# OcNOS®

## Open Compute Network Operating System for Routed Optical Networking Version 6.4.2

Key Features

December 2023

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

# Enhanced Security and Performance

This section, describes the security, performance and authentication enhancements introduced in the Release 6.4.1.

# 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 CLIs introduced in the 6.4.1 release.

The following are the new CLIs introduced to support the NetConf port access control:

- feature netconf-ssh
- feature netconf-tls
- netconf-ssh port
- netconf-tls port
- show netconf server
- show running-config netconf server

The following existing CLI is updated to support the NetConf port access control

- ip access-list tcp|udp

### 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

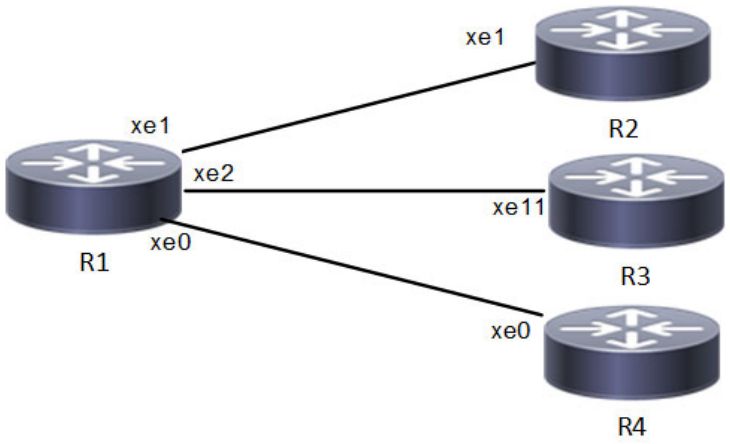
This feature enables the user to control the NetConf port access and change the default port.

## 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

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

# 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.

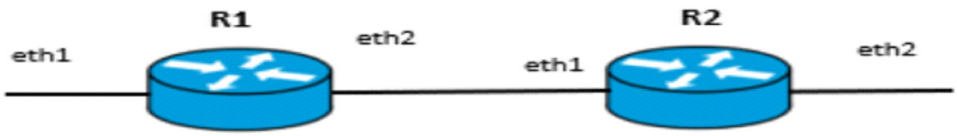
### Benefits

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

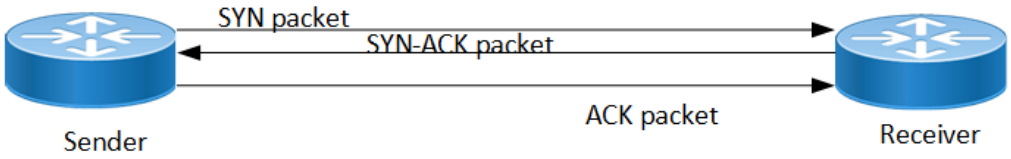
| Acronym | Description |
|---|---|
| ASN | Autonomous System Number |
| EBGP | External Border Gateway Protocol |

# 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.


**TCP MSS for BGP neighbor**

## 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* 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

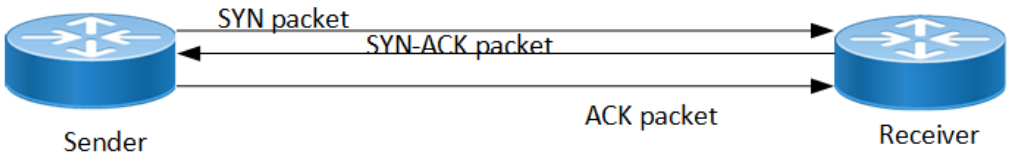
The following provides definitions for key terms used throughout this document.

| | |
|---|---|
| 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.<br>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

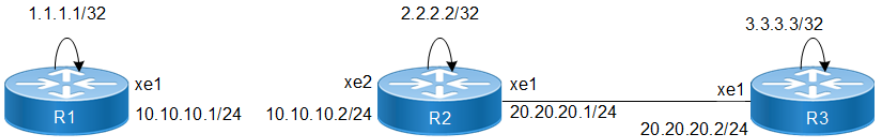
This section shows the procedure to configure TCP MSS for LDP session.

## 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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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. |

# 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
```

Refer to *Authentication, Authorization and Accounting* section in the OcNOS System Management Configuration Guide, Release 6.4.1.

### 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 | Expantion |
|---|---|
| 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 in the *System Management Configuration* guide, Release 6.4.2.

## 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 |

# Improved Network Resilience

This section, describes the failover and error handling enhancements introduced in the Release 6.4.1.

- RSVP Detour Over Ring Topology
- Commit Rollback

# RSVP Detour Over Ring Topology

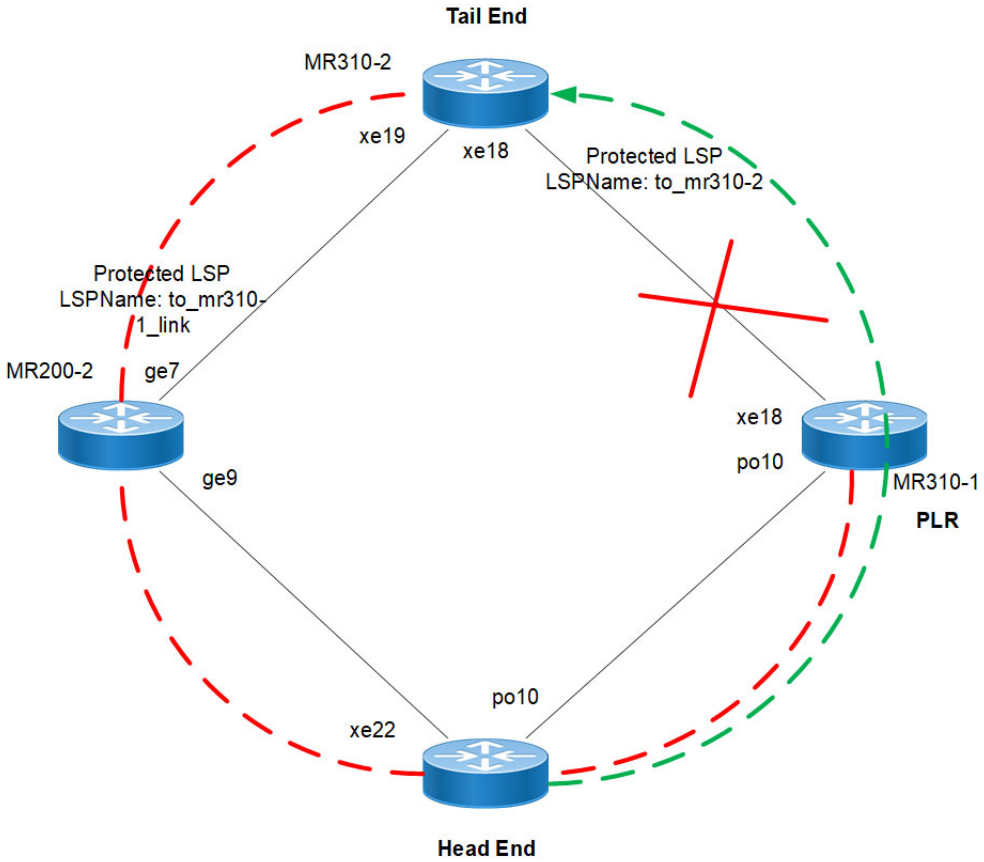
## Overview

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 *Fast Reroute Configuration (one-to-one method)* section of the *RSVP Detour Over Ring Topology* chapter in the *OcNOS Multi-Protocol Label Switching Guide,* Release 6.4.1.

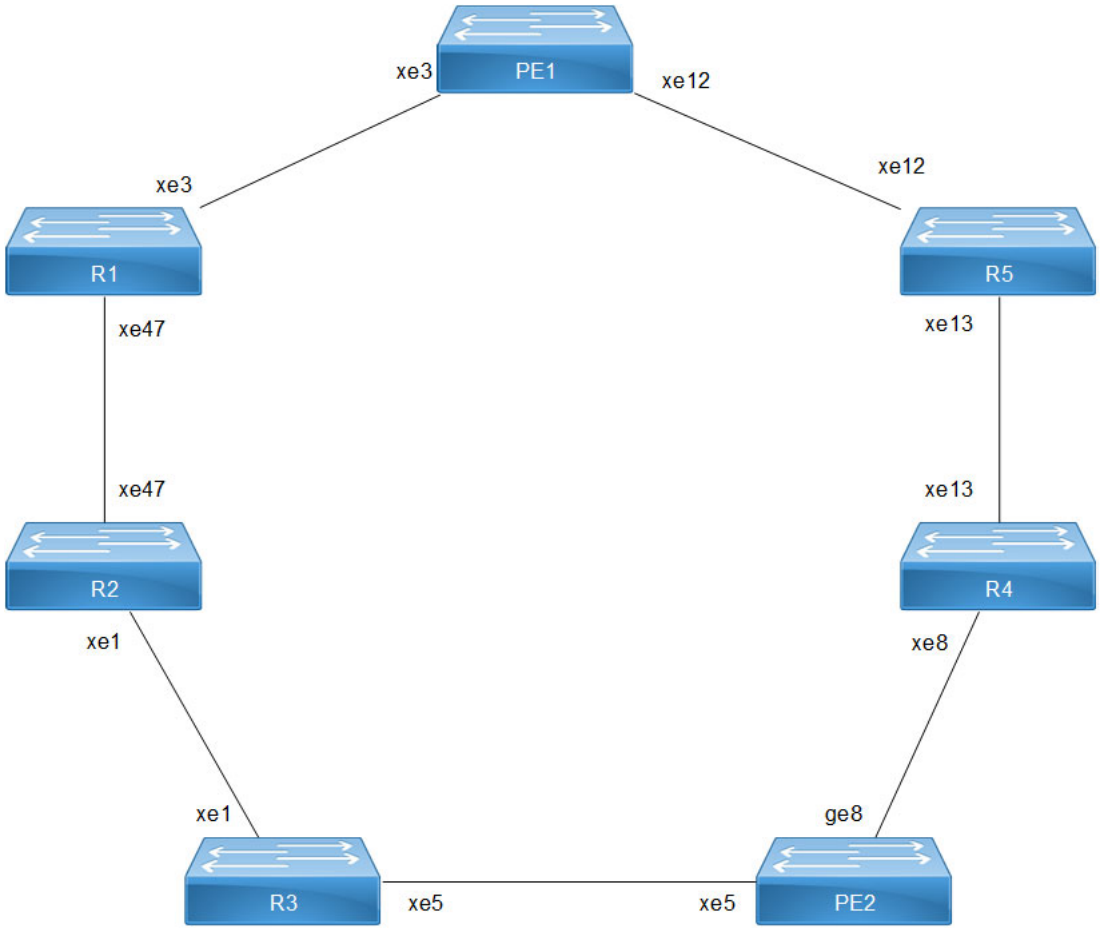
# Configuration

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**

## Configuration

### 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

The below 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

The below 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

The below 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.

### Feature Characteristics

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).*

## Commands for Commit Rollback

For the commands, refer to the *Common Management Layer Commands* section in the *System Management Command Reference guide*.

## Abbreviations

List of key terms used in this document is:

| Term | Description |
|---|---|
| **CMLSH** | Common Management Layer Commands |

# Improved Management

This section, describes the network monitoring and configuration enhancements introduced in the Release 6.4.1.

# 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.

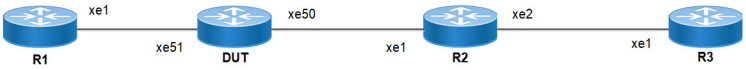



**Figure 1: Route Monitor Topology**

## 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.

# New CLI Commands

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.

### Command Syntax

```
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)#int 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

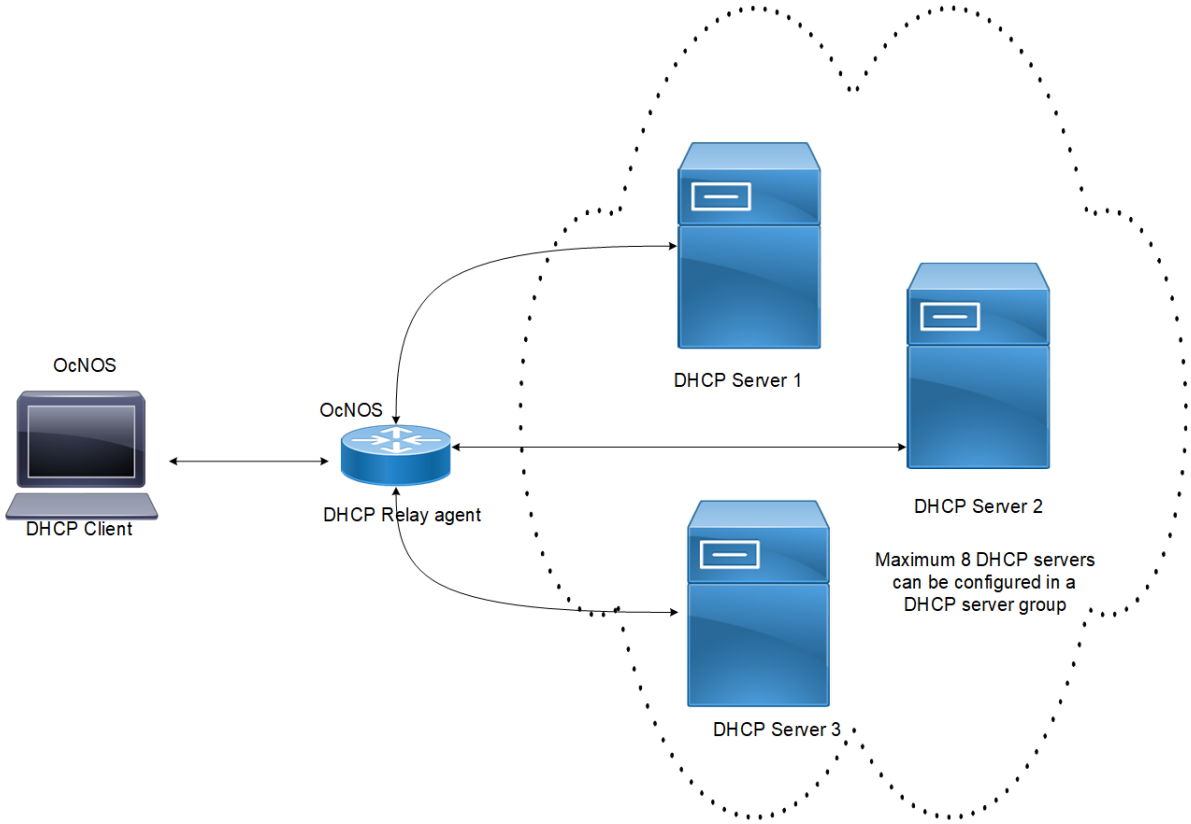
The following provides definitions for key terms used throughout this document.

| | |
|---|---|
| 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

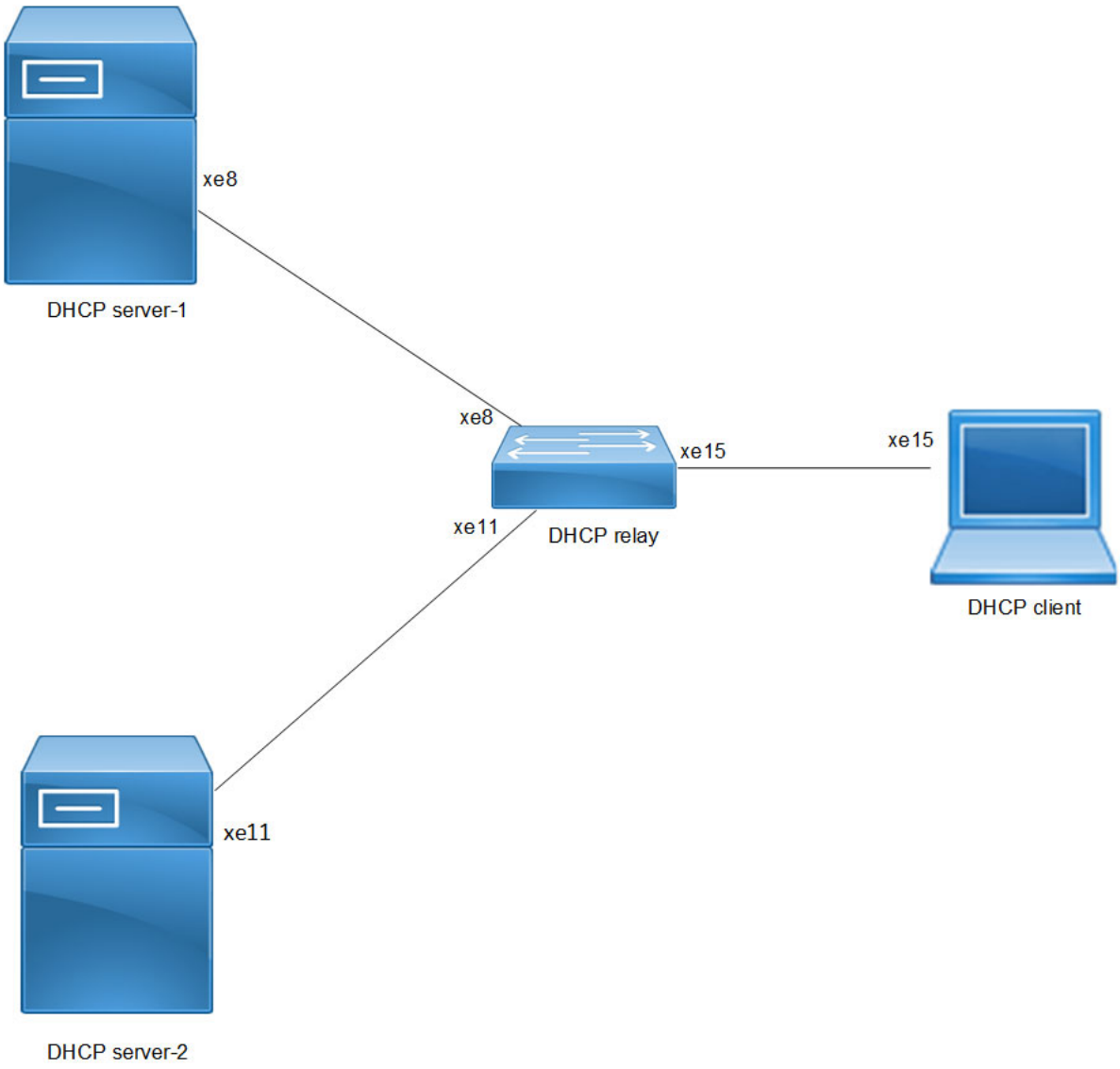
The DHCP relay agent forwards the request message from the DHCP client to multiple DHCP servers in the group. Forwarding the request message to multiple DHCP servers increases the reliability of obtaining the network configuration.

# 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**

## Configuration

### DHCP Client Configuration for IPv4

| | |
|---|---|
| `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 Relay Agent Configuration for IPv4

| | |
|---|---|
| `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 Server-1 Configuration for IPv4

| | |
|---|---|
| `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**

| | |
|---|---|
| `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 Client Configuration for IPv6

| | |
|---|---|
| `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]
```

### DHCP Relay Agent Configuration for IPv6

| | |
|---|---|
| `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 Server-1 Configuration for IPv6

| | |
|---|---|
| `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

| | |
|---|---|
| `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#
```

# 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.<br><br>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. |