OcNOS®

Open Compute Network Operating System for Service Providers Version 6.4.2

Key Features

May 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 OcNOS.

Audience

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

Conventions

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

Table 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

Related Documentation

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

Feature Availability

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

Migration Guide

Check the *Migration Guide* for configuration changes to make when migrating from one version of OcNOS to another.

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.

Enhanced Security and Performance

This section describes the security, performance, scalability, and access control enhancements and new features introduced in the Release 6.4.2 and Release 6.4.1.

Release 6.4.2

- Port Breakout (100G) for 26XAS7316-26XB (Qumran-AX) Platform
- Port Breakout (100G) for S9500-30XS (Qumran-AX) Platform
- Seamless BFD On Qumran2
- Support of 2.5G Speed on Edgecore AS5912-54X Switch

Release 6.4.1

- NetConf Port Access Control
- Role-Based Access Control
- Hide the Remote AS using the neighbor local-as Command
- Port Breakout (400G) for Qumran2 Series Platforms
- Port Breakout (100G) for AS5916-54XKS (Qumran-MX) Platform
- Port Breakout (100G) for AS7315-27X (Qumran-AX) Platform
- Support IGMP Snooping for Provider Bridge
- TCP MSS configuration for LDP sessions
- TCP MSS configuration for BGP neighbors
- Two-Way Active Measurement Protocol Client
- Single-Home for VxLAN IRB with OSPF or ISIS
- Single-Home for VxLAN EVPN IRB with OSPF or ISIS
- Fall Back Option for RADIUS Authentication
- Modified Extended ACL Deny Rule Behavior in VTY
- 400G PM Alarm

Port Breakout (100G) for AS5916-54XKS (Qumran-MX) Platform

Overview

The port breakout system AS5916-54XKS device offers support for 48 ports (1-48) with 10GbE SFP+ interfaces, and 6 ports (0-5) with 100GbEQSFP28 interfaces. Port breakout allows the flexibility to divide each 100G QSFP28 port (ce0, ce1, ce2, ce3, ce4, ce5) into (4X25G) configurations.

Note: The port breakout functionality is not supported on ports other than these designated ports.

Feature Characteristics

Breakout configurations facilitate the connection between network devices with varying port speeds, allowing for the optimal utilization of port bandwidth.

The breakout mode on network equipment, such as switches, routers, and servers, opens up new possibilities for network operators to keep up with the pace of bandwidth demand. By adding high-speed ports that support breakout mode, network operators can increase the front port density and incrementally enable an upgrade to higher data rates.

Benefits

The advantages of utilizing a 100G port breakout:

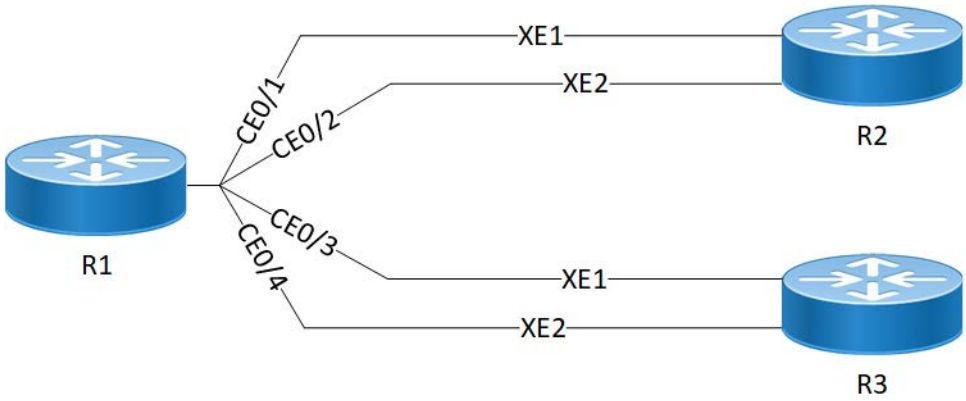
- Boosts port density and saves on rack space
- Reduces power consumption
- Facilitates future upgrades.

Configuration

By default, mode 1 designates the board with 100G ports. If you switch it to mode 2, all 100G ports will be divided into 4x25G ports. To split a 100G port into 4x25G ports, use the following command, save the configuration, and then reload the device.

Topology

The platform supports splitting a single 100G QSFP28 port into the following 4x25G ports.



AS5916-54XKS(QMX) 100G Port Breakout Configuration

R1

The following table outlines the configuration steps for dividing a single port into multiple ports through channelization.

`OcNOS#configure terminal`	Enter Configuration mode.
`OcNOS(config)#hardware-profile port-config mode2`	Breakout 100G ports into 4x25G ports called as ce0/1, ce0/2, ce0/3, ce0/4 as shown in the Topology section.
`OcNOS(config)#commit`	Commit the configuration.

Validation

Use this command to validate the port breakout configuration.

```
OcNOS#show interface brief

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       OTD  - Object Tracking Down
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
Ethernet   Type          PVID  Mode             Status  Reason  Speed Port    Ctl Br/Bu
Loopbk
Interface                                                          Ch #
--------------------------------------------------------------------------------
ce0/1         ETH           --    routed           down    PD      25g   --       No  No
ce0/2         ETH           --    routed           down    PD      25g   --       No  No
ce0/3         ETH           --    routed           down    PD      25g   --       No  No
ce0/4         ETH           --    routed           down    PD      25g   --       No  No
```

```
ce1/1         ETH           --    routed           up      none    25g   --       No  No
ce1/2         ETH           --    routed           up      none    25g   --       No  No
ce1/3         ETH           --    routed           up      none    25g   --       No  No
ce1/4         ETH           --    routed           up      none    25g   --       No  No
ce2/1         ETH           --    routed           down    PD      25g   --       No  No
ce2/2         ETH           --    routed           down    PD      25g   --       No  No
ce2/3         ETH           --    routed           down    PD      25g   --       No  No
ce2/4         ETH           --    routed           down    PD      25g   --       No  No
ce3/1         ETH           --    routed           up      none    25g   --       No  No
ce3/2         ETH           --    routed           down    AD      25g   --       No  No
ce3/3         ETH           --    routed           up      none    25g   --       No  No
ce3/4         ETH           --    routed           up      none    25g   --       No  No
ce4/1         ETH           --    routed           down    PD      25g   --       No  No
ce4/2         ETH           --    routed           down    PD      25g   --       No  No
ce4/3         ETH           --    routed           down    PD      25g   --       No  No
ce4/4         ETH           --    routed           down    PD      25g   --       No  No
ce5/1         ETH           --    routed           down    PD      25g   --       No  No
ce5/2         ETH           --    routed           down    PD      25g   --       No  No
ce5/3         ETH           --    routed           down    PD      25g   --       No  No
ce5/4         ETH           --    routed           down    PD      25g   --       No  No

--------------------------------------------------------------------------------
Interface     Type             Status  Reason  Speed
--------------------------------------------------------------------------------
eth0          METH             up      --      1g


--------------------------------------------------------------------------------
Interface                                          Status      Description
--------------------------------------------------------------------------------
lo                                                 up          --
lo.management                                      up          --

--------------------------------------------------------------------------------
Interface    Status   Reason
--------------------------------------------------------------------------------
vlan1.1      down     PD
vlan1.2      down     PD
```

After reloading the interfaces ce0, ce1, ce2, ce3, ce4, and ce5, the 100G ports are subdivided into four 25G ports, as indicated below.

```
ce0 - ce0/1,ce0/2,ce0/3,ce0/4
ce1 - ce1/1,ce1/2,ce1/3,ce1/4
ce2 - ce2/1,ce2/2,ce2/3,ce2/4
ce3 - ce3/1,ce3/2,ce3/3,ce3/4
ce4 - ce4/1,ce4/2,ce4/3,ce4/4
ce5 - ce5/1,ce5/2,ce5/3,ce5/4
```

Unconfigure Port Breakout

Combine a port that has been previously split into multiple smaller ports. This command allows you to revert the port to its original combined state. For example, if port ce0 was a 100G port that was broken into four 25G ports, this command will allow you to revert the port to its original state as a 100G port.

R1

The following table outlines the unconfiguration steps for port breakout.

`OcNOS#configure terminal`	Enter Configuration mode.
`OcNOS(config)#hardware-profile port-config mode1`	Combine the breakout port to its original port throughput capabilities.
`OcNOS(config)#commit`	Commit the configuration.

Validation

Use this command to validate the port breakout unconfiguration.

```
OcNOS#show interface brief

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
Ethernet   Type          PVID  Mode             Status  Reason  Speed Port    Ctl Br/Bu
Loopbk
Interface                                                          Ch #
--------------------------------------------------------------------------------
ce0           ETH           --    routed           down    PD      100g  --       No  No
ce1           ETH           1     trunk            up      none    100g  --       No  No
ce2           ETH           --    routed           down    PD      100g  --       No  No
ce3           ETH           --    routed           down    PD      100g  --       No  No
ce4           ETH           --    routed           down    PD      100g  --       No  No
ce5           ETH           --    routed           down    PD      100g  --       No  No
```

After reloading the interfaces ce0, ce1, ce2, ce3, ce4, and ce5, all the 4x25G sub-ports will be deleted, and the 100G ports ce0, ce1, ce2, ce3, ce4, and ce5 will be added.

```
ce0 - ce0/1,ce0/2,ce0/3,ce0/4
ce1 - ce1/1,ce1/2,ce1/3,ce1/4
```

```
ce2 - ce2/1,ce2/2,ce2/3,ce2/4
ce3 - ce3/1,ce3/2,ce3/3,ce3/4
ce4 - ce4/1,ce4/2,ce4/3,ce4/4
ce5 - ce5/1,ce5/2,ce5/3,ce5/4
```

Port Breakout (100G) for AS7315-27X (Qumran-AX) Platform

Overview

The AS7315-27X device accommodates a combination of port breakout options with hybrid port speeds. On this device, configure 4 ports (port 1-4) with 25G Ethernet SFP28 interfaces, 20 ports (port 5-24) with 10GbE SFP+ interfaces, and 3 ports (port 25-27) with 100G Ethernet QSFP28 interfaces. Using port breakout, divide the 100G QSFP28 ports (ce0, ce1, and ce2) into 4X25G configurations if desired.

Note: The port breakout functionality is not supported on ports other than these designated ports.

Feature Characteristics

Breakout configurations facilitate the connection between network devices with varying port speeds, allowing for the optimal utilization of port bandwidth.

Enabling breakout mode on network equipment such as switches, routers, and servers introduces innovative approaches for network operators to meet the ever-growing need for higher bandwidth. By incorporating high-speed ports that support breakout functionality, operators can enhance faceplate port density and enable a gradual transition to higher data rates, effectively adapting to evolving bandwidth requirements.

Benefits

The advantages of utilizing a 100G port breakout:

• Boosts port density and saves on rack space

• Reduces power consumption

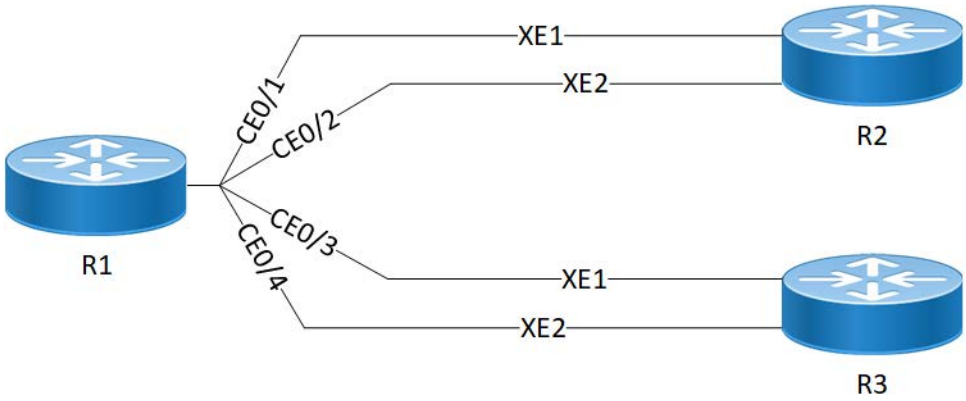
• Facilitates future upgrades.

Configuration

By default, mode 1 designates the board with 100G ports. If you switch it to mode 2, all 100G ports will be divided into 4x25G ports. To split a 100G port into 4x25G ports, use the following command, save the configuration, and then reload the device.

Topology

The platform supports splitting a single 100G QSFP28 port into the following 4x25G ports.



AS7315-27X(QAX) 100G Port Breakout Configuration

R1

The following table outlines the configuration steps for dividing a single port into multiple ports through channelization.

`OcNOS#configure terminal`	Enter Configuration mode.
`OcNOS(config)#hardware-profile port-config mode2`	Breakout 100G ports into 4x25G ports called as ce/1, ce/2, ce/3, ce/4 as shown in the Topology section.
`OcNOS(config)#commit`	Commit the configuration.

Validation

Use this command to validate the port breakout configuration.

```
OcNOS#show interface brief

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       LBG - Link Bonding Group, MODEM - Link Bonding Modem
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       OTD  - Object Tracking Down
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
Ethernet   Type         PVID  Mode            Status  Reason  Speed Port    Ctl Br/Bu
Loopbk
Interface                                                          Ch #
--------------------------------------------------------------------------------
ce0/1         ETH           --    routed           down    PD      25g   --       No  No
ce0/2         ETH           --    routed           down    PD      25g   --       No  No
ce0/3         ETH           --    routed           down    PD      25g   --       No  No
```

```
ce0/4         ETH           --    routed           down    PD      25g   --       No  No
ce1/1         ETH           --    routed           up      none    25g   --       No  No
ce1/2         ETH           --    routed           up      none    25g   --       No  No
ce1/3         ETH           --    routed           up      none    25g   --       No  No
ce1/4         ETH           --    routed           up      none    25g   --       No  No
ce2/1         ETH           --    routed           up      none    25g   --       No  No
ce2/2         ETH           --    routed           down    PD      25g   --       No  No
ce2/3         ETH           --    routed           up      none    25g   --       No  No
ce2/4         ETH           --    routed           up      none    25g   --       No  No
```

After reloading the interfaces ce/1, ce/2, ce/3, and ce/4, the 100G ports are subdivided into four 25G ports, as indicated below.

```
 ce0 - ce0/1,ce0/2,ce0/3,ce0/4
 ce1 - ce1/1,ce1/2,ce1/3,ce1/4
 ce2 - ce2/1,ce2/2,ce21/3,ce2/4
```

Unconfigure Port Breakout

Combine a port that has been previously split into multiple smaller ports. This command allows you to revert the port to its original combined state. For example, if port ce49 was a 100G port that was broken into four 25G ports, this command will allow you to revert the port to its original state as a 100G port.

R1

The following table outlines the unconfiguration steps for port breakout.

`OcNOS#configure terminal`	Enter Configuration mode.
`OcNOS(config)#hardware-profile port-config mode1`	Combine the breakout port to its original port throughput capabilities.
`OcNOS(config)#commit`	Commit the configuration.

Validation

Use this command to validate the port breakout unconfiguration.

```
OcNOS#show interface brief

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       LBG - Link Bonding Group, MODEM - Link Bonding Modem
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       OTD  - Object Tracking Down
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down
```

```
--------------------------------------------------------------------------------
Ethernet   Type          PVID  Mode             Status  Reason  Speed Port    Ctl Br/Bu
Loopbk
Interface                                                          Ch #
--------------------------------------------------------------------------------
ce0           ETH           --    routed           up      none    100g  --       No  No
ce1           ETH           --    routed           up      none    100g  --       No  No
ce2           ETH           --    routed           up      none    100g  --       No  No
```

After reloading the interfaces ce/1, ce/2, ce/3, and ce/4, all the 4x25G sub-ports will be deleted, and the 100G ports ce/1, ce/2, ce/3, and ce/4 will be added.

```
ce0/1,ce0/2,ce0/3,ce0/4
ce1/1,ce1/2,ce1/3,ce1/4
ce2/1,ce2/2,ce21/3,ce2/4
```

Port Breakout (100G) for 26XAS7316-26XB (Qumran-AX) Platform

Overview

The AS7316-26XB supports 16 (port 1-16) 10GbE SFP+ ports, 8 (port 17-24) 25GbE SFP28 ports and 2 (25-26) 100 GbE QSFP28 ports. We can split only the 100G QSFP28 (ce0,ce1)ports into 4X25G. Breakout not supported for other ports.

Note: The port breakout functionality is not supported on ports other than these designated ports.

Feature Characteristics

Breakout configurations facilitate the connection between network devices with varying port speeds, allowing for the optimal utilization of port bandwidth.

The breakout mode on network equipment, such as switches, routers, and servers, opens up new possibilities for network operators to keep up with the pace of bandwidth demand. By adding high-speed ports that support breakout mode, network operators can increase the front port density and incrementally enable an upgrade to higher data rates.

Benefits

The advantages of utilizing a 100G port breakout:

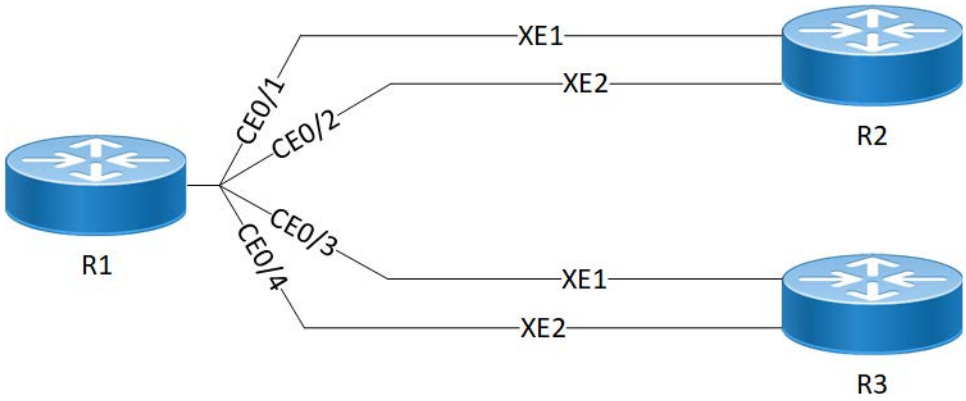
- Boosts port density and saves on rack space
- Reduces power consumption
- Facilitates future upgrades.

Configuration

By default, mode 1 designates the board with 100G ports. If you switch it to mode 2, all 100G ports will be divided into 4x25G ports. To split a 100G port into 4x25G ports, use the following command, save the configuration, and then reload the device.

Topology

The platform supports splitting a single 100G QSFP28 port into the following 4x25G ports.



AS7316-26XB (QAX) 100G Port Breakout Configuration

R1

The following table outlines the configuration steps for dividing a single port into multiple ports through channelization.

`OcNOS#configure terminal`	Enter Configuration mode.
`OcNOS(config)#hardware-profile port-config mode2`	Breakout 100G ports into 4x25G ports called as ce0/1, ce0/2, ce0/3, ce0/4 as shown in the Topology section.
`OcNOS(config)#commit`	Commit the configuration.

Validation

Use this command to validate the port breakout configuration.

```
OcNOS#show interface brief

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       OTD  - Object Tracking Down
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
Ethernet   Type          PVID  Mode             Status  Reason  Speed Port    Ctl Br/Bu
Loopbk
Interface                                                          Ch #
--------------------------------------------------------------------------------
ce0/1         ETH           --    routed           down    PD      25g   --       No  No
ce0/2         ETH           --    routed           down    PD      25g   --       No  No
ce0/3         ETH           --    routed           down    PD      25g   --       No  No
ce0/4         ETH           --    routed           down    PD      25g   --       No  No
```

```
ce1/1         ETH           --    routed           up      none    25g   --       No  No
ce1/2         ETH           --    routed           up      none    25g   --       No  No
ce1/3         ETH           --    routed           up      none    25g   --       No  No
ce1/4         ETH           --    routed           up      none    25g   --       No  No

--------------------------------------------------------------------------------
Interface     Type             Status  Reason  Speed
--------------------------------------------------------------------------------
eth0          METH             up      --      1g


--------------------------------------------------------------------------------
Interface                                          Status      Description
--------------------------------------------------------------------------------
lo                                                 up          --
lo.management                                      up          --

--------------------------------------------------------------------------------
Interface    Status   Reason
--------------------------------------------------------------------------------
vlan1.1      down     PD
vlan1.2      down     PD
```

After reloading the interfaces ce0 and ce1 the 100G ports are subdivided into four 25G ports, as indicated below.

```
ce0 - ce0/1,ce0/2,ce0/3,ce0/4
ce1 - ce1/1,ce1/2,ce1/3,ce1/4
```

Unconfigure Port Breakout

Combine a port that has been previously split into multiple smaller ports. This command allows you to revert the port to its original combined state. For example, if port ce0 was a 100G port that was broken into four 25G ports, this command will allow you to revert the port to its original state as a 100G port.

R1

The following table outlines the unconfiguration steps for port breakout.

`OcNOS#configure terminal`	Enter Configuration mode.
`OcNOS(config)#hardware-profile port-config mode1`	Combine the breakout port to its original port throughput capabilities.
`OcNOS(config)#commit`	Commit the configuration.

Validation

Use this command to validate the port breakout unconfiguration.

```
OcNOS#show interface brief
```

```
Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
Ethernet   Type          PVID  Mode             Status  Reason  Speed Port    Ctl Br/Bu
Loopbk
Interface                                                          Ch #
--------------------------------------------------------------------------------
ce0           ETH           --    routed           down    PD      100g  --       No  No
ce1           ETH           1     trunk            up      none    100g  --       No  No
```

After reloading the interfaces ce0/1, ce0/2, ce0/3, and ce0/4 all the 4x25G sub-ports will be deleted, and the 100G ports ce0 and ce1 will be added.

```
ce0 - ce0/1,ce0/2,ce0/3,ce0/4
ce1 - ce1/1,ce1/2,ce1/3,ce1/4
```

Port Breakout (100G) for S9500-30XS (Qumran-AX) Platform

Overview

The S9500-30XS supports 20 (port 1-20) 10GbE SFP+ ports, 8 (port 21-28) 25GbE SFP28 ports and 2 (29-30) 100 GbE QSFP28 ports. We can split only the 100G QSFP28 (ce0,ce1)ports into 4X25G. Breakout not supported for other ports.

Note: The port breakout functionality is not supported on ports other than these designated ports.

Feature Characteristics

Breakout configurations facilitate the connection between network devices with varying port speeds, allowing for the optimal utilization of port bandwidth.

Enabling breakout mode on network equipment such as switches, routers, and servers introduces innovative approaches for network operators to meet the ever-growing need for higher bandwidth. By incorporating high-speed ports that support breakout functionality, operators can enhance faceplate port density and enable a gradual transition to higher data rates, effectively adapting to evolving bandwidth requirements.

Benefits

The advantages of utilizing a 100G port breakout:

• Boosts port density and saves on rack space

• Reduces power consumption

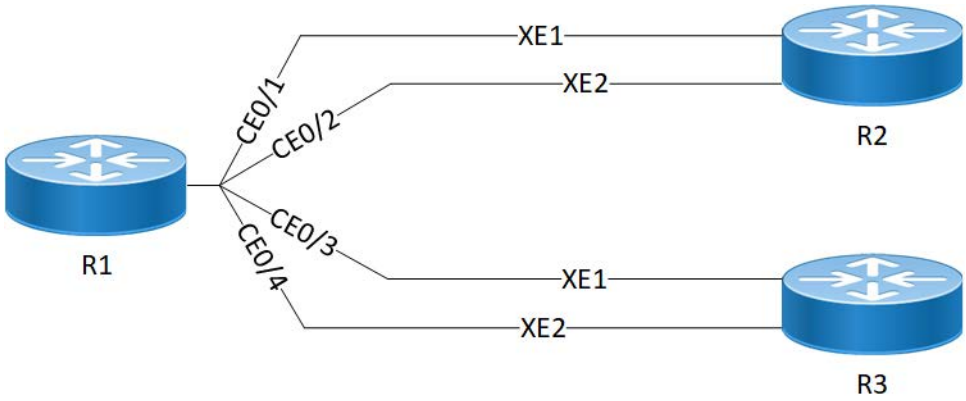
• Facilitates future upgrades.

Configuration

By default, mode 1 designates the board with 100G ports. If you switch it to mode 2, all 100G ports will be divided into 4x25G ports. To split a 100G port into 4x25G ports, use the following command, save the configuration, and then reload the device.

Topology

The platform supports splitting a single 100G QSFP28 port into the following 4x25G ports.



SP9500-30XS (QAX) 100G Port Breakout Configuration

R1

The following table outlines the configuration steps for dividing a single port into multiple ports through channelization.

`OcNOS#configure terminal`	Enter Configuration mode.
`OcNOS(config)#hardware-profile port-config mode2`	Breakout 100G ports into 4x25G ports called as ce1/1, ce1/2, ce1/3, ce1/4 as shown in the Topology section.
`OcNOS(config)#commit`	Commit the configuration.

Validation

Use this command to validate the port breakout configuration.

```
OcNOS#show interface brief

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       LBG - Link Bonding Group, MODEM - Link Bonding Modem
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       OTD  - Object Tracking Down
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
Ethernet   Type         PVID  Mode            Status  Reason  Speed Port    Ctl Br/Bu
Loopbk
Interface                                                          Ch #
--------------------------------------------------------------------------------
ce0/1         ETH           --    routed           down    PD      25g   --       No  No
ce0/2         ETH           --    routed           down    PD      25g   --       No  No
ce0/3         ETH           --    routed           down    PD      25g   --       No  No
```

```
ce0/4         ETH           --    routed           down    PD      25g   --       No  No
ce1/1         ETH           --    routed           up      none    25g   --       No  No
ce1/2         ETH           --    routed           up      none    25g   --       No  No
ce1/3         ETH           --    routed           up      none    25g   --       No  No
ce1/4         ETH           --    routed           up      none    25g   --       No  No
```

After reloading the interfaces ce0 and ce1, the 100G ports are subdivided into four 25G ports, as indicated below.

```
 ce0 - ce0/1,ce0/2,ce0/3,ce0/4
 ce1 - ce1/1,ce1/2,ce1/3,ce1/4
```

Unconfigure Port Breakout

Combine a port that has been previously split into multiple smaller ports. This command allows you to revert the port to its original combined state. For example, if port ce49 was a 100G port that was broken into four 25G ports, this command will allow you to revert the port to its original state as a 100G port.

R1

The following table outlines the unconfiguration steps for port breakout.

`OcNOS#configure terminal`	Enter Configuration mode.
`OcNOS(config)#hardware-profile port-config mode1`	Combine the breakout port to its original port throughput capabilities.
`OcNOS(config)#commit`	Commit the configuration.

Validation

Use this command to validate the port breakout unconfiguration.

```
OcNOS#show interface brief

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       LBG - Link Bonding Group, MODEM - Link Bonding Modem
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       OTD  - Object Tracking Down
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
Ethernet   Type         PVID  Mode            Status  Reason  Speed Port    Ctl Br/Bu
Loopbk
```

```
Interface                                                                    Ch #
-------------------------------------------------------------------------------
ce0           ETH           --    routed           up      none    100g  --       No  No
ce1           ETH           --    routed           up      none    100g  --       No  No
```

After reloading the interfaces ce1/1, ce1/2, ce1/3, and ce1/4, all the 4x25G sub-ports will be deleted, and the 100G ports ce0, ce1, will be added.

```
ce0/1,ce0/2,ce0/3,ce0/4-ce0
ce1/1,ce1/2,ce1/3,ce1/4-ce1
```

Seamless BFD On Qumran2

Overview

Seamless Bidirectional Forwarding Detection (S-BFD) is an extension or enhancement of Bidirectional Forwarding Detection (BFD). This protocol is primarily used in IP-based networks to monitor and detect faults quickly between systems. S-BFD is designed to provide a seamless and rapid fault detection mechanism while minimizing the impact on network resources. It is a simplified mechanism for using BFD with a large proportion of negotiation aspects eliminated. BFD provides a smooth and continuous operational experience for applications in a network.

Feature Characteristics

S-BFD consists of an initiator (a network node hosts an S-BFD Initiator) and a responder (a network node hosts an S-BFD Reflector). In network traffic, S-BFD detects a link failure, and the traffic immediately switches to a backup path. The traffic returns to the primary once the link is up or the corresponding path becomes active.

S-BFD works on the following concepts:

- Initiator: A network node hosting an S-BFDInitiator.
- Responder: A network node hosting an S-BFDReflector.
- S-BFD Initiator: In a network, an S-BFD session performs a continuity test by sending S-BFD packets to a remote entity.
- BFD Discriminator: A BFD Discriminator is allocated for an SBFDInitiator.
- SBFD Reflector: In a network node, S-BFD session gathers incoming S-BFD control packets from local entities and generates responses to S-BFD control packets.

For more information, see the *Seamless BFD for SR-TE* in the *OcNOS Segment Routing Config Guide document*, Release 6.4.1.

Benefits

The following are the benefits of using S-BFD on Q2:

- Quick provisioning: S-BFD can be deployed in any network with less time and effort, ensuring the configured environment is rapid and efficient.
- Improved control: S-BFD continuously monitors the network, predicts the network blocks, and diverts the network traffic to back up path.
- Flexibility for network nodes: S-BFD easily adapts to network functionalities, ensuring efficient traffic distribution and minimizing congestion.
- Initiating path monitoring: Path monitoring in a network involves regular monitoring and checking the communication path between two network endpoints.

S-BFD provides quick convergence time is 50 milliseconds.

Prerequisites

The following prerequisites are mandatory before installing S-BFD:

- Configure ISIS.

- Configure Segment Routing policy.

Configuration

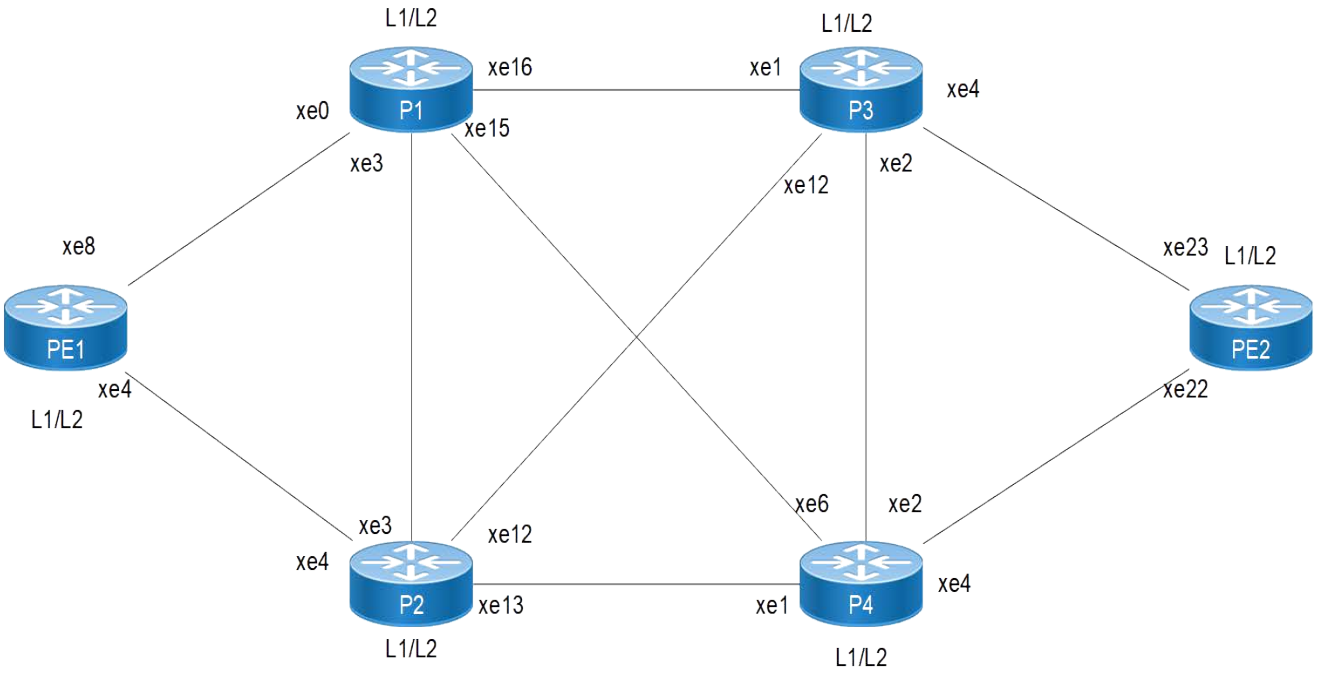
S-BFD is supported only on Qumran2 platforms. The topology below describes active routers PE1,P3,P4, PE2 and as a backup PE1,P2, PE2 with lowest preference.

For more information on the S-BFD configurations, see the *Seamless BFD for SR-TE Configuration* in the *OcNOS Segment Routing Config Guide*.

Topology

In a network, a node can be either the initiator or the reflector, the initiator sends an S-BFD packet for the detection to the reflector. The reflector reflects the received S-BFD packet. As soon as the S-BFD packet is received from the initiator, it checks that the S-BFD discriminator in the packet is the same. If it doesn't match the packet is discarded. If it matches, the reflector reflects the packet.

The following topology illustrates the S-BFD process.



S-BFD on Qumran2

For this topology to work, ensure that these following conditions are met

Note:

1. Ensure that prefix SIDs are unique globally.
2. Use L1 or L2 routers throughout your SR domain.
3. Redistribution from L1 to L2 and vice-versa is not supported for Segment Routing.

Validation

```
PE2-7048#show bfd session

BFD process for VRF: (DEFAULT VRF)
========================================================================================
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Interface
Down-Reason  Remote-Addr
1281     45.45.45.45  MPLS LSP    Single-Hop  Up        00:01:15  po1.10       NA
45.45.45.45/32

Number of Sessions:    1


PE2-7048#show segment-routing policy detail

Policy-Name: 1    Color 1      End-point 45.45.45.45      Tunnel-ID: 1
  Admin-Status: UP    Oper-Status: UP for 00:01:13
  State Transition Count: 1
  CSPF Retry Limit: 100    CSPF Retry Interval: 10
  S-BFD is enabled.
  Binding SID :
  BSID: 25600
  Alloc mode: Dynamic
  Oper State: Programmed

  CP ID: 1, Active
    Preference: 300    Path Type: Explicit    CP Origin: Local
    CP state: Valid
    Segment List:
    Total no. of segments: 2
    Segment0[LABEL]: Label :16042
    Segment1[LABEL]: Label :16045
    Out-if: po1.10       Out-label-stack: 3/16045
    Backup ftn_ix: 6        (calculated based on s-bfd)
    Attributes:
    Configured:
    Explicit segment-list Name: 48-42
    Last Recorded Error: Next-hop resolution failed for SID-LIST, 00:02:15 ago

  CP ID: 2, S-BFD backup
    Preference: 100    Path Type: Explicit    CP Origin: Local
    CP state: Valid
    Segment List:
    Total no. of segments: 2
    Segment0[LABEL]: Label :16043
    Segment1[LABEL]: Label :16045
    Out-if: xe0          Out-label-stack: 3/16045
    Attributes:
```

```
Configured:
Explicit segment-list Name: 48-43
Last Recorded Error: Next-hop resolution failed for SID-LIST, 00:02:15 ago
```

For more information, see the *Seamless BFD for SR-TE Validation* in the *OcNOS Segment Routing Config Guide document*, Release 6.4.1.

Implementation Examples

To achieve minimal traffic convergence time and a quick switch over to backup if there is any link failure in the primary path.

1. Configure the S-BFD Segment Routing policy NAME where the data enters the traffic on a network and decides which path to flow.
2. Configure the S-BFD discriminator A.B.C.D at the outgoing or existing data from the network traffic.
3. S-BFD starts monitoring the segment routing policy path, once it is mapped to S-BFD.

Troubleshooting

1. Check if the discriminator is learnt at initiator.
2. Check if the learnt discriminator is the same as the segment routing policy end-point address.
3. Check if the segment routing policy is mapped to S-BFD is operationally up.

Abbreviations

Acronym	Description
S-BFD	Seamless Bidirectional Forwarding Detection
SR	Segment Routing
SID	Segment Identifiers
ISIS	Intermediate System to Intermediate System
Q2	Qumran

Glossary

The following provides definitions for key terms used throughout this document.

ISIS	ISIS protocol provides the solution for connecting and managing virtual networks within a data center or network infrastructure
SR	Segment Routing is a method where the sender of a packet can partially or completely specify a route in a network through which a packet is sent
SID	A segment routing mapping server allocates Segment Identifiers (SIDs) for prefixes and ranges in an ISIS segment routing domain
Ingress	Flow of data traffic into a network
Egress	Outgoing or exiting data traffic from a network

Support of 2.5G Speed on Edgecore AS5912-54X Switch

Overview

Feature Characteristics

OcNOS support on Edgecore AS5912-54X now includes compatibility with 2.5G speed, expanding its capabilities beyond the originally supported speeds.on 48 ports. The ports designed for 10G speed can now be configured for 2.5G.

Benefits

This improvement provides users to use the 800 Gbps switching capacity and 2.5G speed on ports within Edgecore AS5912-54X switch, delivering adaptability in network configurations and meeting the growing demand for diverse speed options.

Use Case

Here is an example of a use case where the AS5912-54X required support for 2.5G speed:

In the context of providing fiber optics broadband service to residents in multiple dwelling units (MDUs, such as an apartment building, the AS5912-54X operates as an aggregation switch/router. It establishes connections via optical fiber at 2.5Gbps through SFP+ ports to the customer premise equipment (CPE of MDU residents. The role of the AS5912-54X is to aggregate and distribute the traffic of residents to and from a core network, facilitating a symmetric broadband service over fiber.

References

For more insights into the features, benefits, and specifications of the Edgecore AS5912-54X switch, refer to the Edgecore Datasheet available under Supported Hardware Datasheets on the IP Infusion website.

For more information on the Edgecore AS5912-54X port mapping, refer to the *Edgecore AS5912/AS5916 Port Mapping* chapter in the *Edgecore Installation Guide*, Release 6.4.2.

NetConf Port Access Control

Overview

NetConf is a software tool that provides a mechanism to configure and manage remote network devices seamlessly. It uses a simple Remote Procedure Call (RPC mechanism to facilitate communication between a client and a server.

During the OcNOS installation, the NetConf subsystem called “netconf” is installed. It runs on the default access port 830 over SSH and port 6513 over TLS.

Typically, these default access ports are not configurable and controlled. The NetConf port access control feature enhancement ensures that the Netconf-SSH and NetConf-TLS port access can be controlled and configurable through the *New CLI Commands* introduced in the 6.4.1 release.

Feature Characteristics

- This feature allows access control capabilities for the NetConf-SSH and NetConf-TLS ports.
- Enabling/disabling the port.
- Changing the default port.
- Accessing and controlling the NetConf services through Inband and Outband.
- Applying ACL rules to the NetConf port to control its access.

Benefits

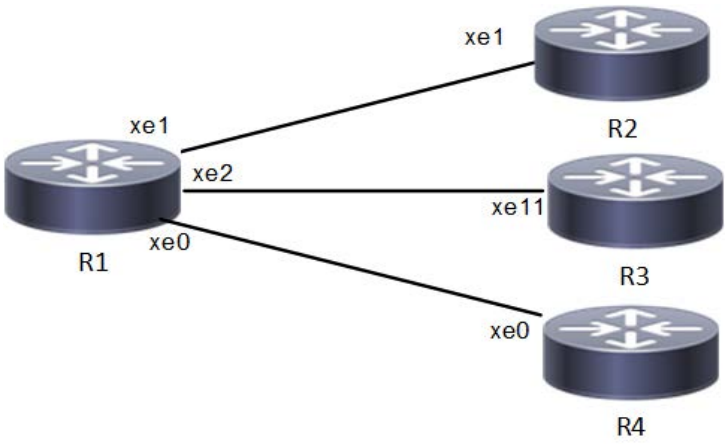
This feature enables the user to control the NetConf port access and change the default port.

Configuration

To configure either NetConf-SSH port or the NetConf-TLS port, perform the following steps. After completing the steps you will be configured with a port for NetConf.

1. Disable `netconf-ssh` and `netconf-tls` feature
2. Configure port for `netconf-ssh` and `netconf-tls`
3. Enable `netconf-ssh` and `netconf-tls` feature

Topology



NetConf Accses Port Topology

Enable Netconf-ssh on the default and vrf management port

R1

`#configure terminal`	Enter Configuration mode.
`R1(config)#feature netconf-ssh`	Enable netconf-ssh via default port.
`R1(config)#feature netconf-ssh vrf management`	Enable netconf-ssh via vrf management port.
`R1(config)#commit`	Commit all the transactions.

Enable Netconf-tls on the default and vrf management port

R1

`#configure terminal`	Enter Configuration mode
`R1(config)#feature netconf-tls`	Enable netconf-tls via default port
`R1(config)#feature netconf-tls vrf management`	Enable netconf-tls via vrf management port
`R1(config)#commit`	Commit all the transactions

Validation

Execute the below commands to verify the NetConf port is enabled on VRF Management.

Following is the output of the NetConf server status and port.

```
#show netconf server
VRF Management
        Netconf SSH Server: Enabled
        SSH-Netconf Port : 830
        Netconf TLS Server: Enabled
        TLS-Netconf Port : 6513
VRF Default
```

```
        Netconf SSH Server: Enabled
        SSH-Netconf Port : 830
        Netconf TLS Server: Enabled
        TLS-Netconf Port : 6513
```

Following is the output of NetConf server configurations.

```
#show running-config netconf-server
!
feature netconf-ssh vrf management
feature netconf-tls vrf management
netconf server ssh-port 2000 vrf management
netconf server tls-port 60000 vrf management
feature netconf-ssh
feature netconf-tls
netconf server ssh-port 1060
netconf server tls-port 5000
!
```

Following is the output of the NetConf server configuration in XML format.

```
#show xml running-config
<netconf-server xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-management-serve
r">
  <vrfs>
    <vrf>
      <vrf-name>default</vrf-name>
      <config>
        <vrf-name>default</vrf-name>
      </config>
      <netconf-ssh-config>
        <config>
          <feature-netconf-ssh>true</feature-netconf-ssh>
          <ssh-port>1060</ssh-port>
        </config>
      </netconf-ssh-config>
      <netconf-tls-config>
        <config>
          <feature-netconf-tls>true</feature-netconf-tls>
          <tls-port>5000</tls-port>
        </config>
      </netconf-tls-config>
    </vrf>
    <vrf>
      <vrf-name>management</vrf-name>
      <config>
        <vrf-name>management</vrf-name>
      </config>
      <netconf-ssh-config>
        <config>
          <feature-netconf-ssh>true</feature-netconf-ssh>
```

```
          <ssh-port>2000</ssh-port>
        </config>
      </netconf-ssh-config>
      <netconf-tls-config>
        <config>
          <feature-netconf-tls>true</feature-netconf-tls>
          <tls-port>60000</tls-port>
        </config>
      </netconf-tls-config>
    </vrf>
  </vrfs>
</netconf-server>
<network-instances xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-network-insta
nce">
  <network-instance>
    <instance-name>default</instance-name>
    <instance-type>vrf</instance-type>
    <config>
      <instance-name>default</instance-name>
      <instance-type>vrf</instance-type>
    </config>
    <vrf xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-vrf">
      <config>
        <vrf-name>default</vrf-name>
      </config>
    </vrf>
  </network-instance>
  <network-instance>
    <instance-name>management</instance-name>
    <instance-type>vrf</instance-type>
    <config>
      <instance-name>management</instance-name>
      <instance-type>vrf</instance-type>
    </config>
    <vrf xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-vrf">
      <config>
        <vrf-name>management</vrf-name>
      </config>
    </vrf>
  </network-instance>
</network-instances>
<interfaces xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-interface">
```

Following is the output after login to the NetConf interface (YangCLI) on R1 node via the default NetConf port:

```
root@OcNOS:~# ip netns exec zebosfib0 yangcli --server=127.1 --user=ocnos --
password=ocnos
```

```
yangcli version 2.5-5
  libssh2 version 1.8.0

  Copyright (c) 2008-2012, Andy Bierman, All Rights Reserved.
  Copyright (c) 2013-2015, Vladimir Vassilev, All Rights Reserved.
  Copyright (c) 2012-2016, OpenClovis Inc, All Rights Reserved.

  Type 'help' or 'help <command-name>' to get started
  Use the <tab> key for command and value completion
  Use the <enter> key to accept the default value in brackets

  These escape sequences are available when filling parameter values:

        ?       help
        ??      full help
        ?s      skip current parameter
        ?c      cancel current command

  These assignment statements are available when entering commands:

        $<varname> = <expr>     Local user variable assignment
        $$<varname> = <expr>    Global user variable assignment
        @<filespec> = <expr>    File assignment
val->res is NO_ERR.

yangcli: Starting NETCONF session for ocnos on 127.1

NETCONF session established for ocnos on 127.1
……..
```

Disable netconf-ssh via default and vrf management port

R1

`#configure terminal`	Enter Configuration mode
`R1(config)#no feature netconf-ssh`	Disable netconf-ssh via default port
`R1(config)#no feature netconf-ssh vrf management`	Disable netconf-ssh via vrf management
`R1(config)#commit`	Commit all the transactions

Disable netconf-tls via default port and vrf management port

R1

`#configure terminal`	Enter Configuration mode
`R1(config)#no feature netconf-tls`	Disable netconf-tls via default
`R1(config)#no feature netconf-tls vrf management`	Disable netconf-tls via vrf management port
`R1(config)#commit`	Commit all the transactions

Validation

Execute the below commands to verify the NetConf port is disabled on VRF Management.

Following is the output of the NetConf server status and port.

```
#show netconf server
VRF Management
        Netconf Server: Disabled
VRF Default
        Netconf Server: Disabled
```

Configuring NetConf Port

R1

`#configure terminal`	Enter Configuration mode
`R1(config)#no feature netconf-ssh`	Disable netconf-ssh via default port
`R1(config)#no feature netconf-ssh vrf management`	Disable netconf-ssh via vrf management port
`R1(config)#no feature netconf-tls`	Disable netconf-tls via default port
`R1(config)#no feature netconf-tls vrf management`	Disable netconf-tls via vrf management port
`R1(config)#commit`	Commit all the transactions
`#configure terminal`	Enter Configuration mode
`R1(config)#netconf server ssh-port 1060`	Configure port for netconf-ssh default
`R1(config)#netconf server ssh-port 2000 vrf management`	Configure port for netconf-ssh vrf management
`R1(config)#netconf server tls-port 5000`	Configure port for netconf-tls default
`R1(config)#netconf server tls-port 60000 vrf management`	Configure port for netconf-tls vrf management
`R1(config)#commit`	Commit all the transactions
`#configure terminal`	Enter Configuration mode
`R1(config)#feature netconf-ssh`	Enable netconf-ssh via default port
`R1(config)#feature netconf-ssh vrf management`	Enable netconf-ssh via vrf management port
`R1(config)#feature netconf-tls`	Enable netconf-tls via default port
`R1(config)#feature netconf-tls vrf management`	Enable netconf-tls via vrf management port
`R1(config)#commit`	Commit all the transactions

Validation

Following is the output of the NetConf server status and port.

```
#show netconf server
VRF Management
        Netconf SSH Server: Enabled
        SSH-Netconf Port : 2000
        Netconf TLS Server: Enabled
        TLS-Netconf Port : 60000
VRF Default
        Netconf SSH Server: Enabled
        SSH-Netconf Port : 1060
        Netconf TLS Server: Enabled
        TLS-Netconf Port : 5000
```

Following is the output after login to the NetConf interface (YangCLI) on R1 node via the user defined NetConf port:

```
root@OcNOS:~# ip netns exec zebosfib1 yangcli --server=127.1 --user=ocnos --
password=ocnos ncport=2000
Warning: Revision date in the future (2022-08-30), further warnings are suppressed
ietf-netconf-notifications.yang:46.4: warning(421): revision date in the future

  yangcli version 2.5-5
  libssh2 version 1.8.0

  Copyright (c) 2008-2012, Andy Bierman, All Rights Reserved.
  Copyright (c) 2013-2015, Vladimir Vassilev, All Rights Reserved.
  Copyright (c) 2012-2016, OpenClovis Inc, All Rights Reserved.

  Type 'help' or 'help <command-name>' to get started
  Use the <tab> key for command and value completion
  Use the <enter> key to accept the default value in brackets

  These escape sequences are available when filling parameter values:

        ?       help
        ??      full help
        ?s      skip current parameter
        ?c      cancel current command

  These assignment statements are available when entering commands:

        $<varname> = <expr>     Local user variable assignment
        $$<varname> = <expr>    Global user variable assignment
        @<filespec> = <expr>    File assignment
val->res is NO_ERR.

yangcli: Starting NETCONF session for ocnos on 127.1

NETCONF session established for ocnos on 127.1
.........................
Checking Server Modules...

yangcli ocnos@127.1>
```

Ping between two nodes via Yang CLI

Perform the following configurations to verify the reachability among R1, R2 and R3 routers via NetConf-SSH and NetConf-TLS port.

R1

`#configure terminal`	Enter Configuration mode
`R1(config)#no feature netconf-ssh`	Disable netconf-ssh via default
`R1(config)#no feature netconf-ssh vrf management`	Disable netconf-ssh via vrf management port
`R1(config)#no feature netconf-tls`	Disable netconf-tls via default port
`R1(config)#no feature netconf-tls vrf management`	Disable netconf-tls via vrf management port
`R1(config)#commit`	Commit all the transactions
`#configure terminal`	Enter Configuration mode
`R1(config)#netconf server ssh-port 1060`	Configure port for netconf-ssh default
`R1(config)#netconf server ssh-port 2000 vrf management`	Configure port for netconf-ssh vrf management
`R1(config)#netconf server tls-port 5000`	Configure port for netconf-tls default
`R1(config)#netconf server tls-port 60000 vrf management`	Configure port for netconf-tls vrf management
`R1(config)#commit`	Commit all the transactions
`#configure terminal`	Enter Configuration mode
`R1(config)#feature netconf-ssh`	Enable netconf-ssh via default port
`R1(config)#feature netconf-ssh vrf management`	Enable netconf-ssh via vrf management port
`R1(config)#feature netconf-tls`	Enable netconf-tls via default port
`R1(config)#feature netconf-tls vrf management`	Enable netconf-tls via vrf management port
`R1(config)#commit`	Commit all the transactions
`#configure terminal`	Enter Configuration mode
`R1(config)#interface xe1`	Enter interface mode
`R1(config)#ip address 10.10.10.1/24`	Configure ipv4 address on the interface xe1.
`R1(config)#commit`	Commit all the transactions

R2

`#configure terminal`	Enter Configuration mode
`R2(config)#no feature netconf-ssh`	Disable netconf-ssh via default
`R2(config)#no feature netconf-ssh vrf management`	Disable netconf-ssh via vrf management
`R2(config)#no feature netconf-tls`	Disable netconf-tls via default

R2(config)#no feature netconf-tls vrf management	Disable netconf-tls via vrf management port
R2(config)#commit	Commit all the transactions
#configure terminal	Enter Configuration mode
R2(config)#netconf server ssh-port 1060	Configure port for netconf-ssh default
R2(config)#netconf server ssh-port 2000 vrf management	Configure port for netconf-ssh vrf management
R2(config)#netconf server tls-port 5000	Configure port for netconf-tls default
R2(config)#netconf server tls-port 60000 vrf management	Configure port for netconf-tls vrf management
R2(config)#commit	Commit all the transactions
#configure terminal	Enter Configuration mode
R2(config)#feature netconf-ssh	Enable netconf-ssh via default port
R2(config)#feature netconf-ssh vrf management	Enable netconf-ssh via vrf management port
R2(config)#feature netconf-tls	Enable netconf-tls via default port
R2(config)#feature netconf-tls vrf management	Enable netconf-tls via vrf management port
R2(config)#commit	Commit all the transactions
#configure terminal	Enter Configuration mode
R2(config)#interface xe1	Enter interface mode
R2(config)#ip address 10.10.10.2/24	Configure ipv4 address on the interface xe1.
R2(config)#commit	Commit all the transactions

Validation

Following is the output of the configured NetConf port.

```
#show netconf server
VRF Management
        Netconf SSH Server: Enabled
        SSH-Netconf Port : 2000
        Netconf TLS Server: Enabled
        TLS-Netconf Port : 60000
VRF Default
        Netconf SSH Server: Enabled
        SSH-Netconf Port : 1060
        Netconf TLS Server: Enabled
        TLS-Netconf Port : 5000

OcNOS#show running-config interface xe1
!
interface xe1
 ip address 10.10.10.1/24
!
OcNOS#ping 10.10.10.2
Press CTRL+C to exit
```

```
PING 10.10.10.2 (10.10.10.2) 56(84) bytes of data.
64 bytes from 10.10.10.2: icmp_seq=1 ttl=64 time=0.567 ms
64 bytes from 10.10.10.2: icmp_seq=2 ttl=64 time=0.258 ms
64 bytes from 10.10.10.2: icmp_seq=3 ttl=64 time=0.241 ms

--- 10.10.10.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 80ms
rtt min/avg/max/mdev = 0.241/0.355/0.567/0.150 ms
```

Following is the output after login to the NetConf interface (YangCLI) on R2 node through the user defined NetConf port:

```
root@OcNOS:~# ip netns exec zebosfib0 yangcli --server=10.10.10.2 --user=ocnos --
password=ocnos ncport=1060
Warning: Revision date in the future (2022-08-30), further warnings are suppressed
ietf-netconf-notifications.yang:46.4: warning(421): revision date in the future

  yangcli version 2.5-5
  libssh2 version 1.8.0

  Copyright (c) 2008-2012, Andy Bierman, All Rights Reserved.
  Copyright (c) 2013-2015, Vladimir Vassilev, All Rights Reserved.
  Copyright (c) 2012-2016, OpenClovis Inc, All Rights Reserved.

  Type 'help' or 'help <command-name>' to get started
  Use the <tab> key for command and value completion
  Use the <enter> key to accept the default value in brackets

  These escape sequences are available when filling parameter values:

        ?       help
        ??      full help
        ?s      skip current parameter
        ?c      cancel current command

  These assignment statements are available when entering commands:

        $<varname> = <expr>     Local user variable assignment
        $$<varname> = <expr>    Global user variable assignment
        @<filespec> = <expr>    File assignment
val->res is NO_ERR.

yangcli: Starting NETCONF session for ocnos on 10.10.10.2

NETCONF session established for ocnos on 10.10.10.2
.........................
Checking Server Modules...

yangcli ocnos@10.10.10.2>
```

ACL Rule with IPv4 Configuration

Perform the following configurations to apply an ACL rule to allow or deny traffic from R1 to other nodes via NetConf port.

R1

`#configure terminal`	Enter Configuration mode
`R1(config)#no feature netconf-ssh`	Disable netconf-ssh via default
`R1(config)#no feature netconf-ssh vrf management`	Disable netconf-ssh via vrf management port
`R1(config)#no feature netconf-tls`	Disable netconf-tls via default port
`R1(config)#no feature netconf-tls vrf management`	Disable netconf-tls via vrf management port
`R1(config)#commit`	Commit all the transactions
`#configure terminal`	Enter Configuration mode
`R1(config)#netconf server ssh-port 1060`	Configure port for netconf-ssh default
`R1(config)#netconf server ssh-port 2000 vrf management`	Configure port for netconf-ssh vrf management
`R1(config)#netconf server tls-port 5000`	Configure port for netconf-tls default
`R1(config)#netconf server tls-port 60000 vrf management`	Configure port for netconf-tls vrf management
`R1(config)#commit`	Commit all the transactions
`#configure terminal`	Enter Configuration mode
`R1(config)#feature netconf-ssh`	Enable netconf-ssh via default port
`R1(config)#feature netconf-ssh vrf management`	Enable netconf-ssh via vrf management port
`R1(config)#feature netconf-tls`	Enable netconf-tls via default port
`R1(config)#feature netconf-tls vrf management`	Enable netconf-tls via vrf management port
`R1(config)#commit`	Commit all the transactions
`#configure terminal`	Enter Configuration mode
`R1(config)#interface xe1`	Enter interface mode
`R1(config)#ip address 10.10.10.1/24`	Configure ipv4 address on the interface xe1.
`R1(config)#commit`	Commit all the transactions
`#configure terminal`	Enter Configuration mode
`R1(config)#interface xe2`	Enter interface mode
`R1(config)#ip address 20.20.20.1/24`	Configure ipv4 address on the interface xe2.
`R1(config)#commit`	Commit all the transactions
`#configure terminal`	Enter Configuration mode
`R1(config)#ip access-list ACL1`	Create ip access list
`R1(config)#permit any host 10.1.1.1 any`	Create an acl rule to permit

`R1(config)#deny any host 20.1.1.1 any`	Create an acl rule to deny
`R1(config)#commit`	Commit all the transactions

R2

Perform the following configurations to apply an ACL rule to allow or deny traffic from R2 to other nodes via NetConf port

`#configure terminal`	Enter Configuration mode
`R2(config)#no feature netconf-ssh`	Disable netconf-ssh via default
`R2(config)#no feature netconf-ssh vrf management`	Disable netconf-ssh via vrf management
`R2(config)#no feature netconf-tls`	Disable netconf-tls via default
`R2(config)#no feature netconf-tls vrf management`	Disable netconf-tls via vrf management port
`R2(config)#commit`	Commit all the transactions
`#configure terminal`	Enter Configuration mode
`R2(config)#netconf server ssh-port 1060`	Configure port for netconf-ssh default
`R2(config)#netconf server ssh-port 2000 vrf management`	Configure port for netconf-ssh vrf management
`R2(config)#netconf server tls-port 5000`	Configure port for netconf-tls default
`R2(config)#netconf server tls-port 60000 vrf management`	Configure port for netconf-tls vrf management
`R2(config)#commit`	Commit all the transactions
`#configure terminal`	Enter Configuration mode
`R2(config)#feature netconf-ssh`	Enable netconf-ssh via default port
`R2(config)#feature netconf-ssh vrf management`	Enable netconf-ssh via vrf management port
`R2(config)#feature netconf-tls`	Enable netconf-tls via default port
`R2(config)#feature netconf-tls vrf management`	Enable netconf-tls via vrf management port
`R2(config)#commit`	Commit all the transactions
`#configure terminal`	Enter Configuration mode
`R2(config)#interface xe1`	Enter interface mode
`R2(config)#ip address 10.10.10.2/24`	Configure ipv4 address on the interface xe1.
`R2(config)#commit`	Commit all the transactions

R3

Perform the following configurations to apply an ACL rule to allow or deny traffic from R3 to other nodes via NetConf port.

`#configure terminal`	Enter Configuration mode
`R3(config)#no feature netconf-ssh`	Disable netconf-ssh via default

R3(config)#no feature netconf-ssh vrf management	Disable netconf-ssh via vrf management port
R3(config)#no feature netconf-tls	Disable netconf-tls via default port
R3(config)#no feature netconf-tls vrf management	Disable netconf-tls via vrf management port
R3(config)#commit	Commit all the transactions
#configure terminal	Enter Configuration mode
R3(config)#netconf server ssh-port 1060	Configure port for netconf-ssh default
R3(config)#netconf server ssh-port 2000 vrf management	Configure port for netconf-ssh vrf management
R3(config)#netconf server tls-port 5000	Configure port for netconf-tls default
R3(config)#netconf server tls-port 60000 vrf management	Configure port for netconf-tls vrf management
R3(config)#commit	Commit all the transactions
#configure terminal	Enter Configuration mode
R3(config)#feature netconf-ssh	Enable netconf-ssh via default port
R3(config)#feature netconf-ssh vrf management	Enable netconf-ssh via vrf management port
R3(config)#feature netconf-tls	Enable netconf-tls via default port
R3(config)#feature netconf-tls vrf management	Enable netconf-tls via vrf management port
R3(config)#commit	Commit all the transactions
#configure terminal	Enter Configuration mode
R3(config)#interface xe11	Enter interface mode
R3(config)#ip address 20.20.20.2/24	Configure ipv4 address on the interface xe11.
R3(config)#commit	Commit all the transactions

Validation

Following is the output to verify the user defined NetConf port.

```
R1#show running-config netconf-server
!
feature netconf-ssh vrf management
feature netconf-tls vrf management
netconf server ssh-port 2000 vrf management
netconf server tls-port 60000 vrf management
feature netconf-ssh
feature netconf-tls
netconf server ssh-port 1060
netconf server tls-port 5000
!

R1#show netconf server
VRF Management
        Netconf SSH Server: Enabled
        SSH-Netconf Port : 2000
```

```
        Netconf TLS Server: Enabled
        TLS-Netconf Port : 60000
VRF Default
        Netconf SSH Server: Enabled
        SSH-Netconf Port : 1060
        Netconf TLS Server: Enabled
        TLS-Netconf Port : 5000
```

Following is the output of the show running-config in XML format.

```
R1#show xml running-config
<netconf-server xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-management-serve
r">
  <vrfs>
    <vrf>
      <vrf-name>default</vrf-name>
      <config>
        <vrf-name>default</vrf-name>
      </config>
      <netconf-ssh-config>
        <config>
          <feature-netconf-ssh>true</feature-netconf-ssh>
          <ssh-port>1060</ssh-port>
        </config>
      </netconf-ssh-config>
      <netconf-tls-config>
        <config>
          <feature-netconf-tls>true</feature-netconf-tls>
          <tls-port>5000</tls-port>
        </config>
      </netconf-tls-config>
    </vrf>
    <vrf>
      <vrf-name>management</vrf-name>
      <config>
        <vrf-name>management</vrf-name>
      </config>
      <netconf-ssh-config>
        <config>
          <feature-netconf-ssh>true</feature-netconf-ssh>
          <ssh-port>2000</ssh-port>
        </config>
      </netconf-ssh-config>
      <netconf-tls-config>
        <config>
          <feature-netconf-tls>true</feature-netconf-tls>
          <tls-port>60000</tls-port>
        </config>
      </netconf-tls-config>
    </vrf>
```

```
  </vrfs>
</netconf-server>
<network-instances xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-network-insta
nce">
  <network-instance>
    <instance-name>default</instance-name>
    <instance-type>vrf</instance-type>
    <config>
      <instance-name>default</instance-name>
      <instance-type>vrf</instance-type>
    </config>
    <vrf xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-vrf">
      <config>
        <vrf-name>default</vrf-name>
      </config>
    </vrf>
  </network-instance>
  <network-instance>
    <instance-name>management</instance-name>
    <instance-type>vrf</instance-type>
    <config>
      <instance-name>management</instance-name>
      <instance-type>vrf</instance-type>
    </config>
    <vrf xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-vrf">
      <config>
        <vrf-name>management</vrf-name>
      </config>
    </vrf>
  </network-instance>
</network-instances>
<interfaces xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-interface">
```

Implementation Examples

The below examples are based on the topology given in Topology section.

Accessing R1 from R2 with default port

Below is an example to access R1 from R2 with default port.

From OcNOS CLI:

```
feature netconf-ssh
feature netconf-ssh vrf management
feature netconf-tls
feature netconf-tls vrf management
```

From Yang CLI:

```
root@OcNOS:~# ip netns exec zebosfib0 yangcli --server=127.1 --user=ocnos --
password=ocnos
```

Accessing R1 from R2 with user defined port

Below is an example to access R1 from R2 via user defined port.

From OcNOS CLI:

```
netconf server ssh-port 1060
netconf server ssh-port 2000 vrf management
netconf server tls-port 5000
netconf server tls-port 60000 vrf management
```

From Yang CLI:

```
root@OcNOS:~#ip netns exec zebosfib1 yangcli --server=10.10.10.1 --user=ocnos --
password=ocnos ncport=2000
```

Applying ACL rule to permit or deny any Node

Below is an example to permit any traffic originating from IP address 10.1.1.1. and deny any traffic originating from 20.1.1.1.

From OcNOS CLI:

```
ip access-list ACL1
permit any host 10.1.1.1  any
deny any host   20.1.1.1 any
Permitting R2 and denying R3
```

From Yang CLI:

```
root@OcNOS:~# ip netns exec zebosfib1 yangcli --server=10.10.10.2 --user=ocnos --
password=ocnos ncport=2000
```

New CLI Commands

feature netconf-ssh

Use this command to enable or disable the netconf-ssh feature specific to the management VRF. When netconf feature-ssh is enabled, it allows the logins through the default netconf-ssh port or through default ssh port if feature SSH is also enabled.

Command Syntax

```
feature netconf-ssh (vrf management|)
no feature netconf-ssh (vrf management|)
```

Parameters

`vrf management` Specifies the management Virtual Routing and Forwarding

Default

Disabled by default.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The following example shows you how to enable NetConf SSH on either the VRF management port or the default port. The no parameter disables the same.

```
(config)#feature netconf-ssh vrf management
(config)#feature netconf-ssh
(config)#no feature netconf-ssh vrf management
(config)#no feature netconf-ssh
#
```

feature netconf-tls

Use this command to enable or disable the NetConf TLS feature specific to a VRF. When netconf feature-ssh is enabled, it allows the logins through the default netconf-tls port and allows login through a default TLS port when the TLS feature is also enabled.

Command Syntax

```
feature netconf-tls (vrf management|)
no feature netconf-tls (vrf management|)
```

Parameters

`vrf management` Specifies management Virtual Routing and Forwarding.

Default

Disabled by default.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The following example shows how to execute the CLI:

```
(config)#feature netconf-tls vrf management
(config)#feature netconf-tls
(config)#no feature netconf-tls vrf management
```

```
(config)#no feature netconf-tls
```

If either NetConf SSH or NetConf TLS are disabled one after the other, the following error message will be displayed, `% Disabling this will stop the netconf service that is running in management vrf"` as shown below.

Management VRF Configuration

```
OcNOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#no feature netconf-ssh vrf management
(config)#commit
(config)#no feature netconf-tls vrf management
(config)#commit
% Disabling this will stop the netconf service that is running in management vrf.
```

Default VRF Configuration

```
OcNOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#no feature netconf-ssh vrf management
(config)#commit
(config)#no feature netconf-tls vrf management
(config)#commit
% Disabling this will stop the netconf service that is running in defualt vrf.
```

netconf-ssh port

Use this command to either configure or unconfigure the custom NetConf SSH port.

Command Syntax

```
netconf-server ssh-port <1024-65535> (vrf management|)
no netconf-server ssh-port (vrf management|)
```

Parameters

`<1024-65535>`	Port range values
`Default`	By default, the netconf-ssh port value is 830.
`vrf`	Specifies the management Virtual Routing and Forwarding name

Command Mode

Config mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The following example shows how to execute the CLI:

```
(config)#netconf server ssh-port ?
```

```
  <1024-65535>  port
(config)#netconf server ssh-port 1024 vrf management
(config)#netconf server ssh-port 2000
(config)#no netconf server ssh-port
(config)#no netconf server ssh-port vrf management
```

netconf-tls port

Use this command to either configure or unconfigure the indicated NetConf TLS port.

Command Syntax

```
netconf-server tls-port <1024-65535> (vrf management|)
no netconf-server tls-port (vrf management|)
```

Parameters

`<1024-65535>`	Port range values
`Default`	By default, the netconf-tls port value is 6513.
`vrf`	Specifies the management Virtual Routing and Forwarding name

Command Mode

Config mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

```
(config)#netconf server tls-port ?
  <1024-65535>  port
(config)#netconf server tls-port 5000 vrf management
(config)#netconf server tls-port 3000
(config)#no netconf server tls-port vrf management
(config)#no netconf server tls-port
```

show netconf server

Use this command to display netconf server status.

Command Syntax

```
show netconf server
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 6.4.1.

Examples

The following example shows the output of the CLI:

```
OcNOS#show netconf server
VRF MANAGEMENT
Netconf Server: Enabled
SSH-Netconf Port : 1000
TLS-Netconf Port : 7000
VRF DEFAULT
Netconf Server: Enabled
SSH-Netconf Port : 4500
TLS-Netconf Port : 3000
```

show running-config netconf server

Use this command to display the NetConf server settings that appear in the running configuration.

Command Syntax

```
show running-config netconf-server
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The following example shows the output of the CLI:

```
OcNOS#show running-config netconf-server
feature netconf vrf management
netconf server ssh-port 1000 vrf management
netconf server tls-port 7000 vrf management
feature netconf
netconf server ssh-port 4500
netconf server tls-port 3000
!
```

Revised CLI Commands

The existing `ip access-list tcp|udp` CLI is updated with the following two options to support the Access List (ACL) rules on the NetConf port. The ACL defines a set of rules to control network traffic and reduce network attacks.

`netconf-ssh`	Secure Shell Network Configuration
`netconf-tls`	Transport Layer Security Network Configuration

ip access-list tcp|udp

Use this command to define a named access control list (ACL) that determines whether to accept or drop an incoming TCP or UDP IP packet based on the specified match criteria. This command filters packets based on source and destination IP address along with the TCP or UDP protocol and port.

Use the `no` form of this command to remove an ACL specification.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Note: TCP flags options and range options like neq, gt, lt and range are not supported by hardware in egress direction.

Note: Both Ack and established flag in tcp have same functionality in hardware.

Command Syntax

```
(<1-268435453>|) (deny|permit) tcp (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)
  ((eq|gt|lt|neq) (<0-65535>|bgp|chargen|cmd|daytime|discard|domain|drip|echo
  |exec|finger|ftp |ftp-data|gopher|hostname|ident|irc|klogin|kshell|login
  |lpd|nntp|pim-auto- rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet|time|
  uucp|whois|www)| range <0-65535> <0-65535>|) (A.B.C.D/M|A.B.C.D A.B.C.D|host
  A.B.C.D|any) ((eq|gt|lt|neq) (<0-65535>|bgp|chargen|cmd|daytime|discard|domain|
  drip|echo|exec|finger|ftp|ftp-data|gopher|hostname|ident|irc|klogin|kshell|login
  |lpd|nntp|pim-auto- rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet
  |time|uucp|whois|www|netconf-ssh|netconf-tls) | range <0-65535> <0-65535>|)
  ((dscp (<0-63>| af11| af12| af13| af21| af22| af23| af31| af32| af33| af41| af42|
  af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef)) |(precedence (<0-7>|
  critical| flash | flashoverride| immediate| internet| network| priority|
  routine)) |) ({ack|established|fin|psh|rst|syn|urg}|) vlan <1-4094>|)(inner-vlan
  <1-4094>|)

(<1-268435453>|) (deny|permit) udp (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)
  ((eq|gt|lt|neq) (<0-65535>|biff|bootpc|bootps|discard|dnsix|domain|
  echo|isakmp|mobile-ip |nameserver | netbios-dgm | netbios-ns| netbios-ss|non500-
  isakmp|ntp|pim-auto-rp|rip|snmp|snmptrap|sunrpc|syslog|tacacs|talk|tftp
  |time|who|xdmcp) | range <0-65535> <0-65535>|) (A.B.C.D/M|A.B.C.D A.B.C.D|host
  A.B.C.D|any) ((eq|gt |lt|neq)(<0-65535> |biff |bootpc |bootps| discard| dnsix|
  domain| echo| isakmp|mobile-ip|nameserver|netbios-dgm|netbios-ns|netbios-
  ss|non500-isakmp |ntp|pim-auto- rp| rip| snmp| snmptrap| sunrpc| syslog| tacacs|
  talk| tftp| time| who| xdmcp) | range <0-65535> <0-65535>|) ((dscp (<0-63>| af11|
  af12| af13| af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3|
  cs4| cs5| cs6| cs7| default| ef)) | (precedence (<0-7>| critical| flash |
  flashoverride| immediate| internet| network| priority| routine))|) (vlan <1-
  4094>|)(inner-vlan <1-4094>|)

no (<1-268435453>|) (deny|permit) tcp (A.B.C.D/M|A.B.C.D A.B.C.D|host
  A.B.C.D|any)((eq|gt|lt|neq) (<0-65535>| bgp| chargen| cmd| daytime| discard|
  domain| drip| echo|exec|finger|ftp |ftp-data |gopher |hostname| ident| irc|
  klogin| kshell|login|lpd|nntp|pim-auto-rp |pop2 |pop3 |smtp| ssh| sunrpc| tacacs
  |talk|telnet|time|uucp|whois|www|netconf-ssh|netconf-tls) | range <0-65535> <0-
  65535>|) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)((eq|gt|lt|neq) (<0-65535>
  |bgp |chargen |cmd |daytime|discard|domain|drip|echo|exec|finger|ftp|ftp-data|
  gopher| hostname| ident| irc| klogin| kshell| login| lpd| nntp| pim-auto-rp |
  pop2| pop3| smtp |ssh |sunrpc|tacacs|talk|telnet|time|uucp|whois|www) | range <0-
  65535> <0-65535>|) ((dscp (<0-63>| af11| af12| af13| af21| af22| af23| af31|
  af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef)) |
```

```
(precedence (<0-7>| critical| flash | flashoverride| immediate| internet|
network| priority| routine)) |) ({ack|established|fin|psh|rst|syn|urg}|)(vlan <1-
4094>|)(inner-vlan <1-4094>|)
```

```
no (<1-268435453>|)(deny|permit) udp (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)
((eq|gt|lt|neq) (<0-65535> |biff| bootpc| bootps| discard| dnsix|
domain|echo|isakmp|mobile-ip|nameserver|netbios-dgm|netbios-ns|netbios-
ss|non500-isakmp|ntp|pim-auto-rp|rip|snmp|snmptrap|sunrpc|syslog|tacacs|talk|
tftp|time|who|xdmcp) | range <0-65535> <0-65535>|)(A.B.C.D/M|A.B.C.D A.B.C.D|host
A.B.C.D| any) ((eq|gt|lt|neq) (<0-65535> |biff| bootpc| bootps| discard| dnsix|
domain|echo| isakmp|mobile- ip|nameserver|netbios-dgm|netbios-ns|netbios-
ss|non500-isakmp| ntp|pim-auto-rp|rip|snmp|snmptrap|sunrpc|syslog|
tacacs|talk|tftp|time|who|xdmcp) | range <0-65535> <0-65535>|) ((dscp (<0-63>|
af11| af12| af13| af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2|
cs3| cs4| cs5| cs6| cs7| default| ef)) | (precedence (<0-7>| critical| flash |
flashoverride| immediate| internet| network| priority| routine)) |)(vlan <1-
4094>|)(inner-vlan <1-4094>|)
```

Parameters

`<1-268435453>`	IPv4 ACL sequence number.
`deny`	Drop the packet.
`permit`	Accept the packet.
`tcp`	Transmission Control Protocol.
`udp`	User Datagram Protocol.
`A.B.C.D/M`	Source or destination IP prefix and length.
`A.B.C.D A.B.C.D`	Source or destination IP address and mask.
`host A.B.C.D`	Source or destination host IP address.
`any`	Any source or destination IP address.
`eq`	Source or destination port equal to.
`gt`	Source or destination port greater than.
`lt`	Source or destination port less than.
`neq`	Source or destination port not equal to.
`<0-65535>`	Source or destination port number.
`range`	Range of source or destination port numbers:
`<0``-65535>`	Lowest value in the range.
`<0-`**`65535>`**	Highest value in the range.
`bgp`	Border Gateway Protocol.
`chargen`	Character generator.
`cmd`	Remote commands.
`daytime`	Daytime.
`discard`	Discard.
`domain`	Domain Name Service.
`drip`	Dynamic Routing Information Protocol.

`echo`	Echo.
`exec`	EXEC.
`finger`	Finger.
`ftp`	File Transfer Protocol.
`ftp-data`	FTP data connections.
`gopher`	Gopher.
`hostname`	NIC hostname server.
`ident`	Ident Protocol.
`irc`	Internet Relay Chat.
`klogin`	Kerberos login.
`kshell`	Kerberos shell.
`login`	Login.
`lpd`	Printer service.
`nntp`	Network News Transport Protocol.
`pim-auto-rp`	PIM Auto-RP.
`pop2`	Post Office Protocol v2.
`pop3`	Post Office Protocol v3.
`smtp`	Simple Mail Transport Protocol.
`ssh`	Secure Shell.
`sunrpc`	Sun Remote Procedure Call.
`tacacs`	TAC Access Control System.
`talk`	Talk.
`telnet`	Telnet.
`time`	Time.
`uucp`	UNIX-to-UNIX Copy Program.
`whois`	WHOIS/NICNAME
`www`	World Wide Web.
`netconf-ssh`	**Secure Shell Network Configuration**
`netconf-tls`	**Transport Layer Security Network Configuration**
`nntp`	Range of source or destination port numbers:
`dscp`	Match packets with given DSCP value.
`<0-63>`	Enter DSCP value between 0-63.
`af11`	AF11 DSCP (001010) decimal value 10.
`af12`	AF12 DSCP (001100) decimal value 12.
`af13`	AF13 DSCP (001110) decimal value 14.
`af21`	AF21 DSCP (010010) decimal value 18.
`af22`	AF22 DSCP (010100) decimal value 20.
`af23`	AF23 DSCP (010110) decimal value 22.
`af31`	AF31 DSCP (011010) decimal value 26.

af32	AF32 DSCP (011100) decimal value 28.
af33	AF33 DSCP (011110) decimal value 30.
af41	AF41 DSCP (100010) decimal value 34.
af42	AF42 DSCP (100100) decimal value 36.
af43	AF43 DSCP (100110) decimal value 38.
cs1	CS1 (precedence 1) DSCP (001000) decimal value 8.
cs2	CS2 (precedence 2) DSCP (010000) decimal value 16.
cs3	CS3 (precedence 3) DSCP (011000) decimal value 24.
cs4	CS4 (precedence 4) DSCP (100000) decimal value 32.
cs5	CS5 (precedence 5) DSCP (101000) decimal value 40.
cs6	CS6 (precedence 6) DSCP (110000) decimal value 48.
cs7	CS7 (precedence 7) DSCP (111000) decimal value 56.
default	Default DSCP (000000) decimal value 0.
ef	EF DSCP (101110) decimal value 46.
precedence	Match packets with given precedence value.
<0-7>	Precedence.
critical	Match packets with critical precedence (5).
flash	Match packets with flash precedence (3).
flashoverride	Match packets with flash override precedence (4).
immediate	Match packets with immediate precedence (2).
internet	Match packets with internetwork control precedence (6).
network	Match packets with network control precedence (7).
priority	Match packets with priority precedence (1).
routine	Match packets with routine precedence (0).
ack	Match on the Acknowledgment (ack) bit.
established	Matches only packets that belong to an established TCP connection.
fin	Match on the Finish (fin) bit.
psh	Match on the Push (psh) bit.
rst	Match on the Reset (rst) bit.
syn	Match on the Synchronize (syn) bit.
urg	Match on the Urgent (urg) bit.
biff	Biff.
bootpc	Bootstrap Protocol (BOOTP) client.
bootps	Bootstrap Protocol (BOOTP) server.
discard	Discard.
dnsix	DNSIX security protocol auditing.
domain	Domain Name Service.
echo	Echo.
isakmp	Internet Security Association and Key Management Protocol.

`mobile-ip`	Mobile IP registration.
`nameserver`	IEN116 name service.
`netbios-dgm`	Net BIOS datagram service.
`netbios-ns`	Net BIOS name service.
`netbios-ss`	Net BIOS session service.
`non500-isakmp`	Non500-Internet Security Association and Key Management Protocol.
`ntp`	Network Time Protocol.
`pim-auto-rp`	PIM Auto-RP.
`rip`	Routing Information Protocol.
`snmp`	Simple Network Management Protocol.
`snmptrap`	SNMP Traps.
`sunrpc`	Sun Remote Procedure Call.
`syslogS`	ystem Logger.
`tacacs`	TAC Access Control System.
`talk`	Talk.
`tftp`	Trivial File Transfer Protocol.
`time`	Time.
`who`	Who service.
`xdmcp`	X Display Manager Control Protocol.
`vlan`	Match packets with given vlan value.
`<1-4094>`	VLAN identifier.
`inner-vlan`	Match packets with given inner vlan value.
`<1-4094>`	VLAN identifier.

Default

No default value is specified.

Command Mode

IP access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following is an example to execute the CLI:

```
#configure terminal
(config)#ip access-list ip-acl-02
(config-ip-acl)#deny udp any any eq tftp
(config-ip-acl)#deny tcp any any eq ssh
(config-ip-acl)#end.
```

Abbreviations

The following are some key abbreviations and their meanings relevant to this document:

Acronym	Description
ACL	Access control list
RPC	Remote Procedure Call
SSH	Secure Shell
TLS	Transport Layer Security

Role-Based Access Control

Overview

The Role-Based Access Control (RBAC) feature in OcNOS allows the creation of custom user roles locally. This provides administrators with the flexibility to define specific groups of commands that can be allowed or denied for each role. Users can then be assigned to these user roles on a per-switch basis or by utilizing a TACACS+ server.

Feature Characteristics

RBAC offers the capability to restrict or permit users from executing CLI commands in OcNOS and command authorization is entirely handled within OcNOS. With Role-Based Command Authorization, administrators can create the following entities:

- Policy
- User Role
- User Name

Policy

A policy is a collection of rules that determine which commands are permitted or denied. The maximum number of policies that can be configured is 20.

User Role

User roles group users together, allowing restrictions to be applied based on the policies associated with the role. When creating a User Role, a default policy should be specified. This default policy determines whether all commands are permitted or denied by default. One or more policies can be attached to a User Role. The maximum number of roles that can be configured is 14.

User Name

Users can be assigned to predefined user roles or customized roles. Some predefined roles include:

- Network-Administrator
- Network-Operator
- Network-Engineer
- Network-User

Multiple users can be assigned the same User Role.

RBAC user accounts will not be deleted when a corresponding RBAC-role is deleted or when the dynamic-RBAC feature is disabled. If an RBAC-user is authenticated but the associated role is not present, the user privilege will default to network-user privilege, and the role will be displayed as RBAC-customized-role in the `show users` command.

Benefits

RBAC ensures secure and controlled access to CLI commands, streamlining network management.

Prerequisites

Ensure there is a supported OcNOS router with management interface access.

Configuration

Here is the example configurations for the RBAC feature. For TACACS+ configurations, see the TACACS Client Configuration chapter in the System Management guide, Release 6.4.1.

Note: When implemented, users will have visibility into the imposed restrictions through the `show running-config` command. Additionally, both the configured policy and role specifics can be observed using the `show running-config` command.

Example 1:

In the provided example, RBAC is employed to define user roles and policies that restrict command access for enhanced security and control. Here is the configuration steps:

```
OcNOS#show running-config rbac
feature dynamic-rbac
policy p1
 permit "enable"
 permit "configure terminal"
 Permit "snmp-server .*"
role custom
 default deny-all
 add policy p1
OcNOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
OcNOS(config)#username test password Test@123
OcNOS(config)#username test role custom
OcNOS(config)#commit
OcNOS#sh user-account
User:ocnos
                roles: network-admin
User:test
                roles: custom
```

- The RBAC feature is enabled with the `feature dynamic-rbac` command.
- A policy named `p1` is created, allowing specific commands such as `enable`, `configure terminal`, and `SNMP-related` commands.
- A custom role called `custom` is established, with a default action to deny all commands (`default deny-all`). The previously defined policy `p1` is added to this role.
- A new user account named `test` is created with the password `Test@123`, and the role custom is assigned to this user.
- The configuration changes are committed using the `commit` command.The output indicates that the user `test` has the custom role, granting specific permissions.

```
root@debian:~# ssh test@10.12.29.130
test@10.12.29.130's password:
Last login: Tue Aug 23 01:06:31 2022 from 10.12.17.153

OcNOS version DELL_S3048-ON-OcNOS-1.3.9.364-ENT_IPBASE-S0-P0  01/21/2022
15:03:56
```

```
OcNOS>en
OcNOS#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
OcNOS(config)#snmp-server community test vrf management -->Allowed
OcNOS(config)#ntp server 1.1.1.1 vrf management      -->Not Allowed
% Access restricted for user %
```

- The user test logs into the system via SSH and demonstrates RBAC enforcement by successfully executing permitted SNMP-related commands but encountering an access restriction when attempting an unauthorized command (`ntp server`).
- This example showcases RBAC in action, illustrating how user roles and policies can control command access based on predefined configurations.

Example 2:

In the below example, the user `test1` establishes an SSH connection and demonstrates the RBAC setup. As the default action `permits all` commands except SNMP-related ones, the user is able to execute various configurations, except for `snmp-server` configurations:

```
OcNOS#show running-config rbac
feature dynamic-rbac
policy p1
 permit "enable"
 permit "configure terminal"
 permit "snmp-server .*" mode config
policy p2
 permit "enable"
 permit "configure terminal"
 deny "snmp-server .*"
role custom-snmp
 default permit-all
 add policy p2
OcNOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
OcNOS(config)#username test1 password Test@1234
OcNOS(config)#username test1 role custom-snmp
OcNOS(config)#commit
OcNOS#sh user-account
User:ocnos
                roles: network-admin
User:test1
                roles: custom-snmp

root@debian:~# ssh test1@10.12.29.130
test1@10.12.29.130's password:

OcNOS version DELL_S3048-ON-OcNOS-1.3.9.364-ENT_IPBASE-S0-P0  01/21/2022
15:03:56
OcNOS>enable
OcNOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
OcNOS(config)#ntp server 1.1.1.1 vrf management          --> Allowed
OcNOS(config)#snmp-server community test vrf management  -->Not Allowed
% Access restricted for user %
```

Implementation Examples

RBAC provides a structured and efficient approach to managing and controlling user access to various resources and functionalities within a system. RBAC is particularly beneficial in scenarios with multiple users with varying levels of permissions and responsibilities. Some common use cases for RBAC include:

Network Security: RBAC enhances network security by restricting users to only the resources and commands they need for their roles, reducing the risk of unauthorized access and potential breaches.

Administrative Efficiency: RBAC simplifies user management by categorizing users into predefined roles and streamlining tasks such as provisioning, access updates, and permissions adjustments.

Regulatory Compliance: RBAC ensures compliance with regulations by enforcing proper access controls and maintaining audit trails, helping organizations meet required standards for data security and privacy.

Reduced Human Error: RBAC minimizes the chance of human errors that could lead to network disruptions or security incidents, as users are limited to the specific commands relevant to their roles.

Access Segmentation: In multi-tenant or multi-customer environments, RBAC facilitates access segmentation, ensuring that different groups can only interact with their designated resources, enhancing isolation and privacy.

New CLI Commands

Here is the compilation of the new commands for configuring RBAC feature. For TACACS+ commands, see the *TACACS+* chapter in the System Management guide, Release 6.4.1.

add policy

Use this command to add a policy to a TACACS+ role-based authorization (RBAC) role.

Use the `no` form of this command to remove a policy from an RBAC role.

Command Syntax

```
add policy POLICY-NAME
no add policy POLICY-NAME
```

Parameters

`POLICY-NAME`	Name of the policy

Default

None

Command Mode

RBAC role mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The following examples demonstrate the configuration of a role named 'myRole,' defining its default permissions, adding 'myPolicy1' to the role, and subsequently removing 'myPolicy2' from it.

```
OcNOS(config)#role myRole
OcNOS(config-role)#default permit-all
OcNOS(config-role)#add policy myPolicy1
OcNOS(config-role)#no add policy myPolicy2
OcNOS(config-role)#exit
```

default

Use this command to set the default rule for a TACACS+ role-based authorization (RBAC) role.

Use the no parameter with this command to remove the default rule for a TACACS+ role-based authorization (RBAC) role.

Command Syntax

```
default (permit-all | deny-all)
no default
```

Parameters

permit-all	Permit all commands
deny-all	Deny all commands

Default

Unless this command is explicitly configured, the default rule for a role is deny-all.

Command Mode

RBAC role mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The below example illustrates the configuration of a role named 'myRole' in OcNOS, and specifying its default permission.

```
OcNOS(config)#role myRole
OcNOS(config-role)#default permit-all
OcNOS(config-role)#exit
```

deny

Use this command to add a deny rule to a TACACS+ role-based authorization (RBAC) policy.

Use the no form of this command to remove a deny rule from an RBAC policy.

Command Syntax

```
deny RULE-STRING (mode MODE-NAME |)
```

```
no deny RULE-STRING (mode MODE-NAME |)
```

Parameters

RULE-STRING	Command string
MODE-NAME	Command prompt string such as “config-router” or “config-if”. Deny access to the command only in this mode.

Default

None

Command Mode

RBAC policy mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The example below illustrates the configuration of a policy named '`myPolicy`' in OcNOS. It includes a deny rule that restricts access to the '`ip address`' command, specifically within the configuration interface mode (`config-if`).

```
OcNOS#configure terminal
OcNOS(config)#policy myPolicy
OcNOS(config-policy)#deny “ip address” mode config-if
OcNOS(config-policy)#end
```

feature dynamic-rbac

Use this command to enable the TACACS+ role-based authorization (RBAC) feature.

Use the `no` form of this command to disable the RBAC feature.

Command Syntax

```
feature dynamic-rbac
```

```
no feature dynamic-rbac
```

Parameters

None

Default

By default, feature TACACS+ RBAC is disabled.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The example below illustrates the configuration of enabling the TACACS+ RBAC feature.

```
OcNOS#configure terminal
OcNOS(config)#feature dynamic-rbac
```

permit

Use this command to add a permit rule to a TACACS+ role-based authorization (RBAC) policy.

Use the `no` form of this command to remove a permit rule in an RBAC policy.

Command Syntax

```
permit RULE-STRING (mode MODE-NAME |)
no permit RULE-STRING (mode MODE-NAME |)
```

Parameters

`RULE-STRING`	Command string
`MODE-NAME`	Command prompt string such as “config-router” or “config-if”. Permit access to the command only in this mode.

Default

None

Command Mode

RBAC policy mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The following examples demonstrate the configuration of a policy named '`myPolicy`', permitting access to the '`ip address`' command specifically in the configuration interface mode.

```
OcNOS#configure terminal
OcNOS(config)#policy myPolicy
OcNOS(config-policy)#permit “ip address” mode config-if
```

policy

Use this command to create a TACACS+ role-based authorization (RBAC) policy and enter RBAC policy mode.

Use the `no` form of this command to remove an RBAC policy.

Command Syntax

```
policy POLICY-NAME
no policy POLICY-NAME
```

Parameters

`POLICY-NAME`	Policy name

Default

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The following examples demonstrate the configuration of creating the RBAC policy named `myPolicy`, and the command prompt enters the policy configuration mode.

```
OcNOS#configure terminal
OcNOS(config)#policy myPolicy
OcNOS(config-policy)#exit
```

role

Use this command to create a TACACS+ role-based authorization (RBAC) role and enter RBAC role mode.

Use the `no` form of this command to remove an RBAC role.

Command Syntax

```
role ROLE-NAME
no role ROLE-NAME
```

Parameters

`ROLE-NAME`	Role name
	User *cannot* specify one of these roles already defined in OcNOS:
	`network-admin`
	`network-user`
	`network-operator`
	`network-engineer`
	For more about these built-in roles, see *username.*

Default

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The following examples demonstrate the configuration of creating the RBAC role named 'myRole,' with the command prompt entering the role configuration mode.

```
OcNOS#configure terminal
OcNOS(config)#role myRole
OcNOS(config-role)#exit
```

show rbac-policy

Use this command to display TACACS+ role-based authorization (RBAC) policies.

Command Syntax

```
show rbac-policy (POLICY-NAME |)
```

Parameters

POLICY-NAME	Policy name

Default

None

Command Mode

Exec and privileged exec mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The following examples display the show output of the RBAC policy named 'myPolicy' and its associated configurations.

```
OcNOS#show rbac-policy myPolicy
-----------------------------------------------------------------------
Policy Name     : myPolicy
permit "ip address" mode config-if
```

show rbac-role

Use this command to display information about TACACS+ role-based authorization (RBAC) roles.

Command Syntax

```
show rbac-role (ROLE-NAME |)
```

Parameters

ROLE-NAME	Role name

Default

None

Command Mode

Exec and privileged exec mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The following examples display the show output of the RBAC role named '`myRole`' and its associated configurations.

```
OcNOS#show rbac-role myRole
-------------------------------------------------------------------------
Role Name           : myRole
Default rule        : permit-all
Attached Policies   : myPolicy1
                    : myPolicy2

-------------------------------------------------------------------------
```

Table P-2-1 explains the output fields.

Table 2-1: show rbac-role fields

Entry	Description
Role Name	Displays the name of the role, in this case, `myRole`.
Default rule	Indicates the default rule associated with the role, which can be `permit-all` or `deny-all`.
Attached Policies	Lists the names of policies that are attached to this role. In the example, `myPolicy1` and `myPolicy2` are attached to `myRole`.

Troubleshooting

For smooth operation, verify accurate sensor path configuration, check encoding method compatibility, and ensure proper router-management system connectivity.

Abbreviations

The following are some key abbreviations and their meanings relevant to this document:

Acronym	Description
RBAC	Role Based Access Control
TACACS	Terminal Access Controller Access Control System
TACACS+	Enhanced version of TACACS

Glossary

The following provides definitions for key terms used throughout this document.

Role-Based Access Control (RBAC)	A security paradigm that restricts system access based on roles assigned to users.
User Role	A predefined or customized grouping of permissions assigned to users.
Policy	A set of rules determining which actions are permitted or denied for a specific user role.
Dynamic-RBAC	Dynamic Role-Based Access Control, allowing role assignment during user authentication.

Hide the Remote AS using the neighbor local-as Command

Overview

In a network, an Autonomous System (AS) is available to define a set of IP routing prefixes that are under a common administration policy control. These defined routing policies are used by other connected routers o n the Internet. When an AS is configured in Border Gateway Protocol (BGP), it is used to share routing information to connected peers. The `neighbor local-as` CLI command configures the AS number to be used with External Border Gateway Protocol (EBGP) peers. By default, the configured AS number is included in the AS-PATH message that is exchanged between the peers.

When a BGP router, configured in one network, connects to another router on the network, it will automatically share routing information with the AS number of both the local and remote routers in the AS-PATH message with other connected, external peers. For example, if a router ISP1-R, accesses services from another router, ISP2-R, ISP1-R router will share routing information with local and remote AS numbers in the AS-PATH message when services are merged. This allows the external peers to learn the AS numbers of remote routers not connected to it (in this case, the AS number of ISP2-R). It is not desirable to disclose the AS number of remote routers to external peers.

To avoid advertising the remote peer's AS number, OcNOS provides an option in the `neighbor local-as` CLI to not include (`no-prepend`) the remote AS number and replace (`replace-as`) it with alternate AS number. Configuring an alternate AS in the BGP neighbor system, provides the ability to hide the AS number of the remote router that actually shares the services. Thus, the AS number of the BGP router that is actually providing services is unknown to the external peer.

Hence, the existing `neighbor local-as` CLI command has been modified in this release.

Feature Characteristics

The `neighbor local-as` CLI is enhanced to hide and replace the AS number of the remote routers not connected to external peer. Two new options '`no-prepend`' and '`replace-as`' have been added. These options replace the AS number with an alternate AS number in the AS_PATH and BGP OPEN message. Hence, the AS of the remote router is unknown to the respective neighbor peer.

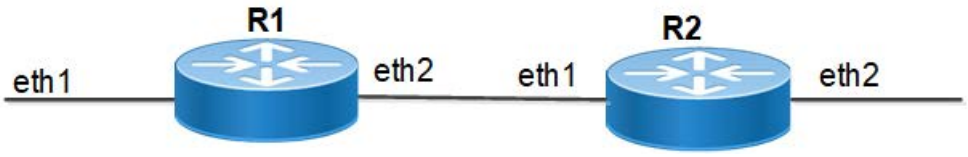
Benefits

The actual Autonomous System number is never shared to the external network.

Configuration

The following configuration assumes the router R1 and R2 is assigned with AS300 and AS100 respectively.

Topology



Disparate Autonomous System Number

R1

Perform the following configuration on R1 router.

`#configure terminal`	Enter configure mode.
`R1(config)#router bgp 300`	Start the BGP process with the Autonomous System number 300
`R1(config-router)#neighbor 10.10.10.2 remote-as 200`	Establish BGP session with neighbor that has AS number 200
`R1(config-router)#address-family ipv4 unicast`	Enter address-family ipv4 unicast mode
`R1(config-router-af)#neighbor 10.10.10.2 activate`	Enable the neighbor 10.10.10.2 router to exchange address family routes
`R1(config-router-af)#redistribute connected`	Redistribute information from connected routes
`R1(config-router-af)#exit-address-family`	Exit address-family IPv4 unicast mode
`R1(config-router)#commit`	Commit the configurations

R2

Perform the following configuration on R2 router.

`#configure terminal`	Enter configure mode
`R2(config)#router bgp 100`	Start the BGP process with the Autonomous System number 100
`R2(config-router)#neighbor 10.10.10.1 remote-as 300`	Establish BGP session with neighbor 10.10.10.1 that has AS number 300
`R2(config-router)#neighbor 10.10.10.1 local-as 200 no-prepend replace-as`	Replace the AS number 300 with AS number 200 that should be used with the neighbor 10.10.10.1
`R2(config-router)#address-family ipv4 unicast`	Enable the neighboring router to exchange address family routes
`R2(config-router-af)#neighbor 10.10.10.2 activate`	Enable the neighbor 10.10.10.2 router to exchange address family routes
`R2(config-router-af)#redistribute connected`	Redistribute information from the connected routes
`R2(config-router-af)#exit-address-family`	Exit address-family ipv4 unicast mode
`R2(config-router)#commit`	Commit the configurations

Validation

Check the AS number 300 running on R1. It has established a BGP connection with 10.10.10.2 router that has AS number of 200.

R1

```
OcNOS#show running-config bgp
!
router bgp 300
 neighbor 10.10.10.2 remote-as 200
 !
 address-family ipv4 unicast
 redistribute connected
 redistribute static
 neighbor 10.10.10.2 activate
 exit-address-family
!

OcNOS#
OcNOS#show ip bgp summary
BGP router identifier 10.10.10.1, local AS number 300
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
10.10.10.2               4   200  185        181       3      0      0  00:00:28       2

Total number of neighbors 1

Total number of Established sessions 1
OcNOS#

OcNOS#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            10.10.10.0/24 is directly connected, ce1, 1d14h18m
B            30.30.30.0/24 [20/0] via 10.10.10.2, ce1, 00:00:18
C            40.40.40.0/24 is directly connected, xe33, 1d13h40m
C            127.0.0.0/8 is directly connected, lo, 1d14h23m
Gateway of last resort is not set
```

```
OcNOS#
```

Check if the AS number 100 for R2 has been replaced with AS number 200 before sharing the information with R1.

R2

```
OcNOS#show running-config bgp
!
router bgp 100
 neighbor 10.10.10.1 remote-as 300
 neighbor 10.10.10.1 local-as 200
 !
 address-family ipv4 unicast
 redistribute connected
 redistribute static
 neighbor 10.10.10.1 activate
 exit-address-family
!
OcNOS#
OcNOS#show ip bgp summary
BGP router identifier 10.10.10.2, local AS number 100
BGP table version is 2
2 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd
10.10.10.1              4   300  180       186      2      0      0       00:00:39       2

Total number of neighbors 1

Total number of Established sessions 1
```

Check if the AS number for R2 is changed to 100 and R1 shares AS 100 in the AS-PATH message.

R1

```
OcNOS#
OcNOS#
OcNOS#show ip bgp
BGP table version is 4, local router ID is 10.10.10.1
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
*> 10.10.10.0/24    0.0.0.0             0         100      32768  ?
*                   10.10.10.2          0         100       0     200 100 ?
*> 30.30.30.0/24    10.10.10.2          0         100       0     200 100 ?
*> 40.40.40.0/24    0.0.0.0             0         100       32768  ?
```

```
Total number of prefixes 3
```

neighbor local-as

Use this command to specify an Autonomous System (AS) number to use with a BGP neighbor.

Use the `no` parameter with this command to disable this command.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) local-as <1-4294967295>  (no-prepend|) (replace-as|)
no neighbor (A.B.C.D|X:X::X:X|WORD) local-as <1-4294967295>
no neighbor (A.B.C.D|X:X::X:X|WORD) local-as <1-4294967295> no-prepend
no neighbor (A.B.C.D|X:X::X:X|WORD) local-as <1-4294967295> replace-as
```

For BGP unnumbered mode:

```
neighbor WORD local-as <1-4294967295>  (no-prepend|) (replace-as|)
no neighbor WORD local-as <1-4294967295>
no neighbor WORD local-as <1-4294967295> no-prepend
no neighbor WORD local-as <1-4294967295> replace-as
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in IPv4 format
`X:X::X:X`	Address of the BGP neighbor in IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`<1-4294967295>`	A neighbor's AS number when extended capabilities are configured
`no-prepend`	Do not prepend local-as to update from EBGP peers
`replace-as`	Replace actual AS with local AS in the EBGP update

Note: The AS number 23456 is a reserved 2-byte AS number. An old BGP speaker (2-byte implementation) should be configured with 23456 as its remote AS number while peering with a non-mappable new BGP speaker (4-byte implementation).

Default

By default, local-as is disabled.

Command Mode

Router mode and Address Family-VRF mode and BGP unnumbered mode

Applicability

This command was introduced before OcNOS version 1.3. The new version of the command with “no-prepend” and “replace-as“ option is introduced in OcNOS version 6.4.1.

Example

The following example show a sample configuration command.

```
#configure terminal
(config)#router bgp 100
(config-router)#neighbor 20.1.1.3 remote-as 300
(config-router)#neighbor 20.1.1.3 local-as 200 no-prepend replace-as

(config)#router bgp 100
(config-router)#address-family ipv6 vrf VRF_A
(config-router-af)#neighbor 3ffe:15:15:15:15::0 remote-as 300
(config-router-af)#neighbor 3ffe:15:15:15:15::0 local-as 200
```

For unnumbered peer below configuration is given in BGP unnumbered-mode.

```
(config)#router bgp 100
(config-router)#bgp unnumbered-mode
(config-router-unnum)#neighbor eth1 local-as 300
```

Abbreviations

Acronym	Description
ASN	Autonomous System Number
EBGP	External Border Gateway Protocol

Port Breakout (400G) for Qumran2 Series Platforms

Overview

The port breakout capability offers a robust and secure solution for divide 400GbE ports into multiple port, ensuring a reliable network infrastructure. In today's networks, there's a demand for a diverse range of Ethernet interface speeds, including 10GbE, 25GbE, 40GbE, and 100GbE. It is essential to have a variety of cost-effective cabling options. This flexibility is crucial to address connectivity requirements and facilitate seamless migrations as network speeds and density needs continue to evolve.

Each 400GbE port (QSFP-DD) has the capacity to support up to eight SERDES, with each SERDES capable of delivering 50G of bandwidth. This capability allows for the following port configurations. The default SERDES mode operates at 50G.

Feature Characteristics

Breakout configurations facilitate the connection between network devices with varying port speeds, allowing for the optimal utilization of port bandwidth.

The breakout mode on network equipment, such as switches, routers, and servers, opens up new possibilities for network operators to keep up with the pace of bandwidth demand. By adding high-speed ports that support breakout mode, network operators can increase the front port density and incrementally enable an upgrade to higher data rates.

Benefits

The 400G platforms empower data centers and high-performance computing environments to meet the increasing demand for greater bandwidth at a reduced cost and power consumption per gigabit. Some key benefits of these platforms include:

• Upgrades from 100G to 400G systems increases the available switching bandwidth by a factor of 4, effectively addressing the need for higher data throughput.

• Enables the use of optical or copper breakouts to create higher density 100G ports, providingmore options for data connectivity and transmission.

• Reduces the number of optical fiber links, connectors, and patch panels required, achieving a fourfold reduction in infrastructure components when compared to 100G platforms with the same aggregate bandwidth. This reduction contributes to cost savings and simplifies network management.

Configuration

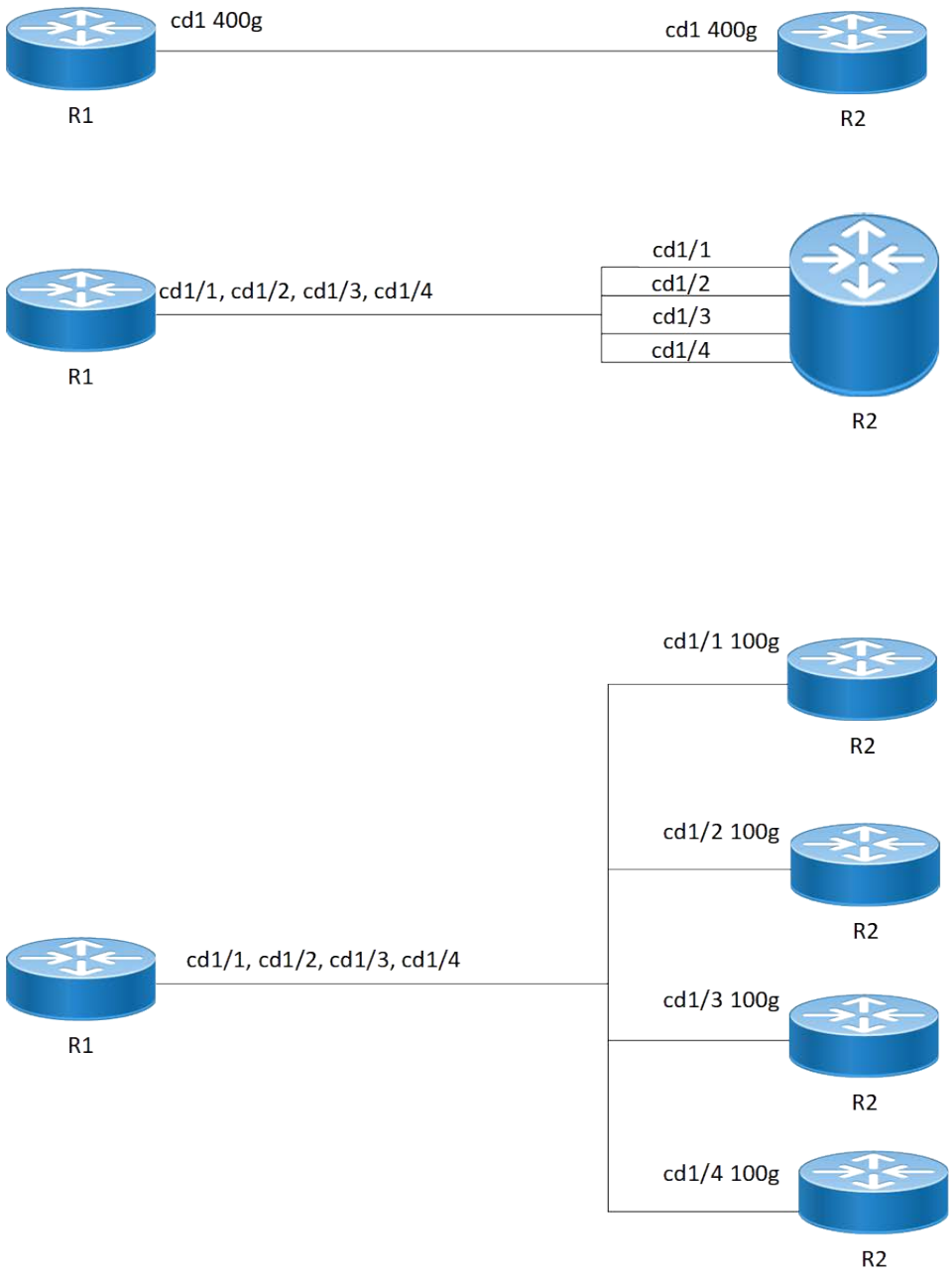
Use the `config# qsfp dd application` command to select the application ID to be configured for this QSFP-DD module.

Note: Only 400G application modes are supported.

Use the `show qsfp ddport no > advertisement applications` command to check the application modes.

Topology

The platform supports splitting a single 400G (QSFP-DD) port into any of the following ports.



400G Port Breakout Configuration

R1

The following table outlines the configuration steps for dividing a single port into multiple ports through channelization.

`OcNOS#configure terminal`	Enter Configuration mode.
`OcNOS(config)# qsfp-dd 49`	Enter the QSFP-DD mode.
`OcNOS(config-qsfp-dd)#application 3`	Select the application ID to be configured for this QSFP-DD module.
`OcNOS(config)#commit`	Commit the configuration.

EEPROM Details for ZR+ Optics

The below show command displays output for “SO-TQSFPDD4CCZRP” optics.

Execute the “`show qsfp-dd 3 eeprom`” command in the terminal window.

```
Port Number                    : 3
Identifier                     : QSFP-DD Double Density 8X Pluggable Transceiver
Name                           : SmartOptics
OUI                            : 0x0 0x53 0x4f
Part No                        : SO-TQSFPDD4CCZRP
Revision Level                 : A
Serial_Number                  : 223950575
Manufacturing Date             : 220926   (yymmddvv, v=vendor specific)
Module Power Class             : 8
Module Max Power               : 23.75 Watt
Cooling Implemented            : Yes
Module Temperature Max         : 80 Celsius
Module Temperature Min         : 0 Celsius
Operating Voltage Min          : 3.12 Volt
Optical Detector               : PIN
Rx Power Measurement           : Average Power
Tx Disable Module Wide         : No
Cable Assembly Link Length     : Separable Media
Connector Type                 : LC (Lucent Connector)
Media Interface Technology     : 1550 nm DFB
CMIS Revision                  : 4.1
Memory Model                   : Paged
MCI Max Speed                  : 1000 kHz
Active Firmware Revision       : 61.20
Inactive Firmware Revision     : 61.20
Hardware Revision              : 1.2
Media Type                     : Optical SMF
Max SMF Link Length            : 630.0 Kilometer
Wavelength Nominal             : 1547.70 nm
Wavelength Tolerance           : 166.55 nm
```

Port Breakout Configuration

Use this command to configure the port breakout on the QSFP-DD module.

R1

The following table outlines the configuration steps for port breakout.

`OcNOS#configure terminal`	Enter Configuration mode.
`OcNOS(config)# qsfp-dd 49`	Enter the QSFP-DD mode.
`OcNOS(config-qsfp-dd)#application 3`	Configure the required application number. The supported range is from <2 to 15>.
`OcNOS(config-qsfp-dd)#commit`	Commit the configuration.
`OcNOS(config-qsfp-dd)#exit`	Exit from the QSFP-DD configuration mode.
`OcNOS(config)#port cd49 breakout 4X100g`	Enable port breakout
`OcNOS(config)# commit`	Commit the configuration.

Validation

Use this command to validate the port breakout configuration.

```
OcNOS#show qsfp-dd 49 application

Port Number                    : 49
-----------------------------------
   User Config    |   H/W Config
-----------------------------------
   Application 3  |   Application 3

OcNOS#show qsfp-dd 49 advertisement applications

Port Number                   : 49
> Application 1:
    | Host |
         Interface            : 400GAUI-8 C2M
         Application BR       : 425.00
         Lane Count           : 8
         Lane Sig BR          : 26.5625
         Modulation Format    : PAM4
         Bits Per Unit Intvl  : 2.000000
         Lane Assigned        : Lane-1
    | Media |
         Interface            : 400ZR, DWDM, Amplified
         Application BR       : 478.75
         Lane Count           : 1
         Lane Sig BR          : 59.84375
         Modulation Format    : DP-16QAM
         Bits Per Unit Intvl  : 8.000000
         Lane Assigned        : Lane-1
  Application 2:
    | Host |
         Interface            : 400GAUI-8 C2M
         Application BR       : 425.00
```

```
        Lane Count           : 8
        Lane Sig BR          : 26.5625
        Modulation Format    : PAM4
        Bits Per Unit Intvl  : 2.000000
        Lane Assigned        : Lane-1
    | Media |
        Interface            : 400ZR, Single Wavelen., Unamp.
        Application BR       : 478.75
        Lane Count           : 1
        Lane Sig BR          : 59.84375
        Modulation Format    : DP-16QAM
        Bits Per Unit Intvl  : 8.000000
        Lane Assigned        : Lane-1
Application 3:
    | Host |
        Interface            : 100GAUI-2 C2M
        Application BR       : 106.25
        Lane Count           : 2
        Lane Sig BR          : 26.5625
        Modulation Format    : PAM4
        Bits Per Unit Intvl  : 2.000000
        Lane Assigned        : Lane-7/Lane-5/Lane-3/Lane-1
    | Media |
        Interface            : 400ZR, DWDM, Amplified
        Application BR       : 478.75
        Lane Count           : 1
        Lane Sig BR          : 59.84375
        Modulation Format    : DP-16QAM
        Bits Per Unit Intvl  : 8.000000
        Lane Assigned        : Lane-1
Application 4:
    | Host |
        Interface            : 400GAUI-8 C2M
        Application BR       : 425.00
        Lane Count           : 8
        Lane Sig BR          : 26.5625
        Modulation Format    : PAM4
        Bits Per Unit Intvl  : 2.000000
        Lane Assigned        : Lane-1
    | Media |
        Interface            : ZR400-OFEC-16QAM
        Application BR       : 481.108374
        Lane Count           : 1
        Lane Sig BR          : 60.1385468
        Modulation Format    : DP-16QAM
        Bits Per Unit Intvl  : 8.000000
```

```
       Lane Assigned        : Lane-1
Application 5:
  | Host |
       Interface            : 100GAUI-2 C2M
       Application BR       : 106.25
       Lane Count           : 2
       Lane Sig BR          : 26.5625
       Modulation Format    : PAM4
       Bits Per Unit Intvl  : 2.000000
       Lane Assigned        : Lane-7/Lane-5/Lane-3/Lane-1
  | Media |
       Interface            : ZR400-OFEC-16QAM
       Application BR       : 481.108374
       Lane Count           : 1
       Lane Sig BR          : 60.1385468
       Modulation Format    : DP-16QAM
       Bits Per Unit Intvl  : 8.000000
       Lane Assigned        : Lane-1
Application 6:
  | Host |
       Interface            : 100GAUI-2 C2M
       Application BR       : 106.25
       Lane Count           : 2
       Lane Sig BR          : 26.5625
       Modulation Format    : PAM4
       Bits Per Unit Intvl  : 2.000000
       Lane Assigned        : Lane-7/Lane-5/Lane-3/Lane-1
  | Media |
       Interface            : ZR300-OFEC-8QAM
       Application BR       : 360.831281
       Lane Count           : 1
       Lane Sig BR          : 60.1385468
       Modulation Format    : DP-8QAM
       Bits Per Unit Intvl  : 6.000000
       Lane Assigned        : Lane-1
Application 7:
  | Host |
       Interface            : 100GAUI-2 C2M
       Application BR       : 106.25
       Lane Count           : 2
       Lane Sig BR          : 26.5625
       Modulation Format    : PAM4
       Bits Per Unit Intvl  : 2.000000
       Lane Assigned        : Lane-7/Lane-5/Lane-3/Lane-1
  | Media |
       Interface            : ZR200-OFEC-QPSK
```

```
        Application BR       : 240.554187
        Lane Count           : 1
        Lane Sig BR          : 60.1385468
        Modulation Format    : DP-QPSK
        Bits Per Unit Intvl  : 4.000000
        Lane Assigned        : Lane-1
  Application 8:
    | Host |
        Interface            : 100GAUI-2 C2M
        Application BR       : 106.25
        Lane Count           : 2
        Lane Sig BR          : 26.5625
        Modulation Format    : PAM4
        Bits Per Unit Intvl  : 2.000000
        Lane Assigned        : Lane-7/Lane-5/Lane-3/Lane-1
    | Media |
        Interface            : ZR100-OFEC-QPSK
        Application BR       : 120.277094
        Lane Count           : 1
        Lane Sig BR          : 30.069273
        Modulation Format    : DP-QPSK
        Bits Per Unit Intvl  : 4.000000
        Lane Assigned        : Lane-1
```

Port Breakout Interfaces

Use this command to configure the to see the interfaces after the port breakout.

```
ROUTER1#show interface brief | include cd49
cd49/1        ETH           --    routed           up      none    100g  --       No  No
cd49/2        ETH           --    routed           up      none    100g  --       No  No
cd49/3        ETH           --    routed           up      none    100g  --       No  No
cd49/4        ETH           --    routed           up      none    100g  --       No  No
```

Port Breakout Unconfiguration

Use this command to unconfigure the port breakout on the QSFP-DD module.

R1

The following table outlines the configuration steps for port breakout.

`OcNOS#configure terminal`	Enter Configuration mode.
`OcNOS(config)# qsfp-dd 49`	Enter the QSFP-DD mode.

`OcNOS(config-qsfp-dd)#no application`	Remove the application.
`OcNOS(config-qsfp-dd)#commit`	Commit the configuration.
`OcNOS(config-qsfp-dd)#exit`	Exit from the QSFP-DD configuration mode.
`OcNOS(config)#no port cd49 breakout`	Remove the port breakout. Your port will revert to functioning as a 400G port.
`OcNOS(config)# commit`	Commit the configuration.

```
OcNOS#show qsfp-dd 49 application

Port Number                    : 49
-----------------------------------
   User Config    |   H/W Config
-----------------------------------
   Application 1  |   Application 1

ROUTER1#show interface brief | include cd49
cd49        ETH           --    routed            up      none    400g  --       No  No
```

Port Breakout Configuration with serdes 25g

Use this command to configure the port breakout on the QSFP-DD module.

R1

The following table outlines the configuration steps for port breakout.

`OcNOS#configure terminal`	Enter Configuration mode.
`OcNOS(config)# qsfp-dd 49`	Enter the QSFP-DD mode.
`OcNOS(config-qsfp-dd)#application 12`	Configure the required application number. The accepted range is from 2 to 15.
`OcNOS(config-qsfp-dd)#commit`	Commit the configuration.
`OcNOS(config-qsfp-dd)#exit`	Exit from the QSFP-DD configuration mode.
`OcNOS(config)#port cd49 breakout 2X100g serdes 25g`	Configure port breakout with 25G Serdes.
`OcNOS(config)# commit`	Commit the configuration.

Validation

Use this command to validate the port breakout configuration.

```
OcNOS#show qsfp-dd 49 application

Port Number                    : 49
-----------------------------------
   User Config    |   H/W Config
```

```
-----------------------------------
   Application 12  |   Application 12
```

Port Breakout Interfaces

Use this command to configure the to see the interfaces after the port breakout.

```
ROUTER1#show interface brief | include cd49
cd49/1        ETH           --    routed           up      none    100g  --       No  No
cd49/2        ETH           --    routed           up      none    100g  --       No  No
```

Port Breakout Unconfiguration with serdes 25g

Use this command to unconfigure the port breakout on the QSFP-DD module.

R1

The following table outlines the configuration steps for port breakout.

`OcNOS#configure terminal`	Enter Configuration mode.
`OcNOS(config)# qsfp-dd 49`	Enter the QSFP-DD mode.
`OcNOS(config-qsfp-dd)#no application`	Remove the application
`OcNOS(config-qsfp-dd)#commit`	Commit the configuration.
`OcNOS(config-qsfp-dd)#exit`	Exit from the QSFP-DD configuration mode.
`OcNOS(config)#no port cd49 breakout`	Remove the port breakout. Your port will revert to functioning as a 400G port.
`OcNOS(config)# commit`	Commit the configuration.

```
OcNOS#show qsfp-dd 49 application

Port Number                    : 49
-----------------------------------
   User Config    |   H/W Config
-----------------------------------
   Application 1  |   Application 1

ROUTER1#show interface brief | include cd49
cd49        ETH           --    routed           up      none    400g  --       No  No
```

Support IGMP Snooping for Provider Bridge

Overview

In Layer-2 switches, multicast IP traffic is handled in the same manner as broadcast traffic and forwards frames received on one interface to all other interfaces. This creates excessive traffic on the network, and affects network performance. The Internet Group Management Protocol (IGMP) Snooping allows switches to monitor network traffic, and determine hosts to receive multicast traffic. Thus, at a time only an host's membership report is relayed from a group instead of a report from each host in the group.

A Provider Bridge (PB) network is a virtual bridge Local Area Network (LAN) that comprises of Service provider bridges (SVLAN and PB) and attached LANs controlled under a single service provider administration. Provider bridges interconnect the MACs of the IEEE 802 LANs separately. This combined provider bridged network relay frames to all the connected LANs that provide customer interfaces for each service instance.

Feature Characteristics

The existing IGMP Snooping extended to support in the Provider Bridged (PB) network. The PB connects customer LANs using the switched provider network consisting of SVLAN bridges and provider edge bridges. Each customer LAN is connected to a separate service VLAN inside the provider network. Current release supports the IGMPv1/ IGMPv2/IGMPv3.

The following are supported:

- Snooping entries are captured in provider bridge network
- Egress traffic from router is tagged with single SVLAN ID
- IGMP snooping feature supported only in SVLAN

Benefits

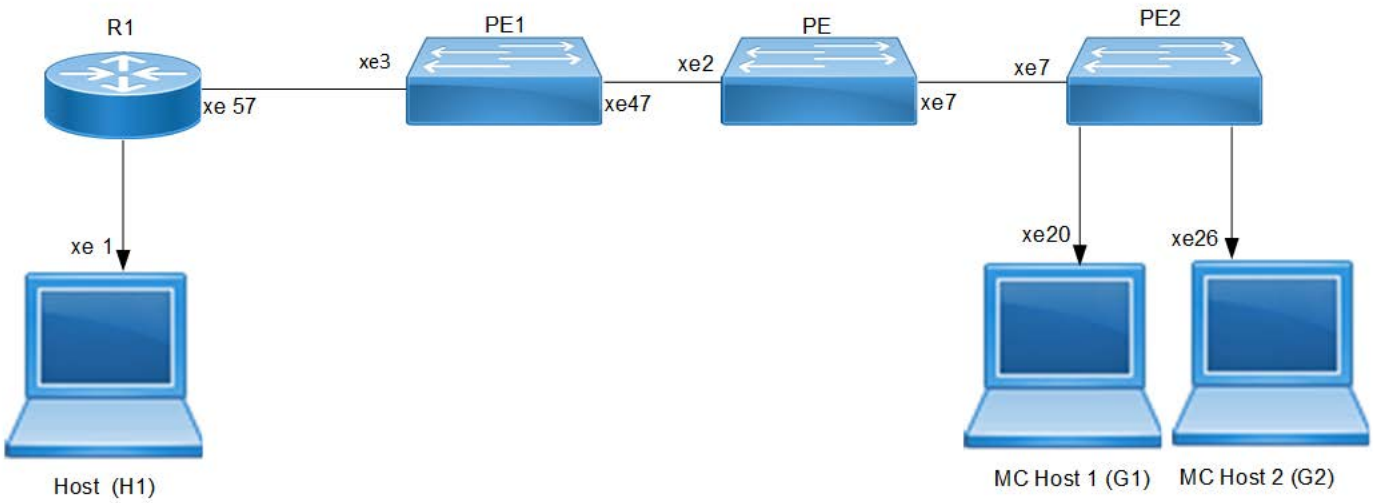
This feature enables a Provider bridging network service provider to conserve bandwidth by efficiently switching the multicast packets.

Prerequisites

IGMP snooping is available over a number of network underlays. In this chapter, it is assumed that Provider Bridge support is configured.

Configuration

Topology



IGMP Snooping Provider Bridge Topology

R1

`#configure terminal`	Enter the configure mode.
`R1(config)#bridge 1 protocol provider-rstp edge`	Configure bridge `1` to the spanning-tree table.
`R1(config)#vlan database`	Configure the VLAN database.
`R1(config)#vlan 2 type service point-point bridge 1 state enable`	Configure the SVLAN 2 to bridge 1.
`R1(config)#ip multicast-routing`	Configure the multicast routing on the router.
`R1(config)#ip pim rp-address 1.1.1.1`	Configure Rendezvous Point (RP) address for multicast groups.
`R1(config)#interface lo`	Enter into lo interface.
`R1(config-if)#ip address 1.1.1.1/24 secondary`	Configure rp address as secondary.
`R1(config-if)#ip pim sparse-mode`	Enable the PIM sparse mode.
`R1(config-if)#exit`	Exit the loopback interface mode.
`R1(config)#interface svlan1.2`	Create the SVLAN interface.
`R1(config-if)#ip address 20.1.1.1/24`	Configure IPv4 address to VLAN interface.
`R1(config-if)#ip pim sparse-mode`	Configure PIM sparse mode.
`R1(config-if)#exit`	Exit the SVLAN interface mode.
`R1(config)#interface xe1`	Enter interface mode.
`R1(config-if)#ip address 10.1.1.1/24`	Configure IPv4 address to interface
`R1(config-if)#ip pim sparse-mode`	Configure PIM sparse mode.
`R1(config-if)#commit`	Commit the configurations.
`R1(config-if)#exit`	Exit the interface mode.
`R1(config)#interface xe57`	Enter interface mode.
`R1(config-if)#switchport`	Configure switchport.
`R1(config-if)#dot1ad ethertype 0x8100`	Configure ether type 0x8100.
`R1(config-if)#bridge-group 1 spanning-tree disable`	Configure bridge group.
`R1(config-if)#switchport mode provider-network`	Configure switchport trunk mode.
`R1(config-if)#switchport provider-network allowed vlan add 2`	Configure the VLAN to switchport trunk mode.
`R1(config-if)#commit`	Commit configurations

PE1

`#configure terminal`	Enter the configure mode.
`PE1(config)#bridge 1 protocol provider-rstp edge`	Configure bridge `1` to the spanning-tree table.

`PE1(config)#vlan database`	Configure the VLAN database.
`PE1(config)#vlan 2 type service point-point bridge 1 state enable`	Configure the SVLAN 2 to bridge 1.
`PE1(config)#ip multicast-routing`	Configure the multicast routing on the router.
`PE1(config)#interface svlan1.2`	Create VLAN interface.
`PE1(config-if)#igmp snooping enable`	Configure IPv4 address to VLAN interface .
`PE1PE1(config-if)#exit`	Exit the interface mode.
`PE1(config)#interface xe3`	Enter interface mode.
`PE1(config-if)#switchport`	Configure Switchport.
`PE1(config-if)#dot1ad ethertype 0x8100`	Configure ethertype.
`PE1(config-if)#bridge-group 1 spanning-tree disable`	Configure bridge group spanning tree disable .
`PE1(config-if)#switchport mode provider-network`	Configure provider network .
`PE1(config-if)#switchport provider-network allowed vlan add 2`	Configure the SVLAN to interface .
`PE1(config-if)#commit`	Commit configurations.
`PE1(config-if)#exit`	Exit the interface mode.
`PE1(config)#interface xe47`	Enter interface mode.
`PE1(config-if)#switchport`	Configure switchport
`PE1(config-if)#dot1ad ethertype 0x8100`	Configure ethertype.
`PE1(config-if)#bridge-group 1 spanning-tree disable`	Configure bridge group spanning tree disable.
`PE1(config-if)#switchport mode provider-network`	Configure provider network.
`PE1(config-if)#switchport provider-network allowed vlan add 2`	Configure service vlan to provider network.
`PE1(config-if)#commit`	Commit configurations.
`PE1(config-if)#exit`	Exit the interface mode.

PE

`#configure terminal`	Enter the configure mode.
`PE(config)#bridge 1 protocol provider-rstp edge`	Configure bridge `1` to the spanning-tree table.
`PE(config)#vlan database`	Configure the VLAN database
`PE(config)#vlan 2 type service point-point bridge 1 state enable`	Configure the SVLAN 2 to bridge 1.
`PE(config)#ip multicast-routing`	Configure the multicast routing on the router.
`PE(config)#interface svlan1.2`	Create VLAN interface.
`PE(config-if)#igmp snooping enable`	Configure IPv4 address to VLAN interface.
`PE(config-if)#exit`	Exit the interface mode.
`PE(config)#interface xe2`	Enter interface mode.
`PE(config-if)#switchport`	Configure Switchport
`PE(config-if)#dot1ad ethertype 0x8100`	Configure ethertype
`PE(config-if)#bridge-group 1 spanning-tree disable`	Configure bridge group spanning tree disable.
`PE(config-if)#switchport mode provider-network`	Configure provider network.
`PE(config-if)#switchport provider-network allowed vlan add 2`	Configure the SVLAN to interface.
`PE(config-if)#commit`	Commit configurations.
`PE(config-if)#exit`	Exit the interface mode.
`PE(config)#interface xe7`	Enter interface mode.
`PE(config-if)#switchport`	Configure switchport.
`PE(config-if)#dot1ad ethertype 0x8100`	Configure ethertype.
`PE(config-if)#bridge-group 1 spanning-tree disable`	Configure bridge group spanning tree disable.
`PE(config-if)#switchport mode provider-network`	Configure provider network.
`PE(config-if)#switchport provider-network allowed vlan add 2`	Configure service vlan to provider network.
`PE(config-if)#commit`	Commit configurations.
`PE(config-if)#exit`	Exit the interface mode.

PE2

`#configure terminal`	Enter the configure mode.
`PE2(config)#bridge 1 protocol provider-rstp edge`	Configure bridge `1` to the spanning-tree table.
`PE2(config)#vlan database`	Configure the VLAN database.
`PE2(config)#vlan 2 type service point-point bridge 1 state enable`	Configure the SVLAN 2 to bridge 1.
`PE2(config)#ip multicast-routing`	Configure the multicast routing on the router.
`PE2(config)#interface svlan1.2`	Create VLAN interface.
`PE2(config-if)#igmp snooping enable`	Enable the IGMP snooping on VLAN interface.
`PE2(config-if)#exit`	Exit the VLAN interface mode.
`PE2(config)#interface xe7`	Enter interface mode.
`PE2(config-if)#switchport`	Configure Switchport.
`PE2(config-if)#dot1ad ethertype 0x8100`	Configure ethertype.
`PE2(config-if)#bridge-group 1 spanning-tree disable`	Configure bridge group spanning tree disable.
`PE2(config-if)#switchport mode provider-network`	Configure provider network.
`PE2(config-if)#switchport provider-network allowed vlan add 2`	Configure the SVLAN to interface.
`PE2(config-if)#commit`	Commit configurations.
`PE2(config-if)#exit`	Exit the interface mode.
`PE2(config)#interface xe20`	Enter interface mode.
`PE2(config-if)#switchport`	Configure switchport.
`PE2(config-if)#dot1ad ethertype 0x8100`	Configure ethertype.
`PE2(config-if)#bridge-group 1 spanning-tree disable`	Configure bridge group spanning tree disable.
`PE2(config-if)#switchport mode provider-network`	Configure provider network.
`PE2(config-if)#switchport provider-network allowed vlan add 2`	Configure service VLAN to provider network.
`PE2(config-if)#commit`	Commit configurations.
`PE2(config-if)#exit`	Exit the interface mode.
`PE2(config)#interface xe22`	Enter interface mode.
`PE2(config-if)#switchport`	Configure switchport.
`PE2(config-if)#dot1ad ethertype 0x8100`	Configure ethertype.
`PE2(config-if)#bridge-group 1 spanning-tree disable`	Configure bridge group spanning tree disable.

`PE2(config-if)#switchport mode provider-network`	Configure provider network.
`PE2(config-if)#switchport provider-network allowed vlan add 2`	Configure service VLAN to provider network.
`PE2(config-if)#commit`	Commit configurations.
`PE2(config-if)#exit`	Exit the interface mode.

Validation

R1

```
MCRTR#show ip igmp groups
IGMP Instance wide G-Recs Count is: 2
IGMP Connected Group Membership
Group Address    Interface            Uptime     Expires   State    Last Reporter
231.1.1.1        svlan1.2             00:00:12   00:04:07  Active   0.0.0.0
231.1.1.2        svlan1.2             00:00:12   00:04:07  Active   0.0.0.0
MCRTR#
MCRTR#show ip pim mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
G/prefix Entries: 0
(*,G) Entries: 2
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 0

(*, 231.1.1.1)
RP: 1.1.1.1
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
 Local     ..i.............................
 Joined    ................................
 Asserted  ................................
FCR:

(*, 231.1.1.2)
RP: 1.1.1.1
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
 Local     ..i.............................
 Joined    ................................
 Asserted  ................................
FCR:

MCRTR#
```

PE1

```
PEB1-7014#show igmp snooping interface
Global IGMP Snooping information
 IGMP Snooping Enabled
 IGMPv1/v2 Report suppression Enabled
 IGMPv3 Report suppression Enabled

IGMP Snooping information for svlan1.2
 IGMP Snooping enabled
 Snooping Querier none
 IGMP Snooping other querier timeout is 255 seconds
 Group Membership interval is 260 seconds
 IGMPv2 fast-leave is disabled
 IGMPv1/v2 Report suppression enabled
 IGMPv3 Report suppression enabled
 Router port detection using IGMP Queries
 Number of router-ports: 1
 Number of Groups: 0
 Number of v1-reports: 0
 Number of v2-reports: 0
 Number of v2-leaves: 0
 Number of v3-reports: 0
 Active Ports:
  xe3
  xe47
PEB1-7014#show igmp snooping groups
IGMP Instance wide G-Recs Count is: 2
IGMP Snooping Group Membership
Group source list: (R - Remote, S - Static, > - Hw Installed)
Vlan   Group/Source Address    Interface      Flags   Uptime      Expires  Last Reporter     Version
2      231.1.1.1              xe47           R    >  00:07:15    00:03:48 0.0.0.0           V3
2      231.1.1.2              xe47           R    >  00:07:15    00:03:48 0.0.0.0           V3
PEB1-7014#
```

PE

```
PB-7024#show igmp snooping interface
Global IGMP Snooping information
 IGMP Snooping Enabled
 IGMPv1/v2 Report suppression Enabled
 IGMPv3 Report suppression Enabled

IGMP Snooping information for svlan1.2
 IGMP Snooping enabled
 Snooping Querier none
 IGMP Snooping other querier timeout is 255 seconds
 Group Membership interval is 260 seconds
 IGMPv2 fast-leave is disabled
 IGMPv1/v2 Report suppression enabled
 IGMPv3 Report suppression enabled
```

```
 Router port detection using IGMP Queries
 Number of router-ports: 1
 Number of Groups: 0
 Number of v1-reports: 0
 Number of v2-reports: 0
 Number of v2-leaves: 0
 Number of v3-reports: 0
 Active Ports:
  xe7
  xe2
PB-7024#
PB-7024#show igmp snooping groups
IGMP Instance wide G-Recs Count is: 2
IGMP Snooping Group Membership
Group source list: (R - Remote, S - Static, > - Hw Installed)
Vlan   Group/Source Address    Interface     Flags   Uptime
Expires  Last Reporter     Version
2      231.1.1.1              xe7           R    >  00:07:15        00:03:45 20.1.1.2         V3
2      231.1.1.2              xe7           R    >  00:07:15        00:03:51 20.1.1.3         V3
PB-7024#
```

PE2

```
PEB2-7019#show igmp snooping interface
Global IGMP Snooping information
 IGMP Snooping Enabled
 IGMPv1/v2 Report suppression Disabled
 IGMPv3 Report suppression Disabled

IGMP Snooping information for svlan1.2
 IGMP Snooping enabled
 Snooping Querier none
 IGMP Snooping other querier timeout is 255 seconds
 Group Membership interval is 260 seconds
 IGMPv2 fast-leave is disabled
 IGMPv1/v2 Report suppression disabled
 IGMPv3 Report suppression disabled
 Router port detection using IGMP Queries
 Number of router-ports: 1
 Number of Groups: 0
 Number of v1-reports: 0
 Number of v2-reports: 0
 Number of v2-leaves: 0
 Number of v3-reports: 0
 Active Ports:
  xe20
  xe26
  xe7
    PEB2-7019#
    PEB2-7019#show igmp snooping groups
    IGMP Instance wide G-Recs Count is: 2
    IGMP Snooping Group Membership
```

```
    Group source list: (R - Remote, S - Static, > - Hw Installed)
Vlan  Group/Source Address   Interface    Flags  Uptime  Expires  Last Reporter   Version
2      231.1.1.1               xe20          R    >  00:07:14  00:03:45 20.1.1.2          V3
2      231.1.1.2               xe26          R    >  00:07:15  00:03:51 20.1.1.3       V3
PEB2-7019#
```

Abbreviations

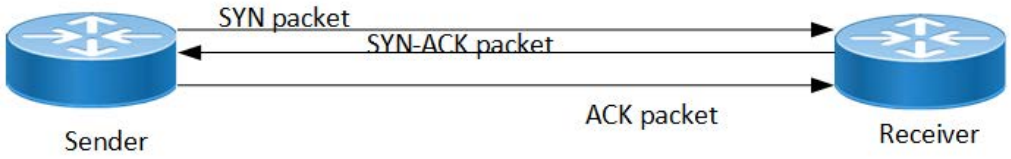
Acronym	Description
IGMP	Internet Group Management Protocol
PB	Provider Bridged
SVLAN	Service Provider VLAN

TCP MSS configuration for BGP neighbors

Overview

The manual configuration between the routing devices establishes the BGP peer that creates a TCP session.

This feature enables the configuration of TCP Maximum Segment Size (MSS) that defines the maximum segment size in a single TCP segment during a communication session. TCP segment is a unit of data transmitted in a TCP connection. TCP uses three-way handshake process for initial establishment of a TCP connection. In the three-way handshake process, the sending host sends a SYN packet. Once the receiving host receives the SYN packet, it acknowledges and sends back a SYN-ACK packet to the sending host. Once the sending host receives the SYN-ACK packet from the receiving host, it sends an ACK packet, establishing a reliable connection. In this three way handshake process, the MSS is negotiated between the BGP neighbors.



Three-way handshake

Feature Characteristics

The configuration of the TCP MSS for BGP neighbors helps the neighbors adjust the MSS value of the TCP SYN packet. Configure the TCP MSS through the CLI and NetConf interface. The configurable MSS range is offered from 40-1440 bytes. By default, the MTU value for ethernet cable is 1500 bytes. When configuring the highest MSS value that is 1440, the total MSS becomes 1440 bytes (MSS) plus 20 bytes (IP Header Size), 20 bytes (TCP Header), and Ethernet header which does not cross the default path MTU value.

TCP MSS for BGP neighbor

Benefits

By default, the interface MTU value determines the MSS value of a packet. When the interface MTU value exceeds the default ethernet path MTU value of 1500 bytes, the MSS value also crosses the default ethernet path MTU value, resulting in packet fragmentation. The configuration of the specific MSS value limits the packet size irrespective of the interface MTU value, preventing packet fragmentation.

Prerequisites

Requires the knowledge on TCP handshake and BGP neighbor discovery.

Configuration

This section shows the procedure to configure TCP MSS between BGP peers.

Topology

The below example shows the configuration required to enable BGP on an interface. PE1 and RR1 are routers belonging to the same Autonomous System (AS) with the Autonomous System Number (ASN) as AS100, connecting to network 10.1.1.0/24. First, define the routing process and the ASN to which the routers belong. Then, define BGP neighbors to start exchanging routing updates and configure the TCP MSS for BGP between PE1 and RR1 devices.

Device topology for BGP

Configuration

The configuration shows how to configure the TCP MSS value for the BGP peer.

PE1

`PE1#configure terminal`	Enter Configuration mode.
`PE1(config)#interface lo`	Enter interface mode for loopback.
`PE1(config-if)#ip address 1.1.1.1/32 secondary`	Specify the interface IP address `1.1.1.1`.
`PE1(config-if)#exit`	Exit the interface mode.
`PE1(config)#interface xe1`	Enter interface mode for `xe1`.
`PE1(config-if)#ip address 10.1.1.1/24`	Specify the IP address `10.1.1.1` for the interface.
`PE1(config-if)#exit`	Exit interface mode for `xe1`.
`PE1(config)#router bgp 100`	Define the routing process. The number 100 specifies the ASN of PE1.
`PE1(config-router)#bgp router-id 1.1.1.1`	Configure bgp router-id same as loopback IP address`1.1.1.1`.
`PE1(config-router)#neighbor 10.1.1.2 remoteas 100`	Define BGP neighbors, and establish a TCP session. `10.1.1.2` is the IP address of the neighbor and 100 is the neighbor's ASN.

`PE1(config-router)#neighbor 10.1.1.2 tcp-mss 800`	Configure TCP MSS value.
`PE1(config-router)#address-family ipv4 unicast`	Enter address-family IPv4 unicast mode.
`PE1(config-router-af)#neighbor 10.1.1.2 activate`	Activate neighbor with IP address `10.1.1.2` in the IPv4 address family.
`PE1(config-router-af)#redistribute connected`	Redistributing connected routes inside BGP.
`PE1(config-router-af)#exit-address-family`	Exit address-family mode.
`PE1(config-router)#commit`	Commit the candidate configuration to the running configuration.

RR1

`RR1#configure terminal`	Enter configuration mode.
`RR1(config)#interface lo`	Enter interface mode for loopback.
`RR1(config-if)#ip address 2.2.2.2/32 secondary`	Specify the interface address `2.2.2.2`.
`RR1(config-if)#exit`	Exit interface mode.
`RR1(config)#interface xe47`	Enter interface mode for `xe47`.
`RR1(config-if)#ip address 10.1.1.2/24`	Specify IP address `10.1.1.2/24` for the interface.
`RR1(config-if)#exit`	Exit interface mode for `xe47`.
`RR1(config)#router bgp 100`	Define the routing process. The number 100 specifies the ASN of RR1.
`RR1(config-router)#bgp router-id 2.2.2.2`	Configure BGP router-id same as loopback IP address `2.2.2.2`.
`RR1(config-router)#neighbor 10.1.1.1 remoteas 100`	Define BGP neighbors, and establish a TCP session. `10.1.1.1` is the ip address of the neighbor and 100 is the neighbor's ASN.
`RR1(config-router)#neighbor 10.1.1.1 passive`	Configure BGP neighbor `10.1.1.1` passive.
`RR1(config-router)#address-family ipv4 unicast`	Enter address-family IPv4 unicast mode
`RR1(config-router-af)#neighbor 10.1.1.1 activate`	Activate the neighbor in the IPv4 address family.
`RR1(config-router-af)#neighbor 10.1.1.1 route-reflector-client`	Configure RR1 as the Route-Reflector (RR) and neighbor PE1 as its client.
`RR1(config-router-af)#redistribute connected`	Redistributing connected routes inside BGP.
`RR1(config-router-af)#exit-address-family`	Exit address-family mode.
`RR1(config-router)#commit`	Commit the candidate configuration to the running configuration.

Validation

PE1

```
PE1#show bgp summary
```

```
BGP router identifier 1.1.1.1, 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/Dow
n   State/PfxRcd
10.1.1.2                 4   100  171        170       1      0      0  00:00:11
               0

Total number of neighbors 1

Total number of Established sessions 1
PE1#

PE1#sh bgp neighbors
BGP neighbor is 10.1.1.2, remote AS 100, local AS 100, internal link, peer index
: 2
  BGP version 4, local router ID 10.1.1.1, remote router ID 10.1.1.2
  BGP state = Established, up for 00:07:29
  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 IPv4 Unicast: advertised and received
  Received 43 messages, 1 notifications, 0 in queue
  Sent 46 messages, 4 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds

For address family: IPv4 Unicast  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  AIGP is enabled
  Community attribute sent to this neighbor (both)
  Large Community attribute sent to this neighbor
  0 accepted prefixes
  0 announced prefixes

 Connections established 6; dropped 5
Local host: 10.1.1.1, Local port: 34738
Foreign host: 10.1.1.2, Foreign port: 179
TCP MSS: (800), Advertise TCP MSS: (800), Send TCP MSS: (800),  Receive TCP MSS:
 (536)
Sock FD : (25)
Nexthop: 10.1.1.1
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:08:45, due to Administratively Reset (Cease Notification sent)
```

RR1

```
RR1#show bgp 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/Dow
n   State/PfxRcd
10.1.1.1                 4   100    2          3       1      0      0  00:00:26
               0

Total number of neighbors 1

Total number of Established sessions 1

RR1#sh bgp neighbors
BGP neighbor is 10.1.1.1, remote AS 100, local AS 100, internal link, peer index
: 2
  BGP version 4, local router ID 10.1.1.2, remote router ID 10.1.1.1
  BGP state = Established, up for 00:08:31
  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 IPv4 Unicast: advertised and received
  Received 46 messages, 4 notifications, 0 in queue
  Sent 47 messages, 1 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds

For address family: IPv4 Unicast  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  AIGP is enabled
  Community attribute sent to this neighbor (both)
  Large Community attribute sent to this neighbor
  0 accepted prefixes
  0 announced prefixes

 Connections established 6; dropped 5
Local host: 10.1.1.2, Local port: 179
Foreign host: 10.1.1.1, Foreign port: 34738
TCP MSS: (0), Advertise TCP MSS: (1460), Send TCP MSS: (800),  Receive TCP MSS:
(536)
Sock FD : (22)
Nexthop: 10.1.1.2
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:09:52, due to BGP Notification received
```

New CLI Commands

neighbor tcp-mss

Use this command to set the BGP TCP MSS of a neighbor.

Use the `no` parameter with this command to remove a TCP MSS setting from a BGP neighbor.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) tcp-mss <40-1440>
no neighbor (A.B.C.D|X:X::X:X|WORD) tcp-mss
```

For BGP unnumbered mode:

```
neighbor WORD tcp-mss <40-1440>
no neighbor WORD tcp-mss
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the *neighbor WORD peer-group range* command. When you specify this parameter, the command applies to all peers in the group.
`<40-1440>`	Configure TCP MSS

Default

By default, `neighbor tcp-mss` is disabled.

Command Mode

Router mode, address family-vrf mode and BGP unnumbered mode.

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.72 tcp-mss 1000
(config)#router bgp 100
(config-router)#address-family ipv6 vrf VRF_A
(config-router-af)#neighbor 3ffe:15:15:15:15::0 tcp-mss 900
```

For unnumbered peer below configuration is given in BGP unnumbered-mode.

```
(config)#router bgp 100
(config-router)#bgp unnumbered-mode
(config-router-unnum)#neighbor eth1 tcp-mss 800
```

Abbreviations

The following are some key abbreviations and their meanings relevant to this document:

Acronym	Description
ACK	Acknowledgment
BGP	Border Gateway Protocol
TCP	Transmission Control Protocol
MSS	Maximum Segment Size
MTU	Maximum Transmission Unit
SYN	Synchronize

Glossary

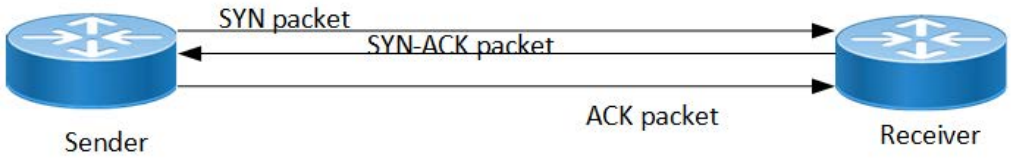
The following provides definitions for key terms used throughout this document.

BGP	BGP is an exterior gateway protocol to exchange route information and interconnect various networks on the global internet.
BGP neighbor	BGP neighbors, called peers, are established by manual configuration among routers to create a TCP session on port 179, which exchanges routing information between two systems, defined by their Autonomous System Numbers (ASNs).
MSS	MSS is a TCP parameter that defines the maximum amount of data in a TCP segment that can be transmitted. TCP - TCP is one of the main protocols in the Internet Protocol (IP) suite. It offers a secure and reliable connection between two devices.
TCP	TCP is one of the main protocols in the Internet Protocol (IP) suite. It offers a secure and reliable connection between two devices.
TCP segment	TCP segment is a unit of data transmitted in a TCP connection. The segment consists of header and payload. The header contains the control information to manage the transmission, and the payload contains the actual data that needs to be transmitted.

TCP MSS configuration for LDP sessions

Overview

Label Distribution Protocol (LDP) uses Transmission Control Protocol (TCP) to establish sessions between the devices. This feature enables the configuration of TCP Maximum Segment Size (MSS) that defines the maximum segment size in a single TCP segment during a communication session.TCP segment is a unit of data transmitted in a TCP connection. TCP uses three-way handshake process for initial establishment of a TCP connection. In the three-way handshake process, the sending host sends a SYN packet. Once the receiving host receives the SYN packet, it acknowledges and sends back a SYN-ACK packet to the sending host. Once the sending host receives the SYN-ACK packet from the receiving host, it sends an ACK packet, establishing a reliable connection. In this three way handshake process, the MSS is negotiated between the LDP neighbors.



Three-way handshake

Feature Characteristics

The configuration of the TCP MSS for LDP neighbors helps the neighbors adjust the MSS value of the TCP SYN packet. Configure the TCP MSS through the CLI and NetConf interface. The configurable MSS range is offered from 560 to 1440. By default, the MTU value for ethernet cable is 1500 bytes. When configuring the highest MSS value that is 1440, the total MSS becomes 1440 bytes (MSS) plus 20 bytes (IP Header Size), 20 bytes (TCP Header), and Ethernet header which does not cross the default path MTU value.

Note: After configuring TCP MSS, use *clear ldp session* command to apply the MSS for the operational session.

Configuring TCP MSS

Benefits

By default, the interface MTU value determines the MSS value of an LDP packet. When the interface MTU value exceeds the default ethernet path MTU value of 1500 bytes, the MSS value also crosses the default ethernet path MTU

value, resulting in packet fragmentation. The configuration of the specific MSS value limits the packet size irrespective of the interface MTU value, preventing packet fragmentation.[

Prerequisites

Requires the knowledge on TCP handshake and the formation of LDP neighbors.

Configuration

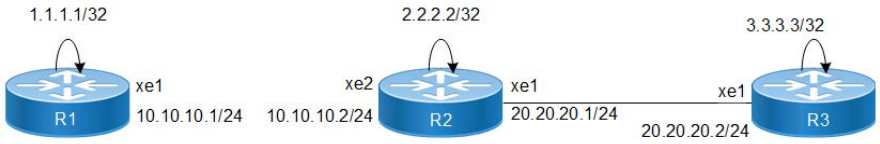
This section shows the procedure to configure TCP MSS for LDP session.

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 Internal Gateway Protocol (IGP), for example, Open Shortest Path first (OSPF), to distribute reachability information within the MPLS cloud.
4. Configuring the transport address.
5. Configure the TCP MSS neighbor on peer node (Active node).

Topology



Device topology for TCP MSS for LDP

Configuration

The below configuration shows how to configure the TCP MSS value for the LDP neighbors.

R1 - NSM

`R1#configure terminal`	Enter configure mode.
`R1(config)#interface xe1`	Specify the interface `xe1` to be configured.
`R1(config-if)#ip address 10.10.10.1/24`	Assign IP address `10.10.10.1/24` to interface.
`R1(config-if)#label-switching`	Enable label switching on interface `xe1`.
`R1(config-if)#exit`	Exit interface mode.

`R1(config)#interface lo`	Specify the loopback interface to be configured.
`R1(config-if)#ip address 1.1.1.1/32 secondary`	Set the IP address of the loopback interface to `1.1.1.1/32`.
`R1(config-if)#commit`	Commit the transaction.

R1 - LDP

`R1(config)#router ldp`	Enter Router mode for LDP.
`R1(config-router)#router-id 1.1.1.1`	Set the router ID to IP address `1.1.1.1`.
`R1(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.
`R1(config-router)#targeted-peer ipv4 3.3.3.3`	Configure targeted peer `3.3.3.3`.
`R1(config-router-targeted-peer)#exit`	Exit targeted peer-mode.
`R1(config-router)#exit`	Exit the router mode and return to the configure mode.
`R1(config)#interface xe1`	Enter interface mode `xe1`.
`R1(config-if)#enable-ldp ipv4`	Enable LDP on `xe1`.
`R1(config-if)#commit`	Commit the transaction.

R1 - OSPF

`R1(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.
`R1(config-router)#network 10.10.10.0/24 area 0`	Define the interface `10.10.10.0/24`,on which OSPF runs and associate the area ID `0` with the interface.
`R1(config-router)#network 1.1.1.1/32 area 0`	Define the interface `1.1.1.1/32`, on which OSPF runs and associate the area ID `0` with the interface.
`R1(config-router)#commit`	Commit the transaction.

R2 - NSM

`R2#configure terminal`	Enter configure mode.
`R2(config)#interface lo`	Specify the loopback interface to be configured.
`R2(config-if)#ip address 2.2.2.2/32 secondary`	Set the IP address of the loopback interface to `2.2.2.2/32`.
`R2(config-if)#exit`	Exit interface mode.
`R2(config)#interface xe1`	Specify the interface `xe1` to be configured.
`R2(config-if)#ip address 20.20.20.1/24`	Assign IP address `20.20.20.1/24` to interface.
`R2(config-if)#label-switching`	Enable label switching on interface `xe1`.
`R2(config-if)#exit`	Exit interface mode.
`R2(config)#interface xe2`	Specify the interface `xe2` to be configured.

`R2(config-if)#ip address 10.10.10.2/24`	Assign IP address `10.10.10.2/24` to interface.
`R2(config-if)#label-switching`	Enable label switching on interface `xe2`.
`R2(config-if)#commit`	Commit the transaction.

R2 - LDP

`R2(config)#router ldp`	Enter Router mode.
`R2(config-router)#router-id 2.2.2.2`	Set the router ID to IP address `2.2.2.2`.
`R2(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.
`R2(config-router)#neighbor 1.1.1.1 tcp-mss 600`	Configure the TCP MSS value on peer node which have active side only.
`R2(config-router)#exit`	Exit router mode and return to configure mode.
`R2(config)#interface xe1`	Specify the interface `xe1` to be configured.
`R2(config-if)#enable-ldp ipv4`	Enable LDP on a specified interface `xe1`.
`R2(config-if)#exit`	Exit interface mode.
`R2(config)#interface xe2`	Specify the interface `xe2` to be configured.
`R2(config-if)#enable-ldp ipv4`	Enable LDP on a specified interface `xe2`.
`R2(config-if)#commit`	Commit the transaction.

R2 - OSPF

`R2(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.
`R2(config-router)#network 10.10.10.0/24 area 0`	Define the interfaces `10.10.10.0/24`, on which OSPF runs and associate the area ID `0` with them.
`R2(config-router)#network 20.20.20.0/24 area 0`	Define the interfaces `20.20.20.0/24`, on which OSPF runs and associate the area ID `0` with them.
`R2(config-router)#network 2.2.2.2/32 area 0`	Define the interfaces `2.2.2.2/32`, on which OSPF runs and associate the area ID `0` with them.
`R2(config-router)#commit`	Commit the transaction.

R3 - NSM

`R3#configure terminal`	Enter configure mode.
`R3(config)#interface lo`	Specify the loopback interface to be configured.
`R3(config-if)#ip address 3.3.3.3/32 secondary`	Set the IP address of the loopback interface to `3.3.3.3/32`.
`R3(config-if)#exit`	Exit interface mode.
`R3(config)#interface xe1`	Specify the interface `xe1` to be configured.

`R3(config-if)#ip address 20.20.20.2/24`	Set the IP address of the interface to `20.20.20.2/24`.
`R3(config-if)#label-switching`	Enable label switching on interface `xe1`.
`R3(config-if)#commit`	Commit the transaction.

R3 - LDP

`R3(config)#router ldp`	Enter Router mode.
`R3(config-router)#router-id 3.3.3.3`	Set the router ID for IP address `3.3.3.3`.
`R3(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.
`R3(config-router)#neighbor 2.2.2.2 tcp-mss 650`	Configure the TCP MSS value on peer node which have active side only.
`R3(config-router)#targeted-peer ipv4 1.1.1.1`	Configure targeted peer.
`R3(config-router-targeted-peer)#exit`	Exit targeted peer-mode.
`R3(config-router)#exit`	Exit the router mode and return to the configure mode.
`R3(config)#interface xe1`	Enter interface mode `xe1`.
`R3(config-if)#enable-ldp ipv4`	Enable LDP on `xe1`.
`R3(config-if)#commit`	Commit the transaction.

R3 - OSPF

`R3(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.
`R3(config-router)#network 20.20.20.0/24 area 0`	Define the interfaces `20.20.20.0/24`, on which OSPF runs and associate the area ID `0` with them.
`R3(config-router)#network 3.3.3.3/32 area 0`	Define the interfaces `3.3.3.3/32`, on which OSPF runs and associate the area ID `0` with them.
`R3(config-router)#commit`	Commit the transaction.

Validation

R3

```
R3#show ldp session
Codes: m - MD5 password is not set/unset.
       g - GR configuration not set/unset.
       t - TCP MSS not set/unset.
       Session has to be cleared manually

Code  Peer IP Address      IF Name    My Role    State       KeepAlive  UpTime
       2.2.2.2            xe1        Active    OPERATIONAL   30    00:03:06
```

```
       1.1.1.1            xe1        Active    OPERATIONAL   30    00:03:06
R3#show ldp targeted-peer count
-----------------------------------------------
Num Targeted Peers: 1          [UP: 1]
-----------------------------------------------
PE2#show ldp session count
-----------------------------------------
 Multicast Peers      : 1          [UP: 1]
 Targeted Peers       : 1          [UP: 1]
 Total Sessions       : 2          [UP: 2]
-----------------------------------------
R3#show ldp routes
Prefix Addr         Nexthop Addr     Intf        Owner
1.1.1.1/32          20.20.20.1       xe1         ospf
2.2.2.2/32          20.20.20.1       xe1         ospf
3.3.3.3/32          0.0.0.0          lo          connected
10.10.10.0/24       20.20.20.1       xe1         ospf
20.20.20.0/24       0.0.0.0          xe1         connected
R3#show ldp fec-ipv4 count
------------------------
Num. IPv4 FEC(s): 5
------------------------
R3#show ldp session 2.2.2.2
Session state                 : OPERATIONAL
Session role                  : Active
TCP Connection                : Established
IP Address for TCP            : 2.2.2.2
Interface being used          : xe1
Peer LDP ID                   : 2.2.2.2:0
Preferred Peer LDP Password   : Not Set
Adjacencies                   : 20.20.20.1
Advertisement mode            : Downstream Unsolicited
Label retention mode          : Liberal
Graceful Restart              : Not Capable
Keepalive Timeout             : 30
Reconnect Interval            : 15
Configured TCP MSS            : 650
Applied TCP MSS               : 650
Preferred TCP MSS             : NA
Address List received         : 2.2.2.2
                                10.10.10.2
                                20.20.20.1
Received Labels :       Fec             Label           Maps To
                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
                IPV4:1.1.1.1/32         25600           none
Sent Labels :   Fec                     Label           Maps To
                IPV4:20.20.20.0/24      impl-null       none
                IPV4:3.3.3.3/32         impl-null       none
```

R2

```
R2#show ldp session
Codes: m - MD5 password is not set/unset.
       g - GR configuration not set/unset.
       t - TCP MSS not set/unset.
       Session has to be cleared manually
Code  Peer IP Address      IF Name    My Role    State      KeepAlive  UpTime
       3.3.3.3            xe1        Passive   OPERATIONAL   30    00:06:10
       1.1.1.1            xe2       Active    OPERATIONAL   30    00:06:10
R2#show ldp session count
-------------------------------------------
 Multicast Peers      : 2          [UP: 2]
 Targeted Peers       : 0          [UP: 0]
 Total Sessions       : 2          [UP: 2]
-------------------------------------------
R2#show ldp routes
Prefix Addr         Nexthop Addr     Intf        Owner
1.1.1.1/32          10.10.10.1       xe2        ospf
2.2.2.2/32          0.0.0.0          lo          connected
3.3.3.3/32          20.20.20.2       xe1         ospf
10.10.10.0/24       0.0.0.0          xe2        connected
20.20.20.0/24       0.0.0.0          xe1         connected

R2#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         : xe2
Peer LDP ID                  : 1.1.1.1:0
Preferred Peer LDP Password  : Not Set
Adjacencies                  : 10.10.10.1
Advertisement mode           : Downstream Unsolicited
Label retention mode         : Liberal
Graceful Restart             : Not Capable
Keepalive Timeout            : 30
Reconnect Interval           : 15
Configured TCP MSS           : 600
Applied TCP MSS              : 600
Preferred TCP MSS            : NA
Address List received        : 1.1.1.1
                               10.10.10.1
                               48.48.48.48
Received Labels :       Fec             Label           Maps To
                IPV4:10.10.10.0/24      impl-null       none
                IPV4:1.1.1.1/32         impl-null       25600
Sent Labels :   Fec                     Label           Maps To
                IPV4:20.20.20.0/24      impl-null       none
                IPV4:10.10.10.0/24      impl-null       none
```

```
               IPV4:3.3.3.3/32         25601           impl-null
               IPV4:2.2.2.2/32         impl-null       none
```

R1

```
R1#show ldp session
Codes: m - MD5 password is not set/unset.
       g - GR configuration not set/unset.
       t - TCP MSS not set/unset.
       Session has to be cleared manually

Code  Peer IP Address      IF Name    My Role    State      KeepAlive  UpTime
       2.2.2.2            xe1        Passive   OPERATIONAL   30    00:07:12
       3.3.3.3            xe1        Passive   OPERATIONAL   30    00:07:12
R1#show ldp session count
-------------------------------------------
 Multicast Peers      : 1          [UP: 1]
 Targeted Peers       : 1          [UP: 1]
 Total Sessions       : 2          [UP: 2]
-------------------------------------------
R1#show ldp targeted-peer count
-------------------------------------------------
Num Targeted Peers: 1          [UP: 1]
-------------------------------------------------
R1#show ldp routes
Prefix Addr         Nexthop Addr     Intf        Owner
1.1.1.1/32          0.0.0.0          lo          connected
2.2.2.2/32          10.10.10.2       xe1        ospf
3.3.3.3/32          10.10.10.2       xe1         ospf
10.10.10.0/24       0.0.0.0          xe1         connected
20.20.20.0/24       10.10.10.2       xe1         ospf
R1#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>     2.2.2.2             25601       No    10.10.10.2
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>     2.2.2.2             impl-null   No    10.10.10.2
48.48.48.48/32      E >     non-existent        none        No    connected
```

Configure TCP MSS on ALL neighbor

R1 - NSM

`R1#configure terminal`	Enter configure mode.
`R1(config)#interface xe1`	Specify the interface `xe1` to be configured.
`R1(config-if)#ip address 10.10.10.1/24`	Assign IP address `10.10.10.1/24` to interface.
`R1(config-if)#label-switching`	Enable label switching on interface `xe1`.
`R1(config-if)#exit`	Exit interface mode.
`R1(config)#interface lo`	Specify the loopback interface to be configured.
`R1(config-if)#ip address 1.1.1.1/32 secondary`	Set the IP address of the loopback interface to 1.1.1.1/32.
`R1(config-if)#commit`	Commit the transaction.

R1 - LDP

`R1(config)#router ldp`	Enter Router mode for LDP.
`R1(config-router)#router-id 1.1.1.1`	Set the router ID to IP address `1.1.1.1`.
`R1(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.
`R1(config-router)#targeted-peer ipv4 3.3.3.3`	Configure targeted peer.
`R1(config-router)#neighbor all tcp-mss 700`	Configure the TCP MSS value with `all` neighbor.
`R1(config-router-targeted-peer)#exit`	Exit-targeted-peer-mode.
`R1(config-router)#exit`	Exit the Router mode and return to the Configure mode.
`R1(config)#interface xe1`	Enter interface mode `xe1`.
`R1(config-if)#enable-ldp ipv4`	Enable LDP on `xe1`.
`R1(config-if)#commit`	Commit the transaction.

R1 - OSPF

`R1(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.
`R1(config-router)#network 10.10.10.0/24 area 0`	Define the interface `10.10.10.0/24`, on which OSPF runs and associate the area ID (0) with the interface.
`R1(config-router)#network 1.1.1.1/32 area 0`	Define the interface `1.1.1.1/32`, on which OSPF runs and associate the area ID (0) with the interface.
`R1(config-router)#commit`	Commit the transaction.

R2 - NSM

`R2#configure terminal`	Enter configure mode.
`R2(config)#interface lo`	Specify the loopback (lo) interface to be configured.
`R2(config-if)#ip address 2.2.2.2/32 secondary`	Set the IP address of the loopback interface to `2.2.2.2/32`.
`R2(config-if)#exit`	Exit interface mode.
`R2(config)#interface xe1`	Specify the interface `xe1` to be configured.
`R2(config-if)#ip address 20.20.20.1/24`	Assign IP address 20.20.20.1/24 to interface.
`R2(config-if)#label-switching`	Enable label switching on interface xe1.
`R2(config-if)#exit`	Exit interface mode.
`R2(config)#interface xe2`	Specify the interface `xe2` to be configured.
`R2(config-if)#ip address 10.10.10.2/24`	Assign IP address `10.10.10.2/24` to interface.
`R2(config-if)#label-switching`	Enable label switching on interface `xe2`.
`R2(config-if)#commit`	Commit the transaction.

R2 - LDP

`R2(config)#router ldp`	Enter Router mode.
`R2(config-router)#router-id 2.2.2.2`	Set the router ID to IP address `2.2.2.2`.
`R2(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.
`R2(config-router)#neighbor all tcp-mss 710`	Configure the TCP MSS value with `all` neighbor.
`R2(config-router)#exit`	Exit Router mode and return to configure mode.
`R2(config)#interface xe1`	Specify the interface `xe1` to be configured.
`R2(config-if)#enable-ldp ipv4`	Enable LDP on a specified interface `xe1`.
`R2(config-if)#exit`	Exit interface mode.
`R2(config)#interface xe2`	Specify the interface `xe2` to be configured.
`R2(config-if)#enable-ldp ipv4`	Enable LDP on a specified interface `xe2`.
`R2(config-if)#commit`	Commit the transaction.

R2 - OSPF

`R2(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.
`R2(config-router)#network 10.10.10.0/24 area 0`	Define the interfaces `10.10.10.0/24`, on which OSPF runs and associate the area ID (0) with them.
`R2(config-router)#network 20.20.20.0/24 area 0`	Define the interfaces `20.20.20.0/24`, on which OSPF runs and associate the area ID (0) with them.

`R2(config-router)#network 2.2.2.2/32 area 0`	Define the interfaces `2.2.2.2/32`, on which OSPF runs and associate the area ID (0) with them.
`R2(config-router)#commit`	Commit the transaction.

R3 - NSM

`R3#configure terminal`	Enter configure mode.
`R3(config)#interface lo`	Specify the loopback interface to be configured.
`R3(config-if)#ip address 3.3.3.3/32 secondary`	Set the IP address of the loopback interface to `3.3.3.3/32`.
`R3(config-if)#exit`	Exit interface mode.
`R3(config)#interface xe1`	Specify the interface `xe1` to be configured.
`R3(config-if)#ip address 20.20.20.2/24`	Set the IP address of the interface to `20.20.20.2/24`.
`R3(config-if)#label-switching`	Enable label switching on interface `xe1`.
`R3(config-if)#commit`	Commit the transaction.

R3 - LDP

`R3(config)#router ldp`	Enter Router mode.
`R3(config-router)#router-id 3.3.3.3`	Set the router ID for IP address `3.3.3.3`.
`R3(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.
`R3(config-router)#neighbor all tcp-mss 720`	Configure the TCP MSS value with `all` neighbor.
`R3(config-router)#targeted-peer ipv4 1.1.1.1`	Configure targeted peer.
`R3(config-router-targeted-peer)#exit`	Exit-targeted-peer-mode.
`R3(config-router)#exit`	Exit the Router mode and return to the Configure mode.
`R3(config)#interface xe1`	Enter interface mode.
`R3(config-if)#enable-ldp ipv4`	Enable LDP on `xe1`.
`R3(config-if)#commit`	Commit the transaction.

R3 - OSPF

`R3(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.
`R3(config-router)#network 20.20.20.0/24 area 0`	Define the interfaces `20.20.20.0/24`, on which OSPF runs and associate the area ID (0) with them.
`R3(config-router)#network 3.3.3.3/32 area 0`	Define the interfaces `3.3.3.3/32`, on which OSPF runs and associate the area ID (0) with them.
`R3(config-router)#commit`	Commit the transaction.

Validation

R1

```
R1#show ldp session
Codes: m - MD5 password is not set/unset.
       g - GR configuration not set/unset.
       t - TCP MSS not set/unset.
       Session has to be cleared manually
Code  Peer IP Address      IF Name    My Role    State      KeepAlive  UpTime
       2.2.2.2           xe1        Passive   OPERATIONAL   30    00:11:22
       3.3.3.3           xe1        Passive   OPERATIONAL   30    00:11:22
R1#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           : xe1
Peer LDP ID                    : 2.2.2.2:0
Preferred 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
Configured TCP MSS             : 700
Applied TCP MSS                : 700
Preferred TCP MSS              : NA
Address List received          : 2.2.2.2
                                 10.10.10.2
                                 20.20.20.1
Received Labels :       Fec              Label           Maps To
                 IPV4:20.20.20.0/24      impl-null       none
                 IPV4:10.10.10.0/24      impl-null       none
                 IPV4:3.3.3.3/32         25601           none
                 IPV4:2.2.2.2/32         impl-null       none
Sent Labels :    Fec                     Label           Maps To
                 IPV4:10.10.10.0/24      impl-null       none
                 IPV4:1.1.1.1/32         impl-null      none
R1#show ldp session 3.3.3.3
Session state                  : OPERATIONAL
Session role                   : Passive
TCP Connection                 : Established
IP Address for TCP             : 3.3.3.3
Interface being used           : xe1
Peer LDP ID                    : 3.3.3.3:0
Preferred Peer LDP Password    : Not Set
Adjacencies                    : 3.3.3.3
Advertisement mode             : Downstream Unsolicited
```

```
Label retention mode          : Liberal
Graceful Restart              : Not Capable
Keepalive Timeout             : 30
Reconnect Interval            : 15
Configured TCP MSS            : 700
Applied TCP MSS               : 700
Preferred TCP MSS             : NA
Address List received         : 3.3.3.3
                                20.20.20.2
Received Labels :       Fec             Label           Maps To
Sent Labels :   Fec                     Label           Maps To
```

R2

```
R2#show ldp session
Codes: m - MD5 password is not set/unset.
       g - GR configuration not set/unset.
       t - TCP MSS not set/unset.
       Session has to be cleared manually
Code  Peer IP Address      IF Name    My Role    State      KeepAlive  UpTime
       3.3.3.3            xe1        Passive   OPERATIONAL   30    00:13:39
       1.1.1.1            xe2       Active    OPERATIONAL   30    00:13:39
R2#show ldp session 3.3.3.3
Session state                 : OPERATIONAL
Session role                  : Passive
TCP Connection                : Established
IP Address for TCP            : 3.3.3.3
Interface being used          : xe1
Peer LDP ID                   : 3.3.3.3:0
Preferred Peer LDP Password   : Not Set
Adjacencies                   : 20.20.20.2
Advertisement mode            : Downstream Unsolicited
Label retention mode          : Liberal
Graceful Restart              : Not Capable
Keepalive Timeout             : 30
Reconnect Interval            : 15
Configured TCP MSS            : 710
Applied TCP MSS               : 710
Preferred TCP MSS             : NA
Address List received         : 3.3.3.3
                                20.20.20.2
Received Labels :       Fec             Label           Maps To
                IPV4:20.20.20.0/24      impl-null       none
                IPV4:3.3.3.3/32         impl-null       25601
Sent Labels :   Fec                     Label           Maps To
                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
                IPV4:1.1.1.1/32         25600           impl-null
R2#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          : xe2
Peer LDP ID                   : 1.1.1.1:0
Preferred Peer LDP Password   : Not Set
Adjacencies                   : 10.10.10.1
Advertisement mode            : Downstream Unsolicited
Label retention mode          : Liberal
Graceful Restart              : Not Capable
Keepalive Timeout             : 30
Reconnect Interval            : 15
Configured TCP MSS            : 710
Applied TCP MSS               : 700
Preferred TCP MSS             : NA
Address List received         : 1.1.1.1
                                10.10.10.1
Received Labels :       Fec             Label           Maps To
                IPV4:48.48.48.48/32     impl-null       none
                IPV4:10.10.10.0/24      impl-null       none
                IPV4:1.1.1.1/32         impl-null       25600
Sent Labels :   Fec                     Label           Maps To
                IPV4:20.20.20.0/24      impl-null       none
                IPV4:10.10.10.0/24      impl-null       none
                IPV4:3.3.3.3/32         25601           impl-null
                IPV4:2.2.2.2/32         impl-null       none
```

R3

```
R3#show ldp session 2.2.2.2
Session state                 : OPERATIONAL
Session role                  : Active
TCP Connection                : Established
IP Address for TCP            : 2.2.2.2
Interface being used          : xe1
Peer LDP ID                   : 2.2.2.2:0
Preferred Peer LDP Password   : Not Set
Adjacencies                   : 20.20.20.1
Advertisement mode            : Downstream Unsolicited
Label retention mode          : Liberal
Graceful Restart              : Not Capable
Keepalive Timeout             : 30
Reconnect Interval            : 15
Configured TCP MSS            : 720
Applied TCP MSS               : 710
Preferred TCP MSS             : NA
Address List received         : 2.2.2.2
                                10.10.10.2
                                20.20.20.1
Received Labels :       Fec             Label           Maps To
                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
                IPV4:1.1.1.1/32         25600           none
Sent Labels :   Fec                     Label           Maps To
                IPV4:20.20.20.0/24      impl-null       none
                IPV4:3.3.3.3/32         impl-null       none
R3#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          : xe1
Peer LDP ID                   : 1.1.1.1:0
Preferred 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
Configured TCP MSS            : 720
Applied TCP MSS               : 700
Preferred TCP MSS             : NA
Address List received         : 1.1.1.1
                                10.10.10.1
Received Labels :       Fec             Label           Maps To
Sent Labels :   Fec                     Label           Maps To
```

Configuration of TCP MSS with Auto-targeted

R1 - NSM

`R1#configure terminal`	Enter configure mode.
`R1(config)#interface xe1`	Specify the interface `xe1` to be configured.
`R1(config-if)#ip address 10.10.10.1/24`	Assign IP address `10.10.10.1/24` to interface.
`R1(config-if)#label-switching`	Enable label switching on interface `xe1`.
`R1(config-if)#exit`	Exit interface mode.
`R1(config)#interface lo`	Specify the loopback interface to be configured.
`R1(config-if)#ip address 1.1.1.1/32 secondary`	Set the IP address of the loopback interface to `1.1.1.1/32`.
`R1(config-if)#commit`	Commit the transaction.

R1 - LDP

`R1(config)#router ldp`	Enter Router mode for LDP.
`R1(config-router)#router-id 1.1.1.1`	Set the router ID to IP address `1.1.1.1`.

`R1(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.
`R1(config-router)#targeted-peer ipv4 3.3.3.3`	Configure targeted peer.
`R1(config-router-targeted-peer)#exit`	Exit-targeted-peer-mode.
`R1(config-router)#exit`	Exit the Router mode and return to the configure mode.
`R1(config)#interface xe1`	Enter interface mode.
`R1(config-if)#enable-ldp ipv4`	Enable LDP on `xe1`.
`R1(config-if)#commit`	Commit the transaction.

R1 - OSPF

`R1(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.
`R1(config-router)#network 10.10.10.0/24 area 0`	Define the interface `10.10.10.0/24`, on which OSPF runs and associate the area ID (0) with the interface.
`R1(config-router)#network 1.1.1.1/32 area 0`	Define the interface `1.1.1.1/32`, on which OSPF runs and associate the area ID (0) with the interface.
`R1(config-router)#commit`	Commit the transaction.

R2 - NSM

`R2#configure terminal`	Enter configure mode.
`R2(config)#interface lo`	Specify the loopback interface to be configured.
`R2(config-if)#ip address 2.2.2.2/32 secondary`	Set the IP address of the loopback interface to `2.2.2.2/32`.
`R2(config-if)#exit`	Exit interface mode.
`R2(config)#interface xe1`	Specify the interface `xe1` to be configured.
`R2(config-if)#ip address 20.20.20.1/24`	Assign IP address `20.20.20.1/24` to interface.
`R2(config-if)#label-switching`	Enable label switching on interface `xe1`.
`R2(config-if)#exit`	Exit interface mode.
`R2(config)#interface xe2`	Specify the interface `xe2` to be configured.
`R2(config-if)#ip address 10.10.10.2/24`	Assign IP address `10.10.10.2/24` to interface.
`R2(config-if)#label-switching`	Enable label switching on interface `xe2`.
`R2(config-if)#commit`	Commit the transaction.

R2 - LDP

`R2(config)#router ldp`	Enter Router mode.
`R2(config-router)#router-id 2.2.2.2`	Set the router ID to IP address `2.2.2.2`.

`R2(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.
`R2(config-router)#neighbor auto-targeted tcp-mss 800`	Configure the TCP MSS value on all `auto-targeted` neighbors.
`R2(config-router)#exit`	Exit Router mode and return to configure mode.
`R2(config)#interface xe1`	Specify the interface `xe1` to be configured.
`R2(config-if)#enable-ldp ipv4`	Enable LDP on a specified interface `xe1`.
`R2(config-if)#exit`	Exit interface mode.
`R2(config)#interface xe2`	Specify the interface `xe2` to be configured.
`R2(config-if)#enable-ldp ipv4`	Enable LDP on a specified interface `xe2`.
`R2(config-if)#commit`	Commit the transaction.

R2 - OSPF

`R2(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.
`R2(config-router)#network 10.10.10.0/24 area 0`	Define the interfaces `10.10.10.0/24`, on which OSPF runs and associate the area ID (0) with them.
`R2(config-router)#network 20.20.20.0/24 area 0`	Define the interfaces `20.20.20.0/24`, on which OSPF runs and associate the area ID (0) with them.
`R2(config-router)#network 2.2.2.2/32 area 0`	Define the interfaces `2.2.2.2/32`, on which OSPF runs and associate the area ID (0) with them.
`R2(config-router)#commit`	Commit the transaction.

R3 - NSM

`R3#configure terminal`	Enter configure mode.
`R3(config)#interface lo`	Specify the loopback interface to be configured.
`R3(config-if)#ip address 3.3.3.3/32 secondary`	Set the IP address of the loopback interface to `3.3.3.3/32`.
`R3(config-if)#exit`	Exit interface mode.
`R3(config)#interface xe1`	Specify the interface `xe1` to be configured.
`R3(config-if)#ip address 20.20.20.2/24`	Set the IP address of the interface to `20.20.20.2/24`.
`R3(config-if)#label-switching`	Enable label switching on interface `xe1`.
`R3(config-if)#commit`	Commit the transaction.

R3 - LDP

`R3(config)#router ldp`	Enter Router mode.
`R3(config-router)#router-id 3.3.3.3`	Set the router ID for IP address `3.3.3.3`.

`R3(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.
`R3(config-router)#neighbor auto-targeted tcp-mss 810`	Configure the TCP MSS value on all `auto-targeted` neighbors.
`R3(config-router)#targeted-peer ipv4 1.1.1.1`	Configure targeted peer.
`R3(config-router-targeted-peer)#exit`	Exit-targeted-peer-mode.
`R3(config-router)#exit`	Exit the Router mode and return to the configure mode.
`R3(config)#interface xe1`	Enter interface mode `xe1`.
`R3(config-if)#enable-ldp ipv4`	Enable LDP on `xe1`.
`R3(config-if)#commit`	Commit the transaction.

R3 - OSPF

`R3(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.
`R3(config-router)#network 20.20.20.0/24 area 0`	Define the interfaces `20.20.20.0/24`, on which OSPF runs and associate the area ID (0) with them.
`R3(config-router)#network 3.3.3.3/32 area 0`	Define the interfaces `3.3.3.3/32`, on which OSPF runs and associate the area ID (0) with them.
`R3(config-router)#commit`	Commit the transaction.

Validation

R1

```
R1#show ldp session
Codes: m - MD5 password is not set/unset.
       g - GR configuration not set/unset.
       t - TCP MSS not set/unset.
       Session has to be cleared manually
Code  Peer IP Address      IF Name    My Role    State       KeepAlive  UpTime
       2.2.2.2            xe1        Passive   OPERATIONAL   30    00:00:03
       3.3.3.3            xe1        Passive   OPERATIONAL   30    00:00:03
R1#show ldp targeted-peers
IP Address          Interface
3.3.3.3             xe1
R1#show ldp session 3.3.3.3
Session state                 : OPERATIONAL
Session role                  : Passive
TCP Connection                : Established
IP Address for TCP            : 3.3.3.3
Interface being used          : xe1
```

```
Peer LDP ID                   : 3.3.3.3:0
Preferred Peer LDP Password   : Not Set
Adjacencies                   : 3.3.3.3
Advertisement mode            : Downstream Unsolicited
Label retention mode          : Liberal
Graceful Restart              : Not Capable
Keepalive Timeout             : 30
Reconnect Interval            : 15
Configured TCP MSS            : Not configured
Applied TCP MSS               : 810
Preferred TCP MSS             : NA
Address List received         : 3.3.3.3
                                20.20.20.2
Received Labels :       Fec             Label           Maps To
                IPV4:20.20.20.0/24      25604           none
                IPV4:3.3.3.3/32         25603           none
                IPV4:10.10.10.0/24      25602           none
                IPV4:2.2.2.2/32         25601           none
                IPV4:1.1.1.1/32         25600           none
Sent Labels :   Fec                     Label           Maps To
                IPV4:10.10.10.0/24      25604           none
                IPV4:1.1.1.1/32         25603           none
                IPV4:20.20.20.0/24      25602           impl-null
                IPV4:3.3.3.3/32         25601           25601
                IPV4:2.2.2.2/32         25600           impl-null
```

R2

```
R2#show ldp session
Codes: m - MD5 password is not set/unset.
       g - GR configuration not set/unset.
       t - TCP MSS not set/unset.
       Session has to be cleared manually
Code  Peer IP Address      IF Name    My Role    State      KeepAlive  UpTime
       3.3.3.3            xe1       Passive   OPERATIONAL   30    00:00:04
       1.1.1.1            xe2       Active    OPERATIONAL   30    00:00:04
R2#show ldp targeted-peers
R2#show ldp session 3.3.3.3
Session state                 : OPERATIONAL
Session role                  : Passive
TCP Connection                : Established
IP Address for TCP            : 3.3.3.3
Interface being used          : xe1
Peer LDP ID                   : 3.3.3.3:0
Preferred Peer LDP Password   : Not Set
Adjacencies                   : 20.20.20.2
Advertisement mode            : Downstream Unsolicited
Label retention mode          : Liberal
Graceful Restart              : Not Capable
Keepalive Timeout             : 30
Reconnect Interval            : 15
```

```
Configured TCP MSS            : Not configured
Applied TCP MSS               : 1460
Preferred TCP MSS             : NA
Address List received         : 3.3.3.3
                                20.20.20.2
Received Labels :       Fec             Label           Maps To
                IPV4:20.20.20.0/24      impl-null       none
                IPV4:3.3.3.3/32         impl-null       25601
Sent Labels :   Fec                     Label           Maps To
                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
                IPV4:1.1.1.1/32         25600           impl-null
```

R3

```
R3#show ldp session
Codes: m - MD5 password is not set/unset.
       g - GR configuration not set/unset.
       t - TCP MSS not set/unset.
       Session has to be cleared manually
Code  Peer IP Address      IF Name    My Role    State      KeepAlive  UpTime
       2.2.2.2            xe1        Active    OPERATIONAL   30    00:02:15
       1.1.1.1            xe1        Active    OPERATIONAL   30    00:02:15
R3#show ldp targeted-peers
IP Address          Interface
1.1.1.1             xe1
PE2#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          : xe1
Peer LDP ID                   : 1.1.1.1:0
Preferred 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
Configured TCP MSS            : 810
Applied TCP MSS               : 810
Preferred TCP MSS             : NA
Address List received         : 1.1.1.1
                                10.10.10.1
Received Labels :       Fec             Label           Maps To
                                IPV4:10.10.10.0/24      25604           none
                IPV4:1.1.1.1/32         25603           none
                IPV4:20.20.20.0/24      25602           none
                IPV4:3.3.3.3/32         25601           none
```

```
                IPV4:2.2.2.2/32         25600           none
Sent Labels :   Fec                     Label           Maps To
                IPV4:20.20.20.0/24      25604           none
                IPV4:3.3.3.3/32         25603           none
                IPV4:10.10.10.0/24      25602           impl-null
                IPV4:2.2.2.2/32         25601           impl-null
                IPV4:1.1.1.1/32         25600           25600
```

New CLI Command

neighbor tcp-mss

Use this command to set the TCP MSS for an LDP session. MSS is a TCP parameter that defines the maximum amount of data in a TCP segment that can be transmitted.

Use the `no` command to remove the TCP MSS from an LDP session.

Command Syntax

```
neighbor (A.B.C.D| auto-targeted | all) tcp-mss <560-1440>
no neighbor (A.B.C.D | auto-targeted | all) tcp-mss
```

Parameters

`A.B.C.D`	To set MSS for the specific peer.
`auto-targeted`	To set MSS for auto-targeted LDP peer. Auto-targeted LDP sessions automatically establish the TCP connection with neighboring routers and do not require the manual configuration of each peer.
`all`	To set MSS for all LDP peers
`<560-1440>`	Configure the TCP MSS between this range.

Default

By default, `neighbor tcp-mss` is disabled and the MSS value is 1460 bytes.

Command Mode

Router LDP mode.

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

```
OcNOS(config)#router ldp
OcNOS(config-router)#neighbor 2.2.2.2 tcp-mss 900
OcNOS(config-router)#neighbor all tcp-mss 1000
OcNOS(config-router)#neighbor auto-targeted tcp-mss 800
OcNOS(config-router)#commit
```

Abbreviations

The following are some key abbreviations and their meanings relevant to this document:

Acronym	Description
ACK	Acknowledgment
IGP	Interior Gateway Protocol
LDP	Label Distribution Protocol
MSS	Maximum Segment Size
MTU	Maximum Transmission Unit
OSPF	Open Short Path First
SYN	Synchronize
TCP	Transmission Control Protocol

Glossary

The following provides definitions for key terms used throughout this document:

LDP	LDP is a routing protocol that manages and distributes the labels to the route in a Multiprotocol Label Switching (MPLS) network. Adding a label to a route helps to control the flow of network traffic and increases the forwarding speed, ensuring a smooth and optimized data transmission.
LDP session	LDP session is the connection established between LDP routers in an MPLS network.
MSS	MSS is a TCP parameter that defines the maximum amount of data in a TCP segment that can be transmitted.
TCP	TCP is one of the main protocols in the Internet Protocol (IP) suite. It offers a secure and reliable connection between two devices.
TCP segment	TCP segment is a unit of data transmitted in a TCP connection. The segment consists of header and payload. The header contains the control information to manage the transmission, and the payload contains the actual data that needs to be transmitted.

Two-Way Active Measurement Protocol Client

Overview

The Two-way Active Measurement Protocol (TWAMP) Client implementation is a network performance measurement feature that facilitates TWAMP on routers. This feature implements the client-side of the control session. The TWAMP Client is responsible for initiating and controlling network performance tests, while the TWAMP server receives these test requests, conducts the tests, and provides measurement results. The TWAMP client is used in conjunction with a TWAMP server on the other end to conduct bidirectional measurements, assess the network, troubleshoot issues, and ensure the quality of service in the network infrastructure.

Feature Characteristics

The Two-way Active Measurement Protocol Client feature has the following characteristics:

- The Twamp client initiates when a user creates a client connection to the server address and port.
- The Twamp client establishes a TCP connection with the designated server address and port.
- The server accepts the connection to establish the TCP session and ensures the seamless communication and exchange control messages with other TWAMP-compliant devices.

Benefits

The TWAMP Client Implementation has following benefits to network management and optimization:

- TWAMP clients adhere to standardized protocols, ensuring compatibility and interoperability with various TWAMP servers.
- TWAMP clients support authentication and access controls, ensuring the security of the measurement process and preventing unauthorized access.

Prerequisites

Ensure that the TWAMP client has a stable and reliable network connection to the TWAMP server.

Topology

The network topology includes the interactions between TWAMP Server and TWAMP Client entities, highlighting the flow of control messages and test packets. The TWAMP Client initiates active measurement sessions by sending control messages to the TWAMP Server over the TWAMP Control Connection. The TWAMP Server, in response, configures the session and directs test packets to the TWAMP Session-Reflector, which ensures proper routing and measurement. The results of these measurements are then relayed back to the TWAMP Client for analysis.

TWAMP Client

Implementation Examples

Scenario: Configure a TWAMP client with VRF settings, specifying the VRF vrf1 and setting up an IPv6 connection with advanced session parameters.

Configuration

Perform the following configuration TWAMP client on the Router.

1. Enable the Hardware profiles.

`Client(config)# hardware-profile filter twamp-ipv6 enable`	Enables the hardware profile filter for IPv6 traffic.
`Client(config-twamp-server)# hardware-profile filter twamp-ipv6-mpls enable`	Enables the hardware profile filter for IPv6 traffic over MPLS.

2. Configure VRF to define a separate virtual routing instance within the network device

Note: This step is optional, pre-existing VRFs can be used.

.

`Client(config)# ip vrf vrf1`	Enters the configuration mode for VRF vrf1.
`Client(config-vrf)# rd 10:100`	Configures the RD for VRF vrf1 to 10:100

3. Configure the interface with VR

.

`Client(config-if)# int xe14`	Enters the configuration mode for interface xe14.
`Client(config-if)# ip vrf forwarding vrf1`	Associates the interface xe14 with VRF vrf1.
`Client(config-if)#ipv6 address 2001:67c:2468::122:e:5/96`	Configures an IPv6 address on the interface.

4. Configure the delay-profile clients to specify parameters and customize the behavior of TWAMP client measurement

.

`Client(config)# delay-profile clients`	Enters the delay profile configuration
`Client(twamp-delay-profile)# burst-interval 1000`	Sets the burst interval to 1000 milliseconds in the delay profile.
`Client(twamp-delay-profile)#burst-count 2`	Sets the burst count to 2 in the delay profile

5. Enable the Twamp control to configure TWAMP control settings in a network device

.

`Client(config)# twamp-light control`	Enters the TWAMP Light control configuration.
`Client(config-twamp-light-ctrl)# control-admin-state enable`	Enables the TWAMP control administrative state.

6. Configure TWAMP Client to define the client's settings, connections, and measurement sessions.

.

`Client(config)# twamp client`	Enters the configuration for the TWAMP client.
`Client(config_twamp_client)# maximum-connections 64`	Sets the maximum number of connections that the TWAMP client can establish to 64.
`Client(config_twamp_client)#maximum-sessions 64`	Sets the maximum number of sessions that the TWAMP client can create to 64.
`client(config_twamp_client)#maximum-sessions-per-connection 64`	Sets the maximum number of sessions that can be created per connection to 64.
`client(config_twamp_client)#connection test_ipv6 vrf-name vrf1`	Configures a specific TWAMP client connection named test_ipv6 within the context of VRF vrf1.
`client(config_twamp_connection)#server ipv6 2001:67c:2468::122:e:4 port 862`	Configures the server for the TWAMP client connection. It specifies the IPv6 address of the TWAMP server (2001:67c:2468::122:e:4) and the port (862) on which the server listens for control connections.
`client(config-twamp-connection)#session session_IPV6 sender-port 5666 receiver-port 5666 sender-address ipv6 2001:67c:2468::122:e:5 receiver-address ipv6 2001:67c:2468::122:e:4`	Configures a specific TWAMP session within the connection. It defines the session name (session_IPV6), sender and receiver ports (5666), sender and receiver IPv6 addresses, and sets up the parameters for the session.
`client(config-twamp-connection)#exit`	Exits the current configuration mode for the TWAMP client connection.
`Client#twamp client start connection test_ipv6 vrf vrf1 packet-count 50`	Initiates the TWAMP client for a specific connection named test_ipv6 in VRF vrf1 with a packet count of 50.
`OcNOS#twamp client stop connection test_ipv6 vrf vrf1`	Stops the TWAMP client for the test_ipv6 connection within VRF vrf1.
`OcNOS#twamp client reset connection test_ipv6 vrf vrf1`	Resets TWAMP client for the test_ipv6 connection within VRF vrf1.

New CLI Commands

Here is the compilation of new commands for configuring TWAMP client.

- `twamp client`, `maximum-sessions`, `maximum-connections`, `maximum-sessions-per-connection`, `connection`, `server`, `session`, `twamp client start connection`, `twamp client stop connection and twamp client reset connection` in the “New Features in Release 6.4.1" document.

twamp client

Use this command to enable and configure the TWAMP client.

Command Syntax

```
twamp client
```

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

```
OcNOS(config)#
OcNOS(config)#twamp client
OcNOS(config-twamp-client)#
```

twamp client maximum-connections

Use this command to set the maximum number of connections that the client can create. The default value of this flag is 64.Use the no form of this command to set the value to the default value 64.

Command Syntax

```
max-connections <1-64>
```

Parameters

<1-64>	Set the maximum number of connections value between 1 and 64.

Default

Default value is 64

Command mode

twamp-client mode

Applicability

This command was introduced in OcNOS version 6.4.1

Examples

```
OcNOS(config)#twamp client
OcNOS(config-twamp-client)# maximum-connections 10
OcNOS(config-twamp-client)#commit
OcNOS(config-twamp-client)#no max-connections
OcNOS(config-twamp-client)#commit
```

twamp client maximum-sessions

Use this command to set the maximum number of test sessions that the client can simultaneously handle. The default value of this flag is 64.

Use the no form of this command to set the value to the default value 64.

Command Syntax

```
maximum-sessions <1-64>
```

Parameters

<1-64>	Set the maximum number of sessions between 1 and 64.

Default

Default value is 64

Command mode

twamp-client mode

Applicability

This command was introduced in OcNOS version 6.4.1

Examples

```
OcNOS(config)#twamp client
OcNOS(config-twamp-client )#maximum-sessions 44
OcNOS(config-twamp-client)#commit
OcNOS(config-twamp-client )#no maximum-sessions
OcNOS(config-twamp-client )#commit
OcNOS(config-twamp-client )#
```

twamp client maximum-sessions-per-connection

Use this command to set the maximum number of test sessions that the client can simultaneously create on the same connection. The default value of this flag is 1.

Use the no form of this command to set the value to the default value 1.

Command Syntax

```
maximum-sessions-per-connection <1-64>
```

Parameters

<1-64>	Set the maximum number of sessions per connection between 1 and 64.

Default

Default value is 1

Command mode

twamp-client mode

Applicability

This command was introduced in OcNOS version 6.4.1

Examples

```
OcNOS(config)#twamp server
OcNOS(config-twamp-client )#maximum-sessions-per-connection 26
OcNOS(config-twamp-client )#commit
OcNOS(config-twamp-client )#no maximum-sessions-per-connection
OcNOS(config-twamp-client)#commit
OcNOS(config-twamp-client)#
```

twamp connection

Use this command to create a connection between the server and the client.

Multiple connections can be specified. The user can issue the same command multiple times, once for each VRF.

Only clients in the configured VRFs are allowed to connect to the server and only sessions to IPs in the configured VRFs are allowed to be established.

Use the no form of this command to remove the connection.

Command Syntax

```
connection NAME <vrf-name NAME>
no connection NAME <vrf-name NAME>
```

Parameters

NAME	connection name to add to the client.

Default

N/A

Command mode

twamp-client mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

```
OcNOS(config)#twamp client
OcNOS(config-twamp-client)#connection Connection1 vrf VRF1
OcNOS(config-twamp-client)#commit
OcNOS(config-twamp-client)#
OcNOS(config-twamp-client)#no connection Connection1 vrf VRF1
OcNOS(config-twamp-client)#commit
```

twamp client server

Use this command to configure the server ip address(ipv4/ipv6), hostname, and port number.

Command Syntax

```
server (ipv4 A.B.C.D|ipv6 X:X::X:X|HOSTNAME) (port (862|<1025-65535>)|)
```

Parameters

`ipv4 A.B.C.D`	Specifies the target server's IPv4 address
`ipv6 X:X::X:X`	Specifies the target server's IPv6 address
`HOSTNAME`	Specifies the target server's hostname
`port (862|<1025-65535>`	Specifies the port number on which the TWAMP server is listening for control connections. 862 is the default port.

Default

N/A

Command mode

twamp-client connection mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

```
OcNOS(config)#twamp client
OcNOS(config_twamp_client)#connection con4
OcNOS(config-twamp-connection)#server ipv4 192.168.1.100 port 862
OcNOS(config-twamp-connection)#commit

OcNOS(config)#twamp client
OcNOS(config_twamp_client)#connection con6
OcNOS(config-twamp-connection)#server ipv6
2001:0db8:85a3:0000:0000:8a2e:0370:7334 port 5000
OcNOS(config-twamp-connection)#commit

OcNOS(config)#twamp client
OcNOS(config_twamp_client)#connection conhost
OcNOS(config-twamp-connection)#server pe1-host port 5100
OcNOS(config-twamp-connection)#commit
```

twamp client session

Use this command to request a session from the server.

Command Syntax

```
session <session-name> sender-port <port> receiver-port <port> (sender-address
  <address>|) (receiver-address <address>|) (start-time <TIME>|) (interface
  <IFNAME>|)
```

Parameters

session-name	Specifies the name of the TWAMP client session.
port	Specifies the sender and receiver port numbers to be used in the session.
address	Specifies the sender and receiver addresses(optional).
TIME	Defines the start time of the session (optional).
IFNAME	specifies the interface to be associated with the session (optional).

Default

N/A

Command mode

twamp-client-connection mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

```
OcNOS(config)#twamp client
OcNOS(config_twamp_client)#connection testipv6
OcNOS(config-twamp-connection)#server ipv6 2001:67c:2468::122:e:5 port 862
OcNOS(config-twamp-connection)#session sessionipv6 sender-port 4555 receiver-
port 4555 sender-address ipv6 20
```

twamp client start connection

Use this command to start the sessions already requested from the server and accepted by the server over the specified connection.

Command Syntax

```
twamp client start connection <NAME> packet-count <0-1000000> (vrf NAME |)
```

Parameters

NAME	Specifies the name of the TWAMP client connection to be used for the session.
0-1000000	Specifies the number of packets to be used in the session. It can be any value between 0 and 1,000,000.
vrf NAME	Specifies the a Virtual Routing and Forwarding (VRF) context for the TWAMP client session (optional).

Default

N/A

Command mode

exec mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

```
OcNOS(config)#twamp client
OcNOS(config-twamp-client)#twamp client start connection MyConnection packet-count 1000 vrf VRF1
OcNOS(config-twamp-client)#commit
```

twamp client stop connection

Use this command to stop the sessions already requested from the server and accepted by the server over the specified connection.

Command Syntax

```
twamp client stop connection <NAME> packet-count <0-1000000> (vrf NAME |)
```

Parameters

`NAME`	Specifies the name of the TWAMP client connection to be used for the session.
`0-1000000`	Specifies the number of packets to be used in the session. It can be any value between 0 and 1,000,000.
`vrf NAME`	Specifies the a VRFcontext for the TWAMP client session (optional).

Default

N/A

Command mode

exec mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

```
OcNOS(config)#twamp client
OcNOS(config-twamp-client)#twamp client stop connection MyConnection packet-count 1000 vrf VRF1
OcNOS(config-twamp-client)#commit
```

twamp client reset connection

Use this command to reset the TWAMP client sessions on a connection.

Command Syntax

```
twamp client reset connection NAME (session NAME|) (vrf WORD|)
```

Parameters

NAME	Specifies the name of the connection where the sessions will be reset.
NAME	Specifies the name of the session to be reset. If not specified, all sessions on the connection will be reset.
WORD	Specifies the name of the vrf where the connection is operating. If not specified, the default vrf will be used.

Default

N/A

Command mode

exec mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

```
    OcNOS#twamp client reset connection test_ipv6 vrf vrf1
```

Validation

Show Output commands.

1.To verify the Client is established

```
OcNOS#sh twamp client connection
connection Name Server address  Server port     VRF     Status
test_ipv6  2001:67c:2468::122:e:4           862          vrf1   Established
```

2.To verify the Session is accepted

```
OcNOS#sh twamp client session

Connection name  Session name    Sender        Receiver      State
test_ipv6        session_IPV6    2001:67c:2468::122:e:52001:67c:2468::122:e:4Accepted
```

3.To measure the Packets from Client to Server

```
OcNOS#sh twamp-statistics
========================================
      TWAMP Test-Session Statistics
========================================
  Test-Session Name        : session_IPV6
  Start Time               : 2023 Oct 16 20:37:32
  Elapsed time(milli sec)  : 15013
  Packets Sent             : 30
  Packets Received         : 30
  Packet Loss(%)           : 0.00
  Round Trip Delay(usec)
      Minimum              : 61
      Maximum              : 260
```

```
      Average              : 112
  Forward Delay(usec)
      Minimum              : (*)
      Maximum              : (*)
      Average              : (*)
  Reverse Delay(usec)
      Minimum              : (*)
      Maximum              : (*)
      Average              : (*)
  Round Trip Delay Variation(usec)
      Minimum              : 75
      Maximum              : 90
      Average              : 84
  Forward Delay Variation(usec)
      Minimum              : (*)
      Maximum              : (*)
      Average              : (*)
  Reverse Delay Variation(usec)
      Minimum              : (*)
      Maximum              : (*)
      Average              : (*)

(*) - Time is not in sync between Sender and Reflector
```

4. Session started

```
OcNOS#sh twamp client connection

connection Name Server address  Server port     VRF     Status
test_ipv6  2001:67c:2468::122:e:4           862          vrf1   Running
OcNOS#
OcNOS#sh twamp client session

Connection name  Session name    Sender        Receiver      State
test_ipv6        session_IPV6    2001:67c:2468::122:e:52001:67c:2468::122:e:4Started

connection Name Server address  Server port     VRF     Status
connection_vrf      10.1.1.1           862          vrf1       Running
```

Abbreviations

The following are some key abbreviations and their meanings relevant to this document:

TCP	Transmission Control Protocol
TWAMP	Two-way Active Measurement Protocol Client

TCP	Transmission Control Protocol
VRF	Virtual Routing and Forwarding
RD	Route Distinguisher

Glossary

The following provides definitions for key terms used throughout this document.

TWAMP	Two-Way Active Measurement Protocol, a standardized protocol for measuring network performance in a bidirectional manner.
Client	In the context of TWAMP, the client is a device or software component responsible for initiating TWAMP test sessions and measuring network performance.
Session	A measurement session in TWAMP involves the exchange of test packets between the client and the server to assess network performance.
Server	The counterpart to the client, the server in TWAMP receives test packets, conducts measurements, and provides results to the client.
Test Packets	Data packets exchanged between the client and server to measure network performance, including metrics like latency, jitter, and packet loss.
Initiate	The action of starting a TWAMP test session from the client to the server.
Latency	The time it takes for data packets to travel from the client to the server and back, often measured in milliseconds.

Single-Home for VxLAN IRB with OSPF or ISIS

Overview

Single Home Virtual Extensible LAN (VxLAN) with Integrated Routing (IRB) using Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (ISIS) protocols provides the solution for connecting and managing virtual networks within a data center or network infrastructure.

This feature offers a solution for networks where the interconnection of VLANs is required. These protocols can be configured on IRB interfaces within layer 3 switches or routers. This configuration enables dynamic routing, facilitating the exchange of routing information with other devices in the network. By assigning IP addresses to the IRB interfaces, they serve as the default gateways for devices within the respective VLANs.

Both OSPF and ISIS routing updates are dynamically exchanged over IRB interfaces, ensuring up-to-date routing tables and optimized traffic routing across different VLANs and networks.

This feature offers flexibility in configuring network topologies, and ensures compatibility and interoperability within diverse network environments.

Feature Characteristics

The OSPF and ISIS support over the IRB Interface feature has the following characteristics:

- Enables the control of Receive (RX)/ Transmit (TX) of OSPF and ISIS packets on IRB interfaces, providing effective management of IRB interfaces interactions with OSPF and ISIS for optimized network communication and routing.
- IRB interfaces process configured MTU size packets.
- Maintains consistency in CLI commands with SVI interfaces for OSPF and ISIS configurations, simplifying network management tasks.

Benefits

The OSPF and ISIS support over the IRB Interface has the following benefits:

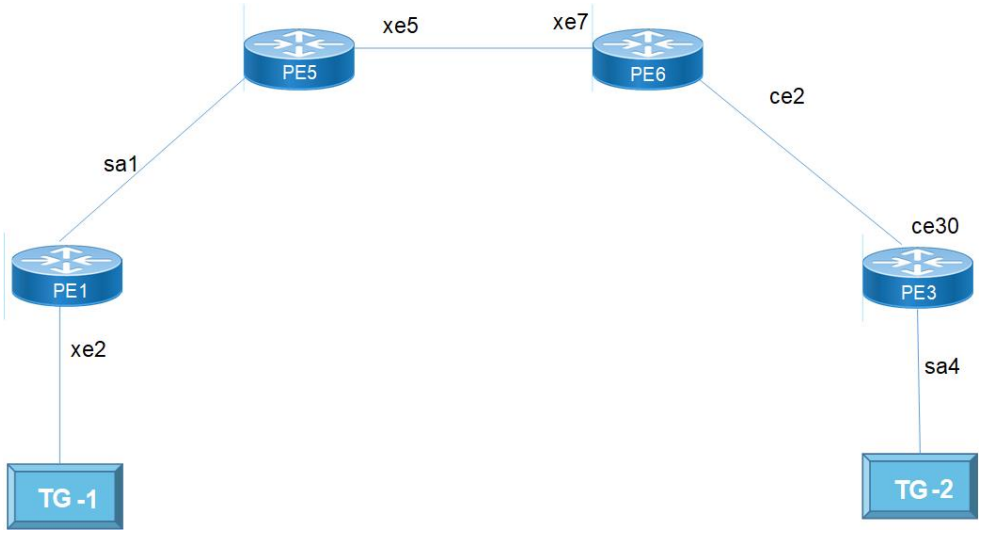
- Enables seamless inter-subnet communication across different VNIDs and subnets within the same customer network.
- Promotes seamless connectivity between devices, irrespective of whether they are connected through IRB or SVI interfaces, and simplifies network management.
- The network gains greater adaptability to various scenarios and evolving requirements, offering greater versatility in its operations.

Prerequisites

- Router must be up and running.
- Maintain synchronization with VRF changes by performing IRB shut/no shut actions when specific events occur within the IPVRF. These events may involve adding or removing Route Targets (RTs), updating Route Distinguishers (RDs), or modifying Layer 3 Virtual Network Identifiers (L3VNIs).

Topology for OSPF

The network topology includes various network elements such as routers, customer edge (CE) devices, Service Aggregator (SA) devices, and Provider Edge (PE) routers. The feature enables OSPF on the IRB interfaces, allowing for efficient routing and communication between network devices within the topology.



Single Home VxLAN IRB with OSPF

Configuration

Perform the following configurations to set up different interfaces, routing protocols, and BGP parameters to enable VXLAN, IRB, and EVPN functionality in the network.

OSPF

PE1

`PEI(Config)# terminal`	Enters the configuration mode.
`PE1(config)#interface sa1`	Configure the sa1 interface as a network interface.
`PE1(config-if)# ip address 10.1.1.1/24`	Assigns an IP address to the sa1 interface with a subnet mask of /24.
`PE1(config-if)# ip ospf cost 10`	Configures the OSPF cost for the sa1 interface, setting it to 10.
`PE1(config-if)# load-interval 30`	Configures the load-interval for monitoring traffic on the sa1 interface.
`PE1(config)#interface xe1`	Enters the interface xe1 mode.
`PE1(config-if)# static-channel-group 1`	Assigns the static channel group 1 to the xe2 interface.
`PE1(config-irb-if)#interface lo`	Configures the loopback (lo) interface.
`PE1(config-if)# ip address 1.1.1.1/32 secondary`	Assigns the primary IP address 1.1.1.1/32 to the loopback interface and specifies it as secondary.

`PE1(config)#router ospf 1`	Enters the OSPF configuration mode for OSPF process 1.
`PE1(config-router)# ospf router-id 1.1.1.1`	Sets the OSPF router ID to 1.1.1.1 for OSPF process 1.
`PE1(config-router)# network 1.1.1.1/32 area 0.0.0.0`	Advertises the network 1.1.1.1/32 into OSPF area 0.0.0.0.
`PE1(config-router)# network 10.1.1.0/24 area 0.0.0.0`	Advertises the network 10.1.1.0/24 into OSPF area 0.0.0.0.
`PE1(config)#hardware-profile filter vxlan enable`	Enables the hardware profile filter for VXLAN.
`PE1(config)#nvo vxlan enable`	Enables the VXLAN feature on the device.
`PE1(config)#nvo vxlan irb`	Enables VXLAN IRB functionality.
`PE1(config-vrf)#mac vrf L2VRF1`	Configures a MAC VRF named L2VRF1.
`PE1(config-vrf)# rd 1.1.1.1:11`	Sets the Route Distinguisher (RD) to 1.1.1.1:11 for the VRF.
`PE1(config-vrf)# route-target both 9.9.9.9:100`	Configures both import and export route targets for the VRF.
`PE1(config-vrf)#ip vrf L3VRF1`	Configures an IP VRF named L3VRF1.
`PE1(config-vrf)# rd 51000:11`	Sets the RD value to 51000:11 for the L3VRF1.
`PE1(config-vrf)# route-target both 100:100`	Configures both import and export route targets for L3VRF1.
`PE1(config-vrf)# l3vni 1000`	Configures the L3 Virtual Network Identifier (L3VNI) with the value 1000.
`PE1(config)#interface irb1001`	Configures the IRB interface for L3VRF1.
`PE1(config-irb-if)# ip vrf forwarding L3VRF1`	Assigns the L3VRF1 to the IRB interface.
`PE1(config-irb-if)# ip address 11.11.11.1/24`	Assigns an IP address 11.11.11.1/24 to the IRB interface.
`PE1(config-irb)#interface irb2001`	Configures the IRB interface for IPv6 in L3VRF1.
`PE1(config-irb-if)# ip vrf forwarding L3VRF1`	Assigns the L3VRF1 to the IPv6 IRB interface.
`PE1(config-irb-if)# ipv6 address 2001::1/64`	Assigns an IP address 11.11.11.1/24 to the IRB interface.
`PE1(config-irb-if)#mtu 9000`	Sets the Maximum Transmission Unit (MTU) for this IRB interface to 9000 bytes.
`PE1(config-router)#router ospf 2 L3VRF1`	Configures OSPF on the L3VRF1.
`PE1(config-router)# network 11.11.11.0/24 area 0.0.0.0`	Advertises the network 11.11.11.0/24 into OSPF area 0.0.0.0.
`PE1(config-router)#router ipv6 vrf ospf L3VRF1`	Configures OSPFv3 on the L3VRF1.
`PE1(config-router)# router-id 1.1.1.1`	Configures the router ID as 1.1.1.1.
`PE1(config-irb)#interface irb2001`	Configures the IPv6 IRB interface.
`PE1(config-irb-if)# ipv6 router ospf area 0.0.0.0 tag L3VRF1 instance-id 0`	Attaches the OSPFv3 instance ID to the IPv6 IRB interface.
`PE1(config)#nvo vxlan vtep-ip-global 1.1.1.1`	Configures the global VTEP IP address as 1.1.1.1.
`PE1(config)#nvo vxlan id 101 ingress-replication`	Configures the VXLAN ID as 101 for ingress replication.
`PE1(config-nvo)# vxlan host-reachability-protocol evpn-bgp L2VRF1`	Maps the EVPN-BGP host reachability protocol to L2VRF1.
`PE1(config-nvo)# evpn irb1001`	Maps the IRB interface 1001 to EVPN.
`PE1(config-nvo)# vni-name VNI-101`	Configures the VNI name as VNI-101.
`PE1(config)#nvo vxlan id 2001 ingress-replication`	Configures the VXLAN ID as 2001 for ingress replication.

`PE1(config-nvo)# vxlan host-reachability-protocol evpn-bgp L2VRF1`	Maps the EVPN-BGP host reachability protocol to L2VRF1.
`PE1(config-nvo)# evpn irb2001`	Maps the IPv6 IRB interface to EVPN.
`PE1(config)#interface xe2`	Configures the xe2 interface.
`PE1(config-if)# switchport`	Configures the port as a Layer 2 (L2) switchport.
`PE1(config-if)# load-interval 30`	Configures the load-interval of 30 minutes for monitoring traffic on the xe2 interface.
`PE1(config-if)#interface xe2.100 switchport`	Configures a Layer 2 access interface subinterface
`PE1(config-if)# encapsulation dot1q 100`	Sets the encapsulation to be a single-tag with VLAN ID 100
`PE1(config-if)# rewrite pop`	Configures the rewrite pop action.
`PE1(config-if)# access-if-evpn`	Configures the port as an access interface for EVPN.
`PE1(config-acc-if-evpn)#  map vpn-id 101`	Maps the VPN ID 101 to the interface.
`PE1(config)#interface xe2.2001 switchport`	Configures a Layer 2 access interface subinterface.
`PE1(config-if)# rewrite pop`	Configures the rewrite pop action.
`PE1(config-if)# access-if-evpn`	Configures the port as an access interface for EVPN.
`PE1(config-acc-if-evpn)#  map vpn-id 2001`	Maps the VPN ID 2001 to the interface.
`PE1(config-router)#router bgp 100`	Configures the BGP process with AS number 100.
`PE1(config-router)# bgp router-id 1.1.1.1`	Assigns the router ID as 1.1.1.1 for the BGP instance.
`PE1(config-router)# neighbor 4.4.4.4 remote-as 100`	Configures neighbor 4.4.4.4 with a remote AS number of 100.
`PE1(config-router)# neighbor 4.4.4.4 update-source lo`	Configures the update source for neighbor 4.4.4.4 to be the loopback interface.
`PE1(config-router)# neighbor 4.4.4.4 advertisement-interval 0`	Configures the advertisement interval for neighbor 4.4.4.4 as 0.
`PE1(config-router)# address-family l2vpn evpn`	Configures the address-family for L2VPN EVPN.
`PE1(config-router-af)# neighbor 4.4.4.4 activate`	Activates the neighbor for the L2VPN EVPN address-family.
`PE1(config-router-af)# exit-address-family`	Exits from the address family configuration.
`PE1(config-router)# address-family ipv4 vrf L3VRF1`	Configures the IPv4 address-family for VRF L3VRF1.
`PE1(config-router-af)# redistribute connected`	Configures the redistribution of connected routes within the IPv4 address-family.
`PE1(config-router-af)# exit-address-family`	Exits the IPv4 address-family configuration.
`PE1(config-router)# address-family ipv6 vrf L3VRF1`	Configures the IPv6 address-family for VRF L3VRF1.
`PE1(config-router-af)# redistribute connected`	Configures the redistribution of connected routes within the IPv6 address-family.
`PE1(config-router-af)# exit-address-family`	Exits the IPv6 address-family configuration.

PE5

`PE5#configure terminal`	Enters the configuration mode
`PE5(config)#interface sa1`	Configure the sa1 interface as a network interface.
`PE5(config-if)# ip address 10.1.1.1/24`	Assigns an IP address to the sa1 interface with a subnet mask of /24.

`PE5(config-if)# ip ospf cost 10`	Configures the OSPF cost for the sa1 interface, setting it to 10.
`PE5(config-if)# load-interval 30`	Configures the load-interval for monitoring traffic on the sa1 interface.
`PE5(config)#interface xe1`	Configure network interface towards PE6.
`PE5(config-if)# static-channel-group 1`	Assigns the static channel group 1 to the xe1 interface.
`PE5(config)#interface xe5`	configures the xe5 interface.
`PE5(config-if)#ip address 30.1.1.1/24`	Assigns the primary IP address 1.1.1.1/32 to the loopback interface and specifies it as secondary.
`PE5(config)#ip ospf cost 10`	Configures the OSPF cost for the xe5 interface, setting it to 10.
`PE5(config-router)# ospf router-id 1.1.1.1`	Assigns an IP address (30.1.1.1) to the xe5 interface with a subnet mask of /24.
`PE5(config)#load-interval 30`	Configures the load-interval for monitoring traffic on the xe5 interface.
`PE5(config)#router ospf 1`	Enters the OSPF configuration mode for OSPF process 1.
`PE5(config-router)# network 30.1.1.0/24 area 0.0.0.0`	Advertises the network 30.1.1.0/24 into OSPF area 0.0.0.0.
`PE5(config-router)# network 10.1.1.0/24 area 0.0.0.0`	Advertises the network 10.1.1.0/24 into OSPF area 0.0.0.0.

PE3

`PE3#configure terminal`	Enters the configuration mode
`PE3(config)#interface  ce30`	Configure the ce30 interface as a network interface.
`PE3(config-if)# ip address 40.1.1.2/24`	Assigns an IP address to the ce30 interface with a subnet mask of /24.
`PE3(config-if)# ip ospf cost 10`	Configures the OSPF cost for the sa1 interface, setting it to 10.
`PE3(config-if)# load-interval 30`	Configures the load-interval for monitoring traffic on the sa1 interface.
`PE3(config)#interface lo`	Configure the loopback interface.
`PE3(config-if)#ip address 4.4.4.4/32 secondary`	Assign an secondary IP to an loopback interface.
`PE3(config)#ip ospf cost 10`	Configures the OSPF cost for the xe7interface, setting it to 10.
`PE3(config)#load-interval 30`	Configures the load-interval for monitoring traffic on the xe5 interface.
`PE3(config)#router ospf 1`	Enters the OSPF configuration mode for OSPF process 1.
`PE3(config-router)# ospf router-id 4.4.4.4`	Configures the router id to an ospf instance.
`PE3(config-router)# network 4.4.4.4/32 area 0.0.0.0`	Advertises the loopback address.
`PE3(config-router)# network 40.1.1.0/24 area 0.0.0.0`	Advertises the network interface IP address.
`PE3(config)#hardware-profile filter vxlan enable`	Enables hardware profile filter for vxlan
`PE3(config)#nvo vxlan enable`	Enables VXLAN on the device, allowing it to participate in VXLAN networks.

`PE3(config)#nvo vxlan irb`	Enables VXLAN IRB functionality, that allows routing between VXLAN and non-VXLAN networks.
`PE3(config-vrf)#mac vrf L2VRF1`	Configures a L2 MAC VRF instance named L2VRF1, which is a logical network segment for L2 traffic isolation.
`PE3(config-vrf)# rd 4.4.4.4:11`	Configures a RD for the L2VRF1, with the value 4.4.4.4:11.
`PE3(config-vrf)# route-target both 9.9.9.9:100`	Configures a route target for the VRF.
`PE3(config-vrf)#ip vrf L3VRF1`	Configures a L3 VRF named L3VRF1.
`PE3(config-vrf)# rd 56000:11`	Configures a RD for the L3VRF1, with the value 56000:11.
`PE3(config-vrf)# route-target both 100:100`	Configures a route target for the VRF.
`PE3(config-vrf)# l3vni 1000`	Configures a L3VNI with the ID 1000 for the VRF.
`PE3(config)#interface irb1001`	Configures the IRB interface with the ID 1001.
`PE3(config-irb-if)# ip vrf forwarding L3VRF1`	Associates the IRB interface with the L3VRF1, ensuring that traffic from this interface is isolated within that VRF.
`PE3(config-irb-if)# ip address 12.12.12.1/24`	Assigns an IP address 12.12.12.1 with a subnet mask of /24 to the IRB interface, enabling it for L3 routing.
`PE3(config-irb-if)# mtu 1500`	Configures the MTU for the interface irb1001 to 1500 bytes.
`PE3(config)#interface irb2001`	Configures another IRB interface with the ID 2001.
`PE3(config-irb-if)# ip vrf forwarding L3VRF1`	Associates the IRB interface with the L3VRF1.
`PE3(config-irb-if)# ipv6 address 2002::1/64`	Assigns an IPv6 address 2002::1 with a subnet mask of /64 to the IRB interface, enabling it for IPv6 routing.
`PE3(config-irb-if)# mtu 1500`	Configures the MTU for the interface irb2001 to 1500 bytes.
`PE3(config-router)#router ospf 2 L3VRF1`	Configures the OSPF routing process on OSPF instance 2 for the L3VRF1.
`PE3(config-router)# network 12.12.12.0/24 area 0.0.0.0`	Advertises the network 12.12.12.0/24 to OSPF area 0.0.0.0.
`PE3(config-router)#router ipv6 vrf ospf L3VRF1`	Configures the OSPFv3 routing process on OSPFv3 instance for the L3VRF1.
`PE3(config-router)# router-id 4.4.4.4`	Sets the router ID for the OSPF/OSPFv3 instances to 4.4.4.4.
`PE3(config)#nvo vxlan vtep-ip-global 4.4.4.4`	Configures the global VTEP IP address as 4.4.4.4 for VXLAN.
`PE3(config)#nvo vxlan id 102 ingress-replication`	Configures the VXLAN with VNI ID 102 for ingress replication.
`PE3(config-nvo)# vxlan host-reachability-protocol evpn-bgp L2VRF1`	Maps the VXLAN configuration with the EVPN-BGP protocol and associates it with the L2VRF1.
`PE3(config-nvo)# evpn irb1001`	Maps the IRB interface irb1001 to the VXLAN.
`PE3(config-nvo)# vni-name VNI-101`	Configures the VNI name as VNI-101.
`PE3(config)#nvo vxlan id 2002 ingress-replication`	Configures another VXLAN with VNI ID 2002 for ingress replication.
`PE3(config-nvo)# vxlan host-reachability-protocol evpn-bgp L2VRF1`	Maps the VXLAN configuration with the EVPN-BGP protocol and associates it with the L2VRF1.
`PE3(config-nvo)# evpn irb2001`	Maps the IPv6 IRB interface irb2001 to the VXLAN.
`PE3(config)#interface sa4`	Configures interface sa4.
`PE3(config-if)# switchport`	Configures the interface as a switchport.
`PE3(config-if)# load-interval 30`	Sets the load interval for the interface to 30 seconds.
`PE3(config-if)# mtu 1500`	Configures the MTU for the interface to 1500 bytes.

`PE3(config)#interface xe1`	Configures interface xe1.
`PE3(config-if)# static-channel-group 4`	Assigns a static channel group to interface xe1.
`PE3(config-if)#interface sa4.100 switchport`	Configures subinterface sa4.100 as a switchport with VLAN 100.
`PE3(config-if)# encapsulation dot1q 100`	Configures the encapsulation with VLAN ID 100.v
`PE3(config-if)# rewrite pop`	Configures the rewrite behavior for popping VLAN tags.
`PE3(config-if)# access-if-evpn`	Configures the interface as an access interface for EVPN.
`PE3(config-acc-if-evpn)# map vpn-id 102`	Maps the access interface to VPN ID 102 for EVPN routing.
`PE3(config)#interface sa4.2002 switchport`	Configures subinterface sa4.2002 as a switchport with VLAN 2002.
`PE3(config-if)# encapsulation dot1q 2002`	Configures the encapsulation with VLAN ID 2002.
`PE3(config-if)# rewrite pop`	Configures the rewrite behavior for popping VLAN tags.
`PE3(config-if)# access-if-evpn`	Configures the interface as an access interface for EVPN.
`PE3(config-acc-if-evpn)# map vpn-id 2002`	Maps the access interface to VPN ID 2002 for EVPN routing.
`PE3(config-router)#router bgp 100`	Configures the BGP with AS number 100.
`PE3(config-router)# bgp router-id 4.4.4.4`	Sets the BGP router ID to 4.4.4.4.
`PE3(config-router)# neighbor 1.1.1.1 remote-as 100`	Configures a BGP neighbor with the remote AS number 100 and the IP address 1.1.1.1.
`PE3(config-router)# neighbor 1.1.1.1 update-source lo`	Specifies the BGP neighbor to use the loopback interface as the source for updates.
`PE3(config-router)# neighbor 1.1.1.1 advertisement-interval 0`	Configures the advertisement interval for BGP neighbor updates.
`PE3(config-router)# address-family l2vpn evpn`	Configures the BGP address family for Layer 2 VPN EVPN.
`PE3(config-router-af)# neighbor 1.1.1.1 activate`	Activates the BGP neighbor for the specified address family.
`PE3(config-router-af)# exit-address-family`	Exits the BGP address family configuration.
`PE3(config-router)# address-family ipv4 vrf L3VRF1`	Configures the BGP address family for IPv4 within VRF L3VRF1.
`PE3(config-router-af)# redistribute connected`	Configures BGP to redistribute connected routes into the BGP process.
`PE3(config-router-af)# exit-address-family`	Exits the BGP address family configuration for IPv4.
`PE3(config-router)# address-family ipv6 vrf L3VRF1`	Configures the BGP address family for IPv6 within VRF L3VRF1.
`PE3(config-router-af)# redistribute connected`	Configures BGP to redistribute connected routes into the BGP process.
`PE3(config-router-af)# exit-address-family`	Exits the BGP address family configuration for IPv6.

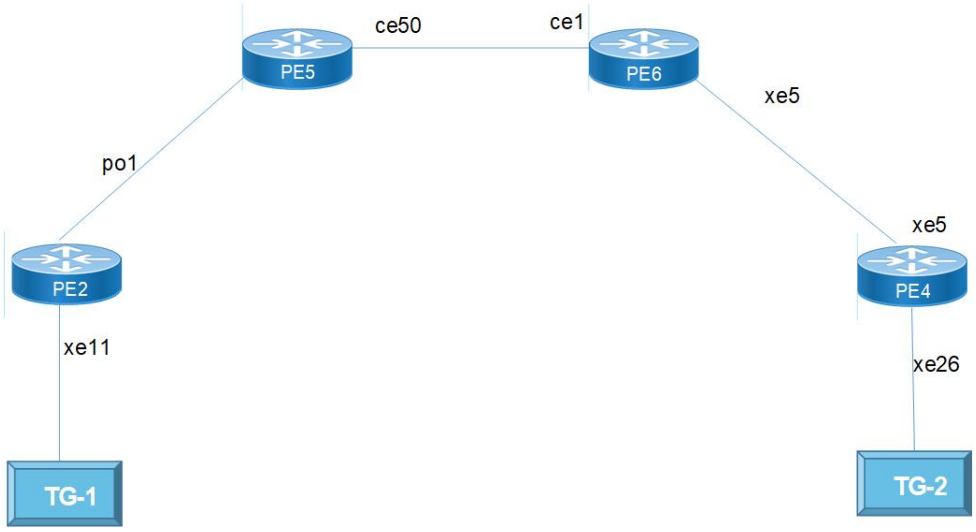
PE6

`PE6#configure terminal`	Enters the configuration mode.
`PE6(config)#interface  ce2`	Configure the ce2 interface as a network interface.
`PE6(config-if)# ip address 10.1.1.1/24`	Assigns an IP address to the sa1 interface with a subnet mask of /24.

`PE6(config-if)# ip ospf cost 10`	Configures the OSPF cost for the sa1 interface, setting it to 10.
`PE6(config-if)# load-interval 30`	Configures the load-interval for monitoring traffic on the sa1 interface.
`PE6(config)#interface xe7`	Configure network interface towards PE5.
`PE6(config-if)# static-channel-group 1`	Assigns the static channel group 1 to the xe1 interface.
`PE6(config-if)#ip address 30.1.1.1/24`	Assign IP address to network interface.
`PE6(config)#ip ospf cost 10`	Configures the OSPF cost for the xe7interface, setting it to 10.
`PE6(config)#load-interval 30`	Configures the load-interval for monitoring traffic on the xe5 interface.
`PE6(config)#router ospf 1`	Enters the OSPF configuration mode for OSPF process 1.
`PE6(config-router)# network 30.1.1.0/24 area 0.0.0.0`	Advertises the network 30.1.1.0/24 into OSPF area 0.0.0.0.
`PE6(config-router)# network 40.1.1.0/24 area 0.0.0.0`	Advertises the network 40.1.1.0/24 into OSPF area 0.0.0.0.

Topology for ISIS

The network topology includes various network elements such as routers, customer edge (CE) devices, Service Aggregator (SA) devices, and Provider Edge (PE) routers. The feature enables OSPF and ISIS support on the IRB interfaces, allowing for efficient routing and communication between network devices within the topology.



Single Home VxLAN IRB with ISIS

Configure ISIS

PE2

`PE2(config-if)# interface po1`	Enters configuration mode for po 1.
`PE2(config-if)# ip address 20.1.1.1/24`	Assigns the IP address 20.1.1.1 with a subnet mask of 255.255.255.0 to the interface.
`PE2(config-if)#ip router isis 1`	Enables ISIS routing protocol on the interface with process ID 1.
`PE2(config-if)#load-interval 30`	Sets the interval for which interface statistics are collected to 30 seconds.
`PE2(config)#hardware-profile filter vxlan enable`	Enables the hardware profile filter for VxLAN on the device.
`PE2(config)#nvo vxlan enable`	Enables the VXLAN feature on the device.
`PE2(config)#nvo vxlan irb`	Enables VXLAN IRB functionality.
`PE2(config-vrf)#mac vrf L2VRF2`	Enters the configuration mode for a MAC VRF named L2VRF2.
`PE2(config-vrf)# rd 2.2.2.2:11`	Sets the route distinguisher (RD) for the VRF to 2.2.2.2:11.
`PE2(config-vrf)#route-target both 10.10.10.10:100`	Specifies import and export route targets for the VRF.
`PE2(config-vrf)#ip vrf L3VRF2`	Enters the configuration mode for an IP VRF named L3VRF2.
`PE2(config-vrf)#rd 61000:11`	Sets the RD for the IP VRF to 61000:11
`PE2(config-vrf)# route-target both 101:101`	Specifies import and export route targets for the IP VRF.
`PE2(config-vrf)# l3vni 2000`	Configures the Layer 3 VNI (Virtual Network Identifier) for the IP VRF.
`PE2(config)#interface irb2001`	Enters the configuration mode for interface IRB2001.
`PE2(config-irb-if)# ip vrf forwarding L3VRF2`	Associates the interface with the IP VRF L3VRF2.
`PE2(config-irb-if)# ip address 13.13.13.1/24`	Configures an IP address with a subnet mask of /24 on IRB2001.
`PE2(config-irb-if)#mtu 9000`	Sets the Maximum Transmission Unit (MTU) for the interface to 9000 bytes.
`PE2(config-irb-if)#ip router isis 2`	Associates the interface with ISIS routing process 2.
`PE2(config-irb)#interface irb3001`	Enters the configuration mode for interface IRB3001.
`PE2(config-irb-if)# ip vrf forwarding L3VRF2`	Associates the interface with the IP VRF L3VRF2.
`PE2(config-irb-if)# ipv6 address 3001::1/64`	Configures an IPv6 address on IRB3001 with the specified prefix length.
`PE2(config-irb-if)#mtu 9000`	Sets the MTU for the interface to 9000 bytes.
`PE2(config-irb)#ipv6 router isis 3`	Associates the interface with IPv6 ISIS routing process 3.
`PE2(config)#router isis 2 L3VRF2`	Enters the configuration mode for ISIS routing process 2 within VRF L3VRF2.
`PE2(config-router)#is-type level-1-2`	Specifies the ISIS level type as level-1-2.
`PE2(config-router)#metric-style wide`	Configures a wide metric style for ISIS.
`PE2(config-router)# dynamic-hostname`	Enables dynamic hostname assignment for the ISIS router.
`PE2(config-router)# bfd all-interfaces`	Enables Bidirectional Forwarding Detection (BFD) on all interfaces within ISIS.

`PE2(config-router)#net 49.0000.0000.0221.00`	Configures the network entity title (NET) for the ISIS process.
`PE2(config)#router isis 3 L3VRF2`	Enters the configuration mode for ISIS routing process 3 within VRF L3VRF2.
`PE2(config-router)#is-type level-1-2`	Specifies the ISIS level type as level-1-2.
`PE2(config-router)# metric-style wide`	Configures a wide metric style for ISIS.
`PE2(config-router)# dynamic-hostname`	Enables dynamic hostname assignment for the ISIS router.
`PE2(config-router)#bfd all-interfaces`	Enables BFD on all interfaces within ISIS.
`PE2(config-router)# net 49.0000.0000.0222.00`	Configures the network entity title (NET) for ISIS routing with the specified value.
`PE2(config)#nvo vxlan vtep-ip-global 2.2.2.2`	Configures the global VxLAN VTEP IP address to 2.2.2.2.
`PE2(config)#nvo vxlan id 201 ingress-replication`	Configures a VxLAN with VNI 201 and specifies ingress-replication for multicast traffic handling.
`PE2(config-nvo)# vxlan host-reachability-protocol evpn-bgp L2VRF2`	Specifies the EVPN-BGP host-reachability-protocol for the VxLAN with the VRF L2VRF2
`PE2(config-nvo)# evpn irb2001`	Enables EVPN IRB (Integrated Routing and Bridging) for VxLAN interface IRB2001.
`PE2(config-nvo)# vni-name VNI-201`	Assigns a name VNI-201 to the VxLAN VNI 201.
`PE2(config)#nvo vxlan id 3001 ingress-replication`	Configures another VxLAN with VNI 3001 and specifies ingress-replicationr for multicast traffic handling.
`PE2(config-nvo)# vxlan host-reachability-protocol evpn-bgp L2VRF2`	Specifies the EVPN-BGP host-reachability-protocol for the VxLAN with the VRF L2VRF2.
`PE2(config-nvo)# evpn irb3001`	Enables EVPN IRB for VxLAN interface IRB3001.
`PE2(config-if)#interface xe11`	Enters the configuration mode for the interface 11.
`PE2(config-if)#switchport`	Configures the interface as a Layer 2 switchport.
`PE2(config-if)#load-interval 30`	Sets the interval for which interface statistics are collected to 30 seconds.
`PE2(config-if)#interface xe11.200 switchport`	Enters the configuration mode for subinterface xe11.200 and configures it as a Layer 2 switchport.
`PE2(config-if)#encapsulation dot1q 200`	Sets the IEEE 802.1Q VLAN encapsulation for subinterface xe11.200 with VLAN ID 200.
`PE2(config-if)#rewrite pop`	Configures the subinterface to rewrite the outer header for provider edge devices.
`PE2(config-if)#access-if-evpn`	Configures the subinterface as an access interface for EVPN (Ethernet VPN).
`PE2(config-if)#map vpn-id 201`	Maps the VPN ID 201 to the subinterface for EVPN.
`PE2(config-if)#interface xe11.3001 switchport`	Configures interface xe11.3001.
`PE2(config-if)#encapsulation dot1q 200`	Sets the IEEE 802.1Q VLAN encapsulation for subinterface xe11.200 with VLAN ID 200.
`PE2(config-if)#rewrite pop`	Configures the subinterface to rewrite the outer header for provider edge devices.
`PE2(config-if)#access-if-evpn`	Configures the subinterface as an access interface for EVPN.
`PE2(config-if)#map vpn-id 3001`	Maps the VPN ID 3001 to the subinterface for EVPN.
`PE2(config-if)#router isis 1`	Starts the ISIS routing process with process ID 1.
`PE2(config-if)#is-type level-1-2`	Specifies that the router participates in both Level 1 and Level 2 routing.

`PE2(config-if)#metric-style wide`	Configures the metric style to be wide, enabling more flexibility in metric calculations.
`PE2(config-if)#mpls traffic-eng router-id 2.2.2.2`	Sets the MPLS Traffic Engineering router ID to 2.2.2.2.
`PE2(config-if)#mpls traffic-eng level-1`	Enables MPLS Traffic Engineering for Level 1 ISIS.
`PE2(config-if)#mpls traffic-eng level-2`	Enables MPLS Traffic Engineering for Level 2 ISIS.
`PE2(config-if)#dynamic-hostname`	Enables the dynamic hostname feature for ISIS.
`PE2(config-if)#bfd all-interfaces`	Configures Bidirectional Forwarding Detection on all interfaces.
`PE2(config-if)#net 49.0000.0000.0001.00`	Specifies the network entity title (NET) for ISIS.

BGP Configuration

`PE2(config)#router bgp 100`	Starts the BGP routing process with an autonomous system number (AS) of 100.
`PE2(config-router)#bgp router-id 2.2.2.2`	Sets the BGP router ID to 2.2.2.2.
`PE2(config-router)#neighbor 3.3.3.3 remote-as 100`	Configures a BGP neighbor with the IP address 3.3.3.3 and specifies the remote AS number as 100.
`PE2(config-router)#neighbor 3.3.3.3 update-source lo`	Specifies that loopback interface (lo) is the source for BGP updates to the neighbor.
`PE2(config-router)#neighbor 3.3.3.3 advertisement-interval 0`	Sets the advertisement interval to 0, which means updates will be sent immediately.
`PE2(config-router)#address-family ipv4 unicast`	Enters the configuration mode for the IPv4 unicast address family within the router configuration.
`PE2(config-router-af)#network 2.2.2.2/32`	Specifies that network 2.2.2.2 with a /32 subnet mask is part of the IPv4 unicast address family.
`PE2(config-router-af)#neighbor 3.3.3.3 activate`	Activates the neighbor with the IP address 3.3.3.3 for the IPv4 unicast address family.
`PE2(config-router-af)#exit-address-family`	Exits the configuration mode for the IPv4 unicast address family.
`PE2(config-router)#address-family l2vpn evpn`	Enters the configuration mode for the L2VPN EVPN address family within the router configuration.
`PE2(config-router-af)#neighbor 3.3.3.3 activate`	Activates the neighbor with the IP address 3.3.3.3 for the L2VPN EVPN address family.
`PE2(config-router-af)#exit-address-family`	Exits the configuration mode for the L2VPN EVPN address family.
`PE2(config-router)#address-family ipv4 vrf L3VRF2`	Enters the configuration mode for the IPv4 address family within the VRF named L3VRF2.
`PE2(config-router-af)#redistribute connected`	Configures the redistribution of directly connected routes into the IPv4 address family for the specified VRF.
`PE2(config-router-af)#exit-address-family`	Exits the configuration mode for the IPv4 address family within the VRF L3VRF2.
`PE2(config-router-af)#address-family ipv6 vrf L3VRF2`	Enters the configuration mode for the IPv6 address family within the VRF named L3VRF2.
`PE2(config-router-af)#redistribute connected`	Configures the redistribution of directly connected routes into the IPv6 address family for the specified VRF.
`PE2(config-router-af)#exit-address-family`	Exits the configuration mode for the IPv6 address family within the VRF L3VRF2.

PE5

`PE5(config-if)#interface po1`	Enters the configuration mode for po1.
`PE5(config-if)#ip address 20.1.1.2/24`	Assigns the IP address 20.1.1.2 with a subnet mask of /24 to this interface.
`PE5(config-if)#ip router isis 1`	Specifies that ISIS routing process 1 is enabled on this interface.
`PE5(config-if)#load-interval 30`	Sets the load interval to 30 seconds for monitoring the interface.
`PE5(config-if)#interface ce50`	Enters the configuration mode for ce50.
`PE5(config-if)#ip address 50.1.1.1/24`	Assigns the IP address 50.1.1.1 with a subnet mask of /24 to this interface.
`PE5(config-if)#ip router isis 1`	Specifies that ISIS routing process 1 is enabled on this interface.
`PE5(config-if)#load-interval 30`	Sets the load interval to 30 seconds for monitoring the interface.
`PE5(config-if)#router isis 1`	Enters ISIS configuration mode with process ID 1.
`PE5(config-if)#is-type level-1-2`	Configures this ISIS router to support both Level 1 and Level 2 routing.
`PE5(config-if)#metric-style wide`	Configures ISIS to use the wide metric style, which allows for greater flexibility in metric values.
`PE5(config-if)#dynamic-hostname`	Allows the hostname to be dynamically generated.
`PE5(config-if)#bfd all-interfaces`	Enables Bidirectional Forwarding Detection on all interfaces.
`PE5(config-if)#net 49.0000.0005.0001.00`	Sets the NET for this router.
`PE5(config-if)#exit`	Exits from the router mode.

PE 6

`PE6#configure terminal`	Enters the configuration maode.
`PE6(config-if)#interface xe5`	Enters configuration mode for interface xe5.
`PE6(config-if)#ip address 60.1.1.1/24`	Assigns the IP address 80.1.1.2 with a subnet mask of 255.255.255.0 to interface sa2.
`PE6(config-if)#ip router isis 1`	Associates ISIS routing protocol with this interface using process ID 1.
`PE6(config-if)#load-interval 30`	Sets the load-interval to 30 seconds.
`PE6(config-if)#interface ce1`	Enters configuration mode for interface ce1.
`PE6(config-if)#ip address 50.1.1.2/24`	Assigns the IP address 50.1.1.2 with a subnet mask of 255.255.255.0 to interface ce1.
`PE6(config-if)#ip router isis 1`	Associates ISIS routing protocol with this interface using process ID 1.
`PE6(config-if)#load-interval 30`	Sets the load-interval to 30 seconds.
`PE6(config-if)#router isis 1`	Enters ISIS configuration mode with process ID 1.
`PE6(config-if)#is-type level-1-2`	Configures this ISIS router to support both Level 1 and Level 2 routing.
`PE6(config-if)#metric-style wide`	Configures ISIS to use the wide metric style, which allows for greater flexibility in metric values.

PE6(config-if)#dynamic-hostname	Allows the hostname to be dynamically generated.
PE6(config-if)#bfd all-interfaces	Enable BFD on all network interfaces.

PE4

PE4#configure terminal	Enters the configuration mode.
PE4(config-if)# interface xe26	Enters configuration mode for xe26.
PE4(config-if)# ip address 60.1.1.2/24	Assigns the IP address 60.1.1.2 with a subnet mask of 255.255.255.0 to the interface.
PE4(config-if)#ip router isis 1	Enables ISIS routing protocol on the interface with process ID 1.
PE4(config-if)#ip router isis 1	Enables ISIS routing protocol on the interface with process ID 1.
PE4(config-if)#load-interval 30	Sets the interval for which interface statistics are collected to 30 seconds.
PE4(config)#hardware-profile filter vxlan enable	Enables the hardware profile filter for VXLAN.
PE4(config)#nvo vxlan enable	Enables the VXLAN feature on the device.
PE4(config)#nvo vxlan irb	Enables VXLAN IRB functionality.
PE4(config-vrf)#mac vrf L2VRF2	Configures a VRF instance named L2VRF2 and associates it with a specific RD
PE4(config-vrf)# rd 3.3.3.3:11	Sets the RD for the L2VRF2 VRF to 3.3.3.3:11.
PE4(config-vrf)#route-target both 10.10.10.10:100	Associates a route target with the L2VRF2 VRF for VPN route distribution.
PE4(config-vrf)#ip vrf L3VRF2	Configures another VRF named L3VRF2.
PE4(config-vrf)#rd 63000:11	Sets the RD for the L3VRF2 VRF to 63000:11.
PE4(config-vrf)# route-target both 101:101	Associates a route target with the L3VRF2 VRF for VPN route distribution.
PE4(config-vrf)# l3vni 2000	Configures the L3VNI for the L3VRF2 VRF.
PE4(config)#interface irb2001	Configuring an IRB interface with the number 2001.
PE4(config-irb-if)# ip vrf forwarding L3VRF2	Associates the IRB interface with the L3VRF2 VRF.
PE4(config-irb-if)# ip address 14.14.14.1/24	Assigns an IP address to the IRB interface.
PE4(config-irb-if)#mtu 9000	Sets the MTU for the IRB interface.
PE4(config-irb-if)#ip router isis 2	Associates the IRB interface with ISIS routing.
PE4(config-irb)#interface irb3002	Configures another IRB interface with the number 3002.
PE4(config-irb-if)# ip vrf forwarding L3VRF2	Associates the second IRB interface with the "L3VRF2" VRF.
PE4(config-irb-if)# ipv6 address 3002::1/64	Assigns an IPv6 address to the second IRB interface.
PE4(config-irb-if)#mtu 9000	Sets the MTU for the second IRB interface.
PE4(config-irb)#ipv6 router isis 3	Associates the IRB interfaces with IPv6 and ISIS routing.
PE4(config)#router isis 2 L3VRF2	Configures ISIS routing with the VRF L3VRF2.
PE4(config-router)#is-type level-1-2	Sets the ISIS level type to level-1-2.
PE4(config-router)# metric-style wide	Configures a wide metric style for ISIS.
PE4(config-router)# dynamic-hostname	Enables dynamic hostname assignment for the ISIS router.
PE4(config-router)#bfd all-interfaces	Enables BFD on all interfaces within ISIS.

`PE4(config-router)# net 49.0000.0000.0441.00`	Configures the network entity title (NET) for ISIS routing with the specified value.
`PE4(config)#router isis 3 L3VRF2`	Configures ISIS routing with the VRF L3VRF2.
`PE4(config-router)#is-type level-1-2`	Sets the ISIS level type to level-1-2.
`PE4(config-router)# metric-style wide`	Configures a wide metric style for ISIS.
`PE4(config-router)# dynamic-hostname`	Enables dynamic hostname assignment for the ISIS router.
`PE4(config-router)#bfd all-interfaces`	Enables BFD on all interfaces within ISIS.
`PE4(config-router)# net 49.0000.0000.0442.00`	Configures the network entity title (NET) for ISIS routing with the specified value.
`PE4(config)#nvo vxlan vtep-ip-global 3.3.3.3`	Configures the global VxLAN VTEP IP address to 3.3.3.3.
`PE4(config)#nvo vxlan id 201 ingress-replication`	Configures a VxLAN with VNI 201 and specifies ingress-replication for multicast traffic handling.
`PE4(config-nvo)# vxlan host-reachability-protocol evpn-bgp L2VRF2`	Specifies the EVPN-BGP host-reachability-protocol for the VxLAN with the VRF L2VRF2
`PE4(config-nvo)# evpn irb2001`	Enables EVPN IRB (Integrated Routing and Bridging) for VxLAN interface IRB2001.
`PE4(config-nvo)# vni-name VNI-201`	Assigns a name VNI-201 to the VxLAN VNI 201.
`PE4(config)#nvo vxlan id 3002 ingress-replication`	Configures another VxLAN with VNI 3002 and specifies ingress-replicationr for multicast traffic handling.
`PE4(config-nvo)# vxlan host-reachability-protocol evpn-bgp L2VRF2`	Specifies the EVPN-BGP host-reachability-protocol for the VxLAN with the VRF L2VRF2.
`PE4(config-nvo)# evpn irb3002`	Enables EVPN IRB for VxLAN interface IRB3002
`PE4(config-if)#interface xe26`	Enters the configuration mode for the interface 26.
`PE4(config-if)#switchport`	Configures the interface as a L2 switchport.
`PE4(config-if)#load-interval 30`	Sets the interval for which interface statistics are collected to 30 seconds.
`PE4(config)#hardware-profile filter vxlan enable`	Enables the hardware profile filter for VxLAN on the device.
`PE4(config-if)#interface xe26.200 switchport`	Enters the configuration mode for subinterface xe26.200 and configures it as a Layer 2 switchport.
`PE4(config-if)#encapsulation dot1q 200`	Sets the IEEE 802.1Q VLAN encapsulation for subinterface xe11.200 with VLAN ID 200.
`PE4(config-if)#rewrite pop`	Configures the subinterface to rewrite the outer header for provider edge devices.
`PE4(config-if)#access-if-evpn`	Configures the subinterface as an access interface for EVPN (Ethernet VPN).
`PE4(config-if)#map vpn-id 201`	Maps the VPN ID 201 to the subinterface for EVPN.
`PE4(config-if)#interface xe26.3001 switchport`	Configures xe26.3001 interface.
`PE4(config-if)#encapsulation dot1q 200`	Sets the IEEE 802.1Q VLAN encapsulation for subinterface xe11.200 with VLAN ID 200.
`PE4(config-if)#rewrite pop`	Configures the subinterface to rewrite the outer header for provider edge devices.
`PE4(config-if)#access-if-evpn`	Configures the subinterface as an access interface for EVPN.
`PE4(config-if)#map vpn-id 3002`	Maps the VPN ID 3002 to the subinterface for EVPN.
`PE4(config-if)#router isis 1`	Starts the ISIS routing process with process ID 1.

`PE4(config-if)#is-type level-1-2`	Specifies that the router participates in both Level 1 and Level 2 routing.
`PE4(config-if)#metric-style wide`	Configures the metric style to be wide, enabling more flexibility in metric calculations.
`PE4(config-if)#mpls traffic-eng router-id 2.2.2.2`	Sets the MPLS Traffic Engineering router ID to 2.2.2.2.
`PE4(config-if)#mpls traffic-eng level-1`	Enables MPLS Traffic Engineering for Level 1 ISIS.
`PE4(config-if)#mpls traffic-eng level-2`	Enables MPLS Traffic Engineering for Level 2 ISIS.
`PE4(config-if)#dynamic-hostname`	Enables the dynamic hostname feature for ISIS.
`PE4(config-if)#bfd all-interfaces`	Configures Bidirectional Forwarding Detection on all interfaces.
`PE4(config-if)#net 49.0000.0003.0001.00`	Specifies the network entity title (NET) for ISIS.

BGP Configuration

`PE4(config)#router bgp 100`	Starts the BGP routing process with an autonomous system number (AS) of 100.
`PE4(config-router)#bgp router-id 3.3.3.3`	Sets the BGP router ID to 3.3.3.3
`PE4(config-router)#neighbor 2.2.2.2 remote-as 100`	Configures a BGP neighbor with the IP address 2.2.2.2 and specifies the remote AS number as 100.
`PE4(config-router)#neighbor 2.2.2.2 update-source lo`	Specifies that loopback interface (lo) is the source for BGP updates to the neighbor.
`PE4(config-router)#neighbor 2.2.2.2 advertisement-interval 0`	Sets the advertisement interval to 0, which means updates will be sent immediately.
`PE4(config-router)#address-family ipv4 unicast`	Enters the configuration mode for the IPv4 unicast address family within the router configuration.
`PE4(config-router-af)#network 3.3.3.3/32`	Specifies that network 3.3.3.3 with a /32 subnet mask is part of the IPv4 unicast address family.
`PE4(config-router-af)#neighbor 2.2.2.2 activate`	Activates the neighbor with the IP address 2.2.2.2 for the IPv4 unicast address family.
`PE4(config-router-af)#exit-address-family`	Exits the configuration mode for the IPv4 unicast address family.
`PE4(config-router)#address-family l2vpn evpn`	Enters the configuration mode for the L2VPN EVPN address family within the router configuration.
`PE4(config-router-af)#neighbor 2.2.2.32 activate`	Activates the neighbor with the IP address 2.2.2.2 for the L2VPN EVPN address family.
`PE4(config-router-af)#exit-address-family`	Exits the configuration mode for the L2VPN EVPN address family.
`PE4(config-router)#address-family ipv4 vrf L3VRF2`	Enters the configuration mode for the IPv4 address family within the VRF named L3VRF2.
`PE4(config-router-af)#redistribute connected`	Configures the redistribution of directly connected routes into the IPv4 address family for the specified VRF.
`PE4(config-router-af)#exit-address-family`	Exits the configuration mode for the IPv4 address family within the VRF L3VRF2.
`PE4(config-router-af)#address-family ipv6 vrf L3VRF2`	Enters the configuration mode for the IPv6 address family within the VRF named L3VRF2.

`PE4(config-router-af)#redistribute connected`	Configures the redistribution of directly connected routes into the IPv6 address family for the specified VRF.
`PE4(config-router-af)#exit-address-family`	Exits the configuration mode for the IPv6 address family within the VRF L3VRF2.

Implementation Examples

Scenario: Configure OSPF and ISIS protocols on an IRB interface with an assigned IP address.

Validation

OSPF Validation

```
PE1#show ip ospf neighbor
Total number of full neighbors: 1
OSPF process 1 VRF(default):
Neighbor ID     Pri   State            Dead Time   Address         Interface
       Instance ID
50.1.1.1          1   Full/DR          00:00:38    10.1.1.2        sa1
           0

Total number of full neighbors: 1
OSPF process 2 VRF(L3VRF1):
Neighbor ID     Pri   State            Dead Time   Address         Interface
       Instance ID
192.0.0.1         0   Full/DROther     00:00:34    11.11.11.2      irb1001
           0
PE1#show nvo vxlan tunnel
VXLAN Network tunnel Entries
Source           Destination      Status        Up/Down       Update
================================================================================
1.1.1.1          4.4.4.4          Installed     00:15:59      00:15:59

Total number of entries are 2
PE1#show nvo vxlan irb-status
IRB is ACTIVE in Hardware
PE1#show nvo vxlan arp-cache
VXLAN ARP-CACHE Information
============================
VNID     Ip-Addr          Mac-Addr       Type        Age-Out    Retries-Left
________________________________________________________________________________
101      11.11.11.1       9819.2ccd.9301 Static Local   ----
101      11.11.11.2       0010.9400.0001 Dynamic Local  ----
Total number of entries are 2
PE1#show ip route vrf all
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, 00:53:03
O            4.4.4.4/32 [110/31] via 10.1.1.2, sa1, 00:16:29
O            7.7.7.7/32 [110/12] via 10.1.1.2, sa1, 00:44:26
C            10.1.1.0/24 is directly connected, sa1, 00:50:10
O            30.1.1.0/24 [110/20] via 10.1.1.2, sa1, 00:44:22
O            40.1.1.0/24 [110/30] via 10.1.1.2, sa1, 00:17:14
O            70.1.1.0/24 [110/11] via 10.1.1.2, sa1, 00:45:18
C            127.0.0.0/8 is directly connected, lo, 00:53:03
IP Route Table for VRF "management"
C            10.12.98.0/24 is directly connected, eth0, 00:53:03
C            127.0.0.0/8 is directly connected, lo.management, 00:53:03
IP Route Table for VRF "L2VRF1"
IP Route Table for VRF "L3VRF1"
B            4.4.4.4/32 [0/0] is directly connected, tunvxlan2, 00:16:25
B            7.7.7.7/32 [0/0] is directly connected, tunvxlan2, 00:44:21
C            11.11.11.0/24 is directly connected, irb1001, 00:53:03
B            12.12.12.0/24 [200/0] via 4.4.4.4 (recursive is directly connected,
 tunvxlan2), 00:16:26
B            16.16.16.0/24 [200/0] via 7.7.7.7 (recursive is directly connected,
 tunvxlan2), 00:44:21
C            127.0.0.0/8 is directly connected, lo.L3VRF1, 00:53:03

Gateway of last resort is not set


PE1#show bgp l2vpn evpn
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

[EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route
5 - Prefix Route

    Network          Next Hop          Metric    LocPrf    Weight     Path Peer       Encap

RD[7100:11]
*>i  [5]:[0]:[0]:[24]:[16.16.16.0]:[0.0.0.0]:[1000]
```

```
                     7.7.7.7             0        100       0    i  7.7.7.7       VXLAN
*>i  [5]:[0]:[0]:[64]:[7002::]:[::]:[1000]
                     7.7.7.7             0        100       0    i  7.7.7.7       VXLAN

RD[56000:11]
*>i  [5]:[0]:[0]:[24]:[12.12.12.0]:[0.0.0.0]:[1000]
                     4.4.4.4             0        100       0    ?  4.4.4.4       VXLAN
*>i  [5]:[0]:[0]:[64]:[2002::]:[::]:[1000]
                     4.4.4.4             0        100       0    ?  4.4.4.4       VXLAN

RD[1.1.1.1:11] VRF[L2VRF1]:
*>   [2]:[0]:[101]:[48,0010:9400:0001]:[0]:[101]
                    1.1.1.1             0        100      32768  i  ---------     VXLAN
*>   [2]:[0]:[101]:[48,0010:9400:0001]:[32,11.11.11.2]:[101]
                    1.1.1.1             0        100      32768  i  ---------     VXLAN
*>   [2]:[0]:[101]:[48,9819:2ccd:9301]:[32,11.11.11.1]:[101]
                    1.1.1.1             0        100      32768  i  ---------     VXLAN
* i  [2]:[0]:[102]:[48,0010:9400:0002]:[0]:[102]
                     4.4.4.4             0        100       0    i  4.4.4.4       VXLAN
* i  [2]:[0]:[102]:[48,0010:9400:0002]:[32,12.12.12.2]:[102]
                     4.4.4.4             0        100       0    i  4.4.4.4       VXLAN
* i  [2]:[0]:[102]:[48,5c07:5813:425e]:[32,12.12.12.1]:[102]
                     4.4.4.4             0        100       0    i  4.4.4.4       VXLAN
*>   [2]:[0]:[2001]:[48,0010:9400:0009]:[0]:[2001]
                    1.1.1.1             0        100      32768  i  ---------     VXLAN
*>   [2]:[0]:[2001]:[48,0010:9400:0009]:[128,2001::2][2001]
                    1.1.1.1             0        100      32768  i  ---------     VXLAN
*>   [2]:[0]:[2001]:[48,9819:2ccd:9301]:[128,2001::1][2001]
                    1.1.1.1             0        100      32768  i  ---------     VXLAN
* i  [2]:[0]:[2002]:[48,0010:9400:000a]:[0]:[2002]
                     4.4.4.4             0        100       0    i  4.4.4.4       VXLAN
* i  [2]:[0]:[2002]:[48,0010:9400:000a]:[128,2002::2][2002]
                     4.4.4.4             0        100       0    i  4.4.4.4       VXLAN
* i  [2]:[0]:[2002]:[48,5c07:5813:425e]:[128,2002::1][2002]
                     4.4.4.4             0        100       0    i  4.4.4.4       VXLAN
*>   [3]:[101]:[32,1.1.1.1]
                    1.1.1.1             0        100      32768  i  ---------     VXLAN
* i  [3]:[102]:[32,4.4.4.4]
                     4.4.4.4             0        100       0    i  4.4.4.4       VXLAN
*>   [3]:[2001]:[32,1.1.1.1]
                    1.1.1.1             0        100      32768  i  ---------     VXLAN
* i  [3]:[2002]:[32,4.4.4.4]
                     4.4.4.4             0        100       0    i  4.4.4.4       VXLAN

RD[4.4.4.4:11]
*>i  [2]:[0]:[102]:[48,0010:9400:0002]:[0]:[102]
                     4.4.4.4             0        100       0    i  4.4.4.4       VXLAN
*>i  [2]:[0]:[102]:[48,0010:9400:0002]:[32,12.12.12.2]:[102]
                     4.4.4.4             0        100       0    i  4.4.4.4       VXLAN
*>i  [2]:[0]:[102]:[48,5c07:5813:425e]:[32,12.12.12.1]:[102]
```

```
                      4.4.4.4             0        100       0    i  4.4.4.4       VXLAN
*>i  [2]:[0]:[2002]:[48,0010:9400:000a]:[0]:[2002]
                      4.4.4.4             0        100       0    i  4.4.4.4       VXLAN
*>i  [2]:[0]:[2002]:[48,0010:9400:000a]:[128,2002::2][2002]
                      4.4.4.4             0        100       0    i  4.4.4.4       VXLAN
*>i  [2]:[0]:[2002]:[48,5c07:5813:425e]:[128,2002::1][2002]
                      4.4.4.4             0        100       0    i  4.4.4.4       VXLAN
*>i  [3]:[102]:[32,4.4.4.4]
                      4.4.4.4             0        100       0    i  4.4.4.4       VXLAN
*>i  [3]:[2002]:[32,4.4.4.4]
                      4.4.4.4             0        100       0    i  4.4.4.4       VXLAN

Total number of prefixes 28

PE3#show nvo vxlan tunnel
VXLAN Network tunnel Entries
Source           Destination      Status        Up/Down       Update
=============================================================================
4.4.4.4          1.1.1.1          Installed     00:18:19      00:18:19

Total number of entries are 1
PE3#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 1 VRF(default):
Neighbor ID     Pri   State            Dead Time   Address         Interface
       Instance ID
40.1.1.2          1   Full/DR          00:00:36    40.1.1.1        ce30
           0

Total number of full neighbors: 1
OSPF process 2 VRF(L3VRF1):
Neighbor ID     Pri   State            Dead Time   Address         Interface
       Instance ID
192.0.0.2         0   Full/DROther     00:00:36    12.12.12.2      irb1001
           0
PE3#show ip route vrf all
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 [110/31] via 40.1.1.1, ce30, 00:18:35
C            4.4.4.4/32 is directly connected, lo, 00:19:22
O            7.7.7.7/32 [110/22] via 40.1.1.1, ce30, 00:18:35
```

```
O            10.1.1.0/24 [110/30] via 40.1.1.1, ce30, 00:18:35
O            30.1.1.0/24 [110/20] via 40.1.1.1, ce30, 00:18:35
C            40.1.1.0/24 is directly connected, ce30, 00:19:21
O            70.1.1.0/24 [110/21] via 40.1.1.1, ce30, 00:18:35
C            127.0.0.0/8 is directly connected, lo, 00:20:05
IP Route Table for VRF "management"
C            10.12.98.0/24 is directly connected, eth0, 00:19:19
C            127.0.0.0/8 is directly connected, lo.management, 00:20:05
IP Route Table for VRF "L3VRF1"
B            1.1.1.1/32 [0/0] is directly connected, tunvxlan2, 00:18:31
B            11.11.11.0/24 [200/0] via 1.1.1.1 (recursive is directly connected,
 tunvxlan2), 00:18:32
C            12.12.12.0/24 is directly connected, irb1001, 00:19:28
C            127.0.0.0/8 is directly connected, lo.L3VRF1, 00:19:29
IP Route Table for VRF "L2VRF1"

Gateway of last resort is not set
PE3# show bgp l2vpn evpn
BGP table version is 4, local router ID is 4.4.4.4
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

[EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route
5 - Prefix Route

    Network          Next Hop       Metric    LocPrf     Weight  Path Peer      Encap

RD[51000:11]
*>i  [5]:[0]:[0]:[24]:[11.11.11.0]:[0.0.0.0]:[1000]
                     1.1.1.1             0        100       0    ?  1.1.1.1       VXLAN
*>i  [5]:[0]:[0]:[64]:[2001::]:[::]:[1000]
                     1.1.1.1             0        100       0    ?  1.1.1.1       VXLAN

RD[1.1.1.1:11]
*>i  [2]:[0]:[101]:[48,0010:9400:0001]:[0]:[101]
                     1.1.1.1             0        100       0    i  1.1.1.1       VXLAN
*>i  [2]:[0]:[101]:[48,0010:9400:0001]:[32,11.11.11.2]:[101]
                     1.1.1.1             0        100       0    i  1.1.1.1       VXLAN
*>i  [2]:[0]:[101]:[48,9819:2ccd:9301]:[32,11.11.11.1]:[101]
                     1.1.1.1             0        100       0    i  1.1.1.1       VXLAN
*>i  [2]:[0]:[2001]:[48,0010:9400:0009]:[0]:[2001]
                     1.1.1.1             0        100       0    i  1.1.1.1       VXLAN
*>i  [2]:[0]:[2001]:[48,0010:9400:0009]:[128,2001::2][2001]
                     1.1.1.1             0        100       0    i  1.1.1.1       VXLAN
```

```
*>i  [2]:[0]:[2001]:[48,9819:2ccd:9301]:[128,2001::1][2001]
                     1.1.1.1             0        100       0    i  1.1.1.1       VXLAN
*>i  [3]:[101]:[32,1.1.1.1]
                     1.1.1.1             0        100       0    i  1.1.1.1       VXLAN
*>i  [3]:[2001]:[32,1.1.1.1]
                     1.1.1.1             0        100       0    i  1.1.1.1       VXLAN

RD[4.4.4.4:11] VRF[L2VRF1]:
* i  [2]:[0]:[101]:[48,0010:9400:0001]:[0]:[101]
                     1.1.1.1             0        100       0    i  1.1.1.1       VXLAN
* i  [2]:[0]:[101]:[48,0010:9400:0001]:[32,11.11.11.2]:[101]
                     1.1.1.1             0        100       0    i  1.1.1.1       VXLAN
* i  [2]:[0]:[101]:[48,9819:2ccd:9301]:[32,11.11.11.1]:[101]
                     1.1.1.1             0        100       0    i  1.1.1.1       VXLAN
*>   [2]:[0]:[102]:[48,0010:9400:0002]:[0]:[102]
                    4.4.4.4             0       100      32768  i  ---------      VXLAN
*>   [2]:[0]:[102]:[48,0010:9400:0002]:[32,12.12.12.2]:[102]
                    4.4.4.4             0       100      32768  i  ---------      VXLAN
*>   [2]:[0]:[102]:[48,5c07:5813:425e]:[32,12.12.12.1]:[102]
                     4.4.4.4             0        100       32768  i  ----------
VXLAN
* i  [2]:[0]:[2001]:[48,0010:9400:0009]:[0]:[2001]
                     1.1.1.1             0        100       0    i  1.1.1.1       VXLAN
* i  [2]:[0]:[2001]:[48,0010:9400:0009]:[128,2001::2][2001]
                     1.1.1.1             0        100       0    i  1.1.1.1       VXLAN
* i  [2]:[0]:[2001]:[48,9819:2ccd:9301]:[128,2001::1][2001]
                     1.1.1.1             0        100       0    i  1.1.1.1       VXLAN
*>   [2]:[0]:[2002]:[48,0010:9400:000a]:[0]:[2002]
                    4.4.4.4             0       100      32768  i  ---------      VXLAN
*>   [2]:[0]:[2002]:[48,0010:9400:000a]:[128,2002::2][2002]
                    4.4.4.4             0       100      32768  i  ---------      VXLAN
*>   [2]:[0]:[2002]:[48,5c07:5813:425e]:[128,2002::1][2002]
                    4.4.4.4             0       100      32768  i  ---------      VXLAN
* i  [3]:[101]:[32,1.1.1.1]
                     1.1.1.1             0        100       0    i  1.1.1.1       VXLAN
*>   [3]:[102]:[32,4.4.4.4]
                    4.4.4.4             0       100      32768  i  ---------      VXLAN
* i  [3]:[2001]:[32,1.1.1.1]
                     1.1.1.1             0        100       0    i  1.1.1.1       VXLAN
*>   [3]:[2002]:[32,4.4.4.4]
                    4.4.4.4             0       100      32768  i  ---------      VXLAN

Total number of prefixes 26
```

ISIS Validation

```
PE2#show nvo vxlan tunnel
VXLAN Network tunnel Entries
Source           Destination      Status        Up/Down       Update
=================================================================
2.2.2.2          3.3.3.3          Installed     00:00:10      00:00:10
```

```
Total number of entries are 1
PE2#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 1
Total number of adjacencies: 2
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
PE5            po1         b86a.9725.a7f2  Up     28        L1   IS-IS
                                           Up     28        L2   IS-IS

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag 2:  VRF : L3VRF2
System Id      Interface   SNPA            State  Holdtime  Type Protocol
Spirent-1      irb2001     0010.9400.0003  Up     28        L2   IS-IS

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag 3:  VRF : L3VRF2
System Id      Interface   SNPA            State  Holdtime  Type Protocol
Spirent-1      irb3001     0010.9400.000c  Up     28        L2   IS-IS
PE2#show ip route vrf all
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            2.2.2.2/32 is directly connected, lo, 02:13:57
i L2         3.3.3.3/32 [115/30] via 20.1.1.2, po1, 00:00:32
i L1         7.7.7.7/32 [115/40] via 20.1.1.2, po1, 01:05:49
C            20.1.1.0/24 is directly connected, po1, 02:13:21
i L1         50.1.1.0/24 [115/20] via 20.1.1.2, po1, 01:06:05
i L1         60.1.1.0/24 [115/30] via 20.1.1.2, po1, 00:00:47
i L1         80.1.1.0/24 [115/30] via 20.1.1.2, po1, 01:05:49
C            127.0.0.0/8 is directly connected, lo, 02:13:57
IP Route Table for VRF "management"
C            10.12.98.0/24 is directly connected, eth0, 02:13:57
C            127.0.0.0/8 is directly connected, lo.management, 02:13:57
IP Route Table for VRF "L3VRF2"
B            3.3.3.3/32 [0/0] is directly connected, tunvxlan2, 00:00:28
C            13.13.13.0/24 is directly connected, irb2001, 02:13:57
```

```
B            14.14.14.0/24 [200/0] via 3.3.3.3 (recursive is directly connected,
 tunvxlan2), 00:00:28
C            127.0.0.0/8 is directly connected, lo.L3VRF2, 02:13:57
IP Route Table for VRF "L2VRF2"

Gateway of last resort is not set
PE2# show bgp l2vpn evpn
BGP table version is 2, local router ID is 2.2.2.2
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

[EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route
5 - Prefix Route

    Network          Next Hop          Metric    LocPrf    Weight   Path Peer         Encap

RD[63000:11]
*>i  [5]:[0]:[0]:[24]:[14.14.14.0]:[0.0.0.0]:[2000]
                      3.3.3.3             0        100       0    ?  3.3.3.3       VXLAN
*>i  [5]:[0]:[0]:[64]:[3002::]:[::]:[2000]
                      3.3.3.3             0        100       0    ?  3.3.3.3       VXLAN

RD[2.2.2.2:11] VRF[L2VRF2]:
*>   [2]:[0]:[201]:[48,0010:9400:0003]:[0]:[201]
                     2.2.2.2             0       100      32768  i  ---------      VXLAN
*>   [2]:[0]:[201]:[48,0010:9400:0003]:[32,13.13.13.2]:[201]
                     2.2.2.2             0       100      32768  i  ---------      VXLAN
* i  [2]:[0]:[201]:[48,0010:9400:0005]:[0]:[201]
                      3.3.3.3             0        100       0    i  3.3.3.3       VXLAN
* i  [2]:[0]:[201]:[48,0010:9400:0005]:[32,14.14.14.2]:[201]
                      3.3.3.3             0        100       0    i  3.3.3.3       VXLAN
*>   [2]:[0]:[201]:[48,e8c5:7a76:581d]:[32,13.13.13.1]:[201]
                     2.2.2.2             0       100      32768  i  ---------      VXLAN
* i  [2]:[0]:[201]:[48,e8c5:7aa8:7cb3]:[32,14.14.14.1]:[201]
                      3.3.3.3             0        100       0    i  3.3.3.3       VXLAN
*>   [2]:[0]:[3001]:[48,0010:9400:000c]:[0]:[3001]
                     2.2.2.2             0       100      32768  i  ---------      VXLAN
*>   [2]:[0]:[3001]:[48,0010:9400:000c]:[128,3001::2][3001]
                     2.2.2.2             0       100      32768  i  ---------      VXLAN
*>   [2]:[0]:[3001]:[48,e8c5:7a76:581d]:[128,3001::1][3001]
                     2.2.2.2             0       100      32768  i  ---------      VXLAN
* i  [2]:[0]:[3002]:[48,0010:9400:000b]:[0]:[3002]
                      3.3.3.3             0        100       0    i  3.3.3.3       VXLAN
* i  [2]:[0]:[3002]:[48,0010:9400:000b]:[128,3002::2][3002]
```

```
                      3.3.3.3              0        100       0    i  3.3.3.3       VXLAN
* i  [2]:[0]:[3002]:[48,e8c5:7aa8:7cb3]:[128,3002::1][3002]
                      3.3.3.3              0        100       0    i  3.3.3.3       VXLAN
*>   [3]:[201]:[32,2.2.2.2]
                     2.2.2.2             0        100       32768  i  ---------     VXLAN
* i  [3]:[201]:[32,3.3.3.3]
                      3.3.3.3              0        100       0    i  3.3.3.3       VXLAN
*>   [3]:[3001]:[32,2.2.2.2]
                     2.2.2.2             0        100       32768  i  ---------     VXLAN
* i  [3]:[3002]:[32,3.3.3.3]
                      3.3.3.3              0        100       0    i  3.3.3.3       VXLAN

RD[3.3.3.3:11]
*>i  [2]:[0]:[201]:[48,0010:9400:0005]:[0]:[201]
                      3.3.3.3              0        100       0    i  3.3.3.3       VXLAN
*>i  [2]:[0]:[201]:[48,0010:9400:0005]:[32,14.14.14.2]:[201]
                      3.3.3.3              0        100       0    i  3.3.3.3       VXLAN
*>i  [2]:[0]:[201]:[48,e8c5:7aa8:7cb3]:[32,14.14.14.1]:[201]
                      3.3.3.3              0        100       0    i  3.3.3.3       VXLAN
*>i  [2]:[0]:[3002]:[48,0010:9400:000b]:[0]:[3002]
                      3.3.3.3              0        100       0    i  3.3.3.3       VXLAN
*>i  [2]:[0]:[3002]:[48,0010:9400:000b]:[128,3002::2][3002]
                      3.3.3.3              0        100       0    i  3.3.3.3       VXLAN
*>i  [2]:[0]:[3002]:[48,e8c5:7aa8:7cb3]:[128,3002::1][3002]
                      3.3.3.3              0        100       0    i  3.3.3.3       VXLAN
*>i  [3]:[201]:[32,3.3.3.3]
                      3.3.3.3              0        100       0    i  3.3.3.3       VXLAN
*>i  [3]:[3002]:[32,3.3.3.3]
                      3.3.3.3              0        100       0    i  3.3.3.3       VXLAN

Total number of prefixes 26
PE2# show nvo vxlan arp-
arp-cache  arp-nd
PE2# show nvo vxlan arp-cache
VXLAN ARP-CACHE Information
===========================
VNID     Ip-Addr          Mac-Addr       Type        Age-Out    Retries-Left
_____________________________________________________________________________
201      13.13.13.1       e8c5.7a76.581d Static Local   ----
201      13.13.13.2       0010.9400.0003 Dynamic Local  ----
201      14.14.14.1       e8c5.7aa8.7cb3 Static Remote  ----
201      14.14.14.2       0010.9400.0005 Dynamic Remote ----
Total number of entries are 4
PE2#show nvo vxlan irb-status
IRB is ACTIVE in Hardware
PE2#

PE4#show nvo vxlan tunnel
VXLAN Network tunnel Entries
Source           Destination      Status        Up/Down       Update
```

```
========================================================================
3.3.3.3          7.7.7.7          Installed     00:01:28      00:01:28
3.3.3.3          2.2.2.2          Installed     00:01:28      00:01:28

Total number of entries are 2
PE4#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 1
Total number of adjacencies: 2
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
PE6            xe5         00e0.4b71.f12c      Up     25        L1   IS-IS
                                               Up     25        L2   IS-IS

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag 2:  VRF : L3VRF2
System Id      Interface   SNPA            State  Holdtime  Type Protocol
Spirent-1      irb2001     0010.9400.0005      Up     28        L2   IS-IS

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag 3:  VRF : L3VRF2
System Id      Interface   SNPA            State  Holdtime  Type Protocol
Spirent-1      irb3002     0010.9400.000b      Up     28        L2   IS-IS
PE4#show ip route vrf all
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"
i L2         2.2.2.2/32 [115/30] via 60.1.1.1, xe5, 00:01:46
C            3.3.3.3/32 is directly connected, lo, 02:09:52
i L1         7.7.7.7/32 [115/30] via 60.1.1.1, xe5, 00:01:46
i L1         20.1.1.0/24 [115/30] via 60.1.1.1, xe5, 00:01:46
i L1         50.1.1.0/24 [115/20] via 60.1.1.1, xe5, 00:01:46
C            60.1.1.0/24 is directly connected, xe5, 00:02:02
i L1         80.1.1.0/24 [115/20] via 60.1.1.1, xe5, 00:01:46
C            127.0.0.0/8 is directly connected, lo, 02:09:52
IP Route Table for VRF "management"
C            10.12.98.0/24 is directly connected, eth0, 02:09:52
C            127.0.0.0/8 is directly connected, lo.management, 02:09:52
```

```
IP Route Table for VRF "L3VRF2"
B            2.2.2.2/32 [0/0] is directly connected, tunvxlan2, 00:01:42
B            7.7.7.7/32 [0/0] is directly connected, tunvxlan2, 00:01:42
B            13.13.13.0/24 [200/0] via 2.2.2.2 (recursive is directly connected,
tunvxlan2), 00:01:42
C            14.14.14.0/24 is directly connected, irb2001, 02:09:52
B            17.17.17.0/24 [200/0] via 7.7.7.7 (recursive is directly connected,
tunvxlan2), 00:01:42
C            127.0.0.0/8 is directly connected, lo.L3VRF2, 02:09:52
IP Route Table for VRF "L2VRF2"

Gateway of last resort is not set
PE4# show bgp l2vpn evpn
BGP table version is 3, 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

[EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route
5 - Prefix Route

    Network          Next Hop            Metric    LocPrf      Weight     Path  Peer  Encap

RD[7400:11]
*>i  [5]:[0]:[0]:[24]:[17.17.17.0]:[0.0.0.0]:[2000]
                     7.7.7.7             0         100       0    i  7.7.7.7         VXLAN
*>i  [5]:[0]:[0]:[64]:[8002::]:[::]:[2000]
                     7.7.7.7             0         100       0    i  7.7.7.7         VXLAN

RD[61000:11]
*>i  [5]:[0]:[0]:[24]:[13.13.13.0]:[0.0.0.0]:[2000]
                     2.2.2.2             0         100       0    ?  2.2.2.2         VXLAN
*>i  [5]:[0]:[0]:[64]:[3001::]:[::]:[2000]
                     2.2.2.2             0         100       0    ?  2.2.2.2         VXLAN

RD[2.2.2.2:11]
*>i  [2]:[0]:[201]:[48,0010:9400:0003]:[0]:[201]
                     2.2.2.2             0         100       0    i  2.2.2.2         VXLAN
*>i  [2]:[0]:[201]:[48,0010:9400:0003]:[32,13.13.13.2]:[201]
                     2.2.2.2             0         100       0    i  2.2.2.2         VXLAN
*>i  [2]:[0]:[201]:[48,e8c5:7a76:581d]:[32,13.13.13.1]:[201]
                     2.2.2.2             0         100       0    i  2.2.2.2         VXLAN
*>i  [2]:[0]:[3001]:[48,0010:9400:000c]:[0]:[3001]
                     2.2.2.2             0         100       0    i  2.2.2.2         VXLAN
*>i  [2]:[0]:[3001]:[48,0010:9400:000c]:[128,3001::2][3001]
                     2.2.2.2             0         100       0    i  2.2.2.2         VXLAN
```

```
*>i  [2]:[0]:[3001]:[48,e8c5:7a76:581d]:[128,3001::1][3001]
                     2.2.2.2             0        100       0    i  2.2.2.2         VXLAN
*>i  [3]:[201]:[32,2.2.2.2]
                     2.2.2.2             0        100       0    i  2.2.2.2         VXLAN
*>i  [3]:[3001]:[32,2.2.2.2]
                     2.2.2.2             0        100       0    i  2.2.2.2         VXLAN

RD[3.3.3.3:11] VRF[L2VRF2]:
* i  [2]:[0]:[201]:[48,0010:9400:0003]:[0]:[201]
                     2.2.2.2             0        100       0    i  2.2.2.2         VXLAN
* i  [2]:[0]:[201]:[48,0010:9400:0003]:[32,13.13.13.2]:[201]
                     2.2.2.2             0        100       0    i  2.2.2.2         VXLAN
*>   [2]:[0]:[201]:[48,0010:9400:0005]:[0]:[201]
                    3.3.3.3              0       100      32768  i  ---------      VXLAN
*>   [2]:[0]:[201]:[48,0010:9400:0005]:[32,14.14.14.2]:[201]
                     3.3.3.3              0        100       32768  i  ----------
VXLAN
* i  [2]:[0]:[201]:[48,e8c5:7a76:581d]:[32,13.13.13.1]:[201]
                     2.2.2.2             0        100       0    i  2.2.2.2         VXLAN
*>   [2]:[0]:[201]:[48,e8c5:7aa8:7cb3]:[32,14.14.14.1]:[201]
                     3.3.3.3              0        100       32768  i  ----------
VXLAN
* i  [2]:[0]:[3001]:[48,0010:9400:000c]:[0]:[3001]
                     2.2.2.2             0        100       0    i  2.2.2.2         VXLAN
* i  [2]:[0]:[3001]:[48,0010:9400:000c]:[128,3001::2][3001]
                     2.2.2.2             0        100       0    i  2.2.2.2         VXLAN
* i  [2]:[0]:[3001]:[48,e8c5:7a76:581d]:[128,3001::1][3001]
                     2.2.2.2             0        100       0    i  2.2.2.2         VXLAN
*>   [2]:[0]:[3002]:[48,0010:9400:000b]:[0]:[3002]
                     3.3.3.3             0       100      32768  i  ---------      VXLAN
*>   [2]:[0]:[3002]:[48,0010:9400:000b]:[128,3002::2][3002]
                     3.3.3.3             0       100      32768  i  ----------     VXLAN
*>   [2]:[0]:[3002]:[48,e8c5:7aa8:7cb3]:[128,3002::1][3002]
                     3.3.3.3             0       100      32768  i  ----------     VXLAN
* i  [3]:[201]:[32,2.2.2.2]
                     2.2.2.2              0        100       0    i  2.2.2.2         VXLAN
*>   [3]:[201]:[32,3.3.3.3]
                     3.3.3.3             0       100      32768  i  ---------      VXLAN
* i  [3]:[3001]:[32,2.2.2.2]
                     2.2.2.2              0        100       0    i  2.2.2.2         VXLAN
*>   [3]:[3002]:[32,3.3.3.3]
                     3.3.3.3             0       100      32768  i  ----------     VXLAN

Total number of prefixes 28

ISIS Validation
PE2#show nvo vxlan tunnel
VXLAN Network tunnel Entries
Source           Destination      Status         Up/Down       Update
=================================================================================
2.2.2.2          3.3.3.3          Installed      00:00:10      00:00:10
```

```
Total number of entries are 1
PE2#show clns neighbors
Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 1
Total number of adjacencies: 2
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
PE5            po1         b86a.9725.a7f2  Up     28        L1   IS-IS
                                           Up     28        L2   IS-IS
Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag 2:  VRF : L3VRF2
System Id      Interface   SNPA            State  Holdtime  Type Protocol
Spirent-1      irb2001     0010.9400.0003  Up     28        L2   IS-IS

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag 3:  VRF : L3VRF2
System Id      Interface   SNPA            State  Holdtime  Type Protocol
Spirent-1      irb3001     0010.9400.000c  Up     28        L2   IS-IS
PE2#
PE2#
PE2#show ip route vrf all
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            2.2.2.2/32 is directly connected, lo, 02:13:57
i L2         3.3.3.3/32 [115/30] via 20.1.1.2, po1, 00:00:32
i L1         7.7.7.7/32 [115/40] via 20.1.1.2, po1, 01:05:49
C            20.1.1.0/24 is directly connected, po1, 02:13:21
i L1         50.1.1.0/24 [115/20] via 20.1.1.2, po1, 01:06:05
i L1         60.1.1.0/24 [115/30] via 20.1.1.2, po1, 00:00:47
i L1         80.1.1.0/24 [115/30] via 20.1.1.2, po1, 01:05:49
C            127.0.0.0/8 is directly connected, lo, 02:13:57
IP Route Table for VRF "management"
C            10.12.98.0/24 is directly connected, eth0, 02:13:57
C            127.0.0.0/8 is directly connected, lo.management, 02:13:57
IP Route Table for VRF "L3VRF2"
B            3.3.3.3/32 [0/0] is directly connected, tunvxlan2, 00:00:28
C            13.13.13.0/24 is directly connected, irb2001, 02:13:57
```

```
B            14.14.14.0/24 [200/0] via 3.3.3.3 (recursive is directly connected,
 tunvxlan2), 00:00:28
C            127.0.0.0/8 is directly connected, lo.L3VRF2, 02:13:57
IP Route Table for VRF "L2VRF2"

Gateway of last resort is not set
PE2# show bgp l2vpn evpn
BGP table version is 2, local router ID is 2.2.2.2
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

[EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route
5 - Prefix Route
Network          Next Hop            Metric    LocPrf       Weight     Path
 Peer          Encap

RD[63000:11]
*>i  [5]:[0]:[0]:[24]:[14.14.14.0]:[0.0.0.0]:[2000]
                     3.3.3.3             0        100       0    ?  3.3.3.3       VXLAN
*>i  [5]:[0]:[0]:[64]:[3002::]:[::]:[2000]
                     3.3.3.3             0        100       0    ?  3.3.3.3       VXLAN

RD[2.2.2.2:11] VRF[L2VRF2]:
*>   [2]:[0]:[201]:[48,0010:9400:0003]:[0]:[201]
                    2.2.2.2             0       100      32768  i  ---------      VXLAN
*>   [2]:[0]:[201]:[48,0010:9400:0003]:[32,13.13.13.2]:[201]
                    2.2.2.2             0       100      32768  i  ---------      VXLAN
* i  [2]:[0]:[201]:[48,0010:9400:0005]:[0]:[201]
                     3.3.3.3             0        100       0    i  3.3.3.3       VXLAN
* i  [2]:[0]:[201]:[48,0010:9400:0005]:[32,14.14.14.2]:[201]
                     3.3.3.3             0        100       0    i  3.3.3.3       VXLAN
*>   [2]:[0]:[201]:[48,e8c5:7a76:581d]:[32,13.13.13.1]:[201]
                     2.2.2.2             0       100      32768  i  ---------      VXLAN
* i  [2]:[0]:[201]:[48,e8c5:7aa8:7cb3]:[32,14.14.14.1]:[201]
                     3.3.3.3             0        100       0    i  3.3.3.3       VXLAN
*>   [2]:[0]:[3001]:[48,0010:9400:000c]:[0]:[3001]
                    2.2.2.2             0       100      32768  i  ---------      VXLAN
*>   [2]:[0]:[3001]:[48,0010:9400:000c]:[128,3001::2][3001]
                    2.2.2.2             0       100      32768  i  ---------      VXLAN
*>   [2]:[0]:[3001]:[48,e8c5:7a76:581d]:[128,3001::1][3001]
                    2.2.2.2             0       100      32768  i  ---------      VXLAN
* i  [2]:[0]:[3002]:[48,0010:9400:000b]:[0]:[3002]
                     3.3.3.3             0        100       0    i  3.3.3.3       VXLAN
* i  [2]:[0]:[3002]:[48,0010:9400:000b]:[128,3002::2][3002]
```

```
                      3.3.3.3              0        100       0    i  3.3.3.3       VXLAN
* i  [2]:[0]:[3002]:[48,e8c5:7aa8:7cb3]:[128,3002::1][3002]
                      3.3.3.3              0        100       0    i  3.3.3.3       VXLAN
*>   [3]:[201]:[32,2.2.2.2]
                     2.2.2.2             0        100       32768  i  ---------     VXLAN
* i  [3]:[201]:[32,3.3.3.3]
                      3.3.3.3              0        100       0    i  3.3.3.3       VXLAN
*>   [3]:[3001]:[32,2.2.2.2]
                     2.2.2.2             0        100       32768  i  ---------     VXLAN
* i  [3]:[3002]:[32,3.3.3.3]
                      3.3.3.3              0        100       0    i  3.3.3.3       VXLAN

RD[3.3.3.3:11]
*>i  [2]:[0]:[201]:[48,0010:9400:0005]:[0]:[201]
                      3.3.3.3              0        100       0    i  3.3.3.3       VXLAN
*>i  [2]:[0]:[201]:[48,0010:9400:0005]:[32,14.14.14.2]:[201]
                      3.3.3.3              0        100       0    i  3.3.3.3       VXLAN
*>i  [2]:[0]:[201]:[48,e8c5:7aa8:7cb3]:[32,14.14.14.1]:[201]
                      3.3.3.3              0        100       0    i  3.3.3.3       VXLAN
*>i  [2]:[0]:[3002]:[48,0010:9400:000b]:[0]:[3002]
                      3.3.3.3              0        100       0    i  3.3.3.3       VXLAN
*>i  [2]:[0]:[3002]:[48,0010:9400:000b]:[128,3002::2][3002]
                      3.3.3.3              0        100       0    i  3.3.3.3       VXLAN
*>i  [2]:[0]:[3002]:[48,e8c5:7aa8:7cb3]:[128,3002::1][3002]
                      3.3.3.3              0        100       0    i  3.3.3.3       VXLAN
*>i  [3]:[201]:[32,3.3.3.3]
                      3.3.3.3              0        100       0    i  3.3.3.3       VXLAN
*>i  [3]:[3002]:[32,3.3.3.3]
                      3.3.3.3              0        100       0    i  3.3.3.3       VXLAN

Total number of prefixes 26
PE2#        show nvo vxlan arp-
arp-cache  arp-nd
PE2#        show nvo vxlan arp-cache
VXLAN ARP-CACHE Information
==========================
VNID     Ip-Addr          Mac-Addr       Type        Age-Out    Retries-Left
_____________________________________________________________________________
201      13.13.13.1       e8c5.7a76.581d Static Local   ----
201      13.13.13.2       0010.9400.0003 Dynamic Local  ----
201      14.14.14.1       e8c5.7aa8.7cb3 Static Remote  ----
201      14.14.14.2       0010.9400.0005 Dynamic Remote ----
Total number of entries are 4
PE2#show nvo vxlan irb-status
IRB is ACTIVE in Hardware
PE2#

PE4#show nvo vxlan tunnel
VXLAN Network tunnel Entries
Source           Destination      Status        Up/Down       Update
```

```
========================================================================
3.3.3.3          7.7.7.7          Installed     00:01:28      00:01:28
3.3.3.3          2.2.2.2          Installed     00:01:28      00:01:28

Total number of entries are 2
PE4#show clns neighbors

Total number of L1 adjacencies: 1
Total number of L2 adjacencies: 1
Total number of adjacencies: 2
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
PE6            xe5         00e0.4b71.f12c      Up     25        L1   IS-IS
                                               Up     25        L2   IS-IS

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag 2:  VRF : L3VRF2
System Id      Interface   SNPA            State  Holdtime  Type Protocol
Spirent-1      irb2001     0010.9400.0005      Up     28        L2   IS-IS

Total number of L1 adjacencies: 0
Total number of L2 adjacencies: 1
Total number of adjacencies: 1
Tag 3:  VRF : L3VRF2
System Id      Interface   SNPA            State  Holdtime  Type Protocol
Spirent-1      irb3002     0010.9400.000b      Up     28        L2   IS-IS
PE4#show ip route vrf all
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"
i L2         2.2.2.2/32 [115/30] via 60.1.1.1, xe5, 00:01:46
C            3.3.3.3/32 is directly connected, lo, 02:09:52
i L1         7.7.7.7/32 [115/30] via 60.1.1.1, xe5, 00:01:46
i L1         20.1.1.0/24 [115/30] via 60.1.1.1, xe5, 00:01:46
i L1         50.1.1.0/24 [115/20] via 60.1.1.1, xe5, 00:01:46
C            60.1.1.0/24 is directly connected, xe5, 00:02:02
i L1         80.1.1.0/24 [115/20] via 60.1.1.1, xe5, 00:01:46
C            127.0.0.0/8 is directly connected, lo, 02:09:52
IP Route Table for VRF "management"
C            10.12.98.0/24 is directly connected, eth0, 02:09:52
C            127.0.0.0/8 is directly connected, lo.management, 02:09:52
```

```
IP Route Table for VRF "L3VRF2"
B            2.2.2.2/32 [0/0] is directly connected, tunvxlan2, 00:01:42
B            7.7.7.7/32 [0/0] is directly connected, tunvxlan2, 00:01:42
B            13.13.13.0/24 [200/0] via 2.2.2.2 (recursive is directly connected,
tunvxlan2), 00:01:42
C            14.14.14.0/24 is directly connected, irb2001, 02:09:52
B            17.17.17.0/24 [200/0] via 7.7.7.7 (recursive is directly connected,
tunvxlan2), 00:01:42
C            127.0.0.0/8 is directly connected, lo.L3VRF2, 02:09:52
IP Route Table for VRF "L2VRF2"

Gateway of last resort is not set
PE4# show bgp l2vpn evpn
BGP table version is 3, 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

[EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route
5 - Prefix Route

   Network         Next Hop           Metric    LocPrf      Weight     Path  Peer
Encap

RD[7400:11]
*>i  [5]:[0]:[0]:[24]:[17.17.17.0]:[0.0.0.0]:[2000]
                     7.7.7.7             0        100       0     i  7.7.7.7         VXLAN
*>i  [5]:[0]:[0]:[64]:[8002::]:[::]:[2000]
                     7.7.7.7             0        100       0     i  7.7.7.7         VXLAN

RD[61000:11]
*>i  [5]:[0]:[0]:[24]:[13.13.13.0]:[0.0.0.0]:[2000]
                     2.2.2.2             0        100       0     ?  2.2.2.2         VXLAN
*>i  [5]:[0]:[0]:[64]:[3001::]:[::]:[2000]
                     2.2.2.2             0        100       0     ?  2.2.2.2         VXLAN

RD[2.2.2.2:11]
*>i  [2]:[0]:[201]:[48,0010:9400:0003]:[0]:[201]
                     2.2.2.2             0        100       0     i  2.2.2.2         VXLAN
*>i  [2]:[0]:[201]:[48,0010:9400:0003]:[32,13.13.13.2]:[201]
                     2.2.2.2             0        100       0     i  2.2.2.2         VXLAN
*>i  [2]:[0]:[201]:[48,e8c5:7a76:581d]:[32,13.13.13.1]:[201]
                     2.2.2.2             0        100       0     i  2.2.2.2         VXLAN
*>i  [2]:[0]:[3001]:[48,0010:9400:000c]:[0]:[3001]
                     2.2.2.2             0        100       0     i  2.2.2.2         VXLAN
*>i  [2]:[0]:[3001]:[48,0010:9400:000c]:[128,3001::2][3001]
```

```
                     2.2.2.2             0       100      0    i  2.2.2.2        VXLAN
*>i  [2]:[0]:[3001]:[48,e8c5:7a76:581d]:[128,3001::1][3001]
                     2.2.2.2             0       100      0    i  2.2.2.2        VXLAN
*>i  [3]:[201]:[32,2.2.2.2]
                     2.2.2.2             0       100      0    i  2.2.2.2        VXLAN
*>i  [3]:[3001]:[32,2.2.2.2]
                     2.2.2.2             0       100      0    i  2.2.2.2        VXLAN

RD[3.3.3.3:11] VRF[L2VRF2]:
* i  [2]:[0]:[201]:[48,0010:9400:0003]:[0]:[201]
                     2.2.2.2             0       100      0    i  2.2.2.2        VXLAN
* i  [2]:[0]:[201]:[48,0010:9400:0003]:[32,13.13.13.2]:[201]
                     2.2.2.2             0       100      0    i  2.2.2.2        VXLAN
*>   [2]:[0]:[201]:[48,0010:9400:0005]:[0]:[201]
                     3.3.3.3             0       100      32768  i  ----------     VXLAN
*>   [2]:[0]:[201]:[48,0010:9400:0005]:[32,14.14.14.2]:[201]
                     3.3.3.3             0       100      32768  i  ----------     VXLAN
* i  [2]:[0]:[201]:[48,e8c5:7a76:581d]:[32,13.13.13.1]:[201]
                     2.2.2.2             0       100      0    i  2.2.2.2        VXLAN
*>   [2]:[0]:[201]:[48,e8c5:7aa8:7cb3]:[32,14.14.14.1]:[201]
                     3.3.3.3             0       100      32768  i  ----------     VXLAN
* i  [2]:[0]:[3001]:[48,0010:9400:000c]:[0]:[3001]
                     2.2.2.2             0       100      0    i  2.2.2.2        VXLAN
* i  [2]:[0]:[3001]:[48,0010:9400:000c]:[128,3001::2][3001]
                     2.2.2.2             0       100      0    i  2.2.2.2        VXLAN
* i  [2]:[0]:[3001]:[48,e8c5:7a76:581d]:[128,3001::1][3001]
                     2.2.2.2             0       100      0    i  2.2.2.2        VXLAN
*>   [2]:[0]:[3002]:[48,0010:9400:000b]:[0]:[3002]
                     3.3.3.3             0       100      32768  i  ----------     VXLAN
*>   [2]:[0]:[3002]:[48,0010:9400:000b]:[128,3002::2][3002]
                     3.3.3.3             0       100      32768  i  ----------     VXLAN
*>   [2]:[0]:[3002]:[48,e8c5:7aa8:7cb3]:[128,3002::1][3002]
                     3.3.3.3             0       100      32768  i  ----------     VXLAN
* i  [3]:[201]:[32,2.2.2.2]
                     2.2.2.2             0       100      0    i  2.2.2.2        VXLAN
*>   [3]:[201]:[32,3.3.3.3]
                     3.3.3.3             0       100      32768  i  ----------     VXLAN
* i  [3]:[3001]:[32,2.2.2.2]
                     2.2.2.2             0       100      0    i  2.2.2.2        VXLAN
*>   [3]:[3002]:[32,3.3.3.3]
                     3.3.3.3             0       100      32768  i  ----------     VXLAN

Total number of prefixes 28
```

Abbreviations

The following are some key abbreviations and their meanings relevant to this document:

Acronym	Description
ECMP	Equal-Cost Multipath
EVPN	Ethernet Virtual Private Netwrok
MPLS	Multiprotocol Label Switching
VxLAN	Virtual Extensible LAN
SR	Segment Routing
IRB	Integrated Routing
OSPF	Open Shortest Path First
ISIS	Intermediate System to Intermediate System

Glossary

The following provides definitions for key terms used throughout this document.

Single Home VxLAN	This refers to a Virtual Extensible LAN (VxLAN) deployment where a single data center or network site is connected to a single external network (usually the internet) for connectivity.
IRB	A networking feature that enables the integration of Layer 3 IP routing and Layer 2 MAC address bridging within the same interface, simplifying network management and resource utilization.
OSPF	A dynamic and efficient link-state routing protocol used to determine the best path for data packets in an IP network. It is characterized by rapid convergence and adaptability, making it suitable for large and dynamic networks.
ISIS	A routing protocol designed for scalability and stability in computer networks, commonly used in large Service Provider networks. It provides a robust framework for routing information exchange.
Layer 3 Routing	Network routing operations at the Network Layer (Layer 3) of the OSI model, focusing on routing IP packets between different subnets or networks.
Layer 2 Bridging	Network bridging operations at the Data Link Layer (Layer 2) of the OSI model, handling the forwarding of data frames based on MAC addresses within the same network segment.
EVPN	Ethernet VPN, a technology that provides advanced and efficient methods for Layer 2 and Layer 3 services in Ethernet networks, often used in data centers and service provider environments.

Single-Home for VxLAN EVPN IRB with OSPF or ISIS

Overview

Single Home EVPN-MPLS IRB with OSPF and ISIS feature provides streamline routing and bridging operations within Service Provider (SP) networks. It seamlessly integrates EVPN-MPLS architecture and handles both Layer 3 routing and Layer2 bridging, making it an ideal choice for SP networks. This feature utilizes routing protocols, OSPF and ISIS, known for their efficiency and reliability. It also supports Integrated Routing and Bridging (IRB), enabling the integration of Layer3 IP routing and Layer2 MAC address bridging within the same interface. It simplifies network operations, enhances efficiency, and ensures network reliability for SP in dynamic environments.

Feature Characteristics

The Single Home EVPN-MPLS IRB with OSPF and ISIS feature has the following characteristics:

- Integrates with the EVPN-MPLS architecture, providing a comprehensive solution for Layer 3 routing and Layer 2 bridging within the network.
- Supports IRB, allowing for the integration of Layer 3 routing and Layer 2 bridging within the same interface.

Benefits

The Single Home EVPN-MPLS IRB with OSPF and ISIS feature has the following benefits:

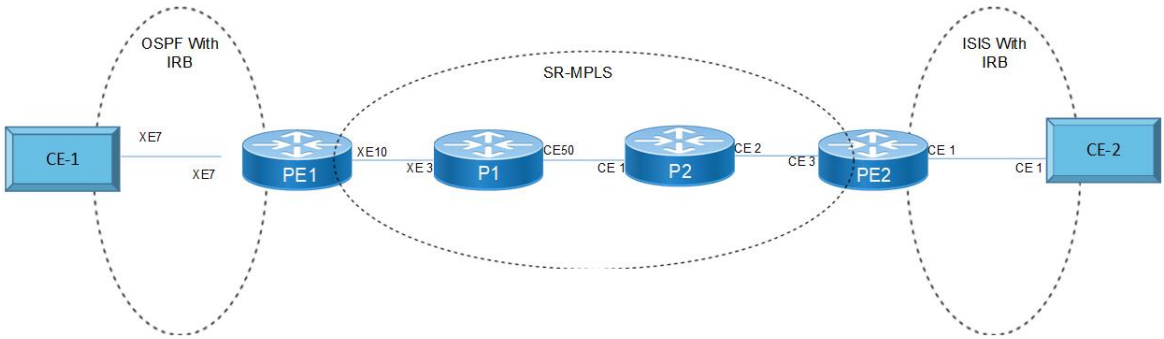
- With OSPF and ISIS support, the network can effortlessly scale to accommodate increased traffic and new network elements.
- The use of robust routing protocols like OSPF and ISIS ensures reliable and fault-tolerant network communication, minimizing downtime and enhancing network stability.
- The integration of multiple functionalities into a single feature simplifies network management, reducing operational complexity and lowering the risk of configuration errors.

Prerequisites

- Router must be up and running.

Topology for OSPF

The network topology includes various network elements such as routers, customer edge (CE) devices, and Provider Edge (PE) routers. The feature enables OSPF on the IRB interfaces, allowing for efficient routing and communication between network devices within the topology.



Single Home EVPN MPLS IRB with OSPF and ISIS

Configuration

Perform the following configurations to set up interfaces, assign IP addresses, configure VLAN encapsulation, establish OSPF routing, and prepare the network for routing and forwarding operations. Please ensure that the subnet mask values are accurate and suitable for your network requirements.

CE1

`CE1#configure terminal`	Enters the configuration mode on the OcNOS device.
`CE1(config)#interface po1`	Enters the configuration mode for a Port-Channel interface named po1.
`CE1(config-if)# load-interval 30`	Sets the load interval for the Port-Channel interface to 30 seconds.
`CE1(config-if)#interface po1.101`	Enters the configuration mode for a subinterface of Port-Channel 1, specifically subinterface 101.
`CE1(config-if)# encapsulation dot1q 101`	Configures the subinterface to use IEEE 802.1Q encapsulation with VLAN ID 101.
`CE1(config-if)# ip address 101.101.101.2/24`	Assigns the IP address 101.101.101.2 with a subnet mask of /24 to the subinterface.
`CE1(config-if)#interface po1.1001`	Enters the configuration mode for another subinterface of Port-Channel 1, specifically subinterface 1001.
`CE1(config-if)# encapsulation dot1q 1001`	Configures the subinterface with IEEE 802.1Q encapsulation using VLAN ID 1001.
`CE1(config-if)# ipv6 address 1001::2/64`	Assigns an IPv6 address 1001::2 with a subnet prefix length of /64 to the subinterface.
`CE1(config-if)# ipv6 router ospf area 0.0.0.0 tag 1001 instance-id 0`	Configures OSPF for IPv6 on the subinterface, specifying area 0.0.0.0 with a tag of 1001 and instance ID 0.

`CE1(config-if)# ip address 99.99.99.1/243`	Assigns the IP address 99.99.99.1 with a subnet mask of /243 to the Gigabit Ethernet interface. Note: The subnet mask value seems to be incorrect; it should typically be in the format /24.
`CE1(config-if)#interface lo`	Enters the configuration mode for a loopback interface.
`CE1(config-if)# ip address 127.0.0.1/8`	Assigns the primary IP address 127.0.0.1 with a subnet mask of /8 to the loopback interface.
`CE1(config-if)# ip address 1.1.1.1/32 secondary`	Adds a secondary IP address, 1.1.1.1 with a /32 subnet mask, to the loopback interface.
`CE1(config-if)# ipv6 address ::1/128`	Assigns the IPv6 address ::1 with a subnet prefix length of /128 to the loopback interface.
`CE1(config-if)#interface xe7`	Enters the configuration mode for Ten Gigabit Ethernet interface 7.
`CE1(config-if)# channel-group 1 mode active`	Configures the interface to be part of an EtherChannel group with group number 1 and sets the mode to active.
`CE1(config-if)#exit`	Exits the interface configuration mode.
`CE1(config)#router ospf 101`	Enters the configuration mode for OSPF (routing process 101.
`CE1(config-router)# ospf router-id 1.1.1.1`	Sets the OSPF router ID to 1.1.1.1.
`CE1(config-router)# redistribute connected`	Configures OSPF to redistribute connected routes into the OSPF routing process.
`CE1(config-router)# network 101.101.101.0/24 area 0.0.0.0`	Specifies that the network 101.101.101.0/24 is part of OSPF Area 0.0.0.0.
`CE1(config-router)#router ipv6 ospf 1001`	Enters the configuration mode for OSPFv3 (OSPF for IPv6) routing process 1001.
`CE1(config-router)# router-id 1.1.1.1`	Sets the OSPFv3 router ID to 1.1.1.1.
`CE1(config-router)#Exit`	Exists from the configurations.

Configure MTU over IRB

`CE1(config)#int po1`	Enters interface configuration mode for port-channel 1 (po1).
`CE1(config-if)#mtu 9216`	Sets the Maximum Transmission Unit (MTU) for the interface po1 to 9216 bytes, which is a jumbo frame MTU size.
`CE1(config-if)#commit`	Commit the changes made to the interface configuration.
`CE1((config-if)#int po1.101`	Enters interface configuration mode for subinterface po1.101.
`CE1(config-if)#mtu 9216`	Sets the MTU to 9216 bytes.
`CE1(config-if)#int po1.1001`	Enters interface configuration mode for subinterface po1.1001.
`CE1(config-if)#mtu 9216`	Sets the MTU to 9216 bytes.
`CE1(config-if)#Exit`	Exits the interface configuration mode.

PE1

`PE1#configure terminal`	Enters the global configuration mode.
`PE1(config)#evpn mpls enable`	Enables EVPN-MPLS within the configuration.
`PE1(config)#evpn mpls irb`	Configures EVPN-MPLS IRB.
`PE1(config)#mac vrf MacVrf1`	Creates a MAC VRF named MacVrf1.

`PE1(config-vrf)# rd 2.2.2.2:100`	Defines a RD for MacVrf1 as 2.2.2.2:100.
`PE1(config-vrf)# route-target both 100:1`	Sets the route target for MacVrf1 to 100:1 for both import and export.
`PE1(config-vrf)#ip vrf IpVrf1`	Creates an IP VRF named IpVrf1.
`PE1(config-vrf)# rd 2.2.2.2:200`	Defines an RD for IpVrf1 as 2.2.2.2:200.
`PE1(config-vrf)# route-target both 100:100`	Sets the route target for IpVrf1 to 100:100 for both import and export.
`PE1(config-vrf)# l3vni 100`	Configures Layer 3 Virtual Network Identifier (L3VNI) as 100 for IpVrf1.
`PE1(config-vrf)#evpn mpls vtep-ip-global 2.2.2.2`	Configures the EVPN-MPLS Virtual Tunnel EndPoint (VTEP) IP address as 2.2.2.2.
`PE1(config)#evpn mpls id 101`	Defines EVPN-MPLS ID as 101.
`PE1(config-evpn-mpls)# host-reachability-protocol evpn-bgp MacVrf1`	Specifies BGP as the host reachability protocol for MacVrf1.
`PE1(config-evpn-mpls)# evpn irb irb101`	Associates IRB 101 with EVPN-MPLS.
`PE1(config-evpn-mpls)#evpn mpls id 1001`	Defines EVPN-MPLS ID as 1001.
`PE1(config-evpn-mpls)# host-reachability-protocol evpn-bgp MacVrf1`	Specifies BGP as the host reachability protocol for MacVrf1.
`PE1(config-evpn-mpls)# evpn irb irb1001`	Associates IRB 1001 with EVPN-MPLS.
`PE1(config-evpn-mpls)#qos enable`	Enables QoS features.
`PE1(config)#qos statistics`	Configures QoS statistics collection.
`PE1(config)#hostname PE1`	Sets the hostname of the device to PE1.
`PE1(config)#segment-routing`	Enters the configuration mode for segment routing.
`PE1(config-sr)# mpls sr-prefer`	Configures MPLS as the preferred segment routing method.
`PE1(config-sr)#exit`	Exits the segment routing configuration mode.
`PE1(config)#interface po1`	Enters the configuration mode for Port-Channel 1.
`PE1(config-if)# switchport`	Configures the interface as a switchport.
`PE1(config-if)# load-interval 30`	Sets the load interval to 30 seconds for the interface.
`PE1(config-if)#interface po1.101 switchport`	Enters the configuration mode for subinterface 101 of Port-Channel 1 and configures it as a switchport.
`PE1(config-if)# encapsulation dot1q 101`	Configures IEEE 802.1Q encapsulation with VLAN ID 101 for the subinterface.
`PE1(config-if)# rewrite pop`	Configures packet rewriting for the subinterface.
`PE1(config-if)# access-if-evpn`	Specifies that this interface is associated with EVPN.
`PE1(config-acc-if-evpn)# map vpn-id 101`	Maps this interface to VPN ID 101.
`PE1(config-acc-if-evpn)#interface po1.1001 switchport`	Enters the configuration mode for subinterface 1001 of Port-Channel 1 and configures it as a switchport.
`PE1(config-if)# encapsulation dot1q 1001`	Configures IEEE 802.1Q encapsulation with VLAN ID 1001 for the subinterface.
`PE1(config-if)# rewrite pop`	Configures packet rewriting for the subinterface.
`PE1(config-if)# access-if-evpn`	Specifies that this interface is associated with E
`PE1(config-acc-if-evpn)# map vpn-id 1001`	Maps this interface to VPN ID 1001.
`PE1(config-acc-if-evpn)#exit`	Exits the access-if-evpn configuration mode.
`PE1(config-if)#interface irb101`	Enters the configuration mode for IRB interface 101.

`PE1(config-irb-if)# ip vrf forwarding IpVrf1`	Associates the IRB interface with the IP VRF IpVrf1.
`PE1(config-irb-if)# ip address 101.101.101.1/24`	Configures the IP address 101.101.101.1 with a subnet mask of /24 on the IRB interface.
`PE1(config-irb-if)#interface irb1001`	Enters the configuration mode for IRB interface 1001.
`PE1(config-irb-if)# ip vrf forwarding IpVrf1`	Associates the IRB interface with the IP VRF IpVrf1.
`PE1(config-irb-if)# ipv6 address 1001::1/64`	Configures an IPv6 address 1001::1 with a subnet prefix length of /64 on the IRB interface.
`PE1(config-irb-if)# ipv6 router ospf area 0.0.0.0 tag IpVrf1 instance-id 0`	Configures OSPF for IPv6 on the IRB interface, specifying area 0.0.0.0 with a tag and instance ID.
`PE1(config-irb-if)#interface lo`	Enters the configuration mode for loopback interface.
`PE1(config-if)# ip address 127.0.0.1/8`	Configures the primary IP address of the loopback interface as 127.0.0.1 with a subnet mask of /8.
`PE1(config-if)# ip address 2.2.2.2/32 secondary`	Adds a secondary IP address 2.2.2.2 with a /32 subnet mask to the loopback interface.
`PE1(config-if)# ipv6 address ::1/128`	Configures an IPv6 address ::1 with a subnet prefix length of /128 on the loopback interface.
`PE1(config-if)# prefix-sid index 2`	Configures a prefix SID with an index of 2.
`PE1(config-if)#interface xe7`	Enters the configuration mode for Ten Gigabit Ethernet interface 7.
`PE1(config-if)# channel-group 1 mode active`	Configures the interface to be part of an EtherChannel group with group number 1 and sets the mode to active.
`PE1(config-if)#interface xe10`	Enters the configuration mode for Ten Gigabit Ethernet interface 10.
`PE1(config-if)# speed 10g`	Sets the speed of the interface to 10 gigabits per second.
`PE1(config-if)# ip address 10.1.1.1/24`	Configures an IP address 10.1.1.1 with a subnet mask of /24 on the interface.
`PE1(config-if)# label-switching`	Enables label switching on the interface.
`PE1(config-if)# exit`	Exits the interface configuration mode.
`PE1(config)#router ospf 100`	Enters the configuration mode for OSPF routing process 100.
`PE1(config-router)# ospf router-id 2.2.2.2`	Sets the OSPF router ID to 2.2.2.2.
`PE1(config-router)# network 2.2.2.2/32 area 0.0.0.0`	Configures the network 2.2.2.2/32 within OSPF Area 0.0.0.0.
`PE1(config-router)# network 10.1.1.0/24 area 0.0.0.0`	Configures the network 10.1.1.0/24 within OSPF Area 0.0.0.0.
`PE1(config-router)# segment-routing mpls`	Configures MPLS for segment routing.
`PE1(config-router)#router ospf 101 IpVrf1`	Enters the configuration mode for OSPF routing process 101 within VRF IpVrf.
`PE1(config-router)# network 10.1.1.0/24 area 0.0.0.0`	Specifies the network 10.1.1.0 with a /24 subnet mask to be included in OSPF Area 0.0.0.0.
`PE1(config-router)# segment-routing mpls`	Enables MPLS-based segment routing in the OSPF configuration.
`PE1(config-router)#router ospf 101 IpVrf1`	Enters the configuration mode for OSPF routing process 101 associated with VRF IpVrf1.
`PE1(config-router)# ospf router-id 2.2.2.2`	Sets the OSPF router ID to 2.2.2.2.
`PE1(config-router)# redistribute bgp`	Configures the redistribution of BGP routes into OSPF.
`PE1(config-router)# network 101.101.101.0/24 area 0.0.0.0`	Specifies the network 101.101.101.0 with a /24 subnet mask to be included in OSPF Area 0.0.0.0 for VRF IpVrf1.

`PE1(config-router)#router ipv6 vrf ospf IpVrf1`	Enters the configuration mode for OSPFv3 (OSPF for IPv6) routing process associated with VRF IpVrf1.
`PE1(config-router)# router-id 2.2.2.2`	Sets the OSPFv3 router ID to 2.2.2.2.
`PE1(config-router)#router bgp 100`	Enters the configuration mode for BGP routing process 100.
`PE1(config-router)# bgp router-id 2.2.2.2`	Sets the BGP router ID to 2.2.2.2.
`PE1(config-router)# neighbor 5.5.5.5 remote-as 100`	Specifies a BGP neighbor with IP address 5.5.5.5 and assigns it the remote autonomous system number 100.
`PE1(config-router)# neighbor 5.5.5.5 update-source lo`	Sets the loopback interface as the source for BGP updates to the neighbor.
`PE1(config-router)# neighbor 5.5.5.5 advertisement-interval 0`	Configures the BGP neighbor's advertisement interval to 0.
`PE1(config-router)# address-family l2vpn evpn`	Enters the configuration mode for the BGP address family l2vpn evpn.
`PE1(config-router-af)# neighbor 5.5.5.5 activate`	Activates the BGP neighbor within the l2vpn evpn address family.
`PE1(config-router-af)# exit-address-family`	Exits the l2vpn evpn address family configuration.
`PE1(config-router)# address-family ipv4 vrf IpVrf1`	Enters the configuration mode for the BGP address family ipv4 vrf IpVrf1.
`PE1(config-router-af)# redistribute ospf 101`	Configures the redistribution of OSPF routes from OSPF process 101 into the ipv4 vrf IpVrf1 address family.
`PE1(config-router-af)# exit-address-family`	Exits the ipv4 vrf IpVrf1 address family configuration.
`PE1(config-router)# address-family ipv6 vrf IpVrf1`	Enters the configuration mode for the BGP address family ipv6 vrf IpVrf1.
`PE1(config-router-af)# redistribute ospf`	Configures the redistribution of OSPFv3 routes into the ipv6 vrf IpVrf1 address family.
`PE1(config-router-af)# exit-address-family`	Exits the ipv6 vrf IpVrf1 address family configuration.
`PE1(config-router)#line console 0`	Enters the configuration mode for the console line.
`PE1(config-line)# exec-timeout 0 0`	Sets the console line's execution timeout values to 0 seconds.
`PE1(config-line)#line vty 0 871`	Enters the configuration mode for virtual terminal lines 0 to 871.
`PE1(config-line)# exec-timeout 0 0`	Sets the execution timeout values for virtual terminal lines to 0 seconds.
`PE1(config-line)# privilege level 16`	Specifies the privilege level for users accessing the virtual terminal lines.
`PE1(config-line)#commit`	Commits the configuration changes.
`PE1(config-line)#end`	Exits the configuration mode.

Configure MTU over IRB

`PE1(config)#interface irb101`	Enters interface configuration mode for IRB interface 101.
`PE1(config-irb-if)#mtu 9216`	Sets the MTU to 9216 bytes.
`PE1(config-irb-if)#commit`	Commit the changes made to the interface configuration.
`PE1(config-irb-if)#exit`	Exits the IRB interface configuration mode and returns to the global configuration mode.
`PE1(config)#interface irb1001`	Enters interface configuration mode for IRB interface 1001.
`PE1(config-irb-if)#mtu 9216`	Sets the MTU to 9216 bytes.
`PE1(config-irb-if)#commit`	Commit the changes made to the interface configuration.

`PE1(config-irb-if)#exit`	Exits the IRB interface configuration mode and returns to the global configuration mode.
`PE1(config)#interface int po1`	Enters interface configuration mode for IRB int po1.
`PE1(config-irb-if)#mtu 9216`	Sets the MTU to 9216 bytes.
`PE1(config-irb-if)#commit`	Commit the changes made to the interface configuration.
`PE1(config-irb-if)#exit`	Exits the IRB interface configuration mode and returns to the global configuration mode.

P1

`P1#configure terminal`	Enters the global configuration mode.
`P1(config)#segment-routing`	Enters the configuration mode for Segment Routing.
`P1(config-sr)# mpls sr-prefer`	Configures the preference for MPLS as part of the Segment Routing setup.
`P1(config-if)#interface ce50`	Enters the configuration mode for interface ce50.
`P1(config-if)# ip address 20.1.1.1/24`	Assigns an IP address of 20.1.1.1 with a /24 subnet mask to interface ce50.
`P1(config-if)# label-switching`	Enables label switching for the interface ce50.
`P1(config-if)#interface lo`	Enters the configuration mode for a loopback interface.
`P1(config-if)# ip address 127.0.0.1/8`	Assigns an IP address of 127.0.0.1 with a /8 subnet mask to the loopback interface.
`P1(config-if)# ip address 3.3.3.3/32 secondary`	Adds a secondary IP address of 3.3.3.3 with a /32 subnet mask to the loopback interface.
`P1(config-if)# ipv6 address ::1/128`	Assigns an IPv6 address of ::1/128 to the loopback interface.
`P1(config-if)# prefix-sid index 3`	Configures a prefix SID with an index of 3 for the loopback interface.
`P1(config-if)#interface xe3`	Enters the configuration mode for Ten Gigabit Ethernet interface 3.
`P1(config-if)# ip address 10.1.1.2/24`	Assigns an IP address of 10.1.1.2 with a /24 subnet mask to interface xe3.
`P1(config-if)# label-switching`	Enables label switching for interface xe3.
`P1(config-if)# exit`	Exits the interface configuration.
`P1(config-router)#router ospf 100`	Enters the configuration mode for OSPF routing process 100.
`P1(config-router)# ospf router-id 3.3.3.3`	Sets the OSPF router ID to 3.3.3.3.
`P1(config-router)# network 3.3.3.3/32 area 0.0.0.0`	Specifies the network 3.3.3.3 with a /32 subnet mask to be included in OSPF Area 0.0.0.0.
`P1(config-router)# network 10.1.1.0/24 area 0.0.0.0`	Specifies the network 10.1.1.0 with a /24 subnet mask to be included in OSPF Area 0.0.0.0.
`P1(config-router)# network 20.1.1.0/24 area 0.0.0.0`	Specifies the network 20.1.1.0 with a /24 subnet mask to be included in OSPF Area 0.0.0.0.
`P1(config-router)# segment-routing mpls`	Enables MPLS-based segment routing in the OSPF configuration.

`P1(config-router)#line console 0`	Enters the configuration mode for the console line.
`P1(config-line)# exec-timeout 0 0`	Sets the console line's execution timeout values to 0 seconds.
`P1(config-line)#line vty 0 871`	Enters the configuration mode for virtual terminal lines 0 to 871.
`P1(config-line)# exec-timeout 0 0`	Sets the execution timeout values for virtual terminal lines to 0 seconds.
`P1(config-line)# privilege level 16`	Specifies the privilege level for users accessing the virtual terminal lines.
`P1(config-line)# Exit`	Exits from configuration mode.

P2

`P2#configure terminal`	Enters the global configuration mode.
`P2(config)#segment-routing`	Enters the configuration mode for Segment Routing.
`P2(config-sr)# mpls sr-prefer`	Configures the preference for MPLS as part of the Segment Routing setup.
`P2(config-sr)#interface ce1`	Enters the configuration mode for interface ce1.
`P2(config-if)# ip address 20.1.1.2/24`	Assigns an IP address of 20.1.1.2 with a /24 subnet mask to interface ce1.
`P2(config-if)# label-switching`	Enables label switching for interface ce1.
`P2(config-if)#interface ce2`	Enters the configuration mode for interface ce2.
`P2(config-if)# speed 40g`	Sets the speed of interface ce2 to 40Gbps.
`P2(config-if)# ip address 30.1.1.1/24`	Assigns an IP address of 30.1.1.1 with a /24 subnet mask to interface ce2.
`P2(config-if)# label-switching`	Enables label switching for interface ce2.
`P2(config-if)#interface lo`	Enters the configuration mode for a loopback interface.
`P2(config-if)# ip address 127.0.0.1/8`	Assigns an IP address of 127.0.0.1 with a /8 subnet mask to the loopback interface.
`P2(config-if)# ip address 4.4.4.4/32 secondary`	Adds a secondary IP address of 4.4.4.4 with a /32 subnet mask to the loopback interface.
`P2(config-if)# ipv6 address ::1/128`	Assigns an IPv6 address of ::1/128 to the loopback interface.
`P2(config-if)# prefix-sid index 4`	Configures a prefix SID with an index of 4 for the loopback interface.
`P2(config)#router ospf 100`	Enters the configuration mode for OSPF routing process 100.
`P2(config-router)# ospf router-id 4.4.4.4`	Sets the OSPF router ID to 4.4.4.4.
`P2(config-router)# network 4.4.4.4/32 area 0.0.0.0`	Specifies the network 4.4.4.4 with a /32 subnet mask to be included in OSPF Area 0.0.0.0.
`P2(config-router)# network 20.1.1.0/24 area 0.0.0.0`	Specifies the network 20.1.1.0 with a /24 subnet mask to be included in OSPF Area 0.0.0.0.
`P2(config-router)# network 30.1.1.0/24 area 0.0.0.0`	Specifies the network 30.1.1.0 with a /24 subnet mask to be included in OSPF Area 0.0.0.0.
`P2(config-router)# segment-routing mpls`	Enables MPLS-based segment routing in the OSPF configuration.
`P2(config-router)#line console 0`	Enters the configuration mode for the console line.
`P2(config-line)# exec-timeout 0 0`	Sets the console line's execution timeout values to 0 seconds.

P2(config-line)#line vty 0 871	Enters the configuration mode for virtual terminal lines 0 to 871.
P2(config-line)# exec-timeout 0 0	Sets the execution timeout values for virtual terminal lines to 0 seconds.
P2(config-line)# privilege level 16	Specifies the privilege level for users accessing the virtual terminal lines.
P2(config-line)#Exit	Exits the configuration.

PE2

PE2#configure terminal	Enters the global configuration mode.
PE2(config)#evpn mpls enable	Enables EVPN MPLS.
PE2(config)#evpn mpls irb	Enables EVPN MPLS IRB.
PE2(config)mac vrf MacVrf2	Enters the configuration mode for MAC VRF with the name MacVrf2.
PE2(config-vrf)# rd 5.5.5.5:100	Sets the route distinguisher for the MAC VRF to 5.5.5.5:100.
PE2(config-vrf)# route-target both 100:1	Specifies route targets for import and export for the MAC VRF.
PE2(config-vrf)#ip vrf IpVrf1	Enters the configuration mode for IP VRF with the name IpVrf1.
PE2(config-vrf)# rd 5.5.5.5:200	Sets the route distinguisher for the IP VRF to 5.5.5.5:200.
PE2(config-vrf)# route-target both 100:100	Specifies route targets for import and export for the IP VRF.
PE2(config-vrf)# l3vni 100	Configures an L3VNI with ID 100 for the IP VRF.
PE2(config-vrf)#evpn mpls vtep-ip-global 5.5.5.5	Sets the global VTEP IP address for EVPN MPLS to 5.5.5.5.
PE2(config)#evpn mpls id 201	Configures an EVPN MPLS instance with ID 201.
PE2(config-evpn-mpls)# host-reachability-protocol evpn-bgp MacVrf2	Specifies BGP as the host reachability protocol for EVPN MPLS using MacVrf2.
PE2(config-evpn-mpls)# evpn irb irb101	Configures EVPN MPLS IRB with the IRB interface named irb101.
PE2(config-evpn-mpls)#evpn mpls id 2001	Configures another EVPN MPLS instance with ID 2001.
PE2(config-evpn-mpls)# host-reachability-protocol evpn-bgp MacVrf2	Specifies BGP as the host reachability protocol for EVPN MPLS using MacVrf2.
PE2(config-evpn-mpls)# evpn irb irb1001	Configures EVPN MPLS IRB with the IRB interface named irb1001.
PE2(config-evpn-mpls)#qos enable	Enables QoS features for EVPN MPLS.
PE2(config)qos statistics	Configures statistics for QoS.
PE2(config)#hostname PE2	Sets the hostname of the device to PE2.
PE2(config)#segment-routing	Enters the configuration mode for Segment Routing.
PE2(config-sr)# mpls sr-prefer	Configures the preference for MPLS in Segment Routing.
PE2(config)#interface ce1	Enters the configuration mode for interface ce1.
PE2(config-if)# switchport	Enables the switchport mode for the interface.
PE2(config-if)# load-interval 30	Sets the load interval to 30 seconds for the interface.
PE2(config)#interface ce1.101 switchport	Enters the configuration mode for subinterface ce1.101 and enables the switchport mode.
PE2(config-if)# encapsulation dot1q 101	Specifies VLAN encapsulation with VLAN ID 101 for the subinterface.

PE2(config-if)# rewrite pop	Configures the rewrite operation as "pop" for the subinterface.
PE2(config-if)# access-if-evpn	Configures the subinterface as an access interface for EVPN.
PE2(config-acc-if-evpn)# map vpn-id 201	Maps the subinterface to EVPN with VPN ID 201.
PE2(config-acc-if-evpn)#exit	Exits the access interface configuration.
PE2(config)#interface ce3	Enters the configuration mode for interface ce3.
PE2(config)# ip address 30.1.1.2/24	Assigns the IP address 30.1.1.2 with a subnet mask of 255.255.255.0 to interface ce3.
PE2(config)# label-switching	Enables label-switching on interface ce3.
PE2(config-if)#interface irb101	Enters the configuration mode for interface irb101.
PE2(config-irb-if)# ip vrf forwarding IpVrf1	Associates interface irb101 with the VRF (Virtual Routing and Forwarding) instance IpVrf1.
PE2(config-irb-if)# ip address 201.201.201.1/24	Assigns the IP address 201.201.201.1 with a subnet mask of 255.255.255.0 to interface irb101.
PE2(config-irb-if)# ip router isis 101	Enables ISIS routing protocol on interface irb101.
PE2(config-irb-if)#interface irb1001	Enters the configuration mode for interface irb1001.
PE2(config-irb-if)# ip vrf forwarding IpVrf1	Associates interface irb1001 with the VRF instance IpVrf1.
PE2(config-irb-if)# ipv6 address 2001::1/64	Assigns the IPv6 address 2001::1 with a prefix length of 64 to interface irb1001.
PE2(config-irb-if)# ipv6 router isis 101	Enables ISIS routing protocol for IPv6 on interface irb1001.
PE2(config-irb-if)#interface lo	Enters the configuration mode for the loopback interface.
PE2(config-if)# ip address 127.0.0.1/8	Assigns the IP address 127.0.0.1 with a subnet mask of 255.0.0.0 to the loopback interface.
PE2(config-if)# ip address 5.5.5.5/32 secondary	Assigns the secondary IP address 5.5.5.5 with a subnet mask of 255.255.255.255 to the loopback interface.
PE2(config-if)# ipv6 address ::1/128	Assigns the IPv6 address ::1 with a prefix length of 128 to the loopback interface.
PE2(config-if)# prefix-sid index 5	Configures a prefix SID with an index of 5.
PE2(config-if)#exit	Exits the interface configuration mode.
PE2(config)#router ospf 100	Enters the configuration mode for OSPF with process ID 100.
PE2(config-router)# ospf router-id 5.5.5.5	Sets the OSPF router ID to 5.5.5.5.
PE2(config-router)# network 5.5.5.5/32 area 0.0.0.0	Advertises the network 5.5.5.5/32 into OSPF area 0.0.0.0.
PE2(config-router)# network 30.1.1.0/24 area 0.0.0.0	Advertises the network 30.1.1.0/24 into OSPF area 0.0.0.0.
PE2(config-router)# segment-routing mpls	Enables MPLS for segment routing.
PE2(config-router)#router isis 101 IpVrf1	Enters the configuration mode for ISIS with process ID 101 and VRF instance IpVrf1.
PE2(config-irb-if)#interface lo	Enters the configuration mode for the loopback interface.
PE2(config-if)# ip address 127.0.0.1/8	Assigns the IP address 127.0.0.1 with a subnet mask of 255.0.0.0 to the loopback interface.
PE2(config-if)# ip address 5.5.5.5/32 secondary	Assigns the secondary IP address 5.5.5.5 with a subnet mask of 255.255.255.255 to the loopback interface.
PE2(config-if)# ipv6 address ::1/128	Assigns the IPv6 address ::1 with a prefix length of 128 to the loopback interface.
PE2(config-if)# prefix-sid index 5	Configures a prefix SID with an index of 5.

`PE2(config)#router ospf 100`	Enters the configuration mode for OSPF with process ID 100.
`PE2(config-router)# ospf router-id 5.5.5.5`	Sets the OSPF router ID to 5.5.5.5.
`PE2(config-router)# network 5.5.5.5/32 area 0.0.0.0`	Advertises the network 5.5.5.5/32 into OSPF area 0.0.0.0.
`PE2(config-router)# network 30.1.1.0/24 area 0.0.0.0`	Advertises the network 30.1.1.0/24 into OSPF area 0.0.0.0.
`PE2(config-router)# segment-routing mpls`	Enables MPLS for segment routing.
`PE2(config-router)#router isis 101 IpVrf1`	Enters the configuration mode for ISIS with process ID 101 and VRF instance IpVrf1.
`PE2(config-router)# is-type level-2-only`	Configures ISIS as a level-2-only routing protocol.
`PE2(config-router)# net 49.0001.0000.0000.0005.00`	Sets the ISIS NET for this router.
`PE2(config-router)# redistribute bgp`	Configures redistribution of BGP routes into ISIS.
`PE2(config-router)#router bgp 100`	Enters the configuration mode for BGP with AS number 100.
`PE2(config-router)# bgp router-id 5.5.5.5`	Sets the BGP router ID to 5.5.5.5.
`PE2(config-router)# neighbor 2.2.2.2 remote-as 100`	Configures a BGP neighbor with the remote AS number 100 and IP address 2.2.2.2.
`PE2(config-router)# neighbor 2.2.2.2 update-source lo`	Specifies the loopback interface as the source for BGP updates to the neighbor.
`PE2(config-router)# neighbor 2.2.2.2 advertisement-interval 0`	Sets the BGP advertisement interval to 0.
`PE2(config-router)# address-family l2vpn evpn`	Enters the address-family configuration mode for L2VPN EVPN.
`PE2(config-router-af)# neighbor 2.2.2.2 activate`	Activates the BGP neighbor for the L2VPN EVPN address family.
`PE2(config-router-af)# exit-address-family`	Exits the address-family configuration.
`PE2(config-router)# address-family ipv4 vrf IpVrf1`	Enters the address-family configuration mode for IPv4 with VRF instance IpVrf1.
`PE2(config-router-af)# redistribute isis`	Configures redistribution of ISIS routes into the IPv4 address family.
`PE2(config-router-af)# exit-address-family`	Exits the address-family configuration.

Configure MTU over IRB

`PE2(config)#interface irb101`	Enters interface configuration mode for IRB interface 101.
`PE2(config-irb-if)#mtu 9216`	Sets the MTU to 9216 bytes.
`PE2(config-irb-if)#commit`	Commit the changes made to the interface configuration.
`PE2(config)#interface irb1001`	Enters interface configuration mode for IRB interface 1001.
`PE2(config-irb-if)#mtu 9216`	Sets the MTU to 9216 bytes.
`PE2(config-irb-if)#commit`	Commit the changes made to the interface configuration.
`PE2(config-irb-if)#exit`	Exits the IRB interface configuration mode and returns to the global configuration mode.
`PE2(config)#interface ce1`	Enters interface configuration mode for IRB interface ce1.
`PE2(config-irb-if)#mtu 9216`	Sets the MTU to 9216 bytes.

PE2(config-irb-if)#commit	Commit the changes made to the interface configuration.
PE2(config-irb-if)#exit	Exits the IRB interface configuration mode and returns to the global configuration mode.

CE2

CE2#Configure Terminal	Enters the configuration mode.
CE2(config)#interface ce1	Enters the configuration mode for interface ce1.
CE2(config-if)# load-interval 30	Sets the load interval for the interface to 30 seconds.
CE2(config-if)#interface ce1.101	Enters the configuration mode for subinterface ce1.101.
CE2(config-if)# encapsulation dot1q 101	Configures 802.1Q encapsulation with VLAN ID 101 for the subinterface.
CE2(config-if)# ip address 201.201.201.2/24	Assigns the IPv4 address 201.201.201.2 with a subnet mask of /24 to the subinterface.
CE2(config-if)# ip router isis 101	Specifies ISIS as the routing protocol for IPv4.
CE2(config-if)#interface ce1.1001	Enters the configuration mode for subinterface ce1.1001.
CE2(config-if)# encapsulation dot1q 1001	Configures 802.1Q encapsulation with VLAN ID 1001 for the subinterface.
CE2(config-if)# ipv6 address 2001::2/64	Assigns the IPv6 address 2001::2 with a /64 prefix length to the subinterface.
CE2(config-if)# ipv6 router isis 101	Specifies ISIS as the routing protocol for IPv6.
CE2(config-if)#interface lo	Enters the configuration mode for the loopback interface.
CE2(config-if)# ip address 127.0.0.1/8	Assigns the primary IPv4 address 127.0.0.1 to the loopback interface with a subnet mask of /8.
CE2(config-if)# ip address 6.6.6.6/32 secondary	Adds a secondary IPv4 address, 6.6.6.6 with a /32 subnet mask, to the loopback interface.
CE2(config-if)# ipv6 address ::1/128	Assigns the primary IPv6 address ::1 to the loopback interface with a /128 prefix length.
CE2(config)#router isis 101	Enters the configuration mode for ISIS with process ID 101.
CE2(config-router)# is-type level-2-only	Configures ISIS as a level-2-only routing protocol.
CE2(config-router)# net 49.0001.0000.0000.0006.00	Sets the ISIS NET for this router.
CE2(config-router)# address-family ipv6	Enters the address-family configuration mode for IPv6.
CE2(config-router-af)# exit-address-family	Exits the address-family configuration for IPv6.
CE2(config)#line console 0	Enters the configuration mode for the console line.
CE2(config-line)# exec-timeout 0 0	Sets the console line's exec-timeout to 0.
CE2(config-line)#line vty 0 871	Enters the configuration mode for VTY lines 0 through 871.
CE2(config-router-af)# exit	Exits the from configuration mode.

Configure MTU over IRB

CE2(config)#int ce1	Enters interface configuration mode for int ce1.
CE2(config-irb-if)#mtu 9216	Sets the MTU to 9216 bytes.
CE2(config-irb-if)#commit	Commit the changes made to the interface configuration.
CE2(config-irb-if)#exit	Exits the IRB interface configuration mode and returns to the global configuration mode.

`CE2(config)#int  ce1.101`	Enters interface configuration mode for int ce1.101.
`CE2(config-irb-if)#mtu 9216`	Sets the MTU to 9216 bytes.
`CE2(config-irb-if)#commit`	Commit the changes made to the interface configuration.
`CE2(config-irb-if)#exit`	Exits the IRB interface configuration mode and returns to the global configuration mode.
`CE2(config)#int  ce1.1001`	Enters interface configuration mode for int ce1.1001.
`CE2(config-irb-if)#mtu 9216`	Sets the MTU to 9216 bytes.
`CE2(config-irb-if)#commit`	Commit the changes made to the interface configuration.
`CE2(config-irb-if)#exit`	Exits the IRB interface configuration mode and returns to the global configuration mode.

Implementation Examples

Scenario: Configure OSPF and ISIS protocols on an IRB interface with an assigned IP address.

Validation

```
CE1#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 101 VRF(default):
Neighbor ID     Pri   State            Dead Time   Address         Interface
Instance ID
2.2.2.2           1   Full/DR         00:00:37    101.101.101.1   po1.101
0
CE1#
CE1#
CE1#show ipv6 ospf neighbor

Total number of full neighbors: 1
OSPFv3 Process (1001)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
2.2.2.2           1   Full/DR         00:00:34    po1.1001   0
CE1#
CE1#
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"
C            1.1.1.1/32 is directly connected, lo, 00:16:58
```

```
C            99.99.99.0/24 is directly connected, ge2, 00:16:59
C            101.101.101.0/24 is directly connected, po1.101, 00:14:10
C            127.0.0.0/8 is directly connected, lo, 00:18:23
O E2         201.201.201.0/24 [110/1] via 101.101.101.1, po1.101, 00:06:14

Gateway of last resort is not set
CE1#
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, 00:18:30
C       1001::/64 via ::, po1.1001, 00:14:17
O E2    2001::/64 [110/20] via fe80::eac5:7aff:fea8:7cb3, po1.1001, 00:03:50
C       fe80::/64 via ::, po1.1001, 00:14:17
PE1  :
PE1#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
3.3.3.3           1   Full/DR         00:00:38    10.1.1.2        xe10                    0

Total number of full neighbors: 1
OSPF process 101 VRF(IpVrf1):
Neighbor ID     Pri   State            Dead Time   Address         Interface
Instance ID
1.1.1.1           1   Full/Backup      00:00:32    101.101.101.2   irb101
0

PE1#show ipv6 ospf neighbor

Total number of full neighbors: 1
OSPFv3 Process (IpVrf1)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
1.1.1.1           1   Full/Backup     00:00:33    irb1001    0

PE1#show evpn mpls tunnel
EVPN-MPLS Network tunnel Entries
Source           Destination      Status        Up/Down       Update        evpn-id
================================================================================
2.2.2.2          5.5.5.5          Installed     00:24:13      00:24:13      100
```

```
Total number of entries are 1

PE1#show bgp l2vpn evpn summary
BGP router identifier 2.2.2.2, local AS number 100
BGP table version is 2
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
5.5.5.5                 4   100   20        21      1     0     0  00:04:09
9      0      5      2      0      2

Total number of neighbors 1

Total number of Established sessions 1

PE1#show evpn mpls
EVPN-MPLS Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged

VPN-ID   EVI-Name     EVI-Type Type Interface ESI                          VLAN      DF-
Status Src-Addr         Dst-Addr
_____________________________________________________________________________________
100      ----         L3       NW   ----      ----                          ----      -
---      2.2.2.2          5.5.5.5
101      ----         --       AC   po1.101   --- Single Homed Port ---     ----      -
---      ----             ----
1001     ----         --       AC   po1.1001  --- Single Homed Port ---     ----      -
---      ----             ----

Total number of entries are 3

Note: Refer sub-interface config for VLAN information.
PE1#
PE1#
PE1#show bgp l2vpn evpn prefix-route

RD[5.5.5.5:200]
ESI             Eth-Tag Prefix-Length    IP-Address      GW-IPAddress    L3VNID/LABEL
Nexthop          Encap     Router-Mac
0               0       24               201.201.201.0   0.0.0.0         16
5.5.5.5          MPLS      e49d:73b1:c301
0               0       64               2001::          ::              16
5.5.5.5          MPLS      e49d:73b1:c301
PE1#
PE1#show bgp l2vpn evpn mac-ip

RD[2.2.2.2:100] VRF[MacVrf1]:
```

```
ESI                          Eth-Tag    Mac-Address    IP-Address
VNID/LABEL     L3VNID    Nexthop         GW-Type          Encap
0                           101        9819:2ccd:9320 --
17             0         2.2.2.2          --               MPLS
0                           101        9819:2ccd:9320 101.101.101.2
17             0         2.2.2.2          --               MPLS
0                           101        e8c5:7aa8:7cb3 101.101.101.1
17             0         2.2.2.2          --               MPLS
0                           201        e49d:73b1:c301 201.201.201.1
17             0         5.5.5.5          --               MPLS
0                           201        e8c5:7a76:583b --
17             0         5.5.5.5          --               MPLS
0                           201        e8c5:7a76:583b 201.201.201.2
17             0         5.5.5.5          --               MPLS
0                           1001       9819:2ccd:9320 --
18             0         2.2.2.2          --               MPLS
0                           1001       e8c5:7aa8:7cb3 1001::1
18             0         2.2.2.2          --               MPLS
0                           2001       e49d:73b1:c301 2001::1
18             0         5.5.5.5          --               MPLS
0                           2001       e8c5:7a76:583b --
18             0         5.5.5.5          --               MPLS

RD[5.5.5.5:100]
ESI                          Eth-Tag    Mac-Address    IP-Address
VNID/LABEL     L3VNID    Nexthop         GW-Type          Encap
0                           201        e49d:73b1:c301 201.201.201.1
17             0         5.5.5.5          --               MPLS
0                           201        e8c5:7a76:583b --
17             0         5.5.5.5          --               MPLS
0                           201        e8c5:7a76:583b 201.201.201.2
17             0         5.5.5.5          --               MPLS
0                           2001       e49d:73b1:c301 2001::1
18             0         5.5.5.5          --               MPLS
0                           2001       e8c5:7a76:583b --
18             0         5.5.5.5          --               MPLS

PE1#show mpls ftn-table
 Primary FTN entry with FEC: 3.3.3.3/32, id: 1, row status: Active, Tunnel-Policy: N/A,
State: Installed
  Owner: OSPF-SR, distance: 110, Action-type: Redirect to Tunnel, Exp-bits: 0x0,
Incoming DSCP: none
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Primary, QoS Resource id: 0, Description:
N/A, , Color: 0
     Cross connect ix: 3, in intf: - in label: 0 out-segment ix: 2
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: N/A, Stale: NO, out intf: xe10, out label: 3
    Nexthop addr: 10.1.1.2        cross connect ix: 3, op code: Push


 Primary FTN entry with FEC: 4.4.4.4/32, id: 2, row status: Active, Tunnel-Policy: N/A,
State: Installed
  Owner: OSPF-SR, distance: 110, Action-type: Redirect to Tunnel, Exp-bits: 0x0,
Incoming DSCP: none
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Primary, QoS Resource id: 0, Description:
N/A, , Color: 0
```

```
     Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 4
      Owner: OSPF-SR, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 4, owner: OSPF-SR, Stale: NO, out intf: xe10, out label:
16004
    Nexthop addr: 10.1.1.2        cross connect ix: 4, op code: Push


 Primary FTN entry with FEC: 5.5.5.5/32, id: 3, row status: Active, Tunnel-Policy: N/A,
State: Installed
  Owner: OSPF-SR, distance: 110, Action-type: Redirect to Tunnel, Exp-bits: 0x0,
Incoming DSCP: none
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Primary, QoS Resource id: 0, Description:
N/A, , Color: 0
     Cross connect ix: 5, in intf: - in label: 0 out-segment ix: 6
      Owner: OSPF-SR, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 6, owner: OSPF-SR, Stale: NO, out intf: xe10, out label:
16005
    Nexthop addr: 10.1.1.2        cross connect ix: 5, op code: Push

PE1#show mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN, ! - using backup
       B - BGP FTN, K - CLI FTN, (t) - tunnel, P - SR Policy FTN, (b) - bypass,
       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, (e) - FTN is ECMP

FTN-ECMP LDP: Disabled
Code    FEC               FTN-ID    Nhlfe-ID  Tunnel-id   Pri   LSP-Type     Out-Label
Out-Intf    ELC   Nexthop
   O>   3.3.3.3/32          1         3         0          Yes   LSP_DEFAULT  3
xe10        No    10.1.1.2
   O>   4.4.4.4/32          2         5         0          Yes   LSP_DEFAULT  16004
xe10        No    10.1.1.2
   O>   5.5.5.5/32          3         7         0          Yes   LSP_DEFAULT  16005
xe10        No    10.1.1.2

PE1#show mpls ilm-table
Codes: > - installed ILM, * - selected ILM, p - stale ILM, ! - using backup
       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

ILM-ECMP LDP: Disabled
Code    FEC/VRF/L2CKT    ILM-ID     In-Label    Out-Label   In-Intf    Out-Intf/VRF
Nexthop                  pri    LSP-Type
   B>   evpn:1001          5          18          Nolabel     N/A        N/A
127.0.0.1                Yes    LSP_DEFAULT
   B>   evpn:101           3          17          Nolabel     N/A        N/A
127.0.0.1                Yes    LSP_DEFAULT
   B>   IpVrf1             1          16          Nolabel     N/A        N/A             N/
A                      Yes    LSP_DEFAULT
```

```
   B>   evpn:101          2          26880       Nolabel     N/A        N/A
127.0.0.1               Yes    LSP_DEFAULT
   O>   4.4.4.4/32        8          16004       16004       N/A        xe10
10.1.1.2                Yes    LSP_DEFAULT
   O>   3.3.3.3/32        6          16003       3           N/A        xe10
10.1.1.2                Yes    LSP_DEFAULT
   O>   5.5.5.5/32        9          16005       16005       N/A        xe10
10.1.1.2                Yes    LSP_DEFAULT
   B>   evpn:1001         4          26881       Nolabel     N/A        N/A
127.0.0.1               Yes    LSP_DEFAULT
   O>   10.1.1.2/32       7          27520       3           N/A        xe10
10.1.1.2                Yes    LSP_DEFAULT

PE2   :
=========

PE2#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
4.4.4.4           1   Full/DR         00:00:28    30.1.1.1        ce3                    0
PE2#
PE2#
PE2#
PE2#show clns is-neighbors

Tag 101:  VRF : IpVrf1
System Id      Interface   State  Type Priority  Circuit Id
0000.0000.0006 irb101      Up     L2   64        0000.0000.0006.01
0000.0000.0006 irb1001     Up     L2   64        0000.0000.0006.02
PE2#
PE2#
PE2#
PE2#
PE2#show clns is-neighbors detail

Tag 101:  VRF : IpVrf1
System Id      Interface   State  Type Priority  Circuit Id
0000.0000.0006 irb101      Up     L2   64        0000.0000.0006.01
  L1  Adjacency ID: 1
  L2  Adjacency ID: 2
  Uptime: 00:11:21
  Area Address(es): 49.0001
  IP Address(es): 201.201.201.2
  Level-2 Protocols Supported: IPv4, IPv6
  Adjacency advertisement: Advertise

0000.0000.0006 irb1001     Up     L2   64        0000.0000.0006.02
  L1  Adjacency ID: 1
  L2  Adjacency ID: 2
```

```
  Uptime: 00:11:21
  Area Address(es): 49.0001
  IPv6 Address(es): fe80::eac5:7aff:fe76:583b
  Level-2 Protocols Supported: IPv4, IPv6
  Adjacency advertisement: Advertise

PE2#show evpn mpls tunnel
EVPN-MPLS Network tunnel Entries
Source           Destination      Status        Up/Down       Update        evpn-id
================================================================================
5.5.5.5          2.2.2.2          Installed     00:24:13      00:24:13      100

Total number of entries are 1
PE2#
PE2#
PE2#
PE2#show bgp l2vpn evpn summary
BGP router identifier 5.5.5.5, local AS number 100
BGP table version is 4
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   93        94       3     0      0  00:14:47
12      0      5      2      0      5

Total number of neighbors 1

Total number of Established sessions 1
PE2#
PE2#
PE2#
PE2#show bgp l2vpn evpn prefix-route

RD[2.2.2.2:200]
ESI             Eth-Tag Prefix-Length    IP-Address      GW-IPAddress    L3VNID/LABEL
Nexthop         Encap     Router-Mac
0               0       24               99.99.99.0      0.0.0.0         16
2.2.2.2         MPLS      e8c5:7aa8:7cb3
0               0       24               101.101.101.0   0.0.0.0         16
2.2.2.2         MPLS      e8c5:7aa8:7cb3
0               0       32               1.1.1.1         0.0.0.0         16
2.2.2.2         MPLS      e8c5:7aa8:7cb3
0               0       64               1001::          ::              16
2.2.2.2         MPLS      e8c5:7aa8:7cb3
0               0       64               9001::          ::              16
2.2.2.2         MPLS      e8c5:7aa8:7cb3
PE2#show bgp l2vpn evpn mac-ip

RD[2.2.2.2:100]
```

```
ESI                          Eth-Tag    Mac-Address    IP-Address
VNID/LABEL     L3VNID    Nexthop         GW-Type          Encap
0                            101        9819:2ccd:9320 --
17             0         2.2.2.2          --               MPLS
0                            101        9819:2ccd:9320 101.101.101.2
17             0         2.2.2.2          --               MPLS
0                            101        e8c5:7aa8:7cb3 101.101.101.1
17             0         2.2.2.2          --               MPLS
0                            1001       9819:2ccd:9320 --
18             0         2.2.2.2          --               MPLS
0                            1001       e8c5:7aa8:7cb3 1001::1
18             0         2.2.2.2          --               MPLS

RD[5.5.5.5:100] VRF[MacVrf2]:
ESI                          Eth-Tag    Mac-Address    IP-Address
VNID/LABEL     L3VNID    Nexthop         GW-Type          Encap
0                            101        9819:2ccd:9320 --
17             0         2.2.2.2          --               MPLS
0                            101        9819:2ccd:9320 101.101.101.2
17             0         2.2.2.2          --               MPLS
0                            101        e8c5:7aa8:7cb3 101.101.101.1
17             0         2.2.2.2          --               MPLS
0                            201        e49d:73b1:c301 201.201.201.1
17             0         5.5.5.5          --               MPLS
0                            201        e8c5:7a76:583b --
17             0         5.5.5.5          --               MPLS
0                            201        e8c5:7a76:583b 201.201.201.2
17             0         5.5.5.5          --               MPLS
0                            1001       9819:2ccd:9320 --
18             0         2.2.2.2          --               MPLS
0                            1001       e8c5:7aa8:7cb3 1001::1
18             0         2.2.2.2          --               MPLS
0                            2001       e49d:73b1:c301 2001::1
18             0         5.5.5.5          --               MPLS
0                            2001       e8c5:7a76:583b --
18             0         5.5.5.5          --               MPLS
PE2#show mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN, ! - using backup
       B - BGP FTN, K - CLI FTN, (t) - tunnel, P - SR Policy FTN, (b) - bypass,
       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, (e) - FTN is ECMP

FTN-ECMP LDP: Disabled
Code    FEC               FTN-ID    Nhlfe-ID  Tunnel-id   Pri   LSP-Type     Out-Label
Out-Intf    ELC   Nexthop
   O>   2.2.2.2/32          1         3         0          Yes   LSP_DEFAULT  16002
ce3         No    30.1.1.1
   O>   3.3.3.3/32          2         5         0          Yes   LSP_DEFAULT  16003
ce3         No    30.1.1.1
   O>   4.4.4.4/32          3         7         0          Yes   LSP_DEFAULT  3
ce3         No    30.1.1.1
PE2#
PE2#show mpls ilm-table
Codes: > - installed ILM, * - selected ILM, p - stale ILM, ! - using backup
```

```
       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

ILM-ECMP LDP: Disabled
Code    FEC/VRF/L2CKT    ILM-ID     In-Label    Out-Label   In-Intf    Out-Intf/VRF
Nexthop                 pri    LSP-Type
   B>   evpn:2001          5          18          Nolabel     N/A        N/A
127.0.0.1               Yes    LSP_DEFAULT
   B>   evpn:201           3          17          Nolabel     N/A        N/A
127.0.0.1               Yes    LSP_DEFAULT
   B>   IpVrf1            1          16          Nolabel     N/A        N/A             N/
A                     Yes    LSP_DEFAULT
   B>   evpn:201           2          26880       Nolabel     N/A        N/A
127.0.0.1               Yes    LSP_DEFAULT
   O>   3.3.3.3/32        7          16003       16003       N/A        ce3
30.1.1.1                Yes    LSP_DEFAULT
   O>   2.2.2.2/32        6          16002       16002       N/A        ce3
30.1.1.1                Yes    LSP_DEFAULT
   O>   4.4.4.4/32        8          16004       3           N/A        ce3
30.1.1.1                Yes    LSP_DEFAULT
   B>   evpn:2001          4          26881       Nolabel     N/A        N/A
127.0.0.1               Yes    LSP_DEFAULT
   O>   30.1.1.1/32       9          27520       3           N/A        ce3
30.1.1.1                Yes    LSP_DEFAULT
PE2#
PE2#
PE2#show mpls ftn-table
 Primary FTN entry with FEC: 2.2.2.2/32, id: 1, row status: Active, Tunnel-Policy: N/A,
State: Installed
  Owner: OSPF-SR, distance: 110, Action-type: Redirect to Tunnel, Exp-bits: 0x0,
Incoming DSCP: none
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Primary, QoS Resource id: 0, Description:
N/A, , Color: 0
     Cross connect ix: 3, in intf: - in label: 0 out-segment ix: 2
      Owner: OSPF-SR, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: OSPF-SR, Stale: NO, out intf: ce3, out label: 16002
    Nexthop addr: 30.1.1.1        cross connect ix: 3, op code: Push


 Primary FTN entry with FEC: 3.3.3.3/32, id: 2, row status: Active, Tunnel-Policy: N/A,
State: Installed
  Owner: OSPF-SR, distance: 110, Action-type: Redirect to Tunnel, Exp-bits: 0x0,
Incoming DSCP: none
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Primary, QoS Resource id: 0, Description:
N/A, , Color: 0
     Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 4
      Owner: OSPF-SR, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 4, owner: OSPF-SR, Stale: NO, out intf: ce3, out label: 16003
    Nexthop addr: 30.1.1.1        cross connect ix: 4, op code: Push
```

```
 Primary FTN entry with FEC: 4.4.4.4/32, id: 3, row status: Active, Tunnel-Policy: N/A,
State: Installed
  Owner: OSPF-SR, distance: 110, Action-type: Redirect to Tunnel, Exp-bits: 0x0,
Incoming DSCP: none
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Primary, QoS Resource id: 0, Description:
N/A, , Color: 0
     Cross connect ix: 5, 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: ce3, out label: 3
    Nexthop addr: 30.1.1.1        cross connect ix: 5, op code: Push


CE2#show clns is-neighbors

Tag 101:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id
0000.0000.0005 ce1.101     Up     L2   64        0000.0000.0006.01
0000.0000.0005 ce1.1001    Up     L2   64        0000.0000.0006.02

CE2#show clns is-neighbors detail

Tag 101:  VRF : default
System Id      Interface   State  Type Priority  Circuit Id
0000.0000.0005 ce1.101     Up     L2   64        0000.0000.0006.01
  L1  Adjacency ID: 1
  L2  Adjacency ID: 2
  Uptime: 00:13:41
  Area Address(es): 49.0001
  IP Address(es): 201.201.201.1
  Level-2 Protocols Supported: IPv4, IPv6
  Adjacency advertisement: Advertise

0000.0000.0005 ce1.1001    Up     L2   64        0000.0000.0006.02
  L1  Adjacency ID: 1
  L2  Adjacency ID: 2
  Uptime: 00:13:41
  Area Address(es): 49.0001
  IPv6 Address(es): fe80::e69d:73ff:feb1:c301
  Level-2 Protocols Supported: IPv4, IPv6
  Adjacency advertisement: Advertise

CE2#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"
i L2         1.1.1.1/32 [115/10] via 201.201.201.1, ce1.101, 00:10:22
C            6.6.6.6/32 is directly connected, lo, 00:13:54
i L2         99.99.99.0/24 [115/10] via 201.201.201.1, ce1.101, 00:10:22
i L2         101.101.101.0/24 [115/10] via 201.201.201.1, ce1.101, 00:10:22
C            127.0.0.0/8 is directly connected, lo, 00:18:45
C            201.201.201.0/24 is directly connected, ce1.101, 00:13:54

Gateway of last resort is not set
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, 00:18:50
i L2    1001::/64 [115/10] via fe80::e69d:73ff:feb1:c301, ce1.1001, 00:10:27
C       2001::/64 via ::, ce1.1001, 00:13:59
C       fe80::/64 via ::, ce1.1001, 00:13:59
```

Abbreviations

The following are some key abbreviations and their meanings relevant to this document:

Acronym	Description
ECMP	Equal-Cost Multipath
EVPN	Ethernet Virtual Private Netwrok
MPLS	Multiprotocol Label Switching
MPLS	Multiprotocol Label Switching
SR	Segment Routing
IRB	Integrated Routing
OSPF	Open Shortest Path First
ISIS	Intermediate System to Intermediate System

Glossary

The following provides definitions for key terms used throughout this document.

Single Home EVPN-MPLS	A network architecture that combines EVPN and MPLS to provide efficient and scalable Layer 2 and Layer 3 services within a network, particularly in SP environments.
IRB	A networking feature that enables the integration of Layer 3 IP routing and Layer 2 MAC address bridging within the same interface, simplifying network management and resource utilization.
OSPF	A dynamic and efficient link-state routing protocol used to determine the best path for data packets in an IP network. It is characterized by rapid convergence and adaptability, making it suitable for large and dynamic networks.
ISIS	A routing protocol designed for scalability and stability in computer networks, commonly used in large Service Provider networks. It provides a robust framework for routing information exchange.
Layer 3 Routing	Network routing operations at the Network Layer (Layer 3) of the OSI model, focusing on routing IP packets between different subnets or networks.
Layer 2 Bridging	Network bridging operations at the Data Link Layer (Layer 2) of the OSI model, handling the forwarding of data frames based on MAC addresses within the same network segment.
EVPN	Ethernet VPN, a technology that provides advanced and efficient methods for Layer 2 and Layer 3 services in Ethernet networks, often used in data centers and service provider environments.

Fall Back Option for RADIUS Authentication

Overview

Currently, the Remote Authentication Dial-In User Service (RADIUS) server authentication fallback to the local authentication server only when the RADIUS server is not reachable.

This behavior is modified in the current release to forward the authentication request to the local authentication server when the RADIUS authentication is failed or not reachable.

Feature Characteristics

The RADIUS authentication mechanism is enhanced to fallback to local authentication server when the user

- is not present on RADIUS server or
- authentication fails from RADIUS server

To implement the above requirements, the existing CLI `aaa authentication login default fallback error local non-existent-user vrf management` is used to enable fallback to local authentication server. This is disabled by default.

Note: For invalid secret key there is no fallback local authentication.
Console authentication is not supported for RADIUS.

Benefits

By default, the fallback to local authentication is applied when the RADIUS server is unreachable. For other scenarios, enable the fallback using the CLI.

Configuration

Below is the existing CLI used to enable the fallback local authentication server.

```
aaa authentication login default fallback error local non-existent-user vrf
  management
```

Validation

Configure `aaa authentication` console and verify console authentication:

```
OcNOS#con t
Enter configuration commands, one per line.  End with CNTL/Z.
OcNOS(config)#radius-server login host 1.1.1.2 seq-num 1 key 0 kumar
OcNOS(config)#commit
OcNOS(config)#aaa authentication login console group radius
OcNOS(config)#commit
OcNOS(config)#exit
OcNOS#exit

OcNOS#show users
```

```
Current user          : (*).  Lock acquired by user : (#).
CLI user              : [C].  Netconf users         : [N].
Location : Applicable to CLI users.
Session  : Applicable to NETCONF users.

Line       User          Idle        Location/Session PID    TYPE   Role
(*) 0 con 0 [C]ocnos      0d00h00m     ttyS0           5531   Remote network-admin
```

Enabled RADIUS local fallback and verify the authentication:

```
OcNOS(config)#aaa authentication login console group radius local
OcNOS(config)#commit
OcNOS(config)#exit
OcNOS#exit
OcNOS>exit

OcNOS>enable
OcNOS#show users
Current user          : (*).  Lock acquired by user : (#).
CLI user              : [C].  Netconf users         : [N].
Location : Applicable to CLI users.
Session  : Applicable to NETCONF users.

Line         User          Idle         Location/Session PID   TYPE   Role
(*) 0 con 0  [C]test        0d00h00m     ttyS0           5713  Local  network-engineer
130 vty 0    [C]test        0d00h01m     pts/0           5688  Local  network-engineer
OcNOS#
```

CLI Commands

aaa authentication login default fallback error

Use this command to enable fallback to local authentication for the default login if remote authentication is configured and all AAA servers are unreachable.

Use the `no` form of this command to disable fallback to local authentication.

Note: If you have specified `local` (use local authentication) in the *aaa authentication login default* command, you do not need to use this command to ensure that “fall back to local” occurs.

Command Syntax

```
aaa authentication login default fallback error local (vrf management|)
no aaa authentication login default fallback error local (vrf management|)
```

Parameters

`management`	Management VRF

Default

By default, AAA authentication is local.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#aaa authentication login default fallback error local vrf management
```

aaa authentication login default

Use this command to set the AAA authentication methods.

Use the `no` form of this command to set the default AAA authentication method (local).

Command Syntax

```
aaa authentication login default (vrf management|) ((group LINE) | (local (|none))
  | (none))
no aaa authentication login default (vrf management|) ((group) | (local (|none)) |
  (none))
```

Parameters

`group`		Use a server group list for authentication
	`LINE`	A space-separated list of up to 8 configured RADIUS or TACACS+, server group names followed by `local` or `none` or both `local` and `none`. The list can also include:
		`radius` All configured RADIUS servers
		`tacacs+` All configured TACACS+ servers
`local`		Use local authentication
`none`		No authentication
`management`		Management VRF

Default

By default, AAA authentication method is local

By default, groups: RADIUS or TACACS+

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#aaa authentication login default vrf management group radius
```

Abbreviations

Acronym	Description
AAA	accounting, authentication, authorization
RADIUS	Remote Authentication Dial-In User Service

Modified Extended ACL Deny Rule Behavior in VTY

Overview

The Access Control List refers to rules that allow or deny management protocols to control the network traffic, thus reducing network attacks from external sources.

Users can create Standard and Extended ACL rules and attach them to a virtual teletype (VTY) command line interface. These ACL rules are applied on both Management and Default virtual routing and forwarding (VRFs).

In the case of Standard ACLs, the permit/deny rules are applied only for management protocols such as Telnet/SSH/ SSH-Netconf protocols (port numbers 22,23,830)).

Extended ACL rules are applied as configured by the user, and it is not limited to management protocols only, unlike Standard ACLs.

When a user configures a rule with 'deny any any any' and attaches it to the VTY, it effectively blocks only the Telnet, SSH, and NetConf protocols on the control plane

For example, when a user configures a rule as below and attach them to VTY, If the deny ACL rule includes ’any’ value in protocol, only Telnet/SSH/SSH-NetConf protocols are denied.

```
ip access-list ssh-access
10 permit tcp 10.12.43.0/24 any eq ssh
20 deny any any any
```

Note: To deny any protocols other than Telnet/SSH/SSH-Netconf, create a deny rule with the specific protocol access on VTY. For example: To deny OSPF protocol from all the source and destination address, apply the rule, `10 deny ospf any any`.

Feature Characteristics

In general, the VTY ACLs are more specific to management protocols. Hence, the Extended ACL “Any” rule translation is enhanced to allow management protocols as follows:

- If the **deny** ACL rule includes any value in protocol, only Telnet/SSH/SSH-Netconf protocols are denied.
- The **permit** ACL rule is unchanged.

Benefits

This feature allows the customer to define a Extended ACL deny rule only to the management protocol without impacting other control protocols.

Configure a separate Extended ACL deny rule to deny protocols other than Telnet, SSH, and NetConf.

Configuration

Refer to *Access Control Lists Configurations* section of the *System Management Configuration* guide.

Implementation Examples

```
OcNOS#show running-config aclmgr
ip access-list ssh-access
 10 permit tcp 10.12.43.0/24 any eq ssh
 20 deny tcp 10.12.33.0/24 any eq 6513
 30 deny any 10.12.34.0/24 any
 40 deny any any any
!
line vty
 ip access-group ssh-access in

#####iptables o/p######

root@OcNOS:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  10.12.43.0/24        anywhere             tcp dpt:ssh
DROP       tcp  --  10.12.33.0/24        anywhere             tcp dpt:tls_netconf
DROP       tcp  --  10.12.34.0/24        anywhere             multiport dports
ssh,telnet,ssh_netconf
DROP       tcp  --  anywhere             anywhere             multiport dports
ssh,telnet,ssh_netconf
```

CLI Commands

Refer to *Access Control List Commands (Standard)* section of the *System Management Configuration* guide.

Abbreviations

Acronym	Expantion
ACL	Access control list
VRF	Virtual Routing Forwarding
VTY	Virtual teletype

400G PM Alarm

Overview

The 400G PM alarm monitors and detects performance issues like the bit error rate and signal power in the network. This feature extends OcNOS performance-related monitoring capabilities and provides additional performance monitors and alarms.

400G coherent module is a high-speed optical transceiver capable of transferring data long-distance with high performance. Its compatibility with single-mode optical fiber makes a robust combination in delivering a high-quality network transmission.

Feature Characteristics

Access the additional set of 400G performance monitoring parameters, such as Transmitter FEC Detected Degrade (Tx FDD), Transmitter FEC Excessive Degrade (Tx FED), Receiver FEC Detected Degrade (Rx FDD), and Receiver FEC Excessive Degrade (Rx FED), to receive an automatic alarm notification on the CLI interface, via an SNMP trap, or thorugh the Netconf interface. The automatic alarm is triggered when the monitored parameter crosses the configured value.

For 400G coherent modules, use this feature to configure custom thresholds for Tx FDD, Tx FED, Rx FDD, Rx FED, Tx Power, Rx Total Power, and Rx Signal Power through a new set of CLI configuration commands and Netconf interface.

Note: Configuration of the threshold value is not possible through SNMP.

Benefits

The capability of this feature to configure the alarm threshold allows customization based on the network requirements and expected error rates. If the signal power exceeds the configured threshold value, it sends a notification to take action that prevents the receiving devices from potential damage.

Prerequisites

The availability of specific parameters or flags is vendor-specific, so read the 400G transceiver data-sheet to determine the available parameters or flags.

Configuration

This section shows the configuration of the 400G PM Alarm.

Topology

R1 is connected to the R2 by 400G ZR/ZR+ transceiver. The interface cd 10 and cd20 are 400G interfaces where the 400G ZR/ZR+ transceiver is connected. Cd10 is the host interface and here the configuration of the threshold value for the host-lane occurs. In cd20 interface, we can configure the media-lane threshold value.

400G PM alarm

Media-lane Configuration

The below configuration is to set up the threshold value for the media lane.

R1

`R1#configure terminal`	Enter configure mode.
`R1(config)#qsfp-dd 20`	Enter QSFP-DD module configuration.
`R1(config-qsfp-dd)#media-lane 1`	Enter the Media lane configuration
`R1(config-qsfp-dd-media)#threshold rx-fdd`	Enter the BER threshold for FDD under Threshold configuration
`R1(config-qsfp-dd-media-thresh)#ha 0.365`	Configure the High alarm threshold
`R1(config-qsfp-dd-media-thresh)#la 0.165`	Configure the low alarm threshold
`R1(config-qsfp-dd-media-thresh)#exit`	Exit threshold Configure mode.
`R1(config-qsfp-dd-media)#threshold rx-fed`	Enter the BER threshold for FED under Threshold configuration
`R1(config-qsfp-dd-media-thresh)#ha 0.365`	Configure the High alarm threshold
`R1(config-qsfp-dd-media-thresh)#la 0.165`	Configure the low alarm threshold
`R1(config-qsfp-dd-media-thresh)#exit`	Exit threshold Configure mode.
`R1(config-qsfp-dd-media)#threshold rx-signal-power`	Enter the threshold for Rx Signal Power under Threshold configuration
`R1(config-qsfp-dd-media-thresh)#ha 4`	Configure the High alarm threshold
`R1(config-qsfp-dd-media-thresh)#la -3`	Configure the low alarm threshold
`R1(config-qsfp-dd-media-thresh)#hw 5`	Configure the High warning threshold
`R1(config-qsfp-dd-media-thresh)#lw -5`	Configure the low warning threshold
`R1(config-qsfp-dd-media-thresh)#exit`	Exit threshold Configure mode.
`R1(config-qsfp-dd-media)#threshold rx-total-power`	Enter the threshold for Rx Total Power under Threshold configuration
`R1(config-qsfp-dd-media-thresh)#ha 2`	Configure the High alarm threshold
`R1(config-qsfp-dd-media-thresh)#la -2`	Configure the low alarm threshold
`R1(config-qsfp-dd-media-thresh)#hw 3`	Configure the High warning threshold
`R1(config-qsfp-dd-media-thresh)#lw -3`	Configure the low warning threshold
`R1(config-qsfp-dd-media-thresh)#exit`	Exit threshold Configure mode.
`R1(config-qsfp-dd-media)#exit`	Exit media Configure mode.
`R1(config-qsfp-dd)#commit`	Commit the candidate configuration to the running configuration

Host-lane Configuration

The below configuration is to set up the threshold value for the host lane.

R1

`R1#configure terminal`	Enter Configure mode
`R1(config)#qsfp-dd 10`	Enter QSFP-DD module configuration
`R1(config-qsfp-dd)#Host-lane 1`	Enter the Media lane configuration
`R1(config-qsfp-dd-host)#threshold tx-fdd`	Enter the BER threshold for FDD under Threshold configuration
`R1(config-qsfp-dd-host-thresh)#ha 0.365`	Configure the High alarm threshold
`R1(config-qsfp-dd-host-thresh)#la 0.165`	Configure the low alarm threshold
`R1(config-qsfp-dd-host-thresh)#exit`	Exit threshold Configure mode.
`R1(config-qsfp-dd-host)#threshold tx-fed`	Enter the BER threshold for FED under Threshold configuration
`R1(config-qsfp-dd-host-thresh)#ha 0.765`	Configure the High alarm threshold
`R1(config-qsfp-dd-host-thresh)#la 0.665`	Configure the Low alarm threshold
`R1(config-qsfp-dd-host-thresh)#exit`	Exit threshold Configure mode.
`R1(config-qsfp-dd-media)#exit`	Exit media Configure mode.
`R1(config-qsfp-dd)#commit`	Commit the candidate configuration to the running configuration

Validation

R1

The below is the show output of media lane threshold parameter:

```
qsfp-dd 20
 media-lane 1
  threshold rx-fdd
   ha 0.365500
   la 0.165000
  threshold rx-fed
   ha 0.365000
   la 0.165000
  threshold rx-total-power
   ha 2.000000
   la -2.000000
   hw 3.000000
   lw -3.000000
  threshold rx-signal-power
   ha 4.000000
   la -3.000000
   hw 5.000000
   lw -5.000000
```

```
!
!
end
```

Verify the user-threshold media-lane:

```
#show qsfp-dd 20 user-threshold status media
Codes: [HA : High Alarm], [LA : Low Alarm], [HW : High Warning], [LW : Low Warning]
Port Number                    : 20
-------------------------------------------------------------------------------------
      Threshold      | Lane | User Config | H/W Config | Minimum   | Maximum   | Unit |
-------------------------------------------------------------------------------------
 Rx FDD Active       | 1    | 3.65e-01    | 3.65e-01   | 0.00e+00 | 1.00e+00 | NA   |
 Rx FDD Clear        | 1    | 1.65e-01    | 1.65e-01   | 0.00e+00 | 1.00e+00 | NA   |
 Rx FED Active       | 1    | 3.65e-01    | 3.65e-01   | 0.00e+00 | 1.00e+00 | NA   |
 Rx FED Clear        | 1    | 1.65e-01    | 1.65e-01   | 0.00e+00 | 1.00e+00 | NA   |
 Rx Total Power HA   | 1    | 2.00        | 2.00       | 0.00     | 15.00    | dBm  |
 Rx Total Power HW   | 1    | 3.00        | 3.00       | -10.00   | 13.00    | dBm  |
 Rx Total Power LW   | 1    | -3.00       | -          | -33.00   | -10.00   | dBm  |
 Rx Total Power LA   | 1    | -2.00       | -          | -40.00   | -15.00   | dBm  |
 Rx Signal Power HA  | 1    | 4.00        | 4.00       | 0.00     | 15.00    | dBm  |
 Rx Signal Power HW  | 1    | 5.00        | 5.00       | -10.00   | 13.00    | dBm  |
 Rx Signal Power LW  | 1    | -5.00       | -          | -33.00   | -10.00   | dBm  |
 Rx Signal Power LA  | 1    | -3.00       | -          | -40.00   | -15.00   | dBm  |
```

The below is the show output of host lane threshold parameter:

```
qsfp-dd 10
 host-lane 1
  threshold tx-fdd
   ha 0.365000
   la 0.165000
  threshold tx-fed
   ha 0.765000
   la 0.665000
```

Verify the user-threshold host-lane:

```
#show qsfp-dd 10 user-threshold status host
Port Number                    : 20
-------------------------------------------------------------------------------------
      Threshold      | Lane | User Config | H/W Config | Minimum   | Maximum   | Unit |
-------------------------------------------------------------------------------------
 Tx FDD Active       | 1    | 3.65e-01    | 3.65e-01   | 0.00e+00 | 1.00e+00 | NA   |
 Tx FDD Clear        | 1    | 1.65e-01    | 1.65e-01   | 0.00e+00 | 1.00e+00 | NA   |
 Tx FED Active       | 1    | 7.65e-01    | 7.65e-01   | 0.00e+00 | 1.00e+00 | NA   |
 Tx FED Clear        | 1    | 6.65e-01    | 6.65e-01   | 0.00e+00 | 1.00e+00 | NA   |
```

Global Threshold Configuration

The below configuration is to set up the threshold value for the global threshold.

R1

R1#configure terminal	Enter Configure mode
R1(config)#qsfp-dd 20	Enter QSFP-DD module configuration
R1(config-qsfp-dd)#threshold rx-fdd	Enter the media Rx BER threshold for FDD under Threshold Configuration
R1(config-qsfp-dd-thresh)#ha 0.963	conc Configure the High alarm threshold
R1(config-qsfp-dd-thresh)#la 0.763	conc Configure the Low alarm threshold
R1(config-qsfp-dd-thresh)#exit	Exit threshold Configure mode.
R1(config-qsfp-dd)#threshold rx-fed	Enter the media Rx BER threshold for FED under Threshold Configuration
R1(config-qsfp-dd-thresh)#ha 0.863	conc Configure the High alarm threshold
R1(config-qsfp-dd-thresh)#la 0.463	conc Configure the Low alarm threshold
R1(config-qsfp-dd-thresh)#exit	Exit threshold Configure mode.
R1(config-qsfp-dd)#threshold rx-signal-power	Enter the media threshold for Rx Signal Power under Threshold Configuration
R1(config-qsfp-dd-thresh)#ha 6	conc Configure the High alarm threshold
R1(config-qsfp-dd-thresh)#la -6	conc Configure the Low alarm threshold
R1(config-qsfp-dd-thresh)#hw 4	conc Configure the High warning threshold
R1(config-qsfp-dd-thresh)#lw -4	conc Configure the Low warning threshold
R1(config-qsfp-dd-thresh)#exit	Exit threshold Configure mode. Exit threshold Configure mode.
R1(config-qsfp-dd)#threshold rx-total-power	Enter the media threshold for Rx Signal Power under Th Enter the media threshold for Rx Total Power under Threshold Configuration
R1(config-qsfp-dd-thresh)#ha 7	conc Configure the High alarm threshold
R1(config-qsfp-dd-thresh)#la -7	conc Configure the Low alarm threshold
R1(config-qsfp-dd-thresh)#hw 9	conc Configure the High warning threshold
R1(config-qsfp-dd-thresh)#lw -9	conc Configure the Low warning threshold
R1(config-qsfp-dd-thresh)#exit	Exit threshold Configure mode. Exit threshold Configure mode.
R1(config)#qsfp-dd 10	Enter QSFP DD module configuration.
R1(config-qsfp-dd)#threshold tx-fdd	Enter the host Rx BER threshold for FDD under Threshold Configuration
R1(config-qsfp-dd-thresh)#ha 0.456	conc Configure the High alarm threshold
R1(config-qsfp-dd-thresh)#la 0.321	conc Configure the Low alarm threshold
R1(config-qsfp-dd-thresh)#exit	Exit threshold Configure mode.
R1(config-qsfp-dd)#threshold tx-fed	Enter the host Rx BER threshold for FED under Threshold Configuration
R1(config-qsfp-dd-thresh)#ha 0.864	conc Configure the High alarm threshold
R1(config-qsfp-dd-thresh)#la 0.666	conc Configure the Low alarm threshold
R1(config-qsfp-dd-thresh)#exit	Exit threshold Configure mode.

Validation

R1

The below is the show output of global threshold parameter:

```
#sh running-config
qsfp-dd 20
 threshold rx-fdd
  ha 0.963000
  la 0.763000
 threshold rx-fed
  ha 0.863000
  la 0.463000
 threshold rx-total-power
  ha 7.000000
  la -7.000000
  hw 9.000000
  lw -9.000000
 threshold rx-signal-power
  ha 6.000000
  la -6.000000
  hw 4.000000
  lw -4.000000
qspf-dd 10
 threshold tx-fdd
  ha 0.456000
  la 0.321000
 threshold tx-fed
  ha 0.864000
  la 0.666000
```

Verify the global threshold:

```
#sh qsfp-dd 20 user-threshold status media
Codes: [HA : High Alarm], [LA : Low Alarm], [HW : High Warning], [LW : Low Warning]
Port Number                    : 20
-------------------------------------------------------------------------------------
      Threshold      | Lane | User Config | H/W Config | Minimum   | Maximum   | Unit |
-------------------------------------------------------------------------------------
 Rx FDD Active       | 1    | 9.63e-01    | 9.63e-01   | 0.00e+00 | 1.00e+00 | NA   |
 Rx FDD Clear        | 1    | 7.63e-01    | 7.63e-01   | 0.00e+00 | 1.00e+00 | NA   |
 Rx FED Active       | 1    | 8.63e-01    | 8.63e-01   | 0.00e+00 | 1.00e+00 | NA   |
 Rx FED Clear        | 1    | 4.63e-01    | 4.63e-01   | 0.00e+00 | 1.00e+00 | NA   |
 Rx Total Power HA   | 1    | 7.00        | 7.00       | 0.00     | 15.00    | dBm  |
 Rx Total Power HW   | 1    | 9.00        | 9.00       | -10.00   | 13.00    | dBm  |
 Rx Total Power LW   | 1    | -9.00       | -          | -33.00   | -10.00   | dBm  |
 Rx Total Power LA   | 1    | -7.00       | -          | -40.00   | -15.00   | dBm  |
 Rx Signal Power HA  | 1    | 6.00        | 6.00       | 0.00     | 15.00    | dBm  |
 Rx Signal Power HW  | 1    | 4.00        | 4.00       | -10.00   | 13.00    | dBm  |
 Rx Signal Power LW  | 1    | -4.00       | -          | -33.00   | -10.00   | dBm  |
```

```
 Rx Signal Power LA  | 1    | -6.00       | -          | -40.00   | -15.00   | dBm  |

#sh qsfp-dd 10 user-threshold status host
Port Number                    : 10
-------------------------------------------------------------------------------------
      Threshold      | Lane | User Config | H/W Config | Minimum  | Maximum  | Unit |
-------------------------------------------------------------------------------------
 Tx FDD Active       | 1    | 4.56e-01    | 4.56e-01   | 0.00e+00 | 1.00e+00 | NA   |
 Tx FDD Clear        | 1    | 3.21e-01    | 3.21e-01   | 0.00e+00 | 1.00e+00 | NA   |
 Tx FED Active       | 1    | 8.64e-01    | 8.64e-01   | 0.00e+00 | 1.00e+00 | NA   |
 Tx FED Clear        | 1    | 6.66e-01    | 6.66e-01   | 0.00e+00 | 1.00e+00 | NA   |
```

New CLI Commands

ha

Use this command to set the high alarm threshold value for the Tx FDD, Tx FED, Rx FDD, Rx FED, Tx power, Rx Total Power, and Rx Signal Power performance monitoring parameters. High alarm threshold is the highest parameter value for the 400G transceiver to operate safely and reliably. For FEC Detected Degrade (FDD) and FEC Excessive Degrade (FED) monitoring, this command sets the active threshold. FDD suggests that the FEC has detected errors in data transmission. The alarm notification is triggered if the average BER exceeds the configured FDD value.

Command Syntax

```
ha VALUE
no ha
```

Parameters

VALUE	high alarm value

Command Mode

Global threshold mode, host-lane threshold mode, and media-lane threshold mode.

Applicability

This command was introduced in OcNOS version 6.4.1.

Example

The below configuration shows to configure the high warning threshold:

```
OcNOS#configure terminal
OcNOS(config)#qsfp-dd 48
OcNOS(config-qsfp-dd)#threshold tx-fdd
OcNOS(config-qsfp-dd-thresh)#ha 0.9876
OcNOS(config-qsfp-dd-thresh)#commit
OcNOS(config-qsfp-dd-thresh)#no ha
OcNOS(config-qsfp-dd-thresh)#commit
```

hw

Use this command to set the high warning threshold value for Tx power, Rx Total Power, and Rx Signal Power. High warning threshold is the highest parameter value for the 400G transceiver, exceeding which the transceiver performance and operational issues can occur.

Note: This command has no effect for FED and FDD thresholds.

Command Syntax

```
hw VALUE
no hw
```

Parameters

VALUE	high warning value

Command Mode

Global threshold mode, host-lane threshold mode, and media-lane threshold mode.

Applicability

This command was introduced in OcNOS version 6.4.1.

Example

The below configuration shows to configure the high warning threshold:

```
OcNOS#configure terminal
OcNOS(config)#qsfp-dd 48
OcNOS(config-qsfp-dd)#threshold rx-total-power
OcNOS(config-qsfp-dd-thresh)#threshold rx-total-power
OcNOS(config-qsfp-dd-thresh)#hw 3.0
OcNOS(config-qsfp-dd-thresh)#commit
OcNOS(config-qsfp-dd-thresh)#no hw
OcNOS(config-qsfp-dd-thresh)#commit
```

la

Use this command to set the low alarm threshold value based on the vendor-specific threshold for all the performance monitoring parameters Tx FDD, Tx FED, Rx FDD, Rx FED, Tx power, Rx Total Power, and Rx Signal Power threshold value. Low alarm threshold is the lowest parameter value for the 400G transceiver to operate with reliability. For FDD and FED monitoring this command sets the clear threshold.

Command Syntax

```
la VALUE
no ha
```

Parameters

VALUE	low alarm value

Command Mode

Global threshold mode, host-lane threshold mode, and media-lane threshold mode.

Applicability

This command was introduced in OcNOS version 6.4.1.

Example

The below configuration shows to configure the low alarm threshold:

```
OcNOS#configure terminal
OcNOS(config)#qsfp-dd 48
OcNOS(config-qsfp-dd)#threshold rx-fed
OcNOS(config-qsfp-dd-thresh)#la 0.001234
OcNOS(config-qsfp-dd-thresh)#commit
OcNOS(config-qsfp-dd-thresh)#no la
OcNOS(config-qsfp-dd-thresh)#commit
```

lw

Use this command to set the low warning threshold value. Low warning threshold is the lowest parameter value for the 400G transceiver, below which the transceiver performance and operational issues can occur.

Note: This command has no effect for FED and FDD thresholds.

Command Syntax

```
lw VALUE
no lw
```

Parameters

`lw`	low warning value

Command Mode

Global threshold mode, host-lane threshold mode, and media-lane threshold mode.

Applicability

This command was introduced in OcNOS version 6.4.1.

Example

The below configuration shows to configure the low warning threshold:

```
OcNOS#configure terminal
OcNOS(config)#qsfp-dd 48
OcNOS(config-qsfp-dd)#threshold rx-total-power
OcNOS(config-qsfp-dd-thresh)#lw -1.0
OcNOS(config-qsfp-dd-thresh)#commit
OcNOS(config-qsfp-dd-thresh)#no lw
OcNOS(config-qsfp-dd-thresh)#commit
```

show qsfp-dd user-threshold status

Use this command to show the current configuration status of user thresholds.

Command Syntax

```
show qsfp-dd <PORT> user-threshold status (host|media)
```

Parameters

PORT	The front panel port number of the device where the transceiver is connected
host	Host side config status
media	Media side config status

Command Mode

Exec mode and privileged Exec mode.

Applicability

This command was introduced in OcNOS version 6.4.1.

Example

This below show command displays the hardware state of the programmed user thresholds.

```
OcNOS#show qsfp-dd 48 user-threshold status host

Port Number                    : 48

-------------------------------------------------------------------------
      Threshold      | Lane | User Config | H/W Config | Minimum  | Maximum  |
-------------------------------------------------------------------------
 Tx FDD Active       | 1    | 9.88e-01    | 9.87e-01   | 0.00e+00 | 1.00e+00 |
 Tx FDD Clear        | 1    | 5.43e-03    | 5.43e-03   | 0.00e+00 | 1.00e+00 |
 Tx FED Active       | 1    | 5.43e-01    | 5.43e-01   | 0.00e+00 | 1.00e+00 |
 Tx FED Clear        | 1    | 9.88e-03    | 9.87e-03   | 0.00e+00 | 1.00e+00 |

OcNOS#show qsfp-dd 48 user-threshold status media

Codes: [HA : High Alarm], [LA : Low Alarm], [HW : High Warning], [LW : Low
Warning]

Port Number                    : 48

-------------------------------------------------------------------------
      Threshold      | Lane | User Config | H/W Config | Minimum  | Maximum  |
-------------------------------------------------------------------------
 Rx FDD Active       | 1    | 1.23e-01    | 1.23e-01   | 0.00e+00 | 1.00e+00 |
 Rx FDD Clear        | 1    | 6.79e-03    | 6.78e-03   | 0.00e+00 | 1.00e+00 |
 Rx FED Active       | 1    | 6.79e-01    | 6.78e-01   | 0.00e+00 | 1.00e+00 |
 Rx FED Clear        | 1    | 1.23e-03    | 1.23e-03   | 0.00e+00 | 1.00e+00 |
 Rx Total Power HA   | 1    | 4.00        | 4.00       | -26.00   | 9.00     |
 Rx Total Power HW   | 1    | 3.00        | 3.00       | -26.00   | 9.00     |
 Rx Total Power LW   | 1    | -3.00       | -3.00      | -26.00   | 9.00     |
 Rx Total Power LA   | 1    | -4.00       | -4.00      | -26.00   | 9.00     |
 Rx Signal Power HA  | 1    | 2.00        | 2.00       | -26.00   | 9.00     |
 Rx Signal Power HW  | 1    | 1.00        | 1.00       | -26.00   | 9.00     |
 Rx Signal Power LW  | 1    | -1.00       | -1.00      | -26.00   | 9.00     |
 Rx Signal Power LA  | 1    | -2.00       | -2.00      | -26.00   | 9.00     |
```

show qsfp-dd 48 user-threshold status host output details

Field	Description
Threshold	The parameters that are monitored.
Lane	Displays the channel number where the thresholds are applied.
User Config	Displays what the user has configured.
H/W Config	Displays what is programmed in the transceiver hardware.
Minimum	The lowest values that are allowed to be used for this configuration.
Maximum	The highest values that are allowed to be used for this configuration.

threshold (host-lane mode)

Use this command to enter host lane level user threshold configuration mode. Host lane mode is a configuration mode that allows configuring specific values for the host lanes.Host lanes are wires that carry the electrical signal from the host interface to the module and vice-versa.

Command Syntax

```
threshold (tx-fdd|tx-fed)
```

Parameters

`tx-fdd`	Tx FDD
`tx-fed`	Tx FED

Command Mode

host-lane mode.

Applicability

This command was introduced in OcNOS version 6.4.1.

Example

The below configuration shows to configure the host-lane threshold:

```
OcNOS#configure terminal
OcNOS(config)#qsfp-dd 48
OcNOS(config-qsfp-dd)#host-lane 1
OcNOS(config-qsfp-dd-host)#threshold tx-fdd
OcNOS(config-qsfp-dd-host-thresh)#ha 0.9876
OcNOS(config-qsfp-dd-host-thresh)#la 0.005432
OcNOS(config-qsfp-dd-host-thresh)#threshold tx-fed
OcNOS(config-qsfp-dd-host-thresh)#ha 0.5432
OcNOS(config-qsfp-dd-host-thresh)#la 0.009876
OcNOS(config-qsfp-dd-host-thresh)#commit
```

threshold (media-lane mode)

Use this command to enter media lane level user threshold configuration mode. Media lane mode is a configuration mode that allows configuring specific values for each media lane. Media lanes are the electrical wire pairs (copper cables) or optical fibers that carry signals from the module to the other router and vice-versa.

Command Syntax

```
threshold (rx-fdd|rx-fed|rx-total-power|rx-signal-power)
```

Parameters

`rx-fdd`	Rx FDD
`rx-fed`	Rx FED
`rx-total-power`	Rx Total Power
`rx-signal-power`	Rx Signal Power

Command Mode

Media-lane mode.

Applicability

This command was introduced in OcNOS version 6.4.1.

Example

The below configuration shows to configure the media-lane threshold:

```
OcNOS#configure terminal
OcNOS(config)#qsfp-dd 48
OcNOS(config-qsfp-dd)#media-lane 1
OcNOS(config-qsfp-dd-media)#threshold rx-fdd
OcNOS(config-qsfp-dd-media-thresh)#ha 0.1234
OcNOS(config-qsfp-dd-media-thresh)#la 0.006789
OcNOS(config-qsfp-dd-media-thresh)#threshold rx-fed
OcNOS(config-qsfp-dd-media-thresh)#ha 0.6789
OcNOS(config-qsfp-dd-media-thresh)#la 0.001234
OcNOS(config-qsfp-dd-media-thresh)#threshold rx-total-power
OcNOS(config-qsfp-dd-media-thresh)#ha 4
OcNOS(config-qsfp-dd-media-thresh)#hw 3
OcNOS(config-qsfp-dd-media-thresh)#lw -3
OcNOS(config-qsfp-dd-media-thresh)#la -4
OcNOS(config-qsfp-dd-media-thresh)#threshold rx-signal-power
OcNOS(config-qsfp-dd-media-thresh)#ha 2
OcNOS(config-qsfp-dd-media-thresh)#hw 1
OcNOS(config-qsfp-dd-media-thresh)#lw -1
OcNOS(config-qsfp-dd-media-thresh)#la -2
OcNOS(config-qsfp-dd-media-thresh)#commit
```

threshold (QSFP-DD mode)

Use this command to enter global level user threshold configuration mode.In global mode, configure the same threshold value across all host or media lanes.

Command Syntax

```
threshold (tx-fdd|tx-fed|rx-fdd|rx-fed|rx-total-power|rx-signal-power)
```

Parameters

`tx-fdd`	Tx FDD
`tx-fed`	Tx FED
`rx-fdd`	Rx FDD
`rx-fed`	Rx FED
`rx-total-power`	Rx Total Power
`rx-signal-power`	Rx Signal Power

Command Mode

QSFP-DD mode.

Applicability

This command was introduced in OcNOS version 6.4.1.

Example

The below configuration shows to configure the threshold in global mode:

```
OcNOS#configure terminal
OcNOS(config)#qsfp-dd 48
OcNOS(config-qsfp-dd)#threshold tx-fdd
OcNOS(config-qsfp-dd-thresh)#ha 0.9876
OcNOS(config-qsfp-dd-thresh)#la 0.005432
OcNOS(config-qsfp-dd-thresh)#threshold tx-fed
OcNOS(config-qsfp-dd-thresh)#ha 0.5432
OcNOS(config-qsfp-dd-thresh)#la 0.009876
OcNOS(config-qsfp-dd-thresh)#threshold rx-fdd
OcNOS(config-qsfp-dd-thresh)#ha 0.1234
OcNOS(config-qsfp-dd-thresh)#la 0.006789
OcNOS(config-qsfp-dd-thresh)#threshold rx-fed
OcNOS(config-qsfp-dd-thresh)#ha 0.6789
OcNOS(config-qsfp-dd-thresh)#la 0.001234
OcNOS(config-qsfp-dd-thresh)#threshold rx-total-power
OcNOS(config-qsfp-dd-thresh)#ha 4
OcNOS(config-qsfp-dd-thresh)#hw 3
OcNOS(config-qsfp-dd-thresh)#lw -3
OcNOS(config-qsfp-dd-thresh)#la -4
OcNOS(config-qsfp-dd-thresh)#threshold rx-signal-power
OcNOS(config-qsfp-dd-thresh)#ha 2
OcNOS(config-qsfp-dd-thresh)#hw 1
OcNOS(config-qsfp-dd-thresh)#lw -1
OcNOS(config-qsfp-dd-thresh)#la -2
OcNOS(config-qsfp-dd-thresh)#commit
```

Abbreviations

The following are some key abbreviations and their meanings relevant to this document:

Acronym	Description
BER	Bit Error Rate
FDD	FEC detected degrade
FEC	Forward error correction
PM	Performance Monitoring
FED	FEC excessive degrade
Rx	Receiver
Tx	Transmitter
SNMP	Simple Network Management Protocol

Glossary

The following provides definitions for key terms used throughout this document.

400G coherent module	400G coherent module is a high-speed optical transceiver capable of transferring data long-distance with high performance. Its compatibility with single-mode optical fiber makes a robust combination in delivering a high-quality network transmission.
Active threshold	This parameter threshold value triggers alarm notification.
Clear threshold	This parameter threshold value does not trigger alarm notification.
FDD	FEC Detected Degrade suggests that the FEC has detected errors in data transmission. The alarm notification is triggered if the average BER exceeds the configured FDD value.
FEC	FEC is a technique that detects and corrects errors during data transmission to maintain the reliability of the communication system.
FED	FEC Excessive Degrade suggests that the FEC has detected very high errors in data transmission. FED is a more severe error condition than FDD and needs more attention. The alarm notification is triggered if the average BER exceeds the configured FED value.
Global mode	In global mode, configure the same threshold value across all host or media lanes.
High alarm threshold	This is the highest parameter value for the 400G transceiver to operate safely. When a given parameter value crosses this threshold, the transceiver operation is unreliable, or the transceiver hardware could get damaged.
High warning threshold	This is the highest parameter value that limits the optimal operation zone. The transceiver can operate after a parameter crosses this threshold, but performance and operational issues can occur.

Host lane	Host lanes are wires that carry the electrical signal from the host interface to the module and vice-versa.
Host-lane mode	Host lane mode is a configuration mode that allows configuring specific values for the host lanes. Contrary to the global mode level that configures the same value across all host lanes.
Low alarm threshold	This is the lowest parameter value for the 400G transceiver to operate safely. When a given parameter value crosses this threshold, the transceiver operation is unreliable.
Low warning threshold	This is the lowest parameter value that limits the optimal operation zone. The transceiver can operate after a parameter crosses this threshold, but performance and operational issues can occur.
Media lane	Media lanes are the electrical wire pairs (copper cables) or optical fibers that carry signals from the module to the other router and vice-versa.
Media-lane mode	Media lane mode is a configuration mode that allows configuring specific values for each media lane (per fiber cable physical channel). Contrary to the global mode level that configures the same value across all media lanes.

Improved Network Resilience

This section describes the load balancing, network resilience, failover and error handling enhancements and new features introduced in the Release 6.4.2 and Release 6.4.1.

Release 6.4.2

- Limitation on Generating SFlow Data
- Entropy Labels for ISIS or OSPF Segment Routing
- EVPN Active-Standby - Single-Active

Release 6.4.1

- ERPS with CFM Down-MEP over Bridge-Domain
- RSVP Detour Over Ring Topology
- Commit Rollback
- EVPN Active-Standby - Port-Active
- Anycast Gateway Routing for Multiple Subnets in EVPN-IRB

Limitation on Generating SFlow Data

Overview

Feature Characteristics

On Qumran1 (Q1) and Qumran2 (Q2) devices the number of different sampling rates that can be configured are limited.

Limitations

- The Qumran 1 (Q1) platform is equipped to handle a total of 9 unique sampling rates. Ingress and egress sampling rate is counted separately.
- The Qumran 2 (Q2) platform is equipped to handle a total of 15 unique sampling rates.
    - For egress, maximum 7 unique sampling rates can be created.
    - If egress sampling is not used, a total of 15 unique ingress sampling rates can be configured.
    - Total ingress sampling = 15 - number of egress sampling rates.

References

For more insights into sFlow Configuration, refer to the ***sFlow Configuration*** chapter in the *System Management Guide*, Release 6.4.2.

Entropy Labels for ISIS or OSPF Segment Routing

Overview

The Entropy feature, which involves integrating Entropy Labels into ISIS or OSPF Segment Routing, aims to enhance load balancing, path distribution, and overall network efficiency.

Feature Characteristics

The Entropy Label feature has the following advantages for optimized traffic distribution:

- At the source node, the Entropy label is added into the ISIS or OSPF Segment Routing framework. This ensures load-balancing and even traffic distribution across available Link Aggregation Groups (LAG) paths.
- Intermediate routers in the network utilize the Entropy label to perform a hash calculation on the packet's header fields. The hashing mechanism (fields) used, is hardware-dependent. To enable entropy label functionality, the hashing mechanism must encompass the MPLS header. The calculated hash value determines the optimal LAG path for the packet to follow.
- Entropy Labels lead to the better utilization of the available network routes.
- Entropy Labels enables dynamic traffic distribution, leading to more balanced network resource utilization.

Benefits

The Entropy Label feature has the following benefits:

- Optimizes traffic distribution and load balancing, resulting in improved network performance and reduced latency.
- Evenly distributes traffic and reduces congestion on specific links.
- Introduces path diversity, allowing ISIS or OSPF Segment Routing to leverage a wider range of routing options for efficient traffic distribution.
- The dynamic traffic distribution achieved through Entropy Labels reduces the need for manual traffic engineering, simplifying network management.
- Enhances the scalability of ISIS or OSPF Segment Routing by enabling efficient utilization of multiple available paths.

Prerequisites

- Ensure that the network devices and routers used support Entropy Label functionality.
- The network must already have MPLS configured and operational.

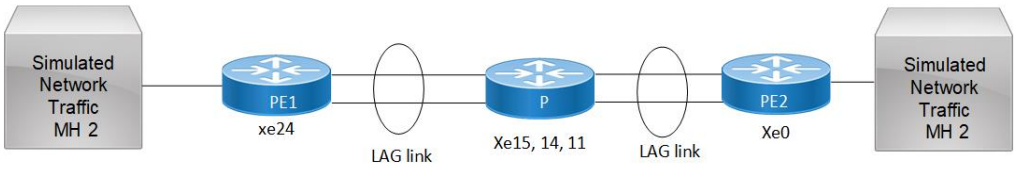
Topology

In the given network topology, each of the nodes is configured to operate using the ISIS or OSPF protocol. Additionally, the network is running an EVPN service, which facilitates the extension of Layer 2 Ethernet services across this network infrastructure.

The topology comprises the links connecting the P and PE nodes, configured as channel groups (LAG) that bundle multiple physical links for increased bandwidth and redundancy. However, the current setup has a limitation: different services may utilize the same MPLS transport, potentially resulting in the same hashing value. Consequently, the network fails to optimize the available resources fully, leading to suboptimal performance and underutilization of the aggregated bandwidth provided by the channel group.

The Entropy label feature addresses this issue by introducing distinct entropy labels for different services within the MPLS label stack. This optimization results in better utilization of the available links in the LAG or ECMP. With this feature, the network evenly distributes traffic across the various physical links within the channel group. Instead of relying on a single link, the network simultaneously utilizes multiple links to handle bidirectional traffic between the P and PE nodes.

Implementation of the Entropy label feature enhances the routing and load balancing of network traffic. Consequently, the network can fully leverage the capabilities of the channel group setup, making the most of the aggregated bandwidth and improving overall network responsiveness.



Entropy Label for ISIS or OSPF

ISIS Configuration

P

`P(config-if)# router ISIS 1`	Enters IS-IS router configuration mode for the IS-IS process ID 1
`P(config-router)# metric-style wide`	Configures the IS-IS metric style as wide.
`P(config-router)# mpls traffic-eng router-id 48.48.48.48`	Sets the MPLS Traffic Engineering router ID to 48.48.48.48.
`P(config-router)# mpls traffic-eng level-1`	Enables MPLS Traffic Engineering for IS-IS Level 1
`P(config-router)# mpls traffic-eng level-2`	Enables MPLS Traffic Engineering for IS-IS Level 2.
`P(config-router)# capability cspf`	Enables the Constraint-Based Shortest Path First (CSPF) capability.
`P(config-router)# dynamic-hostname`	Allows dynamic hostname assignment.
`P(config-router)# bfd all-interfaces`	Enables Bidirectional Forwarding Detection (BFD) on all interfaces.
`P(config-router)# net 49.0000.0000.0048.00`	Sets the IS-IS network entity title (NET) for the router.
`P(config-router)# passive-interface lo`	Sets the loopback interface as a passive interface for IS-IS.
`P(config-router)# segment-routing entropy-label`	Enables the capability for Segment Routing with entropy labels.
`P(config-router)# segment-routing mpls`	Enables MPLS-based Segment Routing.
`P(config-router)#line console 0`	Enters console line configuration mode.

`P(config-line)# exec-timeout 0 0`	Configures the console timeout settings.
`P(config-line)#exit`	Exits the configuration mode of a specific line.

PE1

`PE1(config-router)#router isis 1`	Enters the configuration mode for ISIS routing with process ID 1.
`PE1(config-router)# is-type level-1-2`	Configures the ISIS routing process as a level-1-2 router, supporting both Level 1 and Level 2 routing.
`PE1(config-router)# metric-style wide`	Configures the metric style for ISIS as wide.
`PE1(config-router)# mpls traffic-eng router-id 45.45.45.45`	Sets the MPLS Traffic Engineering (MPLS TE) router ID to 45.45.45.45.
`PE1(config-router)# mpls traffic-eng level-1`	Enables MPLS TE for Level 1 ISIS.
`PE1(config-router)# mpls traffic-eng level-2`	Enables MPLS TE for Level 2 ISIS.
`PE1(config-router)# capability cspf`	Enables the CSPF calculation capability.
`PE1(config-router)# dynamic-hostname`	Enables dynamic hostname generation for ISIS.
`PE1(config-router)# bfd all-interfaces`	Enables BFD on all interfaces.
`PE1(config-router)# net 49.0000.0000.0045.00`	Sets the NET for ISIS.
`PE1(config-router)# passive-interface lo`	Configures the loopback interface as a passive interface in ISIS.
`PE1(config-router)# segment-routing entropy-label`	Enables the capability for Segment Routing with entropy labels.
`PE1(config-router)# segment-routing mpls`	Enables MPLS-based Segment Routing.
`PE1(config-router)#Exit`	Exits the ISIS router configuration mode.

PE2

`PE2(config-router)#router isis 1`	Enters the configuration mode for ISIS routing with instance 1.
`PE2(config-router)# is-type level-1-2`	Sets the ISIS level to level-1-2.
`PE2(config-router)# metric-style wide`	Configures the metric-style as wide for ISIS.
`PE2(config-router)# mpls traffic-eng router-id 22.22.22.22`	Sets the MPLS traffic engineering router ID to 22.22.22.22.
`PE2(config-router)# mpls traffic-eng level-1`	Enables MPLS traffic engineering for ISIS level 1.
`PE2(config-router)# mpls traffic-eng level-2`	Enables MPLS traffic engineering for ISIS level 2.
`PE2(config-router)# capability cspf`	Enables the CSPF capability.
`PE2(config-router)# dynamic-hostname`	Enables dynamic hostname updates for ISIS.
`PE2(config-router)# bfd all-interfaces`	Enables BFD on all interfaces for faster link failure detection.
`PE2(config-router)# net 49.0000.0000.0022.00`	Sets the NET for ISIS.
`PE2(config-router)# passive-interface lo`	Configures the loopback interface as a passive interface for ISIS.
`PE2(config-router)# segment-routing entropy-label`	Enables the capability for Segment Routing with entropy labels.

`PE2(config-router)# segment-routing mpls`	Enables MPLS-based Segment Routing.
`PE2(config-router)#Exit`	Exits the ISIS router configuration mode.

OSPF Configuration

P

`P(config-if)# router ospf 1`	Enters OSPF router configuration mode for the OSPF process ID 1
`P(config-router)# segment-routing entropy-label`	Enables the capability for Segment Routing with entropy labels.
`P(config-router)# segment-routing mpls`	Enables MPLS-based Segment Routing.

PE1

`PE1(config-router)#router ospf 1`	Enters the configuration mode for OSPF routing with process ID 1.
`PE1(config-router)# segment-routing entropy-label`	Enables the capability for Segment Routing with entropy labels.
`PE1(config-router)# segment-routing mpls`	Enables MPLS-based Segment Routing.

PE2

`PE2(config-router)#router ospf 1`	Enters the configuration mode for OSPF routing with instance 1.
`PE2(config-router)# segment-routing entropy-label`	Enables the capability for Segment Routing with entropy labels.
`PE2(config-router)# segment-routing mpls`	Enables MPLS-based Segment Routing.

Implementation Examples

Scenario: Achieve load balancing across Link Aggregation Group (LAG) in a network:

- Configure ISIS with Segment Routing (SR) extensions in the network.
- Enable entropy feature under router isis.

Use entropy labels to distribute traffic evenly across LAG, optimizing resource utilization.

New CLI Commands

Here is the compilation of new commands for configuring Entropy Label for Segment Routing.

- `segment-routing entropy-label` in the “New Features in Release 6.4.1" document.

segment-routing entropy-label

Use this command to enable and configure entropy labels within the Segment Routing framework in ISIS instances. Use `no` form of CLI to disable the entropy labels within the Segment Routing framework.

Command Syntax

```
segment-routing entropy-label
no segment-routing entropy-label
```

Parameters

`enable`	Enable segment routing entropy label in ISIS or OSPF instance.
`disable`	Disable segment routing entropy label in ISIS or OSPF instance.

Command Mode

Router ISIS

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

```
(config-router)#segment-routing entropy-label
```

Validation

ISIS Validation

```
PE2#show isis segment-routing capability
Tag 1  Segment-Routing:
Advertisement Router Capability   :1.1.1.1
Algorithm0                        :0
SRMS Preference                   :0
SR ERLD                           :6
Total SID'S Supported             :3001
SID Range List Count              :1
SID's Range                       :16000 - 23999
Total SID'S Supported (SRLB)      :0
SRLB Range List Count             :0
Advertisement Router Capability   :3.3.3.3
Algorithm0                        :0
SRMS Preference                   :0
SR ERLD                           :6
```

```
Total SID'S Supported             :3001
SID Range List Count              :1
SID's Range                       :16000 - 23999
Total SID'S Supported (SRLB)      :0
SRLB Range List Count             :0
Advertisement Router Capability   :5.5.5.5
Algorithm0                        :0
SRMS Preference                   :0
SR ERLD                           :6
Total SID'S Supported             :3001
SID Range List Count              :1
SID's Range                       :16000 - 23999
Total SID'S Supported (SRLB)      :0
SRLB Range List Count             :0
R3#
R3#show mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN, ! - using backup
       B - BGP FTN, K - CLI FTN, (t) - tunnel, P - SR Policy FTN, (b) - bypass,
       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, (e) - FTN is ECMP

FTN-ECMP LDP: Disabled
CodeFEC FTN-ID Nhlfe-ID Tunnel-id  Pri LSP-Type  Out-Label Out-Intf    ELC   Nexthop
i>  1.1.1.1/32  1    10           Yes   LSP_DEFAULT  16001 xe3        Yes   1.3.0.1
i>   5.5.5.5/32 2    2 0          Yes   LSP_DEFAULT  16005 xe9        Yes   3.5.0.5
```

OSPF Validation

```
PE1#show ip ospf segment-routing capability
OSPF process 1:
Advertisement Router Capability   :1.1.1.1
Algorithm0                        :0
SRMS Preference                   :0
SR ERLD                           :6
Total SID'S Supported             :8000
SID Range List Count              :1
SID's Range                       :16000 - 23999
Total SID'S Supported (SRLB)      :1000
SRLB Range List Count             :1
SID's Range (SRLB)                :24320 - 25319
```

```
Advertisement Router Capability   :3.3.3.3
Algorithm0                        :0
SRMS Preference                   :0
SR ERLD                           :6
Total SID'S Supported             :8000
SID Range List Count              :1
SID's Range                       :16000 - 23999
Total SID'S Supported (SRLB)      :1000
SRLB Range List Count             :1
SID's Range (SRLB)                :24320 - 25319
Advertisement Router Capability   :5.5.5.5
Algorithm0                        :0
SRMS Preference                   :0
SR ERLD                           :6
Total SID'S Supported             :4000
SID Range List Count              :1
SID's Range                       :16000 - 23999
Total SID'S Supported (SRLB)      :1000
SRLB Range List Count             :1
SID's Range (SRLB)                :24320 - 25319
R3#
R3#show mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN, ! - using backup
       B - BGP FTN, K - CLI FTN, (t) - tunnel, P - SR Policy FTN, (b) - bypass,
       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, (e) - FTN is ECMP

FTN-ECMP LDP: Disabled
Code FEC  FTN-ID  Nhlfe-ID  Tunnel-id Pri LSP-Type  Out-Label    Out-Intf   ELC   Nexthop
O>   1.1.1.1/32  1  16 0     Yes       LSP_DEFAULT   16001        xe3       Yes   1.3.0.1
O>   5.5.5.5/32   2  19 0    Yes  LSP_DEFAULT         1600        xe9  Yes   3.5.0.5
po1         Yes   20.1.1.15
```

Abbreviations

The following are some key abbreviations and their meanings relevant to this document:

.

Adj-SID	Adjacency Segment Identifier
ECMP	Equal-Cost Multipath
EL	Entropy Label
ELI	Entropy Label Indicator
ELC	Entropy Label Capability
ERLD	Entropy Readable Label Depth

FEC	Forwarding Equivalence Class
ISIS	Intermediate System to Intermediate System
LAG	Link Aggregation Group
LSP	Label Switched Path
LSR	Label Switching Router
MPLS	Multiprotocol Label Switching
MSD	Maximum SID Depth
Node SID	Node Segment Identifier
OAM	Operations, Administration, and Maintenance
RLD	Readable Label Depth
SID	Segment Identifier
SPT	Shortest Path Tree
SR	Segment Routing
SRGB	Segment Routing Global Block
VPN	Virtual Private Network

Glossary

Entropy Label	An additional label in the MPLS (Multiprotocol Label Switching) header used to enhance load balancing and path distribution in networks.
Load Balancing	The practice of distributing network traffic across multiple paths or resources to prevent congestion and optimize network performance.
Path Distribution	The process of selecting and directing traffic along various network paths, often to ensure efficient utilization and redundancy.
Network Efficiency	The measure of how effectively a network utilizes its resources to deliver data, minimizing waste and maximizing performance.
Multiprotocol Label Switching (MPLS)	A protocol used in telecommunications networks to efficiently direct data packets using labels, enhancing speed and performance.
Label Switching	A mechanism for forwarding data packets based on labels, typically used in MPLS networks for efficient routing.
Hashing Mechanism	A method for computing hash values, often used in load balancing to evenly distribute traffic across network resources.

Hardware-Dependent	Referring to features or functionality that rely on specific hardware components or capabilities.
Segment Routing	A networking technology that allows for the efficient routing of data packets by specifying the exact path they must follow.

ERPS with CFM Down-MEP over Bridge-Domain

Overview

Ethernet Ring Protection Switching (ERPS) over a bridge domain is a network feature that allows the implementation of ring protection in Ethernet networks using bridge domains. ERPS, a protocol specified by ITU-T G.8032, is designed to provide fast and seamless protection switching in ring topologies to ensure network availability. Previously, all ERPS instances were mapped to a single bridge domain. It is now possible to map different flooding domains with ERPS instances.

Feature Characteristics

1. **ERPS Configuration over L2 Sub-Interface:** OcNOS allows the configuration of ERPS over Layer 2 sub-interfaces mapped under Bridge-Domains, enabling efficient utilization of network resources.
2. **L2 Sub-Interface Configuration as Ring Ports:** Layer 2 sub-interfaces can be easily configured as east and west ring ports of an ERPS ring, providing a flexible and intuitive setup.
3. **Support for Multiple ERPS Instances:** The software supports the creation of multiple ERPS instances, facilitating the deployment of different logical ERPS rings across various Bridge-Domains.
4. **Shared ERPS Instances for Logical Rings:** Optionally, multiple ERPS logical rings can utilize a single ERPS instance if the ring ports share the same parent interface, streamlining the configuration process.
5. **Single Bridge-Domain per ERPS Instance:** A single ERPS instance can only have ring ports from a single Bridge-Domain, ensuring consistent and efficient ring management.
6. **CFM Triggering for ERPS Instances:** Configuration of Continuity Fault Management (CFM) over L2-sub-interfaces will trigger signal fail events for ERPS instances created over the same L2-sub-interface upon link fault detection.
7. **Single ERPS Instance Monitoring Multiple ERPS Rings:** The software allows a single ERPS instance to monitor multiple ERPS rings, offering centralized management and improved network oversight.

   Note: When a single instance is utilized to monitor multiple ERPS rings, only a fault detected by the primary ring will trigger a switchover (ERPS) in `associate` rings. Individual sub-interface (`subifp`) link shutdowns of `associate` ring member interfaces will not initiate a switchover in that instance.

Benefits

Network Resilience: ERPS enhances network resiliency by creating a ring topology, where traffic can be rerouted in case of a link or node failure, ensuring uninterrupted connectivity.

Faster Traffic Switchover: In case of a link or node failure within the ring, ERPS ensures rapid traffic switchover to the backup path, minimizing service disruptions.

Prerequisites

Before configuring ERPS over bridge-domains, ensure the following prerequisites are met:

- Properly configure the bridge-domains and L2 sub-interfaces. For more details, refer Bridging Support Over Layer2 Sub Interface and Layer 2 Subinterface Configuration chapters in the *Layer 2 Guide*, *Release 6.4.1*.
- Understand the network topology and ERPS requirements. For more details, refer G.8032 ERPS Version 2 chapter in the *Carrier Ethernet Configuration Guide*, *Release 6.4.1*.
- Knowledge of CFM configuration if integrating CFM with ERPS. For more details, refer *Carrier Ethernet Guide*, *Release 6.4.1.*

Major Ring Configuration

The major ring is the primary ring in an ERPS configuration. It carries the traffic under normal operating conditions. When no failure occurs, traffic flows through the major ring.

Topology

Figure 1 illustrates a sample Ring Protection topology in which protection switching is configured using four bridges. The Ring Protection Link (RPL) owner is the link between Bridge 3 and Bridge 4 (xe16), with Bridge 4 explicitly defined as the RPL owner and Bridge 3 as the RPL neighbor on one side of the link. The other bridges are explicitly configured as RPL non-owners to enable Ethernet Ring Protection Switching (ERPS) within the ring.

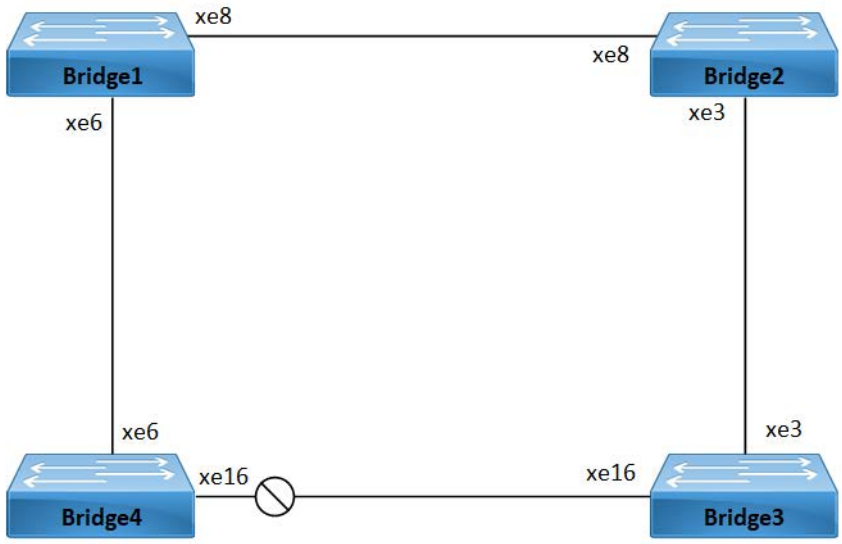


Figure 1: Major Ring Topology

Prerequisite

In configuration mode, enable the following `hardware-profile` commands related to CFM and then reboot the nodes:

```
hardware-profile filter cfm-domain-name-str enable
hardware-profile statistics cfm-ccm enable
```

The following steps provide a detailed configuration of commands for setting up ERPS and CFM on Bridge1, Bridge2, Bridge3, and Bridge4 nodes. These commands enable the creation of rings, maintenance associations, Maintenance End Points (MEPs), and various parameters to ensure network reliability and protection against faults.

Bridge1

`Bridge1#configure terminal`	Enter configure mode.
`Bridge1(config)#hardware-profile filter cfm-domain-name-str enable`	Enable CFM domain name as string.
`Bridge1(config)#interface xe6`	Enter interface mode `xe6`.
`Bridge1(config-if)#dot1ad ethertype 0x88a8`	Configure `xe6` as a Layer 2 port with an Ethernet Type of `0x88a8`.
`Bridge1(config-if)#interface xe6.1 switchport`	Create a Layer 2 sub-interface `xe6.1` within the physical interface `xe6`.
`Bridge1(config-if)encapsulation dot1ad 200`	Encapsulate the sub-interface with APS-channel VLAN ID `200`.
`Bridge1(config-if)encapsulation dot1ad 700`	Encapsulate the sub-interface with data VLAN ID `700`.
`Bridge1(config-if)#exit`	Exit interface mode `xe6`.
`Bridge1(config)#interface xe8`	Enter interface mode `xe8`.
`Bridge1(config-if)#dot1ad ethertype 0x88a8`	Configure `xe8` as a Layer 2 port with an Ethernet Type of `0x88a8`.
`Bridge1(config)#interface xe8.1 switchport`	Create a Layer 2 sub-interface `xe8.1` within the physical interface `xe8`.
`Bridge1(config-if)encapsulation dot1ad 200`	Encapsulate the sub-interface with APS-channel VLAN ID `200`.
`Bridge1(config-if)encapsulation dot1ad 700`	Encapsulate the sub-interface with data VLAN ID `700`.
`Bridge1(config-if)#exit`	Exit interface mode `xe8`.
`Bridge1(config)#bridge-domain 1`	Enter bridge domain configure mode and configure bridge domain instance `1`.
`Bridge1(config-bridge-domain)#interface xe6.1`	Attach the sub-interface `xe6.1` to the bridge domain instance.
`Bridge1(config-bridge-domain)#interface xe8.1`	Attach the sub-interface `xe8.1` to the bridge domain instance.
`Bridge1(config-bridge-domain)#exit`	Exit bridge domain mode.
`Bridge1(config)#ethernet cfm domain-type character-string domain-name P542 level 5`	Create a CFM domain with character string type, name `P542`, and level `5`.
`Bridge1(config-ether-cfm)#service ma-type string ma-name ma542`	Create a CFM Maintenance Association (MA) type as a string with the name `ma542`.
`Bridge1(config-ether-cfm-ma)#vlan 200`	Add VLAN `200` to the CFM MA.
`Bridge1(config-ether-cfm-ma)#ethernet cfm mep down mpid 542 active true xe8.1`	Create a down MEP `542` for `xe8.1` interface and activate it.
`Bridge1(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable Continuity Check (CC) multicast for the MEP.
`Bridge1(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit Ethernet CFM MA-MEP mode.

`Bridge1(config-ether-cfm-ma)#mep crosscheck mpid 452`	Configure crosscheck for the remote MEP with value `452`.
`Bridge1(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet CFM MA mode.
`Bridge1(config-ether-cfm)#exit`	Exit Ethernet CFM mode and return to the configure mode.
`Bridge1(config)#ethernet cfm domain-type character-string domain-name P522 level 5`	Create a CFM domain with character string type, name `P522`, and level `5`.
`Bridge1(config-ether-cfm)#service ma-type string ma-name ma522`	Create a CFM MA type as a string with the name `ma522.`
`Bridge1(config-ether-cfm-ma)#vlan 200`	Add VLAN `200` to the CFM MA.
`Bridge1(config-ether-cfm-ma)#ethernet cfm mep down mpid 522 active true xe6.1`	Create a down MEP 522 for `xe6.1` interface and activate it.
`Bridge1(config-ether-cfm-ma-mep)#cc multicast state enable`	Enables CC multicast for the MEP.
`Bridge1(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit Ethernet CFM MA-MEP mode.
`Bridge1(config-ether-cfm-ma)#mep crosscheck mpid 252`	Configure crosscheck for the remote MEP with value `252`.
`Bridge1(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet CFM MA mode.
`Bridge1(config-ether-cfm)#exit`	Exit Ethernet CFM mode and return to the configure mode.
`Bridge1(config)#g8032 ring RING1`	Create a G.8032 ring named `RING1`.
`Bridge1(g8032-ring-config)#east-interface xe8.1`	Associate `xe8.1` interface as the east interface in `RING1`.
`Bridge1(g8032-ring-config)#west-interface xe6.1`	Associate `xe6.1` interface as the west interface in `RING1`.
`Bridge1(g8032-ring-config)#g8032 profile profile1`	Create a G.8032 profile named `profile1`.
`Bridge1(g8032-profile-config)#timer wait-to-restore 1`	Configure the wait-to-restore timer for `1` minute.
`Bridge1(g8032-profile-config)#timer hold-off 0`	Configure the hold-off timer with a value of `0`.
`Bridge1(g8032-profile-config)#timer guard-timer 10`	Configure the guard timer with a value of `10` milliseconds.
`Bridge1(g8032-profile-config)#switching mode revertive`	Configure the switching mode as `revertive`.
`Bridge1(g8032-profile-config)#exit`	Exit profile configure mode and return to the ring configure mode.
`Bridge1(g8032-ring-config)#exit`	Exit ring configure mode and return to the configure mode.
`Bridge1(config)#g8032 erp-instance erp1`	Create a G.8032 Ethernet Ring Protection (ERP) instance named `erp1`.
`Bridge1(g8032-config-switch)#ring-type major-ring`	Configure the ring type as a `major ring`.

`Bridge1(g8032-config-switch)#ring RING1`	Associate `RING1` with the ERP instance `erp1`.
`Bridge1(g8032-config-switch)#rpl role non-owner`	Configure the node as a `non-owner` node in the ring.
`Bridge1(g8032-config-switch)#g8032-profile profile1`	Associate `profile1` with `erp1` instance.
`Bridge1(g8032-config-switch)#aps-channel level 7`	Configure the R-APS channel level as `7`.
`Bridge1(g8032-config-switch)#aps-channel vlan 200`	Configure the APS channel VLAN as `200`.
`Bridge1(g8032-config-switch)#ring-id 1`	Configure the ring ID as `1`.
`Bridge1(g8032-config-switch)#commit`	Commit the candidate configuration to the running configuration
`Bridge1(g8032-config-switch)#end`	Exit G.8032 configure mode.

Bridge2

`Bridge2#configure terminal`	Enter configure mode.
`Bridge2(config)#hardware-profile filter cfm-domain-name-str enable`	Enable CFM domain name as string.
`Bridge2(config)#interface xe3`	Enter interface mode `xe3`.
`Bridge2(config-if)#dot1ad ethertype 0x88a8`	Configure `xe6` as a Layer 2 port with an Ethernet Type of `0x88a8`.
`Bridge2(config-if)#interface xe3.1 switchport`	Create a Layer 2 sub-interface `xe3.1` within the physical interface `xe3`.
`Bridge2(config-if)encapsulation dot1ad 200`	Encapsulate the sub-interface with APS-channel VLAN ID `200`.
`Bridge2(config-if)encapsulation dot1ad 700`	Encapsulate the sub-interface with data VLAN ID `700`.
`Bridge2(config-if)#exit`	Exit interface mode `xe6`.
`Bridge2(config)#interface xe8`	Enter interface mode `xe8`.
`Bridge2(config-if)#dot1ad ethertype 0x88a8`	Configure `xe8` as a Layer 2 port with an Ethernet Type of `0x88a8`.
`Bridge2(config)#interface xe8.1 switchport`	Create a Layer 2 sub-interface `xe8.1` within the physical interface `xe8`.
`Bridge2(config-if)encapsulation dot1ad 200`	Encapsulate the sub-interface with APS-channel VLAN ID `200`.
`Bridge2(config-if)encapsulation dot1ad 700`	Encapsulate the sub-interface with data VLAN ID `700`.
`Bridge2(config-if)#exit`	Exit interface mode `xe8`.
`Bridge2(config)#bridge-domain 1`	Enter bridge domain configure mode and configure bridge domain instance `1`.
`Bridge2(config-bridge-domain)#interface xe3.1`	Attach the sub-interface `xe3.1` to the bridge domain instance.
`Bridge2(config-bridge-domain)#interface xe8.1`	Attach the sub-interface `xe8.1` to the bridge domain instance.
`Bridge2(config-bridge-domain)#exit`	Exit bridge domain mode.

`Bridge2(config)#ethernet cfm domain-type character-string domain-name P542 level 5`	Create a CFM domain with character string type, name `P542`, and level `5`.
`Bridge2(config-ether-cfm)#service ma-type string ma-name ma542`	Create a CFM Maintenance Association (MA) type as a string with the name `ma542`.
`Bridge2(config-ether-cfm-ma)#vlan 200`	Add VLAN `200` to the CFM MA.
`Bridge2(config-ether-cfm-ma)#ethernet cfm mep down mpid 452 active true xe8.1`	Create a down MEP `452` for `xe8.1` interface and activate it.
`Bridge2(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable Continuity Check (CC) multicast for the MEP.
`Bridge2(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit Ethernet CFM MA-MEP mode.
`Bridge2(config-ether-cfm-ma)#mep crosscheck mpid 542`	Configure crosscheck for the remote MEP with value `542`.
`Bridge2(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet CFM MA mode.
`Bridge2(config-ether-cfm)#exit`	Exit Ethernet CFM mode and return to the configure mode.
`Bridge2(config)#ethernet cfm domain-type character-string domain-name P432 level 5`	Create a CFM domain with character string type, name `P432`, and level `5`.
`Bridge2(config-ether-cfm)#service ma-type string ma-name ma432`	Create a CFM MA type as a string with the name `ma432.`
`Bridge2(config-ether-cfm-ma)#vlan 200`	Add VLAN `200` to the CFM MA.
`Bridge2(config-ether-cfm-ma)#ethernet cfm mep down mpid 432 active true xe3.1`	Create a down MEP `432` for `xe3.1` interface and activate it.
`Bridge2(config-ether-cfm-ma-mep)#cc multicast state enable`	Enables CC multicast for the MEP.
`Bridge2(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit Ethernet CFM MA-MEP mode.
`Bridge2(config-ether-cfm-ma)#mep crosscheck mpid 532`	Configure crosscheck for the remote MEP with value `532`.
`Bridge2(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet CFM MA mode.
`Bridge2(config-ether-cfm)#exit`	Exit Ethernet CFM mode and return to the configure mode.
`Bridge2(config)#g8032 ring RING1`	Create a G.8032 ring named `RING1`.
`Bridge2(g8032-ring-config)#east-interface xe3.1`	Associate `xe3.1` interface as the east interface in `RING1`.
`Bridge2(g8032-ring-config)#west-interface xe8.1`	Associate `xe8.1` interface as the west interface in `RING1`.

`Bridge2(g8032-ring-config)#g8032 profile profile1`	Create a G.8032 profile named `profile1`.
`Bridge2(g8032-profile-config)#timer wait-to-restore 1`	Configure the wait-to-restore timer for `1` minute.
`Bridge2(g8032-profile-config)#timer hold-off 0`	Configure the hold-off timer with a value of `0`.
`Bridge2(g8032-profile-config)#timer guard-timer 10`	Configure the guard timer with a value of `10` milliseconds.
`Bridge2(g8032-profile-config)#switching mode revertive`	Configure the switching mode as `revertive`.
`Bridge2(g8032-profile-config)#exit`	Exit profile configure mode and return to the ring configure mode.
`Bridge2(g8032-ring-config)#exit`	Exit ring configure mode and return to the configure mode.
`Bridge2(config)#g8032 erp-instance erp1`	Create a G.8032 Ethernet Ring Protection (ERP) instance named `erp1`.
`Bridge2(g8032-config-switch)#ring-type major-ring`	Configure the ring type as a `major ring`.
`Bridge2(g8032-config-switch)#ring RING1`	Associate `RING1` with the ERP instance `erp1`.
`Bridge2(g8032-config-switch)#rpl role non-owner`	Configure the node as a `non-owner` node in the ring.
`Bridge2(g8032-config-switch)#g8032-profile profile1`	Associate `profile1` with `erp1` instance.
`Bridge2(g8032-config-switch)#aps-channel level 7`	Configure the R-APS channel level as `7`.
`Bridge2(g8032-config-switch)#aps-channel vlan 200`	Configure the APS channel VLAN as `200`.
`Bridge2(g8032-config-switch)#commit`	Commit the candidate configuration to the running configuration
`Bridge2(g8032-config-switch)#end`	Exit G.8032 configure mode.

Bridge3

`Bridge3#configure terminal`	Enter configure mode.
`Bridge3(config)#hardware-profile filter cfm-domain-name-str enable`	Enable CFM domain name as string.
`Bridge3(config)#interface xe3`	Enter interface mode `xe3`.
`Bridge3(config-if)#dot1ad ethertype 0x88a8`	Configure `xe6` as a Layer 2 port with an Ethernet Type of `0x88a8`.
`Bridge3(config-if)#interface xe3.1 switchport`	Create a Layer 2 sub-interface `xe3.1` within the physical interface `xe3`.
`Bridge3(config-if)encapsulation dot1ad 200`	Encapsulate the sub-interface with APS-channel VLAN ID `200`.
`Bridge3(config-if)encapsulation dot1ad 700`	Encapsulate the sub-interface with data VLAN ID `700`.
`Bridge3(config-if)#exit`	Exit interface mode `xe3`.
`Bridge3(config)#interface xe16`	Enter interface mode `xe8`.
`Bridge3(config-if)#dot1ad ethertype 0x88a8`	Configure `xe16` as a Layer 2 port with an Ethernet Type of `0x88a8`.

`Bridge3(config)#interface xe16.1 switchport`	Create a Layer 2 sub-interface `xe16.1` within the physical interface `xe16`.
`Bridge3(config-if)encapsulation dot1ad 200`	Encapsulate the sub-interface with APS-channel VLAN ID `200`.
`Bridge3(config-if)encapsulation dot1ad 700`	Encapsulate the sub-interface with data VLAN ID `700`.
`Bridge3(config-if)#exit`	Exit interface mode `xe16`.
`Bridge3(config)#bridge-domain 1`	Enter bridge domain configure mode and configure bridge domain instance `1`.
`Bridge3(config-bridge-domain)#interface xe3.1`	Attach the sub-interface `xe3.1` to the bridge domain instance.
`Bridge3(config-bridge-domain)#interface xe16.1`	Attach the sub-interface `xe16.1` to the bridge domain instance.
`Bridge3(config-bridge-domain)#exit`	Exit bridge domain mode.
`Bridge3(config)#ethernet cfm domain-type character-string domain-name P542 level 5`	Create a CFM domain with character string type, name `P542`, and level `5`.
`Bridge3(config-ether-cfm)#service ma-type string ma-name ma542`	Create a CFM Maintenance Association (MA) type as a string with the name `ma542`.
`Bridge3(config-ether-cfm-ma)#vlan 200`	Add VLAN `200` to the CFM MA.
`Bridge3(config-ether-cfm-ma)#ethernet cfm mep down mpid 452 active true xe16.1`	Create a down MEP `452` for `xe16.1` interface and activate it.
`Bridge3(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable Continuity Check (CC) multicast for the MEP.
`Bridge3(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit Ethernet CFM MA-MEP mode.
`Bridge3(config-ether-cfm-ma)#mep crosscheck mpid 542`	Configure crosscheck for the remote MEP with value `542`.
`Bridge3(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet CFM MA mode.
`Bridge3(config-ether-cfm)#exit`	Exit Ethernet CFM mode and return to the configure mode.
`Bridge3(config)#ethernet cfm domain-type character-string domain-name P432 level 5`	Create a CFM domain with character string type, name `P432`, and level `5`.
`Bridge3(config-ether-cfm)#service ma-type string ma-name ma432`	Create a CFM MA type as a string with the name `ma432.`
`Bridge3(config-ether-cfm-ma)#vlan 200`	Add VLAN `200` to the CFM MA.
`Bridge3(config-ether-cfm-ma)#ethernet cfm mep down mpid 342 active true xe3.1`	Create a down MEP `342` for `xe3.1` interface and activate it.
`Bridge3(config-ether-cfm-ma-mep)#cc multicast state enable`	Enables CC multicast for the MEP.

`Bridge3(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit Ethernet CFM MA-MEP mode.
`Bridge3(config-ether-cfm-ma)#mep crosscheck mpid 432`	Configure crosscheck for the remote MEP with value `432`.
`Bridge3(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet CFM MA mode.
`Bridge3(config-ether-cfm)#exit`	Exit Ethernet CFM mode and return to the configure mode.
`Bridge3(config)#g8032 ring RING1`	Create a G.8032 ring named `RING1`.
`Bridge3(g8032-ring-config)#east-interface xe16.1`	Associate `xe16.1` interface as the east interface in `RING1`.
`Bridge3(g8032-ring-config)#west-interface xe3.1`	Associate `xe3.1` interface as the west interface in `RING1`.
`Bridge3(g8032-ring-config)#g8032 profile profile1`	Create a G.8032 profile named `profile1`.
`Bridge3(g8032-profile-config)#timer wait-to-restore 1`	Configure the wait-to-restore timer for `1` minute.
`Bridge3(g8032-profile-config)#timer hold-off 0`	Configure the hold-off timer with a value of `0`.
`Bridge3(g8032-profile-config)#timer guard-timer 10`	Configure the guard timer with a value of `10` milliseconds.
`Bridge3(g8032-profile-config)#switching mode revertive`	Configure the switching mode as `revertive`.
`Bridge3(g8032-profile-config)#exit`	Exit profile configure mode and return to the ring configure mode.
`Bridge3(g8032-ring-config)#exit`	Exit ring configure mode and return to the configure mode.
`Bridge3(config)#g8032 erp-instance erp1`	Create a G.8032 Ethernet Ring Protection (ERP) instance named `erp1`.
`Bridge3(g8032-config-switch)#ring-type major-ring`	Configure the ring type as a `major ring`.
`Bridge3(g8032-config-switch)#ring RING1`	Associate `RING1` with the ERP instance `erp1`.
`Bridge3(g8032-config-switch)#rpl role neighbor east-interface`	Configure the node as the `neighbor` node for the ERPS ring and designate the `east interface` as the owner node in the ring.
`Bridge3(g8032-config-switch)#g8032-profile profile1`	Associate `profile1` with `erp1` instance.
`Bridge3(g8032-config-switch)#aps-channel level 7`	Configure the R-APS channel level as `7`.
`Bridge3(g8032-config-switch)#aps-channel vlan 200`	Configure the APS channel VLAN as `200`.
`Bridge3(g8032-config-switch)#commit`	Commit the candidate configuration to the running configuration
`Bridge3(g8032-config-switch)#end`	Exit G.8032 configure mode.

Bridge4

`Bridge4#configure terminal`	Enter configure mode.
`Bridge4(config)#hardware-profile filter cfm-domain-name-str enable`	Enable CFM domain name as string.
`Bridge4(config)#interface xe6`	Enter interface mode `xe6`.
`Bridge4(config-if)#dot1ad ethertype 0x88a8`	Configure `xe6` as a Layer 2 port with an Ethernet Type of `0x88a8`.
`Bridge4(config-if)#interface xe6.1 switchport`	Create a Layer 2 sub-interface `xe6.1` within the physical interface `xe6`.
`Bridge4(config-if)encapsulation dot1ad 200`	Encapsulate the sub-interface with APS-channel VLAN ID `200`.
`Bridge4(config-if)encapsulation dot1ad 700`	Encapsulate the sub-interface with data VLAN ID `700`.
`Bridge4(config-if)#exit`	Exit interface mode `xe6`.
`Bridge4(config)#interface xe16`	Enter interface mode `xe8`.
`Bridge4(config-if)#dot1ad ethertype 0x88a8`	Configure `xe16` as a Layer 2 port with an Ethernet Type of `0x88a8`.
`Bridge4(config)#interface xe16.1 switchport`	Create a Layer 2 sub-interface `xe16.1` within the physical interface `xe16`.
`Bridge4(config-if)encapsulation dot1ad 200`	Encapsulate the sub-interface with APS-channel VLAN ID `200`.
`Bridge4(config-if)encapsulation dot1ad 700`	Encapsulate the sub-interface with data VLAN ID `700`.
`Bridge4(config-if)#exit`	Exit interface mode `xe16`.
`Bridge4(config)#bridge-domain 1`	Enter bridge domain configure mode and configure bridge domain instance `1`.
`Bridge4(config-bridge-domain)#interface xe6.1`	Attach the sub-interface `xe6.1` to the bridge domain instance.
`Bridge4(config-bridge-domain)#interface xe16.1`	Attach the sub-interface `xe16.1` to the bridge domain instance.
`Bridge4(config-bridge-domain)#exit`	Exit bridge domain mode.
`Bridge4(config)#ethernet cfm domain-type character-string domain-name P522 level 5`	Create a CFM domain with character string type, name `P522`, and level `5`.
`Bridge4(config-ether-cfm)#service ma-type string ma-name ma522`	Create a CFM Maintenance Association (MA) type as a string with the name `ma522`.
`Bridge4(config-ether-cfm-ma)#vlan 200`	Add VLAN `200` to the CFM MA.
`Bridge4(config-ether-cfm-ma)#ethernet cfm mep down mpid 452 active true xe16.1`	Create a down MEP `452` for `xe16.1` interface and activate it.
`Bridge4(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable Continuity Check (CC) multicast for the MEP.
`Bridge4(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit Ethernet CFM MA-MEP mode.

`Bridge4(config-ether-cfm-ma)#mep crosscheck mpid 542`	Configure crosscheck for the remote MEP with value `542`.
`Bridge4(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet CFM MA mode.
`Bridge4(config-ether-cfm)#exit`	Exit Ethernet CFM mode and return to the configure mode.
`Bridge4(config)#ethernet cfm domain-type character-string domain-name P522 level 5`	Create a CFM domain with character string type, name `P522`, and level `5`.
`Bridge4(config-ether-cfm)#service ma-type string ma-name ma522`	Create a CFM MA type as a string with the name `ma522.`
`Bridge4(config-ether-cfm-ma)#vlan 200`	Add VLAN `200` to the CFM MA.
`Bridge4(config-ether-cfm-ma)#ethernet cfm mep down mpid 252 active true xe6.1`	Create a down MEP `252` for `xe6.1` interface and activate it.
`Bridge4(config-ether-cfm-ma-mep)#cc multicast state enable`	Enables CC multicast for the MEP.
`Bridge4(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit Ethernet CFM MA-MEP mode.
`Bridge4(config-ether-cfm-ma)#mep crosscheck mpid 522`	Configure crosscheck for the remote MEP with value `522`.
`Bridge4(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet CFM MA mode.
`Bridge4(config-ether-cfm)#exit`	Exit Ethernet CFM mode and return to the configure mode.
`Bridge4(config)#g8032 ring RING1`	Create a G.8032 ring named `RING1`.
`Bridge4(g8032-ring-config)#east-interface xe6.1`	Associate `xe6.1` interface as the east interface in `RING1`.
`Bridge4(g8032-ring-config)#west-interface xe16.1`	Associate `xe16.1` interface as the west interface in `RING1`.
`Bridge4(g8032-ring-config)#g8032 profile profile1`	Create a G.8032 profile named `profile1`.
`Bridge4(g8032-profile-config)#timer wait-to-restore 1`	Configure the wait-to-restore timer for `1` minute.
`Bridge4(g8032-profile-config)#timer hold-off 0`	Configure the hold-off timer with a value of `0`.
`Bridge4(g8032-profile-config)#timer guard-timer 10`	Configure the guard timer with a value of `10` milliseconds.
`Bridge4(g8032-profile-config)#switching mode revertive`	Configure the switching mode as `revertive`.
`Bridge4(g8032-profile-config)#exit`	Exit profile configure mode and return to the ring configure mode.
`Bridge4(g8032-ring-config)#exit`	Exit ring configure mode and return to the configure mode.
`Bridge4(config)#g8032 erp-instance erp1`	Create a G.8032 Ethernet Ring Protection (ERP) instance named `erp1`.
`Bridge4(g8032-config-switch)#ring-type major-ring`	Configure the ring type as a `major ring`.

`Bridge4(g8032-config-switch)#ring RING1`	Associate `RING1` with the ERP instance `erp1`.
`Bridge4(g8032-config-switch)#rpl role owner west-interface`	Configure the node as the `owner` node for the ERPS ring and designate the `west interface` as the neighbor node in the ring.
`Bridge4(g8032-config-switch)#g8032-profile profile1`	Associate `profile1` with `erp1` instance.
`Bridge4(g8032-config-switch)#aps-channel level 7`	Configure the R-APS channel level as `7`.
`Bridge4(g8032-config-switch)#aps-channel vlan 200`	Configure the APS channel VLAN as `200`.
`Bridge4(g8032-config-switch)#commit`	Commit the candidate configuration to the running configuration
`Bridge4(g8032-config-switch)#end`	Exit G.8032 configure mode.

Validation

The following details provide validation for the G.8032 ERPS configuration on Bridge1, Bridge2, Bridge3, and Bridge4.

Bridge1

```
Bridge1#show g8032 erp-instance
Instance         ID  State       East          state     West          state   Ring
-------------------------------------------------------------------------------------------
 erp1             1   IDLE        xe8.1         Unblocked xe6.1        Unblocked  ring1

Bridge1#show g8032 erp-instance data-traffic
Instance         ID  Data-vlan                 East           West           Ring
-------------------------------------------------------------------------------------
erp1             1   bridge_domain 1           xe8.100 (F)      xe6.1 (F)    ring1


Bridge1#show g8032 erp-instance erp1
Inst Name       : erp1 (1), node-id e8:c5:7a:a8:7c:b6, Profile (1)
Description     :
Ring            : MAJOR-RING (ring1), NON-OWNER,
                  Attached (erp3,),tcn_propagation (0)

State           : G8032_ST_IDLE

East            : xe8.1, Unblocked, UP  , BPR (-), remote (-)
West            : xe6.1, Unblocked, UP  , BPR (0), remote (b8:6a:97:25:a7:d4)

East (cfm)      : mep_id (542), cc-interval (1s), Domain (P5P42), MA (ma542)
West (cfm)      : mep_id (522), cc-interval (1s), Domain (P5P22), MA (ma522)

Channel         : Level (5), vlan (200), RING_ID (1)
```

Bridge2

```
Bridge2#show g8032 erp-instance
Instance         ID  State       East          state     West          state      Ring
-------------------------------------------------------------------------------------------
erp1             1   IDLE        xe3.1         Unblocked xe8.1         Unblocked  ring1

Bridge2#show g8032 erp-instance erp1
Inst Name       : erp1 (1), node-id e4:9d:73:b1:c3:05, Profile (1)
Description     :
Ring            : MAJOR-RING (ring1), NON-OWNER,

State           : G8032_ST_IDLE

East            : xe3.1, Unblocked, UP  , BPR (-), remote (-)
West            : xe8.1, Unblocked, UP  , BPR (0), remote (b8:6a:97:25:a7:d4)
```

```
East (cfm)      : mep_id (432), cc-interval (1s), Domain (P4P32), MA (ma432)
West (cfm)      : mep_id (452), cc-interval (1s), Domain (P5P42), MA (ma542)

Channel         : Level (5), vlan (200), RING_ID (1)

Bridge2#show g8032 erp-instance data-traffic
Instance         ID  Data-vlan                East           West           Ring
-------------------------------------------------------------------------------------
erp1             1   bridge_domain 1          xe3.1 (F)      xe8.1 (F)      ring1
```

Bridge3

```
Bridge3#show g8032 erp-instance erp1
Inst Name       : erp1 (1), node-id 00:e0:4b:71:f1:26, Profile (1)
Description     :
Ring            : MAJOR-RING (ring1), NEIGHBOR (EAST),

State           : G8032_ST_IDLE

East            : xe16.1, Blocked  , UP  , BPR (0), remote (b8:6a:97:25:a7:d4)
West            : xe3.1, Unblocked, UP  , BPR (0), remote (b8:6a:97:25:a7:d4)

East (cfm)      : mep_id (322), cc-interval (1s), Domain (P3P22), MA (ma322)
West (cfm)      : mep_id (342), cc-interval (1s), Domain (P4P32), MA (ma432)

Channel         : Level (5), vlan (200), RING_ID (1)

Bridge3#show g8032 erp-instance
Instance         ID  State       East          state     West          state      Ring
-------------------------------------------------------------------------------------
erp1             1   IDLE        xe16.1 (N)     Blocked   xe3.1         Unblocked  ring1

Bridge3#show g8032 erp-instance data-traffic
Instance         ID  Data-vlan                East           West           Ring
-------------------------------------------------------------------------------------
erp1             1   bridge_domain 1          xe16.1 (B)      xe3.1 (F)      ring1
```

Bridge4

```
Bridge4#show g8032 erp-instance
Instance         ID  State       East          state     West          state      Ring
-------------------------------------------------------------------------------------
erp1             1   IDLE        xe6.1        Unblocked xe16.1 (O)    Blocked    ring1

Bridge4#show g8032 erp-instance erp1
Inst Name       : erp1 (1), node-id b8:6a:97:25:a7:d4, Profile (1)
Description     :
Ring            : MAJOR-RING (ring1), OWNER (WEST),
                  Attached (erp3,),tcn_propagation (0)

State           : G8032_ST_IDLE

East            : xe6.1, Unblocked, UP  , BPR (-), remote (-)
West            : xe16.1, Blocked  , UP  , BPR (-), remote (-)

East (cfm)      : mep_id (252), cc-interval (1s), Domain (P5P22), MA (ma522)
West (cfm)      : mep_id (223), cc-interval (1s), Domain (P3P22), MA (ma322)

Channel         : Level (5), vlan (200), RING_ID (1)

Bridge4#show g8032 erp-instance data-traffic
Instance         ID  Data-vlan                East           West           Ring
-------------------------------------------------------------------------------------
erp1             1   bridge_domain 1          xe6.1 (F)     xe16.1 (B)     ring1
```

Associate Ring Configuration

The `associate-ring` is a newly introduced command for supporting ERPS within a bridge-domain. This command is used when there is a need to establish a single ERPS instance that can manage multiple rings. It is essential that all

rings associated with the `associate-ring` share the same parent interface as the primary ring linked to the ERPS instance. For more details, refer to the *associate-ring* command section.

Prerequisite

Before using the `associate-ring` command, it is necessary to configure the major ring for *Bridge1*, *Bridge2, Bridge3,* and *Bridge4* as described in the *Major Ring Configuration* section.

Bridge1

`Bridge1#configure terminal`	Enter configure mode.
`Bridge1(config)#interface xe6.2 switchport`	Create a Layer 2 sub-interface `xe6.2` for the physical interface `xe6`.
`Bridge1(config-if)encapsulation dot1ad 2003`	Encapsulate the sub-interface with APS-channel VLAN ID `2003`.
`Bridge1(config-if)encapsulation dot1ad 800`	Encapsulate the sub-interface with data VLAN ID `800`.
`Bridge1(config-if)#exit`	Exit interface mode `xe6.2`.
`Bridge1(config)#interface xe8.2 switchport`	Create a Layer 2 sub-interface `xe8.2` for the physical interface `xe8`.
`Bridge1(config-if)encapsulation dot1ad 2003`	Encapsulate the sub-interface with APS-channel VLAN ID `2003`.
`Bridge1(config-if)encapsulation dot1ad 800`	Encapsulate the sub-interface with data VLAN ID `800`.
`Bridge1(config-if)#exit`	Exit interface mode `xe8.2`.
`Bridge1(config)#bridge-domain 2`	Enter bridge domain configure mode and configure bridge domain instance `2`.
`Bridge1(config-bridge-domain)#interface xe6.2`	Attach the sub-interface `xe6.2` to the bridge domain instance.
`Bridge1(config-bridge-domain)#interface xe8.2`	Attach the sub-interface `xe8.2` to the bridge domain instance.
`Bridge1(config-bridge-domain)#exit`	Exit bridge domain mode.
`Bridge1(config)#ethernet cfm domain-type character-string domain-name P543 level 5`	Create a CFM domain with character string type, name `P543`, and level `5`.
`Bridge1(config-ether-cfm)#service ma-type string ma-name ma543`	Create a CFM Maintenance Association (MA) type as a string with the name `ma543`.
`Bridge1(config-ether-cfm-ma)#vlan 2003`	Add VLAN `2003` to the CFM MA.
`Bridge1(config-ether-cfm-ma)#ethernet cfm mep down mpid 543 active true xe8.2`	Create a down MEP `543` for `xe8.2` interface and activate it.
`Bridge1(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable Continuity Check (CC) multicast for the MEP.
`Bridge1(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit Ethernet CFM MA-MEP mode.
`Bridge1(config-ether-cfm-ma)#mep crosscheck mpid 453`	Configure crosscheck for the remote MEP with value `453`.

`Bridge1(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet CFM MA mode.
`Bridge1(config-ether-cfm)#exit`	Exit Ethernet CFM mode and return to the configure mode.
`Bridge1(config)#ethernet cfm domain-type character-string domain-name P523 level 5`	Create a CFM domain with character string type, name `P523`, and level `5`.
`Bridge1(config-ether-cfm)#service ma-type string ma-name ma523`	Create a CFM MA type as a string with the name `ma523.`
`Bridge1(config-ether-cfm-ma)#vlan 2003`	Add VLAN `2003` to the CFM MA.
`Bridge1(config-ether-cfm-ma)#ethernet cfm mep down mpid 523 active true xe6.2`	Create a down MEP 523 for `xe6.2` interface and activate it.
`Bridge1(config-ether-cfm-ma-mep)#cc multicast state enable`	Enables CC multicast for the MEP.
`Bridge1(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit Ethernet CFM MA-MEP mode.
`Bridge1(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet CFM MA mode.
`Bridge1(config-ether-cfm)#exit`	Exit Ethernet CFM mode and return to the configure mode.
`Bridge1(config)#g8032 ring RING2`	Create a G.8032 ring named `RING2`.
`Bridge1(g8032-ring-config)#east-interface xe8.2`	Associate `xe8.2` interface as the east interface in `RING2`.
`Bridge1(g8032-ring-config)#west-interface xe6.2`	Associate `xe6.2` interface as the west interface in `RING2`.
`Bridge1(g8032-ring-config)#exit`	Exit ring configure mode and return to the configure mode.
`Bridge1(config)#g8032 erp-instance erp1`	Create a G.8032 Ethernet Ring Protection (ERP) instance named `erp1`.
`Bridge1(g8032-config-switch)#associate-ring RING2`	**Map the associate ring named `RING2` to the ERPS instance `erp1`.**
`Bridge1(g8032-config-switch)#commit`	Commit the candidate configuration to the running configuration
`Bridge1(g8032-config-switch)#end`	Exit G.8032 configure mode.

Bridge2

`Bridge2#configure terminal`	Enter configure mode.
`Bridge2(config)#interface xe3.2 switchport`	Create a Layer 2 sub-interface `xe3.2` for the physical interface `xe3`.
`Bridge2(config-if)encapsulation dot1ad 2003`	Encapsulate the sub-interface with APS-channel VLAN ID `2003`.
`Bridge2(config-if)encapsulation dot1ad 800`	Encapsulate the sub-interface with data VLAN ID `800`.
`Bridge2(config-if)#exit`	Exit interface mode `xe3.2`.
`Bridge2(config)#interface xe8.2 switchport`	Create a Layer 2 sub-interface `xe8.2` for the physical interface `xe8`.

`Bridge2(config-if)encapsulation dot1ad 2003`	Encapsulate the sub-interface with APS-channel VLAN ID `2003`.
`Bridge2(config-if)encapsulation dot1ad 800`	Encapsulate the sub-interface with data VLAN ID `800`.
`Bridge2(config-if)#exit`	Exit interface mode `xe8.2`.
`Bridge2(config)#bridge-domain 2`	Enter bridge domain configure mode and configure bridge domain instance `2`.
`Bridge2(config-bridge-domain)#interface xe3.2`	Attach the sub-interface `xe3.2` to the bridge domain instance.
`Bridge2(config-bridge-domain)#interface xe8.2`	Attach the sub-interface `xe8.2` to the bridge domain instance.
`Bridge2(config-bridge-domain)#exit`	Exit bridge domain mode.
`Bridge2(config)#ethernet cfm domain-type character-string domain-name P543 level 5`	Create a CFM domain with character string type, name `P543`, and level `5`.
`Bridge2(config-ether-cfm)#service ma-type string ma-name ma543`	Create a CFM Maintenance Association (MA) type as a string with the name `ma543`.
`Bridge2(config-ether-cfm-ma)#vlan 2003`	Add VLAN `2003` to the CFM MA.
`Bridge2(config-ether-cfm-ma)#ethernet cfm mep down mpid 453 active true xe8.2`	Create a down MEP `453` for `xe8.2` interface and activate it.
`Bridge2(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable Continuity Check (CC) multicast for the MEP.
`Bridge2(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit Ethernet CFM MA-MEP mode.
`Bridge2(config-ether-cfm-ma)#mep crosscheck mpid 543`	Configure crosscheck for the remote MEP with value `543`.
`Bridge2(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet CFM MA mode.
`Bridge2(config-ether-cfm)#exit`	Exit Ethernet CFM mode and return to the configure mode.
`Bridge2(config)#ethernet cfm domain-type character-string domain-name P433 level 5`	Create a CFM domain with character string type, name `P433`, and level `5`.
`Bridge2(config-ether-cfm)#service ma-type string ma-name ma433`	Create a CFM MA type as a string with the name `ma433.`
`Bridge2(config-ether-cfm-ma)#vlan 2003`	Add VLAN `2003` to the CFM MA.
`Bridge2(config-ether-cfm-ma)#ethernet cfm mep down mpid 433 active true xe3.2`	Create a down MEP 433 for `xe3.2` interface and activate it.
`Bridge2(config-ether-cfm-ma-mep)#cc multicast state enable`	Enables CC multicast for the MEP.
`Bridge2(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit Ethernet CFM MA-MEP mode.

`Bridge2(config-ether-cfm-ma)#mep crosscheck mpid 533`	Configure crosscheck for the remote MEP with value `533`.
`Bridge2(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet CFM MA mode.
`Bridge2(config-ether-cfm)#exit`	Exit Ethernet CFM mode and return to the configure mode.
`Bridge2(config)#g8032 ring RING2`	Create a G.8032 ring named `RING2`.
`Bridge2(g8032-ring-config)#east-interface xe3.2`	Associate `xe3.2` interface as the east interface in `RING2`.
`Bridge2(g8032-ring-config)#west-interface xe8.2`	Associate `xe8.2` interface as the west interface in `RING2`.
`Bridge2(g8032-ring-config)#exit`	Exit ring configure mode and return to the configure mode.
`Bridge2(config)#g8032 erp-instance erp1`	Create a G.8032 Ethernet Ring Protection (ERP) instance named `erp1`.
`Bridge2(g8032-config-switch)#associate-ring RING2`	Map the associate ring named `RING2` to the ERPS instance `erp1`.
`Bridge2(g8032-config-switch)#commit`	Commit the candidate configuration to the running configuration
`Bridge2(g8032-config-switch)#end`	Exit G.8032 configure mode.

Bridge3

`Bridge3#configure terminal`	Enter configure mode.
`Bridge3(config)#interface xe3.2 switchport`	Create a Layer 2 sub-interface `xe3.2` for the physical interface `xe3`.
`Bridge3(config-if)encapsulation dot1ad 2003`	Encapsulate the sub-interface with APS-channel VLAN ID `2003`.
`Bridge3(config-if)encapsulation dot1ad 800`	Encapsulate the sub-interface with data VLAN ID `800`.
`Bridge3(config-if)#exit`	Exit interface mode `xe3.2`.
`Bridge3(config)#interface xe16.2 switchport`	Create a Layer 2 sub-interface `xe16.2` for the physical interface `xe16`.
`Bridge3(config-if)encapsulation dot1ad 2003`	Encapsulate the sub-interface with APS-channel VLAN ID `2003`.
`Bridge3(config-if)encapsulation dot1ad 800`	Encapsulate the sub-interface with data VLAN ID `800`.
`Bridge3(config-if)#exit`	Exit interface mode `xe16.2`.
`Bridge3(config)#bridge-domain 2`	Enter bridge domain configure mode and configure bridge domain instance `2`.
`Bridge3(config-bridge-domain)#interface xe3.2`	Attach the sub-interface `xe3.2` to the bridge domain instance.
`Bridge3(config-bridge-domain)#interface xe16.2`	Attach the sub-interface `xe16.2` to the bridge domain instance.
`Bridge3(config-bridge-domain)#exit`	Exit bridge domain mode.
`Bridge3(config)#ethernet cfm domain-type character-string domain-name P433 level 5`	Create a CFM domain with character string type, name `P433`, and level `5`.

`Bridge3(config-ether-cfm)#service ma-type string ma-name ma433`	Create a CFM Maintenance Association (MA) type as a string with the name `ma433`.
`Bridge3(config-ether-cfm-ma)#vlan 2003`	Add VLAN `2003` to the CFM MA.
`Bridge3(config-ether-cfm-ma)#ethernet cfm mep down mpid 343 active true xe16.2`	Create a down MEP `343` for `xe16.2` interface and activate it.
`Bridge3(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable Continuity Check (CC) multicast for the MEP.
`Bridge3(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit Ethernet CFM MA-MEP mode.
`Bridge3(config-ether-cfm-ma)#mep crosscheck mpid 433`	Configure crosscheck for the remote MEP with value `433`.
`Bridge3(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet CFM MA mode.
`Bridge3(config-ether-cfm)#exit`	Exit Ethernet CFM mode and return to the configure mode.
`Bridge3(config)#ethernet cfm domain-type character-string domain-name P323 level 5`	Create a CFM domain with character string type, name `P323`, and level `5`.
`Bridge3(config-ether-cfm)#service ma-type string ma-name ma323`	Create a CFM MA type as a string with the name `ma323.`
`Bridge3(config-ether-cfm-ma)#vlan 2003`	Add VLAN `2003` to the CFM MA.
`Bridge3(config-ether-cfm-ma)#ethernet cfm mep down mpid 323 active true xe3.2`	Create a down MEP 323 for `xe3.2` interface and activate it.
`Bridge3(config-ether-cfm-ma-mep)#cc multicast state enable`	Enables CC multicast for the MEP.
`Bridge3(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit Ethernet CFM MA-MEP mode.
`Bridge3(config-ether-cfm-ma)#mep crosscheck mpid 233`	Configure crosscheck for the remote MEP with value `233`.
`Bridge3(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet CFM MA mode.
`Bridge3(config-ether-cfm)#exit`	Exit Ethernet CFM mode and return to the configure mode.
`Bridge3(config)#g8032 ring RING2`	Create a G.8032 ring named `RING2`.
`Bridge3(g8032-ring-config)#east-interface xe16.2`	Associate `xe16.2` interface as the east interface in `RING2`.
`Bridge3(g8032-ring-config)#west-interface xe3.2`	Associate `xe3.2` interface as the west interface in `RING2`.
`Bridge3(g8032-ring-config)#exit`	Exit ring configure mode and return to the configure mode.
`Bridge3(config)#g8032 erp-instance erp1`	Create a G.8032 Ethernet Ring Protection (ERP) instance named `erp1`.

Bridge3(g8032-config-switch)#associate-ring RING2	Map the associate ring named RING2 to the ERPS instance erp1.
Bridge3(g8032-config-switch)#commit	Commit the candidate configuration to the running configuration
Bridge3(g8032-config-switch)#end	Exit G.8032 configure mode.

Bridge4

Bridge4#configure terminal	Enter configure mode.
Bridge4(config)#interface xe6.2 switchport	Create a Layer 2 sub-interface xe6.2 for the physical interface xe6.
Bridge4(config-if)encapsulation dot1ad 2003	Encapsulate the sub-interface with APS-channel VLAN ID 2003.
Bridge4(config-if)encapsulation dot1ad 800	Encapsulate the sub-interface with data VLAN ID 800.
Bridge4(config-if)#exit	Exit interface mode xe6.2.
Bridge4(config)#interface xe16.2 switchport	Create a Layer 2 sub-interface xe16.2 for the physical interface xe16.
Bridge4(config-if)encapsulation dot1ad 2003	Encapsulate the sub-interface with APS-channel VLAN ID 2003.
Bridge4(config-if)encapsulation dot1ad 800	Encapsulate the sub-interface with data VLAN ID 800.
Bridge4(config-if)#exit	Exit interface mode xe16.2.
Bridge4(config)#bridge-domain 2	Enter bridge domain configure mode and configure bridge domain instance 2.
Bridge4(config-bridge-domain)#interface xe6.2	Attach the sub-interface xe6.2 to the bridge domain instance.
Bridge4(config-bridge-domain)#interface xe16.2	Attach the sub-interface xe16.2 to the bridge domain instance.
Bridge4(config-bridge-domain)#exit	Exit bridge domain mode.
Bridge4(config)#ethernet cfm domain-type character-string domain-name P523 level 5	Create a CFM domain with character string type, name P523, and level 5.
Bridge4(config-ether-cfm)#service ma-type string ma-name ma523	Create a CFM Maintenance Association (MA) type as a string with the name ma523.
Bridge4(config-ether-cfm-ma)#vlan 2003	Add VLAN 2003 to the CFM MA.
Bridge4(config-ether-cfm-ma)#ethernet cfm mep down mpid 253 active true xe6.2	Create a down MEP 253 for xe6.2 interface and activate it.
Bridge4(config-ether-cfm-ma-mep)#cc multicast state enable	Enable Continuity Check (CC) multicast for the MEP.
Bridge4(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode	Exit Ethernet CFM MA-MEP mode.
Bridge4(config-ether-cfm-ma)#mep crosscheck mpid 523	Configure crosscheck for the remote MEP with value 523.

`Bridge4(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet CFM MA mode.
`Bridge4(config-ether-cfm)#exit`	Exit Ethernet CFM mode and return to the configure mode.
`Bridge4(config)#ethernet cfm domain-type character-string domain-name P323 level 5`	Create a CFM domain with character string type, name `P323`, and level `5`.
`Bridge4(config-ether-cfm)#service ma-type string ma-name ma323`	Create a CFM MA type as a string with the name `ma323.`
`Bridge4(config-ether-cfm-ma)#vlan 2003`	Add VLAN `2003` to the CFM MA.
`Bridge4(config-ether-cfm-ma)#ethernet cfm mep down mpid 233 active true xe16.2`	Create a down MEP 233 for `xe16.2` interface and activate it.
`Bridge4(config-ether-cfm-ma-mep)#cc multicast state enable`	Enables CC multicast for the MEP.
`Bridge4(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit Ethernet CFM MA-MEP mode.
`Bridge4(config-ether-cfm-ma)#mep crosscheck mpid 323`	Configure crosscheck for the remote MEP with value `323`.
`Bridge4(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet CFM MA mode.
`Bridge4(config-ether-cfm)#exit`	Exit Ethernet CFM mode and return to the configure mode.
`Bridge4(config)#g8032 ring RING2`	Create a G.8032 ring named `RING2`.
`Bridge4(g8032-ring-config)#east-interface xe6.2`	Associate `xe6.2` interface as the east interface in `RING2`.
`Bridge4(g8032-ring-config)#west-interface xe16.2`	Associate `xe16.2` interface as the west interface in `RING2`.
`Bridge4(g8032-ring-config)#exit`	Exit ring configure mode and return to the configure mode.
`Bridge4(config)#g8032 erp-instance erp1`	Create a G.8032 Ethernet Ring Protection (ERP) instance named `erp1`.
`Bridge4(g8032-config-switch)#associate-ring RING2`	Map the associate ring named `RING2` to the ERPS instance `erp1`.
`Bridge4(g8032-config-switch)#commit`	Commit the candidate configuration to the running configuration
`Bridge4(g8032-config-switch)#end`	Exit G.8032 configure mode.

Validation

The following validation output displays data traffic details for ERP instances and provides details for the specified ERP instance using the `show g8032 erp-instance data-traffic` command on Bridge1, Bridge2, Bridge3, and Bridge4.

```
Bridge1#show g8032 erp-instance data-traffic
Instance         ID  Data-vlan                East           West           Ring
-------------------------------------------------------------------------------
erp1             1   bridge_domain 1          xe8.1 (F)      xe25.1 (F)     ring1
                     bridge_domain 2          xe8.2          xe25.2         ring2
```

```
Bridge2#show g8032 erp-instance data-traffic
Instance         ID  Data-vlan                East           West           Ring
-------------------------------------------------------------------------------
erp1             1   bridge_domain 1          xe3.1 (F)      xe82.1 (F)      ring1
                     bridge_domain 2          xe3.2          xe8.2           ring2

Bridge3#show g8032 erp-instance data-traffic
Instance         ID  Data-vlan                East           West           Ring
-------------------------------------------------------------------------------
erp1             1   bridge_domain 1          xe16.1 (B)      xe3.1 (F)      ring1
                     bridge_domain 2          xe16.2          xe3.2          ring2

Bridge4#show g8032 erp-instance data-traffic
Instance         ID  Data-vlan                East           West           Ring
-------------------------------------------------------------------------------
erp1             1   bridge_domain 1          xe16.1 (F)     xe16.1 (B)     ring1
                     bridge_domain 2          xe16.2         xe6.2          ring2
```

Sub-ring with Virtual Channel Configuration

An Ethernet ring connects to a Major Ring at the interconnection nodes. The Sub-Ring, by itself, does not constitute a closed ring. It connects to the interconnection nodes on only one port, which is configured as the east-interface.

Topology

Figure 2 displays a sample Ring Protection topology with five bridges, consisting of one major ring (Bridge1, Bridge2, Bridge3, and Bridge4) and one sub-ring (Bridge5, Bridge1, and Bridge2). In the major ring, the RPL is enabled between Bridge 3 (owner node) and Bridge 4 (neighbor node) on the xe16 interface, while other devices are non-owner nodes for that ring. In the sub-ring, the RPL is enabled between Bridge 5 (neighbor node) and Bridge 4 (owner node) on link xe7, with other devices as non-owner nodes. A virtual channel is enabled for this Sub-Ring on interconnected nodes on VLAN 100, and TCN propagation is also enabled.

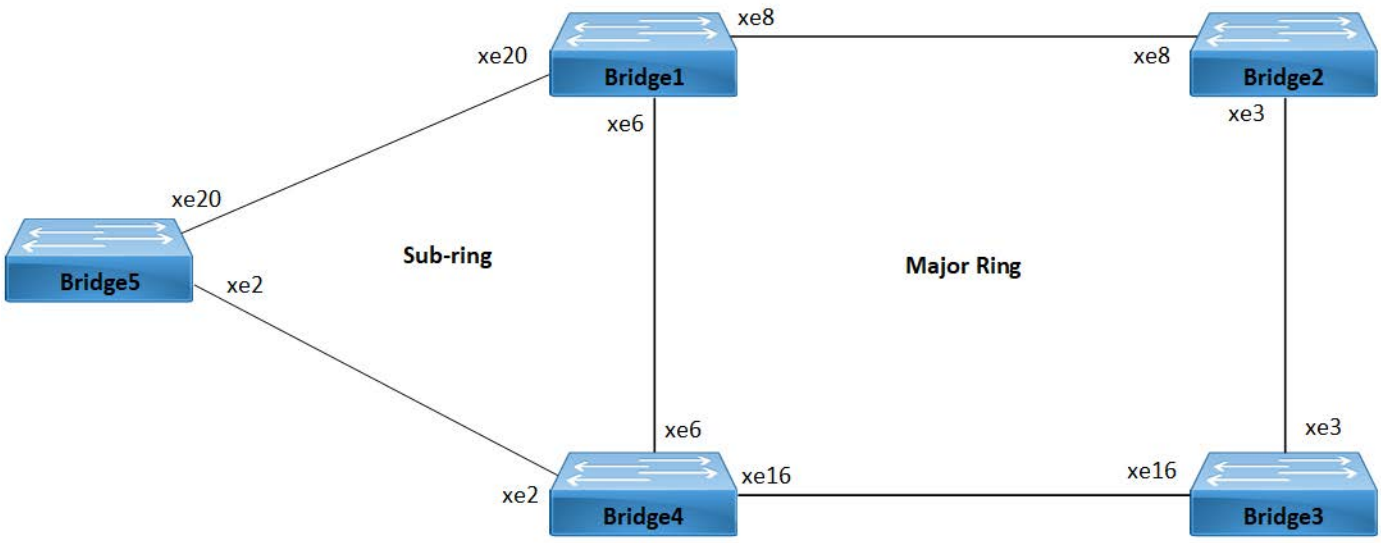


Figure 2: Sub-ring with Virtual Channel

Prerequisite

Before configuring the sub-ring with virtual channel, it is necessary to configure the major ring for *Bridge1, Bridge2, Bridge3,* and *Bridge4* as described in the *Major Ring Configuration* section.

Bridge5

`Bridge5#configure terminal`	Enter configure mode.
`Bridge5(config)#interface xe2`	Enter interface mode `xe2`.
`Bridge5(config-if)#dot1ad ethertype 0x88a8`	Configure `xe2` as a Layer 2 port with an Ethernet Type of `0x88a8`.
`Bridge5(config-if)#interface xe2.1 switchport`	Create a Layer 2 sub-interface `xe2.1` within the physical interface `xe2`.
`Bridge5(config-if)encapsulation dot1ad 200`	Encapsulate the sub-interface with APS-channel VLAN ID `200`.
`Bridge5(config-if)encapsulation dot1ad 600`	Encapsulate the sub-interface with data VLAN ID `600`.
`Bridge5(config-if)#exit`	Exit interface mode `xe2`.
`Bridge5(config)#interface xe20`	Enter interface mode `xe20`.
`Bridge5(config-if)#dot1ad ethertype 0x88a8`	Configure `xe20` as a Layer 2 port with an Ethernet Type of `0x88a8`.
`Bridge5(config)#interface xe20.1 switchport`	Create a Layer 2 sub-interface `xe20.1` within the physical interface `xe20`.
`Bridge5(config-if)encapsulation dot1ad 200`	Encapsulate the sub-interface with APS-channel VLAN ID `200`.
`Bridge5(config-if)encapsulation dot1ad 600`	Encapsulate the sub-interface with data VLAN ID `600`.
`Bridge5(config-if)#exit`	Exit interface mode `xe20`.
`Bridge5(config)#bridge-domain 1`	Enter bridge domain configure mode and configure bridge domain instance `1`.
`Bridge5(config-bridge-domain)#interface xe2.1`	Attach the sub-interface `xe2.1` to the bridge domain instance.
`Bridge5(config-bridge-domain)#interface xe20.1`	Attach the sub-interface `xe20.1` to the bridge domain instance.
`Bridge5(config-bridge-domain)#exit`	Exit bridge domain mode.
`Bridge5(config)#ethernet cfm domain-type character-string domain-name P271 level 5`	Create a CFM domain with character string type, name `P271`, and level `5`.
`Bridge5(config-ether-cfm)#service ma-type string ma-name ma8`	Create a CFM Maintenance Association (MA) type as a string with the name `ma8`.
`Bridge5(config-ether-cfm-ma)#vlan 200`	Add VLAN `200` to the CFM MA.
`Bridge5(config-ether-cfm-ma)#ethernet cfm mep down mpid 801 active true xe2.1`	Create a down MEP `801` for `xe2.1` interface and activate it.
`Bridge5(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable Continuity Check (CC) multicast for the MEP.

`Bridge5(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit Ethernet CFM MA-MEP mode.
`Bridge5(config-ether-cfm-ma)#mep crosscheck mpid 800`	Configure crosscheck for the remote MEP with value `800`.
`Bridge5(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet CFM MA mode.
`Bridge5(config-ether-cfm)#exit`	Exit Ethernet CFM mode and return to the configure mode.
`Bridge5(config)#ethernet cfm domain-type character-string domain-name P571 level 5`	Create a CFM domain with character string type, name `P571`, and level `5`.
`Bridge5(config-ether-cfm)#service ma-type string ma-name ma7`	Create a CFM MA type as a string with the name `ma7.`
`Bridge5(config-ether-cfm-ma)#vlan 200`	Add VLAN `200` to the CFM MA.
`Bridge5(config-ether-cfm-ma)#ethernet cfm mep down mpid 905 active true xe20.1`	Create a down MEP `905` for `xe20.1` interface and activate it.
`Bridge5(config-ether-cfm-ma-mep)#cc multicast state enable`	Enables CC multicast for the MEP.
`Bridge5(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit Ethernet CFM MA-MEP mode.
`Bridge5(config-ether-cfm-ma)#mep crosscheck mpid 906`	Configure crosscheck for the remote MEP with value `906`.
`Bridge5(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet CFM MA mode.
`Bridge5(config-ether-cfm)#exit`	Exit Ethernet CFM mode and return to the configure mode.
`Bridge5(config)#g8032 ring subring2`	Create a G.8032 ring named `subring2`.
`Bridge5(g8032-ring-config)#east-interface xe2.1`	Associate `xe2.1` interface as the east interface in `subring2`.
`Bridge5(g8032-ring-config)#west-interface xe20.1`	Associate `xe20.1` interface as the west interface in `subring2`.
`Bridge5(g8032-ring-config)#g8032 profile profile1`	Create a G.8032 profile named `profile1`.
`Bridge5(g8032-profile-config)#timer wait-to-restore 2`	Configure the wait-to-restore timer for `2` minute.
`Bridge5(g8032-profile-config)#timer hold-off 200`	Configure the hold-off timer with a value of `200`.
`Bridge5(g8032-profile-config)#timer guard-timer 20`	Configure the guard timer with a value of `20` milliseconds.
`Bridge5(g8032-profile-config)#switching mode revertive`	Configure the switching mode as `revertive`.
`Bridge5(g8032-profile-config)#exit`	Exit profile configure mode and return to the ring configure mode.
`Bridge5(g8032-ring-config)#exit`	Exit ring configure mode and return to the configure mode.

`Bridge5(config)#g8032 erp-instance erp2`	Create a G.8032 Ethernet Ring Protection (ERP) instance named `erp2`.
`Bridge5(g8032-config-switch)#ring-type sub-ring-vc`	Configure the ring type as a `sub-ring-vc`.
`Bridge5(g8032-config-switch)#ring subring2`	Associate `subring2` with the ERP instance `erp2`.
`Bridge5(g8032-config-switch)#rpl role neighbor east-interface`	Configure the node as the `neighbor` node for the specified ERPS ring and designate the `east interface` as the owner node in the ring.
`Bridge5(g8032-config-switch)#g8032-profile profile1`	Associate `profile1` with `erp2` instance.
`Bridge5(g8032-config-switch)#aps-channel level 5`	Configure the R-APS channel level as `5`.
`Bridge5(g8032-config-switch)#aps-channel vlan 200`	Configure the APS channel VLAN as `200`.
`Bridge5(g8032-config-switch)#ring-id 3`	Configure the ring ID as `3`.
`Bridge5(g8032-config-switch)#commit`	Commit the candidate configuration to the running configuration
`Bridge5(g8032-config-switch)#end`	Exit G.8032 configure mode.

Bridge1

`Bridge1#configure terminal`	Enter configure mode.
`Bridge1(config)#interface xe20`	Enter interface mode `xe20`.
`Bridge1(config-if)#dot1ad ethertype 0x88a8`	Configure `xe20` as a Layer 2 port with an Ethernet Type of `0x88a8`.
`Bridge1(config-if)#interface xe20.1 switchport`	Create a Layer 2 sub-interface `xe20.1` within the physical interface `xe20`.
`Bridge1(config-if)encapsulation dot1ad 200`	Encapsulate the sub-interface with APS-channel VLAN ID `200`.
`Bridge1(config-if)encapsulation dot1ad 600`	Encapsulate the sub-interface with data VLAN ID `600`.
`Bridge1(config-if)#exit`	Exit interface mode `xe20`.
`Bridge1(config)#bridge-domain 1`	Enter bridge domain configure mode and configure bridge domain instance `1`.
`Bridge1(config-bridge-domain)#interface xe20.1`	Attach the sub-interface `xe20.1` to the bridge domain instance.
`Bridge1(config-bridge-domain)#exit`	Exit bridge domain mode.
`Bridge1(config)#ethernet cfm domain-type character-string domain-name P571 level 5`	Create a CFM domain with character string type, name `P571`, and level `5`.
`Bridge1(config-ether-cfm)#service ma-type string ma-name ma7`	Create a CFM Maintenance Association (MA) type as a string with the name `ma7`.
`Bridge1(config-ether-cfm-ma)#vlan 200`	Add VLAN `200` to the CFM MA.

`Bridge1(config-ether-cfm-ma)#ethernet cfm mep down mpid 906 active true xe20.1`	Create a down MEP `906` for `xe20.1` interface and activate it.
`Bridge1(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable Continuity Check (CC) multicast for the MEP.
`Bridge1(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit Ethernet CFM MA-MEP mode.
`Bridge1(config-ether-cfm-ma)#mep crosscheck mpid 905`	Configure crosscheck for the remote MEP with value `905`.
`Bridge1(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet CFM MA mode.
`Bridge1(config-ether-cfm)#exit`	Exit Ethernet CFM mode and return to the configure mode.
`Bridge1(config)#g8032 ring subring2`	Create a G.8032 ring named `subring2`.
`Bridge1(g8032-ring-config)#east-interface xe20.1`	Associate `xe20.1` interface as the east interface in `subring2`.
`Bridge1(g8032-ring-config)#exit`	Exit ring configure mode and return to the configure mode.
`Bridge1(config)#g8032 erp-instance erp3`	Create a G.8032 Ethernet Ring Protection (ERP) instance named `erp3`.
`Bridge1(g8032-config-switch)#ring-type sub-ring-vc`	Configure the ring type as a `sub-ring-vc`.
`Bridge1(g8032-config-switch)#ring subring2`	Associate `subring2` with the ERP instance `erp3`.
`Bridge1(g8032-config-switch)#rpl role non-owner`	Configure the node as a `non-owner` node in the ring.
`Bridge1(g8032-config-switch)#g8032-profile profile1`	Associate `profile1` with `erp3` instance.
`Bridge1(g8032-config-switch)#aps-channel level 5`	Configure the R-APS channel level as `5`.
`Bridge1(g8032-config-switch)#aps-channel vlan 200`	Configure the APS channel VLAN as `200`.
`Bridge1(g8032-config-switch)#ring-id 3`	Configure the ring ID as `3`.
`Bridge1(g8032-config-switch)#virtual-channel 100 attached-to-instance erp1`	Configure the virtual channel with VLAN `100` and attache it to ERP instance `erp1`.
`Bridge1(g8032-config-switch)#enable-tcn-propagation`	Enable Topology Change Notification (TCN) propagation.
`Bridge1(g8032-config-switch)#commit`	Commit the candidate configuration to the running configuration
`Bridge1(g8032-config-switch)#end`	Exit G.8032 configure mode.

Bridge4

`Bridge4#configure terminal`	Enter configure mode.
`Bridge4(config)#interface xe2`	Enter interface mode `xe2`.
`Bridge4(config-if)#dot1ad ethertype 0x88a8`	Configure `xe2` as a Layer 2 port with an Ethernet Type of `0x88a8`.
`Bridge4(config-if)#interface xe2.1 switchport`	Create a Layer 2 sub-interface `xe2.1` within the physical interface `xe2`.

`Bridge4(config-if)encapsulation dot1ad 200`	Encapsulate the sub-interface with APS-channel VLAN ID `200`.
`Bridge4(config-if)encapsulation dot1ad 600`	Encapsulate the sub-interface with data VLAN ID `600`.
`Bridge4(config-if)#exit`	Exit interface mode `xe2`.
`Bridge4(config)#bridge-domain 1`	Enter bridge domain configure mode and configure bridge domain instance `1`.
`Bridge4(config-bridge-domain)#interface xe2.1`	Attach the sub-interface `xe2.1` to the bridge domain instance.
`Bridge4(config-bridge-domain)#exit`	Exit bridge domain mode.
`Bridge4(config)#ethernet cfm domain-type character-string domain-name P271 level 5`	Create a CFM domain with character string type, name `P271`, and level `5`.
`Bridge4(config-ether-cfm)#service ma-type string ma-name ma8`	Create a CFM Maintenance Association (MA) type as a string with the name `ma8`.
`Bridge4(config-ether-cfm-ma)#vlan 200`	Add VLAN `200` to the CFM MA.
`Bridge4(config-ether-cfm-ma)#ethernet cfm mep down mpid 800 active true xe2.1`	Create a down MEP `800` for `xe2.1` interface and activate it.
`Bridge4(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable Continuity Check (CC) multicast for the MEP.
`Bridge4(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit Ethernet CFM MA-MEP mode.
`Bridge4(config-ether-cfm-ma)#mep crosscheck mpid 801`	Configure crosscheck for the remote MEP with value `801`.
`Bridge4(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet CFM MA mode.
`Bridge4(config-ether-cfm)#exit`	Exit Ethernet CFM mode and return to the configure mode.
`Bridge4(config)#g8032 ring subring2`	Create a G.8032 ring named `subring2`.
`Bridge4(g8032-ring-config)#east-interface xe2.1`	Associate `xe2.1` interface as the east interface in `subring2`.
`Bridge4(g8032-ring-config)#exit`	Exit ring configure mode and return to the configure mode.
`Bridge4(config)#g8032 erp-instance erp3`	Create a G.8032 Ethernet Ring Protection (ERP) instance named `erp3`.
`Bridge4(g8032-config-switch)#ring-type sub-ring-vc`	Configure the ring type as a `sub-ring-vc`.
`Bridge4(g8032-config-switch)#ring subring2`	Associate `subring2` with the ERP instance `erp3`.
`Bridge4(g8032-config-switch)#rpl role owner east-interface`	Configure the node as the `owner` node for the specified ERPS ring and designate the east interface as the neighbor node in the ring.
`Bridge4(g8032-config-switch)#g8032-profile profile1`	Associate `profile1` with `erp3` instance.
`Bridge4(g8032-config-switch)#aps-channel level 5`	Configure the R-APS channel level as `5`.

`Bridge4(g8032-config-switch)#aps-channel vlan 200`	Configure the APS channel VLAN as `200`.
`Bridge4(g8032-config-switch)#ring-id 3`	Configure the ring ID as `3`.
`Bridge4(g8032-config-switch)#virtual-channel 100 attached-to-instance erp1`	Configure the virtual channel with VLAN `100` and attache it to ERP instance `erp1`.
`Bridge4(g8032-config-switch)#enable-tcn-propagation`	Enable Topology Change Notification (TCN) propagation.
`Bridge4(g8032-config-switch)#commit`	Commit the candidate configuration to the running configuration
`Bridge4(g8032-config-switch)#end`	Exit G.8032 configure mode.

Validation

The following validation output displays details for the specified ERP instance using the `show g8032 erp-instance` command on Bridge5, Bridge1, and Bridge4. It describes the sub-ring type for Bridge1 and Bridge4 as virtual. Additionally, it specifies that Bridge1 is a non-owner node, while Bridge4 is the owner node for the specified ERPS ring, designating the east interface as the neighbor node in the ring.

```
Bridge5#show g8032 erp-instance
Instance          ID  State       East      state     West      state      Ring
-------------------------------------------------------------------------------
erps2             1   IDLE        xe2.1     Blocked   xe20.1    Unblocked  subring2

Bridge1#show g8032 erp-instance
Instance          ID  State       East      state     West      state      Ring
-------------------------------------------------------------------------------
erp1              1   IDLE        xe8.1     Unblocked   xe6.1    Unblocked   1
erp3              3   IDLE        xe20.1    Unblocked    -         -         subring2

Bridge4#show g8032 erp-instance
Instance          ID  State       East      state     West      state      Ring
-------------------------------------------------------------------------------
erp1              1   IDLE        xe6.1     Unblocked xe16.1    Blocked    Ring1
erp3              3   IDLE        xe2.1     Blocked    -         -         subring2

Bridge1#show g8032 erp-instance erp3
Inst Name       : erp3 (3), node-id e8:c5:7a:a8:7c:c8, Profile (1)
Description     :
Ring            : SUB-RING (VIRTUAL) (subring2), NON-OWNER, Virtual (vid 100 : r
ing_id 1)
                  Attached to (erp1),
                  tcn_propagation (1)

State           : G8032_ST_IDLE

East            : xe20.1, Unblocked, UP  , BPR (-), remote (-)

East (cfm)      : mep_id (906), cc-interval (1s), Domain (P5P71), MA (ma7)

Channel         : Level (5), vlan (200), RING_ID (2)
```

```
Bridge4#show g8032 erp-instance erp3
Inst Name        : erp3 (3), node-id b8:6a:97:25:a7:bd, Profile (1)
Description      :
Ring             : SUB-RING (VIRTUAL) (subring2), OWNER (EAST), Virtual (vid 100
: ring_id 1)
                   Attached to (erp1),
                   tcn_propagation (1)

State            : G8032_ST_IDLE

East             : xe2.1, Blocked  , UP  , BPR (-), remote (-)

East (cfm)       : mep_id (800), cc-interval (1s), Domain (P2P71), MA (ma8)

Channel          : Level (5), vlan (200), RING_ID (2)
```

Sub-ring without Virtual Channel Configuration

The following section presents a sample Ring Protection topology, demonstrating the configuration of protection switching with five bridges.

Topology

Figure 3 illustrates a sample Ethernet Ring Protection Switching topology. This scenario consists of one major ring, which includes Bridge1, Bridge2, Bridge3, and Bridge4, and one sub-ring involving Bridge5, Bridge1, and Bridge2.

In the major ring, RPL is enabled between Bridge 3 (the owner node) and Bridge 4 (the neighbor node) through interface xe16. The remaining devices within this major ring are non-owner nodes. For the sub-ring, RPL is enabled between Bridge 5 (the neighbor node) and Bridge 4 (the owner node) using link xe7, while the other devices in this sub-ring function as non-owner nodes.

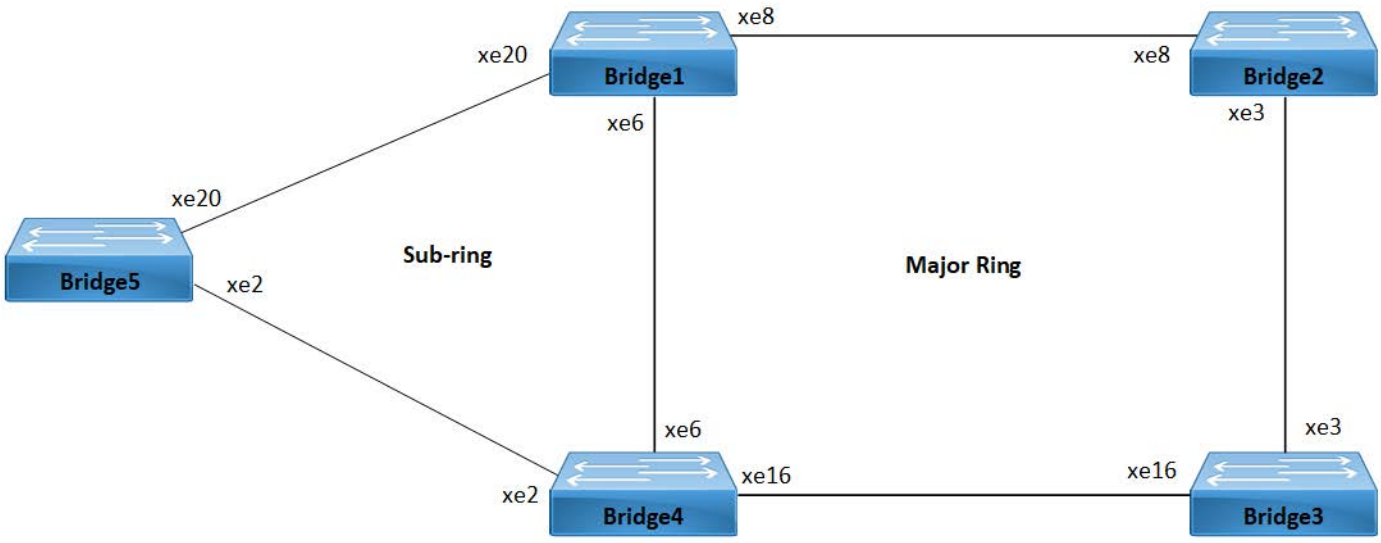


Figure 3: Sub-ring without Virtual Channel

Prerequisite

1. Before configuring the non-virtual channel, ensure that the major ring is configured for *Bridge1, Bridge2, Bridge3,* and *Bridge4* following the instructions provided in the *Major Ring Configuration* section.
2. Repeat the same configuration steps for Bridge5, Bridge1, and *Bridge4* as outlined in the *Sub-ring without Virtual Channel Configuration* section. Instead of using the `virtual-channel` command, configure the `non-virtual channel` command for Bridge1 and Bridge4 as shown below:

`Bridge4(g8032-config-switch)#non-virtual-channel`	Configure the non-virtual channel and attach it to ERP instance.
`Bridge4(g8032-config-switch)#enable-tcn-propagation`	Enable Topology Change Notification (TCN) propagation.
`Bridge4(g8032-config-switch)#tcn-to-instance erp1`	Attach TCN propagation to ERPS instance.

Validation

The following validation output displays details for the specified ERP instance using the `show g8032 erp-instance` command on Bridge5, Bridge1, and Bridge4. It describes the sub-ring type for Bridge1 and Bridge4 as non-virtual. Additionally, it specifies that Bridge1 is a non-owner node, while Bridge4 is the owner node for the specified ERPS ring, designating the east interface as the neighbor node in the ring.

```
Bridge5#show g8032 erp-instance
Instance          ID  State       East      state     West      state      Ring
-------------------------------------------------------------------------------
erps2             1   IDLE        xe2.1     Blocked   xe20.1    Unblocked  subring2

Bridge1#show g8032 erp-instance
Instance          ID  State       East      state     West      state      Ring
-------------------------------------------------------------------------------
erp1              1   IDLE        xe8.1     Unblocked   xe6.1    Unblocked   1
erp3              3   IDLE        xe20.1    Unblocked   -         -          subring2

Bridge4#show g8032 erp-instance
Instance          ID  State       East      state     West      state      Ring
-------------------------------------------------------------------------------
-
erp1              1   IDLE        xe6.1     Unblocked xe16.1    Blocked  Ring1
erp3              3   IDLE        xe2.1     Blocked   -         -          subring2

Bridge1#show g8032 erp-instance erp3
Inst Name       : erp3 (3), node-id e8:c5:7a:a8:7c:c8, Profile (1)
Description     :
Ring            : SUB-RING (NON VIRTUAL) (subring2), NON-OWNER, tcn_propagation
(1)(erp1,)

State           : G8032_ST_IDLE

East            : xe20.1, Unblocked, UP  , BPR (-), remote (-)
```

```
East (cfm)      : mep_id (906), cc-interval (1s), Domain (P5P71), MA (ma7)

Channel         : Level (5), vlan (200), RING_ID (2)

Bridge4#show g8032 erp-instance erp3
Inst Name       : erp3 (3), node-id b8:6a:97:25:a7:bd, Profile (1)
Description     :
Ring            : SUB-RING (NON VIRTUAL) (subring2), OWNER (EAST),tcn_propagation
(1)(erp1,)

State           : G8032_ST_IDLE

East            : xe2.1, Blocked  , UP  , BPR (-), remote (-)

East (cfm)      : mep_id (800), cc-interval (1s), Domain (P2P71), MA (ma8)

Channel         : Level (5), vlan (200), RING_ID (2)
```

Implementation Examples

We explore deploying Ethernet LAN (ELAN) services using a bridge domain and leveraging ERPS to enhance network resilience and accelerate traffic switchover.

ELAN services find common applications in data centers and enterprise networks, facilitating connectivity among multiple endpoints. A bridge domain serves as a logical segment where these services are extended and managed.

Ring Topology in Data Center Network Scenario

In a data center network, multiple access switches are connected to aggregation switches forming a ring topology using bridge domains. The data center operator wants to implement fast protection switching to ensure uninterrupted connectivity for critical services in case of link or node failures.

Use Case: The data center network can achieve network resiliency by configuring ERPS over the bridge domains. In the event of a link failure on one of the ring ports, ERPS will automatically redirect traffic through the backup path, maintaining service continuity and minimizing downtime.

Campus LAN with Redundant Links Scenario

A campus LAN network is designed with redundant links between distribution switches using bridge domains. The network administrators want to implement ring protection to ensure reliable communication between buildings and minimize service disruptions in case of link failures.

Use Case: The campus LAN network can achieve seamless switchover during link failures by deploying ERPS over the bridge domains connecting the distribution switches. ERPS will detect the failure and swiftly switch traffic to the backup link, ensuring continuous connectivity for users and devices.

Industrial Automation Network Scenario

An industrial automation network uses a redundant ring topology with bridge domains to connect various industrial devices and controllers. The network operator requires a solution to achieve rapid network recovery in case of link or node failures.

Use Case: The network operator can achieve seamless switchover during link or node failures by configuring ERPS over the bridge domains in the industrial automation network. ERPS will provide fast protection switching, reducing downtime and ensuring continuous operation of critical industrial processes.

New CLI Commands

The ERPS with CFM Down-MEP over Bridge-Domain introduces the following configuration commands.

associate-ring

Use this command to configure a single ERPS instance to monitor multiple rings. All the rings associated with the `associate-ring` command must share the same parent interface as the primary ring mapped to the ERPS instance.

Note: The primary ring or instance is responsible for monitoring and managing multiple associate rings. However, it's important to note that only failures detected by the primary instance will trigger a switchover in all associated rings. Individual failures, such as link shutdowns on ring ports of associate rings, will not independently trigger failover switches in the associate rings. Instead, the primary instance must detect the failure for it to propagate to the associated rings.

Command Syntax

```
associate-ring RINGNAME
```

Parameters

`RINGNAME`	Specifies the name of the ring to associate with the ERPS instance.

Default

None

Command Mode

G.8032 configure switch mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

Here is a sample example of configuring a G.8032 ERP instance and associate ring in OcNOS device.

```
OcNOS#configure terminal
OcNOS(config)#g8032 erp-instance instance1
OcNOS(g8032-config-switch)#associate-ring ring1
OcNOS(g8032-config-switch)#end
```

hardware-profile aclif failover

Use this command to enable failover for the logical interface (LIF) resources, optimizing ERPS hardware failover ID.

Use the `no` parameter of this command to disable failover for the LIF resources.

Note: Recommend using per-interface-based Access Control List (ACL) failover on ERPS ring ports instead of a global profile.

Command Syntax

```
hardware-profile aclif failover
hardware-profile aclif no-failover
```

Parameters

None

Default

None

Command Mode

Configure mode.

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

Below are examples of configuring hardware profiles for ACL interface (aclif) with and without failover in OcNOS device.

```
OcNOS#configure terminal
OcNOS(config)#hardware-profile aclif failover

OcNOS(config)#hardware-profile aclif no-failover
```

aclif failover

Use this command to enable failover for the logical interface (LIF) resources, enhancing the LIFs hardware profile for ERPS.

Use the `no` parameter of this command to disable failover for the LIF resources, providing control over individual LIFs.

Command Syntax

```
aclif failover
aclif no-failover
```

Parameters

None

Default

None

Command Mode

Interface mode.

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

Below are sample examples of configuring ACL interface (aclif) with and without failover on interface `xe2` in OcNOS device.

```
OcNOS#configure terminal
OcNOS(config)#interface xe2
OcNOS(config)#aclif failover

OcNOS(config)#aclif no-failover
```

Revised CLI Commands

Below is the revised command for configuring ERPS with Bridge-Domain. For more details, refer *G.8032 ERPS Version 2 Commands* chapter in the *Carrier Ethernet Guide, Release 6.4.1*.

clear g8032 erp-instance

- The command *clear g8032 erp-instance* is used to clear ERPS instance.
- The existing syntax now includes the newly added parameter for clearing all ERPS instance, namely `all`.

erp-instance

- The command *erps-instance* is used to set the ERPS-instance for the sub-interface.
- The syntax has been revised to remove the `none` parameter.

g8032 erp-instance force-switch

- The command *g8032 erp-instance force-switch* is used to configure administrative commands related to force switching within ERPS instances.
- The existing syntax now includes the newly added parameter to apply the command to all ERPS instances configured on the device, namely `all`.

g8032 erp-instance manual-switch

- The command *g8032 erp-instance manual-switch* is used to configure administrative commands related to force switching within ERPS instances.
- The existing syntax now includes the newly added parameter to apply the command to all ERPS instances configured on the device, namely `all`.

show g8032 erp-instance

- The command *show g8032 erp-instance* is used to display details about an ERP instance.
- The existing syntax now includes the newly added parameters to display data traffic details for ERP instances and details for a specific ERP instance, namely `data-traffic` and `summary`.

Troubleshooting

ERPSConflictwithVXLAN

In some scenarios, ERPS may encounter conflicts with VXLAN configurations, leading to issues with traffic forwarding. These conflicts primarily arise due to resource conflicts in the hardware for wide LIF data. This section provides insights into identifying and resolving such conflicts.

IssueDescription

When VXLAN is used in conjunction with ERPS, traffic forwarding for xConnects configured in specific scenarios, such as Qumran2 series platform, may fail.

ConflictDetails

ERPS optimizations, particularly those related to hardware failover IDs (`hw-failover-id`), can conflict with VXLAN bridge configurations and VXLAN xConnects, causing VXLAN-related functionalities to stop working as expected. The conflict arises due to resource contention in the hardware, particularly when dealing with wide LIFs data.

Proposed Solution

To address these conflicts and provide granular control over resource usage, a new CLI commands *hardware-profile aclif failover* and *aclif failover* has been introduced. This command allows users to enable or disable the `hardware-aclif-failover` feature for failover on LIFs.

ImpactonERPS

- For bridge and PB configurations, default `aclif-failover` features are available, and there is no impact on ERPS.
- For bridge-domain configurations, conflicts may arise with VXLAN on sub-interface LIFs. To resolve this, the CLI commands *hardware-profile aclif failover and aclif failover* must be configured on ring ports. It's important to note that enabling or configuring `aclif-failover` on ring ports for bridge-domain configurations does not result in any functional changes compared to the previous CLI settings.

Abbreviations

The following are some key abbreviations and their meanings relevant to this document:

Acronym	Description
ERPS	Ethernet Ring Protection Switching
CFM	Continuity Fault Management
ELAN	Ethernet LAN
LIF	Logical Interface
ACLIF	Access Control List Interface

Glossary

The following provides definitions for key terms used throughout this document.

Bridge Domain	A logical network segment where bridging services are extended and managed. It defines a broadcast domain in Ethernet bridging.
Bridge Ports	Physical or virtual ports/interfaces that connect devices within a bridge domain.
Network Resilience	The ability of a network to maintain service availability and performance in the face of failures or abnormal conditions.
Redundant Links	Backup or alternative network connections designed to ensure network reliability.
Distribution Switches	Network switches that aggregate traffic from access switches and connect them to core switches or routers.
Ring Topology	A network topology in which each network device is connected to exactly two other devices, forming a circular path.
Failover	The process of automatically switching to a backup or redundant system or path in case of a failure.
Downtime	The period during which a system, network, or service is unavailable or not functioning correctly.
VLAN	Virtual Local Area Network, a logical segmentation of a network to isolate traffic and improve network efficiency.
Backup Path	An alternative network path that can be used to reroute traffic in case of a failure in the primary path.
Granular Control	Fine-tuned control over specific aspects or resources within a system or network.
Resource Contention	Competition or conflict for limited resources, such as hardware resources in a network device.
Sub-Interface	A logical interface created within a physical interface to allow multiple virtual interfaces with different configurations.
Logical Interface	A virtual or logical network interface on a device.

RSVP Detour Over Ring Topology

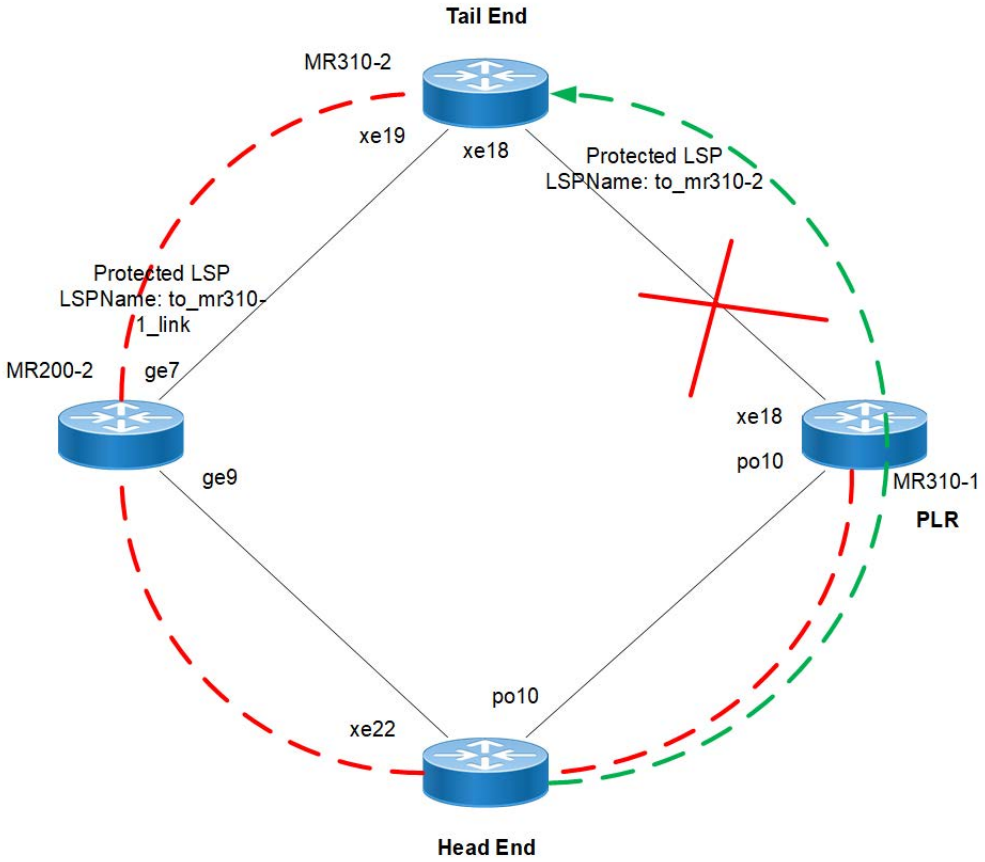
Overview

In OcNOS, this feature allows the detour formation in the ring topology to enhance the routing experience. The detour formation is a local protection mechanism to reroute the data traffic when a failure or congestion occurs in the primary Label Switched Path (LSP). In Multiprotocol Label Switching (MPLS), the primary LSP is the default path through which the data travels from the source to the destination node.

Feature Characteristics

This feature allows detour to take the upstream path of protected LSP, allowing a detour based protection in a ring topology. The upstream path of the protected LSP is the section of the network that precedes the PLR node in the network. This feature works for both path and sender-template method of detour formation. For the inter-op solutions that do not support the sender-template method, use the path method of detour formation.

In the below diagram, the data traffic path highlighted in green dots is the primary LSP. The link shown with the red cross is locally protected at the Point of Local Repair (PLR) node. A PLR node is a network device that reacts and takes action when a link fails. For continued data traffic flow, detour occurs through the red dotted line. Detour in MPLS is an alternate path used when the primary LSP encounters disruption or congestion.



RSVP-TE FRR failover ring topology Feature Characteristics

Benefits

This feature helps detour the data traffic when there is a link or node failure, keeping the data traffic loss to a minimum (less than 50ms when BFD negotiated for fastest detection).

Prerequisite

Before the detour configuration in a ring topology, configure the RSVP tunnel with fast reroute protection of the one-to-one method.

For more information, refer to the F*ast Reroute Configuration (one-to-one method)* section of the *RSVP-TE Configuration* chapter in the *OcNOS Multi-Protocol Label Switching Guide,* Release 6.4.1.

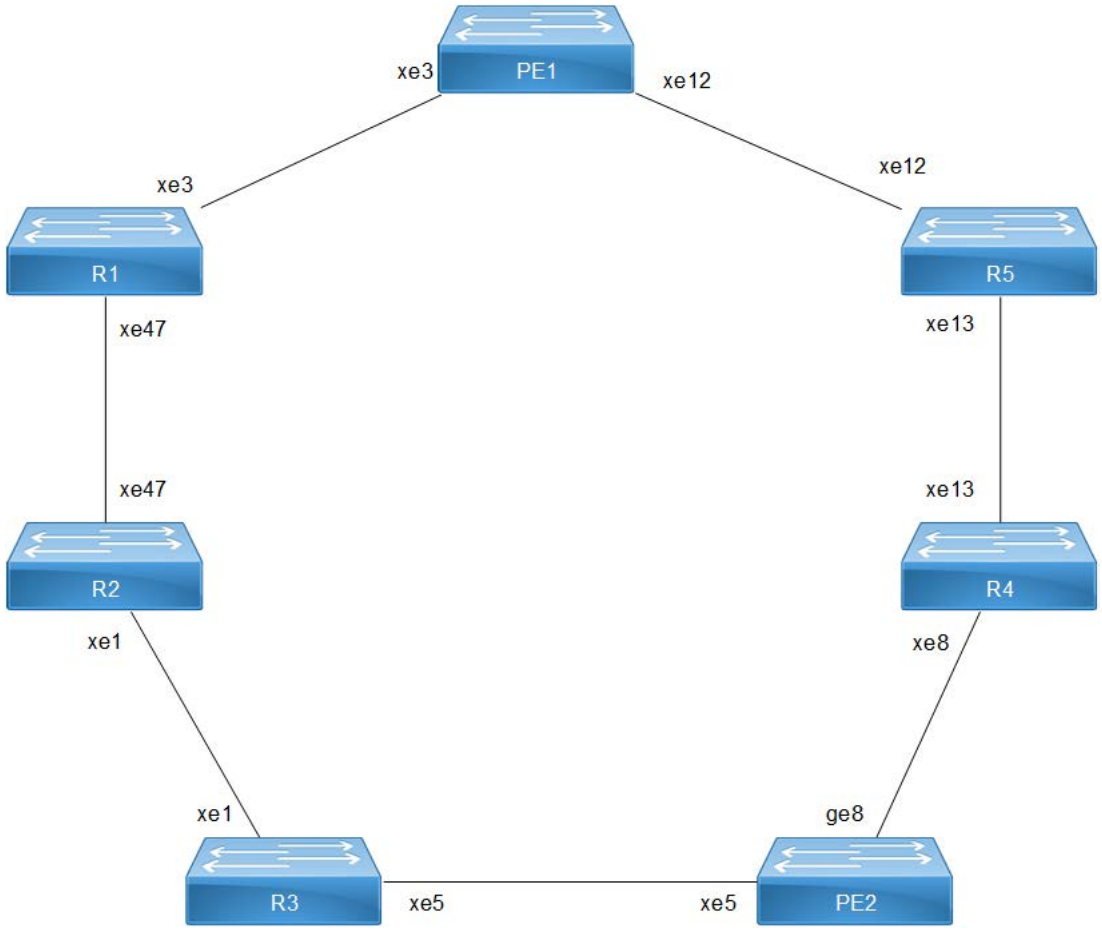
Configuration

This section shows the configuration procedure to create a detour in the ring topology.

Topology

Configure the primary LSP in the below ring topology from the head end to the tail end.

For example, consider PE1 as the head end and PE2 as the tail end, and the primary LSP is via R1, R2, and R3. In this case, first configure the *Fast Reroute Configuration (one-to-one method)* on the PE1 and PE2 and then configure the *detour-allow-primary-upstream-path* command in all the nodes. For example, if the link between R3 and PE2 is down, the detour follows via primary LSP to reach PE2.



RSVP-TE FRR failover ring topology - 1:1 Detour

PE1 - OSPF Configurations

This section shows how to configure the Open Shortest Path First (OSPF) as Interior Gateway Protocol (IGP).

`PE1#configure terminal`	Enter configure mode.
`PE1(config)#interface xe3`	Enter interface mode `xe3`.
`PE1(config-if)#ip address 61.61.61.3/24`	Configure IPv4 address `61.61.61.3.24`.
`PE1(config-if)#label-switching`	Configure label switching on `xe3`.
`PE1(config-if)#enable-rsvp`	Enable RSVP on `xe3`.
`PE1(config-if)#exit`	Exit interface mode.
`PE1(config)#interface xe12`	Enter interface mode `xe12`.
`PE1(config-if)#ip address 58.58.58.2/24`	Configure IPv4 address `58.58.58.2/24`.
`PE1(config-if)#label-switching`	Configure label switching on `xe12`.
`PE1(config-if)#enable-rsvp`	Enable RSVP on `xe12`.
`PE1(config-if)#exit`	Exit interface mode.
`PE1(config)#interface lo`	Enter loopback interface mode.

`PE1(config-if)#ip address 26.26.26.26/32 secondary`	Configure IPv4 address `26.26.26.26/32`.
`PE1(config-if)#exit`	Exit interface mode.
`PE1(config)#router ospf 100`	Enter OSPF router mode.
`PE1(config-router)#ospf router-id 26.26.26.26`	Assign router ID `26.26.26.26` for OSPF.
`PE1(config-router)#network 26.26.26.26/32 area 0.0.0.0`	Define network `26.26.26.26/32` under router OSPF.
`PE1(config-router)#network 58.58.58.0/24 area 0.0.0.0`	Define network `58.58.58.0/24` under router OSPF.
`PE1(config-router)#network 61.61.61.0/24 area 0.0.0.0`	Define network `61.61.61.0/24` under router OSPF.
`PE1(config-router)#exit`	Exit router OSPF mode.
`PE1(config)#commit`	Commit the transaction.
`PE1(config)#exit`	Exit the configure mode.

PE1 - RSVP Configurations

This section shows:

1. The configuration of detour to take the upstream path of protected LSP.
2. The configuration of the primary LSP and attaching it to the RSVP trunk.
3. The configuration of the FRR.

`PE1#configure terminal`	Enter configure mode.
`PE1(config)#router rsvp`	Enable RSVP globally.
`PE1(config-router)#detour-allow-primary-upstream-path`	Configure this CLI to allow detour to take primary upstream path.
`PE1(config-router)#exit`	Exit router RSVP mode.
`PE1(config)#rsvp-path PE1-PE2-01 mpls`	Configure RSVP path PE1-PE2-01 and enter path mode.
`PE1(config-path)#61.61.61.2 strict`	Configure this explicit route path as a strict hop.
`PE1(config-path)#23.23.23.3 strict`	Configure this explicit route path as a strict hop.
`PE1(config-path)#41.41.41.3 strict`	Configure this explicit route path as a strict hop.
`PE1(config-path)#56.56.56.3 strict`	Configure this explicit route path as a strict hop.
`PE1(config-path)#rsvp-trunk TR-PE1-PE2-MP-01 ipv4`	Create an RSVP trunk TR-PE1-PE2-MP-01 and enter the trunk mode.
`PE1(config-trunk)#primary fast-reroute protection one-to-one`	Configure primary fast reroute protection.
`PE1(config-trunk)#primary fast-reroute node-protection`	Configure node protection.
`PE1(config-trunk)#primary path PE1-PE2-01`	Configure trunk PE1-PE2-01 to use as the primary LSP.
`PE1(config-trunk)#from 26.26.26.26`	Assign the source loopback address `26.26.26.26` to the RSVP trunk.
`PE1(config-trunk)#to 22.22.22.22`	Assign the destination loopback address `22.22.22.22` to the RSVP trunk.
`PE1(config-trunk)#exit`	Exit router RSVP trunk mode.

`PE1(config)#commit`	Commit the transaction.
`PE1(config)#exit`	Exit the configure mode.

R1 - OSPF Configurations

This section shows how to configure the Open Shortest Path First (OSPF) as Interior Gateway Protocol (IGP).

`R1#configure terminal`	Enter configure mode.
`R1(config)#interface xe3`	Enter interface mode `xe3`.
`R1(config-if)#ip address 61.61.61.2/24`	Configure IPv4 address `61.61.61.2/24`.
`R1(config-if)#label-switching`	Configure label switching on `xe3`.
`R1(config-if)#enable-rsvp`	Enable RSVP on interface `xe3`.
`R1(config-if)#exit`	Exit interface mode.
`R1(config)#interface xe47`	Enter interface mode `xe47`.
`R1(config-if)#ip address 23.23.23.2/24`	Configure IPv4 address `23.23.23.2/24`.
`R1(config-if)#label-switching`	Configure label switching on `xe47`.
`R1(config-if)#enable-rsvp`	Enable RSVP on interface `xe47`.
`R1(config-if)#exit`	Exit interface mode.
`R1(config)#interface lo`	Enter loopback interface mode.
`R1(config-if)#ip address 24.24.24.24/32 secondary`	Configure IPv4 address `24.24.24.24/32`.
`R1(config-if)#exit`	Exit interface mode.
`R1(config)#router ospf 100`	Enter OSPF router mode.
`R1(config-router)#ospf router-id 24.24.24.24`	Assign router-id for OSPF.
`R1(config-router)#network 23.23.23.0/24 area 0.0.0.0`	Define network `23.23.23.0/24` under router OSPF.
`R1(config-router)#network 24.24.24.24/32 area 0.0.0.0`	Define network `24.24.24.24/32` under router OSPF.
`R1(config-router)#network 61.61.61.0/24 area 0.0.0.0`	Define network `61.61.61.0/24` under router OSPF.
`R1(config-router)#exit`	Exit router OSPF mode.
`R1(config)#commit`	Commit the transaction.
`R1(config)#exit`	Exit the configure mode.

R1 - RSVP Configurations

This section shows how to configure the detour to take the upstream path of protected LSP.

`R1#configure terminal`	Enter configure mode.
`R1(config)#router rsvp`	Enable RSVP globally.
`R1(config-router)#detour-allow-primary-upstream-path`	Configure this CLI to allow detour to take primary upstream path.
`R1(config-router)#exit`	Exit router RSVP mode.
`R1(config)#commit`	Commit the transaction.
`R1(config)#exit`	Exit the configure mode.

R2 - OSPF Configurations

This section shows how to configure the Open Shortest Path First (OSPF) as Interior Gateway Protocol (IGP).

`R2#configure terminal`	Enter configure mode.
`R2(config)#interface xe1`	Enter interface mode `xe1`.
`R2(config-if)#ip address 41.41.41.2/24`	Configure IPv4 address `41.41.41.2/24`.
`R2(config-if)#label-switching`	Configure label switching on `xe1`.
`R2(config-if)#enable-rsvp`	Enable RSVP on `xe1`.
`R2(config-if)#exit`	Exit interface mode.
`R2(config)#interface xe47`	Enter interface mode `xe47`.
`R2(config-if)#ip address 23.23.23.3/24`	Configure IPv4 address `23.23.23.3/24`.
`R2(config-if)#label-switching`	Configure label switching on `xe47`.
`R2(config-if)#enable-rsvp`	Enable RSVP on `xe47`.
`R2(config-if)#exit`	Exit interface mode.
`R2(config)#interface lo`	Enter loopback interface mode.
`R2(config-if)#ip address 88.88.88.88/32 secondary`	Configure IPv4 address `88.88.88.88/32`.
`R2(config-if)#exit`	Exit interface mode.
`R2(config)#router ospf 100`	Enter OSPF router mode.
`R2(config-router)#ospf router-id 88.88.88.88`	Assign router-id `88.88.88.88` for OSPF.
`R2(config-router)#network 23.23.23.0/24 area 0.0.0.0`	Define network `23.23.23.0/24` under router OSPF.
`R2(config-router)#network 41.41.41.0/24 area 0.0.0.0`	Define network `41.41.41.0/24` under router OSPF.
`R2(config-router)#network 88.88.88.88/32 area 0.0.0.0`	Define network `88.88.88.88/32` under router OSPF.
`R2(config-router)#exit`	Exit router OSPF mode.
`R2(config)#commit`	Commit the transaction.
`R2(config)#exit`	Exit the configure mode.

R2 - RSVP Configurations

This section shows how to configure the detour to take the upstream path of protected LSP.

`R2#configure terminal`	Enter configure mode.
`R2(config)#router rsvp`	Enable RSVP globally.
`R2(config-router)#detour-allow-primary-upstream-path`	Configure this CLI to allow detour to take primary upstream path.
`R2(config-router)#exit`	Exit router RSVP mode.
`R2(config)#commit`	Commit the transaction.
`R2(config)#exit`	Exit the configure mode.

R3 - OSPF Configurations

This section shows how to configure the Open Shortest Path First (OSPF) as Interior Gateway Protocol (IGP).

`R3#configure terminal`	Enter configure mode.
`R3(config)#interface xe1`	Enter interface mode `xe1`.
`R3(config-if)#ip address 41.41.41.3/24`	Configure IPv4 address `41.41.41.3/24`.
`R3(config-if)#label-switching`	Configure label switching on `xe1`.
`R3(config-if)#enable-rsvp`	Enable RSVP on `xe1`.
`R3(config-if)#exit`	Exit interface mode.
`R3(config)#interface xe5`	Enter interface mode `xe5`.
`R3(config-if)#ip address 56.56.56.2/24`	Configure IPv4 address `56.56.56.2/24`.
`R3(config-if)#label-switching`	Configure label switching on `xe5`.
`R3(config-if)#enable-rsvp`	Enable RSVP on `xe5`.
`R3(config-if)#exit`	Exit interface mode.
`R3(config)#interface lo`	Enter loopback interface mode.
`R3(config-if)#ip address 99.99.99.99/32 secondary`	Configure IPv4 address `99.99.99.99/32`.
`R3(config-if)#exit`	Exit interface mode.
`R3(config)#router ospf 100`	Enter OSPF router mode.
`R3(config-router)#ospf router-id 99.99.99.99`	Assign router-id for OSPF.
`R3(config-router)#network 41.41.41.0/24 area 0.0.0.0`	Define network `41.41.41.0/24` under router OSPF.
`R3(config-router)#network 56.56.56.0/24 area 0.0.0.0`	Define network `56.56.56.0/24` under router OSPF.
`R3(config-router)#network 99.99.99.99/32 area 0.0.0.0`	Define network `99.99.99.99/32` under router OSPF.
`R3(config-router)#exit`	Exit router OSPF mode.
`R3(config)#commit`	Commit the transaction.
`R3(config)#exit`	Exit the configure mode.

R3 - RSVP Configurations

This section shows how to configure the detour to take the upstream path of protected LSP.

`R3#configure terminal`	Enter configure mode.
`R3(config)#router rsvp`	Enable RSVP globally.
`R3(config-router)#detour-allow-primary-upstream-path`	Configure this CLI to allow detour to take primary upstream path.
`R3(config-router)#exit`	Exit router RSVP mode.
`R3(config)#commit`	Commit the transaction.
`R3(config)#exit`	Exit the configure mode.

R5 - OSPF Configurations

This section shows how to configure the Open Shortest Path First (OSPF) as Interior Gateway Protocol (IGP).

`R5#configure terminal`	Enter configure mode.
`R5(config)#interface xe1`	Enter interface mode `58.58.58.3/24`.
`R5(config-if)#ip address 58.58.58.3/24`	Configure IPv4 address.
`R5(config-if)#label-switching`	Configure label switching on `xe1`.
`R5(config-if)#enable-rsvp`	Enable RSVP on `xe1`.
`R5(config-if)#exit`	Exit interface mode.
`R5(config)#interface xe13`	Enter interface mode `xe13`.
`R5(config-if)#ip address 54.54.54.4/24`	Configure IPv4 address `54.54.54.4/24`.
`R5(config-if)#label-switching`	Configure label switching on `xe13`.
`R5(config-if)#enable-rsvp`	Enable RSVP on `xe13`.
`R5(config-if)#exit`	Exit interface mode.
`R5(config)#interface lo`	Enter loopback interface mode.
`R5(config-if)#ip address 17.17.17.17/32 secondary`	Configure IPv4 address `17.17.17.17/32`.
`R5(config-if)#exit`	Exit interface mode.
`R5(config)#router ospf 100`	Enter OSPF router mode.
`R5(config-router)#ospf router-id 17.17.17.17`	Assign router-id for OSPF.
`R5(config-router)#network 17.17.17.17/32 area 0.0.0.0`	Define network `17.17.17.17/32` under router OSPF.
`R5(config-router)#network 54.54.54.0/24 area 0.0.0.0`	Define network `54.54.54.0/24` under router OSPF.
`R5(config-router)#network 58.58.58.0/24 area 0.0.0.0`	Define network `58.58.58.0/24` under router OSPF.
`R5(config-router)#exit`	Exit router OSPF mode.
`R5(config)#commit`	Commit the transaction.
`R5(config)#exit`	Exit the configure mode.

R5 - RSVP Configurations

This section shows how to configure the detour to take the upstream path of protected LSP.

`R5#configure terminal`	Enter configure mode.
`R5(config)#router rsvp`	Enable RSVP globally.
`R5(config-router)#detour-allow-primary-upstream-path`	Configure this CLI to allow detour to take primary upstream path
`R5(config-router)#exit`	Exit router RSVP mode
`R5(config)#commit`	Commit the transaction.
`R5(config)#exit`	Exit the configure mode.

R4 - OSPF Configurations

This section shows how to configure the Open Shortest Path First (OSPF) as Interior Gateway Protocol (IGP).

`R4#configure terminal`	Enter configure mode.
`R4(config)#interface xe13`	Enter interface mode `xe13`.
`R4(config-if)#ip address 54.54.54.3/24`	Configure IPv4 address `54.54.54.3/24`.
`R4(config-if)#label-switching`	Configure label switching on `xe13`.
`R4(config-if)#enable-rsvp`	Enable RSVP on interface `xe13`.
`R4(config-if)#exit`	Exit interface mode.
`R4(config)#interface xe8`	Enter interface mode `xe8`.
`R4(config-if)#ip address 62.62.62.3/24`	Configure IPv4 address `62.62.62.3/24`.
`R4(config-if)#label-switching`	Configure label switching on `xe8`.
`R4(config-if)#enable-rsvp`	Enable RSVP on `xe8`.
`R4(config-if)#exit`	Exit interface mode.
`R4(config)#interface lo`	Enter loopback interface mode.
`R4(config-if)#ip address 48.48.48.48/32 secondary`	Configure IPv4 address `48.48.48.48/32`.
`R4(config-if)#exit`	Exit interface mode.
`R4(config)#router ospf 100`	Enter OSPF router mode.
`R4(config-router)#ospf router-id 48.48.48.48`	Assign router-id for OSPF.
`R4(config-router)#network 48.48.48.48/32 area 0.0.0.0`	Define network `48.48.48.48/32` under router OSPF.
`R4(config-router)#network 54.54.54.0/24 area 0.0.0.0`	Define network `54.54.54.0/24` under router OSPF.
`R4(config-router)#network 62.62.62.0/24 area 0.0.0.0`	Define network 62.62.62.0/24 under router OSPF.
`R4(config-router)#exit`	Exit router OSPF mode.
`R4(config)#commit`	Commit the transaction.
`R4(config)#exit`	Exit the configure mode.

R4 - RSVP Configurations

This section shows how to configure the detour to take the upstream path of protected LSP.

`R4#configure terminal`	Enter configure mode.
`R4(config)#router rsvp`	Enable RSVP globally.
`R4(config-router)#detour-allow-primary-upstream-path`	Configure this CLI to allow detour to take primary upstream path.
`R4(config-router)#exit`	Exit router RSVP mode.
`R4(config)#commit`	Commit the transaction.
`R4(config)#exit`	Exit the configure mode.

PE2 - OSPF Configurations

This section shows how to configure the Open Shortest Path First (OSPF) as Interior Gateway Protocol (IGP).

`PE2#configure terminal`	Enter configure mode.
`PE2(config)#interface xe5`	Enter interface mode `xe5`.
`PE2(config-if)#ip address 56.56.56.3/24`	Configure IPv4 address `56.56.56.3/24`.
`PE2(config-if)#label-switching`	Configure label switching on `xe5`.
`PE2(config-if)#enable-rsvp`	Enable RSVP on `xe5`.
`PE2(config-if)#exit`	Exit interface mode.
`PE2(config)#interface ge8`	Enter interface mode `ge8`.
`PE2(config-if)#ip address 62.62.62.2/24`	Configure IPv4 address `62.62.62.2/24`.
`PE2(config-if)#label-switching`	Configure label switching on `ge8`.
`PE2(config-if)#enable-rsvp`	Enable RSVP on `ge8`.
`PE2(config-if)#exit`	Exit interface mode.
`PE2(config)#interface lo`	Enter loopback interface mode.
`PE2(config-if)#ip address 22.22.22.22/32 secondary`	Configure IPv4 address `22.22.22.22/32`.
`PE2(config-if)#exit`	Exit interface mode.
`PE2(config)#router ospf 100`	Enter OSPF router mode.
`PE2(config-router)#ospf router-id 22.22.22.22`	Assign router-id for OSPF.
`PE2(config-router)#network 22.22.22.22/32 area 0.0.0.0`	Define network `22.22.22.22/32` under router OSPF.
`PE2(config-router)#network 56.56.56.0/24 area 0.0.0.0`	Define network `56.56.56.0/24` under router OSPF.
`PE2(config-router)#network 62.62.62.0/24 area 0.0.0.0`	Define network `62.62.62.0/24` under router OSPF.
`PE2(config-router)#exit`	Exit router OSPF mode.
`PE2(config)#commit`	Commit the transaction.
`PE2(config)#exit`	Exit the configure mode.

PE2 - RSVP Configurations

This section shows:

1. The configuration of detour to take the upstream path of protected LSP.
2. The configuration of the primary LSP and attaching it to the RSVP trunk.
3. The configuration of the FRR.

`PE2#configure terminal`	Enter configure mode.
`PE2(config)#router rsvp`	Enable RSVP globally.
`PE2(config-router)#detour-allow-primary-upstream-path`	Configure this CLI to allow detour to take primary upstream path.
`PE2(config-router)#exit`	Exit router RSVP mode.
`PE2(config)#rsvp-path PE2-PE1-01 mpls`	Configure RSVP path PE2-PE1-01 and enter path mode.
`PE2(config-path)#56.56.56.2 strict`	Configure this explicit route path as a strict hop.
`PE2(config-path)#41.41.41.2 strict`	Configure this explicit route path as a strict hop.

PE2(config-path)#23.23.23.2 strict	Configure this explicit route path as a strict hop.
PE2(config-path)#61.61.61.3 strict	Configure this explicit route path as a strict hop.
PE2(config-router)#exit	Exit path mode.
PE2(config-path)#rsvp-trunk TR-PE2-PE1-MP-01 ipv4	Create an RSVP trunk TR-PE2-PE1-MP-01 and enter the Trunk mode.
PE2(config-trunk)#primary fast-reroute protection one-to-one	Configure primary fast-reroute protection.
PE2(config-trunk)#primary fast-reroute node-protection	Configure node protection.
PE2(config-trunk)#primary path PE2-PE1-01	Configure trunk PE2-PE1-01 to use as the primary LSP.
PE2(config-trunk)#from 22.22.22.22	Assign the source loopback address 22.22.22.22 to the RSVP trunk.
PE2(config-trunk)#to 26.26.26.26	Assign the destination loopback address 26.26.26.26 to the RSVP trunk.
PE2(config-trunk)#exit	Exit router RSVP trunk mode.
PE2(config)#commit	Commit the transaction.
PE2(config)#exit	Exit the configure mode.

Validation

PE1

Below is the validation output of RSVP LSPs from PE1 to PE2 via R1>R2>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            Tun-ID   LSP-ID   Type   LSPName                          State Uptime    Rt  Style  Labelin
Labelout
22.22.22.22     26.26.26.26     5001     2205     PRI    TR-PE1-PE2-MP-01-Primary         UP    02:12:32  1 1 SE     -
52480
22.22.22.22     58.58.58.2      5001     2205     DTR    TR-PE1-PE2-MP-01-Detour          UP    00:34:04  1 2 SE     -
25600
Total 2 displayed, Up 2, Down 0.

Transit RSVP:
To              From            Tun-ID   LSP-ID   Type   LSPName                          State Uptime    Rt  Style  Labelin
Labelout
22.22.22.22     61.61.61.2      5001     2205     PRI    TR-PE1-PE2-MP-01-Detour          UP    00:33:19  1 2 SE     25602
25600
Total 1 displayed, Up 1, Down 0.

Egress RSVP:
To              From            Tun-ID   LSP-ID   Type   LSPName                          State Uptime    Rt  Style  Labelin
Labelout
26.26.26.26     22.22.22.22     5001     2205     PRI    TR-PE2-PE1-MP-01-Primary         UP    02:12:27  1 1 SE     25601    -
26.26.26.26     62.62.62.2      5001     2205     PRI    TR-PE2-PE1-MP-01-Detour          UP    02:09:08  1 1 SE     25600    -
Total 2 displayed, Up 2, Down 0.
```

Below is the validation output of RSVP ping and trace from PE1 to PE2:

```
#ping mpls rsvp egress 22.22.22.22 detail
Sending 5 MPLS Echos to 22.22.22.22, 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 56.56.56.3 0.91 ms
! seq_num = 2 56.56.56.3 0.54 ms
! seq_num = 3 56.56.56.3 0.48 ms
! seq_num = 4 56.56.56.3 0.47 ms
! seq_num = 5 56.56.56.3 0.50 ms

Success Rate is 100.00 percent (5/5)
round-trip min/avg/max = 0.47/0.69/0.91
PE1#
#trace mpls rsvp egress 22.22.22.22 detail
Tracing MPLS Label Switched Path to 22.22.22.22, 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 61.61.61.3 [Labels:  52480]
R 1 61.61.61.2 [Labels:  25600] 0.71 ms
R 2 23.23.23.3 [Labels:  25600] 0.83 ms
R 3 41.41.41.3 [Labels:  25600] 0.88 ms
! 4 56.56.56.3 0.69 ms
```

Below are the outputs from transit nodes R1, R2 and R3 for primary LSP configured:

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            Tun-ID   LSP-ID   Type   LSPName                         State Uptime    Rt  Style  Labelin
Labelout
22.22.22.22     61.61.61.2      5001     2205     DTR    TR-PE1-PE2-MP-01-Detour         UP    00:38:43  1 2 SE     -
25602
26.26.26.26     23.23.23.2      5001     2205     DTR    TR-PE2-PE1-MP-01-Detour         UP    00:38:44  1 1 SE     -
25603
Total 2 displayed, Up 2, Down 0.

Transit RSVP:
To              From            Tun-ID   LSP-ID   Type   LSPName                         State Uptime    Rt  Style  Labelin
Labelout
22.22.22.22     26.26.26.26     5001     2205     PRI    TR-PE1-PE2-MP-01-Primary        UP    02:17:55  1 1 SE     52480
25600
22.22.22.22     23.23.23.3      5001     2205     PRI    TR-PE1-PE2-MP-01-Detour         UP    00:37:58  1 2 SE     52482
25602
26.26.26.26     22.22.22.22     5001     2205     PRI    TR-PE2-PE1-MP-01-Primary        UP    02:17:50  1 1 SE     52481
25601
Total 3 displayed, Up 3, Down 0.
```

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

Ingress RSVP:
```

```
To              From            Tun-ID   LSP-ID   Type   LSPName                         State Uptime    Rt  Style  Labelin
Labelout
22.22.22.22     23.23.23.3      5001     2205     DTR    TR-PE1-PE2-MP-01-Detour         UP    00:38:07  1 2 SE     -
52482
26.26.26.26     41.41.41.2      5001     2205     DTR    TR-PE2-PE1-MP-01-Detour         UP    00:39:00  1 2 SE     -
25602
Total 2 displayed, Up 2, Down 0.

Transit RSVP:
To              From            Tun-ID   LSP-ID   Type   LSPName                         State Uptime    Rt  Style  Labelin
Labelout
22.22.22.22     26.26.26.26     5001     2205     PRI    TR-PE1-PE2-MP-01-Primary        UP    02:18:05  1 1 SE     25600
25600
22.22.22.22     41.41.41.3      5001     2205     PRI    TR-PE1-PE2-MP-01-Detour         UP    00:37:28  1 2 SE     25602
52482
26.26.26.26     22.22.22.22     5001     2205     PRI    TR-PE2-PE1-MP-01-Primary        UP    02:18:00  1 1 SE     25601
52481
26.26.26.26     23.23.23.2      5001     2205     PRI    TR-PE2-PE1-MP-01-Detour         UP    00:38:53  1 2 SE     25603
25602
Total 4 displayed, Up 4, Down 0.
```

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            Tun-ID   LSP-ID   Type   LSPName                         State Uptime    Rt  Style  Labelin
Labelout
22.22.22.22     41.41.41.3      5001     2205     DTR    TR-PE1-PE2-MP-01-Detour         UP    00:37:31  1 1 SE     -
25602
26.26.26.26     56.56.56.2      5001     2205     DTR    TR-PE2-PE1-MP-01-Detour         UP    00:39:23  1 2 SE     -
25602
Total 2 displayed, Up 2, Down 0.

Transit RSVP:
To              From            Tun-ID   LSP-ID   Type   LSPName                         State Uptime    Rt  Style  Labelin
Labelout
22.22.22.22     26.26.26.26     5001     2205     PRI    TR-PE1-PE2-MP-01-Primary        UP    02:18:08  1 1 SE     25600
25600
26.26.26.26     22.22.22.22     5001     2205     PRI    TR-PE2-PE1-MP-01-Primary        UP    02:18:02  1 1 SE     25601
25601
26.26.26.26     41.41.41.2      5001     2205     PRI    TR-PE2-PE1-MP-01-Detour         UP    00:39:03  1 2 SE     25602
25602
Total 3 displayed, Up 3, Down 0.
```

Below are the outputs from transit nodes R4 and R5 for Detour LSPs formation:

From 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            Tun-ID   LSP-ID   Type   LSPName                         State Uptime    Rt  Style  Labelin
Labelout
22.22.22.22     58.58.58.2      5001     2205     PRI    TR-PE1-PE2-MP-01-Detour         UP    02:14:52  1 1 SE     25600
25601
26.26.26.26     62.62.62.2      5001     2205     PRI    TR-PE2-PE1-MP-01-Detour         UP    00:39:49  1 1 SE     25601
25601
Total 2 displayed, Up 2, Down 0.
```

From 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

Transit RSVP:
```

```
To              From            Tun-ID   LSP-ID   Type   LSPName                          State Uptime    Rt  Style  Labelin
Labelout
22.22.22.22     58.58.58.2      5001     2205     PRI    TR-PE1-PE2-MP-01-Detour          UP    00:39:45  1 1 SE     25600
25600
26.26.26.26     62.62.62.2      5001     2205     PRI    TR-PE2-PE1-MP-01-Detour          UP    02:14:48  1 1 SE     25601
25600
Total 2 displayed, Up 2, Down 0.
```

Now, shutting down one of the interfaces on Primary LSP path and check RSVP tunnel outputs on PE1 and PE2

Shutdown interface xe47 connected between R1 and R2:

`#configure terminal`	Enter Configure mode.
`(config)#interface xe47`	Enter interface mode.
`(config-router)#shutdown`	Administratively bring the interface down.
`(config-router)#exit`	Exit router RSVP mode

Below is the validation output of RSVP LSPs from PE1 to PE2 after admin shutting one of the interfaces on primary LSP path:

```
#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            Tun-ID   LSP-ID   Type   LSPName                          State Uptime    Rt  Style  Labelin
Labelout
22.22.22.22     26.26.26.26     5001     2205     PRI    TR-PE1-PE2-MP-01-Primary         UP*   02:32:40  1 1 SE     -
52480
22.22.22.22     26.26.26.26     5001     2201     PRI    TR-PE1-PE2-MP-01-Primary         DN    N/A       0 0 SE     -        -
22.22.22.22     58.58.58.2      5001     2205     DTR    TR-PE1-PE2-MP-01-Detour          UP    00:54:12  1 2 SE     -
25600
Total 3 displayed, Up 2, Down 1.

Transit RSVP:
To              From            Tun-ID   LSP-ID   Type   LSPName                          State Uptime    Rt  Style  Labelin
Labelout
22.22.22.22     61.61.61.2      5001     2205     PRI    TR-PE1-PE2-MP-01-Detour          UP    00:53:27  1 2 SE     25602
25600
Total 1 displayed, Up 1, Down 0.
```

Below is the validation output of RSVP ping and trace from PE1 to PE2 after shutting one of the interfaces on primary LSP path:

```
Egress RSVP:
To              From            Tun-ID   LSP-ID   Type   LSPName                          State Uptime    Rt  Style  Labelin
Labelout
26.26.26.26     62.62.62.2      5001     2205     PRI    TR-PE2-PE1-MP-01-Detour          UP    02:29:16  1 1 SE     25600    -
Total 1 displayed, Up 1, Down 0.

#ping mpls rsvp egress 22.22.22.22 detail
Sending 5 MPLS Echos to 22.22.22.22, 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 62.62.62.2 0.69 ms
! seq_num = 2 62.62.62.2 0.54 ms
! seq_num = 3 62.62.62.2 0.56 ms
```

```
! seq_num = 4 62.62.62.2 0.49 ms
! seq_num = 5 62.62.62.2 0.51 ms

Success Rate is 100.00 percent (5/5)
round-trip min/avg/max = 0.49/0.59/0.69
#trace mpls rsvp egress 22.22.22.22 detail
Tracing MPLS Label Switched Path to 22.22.22.22, 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 61.61.61.3 [Labels:  52480]
R 1 61.61.61.2 [Labels:  25602] 0.72 ms
R 2 61.61.61.3 [Labels:  25600] 0.67 ms
R 3 58.58.58.3 [Labels:  25600] 0.80 ms
R 4 54.54.54.3 [Labels:  25601] 0.80 ms
! 5 62.62.62.2 0.50 ms
```

Below is the validation output of RSVP LSPs from PE2 to PE1 after admin shutting one of the interfaces on primary LSP path:

```
#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            Tun-ID   LSP-ID   Type   LSPName                          State Uptime    Rt  Style  Labelin
Labelout
26.26.26.26     22.22.22.22     5001     2205     PRI    TR-PE2-PE1-MP-01-Primary         UP*   02:36:19  1 1 SE     -
25601
26.26.26.26     22.22.22.22     5001     2201     PRI    TR-PE2-PE1-MP-01-Primary         DN    N/A       0 0 SE     -        -
26.26.26.26     62.62.62.2      5001     2205     DTR    TR-PE2-PE1-MP-01-Detour          UP    00:57:57  1 2 SE     -
25601
Total 3 displayed, Up 2, Down 1.

Transit RSVP:
To              From            Tun-ID   LSP-ID   Type   LSPName                          State Uptime    Rt  Style  Labelin
Labelout
26.26.26.26     56.56.56.2      5001     2205     PRI    TR-PE2-PE1-MP-01-Detour          UP    00:57:40  1 2 SE     25602
25601
Total 1 displayed, Up 1, Down 0.

Egress RSVP:
To              From            Tun-ID   LSP-ID   Type   LSPName                          State Uptime    Rt  Style  Labelin
Labelout
22.22.22.22     58.58.58.2      5001     2205     PRI    TR-PE1-PE2-MP-01-Detour          UP    02:33:00  1 1 SE     25601    -
Total 1 displayed, Up 1, Down 0.
```

Below is the validation output of RSVP ping and trace from PE2 to PE1 after shutting one of the interfaces on primary LSP path:

```
#ping mpls rsvp egress 26.26.26.26 detail
Sending 5 MPLS Echos to 26.26.26.26, 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 58.58.58.2 0.80 ms
! seq_num = 2 58.58.58.2 0.59 ms
! seq_num = 3 58.58.58.2 0.47 ms
! seq_num = 4 58.58.58.2 0.49 ms
! seq_num = 5 58.58.58.2 0.54 ms

Success Rate is 100.00 percent (5/5)
round-trip min/avg/max = 0.47/0.63/0.80
#trace mpls rsvp egress 26.26.26.26 detail
Tracing MPLS Label Switched Path to 26.26.26.26, 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 56.56.56.3 [Labels:  25601]
R 1 56.56.56.2 [Labels:  25601] 1.01 ms
R 2 41.41.41.2 [Labels:  25602] 0.95 ms
R 3 41.41.41.3 [Labels:  25602] 0.62 ms
R 4 56.56.56.3 [Labels:  25601] 0.79 ms
R 5 62.62.62.3 [Labels:  25601] 0.67 ms
R 6 54.54.54.4 [Labels:  25600] 0.57 ms
! 7 58.58.58.2 0.50 ms
```

Implementation Examples

To implement detour based protection in a ring topology, use the command *detour-allow-primary-upstream-path* that allows the detour formation to consider the upstream path of protected LSP. This is only applicable in ring topology.

New CLI Commands

detour-allow-primary-upstream-path

Use this command to ensure detour formation to consider the upstream path of protected LSPs. This is a deviation to RFC 4090 section 6.2 recommendation (https://datatracker.ietf.org/doc/html/rfc4090). This command is intended to be used in special cases where detour protection is required on ring topology if no alternate path is available.

Use the no parameter with this command to bypass the upstream path to the protected LSP when choosing a detour path.

Note: This command is intended to be used in ring topology if detour support is required at the cost of resource and link bandwidth. This command is not recommended to be configured otherwise.

Command Syntax

```
detour-allow-primary-upstream-path
no detour-allow-primary-upstream-path
```

Parameters

None

Default

By default, detour formation excludes the protected LSP upstream path as per RFC 4090 section 6.2 recommendations.

Command Mode

Router mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

```
#configure terminal
(config)#router rsvp
(config-router)#detour-allow-primary-upstream-path
(config-router)#commit
(config-router)#no detour-allow-primary-upstream-path
(config-router)#commit
```

Abbreviations

The following are some key abbreviations and their meanings relevant to this document:

Acronym	Description
FRR	Fast Reroute
LSP	Label Switched Path
OSPF	Open Shortest Path First
PLR	Point of Local Repair

Glossary

The following provides definitions for key terms used throughout this document:

Detour formation in the ring topology	The detour formation in the ring topology is a mechanism to reroute the data traffic over the backup path when a failure or congestion occurs in the primary Label Switched Path (LSP).
PLR node	A PLR node is a network device that reacts and takes action when a link fails.
Primary LSP	The primary LSP is the default path of the forwarding data packets from the source device to the destination device.
Protected LSP	A protected LSP is a primary LSP with a backup path in an MPLS network. When there is an issue or a failure in the primary LSP, the traffic is rerouted through the backup path, protecting the primary LSP.

RSVP Tunnel	RSVP tunnels are logical paths through which data traffic traverses in an IP network.
Upstream path of the protected LSP	The upstream path of the protected LSP is the section of the network that precedes the PLR node in the network.

Commit Rollback

Overview

The Commit Rollback capability in Common Management Layer Commands (CMLSH) is designed to execute a rollback operation for a set of configurations that were previously committed, with each commit operation identified by a unique commit ID. The Commit ID is numeric value and is generated by the CMLSH Commit, Confirmed Commit and Commit Rollback.

This Commit Rollback application is used for rolling back the commits that are performed after the specified commit ID whether they were executed through either Commit or Confirmed Commit operations.

Here, you find the description for Commit and Confirmed Commit:

- **Commit operation**: Involves committing the candidate configuration to the running configuration.
- **Confirmed Commit operation**: Provides more options to the commit operation with timeout parameter, user could provide timeout for the commit (default is 300 seconds).

During this timeout interval, users can either confirm the commit or cancel it, and if no confirmation or cancellation is provided before the timer expires, commit will be automatically rolled back after timeout. For an example, see the Example section of *commit-rollback* CLI.

FeatureCharacteristics

The Confirmed-Commit operation temporarily applies the configuration for the duration specified in seconds. If the user does not confirm the configuration within this timeframe, an automatic rollback will be initiated once the timer expires. For committing the configurations with timings, see *commit.*

Once the configurations are confirmed, users can use the commit rollback operation to revert the configuration, whether it is for a commit operation or a confirmed commit operation.

Benefits

With the integration of CMLSH Commit Rollback with Standard or Confirmed Commit, users can initiate a rollback operation for any specific commit, utilizing the associated commit ID to revert the configurations to their previous state. In this way, reverting to an earlier state, functional configuration is possible in case the new configuration is compromised or if the configuration makes the device unstable.

Prerequisites

Before configuring this operation, enable cml commit-history to ensure the commit records are stored in the commit history list. By default, `cml commit-history` is enabled. For enabling or disabling it, see *cml commit-history (enable | disable).*

showcommitlist

Use this command to display a record of commit operations stored in the commit history list.

Note: For commit records to be stored in the commit history list, enable *cml commit-history (enable | disable).* Otherwise, commit operations will not be stored.

Command Syntax

```
show commit list
```

Parameter

None

Command Mode

Exec mode

Applicability

This command is introduced in OcNOS 6.4.1.

Example

Example for `show commit list`:

```
#show commit list
S.No.         ID           User    Client         TimeStamp              Commit Status                      Description
~~~~~  ~~~~~~~~~~~~~~~~   ~~~~~   ~~~~~~   ~~~~~~~~~~~~~~~~~~     ~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~~~~
  1    1684542224876712    ocnos    cmlsh    20-05-2023 00:23:44             Confirmed                          NA
```

commit-rollback

Use this command to revert configurations to a previously committed stable state. This action will remove configurations made after the provided commit ID (Word).

Note: To use commit-rollback, cml commit-history must be enabled.

Command Syntax

```
commit-rollback to WORD (description LINE|)
```

Parameter

`Word`	Commit ID associated with recorded commit operations stored within the commit-history list.
`description LINE`	[Optional] Short description about commit-rollback, maximum 65 characters.

Command Mode

Exec mode

Applicability

This command is introduced in OcNOS 6.4.1.

Example

Example output for `commit-rollback WORD`:

```
#show commit list

S.No.         ID           User    Client         TimeStamp              Commit Status                      Description
~~~~~  ~~~~~~~~~~~~~~~~   ~~~~~   ~~~~~~   ~~~~~~~~~~~~~~~~~~     ~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~~~~
  1    1684542445002144   ocnos    cmlsh    20-05-2023 00:27:25             Confirmed                          NA
```

Example of a Commit Rollback to the Commit List ID 1684542445002144:

```
#commit-rollback to 1684542445002144 description commit-rollback Test
#show commit list

S.No.         ID           User    Client         TimeStamp              Commit Status                      Description
~~~~~  ~~~~~~~~~~~~~~~~~   ~~~~~   ~~~~~~   ~~~~~~~~~~~~~~~~~~~     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~~~~
  1    1684542445002144   ocnos    cmlsh    20-05-2023 00:27:25            Confirmed                          NA
  2    1684542402123428   ocnos    cmlsh    20-05-2023 00:28:45     Rollback to 20-05-2023 00:27:25        commit-rollback Test
```

Example of an automatic Commit Rollback

```
#show commit list

S.No.         ID           User    Client         TimeStamp              Commit Status                      Description
~~~~~  ~~~~~~~~~~~~~~~~~   ~~~~~   ~~~~~~   ~~~~~~~~~~~~~~~~~~~   ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~   ~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~
#show run router ospf
!
#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#router ospf 5
(config-router)#router ospf 6
(config-router)#commit confirmed timeout 20 description This is to test auto rollback of config
(config-router)#end
#show commit list

S.No.         ID           User    Client         TimeStamp              Commit Status                      Description
~~~~~  ~~~~~~~~~~~~~~~~~   ~~~~~   ~~~~~~   ~~~~~~~~~~~~~~~~~~~   ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~   ~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~
  1    1698242643599569    root    cmlsh    25-10-2023 14:04:03          Remaining Time: 17            This is to test auto
rollback of config

#show run router ospf
!
router ospf 5
!
router ospf 6
!
#
Warning!!! Confirmed-commit timed out for commitid: 1698242643599569
#show commit list

S.No.         ID           User    Client         TimeStamp              Commit Status                      Description
~~~~~  ~~~~~~~~~~~~~~~~~   ~~~~~   ~~~~~~   ~~~~~~~~~~~~~~~~~~~   ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~   ~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~
  1    1698242643599569    root    cmlsh    25-10-2023 14:04:03          Timed-out (Reverted)         This is to test auto
rollback of config

#show run router ospf
!
#
```

clear cml commit-history (WORD|)

Use this command to delete any specific entry mentioned by commit ID or to delete entire list entries.

Note: To use the commit-rollback operation, the `cml commit-history` operation must be enabled, and note that commit-rollback cannot be used for deleted entries.

Command Syntax

```
clear cml commit-history (WORD|)
```

Parameter

`Word`	commit ID of the recorded commit operations into commit-history list

Default

When no parameter is provided, the commit history is deleted by default. If you specify the 'Word' parameter, it will delete the specific commit record.

Command Mode

Exec mode

Applicability

This command is introduced in OcNOS 6.4.1.

Example

Example for clear commit using Commit History ID:

```
#show commit list

S.No.         ID           User    Client         TimeStamp               Commit Status                      Description
~~~~~  ~~~~~~~~~~~~~~~~~   ~~~~~   ~~~~~~   ~~~~~~~~~~~~~~~~~~~     ~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~~~
  1    1684486018411866   ocnos    cmlsh    19-05-2023 08:46:58             Confirmed                          NA
  2    1684486037040268   ocnos    cmlsh    19-05-2023 08:47:17             Confirmed

#clear cml commit-history 1684486018411866
#show commit list

S.No.         ID           User    Client         TimeStamp               Commit Status                      Description
~~~~~  ~~~~~~~~~~~~~~~~~   ~~~~~   ~~~~~~   ~~~~~~~~~~~~~~~~~~~     ~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~~~
  1    1684486037040268   ocnos    cmlsh    19-05-2023 08:47:17             Confirmed                          NA
```

cml commit-history (enable | disable)

Use this command to enable or disable confirmed commit operation (commit-history operation). To verify the state of the operation, use the command `show cml commit-history state`.

Note:

- By default, cml commit-history operation is enabled.
- After disabling the cml commit-history operation, confirmed commit CLIs cannot be used, rendering the commit confirmed, *confirm-commit,* and *cancel-commit* operations unavailable.

Command Syntax

```
cml commit-history (enable | disable)
```

Parameter

`Enable`	Enables commit confirmed and commit rollback operations
`Disable`	Disables commit confirmed and commit rollback operations

Default

By default, commit confirmed and commit rollback operations are enabled.

Command Mode

Exec mode

Applicability

This command is introduced in OcNOS 6.4.1.

Example

Example for enabling Commit History:

```
#cml commit-history enable
Warning!!! commit-history feature is enabled, confirmed commit and commit-
rollback features are available for use.
```

Example for disabling Commit History:

```
#cml commit-history disable
Warning!!! commit-history feature is disabled, confirmed commit and commit-
rollback features can not be used.
```

cml commit-id rollover (enable | disable)

Use this command to enable or disable commit entry rollover when the maximum count of 50 commit entries is reached. When enabled, older commit entries will be automatically deleted from the commit history list to record new entries.

To verify the state of the operation, use command `show cml commit-id rollover state`.

Note:

- By default, cml commit-id rollover operation is enabled.
- The cml commit-history operation must be enabled to use this operation.
- The commit-rollback operation can not be used for deleted entry.
- When this operation is disabled and the number of commit entries reaches the maximum count, the addition of commit records to the commit history list will be stopped.

Command Syntax

```
cml commit-id rollover (enable | disable)
```

Parameter

`Enable`	Enables commit ID rollover
`Disable`	Disables commit ID rollover

Default

By default, commit ID rollover is enabled.

Command Mode

Exec mode

Applicability

This command is introduced in OcNOS 6.4.1.

Example

Example for verifying commit ID rollover state:

```
#show cml commit-id rollover state
cml commit-id rollover feature is enabled
```

Abbreviations

List of key terms used in this document is:

Term	Description
CMLSH	Common Management Layer Commands

EVPN Active-Standby

Overview

EVPN Multihoming is a mechanism that allows a host or customer edge (CE) device to be connected to multiple Provider Edge (PE) devices called Multihoming (MH) peers for redundancy and load balancing purposes. This provides high availability and resiliency to the network, ensuring continuous connectivity even in case of a PE device failure.

Note: OcNOS support extends to a maximum of two MH peers.

Multihoming supports two kinds of redundancy, namely 1. All Active 2. Active-Standby.

Till now, OcNOS support All-Active (A-A) only. In OcNOS version 6.4.1, Port-Active mode is supported and in OcNOS version 6.4.2, Single-Active mode is supported in the context of Active-Standby redundancy.

Single-Active

- In this mode, traffic for a specific host or MAC address is handled by only one of the PE devices (MH peers) at a time.
- The other PE devices remain in standby mode, ready to take over if the active PE fails.
- The physical link state (either Physical port or LACP port) on the standby PE remains up, enabling a faster transition to the active role in the event of a failover. The CE devices use different interfaces, including LACP or physical connections, to connect to the Peer MH devices.

Port-Active

- In this mode, traffic for a specific host or MAC address is handled by only one of the PE devices (MH peers) at a time.
- Each MH peer connects through LACP with the same key as the CE devices (similar to A-A redundancy).
- The physical link state (LACP port) on the standby PE is made down, effectively blocking traffic on those ports.
- If a failover occurs, the standby PE must bring up its LACP ports to start forwarding traffic.

IRB Active-Standby: Active-standby mode is also applicable to Integrated Routing and Bridging (IRB) for both L3VPN symmetric and asymmetric modes.

Feature Characteristics

Single-Active standby redundancy mechanisms support both ELAN and ELINE services.

Single-Active ELINE

ELINE refers to Ethernet Line services, where two PEs are cross-connected to each other over an Ethernet link.

In Single-Active ELINE, the primary objective is to achieve redundancy for hosts while also using the same link for data exchange until it fails, at which point it should switch to the secondary or standby link. Here's how it works:

- **MH Host Traffic**
  - One of the PE devices (MH peers) acts as the “Active” for the Attachment Circuit (AC) associated with the host. This PE sends and receives traffic to and from the host.
  - The other PE acts as the “Standby” for the same AC and does not allow traffic to or from the host.

    - The standby PE, despite receiving BUM traffic from the Host device (which is unaware of the cross-connect), blocks this traffic at the standby PE itself, as it operates in a standby role for the AC. Conversely, the active PE allows the flow of traffic.
- **Remote Host Traffic:** Traffic originating from remote hosts destined for the multihomed host is only sent to the active MH peer for the corresponding AC. This ensures that the cross connect is established only with the Active MH peer.

Single-Active ELAN

ELAN stands for Ethernet LAN services, where a group of PEs are interconnected in a multipoint Ethernet network.

In Single-Active ELAN, similar to Single-Active ELINE, redundancy for hosts and data exchange over the primary link are priorities, but there are some specific differences for Ethernet LAN (ELAN) scenarios:

- **MH Host Traffic**
    - One of the PE devices (MH peers) is designated as the “Active” for the AC associated with the host. This PE handles sending and receiving traffic to and from remote locations.
    - The other PE acts as the “Standby” role for the same AC. It receives BUM traffic from the host but blocks the traffic. Additionally, it refrains from learning MAC addresses and does not uplift Address Resolution Protocol/ Neighbor Discovery (ARP/ND) packets.
    - Unicast traffic from the host will be directed to the active PE, which will then allow the traffic to be sent across the network.
- **Remote Host Unicast Traffic:** Unicast traffic from remote hosts destined for the multihomed host is sent only to the active MH peer for the corresponding AC. This is because the MAC addresses of the host are learned only from the Active MH peer.
- **Remote Host BUM Traffic:** BUM traffic, such as broadcast and multicast packets from the remote PE device, is replicated to both MH PEs. However, only the active PE, which is also designated as a forwarder, allows this traffic to reach the host. The standby PE, classified as a Non-Designated Forwarder, drops the egress traffic.

Port-Active Ethernet LAN (ELAN) and Ethernet LINE (ELINE) are examples of port-active standby redundancy mechanisms.

Port-Active ELINE

Port-Active ELINE enables redundancy and optimized data exchange by designating an active port for traffic handling in multihomed network setups. Here's how it works:

- **Active AC Link:** Among the Multihomed (MH) peers, a designated PE is assigned as “Active” for the AC associated with the host. This PE manages bidirectional traffic to and from the host. In a port-active configuration, all hosts associated with the ESI link remain in the same state, as the Active and Standby status is determined per ESI link.
- **Standby AC Link:** The AC link attached to the host, designated as “Standby,” remains operationally down. It serves as a backup link for failover scenarios.
- **MH Host traffic:** BUM and unicast traffic from the host are always directed towards the Active PE because the link towards the Active PE is operational UP. Conversely, the link towards the Standby PE from the host devices is operational DOWN.
- **Remote Host Traffic:** Traffic originating from remote hosts and destined for the multihomed host is directed exclusively to the Active MH node that serves the corresponding AC. This ensures efficient traffic routing and intelligent cross-connection establishment.

Port-Active ELAN

Port-Active ELAN enhances redundancy and efficient data exchange by designating an active port for traffic management in multihomed Ethernet LAN environments. Here's how it works:

- **Active AC Link:** Within the MH peers, one PE is identified as the “Active” entity for the AC. It manages traffic to and from remote locations efficiently.
- **Standby AC Link:** Similar to Port-Active ELINE, the standby AC link attached to the host remains operationally down to ensure effective standby redundancy.
- **MH Host Traffic:** In a port-active scenario, the standby link does not receive any traffic from the host. Only the active link manages incoming traffic from the host. The Active PE also learns and advertises host information to remote locations, including MAC addresses and ARP/ND details.
- **Remote Host Unicast Traffic:** Unicast traffic from remote sources is directed exclusively to the Active MH PE that has advertised the host address, optimizing traffic flow.
- **Remote Host BUM Traffic:** BUM traffic is replicated across all MH nodes. However, egress traffic for BUM packets occurs only from the Active PE. The standby PE drops the traffic since the AC links are operational DOWN.

Benefits

The benefits of Single-Active and Port-Active include enhanced redundancy and fault tolerance for hosts and customer edge devices, efficient data exchange, minimized downtime, and improved network resiliency in multihomed Ethernet Line and Ethernet LAN environments. These mechanisms ensure uninterrupted connectivity and optimized traffic management, contributing to higher availability and improved user experience.

Prerequisites

Here are the prerequisites for configuring EVPN Multihoming:

Ensure EVPN Configuration: Make sure that the EVPN is configured already in the network as it is a requirement for EVPN Multihoming.

Configure Attachment Circuits (AC): Ensure that each CE device is appropriately linked to the PE devices through Attachment Circuits. These circuits must be configured correctly.

Set Up LACP Configuration: To use Link Aggregation Control Protocol (LACP) for multihoming, configure LACP appropriately on the relevant interfaces.

EVPN MPLS Global Configuration: To enable EVPN MPLS features, need to configure global settings, such as enabling EVPN MPLS, defining global VTEP IP addresses, enabling hardware profile filtering for multihoming, and activating EVPN MPLS multihoming functionality. These settings are essential for EVPN and MPLS operation.

Access Port Configuration: Depending on the network's redundancy plan (single-active or port-active), configure access ports, including parameters for load balancing, service carving preferences, and EVPN settings. These configurations are crucial for network access and connectivity in an EVPN environment.

These prerequisites ensure that the network is ready for the implementation of EVPN Multihoming, providing redundancy and load balancing for CE devices.

Configuration

Here are sample configurations for *EVPN MPLS Active-Standby MultiHoming Configuration* and *EVPN SR Active-Standby Multi-Homing Configuration,* including topology, configuration procedures, and corresponding validations.

For more information on the EVPN MPLS configurations, see the *EVPN MPLS Configuration* and *EVPN MPLS IRB Configuration* chapters in the *Multi-Protocol Label Switching Guide*, Release 6.4.2.

EVPN MPLS Active-Standby MultiHoming Configuration

This section illustrates the Multi-Homed setup for the EVPN MPLS Active-Standby configuration, showcasing examples for both ELINE and ELAN services with LDP as the underlay MPLS path.

EVPN MPLS Active-Standby MH Topology

Figure 1 consists of customer edge routers CE1 and CE2, along with IPv4 Provider Edge routers PE1, PE2, PE3, and PE4, all interconnected through the core routers P1 and P2 in the IPv4 MPLS provider network.

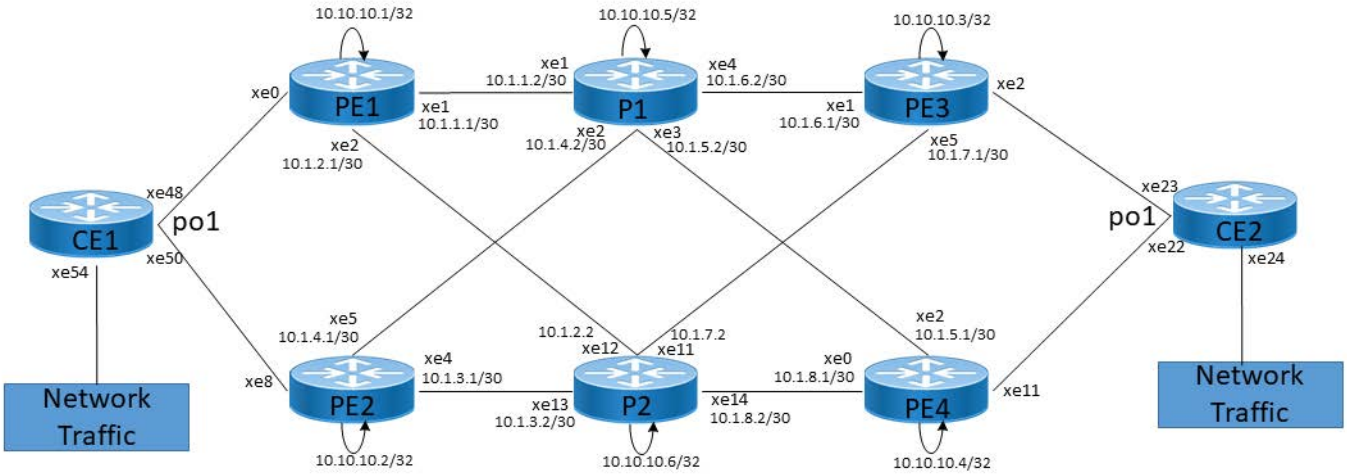


Figure 1: EVPN MPLS AS MH Configuration

CE1

The following configuration steps under CE1 are set up to enable VLANs and configure interfaces for carrying VLAN traffic.

`CE1#configure terminal`	Enter configure mode.
`CE1(config)#bridge 1 protocol ieee vlan-bridge`	Set up `bridge 1` to use the IEEE VLAN bridge protocol.
`CE1(config)#vlan 2-100 bridge 1 state enable`	Configure VLANs from `2-100` and associate them with bridge 1.
`CE1(config)#interface xe54`	Enter interface mode `xe54`.
`CE1(config-if)#switchport`	Configure the interface `xe54` as a Layer 2 switch port.
`CE1(config-if)#bridge-group 1`	Associate `xe54` to bridge 1.
`CE1(config-if)#switchport mode trunk`	Configure `xe54` as a trunk port.
`CE1(config-if)#switchport trunk allowed vlan all`	Allow all configured VLANs on the trunk interface `xe54`.
`CE1(config-if)#exit`	Exit interface mode `xe54`.
`CE1(config)#interface po1`	Enter interface mode and configure LAG interface port-channel 1 (`po1`).
`CE1(config-if)#switchport`	Configures port-channel 1 as a Layer 2 switch port.

CE1(config-if)#bridge-group 1	Associate po1 to bridge 1.
CE1(config-if)#switchport mode trunk	Configure po1 as a trunk port.
CE1(config-if)#switchport trunk allowed vlan all	Allow all configured VLANs on the trunk port-channel po1.
CE1(config-if)#exit	Exit interface mode po1.
CE1(config)#interface xe48	Enter interface mode xe48.
CE1(config-if)#lacp timeout short	Configure LACP timeout as short.
CE1(config-if)#channel-group 1 mode active	Add member to the LAG interface.
CE1(config-if)#exit	Exit interface mode xe48.
CE1(config-if)#interface xe50	Enter interface mode xe50.
CE1(config-if)#lacp timeout short	Configure LACP timeout as short.
CE1(config-if)#channel-group 1 mode active	Add member to the LAG interface.
CE1(config-if)#commit	Commit the transaction.
CE1(config-if)#end	Exit interface mode xe50 and configure mode.

PE1: Loopback Interface

The configuration on PE1 for a loopback interface with IP address 10.10.10.1/32 secondary is set up to provide IP connectivity for the router.

PE1#configure terminal	Enter configure mode.
PE1(config)#interface lo	Enter the interface mode for the loopback interface lo.
PE1(config-if)#ip address 10.10.10.1/32 secondary	Configure a secondary IP address, 10.10.10.1/32, on the loopback interface.
PE1(config-if)#exit	Exit interface mode lo.
PE1(config)#commit	Commit the transaction.

PE1: Global LDP

The configuration on PE1 for the Global LDP router, specifying router ID and targeted peers, is done to set up Label Distribution Protocol (LDP) settings for MPLS.

PE1(config)#router ldp	Enter the Router LDP mode.
PE1(config-router)#router-id 10.10.10.1	Set the router ID for LDP to 10.10.10.1.
PE1(config-router)#transport-address ipv4 10.10.10.1	Configure the transport address for IPv4 (for IPv6 use ipv6 parameter) to be used for a TCP session where LDP operates. Note: It is preferable to use the loopback address as the transport address.
PE1(config-router)#targeted-peer ipv4 10.10.10.2	Configure targeted peer for LDP using IPv4 addresses.
PE1(config-router-targeted-peer)#exit-targeted-peer-mode	Exit router targeted-peer-mode.
PE1(config-router)#targeted-peer ipv4 10.10.10.3	Configure targeted peer for LDP using IPv4 addresses.
PE1(config-router-targeted-peer)#exit-targeted-peer-mode	Exit router targeted-peer-mode.

`PE1(config-router)#targeted-peer ipv4 10.10.10.4`	Configure targeted peer for LDP using IPv4 addresses.
`PE1(config-router-targeted-peer)#exit-targeted-peer-mode`	Exit router targeted-peer-mode.
`PE1(config-router)#exit`	Exit router LDP mode and return to the configure mode.
`PE1(config)#commit`	Commit the transaction.

PE1: Global EVPN MPLS Command

The configuration on PE1 for the Global EVPN MPLS, includes activating EVPN MPLS, defining the global VTEP IP address, enabling hardware profile filtering for EVPN MPLS multi-homing, and activating EVPN MPLS multi-homing functionality, all of which are crucial for enabling EVPN MPLS features.

`PE1(config)#evpn mpls enable`	Activate the EVPN MPLS functionality on `PE1`, enabling it to participate in EVPN MPLS services.
`PE1(config)#commit`	Commit candidate configuration to be running configuration.
`PE1(config)#evpn mpls vtep-ip-global 10.10.10.1`	Configure the global VTEP IP address `10.10.10.1`, associating it with the loopback IP.
`PE1(config)#hardware-profile filter evpn-mpls-mh enable`	Enable hardware-profile filter for EVPN MPLS multi-homing.
`PE1(config)#evpn mpls multihoming enable`	Activate the EVPN MPLS multi-homing functionality, allowing `PE1` to support multi-homed EVPN MPLS services.
`PE1(config)#commit`	Commit the transaction.

PE1: Interface Configuration Network Side

The below configuration is performed to set up network interfaces on PE1 and enable LDP for IPv4, ensuring proper routing and labeling functionality.

`PE1(config)#interface xe1`	Enter interface mode `xe1`.
`PE1(config-if)#ip address 10.1.1.1/30`	Configure an IP address, `10.1.1.1/30`, on the interface `xe1`.
`PE1(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`PE1(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`PE1(config-if)#exit`	Exit interface mode `xe1`.
`PE1(config)#commit`	Commit the transaction.
`PE1(config)#interface xe2`	Enter interface mode `xe2`.
`PE1(config-if)#ip address 10.1.2.1/30`	Configure an IP address, `10.1.2.1/30`, on the interface `xe2`.
`PE1(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`PE1(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.

`PE1(config-if)#exit`	Exit interface mode `xe2`.
`PE1(config)#commit`	Commit the transaction.

PE1: OSPF Configuration

The below configuration is performed to set up OSPF on PE1, specifying the router ID, defining network interfaces, and configuring BFD parameters for efficient routing.

`PE1(config)#router ospf 100`	Enter the router OSPF mode. Configure PE1 to run OSPF with process ID 100.
`PE1(config-router)#ospf router-id 10.10.10.1`	Set the OSPF router ID to `10.10.10.1`, identifying PE1 within the OSPF network.
`PE1(config-router)#network 10.10.10.1/32 area 0.0.0.0`	Advertise loopback address in OSPF.
`PE1(config-router)#network 10.1.1.1/30 area 0.0.0.0`	Advertise network address in OSPF.
`PE1(config-router)#network 10.1.2.1/30 area 0.0.0.0`	Advertise network address in OSPF.
`PE1(config-router)#bfd interval 3 minrx 3 multiplier 3`	Configure BFD interval with an interval of `3`, a minimum receive interval of `3`, and a multiplier of `3`.
`PE1(config-router)#exit`	Exit router OSPF mode and return to configure mode.
`PE1(config)#commit`	Commit the transaction.

PE1: BGP Configuration

The below BGP configuration on PE1 is established to enable BGP routing with ASN 65010, set the BGP router ID, define iBGP neighbors, configure BFD, and enable the EVPN address family for efficient routing in an EVPN environment.

`PE1(config)#router bgp 65010`	Enter the Router BGP mode, ASN: 65010
`PE1(config-router)#bgp router-id 10.10.10.1`	Configure BGP router ID `10.10.10.1`, identifying PE1 within the BGP network.
`PE1(config-router)#neighbor 10.10.10.2 remote-as 65010`	Configure neighbor `10.10.10.2` as an iBGP neighbor with their remote AS number `65010`.
`PE1(config-router)#neighbor 10.10.10.2 update-source lo`	Configure neighbor `10.10.10.2` as an iBGP neighbor, specifying the source of routing updates as the loopback interface.
`PE1(config-router)#neighbor 10.10.10.3 remote-as 65010`	Configure neighbor `10.10.10.3` as an iBGP neighbor with their remote AS number `65010`.
`PE1(config-router)#neighbor 10.10.10.3 update-source lo`	Configure neighbor `10.10.10.3` as an iBGP neighbor, specifying the source of routing updates as the loopback interface.
`PE1(config-router)#neighbor 10.10.10.4 remote-as 65010`	Configure neighbor `10.10.10.4` as an iBGP neighbor with their remote AS number `65010`.
`PE1(config-router)#neighbor 10.10.10.4 update-source lo`	Configure neighbor `10.10.10.4` as an iBGP neighbor, specifying the source of routing updates as the loopback interface.
`PE1(config-router)#neighbor 10.10.10.2 fall-over bfd multihop`	Configure BFD for the BGP neighbor to provide rapid failure detection.

`PE1(config-router)#neighbor 10.10.10.3 fall-over bfd multihop`	Configure BFD for the BGP neighbor to provide rapid failure detection.
`PE1(config-router)#neighbor 10.10.10.4 fall-over bfd multihop`	Configure BFD for the BGP neighbor to provide rapid failure detection.
`PE1(config-router)#neighbor 10.10.10.2 advertisement-interval 0`	Configure advertisement interval for the neighbor, allowing more frequent BGP updates.
`PE1(config-router)#neighbor 10.10.10.3 advertisement-interval 0`	Configure advertisement interval for the neighbor, allowing more frequent BGP updates.
`PE1(config-router)#neighbor 10.10.10.4 advertisement-interval 0`	Configure advertisement interval for the neighbor, allowing more frequent BGP updates.
`PE1(config-router)#address-family l2vpn evpn`	Enter into address family mode for L2VPN EVPN.
`PE1(config-router-af)#neighbor 10.10.10.2 activate`	Activate EVPN for iBGP neighbor `10.10.10.2` within the address family mode, ensuring that EVPN address family is enabled for the neighbor.
`PE1(config-router-af)#neighbor 10.10.10.3 activate`	Activate EVPN for iBGP neighbor `10.10.10.3` within the address family mode, ensuring that EVPN address family is enabled for the neighbor.
`PE1(config-router-af)#neighbor 10.10.10.4 activate`	Activate EVPN for iBGP neighbor `10.10.10.4` within the address family mode, ensuring that EVPN address family is enabled for the neighbor.
`PE1(config-router-af)#exit`	Exit address family mode and return to the router BGP mode.
`PE1(config-router)#commit`	Commit the transaction.
`PE1(config-router)#exit`	Exit router BGP mode and return to the configure mode.

PE1: MAC VRF Configuration

The below MAC VRF configuration on PE1 is carried out to define and set up VRFs named `vrf2` and `vpls1001` with specific Route-Distinguisher (RD) and route-target values, ensuring segregated MAC address spaces for distinct network services.

`PE1(config)#mac vrf vrf2`	Enter VRF mode named `vrf2`.
`PE1(config-vrf)#rd 10.10.10.1:1700`	Configure Route-Distinguisher value of `10.10.10.1:1700`.
`PE1(config-vrf)#route-target both 1700:1700`	Configure import and export values for the `vrf2` as `1700:1700`.
`PE1(config-vrf)#exit`	Exit VRF mode and return to the configure mode.
`PE1(config)#mac vrf vpls1001`	Enter VRF mode named `vpls1001`.
`PE1(config-vrf)#rd 10.10.10.1:1001`	Configure Route-Distinguisher value of `10.10.10.1:1001`.
`PE1(config-vrf)#route-target both 1001:1001`	Configure import and export values for the `vpls1001` as `1001:1001`.
`PE1(config-vrf)#exit`	Exit VRF mode and return to the configure mode.
`PE1(config)#commit`	Commit the transaction.

PE1: EVPN and VRF Mapping

The below EVPN and VRF mapping configuration on PE1 is performed to establish mappings between EVPN identifiers and VRFs, facilitating efficient routing and connectivity in an EVPN network environment.

`PE1(config)#evpn mpls id 1800 xconnect target-mpls-id 1700`	Configure the EVPN-VPWS identifier with a source identifier of `1800` and a target identifier of `1700`.
`PE1(config-evpn-mpls)#host-reachability-protocol evpn-bgp vrf2`	Map VRF `vrf2` to the EVPN-VPWS identifier
`PE1(config-evpn-mpls)#evpn mpls id 3000`	Configure the EVPN-VPLS identifier an identifier of `3000`.
`PE1(config-evpn-mpls)#host-reachability-protocol evpn-bgp vpls1001`	Map VRF `vpls1001` to the EVPN-VPWS identifier
`PE1(config-evpn-mpls)#commit`	Commit the transaction.
`PE1(config-evpn-mpls)#exit`	Exit the EVPN MPLS mode and return to the configure mode.

PE1: Access Port Configuration for Port-active

The below access port configuration for port-active mode on PE1 is carried out to configure various parameters including system-mac, load balancing, service carving preferences, and EVPN settings for efficient network access and connectivity.

`PE1(config)#interface po1`	Enter the port channel interface mode for `po1`
`PE1(config-if)#load-interval 30`	Set the load interval to `30`.
`PE1(config-if)#evpn multi-homed system-mac 0000.1111.7777 load-balancing port-active`	Configure the system-mac address `0000.1111.7777` for port-active mode, which plays a role in load balancing and enter to the EVPN Ethernet Segment (ES) mode.
`PE1(config-if-es)#service-carving auto`	Configure service carving as `auto`.
`PE1(config-if-es)#exit`	Exit the EVPN ES mode and return to the configure mode.
`PE1(config-if)#exit`	Exit interface mode `po1` and return to the configure mode.
`PE1(config)#commit`	Commit the transaction.
`PE1(config)#interface po1.1 switchport`	Create a Layer 2 sub-interface `po1.1` within the port channel.
`PE1(config-if)#encapsulation dot1q 100`	Set encapsulation to dot1q with VLAN ID `100`.
`PE1(config-if)#load-interval 30`	Set the load interval to `30`.
`PE1(config-if)#access-if-evpn`	Enter the access mode for EVPN MPLS ID configuration.
`PE1(config-acc-if-evpn)#map vpn-id 1800`	Map VPN-ID `1800`.
`PE1(config-acc-if-evpn)#exit`	Exit the access mode and return to the interface mode.
`PE1(config-if)#exit`	Exit interface mode `po1.1` and return to the configure mode.
`PE1(config)#interface xe0`	Enter the interface mode for `xe0.`
`PE1(config-if)#speed 10g`	Set the speed to `10g`.
`PE1(config-if)#channel-group 1 mode active`	Attach LAG interface `po1.`
`PE1(config-if)#exit`	Exit interface mode `xe0` and return to the configure mode.
`PE1(config)#commit`	Commit the transaction.

PE1: Access Port Configuration for Single-active

The below access port configuration for single-active mode on PE1 is implemented to set up various parameters, including Ethernet Segment Identifier (ESI) settings, service carving preferences, and EVPN configurations, ensuring efficient network access and connectivity.

`PE1(config)#interface sa1`	Enter the single active interface mode for `sa1`
`PE1(config-if)#load-interval 30`	Set the load interval to `30`.
`PE1(config-if)#evpn multi-homed esi 00:00:11:11:77:77 load-balancing single-active`	Configure the ESI with the value with the value `00:00:11:11:77:77` for single-active mode, which plays a role in load balancing and enter to the EVPN Ethernet Segment (ES) mode.
`PE1(config-if-es)#service-carving auto`	Configure service carving as `auto`, allowing automatic determination of service distribution preferences.
`PE1(config-if-es)#exit`	Exit the EVPN ES mode and return to the configure mode.
`PE1(config-if)#exit`	Exit interface mode `sa1` and return to the configure mode.
`PE1(config)#commit`	Commit the transaction.
`PE1(config)#interface sa1.1 switchport`	Create a Layer 2 sub-interface `sa1.1` within the port channel.
`PE1(config-if)#encapsulation dot1q 100`	Set encapsulation to dot1q with VLAN ID `100`.
`PE1(config-if)#load-interval 30`	Set the load interval to `30`.
`PE1(config-if)#access-if-evpn`	Enter the access mode for EVPN MPLS ID configuration.
`PE1(config-acc-if-evpn)#map vpn-id 1800`	Map VPN-ID `1800`.
`PE1(config-acc-if-evpn)#exit`	Exit the access mode and return to the interface mode.
`PE1(config-if)#exit`	Exit interface mode `sa1.1` and return to the configure mode.
`PE1(config)#interface xe0`	Enter the interface mode for `xe0`.
`PE1(config-if)#speed 10g`	Set the speed to `10g`.
`PE1(config-if)#static-channel-group 1`	Attach the static-channel-group 1, the LAG interface `sa1` to `xe0`.
`PE1(config-if)#exit`	Exit interface mode `xe0` and return to the configure mode.
`PE1(config)#commit`	Commit the transaction.

PE2: Loopback Interface

The configuration on PE2 for a loopback interface with IP address `10.10.10.2/32` secondary is set up to provide IP connectivity for the router.

`PE2#configure terminal`	Enter configure mode.
`PE2(config)#interface lo`	Enter the interface mode for the loopback interface `lo`.
`PE2(config-if)#ip address 10.10.10.2/32 secondary`	Configure a secondary IP address, `10.10.10.2/32`, on the loopback interface.
`PE2(config-if)#exit`	Exit interface mode `lo`.
`PE2(config)#commit`	Commit the transaction.

PE2: Global LDP

The configuration on PE2 for the Global LDP router, specifying router ID and targeted peers, is done to set up Label Distribution Protocol (LDP) settings for MPLS.

`PE2(config)#router ldp`	Enter the Router LDP mode.
`PE2(config-router)#router-id 10.10.10.2`	Set the router ID for LDP to `10.10.10.2`.

`PE2(config-router)#transport-address ipv4 10.10.10.2`	Configure the transport address for IPv4 (for IPv6 use ipv6 parameter) to be used for a TCP session where LDP operates. Note: It is preferable to use the loopback address as the transport address.
`PE2(config-router)#targeted-peer ipv4 10.10.10.1`	Configure targeted peer for LDP using IPv4 addresses.
`PE2(config-router-targeted-peer)#exit-targeted-peer-mode`	Exit router targeted-peer-mode.
`PE2(config-router)#targeted-peer ipv4 10.10.10.3`	Configure targeted peer for LDP using IPv4 addresses.
`PE2(config-router-targeted-peer)#exit-targeted-peer-mode`	Exit router targeted-peer-mode.
`PE2(config-router)#targeted-peer ipv4 10.10.10.4`	Configure targeted peer for LDP using IPv4 addresses.
`PE2(config-router-targeted-peer)#exit-targeted-peer-mode`	Exit router targeted-peer-mode.
`PE2(config-router)#exit`	Exit router LDP mode and return to the configure mode.
`PE2(config)#commit`	Commit the transaction.

PE2: Global EVPN MPLS Command

The configuration on PE2 for the Global EVPN MPLS, includes activating EVPN MPLS, defining the global VTEP IP address, enabling hardware profile filtering for EVPN MPLS multi-homing, and activating EVPN MPLS multi-homing functionality, all of which are crucial for enabling EVPN MPLS features.

`PE2(config)#evpn mpls enable`	Activate the EVPN MPLS functionality on `PE2`, enabling it to participate in EVPN MPLS services.
`PE2(config)#commit`	Commit candidate configuration to be running configuration.
`PE2(config)#evpn mpls vtep-ip-global 10.10.10.2`	Configure the global VTEP IP address `10.10.10.2`, associating it with the loopback IP.
`PE2(config)#hardware-profile filter evpn-mpls-mh enable`	Enable hardware-profile filter for EVPN MPLS multi-homing.
`PE2(config)#evpn mpls multihoming enable`	Activate the EVPN MPLS multi-homing functionality, allowing `PE2` to support multi-homed EVPN MPLS services.
`PE2(config)#commit`	Commit the transaction.

PE2: Interface Configuration Network Side

The below configuration is performed to set up network interfaces on PE2 and enable LDP for IPv4, ensuring proper routing and labeling functionality.

`PE2(config)#interface xe4`	Enter interface mode `xe4`.
`PE2(config-if)#ip address 10.1.3.1/30`	Configure an IP address, `10.1.3.1/30`, on the interface `xe4`.
`PE2(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`PE2(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.

`PE2(config-if)#exit`	Exit interface mode `xe4`.
`PE2(config)#commit`	Commit the transaction.
`PE2(config)#interface xe5`	Enter interface mode `xe5`.
`PE2(config-if)#ip address 10.1.4.1/30`	Configure an IP address, `10.1.4.1/30`, on the interface `xe5`.
`PE2(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`PE2(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`PE2(config-if)#exit`	Exit interface mode `xe5`.
`PE2(config)#commit`	Commit the transaction.

PE2: OSPF Configuration

The below configuration is performed to set up OSPF on PE2, specifying the router ID, defining network interfaces, and configuring BFD parameters for efficient routing.

`PE2(config)#router ospf 100`	Enter the router OSPF mode. Configure PE2 to run OSPF with process ID 100.
`PE2(config-router)#ospf router-id 10.10.10.2`	Set the OSPF router ID to `10.10.10.2`, identifying PE2 within the OSPF network.
`PE2(config-router)#network 10.1.3.1/30 area 0.0.0.0`	Advertise loopback address in OSPF.
`PE2(config-router)#network 10.1.4.1/30 area 0.0.0.0`	Advertise network address in OSPF.
`PE2(config-router)#bfd interval 3 minrx 3 multiplier 3`	Configure BFD interval with an interval of `3`, a minimum receive interval of `3`, and a multiplier of `3`.
`PE2(config-router)#exit`	Exit router OSPF mode and return to the configure mode.
`PE2(config)#commit`	Commit the transaction.

PE2: BGP Configuration

The below BGP configuration on PE2 is established to enable BGP routing with ASN 65010, set the BGP router ID, define iBGP neighbors, configure BFD, and enable the EVPN address family for efficient routing in an EVPN environment.

`PE2(config)#router bgp 65010`	Enter the Router BGP mode, ASN: 65010
`PE2(config-router)#bgp router-id 10.10.10.2`	Configure BGP router ID `10.10.10.2`, identifying PE2 within the BGP network.
`PE2(config-router)#neighbor 10.10.10.1 remote-as 65010`	Configure neighbor `10.10.10.1` as an iBGP neighbor with their remote AS number `65010`.
`PE2(config-router)#neighbor 10.10.10.1 update-source lo`	Configure neighbor `10.10.10.1` as an iBGP neighbor, specifying the source of routing updates as the loopback interface.
`PE2(config-router)#neighbor 10.10.10.3 remote-as 65010`	Configure neighbor `10.10.10.3` as an iBGP neighbor with their remote AS number `65010`.

`PE2(config-router)#neighbor 10.10.10.3 update-source lo`	Configure neighbor `10.10.10.3` as an iBGP neighbor, specifying the source of routing updates as the loopback interface.
`PE2(config-router)#neighbor 10.10.10.4 remote-as 65010`	Configure neighbor `10.10.10.4` as an iBGP neighbor with their remote AS number `65010`.
`PE2(config-router)#neighbor 10.10.10.4 update-source lo`	Configure neighbor `10.10.10.4` as an iBGP neighbor, specifying the source of routing updates as the loopback interface.
`PE2(config-router)#neighbor 10.10.10.1 fall-over bfd multihop`	Configure BFD for the BGP neighbor to provide rapid failure detection.
`PE2(config-router)#neighbor 10.10.10.3 fall-over bfd multihop`	Configure BFD for the BGP neighbor to provide rapid failure detection.
`PE2(config-router)#neighbor 10.10.10.4 fall-over bfd multihop`	Configure BFD for the BGP neighbor to provide rapid failure detection.
`PE2(config-router)#neighbor 10.10.10.1 advertisement-interval 0`	Configure advertisement interval for the neighbor, allowing more frequent BGP updates.
`PE2(config-router)#neighbor 10.10.10.3 advertisement-interval 0`	Configure advertisement interval for the neighbor, allowing more frequent BGP updates.
`PE2(config-router)#neighbor 10.10.10.4 advertisement-interval 0`	Configure advertisement interval for the neighbor, allowing more frequent BGP updates.
`PE2(config-router)#address-family l2vpn evpn`	Enter into address family mode for L2VPN EVPN.
`PE2(config-router-af)#neighbor 10.10.10.1 activate`	Activate EVPN for iBGP neighbor `10.10.10.1` within the address family mode, ensuring that EVPN address family is enabled for the neighbor.
`PE2(config-router-af)#neighbor 10.10.10.3 activate`	Activate EVPN for iBGP neighbor `10.10.10.3` within the address family mode, ensuring that EVPN address family is enabled for the neighbor.
`PE2(config-router-af)#neighbor 10.10.10.4 activate`	Activate EVPN for iBGP neighbor `10.10.10.4` within the address family mode, ensuring that EVPN address family is enabled for the neighbor.
`PE2(config-router-af)#exit`	Exit address family mode and return to the router BGP mode.
`PE2(config-router)#commit`	Commit the transaction.
`PE2(config-router)#exit`	Exit router BGP mode and return to the configure mode.

PE2: MAC VRF Configuration

The below MAC VRF configuration on PE2 is carried out to define and set up VRFs named `vrf2` and `vpls1001` with specific Route-Distinguisher (RD) and route-target values, ensuring segregated MAC address spaces for distinct network services.

`PE2(config)#mac vrf vrf2`	Enter VRF mode named `vrf2`.
`PE2(config-vrf)#rd 10.10.10.2:1700`	Configure Route-Distinguisher value of `10.10.10.2:1700`.
`PE2(config-vrf)#route-target both 1700:1700`	Configure import and export values for the `vrf2` as `1700:1700`.
`PE2(config-vrf)#exit`	Exit VRF mode and return to the configure mode.
`PE2(config)#mac vrf vpls1001`	Enter VRF mode named `vpls1001`.
`PE2(config-vrf)#rd 10.10.10.2:1001`	Configure Route-Distinguisher value of `10.10.10.2:1001`.

`PE2(config-vrf)#route-target both 1001:1001`	Configure import and export values for the `vpls1001` as `1001:1001`.
`PE2(config-vrf)#exit`	Exit VRF mode and return to the configure mode.
`PE2(config)#commit`	Commit the transaction.

PE2: EVPN and VRF Mapping

The below EVPN and VRF mapping configuration on PE2 is performed to establish mappings between EVPN identifiers and VRFs, facilitating efficient routing and connectivity in an EVPN network environment.

`PE2(config)#evpn mpls id 1800 xconnect target-mpls-id 1700`	Configure the EVPN-VPWS identifier with a source identifier of `1800` and a target identifier of `1700`.
`PE2(config-evpn-mpls)#host-reachability-protocol evpn-bgp vrf2`	Map VRF `vrf2` to the EVPN-VPWS identifier
`PE2(config-evpn-mpls)#evpn mpls id 3000`	Configure the EVPN-VPLS identifier an identifier of `3000`.
`PE2(config-evpn-mpls)#host-reachability-protocol evpn-bgp vpls1001`	Map VRF `vpls1001` to the EVPN-VPWS identifier
`PE2(config-evpn-mpls)#commit`	Commit the transaction.
`PE2(config-evpn-mpls)#exit`	Exit the EVPN MPLS mode and return to the configure mode.

PE2: Access Port Configuration for Port-active

The below access port configuration for port-active mode on PE2 is carried out to configure various parameters including system-mac, load balancing, service carving preferences, and EVPN settings for efficient network access and connectivity.

`PE2(config)#interface po1`	Enter the port channel interface mode for `po1`
`PE2(config-if)#load-interval 30`	Set the load interval to `30`.
`PE2(config-if)#evpn multi-homed system-mac 0000.1111.7777 load-balancing port-active`	Configure the system-mac address `0000.1111.7777` for port-active mode, which plays a role in load balancing and enter to the EVPN Ethernet Segment (ES) mode.
`PE2(config-if-es)#service-carving auto`	Configure service carving as `auto`, allowing automatic determination of service distribution preferences.
`PE2(config-if-es)#exit`	Exit the EVPN ES mode and return to the configure mode.
`PE2(config-if)#exit`	Exit interface mode `po1` and return to the configure mode.
`PE2(config)#commit`	Commit the transaction.
`PE2(config)#interface po1.1 switchport`	Create a Layer 2 sub-interface `po1.1` within the port channel.
`PE2(config-if)#encapsulation dot1q 100`	Set encapsulation to dot1q with VLAN ID `100`.
`PE2(config-if)#load-interval 30`	Set the load interval to `30`.
`PE2(config-if)#access-if-evpn`	Enter the access mode for EVPN MPLS ID configuration.
`PE2(config-acc-if-evpn)#map vpn-id 1800`	Map VPN-ID `1800`.
`PE2(config-acc-if-evpn)#exit`	Exit the access mode and return to the interface mode.
`PE2(config-if)#exit`	Exit interface mode `po1.1` and return to the configure mode.
`PE2(config)#interface xe08`	Enter the interface mode for `xe8`.
`PE2(config-if)#speed 10g`	Set the speed to `10g`.

`PE2(config-if)#channel-group 1 mode active`	Attach LAG interface `po1`.
`PE2(config-if)#exit`	Exit interface mode `xe8` and return to the configure mode.
`PE2(config)#commit`	Commit the transaction.

PE2: Access Port Configuration for Single-active

The below access port configuration for single-active mode on PE2 is implemented to set up various parameters, including Ethernet Segment Identifier (ESI) settings, service carving preferences, and EVPN configurations, ensuring efficient network access and connectivity.

`PE2(config)#interface sa2`	Enter the single active interface mode for `sa2`.
`PE2(config-if)#load-interval 30`	Set the load interval to `30`.
`PE2(config-if)#evpn multi-homed esi 00:00:11:11:77:77 load-balancing single-active`	Configure the ESI with the value `00:00:11:11:77:77` for single-active mode, which plays a role in load balancing and enter to the EVPN Ethernet Segment (ES) mode.
`PE2(config-if-es)#service-carving auto`	Configure service carving as `auto`, allowing automatic determination of service distribution preferences.
`PE2(config-if-es)#exit`	Exit the EVPN ES mode and return to the configure mode.
`PE2(config-if)#exit`	Exit interface mode `sa2` and return to the configure mode.
`PE2(config)#commit`	Commit the transaction.
`PE2(config)#interface sa2.1 switchport`	Create a Layer 2 sub-interface `sa2.1` within the port channel.
`PE2(config-if)#encapsulation dot1q 100`	Set encapsulation to dot1q with VLAN ID `100`.
`PE2(config-if)#load-interval 30`	Set the load interval to `30`.
`PE2(config-if)#access-if-evpn`	Enter the access mode for EVPN MPLS ID configuration.
`PE2(config-acc-if-evpn)#map vpn-id 1800`	Map VPN-ID `1800`.
`PE2(config-acc-if-evpn)#exit`	Exit the access mode and return to the interface mode.
`PE2(config-if)#exit`	Exit interface mode `sa2.1` and return to the configure mode.
`PE2(config)#interface xe8`	Enter the interface mode for `xe8`.
`PE2(config-if)#speed 10g`	Set the speed to `10g`.
`PE2(config-if)#static-channel-group 2`	Attach the static-channel-group 2, the LAG interface `sa2` to `xe8`.
`PE2(config-if)#exit`	Exit interface mode `xe8` and return to the configure mode.
`PE2(config)#commit`	Commit the transaction.

P1: Loopback Interface

The configuration on P1 for a loopback interface with IP address `10.10.10.5/32` secondary is set up to provide IP connectivity for the router.

`P1#configure terminal`	Enter configure mode.
`P1(config)#interface lo`	Enter the interface mode for the loopback interface `lo`.
`P1(config-if)#ip address 10.10.10.5/32 secondary`	Configure a secondary IP address, `10.10.10.5/32`, on the loopback interface.
`P1(config-if)#exit`	Exit interface mode `lo`.
`P1(config)#commit`	Commit the transaction.

P1: Global LDP

The configuration on P1 for the Global LDP router, specifying router ID and targeted peer, is done to set up Label Distribution Protocol (LDP) settings for MPLS.

`P1(config)#router ldp`	Enter the Router LDP mode.
`P1(config-router)#router-id 10.10.10.5`	Set the router ID for LDP to `10.10.10.5`.
`P1(config-router)#transport-address ipv4 10.10.10.5`	Configure the transport address for IPv4 (for IPv6 use ipv6 parameter) to be used for a TCP session where LDP operates. Note: It is preferable to use the loopback address as the transport address.
`P1(config-router)#exit`	Exit router LDP mode and return to the configure mode.
`P1(config)#commit`	Commit the transaction.

P1: Interface Configuration

The below configuration is performed to set up interfaces on P1 and enable LDP for IPv4, ensuring proper routing and labeling functionality.

`P1(config)#interface xe1`	Enter interface mode `xe1`.
`P1(config-if)#ip address 10.1.1.2/30`	Configure an IP address, `10.1.1.2/30`, on the interface `xe1`.
`P1(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`P1(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`P1(config-if)#exit`	Exit interface mode `xe1`.
`P1(config)#commit`	Commit the transaction.
`P1(config)#interface xe2`	Enter interface mode `xe2`.
`P1(config-if)#ip address 10.1.4.2/30`	Configure an IP address, `10.1.4.2/30`, on the interface `xe2`.
`P1(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`P1(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`P1(config-if)#exit`	Exit interface mode `xe2`.
`P1(config)#commit`	Commit the transaction.
`P1(config)#interface xe3`	Enter interface mode `xe3`.
`P1(config-if)#ip address 10.1.5.2/30`	Configure an IP address, `10.1.5.2/30`, on the interface `xe3`.
`P1(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`P1(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`P1(config-if)#exit`	Exit interface mode `xe3`.

`P1(config)#commit`	Commit the transaction.
`P1(config)#interface xe4`	Enter interface mode `xe4`.
`P1(config-if)#ip address 10.1.6.2/30`	Configure an IP address, `10.1.6.2/30`, on the interface `xe4`.
`P1(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`P1(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`P1(config-if)#exit`	Exit interface mode `xe4`.
`P1(config)#commit`	Commit the transaction.

P1: OSPF Configuration

The below configuration is performed to set up OSPF on P1, specifying the router ID, and defining network interfaces for efficient routing.

`P1(config)#router ospf 100`	Enter the router OSPF mode. Configure P1 to run OSPF with process ID 100.
`P1(config-router)#ospf router-id 10.10.10.5`	Set the OSPF router ID to `10.10.10.5`, identifying P1 within the OSPF network.
`P1(config-router)#network 10.10.10.5/32 area 0.0.0.0`	Advertise loopback address in OSPF.
`P1(config-router)#network 10.1.1.2/30 area 0.0.0.0`	Advertise network address in OSPF.
`P1(config-router)#network 10.1.4.2/30 area 0.0.0.0`	Advertise network address in OSPF.
`P1(config-router)#network 10.1.5.2/30 area 0.0.0.0`	Advertise network address in OSPF.
`P1(config-router)#network 10.1.6.2/30 area 0.0.0.0`	Advertise network address in OSPF.
`P1(config-router)#exit`	Exit router OSPF mode and return to the configure mode.
`P1(config)#commit`	Commit the transaction.

P2: Loopback Interface

The configuration on P2 for a loopback interface with IP address `10.10.10.6/32` secondary is set up to provide IP connectivity for the router.

`P2#configure terminal`	Enter configure mode.
`P2(config)#interface lo`	Enter the interface mode for the loopback interface `lo`.
`P2(config-if)#ip address 10.10.10.6/32 secondary`	Configure a secondary IP address, `10.10.10.6/32`, on the loopback interface.
`P2(config-if)#exit`	Exit interface mode `lo`.
`P2(config)#commit`	Commit the transaction.

P2: Global LDP

The configuration on P2 for the Global LDP router, specifying router ID and targeted peer, is done to set up Label Distribution Protocol (LDP) settings for MPLS.

`P2(config)#router ldp`	Enter the Router LDP mode.
`P2(config-router)#router-id 10.10.10.6`	Set the router ID for LDP to `10.10.10.6`.
`P2(config-router)#transport-address ipv4 10.10.10.6`	Configure the transport address for IPv4 (for IPv6 use ipv6 parameter) to be used for a TCP session where LDP operates. Note: It is preferable to use the loopback address as the transport address.
`P2(config-router)#exit`	Exit router LDP mode and return to the configure mode.
`P2(config)#commit`	Commit the transaction.

P2: Interface Configuration

The below configuration is performed to set up interfaces on P2 and enable LDP for IPv4, ensuring proper routing and labeling functionality.

`P2(config)#interface xe12`	Enter interface mode `xe12`.
`P2(config-if)#ip address 10.1.2.2/30`	Configure an IP address, `10.1.2.2/30`, on the interface `xe12`.
`P2(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`P2(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`P2(config-if)#exit`	Exit interface mode `xe12`.
`P2(config)#commit`	Commit the transaction.
`P2(config)#interface xe13`	Enter interface mode `xe13`.
`P2(config-if)#ip address 10.1.3.2/30`	Configure an IP address, `10.1.3.2/30`, on the interface `xe13`.
`P2(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`P2(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`P2(config-if)#exit`	Exit interface mode `xe13`.
`P2(config)#commit`	Commit the transaction.
`P2(config)#interface xe11`	Enter interface mode `xe11`.
`P2(config-if)#ip address 10.1.7.2/30`	Configure an IP address, `10.1.7.2/30`, on the interface `xe11`.
`P2(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`P2(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`P2(config-if)#exit`	Exit interface mode `xe11`.

`P2(config)#commit`	Commit the transaction.
`P2(config)#interface xe14`	Enter interface mode `xe14`.
`P2(config-if)#ip address 10.1.8.2/30`	Configure an IP address, `10.1.8.2/30`, on the interface `xe14`.
`P2(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`P2(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`P2(config-if)#exit`	Exit interface mode `xe14`.
`P2(config)#commit`	Commit the transaction.

P2: OSPF Configuration

The below configuration is performed to set up OSPF on P2, specifying the router ID, and defining network interfaces for efficient routing.

`P2(config)#router ospf 100`	Enter the router OSPF mode. Configure P2 to run OSPF with process ID 100.
`P2(config-router)#ospf router-id 10.10.10.6`	Set the OSPF router ID to `10.10.10.6`, identifying P2 within the OSPF network.
`P2(config-router)#network 10.10.10.6/32 area 0.0.0.0`	Advertise loopback address in OSPF.
`P2(config-router)#network 10.1.2.2/30 area 0.0.0.0`	Advertise network address in OSPF.
`P2(config-router)#network 10.1.3.2/30 area 0.0.0.0`	Advertise network address in OSPF.
`P2(config-router)#network 10.1.7.2/30 area 0.0.0.0`	Advertise network address in OSPF.
`P2(config-router)#network 10.1.8.2/30 area 0.0.0.0`	Advertise network address in OSPF.
`P2(config-router)#exit`	Exit router OSPF mode and return to the configure mode.
`P2(config)#commit`	Commit the transaction.

PE3: Loopback Interface

The configuration on PE3 for a loopback interface with IP address `10.10.10.3/32` secondary is set up to provide IP connectivity for the router.

`PE3#configure terminal`	Enter configure mode.
`PE3(config)#interface lo`	Enter the interface mode for the loopback interface `lo`.
`PE3(config-if)#ip address 10.10.10.3/32 secondary`	Configure a secondary IP address, `10.10.10.3/32`, on the loopback interface.
`PE3(config-if)#exit`	Exit interface mode `lo`.
`PE3(config)#commit`	Commit the transaction.

PE3: Global LDP

The configuration on PE3 for the Global LDP router, specifying router ID and targeted peers, is done to set up Label Distribution Protocol (LDP) settings for MPLS.

`PE3(config)#router ldp`	Enter the Router LDP mode.
`PE3(config-router)#router-id 10.10.10.3`	Set the router ID for LDP to `10.10.10.3`.
`PE2(config-router)#transport-address ipv4 10.10.10.3`	Configure the transport address for IPv4 (for IPv6 use ipv6 parameter) to be used for a TCP session where LDP operates. Note: It is preferable to use the loopback address as the transport address.
`PE3(config-router)#targeted-peer ipv4 10.10.10.1`	Configure targeted peer for LDP using IPv4 addresses.
`PE3(config-router-targeted-peer)#exit-targeted-peer-mode`	Exit router targeted-peer-mode.
`PE3(config-router)#targeted-peer ipv4 10.10.10.2`	Configure targeted peer for LDP using IPv4 addresses.
`PE3(config-router-targeted-peer)#exit-targeted-peer-mode`	Exit router targeted-peer-mode.
`PE3(config-router)#targeted-peer ipv4 10.10.10.4`	Configure targeted peer for LDP using IPv4 addresses.
`PE3(config-router-targeted-peer)#exit-targeted-peer-mode`	Exit router targeted-peer-mode.
`PE3(config-router)#exit`	Exit router LDP mode and return to the configure mode.
`PE3(config)#commit`	Commit the transaction.

PE3: Global EVPN MPLS Command

The configuration on PE3 for the Global EVPN MPLS, includes activating EVPN MPLS, defining the global VTEP IP address, enabling hardware profile filtering for EVPN MPLS multi-homing, and activating EVPN MPLS multi-homing functionality, all of which are crucial for enabling EVPN MPLS features.

`PE3(config)#evpn mpls enable`	Activate the EVPN MPLS functionality on `PE3`, enabling it to participate in EVPN MPLS services.
`PE3(config)#commit`	Commit candidate configuration to be running configuration.
`PE3(config)#evpn mpls vtep-ip-global 10.10.10.3`	Configure the global VTEP IP address `10.10.10.3`, associating it with the loopback IP.
`PE3(config)#hardware-profile filter evpn-mpls-mh enable`	Enable hardware-profile filter for EVPN MPLS multi-homing.
`PE3(config)#evpn mpls multihoming enable`	Activate the EVPN MPLS multi-homing functionality, allowing `PE3` to support multi-homed EVPN MPLS services.
`PE3(config)#commit`	Commit the transaction.

PE3: Interface Configuration Network Side

The below configuration is performed to set up network interfaces on PE3 and enable LDP for IPv4, ensuring proper routing and labeling functionality.

`PE3(config)#interface xe1`	Enter interface mode `xe1`.
`PE3(config-if)#ip address 10.1.6.1/30`	Configure an IP address, `10.1.6.1/30`, on the interface `xe1`.
`PE3(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`PE3(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`PE3(config-if)#exit`	Exit interface mode `xe1`.
`PE3(config)#commit`	Commit the transaction.
`PE3(config)#interface xe5`	Enter interface mode `xe5`.
`PE3(config-if)#ip address 10.1.7.1/30`	Configure an IP address, `10.1.7.1/30`, on the interface `xe5`.
`PE3(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`PE3(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`PE3(config-if)#exit`	Exit interface mode `xe5`.
`PE3(config)#commit`	Commit the transaction.

PE3: OSPF Configuration

The below configuration is performed to set up OSPF on PE3, specifying the router ID, defining network interfaces, and configuring BFD parameters for efficient routing.

`PE3(config)#router ospf 100`	Enter the router OSPF mode. Configure PE3 to run OSPF with process ID 100.
`PE3(config-router)#ospf router-id 10.10.10.3`	Set the OSPF router ID to `10.10.10.3`, identifying PE3 within the OSPF network.
`PE3(config-router)#network 10.10.10.3/32 area 0.0.0.0`	Advertise loopback address in OSPF.
`PE3(config-router)#network 10.1.6.1/32 area 0.0.0.0`	Advertise loopback address in OSPF.
`PE3(config-router)#network 10.1.7.1/30 area 0.0.0.0`	Advertise network address in OSPF.
`PE3(config-router)#bfd interval 3 minrx 3 multiplier 3`	Configure BFD interval with an interval of `3`, a minimum receive interval of `3`, and a multiplier of `3`.
`PE3(config-router)#exit`	Exit router OSPF mode and return to the configure mode.
`PE3(config)#commit`	Commit the transaction.

PE3: BGP Configuration

The below BGP configuration on PE3 is established to enable BGP routing with ASN 65010, set the BGP router ID, define iBGP neighbors, configure BFD, and enable the EVPN address family for efficient routing in an EVPN environment.

`PE3(config)#router bgp 65010`	Enter the Router BGP mode, ASN: 65010
`PE3(config-router)#bgp router-id 10.10.10.3`	Configure BGP router ID `10.10.10.2`, identifying PE3 within the BGP network.
`PE3(config-router)#neighbor 10.10.10.1 remote-as 65010`	Configure neighbor `10.10.10.1` as an iBGP neighbor with their remote AS number `65010`.
`PE3(config-router)#neighbor 10.10.10.1 update-source lo`	Configure neighbor `10.10.10.1` as an iBGP neighbor, specifying the source of routing updates as the loopback interface.
`PE3(config-router)#neighbor 10.10.10.2 remote-as 65010`	Configure neighbor `10.10.10.2` as an iBGP neighbor with their remote AS number `65010`.
`PE3(config-router)#neighbor 10.10.10.2 update-source lo`	Configure neighbor `10.10.10.2` as an iBGP neighbor, specifying the source of routing updates as the loopback interface.
`PE3(config-router)#neighbor 10.10.10.4 remote-as 65010`	Configure neighbor `10.10.10.4` as an iBGP neighbor with their remote AS number `65010`.
`PE3(config-router)#neighbor 10.10.10.4 update-source lo`	Configure neighbor `10.10.10.4` as an iBGP neighbor, specifying the source of routing updates as the loopback interface.
`PE3(config-router)#neighbor 10.10.10.1 fall-over bfd multihop`	Configure BFD for the BGP neighbor to provide rapid failure detection.
`PE3(config-router)#neighbor 10.10.10.2 fall-over bfd multihop`	Configure BFD for the BGP neighbor to provide rapid failure detection.
`PE3(config-router)#neighbor 10.10.10.4 fall-over bfd multihop`	Configure BFD for the BGP neighbor to provide rapid failure detection.
`PE3(config-router)#neighbor 10.10.10.1 advertisement-interval 0`	Configure advertisement interval for the neighbor, allowing more frequent BGP updates.
`PE3(config-router)#neighbor 10.10.10.2 advertisement-interval 0`	Configure advertisement interval for the neighbor, allowing more frequent BGP updates.
`PE3(config-router)#neighbor 10.10.10.4 advertisement-interval 0`	Configure advertisement interval for the neighbor, allowing more frequent BGP updates.
`PE3(config-router)#address-family l2vpn evpn`	Enter into address family mode for L2VPN EVPN.
`PE3(config-router-af)#neighbor 10.10.10.1 activate`	Activate EVPN for iBGP neighbor `10.10.10.1` within the address family mode, ensuring that EVPN address family is enabled for the neighbor.
`PE3(config-router-af)#neighbor 10.10.10.2 activate`	Activate EVPN for iBGP neighbor `10.10.10.2` within the address family mode, ensuring that EVPN address family is enabled for the neighbor.
`PE3(config-router-af)#neighbor 10.10.10.4 activate`	Activate EVPN for iBGP neighbor `10.10.10.4` within the address family mode, ensuring that EVPN address family is enabled for the neighbor.
`PE3(config-router-af)#exit`	Exit address family mode and return to the router BGP mode.
`PE3(config-router)#commit`	Commit the transaction.
`PE3(config-router)#exit`	Exit router BGP mode and return to the configure mode.

PE3: MAC VRF Configuration

The below MAC VRF configuration on PE3 is carried out to define and set up VRFs named `vrf2` and `vpls1001` with specific Route-Distinguisher (RD) and route-target values, ensuring segregated MAC address spaces for distinct network services.

`PE3(config)#mac vrf vrf2`	Enter VRF mode named `vrf2`.
`PE3(config-vrf)#rd 10.10.10.3:1700`	Configure Route-Distinguisher value of `10.10.10.3:1700`.
`PE3(config-vrf)#route-target both 1700:1700`	Configure import and export values for the `vrf2` as `1700:1700`.
`PE3(config-vrf)#exit`	Exit VRF mode and return to the configure mode.
`PE3(config)#mac vrf vpls1001`	Enter VRF mode named `vpls1001`.
`PE3(config-vrf)#rd 10.10.10.3:1001`	Configure Route-Distinguisher value of `10.10.10.3:1001`.
`PE3(config-vrf)#route-target both 1001:1001`	Configure import and export values for the `vpls1001` as `1001:1001`.
`PE3(config-vrf)#exit`	Exit VRF mode and return to the configure mode.
`PE3(config)#commit`	Commit the transaction.

PE3: EVPN and VRF Mapping

The below EVPN and VRF mapping configuration on PE3 is performed to establish mappings between EVPN identifiers and VRFs, facilitating efficient routing and connectivity in an EVPN network environment.

`PE3(config)#evpn mpls id 1700 xconnect target-mpls-id 1800`	Configure the EVPN-VPWS identifier with a source identifier of `1700` and a target identifier of `1800`.
`PE3(config-evpn-mpls)#host-reachability-protocol evpn-bgp vrf2`	Map VRF `vrf2` to the EVPN-VPWS identifier
`PE3(config-evpn-mpls)#evpn mpls id 3000`	Configure the EVPN-VPLS identifier an identifier of `3000`.
`PE3(config-evpn-mpls)#host-reachability-protocol evpn-bgp vpls1001`	Map VRF `vpls1001` to the EVPN-VPWS identifier
`PE3(config-evpn-mpls)#commit`	Commit the transaction.
`PE3(config-evpn-mpls)#exit`	Exit the EVPN MPLS mode and return to the configure mode.

PE3: Access Port Configuration for Port-active

The below access port configuration for port-active mode on PE3 is carried out to configure various parameters including system-MAC, load balancing, service carving preferences, and EVPN settings for efficient network access and connectivity.

`PE3(config)#interface po1`	Enter the port channel interface mode for `po1`
`PE3(config-if)#load-interval 30`	Set the load interval to `30`.
`PE3(config-if)#evpn multi-homed system-mac 0000.2222.7777 load-balancing port-active`	Configure the system-mac address `0000.2222.7777` for port-active mode, which plays a role in load balancing and enter to the EVPN Ethernet Segment (ES) mode.
`PE3(config-if-es)#service-carving auto`	Configure service carving as `auto`, allowing automatic determination of service distribution preferences.
`PE3(config-if-es)#exit`	Exit the EVPN ES mode and return to the configure mode.
`PE3(config-if)#exit`	Exit interface mode `po1` and return to the configure mode.
`PE3(config)#commit`	Commit the transaction.

`PE3(config)#interface po1.1 switchport`	Create a Layer 2 sub-interface `po1.1` within the port channel.
`PE3(config-if)#encapsulation dot1q 100`	Set encapsulation to dot1q with VLAN ID `100`.
`PE3(config-if)#load-interval 30`	Set the load interval to `30`.
`PE3(config-if)#access-if-evpn`	Enter the access mode for EVPN MPLS ID configuration.
`PE3(config-acc-if-evpn)#map vpn-id 1800`	Map VPN-ID `1800`.
`PE3(config-acc-if-evpn)#exit`	Exit the access mode and return to the interface mode.
`PE3(config-if)#exit`	Exit interface mode `po1.1` and return to the configure mode.
`PE3(config)#interface xe2`	Enter the interface mode for `xe2`.
`PE3(config-if)#speed 10g`	Set the speed to `10g`.
`PE3(config-if)#channel-group 1 mode active`	Attach LAG interface `po1`.
`PE3(config-if)#exit`	Exit interface mode `xe2` and return to the configure mode.
`PE3(config)#commit`	Commit the transaction.

PE3: Access Port Configuration for Single-active

The below access port configuration for single-active mode on PE3 is implemented to set up various parameters, including Ethernet Segment Identifier (ESI) settings, service carving preferences, and EVPN configurations, ensuring efficient network access and connectivity.

`PE3(config)#interface sa1`	Enter the single active interface mode for `sa1`.
`PE3(config-if)#load-interval 30`	Set the load interval to `30`.
`PE3(config-if)#evpn multi-homed esi 00:00:22:22:77:77 load-balancing single-active`	Configure the ESI with the value with the value `00:00:22:22:77:77` for single-active mode, which plays a role in load balancing and enter to the EVPN Ethernet Segment (ES) mode.
`PE3(config-if-es)#service-carving auto`	Configure service carving as `auto`, allowing automatic determination of service distribution preferences.
`PE3(config-if-es)#exit`	Exit the EVPN ES mode and return to the configure mode.
`PE3(config-if)#exit`	Exit interface mode `sa1` and return to the configure mode.
`PE3(config)#commit`	Commit the transaction.
`PE3(config)#interface sa1.1 switchport`	Create a Layer 2 sub-interface `sa1.1` within the port channel.
`PE3(config-if)#encapsulation dot1q 100`	Set encapsulation to dot1q with VLAN ID `100`.
`PE3(config-if)#load-interval 30`	Set the load interval to `30`.
`PE3(config-if)#access-if-evpn`	Enter the access mode for EVPN MPLS ID configuration.
`PE3(config-acc-if-evpn)#map vpn-id 1800`	Map VPN-ID `1800`.
`PE3(config-acc-if-evpn)#exit`	Exit the access mode and return to the interface mode.
`PE3(config-if)#exit`	Exit interface mode `sa1.1` and return to the configure mode.
`PE3(config)#interface xe2`	Enter the interface mode for `xe2`.
`PE3(config-if)#speed 10g`	Set the speed to `10g`.
`PE3(config-if)#static-channel-group 1`	Attach the static-channel-group 1, the LAG interface `sa1` to `xe2`.

`PE3(config-if)#exit`	Exit interface mode `xe2` and return to the configure mode.
`PE3(config)#commit`	Commit the transaction.

PE4: Loopback Interface

The configuration on PE4 for a loopback interface with IP address `10.10.10.4/32` secondary is set up to provide IP connectivity for the router.

`PE4#configure terminal`	Enter configure mode.
`PE4(config)#interface lo`	Enter the interface mode for the loopback interface `lo`.
`PE4(config-if)#ip address 10.10.10.4/32 secondary`	Configure a secondary IP address, `10.10.10.4/32`, on the loopback interface.
`PE4(config-if)#exit`	Exit interface mode `lo`.
`PE4(config)#commit`	Commit the transaction.

PE4: Global LDP

The configuration on PE4 for the Global LDP router, specifying router ID and targeted peers, is done to set up Label Distribution Protocol (LDP) settings for MPLS.

`PE4(config)#router ldp`	Enter the Router LDP mode.
`PE4(config-router)#router-id 10.10.10.4`	Set the router ID for LDP to `10.10.10.4`.
`PE4(config-router)#transport-address ipv4 10.10.10.4`	Configure the transport address for IPv4 (for IPv6 use ipv6 parameter) to be used for a TCP session where LDP operates. Note: It is preferable to use the loopback address as the transport address.
`PE4(config-router)#targeted-peer ipv4 10.10.10.1`	Configure targeted peer for LDP using IPv4 addresses.
`PE4(config-router-targeted-peer)#exit-targeted-peer-mode`	Exit router targeted-peer-mode.
`PE4(config-router)#targeted-peer ipv4 10.10.10.2`	Configure targeted peer for LDP using IPv4 addresses.
`PE4(config-router-targeted-peer)#exit-targeted-peer-mode`	Exit router targeted-peer-mode.
`PE4(config-router)#targeted-peer ipv4 10.10.10.3`	Configure targeted peer for LDP using IPv4 addresses.
`PE4(config-router-targeted-peer)#exit-targeted-peer-mode`	Exit router targeted-peer-mode.
`PE4(config-router)#exit`	Exit router LDP mode and return to the configure mode.
`PE4(config)#commit`	Commit the transaction.

PE4: Global EVPN MPLS Command

The configuration on PE4 for the Global EVPN MPLS, includes activating EVPN MPLS, defining the global VTEP IP address, enabling hardware profile filtering for EVPN MPLS multi-homing, and activating EVPN MPLS multi-homing functionality, all of which are crucial for enabling EVPN MPLS features.

`PE4(config)#evpn mpls enable`	Activate the EVPN MPLS functionality on `PE4`, enabling it to participate in EVPN MPLS services.
`PE4(config)#commit`	Commit candidate configuration to be running configuration.
`PE4(config)#evpn mpls vtep-ip-global 10.10.10.4`	Configure the global VTEP IP address `10.10.10.4`, associating it with the loopback IP.
`PE4(config)#hardware-profile filter evpn-mpls-mh enable`	Enable hardware-profile filter for EVPN MPLS multi-homing.
`PE4(config)#evpn mpls multihoming enable`	Activate the EVPN MPLS multi-homing functionality, allowing `PE4` to support multi-homed EVPN MPLS services.
`PE4(config)#commit`	Commit the transaction.

PE4: Interface Configuration Network Side

The below configuration is performed to set up network interfaces on PE4 and enable LDP for IPv4, ensuring proper routing and labeling functionality.

`PE4(config)#interface xe2`	Enter interface mode `xe2`.
`PE4(config-if)#ip address 10.1.5.1/30`	Configure an IP address, `10.1.5.1/30`, on the interface `xe2`.
`PE4(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`PE4(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`PE4(config-if)#exit`	Exit interface mode `xe2`.
`PE4(config)#commit`	Commit the transaction.
`PE4(config)#interface xe0`	Enter interface mode `xe0`.
`PE4(config-if)#ip address 10.1.8.1/30`	Configure an IP address, `10.1.8.1/30`, on the interface `xe0`.
`PE4(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`PE4(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`PE4(config-if)#exit`	Exit interface mode `xe0`.
`PE4(config)#commit`	Commit the transaction.

PE4: OSPF Configuration

The below configuration is performed to set up OSPF on PE4, specifying the router ID, defining network interfaces, and configuring BFD parameters for efficient routing.

`PE4(config)#router ospf 100`	Enter the router OSPF mode. Configure PE4 to run OSPF with process ID 100.
`PE4(config-router)#ospf router-id 10.10.10.4`	Set the OSPF router ID to `10.10.10.4`, identifying PE3 within the OSPF network.
`PE4(config-router)#network 10.10.10.4/32 area 0.0.0.0`	Advertise loopback address in OSPF.

`PE4(config-router)#network 10.1.5.1/32 area 0.0.0.0`	Advertise loopback address in OSPF.
`PE4(config-router)#network 10.1.8.1/30 area 0.0.0.0`	Advertise network address in OSPF.
`PE4(config-router)#bfd interval 3 minrx 3 multiplier 3`	Configure BFD interval with an interval of `3`, a minimum receive interval of `3`, and a multiplier of `3`.
`PE4(config-router)#exit`	Exit router OSPF mode and return to the configure mode.
`PE4(config)#commit`	Commit the transaction.

PE4: BGP Configuration

The below BGP configuration on PE4 is established to enable BGP routing with ASN 65010, set the BGP router ID, define iBGP neighbors, configure BFD, and enable the EVPN address family for efficient routing in an EVPN environment.

`PE4(config)#router bgp 65010`	Enter the Router BGP mode, ASN: 65010
`PE4(config-router)#bgp router-id 10.10.10.4`	Configure BGP router ID `10.10.10.4`, identifying PE4 within the BGP network.
`PE4(config-router)#neighbor 10.10.10.1 remote-as 65010`	Configure neighbor `10.10.10.1` as an iBGP neighbor with their remote AS number `65010`.
`PE4(config-router)#neighbor 10.10.10.1 update-source lo`	Configure neighbor `10.10.10.1` as an iBGP neighbor, specifying the source of routing updates as the loopback interface.
`PE4(config-router)#neighbor 10.10.10.2 remote-as 65010`	Configure neighbor `10.10.10.2` as an iBGP neighbor with their remote AS number `65010`.
`PE4(config-router)#neighbor 10.10.10.2 update-source lo`	Configure neighbor `10.10.10.2` as an iBGP neighbor, specifying the source of routing updates as the loopback interface.
`PE4(config-router)#neighbor 10.10.10.3 remote-as 65010`	Configure neighbor `10.10.10.3` as an iBGP neighbor with their remote AS number `65010`.
`PE4(config-router)#neighbor 10.10.10.3 update-source lo`	Configure neighbor `10.10.10.3` as an iBGP neighbor, specifying the source of routing updates as the loopback interface.
`PE4(config-router)#neighbor 10.10.10.1 fall-over bfd multihop`	Configure BFD for the BGP neighbor to provide rapid failure detection.
`PE4(config-router)#neighbor 10.10.10.2 fall-over bfd multihop`	Configure BFD for the BGP neighbor to provide rapid failure detection.
`PE4(config-router)#neighbor 10.10.10.3 fall-over bfd multihop`	Configure BFD for the BGP neighbor to provide rapid failure detection.
`PE4(config-router)#neighbor 10.10.10.1 advertisement-interval 0`	Configure advertisement interval for the neighbor, allowing more frequent BGP updates.
`PE4(config-router)#neighbor 10.10.10.2 advertisement-interval 0`	Configure advertisement interval for the neighbor, allowing more frequent BGP updates.
`PE4(config-router)#neighbor 10.10.10.3 advertisement-interval 0`	Configure advertisement interval for the neighbor, allowing more frequent BGP updates.
`PE4(config-router)#address-family l2vpn evpn`	Enter into address family mode for L2VPN EVPN.
`PE4(config-router-af)#neighbor 10.10.10.1 activate`	Activate EVPN for iBGP neighbor `10.10.10.1` within the address family mode, ensuring that EVPN address family is enabled for the neighbor.

`PE4(config-router-af)#neighbor 10.10.10.2 activate`	Activate EVPN for iBGP neighbor `10.10.10.2` within the address family mode, ensuring that EVPN address family is enabled for the neighbor.
`PE4(config-router-af)#neighbor 10.10.10.3 activate`	Activate EVPN for iBGP neighbor `10.10.10.3` within the address family mode, ensuring that EVPN address family is enabled for the neighbor.
`PE4(config-router-af)#exit`	Exit address family mode and return to the router BGP mode.
`PE4(config-router)#commit`	Commit the transaction.
`PE4(config-router)#exit`	Exit router BGP mode and return to the configure mode.

PE4: MAC VRF Configuration

The below MAC VRF configuration on PE4 is carried out to define and set up VRFs named `vrf2` and `vpls1001` with specific Route-Distinguisher (RD) and route-target values, ensuring segregated MAC address spaces for distinct network services.

`PE4(config)#mac vrf vrf2`	Enter VRF mode named `vrf2`.
`PE4(config-vrf)#rd 10.10.10.4:1700`	Configure Route-Distinguisher value of `10.10.10.4:1700`.
`PE4(config-vrf)#route-target both 1700:1700`	Configure import and export values for the `vrf2` as `1700:1700`.
`PE4(config-vrf)#exit`	Exit VRF mode and return to the configure mode.
`PE4(config)#mac vrf vpls1001`	Enter VRF mode named `vpls1001`.
`PE4(config-vrf)#rd 10.10.10.4:1001`	Configure Route-Distinguisher value of `10.10.10.4:1001`.
`PE4(config-vrf)#route-target both 1001:1001`	Configure import and export values for the `vpls1001` as `1001:1001`.
`PE4(config-vrf)#exit`	Exit VRF mode and return to the configure mode.
`PE4(config)#commit`	Commit the transaction.

PE4: EVPN and VRF Mapping

The below EVPN and VRF mapping configuration on PE4 is performed to establish mappings between EVPN identifiers and VRFs, facilitating efficient routing and connectivity in an EVPN network environment.

`PE4(config)#evpn mpls id 1700 xconnect target-mpls-id 1800`	Configure the EVPN-VPWS identifier with a source identifier of `1700` and a target identifier of `1800`.
`PE4(config-evpn-mpls)#host-reachability-protocol evpn-bgp vrf2`	Map VRF `vrf2` to the EVPN-VPWS identifier
`PE4(config-evpn-mpls)#evpn mpls id 3000`	Configure the EVPN-VPLS identifier an identifier of `3000`.
`PE4(config-evpn-mpls)#host-reachability-protocol evpn-bgp vpls1001`	Map VRF `vpls1001` to the EVPN-VPWS identifier
`PE4(config-evpn-mpls)#commit`	Commit the transaction.
`PE4(config-evpn-mpls)#exit`	Exit the EVPN MPLS mode and return to the configure mode.

PE4: Access Port Configuration for Port-active

The below access port configuration for port-active mode on PE4 is carried out to configure various parameters including system-MAC, load balancing, service carving preferences, and EVPN settings for efficient network access and connectivity.

`PE4(config)#interface po1`	Enter the port channel interface mode for `po1`
`PE4(config-if)#load-interval 30`	Set the load interval to `30`.
`PE4(config-if)#evpn multi-homed system-mac 0000.2222.7777 load-balancing port-active`	Configure the system-mac address `0000.2222.7777` for port-active mode, which plays a role in load balancing and enter to the EVPN Ethernet Segment (ES) mode.
`PE4(config-if-es)#service-carving auto`	Configure service carving as `auto`, allowing automatic determination of service distribution preferences.
`PE4(config-if-es)#exit`	Exit the EVPN ES mode and return to the configure mode.
`PE4(config-if)#exit`	Exit interface mode `po1` and return to the configure mode.
`PE4(config)#commit`	Commit the transaction.
`PE4(config)#interface po1.1 switchport`	Create a Layer 2 sub-interface `po1.1` within the port channel.
`PE4(config-if)#encapsulation dot1q 100`	Set encapsulation to dot1q with VLAN ID `100`.
`PE4(config-if)#load-interval 30`	Set the load interval to `30`.
`PE4(config-if)#access-if-evpn`	Enter the access mode for EVPN MPLS ID configuration.
`PE4(config-acc-if-evpn)#map vpn-id 1800`	Map VPN-ID `1800`.
`PE4(config-acc-if-evpn)#exit`	Exit the access mode and return to the interface mode.
`PE4(config-if)#exit`	Exit interface mode `po1.1` and return to the configure mode.
`PE4(config)#interface xe11`	Enter the interface mode for `xe11.`
`PE4(config-if)#speed 10g`	Set the speed to `10g`.
`PE4(config-if)#channel-group 1 mode active`	Attach LAG interface `po1.`
`PE4(config-if)#exit`	Exit interface mode `xe11` and return to the configure mode.
`PE4(config)#commit`	Commit the transaction.

PE4: Access Port Configuration for Single-active

The below access port configuration for single-active mode on PE4 is implemented to set up various parameters, including Ethernet Segment Identifier (ESI) settings, service carving preferences, and EVPN configurations, ensuring efficient network access and connectivity.

`PE4(config)#interface sa2`	Enter the single active interface mode for `sa2.`
`PE4(config-if)#load-interval 30`	Set the load interval to `30`.
`PE4(config-if)#evpn multi-homed esi 00:00:22:22:77:77 load-balancing single-active`	Configure the ESI with the value with the value `00:00:22:22:77:77` for single-active mode, which plays a role in load balancing and enter to the EVPN Ethernet Segment (ES) mode.
`PE4(config-if-es)#service-carving auto`	Configure service carving as `auto`, allowing automatic determination of service distribution preferences.
`PE4(config-if-es)#exit`	Exit the EVPN ES mode and return to the configure mode.
`PE4(config-if)#exit`	Exit interface mode `sa2` and return to the configure mode.

`PE4(config)#commit`	Commit the transaction.
`PE4(config)#interface sa2.1 switchport`	Create a Layer 2 sub-interface `sa2.1` within the port channel.
`PE4(config-if)#encapsulation dot1q 100`	Set encapsulation to dot1q with VLAN ID `100`.
`PE4(config-if)#load-interval 30`	Set the load interval to `30`.
`PE4(config-if)#access-if-evpn`	Enter the access mode for EVPN MPLS ID configuration.
`PE4(config-acc-if-evpn)#map vpn-id 1800`	Map VPN-ID `1800`.
`PE4(config-acc-if-evpn)#exit`	Exit the access mode and return to the interface mode.
`PE4(config-if)#exit`	Exit interface mode `sa2.1` and return to the configure mode.
`PE4(config)#interface xe11`	Enter the interface mode for `xe11.`
`PE4(config-if)#speed 10g`	Set the speed to `10g`.
`PE4(config-if)#static-channel-group 2`	Attach the static-channel-group 2, the LAG interface `sa2` to `xe11`.
`PE4(config-if)#exit`	Exit interface mode `xe11` and return to the configure mode.
`PE4(config)#commit`	Commit the transaction.

CE2

The following configuration steps under CE2 are set up to enable VLANs and configure interfaces for carrying VLAN traffic.

`CE2#configure terminal`	Enter configure mode.
`CE2(config)#bridge 1 protocol ieee vlan-bridge`	Set up `bridge 1` to use the IEEE VLAN bridge protocol.
`CE2(config)#vlan 2-100 bridge 1 state enable`	Configure VLANs from `2-100` and associate them with bridge 1.
`CE2(config)#interface xe24`	Enter interface mode `xe24`.
`CE2(config-if)#switchport`	Configure the interface `xe24` as a Layer 2 switch port.
`CE2(config-if)#bridge-group 1`	Associate `xe24` to bridge 1.
`CE2(config-if)#switchport mode trunk`	Configure `xe24` as a trunk port.
`CE2(config-if)#switchport trunk allowed vlan all`	Allow all configured VLANs on the trunk interface `xe24`.
`CE2(config-if)#exit`	Exit interface mode `xe24`.
`CE2(config)#interface po1`	Enter interface mode and configure LAG interface port-channel 1 (`po1`).
`CE2(config-if)#switchport`	Configures port-channel 1 as a Layer 2 switch port.
`CE2(config-if)#bridge-group 1`	Associate `po1` to bridge 1.
`CE2(config-if)#switchport mode trunk`	Configure `po1` as a trunk port.
`CE2(config-if)#switchport trunk allowed vlan all`	Allow all configured VLANs on the trunk port-channel `po1`.
`CE2(config-if)#exit`	Exit interface mode `po1`.
`CE2(config)#interface xe22`	Enter interface mode `xe22`.
`CE2(config-if)#lacp timeout short`	Configure LACP timeout as `short`.
`CE2(config-if)#channel-group 1 mode active`	Add member to the LAG interface.

`CE2(config-if)#exit`	Exit interface mode `xe22`.
`CE2(config-if)#interface xe23`	Enter interface mode `xe23`.
`CE2(config-if)#lacp timeout short`	Configure LACP timeout as `short`.
`CE2(config-if)#channel-group 1 mode active`	Add member to the LAG interface.
`CE2(config-if)#commit`	Commit the transaction.
`CE2(config-if)#end`	Exit interface mode `xe23` and configure mode.

EVPN MPLS Active-Standby MH Validation

The following show outputs provide validation results for both single-active and port-active modes, covering ELINE and ELAN services configurations with LDP as the underlay MPLS path.

Single-Active

The following show output displays the types of load-balancing port selection criteria (PSC) used on configured static aggregators for CE1, PE1, PE2, PE3, PE4, and CE2 devices in the network Figure 1 using the **show static-channel-group** command.

```
CE1#show static-channel-group
 Static Aggregator: sa1
 Member Status
  xe48   up
----------------------------------------
 Static Aggregator: sa2
 Member Status
  xe50   up

PE1#show static-channel-group
 Static Aggregator: sa1
 Member Status  weight
  xe0    up

PE2#show static-channel-group
 Static Aggregator: sa2
 Member Status  weight
  xe8    up

PE3#show static-channel-group
 Static Aggregator: sa1
 Member Status  weight
  xe2    up
PE4#show static-channel-group
 Static Aggregator: sa2
 Member Status  weight
  xe11   up

CE2#show static-channel-group
 Static Aggregator: sa1
 Member Status  weight
  xe23   up
----------------------------------------
 Static Aggregator: sa2
 Member Status  weight
  ge11   up
```

Single-Active ELINE

The following show output displays the active EVPN MPLS Tunnels and load balance for ELINE on PE1, PE2, PE3, and PE4 devices in the network Figure 1 using the **show evpn load-balance all** and **show evpn mpls xconnect tunnel** commands.

```
PE1#show evpn load-balance all
ESI                         AC-IF/PE     PE-IP-ADDRESS    Redundancy        Service-carving    weight   Revertive  AC-DF
Status
```

```
================================================================================================================================
=========
00:11:22:33:00:00:00:55:66:77  sa1.1        10.10.10.1       single-active      auto               0        NO           NO
ACTIVE
00:11:22:33:00:00:00:55:66:77  ----         10.10.10.2       single-active      auto               0        NO           NO
----

PE1#show evpn mpls xconnect tunnel
EVPN-MPLS Network tunnel Entries
Source           Destination      Status        Up/Down       Update        local-evpn-id remote-evpn-id
================================================================================================
10.10.10.1       10.10.10.4       Installed     00:14:05      00:03:58      1800          1700
10.10.10.1       10.10.10.3       Installed     00:14:05      00:04:29      1800          1700

Total number of entries are 2

PE2#show evpn load-balance all
ESI                           AC-IF/PE     PE-IP-ADDRESS    Redundancy         Service-carving    weight   Revertive  AC-DF
Status
================================================================================================================================
=========
00:11:22:33:00:00:00:55:66:77  ----         10.10.10.1       single-active      auto               0        NO           NO
----
00:11:22:33:00:00:00:55:66:77  sa2.1        10.10.10.2       single-active      auto               0        NO           NO
STANDBY
ELINE
PE2#show evpn mpls xconnect tunnel
EVPN-MPLS Network tunnel Entries
Source           Destination      Status        Up/Down       Update        local-evpn-id remote-evpn-id
================================================================================================
10.10.10.2       10.10.10.4       Installed     00:12:33      00:04:08      1800          1700
10.10.10.2       10.10.10.3       Installed     00:12:33      00:04:08      1800          1700

Total number of entries are 2

PE3#show evpn load-balance all
ESI                           AC-IF/PE     PE-IP-ADDRESS    Redundancy         Service-carving    weight   Revertive  AC-DF
Status
================================================================================================================================
=========
00:12:22:33:00:00:00:55:66:77  sa1.1        10.10.10.3       single-active      auto               0        NO           NO
ACTIVE
00:12:22:33:00:00:00:55:66:77  ----         10.10.10.4       single-active      auto               0        NO           NO
----

PE3#show evpn mpls xconnect tunnel
EVPN-MPLS Network tunnel Entries
Source           Destination      Status        Up/Down       Update        local-evpn-id remote-evpn-id
================================================================================================
10.10.10.3       10.10.10.2       Installed     00:13:15      00:04:12      1700          1800
10.10.10.3       10.10.10.1       Installed     00:13:15      00:04:44      1700          1800

Total number of entries are 2

PE4#show evpn load-balance all
ESI                           AC-IF/PE     PE-IP-ADDRESS    Redundancy         Service-carving    weight   Revertive  AC-DF
Status
================================================================================================================================
=========
00:12:22:33:00:00:00:55:66:77  ----         10.10.10.3       single-active      auto               0        NO           NO
----
00:12:22:33:00:00:00:55:66:77  sa2.1        10.10.10.4       single-active      auto               0        NO           NO
STANDBY

PE4#show evpn mpls xconnect tunnel
EVPN-MPLS Network tunnel Entries
Source           Destination      Status        Up/Down       Update        local-evpn-id remote-evpn-id
================================================================================================
10.10.10.4       10.10.10.2       Installed     00:12:52      00:04:17      1700          1800
10.10.10.4       10.10.10.1       Installed     00:12:52      00:04:17      1700          1800

Total number of entries are 2
```

Single-Active ELAN

The following show output displays the active EVPN SR Tunnels and load balance for ELAN on PE1, PE2, PE3, and PE4 devices in the network Figure 1 using the **show evpn mpls tunnel** and **show evpn load-balance all** commands.

```
PE1#show evpn mpls tunnel
EVPN-MPLS Network tunnel Entries
Source            Destination      Status        Up/Down       Update        evpn-id
================================================================================
10.10.10.1        10.10.10.2       Installed     00:17:00      00:17:00      3000
10.10.10.1        10.10.10.4       Installed     00:18:10      00:18:10      3000
10.10.10.1        10.10.10.3       Installed     00:18:10      00:18:10      3000

Total number of entries are 3

PE1#show evpn load-balance all
ESI                          AC-IF/PE     PE-IP-ADDRESS    Redundancy         Service-carving    weight   Revertive  AC-DF
Status
=============================================================================================================================
=========
00:11:22:33:00:00:00:55:66:77  sa1.1        10.10.10.1       single-active      auto               0        NO           NO
ACTIVE
00:11:22:33:00:00:00:55:66:77  ----         10.10.10.2       single-active      auto               0        NO           NO
----



PE2#show evpn mpls tunnel
EVPN-MPLS Network tunnel Entries
Source            Destination      Status        Up/Down       Update        evpn-id
================================================================================
10.10.10.2        10.10.10.4       Installed     00:17:09      00:17:09      3000
10.10.10.2        10.10.10.3       Installed     00:17:09      00:17:09      3000
10.10.10.2        10.10.10.1       Installed     00:17:09      00:17:09      3000

Total number of entries are 3

PE2#show evpn load-balance all
ESI                          AC-IF/PE     PE-IP-ADDRESS    Redundancy         Service-carving    weight   Revertive  AC-DF
Status
=============================================================================================================================
=========
00:11:22:33:00:00:00:55:66:77  ----         10.10.10.1       single-active      auto               0        NO           NO
----
00:11:22:33:00:00:00:55:66:77  sa2.1        10.10.10.2       single-active      auto               0        NO           NO
STANDBY

PE3#show evpn mpls tunnel
EVPN-MPLS Network tunnel Entries
Source            Destination      Status        Up/Down       Update        evpn-id
================================================================================
10.10.10.3        10.10.10.2       Installed     00:17:11      00:17:11      3000
10.10.10.3        10.10.10.1       Installed     00:18:21      00:18:21      3000
10.10.10.3        10.10.10.4       Installed     00:29:15      00:28:54      3000

Total number of entries are 3

PE3#show evpn load-balance all
ESI                          AC-IF/PE     PE-IP-ADDRESS    Redundancy         Service-carving    weight   Revertive  AC-DF
Status
=============================================================================================================================
=========
00:12:22:33:00:00:00:55:66:77  sa1.1        10.10.10.3       single-active      auto               0        NO           NO
ACTIVE
00:12:22:33:00:00:00:55:66:77  ----         10.10.10.4       single-active      auto               0        NO           NO
----

PE4#show evpn mpls tunnel
EVPN-MPLS Network tunnel Entries
Source            Destination      Status        Up/Down       Update        evpn-id
================================================================================
10.10.10.4        10.10.10.2       Installed     00:17:13      00:17:13      3000
10.10.10.4        10.10.10.1       Installed     00:18:23      00:18:23      3000
10.10.10.4        10.10.10.3       Installed     00:29:18      00:29:14      3000
```

```
Total number of entries are 3

PE4#show evpn load-balance all
ESI                          AC-IF/PE     PE-IP-ADDRESS    Redundancy         Service-carving    weight   Revertive  AC-DF
Status
=============================================================================================================================
=========
00:12:22:33:00:00:00:55:66:77  ----         10.10.10.3       single-active      auto               0        NO           NO
----
00:12:22:33:00:00:00:55:66:77  sa2.1        10.10.10.4       single-active      auto               0        NO           NO
STANDBY
```

Port-Active

The following show output displays the Ether Channel summary for CE1, CE2, PE1, PE2, PE3, and PE4 devices in the network Figure 1 using the **show etherchannel summary** command.

```
CE1#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 0001 - Oper Key 0001
     Link: xe48 (5049) sync: 0
     Link: xe50 (5051) sync: 1
CE2#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer2
  Admin Key: 0001 - Oper Key 0001
     Link: ge11 (5011) sync: 1
     Link: xe23 (5023) sync: 0
PE1#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer3
  Admin Key: 0001 - Oper Key 0001
     Link: xe0 (10004) sync: 0
PE2#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer3
  Admin Key: 0001 - Oper Key 0001
     Link: xe8 (10029) sync: 1
PE3#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer3
  Admin Key: 0001 - Oper Key 0001
     Link: xe2 (10003) sync: 0
PE4#show etherchannel summary
  Aggregator po1 100001
  Aggregator Type: Layer3
  Admin Key: 0001 - Oper Key 0001
     Link: xe11 (10012) sync: 1
```

The following show output displays the status of LDP sessions on PE1, PE2, PE3, PE4, P1, and P2 devices in the network Figure 1 using the **show ldp session** command.

```
PE1#show ldp session
Codes: m - MD5 password is not set/unset.
       g - GR configuration not set/unset.
       t - TCP MSS not set/unset.
```

```
       Session has to be cleared manually

Code  Peer IP Address      IF Name    My Role    State      KeepAlive  UpTime
       10.10.10.2         xe2        Passive   OPERATIONAL   30    00:06:57
       10.10.10.3         xe14       Passive   OPERATIONAL   30    00:07:12
       10.10.10.4         xe14       Passive   OPERATIONAL   30    00:06:42
       10.10.10.5         xe14       Passive   OPERATIONAL   30    00:07:26
       10.10.10.6         xe2        Passive   OPERATIONAL   30    00:06:36

PE2#show ldp session
Codes: m - MD5 password is not set/unset.
       g - GR configuration not set/unset.
       t - TCP MSS not set/unset.
       Session has to be cleared manually

Code  Peer IP Address      IF Name    My Role    State      KeepAlive  UpTime
       10.10.10.1         xe4        Active    OPERATIONAL   30    00:07:05
       10.10.10.3         xe4        Passive   OPERATIONAL   30    00:07:05
       10.10.10.4         xe4        Passive   OPERATIONAL   30    00:07:05
       10.10.10.5         xe5        Passive   OPERATIONAL   30    00:07:03
       10.10.10.6         xe4        Passive   OPERATIONAL   30    00:07:13

P1#show ldp session
Codes: m - MD5 password is not set/unset.
       g - GR configuration not set/unset.
       t - TCP MSS not set/unset.
       Session has to be cleared manually

Code  Peer IP Address      IF Name    My Role    State      KeepAlive  UpTime
       10.10.10.1         xe1        Active    OPERATIONAL   30    00:07:41
       10.10.10.2         xe2      Active    OPERATIONAL   30    00:07:11
       10.10.10.3         xe4        Active    OPERATIONAL   30    00:07:13
       10.10.10.4         xe3      Active    OPERATIONAL   30    00:07:10

P2#show ldp session
Codes: m - MD5 password is not set/unset.
       g - GR configuration not set/unset.
       t - TCP MSS not set/unset.
       Session has to be cleared manually

Code  Peer IP Address      IF Name    My Role    State      KeepAlive  UpTime
       10.10.10.1         xe12       Active    OPERATIONAL   30    00:06:55
       10.10.10.2         xe13       Active    OPERATIONAL   30    00:07:24
       10.10.10.3         xe11        Active    OPERATIONAL   30    00:01:47
       10.10.10.4         xe14       Active    OPERATIONAL   30    00:06:56

PE3#show ldp session
Codes: m - MD5 password is not set/unset.
       g - GR configuration not set/unset.
       t - TCP MSS not set/unset.
```

```
       Session has to be cleared manually

Code  Peer IP Address      IF Name    My Role    State       KeepAlive  UpTime
       10.10.10.1          xe5        Active    OPERATIONAL   30     00:07:35
       10.10.10.2          xe5        Active    OPERATIONAL   30     00:07:20
       10.10.10.4          xe5        Passive   OPERATIONAL   30     00:07:07
       10.10.10.5          xe1        Passive   OPERATIONAL   30     00:07:21
       10.10.10.6          xe5        Passive   OPERATIONAL   30     00:01:50

PE4#show ldp session
Codes: m - MD5 password is not set/unset.
       g - GR configuration not set/unset.
       t - TCP MSS not set/unset.
       Session has to be cleared manually

Code  Peer IP Address      IF Name    My Role    State       KeepAlive  UpTime
       10.10.10.1          xe0        Active    OPERATIONAL   30     00:07:09
       10.10.10.2          xe2        Active    OPERATIONAL   30     00:07:24
       10.10.10.3          xe0        Active    OPERATIONAL   30     00:07:11
       10.10.10.5          xe2        Passive   OPERATIONAL   30     00:07:22
       10.10.10.6          xe0        Passive   OPERATIONAL   30     00:07:03
```

The below show output displays the details about BGP L2VPN EVPN multihoming ES routes and Ethernet advertisement per ES for PE1, PE2, PE3, and PE4 devices in the network Figure 1 using the **show bgp l2vpn evpn multihoming es-route** command.

```
PE1#show bgp l2vpn evpn multihoming es-route

RD[10.10.10.1:64512] VRF[evpn-gvrf-1]:
ESI                         PE IP-Address   Encap     Peer IP         Algo      AC-DF   DP    weight
00:00:00:11:11:77:77:00:00:00  10.10.10.1      MPLS      ----------      DFT        no     no    0
00:00:00:11:11:77:77:00:00:00  10.10.10.2      MPLS      10.10.10.2      DFT        no     no    0

RD[10.10.10.2:64512]
ESI                         PE IP-Address   Encap     Peer IP         Algo
   AC-DF DP    weight
00:00:00:11:11:77:77:00:00:00  10.10.10.2      MPLS      10.10.10.2      DFT
   no    no    0

PE2#show bgp l2vpn evpn multihoming es-route

RD[10.10.10.1:64512]
ESI                         PE IP-Address   Encap     Peer IP         Algo      AC-DF DP    weight
00:00:00:11:11:77:77:00:00:00  10.10.10.1      MPLS      10.10.10.1      DFT       no    no    0

RD[10.10.10.2:64512] VRF[evpn-gvrf-1]:
ESI                         PE IP-Address   Encap     Peer IP         Algo      AC-DF DP    weight
00:00:00:11:11:77:77:00:00:00  10.10.10.1      MPLS      10.10.10.1      DFT       no    no    0
00:00:00:11:11:77:77:00:00:00  10.10.10.2      MPLS      ----------      DFT       no    no    0

PE3#show bgp l2vpn evpn multihoming es-route

RD[10.10.10.3:64512] VRF[evpn-gvrf-1]:
ESI                         PE IP-Address   Encap     Peer IP         Algo
   AC-DF DP    weight
00:00:00:22:22:77:77:00:00:00  10.10.10.3      MPLS      ----------      DFT
   no    no    0
00:00:00:22:22:77:77:00:00:00  10.10.10.4      MPLS      10.10.10.4      DFT
   no    no    0

RD[10.10.10.4:64512]
ESI                         PE IP-Address   Encap     Peer IP         Algo
   AC-DF DP    weight
```

```
00:00:00:22:22:77:77:00:00:00  10.10.10.4      MPLS      10.10.10.4      DFT
   no    no    0

PE4#show bgp l2vpn evpn multihoming es-route

RD[10.10.10.3:64512]
ESI                           PE IP-Address   Encap     Peer IP         Algo      AC-DF DP    weight
00:00:00:22:22:77:77:00:00:00  10.10.10.3      MPLS      10.10.10.3      DFT       no    no    0

RD[10.10.10.4:64512] VRF[evpn-gvrf-1]:
ESI                           PE IP-Address   Encap     Peer IP         Algo      AC-DF DP    weight
00:00:00:22:22:77:77:00:00:00  10.10.10.3      MPLS      10.10.10.3      DFT       no    no    0
00:00:00:22:22:77:77:00:00:00  10.10.10.4      MPLS      ----------      DFT       no    no    0
```

The following show output displays the details about Layer 2 Virtual Private Network (L2VPN) Ethernet Virtual Private Network (EVPN) routes on PE1, PE2, PE3, and PE4 devices in the network Figure 1 using the **show bgp l2vpn evpn multihoming ethernet-ad-per-es** and **show bgp l2vpn evpn multihoming ethernet-ad-per-evi** comands.

```
PE1#show bgp l2vpn evpn multihoming ethernet-ad-per-es

RD[10.10.10.1:1700] VRF[vrf2]:
ESI                           Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:11:11:77:77:00:00:00  4294967295  440336         10.10.10.2      MPLS      P flag
00:00:00:22:22:77:77:00:00:00  4294967295  440336         10.10.10.3      MPLS      B flag
00:00:00:22:22:77:77:00:00:00  4294967295  440336         10.10.10.4      MPLS      P flag

RD[10.10.10.1:64512] VRF[evpn-gvrf-1]:
ESI                           Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:11:11:77:77:00:00:00  4294967295  440336         10.10.10.1      MPLS      B flag

RD[10.10.10.2:64512]
ESI                           Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:11:11:77:77:00:00:00  4294967295  440336         10.10.10.2      MPLS      P flag

RD[10.10.10.3:64512]
ESI                           Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:22:22:77:77:00:00:00  4294967295  440336         10.10.10.3      MPLS      B flag

RD[10.10.10.4:64512]
ESI                           Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:22:22:77:77:00:00:00  4294967295  440336         10.10.10.4      MPLS      P flag

PE1#show bgp l2vpn evpn multihoming ethernet-ad-per-evi

RD[10.10.10.1:1700] VRF[vrf2]:
ESI                           Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:11:11:77:77:00:00:00  1800        27522          10.10.10.1      MPLS      B flag
00:00:00:11:11:77:77:00:00:00  1800        27520          10.10.10.2      MPLS      P flag
00:00:00:22:22:77:77:00:00:00  1700        27520          10.10.10.3      MPLS      B flag
00:00:00:22:22:77:77:00:00:00  1700        27520          10.10.10.4      MPLS      P flag

RD[10.10.10.2:1700]
ESI                           Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:11:11:77:77:00:00:00  1800        27520          10.10.10.2      MPLS      P flag

RD[10.10.10.3:1700]
ESI                           Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:22:22:77:77:00:00:00  1700        27520          10.10.10.3      MPLS      B flag

RD[10.10.10.4:1700]
ESI                           Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:22:22:77:77:00:00:00  1700        27520          10.10.10.4      MPLS      P flag

PE2#show bgp l2vpn evpn multihoming ethernet-ad-per-es

RD[10.10.10.1:64512]
ESI                           Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:11:11:77:77:00:00:00  4294967295  440336         10.10.10.1      MPLS      B flag

RD[10.10.10.2:1700] VRF[vrf2]:
ESI                           Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:11:11:77:77:00:00:00  4294967295  440336         10.10.10.1      MPLS      B flag
00:00:00:22:22:77:77:00:00:00  4294967295  440336         10.10.10.3      MPLS      B flag
```

```
00:00:00:22:22:77:77:00:00:00  4294967295  440336         10.10.10.4      MPLS      P flag

RD[10.10.10.2:64512] VRF[evpn-gvrf-1]:
ESI                            Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:11:11:77:77:00:00:00  4294967295  440336         10.10.10.2      MPLS      P flag

RD[10.10.10.3:64512]
ESI                            Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:22:22:77:77:00:00:00  4294967295  440336         10.10.10.3      MPLS      B flag

RD[10.10.10.4:64512]
ESI                            Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:22:22:77:77:00:00:00  4294967295  440336         10.10.10.4      MPLS      P flag

PE2#show bgp l2vpn evpn multihoming ethernet-ad-per-evi

RD[10.10.10.1:1700]
ESI                            Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:11:11:77:77:00:00:00  1800        27522          10.10.10.1      MPLS      B flag

RD[10.10.10.2:1700] VRF[vrf2]:
ESI                            Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:11:11:77:77:00:00:00  1800        27522          10.10.10.1      MPLS      B flag
00:00:00:11:11:77:77:00:00:00  1800        27520          10.10.10.2      MPLS      P flag
00:00:00:22:22:77:77:00:00:00  1700        27520          10.10.10.3      MPLS      B flag
00:00:00:22:22:77:77:00:00:00  1700        27520          10.10.10.4      MPLS      P flag

RD[10.10.10.3:1700]
ESI                            Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:22:22:77:77:00:00:00  1700        27520          10.10.10.3      MPLS      B flag

RD[10.10.10.4:1700]
ESI                            Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:22:22:77:77:00:00:00  1700        27520          10.10.10.4      MPLS      P flag

PE3#show bgp l2vpn evpn multihoming ethernet-ad-per-es

RD[10.10.10.1:64512]
ESI                            Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:11:11:77:77:00:00:00  4294967295  440336         10.10.10.1      MPLS      B flag

RD[10.10.10.2:64512]
ESI                            Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:11:11:77:77:00:00:00  4294967295  440336         10.10.10.2      MPLS      P flag

RD[10.10.10.3:1700] VRF[vrf2]:
ESI                            Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:11:11:77:77:00:00:00  4294967295  440336         10.10.10.2      MPLS      P flag
00:00:00:11:11:77:77:00:00:00  4294967295  440336         10.10.10.1      MPLS      B flag
00:00:00:22:22:77:77:00:00:00  4294967295  440336         10.10.10.4      MPLS      P flag

RD[10.10.10.3:64512] VRF[evpn-gvrf-1]:
ESI                            Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:22:22:77:77:00:00:00  4294967295  440336         10.10.10.3      MPLS      B flag

RD[10.10.10.4:64512]
ESI                            Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:22:22:77:77:00:00:00  4294967295  440336         10.10.10.4      MPLS      P flag

PE3#show bgp l2vpn evpn multihoming ethernet-ad-per-evi

RD[10.10.10.1:1700]
ESI                            Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:11:11:77:77:00:00:00  1800        27522          10.10.10.1      MPLS      B flag

RD[10.10.10.2:1700]
ESI                            Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:11:11:77:77:00:00:00  1800        27520          10.10.10.2      MPLS      P flag

RD[10.10.10.3:1700] VRF[vrf2]:
ESI                            Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:11:11:77:77:00:00:00  1800        27520          10.10.10.2      MPLS      P flag
00:00:00:11:11:77:77:00:00:00  1800        27522          10.10.10.1      MPLS      B flag
```

```
00:00:00:22:22:77:77:00:00:00  1700        27520          10.10.10.3      MPLS      B flag
00:00:00:22:22:77:77:00:00:00  1700        27520          10.10.10.4      MPLS      P flag

RD[10.10.10.4:1700]
ESI                            Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:22:22:77:77:00:00:00  1700        27520          10.10.10.4      MPLS      P flag

PE4#show bgp l2vpn evpn multihoming ethernet-ad-per-es

RD[10.10.10.1:64512]
ESI                            Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:11:11:77:77:00:00:00  4294967295  440336         10.10.10.1      MPLS      B flag

RD[10.10.10.2:64512]
ESI                            Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:11:11:77:77:00:00:00  4294967295  440336         10.10.10.2      MPLS      P flag

RD[10.10.10.3:64512]
ESI                            Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:22:22:77:77:00:00:00  4294967295  440336         10.10.10.3      MPLS      B flag

RD[10.10.10.4:1700] VRF[vrf2]:
ESI                            Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:11:11:77:77:00:00:00  4294967295  440336         10.10.10.1      MPLS      B flag
00:00:00:11:11:77:77:00:00:00  4294967295  440336         10.10.10.2      MPLS      P flag
00:00:00:22:22:77:77:00:00:00  4294967295  440336         10.10.10.3      MPLS      B flag

RD[10.10.10.4:64512] VRF[evpn-gvrf-1]:
ESI                            Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:22:22:77:77:00:00:00  4294967295  440336         10.10.10.4      MPLS      P flag

PE4#show bgp l2vpn evpn multihoming ethernet-ad-per-evi

RD[10.10.10.1:1700]
ESI                            Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:11:11:77:77:00:00:00  1800        27522          10.10.10.1      MPLS      B flag

RD[10.10.10.2:1700]
ESI                            Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:11:11:77:77:00:00:00  1800        27520          10.10.10.2      MPLS      P flag

RD[10.10.10.3:1700]
ESI                            Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:22:22:77:77:00:00:00  1700        27520          10.10.10.3      MPLS      B flag

RD[10.10.10.4:1700] VRF[vrf2]:
ESI                            Eth-Tag     VNID/LABEL     Nexthop IP      Encap     Flags
00:00:00:11:11:77:77:00:00:00  1800        27522          10.10.10.1      MPLS      B flag
00:00:00:11:11:77:77:00:00:00  1800        27520          10.10.10.2      MPLS      P flag
00:00:00:22:22:77:77:00:00:00  1700        27520          10.10.10.3      MPLS      B flag
00:00:00:22:22:77:77:00:00:00  1700        27520          10.10.10.4      MPLS      P flag
```

Port-Active ELINE

The following show output displays the active EVPN MPLS Tunnels for ELINE on PE1, PE2, PE3, and PE4 devices in the network Figure 1 using the **show evpn mpls xconnect tunnel** command.

```
PE1#show evpn mpls xconnect tunnel
EVPN-MPLS Network tunnel Entries
Source           Destination      Status        Up/Down       Update        local-evpn-id remote-evpn-id
=============================================================================================================
10.10.10.1       10.10.10.3       AC-Down       00:31:41      00:31:41      4             1700
10.10.10.1       10.10.10.4       AC-Down       00:31:41      00:31:41      4             1700
Total number of entries are 2

PE2#show evpn mpls xconnect tunnel
EVPN-MPLS Network tunnel Entries
Source           Destination      Status        Up/Down       Update        local-evpn-id remote-evpn-id
=============================================================================================================
10.10.10.2       10.10.10.3       Installed     00:12:21      00:11:40      1800          1700
10.10.10.2       10.10.10.4       Installed     00:17:43      00:17:37      1800          1700
Total number of entries are 2
```

```
PE3#show evpn mpls xconnect tunnel
EVPN-MPLS Network tunnel Entries
Source           Destination      Status        Up/Down       Update        local-evpn-id remote-evpn-id
=============================================================================================================
10.10.10.3       10.10.10.1       AC-Down       00:12:26      00:12:26      1700          1800
10.10.10.3       10.10.10.2       AC-Down       00:12:26      00:12:26      1700          1800

Total number of entries are 2


PE4#show evpn mpls xconnect tunnel
EVPN-MPLS Network tunnel Entries
Source           Destination      Status        Up/Down       Update        local-evpn-id remote-evpn-id
=============================================================================================================
10.10.10.4       10.10.10.1       Installed     00:12:28      00:12:28      1700          1800
10.10.10.4       10.10.10.2       Installed     00:12:28      00:12:28      1700          1800

Total number of entries are 2
```

Port-Active ELAN

The following show outputs provide validation for ELAN configurations.

The following show output displays the active EVPN MPLS Tunnels for ELAN on PE1, PE2, PE3, and PE4 devices in the network Figure 1 using the **show evpn mpls tunnel** command.

```
PE1#show evpn mpls tunnel
EVPN-MPLS Network tunnel Entries
Source           Destination      Status        Up/Down       Update        evpn-id
=================================================================================
10.10.10.1       10.10.10.4       Installed     00:02:35      00:02:35      3000

10.10.10.1       10.10.10.3       Installed     00:03:00      00:03:00      3000

10.10.10.1       10.10.10.2       Installed     00:03:26      00:03:26      3000


Total number of entries are 3

PE2#show evpn mpls tunnel
EVPN-MPLS Network tunnel Entries
Source           Destination      Status        Up/Down       Update        evpn-id
=================================================================================
10.10.10.2       10.10.10.4       Installed     00:02:45      00:02:45      3000

10.10.10.2       10.10.10.3       Installed     00:03:10      00:03:10      3000

10.10.10.2       10.10.10.1       Installed     00:03:36      00:03:36      3000


Total number of entries are 3

PE3#show evpn mpls tunnel
EVPN-MPLS Network tunnel Entries
Source           Destination      Status        Up/Down       Update        evpn-id
=================================================================================
10.10.10.3       10.10.10.4       Installed     00:02:56      00:02:56      3000

10.10.10.3       10.10.10.2       Installed     00:03:22      00:03:22      3000

10.10.10.3       10.10.10.1       Installed     00:03:22      00:03:22      3000


Total number of entries are 3

PE4#show evpn mpls tunnel
EVPN-MPLS Network tunnel Entries
Source           Destination      Status        Up/Down       Update        evpn-id
=================================================================================
10.10.10.4       10.10.10.3       Installed     00:03:00      00:03:00      3000
```

```
10.10.10.4       10.10.10.1       Installed     00:03:00      00:03:00      3000

10.10.10.4       10.10.10.2       Installed     00:03:00      00:03:00      3000


Total number of entries are 3
```

The following show output displays the EVPN active multi-homed and load-balanced details on PE1, PE2, PE3, and PE4 devices in the network Figure 1 using the **show evpn load-balance port-active** and **show evpn multi-homing all** commands.

```
PE1#show evpn load-balance port-active
ESI                           AC-IF/PE     PE-IP-ADDRESS    Redundancy         Service-carving    weight   Revertive  AC-DF
Status
=============================================================================================================================
00:00:00:11:11:77:77:00:00:00  LOCAL        10.10.10.1       port-active        auto               0        NO           NA
STANDBY
00:00:00:11:11:77:77:00:00:00  REMOTE       10.10.10.2       port-active        auto               0        NO           NA
ACTIVE
00:00:00:22:22:77:77:00:00:00  REMOTE       10.10.10.3       port-active        ----               ----     ----       ----
STANDBY
00:00:00:22:22:77:77:00:00:00  REMOTE       10.10.10.4       port-active        ----               ----     ----       ----
ACTIVE

PE1#show evpn multi-homing all
ESI                            Access-IF    PE-IP-ADDRESS
=========================================================
00:00:00:11:11:77:77:00:00:00  po1          10.10.10.1
00:00:00:11:11:77:77:00:00:00  ----         10.10.10.2
00:00:00:22:22:77:77:00:00:00  ----         10.10.10.3
00:00:00:22:22:77:77:00:00:00  ----         10.10.10.4
Total number of entries are 4

PE2#show evpn load-balance port-active
ESI                            AC-IF/PE  PE-IP-ADDRESS    Redundancy     Service-carving   weight  Revertive  AC-DF   Status
=============================================================================================================================
00:00:00:11:11:77:77:00:00:00  REMOTE   10.10.10.1       port-active       auto              0        NO        NA    STANDBY
00:00:00:11:11:77:77:00:00:00  LOCAL    10.10.10.2       port-active      auto              0        NO        NA    ACTIVE
00:00:00:22:22:77:77:00:00:00  REMOTE   10.10.10.3      port-active       ---              ----     ----       ----    STANDBY
00:00:00:22:22:77:77:00:00:00  REMOTE   10.10.10.4       port-active       ----              ----     ----       ----    ACTIVE

PE2#show evpn multi-homing all
ESI                            Access-IF    PE-IP-ADDRESS
=========================================================
00:00:00:11:11:77:77:00:00:00  ----         10.10.10.1
00:00:00:11:11:77:77:00:00:00  po1          10.10.10.2
00:00:00:22:22:77:77:00:00:00  ----         10.10.10.3
00:00:00:22:22:77:77:00:00:00  ----         10.10.10.4
Total number of entries are 4

PE3#show evpn load-balance port-active
ESI                            AC-IF/PE     PE-IP-ADDRESS    Redundancy         Service-carving    weight   Revertive  AC-DF
Status
=============================================================================================================================
00:00:00:11:11:77:77:00:00:00  REMOTE       10.10.10.1       port-active        ----               ----     ----       ----
STANDBY
00:00:00:11:11:77:77:00:00:00  REMOTE       10.10.10.2       port-active        ----               ----     ----       ----
ACTIVE
00:00:00:22:22:77:77:00:00:00  LOCAL        10.10.10.3       port-active        auto               0        NO           NA
STANDBY
00:00:00:22:22:77:77:00:00:00  REMOTE       10.10.10.4       port-active        auto               0        NO           NA
ACTIVE

PE3#show evpn multi-homing all
ESI                            Access-IF    PE-IP-ADDRESS
=========================================================
00:00:00:11:11:77:77:00:00:00  ----         10.10.10.1
00:00:00:11:11:77:77:00:00:00  ----         10.10.10.2
00:00:00:22:22:77:77:00:00:00  po1          10.10.10.3
00:00:00:22:22:77:77:00:00:00  ----         10.10.10.4
Total number of entries are 4

PE4#show evpn load-balance port-active
ESI                            AC-IF/PE     PE-IP-ADDRESS    Redundancy         Service-carving    weight   Revertive  AC-DF
Status
```

```
=========================================================================================================================================
=========
00:00:00:11:11:77:77:00:00:00  REMOTE       10.10.10.1       port-active       ----              ----     ----       ----
STANDBY
00:00:00:11:11:77:77:00:00:00  REMOTE       10.10.10.2       port-active       ----              ----     ----       ----
ACTIVE
00:00:00:22:22:77:77:00:00:00  REMOTE       10.10.10.3       port-active       auto              0        NO           NA
STANDBY
00:00:00:22:22:77:77:00:00:00  LOCAL        10.10.10.4       port-active       auto              0        NO           NA
ACTIVE

PE4#show evpn multi-homing all
ESI                            Access-IF    PE-IP-ADDRESS
=========================================================
00:00:00:11:11:77:77:00:00:00  ----         10.10.10.1
00:00:00:11:11:77:77:00:00:00  ----         10.10.10.2
00:00:00:22:22:77:77:00:00:00  ----         10.10.10.3
00:00:00:22:22:77:77:00:00:00  po1          10.10.10.4
```

EVPN SR Active-Standby Multi-Homing Configuration

This section illustrates the Multi-Homed setup for the EVPN Segment Routing (SR) Active-Standby configuration, showcasing examples for both ELINE and ELAN services with SR as the underlay MPLS path.

EVPN SR Active-Standby MH Topology

Figure 1 consists of customer edge routers CE1 and CE2, along with IPv4 Provider Edge routers PE1, PE2, PE3, and PE4, all interconnected through the core routers P1 and P2 in the IPv4 MPLS provider network.

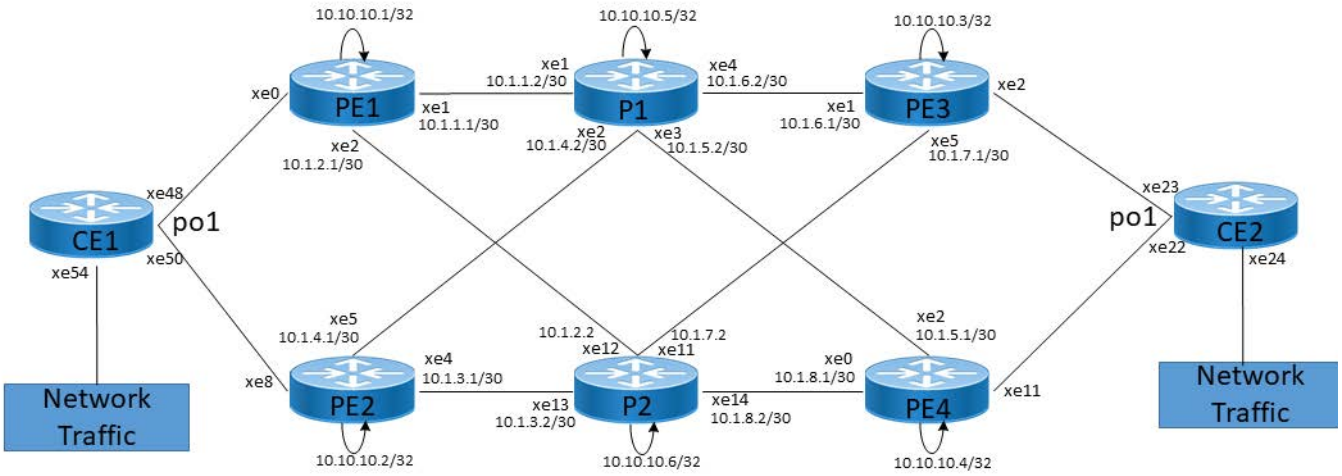


Figure 2: EVPN MPLS AS MH Configuration

CE1

The following configuration steps under CE1 are set up to enable VLANs and configure interfaces for carrying VLAN traffic.

`CE1#configure terminal`	Enter configure mode.
`CE1(config)#bridge 1 protocol ieee vlan-bridge`	Set up `bridge 1` to use the IEEE VLAN bridge protocol.
`CE1(config)#vlan 2-100 bridge 1 state enable`	Configure VLANs from `2-100` and associate them with bridge 1.

`CE1(config)#interface xe54`	Enter interface mode `xe54`.
`CE1(config-if)#switchport`	Configure the interface `xe54` as a Layer 2 switch port.
`CE1(config-if)#bridge-group 1`	Associate `xe54` to bridge 1.
`CE1(config-if)#switchport mode trunk`	Configure `xe54` as a trunk port.
`CE1(config-if)#switchport trunk allowed vlan all`	Allow all configured VLANs on the trunk interface `xe54`.
`CE1(config-if)#exit`	Exit interface mode `xe54`.
`CE1(config)#interface po1`	Enter interface mode and configure LAG interface port-channel 1 (`po1`).
`CE1(config-if)#switchport`	Configures port-channel 1 as a Layer 2 switch port.
`CE1(config-if)#bridge-group 1`	Associate `po1` to bridge 1.
`CE1(config-if)#switchport mode trunk`	Configure `po1` as a trunk port.
`CE1(config-if)#switchport trunk allowed vlan all`	Allow all configured VLANs on the trunk port-channel `po1`.
`CE1(config-if)#exit`	Exit interface mode `po1`.
`CE1(config)#interface xe48`	Enter interface mode `xe48`.
`CE1(config-if)#lacp timeout short`	Configure LACP timeout as `short`.
`CE1(config-if)#channel-group 1 mode active`	Add member to the LAG interface.
`CE1(config-if)#exit`	Exit interface mode `xe48`.
`CE1(config-if)#interface xe50`	Enter interface mode `xe50`.
`CE1(config-if)#lacp timeout short`	Configure LACP timeout as `short`.
`CE1(config-if)#channel-group 1 mode active`	Add member to the LAG interface.
`CE1(config-if)#commit`	Commit the transaction.
`CE1(config-if)#end`	Exit interface mode `xe50` and configure mode.

PE1: Loopback Interface

The configuration on PE1 for a loopback interface with IP address `10.10.10.1/32` secondary is set up to provide IP connectivity for the ISIS router.

`PE1#configure terminal`	Enter configure mode.
`PE1(config)#interface lo`	Enter the interface mode for the loopback interface `lo`.
`PE1(config-if)#ip address 10.10.10.1/32 secondary`	Configure a secondary IP address, `10.10.10.1/32`, on the loopback interface.
`PE1(config-if)#ip router isis 1`	Enable ISIS routing on a loopback interface `lo` for area 1.
`PE1(config-if)#prefix-sid index 800`	Configure a prefix segment identifier (prefix-SID) index value as `800`.
`PE1(config-if)#exit`	Exit interface mode `lo`.
`PE1(config)#commit`	Commit the transaction.

PE1: Configure SR

The following configurations aim to activate Segment Routing (SR) on PE1 and make MPLS the preferred method for segment routing, optimizing routing efficiency.

`PE1(config)#segment-routing`	Configure segment routing on PE1 device.
`PE1(config-sr)#mpls sr-prefer`	Set MPLS as the preferred segment routing protocol over others.
`PE1(config-sr)#exit`	Exit the router SR mode.
`PE1(config)#commit`	Commit the transaction.

PE1: Global LDP

The configuration on PE1 for the Global LDP router, specifying router ID and targeted peers, is done to set up Label Distribution Protocol (LDP) settings for MPLS.

`PE1(config)#router ldp`	Enter the Router LDP mode.
`PE1(config-router)#router-id 10.10.10.1`	Set the router ID for LDP to `10.10.10.1`.
`PE1(config-router)#transport-address ipv4 10.10.10.1`	Configure the transport address for IPv4 (for IPv6 use ipv6 parameter) to be used for a TCP session where LDP operates. Note: It is preferable to use the loopback address as the transport address.
`PE1(config-router)#targeted-peer ipv4 10.10.10.2`	Configure targeted peer for LDP using IPv4 addresses.
`PE1(config-router-targeted-peer)#exit-targeted-peer-mode`	Exit router targeted-peer-mode.
`PE1(config-router)#targeted-peer ipv4 10.10.10.3`	Configure targeted peer for LDP using IPv4 addresses.
`PE1(config-router-targeted-peer)#exit-targeted-peer-mode`	Exit router targeted-peer-mode.
`PE1(config-router)#targeted-peer ipv4 10.10.10.4`	Configure targeted peer for LDP using IPv4 addresses.
`PE1(config-router-targeted-peer)#exit-targeted-peer-mode`	Exit router targeted-peer-mode.
`PE1(config-router)#exit`	Exit router LDP mode and return to the configure mode.
`PE1(config)#commit`	Commit the transaction.

PE1: Global EVPN MPLS Command

The configuration on PE1 for the Global EVPN MPLS, includes activating EVPN MPLS, defining the global VTEP IP address, enabling hardware profile filtering for EVPN MPLS multi-homing, and activating EVPN MPLS multi-homing functionality, all of which are crucial for enabling EVPN MPLS features.

`PE1(config)#evpn mpls enable`	Activate the EVPN MPLS functionality on `PE1`, enabling it to participate in EVPN MPLS services.
`PE1(config)#commit`	Commit candidate configuration to be running configuration.
`PE1(config)#evpn mpls vtep-ip-global 10.10.10.1`	Configure the global VTEP IP address `10.10.10.1`, associating it with the loopback IP.
`PE1(config)#hardware-profile filter evpn-mpls-mh enable`	Enable hardware-profile filter for EVPN MPLS multi-homing.

`PE1(config)#evpn mpls multihoming enable`	Activate the EVPN MPLS multi-homing functionality, allowing `PE1` to support multi-homed EVPN MPLS services.
`PE1(config)#commit`	Commit the transaction.

PE1: Interface Configuration Network Side

The below configuration is performed to set up network interfaces on PE1 and enable LDP for IPv4, ensuring proper routing and labeling functionality.

`PE1(config)#interface xe1`	Enter interface mode `xe1`.
`PE1(config-if)#ip address 10.1.1.1/30`	Configure an IP address, `10.1.1.1/30`, on the interface `xe1`.
`PE1(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`PE1(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`PE1(config-if)#ip router isis 1`	Enable ISIS IPv4 routing on an interface `xe1`.
`PE1(config-if)#exit`	Exit interface mode `xe1`.
`PE1(config)#commit`	Commit the transaction.
`PE1(config)#interface xe2`	Enter interface mode `xe2`.
`PE1(config-if)#ip address 10.1.2.1/30`	Configure an IP address, `10.1.2.1/30`, on the interface `xe2`.
`PE1(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`PE1(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`PE1(config-if)#ip router isis 1`	Enable ISIS IPv4 routing on an interface `xe2`.
`PE1(config-if)#exit`	Exit interface mode `xe2`.
`PE1(config)#commit`	Commit the transaction.

PE1: ISIS Configuration

The below configuration is performed to set up ISIS on PE1, to enable MPLS Traffic Engineering, Segment Routing, and other related features for efficient routing and network management.

`PE1(config)#router isis 1`	Enter router ISIS mode.
`PE1(config-router)#is-type level-1-2`	Configure IS-Type as `Level-1-2` specifies that the router will participate in both Level-1 and Level-2 areas within the ISIS network.
`PE1(config-router)#metric-style wide`	Configure the new style of metric type as `wide`.
`PE1(config-router)#mpls traffic-eng router-id 10.10.10.1`	Configure the router's MPLS Traffic Engineering (TE) router ID TLV to `10.10.10.1`, which is used for MPLS-TE path calculations.
`PE1(config-router)#mpls traffic-eng level-1`	Enable MPLS-TE for IS-Type `Level-1` routing.
`PE1(config-router)#mpls traffic-eng level-2`	Enable MPLS-TE for IS-Type `Level-2` routing.

`PE1(config-router)#capability cspf`	Enable Constraint Shortest Path First (CSPF) computation for traffic engineering.
`PE1(config-router)#dynamic-hostname`	Configure the hostname to be advertised for an ISIS instance.
`PE1(config-router)#fast-reroute ti-lfa level-1 proto ipv4`	Configure Remote Loop-Free Alternate (LFA) to calculate backup paths to those destinations whichever does not satisfy basic LFA FRR inequalities
`PE1(config-router)#fast-reroute ti-lfa level-2 proto ipv4`	Configure Remote Loop-Free Alternate (LFA) to calculate backup paths to those destinations whichever does not satisfy basic LFA FRR inequalities
`PE1(config-router)#bfd all-interfaces`	Configure BFD on all interfaces for fast link failure detection.
`PE1(config-router)#net 49.0000.0000.0001.00`	Set a Network Entity Title (NET) for this ISIS instance, specifying the area address and the system ID.
`PE1(config-router)#isis segment-routing global block 17000 23500`	Enable ISIS SR globally and allocates label blocks for Segment Routing.
`PE1(config-router)#segment-routing mpls`	Enable SR ISIS.
`PE1(config-router)#exit`	Exit router ISIS mode and return to configure mode.
`PE1(config)#commit`	Commit the transaction.

PE1: BGP Configuration

The below BGP configuration on PE1 is established to enable BGP routing with ASN 65010, set the BGP router ID, define iBGP neighbors, configure BFD, and enable the EVPN address family for efficient routing in an EVPN environment.

`PE1(config)#router bgp 65010`	Enter the Router BGP mode, ASN: 65010
`PE1(config-router)#bgp router-id 10.10.10.1`	Configure BGP router ID `10.10.10.1`, identifying PE1 within the BGP network.
`PE1(config-router)#neighbor 10.10.10.2 remote-as 65010`	Configure neighbor `10.10.10.2` as an iBGP neighbor with their remote AS number `65010`.
`PE1(config-router)#neighbor 10.10.10.2 update-source lo`	Configure neighbor `10.10.10.2` as an iBGP neighbor, specifying the source of routing updates as the loopback interface.
`PE1(config-router)#neighbor 10.10.10.3 remote-as 65010`	Configure neighbor `10.10.10.3` as an iBGP neighbor with their remote AS number `65010`.
`PE1(config-router)#neighbor 10.10.10.3 update-source lo`	Configure neighbor `10.10.10.3` as an iBGP neighbor, specifying the source of routing updates as the loopback interface.
`PE1(config-router)#neighbor 10.10.10.4 remote-as 65010`	Configure neighbor `10.10.10.4` as an iBGP neighbor with their remote AS number `65010`.
`PE1(config-router)#neighbor 10.10.10.4 update-source lo`	Configure neighbor `10.10.10.4` as an iBGP neighbor, specifying the source of routing updates as the loopback interface.
`PE1(config-router)#neighbor 10.10.10.2 fall-over bfd multihop`	Configure BFD for the BGP neighbor to provide rapid failure detection.
`PE1(config-router)#neighbor 10.10.10.3 fall-over bfd multihop`	Configure BFD for the BGP neighbor to provide rapid failure detection.
`PE1(config-router)#neighbor 10.10.10.4 fall-over bfd multihop`	Configure BFD for the BGP neighbor to provide rapid failure detection.

`PE1(config-router)#neighbor 10.10.10.2 advertisement-interval 0`	Configure advertisement interval for the neighbor, allowing more frequent BGP updates.
`PE1(config-router)#neighbor 10.10.10.3 advertisement-interval 0`	Configure advertisement interval for the neighbor, allowing more frequent BGP updates.
`PE1(config-router)#neighbor 10.10.10.4 advertisement-interval 0`	Configure advertisement interval for the neighbor, allowing more frequent BGP updates.
`PE1(config-router)#address-family l2vpn evpn`	Enter into address family mode for L2VPN EVPN.
`PE1(config-router-af)#neighbor 10.10.10.2 activate`	Activate EVPN for iBGP neighbor `10.10.10.2` within the address family mode, ensuring that EVPN address family is enabled for the neighbor.
`PE1(config-router-af)#neighbor 10.10.10.3 activate`	Activate EVPN for iBGP neighbor `10.10.10.3` within the address family mode, ensuring that EVPN address family is enabled for the neighbor.
`PE1(config-router-af)#neighbor 10.10.10.4 activate`	Activate EVPN for iBGP neighbor `10.10.10.4` within the address family mode, ensuring that EVPN address family is enabled for the neighbor.
`PE1(config-router-af)#exit`	Exit address family mode and return to the router BGP mode.
`PE1(config-router)#commit`	Commit the transaction.
`PE1(config-router)#exit`	Exit router BGP mode and return to the configure mode.

PE1: MAC VRF Configuration

The below MAC VRF configuration on PE1 is carried out to define and set up VRFs named `vrf2` and `vpls1001` with specific Route-Distinguisher (RD) and route-target values, ensuring segregated MAC address spaces for distinct network services.

`PE1(config)#mac vrf vrf2`	Enter VRF mode named `vrf2`.
`PE1(config-vrf)#rd 10.10.10.1:1700`	Configure Route-Distinguisher value of `10.10.10.1:1700`.
`PE1(config-vrf)#route-target both 1700:1700`	Configure import and export values for the `vrf2` as `1700:1700`.
`PE1(config-vrf)#exit`	Exit VRF mode and return to the configure mode.
`PE1(config)#mac vrf vpls1001`	Enter VRF mode named `vpls1001`.
`PE1(config-vrf)#rd 10.10.10.1:1001`	Configure Route-Distinguisher value of `10.10.10.1:1001`.
`PE1(config-vrf)#route-target both 1001:1001`	Configure import and export values for the `vpls1001` as `1001:1001`.
`PE1(config-vrf)#exit`	Exit VRF mode and return to the configure mode.
`PE1(config)#commit`	Commit the transaction.

PE1: EVPN and VRF Mapping

The below EVPN and VRF mapping configuration on PE1 is performed to establish mappings between EVPN identifiers and VRFs, facilitating efficient routing and connectivity in an EVPN network environment.

`PE1(config)#evpn mpls id 1800 xconnect target-mpls-id 1700`	Configure the EVPN-VPWS identifier with a source identifier of `1800` and a target identifier of `1700`.
`PE1(config-evpn-mpls)#host-reachability-protocol evpn-bgp vrf2`	Map VRF `vrf2` to the EVPN-VPWS identifier

`PE1(config-evpn-mpls)#evpn mpls id 3000`	Configure the EVPN-VPLS identifier an identifier of `3000`.
`PE1(config-evpn-mpls)#host-reachability-protocol evpn-bgp vpls1001`	Map VRF `vpls1001` to the EVPN-VPWS identifier
`PE1(config-evpn-mpls)#commit`	Commit the transaction.
`PE1(config-evpn-mpls)#exit`	Exit the EVPN MPLS mode and return to the configure mode.

PE1: Access Port Configuration for Port-active

The below access port configuration for port-active mode on PE1 is carried out to configure various parameters including system-mac, load balancing, service carving preferences, and EVPN settings for efficient network access and connectivity.

`PE1(config)#interface po1`	Enter the port channel interface mode for `po1`
`PE1(config-if)#load-interval 30`	Set the load interval to `30`.
`PE1(config-if)#evpn multi-homed system-mac 0000.1111.7777 load-balancing port-active`	Configure the system-mac address `0000.1111.7777` for port-active mode, which plays a role in load balancing and enter to the EVPN Ethernet Segment (ES) mode.
`PE1(config-if-es)#service-carving auto`	Configure service carving as `auto`.
`PE1(config-if-es)#exit`	Exit the EVPN ES mode and return to the configure mode.
`PE1(config-if)#exit`	Exit interface mode `po1` and return to the configure mode.
`PE1(config)#commit`	Commit the transaction.
`PE1(config)#interface po1.1 switchport`	Create a Layer 2 sub-interface `po1.1` within the port channel.
`PE1(config-if)#encapsulation dot1q 100`	Set encapsulation to dot1q with VLAN ID `100`.
`PE1(config-if)#load-interval 30`	Set the load interval to `30`.
`PE1(config-if)#access-if-evpn`	Enter the access mode for EVPN MPLS ID configuration.
`PE1(config-acc-if-evpn)#map vpn-id 1800`	Map VPN-ID `1800`.
`PE1(config-acc-if-evpn)#exit`	Exit the access mode and return to the interface mode.
`PE1(config-if)#exit`	Exit interface mode `po1.1` and return to the configure mode.
`PE1(config)#interface xe0`	Enter the interface mode for `xe0.`
`PE1(config-if)#speed 10g`	Set the speed to `10g`.
`PE1(config-if)#channel-group 1 mode active`	Attach LAG interface `po1.`
`PE1(config-if)#exit`	Exit interface mode `xe0` and return to the configure mode.
`PE1(config)#commit`	Commit the transaction.

PE1: Access Port Configuration for Single-active

The below access port configuration for single-active mode on PE1 is implemented to set up various parameters, including Ethernet Segment Identifier (ESI) settings, service carving preferences, and EVPN configurations, ensuring efficient network access and connectivity.

`PE1(config)#interface sa1`	Enter the single active interface mode for `sa1`
`PE1(config-if)#load-interval 30`	Set the load interval to `30`.

`PE1(config-if)#evpn multi-homed esi 00:00:11:11:77:77 load-balancing single-active`	Configure the ESI with the value with the value `00:00:11:11:77:77` for single-active mode, which plays a role in load balancing and enter to the EVPN Ethernet Segment (ES) mode.
`PE1(config-if-es)#service-carving auto`	Configure service carving as `auto`, allowing automatic determination of service distribution preferences.
`PE1(config-if-es)#exit`	Exit the EVPN ES mode and return to the configure mode.
`PE1(config-if)#exit`	Exit interface mode `sa1` and return to the configure mode.
`PE1(config)#commit`	Commit the transaction.
`PE1(config)#interface sa1.1 switchport`	Create a Layer 2 sub-interface `sa1.1` within the port channel.
`PE1(config-if)#encapsulation dot1q 100`	Set encapsulation to dot1q with VLAN ID `100`.
`PE1(config-if)#load-interval 30`	Set the load interval to `30`.
`PE1(config-if)#access-if-evpn`	Enter the access mode for EVPN MPLS ID configuration.
`PE1(config-acc-if-evpn)#map vpn-id 1800`	Map VPN-ID `1800`.
`PE1(config-acc-if-evpn)#exit`	Exit the access mode and return to the interface mode.
`PE1(config-if)#exit`	Exit interface mode `sa1.1` and return to the configure mode.
`PE1(config)#interface xe0`	Enter the interface mode for `xe0`.
`PE1(config-if)#speed 10g`	Set the speed to `10g`.
`PE1(config-if)#static-channel-group 1`	Attach the static-channel-group 1, the LAG interface `sa1` to `xe0`.
`PE1(config-if)#exit`	Exit interface mode `xe0` and return to the configure mode.
`PE1(config)#commit`	Commit the transaction.

PE2: Loopback Interface

The configuration on PE2 for a loopback interface with IP address `10.10.10.2/32` secondary is set up to provide IP connectivity for the ISIS router.

`PE2#configure terminal`	Enter configure mode.
`PE2(config)#interface lo`	Enter the interface mode for the loopback interface `lo`.
`PE2(config-if)#ip address 10.10.10.2/32 secondary`	Configure a secondary IP address, `10.10.10.2/32`, on the loopback interface.
`PE2(config-if)#ip router isis 1`	Enable ISIS routing on a loopback interface `lo` for area 1.
`PE2(config-if)#prefix-sid index 800`	Configure a prefix segment identifier (prefix-SID) index value as `800`.
`PE2(config-if)#exit`	Exit interface mode `lo`.
`PE2(config)#commit`	Commit the transaction.

PE2: Configure SR

The following configurations aim to activate Segment Routing (SR) on PE2 and make MPLS the preferred method for segment routing, optimizing routing efficiency.

`PE2(config)#segment-routing`	Configure segment routing on PE2 device.
`PE2(config-sr)#mpls sr-prefer`	Set MPLS as the preferred segment routing protocol over others.
`PE2(config-sr)#exit`	Exit the router SR mode.
`PE2(config)#commit`	Commit the transaction.

PE2: Global LDP

The configuration on PE2 for the Global LDP router, specifying router ID and targeted peers, is done to set up Label Distribution Protocol (LDP) settings for MPLS.

`PE2(config)#router ldp`	Enter the Router LDP mode.
`PE2(config-router)#router-id 10.10.10.2`	Set the router ID for LDP to `10.10.10.2`.
`PE2(config-router)#transport-address ipv4 10.10.10.2`	Configure the transport address for IPv4 (for IPv6 use ipv6 parameter) to be used for a TCP session where LDP operates. Note: It is preferable to use the loopback address as the transport address.
`PE2(config-router)#targeted-peer ipv4 10.10.10.1`	Configure targeted peer for LDP using IPv4 addresses.
`PE2(config-router-targeted-peer)#exit-targeted-peer-mode`	Exit router targeted-peer-mode.
`PE2(config-router)#targeted-peer ipv4 10.10.10.3`	Configure targeted peer for LDP using IPv4 addresses.
`PE2(config-router-targeted-peer)#exit-targeted-peer-mode`	Exit router targeted-peer-mode.
`PE2(config-router)#targeted-peer ipv4 10.10.10.4`	Configure targeted peer for LDP using IPv4 addresses.
`PE2(config-router-targeted-peer)#exit-targeted-peer-mode`	Exit router targeted-peer-mode.
`PE2(config-router)#exit`	Exit router LDP mode and return to the configure mode.
`PE2(config)#commit`	Commit the transaction.

PE2: Global EVPN MPLS Command

The configuration on PE2 for the Global EVPN MPLS, includes activating EVPN MPLS, defining the global VTEP IP address, enabling hardware profile filtering for EVPN MPLS multi-homing, and activating EVPN MPLS multi-homing functionality, all of which are crucial for enabling EVPN MPLS features.

`PE2(config)#evpn mpls enable`	Activate the EVPN MPLS functionality on `PE2`, enabling it to participate in EVPN MPLS services.
`PE2(config)#commit`	Commit candidate configuration to be running configuration.
`PE2(config)#evpn mpls vtep-ip-global 10.10.10.2`	Configure the global VTEP IP address `10.10.10.2`, associating it with the loopback IP.
`PE2(config)#hardware-profile filter evpn-mpls-mh enable`	Enable hardware-profile filter for EVPN MPLS multi-homing.

`PE2(config)#evpn mpls multihoming enable`	Activate the EVPN MPLS multi-homing functionality, allowing `PE2` to support multi-homed EVPN MPLS services.
`PE2(config)#commit`	Commit the transaction.

PE2: Interface Configuration Network Side

The below configuration is performed to set up network interfaces on PE2 and enable LDP for IPv4, ensuring proper routing and labeling functionality.

`PE2(config)#interface xe4`	Enter interface mode `xe4`.
`PE2(config-if)#ip address 10.1.3.1/30`	Configure an IP address, `10.1.3.1/30`, on the interface `xe4`.
`PE2(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`PE2(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`PE2(config-if)#ip router isis 1`	Enable ISIS routing on an interface `xe4` for area 1.
`PE2(config-if)#exit`	Exit interface mode `xe4`.
`PE2(config)#commit`	Commit the transaction.
`PE2(config)#interface xe5`	Enter interface mode `xe5`.
`PE2(config-if)#ip address 10.1.4.1/30`	Configure an IP address, `10.1.4.1/30`, on the interface `xe5`.
`PE2(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`PE2(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`PE2(config-if)#ip router isis 1`	Enable ISIS routing on an interface `xe5` for area 1.
`PE2(config-if)#exit`	Exit interface mode `xe5`.
`PE2(config)#commit`	Commit the transaction.

PE2: ISIS Configuration

The below configuration is performed to set up ISIS on PE2, to enable MPLS Traffic Engineering, Segment Routing, and other related features for efficient routing and network management.

`PE2(config)#router isis 1`	Enter router ISIS mode.
`PE2(config-router)#is-type level-1-2`	Configure IS-Type as `Level-1-2` specifies that the router will participate in both Level-1 and Level-2 areas within the ISIS network.
`PE2(config-router)#metric-style wide`	Configure the new style of metric type as `wide`.
`PE2(config-router)#mpls traffic-eng router-id 10.10.10.2`	Configure the router's MPLS Traffic Engineering (TE) router ID TLV to `10.10.10.2`, which is used for MPLS-TE path calculations.
`PE2(config-router)#mpls traffic-eng level-1`	Enable MPLS-TE for IS-Type `Level-1` routing.
`PE2(config-router)#mpls traffic-eng level-2`	Enable MPLS-TE for IS-Type `Level-2` routing.

`PE2(config-router)#capability cspf`	Enable Constraint Shortest Path First (CSPF) computation for traffic engineering.
`PE2(config-router)#dynamic-hostname`	Configure the hostname to be advertised for an ISIS instance.
`PE2(config-router)#fast-reroute ti-lfa level-1 proto ipv4`	Configure Remote Loop-Free Alternate (LFA) to calculate backup paths to those destinations whichever does not satisfy basic LFA FRR inequalities
`PE2(config-router)#fast-reroute ti-lfa level-2 proto ipv4`	Configure Remote Loop-Free Alternate (LFA) to calculate backup paths to those destinations whichever does not satisfy basic LFA FRR inequalities
`PE2(config-router)#bfd all-interfaces`	Configure BFD on all interfaces for fast link failure detection.
`PE2(config-router)#net 49.0000.0000.0002.00`	Set a Network Entity Title (NET) for this ISIS instance, specifying the area address and the system ID.
`PE2(config-router)#isis segment-routing global block 17000 23500`	Enable ISIS SR globally and allocates label blocks for Segment Routing.
`PE2(config-router)#segment-routing mpls`	Enable SR ISIS.
`PE2(config-router)#exit`	Exit router ISIS mode and return to configure mode.
`PE2(config)#commit`	Commit the transaction.

PE2: BGP Configuration

The below BGP configuration on PE2 is established to enable BGP routing with ASN 65010, set the BGP router ID, define iBGP neighbors, configure BFD, and enable the EVPN address family for efficient routing in an EVPN environment.

`PE2(config)#router bgp 65010`	Enter the Router BGP mode, ASN: 65010
`PE2(config-router)#bgp router-id 10.10.10.2`	Configure BGP router ID `10.10.10.2`, identifying PE2 within the BGP network.
`PE2(config-router)#neighbor 10.10.10.1 remote-as 65010`	Configure neighbor `10.10.10.1` as an iBGP neighbor with their remote AS number `65010`.
`PE2(config-router)#neighbor 10.10.10.1 update-source lo`	Configure neighbor `10.10.10.1` as an iBGP neighbor, specifying the source of routing updates as the loopback interface.
`PE2(config-router)#neighbor 10.10.10.3 remote-as 65010`	Configure neighbor `10.10.10.3` as an iBGP neighbor with their remote AS number `65010`.
`PE2(config-router)#neighbor 10.10.10.3 update-source lo`	Configure neighbor `10.10.10.3` as an iBGP neighbor, specifying the source of routing updates as the loopback interface.
`PE2(config-router)#neighbor 10.10.10.4 remote-as 65010`	Configure neighbor `10.10.10.4` as an iBGP neighbor with their remote AS number `65010`.
`PE2(config-router)#neighbor 10.10.10.4 update-source lo`	Configure neighbor `10.10.10.4` as an iBGP neighbor, specifying the source of routing updates as the loopback interface.
`PE2(config-router)#neighbor 10.10.10.1 fall-over bfd multihop`	Configure BFD for the BGP neighbor to provide rapid failure detection.
`PE2(config-router)#neighbor 10.10.10.3 fall-over bfd multihop`	Configure BFD for the BGP neighbor to provide rapid failure detection.
`PE2(config-router)#neighbor 10.10.10.4 fall-over bfd multihop`	Configure BFD for the BGP neighbor to provide rapid failure detection.

`PE2(config-router)#neighbor 10.10.10.1 advertisement-interval 0`	Configure advertisement interval for the neighbor, allowing more frequent BGP updates.
`PE2(config-router)#neighbor 10.10.10.3 advertisement-interval 0`	Configure advertisement interval for the neighbor, allowing more frequent BGP updates.
`PE2(config-router)#neighbor 10.10.10.4 advertisement-interval 0`	Configure advertisement interval for the neighbor, allowing more frequent BGP updates.
`PE2(config-router)#address-family l2vpn evpn`	Enter into address family mode for L2VPN EVPN.
`PE2(config-router-af)#neighbor 10.10.10.1 activate`	Activate EVPN for iBGP neighbor `10.10.10.1` within the address family mode, ensuring that EVPN address family is enabled for the neighbor.
`PE2(config-router-af)#neighbor 10.10.10.3 activate`	Activate EVPN for iBGP neighbor `10.10.10.3` within the address family mode, ensuring that EVPN address family is enabled for the neighbor.
`PE2(config-router-af)#neighbor 10.10.10.4 activate`	Activate EVPN for iBGP neighbor `10.10.10.4` within the address family mode, ensuring that EVPN address family is enabled for the neighbor.
`PE2(config-router-af)#exit`	Exit address family mode and return to the router BGP mode.
`PE2(config-router)#commit`	Commit the transaction.
`PE2(config-router)#exit`	Exit router BGP mode and return to the configure mode.

PE2: MAC VRF Configuration

The below MAC VRF configuration on PE2 is carried out to define and set up VRFs named `vrf2` and `vpls1001` with specific Route-Distinguisher (RD) and route-target values, ensuring segregated MAC address spaces for distinct network services.

`PE2(config)#mac vrf vrf2`	Enter VRF mode named `vrf2`.
`PE2(config-vrf)#rd 10.10.10.2:1700`	Configure Route-Distinguisher value of `10.10.10.2:1700`.
`PE2(config-vrf)#route-target both 1700:1700`	Configure import and export values for the `vrf2` as `1700:1700`.
`PE2(config-vrf)#exit`	Exit VRF mode and return to the configure mode.
`PE2(config)#mac vrf vpls1001`	Enter VRF mode named `vpls1001`.
`PE2(config-vrf)#rd 10.10.10.2:1001`	Configure Route-Distinguisher value of `10.10.10.2:1001`.
`PE2(config-vrf)#route-target both 1001:1001`	Configure import and export values for the `vpls1001` as `1001:1001`.
`PE2(config-vrf)#exit`	Exit VRF mode and return to the configure mode.
`PE2(config)#commit`	Commit the transaction.

PE2: EVPN and VRF Mapping

The below EVPN and VRF mapping configuration on PE2 is performed to establish mappings between EVPN identifiers and VRFs, facilitating efficient routing and connectivity in an EVPN network environment.

`PE2(config)#evpn mpls id 1800 xconnect target-mpls-id 1700`	Configure the EVPN-VPWS identifier with a source identifier of `1800` and a target identifier of `1700`.
`PE2(config-evpn-mpls)#host-reachability-protocol evpn-bgp vrf2`	Map VRF `vrf2` to the EVPN-VPWS identifier

`PE2(config-evpn-mpls)#evpn mpls id 3000`	Configure the EVPN-VPLS identifier an identifier of `3000`.
`PE2(config-evpn-mpls)#host-reachability-protocol evpn-bgp vpls1001`	Map VRF `vpls1001` to the EVPN-VPWS identifier
`PE2(config-evpn-mpls)#commit`	Commit the transaction.
`PE2(config-evpn-mpls)#exit`	Exit the EVPN MPLS mode and return to the configure mode.

PE2: Access Port Configuration for Port-active

The below access port configuration for port-active mode on PE2 is carried out to configure various parameters including system-mac, load balancing, service carving preferences, and EVPN settings for efficient network access and connectivity.

`PE2(config)#interface po1`	Enter the port channel interface mode for `po1`
`PE2(config-if)#load-interval 30`	Set the load interval to `30`.
`PE2(config-if)#evpn multi-homed system-mac 0000.1111.7777 load-balancing port-active`	Configure the system-mac address `0000.1111.7777` for port-active mode, which plays a role in load balancing and enter to the EVPN Ethernet Segment (ES) mode.
`PE2(config-if-es)#service-carving auto`	Configure service carving as `auto`, allowing automatic determination of service distribution preferences.
`PE2(config-if-es)#exit`	Exit the EVPN ES mode and return to the configure mode.
`PE2(config-if)#exit`	Exit interface mode `po1` and return to the configure mode.
`PE2(config)#commit`	Commit the transaction.
`PE2(config)#interface po1.1 switchport`	Create a Layer 2 sub-interface `po1.1` within the port channel.
`PE2(config-if)#encapsulation dot1q 100`	Set encapsulation to dot1q with VLAN ID `100`.
`PE2(config-if)#load-interval 30`	Set the load interval to `30`.
`PE2(config-if)#access-if-evpn`	Enter the access mode for EVPN MPLS ID configuration.
`PE2(config-acc-if-evpn)#map vpn-id 1800`	Map VPN-ID `1800`.
`PE2(config-acc-if-evpn)#exit`	Exit the access mode and return to the interface mode.
`PE2(config-if)#exit`	Exit interface mode `po1.1` and return to the configure mode.
`PE2(config)#interface xe8`	Enter the interface mode for `xe8.`
`PE2(config-if)#speed 10g`	Set the speed to `10g`.
`PE2(config-if)#channel-group 1 mode active`	Attach LAG interface `po1.`
`PE2(config-if)#exit`	Exit interface mode `xe8` and return to the configure mode.
`PE2(config)#commit`	Commit the transaction.

PE2: Access Port Configuration for Single-active

The below access port configuration for single-active mode on PE2 is implemented to set up various parameters, including Ethernet Segment Identifier (ESI) settings, service carving preferences, and EVPN configurations, ensuring efficient network access and connectivity.

`PE2(config)#interface sa2`	Enter the single active interface mode for `sa2.`
`PE2(config-if)#load-interval 30`	Set the load interval to `30`.

`PE2(config-if)#evpn multi-homed esi 00:00:11:11:77:77 load-balancing single-active`	Configure the ESI with the value with the value `00:00:11:11:77:77` for single-active mode, which plays a role in load balancing and enter to the EVPN Ethernet Segment (ES) mode.
`PE2(config-if-es)#service-carving auto`	Configure service carving as `auto`, allowing automatic determination of service distribution preferences.
`PE2(config-if-es)#exit`	Exit the EVPN ES mode and return to the configure mode.
`PE2(config-if)#exit`	Exit interface mode `sa2` and return to the configure mode.
`PE2(config)#commit`	Commit the transaction.
`PE2(config)#interface sa2.1 switchport`	Create a Layer 2 sub-interface `sa2.1` within the port channel.
`PE2(config-if)#encapsulation dot1q 100`	Set encapsulation to dot1q with VLAN ID `100`.
`PE2(config-if)#load-interval 30`	Set the load interval to `30`.
`PE2(config-if)#access-if-evpn`	Enter the access mode for EVPN MPLS ID configuration.
`PE2(config-acc-if-evpn)#map vpn-id 1800`	Map VPN-ID `1800`.
`PE2(config-acc-if-evpn)#exit`	Exit the access mode and return to the interface mode.
`PE2(config-if)#exit`	Exit interface mode `sa2.1` and return to the configure mode.
`PE2(config)#interface xe8`	Enter the interface mode for `xe8`.
`PE2(config-if)#speed 10g`	Set the speed to `10g`.
`PE2(config-if)#static-channel-group 2`	Attach the static-channel-group 2, the LAG interface `sa2` to `xe8`.
`PE2(config-if)#exit`	Exit interface mode `xe8` and return to the configure mode.
`PE2(config)#commit`	Commit the transaction.

P1: Loopback Interface

The configuration on P1 for a loopback interface with IP address `10.10.10.5/32` secondary is set up to provide IP connectivity for the router.

`P1#configure terminal`	Enter configure mode.
`P1(config)#interface lo`	Enter the interface mode for the loopback interface `lo`.
`P1(config-if)#ip address 10.10.10.5/32 secondary`	Configure a secondary IP address, `10.10.10.5/32`, on the loopback interface.
`P1(config-if)#ip router isis 1`	Enable ISIS routing on a loopback interface `lo` for area 1.
`P1(config-if)#prefix-sid index 800`	Configure a prefix segment identifier (prefix-SID) index value as `800`.
`P1(config-if)#exit`	Exit interface mode `lo`.
`P1(config)#commit`	Commit the transaction.

P1: Configure SR

The following configurations aim to activate Segment Routing (SR) on P1 and make MPLS the preferred method for segment routing, optimizing routing efficiency.

`P1(config)#segment-routing`	Configure segment routing on P1 device.
`P1(config-sr)#mpls sr-prefer`	Set MPLS as the preferred segment routing protocol over others.
`P1(config-sr)#exit`	Exit the router SR mode.
`P1(config)#commit`	Commit the transaction.

P1: Global LDP

The configuration on P1 for the Global LDP router, specifying router ID and targeted peer, is done to set up Label Distribution Protocol (LDP) settings for MPLS.

`P1(config)#router ldp`	Enter the Router LDP mode.
`P1(config-router)#router-id 10.10.10.5`	Set the router ID for LDP to `10.10.10.5`.
`P1(config-router)#transport-address ipv4 10.10.10.5`	Configure the transport address for IPv4 (for IPv6 use ipv6 parameter) to be used for a TCP session where LDP operates. Note: It is preferable to use the loopback address as the transport address.
`P1(config-router)#exit`	Exit router LDP mode and return to the configure mode.
`P1(config)#commit`	Commit the transaction.

P1: Interface Configuration

The below configuration is performed to set up interfaces on P1 and enable LDP for IPv4, ensuring proper routing and labeling functionality.

`P1(config)#interface xe1`	Enter interface mode `xe1`.
`P1(config-if)#ip address 10.1.1.2/30`	Configure an IP address, `10.1.1.2/30`, on the interface `xe1`.
`P1(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`P1(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`P1(config-if)#ip router isis 1`	Enable ISIS routing on an interface `xe1` for area 1.
`P1(config-if)#exit`	Exit interface mode `xe1`.
`P1(config)#commit`	Commit the transaction.
`P1(config)#interface xe2`	Enter interface mode `xe2`.
`P1(config-if)#ip address 10.1.4.2/30`	Configure an IP address, `10.1.4.2/30`, on the interface `xe2`.
`P1(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`P1(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`P1(config-if)#ip router isis 1`	Enable ISIS routing on an interface `xe2` for area 1.
`P1(config-if)#exit`	Exit interface mode `xe2`.

`P1(config)#commit`	Commit the transaction.
`P1(config)#interface xe3`	Enter interface mode `xe3`.
`P1(config-if)#ip address 10.1.5.2/30`	Configure an IP address, `10.1.5.2/30`, on the interface `xe3`.
`P1(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`P1(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`P1(config-if)#ip router isis 1`	Enable ISIS routing on an interface `xe3` for area 1.
`P1(config-if)#exit`	Exit interface mode `xe3`.
`P1(config)#commit`	Commit the transaction.
`P1(config)#interface xe4`	Enter interface mode `xe4`.
`P1(config-if)#ip address 10.1.6.2/30`	Configure an IP address, `10.1.6.2/30`, on the interface `xe4`.
`P1(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`P1(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`P1(config-if)#ip router isis 1`	Enable ISIS routing on an interface `xe4` for area 1.
`P1(config-if)#exit`	Exit interface mode `xe4`.
`P1(config)#commit`	Commit the transaction.

P1: ISIS Configuration

The below configuration is performed to set up ISIS on P1, to enable MPLS Traffic Engineering, Segment Routing, and other related features for efficient routing and network management.

`P1(config)#router isis 1`	Enter router ISIS mode.
`P1(config-router)#is-type level-1-2`	Configure IS-Type as `Level-1-2` specifies that the router will participate in both Level-1 and Level-2 areas within the ISIS network.
`P1(config-router)#metric-style wide`	Configure the new style of metric type as `wide`.
`P1(config-router)#mpls traffic-eng router-id 10.10.10.5`	Configure the router's MPLS Traffic Engineering (TE) router ID TLV to `10.10.10.5`, which is used for MPLS-TE path calculations.
`P1(config-router)#mpls traffic-eng level-1`	Enable MPLS-TE for IS-Type `Level-1` routing.
`P1(config-router)#mpls traffic-eng level-2`	Enable MPLS-TE for IS-Type `Level-2` routing.
`P1(config-router)#capability cspf`	Enable Constraint Shortest Path First (CSPF) computation for traffic engineering.
`P1(config-router)#dynamic-hostname`	Configure the hostname to be advertised for an ISIS instance.
`P1(config-router)#fast-reroute ti-lfa level-1 proto ipv4`	Configure Remote Loop-Free Alternate (LFA) to calculate backup paths to those destinations whichever does not satisfy basic LFA FRR inequalities
`P1(config-router)#fast-reroute ti-lfa level-2 proto ipv4`	Configure Remote Loop-Free Alternate (LFA) to calculate backup paths to those destinations whichever does not satisfy basic LFA FRR inequalities

`P1(config-router)#bfd all-interfaces`	Configure BFD on all interfaces for fast link failure detection.
`P1(config-router)#net 49.0000.0000.0005.00`	Set a Network Entity Title (NET) for this ISIS instance, specifying the area address and the system ID.
`P1(config-router)#isis segment-routing global block 17000 23500`	Enable ISIS SR globally and allocates label blocks for Segment Routing.
`P1(config-router)#segment-routing mpls`	Enable SR ISIS.
`P1(config-router)#exit`	Exit router ISIS mode and return to the configure mode.
`P1(config)#commit`	Commit the transaction.

P2: Loopback Interface

The configuration on P2 for a loopback interface with IP address `10.10.10.6/32` secondary is set up to provide IP connectivity for the router.

`P2#configure terminal`	Enter configure mode.
`P2(config)#interface lo`	Enter the interface mode for the loopback interface `lo`.
`P2(config-if)#ip address 10.10.10.6/32 secondary`	Configure a secondary IP address, `10.10.10.6/32`, on the loopback interface.
`P2(config-if)#ip router isis 1`	Enable ISIS routing on a loopback interface `lo` for area 1.
`P2(config-if)#prefix-sid index 800`	Configure a prefix segment identifier (prefix-SID) index value as `800`.
`P2(config-if)#exit`	Exit interface mode `lo`.
`P2(config)#commit`	Commit the transaction.

P2: Configure SR

The following configurations aim to activate Segment Routing (SR) on P2 and make MPLS the preferred method for segment routing, optimizing routing efficiency.

`P2(config)#segment-routing`	Configure segment routing on P2 device.
`P2(config-sr)#mpls sr-prefer`	Set MPLS as the preferred segment routing protocol over others.
`P2(config-sr)#exit`	Exit the router SR mode.
`P2(config)#commit`	Commit the transaction.

P2: Global LDP

The configuration on P2 for the Global LDP router, specifying router ID and targeted peer, is done to set up Label Distribution Protocol (LDP) settings for MPLS.

`P2(config)#router ldp`	Enter the Router LDP mode.
`P2(config-router)#router-id 10.10.10.6`	Set the router ID for LDP to `10.10.10.6`.
`P2(config-router)#transport-address ipv4 10.10.10.6`	Configure the transport address for IPv4 (for IPv6 use ipv6 parameter) to be used for a TCP session where LDP operates. Note: It is preferable to use the loopback address as the transport address.

`P2(config-router)#exit`	Exit router LDP mode and return to the configure mode.
`P2(config)#commit`	Commit the transaction.

P2: Interface Configuration

The below configuration is performed to set up interfaces on P2 and enable LDP for IPv4, ensuring proper routing and labeling functionality.

`P2(config)#interface xe12`	Enter interface mode `xe12`.
`P2(config-if)#ip address 10.1.2.2/30`	Configure an IP address, `10.1.2.2/30`, on the interface `xe12`.
`P2(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`P2(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`P2(config-if)#ip router isis 1`	Enable ISIS routing on an interface `xe12` for area 1.
`P2(config-if)#exit`	Exit interface mode `xe12`.
`P2(config)#commit`	Commit the transaction.
`P2(config)#interface xe13`	Enter interface mode `xe13`.
`P2(config-if)#ip address 10.1.3.2/30`	Configure an IP address, `10.1.3.2/30`, on the interface `xe13`.
`P2(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`P2(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`P2(config-if)#ip router isis 1`	Enable ISIS routing on an interface `xe13` for area 1.
`P2(config-if)#exit`	Exit interface mode `xe13`.
`P2(config)#commit`	Commit the transaction.
`P2(config)#interface xe11`	Enter interface mode `xe11`.
`P2(config-if)#ip address 10.1.7.2/30`	Configure an IP address, `10.1.7.2/30`, on the interface `xe11`.
`P2(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`P2(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`P2(config-if)#ip router isis 1`	Enable ISIS routing on an interface `xe11` for area 1.
`P2(config-if)#exit`	Exit interface mode `xe11`.
`P2(config)#commit`	Commit the transaction.
`P2(config)#interface xe14`	Enter interface mode `xe14`.
`P2(config-if)#ip address 10.1.8.2/30`	Configure an IP address, `10.1.8.2/30`, on the interface `xe14`.
`P2(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.

`P2(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`P2(config-if)#ip router isis 1`	Enable ISIS routing on an interface `xe14` for area 1.
`P2(config-if)#exit`	Exit interface mode `xe14`.
`P2(config)#commit`	Commit the transaction.

P2: ISIS Configuration

The below configuration is performed to set up ISIS on P2, to enable MPLS Traffic Engineering, Segment Routing, and other related features for efficient routing and network management.

`P2(config)#router isis 1`	Enter router ISIS mode.
`P2(config-router)#is-type level-1-2`	Configure IS-Type as `Level-1-2` specifies that the router will participate in both Level-1 and Level-2 areas within the ISIS network.
`P2(config-router)#metric-style wide`	Configure the new style of metric type as `wide`.
`P2(config-router)#mpls traffic-eng router-id 10.10.10.6`	Configure the router's MPLS Traffic Engineering (TE) router ID TLV to `10.10.10.6`, which is used for MPLS-TE path calculations.
`P2(config-router)#mpls traffic-eng level-1`	Enable MPLS-TE for IS-Type `Level-1` routing.
`P2(config-router)#mpls traffic-eng level-2`	Enable MPLS-TE for IS-Type `Level-2` routing.
`P2(config-router)#capability cspf`	Enable Constraint Shortest Path First (CSPF) computation for traffic engineering.
`P2(config-router)#dynamic-hostname`	Configure the hostname to be advertised for an ISIS instance.
`P2(config-router)#fast-reroute ti-lfa level-1 proto ipv4`	Configure Remote Loop-Free Alternate (LFA) to calculate backup paths to those destinations whichever does not satisfy basic LFA FRR inequalities
`P2(config-router)#fast-reroute ti-lfa level-2 proto ipv4`	Configure Remote Loop-Free Alternate (LFA) to calculate backup paths to those destinations whichever does not satisfy basic LFA FRR inequalities
`P2(config-router)#bfd all-interfaces`	Configure BFD on all interfaces for fast link failure detection.
`P2(config-router)#net 49.0000.0000.0006.00`	Set a Network Entity Title (NET) for this ISIS instance, specifying the area address and the system ID.
`P2(config-router)#isis segment-routing global block 17000 23500`	Enable ISIS SR globally and allocates label blocks for Segment Routing.
`P2(config-router)#segment-routing mpls`	Enable SR ISIS.
`P2(config-router)#exit`	Exit router ISIS mode and return to the configure mode.
`P2(config)#commit`	Commit the transaction.

PE3: Loopback Interface

The configuration on PE3 for a loopback interface with IP address `10.10.10.3/32` secondary is set up to provide IP connectivity for the router.

`PE3#configure terminal`	Enter configure mode.
`PE3(config)#interface lo`	Enter the interface mode for the loopback interface `lo`.
`PE3(config-if)#ip address 10.10.10.3/32 secondary`	Configure a secondary IP address, `10.10.10.3/32`, on the loopback interface.

`PE3(config-if)#ip router isis 1`	Enable ISIS routing on a loopback interface `lo` for area 1.
`PE3(config-if)#prefix-sid index 800`	Configure a prefix segment identifier (prefix-SID) index value as `800`.
`PE3(config-if)#exit`	Exit interface mode `lo`.
`PE3(config)#commit`	Commit the transaction.

PE3: Configure SR

The following configurations aim to activate Segment Routing (SR) on PE3 and make MPLS the preferred method for segment routing, optimizing routing efficiency.

`PE3(config)#segment-routing`	Configure segment routing on PE3 device.
`PE3(config-sr)#mpls sr-prefer`	Set MPLS as the preferred segment routing protocol over others.
`PE3(config-sr)#exit`	Exit the router SR mode.
`PE3(config)#commit`	Commit the transaction.

PE3: Global LDP

The configuration on PE3 for the Global LDP router, specifying router ID and targeted peers, is done to set up Label Distribution Protocol (LDP) settings for MPLS.

`PE3(config)#router ldp`	Enter the Router LDP mode.
`PE3(config-router)#router-id 10.10.10.3`	Set the router ID for LDP to `10.10.10.3`.
`PE2(config-router)#transport-address ipv4 10.10.10.3`	Configure the transport address for IPv4 (for IPv6 use ipv6 parameter) to be used for a TCP session where LDP operates. Note: It is preferable to use the loopback address as the transport address.
`PE3(config-router)#targeted-peer ipv4 10.10.10.1`	Configure targeted peer for LDP using IPv4 addresses.
`PE3(config-router-targeted-peer)#exit-targeted-peer-mode`	Exit router targeted-peer-mode.
`PE3(config-router)#targeted-peer ipv4 10.10.10.2`	Configure targeted peer for LDP using IPv4 addresses.
`PE3(config-router-targeted-peer)#exit-targeted-peer-mode`	Exit router targeted-peer-mode.
`PE3(config-router)#targeted-peer ipv4 10.10.10.4`	Configure targeted peer for LDP using IPv4 addresses.
`PE3(config-router-targeted-peer)#exit-targeted-peer-mode`	Exit router targeted-peer-mode.
`PE3(config-router)#exit`	Exit router LDP mode and return to the configure mode.
`PE3(config)#commit`	Commit the transaction.

PE3: Global EVPN MPLS Command

The configuration on PE3 for the Global EVPN MPLS, includes activating EVPN MPLS, defining the global VTEP IP address, enabling hardware profile filtering for EVPN MPLS multi-homing, and activating EVPN MPLS multi-homing functionality, all of which are crucial for enabling EVPN MPLS features.

`PE3(config)#evpn mpls enable`	Activate the EVPN MPLS functionality on `PE3`, enabling it to participate in EVPN MPLS services.
`PE3(config)#commit`	Commit candidate configuration to be running configuration.
`PE3(config)#evpn mpls vtep-ip-global 10.10.10.3`	Configure the global VTEP IP address `10.10.10.3`, associating it with the loopback IP.
`PE3(config)#hardware-profile filter evpn-mpls-mh enable`	Enable hardware-profile filter for EVPN MPLS multi-homing.
`PE3(config)#evpn mpls multihoming enable`	Activate the EVPN MPLS multi-homing functionality, allowing `PE3` to support multi-homed EVPN MPLS services.
`PE3(config)#commit`	Commit the transaction.

PE3: Interface Configuration Network Side

The below configuration is performed to set up network interfaces on PE3 and enable LDP for IPv4, ensuring proper routing and labeling functionality.

`PE3(config)#interface xe1`	Enter interface mode `xe1`.
`PE3(config-if)#ip address 10.1.6.1/30`	Configure an IP address, `10.1.6.1/30`, on the interface `xe1`.
`PE3(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`PE3(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`PE3(config-if)#ip router isis 1`	Enable ISIS routing on an interface `xe1` for area 1.
`PE3(config-if)#exit`	Exit interface mode `xe1`.
`PE3(config)#commit`	Commit the transaction.
`PE3(config)#interface xe5`	Enter interface mode `xe5`.
`PE3(config-if)#ip address 10.1.7.1/30`	Configure an IP address, `10.1.7.1/30`, on the interface `xe5`.
`PE3(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`PE3(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`PE3(config-if)#ip router isis 1`	Enable ISIS routing on an interface `xe5` for area 1.
`PE3(config-if)#exit`	Exit interface mode `xe5`.
`PE3(config)#commit`	Commit the transaction.

PE3: ISIS Configuration

The below configuration is performed to set up ISIS on PE3, to enable MPLS Traffic Engineering, Segment Routing, and other related features for efficient routing and network management.

`PE3(config)#router isis 1`	Enter router ISIS mode.
`PE3(config-router)#is-type level-1-2`	Configure IS-Type as `Level-1-2` specifies that the router will participate in both Level-1 and Level-2 areas within the ISIS network.
`PE3(config-router)#metric-style wide`	Configure the new style of metric type as `wide`.
`PE3(config-router)#mpls traffic-eng router-id 10.10.10.3`	Configure the router's MPLS Traffic Engineering (TE) router ID TLV to `10.10.10.3`, which is used for MPLS-TE path calculations.
`PE3(config-router)#mpls traffic-eng level-1`	Enable MPLS-TE for IS-Type `Level-1` routing.
`PE3(config-router)#mpls traffic-eng level-2`	Enable MPLS-TE for IS-Type `Level-2` routing.
`PE3(config-router)#capability cspf`	Enable Constraint Shortest Path First (CSPF) computation for traffic engineering.
`PE3(config-router)#dynamic-hostname`	Configure the hostname to be advertised for an ISIS instance.
`PE3(config-router)#fast-reroute ti-lfa level-1 proto ipv4`	Configure Remote Loop-Free Alternate (LFA) to calculate backup paths to those destinations whichever does not satisfy basic LFA FRR inequalities
`PE3(config-router)#fast-reroute ti-lfa level-2 proto ipv4`	Configure Remote Loop-Free Alternate (LFA) to calculate backup paths to those destinations whichever does not satisfy basic LFA FRR inequalities
`PE3(config-router)#bfd all-interfaces`	Configure BFD on all interfaces for fast link failure detection.
`PE3(config-router)#net 49.0000.0000.0003.00`	Set a Network Entity Title (NET) for this ISIS instance, specifying the area address and the system ID.
`PE3(config-router)#isis segment-routing global block 17000 23500`	Enable ISIS SR globally and allocates label blocks for Segment Routing.
`PE3(config-router)#segment-routing mpls`	Enable SR ISIS.
`PE3(config-router)#exit`	Exit router ISIS mode and return to the configure mode.
`PE3(config)#commit`	Commit the transaction.

PE3: BGP Configuration

The below BGP configuration on PE3 is established to enable BGP routing with ASN 65010, set the BGP router ID, define iBGP neighbors, configure BFD, and enable the EVPN address family for efficient routing in an EVPN environment.

`PE3(config)#router bgp 65010`	Enter the Router BGP mode, ASN: 65010
`PE3(config-router)#bgp router-id 10.10.10.3`	Configure BGP router ID `10.10.10.3`, identifying PE3 within the BGP network.
`PE3(config-router)#neighbor 10.10.10.1 remote-as 65010`	Configure neighbor `10.10.10.1` as an iBGP neighbor with their remote AS number `65010`.
`PE3(config-router)#neighbor 10.10.10.1 update-source lo`	Configure neighbor `10.10.10.1` as an iBGP neighbor, specifying the source of routing updates as the loopback interface.
`PE3(config-router)#neighbor 10.10.10.2 remote-as 65010`	Configure neighbor `10.10.10.2` as an iBGP neighbor with their remote AS number `65010`.
`PE3(config-router)#neighbor 10.10.10.2 update-source lo`	Configure neighbor `10.10.10.2` as an iBGP neighbor, specifying the source of routing updates as the loopback interface.

`PE3(config-router)#neighbor 10.10.10.4 remote-as 65010`	Configure neighbor `10.10.10.4` as an iBGP neighbor with their remote AS number `65010`.
`PE3(config-router)#neighbor 10.10.10.4 update-source lo`	Configure neighbor `10.10.10.4` as an iBGP neighbor, specifying the source of routing updates as the loopback interface.
`PE3(config-router)#neighbor 10.10.10.1 fall-over bfd multihop`	Configure BFD for the BGP neighbor to provide rapid failure detection.
`PE3(config-router)#neighbor 10.10.10.2 fall-over bfd multihop`	Configure BFD for the BGP neighbor to provide rapid failure detection.
`PE3(config-router)#neighbor 10.10.10.4 fall-over bfd multihop`	Configure BFD for the BGP neighbor to provide rapid failure detection.
`PE3(config-router)#neighbor 10.10.10.1 advertisement-interval 0`	Configure advertisement interval for the neighbor, allowing more frequent BGP updates.
`PE3(config-router)#neighbor 10.10.10.2 advertisement-interval 0`	Configure advertisement interval for the neighbor, allowing more frequent BGP updates.
`PE3(config-router)#neighbor 10.10.10.4 advertisement-interval 0`	Configure advertisement interval for the neighbor, allowing more frequent BGP updates.
`PE3(config-router)#address-family l2vpn evpn`	Enter into address family mode for L2VPN EVPN.
`PE3(config-router-af)#neighbor 10.10.10.1 activate`	Activate EVPN for iBGP neighbor `10.10.10.1` within the address family mode, ensuring that EVPN address family is enabled for the neighbor.
`PE3(config-router-af)#neighbor 10.10.10.2 activate`	Activate EVPN for iBGP neighbor `10.10.10.2` within the address family mode, ensuring that EVPN address family is enabled for the neighbor.
`PE3(config-router-af)#neighbor 10.10.10.4 activate`	Activate EVPN for iBGP neighbor `10.10.10.4` within the address family mode, ensuring that EVPN address family is enabled for the neighbor.
`PE3(config-router-af)#exit`	Exit address family mode and return to the router BGP mode.
`PE3(config-router)#commit`	Commit the transaction.
`PE3(config-router)#exit`	Exit router BGP mode and return to the configure mode.

PE3: MAC VRF Configuration

The below MAC VRF configuration on PE3 is carried out to define and set up VRFs named `vrf2` and `vpls1001` with specific Route-Distinguisher (RD) and route-target values, ensuring segregated MAC address spaces for distinct network services.

`PE3(config)#mac vrf vrf2`	Enter VRF mode named `vrf2`.
`PE3(config-vrf)#rd 10.10.10.3:1700`	Configure Route-Distinguisher value of `10.10.10.3:1700`.
`PE3(config-vrf)#route-target both 1700:1700`	Configure import and export values for the `vrf2` as `1700:1700`.
`PE3(config-vrf)#exit`	Exit VRF mode and return to the configure mode.
`PE3(config)#mac vrf vpls1001`	Enter VRF mode named `vpls1001`.
`PE3(config-vrf)#rd 10.10.10.3:1001`	Configure Route-Distinguisher value of `10.10.10.3:1001`.
`PE3(config-vrf)#route-target both 1001:1001`	Configure import and export values for the `vpls1001` as `1001:1001`.

`PE3(config-vrf)#exit`	Exit VRF mode and return to the configure mode.
`PE3(config)#commit`	Commit the transaction.

PE3: EVPN and VRF Mapping

The below EVPN and VRF mapping configuration on PE3 is performed to establish mappings between EVPN identifiers and VRFs, facilitating efficient routing and connectivity in an EVPN network environment.

`PE3(config)#evpn mpls id 1700 xconnect target-mpls-id 1800`	Configure the EVPN-VPWS identifier with a source identifier of `1700` and a target identifier of `1800`.
`PE3(config-evpn-mpls)#host-reachability-protocol evpn-bgp vrf2`	Map VRF `vrf2` to the EVPN-VPWS identifier
`PE3(config-evpn-mpls)#evpn mpls id 3000`	Configure the EVPN-VPLS identifier an identifier of `3000`.
`PE3(config-evpn-mpls)#host-reachability-protocol evpn-bgp vpls1001`	Map VRF `vpls1001` to the EVPN-VPWS identifier
`PE3(config-evpn-mpls)#commit`	Commit the transaction.
`PE3(config-evpn-mpls)#exit`	Exit the EVPN MPLS mode and return to the configure mode.

PE3: Access Port Configuration for Port-active

The below access port configuration for port-active mode on PE3 is carried out to configure various parameters including system-MAC, load balancing, service carving preferences, and EVPN settings for efficient network access and connectivity.

`PE3(config)#interface po1`	Enter the port channel interface mode for `po1`
`PE3(config-if)#load-interval 30`	Set the load interval to `30`.
`PE3(config-if)#evpn multi-homed system-mac 0000.2222.7777 load-balancing port-active`	Configure the system-mac address `0000.2222.7777` for port-active mode, which plays a role in load balancing and enter to the EVPN Ethernet Segment (ES) mode.
`PE3(config-if-es)#service-carving auto`	Configure service carving as `auto`, allowing automatic determination of service distribution preferences.
`PE3(config-if-es)#exit`	Exit the EVPN ES mode and return to the configure mode.
`PE3(config-if)#exit`	Exit interface mode `po1` and return to the configure mode.
`PE3(config)#commit`	Commit the transaction.
`PE3(config)#interface po1.1 switchport`	Create a Layer 2 sub-interface `po1.1` within the port channel.
`PE3(config-if)#encapsulation dot1q 100`	Set encapsulation to dot1q with VLAN ID `100`.
`PE3(config-if)#load-interval 30`	Set the load interval to `30`.
`PE3(config-if)#access-if-evpn`	Enter the access mode for EVPN MPLS ID configuration.
`PE3(config-acc-if-evpn)#map vpn-id 1800`	Map VPN-ID `1800`.
`PE3(config-acc-if-evpn)#exit`	Exit the access mode and return to the interface mode.
`PE3(config-if)#exit`	Exit interface mode `po1.1` and return to the configure mode.
`PE3(config)#interface xe2`	Enter the interface mode for `xe2`.
`PE3(config-if)#speed 10g`	Set the speed to `10g`.
`PE3(config-if)#channel-group 1 mode active`	Attach LAG interface `po1`.

`PE3(config-if)#exit`	Exit interface mode `xe2` and return to the configure mode.
`PE3(config)#commit`	Commit the transaction.

PE3: Access Port Configuration for Single-active

The below access port configuration for single-active mode on PE3 is implemented to set up various parameters, including Ethernet Segment Identifier (ESI) settings, service carving preferences, and EVPN configurations, ensuring efficient network access and connectivity.

`PE3(config)#interface sa1`	Enter the single active interface mode for `sa1.`
`PE3(config-if)#load-interval 30`	Set the load interval to `30`.
`PE3(config-if)#evpn multi-homed esi 00:00:22:22:77:77 load-balancing single-active`	Configure the ESI with the value with the value `00:00:22:22:77:77` for single-active mode, which plays a role in load balancing and enter to the EVPN Ethernet Segment (ES) mode.
`PE3(config-if-es)#service-carving auto`	Configure service carving as `auto`, allowing automatic determination of service distribution preferences.
`PE3(config-if-es)#exit`	Exit the EVPN ES mode and return to the configure mode.
`PE3(config-if)#exit`	Exit interface mode `sa1` and return to the configure mode.
`PE3(config)#commit`	Commit the transaction.
`PE3(config)#interface sa1.1 switchport`	Create a Layer 2 sub-interface `sa1.1` within the port channel.
`PE3(config-if)#encapsulation dot1q 100`	Set encapsulation to dot1q with VLAN ID `100`.
`PE3(config-if)#load-interval 30`	Set the load interval to `30`.
`PE3(config-if)#access-if-evpn`	Enter the access mode for EVPN MPLS ID configuration.
`PE3(config-acc-if-evpn)#map vpn-id 1800`	Map VPN-ID `1800`.
`PE3(config-acc-if-evpn)#exit`	Exit the access mode and return to the interface mode.
`PE3(config-if)#exit`	Exit interface mode `sa1.1` and return to the configure mode.
`PE3(config)#interface xe2`	Enter the interface mode for `xe2.`
`PE3(config-if)#speed 10g`	Set the speed to `10g`.
`PE3(config-if)#static-channel-group 1`	Attach the static-channel-group 1, the LAG interface `sa1` to `xe2`.
`PE3(config-if)#exit`	Exit interface mode `xe2` and return to the configure mode.
`PE3(config)#commit`	Commit the transaction.

PE4: Loopback Interface

The configuration on PE4 for a loopback interface with IP address `10.10.10.4/32` secondary is set up to provide IP connectivity for the router.

`PE4#configure terminal`	Enter configure mode.
`PE4(config)#interface lo`	Enter the interface mode for the loopback interface `lo`.
`PE4(config-if)#ip address 10.10.10.4/32 secondary`	Configure a secondary IP address, `10.10.10.4/32`, on the loopback interface.
`PE4(config-if)#ip router isis 1`	Enable ISIS routing on a loopback interface `lo` for area 1.

`PE4(config-if)#prefix-sid index 800`	Configure a prefix segment identifier (prefix-SID) index value as `800`.
`PE4(config-if)#exit`	Exit interface mode `lo`.
`PE4(config)#commit`	Commit the transaction.

PE4: Configure SR

The following configurations aim to activate Segment Routing (SR) on PE4 and make MPLS the preferred method for segment routing, optimizing routing efficiency.

`PE4(config)#segment-routing`	Configure segment routing on PE4 device.
`PE4(config-sr)#mpls sr-prefer`	Set MPLS as the preferred segment routing protocol over others.
`PE4(config-sr)#exit`	Exit the router SR mode.
`PE4(config)#commit`	Commit the transaction.

PE4: Global LDP

The configuration on PE4 for the Global LDP router, specifying router ID and targeted peers, is done to set up Label Distribution Protocol (LDP) settings for MPLS.

`PE4(config)#router ldp`	Enter the Router LDP mode.
`PE4(config-router)#router-id 10.10.10.4`	Set the router ID for LDP to `10.10.10.4`.
`PE4(config-router)#transport-address ipv4 10.10.10.4`	Configure the transport address for IPv4 (for IPv6 use ipv6 parameter) to be used for a TCP session where LDP operates. Note: It is preferable to use the loopback address as the transport address.
`PE4(config-router)#targeted-peer ipv4 10.10.10.1`	Configure targeted peer for LDP using IPv4 addresses.
`PE4(config-router-targeted-peer)#exit-targeted-peer-mode`	Exit router targeted-peer-mode.
`PE4(config-router)#targeted-peer ipv4 10.10.10.2`	Configure targeted peer for LDP using IPv4 addresses.
`PE4(config-router-targeted-peer)#exit-targeted-peer-mode`	Exit router targeted-peer-mode.
`PE4(config-router)#targeted-peer ipv4 10.10.10.3`	Configure targeted peer for LDP using IPv4 addresses.
`PE4(config-router-targeted-peer)#exit-targeted-peer-mode`	Exit router targeted-peer-mode.
`PE4(config-router)#exit`	Exit router LDP mode and return to the configure mode.
`PE4(config)#commit`	Commit the transaction.

PE4: Global EVPN MPLS Command

The configuration on PE4 for the Global EVPN MPLS, includes activating EVPN MPLS, defining the global VTEP IP address, enabling hardware profile filtering for EVPN MPLS multi-homing, and activating EVPN MPLS multi-homing functionality, all of which are crucial for enabling EVPN MPLS features.

`PE4(config)#evpn mpls enable`	Activate the EVPN MPLS functionality on `PE4`, enabling it to participate in EVPN MPLS services.
`PE4(config)#commit`	Commit candidate configuration to be running configuration.
`PE4(config)#evpn mpls vtep-ip-global 10.10.10.4`	Configure the global VTEP IP address `10.10.10.4`, associating it with the loopback IP.
`PE4(config)#hardware-profile filter evpn-mpls-mh enable`	Enable hardware-profile filter for EVPN MPLS multi-homing.
`PE4(config)#evpn mpls multihoming enable`	Activate the EVPN MPLS multi-homing functionality, allowing `PE4` to support multi-homed EVPN MPLS services.
`PE4(config)#commit`	Commit the transaction.

PE4: Interface Configuration Network Side

The below configuration is performed to set up network interfaces on PE4 and enable LDP for IPv4, ensuring proper routing and labeling functionality.

`PE4(config)#interface xe2`	Enter interface mode `xe2`.
`PE4(config-if)#ip address 10.1.5.1/30`	Configure an IP address, `10.1.5.1/30`, on the interface `xe2`.
`PE4(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`PE4(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`PE4(config-if)#ip router isis 1`	Enable ISIS routing on an interface `xe2` for area 1.
`PE4(config-if)#exit`	Exit interface mode `xe2`.
`PE4(config)#commit`	Commit the transaction.
`PE4(config)#interface xe0`	Enter interface mode `xe0`.
`PE4(config-if)#ip address 10.1.8.1/30`	Configure an IP address, `10.1.8.1/30`, on the interface `xe0`.
`PE4(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`PE4(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`PE4(config-if)#ip router isis 1`	Enable ISIS routing on an interface `xe2` for area 1.
`PE4(config-if)#exit`	Exit interface mode `xe0`.
`PE4(config)#commit`	Commit the transaction.

PE4: ISIS Configuration

The below configuration is performed to set up ISIS on PE4, to enable MPLS Traffic Engineering, Segment Routing, and other related features for efficient routing and network management.

`PE4(config)#router isis 1`	Enter router ISIS mode.
`PE4(config-router)#is-type level-1-2`	Configure IS-Type as `Level-1-2` specifies that the router will participate in both Level-1 and Level-2 areas within the ISIS network.
`PE4(config-router)#metric-style wide`	Configure the new style of metric type as `wide`.
`PE4(config-router)#mpls traffic-eng router-id 10.10.10.4`	Configure the router's MPLS Traffic Engineering (TE) router ID TLV to `10.10.10.4`, which is used for MPLS-TE path calculations.
`PE4(config-router)#mpls traffic-eng level-1`	Enable MPLS-TE for IS-Type `Level-1` routing.
`PE4(config-router)#mpls traffic-eng level-2`	Enable MPLS-TE for IS-Type `Level-2` routing.
`PE4(config-router)#capability cspf`	Enable Constraint Shortest Path First (CSPF) computation for traffic engineering.
`PE4(config-router)#dynamic-hostname`	Configure the hostname to be advertised for an ISIS instance.
`PE4(config-router)#fast-reroute ti-lfa level-1 proto ipv4`	Configure Remote Loop-Free Alternate (LFA) to calculate backup paths to those destinations whichever does not satisfy basic LFA FRR inequalities
`PE4(config-router)#fast-reroute ti-lfa level-2 proto ipv4`	Configure Remote Loop-Free Alternate (LFA) to calculate backup paths to those destinations whichever does not satisfy basic LFA FRR inequalities
`PE4(config-router)#bfd all-interfaces`	Configure BFD on all interfaces for fast link failure detection.
`PE4(config-router)#net 49.0000.0000.0004.00`	Set a Network Entity Title (NET) for this ISIS instance, specifying the area address and the system ID.
`PE4(config-router)#isis segment-routing global block 17000 23500`	Enable ISIS SR globally and allocates label blocks for Segment Routing.
`PE4(config-router)#segment-routing mpls`	Enable SR ISIS.
`PE4(config-router)#exit`	Exit router ISIS mode and return to configure mode.
`PE4(config)#commit`	Commit the transaction.

PE4: BGP Configuration

The below BGP configuration on PE4 is established to enable BGP routing with ASN 65010, set the BGP router ID, define iBGP neighbors, configure BFD, and enable the EVPN address family for efficient routing in an EVPN environment.

`PE4(config)#router bgp 65010`	Enter the Router BGP mode, ASN: 65010
`PE4(config-router)#bgp router-id 10.10.10.4`	Configure BGP router ID `10.10.10.4`, identifying PE4 within the BGP network.
`PE4(config-router)#neighbor 10.10.10.1 remote-as 65010`	Configure neighbor `10.10.10.1` as an iBGP neighbor with their remote AS number `65010`.
`PE4(config-router)#neighbor 10.10.10.1 update-source lo`	Configure neighbor `10.10.10.1` as an iBGP neighbor, specifying the source of routing updates as the loopback interface.
`PE4(config-router)#neighbor 10.10.10.2 remote-as 65010`	Configure neighbor `10.10.10.2` as an iBGP neighbor with their remote AS number `65010`.
`PE4(config-router)#neighbor 10.10.10.2 update-source lo`	Configure neighbor `10.10.10.2` as an iBGP neighbor, specifying the source of routing updates as the loopback interface.

`PE4(config-router)#neighbor 10.10.10.3 remote-as 65010`	Configure neighbor `10.10.10.3` as an iBGP neighbor with their remote AS number `65010`.
`PE4(config-router)#neighbor 10.10.10.3 update-source lo`	Configure neighbor `10.10.10.3` as an iBGP neighbor, specifying the source of routing updates as the loopback interface.
`PE4(config-router)#neighbor 10.10.10.1 fall-over bfd multihop`	Configure BFD for the BGP neighbor to provide rapid failure detection.
`PE4(config-router)#neighbor 10.10.10.2 fall-over bfd multihop`	Configure BFD for the BGP neighbor to provide rapid failure detection.
`PE4(config-router)#neighbor 10.10.10.3 fall-over bfd multihop`	Configure BFD for the BGP neighbor to provide rapid failure detection.
`PE4(config-router)#neighbor 10.10.10.1 advertisement-interval 0`	Configure advertisement interval for the neighbor, allowing more frequent BGP updates.
`PE4(config-router)#neighbor 10.10.10.2 advertisement-interval 0`	Configure advertisement interval for the neighbor, allowing more frequent BGP updates.
`PE4(config-router)#neighbor 10.10.10.3 advertisement-interval 0`	Configure advertisement interval for the neighbor, allowing more frequent BGP updates.
`PE4(config-router)#address-family l2vpn evpn`	Enter into address family mode for L2VPN EVPN.
`PE4(config-router-af)#neighbor 10.10.10.1 activate`	Activate EVPN for iBGP neighbor `10.10.10.1` within the address family mode, ensuring that EVPN address family is enabled for the neighbor.
`PE4(config-router-af)#neighbor 10.10.10.2 activate`	Activate EVPN for iBGP neighbor `10.10.10.2` within the address family mode, ensuring that EVPN address family is enabled for the neighbor.
`PE4(config-router-af)#neighbor 10.10.10.3 activate`	Activate EVPN for iBGP neighbor `10.10.10.3` within the address family mode, ensuring that EVPN address family is enabled for the neighbor.
`PE4(config-router-af)#exit`	Exit address family mode and return to the router BGP mode.
`PE4(config-router)#commit`	Commit the transaction.
`PE4(config-router)#exit`	Exit router BGP mode and return to the configure mode.

PE4: MAC VRF Configuration

The below MAC VRF configuration on PE4 is carried out to define and set up VRFs named `vrf2` and `vpls1001` with specific Route-Distinguisher (RD) and route-target values, ensuring segregated MAC address spaces for distinct network services.

`PE4(config)#mac vrf vrf2`	Enter VRF mode named `vrf2`.
`PE4(config-vrf)#rd 10.10.10.4:1700`	Configure Route-Distinguisher value of `10.10.10.4:1700`.
`PE4(config-vrf)#route-target both 1700:1700`	Configure import and export values for the `vrf2` as `1700:1700`.
`PE4(config-vrf)#exit`	Exit VRF mode and return to the configure mode.
`PE4(config)#mac vrf vpls1001`	Enter VRF mode named `vpls1001`.
`PE4(config-vrf)#rd 10.10.10.4:1001`	Configure Route-Distinguisher value of `10.10.10.4:1001`.
`PE4(config-vrf)#route-target both 1001:1001`	Configure import and export values for the `vpls1001` as `1001:1001`.

`PE4(config-vrf)#exit`	Exit VRF mode and return to the configure mode.
`PE4(config)#commit`	Commit the transaction.

PE4: EVPN and VRF Mapping

The below EVPN and VRF mapping configuration on PE4 is performed to establish mappings between EVPN identifiers and VRFs, facilitating efficient routing and connectivity in an EVPN network environment.

`PE4(config)#evpn mpls id 1700 xconnect target-mpls-id 1800`	Configure the EVPN-VPWS identifier with a source identifier of `1700` and a target identifier of `1800`.
`PE4(config-evpn-mpls)#host-reachability-protocol evpn-bgp vrf2`	Map VRF `vrf2` to the EVPN-VPWS identifier
`PE4(config-evpn-mpls)#evpn mpls id 3000`	Configure the EVPN-VPLS identifier an identifier of `3000`.
`PE4(config-evpn-mpls)#host-reachability-protocol evpn-bgp vpls1001`	Map VRF `vpls1001` to the EVPN-VPWS identifier
`PE4(config-evpn-mpls)#commit`	Commit the transaction.
`PE4(config-evpn-mpls)#exit`	Exit the EVPN MPLS mode and return to the configure mode.

PE4: Access Port Configuration for Port-active

The below access port configuration for port-active mode on PE4 is carried out to configure various parameters including system-MAC, load balancing, service carving preferences, and EVPN settings for efficient network access and connectivity.

`PE4(config)#interface po1`	Enter the port channel interface mode for `po1`
`PE4(config-if)#load-interval 30`	Set the load interval to `30`.
`PE4(config-if)#evpn multi-homed system-mac 0000.2222.7777 load-balancing port-active`	Configure the system-mac address `0000.2222.7777` for port-active mode, which plays a role in load balancing and enter to the EVPN Ethernet Segment (ES) mode.
`PE4(config-if-es)#service-carving auto`	Configure service carving as `auto`, allowing automatic determination of service distribution preferences.
`PE4(config-if-es)#exit`	Exit the EVPN ES mode and return to the configure mode.
`PE4(config-if)#exit`	Exit interface mode `po1` and return to the configure mode.
`PE4(config)#commit`	Commit the transaction.
`PE4(config)#interface po1.1 switchport`	Create a Layer 2 sub-interface `po1.1` within the port channel.
`PE4(config-if)#encapsulation dot1q 100`	Set encapsulation to dot1q with VLAN ID `100`.
`PE4(config-if)#load-interval 30`	Set the load interval to `30`.
`PE4(config-if)#access-if-evpn`	Enter the access mode for EVPN MPLS ID configuration.
`PE4(config-acc-if-evpn)#map vpn-id 1800`	Map VPN-ID `1800`.
`PE4(config-acc-if-evpn)#exit`	Exit the access mode and return to the interface mode.
`PE4(config-if)#exit`	Exit interface mode `po1.1` and return to the configure mode.
`PE4(config)#interface xe11`	Enter the interface mode for `xe11`.
`PE4(config-if)#speed 10g`	Set the speed to `10g`.
`PE4(config-if)#channel-group 1 mode active`	Attach LAG interface `po1`.

`PE4(config-if)#exit`	Exit interface mode `xe11` and return to the configure mode.
`PE4(config)#commit`	Commit the transaction.

PE4: Access Port Configuration for Single-active

The below access port configuration for single-active mode on PE4 is implemented to set up various parameters, including Ethernet Segment Identifier (ESI) settings, service carving preferences, and EVPN configurations, ensuring efficient network access and connectivity.

`PE4(config)#interface sa2`	Enter the single active interface mode for `sa2.`
`PE4(config-if)#load-interval 30`	Set the load interval to `30`.
`PE4(config-if)#evpn multi-homed esi 00:00:22:22:77:77 load-balancing single-active`	Configure the ESI with the value with the value `00:00:22:22:77:77` for single-active mode, which plays a role in load balancing and enter to the EVPN Ethernet Segment (ES) mode.
`PE4(config-if-es)#service-carving auto`	Configure service carving as `auto`, allowing automatic determination of service distribution preferences.
`PE4(config-if-es)#exit`	Exit the EVPN ES mode and return to the configure mode.
`PE4(config-if)#exit`	Exit interface mode `sa2` and return to the configure mode.
`PE4(config)#commit`	Commit the transaction.
`PE4(config)#interface sa2.1 switchport`	Create a Layer 2 sub-interface `sa2.1` within the port channel.
`PE4(config-if)#encapsulation dot1q 100`	Set encapsulation to dot1q with VLAN ID `100`.
`PE4(config-if)#load-interval 30`	Set the load interval to `30`.
`PE4(config-if)#access-if-evpn`	Enter the access mode for EVPN MPLS ID configuration.
`PE4(config-acc-if-evpn)#map vpn-id 1800`	Map VPN-ID `1800`.
`PE4(config-acc-if-evpn)#exit`	Exit the access mode and return to the interface mode.
`PE4(config-if)#exit`	Exit interface mode `sa2.1` and return to the configure mode.
`PE4(config)#interface xe11`	Enter the interface mode for `xe11.`
`PE4(config-if)#speed 10g`	Set the speed to `10g`.
`PE4(config-if)#static-channel-group 2`	Attach the static-channel-group 2, the LAG interface `sa2` to `xe11`.
`PE4(config-if)#exit`	Exit interface mode `xe11` and return to the configure mode.
`PE4(config)#commit`	Commit the transaction.

CE2

The following configuration steps under CE2 are set up to enable VLANs and configure interfaces for carrying VLAN traffic.

`CE2#configure terminal`	Enter configure mode.
`CE2(config)#bridge 1 protocol ieee vlan-bridge`	Set up `bridge 1` to use the IEEE VLAN bridge protocol.
`CE2(config)#vlan 2-100 bridge 1 state enable`	Configure VLANs from `2-100` and associate them with bridge 1.
`CE2(config)#interface xe24`	Enter interface mode `xe24`.

`CE2(config-if)#switchport`	Configure the interface `xe24` as a Layer 2 switch port.
`CE2(config-if)#bridge-group 1`	Associate `xe24` to bridge 1.
`CE2(config-if)#switchport mode trunk`	Configure `xe24` as a trunk port.
`CE2(config-if)#switchport trunk allowed vlan all`	Allow all configured VLANs on the trunk interface `xe24`.
`CE2(config-if)#exit`	Exit interface mode `xe24`.
`CE2(config)#interface po1`	Enter interface mode and configure LAG interface port-channel 1 (`po1`).
`CE2(config-if)#switchport`	Configures port-channel 1 as a Layer 2 switch port.
`CE2(config-if)#bridge-group 1`	Associate `po1` to bridge 1.
`CE2(config-if)#switchport mode trunk`	Configure `po1` as a trunk port.
`CE2(config-if)#switchport trunk allowed vlan all`	Allow all configured VLANs on the trunk port-channel `po1`.
`CE2(config-if)#exit`	Exit interface mode `po1`.
`CE2(config)#interface xe22`	Enter interface mode `xe22`.
`CE2(config-if)#lacp timeout short`	Configure LACP timeout as `short`.
`CE2(config-if)#channel-group 1 mode active`	Add member to the LAG interface.
`CE2(config-if)#exit`	Exit interface mode `xe22`.
`CE2(config-if)#interface xe23`	Enter interface mode `xe23`.
`CE2(config-if)#lacp timeout short`	Configure LACP timeout as `short`.
`CE2(config-if)#channel-group 1 mode active`	Add member to the LAG interface.
`CE2(config-if)#commit`	Commit the transaction.
`CE2(config-if)#end`	Exit interface mode `xe23` and configure mode.

EVPN SR Active-Standby MH Validation

This section provides show outputs validation for port-active mode, covering ELINE and ELAN services with SR as the underlay MPLS path.

The following show output displays the forwarding table entries on PE1, PE2, PE3, and PE4 devices in the network Figure 2 using the **show mpls forwarding-table** command.

```
PE1#show mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN, ! - using backup
       B - BGP FTN, K - CLI FTN, (t) - tunnel, P - SR Policy FTN, (b) - bypass,
       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, (e) - FTN is ECMP

FTN-ECMP LDP: Disabled
Code     FEC                FTN-ID    Nhlfe-ID  Tunnel-id   Pri   LSP-Type     Out-Label    Out-Intf     ELC   Nexthop
   i>    10.10.10.2/32      1         4         0           Yes   LSP_DEFAULT  17700        xe2          No    10.1.2.2
   i>    10.10.10.2/32      10        23        0           No    LSP_DEFAULT  3            xe1        No    10.1.1.2
i(b)>    10.10.10.2/32      6         17        2201        Yes   LSP_DEFAULT  17700        xe1        No    10.1.1.2
   i>    10.10.10.3/32      2         6         0           Yes   LSP_DEFAULT  17400        xe2          No    10.1.2.2
   i>    10.10.10.3/32      11        24        0           No    LSP_DEFAULT  3            xe1        No    10.1.1.2
i(b)>    10.10.10.3/32      7         19        2202        Yes   LSP_DEFAULT  17400        xe1        No    10.1.1.2
i(b)>    10.10.10.3/32      9         22        2204        Yes   LSP_DEFAULT  17400        xe2          No    10.1.2.2
   i>    10.10.10.4/32      3         8         0           Yes   LSP_DEFAULT  17300        xe2          No    10.1.2.2
   i>    10.10.10.4/32      12        25        0           No    LSP_DEFAULT  3            xe1        No    10.1.1.2
i(b)>    10.10.10.4/32      8         21        2203        Yes   LSP_DEFAULT  17300        xe1        No    10.1.1.2
   i>    10.10.10.5/32      4         9         0           Yes   LSP_DEFAULT  3            xe1        No    10.1.1.2
   i>    10.10.10.5/32      13        27        0           No    LSP_DEFAULT  17600        xe2          No    10.1.2.2
   i>    10.10.10.6/32      5         15        0           Yes   LSP_DEFAULT  3            xe2          No    10.1.2.2
```

```
   i>   10.10.10.6/32       14        29        0           No    LSP_DEFAULT  17500        xe1        No    10.1.1.2

PE2#show mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN, ! - using backup
       B - BGP FTN, K - CLI FTN, (t) - tunnel, P - SR Policy FTN, (b) - bypass,
       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, (e) - FTN is ECMP

FTN-ECMP LDP: Disabled
Code    FEC                 FTN-ID    Nhlfe-ID  Tunnel-id   Pri   LSP-Type     Out-Label    Out-Intf    ELC   Nexthop
   i>   10.10.10.1/32       1         10        0           Yes   LSP_DEFAULT  17800        xe4         No    10.1.3.2
   i>   10.10.10.1/32       10        27        0           No    LSP_DEFAULT  3            xe5         No    10.1.4.2
i(b)>   10.10.10.1/32       6         21        2201        Yes   LSP_DEFAULT  17800        xe5         No    10.1.4.2
   i>   10.10.10.3/32       2         11        0           Yes   LSP_DEFAULT  17400        xe4         No    10.1.3.2
   i>   10.10.10.3/32       11        28        0           No    LSP_DEFAULT  3            xe5         No    10.1.4.2
i(b)>   10.10.10.3/32       7         23        2202        Yes   LSP_DEFAULT  17400        xe5         No    10.1.4.2
i(b)>   10.10.10.3/32       9         26        2204        Yes   LSP_DEFAULT  17400        xe4         No    10.1.3.2
   i>   10.10.10.4/32       3         12        0           Yes   LSP_DEFAULT  17300        xe4         No    10.1.3.2
   i>   10.10.10.4/32       12        29        0           No    LSP_DEFAULT  3            xe5         No    10.1.4.2
i(b)>   10.10.10.4/32       8         25        2203        Yes   LSP_DEFAULT  17300        xe5         No    10.1.4.2
   i>   10.10.10.5/32       4         13        0           Yes   LSP_DEFAULT  3            xe5         No    10.1.4.2
   i>   10.10.10.5/32       13        31        0           No    LSP_DEFAULT  17600        xe4         No    10.1.3.2
   i>   10.10.10.6/32       5         19        0           Yes   LSP_DEFAULT  3            xe4         No    10.1.3.2
   i>   10.10.10.6/32       14        33        0           No    LSP_DEFAULT  17500        xe5         No    10.1.4.2


PE3#show mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN, ! - using backup
       B - BGP FTN, K - CLI FTN, (t) - tunnel, P - SR Policy FTN, (b) - bypass,
       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, (e) - FTN is ECMP

FTN-ECMP LDP: Disabled
Code    FEC                 FTN-ID    Nhlfe-ID  Tunnel-id   Pri   LSP-Type     Out-Label    Out-Intf    ELC   Nexthop
   i>   10.10.10.1/32       1         4         0           Yes   LSP_DEFAULT  17800        xe5         No    10.1.7.2
   i>   10.10.10.1/32       10        23        0           No    LSP_DEFAULT  3            xe1         No    10.1.6.2
i(b)>   10.10.10.1/32       6         17        2201        Yes   LSP_DEFAULT  17800        xe1         No    10.1.6.2
i(b)>   10.10.10.1/32       9         22        2204        Yes   LSP_DEFAULT  17800        xe5         No    10.1.7.2
   i>   10.10.10.2/32       2         6         0           Yes   LSP_DEFAULT  17700        xe5         No    10.1.7.2
   i>   10.10.10.2/32       11        24        0           No    LSP_DEFAULT  3            xe1         No    10.1.6.2
i(b)>   10.10.10.2/32       7         19        2202        Yes   LSP_DEFAULT  17700        xe1         No    10.1.6.2
   i>   10.10.10.4/32       3         8         0           Yes   LSP_DEFAULT  17300        xe5         No    10.1.7.2
   i>   10.10.10.4/32       12        25        0           No    LSP_DEFAULT  3            xe1         No    10.1.6.2
i(b)>   10.10.10.4/32       8         21        2203        Yes   LSP_DEFAULT  17300        xe1         No    10.1.6.2
   i>   10.10.10.5/32       4         9         0           Yes   LSP_DEFAULT  3            xe1         No    10.1.6.2
   i>   10.10.10.5/32       13        27        0           No    LSP_DEFAULT  17600        xe5         No    10.1.7.2
   i>   10.10.10.6/32       5         15        0           Yes   LSP_DEFAULT  3            xe5         No    10.1.7.2
   i>   10.10.10.6/32       14        29        0           No    LSP_DEFAULT  17500        xe1         No    10.1.6.2

PE4#show mpls forwarding-table
Codes: > - installed FTN, * - selected FTN, p - stale FTN, ! - using backup
       B - BGP FTN, K - CLI FTN, (t) - tunnel, P - SR Policy FTN, (b) - bypass,
       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, (e) - FTN is ECMP

FTN-ECMP LDP: Disabled
Code    FEC                 FTN-ID    Nhlfe-ID  Tunnel-id   Pri   LSP-Type     Out-Label    Out-Intf    ELC   Nexthop
   i>   10.10.10.1/32       1         4         0           Yes   LSP_DEFAULT  17800        xe0         No    10.1.8.2
   i>   10.10.10.1/32       10        23        0           No    LSP_DEFAULT  3            xe2         No    10.1.5.2
i(b)>   10.10.10.1/32       6         17        2201        Yes   LSP_DEFAULT  17800        xe2         No    10.1.5.2
   i>   10.10.10.2/32       2         6         0           Yes   LSP_DEFAULT  17700        xe0         No    10.1.8.2
   i>   10.10.10.2/32       11        24        0           No    LSP_DEFAULT  3            xe2         No    10.1.5.2
i(b)>   10.10.10.2/32       7         19        2202        Yes   LSP_DEFAULT  17700        xe2         No    10.1.5.2
   i>   10.10.10.3/32       3         8         0           Yes   LSP_DEFAULT  17400        xe0         No    10.1.8.2
   i>   10.10.10.3/32       12        25        0           No    LSP_DEFAULT  3            xe2         No    10.1.5.2
i(b)>   10.10.10.3/32       8         21        2203        Yes   LSP_DEFAULT  17400        xe2         No    10.1.5.2
i(b)>   10.10.10.3/32       9         22        2204        Yes   LSP_DEFAULT  17400        xe0         No    10.1.8.2
   i>   10.10.10.5/32       4         9         0           Yes   LSP_DEFAULT  3            xe2         No    10.1.5.2
   i>   10.10.10.5/32       13        27        0           No    LSP_DEFAULT  17600        xe0         No    10.1.8.2
   i>   10.10.10.6/32       5         15        0           Yes   LSP_DEFAULT  3            xe0         No    10.1.8.2
```

```
   i>   10.10.10.6/32       14        29        0           No    LSP_DEFAULT  17500        xe2         No    10.1.5.2
```

The following show output displays the FEC-To-NHLF (FTN) table information on PE1, PE2, PE3, and PE4 devices in the network Figure 2 using the **show mpls ftn-table** command.

```
PE1#show mpls ftn-table
 Primary FTN entry with FEC: 10.10.10.2/32, id: 1, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Primary, Description: N/A, , Color: 0
     Cross connect ix: 7, in intf: - in label: 0 out-segment ix: 12
      Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 12, owner: ISIS-SR, Stale: NO, out intf: xe2, out label: 17700
    Nexthop addr: 10.1.2.2        cross connect ix: 7, op code: Push


 Non-primary FTN entry with FEC: 10.10.10.2/32, id: 10, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Backup, QoS Resource id: 0, Description: N/A, , Color: 0
     Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: N/A, Stale: NO, out intf: xe1, out label: 3
    Nexthop addr: 10.1.1.2        cross connect ix: 2, op code: Push

  bypass_ftn_ix 6

 Primary FTN entry with FEC: 10.10.10.2/32, id: 6, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 2201, Protected LSP id: 0, LSP-type: Bypass, QoS Resource id: 0, Description: N/A, , Color: 0
     Cross connect ix: 5, in intf: - in label: 0 out-segment ix: 16
      Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 16, owner: ISIS-SR, Stale: NO, out intf: xe1, out label: 17700
    Nexthop addr: 10.1.1.2        cross connect ix: 5, op code: Push


 Primary FTN entry with FEC: 10.10.10.3/32, id: 2, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Primary, Description: N/A, , Color: 0
     Cross connect ix: 3, in intf: - in label: 0 out-segment ix: 13
      Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 13, owner: ISIS-SR, Stale: NO, out intf: xe2, out label: 17400
    Nexthop addr: 10.1.2.2        cross connect ix: 3, op code: Push


 Non-primary FTN entry with FEC: 10.10.10.3/32, id: 11, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Backup, QoS Resource id: 0, Description: N/A, , Color: 0
     Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: N/A, Stale: NO, out intf: xe1, out label: 3
    Nexthop addr: 10.1.1.2        cross connect ix: 2, op code: Push

  bypass_ftn_ix 7

 Primary FTN entry with FEC: 10.10.10.3/32, id: 7, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 2202, Protected LSP id: 0, LSP-type: Bypass, QoS Resource id: 0, Description: N/A, , Color: 0
     Cross connect ix: 8, in intf: - in label: 0 out-segment ix: 18
      Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 18, owner: ISIS-SR, Stale: NO, out intf: xe1, out label: 17400
    Nexthop addr: 10.1.1.2        cross connect ix: 8, op code: Push


 Primary FTN entry with FEC: 10.10.10.3/32, id: 9, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 2204, Protected LSP id: 0, LSP-type: Bypass, QoS Resource id: 0, Description: N/A, , Color: 0
     Cross connect ix: 3, in intf: - in label: 0 out-segment ix: 13
      Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 13, owner: ISIS-SR, Stale: NO, out intf: xe2, out label: 17400
    Nexthop addr: 10.1.2.2        cross connect ix: 3, op code: Push


 Primary FTN entry with FEC: 10.10.10.4/32, id: 3, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
```

```
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Primary, Description: N/A, , Color: 0
     Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 14
      Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 14, owner: ISIS-SR, Stale: NO, out intf: xe2, out label: 17300
    Nexthop addr: 10.1.2.2        cross connect ix: 4, op code: Push


 Non-primary FTN entry with FEC: 10.10.10.4/32, id: 12, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Backup, QoS Resource id: 0, Description: N/A, , Color: 0
     Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: N/A, Stale: NO, out intf: xe1, out label: 3
    Nexthop addr: 10.1.1.2        cross connect ix: 2, op code: Push

  bypass_ftn_ix 8

 Primary FTN entry with FEC: 10.10.10.4/32, id: 8, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 2203, Protected LSP id: 0, LSP-type: Bypass, QoS Resource id: 0, Description: N/A, , Color: 0
     Cross connect ix: 9, in intf: - in label: 0 out-segment ix: 20
      Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 20, owner: ISIS-SR, Stale: NO, out intf: xe1, out label: 17300
    Nexthop addr: 10.1.1.2        cross connect ix: 9, op code: Push


 Primary FTN entry with FEC: 10.10.10.5/32, id: 4, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Primary, Description: N/A, , Color: 0
     Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: N/A, Stale: NO, out intf: xe1, out label: 3
    Nexthop addr: 10.1.1.2        cross connect ix: 2, op code: Push


 Non-primary FTN entry with FEC: 10.10.10.5/32, id: 13, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Backup, QoS Resource id: 0, Description: N/A, , Color: 0
     Cross connect ix: 10, in intf: - in label: 0 out-segment ix: 26
      Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 26, owner: ISIS-SR, Stale: NO, ISIS-SR out intf: xe2, transport out intf: N/A, out label: 17600
    Nexthop addr: 10.1.2.2        cross connect ix: 10, op code: Push and Lookup

  bypass_ftn_ix 9

 Primary FTN entry with FEC: 10.10.10.6/32, id: 5, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Primary, Description: N/A, , Color: 0
     Cross connect ix: 6, in intf: - in label: 0 out-segment ix: 11
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 11, owner: N/A, Stale: NO, out intf: xe2, out label: 3
    Nexthop addr: 10.1.2.2        cross connect ix: 6, op code: Push


 Non-primary FTN entry with FEC: 10.10.10.6/32, id: 14, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Backup, QoS Resource id: 0, Description: N/A, , Color: 0
     Cross connect ix: 11, in intf: - in label: 0 out-segment ix: 28
      Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 28, owner: ISIS-SR, Stale: NO, ISIS-SR out intf: xe1, transport out intf: N/A, out label: 17500
    Nexthop addr: 10.1.1.2        cross connect ix: 11, op code: Push and Lookup

  bypass_ftn_ix 7

PE2#show mpls ftn-table
 Primary FTN entry with FEC: 10.10.10.1/32, id: 1, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Primary, Description: N/A, , Color: 0
     Cross connect ix: 7, in intf: - in label: 0 out-segment ix: 16
      Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 16, owner: ISIS-SR, Stale: NO, out intf: xe4, out label: 17800
    Nexthop addr: 10.1.3.2        cross connect ix: 7, op code: Push
```

```
Non-primary FTN entry with FEC: 10.10.10.1/32, id: 10, row status: Active, Tunnel-Policy: N/A, State: Installed
 Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
 Tunnel id: 0, Protected LSP id: 0, LSP-type: Backup, QoS Resource id: 0, Description: N/A, , Color: 0
    Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
     Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
      Out-segment with ix: 2, owner: N/A, Stale: NO, out intf: xe5, out label: 3
   Nexthop addr: 10.1.4.2        cross connect ix: 2, op code: Push

 bypass_ftn_ix 6

Primary FTN entry with FEC: 10.10.10.1/32, id: 6, row status: Active, Tunnel-Policy: N/A, State: Installed
 Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
 Tunnel id: 2201, Protected LSP id: 0, LSP-type: Bypass, QoS Resource id: 0, Description: N/A, , Color: 0
    Cross connect ix: 5, in intf: - in label: 0 out-segment ix: 20
     Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
      Out-segment with ix: 20, owner: ISIS-SR, Stale: NO, out intf: xe5, out label: 17800
   Nexthop addr: 10.1.4.2        cross connect ix: 5, op code: Push


Primary FTN entry with FEC: 10.10.10.3/32, id: 2, row status: Active, Tunnel-Policy: N/A, State: Installed
 Owner: ISIS-SR, distance: 115, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
 Tunnel id: 0, Protected LSP id: 0, LSP-type: Primary, Description: N/A, , Color: 0
    Cross connect ix: 3, in intf: - in label: 0 out-segment ix: 17
     Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
      Out-segment with ix: 17, owner: ISIS-SR, Stale: NO, out intf: xe4, out label: 17400
   Nexthop addr: 10.1.3.2        cross connect ix: 3, op code: Push


Non-primary FTN entry with FEC: 10.10.10.3/32, id: 11, row status: Active, Tunnel-Policy: N/A, State: Installed
 Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
 Tunnel id: 0, Protected LSP id: 0, LSP-type: Backup, QoS Resource id: 0, Description: N/A, , Color: 0
    Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
     Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
      Out-segment with ix: 2, owner: N/A, Stale: NO, out intf: xe5, out label: 3
   Nexthop addr: 10.1.4.2        cross connect ix: 2, op code: Push

 bypass_ftn_ix 7

Primary FTN entry with FEC: 10.10.10.3/32, id: 7, row status: Active, Tunnel-Policy: N/A, State: Installed
 Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
 Tunnel id: 2202, Protected LSP id: 0, LSP-type: Bypass, QoS Resource id: 0, Description: N/A, , Color: 0
    Cross connect ix: 8, in intf: - in label: 0 out-segment ix: 22
     Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
      Out-segment with ix: 22, owner: ISIS-SR, Stale: NO, out intf: xe5, out label: 17400
   Nexthop addr: 10.1.4.2        cross connect ix: 8, op code: Push


Primary FTN entry with FEC: 10.10.10.3/32, id: 9, row status: Active, Tunnel-Policy: N/A, State: Installed
 Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
 Tunnel id: 2204, Protected LSP id: 0, LSP-type: Bypass, QoS Resource id: 0, Description: N/A, , Color: 0
    Cross connect ix: 3, in intf: - in label: 0 out-segment ix: 17
     Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
      Out-segment with ix: 17, owner: ISIS-SR, Stale: NO, out intf: xe4, out label: 17400
   Nexthop addr: 10.1.3.2        cross connect ix: 3, op code: Push


Primary FTN entry with FEC: 10.10.10.4/32, id: 3, row status: Active, Tunnel-Policy: N/A, State: Installed
 Owner: ISIS-SR, distance: 115, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
 Tunnel id: 0, Protected LSP id: 0, LSP-type: Primary, Description: N/A, , Color: 0
    Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 18
     Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
      Out-segment with ix: 18, owner: ISIS-SR, Stale: NO, out intf: xe4, out label: 17300
   Nexthop addr: 10.1.3.2        cross connect ix: 4, op code: Push


Non-primary FTN entry with FEC: 10.10.10.4/32, id: 12, row status: Active, Tunnel-Policy: N/A, State: Installed
 Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
 Tunnel id: 0, Protected LSP id: 0, LSP-type: Backup, QoS Resource id: 0, Description: N/A, , Color: 0
    Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
     Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
      Out-segment with ix: 2, owner: N/A, Stale: NO, out intf: xe5, out label: 3
   Nexthop addr: 10.1.4.2        cross connect ix: 2, op code: Push
```

```
  bypass_ftn_ix 8

 Primary FTN entry with FEC: 10.10.10.4/32, id: 8, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 2203, Protected LSP id: 0, LSP-type: Bypass, QoS Resource id: 0, Description: N/A, , Color: 0
     Cross connect ix: 9, in intf: - in label: 0 out-segment ix: 24
      Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 24, owner: ISIS-SR, Stale: NO, out intf: xe5, out label: 17300
    Nexthop addr: 10.1.4.2        cross connect ix: 9, op code: Push


 Primary FTN entry with FEC: 10.10.10.5/32, id: 4, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Primary, Description: N/A, , Color: 0
     Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: N/A, Stale: NO, out intf: xe5, out label: 3
    Nexthop addr: 10.1.4.2        cross connect ix: 2, op code: Push


 Non-primary FTN entry with FEC: 10.10.10.5/32, id: 13, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Backup, QoS Resource id: 0, Description: N/A, , Color: 0
     Cross connect ix: 10, in intf: - in label: 0 out-segment ix: 30
      Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 30, owner: ISIS-SR, Stale: NO, ISIS-SR out intf: xe4, transport out intf: N/A, out label: 17600
    Nexthop addr: 10.1.3.2        cross connect ix: 10, op code: Push and Lookup

  bypass_ftn_ix 9

 Primary FTN entry with FEC: 10.10.10.6/32, id: 5, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Primary, Description: N/A, , Color: 0
     Cross connect ix: 6, in intf: - in label: 0 out-segment ix: 15
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 15, owner: N/A, Stale: NO, out intf: xe4, out label: 3
    Nexthop addr: 10.1.3.2        cross connect ix: 6, op code: Push


 Non-primary FTN entry with FEC: 10.10.10.6/32, id: 14, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Backup, QoS Resource id: 0, Description: N/A, , Color: 0
     Cross connect ix: 11, in intf: - in label: 0 out-segment ix: 32
      Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 32, owner: ISIS-SR, Stale: NO, ISIS-SR out intf: xe5, transport out intf: N/A, out label: 17500
    Nexthop addr: 10.1.4.2        cross connect ix: 11, op code: Push and Lookup

  bypass_ftn_ix 7

PE3#show mpls ftn-table
 Primary FTN entry with FEC: 10.10.10.1/32, id: 1, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Primary, Description: N/A, , Color: 0
     Cross connect ix: 7, in intf: - in label: 0 out-segment ix: 12
      Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 12, owner: ISIS-SR, Stale: NO, out intf: xe5, out label: 17800
    Nexthop addr: 10.1.7.2        cross connect ix: 7, op code: Push


 Non-primary FTN entry with FEC: 10.10.10.1/32, id: 10, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Backup, QoS Resource id: 0, Description: N/A, , Color: 0
     Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: N/A, Stale: NO, out intf: xe1, out label: 3
    Nexthop addr: 10.1.6.2        cross connect ix: 2, op code: Push

  bypass_ftn_ix 6

 Primary FTN entry with FEC: 10.10.10.1/32, id: 6, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 2201, Protected LSP id: 0, LSP-type: Bypass, QoS Resource id: 0, Description: N/A, , Color: 0
```

```
    Cross connect ix: 5, in intf: - in label: 0 out-segment ix: 16
     Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
      Out-segment with ix: 16, owner: ISIS-SR, Stale: NO, out intf: xe1, out label: 17800
   Nexthop addr: 10.1.6.2        cross connect ix: 5, op code: Push


Primary FTN entry with FEC: 10.10.10.1/32, id: 9, row status: Active, Tunnel-Policy: N/A, State: Installed
 Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
 Tunnel id: 2204, Protected LSP id: 0, LSP-type: Bypass, QoS Resource id: 0, Description: N/A, , Color: 0
    Cross connect ix: 7, in intf: - in label: 0 out-segment ix: 12
     Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
      Out-segment with ix: 12, owner: ISIS-SR, Stale: NO, out intf: xe5, out label: 17800
   Nexthop addr: 10.1.7.2        cross connect ix: 7, op code: Push


Primary FTN entry with FEC: 10.10.10.2/32, id: 2, row status: Active, Tunnel-Policy: N/A, State: Installed
 Owner: ISIS-SR, distance: 115, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
 Tunnel id: 0, Protected LSP id: 0, LSP-type: Primary, Description: N/A, , Color: 0
    Cross connect ix: 3, in intf: - in label: 0 out-segment ix: 13
     Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
      Out-segment with ix: 13, owner: ISIS-SR, Stale: NO, out intf: xe5, out label: 17700
   Nexthop addr: 10.1.7.2        cross connect ix: 3, op code: Push


Non-primary FTN entry with FEC: 10.10.10.2/32, id: 11, row status: Active, Tunnel-Policy: N/A, State: Installed
 Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
 Tunnel id: 0, Protected LSP id: 0, LSP-type: Backup, QoS Resource id: 0, Description: N/A, , Color: 0
    Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
     Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
      Out-segment with ix: 2, owner: N/A, Stale: NO, out intf: xe1, out label: 3
   Nexthop addr: 10.1.6.2        cross connect ix: 2, op code: Push

 bypass_ftn_ix 7

Primary FTN entry with FEC: 10.10.10.2/32, id: 7, row status: Active, Tunnel-Policy: N/A, State: Installed
 Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
 Tunnel id: 2202, Protected LSP id: 0, LSP-type: Bypass, QoS Resource id: 0, Description: N/A, , Color: 0
    Cross connect ix: 8, in intf: - in label: 0 out-segment ix: 18
     Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
      Out-segment with ix: 18, owner: ISIS-SR, Stale: NO, out intf: xe1, out label: 17700
   Nexthop addr: 10.1.6.2        cross connect ix: 8, op code: Push


Primary FTN entry with FEC: 10.10.10.4/32, id: 3, row status: Active, Tunnel-Policy: N/A, State: Installed
 Owner: ISIS-SR, distance: 115, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
 Tunnel id: 0, Protected LSP id: 0, LSP-type: Primary, Description: N/A, , Color: 0
    Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 14
     Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
      Out-segment with ix: 14, owner: ISIS-SR, Stale: NO, out intf: xe5, out label: 17300
   Nexthop addr: 10.1.7.2        cross connect ix: 4, op code: Push


Non-primary FTN entry with FEC: 10.10.10.4/32, id: 12, row status: Active, Tunnel-Policy: N/A, State: Installed
 Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
 Tunnel id: 0, Protected LSP id: 0, LSP-type: Backup, QoS Resource id: 0, Description: N/A, , Color: 0
    Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
     Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
      Out-segment with ix: 2, owner: N/A, Stale: NO, out intf: xe1, out label: 3
   Nexthop addr: 10.1.6.2        cross connect ix: 2, op code: Push

 bypass_ftn_ix 8

Primary FTN entry with FEC: 10.10.10.4/32, id: 8, row status: Active, Tunnel-Policy: N/A, State: Installed
 Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
 Tunnel id: 2203, Protected LSP id: 0, LSP-type: Bypass, QoS Resource id: 0, Description: N/A, , Color: 0
    Cross connect ix: 9, in intf: - in label: 0 out-segment ix: 20
     Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
      Out-segment with ix: 20, owner: ISIS-SR, Stale: NO, out intf: xe1, out label: 17300
   Nexthop addr: 10.1.6.2        cross connect ix: 9, op code: Push


Primary FTN entry with FEC: 10.10.10.5/32, id: 4, row status: Active, Tunnel-Policy: N/A, State: Installed
 Owner: ISIS-SR, distance: 115, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
```

```
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Primary, Description: N/A, , Color: 0
     Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: N/A, Stale: NO, out intf: xe1, out label: 3
    Nexthop addr: 10.1.6.2        cross connect ix: 2, op code: Push


 Non-primary FTN entry with FEC: 10.10.10.5/32, id: 13, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Backup, QoS Resource id: 0, Description: N/A, , Color: 0
     Cross connect ix: 10, in intf: - in label: 0 out-segment ix: 26
      Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 26, owner: ISIS-SR, Stale: NO, ISIS-SR out intf: xe5, transport out intf: N/A, out label: 17600
    Nexthop addr: 10.1.7.2        cross connect ix: 10, op code: Push and Lookup

  bypass_ftn_ix 9

 Primary FTN entry with FEC: 10.10.10.6/32, id: 5, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Primary, Description: N/A, , Color: 0
     Cross connect ix: 6, in intf: - in label: 0 out-segment ix: 11
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 11, owner: N/A, Stale: NO, out intf: xe5, out label: 3
    Nexthop addr: 10.1.7.2        cross connect ix: 6, op code: Push


 Non-primary FTN entry with FEC: 10.10.10.6/32, id: 14, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Backup, QoS Resource id: 0, Description: N/A, , Color: 0
     Cross connect ix: 11, in intf: - in label: 0 out-segment ix: 28
      Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 28, owner: ISIS-SR, Stale: NO, ISIS-SR out intf: xe1, transport out intf: N/A, out label: 17500
    Nexthop addr: 10.1.6.2        cross connect ix: 11, op code: Push and Lookup

  bypass_ftn_ix 7

PE4#show mpls ftn-table
 Primary FTN entry with FEC: 10.10.10.1/32, id: 1, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Primary, Description: N/A, , Color: 0
     Cross connect ix: 7, in intf: - in label: 0 out-segment ix: 12
      Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 12, owner: ISIS-SR, Stale: NO, out intf: xe0, out label: 17800
    Nexthop addr: 10.1.8.2        cross connect ix: 7, op code: Push


 Non-primary FTN entry with FEC: 10.10.10.1/32, id: 10, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Backup, QoS Resource id: 0, Description: N/A, , Color: 0
     Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 2, owner: N/A, Stale: NO, out intf: xe2, out label: 3
    Nexthop addr: 10.1.5.2        cross connect ix: 2, op code: Push

  bypass_ftn_ix 6

 Primary FTN entry with FEC: 10.10.10.1/32, id: 6, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 2201, Protected LSP id: 0, LSP-type: Bypass, QoS Resource id: 0, Description: N/A, , Color: 0
     Cross connect ix: 5, in intf: - in label: 0 out-segment ix: 16
      Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 16, owner: ISIS-SR, Stale: NO, out intf: xe2, out label: 17800
    Nexthop addr: 10.1.5.2        cross connect ix: 5, op code: Push


 Primary FTN entry with FEC: 10.10.10.2/32, id: 2, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Primary, Description: N/A, , Color: 0
     Cross connect ix: 3, in intf: - in label: 0 out-segment ix: 13
      Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 13, owner: ISIS-SR, Stale: NO, out intf: xe0, out label: 17700
    Nexthop addr: 10.1.8.2        cross connect ix: 3, op code: Push
```

```
Non-primary FTN entry with FEC: 10.10.10.2/32, id: 11, row status: Active, Tunnel-Policy: N/A, State: Installed
 Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
 Tunnel id: 0, Protected LSP id: 0, LSP-type: Backup, QoS Resource id: 0, Description: N/A, , Color: 0
    Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
     Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
      Out-segment with ix: 2, owner: N/A, Stale: NO, out intf: xe2, out label: 3
   Nexthop addr: 10.1.5.2        cross connect ix: 2, op code: Push

 bypass_ftn_ix 7

Primary FTN entry with FEC: 10.10.10.2/32, id: 7, row status: Active, Tunnel-Policy: N/A, State: Installed
 Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
 Tunnel id: 2202, Protected LSP id: 0, LSP-type: Bypass, QoS Resource id: 0, Description: N/A, , Color: 0
    Cross connect ix: 8, in intf: - in label: 0 out-segment ix: 18
     Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
      Out-segment with ix: 18, owner: ISIS-SR, Stale: NO, out intf: xe2, out label: 17700
   Nexthop addr: 10.1.5.2        cross connect ix: 8, op code: Push


Primary FTN entry with FEC: 10.10.10.3/32, id: 3, row status: Active, Tunnel-Policy: N/A, State: Installed
 Owner: ISIS-SR, distance: 115, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
 Tunnel id: 0, Protected LSP id: 0, LSP-type: Primary, Description: N/A, , Color: 0
    Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 14
     Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
      Out-segment with ix: 14, owner: ISIS-SR, Stale: NO, out intf: xe0, out label: 17400
   Nexthop addr: 10.1.8.2        cross connect ix: 4, op code: Push


Non-primary FTN entry with FEC: 10.10.10.3/32, id: 12, row status: Active, Tunnel-Policy: N/A, State: Installed
 Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
 Tunnel id: 0, Protected LSP id: 0, LSP-type: Backup, QoS Resource id: 0, Description: N/A, , Color: 0
    Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
     Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
      Out-segment with ix: 2, owner: N/A, Stale: NO, out intf: xe2, out label: 3
   Nexthop addr: 10.1.5.2        cross connect ix: 2, op code: Push

 bypass_ftn_ix 8

Primary FTN entry with FEC: 10.10.10.3/32, id: 8, row status: Active, Tunnel-Policy: N/A, State: Installed
 Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
 Tunnel id: 2203, Protected LSP id: 0, LSP-type: Bypass, QoS Resource id: 0, Description: N/A, , Color: 0
    Cross connect ix: 9, in intf: - in label: 0 out-segment ix: 20
     Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
      Out-segment with ix: 20, owner: ISIS-SR, Stale: NO, out intf: xe2, out label: 17400
   Nexthop addr: 10.1.5.2        cross connect ix: 9, op code: Push


Primary FTN entry with FEC: 10.10.10.3/32, id: 9, row status: Active, Tunnel-Policy: N/A, State: Installed
 Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
 Tunnel id: 2204, Protected LSP id: 0, LSP-type: Bypass, QoS Resource id: 0, Description: N/A, , Color: 0
    Cross connect ix: 4, in intf: - in label: 0 out-segment ix: 14
     Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
      Out-segment with ix: 14, owner: ISIS-SR, Stale: NO, out intf: xe0, out label: 17400
   Nexthop addr: 10.1.8.2        cross connect ix: 4, op code: Push


Primary FTN entry with FEC: 10.10.10.5/32, id: 4, row status: Active, Tunnel-Policy: N/A, State: Installed
 Owner: ISIS-SR, distance: 115, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
 Tunnel id: 0, Protected LSP id: 0, LSP-type: Primary, Description: N/A, , Color: 0
    Cross connect ix: 2, in intf: - in label: 0 out-segment ix: 2
     Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
      Out-segment with ix: 2, owner: N/A, Stale: NO, out intf: xe2, out label: 3
   Nexthop addr: 10.1.5.2        cross connect ix: 2, op code: Push


Non-primary FTN entry with FEC: 10.10.10.5/32, id: 13, row status: Active, Tunnel-Policy: N/A, State: Installed
 Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
 Tunnel id: 0, Protected LSP id: 0, LSP-type: Backup, QoS Resource id: 0, Description: N/A, , Color: 0
    Cross connect ix: 10, in intf: - in label: 0 out-segment ix: 26
     Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
      Out-segment with ix: 26, owner: ISIS-SR, Stale: NO, ISIS-SR out intf: xe0, transport out intf: N/A, out label: 17600
   Nexthop addr: 10.1.8.2        cross connect ix: 10, op code: Push and Lookup
```

```
  bypass_ftn_ix 9

 Primary FTN entry with FEC: 10.10.10.6/32, id: 5, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to LSP, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Primary, Description: N/A, , Color: 0
     Cross connect ix: 6, in intf: - in label: 0 out-segment ix: 11
      Owner: N/A, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 11, owner: N/A, Stale: NO, out intf: xe0, out label: 3
    Nexthop addr: 10.1.8.2        cross connect ix: 6, op code: Push


 Non-primary FTN entry with FEC: 10.10.10.6/32, id: 14, row status: Active, Tunnel-Policy: N/A, State: Installed
  Owner: ISIS-SR, distance: 115, Action-type: Redirect to Tunnel, Exp-bits: 0x0, Incoming DSCP: none
  Tunnel id: 0, Protected LSP id: 0, LSP-type: Backup, QoS Resource id: 0, Description: N/A, , Color: 0
     Cross connect ix: 11, in intf: - in label: 0 out-segment ix: 28
      Owner: ISIS-SR, Persistent: No, Admin Status: Up, Oper Status: Up
       Out-segment with ix: 28, owner: ISIS-SR, Stale: NO, ISIS-SR out intf: xe2, transport out intf: N/A, out label: 17500
    Nexthop addr: 10.1.5.2        cross connect ix: 11, op code: Push and Lookup

  bypass_ftn_ix 8
```

Port-Active

The following show output displays the Ethernet Segment (ES) and Intermediate System (IS) neighbor adjacencies for PE1, PE2, PE3, PE4, P1, and P2 devices in the network Figure 2 using the **show clns neighbors** command.

```
PE1#show clns neighbors

Total number of L1 adjacencies: 2
Total number of L2 adjacencies: 2
Total number of adjacencies: 4
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
P2             xe2         e8c5.7a55.3c7e  Up     22        L1   IS-IS
                                           Up     22        L2   IS-IS
P1             xe1        e49d.73b3.c107   Up     23        L1   IS-IS

PE2#show clns neighbors

Total number of L1 adjacencies: 2
Total number of L2 adjacencies: 2
Total number of adjacencies: 4
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
P2             xe4         e8c5.7a55.3c7f  Up     8         L1   IS-IS
                                           Up     8         L2   IS-IS
P1             xe5         e49d.73b3.c14c  Up     29        L1   IS-IS
                                           Up     29        L2   IS-IS
                                           Up     23        L2   IS-IS

P1#show clns neighbors

Total number of L1 adjacencies: 4
Total number of L2 adjacencies: 4
Total number of adjacencies: 8
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
PE3            xe4         b86a.97d9.2cdf  Up     19        L1   IS-IS
                                           Up     19        L2   IS-IS
PE2            xe2        e8c5.7a47.9dfc   Up     7         L1   IS-IS
                                           Up     7         L2   IS-IS
PE1            xe1         e8c5.7a78.c918  Up     7         L1   IS-IS
                                           Up     7         L2   IS-IS
PE4            xe3        d077.ceda.7004   Up     19        L1   IS-IS
                                           Up     19        L2   IS-IS

P2#show clns neighbors

Total number of L1 adjacencies: 4
Total number of L2 adjacencies: 4
Total number of adjacencies: 8
```

```
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
PE3            xe11         b86a.97d9.2ccb      Up     19        L1   IS-IS
                                           Up     19        L2   IS-IS
PE1            xe12        e8c5.7a78.c908      Up     7         L1   IS-IS
                                           Up     7         L2   IS-IS
PE2            xe13        e8c5.7a47.9dfb      Up     19        L1   IS-IS
                                           Up     19        L2   IS-IS
PE4            xe14        d077.ceda.7002      Up     19        L1   IS-IS
                                           Up     19        L2   IS-IS


PE3#show clns neighbors

Total number of L1 adjacencies: 2
Total number of L2 adjacencies: 2
Total number of adjacencies: 4
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
P2             xe5         e8c5.7a55.3c77      Up     7         L1   IS-IS
                                           Up     7         L2   IS-IS
P1             xe1         e49d.73b3.c105      Up     5         L1   IS-IS
                                           Up     5         L2   IS-IS

PE4#show clns neighbors

Total number of L1 adjacencies: 2
Total number of L2 adjacencies: 2
Total number of adjacencies: 4
Tag 1:  VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
P2             xe0         e8c5.7a55.3c80      Up     5         L1   IS-IS
                                           Up     5         L2   IS-IS
P1             xe2         e49d.73b3.c14d      Up     6         L1   IS-IS
                                           Up     6         L2   IS-IS
```

Port-Active ELAN

The following show outputs provide validation for ELAN configurations.

The following show output displays the EVPN active multi-homed and load-balanced details on PE1, PE2, PE3, and PE4 devices in the network Figure 2 using the **show evpn load-balance port-active** and **show evpn multi-homing all** commands.

```
PE1#show evpn load-balance port-active
ESI                          AC-IF/PE     PE-IP-ADDRESS    Redundancy         Service-carving    weight   Revertive  AC-DF
Status
=============================================================================================================================
=========
00:00:00:11:11:77:77:00:00:00  LOCAL        10.10.10.1       port-active        auto               0        NO           NA
STANDBY
00:00:00:11:11:77:77:00:00:00  REMOTE       10.10.10.2       port-active        auto               0        NO           NA
ACTIVE
00:00:00:22:22:77:77:00:00:00  REMOTE       10.10.10.3       port-active        ----               ----     ----       ----
STANDBY
00:00:00:22:22:77:77:00:00:00  REMOTE       10.10.10.4       port-active        ----               ----     ----       ----
ACTIVE


PE2#show evpn load-balance port-active
ESI                          AC-IF/PE     PE-IP-ADDRESS    Redundancy         Service-carving    weight   Revertive  AC-DF
Status
=============================================================================================================================
=========
00:00:00:11:11:77:77:00:00:00  REMOTE       10.10.10.1       port-active        auto               0        NO           NA
STANDBY
00:00:00:11:11:77:77:00:00:00  LOCAL        10.10.10.2       port-active        auto               0        NO           NA
ACTIVE
00:00:00:22:22:77:77:00:00:00  REMOTE       10.10.10.3       port-active        ----               ----     ----       ----
STANDBY
00:00:00:22:22:77:77:00:00:00  REMOTE       10.10.10.4       port-active        ----               ----     ----       ----
ACTIVE

PE3#show evpn load-balance port-active
```

```
ESI                           AC-IF/PE     PE-IP-ADDRESS    Redundancy         Service-carving    weight   Revertive  AC-DF
Status
=============================================================================================================================
=========
00:00:00:11:11:77:77:00:00:00  REMOTE       10.10.10.1       port-active        ----               ----     ----       ----
STANDBY
00:00:00:11:11:77:77:00:00:00  REMOTE       10.10.10.2       port-active        ----               ----     ----       ----
ACTIVE
00:00:00:22:22:77:77:00:00:00  LOCAL        10.10.10.3       port-active        auto               0        NO           NA
STANDBY
00:00:00:22:22:77:77:00:00:00  REMOTE       10.10.10.4       port-active        auto               0        NO           NA
ACTIVE

PE4#show evpn load-balance port-active
ESI                           AC-IF/PE     PE-IP-ADDRESS    Redundancy         Service-carving    weight   Revertive  AC-DF
Status
=============================================================================================================================
=========
00:00:00:11:11:77:77:00:00:00  REMOTE       10.10.10.1       port-active        ----               ----     ----       ----
STANDBY
00:00:00:11:11:77:77:00:00:00  REMOTE       10.10.10.2       port-active        ----               ----     ----       ----
ACTIVE
00:00:00:22:22:77:77:00:00:00  REMOTE       10.10.10.3       port-active        auto               0        NO           NA
STANDBY
00:00:00:22:22:77:77:00:00:00  LOCAL        10.10.10.4       port-active        auto               0        NO           NA
ACTIVE

PE1#show evpn multi-homing all
ESI                           Access-IF    PE-IP-ADDRESS
=============================================================
00:00:00:11:11:77:77:00:00:00  po1          10.10.10.1
00:00:00:11:11:77:77:00:00:00  ----         10.10.10.2
00:00:00:22:22:77:77:00:00:00  ----         10.10.10.3
00:00:00:22:22:77:77:00:00:00  ----         10.10.10.4
Total number of entries are 4

PE2#show evpn multi-homing all
ESI                           Access-IF    PE-IP-ADDRESS
=============================================================
00:00:00:11:11:77:77:00:00:00  ----         10.10.10.1
00:00:00:11:11:77:77:00:00:00  po1          10.10.10.2
00:00:00:22:22:77:77:00:00:00  ----         10.10.10.3
00:00:00:22:22:77:77:00:00:00  ----         10.10.10.4
Total number of entries are 4

PE3#show evpn multi-homing all
ESI                           Access-IF    PE-IP-ADDRESS
=============================================================
00:00:00:11:11:77:77:00:00:00  ----         10.10.10.1
00:00:00:11:11:77:77:00:00:00  ----         10.10.10.2
00:00:00:22:22:77:77:00:00:00  po1          10.10.10.3
00:00:00:22:22:77:77:00:00:00  ----         10.10.10.4
Total number of entries are 4

PE4#show evpn multi-homing all
ESI                           Access-IF    PE-IP-ADDRESS
=============================================================
00:00:00:11:11:77:77:00:00:00  ----         10.10.10.1
00:00:00:11:11:77:77:00:00:00  ----         10.10.10.2
00:00:00:22:22:77:77:00:00:00  ----         10.10.10.3
00:00:00:22:22:77:77:00:00:00  po1          10.10.10.4
Total number of entries are 4
```

The following show output displays the active EVPN MPLS Tunnels for ELAN on PE1, PE2, PE3, and PE4 devices in the network Figure 1 using the **show evpn mpls tunnel** command.

```
PE1#show evpn mpls tunnel
EVPN-MPLS Network tunnel Entries
Source           Destination      Status        Up/Down       Update        evpn-id
=============================================================================
10.10.10.1       10.10.10.2       Installed     00:02:19      00:02:19      3000
10.10.10.1       10.10.10.4       Installed     00:10:21      00:10:21      3000
10.10.10.1       10.10.10.3       Installed     00:10:47      00:10:47      3000

Total number of entries are 3
```

```
PE2#show evpn mpls tunnel
EVPN-MPLS Network tunnel Entries
Source           Destination      Status        Up/Down       Update        evpn-id
================================================================================
10.10.10.2       10.10.10.1       Installed     00:02:01      00:02:01      3000
10.10.10.2       10.10.10.4       Installed     00:02:01      00:02:01      3000
10.10.10.2       10.10.10.3       Installed     00:02:01      00:02:01      3000

Total number of entries are 3

PE3#show evpn mpls tunnel
EVPN-MPLS Network tunnel Entries
Source           Destination      Status        Up/Down       Update        evpn-id
================================================================================
10.10.10.3       10.10.10.2       Installed     00:02:27      00:02:27      3000
10.10.10.3       10.10.10.4       Installed     00:10:29      00:10:29      3000
10.10.10.3       10.10.10.1       Installed     00:10:54      00:10:54      3000

Total number of entries are 3

PE4#show evpn mpls tunnel
EVPN-MPLS Network tunnel Entries
Source           Destination      Status        Up/Down       Update        evpn
-id
================================================================================
===
10.10.10.4       10.10.10.2       Installed     00:02:30      00:02:30      3000

10.10.10.4       10.10.10.3       Installed     00:10:32      00:10:32      3000

10.10.10.4       10.10.10.1       Installed     00:10:32      00:10:32      3000


Total number of entries are 3
```

Port-Active ELINE

The following show output displays the active EVPN SR Tunnels for ELINE on PE1, PE2, PE3, and PE4 devices in the network Figure 2 using the **show evpn mpls xconnect tunnel** command.

```
PE1#show evpn mpls xconnect tunnel
EVPN-MPLS Network tunnel Entries
Source           Destination      Status        Up/Down       Update        local-evpn-id remote-evpn-id
================================================================================================================
10.10.10.1       10.10.10.4       AC-Down       01:07:01      01:07:01      1800          1700
10.10.10.1       10.10.10.3       AC-Down       01:07:01      01:07:01      1800          1700

Total number of entries are 2

PE2#show evpn mpls xconnect tunnel
EVPN-MPLS Network tunnel Entries
Source           Destination      Status        Up/Down       Update        local-evpn-id remote-evpn-id
================================================================================================================
10.10.10.2       10.10.10.3       Installed     00:08:20      00:07:31      1800          1700
10.10.10.2       10.10.10.4       Installed     00:08:20      00:07:31      1800          1700

Total number of entries are 2

PE3#show evpn mpls xconnect tunnel
EVPN-MPLS Network tunnel Entries
Source           Destination      Status        Up/Down       Update        local-evpn-id remote-evpn-id
================================================================================================================
10.10.10.3       10.10.10.1       AC-Down       01:04:48      01:04:48      1700          1800
10.10.10.3       10.10.10.2       AC-Down       00:08:48      00:08:48      1700          1800

Total number of entries are 2

PE4#show evpn mpls xconnect tunnel
EVPN-MPLS Network tunnel Entries
Source           Destination      Status        Up/Down       Update        local-evpn-id remote-evpn-id
================================================================================================================
```

```
10.10.10.4       10.10.10.1       Installed     00:09:00      00:08:28      1700          1800
10.10.10.4       10.10.10.2       Installed     00:09:01      00:08:28      1700          1800

Total number of entries are 2
```

Implementation Examples

Scenario: Customer wants to achieve redundancy for its hosts in a network using Single-Active or Port-Active redundancy.

- Customer configures the `evpn multi-homed` command with the `load-balancing single-active or load-balancing port-active` option on the relevant PE interfaces.
- Single-Active or Port-Active redundancy is now in effect, ensuring redundancy for hosts.
- The feature works in conjunction with other EVPN-related configurations, such as VRF, VLAN mapping, and other EVPN settings.

NewCLICommands

The EVPN Active-Standby feature introduces the following configuration commands. For more information of the EVPN MPLS commands, see the *EVPN MPLS Commands* chapter in the *Multi-Protocol Label Switching Guide*, Release 6.4.2.

service-carvingac-driven

Use this command to enable the AC-influenced method for any selected Designated Forwarder (DF) algorithm.

Enabling the `ac-driven` method allows the Designated Forwarder (DF) algorithm to be influenced by the Attachment Circuits (AC's) associated with a specific Ethernet Segment (ES). This means that the DF selection is based on the AC's characteristics and conditions, such as whether an AC is operational UP, mapped, or unmapped on the ESI.

Use `no` form of this command to disable the AC-influenced method for any selected Designated Forwarder (DF) algorithm.

CommandSyntax

```
service-carving ac-driven
no service-carving ac-driven
```

Parameters

None

Default

`ac-driven` is disabled.

Command Mode

EVPN Ethernet Segment (ES) Mode

Applicability

This command was introduced in the OcNOS version 6.4.2.

Example

The provided examples showcase the configuration of the `service-carving ac-driven` command in EVPN Ethernet Segment (ES) mode. The first two examples demonstrate enabling this feature with different DF election methods, and the final example illustrates the command to disable `service-carving ac-driven`.

```
OcNOS#configure terminal
OcNOS(config)#interface sa1
OcNOS(config-if)#evpn multi-homed esi 11:22:33:44:55:66:77:88:99 load-
balancing single-active
OcNOS(config-if-es)#service-carving preference-based
OcNOS(config-if-es)#service-carving ac-driven
OcNOS(config-if-es)#end

OcNOS#configure terminal
OcNOS(config)#interface sa1
OcNOS(config-if)#evpn multi-homed esi 11:22:33:44:55:66:77:88:99 load-
balancing single-active
OcNOS(config-if-es)#service-carving auto
OcNOS(config-if-es)#service-carving ac-driven

OcNOS(config-if-es)#no service-carving ac-driven
OcNOS(config-if-es)#end
```

service-carving

Use this command to provide the flexibility to select the Designated Forwarder (DF) election algorithm based on preference based or modulo-based DF election.

Use no form of this command to disable service-carving.

Command Syntax

```
service-carving (preference-based|auto)
```

```
no service-carving
```

Parameters

`preference-based`	Select the DF election algorithm based on preference based.
`auto`	Select the DF election algorithm based on modulo based.

Default

None

Command Mode

EVPN ES Mode

Applicability

This command was introduced in the OcNOS version 6.4.1.

Example

The following examples demonstrate the configuration of the `service-carving` command in both `single-active` or `port-active` mode for the EVPN multi-homed system, with one utilizing `auto` service carving and the other using `preference-based` service carving.

```
OcNOS#configure terminal
OcNOS(config)#interface sa1
OcNOS(config-if)#evpn multi-homed esi 11:22:33:44:55:66:77:88:99 load-
balancing single-active
OcNOS(config-if-es)#service-carving auto
OcNOS(config-if-es)#end

OcNOS#configure terminal
OcNOS(config)#interface po1
OcNOS(config-if)#evpn multi-homed system-mac 0000.0000.0011 load-balancing
port-active
OcNOS(config-if-es)#service-carving auto
OcNOS(config-if-es)#end

OcNOS#configure terminal
OcNOS(config)#interface po1
OcNOS(config-if)#evpn multi-homed system-mac 0000.0000.0011 load-balancing
port-active
OcNOS(config-if-es)#service-carving preference-based
OcNOS(config-if-es)#end
```

The following example is used to disable the `service-carving` for the EVPN multi-homed system.

```
OcNOS(config-if-es)#no service-carving
OcNOS(config-if-es)#end
```

service-carving weight

Use this command to specify a preference value when the preference-based Designated Forwarder (DF) election algorithm is selected. This preference value determines the priority of the local PE device to become the DF for a particular Ethernet segment.

Use no form of this command to replace the preference weight value and choose the default preference value.

Command Syntax

```
service-carving weight <1-65535>
```

```
no service-carving weight
```

Parameters

`weight <1-65535>` Specifies the preference weight value. A lower weight value indicates a higher priority for becoming the DF.

Default

The service-carving weight command is set to 32767 by default.

Command Mode

EVPN Ethernet Segment (ES) Mode

Applicability

This command was introduced in the OcNOS version 6.4.1.

Example

The `service-carving weight` command is used to configure the preference weight value for service-carving in both port-active and single-active modes.

```
OcNOS#configure terminal
OcNOS(config)#interface po1
OcNOS(config-if)#evpn multi-homed system-mac 0000.0000.0011 load-balancing
port-active
OcNOS(config-if-es)#service-carving preference-based
OcNOS(config-if-es)#service-carving weight 100
OcNOS(config-if-es)#end

OcNOS#configure terminal
OcNOS(config)#interface sa1
OcNOS(config-if)#evpn multi-homed esi 11:22:33:44:55:66:77:88:99 load-
balancing single-active
OcNOS(config-if-es)#service-carving preference-based
OcNOS(config-if-es)#service-carving weight 100
```

To disable the configured weight, use the `no service-carving weight` command.

```
OcNOS(config-if-es)#no service-carving weight
OcNOS(config-if-es)#end
```

Revised CLI Commands

Below is the revised command for configuring EVPN Active-Standby.

evpn multi-homed

- The command `evpn multi-homed` allows users to configure single-active and port-active load-balancing Ethernet Segment Identifier (ESI) on a link with a multihomed Customer Edge (CE) in the context of EVPN multi-homed configurations. For more details, refer to the *evpn multi-homed* command in the *EVPN MPLS Commands* chapter in the Multi-Protocol Label Switching Guide, Release 6.4.2.
- The existing syntax now includes the newly added parameter for load-balancing, namely `single-active and port-active`.

Troubleshooting

To ensure the reliable operation of the single-active or port-active setup and maintain data accuracy and consistency, follow these troubleshooting steps:

1. Verify the Configuration:
   - Use the `show running-config` command to confirm that the ESI configuration includes `load-balancing single-active or port-active`, such as:

     `evpn multi-homed esi 11:22:33:44:55:66:77:88:99 load-balancing single-active`

     or

     `evpn multi-homed system-mac 0000.4321.1234 load-balancing port-active`

- Ensure that the `service-carving` algorithm type is configured.

2. Verify the `show` command:
   - Use the `show bgp l2vpn evpn multihoming es-route` command to confirm that it matches the `service-carving` algorithm type.
   - Use the `show evpn load-balance single-active or port-active` command to verify the status of the Multihomed (MH) nodes as `ACTIVE` and `STANDBY`.
3. **Ensure Proper Connectivity:** Validate the connectivity between the router and the EVPN tunnel to ensure it is up. This involves verifying network settings, ports, and firewalls.
4. **For the server:** Enable debugging on OcNOS and enable debug mode. Verify the logs in `/var/log/messages` for further insights.

Abbreviations

The following are some key abbreviations and their meanings relevant to this document:

Acronym	Description
EVPN	Ethernet Virtual Private Network
ELINE	Ethernet Line services
ELAN	Ethernet LAN services
LAN	Local Area Network
CE	Customer Edge
PE	Provider Edge
MH	Multihoming
AC	Attachment Circuit
LACP	Link Aggregation Control Protocol
BUM	Broadcast, Unknown Unicast, Multicast
MAC	Media Access Control
ARP/ND	Address Resolution Protocol/Neighbor Discovery
DF	Designated Forwarder

Glossary

The following provides definitions for key terms used throughout this document.

Ethernet Virtual Private Network (EVPN)	A network technology that extends Layer 2 Ethernet services over a Layer 3 IP/MPLS network.
Ethernet Line services (ELINE)	Two PEs are directly connected over an Ethernet link, enabling redundancy and efficient data exchange.
Ethernet LAN services (ELAN)	A group of PEs are interconnected in a multipoint Ethernet network, providing redundancy and optimized data transfer.
Port-Active	A redundancy mechanism in which multiple Provider Edge (PE) devices can be active simultaneously for the same host or MAC address, with specific active ports associated with each active PE.
Single-Active	A redundancy mechanism in which only one of the Provider Edge (PE) devices is active at a time for handling traffic for a specific host or MAC address.
Customer Edge (CE)	A device at the customer's network edge that connects to the service provider's network.
Provider Edge (PE)	A device at the service provider's network edge that connects to customer edge devices.
Multihoming (MH)	Connecting a host or CE device to multiple PE devices for redundancy and load balancing.
Attachment Circuit (AC)	The connection between a CE device and a PE device in an EVPN network.
Link Aggregation Control Protocol (LACP)	A protocol used to manage and bundle multiple physical links into a single logical link for higher bandwidth and redundancy.
Broadcast, Unknown Unicast, Multicast (BUM)	Categories of network traffic that includes broadcast, unknown unicast, and multicast packets.
Media Access Control (MAC)	A unique identifier assigned to network interfaces, typically associated with a hardware address.
Address Resolution Protocol/Neighbor Discovery (ARP/ND)	Protocols used to map IP addresses to MAC addresses in a local network.
Designated Forwarder (DF)	A PE device selected to forward broadcast, unknown unicast, and multicast traffic within an Ethernet segment.
Redundancy	The provision of duplicate equipment or links to ensure network availability in case of failures.
Failover	The process of switching to a backup device or link in case of a primary device or link failure.
Resiliency	The ability of a network to maintain its functionality even in the face of failures or disruptions.
Unicast	Communication between a single sender and a single receiver in a network.
Multicast	Communication from a single sender to multiple receivers in a network.
Egress	The process of traffic leaving a device or network segment.
Standby	In redundancy, a secondary device or link that is ready to take over in case the primary device or link fails.
Active	In redundancy, the primary device or link that is currently handling traffic.

Forwarding	The process of transmitting network packets from one device to another.
Link State	The operational status of a network link, indicating whether it is up or down.
Virtual Routing and Forwarding (VRF)	A technology that enables multiple instances of a routing table to coexist within a router.
Virtual Local Area Network (VLAN)	A logical network segment within a physical network.
Data Exchange	The process of sending and receiving data between network devices.
Downtime	The period during which a network or service is not available due to maintenance or failures.

Anycast Gateway Routing for Multiple Subnets in EVPN-IRB

Overview

In the Ethernet VPN Integrated Routing and Bridging (EVPN-IRB) scenario, any two Layer 2 Virtual Network Identifiers (L2 VNID) nodes communicate using the Routing IP Virtual Routing and Forwarding (VRF). This communication is enriched with Anycast Gateway Routing to accommodate communication among multiple subnets under the IRB interface (per VNID).

In the current implementation, the router's primary IPv4 or IPv6 address is either Router Media Access Control (MAC) or Anycast MAC, and the secondary IPv4 or IPv6 address is always the Router MAC address. Hence, Anycast MAC support was only for the primary IP with a single subnet.

Additionally, the BGP router cannot establish a connection with the primary IP as it is in Anycast mode, and the TCP connection is possible only with any of the routers, as both the routes have the IP as Anycast.

To overcome this drawback, the feature is enhanced to configure both Router MAC or Anycast MAC for both primary and secondary subnets.

By default, each subnet uses the Router MAC address received from the ARP/ND cache. The `anycast` argument in `evpn irb-if forwarding anycast gateway` CLI is used to configure the Anycast MAC for primary or secondary subnets. The argument helps to update the ARP/ND cache with Anycast MAC. This enables the user to use Anycast MAC for multiple subnets under L2 VNID. For example, users can have Subnets A, B, C with Anycast MAC and Subnet D with Router MAC.

Feature Characteristics

This feature enhancement provides the following support:

- Enables configuration of either a Router MAC or an Anycast MAC address for primary or secondary subnets.
- Use of Anycast or Routing IP Gateway for multiple subnets under the Layer-2 VNID's.
- Flexibility to have Anycast Gateway for multiple subnets (for example, Subnet A, B, and C) while allowing the other subnet (for example, Subnet D) to be reserved for BGP.
- The InterfaceFull model that provides the flexibility to respond to the ARP/ND requests from the ARP/ND table.
- The InterfaceLess model that use the kernel interface with a unique MAC per interface, either Router MAC or Anycast MAC for all the subnets.

LIMITATIONS:

In InterfaceLess model, the kernel IRB interface has a single MAC that is either Router MAC or Anycast MAC, however, the response message always has Anycast MAC irrespective of whether the interface's IP address is Anycast or Router MAC.

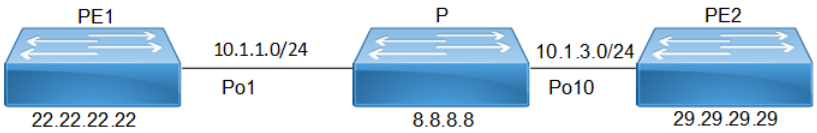
Benefits

Allows users to have primary and secondary subnets with either Router MAC or Anycast MAC. This flexibility provides support for Anycast Gateway for multiple subnets under Layer 2 VNIDs.

Configuration

Following configuration illustrates how to use the `anycast` argument in `evpn irb-if forwarding anycast gateway` CLI to configure the Anycast MAC for both primary or secondary subnets.

Topology



Anycast Gateway support for subnets

PE1 Configuration

PE1: Loopback Interface

`PE1(config)#interface lo`	Enter the loopback interface mode.
`PE1(config-if)#ip address 22.22.22.22/32 secondary`	Configure the IP address on loopback interface.
`PE1(config-if)#ip router isis ISIS-100`	Enable the IS-IS routing on an interface for area 49 (ISIS-100).
`PE1(config-if)#enable-ldp ipv4`	Enable the LDP IPv4.
`PE1(config-if)#Commit`	Commit the configurations
`PE1(config-if)#exit`	Exit the configuration mode.

PE1: Global LDP

`PE1(config)#router ldp`	Enter the Router LDP mode.
`PE1(config-router)#router-id 22.22.22.22`	Enter the LDP router-id.
`PE1(config-router)#targeted-peer ipv4 29.29.29.29`	Configure the LDP target peer address.
`PE1(config-router-targeted-peer)#exit-targeted-peer-mode`	Exit from targeted peer mode.
`PE1(config-router)#transport-address ipv4 22.22.22.22`	Configure the LDP transport address.
`PE1(config-router)#Commit`	Commit the configurations
`PE1(config-router)#exit`	Exit the configuration mode.

PE1: Interface Configuration on Network Side

`PE1(config)#interface po1`	Enter the Interface mode for the port channel interface
`PE1(config-if)#ip address 10.1.1.22/24`	Configure the IP address on port channel interface
`PE1(config-if)#label-switching`	Enable the label switching
`PE1(config-if)#ip router isis ISIS-100`	Enable the IS-IS routing on an interface for area 49 (ISIS-100)
`PE1(config-if)#enable-ldp ipv4`	Enable the LDP IPv4
`PE1(config-if)#interface xe22`	Enter interface mode
`PE1(config-if)#channel-group 1 mode active`	Moving interface to Dynamic LAG 1
`PE1(config-if)#Commit`	Commit the configurations
`PE1(config-if)#exit`	Exit the configuration mode.

PE1: IGP-ISIS Configuration

`PE1(config)#router isis ISIS-100`	Create an ISIS routing instance for area 49 (ISIS-100).
`PE1(config-router)#is-type level-1`	Configure instance as level-1 routing.
`PE1(config-router)#metric-style wide`	Configure the new style of metric type as wide.
`PE1(config-router)#mpls traffic-eng router-id 22.22.22.22`	Configure MPLS-TE unique router-id TLV.
`PE1(config-router)#mpls traffic-eng level-1`	Enable the MPLS-TE in is-type Level-1.
`PE1(config-router)#capability cspf`	Enable the Constrained Shortest Path First (CSPF).
`PE1(config-router)#dynamic-hostname`	Configure the host name to be advertised for an ISIS instance.
`PE1(config-router)#net 49.0001.0000.0000.0001.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.
`PE1(config-router)#Commit`	Commit the configurations
`PE1(config-router)#exit`	Exit the configuration mode.

PE1: BGP Configuration

`PE1(config)#router bgp 65535`	Enter into Router BGP mode.
`PE1(config-router)#bgp router-id 22.22.22.22`	Configure router-id as 22.22.22.22 (loopback ip address).
`PE1(config-router)#neighbor 29.29.29.29 remote-as 65535`	Configuring PE2 as iBGP neighbor using it's loopback IP.
`PE1(config-router)#neighbor 29.29.29.29 update- source lo`	Source of routing updates as loopback.
`PE1(config-router)#neighbor 29.29.29.29 advertisement-interval 0`	Configure advertisement-interval as 0 for fast convergence for PE2
`PE1(config-router)#address-family l2vpn evpn`	Enter into l2vpn EVPN address family mode.

`PE1(config-router-af)#neighbor 29.29.29.29 active`	Enabling EVPN Address family for neighbor.
`PE1(config-router-af)#exit-address-family`	Exiting of Address family mode.
`PE1(config-router)#address-family ipv4 vrf ip_vrf205_mgmt`	Entering into VRF address family mode.
`PE1(config-router-af)#redistribute connected`	Redistribute connected routes to the network.
`PE1(config-router-af)#exit-address-family`	Exiting of Address family mode.
`PE1(config-router)#Commit`	Commit the configurations
`PE1(config-router)#exit`	Exit the configuration mode.

PE1: Global EVPN MPLS Command

`PE1(config)#evpn mpls enable`	Enable the EVPN MPLS globally.
`PE1(config)#evpn mpls irb`	Enable the EVPN MPLS IRB globally.
`PE1(config)#evpn mpls multihoming enable`	Enable the Multi homing, save configures and reboot the board for multi homing to be effective.
`PE1(config)#qos enable`	Enable the QOS.
`PE1(config)#evpn irb-forwarding anycast-gateway-mac 0011.2233.4455`	Configure anycast gateway MAC globally.
`PE1(config)#evpn mpls vtep-ip-global 22.22.22.22`	Configure VTEP global IP.
`PE1(config)#Commit`	Commit the configurations
`PE1(config)#exit`	Exit the configuration mode.

PE1: MAC VRF Configuration

`PE1(config)#mac vrf vrf205_mgmt`	Enter Mac VRF mode.
`PE1(config-vrf)#rd 22.22.22.22:205`	Configuring Route-Distinguisher value.
`PE1(config-vrf)#route-target both evpn-auto-rt`	Configuring import and export value as evpn-auto-rt. Route targets will be derived automatically.
`PE1(config-vrf)#Commit`	Commit the configurations
`PE1(config-vrf)#exit`	Exit the configuration mode.

PE1: IP VRF Configuration

`PE1(config)#ip vrf ip_vrf205_mgmt`	Enter IP VRF mode
`PE1(config-vrf)#rd 22.22.22.22:305`	Configuring Route-Distinguisher value
`PE1(config-vrf)#route-target both 305:305`	Configuring route target values i.e import and export values
`PE1(config-vrf)#l3vni 305`	Configure L3 VNID for routing
`PE1(config-vrf)#Commit`	Commit the configurations
`PE1(config-vrf)#exit`	Exit the configuration mode.

PE1: IRB Interface Configuration with multiple IPs

`PE1(config)#interface irb127`	Create IRB interface irb127
`PE1(config-irb-if)#ip vrf forwarding ip_vrf205_mgmt`	Bind the VRF instance to the interface
`PE1(config-irb-if)#evpn irb-if-forwarding anycast-gateway-mac`	Enable an IRB interface to use the global anycast IRB mac-address
`PE1(config-irb-if)#ip address 98.98.101.1/24 anycast`	Configure the IPv4 primary address and use anycast mac address
`PE1(config-irb-if)#ip address 103.103.102.1/24 secondary`	Configure secondary IPv4 secondary address
`PE1(config-irb-if)#ip address 104.104.103.1/24 secondary anycast`	Configure secondary IPv4 secondary address and use as anycast mac address
`PE1(config-irb-if)#Commit`	Commit the configurations
`PE1(config-irb-if)#exit`	Exit the configuration mode.

PE1: EVPN MPLS Id Configuration

`PE1(config)#evpn mpls id 127`	Configure secondary IPv4 secondary address
`PE1(config-evpn-mpls)#host-reachability-protocol evpn-bgp vrf205_mgmt`	Map the MAC VRF red
`PE1(config-evpn-mpls)#evpn irb irb127`	Map the IRB interface
`PE1(config-evpn-mpls)#Commit`	Commit the configurations
`PE1(config-evpn-mpls)#exit`	Exit the configuration mode.

PE1: Interface Configuration on Access Side

`PE1(config)#interface xe72.127 switchport`	Creating L2 sub interface of physical interface xe72
`PE1(config-if)#encapsulation dot1q 127`	Setting Encapsulation to dot1q with VLAN ID 127 Supported Encapsulation: dot1ad, dot1q, untagged, default
`PE1(config-if)#rewrite pop`	Configure rewrite with action pop
`PE1(config-if)#access-if-evpn`	Entering Access mode for EVPN MPLS ID configuration
`PE1(config-acc-if-evpn)#map vpn-id 127`	Map VPN-ID 127
`PE1(config-acc-if-evpn)#Commit`	Commit the configurations
`PE1(config-acc-if-evpn)#exit`	Exit the configuration mode.

P Configuration

P: Loopback Interface

`P(config)#interface lo`	Enter the Interface mode for the loopback interface.
`P(config-if)#ip address 8.8.8.8/32 secondary`	Configure the IP address on loopback interface.
`P(config-if)#ip router isis ISIS-100`	Enable the IS-IS routing on an interface for area 49 (ISIS-100).
`P(config-if)#enable-ldp ipv4`	Enable the LDP IPv4.
`P(config-if)#Commit`	Commit the configurations
`P(config-if)#exit`	Exit the configuration mode.

P: Global LDP

`P(config)#router ldp`	Enter the Router LDP mode.
`P(config-router)#router-id 8.8.8.8`	Enter the LDP router-id.
`P(config-router)#transport-address ipv4 8.8.8.8`	Configure the LDP transport address.
`P(config-router)#Commit`	Commit the configurations
`P(config-router)#exit`	Exit the configuration mode.

P: Interface Configuration on Network Side

`P(config)#interface po1`	Enter the Interface mode for the port channel interface.
`P(config-if)#ip address 10.1.1.8/24`	Configure the IP address on port channel interface.
`P(config-if)#label-switching`	Enable the label switching.
`P(config-if)#ip router isis ISIS-100`	Enable the IS-IS routing on an interface for area 49 (ISIS-100).
`P(config-if)#enable-ldp ipv4`	Enable the LDP IPv4.
`P(config-if)#Commit`	Commit the configurations
`P(config-if)#exit`	Exit the configuration mode.
`P(config)#interface xe22`	Enter interface mode.
`P(config-if)#channel-group 1 mode active`	Moving interface to Dynamic LAG 1.
`P(config-if)#Commit`	Commit the configurations
`P(config-if)#exit`	Exit the configuration mode.
`P(config)#interface po10`	Enter the Interface mode for the port channel interface.
`P(config-if)#ip address 10.1.3.8/24`	Configure the IP address on port channel interface.
`P(config-if)#label-switching`	Enable the label switching.
`P(config-if)#ip router isis ISIS-100`	Enable the IS-IS routing on an interface for area 49 (ISIS-100).
`P(config-if)#enable-ldp ipv4`	Enable the LDP IPv4.
`P(config-if)#interface xe10`	Enter interface mode.
`P(config-if)#channel-group 10 mode active`	Moving interface to Dynamic LAG 10.
`P(config-if)#Commit`	Commit the configurations
`P(config-if)#exit`	Exit the configuration mode.

P: IGP-ISIS Configuration

`P(config)#router isis ISIS-100`	Create an IS-IS routing instance for area 49 (ISIS-100).
`P(config-router)#is-type level-1`	Configure the instance as level-1 routing.
`P(config-router)#metric-style wide`	Configure the new style of metric type as wide.
`P(config-router)#mpls traffic-eng router-id 8.8.8.8`	Configure MPLS-TE unique router-id TLV.
`P(config-router)#mpls traffic-eng level-1`	Enable the MPLS-TE in is-type Level-1.
`P(config-router)#capability cspf`	Enable the CSPF (Constrained Shortest Path First).
`P(config-router)#dynamic-hostname`	Configure the hostname to be advertised for an ISIS instance.

`P(config-router)#net 49.0001.0000.0000.0002.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.
`P(config-router)#Commit`	Commit the configurations
`P(config-router)#exit`	Exit the configuration mode.

PE2 Configuration

PE2: Loopback Interface

`PE2(config)#interface lo`	Enter the Interface mode for the loopback interface.
`PE2(config-if)#ip address 29.29.29.29/32 secondary`	Configure the IP address on loopback interface.
`PE2(config-if)#ip router isis ISIS-100`	Enable the IS-IS routing on an interface for area 49 (ISIS-100).
`PE2(config-if)#enable-ldp ipv4`	Enable the LDP IPv4.
`PE2(config-if)#Commit`	Commit the configurations
`PE2(config-if)#exit`	Exit the configuration mode.

PE2: Global LDP

`PE2(config)#router ldp`	Enter the Router LDP mode.
`PE2(config-router)#router-id 29.29.29.29`	Enter the LDP router-id.
`PE2(config-router)#targeted-peer ipv4 22.22.22.22`	Configure the LDP target peer address.
`PE2(config-router-targeted-peer)#exit-targeted-peer-mode`	Exit from targeted peer mode.
`PE2(config-router)#transport-address ipv4 29.29.29.29`	Configure the LDP transport address.
`PE2(config-router)#Commit`	Commit the configurations
`PE2(config-router)#exit`	Exit the configuration mode.

PE2: Global LDP

`PE2(config)#router ldp`	Enter the Router LDP mode.
`PE2(config-router)#router-id 29.29.29.29`	Enter the LDP router-id.
`PE2(config-router)#targeted-peer ipv4 22.22.22.22`	Configure the LDP target peer address.
`PE2(config-router-targeted-peer)#exit-targeted-peer-mode`	Exit from targeted peer mode.
`PE2(config-router)#transport-address ipv4 29.29.29.29`	Configure the LDP transport address.
`PE2(config-router)#Commit`	Commit the configurations
`PE2(config-router)#exit`	Exit the configuration mode.

PE2: Interface Configuration on Network Side

`PE2(config)#interface po10`	Enter the Interface mode for the port channel interface.
`PE2(config-if)#ip address 10.1.3.29/24`	Configure the IP address on port channel interface.
`PE2(config-if)#label-switching`	Enable the label switching.
`PE2(config-if)#ip router isis ISIS-100`	Enable the IS-IS routing on an interface for area 49 (ISIS-100).
`PE2(config-if)#enable-ldp ipv4`	Enable the LDP IPv4.
`PE2(config-if)#interface ge1`	Enter interface mode.

`PE2(config-if)#channel-group 10 mode active`	Moving interface to Dynamic LAG 10.
`PE2(config-if)#Commit`	Commit the configurations
`PE2(config-if)#exit`	Exit the configuration mode.

PE2: IGP-ISIS Configuration

`PE2(config)#router isis ISIS-100`	Create an IS-IS routing instance for area 49 (ISIS-100).
`PE2(config-router)#is-type level-1`	Configure instance as level-1 routing.
`PE2(config-router)#metric-style wide`	Configure the new style of metric type as wide.
`PE2(config-router)#mpls traffic-eng router-id 29.29.29.29`	Configure MPLS-TE unique router-id TLV.
`PE2(config-router)#mpls traffic-eng level-1`	Enable the MPLS-TE in is-type Level-1.
`PE2(config-router)#capability cspf`	Enable the CSPF (Constrained Shortest Path First).
`PE2(config-router)#dynamic-hostname`	Configure the hostname to be advertised for an ISIS instance.
`PE2(config-router)#net 49.0001.0000.0000.0029.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.
`PE2(config-router)#Commit`	Commit the configurations
`PE2(config-router)#exit`	Exit the configuration mode.

PE2: BGP Configuration

`PE2(config)#router bgp 65535`	Enter into Router BGP mode.
`PE2(config-router)#bgp router-id 29.29.29.29`	Configure router-id as 29.29.29.29 (loopback ip address).
`PE2(config-router)#neighbor 22.22.22.22 remote-as 65535`	Configuring PE2 as iBGP neighbor using it's loopback IP.
`PE2(config-router)#neighbor 22.22.22.22 update- source lo`	Source of routing updates as loopback.
`PE2(config-router)#neighbor 22.22.22.22 advertisement-interval 0`	Configure advertisement-interval as 0 for fast convergence for PE2.
`PE2(config-router)#address-family l2vpn evpn`	Enter into l2vpn EVPN address family mode.
`PE2(config-router-af)#neighbor 22.22.22.22 active`	Enabling EVPN Address family for neighbor.
`PE2(config-router-af)#exit-address-family`	Exiting of Address family mode.
`PE2(config-router)#address-family ipv4 vrf ip_vrf205_mgmt`	Entering into VRF address family mode.
`PE2(config-router-af)#redistribute connected`	Redistribute connected routes to the network.
`PE2(config-router-af)#exit-address-family`	Exiting of Address family mode.
`PE2(config-router-af)#commit`	Commit the configurations
`PE2(config-router-af)#exit`	Exit the configuration mode.

PE2: Global EVPN MPLS Command

`PE2(config)#evpn mpls enable`	Enable the EVPN MPLS globally.
`PE2(config)#evpn mpls irb`	Enable the EVPN MPLS IRB globally.
`PE2(config)#evpn mpls multihoming enable`	Enable the Multihoming, save configs and reboot the board for multihoming to be effective.
`PE2(config)#qos enable`	Enable the QOS.

`PE2(config)#evpn irb-forwarding anycast-gateway-mac 0011.2233.4567`	Configure anycast gateway MAC globally.
`PE2(config)#evpn mpls vtep-ip-global 29.29.29.29`	Configure VTEP global IP.
`PE2(config)#Commit`	Commit the configurations
`PE2(config)#exit`	Exit the configuration mode.

PE2: MAC VRF Configuration

`PE2(config)#mac vrf vrf205_mgmt`	Enter Mac VRF mode.
`PE2(config-vrf)#rd 29.29.29.29:205`	Configuring Route-Distinguisher value.
`PE2(config-vrf)#route-target both evpn-auto-rt`	Configuring import and export value as evpn-auto-rt. Route target will be derived automatically.
`PE2(config-vrf)#Commit`	Commit the configurations
`PE2(config-vrf#exit`	Exit the configuration mode.

PE2: IP VRF Configuration

`PE2(config)#ip vrf ip_vrf205_mgmt`	Enter IP VRF mode.
`PE2(config-vrf)#rd 29.29.29.29:305`	Configuring Route-Distinguisher value.
`PE2(config-vrf)#route-target both 305:305`	Configuring route target values i.e import and export values.
`PE2(config-vrf)#l3vni 305`	Configure L3 VNID for routing.
`PE2(config-vrf)#Commit`	Commit the configurations
`PE2(config-vrf)#exit`	Exit the configuration mode.

PE2: IRB Interface Configuration with multiple IPs

`PE2(config)#interface irb127`	Create IRB interface irb127.
`PE2(config-irb-if)#ip vrf forwarding ip_vrf205_mgmt`	Bind the VRF instance to the interface.
`PE2(config-irb-if)#evpn irb-if-forwarding anycast-gateway-mac`	Enable an IRB interface to use the global anycast IRB mac-address.
`PE2(config-irb-if)#ip address 99.99.101.1/24 anycast`	Configure the IPv4 primary address and use anycast mac address.
`PE2(config-irb-if)#ip address 103.103.103.1/24 secondary`	Configure secondary IPv4 secondary address.
`PE2(config-irb-if)#ip address 104.104.104.1/24 secondary anycast`	Configure secondary IPv4 secondary address and use as anycast mac address.
`PE2(config-rib-if)#Commit`	Commit the configurations
`PE2(config-rib-if)#exit`	Exit the configuration mode.

PE2: EVPN MPLS Id Configuration

`PE2(config)#evpn mpls id 127`	Configure secondary IPv4 secondary address.
`PE2(config-evpn-mpls)#host-reachability-protocol evpn-bgp vrf205_mgmt`	Map the MAC VRF red.
`PE2(config-evpn-mpls)#evpn irb irb127`	Map the IRB interface.
`PE2(config-evpn-mpls)#Commit`	Commit the configurations
`PE2(config-evpn-mpls)#exit`	Exit the configuration mode.

PE2: Interface Configuration on Access Side

`PE2(config)#interface xe12.127 switchport`	Creating L2 sub interface on physical interface xe12.
`PE2(config-if)#encapsulation dot1q 127`	Setting Encapsulation to dot1q with VLAN ID 127 Supported Encapsulation: dot1ad, dot1q, untagged, default.
`PE2(config-if)#rewrite pop`	Configure rewrite with action pop.
`PE2(config-if)#access-if-evpn`	Entering Access mode for EVPN MPLS ID configuration.
`PE2(config-acc-if-evpn)#map vpn-id 127`	Map VPN-ID 127.
`PE2(config-acc-if-evpn)#Commit`	Commit the configurations
`PE2(config-acc-if-evpn)#exit`	Exit the configuration mode.

Validation

Verify installed EVPN MPLS tunnels information.

PE1:

```
#show evpn mpls
EVPN-MPLS Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged

VPN-ID   EVI-Name     EVI-Type Type Interface ESI                          VLAN      DF-Status Src-Addr         Dst-Addr
_____________________________________________________________________________________________________________________
___
127      ----         L2       NW   ----      ----                         ----      ----      22.22.22.22      29.29.29.29
127      ----         --       AC   xe72.127  --- Single Homed Port ---    ----      ----      ----             ----
```

PE2:

```
#show evpn mpls tunnel
EVPN-MPLS Network tunnel Entries
Source            Destination       Status         Up/Down        Update         evpn-id
=============================================================================================
22.22.22.22       29.29.29.29       Installed      11:40:31       11:40:31       127
```

Verify the MAC addresses that are cached in the EVPN MAC and ARP table.

Verify the Anycast Gateway MAC addresses that are updated when configuring subnets with Anycast MAC:

PE1 verification:

```
#show evpn mpls mac-table
=============================================================================================================================
============
                                                EVPN MPLS MAC Entries
=============================================================================================================================
=============
VNID       Interface VlanId    In-VlanId Mac-Addr       VTEP-Ip/ESI                  Type            Status     MAC move
AccessPortDesc
_____________________________________________________________________________________________________________________
___________
127        irb127    ----      ----      0011.2233.4455 22.22.22.22                  Static Local    -------    0        -------
127        irb127    ----      ----      e49d.73b3.c101 22.22.22.22                  Static Local    -------    0        -------
127        ----      ----      ----      0011.2233.4567 29.29.29.29                  Static Remote   -------    0        -------
127        ----      ----      ----    e8c5.7aff.96de   29.29.29.29                  Static Remote   -------    0        -------
```

```
Total number of entries are 4

#show evpn mpls arp-cache
MPLS-EVPN ARP-CACHE Information
================================
EVPN-ID   Ip-Addr          Mac-Addr        Type         Age-Out   Retries-Left
_____________________________________________________________________________
127       98.98.101.1      0011.2233.4455 Static Local   ----
127       99.99.101.1      0011.2233.4567 Static Remote  ----
127       103.103.102.1    e49d.73b3.c101 Static Local   ----
127       103.103.103.1    e8c5.7aff.96de  Static Remote  ----
127       104.104.103.1    0011.2233.4455 Static Local   ----
127       104.104.104.1    0011.2233.4567 Static Remote  ----
Total number of entries are 6
```

PE2 verification:

```
#show evpn mpls mac-table
================================================================================================================================
=============
                                                EVPN MPLS MAC Entries
================================================================================================================================
=============
VNID       Interface VlanId    In-VlanId Mac-Addr       VTEP-Ip/ESI                  Type            Status     MAC move
AccessPortDesc
________________________________________________________________________________________________________________________
_____________
127        ----      ----      ----      0011.2233.4455 22.22.22.22                Static Remote   -------    0       -------
127        irb127    ----      ----      0011.2233.4567 29.29.29.29                Static Local    -------    0       -------
127        ----      ----      ----      e49d.73b3.c101 22.22.22.22                Static Remote   -------    0       -------
127        irb127    ----      ----      e8c5.7aff.96de 29.29.29.29                Static Local    -------    0       -------

Total number of entries are : 4

#show evpn mpls arp-cache
MPLS-EVPN ARP-CACHE Information
================================
ARP Timeout :  180 sec   Random-Jitter-Max : 200

EVPN-ID   Ip-Addr          Mac-Addr        Type         Age-Out   Retries-Left
_____________________________________________________________________________
127       98.98.101.1      0011.2233.4455 Static Remote  ----
127       99.99.101.1      0011.2233.4567 Static Local   ----
127       103.103.102.1    e49d.73b3.c101 Static Remote  ----
127       103.103.103.1    e8c5.7aff.96de Static Local   ----
127       104.104.103.1    0011.2233.4455 Static Remote  ----
127       104.104.104.1    0011.2233.4567 Static Local   ----
```

Verify EVPN route count information as per VPN-ID or Route type:

PE1 verification:

```
#show evpn mpls route-count
EVPN-MPLS Active route count information
=====================================
Max supported route count   : 131072
Active route count: 8

-------------------------------------------
 VNID      Total    MACONLY  MACIPv4  MACIPv6
```

```
-------------------------------------------
127              8             0                   6            2
```

PE2 verification:

```
#show evpn mpls route-count
EVPN-MPLS Active route count information
====================================
Max supported route count   : 131072
Active route count: 8

-------------------------------------------
 VNID     Total    MACONLY  MACIPv4  MACIPv6
--------------------------------
 127              8             0                   6            2
```

Verify in the BGP EVPN table:

PE1 Verification:

```
#show bgp l2vpn evpn
BGP table version is 2, local router ID is 22.22.22.22
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

[EVPN route type]:[ESI]:[VNID]:[relevant route information]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route
5 - Prefix Route

    Network          Next Hop            Metric    LocPrf       Weight     Path  Peer          Encap

RD[10:200]
*>i  [5]:[0]:[0]:[24]:[80.80.1.0]:[0.0.0.0]:[17]
                     29.29.29.29          0        100       0    ?  29.29.29.29     MPLS

RD[20:200]
*>i  [5]:[0]:[0]:[24]:[80.80.1.0]:[0.0.0.0]:[16]
                     10.10.10.10          0        100       0    ?  10.10.10.10     MPLS

RD[10.10.10.10:123]
*>i  [2]:[0]:[123]:[48,0011:2233:4567]:[32,99.99.99.1]:[22]
                     10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>i  [3]:[123]:[32,10.10.10.10]
                     10.10.10.10          0        100       0    i  10.10.10.10     MPLS

RD[10.10.10.10:124]
*>i  [2]:[0]:[124]:[48,0011:2233:4567]:[32,99.99.100.1]:[24]
                     10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>i  [3]:[124]:[32,10.10.10.10]
                     10.10.10.10          0        100       0    i  10.10.10.10     MPLS

RD[10.10.10.10:125]
*>i  [2]:[0]:[125]:[48,0011:2233:4567]:[32,88.88.3.1]:[21]
                     10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>i  [3]:[125]:[32,10.10.10.10]
```

```
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS

RD[10.10.10.10:126]
*>i  [3]:[126]:[32,10.10.10.10]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS

RD[10.10.10.10:205]
*>i  [2]:[0]:[127]:[48,0011:2233:4567]:[32,99.99.101.1]:[26]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>i  [2]:[0]:[127]:[48,0011:2233:4567]:[32,104.104.104.1]:[26]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>i  [2]:[0]:[127]:[48,0011:2233:4567]:[128,1000::1][26]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>i  [2]:[0]:[127]:[48,d077:ce2a:8001]:[32,103.103.103.1]:[26]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>i  [2]:[0]:[127]:[48,d077:ce2a:8001]:[128,1100::1][26]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>i  [3]:[127]:[32,10.10.10.10]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS

RD[10.10.10.10:305]
*>i  [5]:[0]:[0]:[24]:[99.99.101.0]:[0.0.0.0]:[17]
                      10.10.10.10          0        100       0    ?  10.10.10.10     MPLS
*>i  [5]:[0]:[0]:[24]:[103.103.103.0]:[0.0.0.0]:[17]
                      10.10.10.10          0        100       0    ?  10.10.10.10     MPLS
*>i  [5]:[0]:[0]:[24]:[104.104.104.0]:[0.0.0.0]:[17]
                      10.10.10.10          0        100       0    ?  10.10.10.10     MPLS

RD[10.10.10.10:333]
*>i  [5]:[0]:[0]:[24]:[99.99.99.0]:[0.0.0.0]:[19]
                      10.10.10.10          0        100       0    ?  10.10.10.10     MPLS

RD[10.10.10.10:334]
*>i  [5]:[0]:[0]:[24]:[99.99.100.0]:[0.0.0.0]:[18]
                      10.10.10.10          0        100       0    ?  10.10.10.10     MPLS

RD[10.10.10.10:500]
*>i  [3]:[500]:[32,10.10.10.10]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS

RD[22.22.22.22:123] VRF[vrf100_mgmt]:
*>   [2]:[0]:[123]:[48,0011:2233:4455]:[32,98.98.98.1]:[25618]
                      22.22.22.22          0        100       32768  i  ----------    MPLS
* i  [2]:[0]:[123]:[48,0011:2233:4567]:[32,99.99.99.1]:[28]
                      29.29.29.29          0        100       0    i  29.29.29.29     MPLS
* i                   10.10.10.10          0        100       0    i  10.10.10.10     MPLS
* i  [3]:[123]:[32,10.10.10.10]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>   [3]:[123]:[32,22.22.22.22]
                      22.22.22.22          0        100       32768  i  ----------    MPLS
* i  [3]:[123]:[32,29.29.29.29]
                      29.29.29.29          0        100       0    i  29.29.29.29     MPLS

RD[22.22.22.22:124] VRF[vrf200_mgmt]:
*>   [2]:[0]:[124]:[48,0011:2233:4455]:[32,98.98.99.1]:[25619]
                      22.22.22.22          0        100       32768  i  ----------    MPLS
* i  [2]:[0]:[124]:[48,0011:2233:4567]:[32,99.99.100.1]:[29]
                      29.29.29.29          0        100       0    i  29.29.29.29     MPLS
* i                   10.10.10.10          0        100       0    i  10.10.10.10     MPLS
* i  [3]:[124]:[32,10.10.10.10]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>   [3]:[124]:[32,22.22.22.22]
                      22.22.22.22          0        100       32768  i  ----------    MPLS
* i  [3]:[124]:[32,29.29.29.29]
                      29.29.29.29          0        100       0    i  29.29.29.29     MPLS

RD[22.22.22.22:125] VRF[vrf201_mgmt]:
*>   [2]:[0]:[125]:[48,0011:2233:4455]:[32,88.88.1.1]:[25629]
                      22.22.22.22          0        100       32768  i  ----------    MPLS
* i  [2]:[0]:[125]:[48,0011:2233:4567]:[32,88.88.3.1]:[37]
                      29.29.29.29          0        100       0    i  29.29.29.29     MPLS
* i                   10.10.10.10          0        100       0    i  10.10.10.10     MPLS
* i  [3]:[125]:[32,10.10.10.10]
```

```
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>   [3]:[125]:[32,22.22.22.22]
                      22.22.22.22          0        100       32768  i  ----------    MPLS
* i  [3]:[125]:[32,29.29.29.29]
                      29.29.29.29          0        100       0    i  29.29.29.29     MPLS

RD[22.22.22.22:126] VRF[vrf202_mgmt]:
* i  [3]:[126]:[32,10.10.10.10]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>   [3]:[126]:[32,22.22.22.22]
                      22.22.22.22          0        100       32768  i  ----------    MPLS
* i  [3]:[126]:[32,29.29.29.29]
                      29.29.29.29          0        100       0    i  29.29.29.29     MPLS

RD[22.22.22.22:200] VRF[blue]:
*>   [2]:[0]:[200]:[48,e49d:73b3:c101]:[32,70.70.1.1]:[25636]
                      22.22.22.22          0        100       32768  i  ----------    MPLS
*>   [3]:[200]:[32,22.22.22.22]
                      22.22.22.22          0        100       32768  i  ----------      MPLS

RD[22.22.22.22:205] VRF[vrf205_mgmt]:
*>   [2]:[0]:[127]:[48,0011:2233:4455]:[32,98.98.101.1]:[25608]
                      22.22.22.22          0        100       32768  i  ----------      MPLS
*>   [2]:[0]:[127]:[48,0011:2233:4455]:[32,104.104.103.1]:[25608]
                      22.22.22.22          0        100       32768  i  ----------      MPLS
* i  [2]:[0]:[127]:[48,0011:2233:4567]:[32,99.99.101.1]:[22]
                      29.29.29.29          0        100       0    i  29.29.29.29     MPLS
* i                   10.10.10.10          0        100       0    i  10.10.10.10     MPLS
* i  [2]:[0]:[127]:[48,0011:2233:4567]:[32,104.104.104.1]:[22]
                      29.29.29.29          0        100       0    i  29.29.29.29     MPLS
* i                   10.10.10.10          0        100       0    i  10.10.10.10     MPLS
* i  [2]:[0]:[127]:[48,0011:2233:4567]:[128,1000::1][22]
                      29.29.29.29          0        100       0    i  29.29.29.29     MPLS
* i                   10.10.10.10          0        100       0    i  10.10.10.10     MPLS
* i  [2]:[0]:[127]:[48,d077:ce2a:8001]:[32,103.103.103.1]:[26]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
* i  [2]:[0]:[127]:[48,d077:ce2a:8001]:[128,1100::1][26]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>   [2]:[0]:[127]:[48,e49d:73b3:c101]:[32,103.103.102.1]:[25608]
                      22.22.22.22          0        100       32768  i  ----------    MPLS
* i  [2]:[0]:[127]:[48,e8c5:7aff:96de]:[32,103.103.103.1]:[22]
                      29.29.29.29          0        100       0    i  29.29.29.29     MPLS
* i  [2]:[0]:[127]:[48,e8c5:7aff:96de]:[128,1100::1][22]
                      29.29.29.29          0        100       0    i  29.29.29.29     MPLS
* i  [3]:[127]:[32,10.10.10.10]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>   [3]:[127]:[32,22.22.22.22]
                      22.22.22.22          0        100       32768  i  ----------    MPLS
* i  [3]:[127]:[32,29.29.29.29]
                      29.29.29.29          0        100       0    i  29.29.29.29     MPLS

RD[22.22.22.22:500] VRF[ELAN_vrf500]:
* i  [3]:[500]:[32,10.10.10.10]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>   [3]:[500]:[32,22.22.22.22]
                      22.22.22.22          0        100       32768  i  ----------    MPLS
* i  [3]:[500]:[32,29.29.29.29]
                      29.29.29.29          0        100       0    i  29.29.29.29     MPLS

RD[22.22.22.22:501] VRF[ELAN_vrf501]:
*>   [3]:[501]:[32,22.22.22.22]
                      22.22.22.22          0        100       32768  i  ----------    MPLS
* i  [3]:[501]:[32,29.29.29.29]
                      29.29.29.29          0        100       0    i  29.29.29.29     MPLS

RD[22.22.22.22:502] VRF[ELAN_vrf502]:
*>   [3]:[502]:[32,22.22.22.22]
                      22.22.22.22          0        100       32768  i  ----------    MPLS
* i  [3]:[502]:[32,29.29.29.29]
                      29.29.29.29          0        100       0    i  29.29.29.29     MPLS

RD[22.22.22.22:503] VRF[ELAN_vrf503]:
*>   [3]:[503]:[32,22.22.22.22]
```

```
                      22.22.22.22          0        100       32768  i  ----------    MPLS
* i  [3]:[503]:[32,29.29.29.29]
                      29.29.29.29          0        100       0    i  29.29.29.29     MPLS

RD[22.22.22.22:504] VRF[ELAN_vrf504]:
*>   [3]:[504]:[32,22.22.22.22]
                      22.22.22.22          0        100       32768  i  ----------    MPLS
* i  [3]:[504]:[32,29.29.29.29]
                      29.29.29.29          0        100       0    i  29.29.29.29     MPLS

RD[22.22.22.22:505] VRF[ELAN_vrf505]:
*>   [3]:[505]:[32,22.22.22.22]
                      22.22.22.22          0        100       32768  i  ----------    MPLS
* i  [3]:[505]:[32,29.29.29.29]
                      29.29.29.29          0        100       0    i  29.29.29.29     MPLS

RD[22.22.22.22:506] VRF[ELAN_vrf506]:
*>   [3]:[506]:[32,22.22.22.22]
                      22.22.22.22          0        100       32768  i  ----------    MPLS
* i  [3]:[506]:[32,29.29.29.29]
                      29.29.29.29          0        100       0    i  29.29.29.29     MPLS

RD[22.22.22.22:507] VRF[ELAN_vrf507]:
*>   [3]:[507]:[32,22.22.22.22]
                      22.22.22.22          0        100       32768  i  ----------    MPLS
* i  [3]:[507]:[32,29.29.29.29]
                      29.29.29.29          0        100       0    i  29.29.29.29     MPLS

RD[22.22.22.22:508] VRF[ELAN_vrf508]:
*>   [3]:[508]:[32,22.22.22.22]
                      22.22.22.22          0        100       32768  i  ----------    MPLS
* i  [3]:[508]:[32,29.29.29.29]
                      29.29.29.29          0        100       0    i  29.29.29.29     MPLS

RD[22.22.22.22:509] VRF[ELAN_vrf509]:
*>   [3]:[509]:[32,22.22.22.22]
                      22.22.22.22          0        100       32768  i  ----------    MPLS
* i  [3]:[509]:[32,29.29.29.29]
                      29.29.29.29          0        100       0    i  29.29.29.29     MPLS

RD[22.22.22.22:510] VRF[ELAN_vrf510]:
*>   [3]:[510]:[32,22.22.22.22]
                      22.22.22.22          0        100       32768  i  ----------    MPLS
* i  [3]:[510]:[32,29.29.29.29]
                      29.29.29.29          0        100       0    i  29.29.29.29     MPLS

RD[22.22.22.22:600] VRF[eline600]:
*>   [1]:[0]:[600]:[25628]
                      22.22.22.22          0        100       32768  i  ----------    MPLS

RD[22.22.22.22:602] VRF[eline602]:
*>   [1]:[0]:[602]:[25635]
                      22.22.22.22          0        100       32768  i  ----------    MPLS

RD[22.22.22.22:604] VRF[eline604]:
*>   [1]:[0]:[604]:[25631]
                      22.22.22.22          0        100       32768  i  ----------    MPLS

RD[22.22.22.22:606] VRF[eline606]:
*>   [1]:[0]:[606]:[25634]
                      22.22.22.22          0        100       32768  i  ----------    MPLS

RD[22.22.22.22:608] VRF[eline608]:
*>   [1]:[0]:[608]:[25613]
                      22.22.22.22          0        100       32768  i  ----------    MPLS

RD[22.22.22.22:610] VRF[eline610]:
*>   [1]:[0]:[610]:[25626]
                      22.22.22.22          0        100       32768  i  ----------    MPLS

RD[22.22.22.22:612] VRF[eline612]:
*>   [1]:[0]:[612]:[25632]
                      22.22.22.22          0        100       32768  i  ----------    MPLS
```

```
RD[22.22.22.22:614] VRF[eline614]:
*>   [1]:[0]:[614]:[25625]
                     22.22.22.22          0        100       32768  i  ----------    MPLS

RD[22.22.22.22:616] VRF[eline616]:
*>   [1]:[0]:[616]:[25612]
                     22.22.22.22          0        100       32768  i  ----------    MPLS

RD[22.22.22.22:618] VRF[eline618]:
*>   [1]:[0]:[618]:[25617]
                     22.22.22.22          0        100       32768  i  ----------    MPLS

RD[22.22.22.22:620] VRF[eline620]:
*>   [1]:[0]:[620]:[25638]
                     22.22.22.22          0        100       32768  i  ----------    MPLS

RD[22.22.22.22:2002] VRF[vrf2002]:
*>   [1]:[0]:[2224]:[25630]
                     22.22.22.22          0        100       32768  i  ----------      MPLS

RD[22.22.22.22:2003] VRF[vrf2003]:
*>   [1]:[0]:[2226]:[25637]
                     22.22.22.22          0        100       32768  i  ----------      MPLS

RD[22.22.22.22:2004] VRF[vrf2004]:
*>   [1]:[0]:[2228]:[25633]
                     22.22.22.22          0        100       32768  i  ----------      MPLS

RD[22.22.22.22:2005] VRF[vrf2005]:
*>   [1]:[0]:[2300]:[25639]
                     22.22.22.22          0        100       32768  i  ----------      MPLS

RD[29.29.29.29:123]
*>i  [2]:[0]:[123]:[48,0011:2233:4567]:[32,99.99.99.1]:[28]
                     29.29.29.29          0        100       0    i  29.29.29.29     MPLS
*>i  [3]:[123]:[32,29.29.29.29]
                     29.29.29.29          0        100       0    i  29.29.29.29     MPLS

RD[29.29.29.29:124]
*>i  [2]:[0]:[124]:[48,0011:2233:4567]:[32,99.99.100.1]:[29]
                     29.29.29.29          0        100       0    i  29.29.29.29     MPLS
*>i  [3]:[124]:[32,29.29.29.29]
                     29.29.29.29          0        100       0    i  29.29.29.29     MPLS

RD[29.29.29.29:125]
*>i  [2]:[0]:[125]:[48,0011:2233:4567]:[32,88.88.3.1]:[37]
                     29.29.29.29          0        100       0    i  29.29.29.29     MPLS
*>i  [3]:[125]:[32,29.29.29.29]
                     29.29.29.29          0        100       0    i  29.29.29.29     MPLS

RD[29.29.29.29:126]
*>i  [3]:[126]:[32,29.29.29.29]
                     29.29.29.29          0        100       0    i  29.29.29.29     MPLS

RD[29.29.29.29:205]
*>i  [2]:[0]:[127]:[48,0011:2233:4567]:[32,99.99.101.1]:[22]
                     29.29.29.29          0        100       0    i  29.29.29.29     MPLS
*>i  [2]:[0]:[127]:[48,0011:2233:4567]:[32,104.104.104.1]:[22]
                     29.29.29.29          0        100       0    i  29.29.29.29     MPLS
*>i  [2]:[0]:[127]:[48,0011:2233:4567]:[128,1000::1][22]
                     29.29.29.29          0        100       0    i  29.29.29.29     MPLS
*>i  [2]:[0]:[127]:[48,e8c5:7aff:96de]:[32,103.103.103.1]:[22]
                     29.29.29.29          0        100       0    i  29.29.29.29     MPLS
*>i  [2]:[0]:[127]:[48,e8c5:7aff:96de]:[128,1100::1][22]
                     29.29.29.29          0        100       0    i  29.29.29.29     MPLS
*>i  [3]:[127]:[32,29.29.29.29]
                     29.29.29.29          0        100       0    i  29.29.29.29     MPLS

RD[29.29.29.29:305]
*>i  [5]:[0]:[0]:[24]:[99.99.101.0]:[0.0.0.0]:[18]
                     29.29.29.29          0        100       0    ?  29.29.29.29     MPLS
*>i  [5]:[0]:[0]:[24]:[103.103.103.0]:[0.0.0.0]:[18]
```

```
                     29.29.29.29          0       100       0    ?  29.29.29.29     MPLS
*>i  [5]:[0]:[0]:[24]:[104.104.104.0]:[0.0.0.0]:[18]
                     29.29.29.29          0       100       0    ?  29.29.29.29     MPLS

RD[29.29.29.29:333]
*>i  [5]:[0]:[0]:[24]:[99.99.99.0]:[0.0.0.0]:[20]
                     29.29.29.29          0       100       0    ?  29.29.29.29     MPLS

RD[29.29.29.29:334]
*>i  [5]:[0]:[0]:[24]:[99.99.100.0]:[0.0.0.0]:[19]
                     29.29.29.29          0       100       0    ?  29.29.29.29     MPLS

RD[29.29.29.29:500]
*>i  [3]:[500]:[32,29.29.29.29]
                     29.29.29.29          0       100       0    i  29.29.29.29     MPLS

RD[29.29.29.29:501]
*>i  [3]:[501]:[32,29.29.29.29]
                     29.29.29.29          0       100       0    i  29.29.29.29     MPLS

RD[29.29.29.29:502]
*>i  [3]:[502]:[32,29.29.29.29]
                     29.29.29.29          0       100       0    i  29.29.29.29     MPLS

RD[29.29.29.29:503]
*>i  [3]:[503]:[32,29.29.29.29]
                     29.29.29.29          0       100       0    i  29.29.29.29     MPLS

RD[29.29.29.29:504]
*>i  [3]:[504]:[32,29.29.29.29]
                     29.29.29.29          0       100       0    i  29.29.29.29     MPLS

RD[29.29.29.29:505]
*>i  [3]:[505]:[32,29.29.29.29]
                     29.29.29.29          0       100       0    i  29.29.29.29     MPLS

RD[29.29.29.29:506]
*>i  [3]:[506]:[32,29.29.29.29]
                     29.29.29.29          0       100       0    i  29.29.29.29     MPLS

RD[29.29.29.29:507]
*>i  [3]:[507]:[32,29.29.29.29]
                     29.29.29.29          0       100       0    i  29.29.29.29     MPLS

RD[29.29.29.29:508]
*>i  [3]:[508]:[32,29.29.29.29]
                     29.29.29.29          0       100       0    i  29.29.29.29     MPLS

RD[29.29.29.29:509]
*>i  [3]:[509]:[32,29.29.29.29]
                     29.29.29.29          0       100       0    i  29.29.29.29     MPLS

RD[29.29.29.29:510]
*>i  [3]:[510]:[32,29.29.29.29]
                     29.29.29.29          0       100       0    i  29.29.29.29     MPLS

Total number of prefixes 121
```

PE2 Verification:

```
#show bgp l2vpn evpn
BGP table version is 3, local router ID is 29.29.29.29
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

[EVPN route type]:[ESI]:[VNID]:[relevant route information]
```

```
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route
5 - Prefix Route

    Network          Next Hop            Metric    LocPrf       Weight     Path  Peer          Encap

RD[20:200]
*>i  [5]:[0]:[0]:[24]:[80.80.1.0]:[0.0.0.0]:[16]
                     10.10.10.10          0        100       0    ?  10.10.10.10     MPLS

RD[30:200]
*>i  [5]:[0]:[0]:[24]:[70.70.1.0]:[0.0.0.0]:[25600]
                     22.22.22.22          0        100       0    ?  22.22.22.22     MPLS

RD[10.10.10.10:123]
*>i  [2]:[0]:[123]:[48,0011:2233:4567]:[32,99.99.99.1]:[22]
                     10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>i  [3]:[123]:[32,10.10.10.10]
                     10.10.10.10          0        100       0    i  10.10.10.10     MPLS

RD[10.10.10.10:124]
*>i  [2]:[0]:[124]:[48,0011:2233:4567]:[32,99.99.100.1]:[24]
                     10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>i  [3]:[124]:[32,10.10.10.10]
                     10.10.10.10          0        100       0    i  10.10.10.10     MPLS

RD[10.10.10.10:125]
*>i  [2]:[0]:[125]:[48,0011:2233:4567]:[32,88.88.3.1]:[21]
                     10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>i  [3]:[125]:[32,10.10.10.10]
                     10.10.10.10          0        100       0    i  10.10.10.10     MPLS

RD[10.10.10.10:126]
*>i  [3]:[126]:[32,10.10.10.10]
                     10.10.10.10          0        100       0    i  10.10.10.10     MPLS

RD[10.10.10.10:200]
*>i  [2]:[0]:[100]:[48,d077:ce2a:8001]:[32,80.80.1.1]:[23]
                     10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>i  [3]:[100]:[32,10.10.10.10]
                     10.10.10.10          0        100       0    i  10.10.10.10     MPLS

RD[10.10.10.10:205]
*>i  [2]:[0]:[127]:[48,0011:2233:4567]:[32,99.99.101.1]:[26]
                     10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>i  [2]:[0]:[127]:[48,0011:2233:4567]:[32,104.104.104.1]:[26]
                     10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>i  [2]:[0]:[127]:[48,0011:2233:4567]:[128,1000::1][26]
                     10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>i  [2]:[0]:[127]:[48,d077:ce2a:8001]:[32,103.103.103.1]:[26]
                     10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>i  [2]:[0]:[127]:[48,d077:ce2a:8001]:[128,1100::1][26]
                     10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>i  [3]:[127]:[32,10.10.10.10]
                     10.10.10.10          0        100       0    i  10.10.10.10     MPLS

RD[10.10.10.10:305]
*>i  [5]:[0]:[0]:[24]:[99.99.101.0]:[0.0.0.0]:[17]
                     10.10.10.10          0        100       0    ?  10.10.10.10     MPLS
*>i  [5]:[0]:[0]:[24]:[103.103.103.0]:[0.0.0.0]:[17]
                     10.10.10.10          0        100       0    ?  10.10.10.10     MPLS
*>i  [5]:[0]:[0]:[24]:[104.104.104.0]:[0.0.0.0]:[17]
                     10.10.10.10          0        100       0    ?  10.10.10.10     MPLS

RD[10.10.10.10:333]
*>i  [5]:[0]:[0]:[24]:[99.99.99.0]:[0.0.0.0]:[19]
                     10.10.10.10          0        100       0    ?  10.10.10.10     MPLS
```

```
RD[10.10.10.10:334]
*>i  [5]:[0]:[0]:[24]:[99.99.100.0]:[0.0.0.0]:[18]
                     10.10.10.10          0        100       0    ?  10.10.10.10     MPLS

RD[10.10.10.10:500]
*>i  [3]:[500]:[32,10.10.10.10]
                     10.10.10.10          0        100       0    i  10.10.10.10     MPLS

RD[22.22.22.22:123]
*>i  [2]:[0]:[123]:[48,0011:2233:4455]:[32,98.98.98.1]:[25618]
                     22.22.22.22          0        100       0    i  22.22.22.22     MPLS
*>i  [3]:[123]:[32,22.22.22.22]
                     22.22.22.22          0        100       0    i  22.22.22.22     MPLS

RD[22.22.22.22:124]
*>i  [2]:[0]:[124]:[48,0011:2233:4455]:[32,98.98.99.1]:[25619]
                     22.22.22.22          0        100       0    i  22.22.22.22     MPLS
*>i  [3]:[124]:[32,22.22.22.22]
                     22.22.22.22          0        100       0    i  22.22.22.22     MPLS

RD[22.22.22.22:125]
*>i  [2]:[0]:[125]:[48,0011:2233:4455]:[32,88.88.1.1]:[25629]
                     22.22.22.22          0        100       0    i  22.22.22.22     MPLS
*>i  [3]:[125]:[32,22.22.22.22]
                     22.22.22.22          0        100       0    i  22.22.22.22     MPLS

RD[22.22.22.22:126]
*>i  [3]:[126]:[32,22.22.22.22]
                     22.22.22.22          0        100       0    i  22.22.22.22     MPLS

RD[22.22.22.22:205]
*>i  [2]:[0]:[127]:[48,0011:2233:4455]:[32,98.98.101.1]:[25608]
                     22.22.22.22          0        100       0    i  22.22.22.22     MPLS
*>i  [2]:[0]:[127]:[48,0011:2233:4455]:[32,104.104.103.1]:[25608]
                     22.22.22.22          0        100       0    i  22.22.22.22     MPLS
*>i  [2]:[0]:[127]:[48,e49d:73b3:c101]:[32,103.103.102.1]:[25608]
                     22.22.22.22          0        100       0    i  22.22.22.22     MPLS
*>i  [3]:[127]:[32,22.22.22.22]
                     22.22.22.22          0        100       0    i  22.22.22.22     MPLS

RD[22.22.22.22:305]
*>i  [5]:[0]:[0]:[24]:[98.98.101.0]:[0.0.0.0]:[25601]
                     22.22.22.22          0        100       0    ?  22.22.22.22     MPLS
*>i  [5]:[0]:[0]:[24]:[103.103.102.0]:[0.0.0.0]:[25601]
                     22.22.22.22          0        100       0    ?  22.22.22.22     MPLS
*>i  [5]:[0]:[0]:[24]:[104.104.103.0]:[0.0.0.0]:[25601]
                     22.22.22.22          0        100       0    ?  22.22.22.22     MPLS

RD[22.22.22.22:333]
*>i  [5]:[0]:[0]:[24]:[98.98.98.0]:[0.0.0.0]:[25606]
                     22.22.22.22          0        100       0    ?  22.22.22.22     MPLS

RD[22.22.22.22:334]
*>i  [5]:[0]:[0]:[24]:[98.98.99.0]:[0.0.0.0]:[25605]
                     22.22.22.22          0        100       0    ?  22.22.22.22     MPLS

RD[22.22.22.22:335]
*>i  [5]:[0]:[0]:[24]:[88.88.1.0]:[0.0.0.0]:[25604]
                     22.22.22.22          0        100       0    ?  22.22.22.22     MPLS

RD[22.22.22.22:500]
*>i  [3]:[500]:[32,22.22.22.22]
                     22.22.22.22          0        100       0    i  22.22.22.22     MPLS

RD[22.22.22.22:501]
*>i  [3]:[501]:[32,22.22.22.22]
                     22.22.22.22          0        100       0    i  22.22.22.22     MPLS

RD[22.22.22.22:502]
*>i  [3]:[502]:[32,22.22.22.22]
                     22.22.22.22          0        100       0    i  22.22.22.22     MPLS

RD[22.22.22.22:503]
```

```
*>i  [3]:[503]:[32,22.22.22.22]
                      22.22.22.22          0        100       0    i  22.22.22.22     MPLS

RD[22.22.22.22:504]
*>i  [3]:[504]:[32,22.22.22.22]
                      22.22.22.22          0        100       0    i  22.22.22.22     MPLS

RD[22.22.22.22:505]
*>i  [3]:[505]:[32,22.22.22.22]
                      22.22.22.22          0        100       0    i  22.22.22.22     MPLS

RD[22.22.22.22:506]
*>i  [3]:[506]:[32,22.22.22.22]
                      22.22.22.22          0        100       0    i  22.22.22.22     MPLS

RD[22.22.22.22:507]
*>i  [3]:[507]:[32,22.22.22.22]
                      22.22.22.22          0        100       0    i  22.22.22.22     MPLS

RD[22.22.22.22:508]
*>i  [3]:[508]:[32,22.22.22.22]
                      22.22.22.22          0        100       0    i  22.22.22.22     MPLS

RD[22.22.22.22:509]
*>i  [3]:[509]:[32,22.22.22.22]
                      22.22.22.22          0        100       0    i  22.22.22.22     MPLS

RD[22.22.22.22:510]
*>i  [3]:[510]:[32,22.22.22.22]
                      22.22.22.22          0        100       0    i  22.22.22.22     MPLS

RD[29.29.29.29:123] VRF[vrf100_mgmt]:
* i  [2]:[0]:[123]:[48,0011:2233:4455]:[32,98.98.98.1]:[25618]
                      22.22.22.22          0        100       0    i  22.22.22.22     MPLS
* i  [2]:[0]:[123]:[48,0011:2233:4567]:[32,99.99.99.1]:[22]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>                    29.29.29.29          0        100       32768  i  ----------    MPLS
* i  [3]:[123]:[32,10.10.10.10]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
* i  [3]:[123]:[32,22.22.22.22]
                      22.22.22.22          0        100       0    i  22.22.22.22     MPLS
*>   [3]:[123]:[32,29.29.29.29]
                      29.29.29.29          0        100       32768  i  ----------    MPLS

RD[29.29.29.29:124] VRF[vrf200_mgmt]:
* i  [2]:[0]:[124]:[48,0011:2233:4455]:[32,98.98.99.1]:[25619]
                      22.22.22.22          0        100       0    i  22.22.22.22     MPLS
* i  [2]:[0]:[124]:[48,0011:2233:4567]:[32,99.99.100.1]:[24]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>                    29.29.29.29          0        100       32768  i  ----------    MPLS
* i  [3]:[124]:[32,10.10.10.10]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
* i  [3]:[124]:[32,22.22.22.22]
                      22.22.22.22          0        100       0    i  22.22.22.22     MPLS
*>   [3]:[124]:[32,29.29.29.29]
                      29.29.29.29          0        100       32768  i  ----------    MPLS

RD[29.29.29.29:125] VRF[vrf201_mgmt]:
* i  [2]:[0]:[125]:[48,0011:2233:4455]:[32,88.88.1.1]:[25629]
                      22.22.22.22          0        100       0    i  22.22.22.22     MPLS
* i  [2]:[0]:[125]:[48,0011:2233:4567]:[32,88.88.3.1]:[21]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>                    29.29.29.29          0        100       32768  i  ----------    MPLS
* i  [3]:[125]:[32,10.10.10.10]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
* i  [3]:[125]:[32,22.22.22.22]
                      22.22.22.22          0        100       0    i  22.22.22.22     MPLS
*>   [3]:[125]:[32,29.29.29.29]
                      29.29.29.29          0        100       32768  i  ----------    MPLS

RD[29.29.29.29:126] VRF[vrf202_mgmt]:
* i  [3]:[126]:[32,10.10.10.10]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
```

```
* i  [3]:[126]:[32,22.22.22.22]
                      22.22.22.22          0        100       0    i  22.22.22.22     MPLS
*>   [3]:[126]:[32,29.29.29.29]
                      29.29.29.29          0        100       32768  i  ----------    MPLS

RD[29.29.29.29:200] VRF[blue]:
* i  [2]:[0]:[100]:[48,d077:ce2a:8001]:[32,80.80.1.1]:[23]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>   [2]:[0]:[100]:[48,e8c5:7aff:96de]:[32,80.80.1.1]:[38]
                      29.29.29.29          0        100       32768  i  ----------    MPLS
* i  [3]:[100]:[32,10.10.10.10]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>   [3]:[100]:[32,29.29.29.29]
                      29.29.29.29          0        100       32768  i  ----------    MPLS

RD[29.29.29.29:205] VRF[vrf205_mgmt]:
* i  [2]:[0]:[127]:[48,0011:2233:4455]:[32,98.98.101.1]:[25608]
                      22.22.22.22          0        100       0    i  22.22.22.22     MPLS
* i  [2]:[0]:[127]:[48,0011:2233:4455]:[32,104.104.103.1]:[25608]
                      22.22.22.22          0        100       0    i  22.22.22.22     MPLS
* i  [2]:[0]:[127]:[48,0011:2233:4567]:[32,99.99.101.1]:[26]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>                    29.29.29.29          0        100       32768  i  ----------    MPLS
* i  [2]:[0]:[127]:[48,0011:2233:4567]:[32,104.104.104.1]:[26]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>                    29.29.29.29          0        100       32768  i  ----------    MPLS
* i  [2]:[0]:[127]:[48,0011:2233:4567]:[128,1000::1][26]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>                    29.29.29.29          0        100       32768  i  ----------    MPLS
* i  [2]:[0]:[127]:[48,d077:ce2a:8001]:[32,103.103.103.1]:[26]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
* i  [2]:[0]:[127]:[48,d077:ce2a:8001]:[128,1100::1][26]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
* i  [2]:[0]:[127]:[48,e49d:73b3:c101]:[32,103.103.102.1]:[25608]
                      22.22.22.22          0        100       0    i  22.22.22.22     MPLS
*>   [2]:[0]:[127]:[48,e8c5:7aff:96de]:[32,103.103.103.1]:[22]
                      29.29.29.29          0        100       32768  i  ----------    MPLS
*>   [2]:[0]:[127]:[48,e8c5:7aff:96de]:[128,1100::1][22]
                      29.29.29.29          0        100       32768  i  ----------    MPLS
* i  [3]:[127]:[32,10.10.10.10]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
* i  [3]:[127]:[32,22.22.22.22]
                      22.22.22.22          0        100       0    i  22.22.22.22     MPLS
*>   [3]:[127]:[32,29.29.29.29]
                      29.29.29.29          0        100       32768  i  ----------    MPLS

RD[29.29.29.29:500] VRF[ELAN_vrf500]:
* i  [3]:[500]:[32,10.10.10.10]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
* i  [3]:[500]:[32,22.22.22.22]
                      22.22.22.22          0        100       0    i  22.22.22.22     MPLS
*>   [3]:[500]:[32,29.29.29.29]
                      29.29.29.29          0        100       32768  i  ----------    MPLS

RD[29.29.29.29:501] VRF[ELAN_vrf501]:
* i  [3]:[501]:[32,22.22.22.22]
                      22.22.22.22          0        100       0    i  22.22.22.22     MPLS
*>   [3]:[501]:[32,29.29.29.29]
                      29.29.29.29          0        100       32768  i  ----------    MPLS

RD[29.29.29.29:502] VRF[ELAN_vrf502]:
* i  [3]:[502]:[32,22.22.22.22]
                      22.22.22.22          0        100       0    i  22.22.22.22     MPLS
*>   [3]:[502]:[32,29.29.29.29]
                      29.29.29.29          0        100       32768  i  ----------    MPLS

RD[29.29.29.29:503] VRF[ELAN_vrf503]:
* i  [3]:[503]:[32,22.22.22.22]
                      22.22.22.22          0        100       0    i  22.22.22.22     MPLS
*>   [3]:[503]:[32,29.29.29.29]
                      29.29.29.29          0        100       32768  i  ----------    MPLS

RD[29.29.29.29:504] VRF[ELAN_vrf504]:
```

```
* i  [3]:[504]:[32,22.22.22.22]
                     22.22.22.22          0        100       0    i  22.22.22.22     MPLS
*>   [3]:[504]:[32,29.29.29.29]
                     29.29.29.29          0        100       32768  i  ----------    MPLS

RD[29.29.29.29:505] VRF[ELAN_vrf505]:
* i  [3]:[505]:[32,22.22.22.22]
                     22.22.22.22          0        100       0    i  22.22.22.22     MPLS
*>   [3]:[505]:[32,29.29.29.29]
                     29.29.29.29          0        100       32768  i  ----------    MPLS

RD[29.29.29.29:506] VRF[ELAN_vrf506]:
* i  [3]:[506]:[32,22.22.22.22]
                     22.22.22.22          0        100       0    i  22.22.22.22     MPLS
*>   [3]:[506]:[32,29.29.29.29]
                     29.29.29.29          0        100       32768  i  ----------    MPLS

RD[29.29.29.29:507] VRF[ELAN_vrf507]:
* i  [3]:[507]:[32,22.22.22.22]
                     22.22.22.22          0        100       0    i  22.22.22.22     MPLS
*>   [3]:[507]:[32,29.29.29.29]
                     29.29.29.29          0        100       32768  i  ----------    MPLS

RD[29.29.29.29:508] VRF[ELAN_vrf508]:
* i  [3]:[508]:[32,22.22.22.22]
                     22.22.22.22          0        100       0    i  22.22.22.22     MPLS
*>   [3]:[508]:[32,29.29.29.29]
                     29.29.29.29          0        100       32768  i  ----------    MPLS

RD[29.29.29.29:509] VRF[ELAN_vrf509]:
* i  [3]:[509]:[32,22.22.22.22]
                     22.22.22.22          0        100       0    i  22.22.22.22     MPLS
*>   [3]:[509]:[32,29.29.29.29]
                     29.29.29.29          0        100       32768  i  ----------    MPLS

RD[29.29.29.29:510] VRF[ELAN_vrf510]:
* i  [3]:[510]:[32,22.22.22.22]
                     22.22.22.22          0        100       0    i  22.22.22.22     MPLS
*>   [3]:[510]:[32,29.29.29.29]
                     29.29.29.29          0        100       32768  i  ----------    MPLS

RD[29.29.29.29:650] VRF[vrf650]:
*>   [3]:[650]:[32,29.29.29.29]
                     29.29.29.29          0        100       32768  i  ----------    MPLS

Total number of prefixes 110
```

Verify the specific type of EVPN routes using VRF:

PE1:

```
#show bgp l2vpn evpn vrf vrf205_mgmt
BGP table version is 1, local router ID is 22.22.22.22
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

[EVPN route type]:[ESI]:[VNID]:[relevant route information]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route
5 - Prefix Route
```

```
    Network          Next Hop            Metric    LocPrf       Weight     Path  Peer          Encap
*>   [2]:[0]:[127]:[48,0011:2233:4455]:[32,98.98.101.1]:[25608]
                      22.22.22.22          0        100       32768  i  ----------      MPLS
*>   [2]:[0]:[127]:[48,0011:2233:4455]:[32,104.104.103.1]:[25608]
                      22.22.22.22          0        100       32768  i  ----------      MPLS
* i  [2]:[0]:[127]:[48,0011:2233:4567]:[32,99.99.101.1]:[22]
                      29.29.29.29          0        100       0    i  29.29.29.29     MPLS
* i                   10.10.10.10          0        100       0    i  10.10.10.10     MPLS
* i  [2]:[0]:[127]:[48,0011:2233:4567]:[32,104.104.104.1]:[22]
                      29.29.29.29          0        100       0    i  29.29.29.29     MPLS
* i                   10.10.10.10          0        100       0    i  10.10.10.10     MPLS
* i  [2]:[0]:[127]:[48,0011:2233:4567]:[128,1000::1][22]
                      29.29.29.29          0        100       0    i  29.29.29.29     MPLS
* i                   10.10.10.10          0        100       0    i  10.10.10.10     MPLS
* i  [2]:[0]:[127]:[48,d077:ce2a:8001]:[32,103.103.103.1]:[26]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
* i  [2]:[0]:[127]:[48,d077:ce2a:8001]:[128,1100::1][26]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>   [2]:[0]:[127]:[48,e49d:73b3:c101]:[32,103.103.102.1]:[25608]
                      22.22.22.22          0        100       32768  i  ----------      MPLS
* i  [2]:[0]:[127]:[48,e8c5:7aff:96de]:[32,103.103.103.1]:[22]
                      29.29.29.29          0        100       0    i  29.29.29.29     MPLS
* i  [2]:[0]:[127]:[48,e8c5:7aff:96de]:[128,1100::1][22]
                      29.29.29.29          0        100       0    i  29.29.29.29     MPLS
* i  [3]:[127]:[32,10.10.10.10]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>   [3]:[127]:[32,22.22.22.22]
                      22.22.22.22          0        100       32768  i  ----------      MPLS
* i  [3]:[127]:[32,29.29.29.29]
                      29.29.29.29          0        100       0    i  29.29.29.29     MPLS

Total number of prefixes 13
```

PE2:

```
#show bgp l2vpn evpn vrf vrf205_mgmt
BGP table version is 1, local router ID is 29.29.29.29
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

[EVPN route type]:[ESI]:[VNID]:[relevant route information]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route
5 - Prefix Route

    Network          Next Hop            Metric    LocPrf       Weight     Path  Peer          Encap
* i  [2]:[0]:[127]:[48,0011:2233:4455]:[32,98.98.101.1]:[25608]
                      22.22.22.22          0        100       0    i  22.22.22.22     MPLS
* i  [2]:[0]:[127]:[48,0011:2233:4455]:[32,104.104.103.1]:[25608]
                      22.22.22.22          0        100       0    i  22.22.22.22     MPLS
* i  [2]:[0]:[127]:[48,0011:2233:4567]:[32,99.99.101.1]:[26]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>                    29.29.29.29          0        100       32768  i  ----------      MPLS
* i  [2]:[0]:[127]:[48,0011:2233:4567]:[32,104.104.104.1]:[26]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>                    29.29.29.29          0        100       32768  i  ----------      MPLS
* i  [2]:[0]:[127]:[48,0011:2233:4567]:[128,1000::1][26]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>                    29.29.29.29          0        100       32768  i  ----------      MPLS
* i  [2]:[0]:[127]:[48,d077:ce2a:8001]:[32,103.103.103.1]:[26]
                      10.10.10.10          0        100       0    i  10.10.10.10     MPLS
```

```
* i  [2]:[0]:[127]:[48,d077:ce2a:8001]:[128,1100::1][26]
                     10.10.10.10          0        100       0    i  10.10.10.10     MPLS
* i  [2]:[0]:[127]:[48,e49d:73b3:c101]:[32,103.103.102.1]:[25608]
                     22.22.22.22          0        100       0    i  22.22.22.22     MPLS
*>   [2]:[0]:[127]:[48,e8c5:7aff:96de]:[32,103.103.103.1]:[22]
                     29.29.29.29          0        100       32768  i  ----------      MPLS
*>   [2]:[0]:[127]:[48,e8c5:7aff:96de]:[128,1100::1][22]
                     29.29.29.29          0        100       32768  i  ----------      MPLS
* i  [3]:[127]:[32,10.10.10.10]
                     10.10.10.10          0        100       0    i  10.10.10.10     MPLS
* i  [3]:[127]:[32,22.22.22.22]
                     22.22.22.22          0        100       0    i  22.22.22.22     MPLS
*>   [3]:[127]:[32,29.29.29.29]
                     29.29.29.29          0        100       32768  i  ----------      MPLS

Total number of prefixes 13
```

Verify the specific type of EVPN routes using RD:

PE1:

```
#show bgp l2vpn evpn rd 22.22.22.22:205
BGP table version is 2, local router ID is 22.22.22.22
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

[EVPN route type]:[ESI]:[VNID]:[relevant route information]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route
5 - Prefix Route

    Network          Next Hop            Metric    LocPrf       Weight     Path  Peer          Encap

RD[22.22.22.22:205] VRF[vrf205_mgmt]:
*>   [2]:[0]:[127]:[48,0011:2233:4455]:[32,98.98.101.1]:[25608]
                     22.22.22.22          0        100       32768  i  ----------      MPLS
*>   [2]:[0]:[127]:[48,0011:2233:4455]:[32,104.104.103.1]:[25608]
                     22.22.22.22          0        100       32768  i  ----------      MPLS
* i  [2]:[0]:[127]:[48,0011:2233:4567]:[32,99.99.101.1]:[22]
                     29.29.29.29          0        100       0    i  29.29.29.29     MPLS
* i                  10.10.10.10          0        100       0    i  10.10.10.10     MPLS
* i  [2]:[0]:[127]:[48,0011:2233:4567]:[32,104.104.104.1]:[22]
                     29.29.29.29          0        100       0    i  29.29.29.29     MPLS
* i                  10.10.10.10          0        100       0    i  10.10.10.10     MPLS
* i  [2]:[0]:[127]:[48,0011:2233:4567]:[128,1000::1][22]
                     29.29.29.29          0        100       0    i  29.29.29.29     MPLS
* i                  10.10.10.10          0        100       0    i  10.10.10.10     MPLS
* i  [2]:[0]:[127]:[48,d077:ce2a:8001]:[32,103.103.103.1]:[26]
                     10.10.10.10          0        100       0    i  10.10.10.10     MPLS
* i  [2]:[0]:[127]:[48,d077:ce2a:8001]:[128,1100::1][26]
                     10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>   [2]:[0]:[127]:[48,e49d:73b3:c101]:[32,103.103.102.1]:[25608]
                     22.22.22.22          0        100       32768  i  ----------      MPLS
* i  [2]:[0]:[127]:[48,e8c5:7aff:96de]:[32,103.103.103.1]:[22]
                     29.29.29.29          0        100       0    i  29.29.29.29     MPLS
* i  [2]:[0]:[127]:[48,e8c5:7aff:96de]:[128,1100::1][22]
                     29.29.29.29          0        100       0    i  29.29.29.29     MPLS
* i  [3]:[127]:[32,10.10.10.10]
                     10.10.10.10          0        100       0    i  10.10.10.10     MPLS
*>   [3]:[127]:[32,22.22.22.22]
                     22.22.22.22          0        100       32768  i  ----------      MPLS
* i  [3]:[127]:[32,29.29.29.29]
```

```
                    29.29.29.29         0       100      0    i  29.29.29.29     MPLS

Total number of prefixes 13
```

PE2:

```
#show bgp l2vpn evpn rd 29.29.29.29:205
BGP table version is 3, local router ID is 29.29.29.29
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

[EVPN route type]:[ESI]:[VNID]:[relevant route information]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route
5 - Prefix Route

    Network          Next Hop            Metric    LocPrf       Weight     Path  Peer          Encap

RD[29.29.29.29:205] VRF[vrf205_mgmt]:
* i  [2]:[0]:[127]:[48,0011:2233:4455]:[32,98.98.101.1]:[25608]
                     22.22.22.22          0       100      0    i  22.22.22.22     MPLS
* i  [2]:[0]:[127]:[48,0011:2233:4455]:[32,104.104.103.1]:[25608]
                     22.22.22.22          0       100      0    i  22.22.22.22     MPLS
* i  [2]:[0]:[127]:[48,0011:2233:4567]:[32,99.99.101.1]:[26]
                     10.10.10.10          0       100      0    i  10.10.10.10     MPLS
*>                   29.29.29.29          0       100      32768  i  ----------      MPLS
* i  [2]:[0]:[127]:[48,0011:2233:4567]:[32,104.104.104.1]:[26]
                     10.10.10.10          0       100      0    i  10.10.10.10     MPLS
*>                   29.29.29.29          0       100      32768  i  ----------      MPLS
* i  [2]:[0]:[127]:[48,0011:2233:4567]:[128,1000::1][26]
                     10.10.10.10          0       100      0    i  10.10.10.10     MPLS
*>                   29.29.29.29          0       100      32768  i  ----------      MPLS
* i  [2]:[0]:[127]:[48,d077:ce2a:8001]:[32,103.103.103.1]:[26]
                     10.10.10.10          0       100      0    i  10.10.10.10     MPLS
* i  [2]:[0]:[127]:[48,d077:ce2a:8001]:[128,1100::1][26]
                     10.10.10.10          0       100      0    i  10.10.10.10     MPLS
* i  [2]:[0]:[127]:[48,e49d:73b3:c101]:[32,103.103.102.1]:[25608]
                     22.22.22.22          0       100      0    i  22.22.22.22     MPLS
*>   [2]:[0]:[127]:[48,e8c5:7aff:96de]:[32,103.103.103.1]:[22]
                     29.29.29.29          0       100      32768  i  ----------      MPLS
*>   [2]:[0]:[127]:[48,e8c5:7aff:96de]:[128,1100::1][22]
                     29.29.29.29          0       100      32768  i  ----------      MPLS
* i  [3]:[127]:[32,10.10.10.10]
                     10.10.10.10          0       100      0    i  10.10.10.10     MPLS
* i  [3]:[127]:[32,22.22.22.22]
                     22.22.22.22          0       100      0    i  22.22.22.22     MPLS
*>   [3]:[127]:[32,29.29.29.29]
                     29.29.29.29          0       100      32768  i  ----------      MPLS

Total number of prefixes 13
```

Verify the specific type of EVPN routes using Prefix:

PE1:

```
#show bgp l2vpn evpn prefix [3]:[127]:[32,29.29.29.29]
BGP table version is 2, local router ID is 22.22.22.22
```

```
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

[EVPN route type]:[ESI]:[VNID]:[relevant route information]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route
5 - Prefix Route

    Network          Next Hop            Metric    LocPrf       Weight     Path  Peer          Encap

RD[22.22.22.22:205] VRF[vrf205_mgmt]:
* i  [3]:[127]:[32,29.29.29.29]
                     29.29.29.29          0        100       0    i  29.29.29.29     MPLS

RD[29.29.29.29:205]
*>i  [3]:[127]:[32,29.29.29.29]
                     29.29.29.29          0        100       0    i  29.29.29.29     MPLS

Total number of prefixes 2
```

PE2:

```
#show bgp l2vpn evpn prefix [3]:[127]:[32,22.22.22.22]
BGP table version is 3, local router ID is 29.29.29.29
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

[EVPN route type]:[ESI]:[VNID]:[relevant route information]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route
5 - Prefix Route

    Network          Next Hop            Metric    LocPrf       Weight     Path  Peer          Encap

RD[22.22.22.22:205]
*>i  [3]:[127]:[32,22.22.22.22]
                     22.22.22.22          0        100       0    i  22.22.22.22     MPLS

RD[29.29.29.29:205] VRF[vrf205_mgmt]:
* i  [3]:[127]:[32,22.22.22.22]
                     22.22.22.22          0        100       0    i  22.22.22.22     MPLS

Total number of prefixes 2
```

Verify the specific type of EVPN routes using both VRF and Prefix:

PE1:

```
#show bgp l2vpn evpn vrf vrf205_mgmt  prefix [3]:[127]:[32,29.29.29.29]
BGP table version is 1, local router ID is 22.22.22.22
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

[EVPN route type]:[ESI]:[VNID]:[relevant route information]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route
5 - Prefix Route

    Network                    Next Hop           Metric    LocPrf    Weight     Path   Peer           Encap
* i  [3]:[127]:[32,29.29.29.29]  29.29.29.29         0       100       0            i    29.29.29.29    MPLS

Total number of prefixes 1
```

PE2:

```
#show bgp l2vpn evpn vrf vrf205_mgmt  prefix [3]:[127]:[32,22.22.22.22]
BGP table version is 1, local router ID is 29.29.29.29
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

[EVPN route type]:[ESI]:[VNID]:[relevant route information]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route
5 - Prefix Route

    Network                    Next Hop           Metric    LocPrf       Weight     Path   Peer           Encap
* i  [3]:[127]:[32,22.22.22.22]  22.22.22.22         0         100          0          i     22.22.22.22    MPLS

Total number of prefixes 1
```

Verify detailed information of EVPN routes:

PE1:

```
#show bgp l2vpn evpn vrf vrf205_mgmt  prefix [3]:[127]:[32,29.29.29.29] detail

BGP route entry for prefix : [3]:[127]:[32,29.29.29.29]
 Route-Distinguisher: [29.29.29.29:205]
 Flags : Valid, IBGP
 Nexthop : 29.29.29.29  MED value : 0
 Community:
```

```
 Extended Community: RT:65535:1073741951  Encapsulation:MPLS
 Weight :0,  Local Preference :100
 AS Path : Local
 Origin : IGP
 Last Update : Mon Oct  9 10:14:47 2023
 Peer : 29.29.29.29

Total number of prefixes 1
```

PE2:

```
#show bgp l2vpn evpn vrf vrf205_mgmt  prefix [3]:[127]:[32,22.22.22.22] detail

BGP route entry for prefix : [3]:[127]:[32,22.22.22.22]
 Route-Distinguisher: [22.22.22.22:205]
 Flags : Valid, IBGP
 Nexthop : 22.22.22.22  MED value : 0
 Community:
 Extended Community: RT:65535:1073741951  Encapsulation:MPLS
 Weight :0,  Local Preference :100
 AS Path : Local
 Origin : IGP
 Last Update : Mon Apr 15 07:05:47 2019
 Peer : 22.22.22.22
```

Abbreviations

Acronym	Description
VNID	L2 Virtual Network Identifier
VRF	Virtual Routing and Forwarding
EVPN-IRB	Ethernet VPN Integrated Routing and Bridging
MAC	Media Access Control address

Improved Management

This section describes the network monitoring enhancements and new features introduced in the Release 6.4.1 and Release 6.4.2.

Release 6.4.2

- PTP SMPTE Profile Support
- Streaming Telemetry - Supported Datamodel and Sensor Paths

Release 6.4.1

- Streaming Telemetry
- CFM over EVPN-MPLS for ELINE MultiHoming
- Route MonitorDHCP Server Group
- DHCP Server Group

PTP SMPTE Profile Support

Overview

The IEEE 1588 v2 Precision Time Protocol (PTP) functionality is enhanced to support the Society of Motion Picture and Television Engineers (SMPTE) 2059-2 in OcNOS 6.4.2.

The PTP is a protocol used to synchronize timing among the systems connected in computer networks; it is similar to Network Time Protocol (NTP), which does not have the capability to measure in nanoseconds. The timing capability to measure less than a microsecond is critical while broadcasting multimedia data such as audio, video, etc. The PTP is essential in scenarios where very accurate timing is required.

Currently, the PTP implementation is supported with the following profiles:

- ITU-T G.8275.1
- G.8275.2,
- G.8265.1
- Boundary Clock
- Interworking function (IWF)
- Synchronous Ethernet
- End-to-End (E2E) telecom profile for time/phase synchronization

For more information on existing PTP profiles support refer to *Timing and Synchronization Guide*.

Feature Characteristics

This section describes the PTP SMPTE 2059-2 time and frequency synchronization profile functionalities.

In a computer network, a system installed with a PTP module is called a Grand Master Clock, which performs the timing and synchronization with the other connected systems, called a Slave Clock. The PTP modules can include many timing profiles according to the functionality requirements.

The SMPTE PTP profile is based on IEEE Standard 1588-2008 and includes a description of parameters, their default values, and permitted ranges. This standard specifies a PTP for synchronizing audio/video equipment in a professional broadcast environment.

The SMPTE ST 2059-2 profile defines a point in time, the SMPTE Epoch, which is used for the alignment of real-time signals; formulae that specify the ongoing alignment of signals to time since the SMPTE Epoch; and formulae that specify the calculation of SMPTE ST 12-1 time address values and SMPTE ST 309 date values.

The SMPTE enhanced profile includes the following functionality:

- Implements appropriate algorithm to compare clocks and determines the best clock to use as a source clock
- Implements appropriate configuration management options
- Implements the appropriate path delay mechanisms, delay request-response or peer delay
- Defines the range and default values of all PTP configurable attributes and data set members.
- Defines the transport mechanisms as required, permitted, or prohibited.
- Defines the node types as required, permitted, or prohibited.

Limitations:

- The SMPTE timing profile is supported only on UFI-QUX and UFI-Q2 platforms.
- The new CLI `Priority1` command is supported only on Default and SMPTE profiles

Benefits

The SMPTE PTP Profile is used for time and frequency synchronization in a professional multimedia broadcast environment. It provides the following benefits:

- To permit clocks to be synchronized quickly and accurately to enable professional media over IP applications.
- To convey Synchronization Metadata (SM) required for synchronization and time labeling of audio/video signals.

Prerequisites

The PTP process should be up and running.

Configuration

This chapter shows how to configure a PTP SMPTE profile over IPv4 and IPv6. You can configure T-GM and boundary clock with more than one port.S

Note: The SMPTE profile can be enabled on L2/L3 physical interfaces, Sub interfaces, LAG interfaces and VLAN interfaces.

Topology

Describe the topology

SMPTE PTP Configuration Toplogy

In this example, SW1, SW2 and SW3 are running PTP. SW1 acting as T-GM, SW2 as a boundary clock and SW3 as a slave clock.

SW1 Telecom Grandmaster (T-GM)

Perform the following configurations to set T-GM clock.

`#configure terminal`	Enter Configure mode
`(config)#synce`	Enter configure Synchronous Ethernet mode.
`(config-synce)#synchronization option 1`	Set the synchronization network type.
`(config-synce)#exit`	Exit Synce mode.

(config)#synce-interface gps	Configure synce interface GPS.
(config-synce-if)#mode synchronous	Configure synchronous mode.
(config-synce-if)#input-source 1	Configure the interface as an input source with priority 1.
(config-synce-if)#quality-level QL_PRC	Configure QL-value.
(config-synce-if)#wait-to-restore 1	Configure Wait-to-Restore timer.
(config-synce-if)#exit	Exit Port Configure mode.
(config)#interface eth1	Configure interface eth2.
(config-if)#ip address 192.168.4.101/24	Configure the IP address of the interface.
(config-if)#exit	Exit interface mode.
(config)#ptp clock 0 profile smpte	Enables smpte PTP profile.
(config)# sm-tlv default-frame-rate 4294967295 4294967294	Enables sm tlv colour frame rate value.
(config)# sm-tlv time-address-flags color-frame	Enables sm-tlv time flag as color frame.
(config)# sm-tlv time-address-flags drop-frame	Enables sm-tlv time flag as drop frame.
(config-ptp-clk)#clock-type tgm	Enables clock type as T-GM.
(config-ptp-clk)#number-ports 2	Configure the number of PTP ports on the instance.
(config-ptp-clk)#clock-port 2	Configure PTP port.
(config-clk-port)#transport ipv4-multicast	Set the transport type as IPv4 multicast.
(config-clk-port)#network-interface eth1	Configure underlying interface that is used by this PTP Port.
(config-clk-port)#exit	Exit PTP clock port mode.
(config-ptp-clk)#clock-port 1	Configure PTP port.
(config-clk-port)#network-interface gps	Configure underlying interface that is used by this PTP Port.
(config-clk-port)#exit	Exit PTP clock port mode.

SW2 Boundary Clock (BC)

Perform the following configuration to set Boundary clock. It can function as both Grand Master and Slave to another PTP clock.

#configure terminal	Enter Configure mode.
(config)#interface eth1	Configure interface eth1.
(config-if)#ip address 192.168.4.100/24	Configure the IP address of the interface.
(config)#interface eth2	Configure interface eth1.
(config-if)#ip address 192.168.5.100/24	Configure the IP address of the interface.
(config)#ptp clock 0 profile smpte	Enables SMPTE for PTP time/phase telecom profile.
(config-ptp-clk)#number-ports 2	Configure the number of PTP ports on the instance.
(config-ptp-clk)#clock-port 1	Configure PTP port.
(config-clk-port)#transport ipv4-multicast	Set transport type IPv4 as multicast.

(config-clk-port)#network-interface eth1	Configure underlying interface that is used by this PTP Port.
(config-ptp-clk)#clock-port 2	Configure PTP port.
(config-clk-port)#transport ipv4-multicast	Set transport type IPv4 as multicast.
(config-clk-port)#network-interface eth2	Configure underlying interface that is used by this PTP Port.
(config-clk-port)#exit	Exit PTP clock port mode.

SW3 Slave Clock (SC)

Perform the following configuration to set Slave clock.

#configure terminal	Enter Configure mode.
(config)#interface eth2	Configure interface eth2.
(config-if)#ip address 192.168.5.101/24	Configure the IP address of the interface.
(config-if)#exit	Exit interface mode.
(config)#ptp clock 0 profile smpte	Enables SMPTE PTP profile.
(config-ptp-clk)#number-ports 2	Configure the number of PTP ports on the instance.
(config-ptp-clk)#slave-only	Configure the device as a Slave clock.
(config-ptp-clk)#clock-port 1	Configure PTP port.
(config-clk-port)#transport ipv4-multicast	Set transport type IPv4 as multicast.
(config-clk-port)#network-interface eth2	Configure underlying interface that is used by this PTP Port.
(config-clk-port)#exit	Exit PTP clock port mode.

Validation

SW2(BC)

```
#show ptp clock 0
PTP Clock Profile             : smpte
Default Dataset:
  Two Step Flag               : No
  Clock Identity              : 5C:07:58:FF:FE:54:12:02
  Number Of Ports             : 2
  Priority1                   : 128
  Priority2                   : 128
  Slave Only                  : No
  Local Priority              : 128
  Max Steps Removed           : 255
  Domain Number               : 127
  Clock Quality               :
    Clock Class               : 248
    Clock Accuracy            : 254
    Offset ScaledLogVariance  : 65535

Current Dataset:
```

```
  Steps Removed               : 1
  Offset From Master          : -5318 nsec
  Mean Path Delay             : 89 nsec

Parent Dataset:
  Parent Port ID              :
    Clock Identity            : 5C:07:58:FF:FE:51:13:09
    Port Number               : 2
  Parent Stats                : No
  Observed Parent O.S.L.V     : 65535 (Offset Scaled Log Variance)
  Observed Parent P.C.R.      : 2147483647 (Phase Change Rate)
  Grandmaster Identity        : 5C:07:58:FF:FE:51:13:09
  Grandmaster Priority1       : 128
  Grandmaster Priority2       : 128
  Grandmaster Clock Quality   :
    Clock Class               : 248
    Clock Accuracy            : 32
    Offset ScaledLogVariance  : 20061

Time Dateset:
  Current UTC Offset Valid    : True
  Current UTC Offset          : 37
  Leap 59                     : False
  Leap 61                     : False
  Time Traceable              : True
  Frequency Traceable         : True
  PTP Timescale               : True
  Time Source                 : Global positioning system
  Time of Day                 : Fri 10 Nov 2023 07:52:31 UTC
```

2. show ptp clock 0 port 1

```
Port 1:
  Port State                  : Slave
  Port Identity               : 5C:07:58:FF:FE:54:12:02:00:01
  Peer Mean Path Delay        : 89
  Log Announce Interval       : 0
  Log Min Delay Req Interval  : -3
  Log Sync Interval           : -3
  Announce Receipt Timeout    : 3
  Delay Mechanism             : End to end
  Version Number              : 2
  Local Priority              : 128
  Master only                 : False
  Signal Fail                 : False
  Network Interface           : cd20/1
  Vlan Configured             :
  Description                 :
  TTL                         : 64
  DSCP                        : 56
  Unicast Grant Duration      : 300
```

```
  Configured delay asymmetry  : 0 nsec

  Number of Foreign Masters   : 1
  Current Foreign Master      : 0

  Foreign Master #0
  IPv4 Address                : 192.168.4.100
  Grandmaster clockIdentity   : 5C:07:58:FF:FE:51:13:09
  Port ID                     : 5C:07:58:FF:FE:51:13:09:00:02
  clockClass                  : 6
  Clock accuracy              : 32
  Offset scaled log variance  : 20061
  priority1                   : 128
  priority2                   : 128
  Steps removed               : 1

  Received Packets            : 20087
  Discarded Packets           : 74
  Transmitted Packets         : 8929

  Peer #0
  IPv4 Address                : 192.168.4.100
  Clock Identity              : 5c:07:58:ff:fe:51:13:09
  Received Announce           : 1115
  Received Sync               : 8926
  Received Delay Request      : 41
  Received Delay Response     : 8894
  Received Management         : 1111
  Transmitted Announce        : 4
  Transmitted Sync            : 28
  Transmitted Delay Request   : 8894
  Transmitted Management      : 3

  SMPTE Sync Metadata:
  Default frame rate          : 0xfffffffffffffffe
  GM Lock Status              : 4
  Time Address Flags          : 0x03
  Current Local Offset        : -37
  Jump Seconds                : 0
  Time of Next Jump           : 0x000000000000
  Time of Next Jam            : 0x000000000000
  Time of Previous Jam        : 0x000000000000
  Previous Jam Local Offset   : 0
  Daylight Saving             : 0x00
  Leap Second Jump            : 0x00

  Master #0                   : 192.168.4.100
```

3. show ptp servo

```
PTP servo status for clock 0
```

```
  Servo Config                : Freq + Phase Correction
  Servo State                 : Time Locked
  Servo State Duration        : 00:00:28
  Servo APTS Mode             : N/A
  Frequency Correction        : 24.887 ppb
  Phase Correction            : -370500000.000 nsec
  Offset From Master          : -317 nsec
  Mean Path Delay             : 89 nsec
  APTS GPS to PTP Offset      : N/A
  Sync Packet Rate            : 8
  Delay Packet Rate           : 8
```

SW3(Slave clock)

1.show ptp clock 0

```
PTP Clock Profile             : smpte
Default Dataset:
  Two Step Flag               : No
  Clock Identity              : E8:C5:7A:FF:FE:DA:68:CF
  Number Of Ports             : 1
  Priority1                   : 128
  Priority2                   : 255
  Slave Only                  : Yes
  Local Priority              : 128
  Max Steps Removed           : 255
  Domain Number               : 127
  Clock Quality               :
    Clock Class               : 255
    Clock Accuracy            : 254
    Offset ScaledLogVariance  : 65535

Current Dataset:
  Steps Removed               : 0
  Offset From Master          : 0 nsec
  Mean Path Delay             : 0 nsec

Parent Dataset:
  Parent Port ID              :
    Clock Identity            : E8:C5:7A:FF:FE:DA:68:CF
    Port Number               : 0
  Parent Stats                : No
  Observed Parent O.S.L.V     : 65535 (Offset Scaled Log Variance)
  Observed Parent P.C.R.      : 2147483647 (Phase Change Rate)
  Grandmaster Identity        : E8:C5:7A:FF:FE:DA:68:CF
  Grandmaster Priority1       : 128
  Grandmaster Priority2       : 255
  Grandmaster Clock Quality   :
    Clock Class               : 255
    Clock Accuracy            : 254
```

```
    Offset ScaledLogVariance  : 65535

Time Dateset:
  Current UTC Offset Valid    : True
  Current UTC Offset          : 37
  Leap 59                     : False
  Leap 61                     : False
  Time Traceable              : False
  Frequency Traceable         : False
  PTP Timescale               : True
  Time Source                 : Internal Oscillator
  Time of Day                 : Thu 01 Jan 1970 00:05:58 UTC
```

2.show ptp clock 0 port 1

```
Port 1:
  Port State                  : Slave
  Port Identity               : E8:C5:7A:FF:FE:DA:68:CF:00:01
  Peer Mean Path Delay        : 2974
  Log Announce Interval       : 0
  Log Min Delay Req Interval  : -3
  Log Sync Interval           : -3
  Announce Receipt Timeout    : 3
  Delay Mechanism             : End to end
  Version Number              : 2
  Local Priority              : 128
  Master only                 : False
  Signal Fail                 : False
  Network Interface           : ce2
  Vlan Configured             :
  Description                 :
  TTL                         : 64
  DSCP                        : 56
  Unicast Grant Duration      : 300
  Configured delay asymmetry  : 0 nsec

  Number of Foreign Masters   : 1
  Current Foreign Master      : 0

  Foreign Master #0
  IPv4 Address                : 192.168.4.100
  Grandmaster clockIdentity   : 5C:07:58:FF:FE:51:13:09
  Port ID                     : 5C:07:58:FF:FE:51:13:09:00:02
  clockClass                  : 6
  Clock accuracy              : 32
  Offset scaled log variance  : 20061
  priority1                   : 128
  priority2                   : 128
  Steps removed               : 1

  Received Packets            : 210
```

```
  Discarded Packets           : 33
  Transmitted Packets         : 82

  Peer #0
  IPv4 Address                : 192.168.4.100
  Clock Identity              : 5c:07:58:ff:fe:51:13:09
  Received Announce           : 15
  Received Sync               : 114
  Received Delay Response     : 82
  Transmitted Delay Request   : 82

  Master #0                   : 192.168.4.100
```

3. show ptp servo

```
PTP servo status for clock 0
  Servo Config                : Freq + Phase Correction
  Servo State                 : Time Locked
  Servo State Duration        : 00:01:09
  Servo APTS Mode             : N/A
  Frequency Correction        : -11.610 ppb
  Phase Correction            : -86000000.000 nsec
  Offset From Master          : -4 nsec
  Mean Path Delay             : -52 nsec
  APTS GPS to PTP Offset      : N/A
  Sync Packet Rate            : 8
  Delay Packet Rate           : 8
```

SW1(T-GM)

1. show ptp servo

```
PTP servo status for clock 0
  Servo Config                : Freq + Phase Correction
  Servo State                 : Time Locked
  Servo State Duration        : 00:11:16
  Servo APTS Mode             : GPS
  Frequency Correction        : -234.160 ppb
  Phase Correction            : 0.000 nsec
  Offset From Master          : 0 nsec
  Mean Path Delay             : 0 nsec
  APTS GPS to PTP Offset      : N/A
  Sync Packet Rate            : 8
  Delay Packet Rate           : 8
```

2. show ptp clock 0

```
PTP Clock Profile             : smpte
Default Dataset:
  Two Step Flag               : No
  Clock Identity              : 5C:07:58:FF:FE:51:13:09
```

```
  Number Of Ports             : 2
  Priority1                   : 128
  Priority2                   : 128
  Slave Only                  : No
  Local Priority              : 128
  Max Steps Removed           : 255
  Domain Number               : 127
  Clock Quality               :
    Clock Class               : 248
    Clock Accuracy            : 254
    Offset ScaledLogVariance  : 65535

Current Dataset:
  Steps Removed               : 0
  Offset From Master          : 0 nsec
  Mean Path Delay             : 0 nsec

Parent Dataset:
  Parent Port ID              :
    Clock Identity            : 5C:07:58:FF:FE:51:13:09
    Port Number               : 0
  Parent Stats                : No
  Observed Parent O.S.L.V     : 65535 (Offset Scaled Log Variance)
  Observed Parent P.C.R.      : 2147483647 (Phase Change Rate)
  Grandmaster Identity        : 5C:07:58:FF:FE:51:13:09
  Grandmaster Priority1       : 128
  Grandmaster Priority2       : 128
  Grandmaster Clock Quality   :
    Clock Class               : 6
    Clock Accuracy            : 32
    Offset ScaledLogVariance  : 20061

Time Dateset:
  Current UTC Offset Valid    : True
  Current UTC Offset          : 37
  Leap 59                     : False
  Leap 61                     : False
  Time Traceable              : True
  Frequency Traceable         : True
  PTP Timescale               : True
  Time Source                 : Global positioning system
  Time of Day                 : Fri 10 Nov 2023 04:33:40 UTC
```

3.show ptp clock 0 port 1

```
Port 1:
  Port State                  : Slave
  Port Identity               : 5C:07:58:FF:FE:51:13:09:00:01
  Peer Mean Path Delay        : 0
  Log Announce Interval       : 0
  Log Min Delay Req Interval  : -3
```

```
Log Sync Interval           : -3
Announce Receipt Timeout    : 3
Delay Mechanism             : Disabled
Version Number              : 2
Local Priority              : 0
Master only                 : False
Signal Fail                 : False
Network Interface           : gps
Vlan Configured             :
Description                 :
TTL                         : 64
DSCP                        : 56
Unicast Grant Duration      : 300
Configured delay asymmetry  : 0 nsec

Received Packets            : 0
Discarded Packets           : 0
Transmitted Packets         : 0
```

Note: Use `show ptp stats` to collect the PTP statistics and use `clear ptp stats` to clear the same.

Implementation Examples

Gather typical use cases for this feature. Your information must include the following:

- Where a customer will enable or disable this feature.
- Cover how the new feature works with other existing features?

Note: Work with SE's and TAC to request and understand customer use cases.

New CLI Commands

Following are the new CLIs introduced in this feature.

- sm-tlv time-address-flags color-frame
- sm-tlv time-address-flags drop-frame
- sm-tlv default-frame-rates
- sm-tlv append disable
- sm-tlv process disable
- transport ipv6-multicast type

sm-tlv time-address-flags color-frame

Use this command to set sm-tlv color frame. Applicable only for smpte profile.

Use the `no` form of this command to unconfigure sm-tlv color-frame.

Command Syntax

```
sm-tlv time-address-flags color-frame
```

```
no sm-tlv time-address-flags color-frame
```

Parameters

None

Default

None

Command Mode

PTP Clock mode

Applicability

This command was introduced in the OcNOS version 6.4.2.

Example

Following is an example to execute the CLI.

```
OcNOS(config)#ptp clock 0 profile smpte
OcNOS(config-ptp-clk)#sm-tlv time-address-flags color-frame

OcNOS(config)#ptp clock 0 profile smpte
OcNOS(config-ptp-clk)#no sm-tlv time-address-flags color-frame
```

sm-tlv time-address-flags drop-frame

Use this command to set sm-tlv drop frame. Applicable only for SMPTE profile.

Use the `no` form of this command to unconfigure sm-tlv drop-frame.

Command Syntax

```
sm-tlv time-address-flags drop-frame
no sm-tlv time-address-flags drop-frame
```

Parameters

None

Default

None

Command Mode

PTP Clock mode

Applicability

This command was introduced in the OcNOS version 6.4.2.

Example

Following is an example to execute the CLI.

```
OcNOS(config)#ptp clock 0 profile smpte
OcNOS(config-ptp-clk)#sm-tlv time-address-flags drop-frame

OcNOS(config)#ptp clock 0 profile smpte
OcNOS(config-ptp-clk)#no sm-tlv time-address-flags drop-frame
```

sm-tlv default-frame-rates

Use this command to set the default frame rate. Applicable only for SMPTE profile.For example, if the video default frame rate is 30000/1001 Hz, set first argument to numerator value (i.e 30000) and second argument to denominator value (i.e 1001).

Use the `no` form of this command to unconfigure default frame rates.

Command Syntax

```
sm-tlv default-frame-rates <numerator> <denominator>
no sm-tlv default-frame-rates
```

Parameters

`Numerator`	Setting numerator for the default system frame rate
`Denominator`	Setting denominator for the default system frame rate

Default

None

Command Mode

PTP Clock mode

Applicability

This command was introduced in the OcNOS version 6.4.2.

Example

Following is an example to execute the CLI.

```
OcNOS(config)#ptp clock 0 profile smpte
OcNOS(config-ptp-clk)# sm-tlv default-frame-rate 30000 1001

OcNOS(config)#ptp clock 0 profile smpte
OcNOS(config-ptp-clk)# no sm-tlv default-frame-rate
```

sm-tlv append disable

Use this command to disable tlv append. Applicable only for SMPTE profile.

Use the `no` form of this command to unconfigure sm-tlv append disable.

Command Syntax

```
sm-tlv append disable
```

```
[no]sm-tlv append disable
```

Parameters

None

Default

The sm-tlv append is enabled.

Command Mode

PTP Clock Port mode

Applicability

This command was introduced in the OcNOS version 6.4.2.

Example

Following is an example to execute the CLI.

```
OcNOS(config)#ptp clock 0 profile smpte
OcNOS(config-ptp-clk)#clock-port 1
OcNOS(config-clk-port)#sm-tlv append disable
OcNOS(config)#ptp clock 0 profile smpte
OcNOS(config-ptp-clk)#clock-port 1
OcNOS(config-clk-port)#no sm-tlv append disable
```

sm-tlv process disable

Use this command to disable tlv processing. Applicable only for smpte profile.

Use the `no` form of this command to unconfigure sm-tlv process disable.

Command Syntax

```
sm-tlv process disable
```

```
no sm-tlv process disable
```

Parameters

None

Default

The sm-tlv process is enabled.

Command Mode

PTP Clock Port mode

Applicability

This command was introduced in the OcNOS version 6.4.2.

Example

Following is an example to execute the CLI.

```
OcNOS(config)#ptp clock 0 profile smpte
OcNOS(config-ptp-clk)#clock-port 1
OcNOS(config-clk-port)#sm-tlv process disable

OcNOS(config)#ptp clock 0 profile smpte
OcNOS(config-ptp-clk)#clock-port 1
OcNOS(config-clk-port)#no sm-tlv process disable
```

transport ipv6-multicast type

Use this command to set transport type as ipv6 multicast and we can specify the multicast address type. Applicable for G.8275.2 profile, G 8265.1, SMPTE profile and default profile.

Use the `no` form of this command to unconfigure transport-type.

Command Syntax

```
transport ipv6-multicast type (site-local|interface-local|link-local|admin-
  local|organization-local|global-local)
no transport ipv6-multicast type
```

Parameters

`Site-local` - ff05::181

`interface-local` - ff01::181

`link-local` - ff02::181

`admin-local` - ff04::181

`organization-local` - ff08::181

`global-local` - ff0e::181

Default

None

Command Mode

PTP Clock Port mode

Applicability

This command was introduced in the OcNOS version 6.4.2.

Example

Explain or describe the example.

```
OcNOS(config)#ptp clock 0 profile smpte
OcNOS(config-ptp-clk)#clock-port 1
OcNOS(config-clk-port)#transport ipv6-multicast type admin-local

OcNOS(config)#ptp clock 0 profile smpte
OcNOS(config-ptp-clk)#clock-port 1
OcNOS(config-clk-port)#transport ipv6-multicast type global-local
```

```
OcNOS(config)#ptp clock 0 profile smpte
OcNOS(config-ptp-clk)#clock-port 1
OcNOS(config-clk-port)#no transport ipv6-multicast type
```

Revised CLI Commands

The following existing CLIs are applicable for SMPT profile.

- announce-receipt-timeout
- dscp
- log-announce-interval
- log-min-delay-req-interval
- log-sync-interval
- master
- source-address linklocal
- source-address interface
- ttl
- unicast-grant-duration

For more information about the CLIs, refer to the *PTP Timing and Synchronization Guide*, Release 6.4.2.

The following existing CLIs are updated for SMPT profile.

- ptp clock profile

ptp clock profile

Use this command to enter PTP Clock Mode and to configure the G 8275.1, G 8275.2, Default, SMPTE and G 8265.1 profiles.

Use the `no` form of this command to delete PTP clock.

Note: For a single clock configuration, only clock 0 should be configured. Clock 1 is used only for the IWF use case.

Command Syntax

```
ptp clock <0-1> profile (g8275.1|g8275.2|default|g8265.1|smpte)
no ptp clock <0-1> profile
```

Parameters

`<0-1>`	Clock 0 or 1
`g8275.1`	PTP time/phase g8275.1 telecom profile
`g8275.2`	PTP time/phase g8275.2 telecom profile
`default`	PTP time/phase default profile
`g8265.1`	PTP frequency telecom profile
`smpte`	PTP SMPTE profile

Default

None

Command Mode

Configure Mode

Applicability

This command was introduced in the OcNOS version 6.4.2.

Example

Explain or describe the example.

```
(config)#ptp clock 0 profile g8275.1
(config-ptp-clk)exit
(config)#ptp clock 0 profile g8275.2
(config-ptp-clk)exit
(config)#ptp clock 0 profile default
(config-ptp-clk)exit
(config)#ptp clock 0 profile g8265.1
(config-ptp-clk)exit
(config)#ptp clock 0 profile smpte
(config-ptp-clk)exit
```

Abbreviations

The following are some key abbreviations and their meanings relevant to this document:

Acronym	Description
OC	Ordinary Clock
BC	Boundary Clock
SMPTE	The Society of Motion Picture and Television Engineers
TC	Transparent Clock
T-GM	Telecom Grandmaster
T-TSC	Telecom Time Slave Clock

Glossary

The following provides definitions for key terms used throughout this document.

SMPTE	The SMPTE ST 2059-2 profile defines a point in time, the SMPTE Epoch, which is used for alignment of real-time signals; formulae which specify the ongoing alignment of signals to time since the SMPTE Epoch; and formulae which specify the calculation of SMPTE ST 12-1 time address values and SMPTE ST 309 date values.
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.

Streaming Telemetry

Overview

Streaming telemetry allows users to monitor network health by efficiently streaming operational data of interest from OcNOS routers. This structured data is transmitted to remote management systems for proactive network monitoring and understanding CPU and memory usage in managed devices for troubleshooting.

A machine learning (ML) database can be created with telemetry data to establish a baseline for normal network operation and predict or mitigate network issues.

Feature Characteristics

OcNOS version 6.4.1 introduces the initial features for Streaming Telemetry, which include support for gNMI-based Dial-in mode Telemetry for the management plane. The initial feature list includes support for the "**STREAM**" type and "**SAMPLING**" mode subscription for the Subscribe Remote Procedure Call (RPC). The gNMI-based collector connects to the OcNOS target device and invokes the Subscribe RPC, specifying the set of path(s) of interest. Below are the two key components involved:

- **gNMI Server (OcNOS Target):** The gNMI server operates within the OcNOS device, serving as the source of telemetry data. It supports the gNMI protocol, allowing gNMI-based clients (collectors) to request and receive streaming data. The server streams the requested data to the client according to the specified parameters.
- **gNMI Client (Collector):** The gNMI client, also known as the collector, runs outside the OcNOS target device and is responsible for receiving and gathering telemetry data. In this context, it is the entity that connects to the OcNOS target device to collect data using the gNMI protocol. The collector initiates the Subscribe RPC to specify the data of interest.

Figure 3 illustrates the gNMI client's (Collector) Subscribe request and response (RPC) interaction with the gNMI server (OcNOS Target).

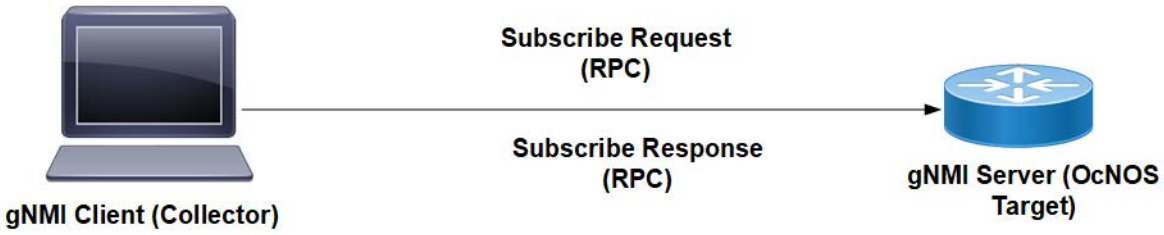


Figure 3: Sample Subscribe Request

Dial-in Mode: Dial-in mode is the method used to establish a telemetry connection where the collector initiates the connection to the server. In this mode, the collector sends a Subscribe RPC request to the target device, and the server running on the target device streams the data to the collector.

Example Message Flow: Subscribe Request and Response

Figure 4 illustrates a sample gnmic Subscribe Request and Subscribe Response between the collector and the OcNOS target device.

Step 1: Subscription Request Initiation

- The gnmic collector server initiates a Subscribe Request by sending a Subscribe RPC in Stream type.
- This subscription request aims explicitly to gather data related to interface state counters and CPU state.
- A fixed 30/45-second sampling interval is set for data collection.

Step 2: Data Collection and Processing

- The gNMI server, within the OcNOS router, is responsible for data collection.
- At regular 30/45-second intervals, it retrieves data from the sensor path, focusing on interface state counters and CPU State.
- The received data undergoes a validation process, and the data is transformed into the required encoding type.

Step 3: Continuous Subscription Response Streaming

- The gNMI Server responds to the subscription request by continuously streaming Subscribe Response data.
- This streaming process maintains the same 30/45-second interval as the data collection.
- The collected data is streamed in real-time to the gnmic collector server.

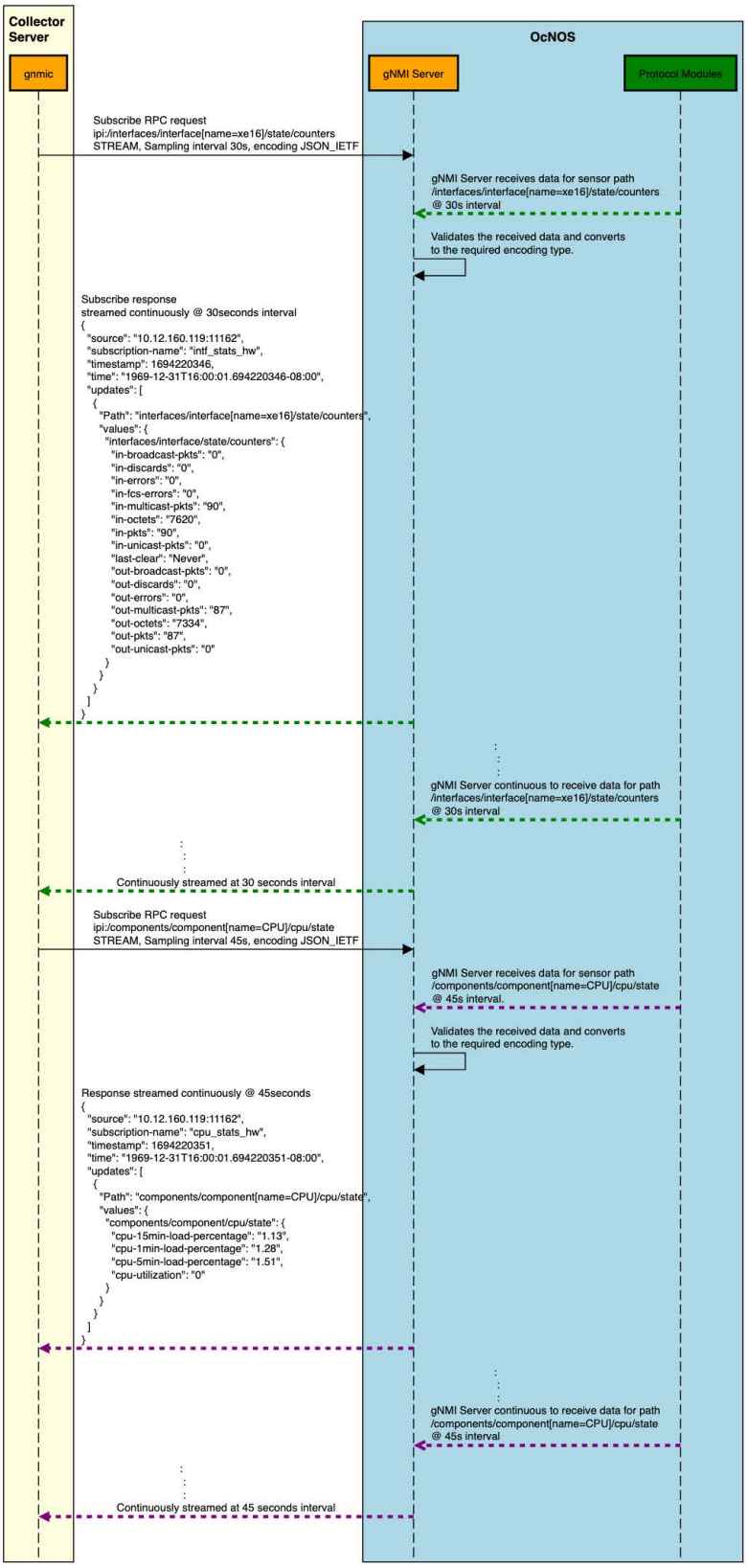


Figure 4: Message Flow: Subscribe Request and Response

Scale and Minimum Sample Interval Supported

To limit the impact of telemetry on critical features of the OcNOS target device, certain limits have been implemented. In Stream mode, there is a maximum limit of 100 sensor paths that can be subscribed to at any given point in time. Additionally, the minimum supported sample interval is 10 seconds.

Scale Scenarios

1. **New Subscribe RPC Request Makes Total Paths To Not Exceed 100:** When these new paths are added to the existing paths already handled by gNMI server, the total number does not exceed the maximum limit of 100 paths. Consequently, the gNMI server accepts this subscribe request and proceeds with the processing.
2. **New Subscribe RPC Request Makes Total Paths To Reach 100:** With the new Subscribe RPC Request, the total paths handled would be exactly equal to 100. The gNMI server accepts the new subscribe request; however, a warning is logged by the gNMI server, indicating that the maximum number of paths has been reached, and it signifies that no new Subscribe RPC Stream mode requests will be handled until the number of currently handled paths drops below 100.
3. **New Subscribe RPC Request Makes Total Paths To Exceed 100:** With the new Subscribe RPC Request, the total paths handled exceed 100. The gNMI server returns an error. The RPC request is not closed but will be accepted and responded to when the total number of paths handled drops to a level that can accommodate this RPC request.

Minimum Sample Interval: The minimum supported sample interval is 10 seconds. Any sampling mode request with a sample interval of less than 10 seconds will result in an error. However, if a sample interval is 0, it defaults to the minimum sample interval supported by the gNMI server, which is 10 seconds.

Benefits

Proactive Network Monitoring: Obtain real-time insights into network health and performance, and how to enable quicker response to issues.

Resource Utilization Monitoring: Monitor CPU and memory utilization to optimize resource allocation and performance.

Predictive Troubleshooting: Identify patterns and potential issues before they impact the network, reducing downtime.

Automation and Resilience: Use telemetry data to automate network management tasks and design a more resilient network.

Prerequisites

Before configuring Streaming Telemetry, ensure that:

- A supported OcNOS router running a compatible release.
- Access to the management interface of the router.
- Any gNMI client that complies with gNMI specifications can be used as a client.

Configuration

In this example, streaming telemetry with OcNOS is demonstrated, using '`gnmic`' as the gNMI Client.

gNMI Specification can be found at: https://github.com/openconfig/reference/blob/master/rpc/gnmi/gnmi-specification.md

The '`gnmic`' tool is available at: https://github.com/openconfig/gnmic

Figure 5: Streaming Telemetry Topology

gnmic installation

To install gnmic, use the following command:

```
bash -c "$(curl -sL https://get-gnmic.openconfig.net)"
```

To enable streaming telemetry on OcNOS:

```
OcNOS#configure terminal
OcNOS(config)#feature streaming-telemetry
OcNOS(config)#commit
```

Telemetry Subscription Request via gnmic Command and YAML Input

Use the gnmic command with a YAML file input to request telemetry subscriptions with multiple paths.

```
gnmic -a <ipaddress:port> -u <UserName> -p <Password> --insecure  --config <path to
  config file> subscribe
```

This command establishes a telemetry subscription with the specified paths defined in the YAML file.

Telemetry Subscription Request via gnmic Command with a Single Path Option

Use the gnmic command with a single path option to request a telemetry subscription for a specific data path.

```
gnmic -a  <ipaddress:port> -u <UserName> -p <Password> --encoding json_ietf --
  insecure --mode STREAM --stream-mode sample --sample-interval sample-interval-
  value sub --path <path>
```

This command creates a telemetry subscription for the specified path with the chosen sample interval and encoding format.

Supported gnmic Options

The below table explains the option fields.

gnmic Options details

Option	Description
--encoding	Specifies the encoding format (`JSON_IETF`).
--mode	Sets the mode of operation (`STREAM`).
--insecure	Allows insecure connections.
--stream-mode	Sets the stream mode (`Sample`).
--sample-interval	Sets the sample interval (`10s`). Note: Interval should be 10s or more.
--config	Specifies the YAML configuration file path (Example: `input_path.yaml`).
--path	Sets the path to subscribe to specific data (Example: `'ipi:/interfaces/interface[name=ce51]/state'`). Note: For multiple paths specify each path with --path option.
--prefix	Defines a common prefix for all specified paths (Example: `'ipi:/interfaces'`).

Invoking Subscribe RPC with gnmic

Use Case 1: Monitoring Interface State with Single Path Option

In this use case, gnmic subscribes to a specific path using the Subscribe RPC, monitoring the state of an interface with the path `'ipi:/interfaces/interface[name=ce51]/state'`.

```
#gnmic -a 10.12.91.111:11162 -u ocnos -p ocnos --encoding json_ietf --insecure
--mode STREAM --stream-mode sample --sample-interval 10s sub --path 'ipi:/
interfaces/interface[name=ce51]/state'

{
  "source": "10.12.91.111:11162",
  "subscription-name": "default-1695368813",
  "timestamp": 1551956933,
  "time": "1970-01-01T05:30:01.551956933+05:30",
  "updates": [
    {
      "Path": "ipi:interfaces/interface[name=ce51]/state",
      "values": {
        "interfaces/interface/state": {
          "admin-status": "up",
          "counters": {
            "in-broadcast-pkts": "0",
            "in-discards": "0",
            "in-errors": "0",
            "in-fcs-errors": "0",
            "in-multicast-pkts": "23",
            "in-octets": "2126",
            "in-pkts": "23",
            "in-unicast-pkts": "0",
            "last-clear": "Never",
            "out-broadcast-pkts": "0",
```

```
                "out-discards": "0",
                "out-errors": "0",
                "out-multicast-pkts": "28",
                "out-octets": "2552",
                "out-pkts": "28",
                "out-unicast-pkts": "0"
              },
              "ifindex": 10051,
              "last-change": 15500,
              "logical": false,
              "oper-status": "up"
            }
          }
        }
      ]
    }
```


The output of the Subscribe RPC includes the following information:

Subscribe RPC Output details

Option	Description
source	The source IP address and port of the gNMI server.
subscription-name	The name of the subscription.
timestamp	The timestamp of the response.
time	The timestamp in a human-readable format.
updates	An array of updates, each containing Path and Values.
Path	The path to the subscribed data.
values	The values of the subscribed data.

Validation

The below show command provides details about the subscriptions that have been established, including the client ID, sampling interval, encoding type, and the sensor paths that are being monitored.

```
OcNOS#show streaming-telemetry dynamic-subscriptions

 Feature streaming telemetry : Enabled

 SI:  Sampling Interval in seconds

 Enc-Type: Encoding type

 Dial-In Subscription Details:

 ClientIP:Port               ID     SI    Enc-Type       Origin:Path

 -------------            ------   ----   --------       ------------

 10.12.43.165:59304        4148   10     JSON_IETF       ipi:interfaces/interface[name=ce51]/state/counters

                                                          ipi:interfaces/interface[name=ce51]/state
```

Use Case 2: Monitoring Interface State with Multiple Path Option

In this use case, gnmic subscribes to a specific path using the Subscribe RPC, monitoring the state of an interface with the multiple path `'ipi:/interfaces/interface[name=ce51]/state'` and `'ipi:/interfaces/interface[name=ce52]/state'`.

```
#gnmic -a  10.12.91.111:11162 -u ocnos -p ocnos --encoding json_ietf  --
insecure   --mode STREAM --stream-mode sample --sample-interval 11s sub --path
'ipi:/interfaces/interface[name=ce51]/state' --path 'ipi:/interfaces/
interface[name=ce52]/state'
```


```
{
  "source": "10.12.91.111:11162",
  "subscription-name": "default-1695377304",
  "timestamp": 1551965423,
  "time": "1970-01-01T05:30:01.551965423+05:30",
  "updates": [
    {
      "Path": "ipi:interfaces/interface[name=ce51]/state",
      "values": {
        "interfaces/interface/state": {
          "admin-status": "up",
          "counters": {
            "in-broadcast-pkts": "0",
            "in-discards": "0",
            "in-errors": "0",
            "in-fcs-errors": "0",
            "in-multicast-pkts": "10",
            "in-octets": "1060",
            "in-pkts": "10",
            "in-unicast-pkts": "0",
            "last-clear": "Never",
            "out-broadcast-pkts": "0",
            "out-discards": "0",
            "out-errors": "0",
            "out-multicast-pkts": "10",
            "out-octets": "1020",
            "out-pkts": "10",
            "out-unicast-pkts": "0"
          },
          "ifindex": 10051,
          "last-change": 22500,
          "logical": false,
          "oper-status": "up"
        }
      }
    }
  ]
}

{
  "source": "10.12.91.111:11162",
  "subscription-name": "default-1695377304",
  "timestamp": 1551965423,
  "time": "1970-01-01T05:30:01.551965423+05:30",
  "updates": [
    {
      "Path": "ipi:interfaces/interface[name=ce52]/state",
```

```
          "values": {
            "interfaces/interface/state": {
              "admin-status": "up",
              "counters": {
                "in-broadcast-pkts": "0",
                "in-discards": "0",
                "in-errors": "0",
                "in-fcs-errors": "0",
                "in-multicast-pkts": "13",
                "in-octets": "1664",
                "in-pkts": "13",
                "in-unicast-pkts": "0",
                "last-clear": "Never",
                "out-broadcast-pkts": "0",
                "out-discards": "0",
                "out-errors": "0",
                "out-multicast-pkts": "10",
                "out-octets": "1020",
                "out-pkts": "10",
                "out-unicast-pkts": "0"
              },
              "ifindex": 10052,
              "last-change": 22500,
              "logical": false,
              "oper-status": "up"
            }
          }
        }
      ]
    }
```


Validation

The below show command provides details about the subscriptions that have been established, including the client ID, sampling interval, encoding type, and the sensor paths that are being monitored.

```
OcNOS#show streaming-telemetry dynamic-subscriptions

 Feature streaming telemetry : Enabled

 SI:  Sampling Interval in seconds

 Enc-Type: Encoding type

 Dial-In Subscription Details:

 ClientIP:Port               ID     SI    Enc-Type       Origin:Path

 -------------            ------   ----   --------       ------------

 10.12.43.145:59334        42000   11     JSON_IETF      ipi:interfaces/interface[name=ce52]/state/counters
                                                         ipi:interfaces/interface[name=ce52]/state
                                                         ipi:interfaces/interface[name=ce51]/state/counters
                                                         ipi:interfaces/interface[name=ce51]/state
```

YAML File Input for Multiple Path Subscription

Use Case 1: Configuring One Subscription Requests with Multiple Path Option

This use case illustrates the configuration of a subscription request with multiple paths using a YAML file input. It streamlines the subscription setup process by specifying the desired paths and subscription parameters directly in the YAML file.

YAML File Content (**single_request.yaml**)

```
#cat single_request.yaml


 subscriptions:                      #Container for subscriptions

   interface_stats_hw:               #A named subscription, where the key is the subscription name

     paths:                          #List of subscription paths for the named subscription
 - "ipi:/interfaces/
 interface[name=xe1]/state"

 - "ipi:/interfaces/
 interface[name=vlan1.10]/
 state"


     stream-mode: sample             #One of [on-change, target-defined, sample]

     sample-interval: 12s            #Sampling interval (e.g., 12 seconds)

     encoding: json_ietf             #Encoding format for telemetry data (e.g., JSON_IETF)
```

gnmic Command

```
# gnmic -a  10.12.91.111:11162 -u ocnos -p ocnos  --insecure  --config
single_request.yaml subscribe

{
  "source": "10.12.91.111:11162",
  "subscription-name": "interface_stats_hw",
  "timestamp": 1551965792,
  "time": "1970-01-01T05:30:01.551965792+05:30",
  "updates": [
    {
      "Path": "ipi:interfaces/interface[name=xe1]/state",
      "values": {
        "interfaces/interface/state": {
          "admin-status": "up",
          "counters": {
            "in-broadcast-pkts": "0",
            "in-discards": "0",
            "in-errors": "0",
            "in-fcs-errors": "0",
            "in-multicast-pkts": "0",
            "in-octets": "0",
            "in-pkts": "0",
            "in-unicast-pkts": "0",
            "last-clear": "Never",
            "out-broadcast-pkts": "0",
            "out-discards": "0",
```

```
            "out-errors": "0",
            "out-multicast-pkts": "2",
            "out-octets": "164",
            "out-pkts": "2",
            "out-unicast-pkts": "0"
          },
          "ifindex": 10001,
          "last-change": 0,
          "logical": false,
          "oper-status": "down"
        }
      }
    }
  ]
}

{
  "source": "10.12.91.111:11162",
  "subscription-name": "interface_stats_hw",
  "timestamp": 1551965792,
  "time": "1970-01-01T05:30:01.551965792+05:30",
  "updates": [
    {
      "Path": "ipi:interfaces/interface[name=vlan1.10]/state",
      "values": {
        "interfaces/interface/state": {
          "admin-status": "up",
          "counters": {
            "in-broadcast-pkts": "0",
            "in-discards": "0",
            "in-errors": "0",
            "in-fcs-errors": "0",
            "in-multicast-pkts": "0",
            "in-octets": "0",
            "in-pkts": "0",
            "in-unicast-pkts": "0",
            "last-clear": "Never",
            "out-broadcast-pkts": "0",
            "out-discards": "0",
            "out-errors": "0",
            "out-multicast-pkts": "0",
            "out-octets": "0",
            "out-pkts": "0",
            "out-unicast-pkts": "0"
          },
          "ifindex": 25010,
          "last-change": 22500,
          "logical": false,
          "oper-status": "up"
        }
      }
    }
  ]
}
```

Validation

The below show command provides details about the subscriptions that have been established, including the client ID, sampling interval, encoding type, and the sensor paths that are being monitored.

```
OcNOS#show streaming-telemetry dynamic-subscriptions

 Feature streaming telemetry : Enabled

 SI:  Sampling Interval in seconds

 Enc-Type: Encoding type

 Dial-In Subscription Details:

 ClientIP:Port              ID     SI    Enc-Type       Origin:Path

 -------------            ------   ----   --------       ------------

 10.12.43.135:58208        45333   12     JSON_IETF      ipi:interfaces/interface[name=xe1]/state/counters
                                                         ipi:interfaces/interface[name=xe1]/state
                                                         ipi:interfaces/interface[name=vlan1.10]/state/counters
                                                         ipi:interfaces/interface[name=vlan1.10]/state
```

Use Case 2: Configuring Multiple Subscription Requests with Multiple Path Option

This use case illustrates the configuration of multiple subscription request with multiple paths using a YAML file input. It streamlines the subscription setup process by specifying the desired paths and subscription parameters directly in the YAML file.

YAML File Content (**multiple_subs.yaml**)

```
#cat multiple_subs.yaml


 subscriptions:                    # Container for subscriptions
   RAM_stats_hw:                   # A named subscription for RAM statistics
     paths:                        # List of subscription paths for the RAM_stats_hw subscription
- "ipi:/components/
component[name=RAM]/ram/state"
     stream-mode: sample           # Stream mode for RAM statistics
     sample-interval: 11s          # Sampling interval for RAM statistics (e.g., 11 seconds)
     encoding: json_ietf           # Encoding format for RAM statistics (e.g., JSON_IETF)


   storage_stats_hw:               # A named subscription for storage statistics
     paths:                        # List of subscription paths for the storage_stats_hw subscription
- "ipi:/components/
component[name=HARD-DISK]/
storage/state"
     stream-mode: sample           # Stream mode for storage statistics
     sample-interval: 12s          # Sampling interval for storage statistics (e.g., 12 seconds)
     encoding: json_ietf           # Encoding format for storage statistics (e.g., JSON_IETF)


   power-supply_stats_hw:          # A named subscription for power supply statistics
```

```
    paths:                          # List of subscription paths for the power-supply_stats_hw subscription
- "ipi:/components/
component[name=PSU-1]/power-
supply/state"

- "ipi:/components/
component[name=PSU-2]/power-
supply/state"
    stream-mode: sample             # Stream mode for power supply statistics
    sample-interval: 13s            # Sampling interval for power supply statistics (e.g., 13 seconds)
    encoding: json_ietf             # Encoding format for power supply statistics (e.g., JSON_IETF)


  intf-tray_stats_hw:               # A named subscription for interface tray statistics
    paths:                          # List of subscription paths for the intf-tray_stats_hw subscription
- "ipi:/interfaces/
interface[name=xe1]/state"

 - "ipi:/interfaces/
interface[name=vlan1.8]/
state"
    stream-mode: sample             # Stream mode for interface tray statistics
    sample-interval: 14s            # Sampling interval for interface tray statistics (e.g., 14 seconds)
    encoding: json_ietf             # Encoding format for interface tray statistics (e.g., JSON_IETF)
```

gnmic Command

```
# gnmic -a  10.12.91.111:11162 -u ocnos -p ocnos  --insecure  --config
multiple_subs.yaml subscribe

{
  "source": "10.12.91.111:11162",
  "subscription-name": "ram_stats_hw",
  "timestamp": 1551967101,
  "time": "1970-01-01T05:30:01.551967101+05:30",
  "updates": [
    {
      "Path": "ipi:components/component[name=RAM]/ram/state",
      "values": {
        "components/component/ram/state": {
          "available-high-memory": "0",
          "available-memory": "14743",
          "buffers": "15",
          "current-process-count": 232,
          "free-swap": "0",
          "shared-memory": "8",
          "total-high-memory": "0",
          "total-memory": "16012",
          "total-swap": "0",
          "used-memory": "1269"
        }
      }
    }
```

```
  ]
}

{
  "source": "10.12.91.111:11162",
  "subscription-name": "storage_stats_hw",
  "timestamp": 1551967102,
  "time": "1970-01-01T05:30:01.551967102+05:30",
  "updates": [
    {
      "Path": "ipi:components/component[name=HARD-DISK]/storage/state",
      "values": {
        "components/component/storage/state": {
          "free-memory": "16908",
          "total-memory": "30208",
          "used-memory": "5020"
        }
      }
    }
  ]
}

{
  "source": "10.12.91.111:11162",
  "subscription-name": "power-supply_stats_hw",
  "timestamp": 1551967103,
  "time": "1970-01-01T05:30:01.551967103+05:30",
  "updates": [
    {
      "Path": "ipi:components/component[name=PSU-1]/power-supply/state",
      "values": {
        "components/component/power-supply/state": {
          "capacity": "650",
          "fan1-rpm": 24288,
          "operational-status": "not-present",
          "output-current": "8.28",
          "output-voltage": "12.07",
          "power-consumption": "99",
          "temperature-sensor1": "22",
          "temperature-sensor2": "28",
          "temperature-sensor3": "24"
        }
      }
    }
  ]
}

{
  "source": "10.12.91.111:11162",
  "subscription-name": "power-supply_stats_hw",
  "timestamp": 1551967103,
  "time": "1970-01-01T05:30:01.551967103+05:30",
  "updates": [
    {
      "Path": "ipi:components/component[name=PSU-2]/power-supply/state",
      "values": {
        "components/component/power-supply/state": {
```

```
            "operational-status": "running",
            "temperature-sensor1": "0",
            "temperature-sensor2": "0",
            "temperature-sensor3": "0"
          }
        }
      }
    ]
  }

  {
    "source": "10.12.91.111:11162",
    "subscription-name": "intf-tray_stats_hw",
    "timestamp": 1551967104,
    "time": "1970-01-01T05:30:01.551967104+05:30",
    "updates": [
      {
        "Path": "ipi:interfaces/interface[name=xe1]/state",
        "values": {
          "interfaces/interface/state": {
            "admin-status": "up",
            "counters": {
              "in-broadcast-pkts": "0",
              "in-discards": "0",
              "in-errors": "0",
              "in-fcs-errors": "0",
              "in-multicast-pkts": "0",
              "in-octets": "0",
              "in-pkts": "0",
              "in-unicast-pkts": "0",
              "last-clear": "Never",
              "out-broadcast-pkts": "0",
              "out-discards": "0",
              "out-errors": "0",
              "out-multicast-pkts": "5",
              "out-octets": "410",
              "out-pkts": "5",
              "out-unicast-pkts": "0"
            },
            "ifindex": 10001,
            "last-change": 0,
            "logical": false,
            "oper-status": "down"
          }
        }
      }
    ]
  }

  {
    "source": "10.12.91.111:11162",
    "subscription-name": "intf-tray_stats_hw",
    "timestamp": 1551967104,
    "time": "1970-01-01T05:30:01.551967104+05:30",
    "updates": [
      {
        "Path": "ipi:interfaces/interface[name=vlan1.8]/state",
```

```
          "values": {
            "interfaces/interface/state": {
              "admin-status": "up",
              "counters": {
                "in-broadcast-pkts": "0",
                "in-discards": "0",
                "in-errors": "0",
                "in-fcs-errors": "0",
                "in-multicast-pkts": "0",
                "in-octets": "0",
                "in-pkts": "0",
                "in-unicast-pkts": "0",
                "last-clear": "Never",
                "out-broadcast-pkts": "0",
                "out-discards": "0",
                "out-errors": "0",
                "out-multicast-pkts": "0",
                "out-octets": "0",
                "out-pkts": "0",
                "out-unicast-pkts": "0"
              },
              "ifindex": 25008,
              "last-change": 22500,
              "logical": false,
              "oper-status": "up"
            }
          }
        }
      ]
    }
```


Validation

The below show command provides details about the subscriptions that have been established, including the client ID, sampling interval, encoding type, and the sensor paths that are being monitored.

```
OcNOS#show streaming-telemetry dynamic-subscriptions

 Feature streaming telemetry : Enabled

 SI:  Sampling Interval in seconds

 Enc-Type: Encoding type

 Dial-In Subscription Details:

 ClientIP:Port              ID      SI    Enc-Type       Origin:Path

 -------------            ------   ----   --------       ------------

 10.12.43.155:58267        9453     14    JSON_IETF      ipi:interfaces/interface[name=xe1]/state/counters
                                                         ipi:interfaces/interface[name=xe1]/state
                                                         ipi:interfaces/interface[name=vlan1.8]/state/counters
                                                         ipi:interfaces/interface[name=vlan1.8]/state
 10.12.43.155:58114        31533    11    JSON_IETF      ipi:components/component[name=RAM]/ram/state
 10.12.43.155:58345        3374     12    JSON_IETF      ipi:components/component[name=HARD-DISK]/storage/state
 10.12.43.155:58222        35994    13    JSON_IETF      ipi:components/component[name=PSU-1]/power-supply/state
                                                         ipi:components/component[name=PSU-2]/power-supply/state
```

Use Case 3: Configuring Multiple Subscription Requests with Prefix Option

This use case illustrates the configuration of multiple subscription request with prefix option using a YAML file input. It streamlines the subscription setup process by specifying the desired paths and subscription parameters directly in the YAML file.

YAML File Content (**prefix_path.yaml**)

```
#cat prefix_path.yaml


 subscriptions:                  #Container for subscriptions
   RAM_stats_hw:                 #A named subscription for RAM statistics
     prefix: "ipi:"              #Common prefix for paths in this subscription
     paths:                      #List of subscription paths for the RAM_stats_hw subscription
- "/components/
component[name=RAM]/ram/
state"
     stream-mode: sample         #Stream mode for RAM statistics
     sample-interval: 11s        #Sampling interval for RAM statistics (e.g., 11 seconds)
     encoding: json_ietf         #Encoding format for RAM statistics (e.g., JSON_IETF)


   intf-tray_stats_hw:           #A named subscription for interface tray statistics
     prefix: "ipi:"              #Common prefix for paths in this subscription
     paths:                      #List of subscription paths for the intf-tray_stats_hw subscription
- "/interfaces/
interface[name=xe1]/state"

 - "/interfaces/
interface[name=vlan1.8]/
state"
     stream-mode: sample         #Stream mode for interface tray statistics
     sample-interval: 14s        #Sampling interval for interface tray statistics (e.g., 14 seconds)
     encoding: json_ietf         #Encoding format for interface tray statistics (e.g., JSON_IETF)
```

gnmic Command

```
# gnmic -a  10.12.91.111:11162 -u ocnos -p ocnos  --insecure  --config
prefix_path.yaml subscribe
{
  "source": "10.12.91.111:11162",
  "subscription-name": "ram_stats_hw",
  "timestamp": 1551968637,
  "time": "1970-01-01T05:30:01.551968637+05:30",
  "updates": [
    {
      "Path": "components/component[name=RAM]/ram/state",
      "values": {
        "components/component/ram/state": {
          "available-high-memory": "0",
          "available-memory": "14793",
          "buffers": "16",
```

```
            "current-process-count": 231,
            "free-swap": "0",
            "shared-memory": "8",
            "total-high-memory": "0",
            "total-memory": "16012",
            "total-swap": "0",
            "used-memory": "1219"
          }
        }
      }
    ]
  }

  {
    "source": "10.12.91.111:11162",
    "subscription-name": "intf-tray_stats_hw",
    "timestamp": 1551968640,
    "time": "1970-01-01T05:30:01.55196864+05:30",
    "updates": [
      {
        "Path": "interfaces/interface[name=xe1]/state",
        "values": {
          "interfaces/interface/state": {
            "admin-status": "up",
            "counters": {
              "in-broadcast-pkts": "0",
              "in-discards": "0",
              "in-errors": "0",
              "in-fcs-errors": "0",
              "in-multicast-pkts": "0",
              "in-octets": "0",
              "in-pkts": "0",
              "in-unicast-pkts": "0",
              "last-clear": "Never",
              "out-broadcast-pkts": "0",
              "out-discards": "0",
              "out-errors": "0",
              "out-multicast-pkts": "9",
              "out-octets": "738",
              "out-pkts": "9",
              "out-unicast-pkts": "0"
            },
            "ifindex": 10001,
            "last-change": 0,
            "logical": false,
            "oper-status": "down"
          }
        }
      }
    ]
  }

  {
    "source": "10.12.91.111:11162",
    "subscription-name": "intf-tray_stats_hw",
    "timestamp": 1551968640,
    "time": "1970-01-01T05:30:01.55196864+05:30",
```

```
      "updates": [
        {
          "Path": "interfaces/interface[name=vlan1.8]/state",
          "values": {
            "interfaces/interface/state": {
              "admin-status": "up",
              "counters": {
                "in-broadcast-pkts": "0",
                "in-discards": "0",
                "in-errors": "0",
                "in-fcs-errors": "0",
                "in-multicast-pkts": "0",
                "in-octets": "0",
                "in-pkts": "0",
                "in-unicast-pkts": "0",
                "last-clear": "Never",
                "out-broadcast-pkts": "0",
                "out-discards": "0",
                "out-errors": "0",
                "out-multicast-pkts": "0",
                "out-octets": "0",
                "out-pkts": "0",
                "out-unicast-pkts": "0"
              },
              "ifindex": 25008,
              "last-change": 22500,
              "logical": false,
              "oper-status": "up"
            }
          }
        }
      ]
    }
```


Validation

The below show command provides details about the subscriptions that have been established, including the client ID, sampling interval, encoding type, and the sensor paths that are being monitored.

```
OcNOS#show streaming-telemetry dynamic-subscriptions

 Feature streaming telemetry : Enabled

 SI:  Sampling Interval in seconds

 Enc-Type: Encoding type

 Dial-In Subscription Details:

 ClientIP:Port              ID      SI    Enc-Type       Origin:Path

 -------------            ------   ----   --------       ------------

 10.12.43.154:50167        32137    11    JSON_IETF      ipi:components/component[name=RAM]/ram/state

 10.12.43.154:50614        36412    14    JSON_IETF     ipi:interfaces/interface[name=vlan1.8]/state/counters
                                              ipi:interfaces/interface[name=vlan1.8]/state
                                              ipi:interfaces/interface[name=xe1]/state/counters
                                              ipi:interfaces/interface[name=xe1]/state
```

Supported Datamodel and Sensor Paths

Streaming telemetry incrementally supports all IPI datamodels, with OcNOS version 6.4.1 introducing support for two IPI datamodels listed below. Telemetry supports only operational containers and a subset of leaf attributes. The Pyang tree output below illustrates the supported containers or leaves, along with a list of supported container-level paths.

ipi-platform

```
 +--rw components
     +--ro component* [name]
        +--ro name            -> ../state/name
        +--ro state
        |  +--ro name?                            string
        |  +--ro type?                            ipi-platform-
types:cmm_component_type_t
        |  +--ro location?                        string
        |  +--ro mfg-name?                        string
        |  +--ro mfg-date?                        yang:date-and-time
        |  +--ro description?                     string
        |  +--ro hardware-version?                string
        |  +--ro firmware-version?                string
        |  +--ro software-version?                string
        |  +--ro serial-no?                       string
        |  +--ro part-no?                         string
        |  +--ro removable?                       boolean
        |  +--ro oper-status?                     ipi-platform-
types:cmm_component_oper_status_t
        |  +--ro product-name?                    string
        |  +--ro asset-tag?                       string
        |  +--ro component-additional-details*   string
        |  +--ro parent?                          -> /components/component/
state/name
        |  +--ro empty?                           boolean
        |  +--ro memory
        |  |  +--ro available?   uint64
        |  |  +--ro utilized?    uint64
        |  +--ro board-fru
        |  |  +--ro board-name?        string
        |  |  +--ro board-serial-no?   string
        |  |  +--ro board-mfg-name?    string
        |  |  +--ro board-mfg-date?    yang:date-and-time
        |  +--ro temperature
        |     +--ro instant?                          decimal64
        |     +--ro min?                              decimal64
        |     +--ro max?                              decimal64
        |     +--ro avg?                              decimal64
        |     +--ro interval?                         uint32
        |     +--ro sensor-name?                      string
        |     +--ro sensor-index?                     uint8
        |     +--ro alarm-status?                     boolean
        |     +--ro alarm-threshold?                  decimal64
        |     +--ro alarm-severity?                   cml_alarm_severity_t
        |     +--ro minimum-emergency-temperature?    decimal64
        |     +--ro maximum-emergency-temperature?    decimal64
        |     +--ro minimum-alert-temperature?        decimal64
        |     +--ro maximum-alert-temperature?        decimal64
        |     +--ro minimum-critical-temperature?     decimal64
```

```
|     +--ro maximum-critical-temperature?    decimal64
+--ro cpu
|  +--ro state
|     +--ro cpu-1min-load-percentage?    decimal64
|     +--ro cpu-5min-load-percentage?    decimal64
|     +--ro cpu-15min-load-percentage?   decimal64
|     +--ro cpu-utilization?             decimal64
+--ro storage
|  +--ro state
|     +--ro total-memory?   uint64
|     +--ro used-memory?    uint64
|     +--ro free-memory?    uint64
+--ro ram
|  +--ro state
|     +--ro total-memory?            uint64
|     +--ro used-memory?             uint64
|     +--ro available-memory?        uint64
|     +--ro shared-memory?           uint64
|     +--ro buffers?                 uint64
|     +--ro total-swap?              uint64
|     +--ro free-swap?               uint64
|     +--ro current-process-count?   uint16
|     +--ro total-high-memory?       uint64
|     +--ro available-high-memory?   uint64
+--ro transceiver
|  +--ro state
|     +--ro grid-spacing?              decimal64
|     +--ro first-frequency?           decimal64
|     +--ro last-frequency?            decimal64
|     +--ro transceiver-temperature?   decimal64
|     +--ro transceiver-voltage?       decimal64
+--ro power-supply
|  +--ro state
|     +--ro operational-status?    cml_cmm_power_supply_operstatus_t
|     +--ro capacity?              decimal64
|     +--ro power-consumption?     decimal64
|     +--ro input-power?           decimal64
|     +--ro input-voltage?         decimal64
|     +--ro output-voltage?        decimal64
|     +--ro input-current?         decimal64
|     +--ro output-current?        decimal64
|     +--ro temperature-sensor1?   decimal64
|     +--ro temperature-sensor2?   decimal64
|     +--ro temperature-sensor3?   decimal64
|     +--ro fan1-rpm?              uint32
|     +--ro fan2-rpm?              uint32
|     +--ro fan3-rpm?              uint32
|     +--ro fan4-rpm?              uint32
+--ro fan
|  +--ro state
|     +--ro rpm?            uint32
|     +--ro fan-status?     cml_cmm_fan_status_t
|     +--ro fan-location?   cml_cmm_fan_location_t
+--ro fan-tray
   +--ro state
      +--ro status?   cml_cmm_fan_tray_status_t
```

ipi-interface

```
      +--rw interfaces
         +--rw interface* [name]
            +--rw name      -> ../config/name
            +--rw config
            |  +--rw name?   string
            +--ro state
               +--ro ifindex?        uint32
               +--ro admin-status?   ipi-if-types:if_interface_admin_status_t
               +--ro oper-status?    ipi-if-types:if_interface_oper_status_t
               +--ro last-change?    yang:timeticks
               +--ro logical?        boolean
               +--ro counters
                  +--ro in-octets?            yang:counter64
                  +--ro in-pkts?              yang:counter64
                  +--ro in-unicast-pkts?      yang:counter64
                  +--ro in-broadcast-pkts?    yang:counter64
                  +--ro in-multicast-pkts?    yang:counter64
                  +--ro in-discards?          yang:counter64
                  +--ro in-errors?            yang:counter64
                  +--ro in-fcs-errors?        yang:counter64
                  +--ro out-octets?           yang:counter64
                  +--ro out-pkts?             yang:counter64
                  +--ro out-unicast-pkts?     yang:counter64
                  +--ro out-broadcast-pkts?   yang:counter64
                  +--ro out-multicast-pkts?   yang:counter64
                  +--ro out-discards?         yang:counter64
                  +--ro out-errors?           yang:counter64
                  +--ro last-clear?           ipi-if-types:if_last_clear_time_t
```

Container Level Sensor Paths and Leaf Attributes

The below section lists the container level sensor paths and leaf attributes supported for telemetry.

ipi-interface

Interface State

```
    Sensor Path
            ipi:/interfaces/interface[name]/state

                /interfaces/interface[name]/state/name
                /interfaces/interface[name]/state/ifindex
                /interfaces/interface[name]/state/admin-status
                /interfaces/interface[name]/state/oper-status
                /interfaces/interface[name]/state/last-change
                /interfaces/interface[name]/state/logical
```

Interface Counters

```
    Sensor Path
            ipi:/interfaces/interface[name]/state/counters

                /interfaces/interface[name]/state/counters/in-octets
                /interfaces/interface[name]/state/counters/in-pkts
                /interfaces/interface[name]/state/counters/in-unicast-pkts
                /interfaces/interface[name]/state/counters/in-broadcast-pkts
                /interfaces/interface[name]/state/counters/in-multicast-pkts
                /interfaces/interface[name]/state/counters/in-discards
```

```
/interfaces/interface[name]/state/counters/in-errors
/interfaces/interface[name]/state/counters/in-fcs-errors
/interfaces/interface[name]/state/counters/out-octets
/interfaces/interface[name]/state/counters/out-pkts
/interfaces/interface[name]/state/counters/out-unicast-pkts
/interfaces/interface[name]/state/counters/out-broadcast-pkts
/interfaces/interface[name]/state/counters/out-multicast-pkts
/interfaces/interface[name]/state/counters/out-discards
/interfaces/interface[name]/state/counters/out-errors
/interfaces/interface[name]/state/counters/last-clear
```

ipi-platform

The paths listed below represent telemetry paths for monitoring the state of various components, including CPU, storage, RAM, power supply, fans, fan trays, and transceivers.

CPU

```
Sensor Path
        ipi:/components/component[name]/cpu/state

Leaf Attributes
            /components/component[name]/cpu/state/cpu-1min-load-percentage
            /components/component[name]/cpu/state/cpu-5min-load-percentage
            /components/component[name]/cpu/state/cpu-15min-load-percentage
            /components/component[name]/cpu/state/cpu-utilization
```

Storage

```
Sensor Path
        ipi:/components/component[name]/storage/state/

Leaf Attributes
            /components/component[name]/storage/state/total-memory
            /components/component[name]/storage/state/used-memory
            /components/component[name]/storage/state/free-memory
```

RAM

```
Sensor Path
        ipi:/components/component[name]/ram/state/

Leaf Attributes
            /components/component[name]/ram/state/total-memory
            /components/component[name]/ram/state/used-memory
            /components/component[name]/ram/state/available-memory
            /components/component[name]/ram/state/shared-memory
            /components/component[name]/ram/state/buffers
            /components/component[name]/ram/state/total-swap
            /components/component[name]/ram/state/free-swap
            /components/component[name]/ram/state/current-process-count
            /components/component[name]/ram/state/total-high-memory
            /components/component[name]/ram/state/available-high-memory
```

Power-Supply

```
Sensor Path
        ipi:/components/component[name]/power-supply/state/

Leaf Attributes
```

```
            /components/component[name]/power-supply/state/capacity
            /components/component[name]/power-supply/state/power-consumption
            /components/component[name]/power-supply/state/input-power
            /components/component[name]/power-supply/state/input-voltage
            /components/component[name]/power-supply/state/input-current
            /components/component[name]/power-supply/state/output-voltage
            /components/component[name]/power-supply/state/output-current
            /components/component[name]/power-supply/state/operational-status
            /components/component[name]/power-supply/state/fan1-rpm
            /components/component[name]/power-supply/state/fan2-rpm
            /components/component[name]/power-supply/state/fan3-rpm
            /components/component[name]/power-supply/state/fan4-rpm
            /components/component[name]/power-supply/state/temperature-sensor1
            /components/component[name]/power-supply/state/temperature-sensor2
            /components/component[name]/power-supply/state/temperature-sensor3
```

Fan

```
    Sensor Path
            ipi:/components/component[name]/fan/state/

    Leaf Attributes
            /components/component[name]/fan/state/rpm
            /components/component[name]/fan/state/fan-status
            /components/component[name]/fan/state/fan-location
```

Fan-Tray

```
    Sensor Path
            ipi:/components/component[name]/fan-tray/state/

    Leaf Attributes
            /components/component[name]/fan-tray/state/status
```

Transceiver

```
    Sensor Path
            ipi:/components/component[name]/transceiver/state/

    Leaf Attributes
            /components/component[name]/transceiver/state/grid-spacing
            /components/component[name]/transceiver/state/first-frequency
            /components/component[name]/transceiver/state/last-frequency
            /components/component[name]/transceiver/state/transceiver-
    temperature
            /components/component[name]/transceiver/state/transceiver-voltage
```

Platform State

```
    Sensor Path
            ipi:/components/component[name]/state/

    Leaf Attributes
            /components/component[name]/state/name
            /components/component[name]/state/type
            /components/component[name]/state/location
            /components/component[name]/state/mfg-name
            /components/component[name]/state/description
            /components/component[name]/state/hardware-version
            /components/component[name]/state/firmware-version
```

```
            /components/component[name]/state/software-version
            /components/component[name]/state/serial-no
            /components/component[name]/state/part-no
            /components/component[name]/state/removable
            /components/component[name]/state/oper-status
            /components/component[name]/state/product-name
            /components/component[name]/state/asset-tag
            /components/component[name]/state/component-additional-details
            /components/component[name]/state/parent
            /components/component[name]/state/empty

Sensor Path
        ipi:/components/component[name]/state/memory
Leaf Attributes
            /components/component[name]/state/memory/available
            /components/component[name]/state/memory/utilized

Sensor Path
        ipi:/components/component[name]/state/board-fru
Leaf Attributes
            /components/component[name]/state/board-fru/board-name
            /components/component[name]/state/board-fru/board-serial-no
            /components/component[name]/state/board-fru/board-mfg-name
            /components/component[name]/state/board-fru/board-mfg-date


Sensor Path
        ipi:/components/component[name]/state/temperature
Leaf Attributes
            /components/component[name]/state/temperature/instant
            /components/component[name]/state/temperature/min
            /components/component[name]/state/temperature/max
            /components/component[name]/state/temperature/avg
            /components/component[name]/state/temperature/interval
            /components/component[name]/state/temperature/sensor-name
            /components/component[name]/state/temperature/sensor-index
            /components/component[name]/state/temperature/alarm-status
            /components/component[name]/state/temperature/alarm-threshold
            /components/component[name]/state/temperature/alarm-severity
            /components/component[name]/state/temperature/minimum-emergency-
temperature
            /components/component[name]/state/temperature/maximum-emergency-
temperature
            /components/component[name]/state/temperature/minimum-alert-
temperature
            /components/component[name]/state/temperature/maximum-alert-
temperature
            /components/component[name]/state/temperature/minimum-critical-
temperature
            /components/component[name]/state/temperature/maximum-critical-
temperature
```

Implementation Examples

Typical Use Cases

- Enable Streaming Telemetry to monitor interface counters and the health of the OcNOS target device, including memory, CPU usage, fan speed, and temperature.
- Use telemetry data to trigger automated network tasks based on specific conditions.

Integration with Existing Features

Streaming Telemetry can be used in conjunction with other network monitoring and management features.

New CLI Commands

The Streaming Telemetry introduces the following configuration commands.

debug cml

Use this command to enable or disable debugging information for CML streaming telemetry.

Command Syntax

```
debug cml enable telemetry
debug cml disable telemetry
```

Parameters

None

Default

By default, debugging information is disabled.

Command Mode

Exec Mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The following example illustrates how to enable and disable the telemetry debugging information.

```
OcNOS#debug cml enable telemetry
OcNOS#debug cml disable telemetry
```

debug telemetry gnmi

Use this command to enable or disable gNMI server debugging logs with severity levels.

Command Syntax

```
debug telemetry gnmi (enable) (severity (debug|info|warning|error|fatal|panic|d-panic)|)
debug telemetry gnmi (disable) (severity (debug|info|warning|error|fatal|panic|d-panic)|)
```

Parameters

`debug`	Logs a message at debug level
`info`	Logs a message at info level
`warning`	Logs a message at warning level
`error`	Logs a message at error level
`fatal`	Logs a message and causes the program to exit with return code 1.
`panic`	Logs a message and triggers the program to generate a traceback.
`d-panic`	Logs at the Panic level

Default

By default, this command is disabled, and the gNMI server debugging level in the disabled state is set to the Error level.

Command Mode

Configure Mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The following example illustrates how to enable and disable the telemetry debug logs and their corresponding show output.

```
OcNOS(config)#feature streaming-telemetry
OcNOS(config)#debug telemetry gnmi enable severity warning
OcNOS(config)#commit
OcNOS(config)#show running-config streaming-telemetry
!
feature streaming-telemetry
debug telemetry gnmi enable severity warning
!
OcNOS(config)#debug telemetry gnmi disable severity warning
OcNOS(config)#commit
OcNOS(config)#show running-config streaming-telemetry
!
feature streaming-telemetry
!
```

feature streaming-telemetry

Use this command to enable the streaming telemetry and, upon configuration, to start the gNMI server. The gNMI server initiates listening for incoming gRPC connections on port 11162.

Use the no parameter of this command to disable the streaming telemetry, It will stop the gNMI server.

Command Syntax

```
feature streaming-telemetry
no feature streaming-telemetry
```

Parameters

None

Default

By default, the streaming-telemetry feature is disabled.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The following example illustrates how to enable the streaming telemetry.

```
OcNOS#configure terminal
OcNOS(config)#feature streaming-telemetry
OcNOS(config)#commit
```

show running-config streaming-telemetry

Use this command to display streaming telemetry status in the running configuration.

Command Syntax

```
show running-config streaming-telemetry
```

Parameters

None

Command Mode

Exec mode and Configuration Mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The following example shows the streaming telemetry status in the `show running-config` output.

```
OcNOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
OcNOS(config)#feature streaming-telemetry
OcNOS(config)#commit
OcNOS(config)#show running-config streaming-telemetry
!
feature streaming-telemetry
```

```
!
OcNOS(config)#exit
OcNOS#show running-config streaming-telemetry
!
feature streaming-telemetry
!
```

show streaming-telemetry dynamic-subscriptions

Use this command to display the streaming telemetry dial-in configurations.

Command syntax

```
show streaming-telemetry dynamic-subscriptions
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The following example displays the streaming telemetry dial-in configuration output.

```
OcNOS#show streaming-telemetry dynamic-subscriptions

 Feature streaming telemetry : Enabled

 SI:  Sampling Interval in seconds

 Enc-Type: Encoding type

 Dial-In Subscription Details:

 ClientIP:Port               ID     SI    Enc-Type       Origin:Path

 -------------            ------   ----   --------       ------------

 10.12.43.175:59108        12396   10     JSON_IETF      ipi:interfaces/interface[name=eth0]/state/counters

                                                         ipi:interfaces/interface[name=eth0]/state

 10.12.43.175:59114        6001    15     JSON_IETF      ipi:components/component[name=CPU]/cpu/state
```

The below table explains the output fields.

show streaming-telemetry dynamic-subscriptions parameters output details

Field	Description
Feature streaming telemetry	Marked as “Enabled” confirms that streaming telemetry is active on the device.
Dial-In Subscription Details	Check the Dial-in subscription details.

show streaming-telemetry dynamic-subscriptions parameters output details

Field	Description
ClientIP: Port	Verify that the client IP and port listed matches the client that should be receiving telemetry data.
SI: Sampling-interval	Confirm that the sampling interval matches the desired frequency at which data is collected and sent.
Enc-type: Encoding-type	Ensure that the encoding type (e.g., JSON_IETF) matches the expected format for telemetry data.
Origin:Path	Review the sensor paths to ensure that they correspond to the specific data sources or paths of interest.

Troubleshooting

Follow the below troubleshooting steps, to debug telemetry related issues:

Verify Collector (gnmic) Command Options: Verify the input parameters, such as the sensor path, prefix and origin "`ipi:`".

Check the Encoding Method Compatibility: Check that the request conforms to the supported JSON-IETF encoding method.

Ensure Proper Connectivity: Validate the connectivity between the router and the remote management system. This involves verifying network settings, ports, firewalls, and any potential disruptions in communication.

Collector: If `gnmic` does not receive a response or not receiving expected response, restart the request using the "`--log`" option. If more verbose debug output is needed, consider adding the "`--debug`" option as well. The gnmic tool displays the possible cause for any error, which helps in debugging the issue.

gNMI Server: If the issue is on server side, follow the steps below to troubleshoot telemetry issues on the OcNOS target. Enable debug and verify the logs in `/var/log/messages` file.

1. In configure mode, enable debug with a specific severity level either "`info`" or "`debug`" level, using the following command:

   ```
   debug telemetry gnmi (enable) (severity
   (debug|info|warning|error|fatal|panic|d-panic)|)
   ```

Note: To disable the debug telemetry, configure `debug telemetry gnmi (disable)` command.

2. In Exec mode, enable telemetry related debugs, using the following command:

   ```
   debug cml enable telemetry
   ```

Note: To disable telemetry related debugs, configure "`debug cml disable telemetry`" command.

3. Collect the output of the following command to check the state of streaming telemetry:

   ```
   show streaming-telemetry dynamic dynamic-subscriptions
   ```

Note: If telemetry is in "`disabled`" state, then telemetry feature need to enabled.

4. Collect the output of the following command to gather diagnostic information and the logs in `/var/log/messages` file, to triage further.

   ```
   show techsupport all
   ```

Abbreviations

The following are some key abbreviations and their meanings relevant to this document:

Acronym	Description
JSON	JavaScript Object Notation
RPC	Remote Procedure Call
gNMI	gRPC Network Management Interface
JSON-IETF	JSON-Internet Engineering Task Force

Glossary

The following provides definitions for key terms used throughout this document.

Streaming Telemetry	A monitoring approach that efficiently transmits operational data from OcNOS routers to remote management systems in real-time for analysis, troubleshooting, and network monitoring.
Telemetry Data	Structured operational data generated by routers that is transmitted in real-time to external systems for analysis.
JSON-IETF	JSON-IETF is a data interchange format that follows the specifications defined by the IETF. It is a lightweight, text-based format used for representing structured data. JSON-IETF is commonly used for configuration and data exchange in various network and Internet-related protocols.
Remote Management System	An external system responsible for monitoring, managing, and analyzing data received from network devices.
Network Health	The overall condition and performance of a network, including factors like stability, resource utilization, and data flow.
Resilient Network	A network designed to withstand failures or disruptions, maintaining functionality even in challenging conditions.

CFM over EVPN-MPLS for ELINE MultiHoming

Overview

The Connectivity Fault Management (CFM) enhances the product offering for the Ethernet LINE (ELINE) services in MultiHoming scenarios. Based on the 802.1ag standard, CFM encompasses Continuity Check Message (CCM), Ping, and Trace functions that help in network fault detection and isolation. This feature extends CFM over EVPN-MPLS from being solely for Single-Homing deployments to a MultiHoming scenario, where a Remote Maintenance End Point (R-MEP) is treated as a single instance by MultiHoming peers.

The Topology illustrates the configuration of User-to-Provider (UP) MEP on PE2 and PE3 Access Circuit (AC) ports, along with the corresponding UP MEP configured on the remote AC port (PE1). This configuration results in the establishment of a CFM session between the PE VTEPs and the remote VTEP.

Feature Characteristics

Functional requirements for CFM over ELINE MultiHoming:

Continuity Check Message

Continuity Check Message (CCM) provides the following capabilities:

- Ensures error-free base configuration for EVPN-MPLS MultiHoming.
- Maintains uniformity of R-MEP and remote-MAC on MultiHoming nodes.
- Enables the data plane to notify the control plane of CCM timeout, port/interface state changes, and Remote Defect Indication (RDI).
- Configures the data plane to send and process CCMs at specified intervals, with options to enable/disable CCM transmission.
- Detects connectivity failures when no CCM frames are received within a set interval and notifies the control plane.
- Programs the data plane to include Port and Interface Status Type-Length-Values (TLVs) in transmitted CCM frames.
- Transmits CC Protocol Data Unit (PDU) frames with IEEE 802.1ag-2007 compliance and supports RDI bit set or reset operations.

Ping and Trace

Ping and Trace provide the following capabilities:

- Facilitates data plane snooping of LBM or Linktrace Message (LTM) received on MEP.
- Traps LTR PDUs received on MEP and processes/replies to LBM received on User-to-Provider (UP) MEP.
- Uplifts CFM PDUs from the data plane to the control plane, and sends CFM PDUs from the control plane to the data plane.
- Provides statistics counters for transmitted Loopback Replies (LBR) and encodes service frame counts in LBM and LBR PDUs.

Benefits

Enhanced Network Monitoring: CFM enables continuous monitoring of network connections, providing real-time insights into connectivity status and performance. This ensures that any issues are quickly detected and addressed.

Quick Fault Detection: Through CCM, the system promptly identifies any disruptions or faults in the network. This swift detection allows for rapid response and minimized downtime.

Efficient Troubleshooting: CFM's Ping and Trace functions help troubleshoot network problems by pinpointing the origin of issues and the paths taken by data packets. This capability streamlines the resolution process.

Robust MultiHoming Support: The extension of CFM support to MultiHoming scenarios ensures that complex network setups remain resilient and well-monitored, even in challenging environments.

Prerequisites

Before configuring and utilizing CFM for ELINE MultiHoming, ensure the following prerequisites are met:

- **Hardware Profiles Configuration**
  - Enable the required hardware profiles to facilitate CFM operations. These include `cfm-domain-name-str`, `cfm-ccm`, and `evpn-mpls-mh` profiles.
  - Establish the hardware-profile filter (`evpn-mpls-mh`) for EVPN-MPLS MultiHoming.
- **EVPN-MPLS Configuration**
  - Enable and configure EVPN MPLS on the relevant devices and enable MultiHoming support within EVPN MPLS.
- **ELINE Service Setup**
  - Establish the ELINE service and assign the corresponding VPN identifiers (VPN-ID).
  - Configure the host-reachability-protocol using EVPN BGP with the associated Virtual Routing and Forwarding (VRF).
- **ELINE AC MultiHoming Configuration**
  - Configure ELINE MultiHoming features with proper encapsulation settings (e.g., `dot1q`) and `access-if-evpn` settings on relevant interfaces.
  - Define the necessary mapping of VPN identifiers (VPN-ID) for the EVPN service.

For more information on the EVPN MPLS configurations, refer to the *EVPN MPLS Configuration* and *EVPN MPLS Commands* chapters in the *Multi-Protocol Label Switching Guide*, Release 6.4.1.

- **MAC and MEP Considerations**
  - Ensure that the MEP on MultiHoming nodes has the same MAC. Consistent Media Access Control (MAC) addressing across Access Circuit (AC) ports is essential to facilitate single R-MEP consideration on MultiHoming peers.

For more information on the EVPN MPLS configurations, refer to the *EVPN MPLS Configuration* and *CFM and Y.1731 Commands* chapters in the *Carrier Ethernet Guide*, Release 6.4.1.

Meeting these prerequisites ensures a successful setup of CFM for ELINE MultiHoming, enabling enhanced network fault detection and isolation capabilities.

Configuration

This section illustrates the MultiHomed setup for the CFM over EVPN MPLS feature, showcasing examples for ELINE services with LDP as the underlay MPLS path.

Topology

Figure 6 consists of customer edge routers CE1 and CE2, and with IPv4 Provider Edge routers PE1, PE2, and PE3, all interconnected through the core router P in the IPv4 MPLS provider network.

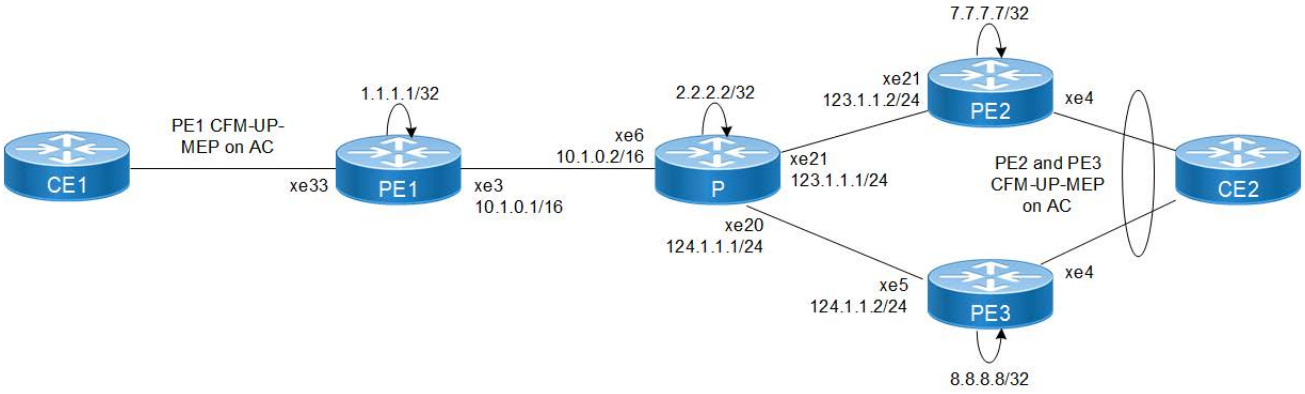


Figure 6: CFM over EVPN-MPLS for ELINE MH configuration

CFM Configuration

To enhance network management, monitoring, performance, and fault detection, configure the following hardware-profile commands on PE1, PE2, and PE3 devices, and here are the steps for the configurations: PE1: CFM and PE2/PE3: CFM.

- Enable the filter for CFM domain name strings with the command `hardware-profile filter cfm-domain-name-str enable`. This filter enhances the network devices ability to process CFM domain name strings, facilitating better network management and service identification.
- Enable statistics collection for CFM Continuity Check Messages (CCM) using the command `hardware-profile statistics cfm-ccm enable`. This feature allows the network devices to gather valuable insights into network performance and fault detection by collecting and analyzing data related to CFM CCMs.

PE1: Loopback Interface

The configuration on PE1 for a loopback interface with IP address `1.1.1.1/32` secondary is set up to provide IP connectivity for the router.

`PE1#configure terminal`	Enter configure mode.
`PE1(config)#interface lo`	Enter the interface mode for the loopback interface `lo`.
`PE1(config-if)#ip address 1.1.1.1/32 secondary`	Configure a secondary IP address, `1.1.1.1/32`, on the loopback interface.
`PE1(config-if)#exit`	Exit interface mode `lo`.
`PE1(config)#commit`	Commit the transaction.

PE1: Global LDP

The configuration on PE1 for the Global LDP router, specifying router ID and targeted peers, is done to set up Label Distribution Protocol (LDP) settings for MPLS.

`PE1(config)#router ldp`	Enter the Router LDP mode.
`PE1(config-router)#router-id 1.1.1.1`	Set the router ID for LDP to `1.1.1.1`.
`PE1(config-router)#targeted-peer ipv4 7.7.7.7`	Configure targeted peer for LDP using IPv4 addresses.
`PE1(config-router-targeted-peer)#exit-targeted-peer-mode`	Exit router targeted-peer-mode.
`PE1(config-router)#targeted-peer ipv4 8.8.8.8`	Configure targeted peer for LDP using IPv4 addresses.
`PE1(config-router-targeted-peer)#exit-targeted-peer-mode`	Exit router targeted-peer-mode.
`PE1(config-router)#exit`	Exit router LDP mode and return to the configure mode.
`PE1(config)#commit`	Commit the transaction.

PE1: Global EVPN MPLS Command

The configuration on PE1 for the Global EVPN MPLS includes activating EVPN MPLS defining the global VTEP IP address, enabling hardware profile filtering for EVPN MPLS multihoming, and activating EVPN MPLS multihoming functionality, all of which are crucial for enabling EVPN MPLS features.

`PE1(config)#evpn mpls enable`	Activate the EVPN MPLS functionality on `PE1`, enabling it to participate in EVPN MPLS services.
`PE1(config)#commit`	Commit candidate configuration to be running configuration.
`PE1(config)#evpn mpls vtep-ip-global 1.1.1.1`	Configure the global VTEP IP address `1.1.1.1`, associating it with the loopback IP.
`PE1(config)#hardware-profile filter evpn-mpls-mh enable`	Enable hardware-profile filter for EVPN MPLS multihoming.
`PE1(config)#evpn mpls multihoming enable`	Activate the EVPN MPLS multihoming functionality, allowing `PE1` to support multihomed EVPN MPLS services.
`PE1(config)#commit`	Commit the transaction.

PE1: Interface Configuration Network Side

The below configuration is performed to set up network interfaces on PE1 and enable LDP for IPv4, ensuring proper routing and labeling functionality.

`PE1(config)#interface xe3`	Enter interface mode `xe3`.
`PE1(config-if)#ip address 10.1.0.1/16`	Configure an IP address, `10.1.0.1/16`, on the interface `xe3`.
`PE1(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`PE1(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`PE1(config-if)#exit`	Exit interface mode `xe3`.
`PE1(config)#commit`	Commit the transaction.

PE1: OSPF Configuration

The below configuration is performed to set up OSPF on PE1, specifying the router ID and defining network interfaces.

`PE1(config)#router ospf 1`	Enter the router OSPF mode. Configure PE1 to run OSPF with process ID 1.
`PE1(config-router)#ospf router-id 1.1.1.1`	Set the OSPF router ID to `1.1.1.1`, identifying PE1 within the OSPF network.
`PE1(config-router)#network 1.1.1.1/32 area 0.0.0.0`	Advertise loopback address in OSPF.
`PE1(config-router)#network 10.1.0.0/16 area 0.0.0.0`	Advertise network address in OSPF.
`PE1(config-router)#exit`	Exit router OSPF mode and return to configure mode.
`PE1(config)#commit`	Commit the transaction.

PE1: BGP Configuration

The below BGP configuration on PE1 is established to enable BGP routing with ASN 1, set the BGP router ID, define iBGP neighbors, and enable the EVPN address family for efficient routing in an EVPN environment.

`PE1(config)#router bgp 1`	Enter the Router BGP mode, ASN: 1
`PE1(config-router)#bgp router-id 1.1.1.1`	Configure BGP router ID `1.1.1.1`, identifying PE1 within the BGP network.
`PE1(config-router)#neighbor 7.7.7.7 remote-as 1`	Configure neighbor `7.7.7.7` as an iBGP neighbor with their remote AS number `1`.
`PE1(config-router)#neighbor 7.7.7.7 update-source lo`	Configure neighbor `7.7.7.7` as an iBGP neighbor, specifying the source of routing updates as the loopback interface.
`PE1(config-router)#neighbor 8.8.8.8 remote-as 1`	Configure neighbor `8.8.8.8` as an iBGP neighbor with their remote AS number `1`.
`PE1(config-router)#neighbor 8.8.8.8 update-source lo`	Configure neighbor `8.8.8.8` as an iBGP neighbor, specifying the source of routing updates as the loopback interface.
`PE1(config-router)#address-family l2vpn evpn`	Enter into address family mode for L2VPN EVPN.
`PE1(config-router-af)#neighbor 7.7.7.7 activate`	Activate EVPN for iBGP neighbor `7.7.7.7` within the address family mode, ensuring that EVPN address family is enabled for the neighbor.
`PE1(config-router-af)#neighbor 8.8.8.8 activate`	Activate EVPN for iBGP neighbor `8.8.8.8` within the address family mode, ensuring that EVPN address family is enabled for the neighbor.
`PE1(config-router-af)#exit`	Exit address family mode and return to the router BGP mode.
`PE1(config-router)#commit`	Commit the transaction.
`PE1(config-router)#exit`	Exit router BGP mode and return to the configure mode.

PE1: MAC VRF Configuration

The below MAC VRF configuration on PE1 is carried out to define and set up VRF named `vrf2` with specific Route-Distinguisher (RD) and route-target values, ensuring segregated MAC address spaces for distinct network services.

`PE1(config)#mac vrf vrf2`	Enter VRF mode named `vrf2`.
`PE1(config-vrf)#rd 1.1.1.1:2`	Configure Route-Distinguisher value of `1.1.1.1:2`.
`PE1(config-vrf)#route-target both 2:2`	Configure import and export values for the `vrf2` as `2:2`.

`PE1(config-vrf)#exit`	Exit VRF mode and return to the configure mode.
`PE1(config)#commit`	Commit the transaction.

PE1: EVPN and VRF Mapping

The EVPN and VRF mapping configuration on PE1 establishes mappings between the EVPN identifier and VRF, facilitating efficient routing and connectivity in an EVPN network environment.

`PE1(config)#evpn mpls id 52 xconnect target-mpls-id 2`	Configure the EVPN-VPWS identifier with a source identifier of `52` and a target identifier of `2`.
`PE1(config-evpn-mpls)#host-reachability-protocol evpn-bgp vrf2`	Map VRF `vrf2` to the EVPN-VPWS identifier
`PE1(config-evpn-mpls)#commit`	Commit the transaction.
`PE1(config-evpn-mpls)#exit`	Exit the EVPN MPLS mode and return to the configure mode.

PE1: Access Port Configuration

The below access port configuration on PE1 is carried out to create a Layer 2 sub-interface within the physical interface, description the interface, configure the encapsulation with VLAN ID, and map VPN-ID for efficient network access and connectivity.

`PE1(config)#interface xe33`	Enter interface mode `xe33`.
`PE1(config-if)#interface xe33.2 switchport`	Create a Layer 2 sub-interface `xe33.2` within the physical interface `xe33`.
`PE1(config-if)#description access-side-int`	Provide a description for the interface.
`PE1(config-if)#encapsulation dot1q 2`	Set encapsulation to dot1q with VLAN ID `2`.
`PE1(config-if)#access-if-evpn`	Enter the access mode for EVPN MPLS ID configuration.
`PE1(config-acc-if-evpn)#map vpn-id 52`	Map VPN-ID `52`.
`PE1(config-acc-if-evpn)#exit`	Exit the access mode and return to the interface mode.
`PE1(config-if)#exit`	Exit interface mode `xe33` and return to the configure mode.
`PE1(config)#commit`	Commit the transaction.

P: Loopback Interface

The configuration on P for a loopback interface with IP address `2.2.2.2/32` secondary is set up to provide IP connectivity for the router.

`P#configure terminal`	Enter configure mode.
`P(config)#interface lo`	Enter the interface mode for the loopback interface `lo`.
`P(config-if)#ip address 2.2.2.2/32 secondary`	Configure a secondary IP address, `2.2.2.2/32`, on the loopback interface.
`P(config-if)#exit`	Exit interface mode `lo`.
`P(config)#commit`	Commit the transaction.

P: Global LDP

The configuration on P for the Global LDP router, specifying router ID to set up Label Distribution Protocol (LDP) settings for MPLS.

`P(config)#router ldp`	Enter the Router LDP mode.
`P(config-router)#router-id 2.2.2.2`	Set the router ID for LDP to `2.2.2.2`.
`P(config-router)#exit`	Exit router LDP mode and return to the configure mode.
`P(config)#commit`	Commit the transaction.

P: Interface Configuration

The below configuration is performed to set up interfaces on P and enable LDP for IPv4, ensuring proper routing and labeling functionality.

`P(config)#interface xe6`	Enter interface mode `xe6`.
`P(config-if)#ip address 10.1.0.2/16`	Configure an IP address, `10.1.0.2/16`, on the interface `xe6`.
`P(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`P(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`P(config-if)#exit`	Exit interface mode `xe6`.
`P(config)#commit`	Commit the transaction.
`P(config)#interface xe21`	Enter interface mode `xe21`.
`P(config-if)#ip address 123.1.1.1/24`	Configure an IP address, `123.1.1.1/24`, on the interface `xe21`.
`P(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`P(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`P(config-if)#exit`	Exit interface mode `xe21`.
`P(config)#commit`	Commit the transaction.
`P(config)#interface xe20`	Enter interface mode `xe20`.
`P(config-if)#ip address 124.1.1.1/24`	Configure an IP address, `124.1.1.1/24`, on the interface `xe20`.
`P(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`P(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`P(config-if)#exit`	Exit interface mode `xe20`.
`P(config)#commit`	Commit the transaction.

P: OSPF Configuration

The below configuration is performed to set up OSPF on P, specifying the router ID and defining network interfaces for efficient routing.

`P(config)#router ospf 1`	Enter the router OSPF mode. Configure P to run OSPF with process ID `1`.
`P(config-router)#ospf router-id 2.2.2.2`	Set the OSPF router ID to `2.2.2.2`, identifying P within the OSPF network.
`P(config-router)#network 2.2.2.2/32 area 0.0.0.0`	Advertise loopback address in OSPF.
`P(config-router)#network 10.1.0.2/16 area 0.0.0.0`	Advertise network address in OSPF.
`P(config-router)#network 123.1.1.1/24 area 0.0.0.0`	Advertise network address in OSPF.
`P(config-router)#network 124.1.1.1/24 area 0.0.0.0`	Advertise network address in OSPF.
`P(config-router)#exit`	Exit router OSPF mode and return to the configure mode.
`P(config)#commit`	Commit the transaction.

PE2: Loopback Interface

The configuration on PE2 for a loopback interface with IP address `7.7.7.7/32` secondary is set up to provide IP connectivity for the router.

`PE2#configure terminal`	Enter configure mode.
`PE2(config)#interface lo`	Enter the interface mode for the loopback interface `lo`.
`PE2(config-if)#ip address 7.7.7.7/32 secondary`	Configure a secondary IP address, `7.7.7.7/32`, on the loopback interface.
`PE2(config-if)#exit`	Exit interface mode `lo`.
`PE2(config)#commit`	Commit the transaction.

PE2: Global LDP

The configuration on PE2 for the Global LDP router, specifying router ID and targeted peers, is done to set up Label Distribution Protocol (LDP) settings for MPLS.

`PE2(config)#router ldp`	Enter the Router LDP mode.
`PE2(config-router)#router-id 7.7.7.7`	Set the router ID for LDP to `7.7.7.7`.
`PE2(config-router)#targeted-peer ipv4 1.1.1.1`	Configure targeted peer for LDP using IPv4 addresses.
`PE2(config-router-targeted-peer)#exit-targeted-peer-mode`	Exit router targeted-peer-mode.
`PE2(config-router)#targeted-peer ipv4 8.8.8.8`	Configure targeted peer for LDP using IPv4 addresses.
`PE2(config-router-targeted-peer)#exit-targeted-peer-mode`	Exit router targeted-peer-mode.
`PE2(config-router)#exit`	Exit router LDP mode and return to the configure mode.
`PE2(config)#commit`	Commit the transaction.

PE2: Global EVPN MPLS Command

The configuration on PE2 for the Global EVPN MPLS, includes activating EVPN MPLS defining the global VTEP IP address, enabling hardware profile filtering for EVPN MPLS multihoming, and activating EVPN MPLS multihoming functionality, all of which are crucial for enabling EVPN MPLS features.

`PE2(config)#evpn mpls enable`	Activate the EVPN MPLS functionality on `PE2`, enabling it to participate in EVPN MPLS services.
`PE2(config)#commit`	Commit candidate configuration to be running configuration.
`PE2(config)#evpn mpls vtep-ip-global 7.7.7.7`	Configure the global VTEP IP address `7.7.7.7`, associating it with the loopback IP.
`PE2(config)#hardware-profile filter evpn-mpls-mh enable`	Enable hardware-profile filter for EVPN MPLS multihoming.
`PE2(config)#evpn mpls multihoming enable`	Activate the EVPN MPLS multihoming functionality, allowing `PE2` to support multihomed EVPN MPLS services.
`PE2(config)#commit`	Commit the transaction.

PE2: Interface Configuration Network Side

The below configuration is performed to set up network interfaces on PE2 and enable LDP for IPv4, ensuring proper routing and labeling functionality.

`PE2(config)#interface xe21`	Enter interface mode `xe21`.
`PE2(config-if)#ip address 123.1.1.2/24`	Configure an IP address, `123.1.1.2/24`, on the interface `xe21`.
`PE2(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`PE2(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`PE2(config-if)#exit`	Exit interface mode `xe21`.
`PE2(config)#commit`	Commit the transaction.

PE2: OSPF Configuration

The below configuration is performed to set up OSPF on PE2, specifying the router ID and defining network interfaces.

`PE2(config)#router ospf 1`	Enter the router OSPF mode. Configure PE2 to run OSPF with process ID 1.
`PE2(config-router)#ospf router-id 7.7.7.7`	Set the OSPF router ID to `7.7.7.7`, identifying PE2 within the OSPF network.
`PE2(config-router)#network 7.7.7.7/32 area 0.0.0.0`	Advertise loopback address in OSPF.
`PE2(config-router)#network 123.1.1.0/24 area 0.0.0.0`	Advertise network address in OSPF.
`PE2(config-router)#exit`	Exit router OSPF mode and return to configure mode.
`PE2(config)#commit`	Commit the transaction.

PE2: BGP Configuration

The below BGP configuration on PE2 is established to enable BGP routing with ASN 1, set the BGP router ID, define iBGP neighbors, and enable the EVPN address family for efficient routing in an EVPN environment.

`PE2(config)#router bgp 1`	Enter the Router BGP mode, ASN: 1
`PE2(config-router)#bgp router-id 7.7.7.7`	Configure BGP router ID `7.7.7.7`, identifying PE2 within the BGP network.
`PE2(config-router)#neighbor 1.1.1.1 remote-as 1`	Configure neighbor `1.1.1.1` as an iBGP neighbor with their remote AS number `1`.
`PE2(config-router)#neighbor 1.1.1.1 update-source lo`	Configure neighbor `1.1.1.1` as an iBGP neighbor, specifying the source of routing updates as the loopback interface.
`PE2(config-router)#neighbor 8.8.8.8 remote-as 1`	Configure neighbor `8.8.8.8` as an iBGP neighbor with their remote AS number `1`.
`PE2(config-router)#neighbor 8.8.8.8 update-source lo`	Configure neighbor `8.8.8.8` as an iBGP neighbor, specifying the source of routing updates as the loopback interface.
`PE2(config-router)#address-family l2vpn evpn`	Enter into address family mode for L2VPN EVPN.
`PE2(config-router-af)#neighbor 1.1.1.1 activate`	Activate EVPN for iBGP neighbor `1.1.1.1` within the address family mode, ensuring that EVPN address family is enabled for the neighbor.
`PE2(config-router-af)#neighbor 8.8.8.8 activate`	Activate EVPN for iBGP neighbor `8.8.8.8` within the address family mode, ensuring that EVPN address family is enabled for the neighbor.
`PE2(config-router-af)#exit`	Exit address family mode and return to the router BGP mode.
`PE2(config-router)#commit`	Commit the transaction.
`PE2(config-router)#exit`	Exit router BGP mode and return to the configure mode.

PE2: MAC VRF Configuration

The below MAC VRF configuration on PE2 is carried out to define and set up VRF named `vrf2` with specific Route-Distinguisher (RD) and route-target values, ensuring segregated MAC address spaces for distinct network services.

`PE2(config)#mac vrf vrf2`	Enter VRF mode named `vrf2`.
`PE2(config-vrf)#rd 7.7.7.7:2`	Configure Route-Distinguisher value of `7.7.7.7:2`.
`PE2(config-vrf)#route-target both 2:2`	Configure import and export values for the `vrf2` as `2:2`.
`PE2(config-vrf)#exit`	Exit VRF mode and return to the configure mode.
`PE2(config)#commit`	Commit the transaction.

PE2: EVPN and VRF Mapping

The EVPN and VRF mapping configuration on PE2 establishes mappings between the EVPN identifier and VRF, facilitating efficient routing and connectivity in an EVPN network environment.

`PE2(config)#evpn mpls id 2 xconnect target-mpls-id 52`	Configure the EVPN-VPWS identifier with a source identifier of `2` and a target identifier of `52`.
`PE2(config-evpn-mpls)#host-reachability-protocol evpn-bgp vrf2`	Map VRF `vrf2` to the EVPN-VPWS identifier

`PE2(config-evpn-mpls)#commit`	Commit the transaction.
`PE2(config-evpn-mpls)#exit`	Exit the EVPN MPLS mode and return to the configure mode.

PE2: Access Port Configuration

The below access port configuration on PE2 is carried out to create a Layer 2 sub-interface within the port channel interface, set the load balancing, configure system MAC and the encapsulation with VLAN ID, map VPN-ID for efficient network access and connectivity.

`PE2(config)#interface po1`	Enter the port channel interface mode for `po1`
`PE2(config-if)#load-interval 30`	Set the load interval to `30`.
`PE2(config-if)#evpn multi-homed system-mac 0000.aaaa.bbbc`	Configure the system-mac address `0000.aaaa.bbbc` which plays a role in load balancing.
`PE2(config-if)#interface po1.2 switchport`	Create a Layer 2 sub-interface `po1.2` within the port channel.
`PE2(config-if)#encapsulation dot1q 2`	Set encapsulation to dot1q with VLAN ID `2`.
`PE2(config-if)#access-if-evpn`	Enter the access mode for EVPN MPLS ID configuration.
`PE2(config-acc-if-evpn)#map vpn-id 2`	Map VPN-ID `2`.
`PE2(config-acc-if-evpn)#exit`	Exit the access mode and return to the interface mode.
`PE2(config-if)#exit`	Exit interface mode `po1` and return to the configure mode.
`PE2(config)#commit`	Commit the transaction.

PE3: Loopback Interface

The configuration on PE3 for a loopback interface with IP address `8.8.8.8/32` secondary is set up to provide IP connectivity for the router.

`PE3#configure terminal`	Enter configure mode.
`PE3(config)#interface lo`	Enter the interface mode for the loopback interface `lo`.
`PE3(config-if)#ip address 8.8.8.8/32 secondary`	Configure a secondary IP address, `8.8.8.8/32`, on the loopback interface.
`PE3(config-if)#exit`	Exit interface mode `lo`.
`PE3(config)#commit`	Commit the transaction.

PE3: Global LDP

The configuration on PE3 for the Global LDP router, specifying router ID and targeted peers, is done to set up Label Distribution Protocol (LDP) settings for MPLS.

`PE3(config)#router ldp`	Enter the Router LDP mode.
`PE3(config-router)#router-id 8.8.8.8`	Set the router ID for LDP to `7.7.7.7`.
`PE3(config-router)#targeted-peer ipv4 1.1.1.1`	Configure targeted peer for LDP using IPv4 addresses.
`PE3(config-router-targeted-peer)#exit-targeted-peer-mode`	Exit router targeted-peer-mode.
`PE3(config-router)#targeted-peer ipv4 7.7.7.7`	Configure targeted peer for LDP using IPv4 addresses.

`PE3(config-router-targeted-peer)#exit-targeted-peer-mode`	Exit router targeted-peer-mode.
`PE3(config-router)#exit`	Exit router LDP mode and return to the configure mode.
`PE3(config)#commit`	Commit the transaction.

PE3: Global EVPN MPLS Command

The configuration on PE3 for the Global EVPN MPLS, includes activating EVPN MPLS defining the global VTEP IP address, enabling hardware profile filtering for EVPN MPLS multihoming, and activating EVPN MPLS multihoming functionality, all of which are crucial for enabling EVPN MPLS features.

`PE3(config)#evpn mpls enable`	Activate the EVPN MPLS functionality on `PE3`, enabling it to participate in EVPN MPLS services.
`PE3(config)#commit`	Commit candidate configuration to be running configuration.
`PE3(config)#evpn mpls vtep-ip-global 8.8.8.8`	Configure the global VTEP IP address `8.8.8.8`, associating it with the loopback IP.
`PE3(config)#hardware-profile filter evpn-mpls-mh enable`	Enable hardware-profile filter for EVPN MPLS multihoming.
`PE3(config)#evpn mpls multihoming enable`	Activate the EVPN MPLS multihoming functionality, allowing `PE3` to support multihomed EVPN MPLS services.
`PE3(config)#commit`	Commit the transaction.

PE3: Interface Configuration Network Side

The below configuration is performed to set up network interfaces on PE3 and enable LDP for IPv4, ensuring proper routing and labeling functionality.

`PE3(config)#interface xe5`	Enter interface mode `xe5`.
`PE3(config-if)#ip address 124.1.1.2/24`	Configure an IP address, `124.1.1.2/24`, on the interface `xe5`.
`PE3(config-if)#enable-ldp ipv4`	Enable LDP on the physical interface, facilitating the exchange of label information between devices in the network.
`PE3(config-if)#label-switching`	Enable label switching on the interface to enable MPLS-based packet forwarding.
`PE3(config-if)#exit`	Exit interface mode `xe5`.
`PE3(config)#interface xe4`	Enter the interface mode for `xe4`.
`PE3(config-if)#channel-group 1 mode active`	Attach LAG interface `xe4`.
`PE3(config-if)#exit`	Exit interface mode `xe4` and return to the configure mode.
`PE3(config)#commit`	Commit the transaction.

PE3: OSPF Configuration

The below configuration is performed to set up OSPF on PE3, specifying the router ID and defining network interfaces.

`PE3(config)#router ospf 1`	Enter the router OSPF mode. Configure PE3 to run OSPF with process ID 1.
`PE3(config-router)#ospf router-id 8.8.8.8`	Set the OSPF router ID to `8.8.8.8`, identifying PE3 within the OSPF network.

`PE3(config-router)#network 8.8.8.8/32 area 0.0.0.0`	Advertise loopback address in OSPF.
`PE3(config-router)#network 124.1.1.0/24 area 0.0.0.0`	Advertise network address in OSPF.
`PE3(config-router)#exit`	Exit router OSPF mode and return to configure mode.
`PE3(config)#commit`	Commit the transaction.

PE3: BGP Configuration

The below BGP configuration on PE3 is established to enable BGP routing with ASN 1, set the BGP router ID, define iBGP neighbors, and enable the EVPN address family for efficient routing in an EVPN environment.

`PE3(config)#router bgp 1`	Enter the Router BGP mode, ASN: 1
`PE3(config-router)#bgp router-id 8.8.8.8`	Configure BGP router ID `8.8.8.8`, identifying PE3 within the BGP network.
`PE3(config-router)#neighbor 1.1.1.1 remote-as 1`	Configure neighbor `1.1.1.1` as an iBGP neighbor with their remote AS number `1`.
`PE3(config-router)#neighbor 1.1.1.1 update-source lo`	Configure neighbor `1.1.1.1` as an iBGP neighbor, specifying the source of routing updates as the loopback interface.
`PE3(config-router)#neighbor 7.7.7.7 remote-as 1`	Configure neighbor `7.7.7.7` as an iBGP neighbor with their remote AS number `1`.
`PE3(config-router)#neighbor 7.7.7.7 update-source lo`	Configure neighbor `7.7.7.7` as an iBGP neighbor, specifying the source of routing updates as the loopback interface.
`PE3(config-router)#address-family l2vpn evpn`	Enter into address family mode for L2VPN EVPN.
`PE3(config-router-af)#neighbor 1.1.1.1 activate`	Activate EVPN for iBGP neighbor `1.1.1.1` within the address family mode, ensuring that EVPN address family is enabled for the neighbor.
`PE3(config-router-af)#neighbor 7.7.7.7 activate`	Activate EVPN for iBGP neighbor `7.7.7.7` within the address family mode, ensuring that EVPN address family is enabled for the neighbor.
`PE3(config-router-af)#exit`	Exit address family mode and return to the router BGP mode.
`PE3(config-router)#commit`	Commit the transaction.
`PE3(config-router)#exit`	Exit router BGP mode and return to the configure mode.

PE3: MAC VRF Configuration

The below MAC VRF configuration on PE3 is carried out to define and set up VRF named `vrf2` with specific Route-Distinguisher (RD) and route-target values, ensuring segregated MAC address spaces for distinct network services.

`PE3(config)#mac vrf vrf2`	Enter VRF mode named `vrf2`.
`PE3(config-vrf)#rd 8.8.8.8:2`	Configure Route-Distinguisher value of `8.8.8.8:2`.
`PE3(config-vrf)#route-target both 2:2`	Configure import and export values for the `vrf2` as `2:2`.
`PE3(config-vrf)#exit`	Exit VRF mode and return to the configure mode.
`PE3(config)#commit`	Commit the transaction.

PE3: EVPN and VRF Mapping

The EVPN and VRF mapping configuration on PE3 establishes mappings between the EVPN identifier and VRF, facilitating efficient routing and connectivity in an EVPN network environment.

`PE3(config)#evpn mpls id 2 xconnect target-mpls-id 52`	Configure the EVPN-VPWS identifier with a source identifier of `2` and a target identifier of `52`.
`PE3(config-evpn-mpls)#host-reachability-protocol evpn-bgp vrf2`	Map VRF `vrf2` to the EVPN-VPWS identifier
`PE3(config-evpn-mpls)#commit`	Commit the transaction.
`PE3(config-evpn-mpls)#exit`	Exit the EVPN MPLS mode and return to the configure mode.

PE3: Access Port Configuration

The below access port configuration on PE3 is carried out to create a Layer 2 sub-interface within the port channel interface, set the load balancing, configure system MAC and the encapsulation with VLAN ID, map VPN-ID for efficient network access and connectivity.

`PE3(config)#interface po1`	Enter the port channel interface mode for `po1`
`PE3(config-if)#load-interval 30`	Set the load interval to `30`.
`PE3(config-if)#evpn multi-homed system-mac 0000.aaaa.bbbc`	Configure the system-mac address `0000.aaaa.bbbc` which plays a role in load balancing.
`PE3(config-if)#interface po1.2 switchport`	Create a Layer 2 sub-interface `po1.2` within the port channel.
`PE3(config-if)#encapsulation dot1q 2`	Set encapsulation to dot1q with VLAN ID `2`.
`PE3(config-if)#access-if-evpn`	Enter the access mode for EVPN MPLS ID configuration.
`PE3(config-acc-if-evpn)#map vpn-id 2`	Map VPN-ID `2`.
`PE3(config-acc-if-evpn)#exit`	Exit the access mode and return to the interface mode.
`PE3(config-if)#exit`	Exit interface mode `po1` and return to the configure mode.
`PE3(config)#commit`	Commit the transaction.

PE1: CFM

The following configuration enables CFM monitoring and maintenance for EVPN services on PE1.

`PE1(config)#hardware-profile filter cfm-domain-name-str enable`	Enable the CFM domain name as a character string profile for CFM filtering.
`PE1(config)#ethernet cfm domain-type character-string domain-name evpn1 level 7 mip-creation none`	Create a CFM domain for EVPN ELINE with a character string type and set MIP creation to `none`.
`PE1(config-ether-cfm)#service ma-type string ma-name evp1`	Define a maintenance association (MA) type with the string `evp1`.
`PE1(config-ether-cfm-ma)#evpn 52`	Configure the MA for EVPN ID `52`.
`PE1(config-ether-cfm-ma)#ethernet cfm mep up mpid 20 active true evpn 52`	Create an up-maintenance endpoint (MEP) for local EVPN ID `52`.
`PE1(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable multicast continuity check (CC) state for the MEP.
`PE1(config-ether-cfm-ma-mep)#cc interval 100`	Set the CC interval to 100 milliseconds.

`PE1(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit Ethernet MA MEP mode.
`PE1(config-ether-cfm-ma)#mep crosscheck mpid 10`	Configure cross-check to the remote MEP.
`PE1(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet MA mode.
`PE1(config-ether-cfm)#exit`	Exit Ethernet CFM mode and return to the configure mode.
`PE1(config)#commit`	Commit candidate configuration to be running configuration.

PE2/PE3: CFM

The following configuration enables CFM monitoring and maintenance for EVPN services on PE2 and PE3 devices.

Note: Apply the same set of configurations to the PE3 device.

`PE2(config)#hardware-profile filter cfm-domain-name-str enable`	Enable the CFM domain name as a character string profile for CFM filtering.
`PE2(config)#ethernet cfm domain-type character-string domain-name evpn1 level 7 mip-creation none`	Create a CFM domain for EVPN ELINE with a character string type and set MIP creation to `none`.
`PE2(config-ether-cfm)#service ma-type string ma-name evp1`	Define a maintenance association (MA) type with the string `evp1`.
`PE2(config-ether-cfm-ma)#evpn 2`	Configure the MA for EVPN ID `2`.
`PE2(config-ether-cfm-ma)#ethernet cfm mep up mpid 10 active true evpn 2`	Create an up-maintenance endpoint (MEP) for local EVPN ID `2`.
`PE2(config-ether-cfm-ma-mep)#cc multicast state enable`	Enable multicast continuity check (CC) state for the MEP.
`PE2(config-ether-cfm-ma-mep)#cc interval 100`	Set the CC interval to 100 milliseconds.
`PE2(config-ether-cfm-ma-mep)#exit-ether-ma-mep-mode`	Exit Ethernet MA MEP mode.
`PE2(config-ether-cfm-ma)#mep crosscheck mpid 20`	Configure cross-check to the remote MEP.
`PE2(config-ether-cfm-ma)#exit-ether-ma-mode`	Exit Ethernet MA mode.
`PE2(config-ether-cfm)#exit`	Exit Ethernet CFM mode and return to the configure mode.
`PE2(config)#commit`	Commit candidate configuration to be running configuration.

Validation

The following output displays the validation results for PE1, PE2, and PE3 in an EVPN setup, which includes EVPN xconnect status, Ethernet CFM errors, remote maintenance points, local maintenance points, and successful ping tests.

PE1: Display xConnect Status

```
PE1#show evpn mpls xconnect
EVPN Xconnect Info
========================
AC-AC: Local-Cross-connect
AC-NW: Cross-connect to Network
AC-UP: Access-port is up
AC-DN: Access-port is down
NW-UP: Network is up
NW-DN: Network is down
NW-SET: Network and AC both are up
```

```
Local                            Remote       Connection-Details
================================ ============
================================================================================
VPN-ID       EVI-Name      MTU   VPN-ID       Source       Destination                  PE-IP           MTU   Type   NW-Status
================================ ============
================================================================================
52           ----          1500  2            xe33.2       00:00:00:aa:aa:bb:bb:00:00:00 7.7.7.7         1500  AC-NW  NW-SET
                                                                                      8.8.8.8         1500  ----   ----
```

PE1: Display Ethernet CFM errors

```
PE1#show ethernet cfm errors domain evpn1

Domain Name         Level     MEPID     Defects
-----------------------------------------------
evpn1               7         20        .....
```

PE1: Display Remote Maintenance Points

```
PE1#show ethernet cfm maintenance-points remote domain evpn1 ma-name evp1
 MEPID     RMEPID     LEVEL     Rx CCM    RDI    PEER-MAC        TYPE
-------------------------------------------------------------------------
 20        10         7         Yes       False  00aa.bb00.0002 Configured
```

PE1: Display Local Maintenance Points

```
PE1#show ethernet cfm maintenance-points local mep domain evpn1 ma-name evp1
MPID Dir Lvl CC-Stat HW-Status  CC-Intvl MAC-Address    Def Port  MD Name
-------------------------------------------------------------------------
20   Up  7   Enable  Installed  100 ms   3417.ebe4.af22 F   xe33.2 evpn1
```

PE1: Ping Test

```
PE1#ping ethernet mac 00aa.bb00.0002 unicast source 20 domain evpn1 ma evp1
 success rate is  100 (5/5)
```

PE2/PE3: Display xConnect Status

```
PE2#show evpn mpls xconnect
EVPN Xconnect Info
========================
AC-AC: Local-Cross-connect
AC-NW: Cross-connect to Network
AC-UP: Access-port is up
AC-DN: Access-port is down
NW-UP: Network is up
NW-DN: Network is down
NW-SET: Network and AC both are up

Local                            Remote       Connection-Details
================================ ============
================================================================================
VPN-ID       EVI-Name      MTU   VPN-ID       Source       Destination                  PE-IP           MTU   Type   NW-Status
================================ ============
================================================================================
2            ----          1500  52           po1.2        --- Single Homed Port ---    1.1.1.1         1500  AC-NW  NW-SET
```

PE2/PE3: Display Ethernet CFM errors

```
PE2#show ethernet cfm errors domain evpn1

Domain Name         Level     MEPID     Defects
-----------------------------------------------
evpn1               7         10        .....
```

PE2/PE3: Display Local Maintenance Points

```
PE2#show ethernet cfm maintenance-points local mep domain evpn1 ma-name evp1
MPID Dir Lvl CC-Stat HW-Status  CC-Intvl MAC-Address    Def Port  MD Name
-------------------------------------------------------------------------
10   Up  7   Enable  Installed  100 ms   00aa.bb00.0002 F   po1.2 evpn1
```

PE2/PE3: Display Remote Maintenance Points

```
PE2#show ethernet cfm maintenance-points remote domain evpn1 ma-name evp1
 MEPID     RMEPID     LEVEL     Rx CCM    RDI    PEER-MAC        TYPE
------------------------------------------------------------------------
 10        20         7         Yes       False  3417.ebe4.af22 Configured
```

PE2/PE3: Ping and Traceroute Test

```
PE2#ping ethernet mac 3417.ebe4.af22 unicast source 10 domain evpn1 ma evp1
 success rate is  100 (5/5)
PE2#traceroute ethernet 3417.ebe4.af22 mepid 10 domain evpn1 ma evp1
 MP Mac         Hops  Relay-action          Ingress/Egress  Ingress/Egress action
3417.ebe4.af22   1     RlyHit                Ingress         IngOK
```

Implementation Examples

Here is a practical scenario and use case for CFM (802.1ag) implementation for ELINE MultiHoming in the context of a telecommunications service provider who offers Ethernet-based Virtual Private Network (EVPN) services to various enterprises.

Use Case: Ensuring Service Reliability and Quality

Scenario: Consider a company with several branch offices that rely heavily on its ELINE connections to ensure smooth communication and data exchange between offices. The company subscribes to an EVPN service provided by a telecommunications service provider.

Use Case Details

1. **MultiHoming Resilience:** The company's critical applications and services require high availability. MultiHoming ensures redundancy by connecting each branch office to the provider's network through multiple paths. This way, if one path fails due to network issues, the traffic can be rerouted through the alternative path without causing a disruption.

2. **Continuous Monitoring:** CFM implementation allows the service provider to continuously monitor the connectivity and performance of the ELINE connections between the branch offices. By sending CCMs, the provider can quickly identify any interruptions in connectivity.

3. **Swift Issue Detection and Resolution:** In case of a network disruption or fault, the service provider receives immediate alerts through CFM CCMs. This enables the provider's network operations team to pinpoint the issue's location and take prompt action to restore services, minimizing downtime for the company.

4. **Troubleshooting Efficiency:** The CFM Ping and Trace functions assist in troubleshooting network issues. If the company's IT team reports a performance issue or communication problem, use CFM diagnostic capabilities to trace the path of packets and identify bottlenecks or faulty segments.

In this use case, the CFM implementation for ELINE MultiHoming provides a robust solution for ensuring reliable and high-quality connectivity for the company's distributed offices. It enables proactive monitoring and rapid issue resolution, which are critical for maintaining the company's communication and operational efficiency.

Troubleshooting

Follow the troubleshooting steps below to resolve connectivity issues related to CFM EVPN-ID and crosscheck local and remote MEP ID matching.

1. **Check Local EVPN-ID:** Verify the EVPN-ID configured on the local device (Example: PE1) and ensure that it matches the intended EVPN-ID for the target service or connection.

2. **Verify Remote EVPN-ID:** Check the EVPN-ID configured on the remote device (Example: PE2) and confirm that it matches the EVPN-ID expected by the local device.
3. **Crosscheck MEP ID:** Examine the MEP ID configured on the local device (PE1) and ensure it matches the expected R-MEP ID on the remote device (PE2).
4. **Validate Remote MEP ID:** Verify the MEP ID configured on the remote device (PE2) and ensure it matches the R-MEP ID expected by the local device (PE1).
5. **Reconfigure If Needed:** If there are discrepancies between the local and remote EVPN-IDs or MEP IDs, reconfigure the devices to match.
6. **Test the Connection:** After ensuring that EVPN-IDs and MEP IDs match on both devices, test the connection to confirm it is established correctly.

Abbreviations

The following are some key abbreviations and their meanings relevant to this document:

Acronym	Description
CFM	Continuity Fault Management
CCM	Continuity Check Messages
EVPN	Ethernet Virtual Private Network
ELINE	Ethernet-LINE
MPLS	Multi-Protocol Label Switching
UP	User-to-Provider
MEP	Maintenance End Point
MH	MultiHoming
R-MEP	Remote Maintenance End Point
MAC	Media Access Control
AC	Access Circuit
TLV	Type-Length-Value
RDI	Remote Defect Indicator
LB	Loopback
LBM	Loopback Message
LTR	Looptrace Reply

Glossary

The following provides definitions for key terms used throughout this document.

Continuity Fault Management (CFM)	A protocol (802.1ag) that facilitates the monitoring of network connectivity by using Continuity Check Messages (CCM) to detect faults.
Continuity Check Messages (CCM)	Periodic messages are used in CFM to check the continuity of a network connection.
Ethernet Virtual Private Network (EVPN)	A technology that enables the extension of Layer 2 Ethernet networks over a Layer 3 infrastructure.
Multi-Protocol Label Switching (MPLS)	In telecommunications networks, a routing technique is employed to guide data from one node to the next using concise path labels rather than relying on lengthy network addresses.
User-to-Provider (UP)	Refers to the connection between the user's and service provider's networks.
Maintenance End Point (MEP)	A point in a network where maintenance operations are initiated or terminated.
MultiHoming (MH)	A networking architecture that allows a device to be connected to multiple network paths or points of attachment.
Remote Maintenance End Point (R-MEP)	A maintenance end point located remotely from the originating point.
Media Access Control (MAC)	A unique identifier assigned to a network interface card.
Attachment Circuit (AC)	A circuit that connects a customer's equipment to a provider's network.
Type-Length-Value (TLV)	A format used to encapsulate data in a variety of protocols.
Remote Defect Indication (RDI)	A signal used to indicate a fault condition in a network link.
Loopback Message (LBM)	A message used in loopback testing to check connectivity.

Route Monitor

Overview

Object Tracking provides a mechanism for tracking the reachability status of objects, such as IP status, using Internet Protocol Service Level Agreement (IP SLA). This feature empowers users to monitor the state of these objects and make decisions based on their status. It permits the configuration of multiple track objects on interfaces, delivering flexibility in managing network link status.

Feature Characteristics

Object Tracking establishes a distinct separation between the tracked objects and the actions initiated by a client when there's a change in the state of a tracked object. Users can configure object tracking types as `any` or `all` on the interface, alongside track IDs that specify which statuses to monitor. Modify the interface's link status to either `up` or `down` based on the selected track type and the statuses of the associated track IDs.

When using `Track type all`, the feature performs a `Boolean AND` operation, requiring every object configured on the interface to be in an `up` state for the interface itself to be considered `up`. If any of these objects are not in an `up` state, the interface is set to d`own`.

Conversely, `Track type any` operates as a `Boolean OR` function, necessitating that at least one object configured on the interface must be in an `up` state for the interface to remain `up`. If none of the tracked objects are in an `up` state, the interface is marked as `down`.

Benefits

Users can ensure network reliability by defining specific tracking criteria and actions, allowing them to take appropriate measures when tracked objects experience status change. This contributes to improved network management and performance.

Prerequisites

Before configuring and utilizing Object Tracking, ensure the following prerequisites:

Track IDs: Users must define and configure the track IDs and corresponding objects they want to track for reachability. These track IDs are essential for the feature to work effectively. Deleting all track IDs from the interface will bring the interface up if it was previously down.

Interface Configuration: The feature involves configuring track types on interfaces. Therefore, ensuring that the interfaces are correctly configured and operational is important. In cases where an interface has both object tracking configurations and next-hop reachability, deleting the object tracking configurations is necessary to bring the interface back up if it goes down.

Object Tracking Criteria: Define the specific criteria and conditions for tracking an object’s reachability, such as IP status, using IP SLA.

Configuration

The below topology illustrates a network configuration involving three routers, R1, R2, and R3, with a central device referred to as the Device Under Test (DUT) positioned in the middle. This topology represents a linear or sequential network structure that showcases the Route Monitor feature.

Topology

A series of configurations were implemented on routers R1, R2, and R3, as well as on the DUT, to showcase the functionality of the Route Monitor feature. The objective was to demonstrate the configuration of network routers to monitor the reachability status of specific IPv4 and IPv6 addresses using IP SLA and illustrate that these configurations can work in conjunction with the Route Monitor feature to enable informed decisions based on the reachability status of tracked objects.

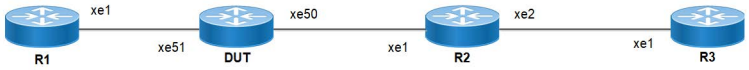


Figure 7: Route Monitor Topology

IPv4 Configuration

DUT

Use the following configuration to set up an IP SLA and enable object tracking on a network device. These commands assign IPv4 addresses to interfaces, configure specific IP SLA parameters such as threshold, timeout, and frequency, create a time-range for scheduling measurements, and establish static routes with nexthop addresses. Configure object tracking to monitor the reachability of tracked objects. These configurations highlight the versatility and functionality of the network device by allowing it to monitor IPv4 addresses, make decisions based on object tracking, and optimize network operations.

`DUT#configure terminal`	Enter configure mode.
`DUT(config)#interface xe50`	Enter interface mode `xe50`.
`DUT(config-if)#ip address 2.2.2.1/24`	Assign the IP address `2.2.2.1` with a subnet mask of `/24` to interface `xe50`.
`DUT(config-if)#exit`	Exit interface mode `xe50`.
`DUT(config)#interface xe51`	Enter interface mode `xe51`.
`DUT(config-if)#ip address 1.1.1.2/24`	Assign the IP address 1.1.1.2 with a subnet mask of /24 to interface xe51.
`DUT(config-if)#exit`	Exit interface mode `xe51`.
`DUT(config)#ip sla 1`	Create an IP SLA operation with index `1`.
`DUT(config-ip-sla)#icmp-echo ipv4 3.3.3.1 source-interface xe50`	Configure the SLA to send ICMP echo requests to destination IPv4 address `3.3.3.1` using interface `xe50` as the source.
`DUT(config-ip-sla-echo)#threshold 1000`	Set the threshold value for SLA to `1000` milliseconds.
`DUT(config-ip-sla-echo)#timeout 1000`	Set the timeout value for SLA to `1000` milliseconds.
`DUT(config-ip-sla-echo)#frequency 5`	Configure the frequency value for SLA to send ICMP echo packets every 5 seconds.
`DUT(config-ip-sla-echo)#exit`	Exit IP SLA echo mode.

`DUT(config-ip-sla)#exit`	Exit IP SLA mode.
`DUT(config)#time-range tr1`	Create a time range named `tr1`.
`DUT(config-tr)#start-time 11:22 3 july 2021`	Set the start time for the time range to `11:22 on July 3, 2021`.
`DUT(config-tr)#end-time after 200`	Set the end time to be `200` minutes from the start time.
`DUT(config-tr)#exit`	Exit time-range mode.
`DUT(config)#ip sla schedule 1 time-range tr1`	Schedule IP SLA operation 1 to run within the specified time range `tr1`.
`DUT(config)#track 1 ip sla 1 reachability`	Creating a tracking object to monitor the reachability status of IP SLA operation `1`.
`DUT(config-object-track)#exit`	Exit object track mode.
`DUT(config)#ip route 3.3.3.0/24 2.2.2.2 track 1`	Add a static route for the destination network `3.3.3.0/24` with next-hop IP `2.2.2.2`, tracked by tracking object `1`.
`DUT(config)#ip route 5.5.5.0/24 1.1.1.2`	Add a static route for the destination network `5.5.5.0/24` with next-hop IP `1.1.1.2`.
`DUT(config)#ip route 6.6.6.0/24 2.2.2.2 track 1`	Add a static route for the destination network `6.6.6.0/24` with next-hop IP `2.2.2.2`, tracked by tracking object `1`.
`DUT(config)#ip route 6.6.6.0/24 1.1.1.2 10`	Add a static route for the destination network `6.6.6.0/24` with next-hop IP `1.1.1.2` and a metric of `10`.
`DUT(config)#commit`	Commit the candidate configuration to the running configuration.
`DUT(config)#interface xe51`	Enter interface mode `xe51`.
`DUT(config-if)#object-tracking all`	Enable object tracking for `all` tracking objects on interface `xe51`.
`DUT(config-if)#object-tracking 1`	Configure object tracking `1` on interface `xe51`.
`DUT(config-if)#object-tracking 2`	Configure object tracking `2` on interface `xe51`.
`DUT(config-if)#exit`	Exit interface mode.
`DUT(config)#exit`	Exit configure mode.

By configuring the routes below, R1, R2, and R3 effectively forward network traffic to its designated destinations within the network. These configurations actively contribute to efficient routing operations and ensure network traffic reaches its targets.

R1

`R1#configure terminal`	Enter configure mode.
`R1(config)#interface xe1`	Enter interface mode `xe1`.
`R1(config-if)#ip address 1.1.1.1/24`	Assign the IP address `1.1.1.1` with a subnet mask of `/24` to interface `xe1`.
`R1(config-if)#commit`	Commit the candidate configuration to the running configuration.
`R1(config-if)#exit`	Exit interface mode `xe1`.
`R1(config)#ip route 2.2.2.0/24 1.1.1.2`	Add a static route for the destination network `2.2.2.0/24` with next-hop IP `1.1.1.2`.
`R1(config)#ip route 3.3.3.0/24 1.1.1.2`	Add a static route for the destination network `3.3.3.0/24` with next-hop IP `1.1.1.2`.

`R1(config)#commit`	Commit the candidate configuration to the running configuration.
`R1(config)#exit`	Exit configure mode.

R2

`R2#configure terminal`	Enter configure mode.
`R2(config)#interface xe1`	Enter interface mode `xe1`.
`R2(config-if)#ip address 2.2.2.2/24`	Assign the IP address `2.2.2.2` with a subnet mask of `/24` to interface `xe1`.
`R2(config-if)#exit`	Exit interface mode `xe1`.
`R2(config)#interface xe2`	Enter interface mode `xe2`.
`R2(config-if)#ip address 3.3.3.1/24`	Assign the IP address `3.3.3.1` with a subnet mask of `/24` to interface `xe2`.
`R2(config-if)#exit`	Exit interface mode `xe2`.
`R2(config)#ip route 1.1.1.0/24 2.2.2.1`	Add a static route for the destination network `1.1.1.0/24` with next-hop IP `2.2.2.1`.
`R2(config)#commit`	Commit the candidate configuration to the running configuration.
`R2(config)#exit`	Exit configure mode.

R3

`R3#configure terminal`	Enter configure mode.
`R3(config)#interface xe1`	Enter interface mode `xe1`.
`R3(config-if)#ip address 3.3.3.2/24`	Assign the IP address `3.3.3.2` with a subnet mask of `/24` to interface `xe1`.
`R3(config-if)#commit`	Commit the candidate configuration to the running configuration.
`R3(config-if)#exit`	Exit interface mode `xe1`.
`R3(config)#ip route 1.1.1.0/24 3.3.3.1`	Add a static route for the destination network `1.1.1.0/24` with next-hop IP `3.3.3.1`.
`R3(config)#ip route 2.2.2.0/24 3.3.3.1`	Add a static route for the destination network `2.2.2.0/24` with next-hop IP `3.3.3.1`.
`R3(config)#commit`	Commit the candidate configuration to the running configuration.
`R3(config)#exit`	Exit configure mode.

Validation

The following show output displays information about the IPv4 route table, IP SLA reachability tracking, and interface status on a network device running OcNOS.

DUT

```
DUT#show track
TRACK Id: 1
  IP SLA 1 reachability
```

```
  Reachability is UP
    4 changes, last change : 2019 Mar 14 14:53:47
Track interface : xe51

DUT#show ip route track-table
 ip route 3.3.3.0 255.255.255.0 2.2.2.2 track 1 state is [up]
 ip route 6.6.6.0 255.255.255.0 2.2.2.2 track 1 state is [up]

DUT#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            1.1.1.0/24 is directly connected, xe51, 00:55:38
C            2.2.2.0/24 is directly connected, xe50, 00:49:50
S            3.3.3.0/24 [1/0] via 2.2.2.2, xe50, 00:00:03
S            5.5.5.0/24 [1/0] via 1.1.1.2, xe51, 00:08:12
S            6.6.6.0/24 [1/0] via 2.2.2.2, xe50, 00:00:03

Gateway of last resort is not set

DUT#show interface brief xe51

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       OTD  - Object Tracking Down
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)


--------------------------------------------------------------------------------
Ethernet  Type    PVID   Mode     Status  Reason  Speed Port ch#  Ctl Br/Bu  Loopbk Interface
--------------------------------------------------------------------------------
xe51       ETH    --    routed   down    OTD     10g   --      No       No
```

IPv6 Configuration

DUT

Use the following configuration to set up an IP SLA and enable object tracking on a network device. These commands assign IPv6 addresses to interfaces, configure specific IP SLA parameters such as threshold, timeout, and frequency, create a time-range for scheduling measurements, and establish static routes with nexthop addresses. Configure object tracking to monitor the reachability of tracked objects. These configurations highlight the versatility and functionality of the network device by allowing it to monitor IPv6 addresses, make decisions based on object tracking, and optimize network operations.

`DUT#configure terminal`	Enter configure mode.
`DUT(config)#interface xe50`	Enter interface mode `xe50`.
`DUT(config-if)#ipv6 address 2000::1/64`	Assign an IPv6 address (`2000::1/64`) to interface `xe50`.
`DUT(config-if)#exit`	Exit interface mode `xe50`.
`DUT(config)#interface xe51`	Enter interface mode `xe51`.
`DUT(config-if)#ipv6 address 1000::2/64`	Assign an IPv6 address (`1000::2/64`) to interface `xe51`.

DUT(config-if)#exit	Exit interface mode xe51.
DUT(config)#ip sla 1	Create an IP SLA operation with index 1.
DUT(config-ip-sla)#icmp-echo ipv6 3000::1 source-interface xe50	Configure the SLA to send IPv6 ICMP echo requests to destination IPv6 address 3000::1 using interface xe50 as the source.
DUT(config-ip-sla-echo)#threshold 1000	Set the threshold value for SLA to 1000 milliseconds.
DUT(config-ip-sla-echo)#timeout 1000	Set the timeout value for SLA to 1000 milliseconds.
DUT(config-ip-sla-echo)#frequency 5	Configure the frequency value for SLA to send IPv6 ICMP echo packets every 5 seconds.
DUT(config-ip-sla-echo)#exit	Exit IP SLA echo mode.
DUT(config-ip-sla)#exit	Exit IP SLA mode.
DUT(config)#time-range tr1	Create a time range named tr1.
DUT(config-tr)#start-time 11:22 3 july 2021	Set the start time for the time range to 11:22 on July 3, 2021.
DUT(config-tr)#end-time after 200	Set the end time to be 200 minutes from the start time.
DUT(config-tr)#exit	Exit time-range mode.
DUT(config)#ip sla schedule 1 time-range tr1	Schedule IP SLA operation 1 to run within the specified time range tr1.
DUT(config)#track 1 ip sla 1 reachability	Creating a tracking object to monitor the reachability status of IP SLA operation 1.
DUT(config-object-track)#exit	Exit object track mode.
DUT(config)#ipv6 route 3000::0/64 2000::2 track 1	Add an IPv6 static route for the destination network 3000::0/64 with a next-hop IPv6 2000::2, tracked by tracking object 1.
DUT(config)#ipv6 route 3333::1/128 1000::1	Add an IPv6 static route for the destination network 3333::1/128 with next-hop IPv6 1000::1.
DUT(config)#ipv6 route 3333::1/128 2000::2 track 1	Add an IPv6 static route for the destination network 6.6.6.0/24 with next-hop IPv6 2000::2, tracked by tracking object 1.
DUT(config)#ipv6 route 3333::1/128 1000::1 10	Add an IPv6 static route for the destination network 3333::1/128 with next-hop IP 1000::1 and a metric of 10.
DUT(config)#commit	Commit the candidate configuration to the running configuration.
DUT(config)#interface xe51	Enter interface mode xe51.
DUT(config-if)#object-tracking all	Enable object tracking for all tracking objects on interface xe51.
DUT(config-if)#object-tracking 1	Configure object tracking 1 on interface xe51.
DUT(config-if)#object-tracking 2	Configure object tracking 2 on interface xe51.
DUT(config-if)#exit	Exit interface mode.
DUT(config)#exit	Exit configure mode.

By configuring the routes below, R1, R2, and R3 effectively forward network traffic to its designated destinations within the network. These configurations actively contribute to efficient routing operations and ensure network traffic reaches its targets.

R1

`R1#configure terminal`	Enter configure mode.
`R1(config)#interface xe1`	Enter interface mode `xe1`.
`R1(config-if)#ipv6 address 1000::1/64`	Assign the IPv6 address `1000::1` with a subnet mask of `/64` to interface `xe1`.
`R1(config-if)#commit`	Commit the candidate configuration to the running configuration.
`R1(config-if)#exit`	Exit interface mode `xe1`.
`R1(config)#ipv6 route 2000::0/64 1000::2`	Add an IPv6 static route for the destination network `2000::0/64` with next-hop IPv6 `1000::2`.
`R1(config)#ipv6 route 3000::0/64 1000::2`	Add an IPv6 static route for the destination network `3000::0/64` with next-hop IPv6 `1000::2`.
`R1(config)#commit`	Commit the candidate configuration to the running configuration.
`R1(config)#exit`	Exit configure mode.

R2

`R2#configure terminal`	Enter configure mode.
`R2(config)#interface xe1`	Enter interface mode `xe1`.
`R2(config-if)#ipv6 address 2000::2/64`	Assign the IPv6 address `2000::2` with a subnet mask of `/64` to interface `xe1`.
`R2(config-if)#exit`	Exit interface mode `xe1`.
`R2(config)#interface xe2`	Enter interface mode `xe2`.
`R2(config-if)#ipv6 address 3000::1/64`	Assign the IPv6 address `3000::1` with a subnet mask of `/64` to interface `xe2`.
`R2(config-if)#exit`	Exit interface mode `xe2`.
`R2(config)#ipv6 route 1000::0/64 2000::1`	Add an IPv6 static route for the destination network `1000::0/64` with next-hop IPv6 `2000::1`.
`R2(config)#commit`	Commit the candidate configuration to the running configuration.
`R2(config)#exit`	Exit configure mode.

R3

`R3#configure terminal`	Enter configure mode.
`R3(config)#interface xe1`	Enter interface mode `xe1`.
`R3(config-if)#ipv6 address 3000::2/64`	Assign the IPv6 address `3000::2` with a subnet mask of `/64` to interface `xe1`.
`R3(config-if)#commit`	Commit the candidate configuration to the running configuration.
`R3(config-if)#exit`	Exit interface mode `xe1`.
`R3(config)#ipv6 route 1000::0/64 3000::1`	Add an IPv6 static route for the destination network `1000::0/64` with next-hop IPv6 `3000::1`.

`R3(config)#ipv6 route 2000::0/64 3000::1`	Add an IPv6 static route for the destination network `2000::0/64` with next-hop IPv6 `3000::1`.
`R3(config)#commit`	Commit the candidate configuration to the running configuration.
`R3(config)#exit`	Exit configure mode.

Validation

The following show output displays the information about IP SLA reachability tracking, IPv6 route tables, and interface status on a network device running OcNOS.

DUT

```
DUT#show track
TRACK Id: 1
  IP SLA 1 reachability
  Reachability is UP
    4 changes, last change : 2019 Mar 14 14:53:47
Track interface : xe51

DUT#show ip route track-table
 ipv6 route 3000::0/64 2000::2 track 1 state is [up]
 ipv6 route 3333::1/128 2000::2 track 1 state is [up]

DUT#show ip sla summary
IP SLA Operation Summary
Codes: * active, ^ inactive

ID       Type        Destination       Stats       Return      Last
                                       (usec)        Code        Run
------------------------------------------------------------------
*1      icmp-echo   3000::1                16000         OK        2019 Mar 11 1
6:11:40
------------------------------------------------------------------

DUT#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, 00:04:46
C       1000::/64 via ::, xe51, 00:02:48
C       2000::/64 via ::, xe50, 00:02:48
S       3000::/64 [1/0] via 2000::2, xe50, 00:02:48
S       3333::1/128 [1/0] via 2000::2, xe50, 00:02:48

DUT#show interface brief xe51

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       OTD  - Object Tracking Down
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)


--------------------------------------------------------------------------------
Ethernet   Type     PVID  Mode      Status  Reason  Speed Port Ch #  Ctl Br/Bu  Loopbk
Interface
```

```
--------------------------------------------------------------------------------
xe51        ETH     --    routed     down    OTD     10g   --         No         No
```

Implementation Examples

Here is a practical scenario and use case for Object Tracking implementation:

Link Redundancy: Object Tracking can be used to monitor the reachability of primary and backup network links. If the primary link fails or becomes congested, the system can automatically switch traffic to the backup link, ensuring uninterrupted network connectivity.

Load Balancing: Object Tracking helps optimize load balancing by continuously assessing the health and availability of servers or paths. If a server becomes overloaded or fails, traffic can be intelligently redirected to healthy servers, improving resource utilization and user experience.

Failover Testing and Verification: Object Tracking provides a mechanism for simulating network failures and verifying failover mechanisms. By configuring tracked objects to mimic real-world conditions, network administrators can assess the resilience of their network configurations and ensure they perform as expected during failures.

NewCLICommands

The Route Monitor feature introduces the following configuration commands. For more information, refer to the *Interface Commands, IP Service Level Agreements Commands*, and *Object Tracking Commands* chapters in the System Management Guide, Release 6.4.1.

object-tracking

Use this command to configure track IDs and options on the interfaces.

Use the no parameter with this command to remove the configurations.

These commands configure object tracking on interfaces, with specific track IDs and tracked objects set to determine what gets tracked and affects the interface's status.

The `object-tracking` command provides flexibility, enabling both `all` and `any` tracking behaviors for influencing the interface's status. A maximum of 8 track IDs can be configured per interface. It is possible to configure the same track IDs or options on multiple interfaces.

CommandSyntax

```
object-tracking <1-500>
object-tracking <all | any>
no object-tracking <1-500>
no object-tracking <all | any>
```

Parameters

`<1-500>`	Object tracking ID
`all`	Boolean AND operation. Each object configured on the interface must be in an up state for the interface itself to be in an up state; otherwise, it will be brought down.
`any`	Boolean OR operation. At least one object configured on the interface must be in an up state; otherwise, the interface will be brought down.

Default

None

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Example

Here are some example commands for configuring object tracking in the interface mode.

```
OcNOS(config)#interface xe5
OcNOS(config-if)#object-tracking 10
OcNOS(config-if)#object-tracking all
OcNOS(config-if)#commit

OcNOS(config-if)#no object-tracking 10
OcNOS(config-if)#no object-tracking all
OcNOS(config-if)#commit
OcNOS(config-if)#exit
```

Troubleshooting

Interface Status: Verify the status of the interface linked with object tracking. If the configured track type is `all`, confirm that all tracked objects are in an `up` state to consider the interface as `up`. In the case of the track type being `any`, ensure that at least one tracked object is `up` to maintain the interface in an `up` state.

Abbreviations

The following are some key abbreviations and their meanings relevant to this document:

Acronym	Description
NSM	Network and Service Management
IP SLA	Internet Protocol Service Level Agreement
DUT	Device Under Test

Glossary

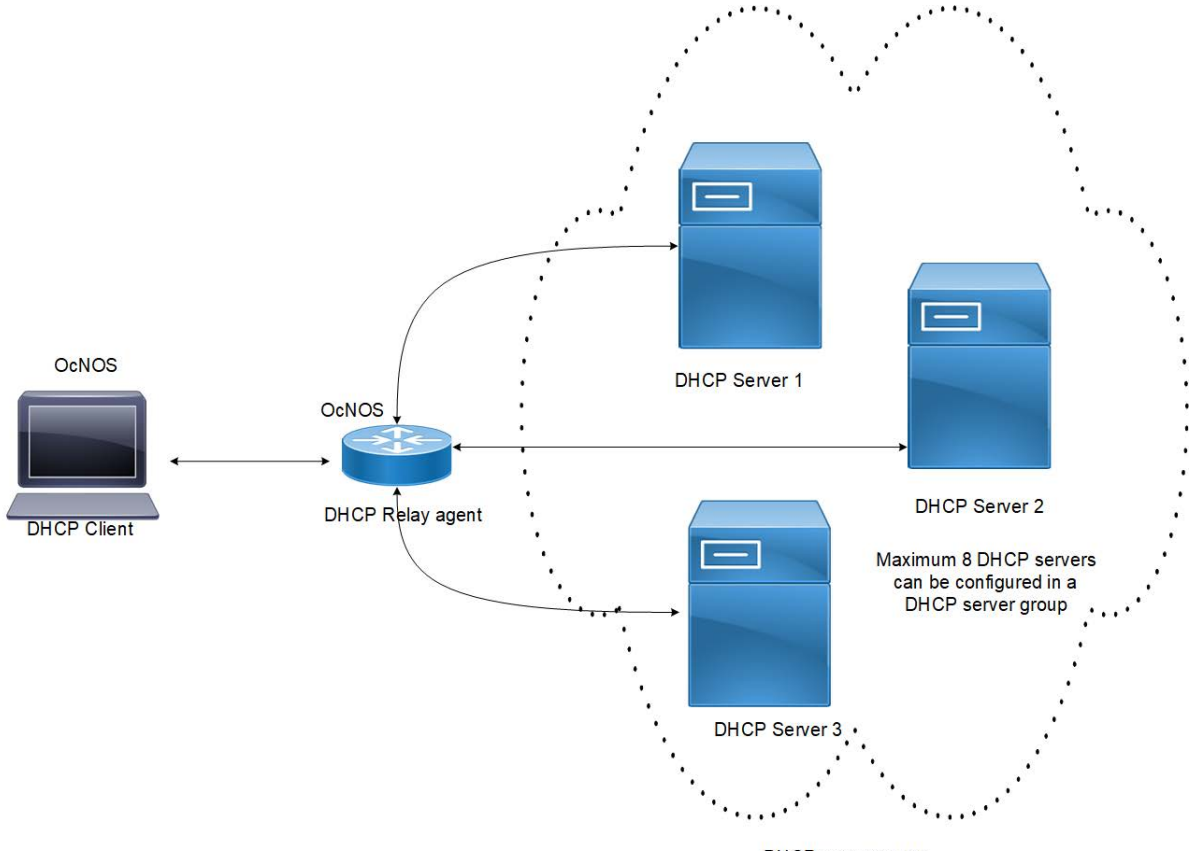
The following provides definitions for key terms used throughout this document.

Object Tracking	A feature that monitors the reachability status of objects, such as IP status, using IP SLA and allows users to take actions based on their status.
Track Object	An object configured for tracking within the Object Tracking feature. These objects can represent specific network components or conditions, such as IP addresses or link statuses.
Track ID	A unique identifier associated with a track object that enables the system to monitor and assess the status of that object.
Track Type	The configuration specifies how the interface's link status should be determined based on the statuses of associated track objects. It can be set to all or any.
Track Type “All”	A track type that uses a Boolean AND function, requiring that all tracked objects be in an up state for the interface to be considered up.
Track Type “Any”	A track type that uses a Boolean OR function, ensuring that at least one tracked object is in an up state for the interface to remain up.

DHCP Server Group

Overview

Dynamic Host Control Protocol (DHCP) Group provides the capability to specify multiple DHCP servers as a group on the DHCP relay agent and to correlate a relay agent interface with the server group. When the interface receives request messages from clients, the relay agent forwards the message to all the DHCP servers of the group. One or multiple DHCP servers in the group process the request and respond with an offer to the client. The client reviews the offer and sends the request message to the chosen server to obtain the network configuration that includes an IP address. The illustration below shows a DHCP client sending a request message to a DHCP relay agent that forwards the message to the three servers in the DHCP server group to get their network configuration. The DHCP client and DHCP relay agent run OcNOS, but the DHCP servers can be OcNOS or Linux devices.



DHCP server group

Feature Characteristics

This feature enables the configuration of the DHCP server group and attaches it to a DHCP relay agent through the CLI and the NetConf interface. A DHCP server group can be attached with multiple DHCP relay uplink interfaces, but at a given time, a single DHCP relay uplink interface is allowed to be attached with a single DHCP server group. The attachment of the DHCP relay uplink interface to another DHCP server group dissociates its attachment with the earlier attached DHCP server group.

This feature helps to configure DHCP IPv4 and IPv6 groups and attach server IP addresses to the group. Creating a maximum of 32 IPv4 and 32 IPv6 groups per VRF is allowed, and configuring 8 DHCP servers is permitted for each DHCP server group.

Benefits

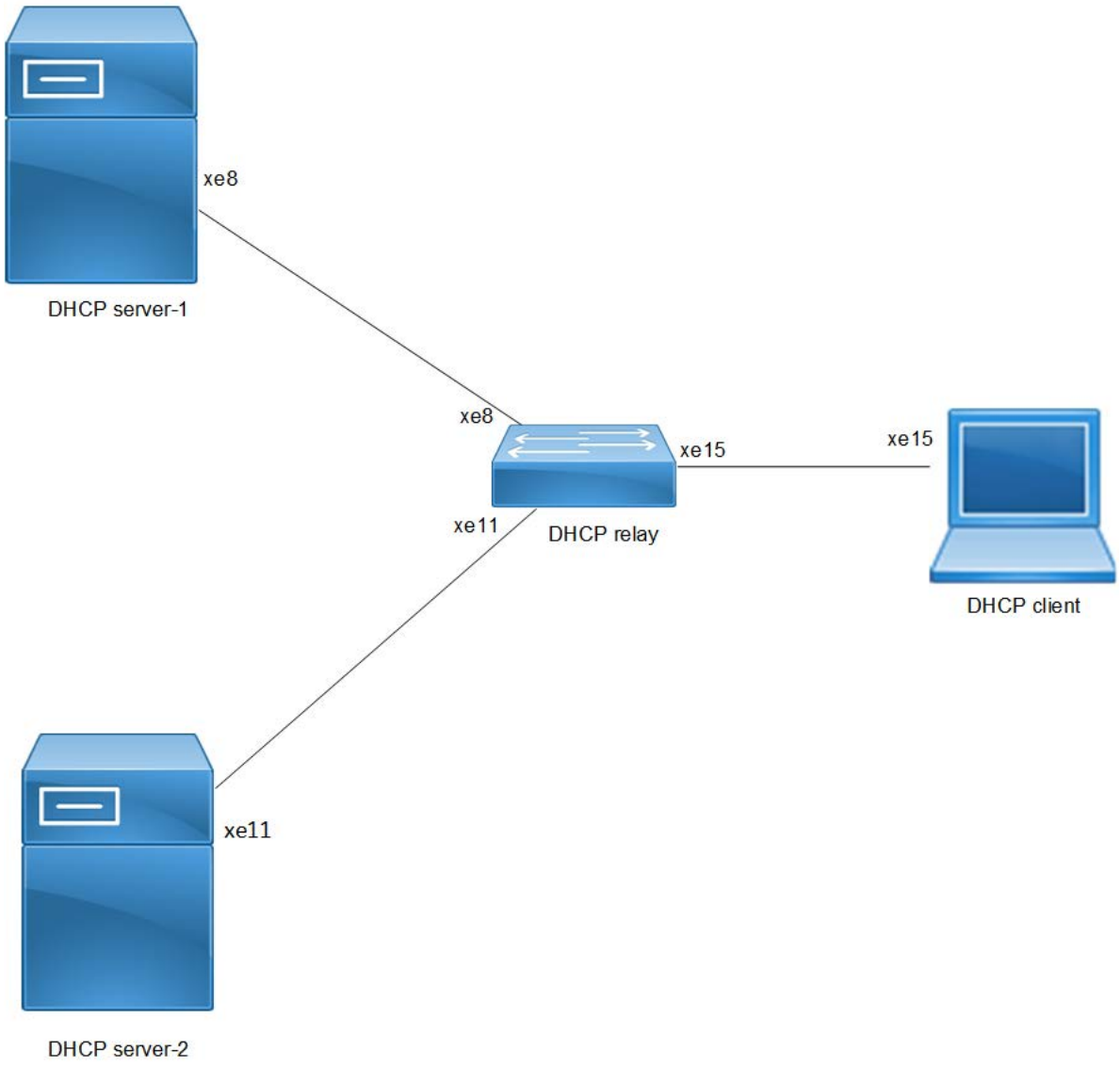
The DHCP relay agent forwards the request message from the DHCP client to multiple DHCP servers in the group. Forwarding the request message to multiple DHCP servers increases the reliability of obtaining the network configuration.

Configuration

Before configuring the DHCP client and the DHCP relay agent, make sure that DHCP server is configured and the `dhcpd` service is running in the DHCP server.

Topology

In the below example, DHCP server1 and DHCP server2 (OcNOS or Linux devices) are connected to the DHCP relay agent (an OcNOS device), and the DHCP relay is connected to a DHCP client (an OcNOS device). The DHCP client sends discover message to the DHCP servers through the DHCP relay agent.



DHCP server group topology

DHCP Server-1 Configuration for IPv4

This section shows how to configure the DHCPv4 Server-1.

DHCPv4 Server-1

`OcNOS#configure terminal`	Enter configure mode.
`OcNOS(config)ip dhcp server pool DHCP-Server-1`	Configure DHCP server group for server in global mode.
`OcNOS(dhcp-config)#network 10.10.10.0 netmask 255.255.255.0`	Configure network `10.10.10.0` and netmask `255.255.255.0`.
`OcNOS(dhcp-config)#address range low-address 10.10.10.1 high-address 10.10.10.254`	Configure address range from `10.10.10.1` to `10.10.10.254`.

`OcNOS(dhcp-config)#dns-server 192.2.2.2`	Configure the DNS server `192.2.2.2`.
`OcNOS(dhcp-config)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(dhcp-config)#exit`	Exit DHCP config mode.
`OcNOS(config)#ip dhcp server pool DHCP-SER`	Configure DHCP server group for client in global mode.
`OcNOS(dhcp-config)#network 20.20.20.0 netmask 255.255.255.0`	Configure network `20.20.20.0` and netmask `255.255.255.0`.
`OcNOS(dhcp-config)#address range low-address 20.20.20.1 high-address 20.20.20.30`	Configure address range from `20.20.20.1` to `20.20.20.30`.
`OcNOS(dhcp-config)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(dhcp-config)#exit`	Exit dhcp config mode.
`OcNOS(config)#interface xe8`	Enter interface mode `xe8`.
`OcNOS(config-if)#ip address 10.10.10.2/24`	Configure IP address on the interface `xe8`.
`OcNOS(config-if)#ip dhcp server`	Server should be configured on the interface while connected to the relay.
`OcNOS(config-if)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(config-if)#exit`	Exit interface mode.
`OcNOS(config)#ip route 20.20.20.0/24 10.10.10.3`	Configure static route of `20.20.20.0/24` by next hop interface `10.10.10.3`.
`OcNOS(config)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(config)#exit`	Exit config mode.

Validation

The below shows the running configuration of the DHCPv4 Server-1 node:

```
OcNOS#show running-config dhcp
interface eth0
 ip address dhcp
!
!

ip dhcp server pool DHCP-Server-1
 network 10.10.10.0 netmask 255.255.255.0
 address range low-address 10.10.10.1 high-address 10.10.10.254
 dns-server 192.2.2.2
ip dhcp server pool DHCP-SER
 network 20.20.20.0 netmask 255.255.255.0
 address range low-address 20.20.20.1 high-address 20.20.20.30
interface xe8
 ip dhcp server
!
OcNOS#
```

DHCP Server-2 Configuration for IPv4

This section shows how to configure the DHCPv4 Server-2.

DHCPv4 Server-2

`OcNOS#configure terminal`	Enter configure mode.
`OcNOS(config)#ip dhcp server pool DHCP-Server-2`	Configure DHCP server group for server in global mode.
`OcNOS(dhcp-config)#network 40.10.10.0 netmask 255.255.255.0`	Configure network `40.10.10.0` and netmask `255.255.255.0`.
`OcNOS(dhcp-config)#address range low-address 40.10.10.1 high-address 40.10.10.254`	Configure address range from `40.10.10.1` to `40.10.10.254`.
`OcNOS(dhcp-config)#dns-server 192.2.2.2`	Configure DNS server `192.2.2.2`.
`OcNOS(dhcp-config)#ip dhcp server pool DHCP-SER`	Configure DHCP server group for client in global mode.
`OcNOS(dhcp-config)#network 20.20.20.0 netmask 255.255.255.0`	Configure network `20.20.20.0` and netmask `255.255.255.0`.
`OcNOS(dhcp-config)#address range low-address 20.20.20.1 high-address 20.20.20.30`	Configure address range from `20.20.20.1` to `20.20.20.30`.
`OcNOS(dhcp-config)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(dhcp-config)#exit`	Exit DHCPv6 config mode.
`OcNOS(config)#interface xe11`	Enter interface mode `xe11`.
`OcNOS(config-if)#ip address 40.10.10.2/24`	Configure IP address `40.10.10.2/24` on the interface `xe11`.
`OcNOS(config-if)#ip dhcp server`	Server should be configured on the interface while connected to the relay.
`OcNOS(config-if)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(config-if)#exit`	Exit interface mode.
`OcNOS(config)#ip route 20.20.20.0/24 40.10.10.3`	Configure static route `20.20.20.0/24` by next hop interface `40.10.10.3`.
`OcNOS(config)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(config)#exit`	Exit config mode.

Validation

The below shows the running configuration of the DHCPv4 Server-2 node:

```
OcNOS#show running-config dhcp
interface eth0
 ip address dhcp
!
!

ip dhcp server pool DHCP-Server-2
 network 40.10.10.0 netmask 255.255.255.0
 address range low-address 40.10.10.1 high-address 40.10.10.254
 dns-server 192.2.2.2
ip dhcp server pool DHCP-SER
 network 20.20.20.0 netmask 255.255.255.0
```

```
 address range low-address 20.20.20.1 high-address 20.20.20.30
interface xe11
 ip dhcp server
!
OcNOS#
```

DHCP Relay Agent Configuration for IPv4

This section shows how to configure the DHCPv4 relay agent.

DHCPv4 Relay Agent

`OcNOS#configure terminal`	Enter configure mode.
`OcNOS(config)#ip dhcp relay server-group dhcp-relay-gp`	Configure relay server-group group name in global mode.
`OcNOS(dhcp-relay-group)#server 10.10.10.2`	Configure server `10.10.10.2`.
`OcNOS(dhcp-relay-group)#exit`	Exit DHCP relay group.
`OcNOS(config)#interface xe15`	Enter interface mode `xe15`.
`OcNOS(config-if)#ip address 20.20.20.2/24`	Configure IPv4 address `20.20.20.2` on the interface `xe15`.
`OcNOS(config-if)#ip dhcp relay`	Relay should be configured on the interface connecting to the client.
`OcNOS(config-if)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(config-if)#exit`	Exit interface mode.
`OcNOS(config)#interface xe8`	Enter interface mode `xe8`.
`OcNOS(config-if)#ip address 10.10.10.3/24`	Configure IPv4 address `10.10.10.3` on the interface `xe8`.
`OcNOS(config-if)#ip dhcp relay uplink`	Configure relay uplink on the device connecting the server.
`OcNOS(config-if)#ip dhcp relay server-select dhcp-relay-gp`	Configure relay server-select group name on the device connected to the server.
`OcNOS(config-if)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(config-if)#exit`	Exit interface mode.
`OcNOS(config)#ip dhcp relay server-group dhcp-relay-gp`	Configure relay server-group group name in global mode.
`OcNOS(dhcp-relay-group)#server 40.10.10.2`	Configure IPv4 DHCP server address `40.10.10.2` on the server group.
`OcNOS(dhcp-relay-group)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(dhcp-relay-group)#exit`	Exit DHCP relay group.
`OcNOS(config)#interface xe11`	Enter interface mode `xe11`.
`OcNOS(config-if)#ip address 40.10.10.3/24`	Configure IPv4 address `40.10.10.3` on the interface `xe11`.
`OcNOS(config-if)#ip dhcp relay uplink`	Configure relay uplink on the device connecting the server.
`OcNOS(config-if)#ip dhcp relay server-select dhcp-relay-gp`	Configure relay server-select group name on the device connected to the server.

`OcNOS(config-if)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(config-if)#exit`	Exit interface mode.

Validation

The below shows the running configuration of the DHCPv4 relay agent node:

```
OcNOS#show running-config dhcp
interface eth0
 ip address dhcp
!
!

ip dhcp relay server-group dhcp-relay-gp
 server 10.10.10.2
 server 40.10.10.2
interface xe8
 ip dhcp relay uplink
 ip dhcp relay server-select dhcp-relay-gp
!
interface xe11
 ip dhcp relay uplink
 ip dhcp relay server-select dhcp-relay-gp
!
interface xe15
 ip dhcp relay
!
OcNOS#
OcNOS#
OcNOS#show ip dhcp relay
DHCP relay service is Enabled.
VRF Name: default
  Option 82: Disabled
  Interface               Uplink/Downlink
  ---------               -------------
  xe8                     Uplink
  xe11                    Uplink
  xe15                    Downlink
  Interface               Group-Name              Server
  ---------               -------------           ------
  xe11                    dhcp-relay-gp     10.10.10.2,40.10.10.2
Incoming DHCPv4 packets which already contain relay agent option are FORWARDED
u
nchanged.
OcNOS#
```

DHCP Client Configuration for IPv4

This section shows how to configure the DHCPv4 Client.

DHCPv4 Client

`OcNOS#configure terminal`	Enter configure mode.
`OcNOS(config)#feature dhcp`	Enable the feature DHCP. This will be enabled by default.
`OcNOS(config)#int xe15`	Enter interface mode `xe15`.
`OcNOS(config-if)#ip address dhcp`	The client requests for the IP address to the server, once it receives the acknowledgment from the server, it assigns the IP address to the interface in which this command is enabled.
`OcNOS(config-if)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(config-if)#exit`	Exit interface mode.

Validation

The below shows the running configuration of the DHCPv4 client node:

```
OcNOS#show running-config dhcp
interface eth0
 ip address dhcp
!
interface xe15
 ip address dhcp

OcNOS#show ip interface brief

'*' - address is assigned by dhcp client

Interface            IP-Address      Admin-Status          Link-Status
cd1                  unassigned      up                    down
cd3                  unassigned      up                    down
ce0                  unassigned      up                    down
ce2                  unassigned      up                    down
eth0                *10.12.121.156   up                    up
lo                   127.0.0.1       up                    up
lo.management        127.0.0.1       up                    up
xe4                  unassigned      up                    down
xe5                  unassigned      up                    down
xe6                  unassigned      up                    down
xe7                  unassigned      up                    down
xe8                  unassigned      up                    down
xe9                  unassigned      up                    down
xe10                 unassigned      up                    down
xe11                 unassigned      up                    down
xe12                 unassigned      up                    down
xe13                 unassigned      up                    down
xe14                 unassigned      up                    down
xe15                *20.20.20.1      up                    up
xe16                 unassigned      up                    down
xe17                 unassigned      up                    down
xe18                 unassigned      up                    down
xe19                 unassigned      up                    down
xe20                 unassigned      up                    down
xe21                 unassigned      up                    down
xe22                 unassigned      up                    down
```

```
xe23                  unassigned      up                    down
xe24                  unassigned      up                    down
xe25                  unassigned      up                    down
xe26                  unassigned      up                    down
xe27                  unassigned      up                    down
OcNOS#--
OcNOS#
OcNOS#show ip int xe15 br

'*' - address is assigned by dhcp client

Interface             IP-Address      Admin-Status          Link-Status
xe15                 *20.20.20.1      up                    up
OcNOS#
```

DHCP Server-1 Configuration for IPv6

This section shows how to configure the DHCPv6 Server-1.

DHCPv6 Server-1

`OcNOS#configure terminal`	Enter configure mode.
`OcNOS(config)#ipv6 dhcp server pool DHCPv6-Server-1`	Configure DHCP server group for server in global mode.
`OcNOS(dhcp6-config)#network 2001:: netmask 64`	Configure network `2001::` and netmask `64`.
`OcNOS(dhcp6-config)#address range low-address 2001::1 high-address 2001::124`	Configure address range from `2001::1` to `2001::124`.
`OcNOS(dhcp6-config)#ipv6 dhcp server pool DHCPv6-SER`	Configure DHCP server group for client in global mode.
`OcNOS(dhcp6-config)#network 3001:: netmask 64`	Configure network `3001::` and netmask `64`.
`OcNOS(dhcp6-config)#address range low-address 3001::1 high-address 3001::124`	Configure address range from `3001::1` to `3001::124`.
`OcNOS(dhcp6-config)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(dhcp6-config)#exit`	Exit DHCPv6 config mode.
`OcNOS(config)#interface xe8`	Enter interface mode `xe8`.
`OcNOS(config-if)#ipv6 address 2001::2/64`	Configure IPv6 address `2001::2/64` on the interface `xe8`.
`OcNOS(config-if)#ipv6 dhcp server`	Server should be configured on the interface while connected to the relay.
`OcNOS(config-if)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(config-if)#exit`	Exit interface mode.
`OcNOS(config)#ipv6 route 3001::/64 2001::3`	Configure static route `3001::/64` by next hop interface `2001::3`.
`OcNOS(config)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(config)#exit`	Exit config mode.

Validation

The below shows the running configuration of the DHCPv6 Server-1 node:

```
OcNOS#show running-config dhcp
interface eth0
 ip address dhcp
!
!

ipv6 dhcp server pool DHCPv6-Server-1
 network 2001:: netmask 64
 address range low-address 2001::1 high-address 2001::124
ipv6 dhcp server pool DHCPv6-SER
 network 3001:: netmask 64
 address range low-address 3001::1 high-address 3001::124
interface xe8
 ipv6 dhcp server
!
OcNOS#
```

DHCP Server-2 Configuration for IPv6

This section shows how to configure the DHCPv6 Server-2.

DHCPv6 Server-2

`OcNOS#configure terminal`	Enter configure mode.
`OcNOS(config)#ipv6 dhcp server pool DHCPv6-Server-2`	Configure dhcp server group for server in global mode.
`OcNOS(dhcp6-config)#network 4001:: netmask 64`	Configure network `4001::` and netmask `64`.
`OcNOS(dhcp6-config)#address range low-address 4001::1 high-address 4001::124`	Configure address range from `4001::1` to `4001::124`.
`OcNOS(dhcp6-config)#ipv6 dhcp server pool DHCPv6-SER`	Configure DHCP server group for client in global mode.
`OcNOS(dhcp6-config)#network 3001:: netmask 64`	Configure network `3001::` and netmask `64`.
`OcNOS(dhcp6-config)#address range low-address 3001::1 high-address 3001::124`	Configure address range from `3001::1` to `3001::124`.
`OcNOS(dhcp6-config)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(dhcp6-config)#exit`	Exit DHCPv6 config mode.
`OcNOS(config)#interface xe11`	Enter interface mode `xe11`.
`OcNOS(config-if)#ipv6 address 4001::2/64`	Configure IPv6 address on the interface `xe11`.
`OcNOS(config-if)#ipv6 dhcp server`	Server should be configured on the interface while connected to the relay.
`OcNOS(config-if)#commit`	Commit the candidate configuration to the running configuration.

`OcNOS(config-if)#exit`	Exit interface mode.
`OcNOS(config)#ipv6 route 3001::/64 4001::3`	Configure static route `3001::/64` by next hop interface `4001::3`.
`OcNOS(config)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(config)#exit`	Exit config mode.

Validation

The below shows the running configuration of the DHCPv6 Server-2 node:

```
OcNOS#show running-config dhcp
interface eth0
 ip address dhcp
!
!

ipv6 dhcp server pool DHCPv6-Server-2
 network 4001:: netmask 64
 address range low-address 4001::1 high-address 4001::124
ipv6 dhcp server pool DHCPv6-SER
 network 3001:: netmask 64
 address range low-address 3001::1 high-address 3001::124
interface xe11
 ipv6 dhcp server
!
OcNOS#
```

DHCP Relay Agent Configuration for IPv6

This section shows how to configure the DHCPv6 relay agent.

DHCPv6 Relay Agent

`OcNOS#configure terminal`	Enter configure mode.
`OcNOS(config)#ipv6 dhcp relay server-group dhcpv6-relay-gp`	Configure relay server-group group name in global mode.
`OcNOS(dhcp6-relay-group)#server 2001::2`	Configure server address `2001::2`.
`OcNOS(dhcp6-relay-group)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(dhcp6-relay-group)#exit`	Exit DHCPv6 relay group.
`OcNOS(config)#interface xe8`	Enter interface mode `xe8`.
`OcNOS(config-if)#ipv6 address 2001::3/64`	Configure IPv6 address `2001::3/64` on the interface `xe8`.
`OcNOS(config-if)#ipv6 dhcp relay uplink`	Configure relay uplink on the device connecting the server.
`OcNOS(config-if)#ipv6 dhcp relay server-select dhcpv6-relay-gp`	Configure relay server-select group name on the device connected to the server.
`OcNOS(config-if)#commit`	Commit the candidate configuration to the running configuration.

`OcNOS(config-if)#exit`	Exit interface mode.
`OcNOS(config)#interface xe15`	Enter interface mode.
`OcNOS(config-if)#ipv6 address 3001::2/64`	Configure IPv6 address on the interface `xe15`.
`OcNOS(config-if)#ipv6 dhcp relay`	By default, this will be enabled. This command starts the IPv6 dhcp relay service.
`OcNOS(config-if)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(config-if)#exit`	Exit interface mode.
`OcNOS(config)#ipv6 dhcp relay server-group dhcpv6-relay-gp`	Configure relay server-group group name in global mode.
`OcNOS(dhcp6-relay-group)#server 4001::2`	Configure server address `4001::2`.
`OcNOS(dhcp6-relay-group)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(dhcp6-relay-group)#exit`	Exit DHCPv6 relay group.
`OcNOS(config)#interface xe11`	Enter interface mode.
`OcNOS(config-if)#ipv6 address 4001::3/64`	Configure IPv6 `4001::3/64` address on the interface `xe11`.
`OcNOS(config-if)#ipv6 dhcp relay uplink`	Configure relay uplink on the device connecting the server.
`OcNOS(config-if)#ipv6 dhcp relay server-select dhcpv6-relay-gp`	Configure relay server-select group name on the device connected to the server.
`OcNOS(config-if)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(config-if)#exit`	Exit interface mode.

Validation

The below shows the running configuration of the DHCPv6 relay agent node:

```
OcNOS#show running-config dhcp
interface eth0
 ip address dhcp
!
!

ipv6 dhcp relay server-group dhcpv6-relay-gp
 server 2001::2
 server 4001::2
interface xe8
 ipv6 dhcp relay uplink
 ipv6 dhcp relay server-select dhcpv6-relay-gp
!
interface xe11
 ipv6 dhcp relay uplink
 ipv6 dhcp relay server-select dhcpv6-relay-gp
!
interface xe15
 ipv6 dhcp relay
OcNOS#show ipv6 dhcp relay
```

```
IPv6 DHCP relay service is Enabled.
VRF Name: default
  DHCPv6 IA_PD Route injection: Disabled
  Interface                Uplink/Downlink
  ---------                -------------
  xe8                      Uplink
  xe11                     Uplink
  xe15                     Downlink
  Interface                Group-Name              Server
  ---------                -------------           ------
  xe11                     dhcpv6-relay-gp     2001::2,4001::2
OcNOS#
```

DHCP Client Configuration for IPv6

This section shows how to configure the DHCPv6 client.

DHCPv6 client

`OcNOS#configure terminal`	Enter configure mode.
`OcNOS (config)#feature dhcp`	Enable the feature dhcp. This is enabled by default.
`OcNOS(config)#int xe15`	Enter interface mode `xe15`.
`OcNOS(config-if)#ipv6 address dhcp`	The client requests for the IPv6 address to the server. Once it receives the acknowledgment from the server, it assigns the IPv6 address to the interface in which this command is enabled.
`OcNOS(config-if)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(config-if)#exit`	Exit interface mode.

Validation

The below shows the running configuration of the DHCPv6 client node:

```
OcNOS#show running-config dhcp
interface eth0
 ip address dhcp
!
interface xe15
 ipv6 address dhcp

OcNOS#show ipv6 int br
Interface            IPv6-Address                                    Admin-Sta
tus
cd1                  unassigned                                      [up/down]

cd3                  unassigned                                      [up/down]

ce0                  unassigned                                      [up/down]
```

```
ce2                 unassigned                                [up/down]

eth0                fe80::d277:ceff:fe9f:4500                 [up/up]

lo                  ::1                                       [up/up]

lo.management       ::1                                       [up/up]

xe4                 unassigned                                [up/down]

xe5                 unassigned                                [up/down]

xe6                 unassigned                                [up/down]

xe7                 unassigned                                [up/down]

xe8                 unassigned                                [up/down]

xe9                 unassigned                                [up/down]

xe10                unassigned                                [up/down]

xe11                unassigned                                [up/down]

xe12                unassigned                                [up/down]

xe13                unassigned                                [up/down]

xe14                unassigned                                [up/down]

xe15                *3001::124
                    fe80::d277:ceff:feda:4511                 [up/up]

xe16                unassigned                                [up/down]

xe17                unassigned                                [up/down]

xe18                unassigned                                [up/down]

xe19                unassigned                                [up/down]

xe20                unassigned                                [up/down]

xe21                unassigned                                [up/down]

xe22                unassigned                                [up/down]

xe23                unassigned                                [up/down]

xe24                unassigned                                [up/down]
```

```
xe25                unassigned                                      [up/down]

xe26                unassigned                                      [up/down]

xe27                unassigned                                      [up/down]

OcNOS#
OcNOS#
OcNOS#
OcNOS#
OcNOS#

OcNOS#show ipv6 int xe15 br
Interface           IPv6-Address                                    Admin-Sta
tus
xe15                *3001::124
                    fe80::d277:ceff:feda:4511                       [up/up]
```

New CLI Commands

ip dhcp relay server-group

Use this command to create the DHCP IPv4 server group. This group lists the servers to which DHCP Relay forwards the DHCP client requests.

Use the `no` form of this command to unconfigure the DHCP IPv4 server group.

Command Syntax

```
ip dhcp relay server-group GROUP_NAME
no ip dhcp relay server-group GROUP_NAME
```

Parameters

`GROUP_NAME`	Name of the DHCP server group (specify a maximum 63 alphanumeric characters).

Command Mode

Configure mode and VRF mode. In the configure mode, the DHCP IPv4 server group is created in the default VRF. In the configure-vrf mode, the DHCP IPv4 server group is created in the user-defined VRF.

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The example below shows the creation of DHCP IPv4 server groups.

```
OcNOS(config)#ip vrf vrf1
OcNOS(config-vrf)#ip dhcp relay server-group Group1
OcNOS(dhcp-relay-group)#end
```

```
OcNOS#configure terminal
OcNOS(config)#ip dhcp relay server-group Group2
```

ip dhcp relay server-select

Use this command to attach the DHCP IPv4 server group to the DHCP relay uplink interface.

Use the `no` form of this command to remove the DHCP IPv4 server group attached to the DHCP relay interface.

Note: Attach the groups only to the DHCP relay uplink interfaces.

Command Syntax

```
ip dhcp relay server-select GROUP_NAME
no ip dhcp relay server-select
```

Parameters

`GROUP_NAME`	Name of the DHCP server group (specify a maximum 63 alphanumeric characters).

Command Mode

Interface mode.

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The below example shows attaching the DHCP IPv4 server group to the DHCP relay uplink interface:

```
OcNOS#configure terminal
OcNOS(config)#interface xe1
OcNOS(config-if)#ip dhcp relay server-select group1
```

ipv6 dhcp relay server-group

Use this command to create the DHCP IPv6 server group. This group lists the servers to which DHCP relay forwards the DHCP client requests.

Use the no form of this command to unconfigure the DHCP IPv6 server group.

Command Syntax

```
ipv6 dhcp relay server-group GROUP_NAME
no ipv6 dhcp relay server-group GROUP_NAME
```

Parameters

`GROUP_NAME`	Name of the DHCP server group (specify a maximum of 63 alphanumeric characters).

Command Mode

Configure mode and VRF mode. In the configure mode, the DHCP IPv6 server group is created in the default VRF. In the configure-vrf mode, the DHCP IPv6 server group is created in the user-defined VRF.

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The example below shows the creation of DHCP IPv6 server groups:

```
OcNOS#configure terminal
OcNOS(config)#ip vrf vrf1
OcNOS(config-vrf)#ipv6 dhcp relay server-group Group1
OcNOS(dhcp relay server-group)#end
OcNOS#configure terminal
OcNOS(config)#ipv6 dhcp relay server-group Group2
```

ipv6 dhcp relay server-select

Use this command to attach the DHCP IPv6 group to the DHCP relay uplink interface.

Use the `no` form of this command to remove the DHCP IPv6 group attached to the interface.

Note: Attach the groups only to the DHCP relay uplink interfaces.

Command Syntax

```
ipv6 dhcp relay server-select GROUP_NAME
no ipv6 dhcp relay server-select
```

Parameters

`GROUP_NAME`	Name of the DHCP server group (specify a maximum of 63 alphanumeric characters).

Command Mode

Interface mode.

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The below example shows how to attach the DHCP IPv6 server group to the DHCP relay uplink interface:

```
#configure terminal
(config)#interface xe1
(config-if)#ipv6 dhcp relay server-select group1
```

server A.B.C.D

Use this command to add the DHCP IPv4 servers to the DHCP server group.

Use the `no` form of this command to remove the DHCP IPv4 servers from the DHCP server Group.

Note: A maximum of eight servers can be added to a DHCP group.

Command Syntax

```
server A.B.C.D
no server A.B.C.D
```

Parameters

A.B.C.D	DHCP IPv4 Relay group server address to be added in the DHCP server group.

Command Mode

DHCP Relay Group Mode.

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The below example shows the addition of DHCP IPv4 servers to a DHCP server group:

```
OcNOS#configure terminal
OcNOS(config)#ip vrf vrf1
OcNOS(config-vrf)#ip dhcp relay server-group group
OcNOS(dhcp-relay-group)#server 10.12.23.205
OcNOS(dhcp-relay-group)#end
OcNOS#configure terminal
OcNOS(config)#ip dhcp relay server-group group1
OcNOS(dhcp-relay-group)#server 10.12.33.204
```

server X:X::X:X

Use this command to add the DHCP IPv6 servers to the DHCP server group.

Use the `no` form of this command to remove the DHCP IPv6 servers from the DHCP server group.

Note: A maximum of eight servers can be added to a DHCP group.

Command Syntax

```
server X:X::X:X
no server X:X::X:X
```

Parameters

X:X::X:X	DHCP IPv6 Relay Group server address to be added in the DHCP server group.

Command Mode

DHCPv6 Relay Group Mode.

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The below example shows the addition of DHCP IPv6 servers to a DHCP server group:

```
OcNOS#configure terminal
OcNOS(config)#ip vrf vrf1
OcNOS(config-vrf)#ipv6 dhcp relay server-group group
OcNOS(dhcp6-relay-group)#server 2003::1
OcNOS(dhcp6-relay-group)#end
```

```
OcNOS#configure terminal
OcNOS(config)#ipv6 dhcp relay server-group group1
OcNOS(dhcp-relay-group)#server 2001::1
OcNOS(dhcp6-relay-group)end
```

Abbreviations

The following are some key abbreviations and their meanings relevant to this document:

Acronym	Description
DHCP	Dynamic Host Configuration Protocol
VRF	Virtual Routing and Forwarding

Glossary

The following provides definitions for key terms used throughout this document:

DHCP Client	A DHCP client is a hardware device or software that uses DHCP to get the network configuration information from a DHCP Server. VRF: VRF creates a logically isolated routing table within a single physical network device. Each VRF instance works as an independent routing instance that enables separate network traffic, maintains different routing tables, and provides network isolation.
DHCP Server	A DHCP server is a hardware device or software that leases a dynamic IP address to the DHCP client.
DHCP relay agent	A DHCP relay forwards the request from a DHCP client to the DHCP server group and takes the response from the DHCP server group to the DHCP client.
VRF	VRF creates a logically isolated routing table within a single physical network device. Each VRF instance works as an independent routing instance that enables separate network traffic, maintains different routing tables, and provides network isolation.