching Routers (LSRs) that participate in label switching (adjacencies). Hello messages are sent to the All Routers Multicast Group (224.0.0.2). Whenever a new router comes up, it sends out a hello packet to a specified, multicast address announcing itself to the network. Every router directly connected to the network receives the packet. Receipt of a hello packet from another LSR creates a `hello adjacency` with that LSR. Use this command to specify the interval after which the hello packets will be sent.

Used as a global command, the hello-interval value may be overridden by the hello-interval set on the interface (see ldp hello-interval). For optimum performance, set this value to no more than one-third the value of the hold-time specified.

Use the `no` parameter to revert to default hello interval.

Command Syntax

```
hello-interval <1-21845>
no hello-interval
```

Parameters

`<1-21845>`	Specify the interval in seconds. The default is 5 seconds.

Default

By default, hello interval is 5 seconds

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This example shows how to set the hello-interval value for all interfaces of an LSR.

```
#configure terminal
(config)#router ldp
(config-router)#hello-interval 35

(config-router)#no hello-interval
```

hold-time

Use this command to set the global value for the hold-time after which the LSR rejects adjacencies.

An LSR maintains a record of `hellos` received from peers. `Hold-time` specifies the time an LSR maintains its record of hellos from a peer on not receiving another hello from that peer. A pair of LSRs negotiates the hold-time they use for hellos from each other. Each proposes a hold time value, and the LSR uses the lower of the two hold-time values. The hold-time value set on the interface overrides the hold-time value set by this command (see ldp hold-time). For optimum performance, set this value to no less than three times the value of the hello-interval specified.

Use the `no` parameter to revert to the default hold time.

Command Syntax

```
hold-time <3-65535>
no hold-time
```

Parameters

`<3-65535>`	Specify the hold-time value in seconds.

Default

By default, hold time is 15 seconds

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows how to set the hold-time value for all interfaces of an LSR.

```
#configure terminal
(config)#router ldp
(config-router)#hold-time 635

(config-router)#no hold-time
```

import-bgp-routes

Use this command to import BGP routes into LDP. BGP routes are not imported into LDP by default.

Use the `no` parameter to flush out all BGP routes currently being used by LDP, and to reject any further BGP specific routing updates from OcNOS.

Command Syntax

```
import-bgp-routes
no import-bgp-routes
```

Parameters

None

Default

By default, import bgp route is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ldp
(config-router)#import-bgp-routes
```

inter-area-lsp

Use this command to enable creation of inter-area LSPs.

Use the `no` form of the command to disable this configuration.

Command Syntax

```
inter-area-lsp (PREFIX_ACL|)(config-only|)
no inter-area-lsp
```

Parameters

`PREFIX_ACL`	Access-list name for Prefix Based inter-area lsp
`config-only`	Optional. When this option is used, existing LDP sessions are not torn down.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS-OTN version 4.2.

Example

```
#configure terminal
(config)#router ldp
(config-router)#inter-area-lsp

#configure terminal
(config)#router ldp
(config-router)#inter-area-lsp config-only

#configure terminal
(config)#router ldp
(config-router)#inter-area-lsp acl1

#configure terminal
(config)#router ldp
(config-router)#inter-area-lsp acl1 config-only
```

keepalive-interval

Use this command to set the global value for the interval after which keep-alive packets are sent out.

Each LSR must send keep-alive messages at regular intervals to its LDP peers to keep the sessions active. The keep-alive interval determines the time interval between successive keep-alive messages. Use this command to set this interval. This value is overridden by the keep-alive interval set on the interface. For optimum performance, set this value to no more than one-third the value of the specified keep-alive time-out value.

Use the `no` parameter to revert to default keep-alive interval.

Command Syntax

```
keepalive-interval <1-21845>
no keepalive-interval
```

Parameters

`<1-21845>`	Specify the value of interval in seconds.

Default

By default, keepalive interval is 10 seconds

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows how to set the keep-alive timer for all interfaces of an LSR.

```
#configure terminal
(config)#router ldp
(config-router)#keepalive-interval 635

(config-router)#no keepalive-interval
```

keepalive-timeout

Use this command to set the global value for the time-out after which sessions are rejected.

Use this command to set the time period for which an LSR must wait for successive keep-alive messages from LDP peers. The keep-alive time-out value is overridden by the keep-alive time-out set on the interface (see ldp keepalive-timeout). For optimum performance, set this value to no less than three times the value of the specified keep-alive interval value.

Use the `no` parameter to revert to default keep-alive time-out.

Command Syntax

```
keepalive-timeout <3-65535>
no keepalive-timeout
```

Parameters

`<3-65535>`	Specify the time-out value in seconds.

Default

By default, keepalive timeout is 30 seconds.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows how to set the keep-alive time-out value for all interfaces of an LSR.

```
#configure terminal
(config)#router ldp
(config-router)#keepalive-timeout 635

(config-router)#no keepalive-timeout
```

label-retention-mode

Use this command to set the retention mode to be used for all labels exchanged.

When an LSR receives a label binding for a particular FEC (Forwarding Equivalence Class) from another LSR that is not its next hop for that FEC, it might keep track of such bindings or discard them. Use the `liberal` parameter to retain all labels binding to FEC received from label distribution peers, even if the LSR is not the current next-hop. Use the `conservative` parameter to maintain only the label bindings for valid next-hops in a LSP. Liberal label retention mode allows for quicker adaptation to routing changes, whereas conservative label retention mode requires an LSR to maintain fewer labels.

Note: label-retention-mode "liberal" is supported with advertisement mode "DU" only.
label-retention-mode "liberal" is not supported with advertisement mode "DOD".
When the advertisement mode is set as "DU", label-retention-mode automatically sets to "liberal".
label-retention-mode "conservative" is supported with advertisement mode "DOD" only.
label-retention-mode "conservative" is not supported with advertisement mode "DU".
When the advertisement mode is set as "DOD", label-retention-mode automatically sets to "conservative".

Use the `no` parameter to revert to default retention mode.

Command Syntax

```
label-retention-mode (conservative|liberal)
no label-retention-mode (conservative|liberal)
```

Parameters

`conservative`	Specify to delete all unused labels and FECs.
`liberal`	Specify to retain all labels, regardless of use.

Default

By default, label retention mode is liberal

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows how to set the retention mode for all interfaces of an LSR.

```
#configure terminal
(config)#router ldp
(config-router)#label-retention-mode liberal
```

ldp advertisement-mode

Use this command to set the label advertisement mode for an interface for the current LSR to either downstream-on-demand (label is sent only when requested) or downstream-unsolicited (label is sent unrequested). Specifying downstream-on-demand and downstream-unsolicited mode affects which LSR initiates mapping requests and mapping advertisements.

This is an interface-specific command; it overrides the advertisement mode set for an LSR using the advertisement-mode command (see advertisement-mode). Use this command after the advertisement-mode command sets all the interface advertisement modes. In addition, users should use this command before starting the interface, since all affected sessions will be closed and restarted.

Use the `no` parameter to revert to the advertisement mode value set for the main LDP process.

Command Syntax

```
ldp advertisement-mode (downstream-on-demand|downstream-unsolicited)
no ldp advertisement-mode (downstream-on-demand|downstream-unsolicited)
```

Parameters

`downstream-on-demand`

Indicates that the sent label was requested. When a user uses this parameter, a router distributes a label to a peer only if there is a pending label request from a peer. The reaction of the downstream router to this request depends on the label advertising mode supported on the next hop. The downstream-on-demand mode is typically used with the conservative label retention mode.

`downstream-unsolicited`

Indicates that the label was sent unrequested. This parameter distributes labels to peers without waiting for a label request. This mode is typically used with the liberal label retention mode.

Default

By default, ldp advertisement mode is downstream unsolicited mode

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ldp advertisement-mode downstream-on-demand
```

ldp hello-interval

Use this command to set the interval for sending multicast Hello packets via an interface.

LDP defines a mechanism for discovering adjacent Label Switching Routers (LSR) that participate in label switching (adjacencies). Whenever a new router comes up, it sends out a hello packet to a specified, multicast address announcing itself to the network. Every router directly connected to the network receives the packet. Receipt of a hello packet from another LSR creates a hello adjacency with that LSR. Use this command to specify the interval after which the hello packets will be sent.

For optimum performance, set the hello-interval value to no more than one-third the hold-time value.

Note: This command is an interface-specific command and overrides the value set for an LSR using the global hello-interval command.

Use the `no` parameter with this command to revert to the hello-interval value set for the main LDP process.

Command Syntax

```
ldp hello-interval <1-21845>
no ldp hello-interval
```

Parameters

`<1-21845>`	Specify the interval in seconds.

Default

By default, ldp hello interval is 5 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This example shows how to set the hello-interval for a specific interface.

```
#configure terminal
(config)#interface eth0
(config-if)#ldp hello-interval 635

(config-if)#no ldp hello-interval
```

ldp hold-time

Use this command to set the hold-time value after which the LSR rejects adjacencies.

The hold-time timer is reset every time a hello packet is received from the peer in question. For optimum performance, set this value to no less than three times the hello-interval value.

Note: This command is an interface-specific command, and overrides the value set for an LSR using the global hold-time command.

Use the `no` parameter to revert to the hold-time value set for the main LDP process.

Command Syntax

```
ldp hold-time <3-65535>
no ldp hold-time
```

Parameters

`<3-65535>`	Specify the hold-time value in seconds.

Default

By default, ldp hold time is 15 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows how to set the hold-time for a specific interface:

```
#configure terminal
(config)#interface eth0
(config-if)#ldp hold-time 635

(config-if)#no ldp hold-time
```

ldp keepalive-interval

Use this command to set the interval for sending keep-alive messages to the peer in order to maintain a session.

Each LSR must send keep-alive messages at regular intervals to its LDP peers to keep the sessions active. The keep-alive interval determines the time-interval between successive keep-alive messages. This command sets this interval.

Note: This command is an interface-specific command, and overrides the value set for an LSR using the global `keepalive-interval` command.

Use the `no` parameter to revert to the keep-alive interval set for the main LDP process.

Command Syntax

```
ldp keepalive-interval <1-21845>
no ldp keepalive-interval
```

Parameters

`<1-21845>`	Specify the interval in seconds.

Default

By default, ldp keepalive interval is 10 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This example shows how to set the hello-interval for a specific interface:

```
#configure terminal
(config)#interface eth0
(config-if)#ldp keepalive-interval 635

(config-if)#no ldp keepalive-interval
```

ldp keepalive-timeout

Use this command to set the keep-alive time-out value for rejecting a session with a peer.

Use this command to set the time period for which an LSR must wait for successive keep-alive messages from LDP peers. The keep-alive timer is reset every time a keep-alive packet is received from the peer in question. For optimum performance, set this value to no more than three times the keep-alive interval value.

Note: This command is an interface-specific command and overrides the value set for an LSR using the global `keepalive-timeout` command.

Use the `no` parameter to revert to the keep-alive time-out set for the main LDP process.

Command Syntax

```
ldp keepalive-timeout <3-65535>
no ldp keepalive-timeout
```

Parameters

`<3-65535>`	Specify the value in seconds.

Default

By default, ldp keepalive timeout is 30 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows how to set the keep-alive time-out timer for a specific interface:

```
#configure terminal
(config)#interface eth0
(config-if)#ldp keepalive-timeout 635

(config-if)#no ldp keepalive-timeout
```

ldp label-retention-mode

Use this command to set the retention mode to be used for all labels exchanged via the given interface.

When an LSR receives a label binding for a particular FEC (Forwarding Equivalence Class) from another LSR that is not its next hop for that FEC, it might keep track of such bindings or discard them. Use the `liberal` parameter to retain all labels binding to FEC received from label distribution peers, even if the LSR is not the current next-hop. Use the `conservative` parameter to maintain only the label bindings for valid next-hops in a LSP. Liberal label retention mode allows for quicker adaptation to routing changes, whereas conservative label retention mode requires an LSR to maintain fewer labels.

Note: The retention mode value set on the interface (see label-retention-mode) overrides the value set by this command. This command is an interface-specific command, and overrides the setting for an LSR using the global `label-retention-mode` command.

Use the `no` parameter to revert to the retention mode set for the main LDP process.

Command Syntax

```
ldp label-retention-mode (conservative|liberal)
no ldp label-retention-mode (conservative|liberal)
```

Parameters

`conservative`	Specify to delete all unused labels and FECs.
`liberal`	Specify to retain all labels, regardless of use.

Default

By default, ldp label retention mode is liberal

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows how to set the label retention mode for a specific interface:

```
#configure terminal
(config)#interface eth0
(config-if)#ldp label-retention-mode liberal
```

ldp multicast-hellos

Use this command to enable multicast hello exchange on a specified interface.

Use the `no` parameter to disable multicast hello exchange. R

Command Syntax

```
ldp multicast-hellos
no ldp multicast-hellos
```

Parameters

None

Default

By default, ldp multicast hello is enabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ldp multicast-hellos
```

ldp-optimization

This command helps optimize the resetting of an LDP session by enabling the following two scalability features for LDP:

- Resets the session keepalive timer on receipt of a hello message
- Resets the hold timer on receipt of any LDP control message

Use the `no` parameter to disable the two previously listed scalability features.

Command Syntax

```
ldp-optimization
no ldp-optimization
```

Parameters

None

Default

By default, ldp optimization is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ldp
(config-router)#ldp-optimization
```

loop-detection

Use this command to enable loop detection on the current LSR. This command detects looping LSPs, and prevent Label Request messages from looping because of non-merge capable LSRs. This loop detection mechanism is useful for networks of non time-to-live (non TTL) decrementing devices that can not allocate resources among traffic flows.

There are two methods supported for the loop detection mechanism: A Hop Count detection system, that is always enabled; and the Path Vector detection system, that can be toggled:

- Hop Count - During the setup of an LSP, the LSP passes a hop count with the LSP setup messages. This hop count is incremented by each node router participating in LSP establishment. If the hop count exceeds the maximum configured value, the LSP setup process is stopped, and a notification message is passed back to the message originator.
- Path Vector - A path vector contains a list of LSR identifiers. This is passed as a part of LSP setup messages. Each LSR participating in the LSP establishment adds its own LSR identifier to the path vector. If an LSR finds its own identifier in the path vector, it drops the message, and sends a message back to the originator.

The use of these messages ensures that a loop is detected while establishing a label switched path and before any data is passed over that LSP.

Use the `no` parameter to disable loop detection.

Command Syntax

```
loop-detection
no loop-detection
```

Parameters

None

Default

By default, loop detection is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ldp
(config-router)#loop-detection
```

loop-detection-hop-count

Use this command to set the loop detection hop count, which determines the maximum hop-count value.

This command sets the maximum hop count value, which specifies the permitted maximum permitted hop-count. An LSR that detects a maximum hop count behaves as if the containing message has traversed a loop. The use of this command ensures that a loop is detected while establishing a label switched path before any data is passed via LSP.

Use the `no` parameter to revert to the default loop detection count

Command Syntax

```
loop-detection-hop-count <1-255>
```

Parameters

`<1-255>`	Indicates the loop detection hop count.

Default

By default, loop detection hop is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ldp
(config-router)#loop-detection-hop-count 128
```

loop-detection-path-vec-count

Use this command to set the loop detection vec (vector) count, which determines the maximum supported path vectors.

This command sets the maximum supported path vectors for loop detection, which specifies the permitted path vector length. An LSR that detects a path vector has reached the maximum length behaves as if the containing message has traversed a loop. This command ensures that a loop is detected while establishing a label switched path before any data is passed over that LSP.

Use the `no` parameter to revert to the default loop detection count

Command Syntax

```
loop-detection-path-vec-count <1-255>
```

Parameters

`<1-255>`	Indicates the loop detection hop count.

Default

By default, loop detection path vec count is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ldp
(config-router)#loop-detection-path-vec-count 123
```

mpls ldp-igp sync isis

Use this command to enable LDP ISIS synchronization and to set the holddown timer for synchronization.

Use the `no` parameter to disable the LDP ISIS synchronization.

Note: Holddown timer value should be higher than LDP IGP sync timer.

Command Syntax

```
mpls ldp-igp sync isis (level-1|level-2|level-1-2) (holddown-timer <1-2147483>| )
```

Parameters

`level-1|level-2|level-1-2`
The ISIS level.

`holddown-timer` How long IGP should wait for LDP to converge in seconds.

Default

None

Command Mode

Interface configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
#int eth 1
#mpls ldp-igp sync isis level-1-2 holddown-timer 500
```

mpls ldp-igp sync ospf

Use this command to enable LDP-OSPF synchronization. This command also provides option to configure the hold-down timer for which OSPF will wait for LDP to converge and advertises Max cost. When the configured time expires, OSPF starts advertising the actual cost in the Router-LSA.

Note: Holddown timer value should be higher than LDP IGP sync timer.

Command Syntax

```
mpls ldp-igp sync ospf (holddown-timer <1-2147483>|)
```

Parameters

`holddown-timer`	Set holddown timer for the OSPF Sync
`<1-2147483>`	Hold down timer in seconds

Default

OSPF waits infinite when no hold-down timer is configured.

Command Mode

Interface configuration mode

Applicability

This command was introduced before OcNOS-OTN version 4.2.

Example

Enabling OSPF-LDP sync in interface eth3

```
#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#int eth3
(config-if)#mpls ldp-igp sync ospf
(config-if)#end
```

Enabling OSPF-LDP sync with holdown-timer enabled

```
#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#int eth3
(config-if)#mpls ldp-igp sync ospf holddown-timer 200
(config-if)#no mpls ldp-igp sync ospf
(config-if)#end
#
```

mpls ldp-igp sync-delay

Use this command to set the time delay for LDP-IGP synchronization.

Use the `no` parameter to disable the time delay.

Command Syntax

```
mpls ldp-igp sync-delay <5-60>
no mpls ldp-igp sync-delay
```

Parameters

`sync-delay`	Time delay for LDP to converge in seconds.
`<5-60>`	Time delay for notification of LDP convergence to IGP, in seconds

Default

If not configured the delay will be 0 seconds.

Command Mode

Interface configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config-if)# interface eth0
(config-if)# mpls ldp-igp sync-delay 15
(config-if)# no mpls ldp-igp sync-delay
```

multicast-hellos

Use this command to enable multicast hello exchange on all interfaces enabled for LDP. This is used for auto-discovery of LDP peers on directly connected networks. This option is enabled by default.

Use the `no` parameter with this command to disable multicast hello exchange.

Command Syntax

```
multicast-hellos
no multicast-hellos
```

Parameters

None

Default

By default, multicast hello is enabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ldp
(config-router)#multicast-hellos
```

neighbor

Use this command include or exclude password neighbors of LDP.

Use the `no` parameter with this command to unconfigure the LDP neighbor password.

Command Syntax

```
neighbor (A.B.C.D|all|auto-targeted) auth AUTH-TYPE password (plain-text|encrypt)
  WORD
neighbor (A.B.C.D) auth AUTH-TYPE password exclude
no neighbor A.B.C.D auth AUTH-TYPE password
```

Parameters

`(A.B.C.D |all|auto-targeted)`	Neighbor address or auto-targeted for auto targeted peers or all for other peers
`auth AUTH-TYPE`	Authentication Type md5
`password`	Set password to the neighbor
`(plain-text|encrypt)`	Password Type
`WORD`	Password

Default

By default, neighbor is disabled.

Command Mode

Router mode

Applicability

This command is introduced from OcNOS version 6.1.0.

Example

```
#configure terminal
(config)#router ldp
(config-router)#neighbor 1.1.1.1 auth md5 password plain-text myPass
(config-router)#no neighbor 1.1.1.1 auth md5 password
(config-router)#neighbor 2.2.2.2 auth md5 password exclude
(config-router)#no neighbor 2.2.2.2 auth md5 password
(config-router)#neighbor auto-targeted auth md5 password encrypt   myPass
(config-router)#no neighbor auto-targeted auth md5 password
```

propagate-release

Use this command to propagate the release of labels to downstream routers.

Use the `no` parameter to prevent the propagate-release of labels.

Command Syntax

```
propagate-release
no propagate-release
```

Parameters

None

Default

By default, propagate release is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ldp
(config-router)#propagate-release
```

pw-status-tlv

Use this command to enable the use of the PW Status TLV to signal the pseudowire status.

Use the `no` option with this command to disable the use of the PW Status TLV to signal the pseudowire status.

Command Syntax

```
pw-status-tlv
no pw-status-tlv
```

Parameters

None

Default

By default, pw status tlv is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ldp
(config-router)#pw-status-tlv
```

request-labels-for

Use this command to request labels for the prefixes in the given IP prefix list. LDP request labels for the prefixes only if the valid and exact route is present for that prefix.

Use the no form of this command to disable multicast hello exchange.

Command Syntax

```
request-labels-for prefix-list-ipv4 NAME
no request-labels-for prefix-list-ipv4
```

Parameters

NAME	IPv4 prefix list name

Command Mode

LDP router mode

Applicability

This command was introduced in OcNOS-OTN version 4.2.

Examples

```
#configure terminal
(config)#router ldp
(config-router)#request-labels-for prefix-list-ipv4 myPrefixList
```

request-retry

Use this command to enable the retry of requests once a request for a label has been rejected for a valid reason. This command enables the LSR to send a maximum of five label requests if a label request is rejected by an LDP peer.

Use the `no` parameter to disable the retry of requests.

Command Syntax

```
request-retry
no request-retry
```

Parameters

None

Default

By default, request retry is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ldp
(config-router)#request-retry
```

request-retry-timeout

Use this command to set the interval between retries. Before this time is over, a request is re-sent to a peer. This command changes the interval between request messages that are resent to a peer to account for routing changes.

Use the `no` parameter to revert to the default request-retry time-out set.

Command Syntax

```
request-retry-timeout <1-65535>
no request-retry-timeout
```

Parameter

`<1-65535>`	Specify the interval between retries in seconds.

Default

By default, timeout is 5 seconds.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ldp
(config-router)#request-retry-timeout 512

(config-router)#no request-retry-timeout
```

restart ldp graceful

Use this command to restart ldp gracefully.

Command Syntax

```
restart ldp graceful
```

Parameter

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS-SP version 5.0.

Example

```
OcNOS#restart ldp graceful
% Warning : You may loose ldp configuration, if not saved
 Proceed for graceful restart? (y/n):y
%% Managed module is down or crashed
```

router ldp

This command is used to enter the LDP specific command-line mode in which global attributes for the LDP process can be set. Without this command, the LSR does not perform any LDP operations, such as sending `hello` packets.

Use the `no` parameter with this command to disable this configuration.

Command Syntax

```
router ldp
no router ldp
```

Parameters

None

Default

By default, router ldp is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example shows the change in the prompt after using this `router ldp` command to enter router mode.

```
#configure router
(config)#router ldp
(config-router)#
```

router-id

Use this command to set the router-id to the supplied IP address; the router uses this address to generate the LDP-ID.

OcNOS has three methods to choose the router-id of LDP. The first priority router-id is the configured router-id in router mode (local configured router-id). The second priority router-id is the configured router-id in configure mode (global configured router-id). The lowest priority router-id is chosen by OcNOS among interfaces (global computed router-id).

Use the `no` parameter with this command to revert to using the first IP address configured on the box as the router-id for LDP-ID generation purposes.

Command Syntax

```
router-id A.B.C.D
no router-id A.B.C.D
no router-id
```

Parameter

`A.B.C.D`	Indicates the LDP router ID value.

Default

By default, router id is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure router
(config)#router ldp
(config-router)#router-id 123.123.123.8
```

session-group

Use this command to configure password to a neighbor session-group of LDP.

Use the no parameter with this command to unconfigure password to the LDP neighbor session-group.

Command Syntax

```
Session-group name NAME
neighbor prefix-list PREFIX-LIST-NAME
auth AUTH-TYPE password (plain-text|encrypt) WORD
no session-group name NAME
```

Parameters

NAME	Session group name
PREFIX-LIST-NAME	Prefix-list name with addresses associated to the group.
auth AUTH-TYPE	Authentication Type md5.
password	Set password to the neighbor.
(plain-text|encrypt)	Password Type.
WORD	Password.

Default

By default, snmp restart ldp is disabled

Command Mode

Router mode.

Applicability

This command is introduced from OcNOS version 6.1.0.

Examples

```
#configure terminal
(config)#router ldp
(config-router)#session-group name grp1
(config-router-sg)#neighbor prefix-list ldp1
(config-router-sg)auth md5 password plain-text test-grp1-6
(config-router)#no session-group name grp1
```

snmp restart ldp

Use this command to restart SNMP in Label Distribution Protocol (LDP)

Command Syntax

```
snmp restart ldp
```

Parameters

None

Default

By default, snmp restart ldp is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#snmp restart ldp
```

targeted-peer ipv4

Use this command to enter a targeted IPv4 LDP peer mode.

A targeted session is an LDP session between non-directly connected LSRs. Set this command to send a targeted hello messages to specific IP addresses. This command is specific to a targeted IPv4 LDP peer.

Command Syntax

```
targeted-peer ipv4 A.B.C.D
no targeted-peer ipv4 A.B.C.D
```

Parameter

A.B.C.D	Specify the IPv4 address of the targeted peer.

Default

By default, targeted peer IPv4 is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router ldp
(config-router)#targeted-peer ipv4 10.10.10.10
(config-router-targeted-peer)#
```

targeted-peer-hello-interval

Use this command to set the interval for sending unicast `hello` packets to targeted peers.

Use the `no` parameter with this command to revert to the default targeted-peer hello-interval value.

Command Syntax

```
targeted-peer-hello-interval <1-21845>
no targeted-peer-hello-interval
```

Parameter

`<1-21845>`	Specify the interval in seconds.

Default

By default, targeted peer hello interval is 15 seconds.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ldp
(config-router)#targeted-peer-hello-interval 1
```

targeted-peer-hold-time

Use this command to set the time-out value that is the time that the router waits before rejecting an adjacency with targeted peers.

Use the `no` parameter to revert to the default targeted-peer hold-time value.

Command Syntax

```
targeted-peer-hold-time <3-65535>
no targeted-peer-hold-time
```

Parameter

`<3-65535>`	Specify the interval in seconds.

Default

By default, hold time is 45 seconds.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router ldp
(config-router)#targeted-peer-hold-time 555

(config-router)#no targeted-peer-hold-time
```

transport-address ipv4

Use this command to configure the IPv4 transport address for a label space.

The transport address is the address used for the TCP session over which LDP is running. Use this command to manually configure the transport address. Transport addresses may either be bound to a loopback interface, or to a physical interface that is bound to the label space in question. A transport address can also be manually configured using the CLI with the loopback address as the transport address.

Note: The CLI accepts only the loopback address to be configured as the transport address.

Use the `no` parameter to stop using the transport address as the IPv4 transport address. If the label space is not specified for either form of this command, a label space of zero is assumed.

Command Syntax

```
transport-address ipv4 A.B.C.D
transport-address ipv4 A.B.C.D ((0)|)
no transport-address ipv4 A.B.C.D
no transport-address ipv4 A.B.C.D LABELSPACE
```

Parameters

`A.B.C.D`	Specify the IPv4 address to be used as the transport address. Only addresses bound to a loopback interface are valid for manual transport address configuration.
`0`	Platform-wide label space (0) is supported.

Default

Transport addresses are chosen for label spaces. By default, the loopback address is selected as the transport address. If a loopback address is not configured, the label space value is examined. The IP address of the interface is bound to the same label space is chosen as the transport address.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure router
(config)#router ldp
(config-router)#transport-address ipv4 10.10.0.5 20
```

CHAPTER 2 LDP Show Commands

This chapter provides an alphabetized reference for each of the LDP commands. It includes the following commands:

show debugging ldp

Use this command to display the status of the debugging of the LDP system.

Command Syntax

```
show debugging ldp
```

Parameter

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output from the `show debugging ldp` command.

```
#show debugging ldp
LDP debugging status:
  LDP event debugging is on
  LDP packet debugging is on
  LDP finite state machine debugging is on
  LDP pdu hexdump debugging is on
  LDP downstream state machine debugging is on
  LDP upstream state machine debugging is on
  LDP trunk state machine debugging is on
  LDP QoS debugging is on
  LDP CSPF debugging is on
  LDP VC USM debugging is on
  LDP VC DSM debugging is on
  LDP NSM debugging is on
  LDP Advertise-labels debugging is on
#
```

Table 2-36 explains the show command output fields.

Table 2-36: show debugging ldp output fields details

Field	Description
LDP debugging status	Status of the LDP debugging protocol.

show ldp

Use this command to display basic LDP attributes defined for the current LSR.

Command Syntax

```
show ldp
```

Parameter

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following is a sample output from the `show ldp` command displaying basic LDP attributes.

```
#show ldp
Router ID                : 20.1.1.1
LDP Version              : 1
Global Merge Capability  : Merge Capable
Label Advertisement Mode : Downstream Unsolicited
Label Retention Mode     : Liberal
Label Control Mode       : Independent
Instance Loop Detection  : On
Instance Hop Count Limit : 255
Instance Path Vec Count  : 255
Request Retry            : Off
Propagate Release        : Disabled
Graceful Restart         : Disabled
Hello Interval           : 5
Targeted Hello Interval  : 15
Hold time                : 15
Targeted Hold time       : 45
Keepalive Interval       : 10
Keepalive Timeout        : 30
Request retry Timeout    : 5
Transport Address data   :
Labelspace 0           : 20.1.1.1 (in use)
Import BGP routes        : No
#
```

Table 2-37 explains the show command output fields.

Table 2-37: show ldp output fields details:

Field	Description
Router ID	Router identifier in IP address format for this system.
LDP Version	Details of Link Layer Discovery Protocol (LLDP) version.
Global Merge Capability	Used to override the default merge capability setting of all the interfaces for the current LSR.
Label Advertisement Mode	Used to set the label advertisement mode for an interface for the current LSR to either downstream-on-demand (label is sent only when requested) or downstream-unsolicited (label is sent unrequested).
Label Retention Mode	Used for all labels exchanged via the given interface.
Label Control Mode	LSR generates a local label for a FEC which the router learned from routing table independently from other LSRs.
Loop Detection	Used to enable loop detection on the current LSR.
Loop Detection Count	Indicates the loop detection hop count.
Request Retry	Enables the LSR to send a maximum of five label requests.
Propagate Release	Used to propagate the release of labels to downstream routers.
Hello Interval	Sets the interval for sending unicast hello packets to peers.
Targeted Hello Interval	Sets the interval for sending unicast hello packets to targeted peers.
Hold time	Sets the time-out value to peers.
Targeted Hold time	Sets the time-out value that is the time that the router waits before rejecting an adjacency with targeted peers.
Keepalive Interval	Used to set the interval for sending keep-alive messages to the peer in order to maintain a session.
Keepalive Timeout	Time-out value for rejecting a session with a peer.
Request retry Timeout	Used to set the interval between retries.
Targeted Hello Receipt	Status of the hello receipt.
Transport Address	The transport address is the address used for the TCP session over which LDP is running.
Transport Interface	Interface is used for the TCP session over which LDP is running.
Import BGP routes	Used to import BGP routes into LDP.

show ldp adjacency

Use this command to display all the adjacencies for the current LSR.

Command Syntax

```
show ldp adjacency
```

Parameter

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output from the `show ldp adjacency` command displaying all the adjacencies for this LSR.

```
#show ldp adjacency
IP AddressInterface NameHoldtimeLDP ID
192.168.3.5eth11510.10.0.18:0
192.168.4.5  eth2   15 10.10.0.18:0
```

Table 2-38 explains the show command output fields.

Table 2-38: show ldp adjacency output fields details

Field	Description
IP Address	IP address of the interface.
Interface Name	Name of the interface.
Hold time	Sets the time-out value to peers.
LDP ID	LDP identifier for this protocol.

show ldp advertise-labels

Use this command to display the IP access list of LDP advertise-labels.

Command Syntax

```
show ldp advertise-labels
```

Parameter

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output from the `show ldp advertise-labels` command.

```
#show ldp statistics advertise-labels
Advertisement spec:
Prefix list = prefix1; Peer plist = peer1
Deny : Label Mapping = 1
Label Request = 0
```

Table 2-39 explains the show command output fields.

Table 2-39: show ldp advertise-labels output fields details

Field	Description
Advertisement spec	Details of the advertisement spec.
Prefix list	The label is advertised to all peers permitted by the peer plist.
Peer plist	The prefix list permits the prefix and there is a peer plist.

show ldp downstream

Use this command to display the status of all downstream sessions and the label information exchanged.

Command Syntax

```
show ldp downstream
```

Parameter

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is an output from the `show ldp downstream` command showing the status of all downstream sessions.

```
#show ldp downstream
Session peer 1.1.1.1:
  FEC                         Nexthop Addr       State            Label
Req.ID   Attr
  20.0.0.0/24                  connected      Established       impl-null  0
  10.0.2.0/24                  connected      Established       impl-null  0
  1.1.1.1/32                    20.0.0.1      Established       impl-null  0
Session peer 3.3.3.3:
  FEC                         Nexthop Addr       State            Label
Req.ID   Attr
  60.0.0.0/24                  connected      Established          52481  0
  50.0.0.0/24                   30.0.0.2      Established       impl-null  0
  30.0.0.0/24                  connected      Established       impl-null  0
  10.0.2.0/24                  connected      Established       impl-null  0
  5.5.5.5/32                    30.0.0.2      Established          52480  0
  3.3.3.3/32                    30.0.0.2      Established       impl-null  0
Session peer 4.4.4.4:
  FEC                         Nexthop Addr       State            Label
Req.ID   Attr
  50.0.0.0/24                  connected      Established          52483  0
  40.0.0.0/24                  connected      Established       impl-null  0
  10.0.2.0/24                  connected      Established       impl-null  0
  5.5.5.5/32                    40.0.0.2      Established          52480  0
  60.0.0.0/24                   40.0.0.2      Established       impl-null  0
  4.4.4.4/32                    40.0.0.2      Established       impl-null  0
Session peer 1.1.1.1:
  FEC                           State             Label     Req.ID    Attr
  60.0.0.0/24                Established           52486        0     None
  4.4.4.4/32                 Established           52484        0     None
  50.0.0.0/24                Established           52483        0     None
  40.0.0.0/24                Established       impl-null        0     None
  30.0.0.0/24                Established       impl-null        0     None
  20.0.0.0/24                Established       impl-null        0     None
```

```
    10.0.2.0/24              Established       impl-null         0     None
    5.5.5.5/32               Established           52482         0     None
    3.3.3.3/32               Established           52481         0     None
    2.2.2.2/32               Established       impl-null         0     None
  Session peer 3.3.3.3:
    FEC                        State              Label     Req.ID    Attr
    60.0.0.0/24              Established           52487         0     None
    4.4.4.4/32               Established           52485         0     None
    1.1.1.1/32               Established           52480         0     None
    40.0.0.0/24              Established       impl-null         0     None
    30.0.0.0/24              Established       impl-null         0     None
    20.0.0.0/24              Established       impl-null         0     None
    10.0.2.0/24              Established       impl-null         0     None
    2.2.2.2/32               Established       impl-null         0     None
  Session peer 4.4.4.4:
    FEC                        State              Label     Req.ID    Attr
    50.0.0.0/24              Established           52483         0     None
    40.0.0.0/24              Established       impl-null         0     None
    30.0.0.0/24              Established       impl-null         0     None
    20.0.0.0/24              Established       impl-null         0     None
    10.0.2.0/24              Established       impl-null         0     None
    3.3.3.3/32               Established           52481         0     None
    2.2.2.2/32               Established       impl-null         0     None
    1.1.1.1/32               Established           52480         0     None
```

Table 2-40 explains the show command output fields.

Table 2-40: show ldp downstream output fields details

Field	Description
Session peer	Used to group and apply the configuration of general session commands to groups of neighbors that share common session configuration elements.
FEC	Displays the Forward Equivalency Class (FEC) for this entry.
Nexthop addr	Displays the IP address of the next hop.
State	Displays the current status of the ldp.
Label	Details of the ldp downstream labels.
Req.ID	Request identifier for the protocol.
Attr	The attribute is used to sent to a customer router.

show ldp fec

Use the following command to display all FECs (Forwarding Equivalence Classes) known to this LSR.

Command Syntax

```
show ldp fec
show ldp fec (prefix)
show mpls ldp fec
show mpls ldp fec (prefix|)
```

Parameter

`prefix`	Display prefix FEC information.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ldp fec
LSR codes    : E/N - LSR is egress/non-egress for this FEC,
               L - LSR received a label for this FEC,
               > - LSR will use this route for the FEC
FEC                    Code    Session         Out Label       Nexthop Addr
1.1.1.1/32             NL>     1.1.1.1         impl-null       20.0.0.1
2.2.2.2/32             E >     non-existent    none            connected
3.3.3.3/32             NL>     3.3.3.3         impl-null       30.0.0.2
4.4.4.4/32             NL>     4.4.4.4         impl-null       40.0.0.2
5.5.5.5/32             NL>     4.4.4.4         impl-null       40.0.0.2
                       NL>     3.3.3.3         impl-null       30.0.0.2
20.0.0.0/24            NL      1.1.1.1         impl-null       invalid
                       E >     non-existent    none            connected
30.0.0.0/24            NL      3.3.3.3         impl-null       invalid
                       E >     non-existent    none            connected
40.0.0.0/24            NL      4.4.4.4         impl-null       invalid
                       E >     non-existent    none            connected
50.0.0.0/24            NL      4.4.4.4         impl-null       invalid
                       NL>     3.3.3.3         impl-null       30.0.0.2
60.0.0.0/24            NL>     4.4.4.4         impl-null       40.0.0.2
                       NL      3.3.3.3         impl-null       invalid
```

Table 2-41 shows the codes at the end of each route entry that indicate where the route originated.

Table 2-41: Origin Codes

Origin Code	Description	Comments
E/N	Egress/Non-egress	LSR is egress/non-egress for this FEC.
L	LSR	LSR received a label for this FEC.
>		LSR will use this route for the FEC.

Table 2-42 explains the show command output fields.

Table 2-42: show ldp fec output fields details

Field	Description
FEC	Displays the Forward Equivalency Class (FEC) for this entry.
Session	Reports the current session state.
Out Label	Label received from downstream neighbor for route.
Nexthop addr	Displays the IP address of the next hop.

show ldp igp sync

Use the following command to display the LDP synchronization status.

Command Syntax

```
show ldp igp sync
show mpls ldp igp sync
```

Parameter

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ldp igp sync
eth1
LDP configured; LDP-IGP Synchronization enabled.
Sync status: sync achieved
Delay timer: Not Configured , Not Running
```

show ldp interface

Table 2-43: show ldp fec output fields details

Field	Description
FEC	Displays the Forward Equivalency Class (FEC) for this entry.
Session	Reports the current session state.
Out Label	Label received from downstream neighbor for route.
Nexthop addr	Displays the IP address of the next hop.

Use this command to display the list of all interfaces on the current LSR, and to indicate whether a given interface is label-switching or not.

Command Syntax

```
show ldp interface
show ldp interface IFNAME
```

Parameter

`IFNAME` Displays the name of the interface.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following output displays a list of all interfaces on the LSR.

```
#show ldp interface
Interface    LDP Identifier          Label-switching    Merge Capability
eth0         10.10.0.11:0            Disabled           N/A
lo           10.10.0.11:0            Disabled           N/A
eth1         10.10.0.11:0            Enabled            Merge capable
eth2         10.10.0.11:0            Enabled            Merge capable
vmnet1        10.10.0.11:0           Disabled            N/A
```

The following is a sample output from the `show ldp interface IFNAME` command displaying information about the specified interface `eth1`.

```
#show ldp interface eth1
Status                  : Enabled
Primary IP Address      : 192.168.3.4
Interface Type          : Ethernet
Label Merge Capability  : Merge Capable
Hello Interval          : 5
Targeted Hello Interval : 15
Hold Time               : 15
Targeted Hold Time      : 45
```

```
Keepalive Interval      : 10
Keepalive Timeout       : 30
Advertisement Mode      : Downstream On Demand
Label Retention Mode    : Liberal
Administrative Groups   : myGroup
```

Table 2-44 explains the show command output fields.

Table 2-44: show ldp interface output fields details

Field	Description
Interface	Name of the interface.
LDP Identifier	LDP identifier for this protocol.
Label-switching	Status of the label-switching on interface..
Merge Capability	Used to override the default merge capability setting of all the interfaces.
Status	Status of the ldp interface.
Primary IP Address	Address of the primary Internet protocol in the interface.
Interface Type	Type of interface.
Label Merge Capability	Used to override the default merge capability setting of all the interfaces for the label.
Hello Interval	Sets the interval for sending unicast hello packets to peers.
Targeted Hello Interval	Sets the interval for sending unicast hello packets to targeted peers.
Hold time	Sets the time-out value to peers.
Targeted Hold time	Sets the time-out value that is the time that the router waits before rejecting an adjacency with targeted peers.
Keepalive Interval	Used to set the interval for sending keep-alive messages to the peer in order to maintain a session.
Keepalive Timeout	Time-out value for rejecting a session with a peer.
Label Advertisement Mode	Used to set the label advertisement mode for an interface for the current LSR to either downstream-on-demand (label is sent only when requested) or downstream-unsolicited (label is sent unrequested).
Label Retention Mode	Used for all labels exchanged via the given interface.
Administrative Groups	Administrative group to be used for links.

show ldp lsp

Use this command to display LDP LSP and, optionally, advertise-label information.

Command Syntax

```
show ldp lsp
show ldp lsp prefix detail
show ldp lsp (prefix|detail)
```

Parameter

`prefix`	Displays advertise-label information in addition to LDP LSP information.
`detail`	Displays advertise-label information in addition to LDP LSP information.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output from the `show ldp lsp prefix detail` command displaying LDP LSP prefix information with advertise-label information.

```
#show ldp lsp prefix detail
Advertisement spec:
    Prefix list = pfx1; Peer plist = pfx1
    Prevent the distribution of any assigned labels

FEC IPV4:1.1.1.0/30 -> 0.0.0.0
  Downstream state: Established Label: impl-null RequestID: 0 Peer:
50.50.50.50
Attr:
  Advert acl(s): Prevent the distribution of any assigned labels
FEC IPV4:3.3.3.0/30 -> 0.0.0.0
  Advert acl(s): Prevent the distribution of any assigned labels
FEC IPV4:10.30.0.0/24 -> 0.0.0.0
  Downstream state: Established Label: impl-null RequestID: 0 Peer:
50.50.50.50
Attr:
  Advert acl(s): Prevent the distribution of any assigned labels
FEC IPV4:50.50.50.50/32 -> 1.1.1.1
  Advert acl(s): Prefix list = pfx1; Peer plist = pfx1
FEC IPV4:55.55.55.55/32 -> 3.3.3.2
  Advert acl(s): Prevent the distribution of any assigned labels
FEC IPV4:169.254.0.0/16 -> 0.0.0.0
  Downstream state: Established Label: impl-null RequestID: 0 Peer:
50.50.50.50
Attr:
  Advert acl(s): Prevent the distribution of any assigned labels
```

Table 2-45 explains the show command output fields.

Table 2-45: show ldp lsp output fields details

Field	Description
Advertisement spec	Details of the advertisement spec.
Prefix list	The label is advertised to all peers permitted by the peer plist.
Peer plist	The prefix list permits the prefix and there is a peer plist.
Downstream state	Details of the downstream state.
Established Label	LSP established by the Downstream on Demand method of label distribution.
Req.ID	Request identifier for the protocol.
Peer	Details of the peer.
Attr	The attribute is used to sent packets to a customer router.

show ldp mpls-l2-circuit

Use this command to display summarized Layer-2 Virtual Circuit information about all MPLS virtual circuits configured on the current LSR. When the Virtual Circuit ID is specified, this command displays summarized information for the Virtual Circuit matching the specified ID only.

Command Syntax

```
show ldp mpls-l2-circuit
show ldp mpls-l2-circuit <1-4294967295>
show ldp mpls-l2-circuit detail
show ldp mpls-l2-circuit count
show ldp mpls-l2-circuit <1-4294967295> detail
```

Parameter

`<1-4294967295>`	Indicates the virtual circuit ID.
`detail`	Displays detailed LDP information.
`count`	Count of PWs from LDP standpoint.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of this command displaying summarized information of VID 1000:

```
#show ldp mpls-l2-circuit 1000
Transport Client     VC     Trans    Local       Remote      Destination
VC ID     Binding    State  Type     VC Label    VC Label    Address
1000      eth2       UP     ethernet 640         640         192.168.0.80

#show ldp mpls-l2-circuit
Transport Client     VC     Trans    Local       Remote      Destination
VC ID     Binding    State  Type     VC Label    VC Label    Address
1000      eth2       UP     ethernet 640         640         192.168.0.80
2000      eth3       UP     ethernet 641         648         192.168.0.80
3000      eth4       UP     ethernet 642         645         192.168.0.90
```

The following is a sample output of this command when using the `detail` parameter:

```
#show ldp mpls-l2-circuit detail
vcid: 100, type: ethernet, local groupid: 4, remote groupid: 4 (vc is up)
destination: 10.0.0.2, Peer LDP Ident: 10.0.0.2
Local label: 53120, remote label: 53120
Access IF: eth3, Network IF: eth4
Local MTU: 1500, Remote MTU: 1500
Local Control Word: 0, Remote Control Word: 0
Local PW Status Capability : enabled
```

```
Remote PW Status Capability : enabled
Current PW Status TLV : enabled
Local PW Status :
Not Forwarding
Remote PW Status :
Not Forwarding
Standby
```

Table 2-46 explains the show command output fields.

Table 2-46: show ldp mpls-l2-circuit output fields details

Field	Description
Transport VC ID	Transport VC identifier for the protocol.
Client Binding	Show whether the interface is client bound and (if bound) with which client.
VC State	State of the VC.
Trans Type	Type of transmit.
Local VC Label	Incoming VC label details.
Remote VC Label	Outgoing VC label details.
Destination Address	Destination IP address for the protocol.
VCid	Address for the VC.
Type	Type of Ethernet interface.
local groupid	Address for the local group.
remote groupid	Address for the remote group.
destination	Destination IP address.
Peer LDP Ident	Identification for the peer LDP.
Local label	Number of Local label
remote label	Number remote label.
Access IF	Map the access port.
Network IF	Map the network port in the interface.
Local MTU	Number of local MTU., Remote MTU - Number of local MTU.
Local Control Word	Number of local control word.
Remote Control Word	Number of local control word.
Local PW Status Capability	PW Status capability of Local end of PW.

Table 2-46: show ldp mpls-l2-circuit output fields details (Continued)

Field	Description
Remote PW Status Capability	PW Status capability of Remote end of PW.
Current PW Status TLV	A data structure used to encode optional information in a data communications protocol.
Local PW Status	PW Status of Local end of PW.
Remote PW Status	PW Status of Remote end of PW.

show ldp routes

Use this command to display LDP routes.

Command Syntax

```
show ldp routes
```

Parameter

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ldp routes
Prefix: 0.0.0.0/0   Nexthop: 10.0.2.2   IFINDEX: 2
Prefix: 1.1.1.1/32   Nexthop: 20.0.0.1   IFINDEX: 3
Prefix: 2.2.2.2/32   Nexthop: 0.0.0.0   IFINDEX: 1
Prefix: 3.3.3.3/32   Nexthop: 30.0.0.2   IFINDEX: 4
Prefix: 4.4.4.4/32   Nexthop: 40.0.0.2   IFINDEX: 5
Prefix: 5.5.5.5/32   Nexthop: 30.0.0.2   IFINDEX: 4
                     Nexthop: 40.0.0.2   IFINDEX: 5
Prefix: 20.0.0.0/24   Nexthop: 0.0.0.0   IFINDEX: 3
Prefix: 30.0.0.0/24   Nexthop: 0.0.0.0   IFINDEX: 4
Prefix: 40.0.0.0/24   Nexthop: 0.0.0.0   IFINDEX: 5
Prefix: 50.0.0.0/24   Nexthop: 30.0.0.2   IFINDEX: 4
Prefix: 60.0.0.0/24   Nexthop: 40.0.0.2   IFINDEX: 5
```

Table 2-47 explains the show command output fields.

Table 2-47: show ldp routes output fields details

Field	Description
Prefix	Details of the network address prefix.
Nexthop	Displays the IP address of the next hop.
IFINDEX	Displays an interface index.

show ldp session

Use this command to display sessions established between this LSR and other LSRs.

Command Syntax

```
show ldp session
show ldp session A.B.C.D
show ldp session X:X::X:X
show mpls ldp session
show mpls ldp session A.B.C.D
show mpls ldp session X:X::X:X
```

Parameter

`A.B.C.D`	IPv4 address of the peer.
`X:X::X:X`	IPv6 address of the peer.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
OcNOS#show ldp session 192.168.3.5
Session state: OPERATIONAL
Session role: Passive
TCP Connection: Established
IP Address for TCP: 192.168.3.5
Interface being used : eth1
Peer LDP ID: 10.10.0.18:0
Peer Password : mypwd
Authentication type: MD5
Adjacencies: 192.168.3.5
192.168.4.5
Advertisement mode: Downstream Unsolicited
Label retention mode : Liberal
Graceful Restart              : Capable
Reconnect Timeout             : 120
Recovery Timeout (max)        : 120
Recovery Timeout [negotiated] : 0 [120]
Keepalive Timeout: 30
Reconnect Interval: 15
Address List received : 192.168.3.5
192.168.4.5
Received Labels :FecLabelMaps To
IPV4:10.10.0.0/24
impl-null none
IPV4:192.168.3.0/24 impl-null none
IPV4:192.168.4.0/24 impl-null none
```

```
    IPV4:192.168.5.0/24 impl-null none
    Sent Labels :FecLabelMaps To
    IPV4:10.10.0.0/24
    impl-null none
    IPV4:192.168.3.0/24 impl-null none
    IPV4:192.168.4.0/24 impl-null none
```

Table 2-48 explains the show command output fields.

Table 2-48: show ldp session output fields details

Field	Description
Session state	Reports the current session state.
Session role	Displays the status of the session role.
TCP Connection	Details of the TCP connection.
IP Address for TCP	Transmission control protocol IP address for the network.
Interface	Name of interface used in the network.
Peer LDP ID	Identifier for the peer LDP.
Peer Password	Credential details for the neighbor.
Authentication type	Type of authentication.
Adjacencies	IP address for the neighbor adjacencies.
Advertisement mode	Details of the advertisement mode.
Label retention mode	Details of the label retention mode.
Graceful Restart	Indicates if the peer session is “Capable” or “Not Capable”.
Reconnect Timeout	The amount of time the router keeps the labels until session re-connection, the value is the lower value between local and remote neighbor-liveness timer. It appears when the session is GR capable.
Recovery Timeout (max)	Indicates the amount of time for the recovery session to send the initialization message to the peer, according to the local max-recovery timer. It appears when the session is GR capable.
Recovery Timeout [negotiated]	Indicates the actual timer value and the initial amount of time to recovery session (between brackets) that is negotiated with the peer to the lower value between local and remote values. Negotiated value 0 indicates the labels are not preserved after session disconnection. It appears when the session is GR capable.
Keepalive Interval	Used to set the interval for sending keep-alive messages to the peer in order to maintain a session.
Keepalive Timeout	Time-out value for rejecting a session with a peer.
Address List received	List of address that is received from neighbor.
Received Labels	Number of labels received from neighbor session.
Sent Labels	Number of labels transmitted to neighbor session.

show ldp statistics

Use this command to display LDP statistics.

Command Syntax

```
show ldp statistics
```

Parameter

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output from the `show ldp statistics` command.

```
#show ldp statistics

=======================================================
 LSR ID = 0.0.0.0:0 : TARGETED PEER: 10.10.10.10
=======================================================
  PacketType                      Total
                             Sent       Received
  Notification                 0            0
  Hello                        0            0
  Initialization               0            0
  Keepalive                    0            0
  Address                      0            0
  Address Withdraw             0            0
  Label Mapping                0            0
  Label Request                0            0
  Label Withdraw               0            0
  Label Release                0            0
  Request Abort                0            0
=======================================================
#
```

Table 2-49 explains the show command output fields.

Table 2-49: show ldp statistics output fields details

Field	Description
LSR ID	Identifier of the LSR.
Targeted Peer	Targeted LDP neighbor can improve the label convergence time compared to the convergence time with directly connected LDP peers when there are flapping links.

Table 2-49: show ldp statistics output fields details (Continued)

Field	Description
Packet Type	Type of packet in the interface that has been received or transmitted to the neighbors.
Total	Number of total packets that has been received and transmitted.

show ldp statistics advertise-labels

Use this command to display the count per each operation filtered by an advertisement list.

Command Syntax

```
show ldp statistics advertise-labels
```

Parameter

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output from the `show ldp statistics advertise-labels` command.

```
#show ldp statistics advertise-labels
Advertisement spec:
    Prefix list = pfx1; Peer plist = pfx1
      Deny : Label Mapping = 2
             Label Request = 0
    Prevent the distribution of any assigned labels
      Deny : Label Mapping = 9
             Label Request = 3
#
```

Table 2-50 explains the show command output fields.

Table 2-50: show ldp statistics advertise-labels output fields details

Field	Description
Advertisement spec	Details of the advertisement spec.
Prefix list	It is an ordered list and entries are evaluated in order of increasing sequence number.
Peer plist	The peer keyword enables the device to receive time requests and used to synchronize itself to the servers specified in the access list.
Label Mapping	Number of label mapping that is denied.
Label Request	Number of label request that is denied.

show ldp targeted-peers

Use this command to display the list of targeted peers configured on the current LSR.

Command Syntax

```
show ldp targeted-peers
```

Parameter

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output from the `show ldp targeted-peers` command.

```
#show ldp targeted-peers
IP Address          Interface

192.168.201.2       eth1
```

Table 2-51 explains the show command output fields.

Table 2-51: show ldp targeted-peers output fields details

Field	Description
IP Address	Internet protocol address for the interface.
Interface	Name of the interface.

show ldp upstream

Use this command to display the status of all upstream sessions and label information exchanged.

Command Syntax

```
show ldp upstream
```

Parameter

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of the `show ldp upstream` command showing the status of all upstream sessions.

```
#show ldp upstream
Session peer 1.1.1.1:
  FEC                       State              Label     Req.ID    Attr
  60.0.0.0/24             Established           52486        0     None
  4.4.4.4/32              Established           52484        0     None
  50.0.0.0/24             Established           52483        0     None
  40.0.0.0/24             Established       impl-null        0     None
  30.0.0.0/24             Established       impl-null        0     None
  20.0.0.0/24             Established       impl-null        0     None
  10.0.2.0/24             Established       impl-null        0     None
  5.5.5.5/32              Established           52482        0     None
  3.3.3.3/32              Established           52481        0     None
  2.2.2.2/32              Established       impl-null        0     None
Session peer 3.3.3.3:
  FEC                       State              Label     Req.ID    Attr
  60.0.0.0/24             Established           52487        0     None
  4.4.4.4/32              Established           52485        0     None
  1.1.1.1/32              Established           52480        0     None
  40.0.0.0/24             Established       impl-null        0     None
  30.0.0.0/24             Established       impl-null        0     None
  20.0.0.0/24             Established       impl-null        0     None
  10.0.2.0/24             Established       impl-null        0     None
  2.2.2.2/32              Established       impl-null        0     None
Session peer 4.4.4.4:
  FEC                       State              Label     Req.ID    Attr
  50.0.0.0/24             Established           52483        0     None
  40.0.0.0/24             Established       impl-null        0     None
  30.0.0.0/24             Established       impl-null        0     None
  20.0.0.0/24             Established       impl-null        0     None
  10.0.2.0/24             Established       impl-null        0     None
  3.3.3.3/32              Established           52481        0     None
  2.2.2.2/32              Established       impl-null        0     None
  1.1.1.1/32              Established           52480        0     None
```

Table 2-52 explains the show command output fields.

Table 2-52: show ldp upstream output fields details

Field	Description
Session peer	Details of the session peers.
FEC	Displays the Forward Equivalency Class (FEC) for this entry.
State	Reports the current session state.
Label	Number of Label received from upstream neighbor for route.
Req.ID	Requested session identifier for the protocol.
Attr	The attribute is used to sent packets to a customer router.

show mpls ldp discovery

Use this command to display the sources for locally generated LDP Discovery Hello PDUs, and to indicate whether an interface is label-switching.

Command Syntax

```
show mpls ldp discovery
show mpls ldp discovery IFNAME
```

Parameter

IFNAME	Interface name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mpls ldp discovery
Interface           LDP Identifier          Label-switching Merge Capability
eth0                10.10.0.11:0            Disabled        N/A
lo                  10.10.0.11:0            Disabled        N/A
eth1                10.10.0.11:0            Enabled         Merge capable
eth2                10.10.0.11:0            Enabled         Merge capable
vmnet1              10.10.0.11:0            Disabled         N/A
```

Table 2-53 explains the show command output fields.

Table 2-53: show ldp discovery output fields details

Field	Description
Interface	Name of the interface.
LDP Identifier	LDP identifier for this protocol.
Label-switching	Status of the label-switching on interface.
Merge Capability	Used to override the default merge capability setting of all the interfaces.

show mpls ldp neighbor

Use this command to display LDP neighbor information.

Command Syntax

```
show mpls ldp neighbor
show mpls ldp neighbor detail
```

Parameter

`detail`	Details for adjacencies.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mpls ldp neighbor detail
IP Address            Interface Name    Holdtime    LDP ID
192.168.3.5           eth1              15          10.10.0.18:0
192.168.4.5           eth2              15          10.10.0.18:0
```

Table 2-54 explains the show command output fields.

Table 2-54: show mpls ldp neighbor output fields

Field	Description
IP Address	Address of the interface.
Interface Name	Name of the interface.
Holdtime	The amount of time this device waits between SPFs.
LDP ID	Local label space ID. The first four bytes of an LDP ID is a platform IP address called the LDP router ID. The last two bytes are called the local label space ID.

show mpls ldp parameter

Use this command to display LDP configuration parameters.

Command Syntax

```
show mpls ldp parameter
```

Parameter

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mpls ldp parameter
Router ID                 : 0.0.0.0
LDP Version               : 1
Global Merge Capability   : Merge Capable
Label Advertisement Mode  : Downstream Unsolicited
Label Retention Mode      : Liberal
Label Control Mode        : Independent
Instance Loop Detection   : Off
Request Retry             : Off
Propagate Release         : Disabled
Graceful Restart          : Disabled
Hello Interval            : 5
Targeted Hello Interval   : 15
Hold time                 : 15
Targeted Hold time        : 45
Keepalive Interval        : 10
Keepalive Timeout         : 30
Request retry Timeout     : 5
Transport Address data    :
  Labelspace 0            : 192.168.201.2 (not in use)
Import BGP routes         : No
```

Table 2-55 explains the show command output fields.

Table 2-55: show mpls ldp parameters output fields

Field	Description
Router ID	A preferred interface address for LDP router.
LDP Version	Latest LDP version details.

Table 2-55: show mpls ldp parameters output fields

Field	Description
Global Merge Capability	Override the default merge capability setting of all the interfaces.
Label Advertisement mode	Label advertisement mode details in the interface.
Label retention mode	Label retention mode details in the interface.
Label Control Mode	Controls the mode used for handling label binding requests on interfaces.
Instance Loop Detection	Disables the LDP optional loop detection mechanism.
Request Retry	Request causes the target peer to respond with targeted Hello messages.
Propagate Release	Propagate release is disabled in the interface.
Graceful Restart	Graceful Restart (GR) is a mechanisms to prevent routing protocol re-convergence during a processor switchover. Hello Interval - Hello interval sets the interval for sending unicast hello packets to peers.
Targeted Hello Interval	Targeted hello interval sets the interval for sending unicast hello packets to targeted peers.
Hold time	Hold time sets the time-out value to peers.
Targeted Hold time	Time-out value is the time that the router waits before rejecting an adjacency with targeted peers.
Keepalive Interval	Keepalive interval sets the interval for sending keep-alive messages to the peer in order to maintain a session.
Keepalive Timeout	Time-out value for rejecting a session with a peer.
Request retry Timeout	Request for the maximum retry duration (the number of retries times the length of the timeout).
Transport Address data	Transport address advertised in LDP Discovery Hello messages sent on an interface.
Label space	Label used in a label binding is allocated from a set of possible labels called a label space.
Import BGP routes	The BGP Support for IP Prefix Import from Global Table into a VRF Table feature introduces the capability to import IPv4 unicast prefixes from the global routing table into a Virtual Private Network (VPN) routing/forwarding (VRF) instance table using an import route map.

RSVP-TE Command Reference

CHAPTER 1 RSVP-TE Commands

This chapter describes the RSVP-TE commands.

- no-php
- no-refresh-path-parsing
- no-refresh-path-parsing
- no-refresh-resv-parsing
- php
- primary ADMIN-GROUP-NAMEprimary affinity
- primary bandwidth
- primary cspf
- primary cspf-retry-limit
- primary cspf-retry-timer
- primary filter
- primary hold-priority
- primary hop-limit
- primary label-record
- primary local-protection
- primary no-affinity
- primary no-cspf
- primary no-record
- primary path
- primary policer
- primary record
- primary retry-limit
- primary retry-timer
- primary reuse-route-record
- primary setup-priority
- primary traffic
- refresh-time
- refresh-path-parsing
- refresh-resv-parsing
- restart rsvp graceful
- router rsvp
- rsvp hello-interval
- rsvp hello-receipt
- rsvp hello-timeout
- rsvp keep-multiplier
- rsvp refresh-time

- rsvp-path
- rsvp-trunk
- rsvp-trunk-restart
- secondary ADMIN-GROUP-NAME
- secondary bandwidth
- secondary bandwidth
- secondary cspf
- secondary cspf-retry-limit
- secondary cspf-retry-timer
- secondary filter
- secondary hold-priority
- secondary hop-limit
- secondary label-record
- secondary local-protection
- secondary no-affinity
- secondary no-cspf
- secondary no-record
- secondary path
- secondary policer
- secondary record
- secondary retry-limit
- secondary retry-timer
- secondary reuse-route-record
- secondary setup-priority
- secondary traffic
- snmp restart rsvp
- to A.B.C.D
- to X:X::X:X
- update-type
- X:X::X:X

A.B.C.D

Use this command to configure an explicit IPv4 route sub-object as either loose or strict. A list of sub-objects specifies an explicit route to the egress router for an LSP.

- For the strict type of route addresses, the route taken from the previous router to the current router must be a directly connected path and a message exchanged between the two routers should not pass any intermediate routers. This ensures that routing is enforced on the basis of each link.
- For the loose type of route addresses, the route taken form the previous router to the current router need not be a direct path and a message exchanged between the two routers can pass other routers.

Use the `no` parameter with this command to disable the configuration.

Note: Refer to X:X::X:X to configure an explicit IPv6 route sub-object as either loose or strict.

Command Syntax

```
A.B.C.D
A.B.C.D (loose|strict)
no A.B.C.D
no A.B.C.D (loose|strict)
```

Parameters

`loose`	Make this node loose
`strict`	Make this node strict

Default

By default, A.B.C.D is disabled

Command Mode

Path mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-path mypath
(config-path)#10.10.0.5 strict
```

clear rsvp session

Use this command to reset either all or specified sessions originating from a specific ingress and terminating on the specific egress.

Note: If the affected session originates from the router where the command is issued, it is stopped and started. If the affected session does not originate from the router where the command is issued, it is stopped and deleted.

Command Syntax

```
clear rsvp session TUNNEL-ID LSP-ID INGRESS EGRESS
```

Parameters

TUNNELID	Clear tunnel ID sessions
LSP-ID	Clear LSP ID sessions
INGRESS	Clear ingress sessions
EGRESS	Clear egress sessions

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear rsvp session 1 1 1.2.3.4 192.168.1.1
```

clear rsvp trunk

Use this command to clear an RSVP trunk or to clear all RSVP trunks.

Clearing a trunk also kills any session associated with the trunk. This command is useful when a trunk is missing required data such as routing information. When data is missing, the trunk is in an incomplete state, and clearing it correctly re-initializes the session.

Note: If this command is given in the session on the ingress router, the session stops and restarts. If this command is given in the session on the egress router, the session is not cleared.

Command Syntax

Note: Use the following commands to clear standard RSVP Trunks:

```
clear rsvp trunk *
clear rsvp trunk ingress (TRUNKNAME|*)
clear rsvp trunk non-ingress (TRUNKNAME|*)
clear rsvp trunk (TRUNKNAME|*)
clear rsvp trunk (TRUNKNAME|*) primary
clear rsvp trunk (TRUNKNAME|*) secondary
```

Parameters

`*`	Clear all RSVP trunks configured
`TRUNKNAME`	Name of a specific trunk to be cleared
`ingress`	Clear an RSVP ingress trunk
`non-ingress`	Clear an RSVP non-Ingress trunk
`primary`	Clear all primary sessions configured for this trunk
`secondary`	Clear all secondary sessions configured for this trunk

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear rsvp trunk mytrunk
#clear rsvp trunk *
#clear rsvp trunk ingress mytrunk
#clear rsvp trunk ingress *
#clear rsvp trunk non-ingress mytrunk
#clear rsvp trunk non-ingress *
#clear rsvp trunk mytrunk primary
#clear rsvp trunk * primary
#clear rsvp trunk mytrunk secondary
#clear rsvp trunk * secondary
```

cspf

Use this command to enable the use of Constrained Shortest Path First (CSPF) server for all RSVP sessions. If CSPF is turned off globally, it cannot be enabled for any LSP.

The CSPF server computes paths for LSPs that are subject to various constraints such as bandwidth, hop count, administrative groups, priority, and explicit routes. When computing paths for LSPs, CSPF considers not only the topology of the network and the attributes defined for the LSP but also the links. It attempts to minimize congestion by intelligently balancing the network load.

Use the no-cspf command to disable this configuration.

Command Syntax

```
cspf
```

Parameters

None

Default

By default, CSPF server is enabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows using the `no-cspf` command in Router mode to disable CSPF for all RSVP sessions.

```
#configure terminal
(config)#router rsvp
(config-router)#cspf
```

debug rsvp all

Use this command to enable all debugging options for an RSVP daemon.

Use the `no` parameter with this command to stop logging all debugging information.

Command Syntax

```
debug rsvp (all|)
no debug rsvp (all|)
```

Parameters

None

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug rsvp all
```

debug rsvp cspf

Use this command to enable the exchange of debugging messages between the RSVP module and the CSPF module.

Use the `no` parameter with this command to stop logging CSPF debugging information.

Command Syntax

```
debug rsvp cspf
no debug rsvp cspf
```

Parameters

None

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug rsvp cspf
```

debug rsvp events

Use this command to enable debugging of events that were generated from an RSVP daemon.

Use the `no` parameter with this command to stop logging RSVP debugging information.

Command Syntax

```
debug rsvp events
no debug rsvp events
```

Parameters

None

Command Mode

Privileged Exec and Configure modes

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug rsvp events
```

debug rsvp fsm

Use these commands to enable debugging of events related to RSVP finite state machines (FSM). Commands are available to log debugging information for the egress FSM, the ingress FSM, the transit FSM, the transit upstream FSM, or the transit downstream FSM.

Use the `no` parameter with these commands to stop logging FSM debugging information.

Command Syntax

```
debug rsvp fsm
debug rsvp fsm egress
debug rsvp fsm ingress
debug rsvp fsm transit
debug rsvp fsm transit upstream
debug rsvp fsm transit downstream
no debug rsvp fsm
no debug rsvp fsm egress
no debug rsvp fsm ingress
no debug rsvp fsm transit
no debug rsvp fsm transit upstream
no debug rsvp fsm transit downstream
```

Parameters

None

Command Mode

Privileged Exec and Configure modes

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#debug rsvp fsm transit upstream
```

debug rsvp hexdump

Use this command to enable the hexdump debugging option for an RSVP daemon.

Use the `no` parameter with this command to stop logging hexdump debugging information.

Command Syntax

```
debug rsvp hexdump
no debug rsvp hexdump
```

Parameters

None

Command Mode

Privileged Exec and Configure modes

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug rsvp hexdump
```

debug rsvp nsm

Use this command to enable the NSM debugging option for an RSVP daemon.

Use the `no` parameter with this command to stop logging NSM debugging information.

Command Syntax

```
debug rsvp nsm
no debug rsvp nsm
```

Parameters

None

Command Mode

Privileged Exec and Configure modes

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug rsvp nsm
```

debug rsvp packet

Use this command to enable packet debugging options for an RSVP daemon. Using the `in` option command enables debugging for incoming packets. Using the `out` option command enables debugging for outgoing packets.

Use the `no` parameter with these commands to stop logging debugging information.

Command Syntax

```
debug rsvp packet
debug rsvp packet in
debug rsvp packet out
no debug rsvp packet
no debug rsvp packet in
no debug rsvp packet out
```

Parameters

None

Command Mode

Privileged Exec and Configure modes

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug rsvp packet in
#debug rsvp packet out
```

disable-rsvp

Use this command to disable RSVP message exchange on an interface.

RSVP can be enabled using the enable-rsvp command.

Command Syntax

```
disable-rsvp
```

Parameters

None

Default

By default, RSVP message exchange is disabled on an interface.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#disable-rsvp
```

elsp-signal-map

Use this command to configure node-level PHB-EXP mapping for e-lsp signaled LSP.

Use the no parameter with this command to remove a PHB-EXP mapping.

Command Syntax

```
elsp-signal-map class <0-7> exp <0-7>
no elsp-signal-map class <0-7> exp <0-7>
```

Parameters

<0-7>	Diffserv class (queue) mapped to a PHB (per-hop behavior)
<0-7>	EXP bit mapped to the PHB

Command Mode

Router mode

Default

By default, elsp signal map is disabled

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router rsvp
(config-router)#elsp-signal-map class 0 exp 1
(config-router)#elsp-signal-map class 1 exp 4
(config-router)#elsp-signal-map class 3 exp 6
(config-router)#no elsp-signal-map class 1 exp 4
```

enable-rsvp

Use this command to enable RSVP message exchange on an interface.

Note: To use this command, the corresponding interface in the NSM needs to be enabled for label-switching using the label-switching command.

See disable-rsvp to undo the effects of this command.

Command Syntax

```
enable-rsvp
```

Parameters

None

Default

By default, RSVP message exchange is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#enable-rsvp
```

explicit-null

Use this command to send explicit-null labels for directly-connected forwarding equivalency classes (FECs) instead of implicit-null labels.

This command controls the label value advertised to an egress router of an LSP. By default, implicit null label (label 3) is advertised for directly connected FECs. If implicit-null label is advertised, the penultimate hop removes the label and sends the packet as a plain IP packet to the egress router. The explicit-null command advertises label 0 and retains the label so the egress router can pop it. For details about usage of explicit-null, please refer to *RFC 3032*.

Use the `no` parameter with this command to stop sending explicit-null labels for directly-connected FECs and resume sending implicit-null labels.

Command Syntax

```
explicit-null
no explicit-null
```

Parameters

None

Default

By default implicit-null labels are advertised.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#explicit-null
```

ext-tunnel-id A.B.C.D

Use this command to configure an extended-tunnel identifier as an IPv4 address. These identifiers are used in RSVP messages. If no extended-tunnel ID is specified, the LSR-ID for the router is used as the extended-tunnel ID for all LSPs. The extended-tunnel ID is a simple way of identifying all LSPs belonging to the same trunk.

Use the `no` parameter with this command to remove a configured extended-tunnel ID.

Command Syntax

```
ext-tunnel-id A.B.C.D
no ext-tunnel-id A.B.C.D
no ext-tunnel-id
```

Parameters

`A.B.C.D`	Extended tunnel identifier for this trunk in IPv4 address format

Default

By default, the LSR-ID of the router is used as the extended-tunnel ID for all sessions.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk t1
(config-trunk)#ext-tunnel-id 10.10.10.30

(config)#rsvp-trunk t1
(config-trunk)#no ext-tunnel-id 10.10.10.30
```

ext-tunnel-id X:X::X:X

Use this command to configure an extended-tunnel identifier as an IPv6 address. These identifiers are used in RSVP messages. If no extended-tunnel ID is specified, the LSR-ID for the router is used as the extended-tunnel ID for all LSPs. The extended-tunnel ID is a simple way of identifying all LSPs belonging to the same trunk.

Use the `no` parameter with this command to remove a configured extended-tunnel ID.

Command Syntax

```
ext-tunnel-id X:X::X:X
no ext-tunnel-id X:X::X:X
no ext-tunnel-id
```

Parameters

`X:X::X:X`	Extended tunnel identifier for this trunk in IPv6 address format

Default

By default, the LSR-ID of the router is used as the extended-tunnel ID for all sessions.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk t1
(config-trunk)#ext-tunnel-id 1:2::3:4


(config)#rsvp-trunk t1
(config-trunk)#no ext-tunnel-id 1:2::3:4
```

from A.B.C.D

Use this command to specify a “from” IPv4 address for the RSVP daemon. This command can be invoked from either the router rsvp mode or from the rsvp-trunk mode. In the RSVP router mode, this command defines the source address as an IPv4 packet sent out by the RSVP daemon. In the RSVP trunk mode, this command indicates a sender’s address in the sender template object that is used in path messages.

Use the `no` parameter with this command to revert to the default settings.

Command Syntax

```
from A.B.C.D
no from A.B.C.D
no from
```

Parameters

`A.B.C.D`	When in trunk mode, this is the IPv4 address of a tunnel ingress node
`A.B.C.D`	When in router mode, this is the loopback IPv4 address

Default

By default, from A.B.C.D is enabled

Command Mode

Router or Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#from 10.10.0.5

#configure terminal
(config)#router rsvp
(config-router)#from 10.10.0.5
```

from X:X::X:X

Use this command to specify a “from” IPv6 address for the RSVP daemon. This command can be invoked from either the router rsvp mode or from the rsvp-trunk mode. In the router rsvp mode, this command defines the source address as an IPv4 packet being sent out by the RSVP daemon. In the rsvp trunk mode, this command indicates a sender’s address in the sender template object that is used in path messages.

Use the `no` parameter with this command to revert to the default settings.

Command Syntax

```
from X:X::X:X
no from X:X::X:X
```

Parameters

`X:X::X:X`	In trunk mode, this is the address of a tunnel ingress
`X:X::X:X`	In router mode, this is the loopback address

Default

By default, from X:X::X:X is enabled

Command Mode

Router or Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk ipv6
(config-trunk)#from 3ffe::3:34

#configure terminal
(config)#router rsvp
(config-router)#from 3ffe::3:34
```

graceful-restart

Use this command to enable RSVP-TE Graceful Restart capability on a router. This is a global parameter. RSVP-TE determines whether or not to send the graceful restart capability object in its hello message. However, this capability also depends on support for graceful restart on the neighbor router.

The following conditions must be met in order to activate RSVP-TE Graceful Restart:

- This command is used on the local router.
- The neighbor router is explicitly set with a neighbor command (refer to either the neighbor A.B.C.Dor neighborX:X::X:X command for details).
- The neighbor router supports Graceful Restart, and it is activated.

Command Syntax

```
graceful-restart
no graceful-restart
```

Parameters

None

Default

Graceful restart is disabled by default

Command Mode

Router mode

Applicability

This command was introduced before OcNOS-SP version 5.0.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#graceful-restart
(config-router)#no graceful-restart
```

graceful-restart recovery-time

Use this command to set a recovery time for an RSVP-TE graceful restart configuration.

Use the `no` parameter with this command to reset the recovery time.

Command Syntax

```
graceful-restart recovery-time <60000-3600000>
no graceful-restart recovery-time
```

Parameters

`<60000-3600000>` Recovery time value in milliseconds

Default

Default value is 360000 ms.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS-SP version 5.0.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#graceful-restart recovery-time 600000
```

graceful-restart restart-time

Use this command to set a restart time for an RSVP-TE graceful restart configuration.

Use the `no` parameter with this command to reset the restart time.

Command Syntax

```
graceful-restart restart-time <10000-600000>
no graceful-restart restart-time
```

Parameters

`<10000-600000>` Restart time value in milliseconds

Default

Default value is 180000 ms.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS-SP version 5.0.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#graceful-restart restart-time 100000
```

hello-interval

Use this command to set an interval between Hello packets.

Used as a global command, this value is over-ridden by the hello-interval set on the interface (see rsvp hello-interval). For optimum performance, set this value no more than one-third of the hello-timeout value.

Use the `no` parameter with this command to return to the default hello interval value.

Command Syntax

```
hello-interval <1-65535>
no hello-interval
```

Parameter

`<1-65535>`	The time in seconds after which hello packets are sent

Default

By default, hello interval is 2 seconds

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#hello-interval 5

(config)#router rsvp
(config-router)#no hello-interval
```

hello-receipt

Use this command to enable the receipt of Hello messages from peers.

Use the `no` parameter with this command to disable the exchange of Hello messages.

Command Syntax

```
hello-receipt
no hello-receipt
```

Parameters

None

Default

By default, hello receipt is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#hello-receipt
```

hello-timeout

If an LSR has not received a Hello message from a peer within the number of seconds set with this command, all sessions shared with this peer are reset. The hello-timeout determines how long an RSVP node waits for a hello message before declaring a neighbor to be down.

Use the `no` parameter with this command to return to the default hello timeout value.

Command Syntax

```
hello-timeout <1-65535>
no hello-timeout
```

Parameter

`<1-65535>`	Time set to receive a Hello message, in seconds

Default

By default, hello-timeout value is 10 seconds.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#hello-timeout 12

(config)#router rsvp
(config-router)#no hello-timeout
```

keep-multiplier

Use this command to configure the constant to be used to calculate a valid reservation lifetime for a Labeled Switched Path (LSP).

The refresh time and keep multiplier are two interrelated timing parameters used to calculate the valid reservation lifetime for an LSP. Use the following formula to calculate the reservation lifetime for an LSP:

```
L >= (K + 0.5)* 1.5 * R
```

`K` = keep-multiplier

`R` = refresh timer

The router sends refresh messages periodically so that the neighbors do not timeout.

Use the `no` parameter with this command to return to the default keep-multiplier setting.

Command Syntax

```
keep-multiplier <1-255>
no keep-multiplier <1-255>
```

Parameters

`<1-255>`	The keep-multiplier value

Default

By default, keep-multiplier value is 3

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#keep-multiplier 2
```

loop-detection

Use this command to turn on loop detection for Path and Reservation messages exchanged between LSRs.

Use the no-loop-detection command to return to default settings.

Command Syntax

```
loop-detection
```

Parameters

None

Default

By default, loop detection is enabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#loop-detection
```

map-route A.B.C.D

Use this command to map a route using an IPv4 to an RSVP trunk. If the primary LSP for a trunk goes down, all mapped routes are sent automatically to a secondary LSP configured as backup for a primary LSP.

Use the `no` parameter with this command to unmap routes from specified trunks.

Command Syntax

```
map-route A.B.C.D/M
map-route A.B.C.D/M CLASS
map-route A.B.C.D A.B.C.D
map-route A.B.C.D A.B.C.D CLASS
no map-route A.B.C.D/M
no map-route A.B.C.D/M CLASS
no map-route A.B.C.D A.B.C.D
no map-route A.B.C.D A.B.C.D CLASS
```

Parameters

`A.B.C.D/M`	Prefix to map, plus mask
`A.B.C.D`	Prefix to be mapped
`A.B.C.D`	Prefix mask
`CLASS`	Incoming DiffServ Class (for example, be, ef, etc.) to map to the RSVP trunk

Default

By default, map route A.B.C.D/M is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#map-route 2.2.2.2/16
```

map-route X:X::X:X

Use this command to map a route using an IPv6 to an RSVP trunk. If the primary LSP for a trunk goes down, all mapped routes are sent automatically to a secondary LSP configured as backup for a primary LSP.

Use the `no` parameter with this command to unmap routes from specified trunks.

Command Syntax

```
map-route X:X::X:X/M
map-route X:X::X:X/M CLASS
map-route X:X::X:X X:X::X:X
map-route X:X::X:X X:X::X:X CLASS
no map-route X:X::X:X/M
no map-route X:X::X:X/M CLASS
no map-route X:X::X:X X:X::X:X
no map-route X:X::X:X X:X::X:X CLASS
```

Parameters

`X:X::X:X/M`	Prefix to be mapped, plus mask
`X:X::X:X`	Prefix to be mapped
`X:X::X:X`	Prefix map
`CLASS`	Incoming DiffServ Class (for example, be, ef, etc.) to map to the trunk

Default

By default, map route X:XX::X:X/M is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#map-route 1:2::3:4/16
```

neighbor A.B.C.D

Use this command to designate a neighbor IPv4 address to use when exchanging hello messages. Any neighbor hello message that is not explicitly identified is rejected.

Use the `no` parameter with this command to remove an IP neighbor from the system.

Command Syntax

```
neighbor A.B.C.D
no neighbor A.B.C.D
```

Parameters

None

Default

By default, neighbor A.B.C.D is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#neighbor 10.10.0.5
```

neighbor X:X::X:X

Use this command to designate a neighbor IPv6 address to use when exchanging hello messages. Any neighbor hello message that is not explicitly identified is rejected.

Use the `no` parameter with this command to remove an IP neighbor from the system.

Command Syntax

```
neighbor X:X::X:X
no neighbor X:X::X:X
```

Parameters

None

Default

By default, neighbor X:X::X:X is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#neighbor 3ffe::3:34
```

no-cspf

Use this command to disable the use of the Constrained Shortest Path First (CSPF) server for all RSVP sessions. Disable CSPF when no nodes support the required traffic engineering extensions.

When this command is executed in Router mode, CSPF is disabled for all configured RSVP sessions, and all RSVP sessions configured from this point forward. If the default CSPF per RSVP session is enabled, it will be disabled. The CSPF status for RSVP sessions can be verified using the show rsvp session command with the detail option.

Use the cspf command to revert to the default settings.

Command Syntax

```
no-cspf
```

Parameters

None

Default

By default, no cspf is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows using the `no-cspf` command in Router mode to disable CSPF for all RSVP sessions.

```
#configure terminal
(config)#router rsvp
(config-router)#no-cspf
```

no-loop-detection

Use this command to turn off loop detection for Path and Reservation messages exchanged between LSRs. When a Path or Resv message is received, the primary IP address of the incoming interface is compared with the received route record list.

Use the loop-detection command to revert to default settings.

Command Syntax

```
no-loop-detection
```

Parameters

None

Default

By default, no loop detection is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#no-loop-detection
```

no-php

Use this command to disable Penultimate-Hop-Popping (PHP) for the router. An egress router sends either the implicit-null or the explicit-null label for LSPs. hen the `no-php` command is used, the egress router sends non-reserved labels (those labels in the label pool range allotted to RSVP) to the upstream router.

Note: Use the show rsvp command to display the status of Penultimate-Hop-Popping.

Use the php command to revert to default settings.

Command Syntax

```
no-php
```

Parameters

None

Default

By default, Penultimate-Hop-Popping is enabled for standard RSVP LSP.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#no-php
```

no-refresh-path-parsing

Use this command to disable parsing of Refresh PATH messages received from upstream nodes. Enable this command to minimize message processing by RSVP, if you are sure that a particular router does not need to parse Refresh-PATH messages to check for changes because LSPs passing through this router are not required to be updated, simultaneously.

Use the refresh-path-parsing command to revert to the default settings.

Command Syntax

```
no-refresh-path-parsing
```

Parameters

None

Default

By default, refresh-path-parsing is enabled.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
Router#configure terminal
Router(config)#router rsvp
Router(config-router)#no-refresh-path-parsing
```

no-refresh-resv-parsing

Use this command to disable parsing of Refresh RESV messages received from upstream nodes. Enable this command to minimize message processing by RSVP, if you are sure that a particular router does not need to parse Refresh RESV messages to check for changes because LSPs passing through this router are not required to be updated simultaneously.

Command Syntax

```
no-refresh-resv-parsing
```

Parameters

None

Default

By default, refresh reservation parsing is enabled.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
Router#configure terminal
Router(config)#router rsvp
Router(config-router)#no-refresh-resv-parsing
```

php

Use this command to enable Penultimate-Hop-Popping for the router. An egress router sends either the implicit-null or the explicit-null label for LSPs. If the `no-php` command has been enabled, the egress router sends `non-reserved` labels (those labels in the label pool range allotted to RSVP) to the upstream router.

Note: Use the show rsvp command to display the status of Penultimate-Hop-Popping.

Use the no-php command to disable this setting.

Command Syntax

```
php
```

Parameters

None

Default

By default, Penultimate-Hop-Popping is enabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#php
```

primary ADMIN-GROUP-NAME

Use this command to configure primary administrative groups. Administrative groups are manually assigned attributes that describe the color of links, so that links with the same color are in one class. These groups are used to implement different policy-based LSP setups. Administrative group attributes can be included or excluded for an LSP or for a path's primary and secondary paths.

Note: A link can be added to a specific Administrative Group via the Network Services Module. Refer to the *Network Services Module Command Reference* for details.

Use the `no` parameter to remove a previously configured group from an administrative group list.

Command Syntax

```
primary (include-any|include-all|exclude-any) ADMIN-GROUP-NAME
primary (include-any|exclude-any) ADMIN-GROUP-NAME
primary (include-any|include-all|exclude-any) ADMIN-GROUP-NAME
primary (include-any|exclude-any) ADMIN-GROUP-NAME
```

Parameters

`include-any`	Include any attributes
`include-all`	Include all attributes
`exclude-any`	Exclude any attribute
`ADMIN-GROUP-NAME`	Administrative group name

Default

By default, primary admin group name is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary exclude-any myadmingroup

#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary include-all admingrp2

#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary include-any admingrp2
```

primary affinity

Use this command to enable sending of session attribute objects with resource affinity data.

Use the primary no-affinity command to disable sending of session attribute objects.

Command Syntax

```
primary affinity
```

Parameters

None

Default

By default, primary affinity is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary affinity
```

primary bandwidth

Use this command to reserve the primary bandwidth in bits per second for the current trunk.

Each LSP has an associated bandwidth attribute. The bandwidth value is included in the sender's RSVP Path message and specifies the bandwidth to be reserved for the LSP. It is specified in bits per second, with a higher value indicating a greater user traffic volume. A zero bandwidth reserves no resources, although exchanges labels.

Use the `no` parameter to remove configured bandwidth information.

Command Syntax

```
primary bandwidth BANDWIDTH
no primary bandwidth BANDWIDTH
```

Parameter

`BANDWIDTH`	<1-999>k for 1 to 999 kilobits/s
	<1-999>m for 1 to 999 megabits/s
	<1-100>g for 1 to 100 gigabits/s

Default

The default bandwidth is 0 bits per second, which allows data to flow through but does not reserve bandwidth.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary bandwidth 100m
```

primary cspf

Use this command to enable the use of Constrained Shortest Path First (CSPF) server for an explicit route to the egress, or all RSVP sessions. When CSPF is turned off globally, it cannot be enabled for any LSP.

The CSPF server computes paths for LSPs that are subject to constraints such as bandwidth, hop count, administrative groups, priority, and explicit routes. When computing paths for LSPs, CSPF considers not only the topology of the network and the attributes defined for the LSP, but also the links. It attempts to minimize congestion by intelligently balancing the network load.

Use the primary no-cspf command to revert to the default settings.

Command Syntax

```
primary cspf
```

Parameters

None

Default

By default, primary cspf is enabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary cspf
```

primary cspf-retry-limit

Use this command to specify the number of retries that CSPF should carry out for a request received from RSVP.

Use the `no` parameter with this command to disable this configuration.

Command Syntax

```
primary cspf-retry-limit <1-65535>
no primary cspf-retry-limit <1-65535>
no primary cspf-retry-limit
```

Parameter

`<1-65535>`	Set the number of times CSPF should retry for this LSP

Default

By default, retry-limit is 0.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#primary cspf-retry-limit 535

(config)#rsvp-trunk T1
(config-trunk)#no primary cspf-retry-limit
```

primary cspf-retry-timer

Use this command to specify the time between each retry that CSPF might carry out for a request received from RSVP.

Use the `no` parameter with this command to disable this configuration.

Command Syntax

```
primary cspf-retry-timer <1-600>
no primary cspf-retry-timer <1-600>
no primary cspf-retry-timer
```

Parameter

`<1-600>`	Timeout between successive retries, in seconds

Default

By default, retry-timer is 0

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#primary cspf-retry-timer 45

(config)#rsvp-trunk T1
(config-trunk)#no primary cspf-retry-timer 45
```

primary filter

Use this command to set the filter to the fixed or shared style for an LSP.

- The shared filter style identifies a shared reservation environment. It creates a single reservation into which flows from all senders are mixed.
- The fixed filter style designates a distinct reservation. A distinct reservation request is created for data packets from a particular sender. The fixed filter style is also used style to prevent rerouting of an LSP and to prevent another LSP from using this bandwidth.

Use the `no` parameter to reset the configured filter to the default.

Command Syntax

```
primary filter (fixed|shared-explicit)
no primary filter (fixed|shared-explicit)
```

Parameters

`fixed`	Use a fixed filter for this LSP
`shared-explicit`	Use a shared-explicit filter for this LSP

Default

By default, primary filter is fixed

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary filter shared-explicit
```

primary hold-priority

Use this command to configure the hold priority value for the selected trunk. In case of insufficient bandwidth, remove less important existing LSPs to free up a portion of the bandwidth. This can be done by preempting one or more of the signaled LSPs. Hold priority determines the degree to which an LSP holds onto its reservation for a session after the LSP has been configured successfully. When the hold priority is high, the existing LSP is less likely to give up its reservation.

Use the `no` parameter to reset the trunk to the default hold-priority value.

Command Syntax

```
primary hold-priority <0-7>
no primary hold-priority <0-7>
no primary hold-priority
```

Parameter

`<0-7>`	Set a hold priority for the LSP

Default

The default hold-priority value is 0, which is the highest. Once a session is configured with a hold priority of 0, no other session can preempt it.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary hold-priority 2
```

primary hop-limit

Use this command to specify a limit of hops for an RSVP trunk. Hop-limit data is sent to the CSPF server if CSPF is used.

Upon configuration of an arbitrary hop-limit, the hop-limit is compared with the number of hops configured in the primary path, if a primary path has been configured. If the number of hops in the primary path exceeds the hop-limit configured, no `Path` messages are sent, and any existing session is torn down. If no primary path is configured, the trunk is processed normally and Path messages are sent.

Use the `no` parameter to reset the trunk to the default hop-limit value.

Command Syntax

```
primary hop-limit <1-255>
no primary hop-limit <1-255>
no primary hop-limit
```

Parameters

`<1-255>`	Set the number of acceptable hops for the LSP

Default

By default, primary hop limit is 255

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary hop-limit 23
```

primary label-record

Use this command to record all labels exchanged between RSVP-enabled routers during the reservation setup process.

Use the `no` parameter with this command to turn off recording.

Command Syntax

```
primary label-record
no primary label-record
```

Parameters

None

Default

By default, primary label record is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary label-record
```

primary local-protection

Use this command to enable the local repair of explicit routes for which this router is a transit node.

Use the `no` parameter with this command to disable local repair of explicit routes.

Command Syntax

```
primary local-protection
no primary local-protection
```

Parameters

None

Default

By default, primary local protection is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#primary local-protection
```

primary no-affinity

Use this command to disable the use of sending out session attribute objects with resource affinity data.

Use the primary affinity command to return to the default settings.

Command Syntax

```
primary no-affinity
```

Parameters

None

Default

By default, primary no affinity is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary no-affinity
```

primary no-cspf

Use this command to disable the use of Constrained Shortest Path First (CSPF) server for an explicit route to the egress, or all RSVP sessions. When CSPF is turned off globally it cannot be enabled for any LSP. If used per LSP, it can be used to turn off CSPF computation for a specific LSP.

Disable CSPF when all nodes do not support the required traffic engineering extensions, and configure LSPs manually to use an explicit path. The LSP is then established only along the path specified by the operator.

Use the primary cspf command to enable this setting.

Command Syntax

```
primary no-cspf
```

Parameters

None

Default

By default, primary no cspf is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows using the `no-cspf` command in Trunk mode to disable CSPF for the primary LSP.

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary no-cspf
```

primary no-record

Use this command to disable recording of the route taken by Path and Reservation Request (Resv) messages to confirm establishment of reservations and identify errors. Routes are recorded by means of the Route Record Object (RRO) in RSVP messages.

Use the primary record command to return to the default settings.

Command Syntax

```
primary no-record
```

Parameters

None

Default

By default, routes are recorded

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary no-record
```

primary path

Use this command to specify an RSVP path to be used. The `PATHNAME` in this command is the string (name) used to identify an RSVP path defined for the node (refer to `rsvp-path` command).

Use the `no` parameter with this command to remove a configured RSVP path.

Command Syntax

```
primary path PATHNAME
no primary path PATHNAME
no primary path
```

Parameters

`PATHNAME`	The name of the path to use

Default

By default, primary path is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary path mypath
```

primary policer

Use this command to configure policing in hardware for the configured primary bandwidth.

Use the no parameter with this command to remove a policing from hardware.

Command Syntax

```
primary policer
no primary policer
```

Parameters

None

Default

By default, primary policer is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary bandwidth 100m
(config-trunk)#primary policer
(config-trunk)#no primary policer
```

primary record

Use this command to enable recording of the route taken by Path and Reservation Request (Resv) messages to confirm establishment of reservations and identify errors. Routes are recorded by means or the Route Record Object (RRO) in RSVP messages.

Use the primary no-record command to disable recording of routes.

Command Syntax

```
primary record
```

Parameters

None

Default

By default, routes are recorded

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary record
```

primary retry-limit

Use this command to specify a retry count this RSVP Trunk.

If a session is in a `nonexistent` state due to a path error message, the system tries to recreate the LSP for the number of times specified by the `retry-limit` command.

Although the same retry command controls both the trunk and the session, the retry-limit value affects only the session and not the trunk. If the trunk is in an `incomplete` state, the code keeps trying forever to bring it to a `complete` state regardless of the retry-limit value.

Use the `no` parameter with this command to revert to the default retry-limit value.

Command Syntax

```
primary retry-limit <1-65535>
no primary retry-limit <1-65535>
no primary retry-limit
```

Parameter

`<1-65535>`	The set number of times the system should try setting up the LSP

Default

By default, the retry-limit value is 0, and the trunk and session try to create the LSP indefinitely.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary retry-limit 256
```

primary retry-timer

Use this command to specify a retry interval for an RSVP Trunk. When an ingress node tries to configure an LSP and the setup fails due to the receipt of a Path Error message, the system waits for the time configured with this command, before retrying the LSP setup process.

Use the `no` parameter with this command to revert to the default retry-time value.

Command Syntax

```
primary retry-timer <1-600>
no primary retry-timer <1-600>
no primary retry-timer
```

Parameter

`<1-600>`	Time in seconds after which the system should retry setting up the LSP

Default

By default, retry-timer value is 30 seconds.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary retry-timer 12
```

primary reuse-route-record

Use this command to use the updated Route Record List as an Explicit Route (with all strict nodes) when a path message is sent out at the next refresh.

The ERO list contains the hops to be taken to reach the egress from the current LSR. If CSPF is not available, to place an ERO with all strict routes, use this command to modify the ERO after receiving the Resv message. The future Path messages have the ERO with all strict nodes, identifying each and every node to be traversed.

Use the `no` parameter with this command to disable the use of the Route Record List as the explicit route.

Command Syntax

```
primary reuse-route-record
no primary reuse-route-record
```

Parameters

None

Default

By default, primary reuse route record is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary reuse-route-record
```

primary setup-priority

Use this command to configure a setup priority value for a trunk. In case of insufficient bandwidth, users must remove less important LSPs to free up the bandwidth. This can be done by preempting one or more of the existing LSPs. The primary setup priority determines if a new LSP can preempt an existing LSP.

The setup priority of the new LSP must be higher than the hold priority of an existing LSP for the existing LSP to be preempted. Note that for a trunk, the setup priority should not be higher than the hold priority.

Use the `no` parameter with this command to revert to the default primary setup priority value.

Command Syntax

```
primary setup-priority <0-7>
no primary setup-priority <0-7>
no primary setup-priority
```

Parameters

`<0-7>`	Set the priority value

Default

By default, setup priority is 7, which is the lowest.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary setup-priority 2
```

primary traffic

Use this command to specify the traffic type for this RSVP Trunk.

Use the `no` parameter with this command to reset the configured traffic type.

Command Syntax

```
primary traffic (guaranteed|controlled-load)
no primary traffic (guaranteed|controlled-load)
no primary traffic
```

Parameters

`controlled-load` Controlled loaded traffic

`guaranteed` Guaranteed traffic

Default

By default, primary traffic type is controlled-load

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#primary traffic guaranteed
```

refresh-time

Use this command to configure RSVP refresh interval timer. The timer specifies the interval after which Path and/ or Reservation Request (Resv) messages will be sent out.

The refresh time and keep multiplier are two interrelated timing parameters used to calculate the valid Reservation Lifetime for an LSP. Refresh time regulates the interval between Refresh messages which include Path and Reservation Request (Resv) messages. Refresh messages are sent periodically so that reservation does not timeout in the neighboring nodes. Each sender and receiver host sends Path and Resv messages, downstream and upstream respectively, along the paths.

Use the `no` parameter with this command to return to the default refresh-time interval.

Command Syntax

```
refresh-time <1-65535>
no refresh-time <1-65535>
no refresh-time
```

Parameter

`<1-65535>`	The duration for which messages are sent, in seconds

Default

By default, refresh-time interval is 30 seconds

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#refresh-time 20
```

refresh-path-parsing

Use this command to disable parsing of Refresh PATH messages received from upstream nodes. Use this command to minimize message processing by RSVP when you are sure that a particular router does not need to parse Refresh-PATH messages to check for changes, because LSPs passing through this router are not required to be updated simultaneously.

Use the no-refresh-path-parsing command to disable this setting.

Command Syntax

```
refresh-path-parsing
```

Parameters

None

Default

By default, refresh-path-parsing is enabled.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
Router#configure terminal
Router(config)#router rsvp
Router(config-router)#refresh-path-parsing
```

refresh-resv-parsing

Use this command to disable parsing of Refresh RESV messages received from upstream nodes. Use this command to minimize message processing by RSVP when you are sure that a particular router does not need to parse Refresh RESV messages to check for changes because LSPs passing through this router are not required to be updated simultaneously.

Use the no-refresh-resv-parsing command to disable this setting.

Command Syntax

```
refresh-resv-parsing
```

Parameters

None

Default

By default, refresh reservation parsing is enabled.

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
Router#configure terminal
Router(config)#router rsvp
Router(config-router)#refresh-resv-parsing
```

restart rsvp graceful

Use this command to restart RSVP gracefully.

To restart RSVP gracefully, you must give the graceful-restart command to enable graceful restart capability on the device in RSVP router mode.

Command Syntax

```
restart rsvp graceful
```

Parameter

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS-SP version 5.0.

Example

```
#restart rsvp graceful
% Warning : You may loose rsvp configuration, if not saved
Proceed for graceful restart? (y/n):y
%% Managed module is down or crashed
```

router rsvp

Use this command to enter router mode from configure mode and to enable the RSVP daemon, if it is not already enabled.

Use the `no` parameter with this command to disable RSVP on the node.

Command Syntax

```
router rsvp
no router rsvp
```

Parameters

None

Default

RSVP is started only if this command is executed.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The command prompt changes from config to config-router, as illustrated below:

```
#configure terminal
(config)#router rsvp
(config-router)#

(config-router)#exit
(config)#no router rsvp
```

rsvp hello-interval

Use this command to enable the sending of Hello packets on the interface and to set the interval value between successive Hello packets to neighbor. For optimum performance, set this value to less than one-third the value of the configured RSVP hello-timeout. See the rsvp hello-timeout command for more information.

Note: This is an interface-specific command and when not used, the global hello-interval state applies.

Use the `no` parameter with this command to return to the default hello interval value.

Command Syntax

```
rsvp hello-interval <1-65535>
no rsvp hello-interval
```

Parameter

`<1-65535>`	RSVP hello interval in seconds

Default

By default, RSVP hello interval is 2 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#rsvp hello-interval 110

(config)#interface eth0
(config-if)#no rsvp hello-interval
```

rsvp hello-receipt

Use this command to enable the receipt of hello messages from peers connected through this interface. This is an interface-specific command and when not used, the global hello-receipt command applies.

Use the `no` parameter with this command to disable the exchange of hello messages for this interface.

Command Syntax

```
rsvp hello-receipt
no rsvp hello-receipt
```

Parameters

None

Default

By default, rsvp hello receipt is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#rsvp hello-receipt
```

rsvp hello-timeout

This command determines how long an RSVP node should wait for a hello message before declaring a neighbor to be down. If an LSR does not received a hello message from a peer connected to an interface within the specified duration, the LSR resets all sessions that are shared with this particular peer. This is an interface-specific command and when not used, the global hello-timeout command applies.

Use the `no` parameter to revert to the default hello timeout value.

Command Syntax

```
rsvp hello-timeout <1-65535>
no rsvp hello-timeout
```

Parameters

`<1-65535>`	Time to receive a hello message, in seconds

Default

By default, hello-timeout value is 10 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#rsvp hello-timeout 550

(config)#interface eth0
(config-if)#no rsvp hello-timeout
```

rsvp keep-multiplier

This command sets the constant for calculating a valid reservation lifetime for an LSP, which allows messages to be exchanged through this interface. This is an interface-specific command and when not specified, the global keep-multiplier command applies.

Reservation lifetime is the duration of bandwidth reservation for the LSP. The refresh time and keep multiplier are two interrelated timing parameters used to calculate the valid reservation lifetime for an LSP. Use the following formula to calculate the reservation lifetime for an LSP:

```
L >= (K + 0.5)* 1.5 * R
```

`K` = keep-multiplier

`R` = refresh timer

Refresh messages are sent periodically so that neighbors do not timeout.

Use the `no` parameter with this command to return to the global keep-multiplier value.

Command Syntax

```
rsvp keep-multiplier <1-255>
no rsvp keep-multiplier <1-255>
```

Parameter

`<1-255>`	Set a value for the lifetime constant

Default

By default RSVP keep-multiplier value is 3

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#rsvp keep-multiplier 3

(config)#interface eth0
(config-if)#no rsvp keep-multiplier 3
```

rsvp refresh-time

Use this command to configure RSVP refresh interval timer for the current interface. This is an interface-specific command and when not used, the global refresh-time command applies.

The refresh time and keep multiplier are two interrelated timing parameters used to calculate the valid reservation lifetime for an LSP. Refresh time regulates the interval between refresh messages that include path and reservation request (Resv) messages. Refresh messages are sent periodically so that the reservation does not timeout in the neighboring nodes. Each sender and receiver host sends path and resv messages, downstream and upstream respectively, along the paths.

Use the `no` parameter with this command to revert to the refresh-time value set in RSVP mode.

Command Syntax

```
rsvp refresh-time <1-65535>
no rsvp refresh-time <1-65535>
```

Parameter

`<1-65535>`	The duration for which messages are sent, in seconds

Default

By default, refresh interval is 30 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#rsvp refresh-time 5055

(config)#interface eth0
(config-if)#no rsvp refresh-time 5055
```

rsvp-path

Use this command to create a new RSVP path or to enter the `Path` command mode. In this mode, you can add or delete paths and also specify the path to be loose or strict.

Use the `no` parameter with this command to delete the path and its specified hops.

Command Syntax

```
rsvp-path PATHNAME
no rsvp-path PATHNAME
```

Parameter

`PATHNAME`	Name of the path

Default

By default, rsvp path is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-path mypath
(config-path)#
```

rsvp-trunk

Use this command to create a new RSVP trunk. When the trunk is created, the attributes required to configure an explicitly-routed or traditionally-routed LSP are set. Once a trunk is configured with the required attributes, an RSVP session (and PSB) is created for this trunk, which enables the exchange of messages and completes the LSP setup.

This command also modifies an existing RSVP path to configure an explicitly-routed or traditionally-routed LSP. In addition, this command can be used to set the address family (IPv4 or IPv6) of an RSVP trunk. If no address family is assigned, the default value is used. If the address family is already set, a check is made to see whether the address family configured and the one already in the database are the same. An error message is returned if the two do not match.

Use the `no` parameter with this command to remove an RSVP trunk and all configured attributes, except the primary path.

Note: The RSVP trunk's name (`TRUNKNAME`) is limited to 32 characters.

Command Syntax

```
rsvp-trunk TRUNKNAME (ipv4|ipv6)
no rsvp-trunk TRUNKNAME
```

Parameters

`TRUNKNAME`	Name to use for the trunk
`ipv4`	IPv4 address family trunk
`ipv6`	IPv6 address family trunk

Default

By default, rsvp trunk is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The command prompt changes from `config` to `config-trunk` as illustrated below:

```
#configure terminal
(config)#rsvp-trunk mytrunk ipv4
(config-trunk)#
```

rsvp-trunk-restart

Use this command to restart the RSVP trunk. This command “kills” an existing LSP and restarts the LSP setup process.

Command Syntax

```
rsvp-trunk-restart
```

Parameters

None

Default

By default, rsvp trunk restart is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#rsvp-trunk-restart
```

secondary ADMIN-GROUP-NAME

Use this command to configure secondary administrative groups. Administrative groups are manually assigned attributes that describe the color of links, so that links with the same color are in one class. These groups are used to implement different policy-based LSP setups. Administrative group attributes can be included or excluded for an LSP or for a path's primary and secondary paths.

Note: A link can be added to a specific Administrative Group via NSM. Refer to the *Network Services Module Command Reference* for details.

Use the `no` parameter to remove a previously set group from an administrative group list.

Command Syntax

```
secondary (include-any|include-all|exclude-any) ADMIN-GROUP-NAME
secondary (include-any|exclude-any) ADMIN-GROUP-NAME
no secondary (include-any|include-all|exclude-any) ADMIN-GROUP-NAME
no secondary (include-any|exclude-any) ADMIN-GROUP-NAME
```

Parameters

`include-any`	Include any attribute
`include-all`	Include all attribute
`exclude-any`	Exclude any attribute
`ADMIN-GROUP-NAME`	Administrative group name

Default

By default, secondary admin group name is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary exclude-any myadmingroup

#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary include-any myadmingroup

#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary include-all myadmingroup
```

secondary bandwidth

Use this command to reserve the bandwidth in bits per second for the current trunk.

Each LSP has an associated bandwidth attribute. The bandwidth value is included in the sender's RSVP Path message and specifies the bandwidth to be reserved for the LSP. It is set in bits per second, with a higher value indicating a greater user traffic volume. A zero bandwidth reserves no resources, although label exchanges are possible.

Use the `no` parameter with this command to unset the configured bandwidth information.

Command Syntax

```
secondary bandwidth BANDWIDTH
no secondary bandwidth BANDWIDTH
no secondary bandwidth
```

Parameter

`BANDWIDTH`	<1-999>k for 1 to 999 kilobits/s
	<1-999>m for 1 to 999 megabits/s
	<1-100>g for 1 to 100 gigabits/s

Default

By default, bandwidth is 0 bits per second, which allows data to flow through but does not reserve bandwidth.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary bandwidth 100m
```

secondary cspf

Use this command to enable the use of Constrained Shortest Path First (CSPF) server for an explicit route to the egress, or all RSVP sessions.

The CSPF server computes paths for LSPs that are subject to constraints such as bandwidth, hop count, administrative groups, priority, and explicit routes. When computing paths for LSPs, CSPF considers not only the topology of the network and the attributes defined for the LSP, but also the links. It attempts to minimize congestion by intelligently balancing the network load.

Use the secondary no-cspf command to revert to the default settings.

Command Syntax

```
secondary cspf
```

Parameters

None

Default

By default, secondary cspf is enabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows using the `no-cspf` command in Trunk mode to disable CSPF for the primary LSP.

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary cspf
```

secondary cspf-retry-limit

Use this command to specify the number of retries that CSPF should carry out for a request received from RSVP.

Use the `no` parameter with this command to remove this configuration.

Command Syntax

```
secondary cspf-retry-limit <1-65535>
no secondary cspf-retry-limit <1-65535>
no secondary cspf-retry-limit
```

Parameter

`<1-65535>`	The number of times CSPF should retry for this LSP

Default

By default, no retry limit for CSPF route calculations is configured, so the value is 0.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#secondary cspf-retry-limit 535
```

secondary cspf-retry-timer

Use this command to specify the time between each retry that CSPF might carry out for a request received from RSVP.

Use the `no` parameter with this command to remove this configuration.

Command Syntax

```
secondary cspf-retry-timer <1-600>
no secondary cspf-retry-timer <1-600>
no secondary cspf-retry-timer
```

Parameters

`<1-600>`	Timeout between successive retries, in seconds

Default

By default, no retry-timer configuration is defined for CSPF calculations, so the value is set to 0.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#secondary cspf-retry-timer 45
```

secondary filter

Use this command to set the filter to fixed or shared filter style for RSVP trunk.

- The shared filter style identifies a shared reservation environment. It creates a single reservation into which flows from all senders are mixed.
- The fixed filter style designates a distinct reservation. A distinct reservation request is created for data packets from a particular sender. The fixed filter style is also used style to prevent rerouting of an LSP and to prevent another LSP from using this bandwidth.

Use the `no` parameter to reset the configured filter to the default style.

Command Syntax

```
secondary filter (fixed|shared-explicit)
no secondary filter (fixed|shared-explicit)
no secondary filter
```

Parameters

`fixed`	Use a Fixed Filter for this RSVP Trunk.
`shared-explicit`	Use a Shared Explicit Filter for this RSVP Trunk.

Default

By default, secondary filter is fixed style

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Usage

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary filter shared-explicit
```

secondary hold-priority

Use this command to configure the hold priority value for the selected trunk.

In case of insufficient bandwidth, the user must remove any less important existing LSP to free up the bandwidth. This can be done by preempting one or more of the signaled LSPs. Hold priority determines the degree to which an LSP holds onto its reservation for a session after the LSP has been configured successfully. When the hold priority is high, the existing LSP is less likely to give up its reservation.

Use the `no` parameter to revert to the default hold-priority value.

Command Syntax

```
secondary hold-priority <0-7>
no secondary hold-priority <0-7>
no secondary hold-priority
```

Parameter

`<0-7>`	Specify a value for hold priority

Default

The default hold-priority is 0, the highest value. Once a session is configured with a 0 hold priority value, no other session can preempt it.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary hold-priority 2
```

secondary hop-limit

Use this command to specify a limit of hops for an RSVP trunk.

Upon configuration of an arbitrary hop-limit, the hop-limit is compared with the number of hops configured in the primary path, if a primary path has been configured. If the number of hops in the primary path exceed the hop-limit configured, no path messages are sent out and any existing session is torn down. If no primary path is configured, the trunk is processed normally and the path messages are sent out. The hop-limit data is sent to the CSPF server, if CSPF is being used.

Use the `no` parameter to revert to the default hop-limit value.

Command Syntax

```
secondary hop-limit <1-255>
no secondary hop-limit <1-255>
no secondary hop-limit
```

Parameter

`<1-255>`	The number of acceptable hops

Default

By default, secondary hop limit is 255

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary hop-limit 23
```

secondary label-record

Use this command to record all labels exchanged between RSVP enabled routers during the reservation setup process. This command records all labels exchanged for an LSP from the ingress to the egress, and helps with debugging.

Use the `no` parameter to turn off recording.

Command Syntax

```
secondary label-record
no secondary label-record
```

Default

By default, secondary label record is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary label-record
```

secondary local-protection

Use this command to enable the local repair of explicit routes for which this router is a transit node.

Use the `no` parameter with this command to disable local repair of explicit routes.

Command Syntax

```
secondary local-protection
no secondary local-protection
```

Parameters

None

Default

By default, secondary local protection is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#secondary local-protection
```

secondary no-affinity

Use this command to disable the use of sending out session attribute objects with resource affinity data.

Use the secondary bandwidth command to revert to the default settings.

Command Syntax

```
secondary no-affinity
```

Parameters

None

Default

By default, secondary no affinity is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary no-affinity
```

secondary no-cspf

Use this command to disable the use of Constrained Shortest Path First (CSPF) server for an explicit route to the egress, or all RSVP sessions.

If CSPF is turned off globally, it cannot be enabled for any LSP. If used per LSP, it can be used to turn off CSPF computation for a specific LSP. The CSPF server computes paths for LSPs that are subject to various constraints such as bandwidth, hop count, administrative groups, priority, and explicit routes. When computing paths for LSPs, CSPF considers not only the topology of the network and the attributes defined for the LSP, but, also the links. It attempts to minimize congestion by intelligently balancing the network load.

Disable CSPF when all nodes do not support the required traffic engineering extensions and configure LSPs manually to use an explicit path. The LSP is then established only along the path specified by the operator.

Use the secondary cspf command to revert to the default settings.

Command Syntax

```
secondary no-cspf
```

Parameters

None

Default

By default, secondary no cspf is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows using the `no-cspf` command in Trunk mode to disable CSPF for the primary LSP.

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary no-cspf
```

secondary no-record

This command is used to disable recording of the route taken by path and resv messages and confirms the establishment of reservations and to identify errors. Routes are recorded by means of the route record object (RRO) in an RSVP message.

Use the secondary record command to revert to the default settings.

Command Syntax

```
secondary no-record
```

Parameters

None

Default

By default, routes are recorded

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary no-record
```

secondary path

Use this command to specify an RSVP path to be used.

Use the `no` parameter with this command to remove a configured RSVP path.

Command Syntax

```
secondary path PATHNAME
no secondary path PATHNAME
no secondary path
```

Parameters

`PATHNAME`	The name of the path to be used. `PATHNAME` is a string (name) used to identify an RSVP path defined for the node (refer to the rsvp-path command).

Default

By default, secondary path is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary path mypath
```

secondary policer

Use this command to configure policing in hardware for the configured secondary bandwidth.

Use the no parameter with this command to remove a policing from hardware.

Command Syntax

```
secondary policer
no secondary policer
```

Parameters

None

Default

By default, secondary policer is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary bandwidth 200m
(config-trunk)#secondary policer
(config-trunk)#no secondary policer
```

secondary record

This command is used to enable recording of the route taken by path and resv messages to confirm the establishment of reservations and to identify errors. Routes are recorded by means of the route record object (RRO) in RSVP messages.

Use the secondary no-record command to revert to the default settings.

Command Syntax

```
secondary record
```

Parameters

None

Default

By default, routes are recorded

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary record
```

secondary retry-limit

Use this command to specify a retry count this RSVP Trunk.

If a session is in a nonexistent state due to the receipt of a path error message, it tries to recreate the LSP for the number of times specified by primary retry-limit. Although the same retry command controls both the trunk and the session, the retry-limit value affects only the session and not the trunk. If the trunk is in an incomplete state, the code keeps trying to bring it to a complete state, irrespective of the retry-limit value.

Use the `no` parameter to revert to the default retry-limit value.

Command Syntax

```
secondary retry-limit <1-65535>
no secondary retry-limit <1-65535>
```

Parameter

`<1-65535>`	The set number of times the system should try setting up the LSP

Default

By default, the retry-limit value is 0 so the trunk and session try to create the LSP indefinitely.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary retry-limit 256
```

secondary retry-timer

Use this command to specify a retry interval for an RSVP Trunk. When the ingress tries to configure an LSP and the setup fails due to the receipt of a path error message, the system waits for the time configure by this command before retrying the LSP setup process.

Use the `no` parameter to revert to the default.

Command Syntax

```
secondary retry-timer <1-600>
no secondary retry-timer <1-600>
no secondary retry-timer
```

Parameter

`<1-600>`	Interval after which the system should retry setting up the LSP, in seconds

Default

By default, retry time is 30 seconds

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary retry-timer 12
```

secondary reuse-route-record

Use this command to use the updated route record list as an explicit route (with all strict nodes) when a path message is sent out at the next refresh.

An explicit route object (ERO) list contains the hops to be taken to reach the egress from the current LSR. If CSPF can not place an ERO with all strict routes, then this command helps modify the ERO after receiving resv messages. Future path messages have the ERO with all strict nodes, which identify each and every node to be traversed.

Use the `no` parameter to disable the use of the route record list as the explicit route.

Command Syntax

```
secondary reuse-route-record
no secondary reuse-route-record
```

Parameters

None

Default

By default, secondary reuse route record is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary reuse-route-record
```

secondary setup-priority

Use this command to configure a setup priority value for this trunk.

In case of insufficient bandwidth, the user must remove any less important LSPs to free up bandwidth. This can be done by preempting one or more of the existing LSPs. The setup priority determines whether a new LSP that preempts an existing LSP may be established. The setup priority of the new LSP must be higher than the hold priority of an existing LSP for the existing LSP to be preempted. Note that for a trunk, the setup priority should not be higher than the hold priority.

Use the `no` parameter with this command to revert to the default setup priority value.

Command Syntax

```
secondary setup-priority <0-7>
no secondary setup-priority <0-7>
```

Parameters

`<0-7>`	The priority value

Default

By default, setup value is 7 (the lowest).

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary setup-priority 2
```

secondary traffic

Use this command to identify the traffic type for this RSVP Trunk.

Use the `no` parameter with this command to unset the configured traffic type.

Command Syntax

```
secondary traffic (guaranteed|controlled-load)
no secondary traffic (guaranteed|controlled-load)
no secondary traffic
```

Parameters

`guaranteed`	Guaranteed traffic
`controlled-load`	Controlled load traffic

Default

Controlled load is the default traffic type.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#secondary traffic guaranteed
```

snmp restart rsvp

Use this command to restart SNMP in Resource Reservation Protocol -Traffic Engineering (RSVP-TE)

Command Syntax

```
snmp restart rsvp
```

Parameters

None

Default

By default, snmp restart rsvp is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#snmp restart rsvp
```

to A.B.C.D

Use this command to specify an IPv4 egress for an LSP. When configuring an LSP, you must specify the address of the egress router by using this command in the trunk node. An egress definition is a mandatory attribute; no RSVP session is created when an egress is not defined.

Use the `no` parameter with this command to unset the configured egress address.

Command Syntax

```
to A.B.C.D
no to A.B.C.D
```

Parameters

None

Default

The operator must specify an egress for LSP initialization to begin.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#to 10.10.0.5
```

to X:X::X:X

Use this command to specify an IPv6 egress for an LSP. When configuring an LSP, you must specify the address of the egress router by using this command in the trunk node. An egress definition is a mandatory attribute; no RSVP session is created when an egress is not defined.

Use the `no` parameter with this command to unset the configured egress address.

Command Syntax

```
to X:X::X:X
no to X:X::X:X
```

Parameters

None

Default

The operator must specify an egress for LSP initialization to begin.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk ipv6
(config-trunk)#to 3ffe::3:34
```

update-type

Use this command to change the method of updating attributes for sessions (primary/ secondary) for this trunk.

- If make-before-break is configured (default type), a new LSP is created for each attribute update. When the new LSP becomes operational, the original LSP is torn down.
- If break-before-make is configured, the existing LSP is torn down and restarted for each attribute update.

Use the `no` parameter with this command to remove an update type.

Command Syntax

```
update-type (make-before-break|break-before-make)
update-type (make-before-break|break-before-make)
no update-type (make-before-break|break-before-make)
no update-type (make-before-break|break-before-make)
no update-type
```

Parameters

`make-before-break`

Make before break update

`break-before-make`

Break before make update

Default

By default, make-before-break types of updates are carried out.

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#update-type break-before-make

#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#update-type make-before-break
```

X:X::X:X

Use this command to define an explicit IPv6 route sub-object as either loose or strict. A list of sub-objects specifies an explicit route to the egress router for an LSP.

- For the strict type of route addresses, the route taken from the previous router to the current router must be a directly-connected path and a message exchanged between the two routers should not pass any intermediate routers. This ensures that routing is enforced on the basis of each link.
- For the loose type of route addresses, the route taken form the previous router to the current router need not be a direct path and a message exchanged between the two routers can pass other routers.

Use the `no` parameter with this command to disable the configuration.

Command Syntax

```
X:X::X:X
X:X::X:X (loose|strict)
no X:X::X:X
no X:X::X:X (loose|strict)
```

Parameters

`loose`	Make this node loose
`strict`	Make this node strict

Default

By default, X:X::X:X is disabled

Command Mode

Path mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-path mypath
(config-path)#3ffe::3:34 strict
```

CHAPTER 2 Fast Reroute Commands

This chapter describes the RSVP-TE Fast Reroute commands.

default-frr-protection

Use this command to configure the default method of fast reroute protection when sender has not specified a method via FRR object but asked for local protection. This command is particularly useful with interop with Cisco as Cisco doesn't send FRR object in path message. By default, default FRR protection considered to be one-to-one in OcNOS and in case of interop with Cisco where default protection needed is facility, this command shall be configured on all OcNOS devices in the network.

Note: Having this command configured in one OcNOS device and not configured in other OcNOS device in the network will cause unpredictable behavior as RFC recommendation for merge node behavior of facility and one-to-one are different.

Note: This command is applicable only when path message contains local protection flag set but doesn't contain FRR object. When FRR object mentions protection type explicitly, this command is not applicable and also, if path message doesn't request local protection, then also this command is not applicable.

Command Syntax

```
default-frr-protection (one-to-one | facility)
no default-frr-protection
```

Parameters

`facility`	Facility Backup (Bypass) protection
`one-to-one`	One-to-One protection mechanism

Default

By default, if local protection requested but FRR object not available, one-to-one protection is considered.

Command Mode

Router mode

Applicability

This command was introduced in OcNOS version 6.3.1.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)# default-frr-protection facility
(config-router)# commit
(config-router)# no default-frr-protection
(config-router)# commit
```

detour-identification

Use this command to set a path-specific detour LSP identification method, using the detour object.

Use the no parameter with this command to unset the detour LSP identification method.

Note: This command helps identify the backup LSP identification method for one-to-one protection only.

Command Syntax

```
detour-identification (path|sender-template)
no detour-identification (path|sender-template|)
```

Parameters

`path`	Set a path-specific detour identification method
`sender-template`	Set a sender template-specific detour identification method

Default

By default, detour identification is sender template

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#detour-identification path

#configure terminal
(config)#router rsvp
(config-router)#detour-identification sender-template

#configure terminal
(config)#router rsvp
(config-router)#no detour-identification path

#configure terminal
(config)#router rsvp
(config-router)#no detour-identification sender-template
```

from X:X::X:X

Use this command to specify a “from” IPv6 address for tunnel ingress.

Use the `no` parameter with this command to remove an IPv6 address from tunnel ingress.

Command Syntax

```
from X:X::X:X
no from X:X::X:X
no from
```

Parameters

None

Default

By default, from X:X::X:X is disabled

Command Mode

Router mode or Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk mytrunk
(config-trunk)#from 3ffe::3:34

#configure terminal
(config)#router rsvp
(config-router)#from 3ffe::3:34
```

primary fast-reroute bandwidth

Use this command to set the detour LSP bandwidth.

Note: This command helps identify attributes of the FRR backup LSP for the one-to-one protection method.

Use the `no` parameter with this command to unset fast-reroute LSP bandwidth.

Command Syntax

```
primary fast-reroute bandwidth BANDWIDTH
no primary fast-reroute bandwidth BANDWIDTH
no primary fast-reroute BANDWIDTH
```

Parameter

`BANDWIDTH`	<1-999>k for 1 to 999 kilobits/s
	<1-999>m for 1 to 999 megabits/s
	<1-100>g for 1 to 100 gigabits/s

Default

By default, primary fast reroute bandwidth is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#primary fast-reroute bandwidth 10000000
```

primary fast-reroute hold-priority

Use this command to set the hold-priority for a detour LSP.

Note: This command helps identify attributes of the FRR backup LSP for the one-to-one protection method.

Use the `no` parameter with this command to unset the detour LSP hold-priority.

Command Syntax

```
primary fast-reroute hold-priority <0-7>
no primary fast-reroute hold-priority (<0-7>|)
```

Parameter

`<0-7>`	Set the value for hold-priority

Default

By default, primary fast reroute hold priority is 0

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#primary fast-reroute hold-priority 3
```

primary fast-reroute hop-limit

Use this command to set the hop-limit for a detour LSP.

Note: This command helps identify attributes of the FRR backup LSP for the one-to-one protection method.

Use the `no` parameter with this command to unset the detour LSP hop-limit.

Command Syntax

```
primary fast-reroute hop-limit <1-255>
no primary fast-reroute hop-limit (<1-255>|)
```

Parameter

`<1-255>`	Set the number of hops

Default

By default, primary fast reroute hop limit is 255

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#primary fast-reroute hop-limit 25
```

primary fast-reroute node-protection

Use this command to set node protection.

Note: This command helps identify attributes of the FRR backup LSP for the one-to-one protection method.

Use the `no` parameter with this command to remove node protection.

Command Syntax

```
primary fast-reroute node-protection
no primary fast-reroute node-protection
```

Parameters

None

Default

By default, primary fast reroute node protection is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#primary fast-reroute node-protection
```

primary fast-reroute protection

Use this command to create an Fast Reroute backup and to set an LSP one-to-one protection mechanism.

Note: This command helps identify attributes of the FRR backup LSP for the one-to-one protection method.

Use the `no` parameter with this command to remove LSP protection mechanism.

Parameters

None

Command Syntax

```
primary fast-reroute protection (one-to-one | facility)
no primary fast-reroute protection (one-to-one | facility)
```

Parameters

`one-to-one`	Set the one-to-one protection mechanism
`facility`	Facility backup (bypass) protection

Default

By default, primary fast reroute protection is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#primary fast-reroute protection one-to-one
```

primary fast-reroute setup-priority

Use this command to configure a setup-priority for the detour LSP.

Note: This command helps identify attributes of the FRR backup LSP for the one-to-one protection method.

Use the `no` parameter with this command to remove the detour LSP setup-priority.

Command Syntax

```
primary fast-reroute setup-priority <0-7>
no primary fast-reroute setup-priority (<0-7>|)
```

Parameter

`<0-7>`	Set a value for setup priority

Default

By default, primary fast reroute setup priority is 0

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#primary fast-reroute setup-priority 2
```

CHAPTER 3 Refresh Reduction Commands

This chapter describes the RSVP-TE Refresh Reduction commands:

ack-wait-timeout

Use this command to configure the acknowledgement wait timeout for all RSVP-TE neighbors.

Use the `no` parameter with this command to revert to the default acknowledgement wait timeout.

Command Syntax

```
ack-wait-timeout <1-65535>
no ack-wait-timeout <1-65535>
no ack-wait-timeout
```

Parameter

`<1-65535>`	Specify a value for the acknowledgement wait timeout in seconds. The default timeout value is 10 seconds.

Default

By default, ack wait timeout is 10 seconds

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#ack-wait-timeout 5

(config)#router rsvp
(config-router)#no ack-wait-timeout 5
```

message-ack

Use this command to enable message acknowledgment for all messages being sent to neighbors that are known to support refresh reduction.

Use the `no` parameter with this command to disable message acknowledgment for all messages being sent to neighbors.

Command Syntax

```
message-ack
no message-ack
```

Parameters

None

Default

By default, Message Acknowledgment is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#message-ack

(config)#router rsvp
(config-router)#no message-ack
```

refresh-reduction

Use this command to enable refresh reduction capability advertisement for all interfaces.

Use the `no` parameter with this command disable refresh reduction capability advertisement for all interfaces.

Command Syntax

```
refresh-reduction
no refresh-reduction
```

Parameters

None

Default

By default, Refresh reduction mechanism is enabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#refresh-reduction

(config)#router rsvp
(config-router)#no refresh-reduction
```

rsvp ack-wait-timeout

Use this command to configure the acknowledgment wait timeout for all neighbors detected via the specific interface.

Use the `no` parameter with this command to revert to the default acknowledgment wait timeout for the specified interface.

Command Syntax

```
rsvp ack-wait-timeout <1-65535>
no rsvp ack-wait-timeout <1-65535>
no rsvp ack-wait-timeout
```

Parameters

`<1-65535>`	Specify a value for the acknowledgment wait timeout in seconds. The default timeout value is 10 seconds.

Default

By default, rsvp ack wait timeout is 10 seconds

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#rsvp ack-wait-timeout 5

(config)#interface eth0
(config-if)#no rsvp ack-wait-timeout 5
```

rsvp message-ack

Use this command to enable message acknowledgment for all messages being sent to the neighbors that have been detected via the specific interface.

Use the `no` parameter with this command to disable message acknowledgment for all messages being sent to the neighbors that have been detected via the specified interface.

Command Syntax

```
rsvp message-ack
```

```
no rsvp message-ack
```

Parameters

None

Default

By default, Message Acknowledgment is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#rsvp message-ack

(config)#interface eth0
(config-if)#no rsvp message-ack
```

rsvp refresh-reduction

Use this command to enable Refresh Reduction capability advertisement for a specific interface.

Use the `no` parameter with this command disable Refresh Reduction capability advertisement for the specified interface.

Command Syntax

```
rsvp refresh-reduction
no rsvp refresh-reduction
```

Parameters

None

Default

Refresh Reduction mechanism is enabled by default for all interfaces.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#rsvp refresh-reduction

(config)#interface eth0
(config-if)#no rsvp refresh-reduction
```

CHAPTER 4 Facility Backup Commands

This chapter describes the RSVP-TE bypass commands for facility backup protection

backup-bw-type

Use this command to select the bypass trunk bandwidth support type.

Bypass trunks of dedicated bandwidth type will serve only bandwidth protections requested LSPs. The total bandwidth requirement of served LSPs will be less than or equal to the bandwidth configured on the bypass trunk. If an LSP with bandwidth protection and higher setup priority requests protection and bypass doesn't have sufficient bandwidth available, then LSPs with lower hold priority will be preempted to serve the LSP with higher setup priority.

Use the `no` parameter to remove configured backup bandwidth type.

Command Syntax

```
backup-bw-type (dedicated | best-effort)
no backup-bw-type
```

Parameters

`dedicated`	Dedicated backup bandwidth support
`best-effort`	Best effort backup bandwidth support

Default

best-effort

Command Mode

Bypass mode

Applicability

This command was introduced in OcNOS version 6.3.0.

Examples

```
#configure terminal
(config)#rsvp-bypass bp1
(config-bypass)#backup-bw-type dedicated
```

bandwidth

Use this command to reserve the bypass bandwidth in bits per second for the current trunk.

Each LSP has an associated bandwidth attribute. The bandwidth value is included in the sender's RSVP Path message and specifies the bandwidth to be reserved for the LSP. It is specified in bits per second, with a higher value indicating a greater user traffic volume. A zero bandwidth reserves no resources, although exchanges labels.

Use the `no` parameter to remove configured bandwidth information.

Command Syntax

```
bandwidth BANDWIDTH
no bandwidth BANDWIDTH
no bandwidth
```

Parameter

`BANDWIDTH`	<1-999>k for 1 to 999 kilobits/s
	<1-999>m for 1 to 999 megabits/s
	<1-100>g for 1 to 100 gigabits/s

Default

The default bandwidth is 0 bits per second, which allows data to flow through but does not reserve bandwidth.

Command Mode

Bypass mode

Applicability

This command was introduced in OcNOS version 6.3.0.

Examples

```
#configure terminal
(config)#rsvp-bypass bp1
(config-bypass)#bandwidth 100m
(config-bypass)#no bandwidth
```

bypass-lsp-addr-query-interval

Use this command to set the interval at which bypass trunk must query CSPF for LSP address. This mechanism ensures to update bypass trunk LSP addresses regularly so that, it can verify regularly if it can protect any LSP requesting protection.

Use the `no` parameter with this command to reset the interval to default value.

Note: Reducing interval to lower values may impact performance.

Command Syntax

```
bypass-lsp-addr-query-interval <10-60>
no bypass-lsp-addr-query-interval
```

Parameter

`<10-60>`	Set interval of bypass trunk querying LSP address.

Default

By default, interval is set to 60 seconds.

Command Mode

Router mode

Applicability

This command was introduced in OcNOS version 6.3.0.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)# bypass-lsp-addr-query-interval 50
```

cspf-retry-limit

Use this command to specify the number of retries that CSPF should carry out for a request received from RSVP.

Use the `no` parameter with this command to disable this configuration.

Command Syntax

```
cspf-retry-limit <1-65535>
no cspf-retry-limit
```

Parameter

`<1-65535>`	Set the number of times CSPF should retry for this LSP

Default

By default, retry-limit is 0 which means infinite retry.

Command Mode

Bypass mode

Applicability

This command was introduced in OcNOS version 6.3.0.

Examples

```
#configure terminal
(config)#rsvp-bypass bp1
(config-bypass)#cspf-retry-limit 535

(config)#rsvp-bypass bp1
(config-bypass)#no cspf-retry-limit
```

cspf-retry-timer

Use this command to specify the time between each retry that CSPF might carry out for a request received from RSVP. Use the no parameter with this command to disable this configuration.

Command Syntax

```
primary cspf-retry-timer <1-600>
no primary cspf-retry-timer
```

Parameter

<1-600>	Timeout between successive retries, in seconds

Default

By default, retry-timer is 0

Command Mode

Bypass mode

Applicability

This command was introduced in OcNOS version 6.3.0.

Examples

```
#configure terminal
(config)#rsvp-bypass bp1
(config-bypass)#cspf-retry-timer 45

(config)#rsvp-bypass bp1
(config-bypass)#no cspf-retry-timer
```

filter

Use this command to set the filter to the fixed or shared style for an LSP.

- The shared filter style identifies a shared reservation environment. It creates a single reservation into which flows from all senders are mixed.
- The fixed filter style designates a distinct reservation. A distinct reservation request is created for data packets from a particular sender. The fixed filter style is also used style to prevent rerouting of an LSP and to prevent another LSP from using this bandwidth.

Use the `no` parameter to reset the configured filter to the default.

Command Syntax

```
filter fixed
no filter
```

Parameters

`fixed`	Use a fixed filter for this LSP

Default

By default, bypass filter is shared-explicit.

Command Mode

Bypass mode

Applicability

This command was introduced in OcNOS version 6.3.0.

Examples

```
#configure terminal
(config)#rsvp-bypass bp1
(config-bypass)#filter fixed
```

hold-priority

Use this command to configure the hold priority value for the selected bypass trunk. In case of insufficient bandwidth, remove less important existing LSPs to free up a portion of the bandwidth. This can be done by preempting one or more of the signaled LSPs. Hold priority determines the degree to which an LSP holds onto its reservation for a session after the LSP has been configured successfully. When the hold priority is high, the existing LSP is less likely to give up its reservation.

Use the `no` parameter to reset the trunk to the default hold-priority value.

Command Syntax

```
hold-priority <0-7>
no hold-priority
```

Parameters

`<0-7>`	Set a hold priority for the bypass LSP

Default

The default hold-priority value is 0, which is the highest. Once a session is configured with a hold priority of 0, no other session can preempt it.

Command Mode

Bypass mode

Applicability

This command was introduced in OcNOS version 6.3.0.

Examples

```
#configure terminal
(config)#rsvp-bypass bp1
(config-bypass)#hold-priority 2
```

hop-limit

Use this command to specify a limit of hops for an RSVP bypass trunk. Hop-limit data is sent to the CSPF server if CSPF is used.

Upon configuration of an arbitrary hop-limit, the hop-limit is compared with the number of hops configured in the bypass path, if a bypass path has been configured. If the number of hops in the bypass path exceeds the hop-limit configured, no Path messages are sent, and any existing session is torn down. If no bypass path is configured, the bypass trunk is processed normally and Path messages are sent.

Use the `no` parameter to reset the bypass trunk to the default hop-limit value.

Command Syntax

```
hop-limit <1-255>
no hop-limit
```

Parameters

`<1-255>`	Set the number of acceptable hops for the LSP

Default

By default, bypass hop limit is 255

Command Mode

Bypass mode

Applicability

This command was introduced in OcNOS version 6.3.0

Examples

```
#configure terminal
(config)#rsvp-bypass bp1
(config-bypass)#hop-limit 23
```

label-record

Use this command to record all labels exchanged between RSVP-enabled routers during the reservation setup process.

Use the `no` parameter with this command to turn off recording.

Command Syntax

```
label-record
no label-record
```

Parameters

None

Default

By default, bypass label record is disabled

Command Mode

Bypass mode

Applicability

This command was introduced in OcNOS version 6.3.0.

Examples

```
#configure terminal
(config)#rsvp-bypass bp1
(config-bypass)#label-record
```

no record

Use this command to disable recording of the route taken by Path and Reservation Request (Resv) messages to confirm establishment of reservations and identify errors. Routes are recorded by means of the Route Record Object (RRO) in RSVP messages.

Use the `record` command to return to the default settings.

Command Syntax

```
no record
```

Parameters

None

Default

By default, routes are recorded

Command Mode

Bypass mode

Applicability

This command was introduced in OcNOS version 6.3.0.

Examples

```
#configure terminal
(config)#rsvp-bypass bp1
(config-bypass)#no record
```

path

Use this command to specify an RSVP path to be used. The PATHNAME in this command is the string (name) used to identify an RSVP path defined for the node (refer to rsvp-path command).

Use the `no` parameter with this command to remove a configured RSVP path.

Command Syntax

```
path PATHNAME
no path
```

Parameters

`PATHNAME`	The name of the path to use

Default

By default, bypass path is disabled

Command Mode

Bypass mode

Applicability

This command was introduced in OcNOS version 6.3.0.

Examples

```
#configure terminal
(config)#rsvp-bypass bp1
(config-bypass)#path mypath
```

preemption-type

Use this command to configure preemption type which decides the criteria to be considered in case of preemption.

Use the `no` parameter to remove configured preemption type.

Command Syntax

```
preemption-type (less-lsp-preempted | less-unused-bandwidth)
no preemption-type
```

Parameters

`less-lsp-preempted`	Set preemption type to minimize number of LSPs preempted
`less-unused-bandwidth`	Set preemption type to ensure less bypass bandwidth unused

Default

By default, preemption type is set to less-lsp-preempted.

Command Mode

Router mode

Applicability

This command was introduced in OcNOS version 6.3.0.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#preemption-type less-unused-bandwidth
```

record

Use this command to enable recording of the route taken by Path and Reservation Request (Resv) messages to confirm establishment of reservations and identify errors. Routes are recorded by means or the Route Record Object (RRO) in RSVP messages.

Use the `no record` command to disable recording of routes.

Command Syntax

```
record
```

Parameters

None

Default

By default, routes are recorded

Command Mode

Bypass mode

Applicability

This command was introduced in OcNOS version 6.3.0.

Examples

```
#configure terminal
(config)#rsvp-bypass bp1
(config-bypass)#record
```

retry-limit

Use this command to specify a retry count this RSVP bypass Trunk.

If a session is in a nonexistent state due to a path error message, the system tries to recreate the LSP for the number of times specified by the retry-limit command.

Although the same retry command controls both the trunk and the session, the retry-limit value affects only the session and not the trunk. If the trunk is in an incomplete state, the code keeps trying forever to bring it to a complete state regardless of the retry-limit value.

Use the `no` parameter with this command to revert to the default retry-limit value.

Command Syntax

```
retry-limit <1-65535>
no retry-limit
```

Parameter

`<1-65535>`	The set number of times the system should try setting up the LSP

Default

By default, the retry-limit value is 0, and the trunk and session try to create the LSP indefinitely.

Command Mode

Bypass mode

Applicability

This command was introduced in OcNOS version 6.3.0.

Examples

```
#configure terminal
(config)#rsvp-bypass bp1
(config-bypass)#retry-limit 256
```

retry-timer

Use this command to specify a retry interval for an RSVP bypass Trunk. When an ingress node tries to configure an LSP and the setup fails due to the receipt of a Path Error message, the system waits for the time configured with this command, before retrying the LSP setup process.

Use the `no` parameter with this command to revert to the default retry-time value.

Command Syntax

```
retry-timer <1-600>
no retry-timer
```

Parameters

`<1-600>`	Time in seconds after which the system should retry setting up the LSP

Default

By default, retry-timer value is 30 seconds.

Command Mode

Bypass mode

Applicability

This command was introduced in OcNOS version 6.3.0.

Examples

```
#configure terminal
(config)#rsvp-bypass bp1
(config-bypass)#retry-timer 12
```

reuse-route-record

Use this command to use the updated Route Record List as an Explicit Route (with all strict nodes) when a path message is sent out at the next refresh.

The ERO list contains the hops to be taken to reach the egress from the current LSR. If CSPF is not available, to place an ERO with all strict routes, use this command to modify the ERO after receiving the Resv message. The future Path messages have the ERO with all strict nodes, identifying each and every node to be traversed.

Use the `no` parameter with this command to disable the use of the Route Record List as the explicit route.

Command Syntax

```
reuse-route-record
no reuse-route-record
```

Parameters

None

Default

By default, reuse route record is disabled

Command Mode

Bypass mode

Applicability

This command was introduced in OcNOS version 6.3.0.

Examples

```
#configure terminal
(config)#rsvp-bypass bp1
(config-bypass)#reuse-route-record
```

rsvp-bypass

Use this command to create a new RSVP bypass trunk. When the bypass trunk is created, the attributes required to configure an explicitly-routed or traditionally-routed LSP are set. Once a trunk is configured with the required attributes, an RSVP bypass session (and PSB) is created for this trunk, which enables the exchange of messages and completes the LSP setup.

This command also modifies an existing RSVP path to configure an explicitly-routed or traditionally-routed LSP.

Use the `no` parameter with this command to remove an RSVP bypass trunk and all configured attributes.

Note: The RSVP bypass' name (BYPASSNAME) is limited to 32 characters.

Command Syntax

```
rsvp-bypass BYPASSNAME
no rsvp-bypass BYPASSNAME
```

Parameters

`BYPASSNAME`	Name to use for the bypass trunk

Default

By default, `rsvp bypass trunk` is disabled

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 6.3.0.

Examples

The command prompt changes from `config` to `config-bypass` as illustrated below:

```
#configure terminal
(config)#rsvp-bypass bp1
(config-bypass)#
```

setup-priority

Use this command to configure a setup priority value for a trunk. In case of insufficient bandwidth, users must remove less important LSPs to free up the bandwidth. This can be done by preempting one or more of the existing LSPs. The primary setup priority determines if a new LSP can preempt an existing LSP.

The setup priority of the new LSP must be higher than the hold priority of an existing LSP for the existing LSP to be preempted. Note that for a trunk, the setup priority should not be higher than the hold priority.

Use the `no` parameter with this command to revert to the default primary setup priority value.

Command Syntax

```
setup-priority <0-7>
no setup-priority
```

Parameters

`<0-7>`	Set the priority value

Default

By default, setup priority is 7, which is the lowest.

Command Mode

Bypass mode

Applicability

This command was introduced in OcNOS version 6.3.0.

Examples

```
#configure terminal
(config)#rsvp-bypass bp1
(config-bypass)#setup-priority 2
```

to A.B.C.D

Use this command to specify an IPv4 egress for a bypass LSP. When configuring an LSP, you must specify the address of the egress router by using this command in the bypass node. An egress definition is a mandatory attribute; no RSVP session is created when an egress is not defined.

Use the `no` parameter with this command to unset the configured egress address.

Command Syntax

```
to A.B.C.D
no to
```

Parameters

None

Default

The operator must specify an egress for LSP initialization to begin.

Command Mode

Bypass mode

Applicability

This command was introduced in OcNOS version 6.3.0.

Examples

```
#configure terminal
(config)#rsvp-bypass bp1
(config-bypass)#to 10.10.0.5
```

traffic

Use this command to specify the traffic type for this RSVP bypass Trunk.

Use the `no` parameter with this command to reset the configured traffic type.

Command Syntax

```
traffic (guaranteed|controlled-load)
no traffic
```

Parameters

`controlled-load`	Controlled loaded traffic
`guaranteed`	Guaranteed traffic

Default

By default, primary traffic type is controlled-load

Command Mode

Bypass mode

Applicability

This command was introduced in OcNOS version 6.3.0.

Examples

```
#configure terminal
(config)#rsvp-bypass bp1
(config-bypass)#traffic guaranteed
```

CHAPTER 5 Differentiated Services Commands

This chapter describes the RSVP Differentiated Services (DiffServ) commands.

map-route A.B.C.D

Use this command to map a IPv4 prefix route onto a trunk. This route is to be used for packets that are mapped to a specific RSVP trunk.

Use the `no` parameter with this command for unmapping routes from specified trunks.

Command Syntax

```
map-route A.B.C.D A.B.C.D
map-route A.B.C.D A.B.C.D CLASS
map-route A.B.C.D/M
map-route A.B.C.D/M CLASS
no map-route A.B.C.D A.B.C.D
no map-route A.B.C.D A.B.C.D CLASS
no map-route A.B.C.D/M
no map-route A.B.C.D/M CLASS
```

Parameters

`A.B.C.D`	Specify the IPV4 address to be mapped.
`A.B.C.D`	Specify a mask to be applied to the address being mapped.
`A.B.C.D/M`	Specify the IPV4 address to be mapped, with mask.
`CLASS`	Specify the DiffServ Class Name (for example, `be`, `ef` etc.) used for selecting incoming IP packets to be mapped to a specified RSVP trunk.

Default

By default, map route A.B.C.D is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#map-route 1.1.2.2/24 be
```

map-route X:X::X:X

Use this command to map a IPv6 prefix route onto a trunk. This route is to be used for packets that are mapped to a specific RSVP trunk.

Use the `no` parameter with this command for unmapping routes from specified trunks.

Command Syntax

```
map-route X:X::X:X X:X::X:X
map-route X:X::X:X X:X::X:X CLASS
map-route X:X::X:X/M
map-route X:X::X:X/M CLASS
no map-route X:X::X:X X:X::X:X
no map-route X:X::X:X X:X::X:X CLASS
no map-route X:X::X:X/M
no map-route X:X::X:X/M CLASS
```

Parameters

`X:X::X:X`	Specify the IPV6 address to be mapped.
`X:X::X:X`	Specify a mask to be applied to the address being mapped.
`X:X::X:X/M`	Specify the IPV6 address to be mapped, with mask.
`CLASS`	Specify the DiffServ Class Name (for example, `be`, `ef` etc.) used for selecting incoming IP packets to be mapped to a specified RSVP trunk.

Default

By default, map route X:X::X:X is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#map-route 1.1.2.2/24 be
```

override-diffserv

Use this command to enable the Differentiated Services (Diff-Serv) override configuration.

If a Path message is received without a Diff-Serv object by a Diff-Serv enabled node, it can be interpreted either as a request for an E-LSP (EXP-Inferred-PSC LSP) or as a request for Non-Diff-Serv LSP. This command supports the override option and when configured, the LSR interprets a path message without a Diff-Serv object as a request for Non-Diff-Serv LSP.

Use the `no` parameter with this command disable this feature.

Command Syntax

```
override-diffserv
no override-diffserv
```

Parameters

None

Default

By default, override diffserv is disabled

Command Mode

Router mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#router rsvp
(config-router)#override-diffserv
```

primary map class

Use this command to configure a primary PHB-EXP (Per-Hop Behavior-Experimental) mapping to be used by an E-LSP (EXP-Inferred-PSC LSP). This mapping is different from the node level PHB-EXP mapping.

Use the `no` parameter with this command to remove a PHB-EXP mapping configuration from current E-LSP PHB-EXP mapping.

Command Syntax

```
primary map class <0-7> exp <0-7>
no primary map class <0-7> exp <0-7>
```

Parameters

`<0-7>`	Diff-Serv class (queue) mapped to the particular PHB.
`<0-7>`	Exp bit which is to be mapped to this PHB.

Default

By default, primary map class is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#primary map class 4 exp 3

(config)#rsvp-trunk T1
(config-trunk)#no primary map class 4 exp 3
```

primary elsp-signaled

Use this command to configure a primary Diff-Serv (Differentiated Services) explicitly signaled E-LSP (EXP-Inferred-PSC LSP) interface.

The classes 1 to 7 are optional parameters that can be selected from node level PHB-EXP (Per-Hop Behavior) mapping as PHBs, which will then be used for an E-LSP. If you do not specify a class with this command, all classes will be selected for the E-LSP.

Use the no parameter with this command to remove the configuration.

Command Syntax

```
primary elsp-signaled
primary elsp-signaled class <0-7>
primary elsp-signaled class <0-7> <0-7>
primary elsp-signaled class <0-7> <0-7> <0-7>
primary elsp-signaled class <0-7> <0-7> <0-7> <0-7>
primary elsp-signaled class <0-7> <0-7> <0-7> <0-7> <0-7>
primary elsp-signaled class <0-7> <0-7> <0-7> <0-7> <0-7> <0-7>
primary elsp-signaled class <0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <0-7>
no primary elsp-signaled
```

Parameter

CLASS<0-7>	Diff-Serv class (queue).

Default

By default, primary elsp signaled is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#primary elsp-signaled 2 5 0 6

(config)#rsvp-trunk T1
(config-trunk)#no primary elsp-signaled
```

primary llsp

Use this command to configure a primary Differentiated Services Label-Only-Inferred-PSC (Diff-Serv L-LSP) interface, which will use Diff-Serv Class as its PHB Scheduling Class (PSC).

Use the no parameter with this command to remove the Diff-Serv L-LSP configuration.

Command Syntax

```
primary llsp class <0-7>
no primary llsp
```

Parameters

<0-7>	Diff-Serv class (queue).

Default

By default, primary llsp is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#primary llsp class 4

(config)#rsvp-trunk T1
(config-trunk)#no primary llsp
```

secondary map class

Use this command to configure a secondary PHB-EXP (Per-Hop Behavior-Experimental) mapping to be used by an E-LSP (EXP-Inferred-PSC LSP). This mapping is different from the node level PHB-EXP mapping.

Use the no parameter with this command to remove a PHB-EXP mapping configuration from current E-LSP PHB-EXP mapping.

Command Syntax

```
secondary map class <0-7> exp <0-7>
no secondary map class <0-7> exp <0-7>
```

Parameters

<0-7>	Diff-Serv class (queue) mapped to the particular PHB.
<0-7>	Exp bit that is to be mapped to this PHB.

Default

By default, secondary map class is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#secondary map class 4 exp 3

(config)#rsvp-trunk T1
(config-trunk)#no secondary map class 4 exp 3
```

secondary elsp-signaled

Use this command to configure a secondary Diff-Serv (Differentiated Services) explicitly signaled E-LSP (EXP-Inferred-PSC LSP) interface. The classes 1 to 7 are optional parameters can be selected from the node level PHB-EXP (Per-Hop Behavior) mapping as PHBs. They will then be used for an E-LSP. If you do not specify a class with this command, all classes will be selected for the E-LSP.

Use the no parameter with this command to remove the configuration.

Command Syntax

```
secondary elsp-signaled
secondary elsp-signaled class <0-7>
secondary elsp-signaled class <0-7> <0-7>
secondary elsp-signaled class <0-7> <0-7> <0-7>
secondary elsp-signaled class <0-7> <0-7> <0-7> <0-7>
secondary elsp-signaled class <0-7> <0-7> <0-7> <0-7> <0-7>
secondary elsp-signaled class <0-7> <0-7> <0-7> <0-7> <0-7> <0-7>
secondary elsp-signaled class <0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <0-7>
no secondary elsp-signaled
```

Parameters

CLASS<0-7>	Diff-Serv class (queue).

Default

By default, secondary elsp signaled is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#secondary elsp-signaled class 3 6 2 0 5

(config)#rsvp-trunk T1
(config-trunk)#no secondary elsp-signaled
```

secondary llsp

Use this command to configure a secondary Differentiated Services Label-Only-Inferred-PSC (Diff-Serv L-LSP) interface, which will use Diff-Serv Class as its PHB Scheduling Class (PSC).

Use the no parameter with this command to remove the Diff-Serv L-LSP configuration.

Command Syntax

```
secondary llsp class <0-7>
no secondary llsp
```

Parameters

CLASS<0-7>	Diff-Serv class (queue).

Default

By default, secondary llsp is disabled

Command Mode

Trunk mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#rsvp-trunk T1
(config-trunk)#secondary llsp class 5

(config)#rsvp-trunk T1
(config-trunk)#no secondary llsp
```

show rsvp diffserv-info

Use this command to display node level Differentiated Services (Diff-Serv) configuration information. This information includes the node level PHB-EXP mapping configured for ELSP-signaled LSP.

Command Syntax

```
show rsvp diffserv-info
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

Following is a sample output of the `show rsvp diffserv-info` command.

```
#show rsvp diffserv-info
E-LSP SIGNAL CLASS-EXP mapping:
CLASS    EXP_value
    5      0
    0      1
    1      2
    3      3
    2      4
    4      5
    6      6
    7      7
```

Table 5-56 explains the show command output fields.

Table 5-56: show rsvp diffserv-info output fields

Field	Description
CLASS	MPLS class type that corresponds to the DiffServ traffic engineering class.
EXP_value	Exp value is initialized at the ingress routing device only and overrides the rewrite configuration established for that forwarding class.

CHAPTER 6 Show Commands

This chapter describes the RSVP-TE show commands.

show debugging rsvp

This command displays the status of the options selected by the `debug RSVP` command.

Command Syntax

```
show debugging rsvp
```

Parameters

None

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show debugging rsvp
NSM debugging status:
  RSVP event debugging is on
  RSVP packet debugging is on
  RSVP incoming packet debugging is on
  RSVP outgoing packet debugging is on
  RSVP hexadecimal dump debugging is on
#
```

Table 6-57 explains the show command output fields.

Table 6-57: show debugging rsvp output fields

Field	Description
`NSM debugging status`	Debugging is enabled or disabled on a per-interface basis, using the commands.

show rsvp

Use this command to display data about the RSVP daemon.

Command Syntax

```
show rsvp
```

Parameters

None

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show rsvp
RSVP Version                  : 1
Process uptime                : 8 minutes
RSVP Refresh Reduction        : Enabled
RSVP Message Acknowledgement  : Disabled
Bundle Send                   : Disabled
NSM Connection                : Up
CSPF Connection               : Up
CSPF usage                    : Enabled
RSVP Refresh Timer            : 5
Keep Multiplier               : 3
Acknowledgement Await Timeout : 10
Explicit-Null For Direct Conn : Disabled
Local Protection              : Disabled
Hello Receipt                 : Disabled
Hello Interval                : 2
Hello Timeout                 : 10
Loop detection                : Enabled (all interface)
Override Diffserv             : Disabled
Ingress                       : 1.1.1.1
Penultimate Hop Popping       : Enabled
Refresh PATH msg parsing      : Enabled
Refresh RESV msg parsing      : Enabled
Detour identification         : Sender-Template

#
```

Table 6-58 explains the show command output fields.

Table 6-58: show rsvp output fields

Field	Description
RSVP Version	Version number associated with the RSVP ingress route.
Process uptime	Duration of the process running time.
RSVP Refresh Reduction	Measure of processing over head requests of refresh messages. Refresh reduction detail extensions improve routing device performance by reducing the process overhead, thus increasing the number of LSPs a routing device can support.
RSVP Message Acknowledgement	Acknowledge message for refresh reductions.
Bundle Send	Disables sending of Bundle Messages for a system.
NSM Connection	The Network Services Module (NSM) sends unsolicited messages to, or receives unsolicited messages from, the QoS (quality of service) module.
CSPF Connection	NSM passes the information to CSPF.
CSPF usage	CSPF finds the shortest path toward the LSP's egress router, taking into account explicit-path constraints.
RSVP Refresh Timer	Time interval used to generate periodic RSVP messages.
Keep Multiplier	Number of RSVP messages that can be lost before an RSVP state is declared stale.
Acknowledgment Await Timeout	The router that initiates the acknowledgment messages for an RSVP session waits for the timeout.
Explicit-Null For Direct Conn	Advertise label 0 to the egress routing device of an LSP. Explicit null: enabled or disabled.
Local Protection	A local repair mechanism is in use to maintain this tunnel.
Hello Receipt	To exchange Hello messages among neighbors.
Hello Interval	Frequency at which RSVP hellos are sent on this interface (in seconds).
Hello Timeout	RSVP Hello State Timer feature detects when a neighbor is down and triggers faster state timeout.
Loop detection	Loop back Detection (LBD) provides protection against loops by transmitting loop protocol packets out of ports where loop protection has been enabled.
Override Diffserv	Diffserv helps to carry the EXP-to-PHB mapping for signaled E-LSP or the PSC value for L-LSP.
Ingress	Information about ingress RSVP sessions.
Penultimate Hop Popping	Removes the label one hop before its destination.
Refresh PATH msg parsing	Refresh message supports the refreshing of RSVP state without the transmission of conventional Path messages.
Refresh RESV msg parsing	Refresh message supports the refreshing of RSVP state without the transmission of conventional Resv messages.
Detour identification	Detours are calculated to avoid the immediate downstream link and node.

show rsvp admin-groups

Use this command to display all known administrative groups configured through the NSM for the system.

Command Syntax

```
show rsvp admin-groups
```

Parameters

None

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

This is a sample output showing four administrative groups configured through NSM.

```
#show rsvp admin-groups
 Admin group detail:
  Value of 0 associated with admin group 'a'
  Value of 1 associated with admin group 'b'
  Value of 2 associated with admin group 'c'
  Value of 3 associated with admin group 'd'
#
```

Table 6-59 explains the show command output fields.

Table 6-59: show rsvp admin-groups output field

Field	Description
Admin group detail	Administrative groups details which implements the link coloring of resource classes.

show rsvp bypass

Use this command to display bypass session related information for configured bypass LSPs.

Command Syntax

```
show rsvp bypass
```

Parameters

None

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show rsvp bypass
Ingress RSVP:
To              From            Tun-ID   LSP-ID   LSPName                          State Uptime    Rt  Style  Labelin  Labelout
172.31.54.4     172.31.54.1     5001     2201     BYPASS2-172.31.222.19-Bypass     UP    02d15h11m 1 1 SE     -        52516
172.31.54.2     172.31.54.1     5002     2202     BYPASS3-172.31.222.9-Bypass      UP    02d15h11m 1 1 SE     -        0
172.31.54.2     172.31.54.1     5003     2203     BYPASS4-172.31.222.7-Bypass      UP    02d15h11m 1 1 SE     -        0
172.31.53.18    172.31.54.1     5004     2204     BYPASS5-172.31.189.179-Bypass    UP    02d15h11m 1 1 SE     -        52501
```

show rsvp bypass detail

Use this command to display bypass session related information in detail for all configured bypass LSPs or the bypass session with specified bypass tunnel name.

Command Syntax

```
show rsvp bypass (BYPASSNAME | detail)
```

Parameters

BYPASSNAME	Bypass tunnel name
detail	Detailed information of all configured bypass sessions

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show rsvp bypass BYPASS2-172.31.222.19
Ingress (Bypass)
172.31.54.4
  From: 172.31.54.1, LSPstate: Up, LSPname: BYPASS2-172.31.222.19-Bypass
  Ingress FSM state: Operational
  Establishment Time: 0s 324ms
  Setup priority: 7, Hold priority: 0
  CSPF usage: Enabled, CSPF Retry Count: 0, CSPF Retry Interval: 30 seconds
  LSP Re-Optimization: Disabled, Re-Optimization Timer: NA, Cspf Client: OSPF
  IGP-Shortcut: Disabled, LSP metric: 1
  LSP Protection: None
  Bypass trunk bandwidth type: Best-effort
   Label in: -,  Label out:    52516,
  Tspec rate: 0, Fspec rate: 0
  Policer: Not Configured
  Tunnel Id: 5001, LSP Id: 2201, Ext-Tunnel Id: 172.31.54.1
  Bind value: 0, Oper state: NA, Alloc mode: NA
  Downstream: 172.31.222.25, po22
  Path refresh: 30 seconds (RR enabled) (due in 12409 seconds)
  Resv lifetime: 157 seconds (due in 130 seconds)
  Retry count: 0, intrvl: 30 seconds
  RRO re-use as ERO: Disabled
  Label Recording: Disabled
  Admin Groups: none
  Configured Path: none
  Exclude Link: 172.31.222.19
  Session Explicit Route Detail :
   172.31.222.25/32 strict
   172.31.180.3/32 strict
   172.31.180.4/32 strict
  Record route:
   ----------------------------------------------------------
```

```
 IP Address        Label
 ------------------------------------------------------------
 <self>
 172.31.222.25
 172.31.180.3
 172.31.180.4
Style: Shared Explicit Filter
Traffic type: controlled-load
Minimum Path MTU: 9174
Current Error:
  Code : None, Value : None
  Originated Node : None, Recorded Time : N/A
Last Signaled Error:
  Code : None, Value : None
  Originated Node : None, Recorded Time : N/A
Trunk Type: mpls
Total LSP protected : 0, Bandwidth in use : 0
```

show rsvp bypass lsp-address-list

Use this command to display address details of every node of a bypass session shown as merge node detail for egress node of bypass session and transit node detail for transit node details of bypass session.

Command Syntax

```
show rsvp bypass (BYPASSNAME|) lsp-address-list
```

Parameters

BYPASSNAME	(Optional) Bypass tunnel name

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show rsvp bypass BYPASS2-172.31.222.19 lsp-address-list
Bypass trunk: BYPASS2-172.31.222.19

Merge Point Router ID: 172.31.54.4

Number of Merge Point IP addresses: 6
IP address:
  172.31.222.22    172.31.180.4     172.31.222.19    172.31.222.27
  172.31.222.31    172.31.186.4

Number of Transit Point IP addresses: 9
IP address:
  172.31.54.3      172.31.222.23    172.31.222.30    172.31.180.2
  172.31.222.25    172.31.186.20    172.31.33.120    172.31.180.3
  172.31.180.5

LSP address query interval: 60 seconds, next retry in: 27 seconds
```

show rsvp bypass protected-lsp-list

Use this command to display the list of sessions protected by a bypass session and match code provides the details bypass is a perfect match or any constraint compromised.

Note: Match code 0 is an indication of perfect match i.e. all constraint of protected session matched. i.e. If protected session asked for node protection, then bypass provides perfect node protection by merging exactly at next to next hop node. If protected session asked for bandwidth protection, bypass provides bandwidth protection. In case of PHP node, even when node protection is requested by protected session, it is not applicable and node protection request is not applicable on PHP node. Thus, a bypass providing link protection with other criteria matching is considered as perfect match.

Note: If a bypass protected session requested for link protection but it is mapped to a bypass node protection, then it is not a perfect match. Match code will be 4 in that case.

Note: When bandwidth protection is requested, highest importance of bypass mapping given to bandwidth protection. When bandwidth protection cannot be provided, then the remaining constraints given importance.

Command Syntax

```
show rsvp bypass (BYPASSNAME|) protected-lsp-list
```

Parameters

BYPASSNAME	Bypass tunnel name

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show rsvp bypass protected-lsp-list
Match Code: 0 - Perfect match (all criteria matching), 1 - Bandwidth protection miss, 2 - Node protection miss,
            3 - SRLG protection miss, 4 - Merge point not ideal, 255 - Invalid

Bypass trunk: BYPASS2-172.31.222.19
Bypass trunk bandwidth type: best-effort
Total LSP protected : 0
 Bandwidth in use : 0

Bypass trunk: BYPASS3-172.31.222.9
Bypass trunk bandwidth type: best-effort
List of LSP's Protected:
Tunnel-id  Lsp-Id     Lsp-Name                      Role      Ext_tnl_id      Ingress         Egress          Match-Code
61976      3          to_OKL_STRICT                  Transit    172.31.2.52     172.31.2.52     172.31.54.2     0
61975      4          to_OKL_2ND_LOOSE               Transit    172.31.2.52     172.31.2.52     172.31.54.2     0
20         23884      to_OKL_1ST_LOOSE::to_OKL_1ST_LOOSE
                                                    Transit    172.31.33.120   172.31.33.120   172.31.54.2     0
22         5478       to_OKL_2ND_LOOSE::to_OKL_2ND_LOOSE
                                                    Transit    172.31.33.120   172.31.33.120   172.31.54.2     0
61974      3          to_OKL_1ST_LOOSE              Transit    172.31.2.52     172.31.2.52     172.31.54.2     0
21         36172      to_OKL_STRICT::to_OKL_STRICT  Transit    172.31.33.120   172.31.33.120   172.31.54.2     0
Total LSP protected : 6
 Bandwidth in use : 0
```

show rsvp control-adjacency

Use this command to display RSVP specific information for control adjacency.

Command Syntax

```
show rsvp control-adjacency
show rsvp control-adjacency CANAME
```

Parameters

CANAME	Use this parameter to display the name of a control-adjacency

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#"show rsvp control-adjacency" without parameters:
Control Adj    Admin status   Oper Status    Peer-address   Gifindex       Control
Channel

#"show rsvp control-adjacency" with parameters:
Admin Status"Enabled" : "Disabled"
Oper Status"Up" : "Down"
Peer-address
Gifindex
Control-Channel in usecc->name : "N/A"
Control-Channel Gifindex
Control-Channel Local-address
Control-Channel Peer-address
Control-Channel ID
Control-Channel Binding Ifindex
Refresh Reduction usage"Disabled" : "Enabled"
Message Acknowledgement"Enabled" : "Disabled"
Bundle Buffer size
Current Epoch Value
Primary IPv4 addressIPv4_address : "N/A"
Primary IPv6 addressIPv6_address : "N/A"
Configured refresh time
Configured keep multiplier
Acknowledgement Await Timeout
Hello Receipt"Enabled" : "Disabled"
Hello Interval
Hello Timeout
Non IANA Hello exchange"Enabled" : "Disabled"
```

Table 6-61 explains the show command output fields.

Table 6-60: show rsvp control-adjacency output field

Field	Description
Control Adj	Control Adjacency status and configuration.
Admin status	Indicates whether the user can administratively disable a peer while still preserving its configuration. Up = Yes, Down = No.
Oper Status	Displays the current status of the cross-connect segment – Up or Down.
Peer-address	Peer address in aa IPv4 and IPv6 format.
Gifindex	Number of gif index on which RSVP is active.
Control Channel	Control Channel status and configuration.
Refresh Reduction usage	Measure of processing over head requests of refresh messages.
Message Acknowledgment	The router that initiates the acknowledgment messages for an RSVP session.
Bundle Buffer size	Number of bundle buffer size.
Current Epoch Value	Value of the database epoch and number of entries in the epoch.
Primary IPv4 address	Primary IPv4 address of the neighbor interface.
Primary IPv6 address	Primary IPv6 address of the neighbor interface.
Configured Refresh Time	Time refresher which takes to generate periodic RSVP messages.
Configured Keep Multiplier	Number of RSVP messages that can be lost before an RSVP state is declared stale.
Acknowledgment Await Timeout	The router that initiates the acknowledgment messages for an RSVP session waits for the timeout.
Hello Receipt	To exchange Hello messages among neighbors.
Hello Interval	Frequency at which RSVP hellos are sent on this interface (in seconds).
Hello Timeout	RSVP Hello State Timer feature detects when a neighbor is down and triggers faster state timeout.
Non IANA Hello exchange	Hello exchange state in the interface.

show rsvp data-link

Use this command to display RSVP specific information for data links.

Command Syntax

```
show rsvp data-link
show rsvp data-link DLNAME
```

Parameters

DLNAME	Data link name

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#sh rsvp data-link
```

show rsvp dste-info

Use this command to display data about a DSTE configuration for an RSVP bypass session.

Command Syntax

```
show rsvp dste-info
```

Parameters

None

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show rsvp dste-info
te0: { default, 7 }
te1: { data, 6 }
te2: { voice-low, 5 }
te3: { voice-high, 4 }
ct0: default
ct1: data
ct2: voice-low
ct3: voice-high
```

Table 6-61 explains the show command output fields.

Table 6-61: show rsvp dste-info output field

Field	Description
ct0	TE Class and Class type for class 0.
ct1	TE Class and Class type for class 1.
ct2	TE Class and Class type for class 2.
ct3	TE Class and Class type for class 3.

show rsvp graceful-restart

To modify the lines displayed, use the | (output modifier token); to save the output to a file, use the > output redirection token.

Command Syntax

```
show rsvp graceful-restart
show rsvp graceful-restart A.B.C.D
```

Parameters

A.B.C.D	IPv4 address of a specific neighbor (optional).

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before OcNOS-SP version 5.0.

Example

```
#show rsvp graceful-restart
Graceful Restart: Enabled
Advertised Restart Time: 180000 msec
Advertised Recovery Time: 360000 msec
Sending Recovery Time: Yes
Remote addr: 172.16.10.2 Local addr: 172.16.10.1
Nbr State: Normal Type: Reroute
Nbr Hello State: Up
LSPs protecting: 0
Restart Time: 0 msec, Recovery Time: 0 msec
Rest of Restart Time: 0 msec, Rest of Recovery Time: 0 msec
```

show rsvp interface

Use this command to display data about RSVP-specific information for interfaces, or about a specific interface.

Command Syntax

```
show rsvp interface
show rsvp interface IFNAME
```

Parameter

IFNAME	The name of the interface to display data.

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show rsvp interface eth0
Status                          : Enabled
Interface Index                 : 2
Refresh Reduction usage         : Enabled
Message Acknowledgement         : Disabled
Bundle Buffer size              : 65535
Current Epoch Value             : 208043005
Primary IPv4 address            : 10.10.23.1
Primary IPv6 address            : N/A
Interface Type                  : Ethernet
Administrative Group            : a
                                : d
Configured refresh time         : 5
Configured keep multiplier      : 3
Acknowledgement Await Timeout   : 10
Hello Receipt                   : Disabled
Hello Interval                  : 2
Hello Timeout                   : 10
Non IANA Hello exchange         : Disabled
#
```

Table 6-62 explains the show command output fields.

Table 6-62: show rsvp interface output field

Field	Description
Status	Display the status of Resource Reservation Protocol (RSVP).
Interface Index	Number of interface index on which RSVP is active.
Refresh Reduction usage	Measure of processing over head requests of refresh messages.

Table 6-62: show rsvp interface output field

Field	Description
Message Acknowledgement	The router that initiates the acknowledgment messages for an RSVP session.
Bundle Buffer size	Number of bundle buffer size.
Current Epoch Value	Value of the database epoch and number of entries in the epoch.
Primary IPv4 address	Primary IPv4 address of the neighbor interface.
Primary IPv6 address	Primary IPv6 address of the neighbor interface.
Interface Type	Type of interface.
Administrative Group	The administrators who belong to the same administrative group.
Configured Refresh Time	Time refresher which takes to generate periodic RSVP messages.
Configured Keep Multiplier	Number of RSVP messages that can be lost before an RSVP state is declared stale.
Acknowledgment Await Timeout	The router that initiates the acknowledgment messages for an RSVP session waits for the timeout.
Hello Receipt	To exchange Hello messages among neighbors.
Hello Interval	Frequency at which RSVP hellos are sent on this interface (in seconds).
Hello Timeout	RSVP Hello State Timer feature detects when a neighbor is down and triggers faster state timeout.
Non IANA Hello exchange	Hello exchange state in the interface.

show rsvp l2-info

Use this command to display MAC and out interface details of a bypass tunnel which is used to send control messages of protected sessions over bypass tunnel when protected session is using backup.

Command Syntax

```
show rsvp l2-info
```

Parameters

None

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show rsvp l2-info
============================================================
## Bypass ftn l2 info ##
Ftn IX: 1
Out label: 52521 Out if 100022
src addr:(34ef.b63d.57a9)
Dst addr:(34ef.b694.3e08)
============================================================
============================================================
## Bypass ftn l2 info ##
Ftn IX: 2
Out label: 3 Out if 100022
src addr:(34ef.b63d.57a9)
Dst addr:(34ef.b694.3e08)
============================================================
```

show rsvp local-addresses

Use this command to display data about any configured RSVP local address, including either IPv4 or IPv6 addresses.

Command Syntax

```
show rsvp local-addresses
show rsvp local-addresses ipv4
show rsvp local-addresses ipv6
```

Parameters

`ipv4`	Use this parameter to display IPv4 local addresses.
`ipv6`	Use this parameter to display IPv6 local addresses.

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show rsvp local-addresses
IPv4 Addresses:
 Address                       Interface
 4.4.4.40                      lo
 10.1.2.40                     eth0
 14.14.14.8                    eth4
 34.0.0.40                     eth2
 80.0.0.40                     eth2
 127.0.0.1                     lo
IPv6 Addresses:
 Address                       Interface
 ::1                           lo
 fe80::202:b3ff:fed5:8dbb      eth4
 fe80::202:b3ff:fed5:9842      eth2
 fe80::20e:cff:fe83:3727       eth0
#
```

Table 6-63 explains the show command output fields.

Table 6-63: show rsvp local-addresses output field

Field	Description
IPv4 Addresses	IPv4 address for the interface.
IPv6 Addresses	IPv6 address for the interface.

Table 6-63: show rsvp local-addresses output field

Field	Description
Address	Address for the interface.
Interface	Name of the interface.

show rsvp neighbor

Use this command to display a list of IPv4 RSVP neighbors or just a single IPv4 RSVP neighbor.

Command Syntax

```
show rsvp neighbor
show rsvp neighbor A.B.C.D
```

Parameters

A.B.C.D	Use this parameter to display the IP address of the IPv4 RSVP neighbor.

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show rsvp neighbor
IP Address          UpStrm LSP DnStrm LSP RefreshReduc Srefresh In  Type
10.10.20.4          0          1          Enabled      5s           Implicit
10.10.23.2          0          1          Enabled      8s           Implicit
#
```

Table 6-64 explains the show command output fields.

Table 6-64: show rsvp neighbor output field

Field	Description
IP Address	Address for the interface.
UpStrm LSP	Specify the upstream label for the bidirectional label-switched path (LSP).
DnStrm LSP	Specify the dnstream label for the bidirectional label-switched path (LSP).
Refresh Reduc	Refresh reduction improves the scalability, latency, and reliability of Resource Reservation Protocol (RSVP) signaling to enhance network performance and message delivery.
Srefresh In	Remaining seconds for srefresh timer expiry.
Type	Type of neighbor interface.

show rsvp nexthop-cache

Use this command to display the current nexthops being cached by RSVP.

Command Syntax

```
show rsvp nexthop-cache
```

Parameters

None

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show rsvp nexthop-cache
Prefix              Nexthop          Outgoing Intf  Valid For   Num Sessions
10.10.20.80/32      0.0.0.0          eth1           12 seconds  1
10.10.23.60/32      0.0.0.0          eth0           17 seconds  1
#
```

Table 6-65 explains the show command output fields.

Table 6-65: show rsvp nexthop-cache output field

Field	Description
Prefix	It is an ordered list and entries are evaluated in order of increasing sequence number.
Nexthop	IP address of the next hop.
Outgoing Intf	Short name of the physical interface through which traffic goes to the protected link.
Valid For	Frequency at which RSVP hellos are sent next hop on this interface (in seconds).
Num Sessions	Number of session in the interface.

show rsvp path

Use this command to display the configured rsvp paths and their configured hops. Specify the pathname to show hops related to a specific path. If no pathname is specified all the rsvp paths are displayed.

Command Syntax

```
show rsvp path
show rsvp path PATHNAME
```

Parameter

PATHNAME	The name of a specific path.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

Following are sample outputs from this command, with and without a PATHNAME (PRI) specified.

```
#show rsvp path
Path name: PRI, id: 1
 10.10.11.51 strict
 10.10.12.50 strict
 10.10.13.51 strict

Path name: SEC, id: 2
 10.10.10.51 strict

Path name: loop, id: 3
 10.10.11.51 strict
 10.10.12.50 strict
 10.10.13.51 strict
 10.10.14.50 strict
#

#show rsvp path PRI
Path name: PRI, id: 1
 10.10.11.51 strict
 10.10.12.50 strict
 10.10.13.51 strict
#
```

Table 6-66 explains the show command output fields.

Table 6-66: show rsvp path output field

Field	Description
Path name	Name of the path.
id	Address of the rsvp path.

show rsvp protected-lsp-reop-list

Use this command to display list of facility protected sessions which didn't get any bypass protection or didn't get a perfect bypass protection. These sessions are checked for better protection whenever a new bypass session comes up.

Command Syntax

```
show rsvp protected-lst-reop-list
```

Parameters

None

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show rsvp protected-lsp-reop-list
Tunnel-id  Lsp-Id     Lsp-Name                        Role       Ext_tnl_id       Ingress          Egress           Protected
222        169        LHR_t222                        Transit    172.31.53.18     172.31.53.18     172.31.2.52      Yes
204        1522       LHR_t204                        Transit    172.31.53.18     172.31.53.18     172.31.33.120    Yes
17         52608      GGN_NDLS_2ND_LOOSE::to_CISCO_2ND_LOOSE
                                                      Transit    172.31.33.120    172.31.33.120    172.31.53.18     Yes
```

show rsvp session

Use this command to display session-related information for configured LSPs.

Command Syntax

```
show rsvp session
show rsvp session up
show rsvp session up detail
show rsvp session down
show rsvp session down detail
```

Parameters

`up`	Use this parameter to display sessions that are currently operational.
`down`	Use this parameter to display sessions that are currently not operational.
`detail`	Use this parameter to display detailed session-related information.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

Following is a sample output from the command using the detail parameter.

```
#show rsvp session detail
Ingress (Primary)
10.10.21.3
  From: 1.1.1.1, LSPstate: Up, LSPname: t1
  Setup priority: 5, Hold priority: 5
  CSPF usage: Disabled
  LSP Protection: None
  Label in: -,  Label out: 16,
  Tspec rate: 10m, Fspec rate: 10m
  Tunnel Id: 1, LSP Id: 2, Ext-Tunnel Id: 1.1.1.1
  Downstream: 10.10.23.2, eth0
  Path refresh: 5 seconds (due in 6772 seconds)
  Resv lifetime: 26 seconds (due in 25 seconds)
  Retry count: 0, intrvl: 30 seconds
  RRO re-use as ERO: Disabled
  Label Recording: Disabled
  Admin Groups: none
  Configured Path: p1 (in use)
  Configured Explicit Route Detail :
   10.10.23.2/32 strict
  Session Explicit Route Detail :
   10.10.23.2/32 strict
  Record route: <self> 10.10.23.2 10.10.21.3
  Style: Shared Explicit Filter
```

```
    Traffic type: controlled-load
    Minimum Path MTU: 1500
    LSP Type:  ELSP_SIGNAL
    CLASS    DSCP_value     EXP_value
  #
```

Table 6-67 explains the show command output fields.

Table 6-67: show rsvp session output field

Field	Description
Ingress (Primary)	Information about ingress RSVP sessions. Each session has one line of output.
From	Source (ingress switch) of the session.
LSP state	State of the LSP that is being handled by this RSVP session. It can be either Up, Dn (down), or Admin Dn. Admin Dn indicates that the LSP is being taken down gracefully.
LSPname	Name of the LSP.
Setup priority	Value of the setup priority.
Hold priority	Determines the degree to which an LSP holds onto its session reservation after the LSP has been set up successfully.
CSPF usage	CSPF usage state in the rsvp session.
LSP Protection	Protects the traffic failures.
Label in	Incoming label for this LSP.
Label out	Outgoing label for this LSP.
Tspec rate	Sender's traffic specification, which describes the sender's traffic parameters.
Fspec rate	Fspec peak rate values.
Tunnel id	Tunnel address (destination port) for the session.
LSP id	Address of the LSP in the interface.
Ext-Tunnel Id	Session address for the ext-tunnel.
Down stream	Specify the dnstream label for the bidirectional label-switched path (LSP).
Path refresh	Path messages are sent periodically to refresh path states. The refresh interval is controlled by a variable called the refresh time.
Resv lifetime	Number of seconds remaining in the lifetime of the reservation.
Retry count	Number of times sanity polling periodically checks for an error condition in the FPC.
intrvl	Interval sets the time for the messages in order to control the session.
LSP Type	Type of ELSP signal.

show rsvp session count

Use this command to display session-related information for configured LSPs.

Command Syntax

```
show rsvp session count
show rsvp session count egress
show rsvp session count ingress
show rsvp session count transit
```

Parameters

`egress`	Use this parameter to display the number of configured egress sessions.
`ingress`	Use this parameter to display the number of configured ingress sessions.
`transit`	Use this parameter to display the number of configured transmit sessions.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show rsvp session count
Total configured: 1520, Up 1520, Down 0
#
```

Table 6-68 explains the show command output fields.

Table 6-68: show rsvp session count output field

Field	Description
Total configured	Number of configured rsvp session in the interface.

show rsvp session egress

Use this command to display session-related information for an egress router.

Command Syntax

```
show rsvp session egress
show rsvp session egress A.B.C.D
show rsvp session egress X:X::X:X
show rsvp session egress detail
show rsvp session egress down
show rsvp session egress down detail
show rsvp session egress up
show rsvp session egress up detail
```

Parameters

`A.B.C.D`	Use this parameter to display an IPv4 address of an egress router
`X:X::X:X`	Use this parameter to display an IPv6 address of an egress router
`down`	Use this parameter to display sessions that are currently not operational
`up`	Use this parameter to display sessions that are currently operational
`detail`	Use this parameter to display detailed session-related information

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show rsvp session egress without parameters or with "up" or "down":
%s RSVP:
To              From            State                Pri Rt  Style Labelin
Labelout LSPName                          Uptime  Est.time   DSType
...
Total %d displayed

#show rsvp session egress with parameters:
"Bypass", "Primary", "Detour", "Secondary"
 Make-Before-Break Sibling for session with LSP-ID:prefix4: prefix6
  From: u.prefix4: u.prefix6
LSPstate: %s, LSPname:
      "Up/"Using Backup"/"Using Secondary"
      "Dn",
  Revert hold timer is ON due to expire in %d seconds
  Revert Timer Finished, Forced Switch to Secondary LSP In Effect
  CSPF usage: "Disabled" : "Enabled"
  , CSPF Retry Count: %d, CSPF Retry Interval: %d seconds"
  IGP-Shortcut: Enabled, LSP metric:
```

```
  IGP-Shortcut: Disabled, LSP metric:
  LSP Protection:
  Bypass trunk:
  Label in:
  Label out:
  Tspec rate:
  Fspec rate:
  Policer: Configured
      and installed in hardware
      but not installed in hardware
      Not Configured
  Tunnel Id: %d, LSP Id: %d
Ext-Tunnel Id:
  Downstream:
  Upstream:
  Path refresh: %d seconds (RR enabled), (due in %d seconds)
  Path lifetime: %d seconds (due in %d seconds)
  Resv refresh: %d seconds (due in %d seconds)
  Resv lifetime: %d seconds (due in %d seconds)
  Retry count: %d, intrvl: %d seconds", # remaining, next retry in: %d
seconds",
  RRO re-use as ERO:  "Enabled" : "Disabled"
  Label Recording: "Enabled" : "Disabled"
  FRR Admin Groups/Admin Groups:
     ***admin group info***
  Exclude path detail:
   Exclude "Link" : "Node
   Configured Path: "none" : "in use" : "not in use"
   %s Explicit Route Detail  "Configured" : "Received"
       "strict" : "loose"
  Record route: " <self>") "  ...incomplete"
  Style: %s\n", rsvp_style_to_str (style));
  Traffic type:  "guaranteed" : "controlled-load" : "none"
  Minimum Path MTU:
  Traffic type: N/A
  Minimum Path MTU: N/A
  LSP Type:  "ELSP_SIGNAL" : "ELSP_CONFIG"
  CLASS    DSCP_value     EXP_value
  The class to exp bits mapping is invalid.
  LSP Type:  L-LSP
  LLSP DSCP: %d%d%d%d%d%d   CLASS: %4s",
  DSTE CLass Type Number: Invalid, Class Type name(configured):
  DSTE Class Type Number: %d, Class Type name:
  Last Recorded Error Code: %s (%d)
  Last Recorded Error Value: %s (%d)
  Node where Last Recorded Error originated:
  Trunk Type: "gmpls" : "mpls"
  Tesid:
Merge Point Adderss [%d] =
```

Table 6-69 explains the show command output fields.

Table 6-69: show rsvp session egress output field

Field	Description
LSP state	State of the LSP that is being handled by this RSVP session. It can be either Up, Dn (down), or Admin Dn. Admin Dn indicates that the LSP is being taken down gracefully.
LSP name	Name of the LSP.
CSPF usage	CSPF usage state in the rsvp session.
CSPF Retry Count	Number of times CSPF tried to find the path.
CSPF Retry Interval	The interval at which CSPF retry to find the path.
IGP-Shortcut	Status of IGP shortcut for the RSVP trunk.
LSP metric	Relative/Absolute metric value of the LSP.
LSP Protection	LSP Protection configured for the RSVP trunk.
Bypass trunk	Name for the configured Bypass trunk.
Tspec rate	Sender's traffic specification, which describes the sender's traffic parameters.
Fspec rate	Fspec peak rate values.
Policer	QoS Policy configured for the RSVP trunk.
Tunnel Id	Tunnel identifier (destination port) for the RSVP session.
LSP Id	Address of the LSP in the interface.
Ext-Tunnel Id	Ext Tunnel identifier (destination port) for the RSVP session.
Down stream	Specify the dn stream label for the bidirectional label-switched path (LSP).
Upstream	Address of the previous hop for the egress session.
Path refresh	Path messages are sent periodically to refresh path states. The refresh interval is controlled by a variable called the refresh time.
Path lifetime	Number of seconds remaining in the lifetime of the reservation.
Resv refresh	Remaining time in seconds for the next Resv refresh.
Resv lifetime	Number of seconds remaining in the lifetime of the reservation.
Retry count	Number of times sanity polling periodically checks for an error condition in the FPC.
intrvl	Interval sets the time for the messages in order to control the session.
next retry in	Remaining time in seconds for the next retry.
RRO re-use as ERO	Enabling to re-use Record route as Explicit route for rsvp session.
Label Recording	Enabling to record the labels exchanged by all the peers.
FRR Admin Groups/Admin Groups	Resource affinities associated with the rsvp session.

Table 6-69: show rsvp session egress output field

Field	Description
Exclude path detail	Detailed List of the link addresses to be excluded for RSVP Bypass session.
Exclude Link	Address of the Link to be excluded for RSVP Bypass session.
Configured Path	Configured path name associated with the rsvp session.
Record route	Established rsvp path with each hop information.
Style	Reservation style associated with the rsvp session.
Traffic type	Traffic type associated with the rsvp session.
Minimum Path MTU	Path maximum transmission unit (MTU) discovery in the interface.
LSP Type	Type of ELSP signal.
CLASS	Name of the class which is associated with rsvp session.
DSCP_value	DSCP value of diff-serv class which is associated with rsvp session.
EXP_value	EXP value of diff-serv class which is associated with rsvp sess
DSTE Class Type Number	Diff-serv class type number associated with rsvp session.
Class Type name	Diff-serv class type name associated with rsvp session.
Last Recorded Error Code	The last recorded error code for the RSVP session.
Last Recorded Error Value	The last recorded error for the RSVP session.
Node where Last Recorded Error originated	Error originated node in the rsvp session.
Trunk Type	Trunk type in the rsvp session.
Tesid	Traffic Engineering Service Instance Identifier
Merge Point Adderss	Address of the node where the Bypass LSP joins with the protected LSP.

show rsvp session ingress

Use this command to display session-related information for an ingress router.

Command Syntax

```
show rsvp session ingress
show rsvp session ingress A.B.C.D
show rsvp session ingress X:X::X:X
show rsvp session ingress detail
show rsvp session ingress down
show rsvp session ingress down detail
show rsvp session ingress up
show rsvp session ingress up detail
```

Parameters

`A.B.C.D`	Use this parameter to display an IPv4 address of an ingress router
`X:X::X:X`	Use this parameter to display an IPv6 address of an ingress router.
`down`	Use this parameter to display sessions that are currently not operational
`up`	Use this parameter to display sessions that are currently operational
`detail`	Use this parameter to display detailed session-related information

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show rsvp session ingress without parameters or with "up" or "down":
%s RSVP:
To              From            State               Pri Rt  Style Labelin
Labelout LSPName                          Uptime  Est.time   DSType
...
Total %d displayed

#show rsvp session ingress with parameters:
"Bypass", "Primary", "Detour", "Secondary"
 Make-Before-Break Sibling for session with LSP-ID:prefix4: prefix6
  From: u.prefix4: u.prefix6
LSPstate: %s, LSPname:
      "Up/"Using Backup"/"Using Secondary"
      "Dn",
  Revert hold timer is ON due to expire in %d seconds
  Revert Timer Finished, Forced Switch to Secondary LSP In Effect
  CSPF usage: "Disabled" : "Enabled"
  , CSPF Retry Count: %d, CSPF Retry Interval: %d seconds"
```

```
  IGP-Shortcut: Enabled, LSP metric:
  IGP-Shortcut: Disabled, LSP metric:
  LSP Protection:
  Bypass trunk:
  Label in:
  Label out:
  Tspec rate:
  Fspec rate:
  Policer: Configured
      and installed in hardware
      but not installed in hardware
      Not Configured
  Tunnel Id: %d, LSP Id: %d
Ext-Tunnel Id:
  Downstream:
  Upstream:
  Path refresh: %d seconds (RR enabled), (due in %d seconds)
  Path lifetime: %d seconds (due in %d seconds)
  Resv refresh: %d seconds (due in %d seconds)
  Resv lifetime: %d seconds (due in %d seconds)
  Retry count: %d, intrvl: %d seconds", # remaining, next retry in: %d
seconds",
  RRO re-use as ERO:  "Enabled" : "Disabled"
  Label Recording: "Enabled" : "Disabled"
  FRR Admin Groups/Admin Groups:
     ***admin group info***
  Exclude path detail:
   Exclude "Link" : "Node
   Configured Path: "none" : "in use" : "not in use"
   %s Explicit Route Detail  "Configured" : "Received"
       "strict" : "loose"
  Record route: " <self>") "  ...incomplete"
  Style: %s\n", rsvp_style_to_str (style));
  Traffic type:  "guaranteed" : "controlled-load" : "none"
  Minimum Path MTU:
  Traffic type: N/A
  Minimum Path MTU: N/A
  LSP Type:  "ELSP_SIGNAL" : "ELSP_CONFIG"
  CLASS    DSCP_value     EXP_value
  The class to exp bits mapping is invalid.
  LSP Type:  L-LSP
  LLSP DSCP: %d%d%d%d%d%d   CLASS: %4s",
  DSTE CLass Type Number: Invalid, Class Type name(configured):
  DSTE Class Type Number: %d, Class Type name:
  Last Recorded Error Code: %s (%d)
  Last Recorded Error Value: %s (%d)
  Node where Last Recorded Error originated:
  Trunk Type: "gmpls" : "mpls"
  Tesid:
Merge Point Adderss [%d] =
```

Table 6-70 explains the show command output fields.

Table 6-70: show rsvp session ingress output field

Field	Description
LSP state	State of the LSP that is being handled by this RSVP session. It can be either Up, Dn (down), or Admin Dn. Admin Dn indicates that the LSP is being taken down gracefully.
LSP name	Name of the LSP.
CSPF usage	CSPF usage state in the rsvp session.
CSPF Retry Count	Number of times CSPF tried to find the path.
CSPF Retry Interval	The interval at which CSPF retry to find the path.
IGP-Shortcut	Status of IGP shortcut for the RSVP trunk.
LSP metric	Relative/Absolute metric value of the LSP.
LSP Protection	LSP Protection configured for the RSVP trunk.
Bypass trunk	Name for the configured Bypass trunk.
Tspec rate	Sender's traffic specification, which describes the sender's traffic parameters.
Fspec rate	Fspec peak rate values.
Policer	QoS Policy configured for the RSVP trunk.
Tunnel Id	Tunnel identifier (destination port) for the RSVP session.
LSP Id	Address of the LSP in the interface.
Ext-Tunnel Id	Ext Tunnel identifier (destination port) for the RSVP session.
Down stream	Specify the dn stream label for the bidirectional label-switched path (LSP).
Upstream	Address of the previous hop for the egress session.
Path refresh	Path messages are sent periodically to refresh path states. The refresh interval is controlled by a variable called the refresh time.
Path lifetime	Number of seconds remaining in the lifetime of the reservation.
Resv refresh	Remaining time in seconds for the next Resv refresh.
Resv lifetime	Number of seconds remaining in the lifetime of the reservation.
Retry count	Number of times sanity polling periodically checks for an error condition in the FPC.
intrvl	Interval sets the time for the messages in order to control the session.
next retry in	Remaining time in seconds for the next retry.
RRO re-use as ERO	Enabling to re-use Record route as Explicit route for rsvp session.
Label Recording	Enabling to record the labels exchanged by all the peers.
FRR Admin Groups/Admin Groups	Resource affinities associated with the rsvp session.

Table 6-70: show rsvp session ingress output field

Field	Description
Exclude path detail	Detailed List of the link addresses to be excluded for RSVP Bypass session.
Exclude Link	Address of the Link to be excluded for RSVP Bypass session.
Configured Path	Configured path name associated with the rsvp session.
Record route	Established rsvp path with each hop information.
Style	Reservation style associated with the rsvp session.
Traffic type	Traffic type associated with the rsvp session.
Minimum Path MTU	Path maximum transmission unit (MTU) discovery in the interface.
LSP Type	Type of ELSP signal.
CLASS	Name of the class which is associated with rsvp session.
DSCP_value	DSCP value of diff-serv class which is associated with rsvp session.
EXP_value	EXP value of diff-serv class which is associated with rsvp sess
DSTE Class Type Number	Diff-serv class type number associated with rsvp session.
Class Type name	Diff-serv class type name associated with rsvp session.
Last Recorded Error Code	The last recorded error code for the RSVP session.
Last Recorded Error Value	The last recorded error for the RSVP session.
Node where Last Recorded Error originated	Error originated node in the rsvp session.
Trunk Type	Trunk type in the rsvp session.
Tesid	Traffic Engineering Service Instance Identifier.
Merge Point Adderss	Address of the node where the Bypass LSP joins with the protected LSP.

show rsvp session LSP-NAME

Use this command to display information only for sessions with a specified name.

Command Syntax

```
show rsvp session LSP-NAME
show rsvp session LSP-NAME primary
show rsvp session LSP-NAME secondary
```

Parameters

`primary`	Use this parameter to display any primary LSP sessions
`secondary`	Use this parameter to display any secondary LSP sessions

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Usage

Following is a sample output from the command displaying session information about the LSP named `t1`.

```
#show rsvp session t1
Ingress (Primary)
192.168.0.90
  From: 192.168.0.63, LSPstate: Up, LSPname: t1
  Setup priority: 7, Hold priority: 0
  CSPF usage: Disabled, CSPF Retry Count: 0, CSPF Retry Interval: 30 seconds
  Label in: -,  Label out: 17,
  Tspec rate: 0
  Tunnel Id: 1, LSP Id: 1, Ext-Tunnel Id: 192.168.0.63
  Downstream: 10.10.23.60, eth0
  Path refresh: 30 seconds (due in 34 seconds)
  Resv lifetime 157 seconds (due in 155 seconds)
  Retry Count: 0, Retry Interval: 30 seconds
  RRO re-use as ERO: Enabled
  Labels Recording: Disabled
  Admin Groups: include-any -->  0(a)
  Configured Path: p1 (in use)
  Configured Explicit Route Detail :
   10.10.23.60/32 loose
  Session Explicit Route Detail :
   10.10.23.60/32 loose
   10.10.21.90/32 loose
  Record route: <self> 10.10.23.60 10.10.21.90
  Style: Shared Explicit Filter
  Traffic type: controlled-load
  Minimum Path MTU: 1500
  Last Recorded Error Code: None
  Last Recorded Error Value: None
```

```
#
```

Table 6-71 explains the show command output fields.

Table 6-71: show rsvp session LSP-NAME output field

Field	Description
Ingress (Primary)	Information about ingress RSVP sessions. Each session has one line of output.
From	Source (ingress switch) of the session.
LSP state	State of the LSP that is being handled by this RSVP session. It can be either Up, Dn (down), or Admin Dn. Admin Dn indicates that the LSP is being taken down gracefully.
LSPname	Name of the LSP.
Setup priority	Value of the setup priority.
Hold priority	Determines the degree to which an LSP holds onto its session reservation after the LSP has been set up successfully.
CSPF usage	CSPF usage state in the rsvp session.
LSP Protection	Protects the traffic failures.
Label in	Incoming label for this LSP.
Label out	Outgoing label for this LSP.
Tspec rate	Sender's traffic specification, which describes the sender's traffic parameters.
Fspec rate	Fspec peak rate values.
Tunnel id	Tunnel address (destination port) for the session.
LSP id	Address of the LSP in the interface.
Ext-Tunnel Id	Session address for the ext-tunnel.
Down stream	Specify the dnstream label for the bidirectional label-switched path (LSP).
Path refresh	Path messages are sent periodically to refresh path states. The refresh interval is controlled by a variable called the refresh time.
Resv lifetime	Number of seconds remaining in the lifetime of the reservation.
Retry count	Number of times sanity polling periodically checks for an error condition in the FPC.
intrvl	Interval sets the time for the messages in order to control the session.
RRO re-use as ERO	Enabling to re-use Record route as Explicit route for rsvp session.
Label Recording	Enabling to record the labels exchanged by all the peers.
Admin Groups	Resource affinities associated with the rsvp session.
Configured Path	Configured path name associated with the rsvp session.

Table 6-71: show rsvp session LSP-NAME output field

Field	Description
Configured Explicit Route Detail	Configured explicit route with each hop information.
Session Explicit Route Detail	Established explicit route with each hop information.
Record route	Established rsvp path with each hop information.
Style	Reservation style associated with the rsvp session.
Traffic type	Traffic type associated with the rsvp session.
Minimum Path MTU	Path maximum transmission unit (MTU) discovery in the interface.
Last Recorded Error Code	Recorded error code for the last time service ran.
Last Recorded Error Value	No Recorded error value for the last time service ran.

show rsvp session transit

Use this command to display session-related information for the transit or intermediate router.

Command Syntax

```
show rsvp session transit
show rsvp session transit detail
show rsvp session transit up
show rsvp session transit down
show rsvp session transit up detail
show rsvp session transit down detail
```

Parameters

`up`	Use this parameter to display sessions that are operational
`down`	Use this parameter to display sessions that are not operational
`detail`	Use this parameter to display detailed session-related information

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

Following are sample outputs from the command displaying detailed session information for the transit router.

```
#show rsvp session transit detail
Transit (Primary)
10.10.21.3
  From: 1.1.1.1, LSPstate: Up, LSPname: t1
  Setup priority: 5, Hold priority: 5
  LSP Protection: None
  Label in: 16,  Label out: 3,
  Tspec rate: 10m, Fspec rate: 10m
  Tunnel Id: 1, LSP Id: 2, Ext-Tunnel Id: 1.1.1.1
  Downstream: 10.10.21.3, eth1   Upstream: 10.10.23.1, eth3
  Path refresh: 5 seconds (due in 6155 seconds)
  Path lifetime: 26 seconds (due in 25 seconds)
  Resv refresh: 5 seconds (due in 2533 seconds)
  Resv lifetime: 26 seconds (due in 25 seconds)
  RRO re-use as ERO: Disabled
  Label Recording: Disabled
  Admin Groups:   Received Explicit Route Detail :
   10.10.23.2/32 strict
  Record route: 10.10.23.1 <self> 10.10.21.3
  Style: Shared Explicit Filter
  Traffic type: controlled-load
  Minimum Path MTU: 1500
  LSP Type:  ELSP_SIGNAL
```

```
  CLASS    DSCP_value     EXP_value
  af43      100110           7
  DSTE Class Type Number: 0, Class Type name: default
#
```

Table 6-72 explains the show command output fields.

Table 6-72: show rsvp session transit output field

Field	Description
Transit (Primary)	Transit RSVP sessions information in the interface.
From	Source (ingress switch) of the session.
LSP state	State of the LSP that is being handled by this RSVP session. It can be either Up, Dn (down), or Admin Dn. Admin Dn indicates that the LSP is being taken down gracefully.
LSP name	Name of the LSP.
Setup priority	Value of the setup priority.
Hold priority	Determines the degree to which an LSP holds onto its session reservation after the LSP has been set up successfully.
LSP Protection	Protects the traffic failures.
Label in	Incoming label for this LSP.
Label out	Outgoing label for this LSP.
Tspec rate	Sender's traffic specification, which describes the sender's traffic parameters.
Fspec rate	Fspec peak rate values.
Tunnel id	Tunnel address (destination port) for the session.
LSP id	Address of the LSP in the interface.
Ext-Tunnel Id	Session address for the ext-tunnel.
Down stream	Specify the dnstream label for the bidirectional label-switched path (LSP).
Path refresh	Path messages are sent periodically to refresh path states. The refresh interval is controlled by a variable called the refresh time.
Resv lifetime	Number of seconds remaining in the lifetime of the reservation.
RRO re-use as ERO	Enabling to re-use Record route as Explicit route for rsvp session.
Label Recording	Enabling to record the labels exchanged by all the peers.
Admin Groups	Resource affinities associated with the rsvp session.
Configured Explicit Route Detail	Configured path name associated with the rsvp session.

Table 6-72: show rsvp session transit output field

Field	Description
Record route	Recorded route for the session, taken from the record route object. Normally this value will be the same as that of explct route. Differences indicate that path rerouting has occurred, typically during fast reroute.
Style	Reservation style associated with the rsvp session.
Traffic type	Traffic type associated with the rsvp session.
Minimum Path MTU	Path maximum transmission unit (MTU) discovery in the interface.
LSP Type	Type of LSP for Diffserv services(E-LSP or L-LSP).
CLASS	Name of the class which is associated with rsvp session.
DSCP_value	DSCP value of diff-serv class which is associated with rsvp session.
EXP_value	EXP value of diff-serv class which is associated with rsvp session.
DSTE Class Type Number	Diff-serv class type number associated with rsvp session.
Class Type name	Diff-serv class type name associated with rsvp session.

show rsvp statistics

Use this command to display overall statistics of different type of RSVP control messages sent and received in a node.

Command Syntax

```
show rsvp statistics
```

Parameters

None

Command Mode

```
Exec and Privileged Exec modes
```

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show rsvp statistics
  PacketType              Total
                  Sent      Received
  Path             627          501
  PathErr            0           24
  PathTear           1           27
  Resv FF           30            9
  Resv WF            0            0
  Resv SE          646          583
  Resv Err           0            0
  ResvTear           0            0
  ResvConf           0            0
  Hello         330604       334461
  Bundle          1006          866
  Ack               50           14
  SRefresh       34348        32424
  Notify             0            0
```

show rsvp summary-refresh

Use this command to display RSVP summary refresh data.

Command Syntax

```
show rsvp summary-refresh
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show rsvp summary-refresh:
Neighbor Addr       Tunnel ID  LSP ID     Ingress             Egress
```

Table 6-73 explains the show command output fields.

Table 6-73: show rsvp trunk output field

Field	Description
Neighbor Addr	Neighbor address on the primary address of the interface.
Tunnel ID	Tunnel identifier (destination port) for the RSVP session.
LSP ID	Address of the LSP in the interface.
Ingress	Information about ingress RSVP sessions.
Egress	Information about egress RSVP sessions.

show rsvp trunk

Use this command to display information for a specific trunk or for all trunks.

Command Syntax

```
show rsvp trunk
show rsvp trunk NAME
show rsvp trunk detail
```

Parameters

NAME	Enter the name of a trunk
detail	Use this parameter to display detailed information for all trunks

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show rsvp trunk
Trunk Name      Trunk ID  Type       # Sess       Egress Address(es)
T1              101       P2P             1       4.4.4.4
T2              102       P2P             2       5.5.5.5
Total trunks configured: 3.
#
```

Following is a sample output from the command using the detail parameter.

```
#show rsvp trunk detail
Trunk name: T1, tunnel-id: 101
 Type: P2P
 Ext-tunnel-id: 1.1.1.1/32
 Egress: 4.4.4.4/32
 # of LSPs in trunk: 1
 Mapped-routes: none

Trunk name: T2, tunnel-id: 102
 Type: P2P
 Ext-tunnel-id: 1.1.1.1/32
 Egress: 5.5.5.5/32
 # of LSPs in trunk: 2
 Mapped-routes: none
```

Table 6-74 explains the show command output fields.

Table 6-74: show rsvp trunk output field

Field	Description
Trunk Name	Name of the trunk.
Trunk ID	Session address for the trunk.
Type	Trunk type in the rsvp session.
Sess	Number of sessions associated with rsvp trunk.
Egress	Information about egress RSVP sessions.
Total trunks configured	Number of configured trunk in the rsvp session.
Ext-tunnel-id	Extended Tunnel identifier (destination port) for the RSVP session.
Mapped-routes	Map the route of the interface.

show rsvp version

Use this command to display the version of the RSVP daemon. Current RSVP version is 1.

Command Syntax

```
show rsvp version
```

Parameters

None

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show rsvp version
Resource ReSerVation Protocol, version 1. rfc2205
   RSVP protocol      = Enabled
   R(refresh timer)   = 30 seconds
   K(keep multiplier) = 3
   Preemption         = Normal
#
```

Table 6-75 explains the show command output fields.

Table 6-75: show rsvp version output field

Field	Description
Resource Reservation Protocol	RSVP software version.
RSVP protocol	Status of RSVP.
R (refresh timer)	Configured time interval used to generate periodic RSVP messages.
K (keep multiplier)	Number of RSVP messages that can be lost before an RSVP state is declared stale.
Preemption	Currently configured preemption capability.

Terms

Numbers

1588v2. IEEE specification for Precision Time Protocol (PTP).

802. A family of IEEE Local Area Network (LAN) standards. The services and protocols specified by the 802 standards map to Layer 1 (L1) and Layer 2 (L2) of the Open Systems Interconnection (OSI) Reference Model:

- 802.1: Overview architecture of LANs and interneworking
- 802.2: The logical link control (LLC) sublayer of Layer 2 (L2)
- 802.3: Layer 1 (L1) and the Media Access Control (MAC) sublayer of Layer 2 (L2), Also called Ethernet.

802.1AB. IEEE specification for Link Layer Discovery Protocol (LLDP).

802.1ad. Amendment to IEEE 802.1Q for Provider Bridging (PB).

802.1ag. Amendment to IEEE 802.1Q for Connectivity Fault Management (CFM).

802.1ah. IEEE specification that adds Provider Backbone Bridging (PBB) to 802.1ad Provider Bridging (PB):

802.1ak. Amendment to IEEE 802.1Q for Multiple Registration Protocol (MRP).

802.1aq. Amendment to IEEE 802.1D for Shortest Path Bridging (SPB).

802.1AX. IEEE specification for link aggregation and Multi-Chassis Link Aggregation (MLAG).

802.1D. IEEE specification which allows multiple LANs to be connected together through what the standard calls a “MAC bridge” which filters data sent between LAN segments, allowing networks to be partitioned for administrative purposes and reducing network congestion. The more common term for a MAC bridge is switch. The 802.1D standard includes Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP).

802.1p. IEEE 802.1Q defines priority signaling for traffic that can be used by Quality of Service (QoS) mechanisms to differentiate traffic. Packets are tagged as belonging to a queue, which determines the priority of the packet. Although this technique is often called “802.1p”, there is no standard by that name. Instead, the technique is incorporated into 802.1Q standard.

802.1Q. IEEE Virtual Local Area Network (VLAN) and Multiple Spanning Tree Protocol (MSTP) specifications. This standard refers to VLANs as “virtual bridged networks”. The 802.1D standard covers “VLAN-unaware” switches, while 802.1Q extends 802.1D for “VLAN-aware” switches.

802.1Qau. Amendment to IEEE 802.1Q for Quantized Congestion Notification (QCN).

802.1Qay. Amendment to IEEE 802.1Q for Provider Backbone Bridge-Traffic Engineering (PBB-TE).

802.1Qaz. Amendment to IEEE 802.1Q for Data Center Bridging Capability Exchange (DCBX) and Enhanced Transmission Selection (ETS).

802.1Qbb. Amendment to IEEE 802.1Q for Priority-based Flow Control (PFC).

802.1Qbg. Amendment to IEEE 802.1Q for Edge Virtual Bridging (EVB).

802.1v. Amendment to IEEE 802.1Q to classify incoming packets based on data link layer protocol identification.

802.3ah. IEEE specification for Ethernet to the First Mile (EFM).

802.3x. IEEE specification for flow control.

G.8031. ITU-T specification for Ethernet Linear Protection Switching (ELPS).

G.8032. ITU-T specification for Ethernet Ring Protection Switching (ERPS).

A

Access Control List (ACL). A set of rules used to filter traffic. Each rule specifies a set of conditions (such as source address, destination address, type of packet, or combination of these items) that a packet must meet to match the rule. When a device determines that an ACL applies to a packet, it tests the packet against the conditions of all rules. The first match determines whether the packet is permitted or denied.

access layer. In the network design model, the layer that connects devices such as desktops, laptops, servers, and printers to the network and provides end users access to network resources. This layer accepts traffic into a network and can pass that traffic to the distribution layer. The access layer is usually built using Layer 2 (L2) switching such as Spanning Tree Protocol (STP). This layer connects logical broadcast domains and provides isolation to groups of users. Typically, Virtual Local Area Network (VLAN) instances are implemented as broadcast domains in the access layer. Also called the edge layer. See also customer edge (CE), provider edge (PE).

acknowledgment (ACK). Notification sent from one network device to another to acknowledge that some event (for example, receipt of a message) has occurred.

active route. Route chosen from all routes in a Routing Information Base (RIB) to reach a destination. Active routes are installed in the Forwarding Information Base (FIB).

address. A unique identifier for a device on a network, either as a sender or receiver. An address can be a physical address or a logical address.

See also address family, address resolution, Classless Interdomain Routing (CIDR), domain name, Domain Name Service (DNS), dynamic address, IP address, MAC address, name resolution, static address.

address family. A specific type of network addressing supported by a routing protocol. Examples are IPv4 unicast and IPv4 multicast.

address resolution. The process of translating the address of an entity on one system to the equivalent address of the same entity on another system. For instance, translating an IP address to its Domain Name Service (DNS) name. See also Address Resolution Protocol (ARP).

Address Resolution Protocol (ARP). A Transmission Control Protocol/Internet Protocol (TCP/IP) mechanism that maps a MAC address to an IP address in the ARP cache data structure. Defined in RFC 826. See also Neighbor Discovery Protocol (NDP).

adjacency. The relationship between neighboring devices for exchanging routing information. Adjacent devices share a common network segment.

A given device can have multiple adjacencies, but each adjacency consists of only two devices connected by one link. A protocol data unit (PDU) that goes between them does not have to pass through any other network devices. See also neighbor.

administrative distance. How reliable the source of the route is considered to be. A lower value is preferred over a higher value. An administrative distance of 255 indicates no confidence in the source; routes with this distance are not installed in the Routing Information Base (RIB). Also called route preference.

Advanced Encryption Standard (AES). A cryptographic algorithm for use by U.S. Government organizations to protect sensitive (unclassified) information. Defined in Federal Information Processing Standards (FIPS) PUB 197.

advertising. Process in which routing or service updates are sent at specified intervals so that other devices on the network can maintain lists of usable routes.

Agent Extensibility (AgentX). A protocol used to implement Simple Network Management Protocol (SNMP) that defines communications between an SNMP agent and an SNMP client. AgentX does not directly communicate with an SNMP client, but relies on the agent to handle the protocol details of SNMP. Defined by RFC 2741.

aggregate route. A single entry in a routing table that represents a combination of groups of routes that have common addresses. See also route summarization.

alarm indication signal (AIS). A signal transmitted instead of the normal signal to maintain transmission continuity and to indicate to the receiving device that a transmission interruption (fault) has occurred either at the equipment originating the AIS signal or upstream of that equipment.

American National Standards Institute (ANSI). A voluntary organization of corporate, government, and other members that develops international and U.S. standards relating to, among other things, communications and networking. ANSI is a member of the International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO).

application-specific integrated circuit (ASIC). An integrated circuit that is designed for a specific application.

area. A logical division of devices that maintains detailed routing information about itself as well as routing information that allows it to reach other routing subdomains. An area divides a network into small, manageable pieces, reducing the amount of information each device must store and maintain about all other devices.

In Intermediate System to Intermediate System (IS-IS) and Open Shortest Path First (OSPF), an area is a set of contiguous networks and hosts within an autonomous system (AS) that have been administratively grouped together.

area border router (ABR). A router on the border of one or more Open Shortest Path First (OSPF) areas that connects those areas to the backbone network. An ABR is a member of both the OSPF backbone and its attached areas. Therefore, an ABR maintains routing tables for both the backbone topology and the topology of the other areas. See also Not-So-Stubby-Area (NSSA), stub area.

authentication. A process that verifies that data is not altered during transmission and ensures that users are communicating with the individual or organization that they believe they are communicating with.

authentication, authorization, and accounting (AAA). A framework for controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services:

- Authentication determines who the user is and whether to grant that user access to the network
- Authorization determines what the user can do
- Accounting tracks the user's activities and provides an audit trail that can be used for billing or resource tracking

See also Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial In User Service (RADIUS), Terminal Access Controller Access Control System Plus (TACACS+).

Authentication Header (AH). An Internet Protocol Security (IPsec) protocol that authenticates either all or part of the contents of a packet by adding a header with a a hash message authentication code (HMAC) calculated based on the values in the packet. AH provides authentication but not confidentiality. See also Encapsulating Security Payload (ESP).

Automatic Protection Switching (APS). A means to detect a signal failure or signal degrade on a working channel and switch traffic to a protection channel. There are two types of APS:

- Ethernet Linear Protection Switching (ELPS)
- Ethernet Ring Protection Switching (ERPS)

autonomous system (AS). A network controlled as a single administrative entity sharing a common routing strategy. An autonomous system is subdivided into areas. An AS runs an Interior Gateway Protocol (IGP) such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF), or Intermediate System to Intermediate System (IS-IS) within its boundaries. An AS uses an Exterior Gateway Protocol (EGP) to exchange routing information with other ASs.

autonomous system border router (ASBR). An area border router (ABR) located between an Open Shortest Path First (OSPF) autonomous system (AS) and a non-OSPF network. ASBRs run both OSPF and another routing protocol, such as Routing Information Protocol (RIP).

An ASBR is a link between the OSPF autonomous system and the outside network. An ASBR exchanges routing information with routers in other ASes. The ASBR redistributes routing information received from other ASs throughout its own AS. An ASBR must reside in a standard OSPF area.

availability. The amount of time that a system is available during time periods when it is expected to be available. Availability is often measured as a percentage of an elapsed year. For example, 99.95% availability equates to 4.38 hours of downtime in a year (0.0005 * 365 * 24=4.38) for a system that is expected to be available all the time.

B

B-MAC. A source and destination backbone MAC address (B-AA and a B-DA) in a Provider Backbone Bridging (PBB) header.

B-TAG. See backbone VLAN (B-VLAN).

backbone. The part of a network used as the primary path for transporting traffic between network segments.

backbone core bridge (BCB). A device that bridges frames based on backbone VLAN (B-VLAN) and backbone MAC address (B-MAC) information in a Provider Backbone Bridging (PBB) network core.

backbone edge bridge (BEB). A device that encapsulates customer frames for transmission across a Provider Backbone Bridging (PBB) network. There are two types:

- B-BEB (B type BEB): Contains a B-component for bridging in the provider space based on backbone MAC address (B-MAC) and backbone VLAN (B-VLAN) information.
- I-BEB (I type BEB): Contains an I-component for bridging in the customer space based on customer MAC address (C-MAC) and service VLAN (S-VLAN) information.

backbone VLAN (B-VLAN). A field in a Provider Backbone Bridging (PBB) header that carries the backbone VLAN identifier information. The format is the same as a service VLAN (S-VLAN) tag. Also called B-VID tag, B-TAG.

backhaul. The part of a hierarchical network that connects small subnetworks at the edge of the network to the core or backbone network.

In wireless backhaul, the part of the network that transports traffic from a cellular base station to a core network that routes and switches voice and data traffic.

bandwidth. A measure of the data transfer rate of a communications transport medium.

base station. An earth-based transmitting/receiving station for cellular phones and other wireless transmission systems.

Bellman-Ford algorithm. Used in distance-vector routing protocols such as Routing Information Protocol (RIP) to determine the best path to all routes in the network. Contrast with Dijkstra algorithm.

best effort. Traffic class in which the network forwards as many packets as possible in as reasonable a time as possible. By default, packets not explicitly assigned to a specific traffic class are assigned to the best-effort class.

BGP confederation. A method to solve scaling problems created by the iBGP full-mesh requirement. BGP confederations effectively break up a large autonomous system (AS) into subautonomous systems (sub-ASs). Each sub-AS must be uniquely identified within the confederation AS by a sub-AS number.

Within a sub-AS, the same iBGP full mesh requirement exists. Connections to other confederations are made with eBGP, and peers outside the sub-AS are treated as external. To avoid routing loops, a sub-AS uses a confederation sequence, which operates like an AS path but uses only the privately assigned sub-AS numbers.

BGP neighbor. Another device on the network that is running Border Gateway Protocol (BGP). There are two types of BGP neighbors: internal neighbors in the same autonomous system (AS) and external neighbors in different autonomous systems.

BGP peer. A remote Border Gateway Protocol (BGP) speaker that is an established neighbor of the local BGP speaker. BGP peers do not have to be directly connected to each other to share a BGP session.

BGP speaker. A router configured to run the Border Gateway Protocol (BGP) routing protocol. A BGP speaker must be explicitly configured with a set of BGP peers with which it exchanges routing information.

Bidirectional Forwarding Detection (BFD). Protocol that reduces the reliance upon the relatively slow hello mechanism in routing protocols to detect failures where no hardware signaling is available. BFD works with Border Gateway Protocol (BGP), Open Shortest Path First (OSPF) v2, and Intermediate System to Intermediate System (IS-IS) to enable them to receive failure notifications. Defined in RFCs 5880 and 5881.

bit error rate (BER). The ratio of error bits to the total number of bits transmitted. A BER is generally shown as a negative exponent (for example, 10-7, which means one out of 10,000,000 bits is in error).

Border Gateway Protocol (BGP). An Exterior Gateway Protocol (EGP) that maintains a table of IP networks, or prefixes, which designate network reachability among autonomous system (AS) instances. BGP uses path-vector routing that makes decisions based on path, network policies, and/or rule sets. BGP is the primary protocol for the global Internet. First defined by RFC 1163.

BGP Version 4 (BGP4) defined in RFC 4271 supports Classless Interdomain Routing (CIDR) and route summarization.

BGP performs these tasks:

- Collects information about reachable networks from neighboring autonomous systems

- Advertises its reachable networks to routers inside the AS and to neighboring autonomous systems
- Selects routes if there are multiple routes available.

Each BGP device can have both external and internal connections to other BGP devices:

- Internal BGP (iBGP) connections are within the same autonomous system
- External BGP (eBGP) connections are between different autonomous systems

The configuration and behavior is slightly different between eBGP and iBGP.

You can use iBGP for multihomed BGP networks (with more than one connection to the same external autonomous system).

To avoid routing loops, iBGP does not advertise routes learned from an internal BGP peer to other internal BGP peers. Instead, BGP requires that all internal peers be fully meshed so that any route advertised by one router is advertised to all peers within the autonomous system (AS). As a network grows, the full-mesh requirement becomes difficult to manage. To combat scaling problems, BGP uses route reflection and BGP confederations.

Multiprotocol BGP (MP-BGP) allows different types of addresses (address families) to be distributed in parallel. MP-BGP supports IPv4 and IPv6 addresses as well as unicast and multicast variants of each. Defined in RFC 4760. See also IPv6 Provider Edge (6PE).

See also community.

bridge. A device operating at Layer 1 (L1) and Layer 2 (L2) of the Open Systems Interconnection (OSI) Reference Model that forwards frames from one network segment to another based on the MAC address.

The term bridge also describes a device that connects collision domains. Collisions that appear on one side of a switch are not allowed to propagate to the other.

Originally, bridges only had two ports, with each one connected to a network segment. Later, bridges had multiple ports that could connect more than two network segments as well as directly connecting hosts. As bridges evolved, they were also able to filter frames, that is, forward only certain traffic from one network segment to another. This type of device is sometimes called an intelligent bridge, but the more modern term is switch. The term “bridge” is somewhat archaic but is still often used in standards documents.

bridge protocol data unit (BPDU). A protocol data unit (PDU) sent by switches running the Spanning Tree Protocol (STP) to learn about other switches in the network and maintain the spanning tree.

broadcast. The process of a single host simultaneously sending the same message to all nodes on a network. Compare to multicast, where a only a subset of the receivers are addressed. See also unicast.

bursty. The tendency of the bandwidth needed in a network to vary greatly from one moment to the next.

C

C-MAC. A source and destination customer MAC address (C-SA and a C-DA) in a Provider Backbone Bridging (PBB) header.

C-TAG. See customer VLAN (C-VLAN).

Carrier Ethernet. Extensions to Ethernet that enable network operators to provide Ethernet services to customers and to use Ethernet technology in their networks. See also Metro Ethernet Forum (MEF).

certificate. Electronic document that identifies a person or entity. Through the use of keys and certificates, the entities exchanging data can authenticate each other.

channel. A connecting path that carries information from a sending device to a receiving device. A channel can refer to a physical medium (such as a coaxial cable or fiber optic cable).

circuit. A communications channel or path between two devices capable of carrying electrical current.

circuit switching. A network where a dedicated circuit must be opened between devices before they can communicate and, while the circuit is open, no other devices may use that circuit or parts of it. A circuit can remain open without any information transmission, and still be unusable by other devices; it must be closed before it is available to other users. Contrast with packet switching.

Class of Service (CoS). A way of managing traffic in a network by grouping similar types of traffic (for example, e-mail, video, voice, file transfer) together and treating each type as a class with its own level of service priority. However, no guarantees are made that a given priority will meet any specified minimum level. See also Quality of Service (QoS).

classful IP addressing. An older addressing scheme for configuring the ratio of networks to hosts using fixed length prefixes. See Classless Interdomain Routing (CIDR).

Classless Interdomain Routing (CIDR). A notation for specifying an IP addresses and its network prefix which appends a slash character to the address and a decimal number indicating the leading bits in the network prefix. For example:

- In the IPv4 notation “192.168.0.0/16”:
  - “192.168” (the first 16 bits) defines the network address.
  - .0.0 up to .255.255 refer to the host addresses on that network. This leaves 16 bits to contain host addresses, enough for 65536 host addresses.
- In the IPv6 notation “2001:db8::/32”:
  - “2001:db8” (the first 32 bits) defines the network address.
  - :0:0:0:0:0:0 to:ffff:ffff:ffff:ffff:ffff:ffff refer to host addresses on that network. This leaves 96 bits to contains host addresses, enough for 7,922,816,251,426,433 host addresses.

The lower the number after the slash, the more hosts contained in that block.

CIDR uses variable length subnet masking (VLSM) based on arbitrary length prefixes. In VLSM, the number of network and host bits assigned to a subnet can vary based on the number of hosts the subnet needs to support.

CIDR replaced traditional classful IP addressing, in which address allocation was based on octet (8-bit) boundary segments of the IP address. In CIDR, the boundary between the network and host portions of an IP address can be on any bit boundary. The old classful A, B, and C network designations correspond to CIDR prefixes of /8, /16, or /24. 192.168.0.0/16 corresponds to an old class B network. With CIDR, finer grained division of networks are possible, down to individual IP addresses, such as 192.168.100.2/32.

CIDR routes can be carried by Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS), and Routing Information Protocol (RIP).

Before CIDR notation, IPv4 networks were represented using dotted decimal notation for both the address and a subnet mask.

Also called route summarization or supernetting.

client/server architecture. A computing architecture that distributes processing between clients and servers on the network. A client program makes a service request from a server which fulfils the request.

collapsed core. Collapsing the core layer and the distribution layer into one layer (one device) in the network design model. A collapsed core design reduces cost, while maintaining most of the benefits of the network design model for small networks that do not grow significantly larger over time.

collision domain. A network segment where data frames can collide with one another when being sent on a shared medium such as Ethernet. Hosts in a collision domain arbitrate among themselves using an access control mechanism.

command-line interface (CLI). Environment for entering commands to configure and monitor routing and switching software and hardware.

committed information rate (CIR). The average rate at which packets are admitted to the network. Each packet is counted as it enters the network. Packets that do not exceed the CIR are marked green, which corresponds to low loss priority. Packets that exceed the CIR but are below the peak information rate (PIR) are marked yellow, which corresponds to medium loss priority.

common and internal spanning tree (CIST). A single topology connecting all Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP) switches into one active topology. In other words, an entire spanning tree fabric.

common spanning tree (CST). The topology connecting all Spanning Tree Protocol (STP)/Rapid Spanning Tree Protocol (RSTP) *switches* and multiple spanning-tree (MST) region *instances*. An MST region appears as a single switch to spanning tree configurations outside the region.

community. In Border Gateway Protocol (BGP), a logical group of prefixes or destinations that share a common attribute; used to simplify a routing policy. Community members can be on different networks and in different autonomous systems.

In Simple Network Management Protocol (SNMP), an authentication scheme that authorizes SNMP clients based on the source IP address of incoming SNMP packets, defines which Management Information Base (MIB) objects are available, and specifies the operations (read-only or read-write) allowed on those objects.

congestion. The state in which the network load exceeds the available resources such as link capacity or memory buffers.

connection-oriented. A packet switching technology where a virtual circuit between sending and receiving devices makes it seem like the devices are connected by a switched circuit with a fixed bandwidth without regard to their physical addresses. In a connection-oriented service, packets always reach their destination in the same order as they were sent. Transmission Control Protocol (TCP) is a connection-oriented transport service. See also connectionless.

Connection-oriented protocols can be used to send information that requires a constant delay and bandwidth such as voice and video.

connectionless. A packet switching technology where the source and destination addresses are included in each packet so that a direct connection or an established session between sender and receiver is not required for communications. In a connectionless service, each packet is handled independently of all others, and packets might not reach their destination in the same order in which they were sent. User Datagram Protocol (UDP) is a connectionless transport service. See also connection-oriented.

Connectivity Fault Management (CFM). An Operation, Administration, and Maintenance (OAM) protocol that can manage Ethernet services and detect, verify, and isolate connectivity failures in VLANs. CFM enables service providers to configure:

- Maintenance association End Point (MEP) on a per-port, per-VLAN, or per-domain basis
- Maintenance domain Intermediate Point (MIP) on a per-port and per-level basis

CFM can operate over a LAN segment, customer VLAN (C-VLAN), service VLAN (S-VLAN), backbone VLAN (B-VLAN), or backbone identified by an I-SID (Service Instance Identifier). Defined by IEEE 802.1ag and 802.1ah.

Constrained Shortest Path First (CSPF). An extension of shortest path first (SPF). The path computed using CSPF is the shortest path that fulfills a set of constraints. After running the shortest path algorithm, the paths are pruned, removing those links that violate a given set of constraints.

See also Resource Reservation Protocol—Traffic Engineering (RSVP-TE).

Content Addressable Memory (CAM). An integrated circuit in a device that stores a table used to make frame forwarding and classification decisions. CAM can perform a massively parallel search of entries in the table much faster than a serial search than in conventional Random Access Memory (RAM).

There are two types of CAM:

- Binary CAM: A binary lookup that returns either a 1 or 0. A MAC address in an Ethernet frame comes into a switch, the switch looks in its MAC address table and either finds that MAC address or does not (1 or 0).
- Ternary CAM (TCAM): A binary lookup that returns either a 1 or 0 but also has a “do not care” bit. TCAM can have multiple matches and can determine a best match. This is necessary because Classless Interdomain Routing (CIDR) lookups need a longest prefix match. For example, 192.168.1.7/32 matches both 192.168.1.0/24 and 192.168.1.0/25. The closest match to 192.168.1.7/32 is 192.168.1.0/25 which would be chosen.

Continuity Check Message (CCM). A multicast Connectivity Fault Management (CFM) protocol data unit (PDU) transmitted periodically by a Maintenance association End Point (MEP) in ensure continuity over the Maintenance Association (MA) to which the transmitting MEP belongs.

control plane. The part of switch or router architecture that makes decisions about where traffic is sent. Control plane processing is the “signalling” of the network. Anything that is needed to get routing and switching working on a device is considered part of the control plane. The control plane serves the data plane.

The control plane functions include the manual system configuration and management operations performed by a network administrator. The control plane functions also include dynamic routing protocols such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF), or Border Gateway Protocol (BGP) that exchange topology information with other routers and construct a Routing Information Base (RIB).

The control plane functions are not performed on each arriving individual packet, so they do not have a strict speed constraint and are not time-critical.

Control plane packets are sent to or are locally originated by the device itself.

convergence. The synchronization process that a network must go through immediately after a topology change. Convergence time is the time required to update all the devices on the network with the routing information changes. See also routing table.

core layer. In the network design model, the layer that provides a transit function to access the internal network and external networks. The core layer moves packets between distribution layer devices. The core layer also links to the devices at the enterprise edge to support Internet, virtual private networks (VPN), extranet, and WAN access.

The core layer uses Layer 3 (L3) routing protocols that scale well and converge quickly such as Open Shortest Path First (OSPF).

The core serves as the backbone for the network and is critical for connecting distribution layer devices, so it is important for the core to be fast with low-latency, reliable, and scalable.

Also called backbone or trunk.

count-to-infinity. A distance-vector routing problem where if A tells B that it has a path somewhere, there is no way for B to know if the path has B as a part of it.

The count-to-infinity problem is caused by a link failure that partitions the network into two or more segments. When the network is partitioned, devices in one part of the segment cannot reach devices in the other part of the segment. The distance-vector algorithm adjusts the distance value slowly upwards toward infinity.

The count-to-infinity problem can be solved through split horizon methods.

cryptography. Rendering information unintelligible and restoring encrypted information to an intelligible form.

customer edge (CE). A device that provides an interface between a Local Area Network (LAN) and an enterprise or service provider core network. Outbound packets from the LAN are forwarded from the CE to a provider edge (PE) device, and inbound packets are forwarded from the PE to the CE.

customer VLAN (C-VLAN). In a Provider Bridging (PB) frame, a field that identifies the customer VLAN. See also service VLAN (S-VLAN). Also called C-TAG.

D

daemon. A background program that runs unattended and is usually invisible to users and that provides important system services. Pronounced “dee-mon” or “day-mon”.

Data Center Bridging (DCB). A collection of extensions for Ethernet that allows LANs and Storage Area Networks (SANs) to use a single unified fabric in a data center. DCB can carry Fibre Channel, TCP/IP, and inter-process communication traffic over a single, converged Ethernet network. DCB features include:

- Priority-based Flow Control (PFC)
- Enhanced Transmission Selection (ETS)
- Quantized Congestion Notification (QCN)
- Data Center Bridging Capability Exchange (DCBX)

Data Center Bridging Capability Exchange (DCBX). Defined in IEEE 802.1Qaz, a protocol that uses Link Layer Discovery Protocol (LLDP) to convey configuration of Data Center Bridging (DCB) features between neighbors.

data communications equipment (DCE). The interface between data terminal equipment (DTE) and a network.

Data Encryption Standard (DES). A method of data encryption using a private (secret) key. There are 72 quadrillion or more possible encryption keys that can be used. For each given message, the key is chosen at random from among these. Both the sender and the receiver must know and use the same private key.

In triple DES (3DES), a symmetric-key block cipher applies the DES cipher algorithm three times to each data block.

data link layer. See Layer 2 (L2).

data plane. The part of switch or router architecture that forwards frames and packets arriving on an interface. Routers and switches use what the control plane has built to process incoming frames and packets. The data plane forwards traffic to the next hop along the path to the destination according to the control plane logic. Data plane frames or packets go *through* the device.

Also called forwarding plane.

data terminal equipment (DTE). Any device such as a host, router, or switch connected to a network. A DTE connects to a network through data communications equipment (DCE).

default gateway. A router that connects hosts on a network segment to the Internet.

default route. A route used to forward Internet Protocol (IP) packets when a more specific route is not present in the Routing Information Base (RIB). Often represented as 0.0.0.0/0, the default route is sometimes called the “route of last resort”.

Differentiated Services (DiffServ). A mechanism to classify and manage network traffic and provide Quality of Service (QoS) guarantees for service providers. DiffServ extends the Resource Reservation Protocol—Traffic Engineering (RSVP-TE). DiffServ enables traffic to be prioritized by class, so that certain kinds of traffic, for example voice traffic, can take precedence over other types of traffic.

DiffServ redefines bits in the type of service (ToS) field of an IP packet header. DiffServ uses the Differentiated Services Code Point (DSCP) field for the QoS priority and supports 64 levels of classification.

Defined by RFC 2474; Multi-Protocol Label Switching (MPLS) support is defined in RFCs 3270 and 4124.

Differentiated Services Code Point (DSCP). A six-bit field in an IP header that enables service providers to allocate resources on a per-packet basis to meet customer requirements. See also Differentiated Services (DiffServ).

Diffie–Hellman. A method of securely exchanging cryptographic keys that allows two parties with no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

Digital Signature Algorithm (DSA). An asymmetric cryptographic algorithm that produces a digital signature in the form of a pair of large numbers. The signature is computed using rules and parameters such that the identity of the signer and the integrity of the signed data can be verified.

Dijkstra algorithm. An algorithm used by Intermediate System to Intermediate System (IS-IS) and Open Shortest Path First (OSPF) to make routing decisions based on link state. Also called shortest path first (SPF). Contrast with Bellman-Ford algorithm.

distance-vector routing. A family of routing algorithms that calculate the best route to use to send data based on information from adjacent (directly connected) routers on the network.

“Distance-vector” means that routes are advertised with two characteristics:

- Distance: How far it is to the destination based on a metric such as the number of hops, cost, bandwidth, or delay.
- Vector: The direction (exit interface) of the next hop router to reach the destination.

Each router sends its neighbors a list of networks it can reach and the distance to that network. For each network path, the receiving router picks the neighbor advertising the lowest metric, then adds this entry into its Routing Information Base (RIB). These best paths are advertised to each adjacent router.

Routing information is broadcast periodically rather than only when a change occurs, which makes the method compute- and bandwidth-intensive. For this reason, a distance-vector algorithm is best used in relatively small networks with few interrouter connections.

The Bellman-Ford algorithm is often used to determine the best path, which is used by the Routing Information Protocol (RIP).

Distance-vector routing can be prone to routing loops which are avoided through split horizon techniques.

Contrast with link-state routing and shortest-path routing.

distribution layer. In the network design model, the layer that aggregates the data received from the access layer and sends it to the core layer or to other segments of the local network. Routers or multilayer switches in the distribution layer performs many functions including:

- Routing between subnetworks and Virtual Local Area Network (VLAN) instances in the access layer
- Managing access control, routing, filtering, and QoS policies
- Managing firewalls and network address translation (NAT)
- Managing queues and prioritizing traffic
- Summarizing routes before advertising them to the core
- Isolating the core from access layer failures or disruptions

The distribution layer uses Layer 3 (L3) routing to connect to the core layer and Layer 2 (L2) switching to connect to the access layer.

Also called the aggregation layer or concentration layer.

domain. A representation of all or a subset of a network used for addressing and administrative purposes. Also refers to a collection of routers that use a common Interior Gateway Protocol (IGP). See also area and autonomous system (AS).

domain name. A meaningful and easy-to-remember name for an IP address. A domain name is a sequence of names (labels) separated by periods such as “example.com”.

Domain Name Service (DNS). A service that translates a domain name into a numeric IP address needed to locate devices. The DNS database is hierarchical. When a client such as a Web browser gives a request that specifies a host name, the DNS resolver on the client first contacts a DNS server to determine the server's IP address. If the DNS server does not contain the needed mapping, it forwards the request to a different DNS server at the next higher level in the hierarchy. After potentially several forwarding and delegation exchanges within the DNS hierarchy, the IP address for the given host eventually arrives at the client. Defined in RFCs 1034 and 1035.

dotted decimal. A method of representing an IPv4 address as four decimal numbers separated by dots, or periods; for example, 194.65.87.3. See also IP address.

double colon. A notation used to represent a consecutive block of zeroes in the middle of an IPv6 address. For example, given this address:

FE80:0000:0000:0000:0202:B3FF:FE1E:8329

With double colon notation, the address shown above becomes:

FE80::0202:B3FF:FE1E:8329

You can only use the double colon notation once in an address.

double tagged. See Provider Bridging (PB).

dynamic address. An address assigned to a device on a network with no regard to matching a specific address to that device. When a client device (such as a laptop) is given a dynamic address, it simply receives one from a pool of available addresses. It might or might not be allocated the same IP address as on previous connections. See also Dynamic Host Configuration Protocol (DHCP).

Dynamic Host Configuration Protocol (DHCP). A protocol where a client can obtain an IP address and other information such as default gateway, subnet mask, and Domain Name Service (DNS) servers, for the client to use to connect to a network. Defined in RFCs 2131 and 3315. See also Transmission Control Protocol/Internet Protocol (TCP/IP).

A DHCP server “leases” an IP address for a predetermined period of time, and reclaims the address for reassignment at the expiration of that period. DHCP greatly simplifies the administration of large networks, and networks in which nodes such as laptops, tablets, and smart phones frequently join and leave.

dynamic routing. A technique used by routing protocols where devices send and receive messages about the network topology to and from other devices and update a local Routing Information Base (RIB) used to locate the best available path to a destination.

There are different forms of dynamic routing: distance-vector routing, link-state routing, and path-vector routing. Several protocols use dynamic routing such as Border Gateway Protocol (BGP), Intermediate System to Intermediate System (IS-IS), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP).

Also called adaptive routing. Contrast with static routing.

E

east/west. The flow of traffic traversing a data center or cloud horizontally between servers. Contrast with north/south.

Edge Virtual Bridging (EVB). A mechanism that enables a virtual switch to send all traffic to an adjacent physical switch. This moves the forwarding decisions and network operations from the host CPU to the switch. EVB leverages the advanced management capabilities in access or aggregation layer switches. Defined by IEEE 802.1Qbg.

egress. Outbound or outgoing, referring to a protocol data unit (PDU) exiting a device. See also ingress.

encapsulation. The technique used by layered protocols in which a layer adds its own header information to the protocol data unit (PDU) from the layer above. As an example, in the Open Systems Interconnection (OSI) Reference Model, a PDU can contain a header for Layer 1 (L1), followed by a header for Layer 2 (L2), followed by a header for the Layer 3 (L3), followed by a header for the transport layer (Transmission Control Protocol (TCP), followed by data for the higher layers.

encryption. The process of encoding information in an attempt to make it secure from unauthorized access, particularly during transmission. The reverse of this process is known as decryption. Two main encryption schemes are in common use:

- Private (symmetrical) key: Using a private encryption key known to both the sender and the receiver of the information.
- Public (asymmetrical) key: Using a public key to encrypt and a private key to decrypt.

See also Data Encryption Standard (DES).

end-of-row switch. A chassis-based switch in a rack or cabinet at either end of the server row in a data center that connects to hundreds of servers in that row. Each cabinet in the row has cabling connecting 48 (or more) servers to the end-of-row switch. An end-of-row switch typically has redundant supervisor engines, power supplies, and overall better high availability characteristics than a Top-of-Rack (ToR) switch.

An end-of-row switch extends Layer 1 (L1) cabling topology from the switch to each rack, resulting in a smaller Layer 2 (L2) footprint and fewer Spanning Tree Protocol (STP) nodes in the topology.

Enhanced Transmission Selection (ETS). A protocol for assigning bandwidth to frame priorities. Defined in IEEE 802.1Qaz.

equal-cost multipath (ECMP). A forwarding mechanism for routing traffic along multiple paths of equal cost that ensures load balancing. The link-state routing protocols that use a cost-based metric such as Intermediate System to Intermediate System (IS-IS) and Open Shortest Path First (OSPF) explicitly allow ECMP routing.

Encapsulating Security Payload (ESP). An Internet Protocol Security (IPsec) protocol that ensures confidentiality by encrypting IP packets. An encryption algorithm combines the data in a packet with a key to transform the packet into an encrypted form. At the destination, the packet is decrypted it using the same algorithm. ESP also

ensures the integrity of a packet using a hash message authentication code (HMAC). ESP also supports an authentication scheme like that used in Authentication Header (AH), or can be used in conjunction with AH.

Ethernet. A specification for a LAN technology at Layer 1 (L1) and Layer 2 (L2) of the Open Systems Interconnection (OSI) Reference Model based on packetized transmissions between physical ports over a variety of electrical and optical media. Ethernet can transport several upper-layer protocols, the most popular of which is Transmission Control Protocol/Internet Protocol (TCP/IP). Ethernet standards are maintained by the IEEE 802.3 committee.

Ethernet uses a bus topology and CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to resolve contention when two devices try to access the network at exactly the same time. Transmission speeds range from 10 Mbps, to Fast Ethernet at 100 Mbps, to Gigabit Ethernet at 1000 Mbps.

Ethernet Linear Protection Switching (ELPS). A type of Automatic Protection Switching (APS) that specifies these techniques:

- Linear 1+1 (One-plus-One) operates with either uni-directional or bi-directional switching; normal traffic is copied and fed to both working and protection transport entities
- Linear 1:1 (One-to-One) operates with bi-directional switching; normal traffic is transported either on the working transport entity or on the protection transport entity, using a selector bridge at the source

Defined by ITU-T G.8031.

Ethernet Local Management Interface (E-LMI). An Operation, Administration, and Maintenance (OAM) protocol for communications between two User-to-Network Interface (UNI) instances. E-LMI provides both UNI and Ethernet Virtual Connection (EVC) status information to customer edge devices. This information enables automatic configuration of customer edge operation based on the configuration. Defined by Metro Ethernet Forum (MEF) 16.

Ethernet Ring Protection Switching (ERPS). A type of Automatic Protection Switching (APS) that protects traffic in a ring topology by ensuring that no loops are within the ring. Loops are prevented by blocking traffic on either a predetermined link or a failed link. ERPS integrates Operation, Administration, and Maintenance (OAM) functions with a simple APS protocol. An Ethernet ring uses normal learning, forwarding, filtering, and flooding mechanisms and a forwarding database (FDB). Defined by ITU-T G.8032.

Ethernet to the First Mile (EFM). A set of extensions to the 802.3 MAC and MAC sub layer. EFM describes technologies and the physical layer specifications for subscriber access, including remote failure detection, remote loop back, and link monitoring. Defined by IEEE 802.3ah.

Ethernet Virtual Connection (EVC). An association of two or more instances of a User-to-Network Interface (UNI). There are three types of EVC:

- In a point-to-point EVC, exactly two UNIs are associated with one another.
- In a multipoint EVC, two or more UNIs are associated with one another.
- In a rooted-multipoint EVC, one or more of the UNIs must be designated as root and each of the other UNIs must be designated as a leaf. If root, the UNI can send service frames to all other points in the EVC; if leaf, the UNI can send and receive service frames to and from root only.

Explicit Route Object (ERO). An extension to Resource Reservation Protocol (RSVP) that allows a path message to traverse an explicit sequence of routers that is independent of conventional shortest-path IP routing.

Exterior Gateway Protocol (EGP). An interdomain protocol such as Border Gateway Protocol (BGP) used to exchange network reachability information between autonomous system (AS) instances. Contrast with Interior Gateway Protocol (IGP).

F

FEC-to-NHLFE (FTN) map. In Multi-Protocol Label Switching (MPLS), a mapping from the forwarding equivalence class (FEC) of incoming packets to the corresponding Next Hop Label Forwarding Entry (NHLFE).

filtering. The process of determining whether to forward a frame or packet through a port. The simplest form of filtering is to not forward frames out the same port on which they were received. A network administrator can configure filtering manually or a device can be "self-learning" and record the source addresses of devices on each segment of a network in a filtering database.

Filtering behavior is sometimes referred to as "drop, flood, or forward":

- If the switch determines that the destination MAC is on the same port, it does not forward the frame, dropping it.
- If the switch determines that the destination MAC is on a different port, it forwards the frame on that port.
- If the switch does not know where to send the frame (or if it is multicast or broadcast), the frame is flooded out all ports (except the port it was received on).

filtering database. A data structure in a switch that maps addresses to ports, addresses to VLANs, and/or ports to VLANs. A switch learns the location of hosts by recording the source MAC address-port number association for each frame received at an incoming port. All future transmissions destined to a MAC address in the filtering database are only directed to the port associated with that MAC address unless the transmission originated on that port.

A switch can also be configured and act as several independent switches by creating VLAN associations to switch ports.

flapping. Condition of network instability when a route is announced and then withdrawn repeatedly, usually as the result of an intermittently failing link. Also called route flapping.

flooding. Forwarding a frame onto all ports except the port upon which it arrived. In Open Shortest Path First (OSPF), distributing and synchronizing the link-state database (LSDB) between routers.

flow control. Any mechanism that prevents a source from sending faster than the destination is capable of receiving.

Forward Error Correction (FEC). A system of error control that allows the receiver to correct some errors without having to request a re-transmission of data.

forwarding. Finding the output port to which a frame needs to go, and relaying the frame to that port.

forwarding equivalence class (FEC). A set of packets with similar characteristics that are forwarded in the same manner, on the same path, with the same forwarding treatment, and using the same Multi-Protocol Label Switching (MPLS) label. FECs are defined by the Label Distribution Protocol (LDP). FECs are also represented in other label distribution protocols.

Forwarding Information Base (FIB). A data structure used to find the interface to which to forward a packet. The FIB contains the minimum amount of information required to make a forwarding decision for a particular packet, such as destination prefix and nexthop. The FIB is an abbreviated form of the information in the Routing Information Base (RIB).

Also called forwarding table.

frame. A protocol data unit (PDU) at Layer 2 (L2) with addressing and protocol control information. A frame contains a header field and a trailer field that "frame" the user data. (Some control frames contain no data.)

See also packet.

G

GARP Multicast Registration Protocol (GMRP). A Generic Attribute Registration Protocol (GARP) application that allows switches to exchange multicast group information with other GMRP switches, prune unnecessary broadcast traffic, and dynamically create and manage multicast groups. See also Multiple MAC Registration Protocol (MMRP).

GARP VLAN Registration Protocol (GVRP). A Generic Attribute Registration Protocol (GARP) application that provides VLAN registration services. A switch can exchange VLAN configuration information with other GVRP switches, prune unnecessary broadcast and unknown unicast traffic, and dynamically create and manage VLANs. Defined by 802.1Q. See also Multiple VLAN Registration Protocol (MVRP).

gateway. A device that understands and converts between two different networking models. Since Transmission Control Protocol/Internet Protocol (TCP/IP) has become the dominant model, gateways are not used much at this time.

See also default gateway.

Generic Attribute Registration Protocol (GARP). A generic framework for devices to register attributes, such as VLAN identifiers and multicast group membership. See also Multiple Registration Protocol (MRP).

generic routing encapsulation (GRE). A tunneling protocol that encapsulates Layer 3 (L3) packets inside IP packets. GRE provides a virtual point-to-point link over an IP network. GRE is completely insecure, but provides a fast and simple way to access a remote network.

graceful restart. A process that allows a router whose control plane is restarting to continue forwarding traffic while recovering its state from neighboring routers. Without graceful restart, a control plane restart disrupts services provided by the router. Also called nonstop forwarding.

gratuitous ARP. Broadcast request for a router's own IP address to check whether that address is being used by another node. Used to detect IP address duplication.

H

hash message authentication code (HMAC). A method of calculating a message authentication code (MAC) using a cryptographic hash function in combination with a secret cryptographic key. As with any MAC, it can be used to simultaneously verify both the data integrity and the authenticity of a message. Any cryptographic hash function, such as MD5 or SHA-2, can be used to calculate an HMAC.

header. The portion of a protocol data unit (PDU) that contains control information for the message such as destination address, source address, input sequence number, the type of message, and priority level.

hello packet. A multicast packet that is used by protocols for neighbor discovery and recovery. Hello packets also indicate that a client is still operating and network-ready.

high availability. The ability of a system or component to limit or avoid network disruption when a component fails. High availability provides both hardware and software methods to minimize downtime and improve the performance of a network.

hold down. A state that a route is placed into so that devices will neither advertise the route nor accept advertisements about the route for a specific length of time (the hold down period). A hold down is used to flush bad information about a route from all devices in a network. A route is placed into hold down when a link in that route fails.

hop. A single link between two computer systems that a protocol data unit (PDU) must cross on its way to its destination. See also hop count.

hop count. The number of links that must be crossed to get from a source to a destination. A protocol data unit (PDU) might pass over many hops to reach its destination. If it must pass between five computers, it is said to have taken four hops to reach its destination. Hop count is often used as a metric for evaluating a route in distance-vector routing. Routing Information Protocol (RIP) uses hop count as its sole metric.

host. A computer connected to a network that is assigned a Layer 3 (L3) address and that provides an access point to that network. Similar to a node, except that host usually implies a computer system, whereas node generally applies to any networked device such as a router or switch.

hypervisor. A thin operating system designed solely to provide virtualization. A hypervisor drives physical hardware, executes virtual machine (VM) instances, and dynamically shares the underlying hardware with the associated virtual hardware. A hypervisor does not serve as a general-purpose operating system, but instead provides the platform on which VMs can run.

I

I-SID (Service Instance Identifier). A field in an I-TAG that defines the service instance to which the Provider Backbone Bridging (PBB) frame is mapped.

I-TAG. Field in the Provider Backbone Bridging (PBB) header that carries the I-SID (Service Instance Identifier) associated with the frame.

Incoming Label Map (ILM). In Multi-Protocol Label Switching (MPLS), a mapping from incoming labels to corresponding Next Hop Label Forwarding Entry (NHLFE).

ingress. Inbound or incoming, referring to a protocol data unit (PDU) entering a device. See also egress.

Institute of Electrical and Electronics Engineers (IEEE). A coordinating body for computing and communications standards. The IEEE mainly covers Layer 1 (L1) and Layer 2 (L2) of the Open Systems Interconnection (OSI) Reference Model. (Pronounced “eye-triple-ee”.) See http://www.ieee.org.

interface. The point at which a connection is made between two devices. An interface describes the logical and physical connections and usually means the same thing as the term port.

Interior Gateway Protocol (IGP). An intradomain protocol used to exchange network reachability and routing information among devices within an autonomous system (AS), such as Intermediate System to Intermediate System (IS-IS), Open Shortest Path First (OSPF), or Routing Information Protocol (RIP). Contrast with Exterior Gateway Protocol (EGP).

Intermediate System to Intermediate System (IS-IS). An Interior Gateway Protocol (IGP) that floods link state information throughout a network of routers. Each IS-IS router independently builds a database of the network's topology, aggregating the flooded network information. A Routing Information Base (RIB) is calculated from the database by constructing a shortest path tree (SPT).

Like Open Shortest Path First (OSPF), IS-IS uses the Dijkstra algorithm to find the best path through a network. Packets are then forwarded, based on the computed ideal path, through the network to the destination.

Defined by International Organization for Standardization (ISO) 10589.

internal spanning tree (IST). A special type of multiple spanning-tree instance (MSTI) that runs in an multiple spanning-tree (MST) region. An IST connects all the switches in the MST region and appears as a subtree in the common and internal spanning tree (CIST) that encompasses the entire switched domain.

An IST is identified by the number zero (0) and exists on all ports; you cannot delete the IST. By default, all VLANs are assigned to the IST. The IST is the only spanning tree instance that sends and receives bridge protocol data unit (BPDU) messages.

Any other spanning tree instance within an MST region is called a multiple spanning-tree instance (MSTI).

International Organization for Standardization (ISO). An international standards body that establishes global standards for communications and information exchange. Voting members are designated standards bodies of participating nations; American National Standards Institute (ANSI) is the U.S. member of the ISO. The Open Systems Interconnection (OSI) Reference Model is one of the ISO's most widely accepted recommendations.

Sometimes mistakenly referred to as the "International Standards Organization". Because "International Organization for Standardization" has different acronyms in different languages (IOS in English, OIN in French for *Organisation internationale de normalisation*), the founders gave it the short form ISO. ISO is derived from the Greek *isos*, meaning "equal".

For more, see http://www.iso.org/iso/home.html.

International Telecommunication Union (ITU). An international organization that develops standards for telecommunications. Formerly known as the CCITT. See http://www.itu.int.

Internet. The world's largest computer network, serving universities, commercial interests, government agencies, and private individuals. The Internet uses Transmission Control Protocol/Internet Protocol (TCP/IP) protocols, and Internet computers and devices run many different operating systems.

No government agency, single person, or corporate entity controls the Internet. All decisions on methods and standards are made by standards groups based on input from users.

See also Internet Engineering Task Force (IETF); Request for Comments (RFC).

Internet Control Message Protocol (ICMP). An Internet Protocol (IP) that provides management and control functions. Routers send ICMP messages to respond to undeliverable datagrams by placing an ICMP message in an IP datagram and then sending the datagram back to the original source. ICMP is also used by the ping (packet internet groper) command and enables a host to discover addresses of operating routers on the subnet. Defined in RFC 792.

IPv6 makes greater use of ICMP (ICMPv6 defined in RFC 4443) than IPv4, including neighbor solicitation, neighbor advertisement, router solicitation, router advertisement, and redirect.

Internet Engineering Task Force (IETF). An international community of network designers, operators, vendors, and researchers that develops Request for Comments (RFC) documents that define protocols and specifications for the Internet. The IETF mainly covers Layer 2 (L2) and Layer 3 (L3) of the Open Systems Interconnection (OSI) Reference Model. See http://www.ietf.org.

Internet Group Management Protocol (IGMP). An IPv4 protocol that allows hosts to add or remove themselves from a multicast group. Defined by RFC 3376.

IGMP enables receivers to register that they want to receive a particular multicast transmission, but does not route multicast traffic from the source to receivers. That task is left to a multicast routing protocol, such as Protocol Independent Multicast (PIM).

See also Multicast Listener Discovery (MLD), multicast group, (S,G).

Internet Key Exchange (IKE or IKEv2). An Internet Protocol Security (IPsec) protocol used to set up a security association (SA) by negotiating keys in secret. IKE builds upon Internet Security Association and Key Management Protocol (ISAKMP) using X.509 certificates for authentication and a Diffie–Hellman key exchange to set up a shared session secret from which cryptographic keys are derived. In addition, a security policy for every peer which will connect must be manually maintained.

The IKE protocol runs in two phases. The first phase establishes a ISAKMP SA which is used in the second phase to negotiate and set up the IPsec SAs.

Internet Protocol (IP). A Layer 3 (L3) protocol that provides connectionless delivery of data across heterogeneous physical networks. IP provides features for addressing, type-of-service, fragmentation and reassembly, and security. Defined by RFCs 791 and 1349.

Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet.

IP is best effort and provides no guarantees of reliability, so if packets are lost in transit, accidentally duplicated, arrive in the wrong order, or arrive corrupted, no effort is made to address the problem on the IP level—that is left to protocols a layer above, such as Transmission Control Protocol (TCP).

Internet Protocol Security (IPsec). A protocol suite for securing IP communications by authenticating and encrypting packets during a communication session. Authentication Header (AH) and Encapsulating Security Payload (ESP) are the main wire-level protocols used by IPsec. Before either AH or ESP can be used, however, the two devices must share a public key through Internet Key Exchange (IKE or IKEv2).

RFC 2401 specifies the base architecture for IPsec compliant systems. RFCs 2402, 2406, and 2407 provide more details about IPsec.

Internet Security Association and Key Management Protocol (ISAKMP). A framework for authentication and key exchange with actual authenticated keying material provided either by manual configuration with pre-shared keys or Internet Key Exchange (IKE or IKEv2). See also Internet Protocol Security (IPsec).

IP address. A unique number that identifies a device on an Internet Protocol (IP) network. IP addresses have two formats:

- An IPv4 address is 32 bits and is usually written in dotted decimal notation as four decimal numbers separated by periods. For example, 192.168.50.4 is an IPv4 address.
- An IPv6 address is 128 bits and is written in a hexadecimal notation of eight 16-bit parts separated by colons. For example, FE80:0000:0000:0000:0202:B3FF:FE1E:8329 is an IPv6 address. In the double colon address format, consecutive colons (“::”) represent successive 16-bit blocks that contain zeros: FE80::0202:B3FF:FE1E:8329. While a much larger address space is a feature, IPv6 also has other features such as multicast support, jumbograms (packets up to 4 GB in size), and stateless host auto-configuration.

Table 7-76 compares the IPv4 and IPv6 address formats.

Table 7-76: IPv6 and IPv4 Address Formats

Feature	IPv6	IPv4
Address space	128-bits = 3.4 x 1038 (340 unidecillion)	32-bits = 4.3 x 109 (4.2 billion)
Field separator	colon (:)	period (.)

Table 7-76: IPv6 and IPv4 Address Formats

Feature	IPv6	IPv4
Notation	hexadecimal	decimal
Example	db8:0:0:1	0.23.2.3

Each IP address contains a network part, an optional subnetwork part, and a host part. The network and subnetwork parts together are used for routing, while the host part is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and subnetwork parts from the IP address. Classless Interdomain Routing (CIDR) provides a way to represent IP addresses and subnet masks.

IP addresses are difficult to remember, so people tend to refer to computers by their domain names instead.

IPv6 Provider Edge (6PE). A protocol that enables IPv6 domains to communicate with each other over an Multi-Protocol Label Switching (MPLS) IPv4 core network. V6PE routers are “dual stack” and run both IPv4 and IPv6. Multiprotocol Border Gateway Protocol (BGP) (MP-BGP) in the IPv4 network is used to exchange IPv6 reachability information along with a label for each IPv6 prefix announced. Defined in RFC 4798.

Also called V6PE.

K

keepalive message. A message sent between devices when no data traffic has been detected for a given period of time. This communication verifies that the virtual and physical connection between the devices is still active.

kernel. The part of an operating system that performs basic functions such as allocating hardware resources.

KVM (Kernel-based Virtual Machine). A virtualization infrastructure for the Linux kernel that turns it into a hypervisor. KVM requires a processor with hardware virtualization technology extensions. By itself, KVM does not perform any emulation. Instead, KVM exposes an interface with which a user space host can then set up guest virtual machine (VM) instances.On Linux, QEMU (Quick EMUlator) is one such user space host.

L

Label Distribution Protocol (LDP). A protocol for distributing labels in non-traffic-engineered applications. LDP allows routers to create label-switched path (LSP) instances through a network by mapping network layer routing information directly to data-link layer switched paths.

A label is a short fixed-length, locally-significant identifier that identifies a forwarding equivalence class (FEC).

LDP works with other routing protocols such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and Border Gateway Protocol (BGP) to create LSPs.

See also Resource Reservation Protocol—Traffic Engineering (RSVP-TE).

label edge router (LER). A router that operates at the edge of an Multi-Protocol Label Switching (MPLS) network and acts as the entry and exit points for the network.

When forwarding IP packets into an MPLS domain, an LER makes the initial path selection, add the appropriate labels to the packet, and forwards the labelled packets into the MPLS domain. Likewise, upon receiving a labelled packet which is destined to exit the MPLS domain, the LER strips off the label and forwards the resulting IP packet using

normal IP forwarding rules. (Under penultimate hop popping (PHP), the popping function might be performed by an label switch router (LSR) directly connected to the LER.)

Also called an edge LSR.

label switch router (LSR). A Multi-Protocol Label Switching (MPLS) router located in the middle of a MPLS network. When an LSR receives a packet, it uses the label included in the packet header to determine the next hop on the label-switched path (LSP) and find a corresponding label for the packet from a lookup table. The old label is then removed from the header and replaced with the new label before the packet is forwarded.

Also called transit router.

label-switched path (LSP). A sequence of routers that cooperatively perform Multi-Protocol Label Switching (MPLS) operations for a packet stream. An LSP is a unidirectional, point-to-point, half-duplex connection carrying information downstream from the ingress (first) router to the egress (last) router. The ingress and egress routers cannot be the same device.

latency. Delay in the transmission through a network from source to destination. See also line rate, wire speed.

Layer 1 (L1). The physical layer in the Open Systems Interconnection (OSI) Reference Model that conveys the bit stream through electrical impulse, light waves, or radio signals through the network. L1 represents the basic network hardware and specifies the type of medium used for transmission and the network topology.

Layer 2 (L2). The data link layer in the Open Systems Interconnection (OSI) Reference Model that provides reliable transit of data across a physical link between two directly connected devices. L2 refers to physical addressing, network topology, line discipline, error notification, sequenced delivery of frames, and flow control.

L2 transfers data between network entities by splitting data into frames to send on Layer 1 (L1) and receiving acknowledgment frames. The data link layer performs error checking and retransmits frames not received correctly. In general, the data link layer controls the flow of information across the link, providing an error-free virtual channel to Layer 3 (L3).

The data-link layer has two sublayers:

- logical link control (LLC)
- Media Access Control (MAC)

Also called link layer.

Layer 3 (L3). The network layer in the Open Systems Interconnection (OSI) Reference Model that routes packets of data from source to destination across a network. L3 provides network-wide communication, including global addressing, lifetime control, fragmentation, and reassembly. Internet Protocol (IP) is an example.

Layer 4 (L4). The transport layer in the Open Systems Interconnection (OSI) Reference Model that provides logical communication between processes running on different hosts. L4 manages the end-to-end delivery of payload from a source to a destination within and between networks while maintaining the quality of service. Transmission Control Protocol (TCP) is an example.

Lightweight Directory Access Protocol (LDAP). A protocol used to locate organizations, individuals, and other resources in a network. Defined in RFC 4511. See also authentication, authorization, and accounting (AAA), Remote Authentication Dial In User Service (RADIUS), Terminal Access Controller Access Control System Plus (TACACS+).

line rate. Total number of physically transferred bits per second, including useful data and protocol overhead, over a communication link. For example, if the line rate of a link is 10 Gbps, the link transmits 10 gigabits of data every second over its physical interface. Contrast with throughput. See also latency, wire speed.

link. Communication path between two neighbor nodes.

link aggregation. A method for using multiple parallel links between a pair of devices as if they were a single higher-performance channel. The aggregated interface is viewed as a single link to each device. Spanning Tree Protocol (STP) also views it as one interface. Link aggregation can also be used to increase availability so that when there is a failure in one physical link, the remaining links stay up, and there is no disruption. Defined by IEEE 802.1AX.

Also called link aggregation group (LAG), LAG bundle, and EtherChannel. See also Link Aggregation Control Protocol (LACP), Multi-Chassis Link Aggregation (MLAG).

Link Aggregation Control Protocol (LACP). Mechanism for exchanging port and system information to create and maintain link aggregation groups.

link cost. An arbitrary number configured on an Open Shortest Path First (OSPF) interface which is used in shortest path first calculations.

Link Layer Discovery Protocol (LLDP). A mechanism for the devices on a network to advertise their identity, capabilities, and neighbors to each other. Defined by IEEE 802.1AB.

link state. Information about a link and link cost to neighboring routers.

link-state advertisement (LSA). An Open Shortest Path First (OSPF) protocol data unit (PDU) to share information on the operating state of a link, link cost, and other OSPF neighbor information. LSAs are used by the receiving routers to update their Routing Information Base (RIB)s.

link-state database (LSDB). The data structure on a router that contains all routing knowledge in a link-state network. An LSDB stores all link-state advertisement (LSA) instances produced by a link-state routing protocol such as Open Shortest Path First (OSPF) or Intermediate System to Intermediate System (IS-IS). Each router runs shortest path first (SPF) algorithm against this database to locate the best network path to each destination in the network.

link-state routing. A routing technique used by Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (IS-IS) where each router shares information with other routers by flooding information about itself to every reachable router in the area. Link-state protocols use characteristics of the route such as speed and cost to determine the best path. Link-state information is transmitted only when something has changed in the network.

Every router constructs a map of the connectivity of the network, determining the interconnections between all routers. As a router receives an advertisement, it stores this information in a link-state database (LSDB). Each router then independently calculates the best next hop from it to every possible destination in the network using the shortest path first (SPF) algorithm to build a shortest path tree (SPT) with itself as the center of that tree. The shortest path to each reachable destination within the network is found by traversing the tree. The collection of best next hops forms the router's Routing Information Base (RIB).

Link-state algorithms create a consistent view of the network and are therefore not prone to routing loops, but they achieve this at the cost of more computing cycles and more traffic compared to distance-vector routing.

See also Dijkstra algorithm.

Linktrace Message (LTM). A Connectivity Fault Management (CFM) protocol data unit (PDU) initiated by a Maintenance association End Point (MEP) to trace a path to a target MAC address, forwarded from Maintenance domain Intermediate Point (MIP) to MIP, up to the point at which the LTM reaches its target MEP.

Linux. A Unix-like computer operating system assembled under the model of free and open source software development and distribution. The defining component of Linux is the kernel, the central part of the operating system that manages system services. Many people use the name “Linux” to refer to the complete operating system package which is called a Linux distribution which is made up of a collection of software based around the Linux kernel.

Linux has since been ported to more computer hardware platforms than any other operating system and is available for a wide variety of systems from small embedded systems up to supercomputers. In particular, networking devices such as switches and routers almost universally run some Linux distribution.

As an open operating system, Linux is developed collaboratively, meaning no one organization is solely responsible for its development or ongoing support. Companies participating in the Linux community share research and development costs with their partners and competitors.

Local Area Network (LAN). A group of computers and devices connected by a communications channel, capable of sharing resources among several users. LANs are based on a small physical area such as a building, floor, or department. LANs can connect to a wide area network (WAN). Ethernet is the most popular LAN technology.

logical link control (LLC). The higher sublayer of Layer 2 (L2) in the Open Systems Interconnection (OSI) Reference Model. The LLC sublayer provides the interface for Layer 3 (L3) and handles error control, flow control, framing, and MAC-sublayer addressing. The most prevalent LLC protocol is IEEE 802.2, which includes both connectionless and connection-oriented variants. See also Media Access Control (MAC).

loopback. A troubleshooting test in which a signal is transmitted from a source to a destination and then back to the source again so that the signal can be measured and evaluated.

M

MAC address. A permanent, unique serial number that uniquely identifies a network device among all other network devices in the world. MAC addresses are 12-digit numbers, 48 bits in length. MAC addresses are usually written as six groups of two hexadecimal digits, separated by hyphens (“-”) or colons (“:”):

MM:MM:MM:SS:SS:SS

MM-MM-MM-SS-SS-SS

Each pair of hexadecimal digits represents one byte of the 6-byte (48-bit) address.

An example of a MAC address is 68:A3:C4:3B:8D:24:

- The first three parts (68:A3:C4) identify the manufacturer (Liteon Technologies)
- The second three parts (3B:8D:24) is the serial number assigned by the manufacturer

At Layer 2 (L2), other devices use MAC addresses to locate specific ports in a network, and to create and update a Routing Information Base (RIB). A MAC address maps to an IP address through the Address Resolution Protocol (ARP).

Also called physical address, Ethernet address, or hardware address.

MAC-in-MAC. See Provider Backbone Bridging (PBB).

Maintenance Association (MA). In Connectivity Fault Management (CFM), a set of Maintenance association End Point (MEP) instances, each configured with the same MAID (Maintenance Association Identifier) and Maintenance Domain (MD) Level, established to verify the integrity of a single service instance.

Maintenance association End Point (MEP). A Connectivity Fault Management (CFM) entity at the edge of a Maintenance Domain (MD) that confines CFM messages within the domain via the MD level. MEPs periodically transmit and receive Continuity Check Message (CCM) instances from other MEPs within the domain. MEPs are either “Up” (toward the switch) or “Down” (toward the wire).

Maintenance Domain (MD). In Connectivity Fault Management (CFM), the network or the part of the network for which faults in connectivity can be managed.

Maintenance domain Intermediate Point (MIP). A Connectivity Fault Management (CFM) entity that catalogs and forwards information received from Maintenance association End Point (MEP) instances. MIPs are passive points that respond only to CFM Linktrace Message (LTM) and loopback messages.

Management Information Base (MIB). A specification of objects used by Simple Network Management Protocol (SNMP) to monitor or change network settings. MIBs provides a logical naming scheme for resources on a network. A MIB contains information about a device such as settings, usage statistics, performance data, or physical properties (such as temperature or fan speed). MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches. Standard MIBs are defined by the IETF.

Maximum Transmission Unit (MTU). The maximum number of bytes in a packet or frame. For Ethernet, the default MTU is 1500 bytes (data payload), but each media has different sizes. The Ethernet MTU is defined in RFC 894.

Media Access Control (MAC). The lower sublayer of Layer 2 (L2) in the Open Systems Interconnection (OSI) Reference Model. The MAC sublayer provides addressing and channel access control mechanisms that make it possible for several network nodes to communicate within a multiple-access network that uses a shared medium such as Ethernet. The MAC sublayer is the interface between the logical link control (LLC) sublayer and Layer 1 (L1).

mesh. A physical or logical network topology in which devices have many redundant interconnections. A full mesh is when all devices in a network have a connection to all other devices, a partial mesh is when some devices have a connection to all other devices.

Metro Ethernet Forum (MEF). A defining body for Carrier Ethernet with many participating organizations including service providers, and network hardware and software manufacturers. The MEF's mission is to accelerate the worldwide adoption of carrier-class Ethernet networks and services. For more, see http://metroethernetforum.org/.

Multi-Chassis Link Aggregation (MLAG). A technique that extends the link aggregation concept. At either one or both ends of a link aggregation group, a single aggregation system is replaced by a *portal* that is a collection of one to three portal systems. Defined by IEEE 802.1AX.

Also called MC-LAG and Distributed Resilient Network Interconnect (DRNI).

Multi-Protocol Label Switching (MPLS). A method for forwarding packets through a network. MPLS operates between the traditional definitions of Layer 2 (L2) and Layer 3 (L3).

In a traditional IP network, each router performs an IP lookup to determine a next hop based on its routing table, and forwards the packet to that next hop. Every router in the path repeats this process, making its own independent routing decisions, until the final destination is reached.

In an MPLS network, the first device does a routing lookup, but instead of finding a next hop, it finds the final destination router and finds a pre-determined path from the source to the destination. The router applies a "label" based on this information. Other routers in the path use the label to route the traffic without needing to perform any additional IP lookups.

At each incoming (ingress) point of the network, packets are assigned a label by a label edge router (LER). Packets are forwarded along an label-switched path (LSP) where each label switch router (LSR) makes forwarding decisions based on the label information. At each hop, an LSR swaps the existing label for a new label that tells the next hop how to forward the packet. At the outgoing (egress) point, an LER removes the label, and forwards the packet to its destination via IP routing.

MPLS enables these applications: Virtual Private Network (VPN), traffic engineering (TE), and Quality of Service (QoS).

See also Label Distribution Protocol (LDP), Resource Reservation Protocol—Traffic Engineering (RSVP-TE).

Multi-Protocol Label Switching - Transport Profile (MPLS-TP). A subset of Multi-Protocol Label Switching (MPLS) with extensions that address transport network requirements. The extensions provide the same QoS, protection and restoration, and Operation, Administration, and Maintenance (OAM) as in SONET/SDH. In MPLS-TP, some of the MPLS functions are turned off, such as penultimate hop popping (PHP), label-switched path (LSP) merge, and equal-cost multipath (ECMP).

The use of a control plane protocol is optional in MPLS-TP. The control plane can set up an LSP automatically across a packet-switched network domain. However, some network operators might prefer to configure the LSPs statically without using an IP or routing protocol.

multicast. The process of a single host sending messages to a selected group of receivers. See also broadcast, unicast.

multicast group. A collection of hosts receiving packets from a host that is transmitting multicast packets. Only hosts that need to hear a particular multicast declare that requirement. A multicast group restricts traffic to just those paths between the sources and destinations associated with the multicast address. Membership is dynamic; when a host joins a group, it starts receiving the datastream, and when a host leaves a group, it stops receiving the datastream. When there are no more members, the group simply ceases to exist.

See also GARP Multicast Registration Protocol (GMRP), Internet Group Management Protocol (IGMP), Multicast Listener Discovery (MLD), Multiple MAC Registration Protocol (MMRP), (S,G).

Multicast Listener Discovery (MLD). An IPv6 protocol that allows hosts to add or remove themselves from a multicast group. Defined by RFC 3810.

See also Internet Group Management Protocol (IGMP), multicast group, (S,G).

Multiple MAC Registration Protocol (MMRP). A protocol that manages multicast group MAC addresses. In addition, MMRP improves the convergence time of GARP Multicast Registration Protocol (GMRP). Defined by 802.1ak.

Multiple Registration Protocol (MRP). A generic registration framework with protocols, procedures, and managed objects for switches to register attributes with other switches in a LAN. Defined by 802.1ak. MRP replaces Generic Attribute Registration Protocol (GARP)

Multiple Spanning Tree Protocol (MSTP). An enhancement to the Rapid Spanning Tree Protocol (RSTP) where a separate spanning tree for can be configured for a VLAN group. Each VLAN group belongs to a multiple spanning-tree instance (MSTI). Several MSTIs can run in an multiple spanning-tree (MST) region, with each region interconnected in a common and internal spanning tree (CIST).

MSTP is backward compatible with both RSTP and Spanning Tree Protocol (STP).

Originally defined in IEEE 802.1s and later merged into 802.1Q.

multiple spanning-tree (MST) region. A collection of interconnected switches that have the same Multiple Spanning Tree Protocol (MSTP) configuration which includes region name, revision number, and VLAN-to-instance map. Each MST region can contain multiple instances of spanning trees. The network administrator must properly configure participating switches throughout the region. All regions are bound together using a common and internal spanning tree (CIST), which creates a loop-free topology across regions. An MST region appears as a single switch to spanning tree configurations outside the region.

multiple spanning-tree instance (MSTI). A group of VLANs in a spanning-tree instance managed by Multiple Spanning Tree Protocol (MSTP) within an multiple spanning-tree (MST) region. Within each MST region, MSTP maintains multiple spanning-tree instances. Each instance has a spanning-tree topology independent of other

spanning-tree instances. An MSTI provides a fully connected active topology for frames belonging to a VLAN. You can assign a VLAN to only one spanning-tree instance at a time.

An internal spanning tree (IST) is a special type of MTSI.

Multiple VLAN Registration Protocol (MVRP). A protocol that manages registration of VLANs, tracking which routers are members of which VLANs and which router interfaces are in which VLAN. MVRP removes routers and interfaces from the VLAN information when they become unavailable. MVRP improves the convergence time of GARP VLAN Registration Protocol (GVRP). Defined by 802.1ak.

N

name resolution. The process of translating an IP address to a name that is easily remembered by a person. In a TCP/IP environment, a name such as www.example.com is translated into its IP equivalent by the Domain Name Service (DNS).

neighbor. An adjacent system reachable by traversing a single subnetwork; an immediately adjacent device. Also called peer. See also adjacency.

Neighbor Discovery Protocol (NDP). An IPv6 protocol that nodes on the same link use to discover each other's presence, determine each other's Link Layer addresses, find routers, and maintain reachability information about the paths to active neighbors. NDP is defined in RFC 2461 and is equivalent to the Address Resolution Protocol (ARP) used with IPv4.

NETCONF (Network Configuration Protocol). A mechanism to install, manipulate, and delete the configuration of network devices. The operations, notifications, and the database contents supported by a particular NETCONF server are extensible, and defined with a modeling language called YANG. The database is used to store YANG data structures which represent the configuration of the device containing the NETCONF server. This configuration can be saved in non-volatile storage so the configuration can be restored upon reboot. Defined in RFC 6241.

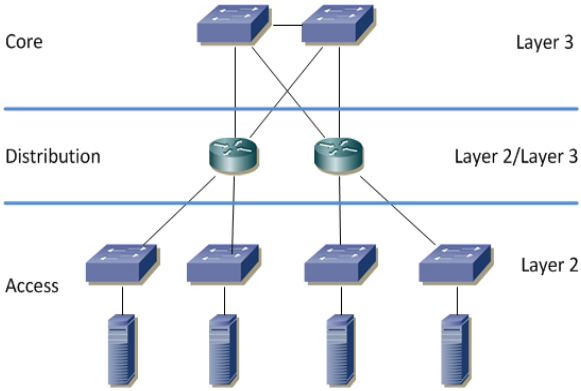
network. A group of computers and related devices connected by a communications channel capable of sharing resources among several users. A network consists of transmission media, devices such as routers or switches, and protocols that make message sequences meaningful.

A network can range from a peer-to-peer network connecting a small number of users in an office or department, to a Local Area Network (LAN) connecting many users, to a wide area network (WAN) connecting users on several networks spread over a wide geographic area.

network address translation (NAT). A method to use one set of IP addresses for an internal inetwork and a second set of addresses for the public Internet. This allows an organization to shield internal addresses from the public Internet. NAT is configured on the router at the border of an internal network and the Internet. NAT translates the internal local addresses to globally unique IP addresses before sending packets to the Internet and vice versa. Defined by RFC 1631.

network administrator. The person responsible for the day-to-day operation and management of a network.

network design model. A hierarchical model originally defined by Cisco that divides a network into three functional areas, or layers. This model optimizes network hardware and software to perform specific roles.



The roles that each layer performs are:

- The access layer provides local user access to the network
- The distribution layer connects network services to the access layer, and implements policies regarding security, traffic loading, and routing
- The core layer provides high-speed transport for the distribution layer

See also collapsed core.

Network Element (NE). Any device in a network such as a host, router, switch, or firewall that performs a service or function for the network.

Network Functions Virtualization (NFV). The ability to decouple network services from dedicated hardware devices to be hosted on a virtual machine (VM). Once the network services are under the control of a hypervisor, the services can be performed on standard x86 servers.

network layer. See Layer 3 (L3).

network segment. A portion of a computer network that is separated from the rest of the network by a device such as a router or switch. Each segment can contain one or more hosts.

Network Services Module (NSM). The base module in OcNOS that communicates with every OcNOS routing and switching process. The protocol components use APIs exposed by the NSM client, which act as conduits to transfer data between the protocol modules and NSM.

Network Time Protocol (NTP). A protocol used to synchronize the system clocks of hosts on a network to Universal Coordinated Time (UTC). A device can update its clock automatically by configuring itself as an NTP client. Using NTP enables the device to record accurate times of events. Defined by RFC 5905.

Neutron. The networking component of OpenStack that provides “networking as a service” between virtual NICs managed by other OpenStack services.

Neutron provides a “plug-in” mechanism that lets network operators enable different technologies. It also lets tenants create multiple private networks and control their IP addressing. Organizations have control over security and compliance policies, Quality of Service (QoS), monitoring and troubleshooting, as well as the ability to deploy network services, such as a firewall, intrusion detection, and Virtual Private Network (VPN) instances.

next hop. The next device to which a protocol data unit (PDU) is sent on its way to its destination.

Next Hop Label Forwarding Entry (NHLFE). An Multi-Protocol Label Switching (MPLS) entry containing next hop information (interface and next hop address) and label manipulation instructions; it can also include label encoding, L2 encapsulation information, and other information to process packets in the associated stream.

node. An addressable device such as a host, router, or switch, attached to a network, that transmits and receives data.

north/south. The flow of traffic traversing between users and a data center (spanning-tree). Contrast with east/west.

northbound. An interface that allows a network component to communicate with a higher-level component. A northbound interface hides complex details of operations. Northbound flow can be thought of as going upward. In architectural diagrams, northbound interfaces are drawn at the top of the component. See also southbound.

Not-So-Stubby-Area (NSSA). An extension of a Open Shortest Path First (OSPF) stub area. OSPF uses an NSSA as a transit to send external routes to other areas or to domains that are not part of the OSPF autonomous system. OSPF does not flood external routes from other areas into an NSSA, but does translate and flood route information from the NSSA into other areas such as the backbone. Defined by RFC 1587.

O

Open Network Foundation (ONF). A non-profit organization responsible for the development and standardization of a software architecture that supports Software-Defined Networking (SDN). ONF is also responsible for the commercialization and promotion of SDN as a concept and its underlying technologies. For more, see: https://www.opennetworking.org/.

Open Shortest Path First (OSPF). An Interior Gateway Protocol (IGP) based on link-state routing. OSPF is widely deployed in large networks because of its efficient use of network bandwidth and its rapid convergence after changes in topology. Defined in RFCs 2328 and RFC 5340.

OSPF advertises the states of local network links within an autonomous system (AS) and makes routing decisions based on the shortest path first (SPF) algorithm. Each OSPF router maintains an identical database describing the autonomous system's topology. From this database, a Routing Information Base (RIB) is calculated by constructing a shortest path tree (SPT).

OSPF features include least-cost routing, multipath routing, and load balancing. OSPF includes explicit support for Classless Interdomain Routing (CIDR) and the tagging of externally derived routing information.

OSPF version 2 supports IPv4 and OSPF version 3 supports IPv6.

OSPF divides an autonomous system into contiguous groups of networks called areas.

- In a standard area, intra-area routes, inter-area routes, and external routes (learned from other routing protocols such as RIP and BGP) are distributed. Inter-area routes and external routes are distributed as summary addresses.
- A backbone area is essentially a standard area which has been designated as the central point to which all other areas connect. A backbone area combines a set of independent areas into an AS and acts as a hub for inter-area transit traffic and routing information distribution. Each non-backbone area is directly connected to the backbone area.
- OSPF uses stub area instances and Not-So-Stubby-Area (NSSA) instances to limit distribution of inter-area routes and external routes.

See also area border router (ABR), autonomous system border router (ASBR).

Open Systems Interconnection (OSI) Reference Model. A conceptual model defined by the International Organization for Standardization (ISO) that organizes the computer-to-computer communications process into seven layers. Each layer provides services to the layer above and receives services from the layer below. Such a set of layers is called a protocol stack.

Layers seven through five manage end-to-end communications between the message source and destination, while layers one through four manage network access:

- Layer 4 (L4) ensures the end-to-end delivery from a source to a destination
- Layer 3 (L3) routes packets of data from source to destination across a network
- Layer 2 (L2) reliably transports data across the physical link between two directly connected nodes
- Layer 1 (L1) conveys the bit stream at the electrical and mechanical level

The OSI Reference Model is often compared to the more descriptive (versus prescriptive) Transmission Control Protocol/Internet Protocol (TCP/IP) model.

Open vSwitch (OVS). A software switch used in virtualized server environments that forwards traffic between different virtual machine (VM) instances on the same physical host and between VMs and the physical network. OVS enables network automation through programmatic extension, while still supporting standard management interfaces and protocols. For more, see http://openvswitch.org/.

OpenStack. A cloud operating system that controls pools of compute, storage, and networking resources in a data center which users manage through a Web-based dashboard, command-line tools, or a RESTful API. See also Neutron.

Operation, Administration, and Maintenance (OAM). A set of Ethernet specifications that provide connectivity monitoring, fault detection and notification, fault verification, fault isolation, loopback, and remote defect identification. The primary specifications are 802.3ah link-fault management (LFM) and 802.1ag Connectivity Fault Management (CFM).

P

packet. A protocol data unit (PDU) at Layer 3 (L3) of the Open Systems Interconnection (OSI) Reference Model. A packet contains source and destination addresses, user data, and control information such as the length of the packet, the header checksum, and flags indicating whether the packet has been fragmented. The user data in a packet is often referred to as the payload. The actual format of a packet depends on the protocol that creates the packet.

A packet sent through a connectionless protocol such as User Datagram Protocol (UDP) is sometimes called a datagram.

See also frame, packet switching.

packet switching. A data-transmission method that transmits information over one of several routes. Information is sent to the destination through the best route, determined by a routing algorithm.

A packet switched network breaks information to be transmitted into discrete packets. Related packets might not all follow the same path to their destination. Packet sequence numbers are used to reassemble the original message at the destination.

A packet-switched network is connectionless because each packet contains its destination address and does not require a dedicated path to reach that destination. Multiple users may transmit packets over the same connection at the same time, independent of one another.

The Internet is an example of a packet-switched network.

Contrast with circuit switching.

paravirtualized. A software component that is aware that it is running in a virtual machine (VM). For example, a paravirtualized virtual device driver runs in a VM that communicates with the underlying host OS. Typically, a paravirtualized driver is optimized to share queues, buffers, or other data items with the underlying host OS to improve throughput and reduce latency.

path computation element (PCE). An entity (component, application, or server) that can compute a network path or route based on a network graph and constraints (see RFC 4655).

path-vector routing. A routing technique that advertises a network as a destination address and a complete path to reach that destination. Each entry in the Routing Information Base (RIB) contains the destination network, the next router, and the path to reach the destination.

A path vector protocol guarantees loop-free paths by recording each hop the routing advertisement traverses through the network. A node can easily detect a loop by looking for its own node identifier in the path.

This technique is sometimes used in Bellman-Ford algorithm to avoid count-to-infinity problems.

Border Gateway Protocol (BGP) is an example of a prefix-based path-vector protocol where the Routing Information Base (RIB) maintains the autonomous systems to traverse to reach a destination.

peer. Immediately adjacent device with which a protocol relationship has been established. Also called neighbor.

penultimate hop popping (PHP). A technique where the outermost label of an Multi-Protocol Label Switching (MPLS) packet is removed by a label switch router (LSR) before the packet is passed to an adjacent label edge router (LER).

physical layer. See Layer 1 (L1).

ping (packet internet groper). A command used to test network connectivity by transmitting an Internet Control Message Protocol (ICMP) diagnostic packet to a specific node on the network, forcing the node to acknowledge that the packet reached the correct destination. If the node responds, the link is operating; if not, something is wrong.

The word ping is often used as a verb, as in “ping that workstation to see if it is alive.”

policing. Applying rate limits on bandwidth and burst size for traffic for a particular interface.

policy-based routing (PBR). Classifying packets to determine their forwarding path within a device. PBR is used to redirect traffic for analysis. Also called filter-based forwarding (FBF).

port. The point at which a communications circuit terminates on a network. A port can be logical, physical or both. Examples include:

- The physical interface between a device and a communications circuit, usually identified by a number or name.
- The logical interface between a TCP/IP applications and a communications facility which use well-known port numbers such as FTP: 20, HTTP: 80, and NFS: 2049.
- The logical interface between a process and a communications facility that allows more than one logical port to be associated with one physical port. For example, Ethernet uses multiple MAC addresses to distinguish between separate logical channels connecting two ports on the same physical transport network interface.

Also called interface.

Precision Time Protocol (PTP). A protocol that synchronizes clocks throughout a computer network. On a LAN, PTP achieves clock accuracy in the sub-microsecond range, making it suitable for measurement and control systems.

The time synchronization is achieved through packets that are transmitted and received in a session between a master clock and a slave clock. Defined by IEEE 1588v2.

Priority-based Flow Control (PFC). A flow control mechanism that can be set independently for each frame priority on full-duplex links. Defined by IEEE 802.1Qbb.

private VLAN (PVLAN). A switch with ports that cannot communicate with each other, but can access other networks. A PVLAN has at least one private port and a trunk port. All traffic received on a private port is forwarded out the trunk port. All traffic received on a trunk port is handled as normal switch traffic. No traffic communication occurs between the private ports.

protocol. A set of rules that end points in a network connection must follow when they communicate. A protocol includes data representation, data item ordering, message formats, message and response sequencing rules, block data transmission conventions, and timing requirements.

The Open Systems Interconnection (OSI) Reference Model and Transmission Control Protocol/Internet Protocol (TCP/IP) are both used as a model for many protocols. There are one or more protocols at each layer in the models that both ends of the connection must recognize and observe.

protocol data unit (PDU). A unit of data transmitted as a composite by a protocol.

In the Open Systems Interconnection (OSI) Reference Model, the actual name used for a PDU depends on the layer:

- Layer 4 (L4): segment
- Layer 3 (L3): packet
- Layer 2 (L2): frame
- Layer 1 (L1): stream, symbol stream, or bit stream

See also bridge protocol data unit (BPDU). Sometimes called datagram.

Protocol Independent Multicast (PIM). A method to determine the best paths for distributing a multicast transmission. PIM uses unicast routing tables (such as those used by Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP)) and static routes to perform multicasting. Each host must be registered using IGMP to receive the transmission.

PIM has these variations:

- PIM dense mode (PIM-DM: RFC 3973) uses a push model. PIM-DM initially floods multicast traffic throughout the network. Routers that have no downstream neighbors prune back the unwanted traffic. This process repeats periodically.
- PIM sparse mode (PIM-SM: RFC 4601) uses a pull model. PIM-SM uses a shortest path tree (SPT) where sources forward multicast packets to a designated router which unicasts the packets to an assigned rendezvous point router, which then forwards the packets to members of multicast groups.
- PIM source-specific multicast (PIM-SSM: RFC 3569) uses PIM-SM functionality to create a SPT between the client and the source without using a rendezvous point.
- Bidirectional PIM (Bidir-PIM: RFC 5015) uses PIM-SM functionality to route traffic only along a bidirectional SPT that is rooted at the rendezvous point for a group.

protocol stack. The layers of software used in network communications.

Provider Backbone Bridge-Traffic Engineering (PBB-TE) . An extension to Provider Backbone Bridging (PBB) that removes features such as flooding, dynamically created forwarding tables, and spanning tree protocols. PBB-TE also covers Connectivity Fault Management (CFM) and Ethernet Linear Protection Switching (ELPS).

In PBB-TE, a network administrator configures the forwarding tables in the backbone switches with static routes to ensure that frames take predetermined paths within the network. Frames with destination MAC addresses not in a forwarding table are dropped. Broadcast frames are not supported and are also dropped by backbone switches.

Defined in IEEE 802.1Qay.

Provider Backbone Bridging (PBB). A technique to create Ethernet backbones for service access networks. Defined in IEEE 802.1ah, PBB extends Provider Bridging (PB) defined in 802.1ad in these ways:

- The 802.1ah header adds an I-SID (Service Instance Identifier) which is a label that maps to a customer VLAN identifier. An I-SID virtualizes VLANs across a network. VLANs are mapped into I-SIDs by configuring only the edge of the network at a backbone edge bridge (BEB). This makes the maximum number of service instances 16 million.
- The 802.1ah header encapsulates backbone source and destination MAC addresses (B-MAC) along with the customer source and destination MAC addresses (C-MAC). The B-MAC contains MAC addresses of the service provider's PBB edge switches. The 802.1ah format is sometimes called “MAC-in-MAC” because of this MAC address encapsulation. The encapsulation of customer MAC addresses in backbone MAC addresses means that the backbone does not need to learn customer MAC addresses. Customer MAC addresses are learned at BEB ports only.

Provider Bridging (PB). A technique that enables a service provider to use the architecture and protocols of 802.Q to offer the equivalent of separate LANs, bridged LANs, or VLANs to multiple customers. Provider bridging requires no active cooperation between customers and requires minimal cooperation between an individual customer and the service provider.

When VLANs were originally defined in 802.1Q, the number of unique VLAN identifiers was limited to 4096. In large provider networks, each subscriber needs a separate address, so this limit could prevent a provider from having more than 4096 subscribers.

To overcome this limit, 802.1ad inserts an additional VLAN tag into a single 802.1Q Ethernet frame. Frames passing through the provider network are doubly tagged with:

- customer VLAN (C-VLAN) tag which identifies the customer network VLAN
- service VLAN (S-VLAN) tag which identifies the service provider network VLAN

With two VLAN identifiers in combination for each provider-customer pair, it is possible to define up to 16,777,216 VLANs.

The frame format for 802.1ad is also called Q-in-Q, double tagged, stacked VLANs, or VLAN stacking.

provider edge (PE). A device at the edge of an enterprise or service provider core network. A PE offers an initial, first level of network traffic aggregation for many customer edge (CE) devices.

pseudowire (PW). An emulation of a point-to-point connection over a packet-switching network. A pseudowire is a way to transport legacy services such as TDM over a packet-switched network:

- Structure-aware TDM circuit emulation service over packet-switched network (CESoPSN)
- Structure-agnostic TDM over packet (SAToP)

A pseudowire that both originates and terminates on the edge of a single packet-switched network (autonomous system or carrier network) is called a single-segment pseudowire (SS-PW). A pseudowire that extends through multiple autonomous systems or carrier networks is called a multi-segment pseudowire (MS-PW).

Q

Q-in-Q. See Provider Bridging (PB).

QEMU (Quick EMUlator). A hosted hypervisor that performs hardware virtualization. QEMU emulates CPUs through dynamic binary translation and provides a set of device models enabling it to run a variety of unmodified guest operating systems. QEMU also can be used together with KVM (Kernel-based Virtual Machine) to run virtual machines at near-native speed (requiring hardware virtualization extensions on x86 machines). QEMU can also be used purely for CPU emulation for user-level processes, allowing applications compiled for one architecture to be run on another.

Quality of Service (QoS). The ability to *guarantee* the delivery, control the bandwidth, set priorities for specific network traffic, and provide an appropriate level of security. QoS provides a level of predictability and control beyond the best effort delivery that a device provides by default.

See also Class of Service (CoS).

Quantized Congestion Notification (QCN). An end-to-end congestion management scheme for protocols capable of transmission rate limiting. Defined by IEEE 802.1Qau.

R

radio access network (RAN). The air interface and base station technology in a cellular network. In addition to the RAN, the entire cellular system includes the core network, which provides the backbone and services, as well as the cellphones.

Rapid Per-VLAN Spanning Tree Plus (RPVST+). A version of Cisco Per VLAN Spanning Tree Plus (PVST+) that uses the Rapid Spanning Tree Protocol (RSTP) state machine. PVST+ runs a spanning tree instance for each VLAN in the network. PVST+ is not scalable when there are many VLANs in a network. A compromise between RSTP and R-PVST+ is Multiple Spanning Tree Protocol (MSTP) which runs multiple instances of spanning tree that are independent of VLANs. MSTP maps a set of VLANs to each spanning tree instance.

Rapid Spanning Tree Protocol (RSTP). An enhancement to the Spanning Tree Protocol (STP) that re-configures quickly after a topology change. RSTP can verify if a port can change to a forwarding state safely without waiting for timers to start convergence. RSTP is not aware of VLANs and blocks ports at the physical level. Defined by IEEE 802.1D. See also Multiple Spanning Tree Protocol (MSTP).

Remote Authentication Dial In User Service (RADIUS). An authentication and accounting protocol to authenticate users and authorize their access to the requested system or service.

Defined in RFCs 2058, 2059, and 2865. See also authentication, authorization, and accounting (AAA), Lightweight Directory Access Protocol (LDAP), Terminal Access Controller Access Control System Plus (TACACS+).

remote monitoring (RMON). A Management Information Base (MIB) specification that defines functions for remotely monitoring networked devices. The RMON specification provides many problem detection and reporting capabilities. Defined by RFC 2819.

Request for Comments (RFC). Proposals and standards that define protocols for communications over the Internet. RFCs are developed and published by the Internet Engineering Task Force (IETF).

Resource Reservation Protocol (RSVP). A signalling protocol for reserving resources across a network. RSVP is rarely used by itself, but Resource Reservation Protocol—Traffic Engineering (RSVP-TE) is widely used.

Resource Reservation Protocol—Traffic Engineering (RSVP-TE). RSVP with traffic engineering extensions, as defined by RFC 5101, that allows RSVP to establish label-switched path (LSP) instances in Multi-Protocol Label Switching (MPLS) networks, using Constrained Shortest Path First (CSPF), taking into consideration constraints such as available bandwidth and explicit hops. The LSPs might not agree with the route suggested by the Open Shortest Path First (OSPF) or Intermediate System to Intermediate System (IS-IS).

reverse path forwarding (RPF). An algorithm that checks the unicast Routing Information Base (RIB) to determine whether there is a shortest path back to the source address of an incoming multicast packet. Unicast RPF helps determine the source of denial-of-service attacks and rejects packets from unexpected source addresses.

Rivest-Shamir-Adleman (RSA). A public key, or asymmetric, encryption scheme. The oretical background to RSA is that it is difficult to find the factors of a very large number that is the product of two prime numbers. RSA is considered very secure provided a sufficiently long key is used.

route. The path from source to destination through a network.

route flap damping. Method for minimizing instability caused by route flapping. The router stores a penalty value for each route. Each time the route flaps, the router increases this value. If the penalty for a route reaches a configured suppress value, the router does not include the route as a forwarding entry and does not advertise the route to peers.

route redistribution. One protocol learning routes from another protocol running on the same device. Also called redistribution or route leakage.

route reflection. A method of allowing iBGP routers to accept and propagate iBGP routes to their clients.

To avoid routing loops, Border Gateway Protocol (BGP) does not advertise routes learned from an internal BGP peer to other internal BGP peers. Instead, BGP requires that all internal peers be fully meshed so that any route advertised by one router is advertised to all peers within the autonomous system (AS). As a network grows, the full mesh requirement becomes difficult to manage. To handle scaling problems, BGP uses route reflection and BGP confederations.

Route reflection allows you to designate one or more routers as route reflectors. BGP relaxes the re-advertising restriction on route reflectors, allowing them to accept and propagate iBGP routes to their clients.

route summarization. Consolidating multiple routes into a single route advertisement, in contrast to flat routing where a Routing Information Base (RIB) contains a unique entry for each route.

Classless Interdomain Routing (CIDR) is used to implement route summarization. All IP addresses in the route advertisement must have identical high-order bits.

Also called route aggregation. See also subnet mask.

router. A Layer 3 (L3) device that makes decisions about the paths over which network traffic will flow. Routers use dynamic routing protocols to learn about the network and to find the best route to forward packets toward their final destination:

1. Find a matching destination address in the Routing Information Base (RIB)
2. Find the MAC address for the packet from the Address Resolution Protocol (ARP) cache
3. Write the new MAC address in the IP packet
4. Send the packet on the port associated with the MAC address

routing. The process of finding a path to a destination to use to transmit a protocol data unit (PDU) over a network. Routing is usually controlled by a Routing Information Base (RIB) which defines where a PDU should go. Each router only needs to know where a PDU should be sent on its next hop, and does not know nor care what happens afterward; the next hop plus one is the responsibility of the next router, and so on through the network until a PDU reaches its destination.

Routing Information Base (RIB). A data structure in a device that lists the routes to destinations and metrics (distances) associated with those routes. A RIB contains information about the topology of the network immediately around it. Maintaining a RIB by discovering network topology is the primary purpose of dynamic routing protocols such as Border Gateway Protocol (BGP), Routing Information Protocol (RIP), and Open Shortest Path First (OSPF). Network administrators can also add fixed routes to the RIB for static routing.

Also called a routing table. Contrast with Forwarding Information Base (FIB).

Routing Information Protocol (RIP). An Interior Gateway Protocol (IGP) that implements a distributed variant of the Bellman-Ford algorithm to provide distance-vector routing capabilities. RIP uses the hop count of a destination to detect the best path to route packets, but limits the maximum number of hops to 15 to prevent routing loops. RIP implements split horizon techniques. Defined in RFC 1058.

RIP is easy to configure and has low processing requirements. However, the hop count limit restricts the size of the network that RIP can support. Also, RIP can be slow to converge.

RIPv2 defined in RFC 2453 also supports subnet information, allowing Classless Interdomain Routing (CIDR).

RIPng (next generation), an extension of RIPv2 defined in RFC 2080, supports IPv6.

routing protocol. A set of processes, algorithms, and messages that are used to exchange routing information and populate the local Routing Information Base (RIB) with the best path between a source and destination.

The term “routing protocol” usually implies dynamic routing, where a device reports changes and shares information with other devices in the network. Each router starts with knowledge of only the devices to which it is directly attached. The routing protocol shares this information first with its immediate neighbors, and then throughout the network. This way, routers learn the topology of the network.

A primary benefit of dynamic routing protocols over static routing is that routers exchange information when there is a topology change. This exchange allows routers to automatically learn about new devices and networks and also to find alternate paths when there is a link failure in the current network.

Table 7-77 summarizes the characteristics of the dynamic routing protocols supported by OcNOS:

Table 7-77: Dynamic routing protocols

	Border Gateway Protocol (BGP)	Routing Information Protocol (RIP)	Open Shortest Path First (OSPF)	Intermediate System to Intermediate System (IS-IS)
Algorithm	path-vector routing	distance-vector routing	link-state routing	link-state routing
Type	Exterior Gateway Protocol (EGP)	Interior Gateway Protocol (IGP)	Interior Gateway Protocol (IGP)	Interior Gateway Protocol (IGP)
Classless Interdomain Routing (CIDR)	Yes	RIP v1: No RIP v2: Yes	Yes	Yes
Scalable	Yes	No	Yes	Yes
Speed of convergence	Moderate	Slow	Fast	Fast

Table 7-77: Dynamic routing protocols

	Border Gateway Protocol (BGP)	Routing Information Protocol (RIP)	Open Shortest Path First (OSPF)	Intermediate System to Intermediate System (IS-IS)
Resource Use	High	Low	High	High
Configuration ease	Complex	Simple	Complex	Complex

routing table. See Routing Information Base (RIB).

S

S-TAG. See service VLAN (S-VLAN).

(S,G). A notation used in multicast that enumerates a shortest path tree (SPT) where:

- S is the IP address of the source
- G is the multicast group address that identifies the receivers

If the IP address of the source is 192.1.1.1, and the IP address of the multicast group is 224.1.1.1, the source group is written as (192.1.1.1, 224.1.1.1).

Secure Shell (SSH). A protocol that allows the opening of a secure, encrypted channel between two computers with secure authentication. SSH is most often used to provide a secure shell to log in to a remote machine, but also supports file transfers, TCP, and other functions.

segment routing. A form of source routing where nodes and links are represented as segments. The path that a particular protocol data unit (PDU) needs to traverse is represented by one or more segments.

server. A system entity that provides a service to other entities called clients.

service VLAN (S-VLAN). In a Provider Bridging (PB) frame, a tag that identifies the service provider network VLAN. See also customer VLAN (C-VLAN). Also called an S-TAG or S-VID tag.

Shortest Path Bridging (SPB). A control plane protocol that combines an Ethernet data path with an Intermediate System to Intermediate System (IS-IS) link state protocol running between switches. SPB does not depend on spanning tree protocols to provide a loop-free topology, but instead uses IS-IS link-state packets to discover and advertise the network topology and compute the shortest path tree (SPT) instances from all bridges in the SPB area. SPB only requires provisioning at the edge of the network. Defined by IEEE 802.1aq, with RFC 6329 describing the IS-IS extensions to support SPB.

There are two types of SPB depending on the type of Ethernet data path:

- Shortest Path Bridging - VID (SPBV) uses a Provider Bridging (PB) (802.1ad) data path
- Shortest Path Bridging - MAC (SPBM) uses a Provider Backbone Bridging (PBB) (802.1ah) data path

shortest path first (SPF). Algorithm used by Intermediate System to Intermediate System (IS-IS) and Open Shortest Path First (OSPF) to make routing decisions based on the state of network links. Also called the Dijkstra algorithm.

shortest path tree (SPT). A Routing Information Base (RIB) formed by using the shortest path first (SPF) algorithm.

shortest-path routing. A routing algorithm in which paths to all network destinations are calculated. The shortest path is then determined by a cost assigned to each link.

signalling. The ability to transfer information within a network or between different networks.

Simple Network Management Protocol (SNMP). A standardized framework for monitoring and managing devices in a network. The SNMP framework consists of three parts:

- SNMP manager: The system used to control and monitor the activities of network devices.
- SNMP agent: The component within a managed device that maintains the data for the device and reports the data SNMP managers.
- Management Information Base (MIB): How SNMP exposes data as variables which describe the system configuration. These variables can be queried (and sometimes set) by SNMP managers.

SNMP uses User Datagram Protocol (UDP) to send and receive messages on the network.

Single Root I/O Virtualization (SR-IOV). A specification that allows a single Peripheral Component Interconnect Express (PCIe) physical device under a single root port to appear to be multiple separate physical devices to the hypervisor or the guest operating system.

SR-IOV uses physical functions (PFs) and virtual functions (VFs) to manage global functions for the SR-IOV devices:

- PFs are used to configure and manage the SR-IOV functionality
- VFs are lightweight and contain all the resources necessary for data movement but have a minimal set of configuration resources

SR-IOV enables network traffic to bypass the software switch layer of a virtualization stack. The I/O overhead in the software emulation layer is nearly the same as in nonvirtualized environments.

Software-Defined Networking (SDN). An approach to designing, building, and operating networks that decouples the control plane from the data plane. The control plane is centralized in the form of a controller system. Communication between the controller system and the network device uses a standard protocol or other agents. The controller system can consist of multiple, domain specific, clustered controllers. An SDN architecture usually includes APIs that developers use to control the underlying network. These APIs can be standards-based, or they can be vendor-specific.

source routing. A technique where the sender of a protocol data unit (PDU) can partially or completely specify the route that the PDU should take through the network. See also segment routing.

southbound. An interface that allows a network component to communicate with a lower-level component. A southbound interface breaks down the concepts into smaller technical details that are specifically geared toward the lower-layer component within the architecture. Southbound flow can be thought of as going downward. In architectural diagrams, southbound interfaces are drawn at the bottom of the component. See also northbound.

spanning tree algorithm. A technique that finds the best path between segments of a multilooped, mesh network. If multiple paths exist in the network, the spanning tree algorithm finds the most efficient path and limits the link between the two networks to this single active path. If this path fails because of a cable failure or other problem, the algorithm reconfigures the network to use another path.

From the point of view of an individual switch, a spanning tree has a root node and one path that connects all the other switches.

Spanning Tree Protocol (STP). A protocol that creates spanning trees within mesh networks of connected devices, disabling any links that are not a part of the tree and leaving a single active connection between any two unique network nodes. Defined by 802.1D.

STP devices exchange bridge protocol data unit (BPDU) messages. The spanning tree algorithm calculates the best path and prevents multiple paths between network segments. STP elects a root bridge, finds paths and determines the least cost path to the root bridge, then disables all other paths.

Network managers can set up redundant links as backups in case active links fails. Automatic backup takes place without the pitfalls of bridge loops or the need to manually enable or disable backup links.

See also Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP).

split horizon. A technique where routes learned from an interface are not advertised on that same interface, preventing the router from seeing its own route updates.

In split horizon with poison reverse, routes learned from an interface are set as unreachable and advertised on that same interface which also prevents the router from seeing its own route updates.

stacked VLAN. See Provider Bridging (PB).

static address. An address permanently assigned to a device. Contrast with a dynamic address.

static routing. A method where a network administrator programs connecting paths between networks into a router. If a connection fails, the administrator must reprogram the router to use a new path. Static routes have precedence over routes chosen by dynamic routing protocols.

stub area. A type of Open Shortest Path First (OSPF) area where external routes are distributed as a single default route (address 0.0.0.0). Inter-area routes are distributed in a stub area as summary addresses.

In a *totally stubby area*, a single default route is distributed for all external *and* inter-area routes. Addresses from both other areas and external networks are distributed as the default route (address 0.0.0.0).

See also Not-So-Stubby-Area (NSSA).

subnet mask. A bit pattern that shows how an Internet address is divided into network, subnetwork, and host parts. The mask has ones in the bit positions to be used for the network and subnet parts, and zeros for the host part. The mask should contain at least the standard network portion, and the subnet field should be contiguous with the network portion.

This is an example is this IPv4 address and subnet mask:

192.168.100.12 with subnet mask of 255.255.255.0

The first 24 bits of the address is the network address (192.168.100.0) and the last 8 bits are the hosts (12). The entire subnet spans the address range 192.168.100.0 to 192.168.100.255.

The addresses on a given subnet are always contiguous and can all be derived from the network address. Bit masks are always with respect to binary digits, so the number of IP addresses on a given subnet is always some power of two.

A mask gives the first address in the block (the network address) when ANDed with an address in the block.

Classless Interdomain Routing (CIDR) represents the equivalent of a subnet mask by adding a prefix length to an IP address that is the number of bits in the network portion. For example, the subnet mask above can be written as:

192.168.100.12/24

where 192.168.100.12 is the IP address and /24 is the number of bits in the subnet mask.

A subnet mask represents the same information as a prefix length, but predates the use of CIDR.

Also called address mask, network mask.

subnetwork. A group of related IP addresses that all begin with the same network portion and end with a unique portion identifying the host within the subnet.

Also called subnet. See also subnet mask.

subsequent address family identifier (SAFI). Number that further identifies an address family.

supernetting. The process of taking several discrete network addresses and advertising them as one route. For example, if an organization is using 192.10.1.0/24 to 192.10.254.0/24, instead of advertising 254 separate networks, the organization can advertise only the single route 192.10.0.0/16.

switch. A Layer 2 (L2) device that forwards frames based on a destination MAC address. A switch finds a destination address in its filtering database and transmits the frame on the port associated with the destination address. The filtering database is populated through a self-learning process, where each incoming frame is used to update the entries in the filtering database.

A switch that is VLAN-aware can also forward frames based on VLAN identifiers. A network administrator can configure this mapping manually or a switch can dynamically learn mappings via GARP VLAN Registration Protocol (GVRP).

Basic switch behavior is defined in IEEE 802.1D and 802.1Q.

See also bridge. Contrast with router.

Synchronous Ethernet (SyncE). SONET/SDH/PDH-based synchronization that is used to synchronize and send frequency information to devices on an Ethernet network. Synchronous Ethernet provides only frequency synchronization, not time or phase synchronization.

T

telnet. A client/server protocol that establishes a session between a user terminal and a remote host:

- The telnet client software takes input from the user and sends it to the server's operating system
- The telnet server takes output from the host and sends it to the client to display to the user

While telnet is most often used to implement remote login capability, the protocol is general enough to allow it to be used for a variety of purposes.

Terminal Access Controller Access Control System Plus (TACACS+). An authentication method that provides access control for networked devices using one or more centralized servers. TACACS+ provides separate authentication, authorization, and accounting (AAA) services. (Usually pronounced like tack-axe.)

See also Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial In User Service (RADIUS).

throughput. Average rate of successful delivery of data packets over a communication link. Throughput is measured in bits per second, data packets per second, or sometimes data packets per time slot. See also line rate, latency, wire speed.

time to live (TTL). A limit on how long a piece of information can exist before it should be discarded. TTL is a field in an IP header that is (usually) decremented by 1 for each hop through which the packet passes. If the field reaches zero, the packet is discarded, and a corresponding error message is sent to the source of the packet.

Top-of-Rack (ToR) switch. In a data center, an access layer switch that connects to servers installed in the same rack. A ToR switch is usually low profile (one or two rack units in height) with a low port count (typically 48 ports). All cabling for servers stays within the rack as relatively short cables from the servers to the switch. The switch connects

the rack to the data center network with one fiber uplink to a distribution layer switch. There is no need to run cabling between racks and each rack can be managed as a modular unit.

A ToR switch extends the Layer 2 (L2) topology from the aggregation switch to each individual rack resulting in a larger Layer 2 footprint.

See also end-of-row switch.

topology. The physical or logical layout of a network.

topology change notification (TCN). In Spanning Tree Protocol (STP), a bridge protocol data unit (BPDU) that a switch sends to signal a topology change.

traffic engineering (TE). The ability to control the path taken through a network based on a set of traffic parameters. Traffic engineering optimizes the performance of networks and their resources by balancing traffic load across links, routers, and switches in the network. See also Resource Reservation Protocol—Traffic Engineering (RSVP-TE).

Transmission Control Protocol (TCP). A Layer 4 (L4) protocol that works above Internet Protocol (IP) and provides reliable data delivery over connection-oriented links.

TCP splits the stream of data into packets with a sequence number, and sends the packets over an IP-based network. At the destination, TCP acknowledges packets that have been received (so that missing packets can be resent) and reassembles received packets in the correct order to provide an in-order data stream to the remote application. If TCP detects a missing, corrupted, or out of order packet, it requests it be resent from the source.

See also Transmission Control Protocol/Internet Protocol (TCP/IP), User Datagram Protocol (UDP).

Transmission Control Protocol/Internet Protocol (TCP/IP). A family of Internet protocols that describe how data should be formatted, addressed, transmitted, routed, and received to enable computers to communicate over a network.

The Open Systems Interconnection (OSI) Reference Model is a more prescriptive (versus descriptive) approach to network design. TCP/IP does not map cleanly to the OSI model because it was developed before the OSI model and was designed to solve a specific set of problems, not to be a general description for all network communications.

TCP/IP is a widely published open standard and is supported by many vendors and is available on many different computers running many different operating systems. TCP/IP is separated from the network hardware and will run over Ethernet and other connections.

TCP/ IP also refers to the specific functionality at layers 4 and 3:

- Transmission Control Protocol (TCP) at Layer 4 (L4) splits a message into packets that are transmitted over the Internet and reassembles the packets into the original message at the destination
- Internet Protocol (IP) at Layer 3 (L3) addresses and routes each packet so that it gets to its destination

transport layer. See Layer 4 (L4).

tunneling. A method of transporting data in one protocol by encapsulating it in another protocol. Tunneling is used for reasons of incompatibility, implementation simplification, or security. For example, a tunnel lets a remote VPN client have encrypted access to a private network.

type of service (ToS). A field in the IPv4 header used to differentiate packet flows. See also Differentiated Services (DiffServ).

type-length-value (TLV). A data structure used to encode optional information in a data communications protocol:

- Type: the kind of field that this part of the message represents

- Length: the size of the value field, usually in bytes
- Value: a variable-sized set of bytes that contains the data of the message

U

unicast. The process of a single host sending messages to one destination.See also broadcast, multicast.

User Datagram Protocol (UDP). A connectionless transport layer protocol that exchanges datagrams without acknowledgments or guaranteed delivery and which requires other protocols to handle error processing and retransmission. Defined in RFC 768.

Multicast applications that deliver audio and video streams use UDP as their delivery mechanism because the acknowledgment and retransmission services offered by Transmission Control Protocol (TCP) are not needed and add too much overhead.

User-to-Network Interface (UNI). The physical interface/demarcation between a service provider and a subscriber, the service start or end point. There are two types of UNI:

- UNI-C: customer-side processes
- UNI-N: network-side processes

V

VirNOS. An IP Infusion product based on Network Functions Virtualization (NFV) that helps network operators deploy and manage networking services. Many core networking services, including switching, routing, load balancing and VPN can be performed by software either running directly on x86-64 servers or running as virtual machine (VM) instances instead of requiring expensive networking equipment. Therefore, organizations are migrating networking functions to standard, high-volume server environments and replacing dedicated network hardware with virtualization software that runs on commodity servers. Carriers, service providers, enterprises and network equipment manufacturers can run VirNOS as-is, on top of a standard server platform. IP Infusion customers can integrate VirNOS into their software offering and thereby add services and features quickly.

Virtual Ethernet Bridge (VEB). A virtual switch implemented in a virtualized server environment. A VEB mimics a traditional external Layer 2 (L2) switch for connecting to a virtual machine (VM). VEBs can communicate between VMs on a single physical server, or they can connect VMs to the external network. The most common implementations of VEBs are software-based vSwitches built into hypervisors.

Virtual Local Area Network (VLAN). A logical group of network devices that appear to be on the same LAN, regardless of their physical location. VLANs enable multiple bridged LANs to transparently share the same physical network link while maintaining isolation between networks. Traffic between VLANs is restricted to devices that forward unicast, multicast, or broadcast traffic only on the LAN segments that serve the VLAN to which the traffic belongs.

VLANs make it easy to administer logical groups of hosts that can communicate as if they were on the same LAN.

Membership in a particular VLAN can be by port, MAC address, protocol, or subnet.

VLANs are configured as unique Layer 2 (L2) broadcast domains. VLANs allow network administrators to resegment their networks without physically rearranging the devices or network connections. VLANs span one or more ports on multiple devices and several VLANs can co-exist on a single physical switch. By default, each VLAN maintains its own filtering database containing MAC addresses learned from frames received on ports belonging to the VLAN.

IEEE 802.1Q provides for tagging Ethernet frames with VLAN identifiers. 802.1Q only supports up to 4094 VLANs, which is a scaling constraint for service providers.

virtual machine (VM). An operating system or application environment installed on emulated hardware and not physically installed on dedicated hardware. The virtual machine's guest operating system does not have to be modified to run in a virtualized environment. A VM behaves like a traditional, physical server and runs a traditional operating system such as Windows or Linux.

A hypervisor emulates the computer's CPU, memory, hard disk, network and other hardware resources completely, enabling virtual machines to share the resources. The hypervisor can emulate multiple virtual hardware platforms that are isolated from each other. For example, virtual machines can run Linux and Windows operating systems and share the same underlying physical host. An operating sysem is unaware that it is running in a VM.

See also paravirtualized, virtualization.

virtual port. A port on a vSwitch (Virtual Switch) where virtual Ethernet adapters or physical uplinks can be attached. During their creation, virtual switches are typically configured with a specific number of virtual ports.

virtual private LAN service (VPLS). Multipoint-to-multipoint Layer 2 (L2) VPN service used to interconnect multiple Ethernet LANs across an Multi-Protocol Label Switching (MPLS) backbone.

VPLS evolved as a logical extension of Virtual Private Wire Service (VPWS) based on RFC 4447.

VPLS can be defined as several instances of a virtual switch instance (VSI) that are interconnected to form a single logical bridge domain.

Virtual Private Network (VPN). A network service which uses encryption and tunneling to provide a subscriber with a secure private network that runs over the public network infrastructure.

Virtual Private Wire Service (VPWS). Point-to-point Layer 2 (L2) VPN service used to interconnect multiple Ethernet LANs across an Multi-Protocol Label Switching (MPLS) backbone. Also called Virtual Leased Line (VLL) or Ethernet over MPLS (EoMPLS).

virtual router (VR). A OcNOS proprietary abstraction where multiple distinct logical routers exist within a single device. Each virtual router executes separate instances of the routing protocol and network management software. A virtual router provides support for multiple Routing Information Base (RIB) instances and multiple Forwarding Information Base (FIB) instances per physical router. Each VR might consist of an Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), or Routing Information Protocol (RIP) routing process, each with its own Routing Information Base (RIB) and Forwarding Information Base (FIB). Applications include segregating traffic dedicated to different customers, enterprise Virtual Private Network (VPN) users, or a specific traffic type such as streaming video.

Do not confuse a Virtual Router Redundancy Protocol (VRRP) virtual router with a OcNOS virtual router. They are two different things.

Virtual Router Redundancy Protocol (VRRP). A protocol that uses a *virtual router*, an abstract representation of multiple routers (master and backup routers) that act as a group. VRRP advertises a virtual router as the default gateway instead of one physical router. Two or more physical routers are configured, with only one doing the actual routing at any given time. If the current physical router that is routing on behalf of the virtual router fails, the other physical router automatically takes over. Defined by RFC 5798.

Do not confuse a VRRP virtual router with an OcNOS virtual router (VR). They are two different things.

Virtual Routing and Forwarding (VRF). A technology that allows multiple instances of a Routing Information Base (RIB) to co-exist within the same router at the same time. Multiple VRFs inside a virtual router (VR) logically subdivide the RIBs. Service providers can use VRF technology to create a separate Virtual Private Network (VPN) for each of their customers. Therefore, the technology is also called VPN routing and forwarding.

virtual switch instance (VSI). A mechanism for VLANs to pass packets to other VLANs without sending the packets through a router. With a VSI, the switch recognizes packet destinations that are local to the sending VLAN and bridges (switches) those packets. Only packets destined for another VLAN are routed.

A VSI is similar to the bridging defined in IEEE 802.1Q; a frame is switched, based on the destination MAC and membership in a Layer 2 (L2) VPN. A VSI floods unknown, broadcast, or multicast frames to all ports associated with the VSI.

virtualization. A technology that abstracts the physical characteristics of a machine, creating a logical version of it, including creating logical versions of entities such as operating systems and network resources. See also hypervisor, virtual machine (VM).

vNIC (Virtual Network Interface Card). Software that behaves like a Ethernet hardware adapter. It has a MAC address, and it sends and receives Ethernet frames.

VPN routing and forwarding. See Virtual Routing and Forwarding (VRF).

vSwitch (Virtual Switch). Software that behaves like a physical Ethernet switch. A vSwitch connects virtual machine (VM) instances in a virtual network at layer 2:

- Connects vNIC (Virtual Network Interface Card) instances from multiple VMs to virtual ports
- Connects physical network interface cards to virtual ports
- Uplinks to the physical network

A vSwitch maintains a MAC address table and routes traffic to specific ports, rather than repeating traffic on all ports. A vSwitch can include other features found in physical Ethernet switches, such as VLANs.

See also Open vSwitch (OVS).

W

weighted fair queuing (WFQ). Queue scheduling discipline where each queue has a weight and is assigned a different percentage of output port bandwidth. WFQ supports variable-length packets so that flows with larger packets are not allocated more bandwidth than flows with smaller packets.

WFQ classifies traffic as high- or low-bandwidth with low-bandwidth traffic getting priority and high-bandwidth traffic sharing what is left over. If traffic bursts ahead of the rate at which the interface can transmit, new high-bandwidth traffic is discarded after a congestive-messages threshold has been reached.

WFQ provides preferential treatment for higher priority traffic while preventing total starvation of lower priority traffic under sustained overload conditions.

weighted random early detection (WRED). Congestion avoidance mechanism which prevents an output queue from ever filling to capacity. WRED provides separate thresholds and weights for different IP precedences, allowing you to provide different qualities of service in regard to packet dropping for different traffic types. Standard traffic may be dropped more frequently than premium traffic during periods of congestion.

weighted round-robin queuing (WRR). Queue scheduling discipline that supports flows with significantly different bandwidth requirements. Each queue can be assigned a weight that is relative to other queues. WRR ensures that lower-priority queues are not denied access to buffer space and output port bandwidth. At least one packet is removed from each queue during each service round.

white box switch. In computer hardware, a white box is a server without a well-known brand name made from commonly available parts. White box switches are like white box servers, offering low cost without the brand name or tight integration of silicon and network software features.

Traditional black box switches are built with vertically integrated hardware and software. Some vendors use custom application-specific integrated circuit (ASIC) components to boost performance and add features, which adds to the cost. A white box switch decouples the software from the switching hardware. By decoupling software and hardware, customers have more flexibility and can potentially change software without changing hardware.

A white box switch runs a network operating system on generic x86 hardware with “merchant silicon” chipsets from manufacturers such as Broadcom, Centec, Intel, Marvell, and Mellanox. White box switches rely on an operating system such as Linux to integrate the Layer 2 (L2)/Layer 3 (L3) networking functions.

White box switches do not have the same complex features as black box switches because most interact with Software-Defined Networking (SDN) controllers to make forwarding and control plane decisions from a centralized point for all switches in the network. The SDN controller uses a southbound API to program the forwarding table of the white box switches.

Some vendors sell a complete white box solution with the operating system already installed, while others supply just the “bare-metal” switch and you buy the operating system direct from the software vendor.

wide area network (WAN). A network that provides communication services to a geographic area larger than that served by a Local Area Network (LAN) and that may use or provide public communication facilities.

wire speed. The ability of a device to achieve throughput equal to the maximum throughput of a communication standard.

Y

YANG. A data modeling language that specifies the syntax and semantics for NETCONF (Network Configuration Protocol) operations, notification events, and database content. YANG tools can automate behavior within the NETCONF protocol for clients and servers.

YANG can model both configuration and state data of network elements. YANG structures the data definitions into tree structures and provides many modeling features, including an extensible type system, formal separation of state and configuration data and a variety of syntactic and semantic constraints. YANG data definitions provide a strong set of features for extensibility and reuse. Defined in RFC 6020.

Master Command Index

Index

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W