Mapping VPN Traffic onto LSPs Using Route Policies

Test Case

February 2017
Version 1.0
Overview

Many enterprise customers are migrating towards using Multiprotocol Label Switching (MPLS) as a core technology for interconnecting data centers. MPLS provides traffic engineering capabilities; the ability to establish logical paths [Label Switched Paths (LSPs)] through the network based on different constraints such as bandwidth, link color, and priority while protecting traffic in the event of link or node failures using fast re-route mechanisms. The enterprise’s IT department can also use the core to offer MPLS based Layer 2 and Layer 3 VPN services to their internal customers (to different company departments) and external partners.

Based on business requirements, you can map traffic flows onto the specific LSPs based on various criteria such as VPN, destination IP address, or class of service (CoS). To explain this functionality, a simplified MPLS lab network was constructed, and different scenarios were configured and tested. After examining the default forwarding behavior of VPN traffic by a provider edge (PE) router, route policies were configured to map specific VPN traffic to specific LSPs, and then modified to map traffic to specific destinations within a VPN to specific LSPs. When the incoming traffic did not match any terms in the route policy, and when the referenced LSP was inactive, additional tests were performed to determine the forwarding behavior.

This document describes the configuration and verifies the functionality of using route policies to place VPN traffic onto specific LSPs.
**Test Network**

Figure 1 shows two data centers (DC1 and DC2) interconnected by a pair of MX Series routers forming an IP/MPLS core. This core network offers the following services:

- Two IP VPNs, “Blue” and “Red”, each with two sites
- One Layer 2 VPLS VPN, “Grey”, with two sites

A single OSPF area is configured to establish connectivity between all core devices and interfaces. Multiprotocol IBGP is configured to exchange Network Layer Reachability Information (NLRI) for the various VPNs within the core with routers 12 and 21 acting as route reflector (RR) servers. Provider edge (PE) routers 11 and 21 have a Layer 3 EBGP connection to customer edge (CE) routers 13 and 23 for the IP VPNs, and Layer 2 connectivity to CEs 14 and 24 for the VPLS service.

RSVP is used in the core to establish the following LSPs from Router 11 to 21:

1. from-11-to-21-fast-1
2. from-11-to-21-fast-2
3. from-11-to-21-slow-3
The “fast” and “slow” represent the relative speed of the links. In this network, the inter-data center WAN link speeds between routers 11 and 21 are faster than the connections between routers 12 and 22 (see Figure 2).

Other LSPs are configured on PE router 21 to enable forwarding of VPN traffic between PEs. However, the focus of the testing is on PE 11 with traffic flows between CE 13 to 23, and CE 14 to 24 that utilize the three LSPs previously listed.

All devices were running Junos OS Release 10.4R3, and all core interfaces were on line cards containing the Trio chipset.
Test Scenarios for Placing VPN Traffic onto LSPs

Default Forwarding Behavior

Initial Configuration

This initial configuration focuses on the portion most relevant to the tests. For additional configuration details for PE 11, see Appendix A – PE 11 Configuration.

Use the `protocols mpls` hierarchy to define the LSPs from PE 11 to PE 21, and their paths:

```
label-switched-path from-11-to-21-fast-1 {
  from 10.0.0.11;
  to 10.0.0.21;
  primary path-11-to-21-1;
}
label-switched-path from-11-to-21-fast-2 {
  from 10.0.0.11;
  to 10.0.0.21;
  primary path-11-to-21-2;
}
label-switched-path from-11-to-21-slow-3 {
  from 10.0.0.11;
  to 10.0.0.21;
  primary path-11-to-21-3;
}
path path-11-to-21-1 {
  10.12.1.21;
}
path path-11-to-21-2 {
  10.12.2.21;
}
path path-11-to-21-3 {
  10.0.0.12;
}
```

Use the `policy-options` hierarchy to create a policy to load-balance traffic, and use the `routing-options` hierarchy to apply the policy:

**Note:** This routing policy is evaluated when routes are exported from the routing table into the forwarding table.

```
policy-statement load-balance-per-packet {
  term 1 {
    then {
      load-balance per-packet;
    }
  }
}
```

```
routing-options {
  router-id 10.0.0.11;
  autonomous-system 64512;
  forwarding-table {
    export load-balance-per-packet;
  }
}
```
Verification

On PE 11, viewing the route in the IP-VPN-Blue table to destination 10.2.231.0/24 on CE 23 shows that there are three equal cost paths as the next-hop towards the destination.

```
user@PE11-re0> show route 10.2.231.0/24 table IP-VPN-Blue

IP-VPN-Blue.inet.0: 15017 destinations, 25027 routes (15017 active, 0 holddown, 0 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both

10.2.231.0/24      *[BGP/170] 04:00:53, localpref 100, from 10.0.0.21
  AS path: 65521 I
      to 10.12.1.21 via xe-2/1/0.0, label-switched-path from-11-to-21-fast-1
      to 10.12.2.21 via xe-2/2/0.0, label-switched-path from-11-to-21-fast-2
    > to 10.1.1.12 via xe-2/0/0.0, label-switched-path from-11-to-21-slow-3
[BGP/170] 04:00:53, localpref 100, from 10.0.0.12
  AS path: 65521 I
      to 10.12.1.21 via xe-2/1/0.0, label-switched-path from-11-to-21-fast-1
      to 10.12.2.21 via xe-2/2/0.0, label-switched-path from-11-to-21-fast-2
    > to 10.1.1.12 via xe-2/0/0.0, label-switched-path from-11-to-21-slow-3
```

Although the output shows that only one of the LSPs as selected (indicated with the > symbol), the forwarding table shows that all three paths are active:

```
user@PE11-re0> show route forwarding-table destination 10.2.231.0/24 table IP-VPN-Blue
Routing table: IP-VPN-Blue.inet
Internet:
  Destination         Type RtRef Next hop          Type Index NhRef Netif
  10.2.231.0/24        user  0                    indr 1048588  3103
                         ulst 1048598     3
                      10.12.1.21  Push 16   801     1 xe-2/1/0.0
                      10.12.2.21  Push 16   880     1 xe-2/2/0.0
                     10.1.1.12  Push 16, Push 300160(top)   881     1 xe-2/0/0.0

The equal cost LSPs are also present in the inet.3 table. The following output shows the paths used to reach the egress PE’s IP address, for this example, PE 21. There are three LSPs with a metric of “1”, and as a result, all of them are used to forward traffic.

```
user@PE11-re0> show route 10.0.0.21 table inet.3 extensive

inet.3: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
Restart Complete
10.0.0.21/32 (1 entry, 1 announced)
  State: <FlashAll>
*RSVP    Preference: 7/1
  Next hop type: Router
  Next-hop reference count: 13
  Next hop: 10.12.1.21 via xe-2/1/0.0 weight 0x1
  Label-switched-path from-11-to-21-fast-1
  Next hop: 10.12.2.21 via xe-2/2/0.0 weight 0x1
  Label-switched-path from-11-to-21-fast-2
  Next hop: 10.1.1.12 via xe-2/0/0.0 weight 0x1, selected
  Label-switched-path from-11-to-21-slow-3
  Label operation: Push 300112
  Label TTL action: prop-ttl
  State: <Active Int>
  Local AS:  64512
```
Using the tester (shown in Figure 3), ten streams were transmitted on the Blue VPN from CE 13 to destination subnet 10.2.231.0/24 on CE 23 with a total rate of 10000 packets/seconds (pps). Monitoring the interface statistics showed that the flows are load-balanced among the three interfaces corresponding to the three LSPs.

Additionally, the MPLS LSP statistics show the active load-balancing behavior:

```
{master}
user@PE11-re0> clear mpls lsp statistics

{master}
user@PE11-re0> show mpls lsp statistics ingress name from-11-to-21-*
Ingress LSP: 9 sessions
To       From          State Packets          Bytes LSPname
10.0.0.21 10.0.0.11    Up     7953   72833574 from-11-to-21-fast-1
10.0.0.21 10.0.0.11    Up     3977   36421366 from-11-to-21-fast-2
10.0.0.21 10.0.0.11    Up     7955   72851890 from-11-to-21-slow-3
Total 3 displayed, Up 3, Down 0
```
Scenario 1 – Mapping VPNs to Specific LSPs

Configuration

In this example, a routing policy is created with traffic flows mapped from DC1 to DC2:

- Layer 2 VPN Grey traffic maps to LSP “from-11-to-21-fast-2”
- Layer 3 VPN Blue traffic maps to LSPs “from-11-to-21-fast-1” and “from-11-to-21-fast-2”
- Layer 3 VPN Red traffic maps to LSP “from-11-to-21-slow-3”

Each VPN is configured using the same VRF target parameter at all locations (see Table 1). This means that PE 21 advertised NLRI information with equivalent targets to PE 11. For additional configuration for each routing instance on PE 11, see Appendix A – PE 11 Configuration.

Table 1 – VPN and VRF Route Target Information

<table>
<thead>
<tr>
<th>VPN</th>
<th>VRF Route Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grey</td>
<td>target:64512:10</td>
</tr>
<tr>
<td>Blue</td>
<td>target:64512:1</td>
</tr>
<tr>
<td>Red</td>
<td>target:64512:2</td>
</tr>
</tbody>
</table>

When creating the route policy, this VRF target information is used as match criteria to uniquely identify the VPN to which the incoming traffic belongs. The action of the route policy is to map the traffic onto a specific LSP(s).

**Note:** For the policy action to take effect, the specified next-hop LSP must be an active and selected path to the destination PE.

Use the policy-options hierarchy to configure the route policy:

```plaintext
policy-statement MapVpnToLsp {
  term 1 {
    from community vpls-grey;
    then {
      install-nexthop lsp from-11-to-21-fast-2;
      accept;
    }
  }
  term 2 {
    from community vpn-blue;
    then {
      install-nexthop lsp [ from-11-to-21-fast-1 from-11-to-21-fast-2 ];
      load-balance per-packet;
      accept;
    }
  }
  term 3 {
    from community vpn-red;
    then {
      install-nexthop lsp from-11-to-21-slow-3;
      accept;
    }
  }
}
```
community vpls-grey members target:64512:10;
community vpn-blue members target:64512:1;
community vpn-red members target:64512:2;

Next, under the routing-options hierarchy, apply this policy to the forwarding-table. This new policy is applied before the existing load-balancing policy so that it is evaluated first. You can use the `insert` command to modify the order, if necessary.

```
user@PE11-re0# show routing-options
forwarding-table {
    export [ MapVpnToLsp load-balance-per-packet ];
}
```

### Verification

First, ten streams of Grey VPLS traffic were transmitted from CE 14 to CE 24. The MPLS LSP statistics show that all traffic maps to the correct LSP “from-11-to-21-fast-2”:

```
user@PE11-re0> show mpls lsp statistics ingress name from-11-to-21*
Ingress LSP: 9 sessions
To        From     State  Packets  Bytes LSPname
10.0.0.21  10.0.0.11 Up      0        0 from-11-to-21-fast-1
10.0.0.21  10.0.0.11 Up   18941   173187412 from-11-to-21-fast-2
10.0.0.21  10.0.0.11 Up      0        0 from-11-to-21-slow-3
Total 3 displayed, Up 3, Down 0
```

Next, ten streams of Blue VPN traffic from CE 13 to CE 23 were transmitted. The MPLS LSP statistics show that traffic maps correctly to the two “fast” LSPs:

```
user@PE11-re0> show mpls lsp statistics ingress name from-11-to-21*
Ingress LSP: 9 sessions
To        From     State  Packets  Bytes LSPname
10.0.0.21  10.0.0.11 Up   15908  145685464 from-11-to-21-fast-1
10.0.0.21  10.0.0.11 Up  23860  218509880 from-11-to-21-fast-2
10.0.0.21  10.0.0.11 Up      0        0 from-11-to-21-slow-3
```

Finally, ten streams of the Red VPN traffic from CE 13 to CE23 were transmitted. The MPLS LSP statistics show that traffic flows map to the “slow” LSP, as expected:

```
user@PE11-re0> show mpls lsp ingress statistics name from-11-to-21-*
Ingress LSP: 9 sessions
To        From     State  Packets  Bytes LSPname
10.0.0.21  10.0.0.11 Up      0        0 from-11-to-21-fast-1
10.0.0.21  10.0.0.11 Up      0        0 from-11-to-21-fast-2
10.0.0.21  10.0.0.11 Up  59652  546293016 from-11-to-21-slow-3
Total 3 displayed, Up 3, Down 0
Scenario 2 – Mapping Specific Destinations to Specific LSPs

Configuration

In this example, PE 21 is configured to advertise, through MP-IBGP in the core, the IP VPN Blue subnets 10.2.231.0/24 and 10.231.0.0/16 with unique VRF targets. The corresponding Blue VRF on PE 11 is configured to accept network prefixes with both of these VRF targets.

On PE 21, configure the “BlueRouteCommAnnounce” policy using the policy-options hierarchy:

```
policy-statement BlueRouteCommAnnounce {
  term 1 {
    from {
      route-filter 10.2.231.0/24 exact;
    }
    then {
      community set vpn-blue;
      accept;
    }
  }
  term 2 {
    from {
      route-filter 10.231.0.0/16 orlonger;
    }
    then {
      community set vpn-blue2;
      accept;
    }
  }
}
community vpn-blue members target:64512:1;
community vpn-blue2 members target:64512:101;
```

On PE 21, the policy is applied as a VRF export policy on the Blue VRF (under the routing-instances hierarchy):

```
IP-VPN-Blue {
  instance-type vrf;
  interface xe-2/0/0.230;
  interface lo0.1;
  route-distinguisher 10.0.0.21:1;
  vrf-export BlueRouteCommAnnounce;
  vrf-target target:64512:1;
  vrf-table-label;
  etc ...
}
```

On PE 11, there are two policies configured under the policy-options hierarchy. The “MapVpnToLsp” policy (used in the previous configuration example) is modified so that the traffic destined to 10.231/16 is mapped to the “slow” LSP. The policy remains applied under the routing-options forwarding-table export configuration (not shown below).

```
policy-statement MapVpnToLsp {
  term 1 {
    from community vpls-grey;
    then {
      install nexthop lsp from-11-to-21-fast-2;
      accept;
    }
  }
}
```
term 2 {
    from community vpn-blue;
    then {
        install-nexthop lsp [ from-11-to-21-fast-1 from-11-to-21-fast-2 ];
        load-balance per-packet;
        accept;
    }
}

term 3 {
    from community [ vpn-blue2 vpn-red ];
    then {
        install-nexthop lsp from-11-to-21-slow-3;
        accept;
    }
}

policy-statement BlueRouteCommAccept {
    term 1 {
        from community [ vpn-blue vpn-blue2 ];
        then accept;
    }
}

community vpls-grey members target:64512:10;
community vpn-blue members target:64512:1;
community vpn-blue2 members target:64512:101;
community vpn-red members target:64512:2;

The second policy, “BlueRouteCommAccept” (shown in the above configuration), accepts routes with both communities into the Blue VRF. This policy is applied as a VRF target import policy on the Blue IP VPN under the routing-instances hierarchy:

IP-VPN-Blue {
    instance-type vrf;
    interface xe-2/0/1.130;
    interface lo0.1;
    route-distinguisher 10.0.0.11:1;
    vrf-import BlueRouteCommAccept;
    etc...}

Verification

First, confirm that each of the routes is received and placed into the Blue VRF with the appropriate community string:

user@PE11-re0> show route 10.2.231.0/24 table IP-VPN-Blue detail | match "10.2.231|Comm"
10.2.231.0/24 (2 entries, 1 announced)
    Communities: target:64512:1
    Communities: target:64512:1

user@PE11-re0> show route 10.231.0.0/16 table IP-VPN-Blue detail | match "10.231.0|Comm"
10.231.0.0/16 (2 entries, 1 announced)
    Communities: target:64512:101
    Communities: target:64512:101
The configured LSP next-hops are reflected in the routing table for the unique destinations:

```
user@PE11-re0> show route 10.2.231.0/24 table IP-VPN-Blue
IP-VPN-Blue.inet.0: 10017 destinations, 20027 routes (10017 active, 0 holddown, 0 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both
10.2.231.0/24       *[BGP/170] 05:07:33, localpref 100, from 10.0.0.21
   AS path: 65521 I
     > to 10.12.1.21 via xe-2/1/0.0, label-switched-path from-11-to-21-fast-1
     to 10.12.2.21 via xe-2/2/0.0, label-switched-path from-11-to-21-fast-2
   [BGP/170] 05:07:33, localpref 100, from 10.0.0.12
   AS path: 65521 I
     > to 10.12.1.21 via xe-2/1/0.0, label-switched-path from-11-to-21-fast-1
     to 10.12.2.21 via xe-2/2/0.0, label-switched-path from-11-to-21-fast-2
[master]
```

```
user@PE11-re0> show route 10.231.0.0/16 table IP-VPN-Blue
IP-VPN-Blue.inet.0: 10017 destinations, 20027 routes (10017 active, 0 holddown, 0 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both
10.231.0.0/16       *[BGP/170] 00:29:36, MED 2, localpref 100, from 10.0.0.21
   AS path: 65521 I
   to 10.1.1.12 via xe-2/0/0.0, label-switched-path from-11-to-21-slow-3
   [BGP/170] 00:29:36, MED 2, localpref 100, from 10.0.0.12
   AS path: 65521 I
   to 10.1.1.12 via xe-2/0/0.0, label-switched-path from-11-to-21-slow-3
```

The tester was configured to send ten traffic streams from CE 13 to ten unique hosts on the 10.2.231.0/24 subnet connected to CE 23. The MPLS LSP statistics confirm that traffic traverses the two “fast” LSPs:

```
user@PE11-re0> show mpls lsp statistics ingress name from-11-to-21*
Ingress LSP: 9 sessions
To          From          State    Packets    Bytes          LSPname
10.0.0.21    10.0.0.11     Up        15907     145676306  from-11-to-21-fast-1
10.0.0.21    10.0.0.11     Up        23861     218519038  from-11-to-21-fast-2
10.0.0.21    10.0.0.11     Up        0         0          from-11-to-21-slow-3
Total 3 displayed, Up 3, Down 0
```

The tester was reconfigured to send traffic from CE 13 to destination 10.231.0.0/16 on CE 23. The MPLS LSP statistics confirm that this traffic traverses the “slow” LSP:

```
user@PE11-re0> show mpls lsp statistics ingress name from-11-to-21*
Ingress LSP: 9 sessions
To          From          State    Packets    Bytes          LSPname
10.0.0.21    10.0.0.11     Up        0         0          from-11-to-21-fast-1
10.0.0.21    10.0.0.11     Up        0         0          from-11-to-21-fast-2
10.0.0.21    10.0.0.11     Up        158509    1451625422  from-11-to-21-slow-3
Total 3 displayed, Up 3, Down 0
```
Additional Tests

Non-matching Traffic

To test the behavior of incoming traffic with a destination that does not match any of the terms in the “MapVpnToLsp” policy, “Term 3” of the policy was temporarily deactivated.

```
user@PE11-re0# deactivate policy-options policy-statement MapVpnToLsp term 3
user@PE11-re0# commit and-quit
```

The routing table for destination 10.231/16 (corresponding to the vpn-blue2 community in the deactivated term), shows that all three LSPs are now available for forwarding to that destination:

```
user@PE11-re0> show route 10.231.0.0
IP-VPN-Blue.inet.0: 15017 destinations, 25027 routes (15017 active, 0 holddown, 0 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both
10.231.0.0/16    *[BGP/170] 01:03:45, MED 2, localpref 100, from 10.0.0.21
    AS path: 65521 I
    > to 10.12.1.21 via xe-2/1/0.0, label-switched-path from-11-to-21-fast-1
    to 10.12.2.21 via xe-2/2/0.0, label-switched-path from-11-to-21-fast-2
    to 10.1.1.12 via xe-2/0/0.0, label-switched-path from-11-to-21-slow-3
etc...
```

When resending the streams in the Red VPN, and streams with destination 10.231/16 in the Blue VPN, traffic was load-balanced among the three LSPs, and ultimately delivered to the destination. This is essentially the default forwarding behavior described in the first section.

```
user@PE11-re0# activate policy-options policy-statement MapVpnToLsp term 3
user@PE11-re0# commit and-quit
```

Forwarding Behavior When LSP is Down

To test the behavior when the LSP, specified as a next-hop in the policy, is down, deactivate the LSP “from-11-to-21-slow-3”.

```
user@PE11-re0# deactivate protocols mpls lsp from-11-to-21-slow-3
user@PE11-re0# commit and-quit
```

The traffic streams corresponding to the Red VPN, and to destination 10.231/16 in the Blue VPN (corresponding to community vpn-blue2 as configured in the policy), were transmitted. Traffic to a given destination subnet took a single path (as shown below). Traffic was not load-balanced as before, and delivered to the destination ultimately. However, traffic to different destinations was load-balanced.

```
user@PE11-re0> show mpls lsp statistics ingress name from-11-to-21-*
Ingress LSP: 8 sessions
To From State    Packets     Bytes    LSPname
10.0.0.21 10.0.0.11 Up  129680  1187609440 from-11-to-21-fast-1
10.0.0.21 10.0.0.11 Up    0            0 from-11-to-21-fast-2
Total 2 displayed, Up 2, Down 0
```
The reason for this is that the “accept” action in “term 3” of the policy is a terminating action. As a result, no load-balancing action is applied to the traffic because the second “load-balance-per-packet” policy is not invoked. To force traffic to a specific destination subnet to be load-balanced, the “load-balance-per-packet” action was added to “term 3” of the policy. Any traffic matching “term 3” was confirmed as being load-balanced.

```
user@PE11-re0# set policy-options policy-statement MapVpnToLsp term 3 then load-balance per-packet
user@PE11-re0# commit and-quit
user@PE11-re0> show mpls lsp statistics ingress name from-11-to-21- *
Ingress LSP: 8 sessions
  To   From            State    Packets            Bytes LSPname
  10.0.0.21  10.0.0.11     Up       133731       1224708498 from-11-to-21-fast-1
  10.0.0.21  10.0.0.11     Up       133732       1224717656 from-11-to-21-fast-2
Total 2 displayed, Up 2, Down 0
```

You can achieve the same result by deleting the “accept” action in “term 3”. Traffic matches “term 3” and the second policy, “load-balance-per-packet”, is applied to the traffic and load-balanced among the two active LSPs. The test for this configuration was successful.

**The “Strict” Option**

In some cases, it may be desirable not to forward traffic when the next-hop LSP specified in the policy is “down”. You can implement this behavior by including the “strict” keyword when configuring the next-hop LSP. This keyword was added to “term 3” of the route policy:

```
policy-statement MapVpnToLsp {
  term 1 {
    from community vpls-grey;
    then {
      install-nexthop lsp from-11-to-21-fast-2;
      accept;
    }
  }
  term 2 {
    from community vpn-blue;
    then {
      install-nexthop lsp [ from-11-to-21-fast-1 from-11-to-21-fast-2 ];
      load-balance per-packet;
      accept;
    }
  }
  term 3 {
    from community [ vpn-blue2 vpn-red ];
    then {  
      install-nexthop strict lsp from-11-to-21-slow-3;  \ include “strict” keyword
      accept;
    }
  }
}
```

The traffic streams corresponding to the Red VPN and to destinations 10.231/16 in the Blue VPN (corresponding to community vpn-blue2 as configured in the policy) were dropped on ingress PE 11, since they matched “term 3” of the route policy.
Appendix A – PE 11 Configuration

This appendix includes CLI configuration code examples used to configure the PE 11 device.

Interfaces Hierarchy

CLI configuration for the interfaces hierarchy:

```
ge-1/0/0 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 10 {
        encapsulation vlan-vpls;
        vlan-id 10;
    }
}

xe-2/0/0 {
    description Core-to-12;
    unit 0 {
        family inet {
            address 10.1.1.11/24;
        }
        family mpls;
    }
}

xe-2/0/1 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 130 {
        vlan-id 130;
        family inet {
            address 10.1.30.11/24;
        }
    }
    unit 150 {
        vlan-id 150;
        family inet {
            address 10.1.50.11/24;
        }
    }
}

xe-2/1/0 {
    description Core-to-21;
    unit 0 {
        family inet {
            address 10.12.1.11/24;
        }
        family mpls;
    }
}

xe-2/2/0 {
    description Core-to-21;
    unit 0 {
        family inet {
            address 10.12.2.11/24;
        }
        family mpls;
    }
```
xe-2/3/0 {
  description Core-to-12;
  mtu 9192;
  unit 0 {
    family inet {
      address 10.1.2.11/24;
    }
    family mpls;
  }
}

lo0 {
  unit 0 {
    family inet {
      address 10.0.0.11/32;
    }
  }
}

Protocols OSPF Hierarchy

CLI configuration for the protocols ospf hierarchy:

protocols {
  ospf {
    traffic-engineering;
    area 0.0.0.0 {
      interface all;
      interface fxp.0 {
        disable
      }
    }
  }
}

Protocols BGP Hierarchy

CLI configuration for the protocols bgp hierarchy:

protocols {
  bgp {
    log-updown;
    local-as 64512;
    group Internal {
      type internal;
      local-address 10.0.0.11;
      family inet-vpn {
        any;
      }
      family l2vpn {
        signaling;
      }
    }
    peer-as 64512;
    neighbor 10.0.0.21;
    neighbor 10.0.0.12;
  }
}
Protocols RSVP Hierarchy

**CLI configuration for the protocols rsvp hierarchy:**

```
protocols {
    rsvp {
        interface all;
        interface fxp0.0 {
            disable;
        }
    }
}
```

Routing Instances Hierarchy

**CLI configuration for the routing-instances hierarchy where two IP VPN instances and the VPLS instance are defined:**

**IP-VPN-Blue**

```
instance-type vrf;
interface xe-2/0/1.130;
route-distinguisher 10.0.0.11:1;
vrf-target target:64512:1;
vrf-table-label;
protocols {
    bgp {
        group EbgpTo13 {
            type external;
            hold-time 20;
            peer-as 65511;
            local-as 64512;
            neighbor 10.1.30.13;
        }
    }
}
```

**IP-VPN-Red**

```
instance-type vrf;
interface xe-2/0/1.150;
route-distinguisher 10.0.0.11:2;
vrf-target target:64512:2;
vrf-table-label;
protocols {
    bgp {
        group EbgpTo13 {
            type external;
            hold-time 20;
            peer-as 65511;
            local-as 64512;
            neighbor 10.1.50.13;
        }
    }
}
```

**VPLS-Grey**

```
instance-type vpls;
vlan-id none;
interface ge-1/0/0.10;
route-distinguisher 10.0.0.11:10;
vrf-target target:64512:10;
```
protocols {
  vpls {
    site-range 100;
    no-tunnel-services;
  }
}