Managing MPLS Networks

The following topics describe how to view and manage aspects of Multiprotocol Label Switching (MPLS) services using the Vision client, including the MPLS service view, business configuration, and maps. The topics also describe the device inventory specific to MPLS VPNs, including routing entities, label switched entities (LSEs), BGP neighbors, Multiprotocol BGP (MP-BGP), VRF instances, pseudowires, and TE tunnels. If you cannot perform an operation that is described in these topics, you may not have sufficient permissions; see Permissions for Managing MPLS Services, page B-17.

- Working with MPLS-TP Tunnels, page 17-6
- Viewing VPNs, page 17-19
- Managing VPNs, page 17-22
- Working with VPN Overlays, page 17-25
- Monitoring MPLS Services, page 17-27
- Configuring VRFs, page 17-61
- Configuring IP Interfaces, page 17-62
- Auto-IP in PN, page 17-62
- Configuring Auto-IP, page 17-62
- Configuring MPLS-TP, page 17-62
- Configuring MPLS-TE, page 17-70
- Configuring MPLS, page 17-70
- Configuring RSVP, page 17-71
- Configuring BGP, page 17-71
- Configuring VRRP, page 17-72
- Configuring Bundle Ethernet, page 17-72

Viewing IPv6 Information (6VPE)

Prime Network supports IPv6 for:
- Gateways, clients, and units using IPv6.
- Communications between VNEs and devices in IPv6 environments, whether the device management IP address is IPv4 or IPv6.
- Polling and notification using the following protocols over IPv6:

Prime Network supports IPv6 for:
Viewing IPv6 Information (6VPE)

- SNMP v1, SNMPv2c, and SNMPv3
- Telnet
- SSHv2
- ICMP
- XML (for Cisco IOS XR devices)
- HTTP (for Cisco UCS and VMware vCenter devices)

- All reports with devices that use IPv6 addresses.
- Fault management, including event processing and service alarm generation.

Prime Network supports correlation and path tracing for:

- 6PE and native IPv6 networks.
- IPv6 BGP address families.
- IPv6 GRE tunnels.

IPv6 VPN over MPLS, also known as 6VPE, uses the existing MPLS IPv4 core infrastructure for IPv6 transport to enable IPv6 sites to communicate over an MPLS IPv4 core network using MPLS label switch paths (LSPs). 6VPE relies on MP-BGP extensions in the IPv4 network configuration on the PE router to exchange IPv6 reachability information. Edge routers are configured to be dual-stacks running both IPv4 and IPv6, and use the IPv4-mapped IPv6 address for IPv6 prefix reachability exchange.

In 6VPE environments, Prime Network supports:

- Modeling of OSPFv3 routes between PE and CE devices.
- IPv6 addresses for BGP neighbors for MP-BGP.
- Correlation and path tracing.

The Vision client displays IPv6 addresses when they are configured on PE and CE routers in the IP interface table. IPv6 addresses are:

- Displayed in the Vision client map pane for IPv6 links.
- Displayed in logical and physical inventory for routing and interface information, including IP, PPP, and High-Level Data Link Control (HDLC).
- Used in Cisco PathTracer to trace paths and present path trace results.
Table 17-1 describes where IPv6 information appears in logical and physical inventory.

**Table 17-1  IPv6 Information in Inventory**

<table>
<thead>
<tr>
<th>Logical Inventory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6rd Tunnels</td>
<td>The Tunnel Edges table displays IPv6 addresses and the IPv6 prefixes that are used to translate IPv4 addresses to IPv6 addresses. For more information, see Viewing 6rd Tunnel Properties, page 17-48.</td>
</tr>
</tbody>
</table>
| Access Lists      | • The Type field displays IPv6 for IPv6 access lists.  
                     • If an IPv6 access list is configured, the Access List Properties window displays IPv6 addresses in the Source, Destination, Source Wildcard, and Destination Wildcard fields. |
| Carrier Grade NAT | Carrier Grade NAT service types include 6rd and XLAT. For more information, see Viewing Carrier Grade NAT Properties in Logical Inventory, page 20-2. |
| GRE Tunnels       | The IP Address field supports IPv6 addresses. For more information, see Viewing MPLS Pseudowire Over GRE Properties, page 26-31. |
| IS-IS             | IS-IS properties support:  
                     • IPv6 address families in the Metrics tab.  
                     • IPv6 addresses in the Neighbors tab and the IS-IS Neighbor Properties window. For more information, see Viewing IS-IS Properties, page 18-129. |
| MPBGP3s           | • IP address family identifiers indicate the BGP peer address family: IPv4, IPv6, Layer 2 VPN, VPNv4, or VPNv6.  
                     • MP-BGP BGP neighbor entries display IPv6 addresses. For information, see Viewing MP-BGP Information, page 17-47. |
| OSPFv3            | IPv6 addresses are displayed for OSPF neighbor interface addresses, OSPF interface internet addresses, OSPF neighbor properties window, and OSPF interface properties window. For more information, see Viewing OSPF Properties, page 18-132. |
| Routing Entities  | • IPv6 addresses appear in the IP Interfaces tab, the IPv6 Routing tab, and the interface properties window.  
                     • IPv6 addresses are displayed in the NDP Table tab and the ARP Entry Properties window.  
                     • VRRP groups using IPv6 display IPv6 addresses in the IP Interfaces Properties window in the VRRP group tab. For more information, see Viewing Routing Entities, page 17-32. |
| VRFs              | IPv6 addresses appear in the IPv6 tab, Sites tab, VRF Properties window, and IP Interface Properties window. For more information, see Viewing VRF Properties, page 17-28. |
The IP addresses that appear depend on whether the interface has only IPv4 addresses, only IPv6 addresses, or both IPv4 and IPv6 addresses, as shown in Table 17-2.

Table 17-2  IP Addresses Displayed in the Interface Table and Properties Window

<table>
<thead>
<tr>
<th>Addresses</th>
<th>Interface Table</th>
<th>Properties Window</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 only</td>
<td>Primary IPv4 address</td>
<td>The primary IPv4 address and any secondary IPv4 addresses.</td>
</tr>
<tr>
<td>IPv6 only</td>
<td>Lowest IPv6 address</td>
<td>All IPv6 addresses.</td>
</tr>
<tr>
<td>IPv6 and IPv4</td>
<td>Primary IPv4 address</td>
<td>All IPv4 and IPv6 addresses.</td>
</tr>
</tbody>
</table>

Note the following when working with IPv6 addresses:

- MPLS label switching entries and Label Switching Entities (LSEs) do not display IPv6 addresses. However, the Neighbor Discovery Protocol (NDP) table does display IPv6 addresses.
- Prime Network supports all the textual presentations of address prefixes. However, the Vision client displays both the IP address and the subnet prefix, for example:
  
  12AB::CD30:123:4567:89AB:CDEF, 12AB:0:0:CD30::/60

Interfaces or subinterfaces that do not have IP addresses are not discovered and therefore are not shown in the Vision client.

Figure 17-1 shows a port inventory view of a port with IPv4 and IPv6 addresses. In this example, one IPv4 address and multiple IPv6 addresses are provisioned on the interface.

- The primary IPv4 address appears in the interface table and properties window. If secondary IPv4 addresses were provisioned on the interface, they would appear in the properties window.
- IPv6 addresses provisioned on the interface appear in the properties window and Sub Interfaces tab.
Figure 17-1 Port with IPv4 and IPv6 Addresses

Figure 17-2 shows a port with only IPv6 addresses provisioned. In this example, the lowest IPv6 address is shown in the subinterface table, and all IPv6 addresses are shown in the interface properties window.

Figure 17-2 Port with IPv6 Addresses
Working with MPLS-TP Tunnels

MPLS-Transport Profile (MPLS-TP) is considered to be the next generation transport for those using SONET/SDH TDM technologies as they migrate to packet-switching technology. Although still under definition by the IETF, MPLS-TP provides:

- Predetermined and long-lived connections.
- Emphasis on manageability and deterministic behavior.
- Fast fault detection and recovery.
- Inband OAM.

MPLS-TP features include:

- Manually provisioned MPLS-TP LSPs.
- Reserved bandwidth for static MPLS-TP LSPs.
- One-to-one path protection for MPLS-TP LSPs.
- Working/Protected LSP switchover.
- Continuity Check (CC), Proactive Continuity Verification (CV), and Remote Defect Indication (RDI) based on BFD.
- New fault OAM functions resulting from the MPLS-TP standardization effort.

Prime Network automatically discovers network MPLS-TP tunnels from end to end, including LSPs, tunnel endpoints, and bandwidth. Network LSPs contain LSP endpoints and midpoints and are identified as working or protected.

Prime Network links the MPLS-TP tunnel components appropriately, provides a visual representation in Vision client maps, and displays the properties in logical inventory.

Prime Network employs warm start technology when rebooting. That is, when rebooting, Prime Network compares existing MPLS-TP tunnel information to topology changes that occur while Prime Network is down and updates MPLS-TP tunnel accordingly when Prime Network returns to operation.

The following options are available for working with MPLS-TP tunnels in the Vision client:

- Adding an MPLS-TP Tunnel, page 17-7
- Viewing MPLS-TP Tunnel Properties, page 17-9
- Viewing LSPs Configured on an Ethernet Link, page 17-13
- Viewing LSP Endpoint Redundancy Service Properties, page 17-15
- Applying an MPLS-TP Tunnel Overlay, page 17-17
- Viewing BFD Session Properties, page 17-49.
Adding an MPLS-TP Tunnel

Prime Network automatically discovers MPLS-TP tunnels, endpoints, and midpoints and enables you to add MPLS-TP tunnels to maps.

To add an MPLS-TP tunnel to a map:

**Step 1**
In the Vision client, display the map to which you want to add the MPLS-TP tunnel.

**Step 2**
Do either of the following:

- From the File menu, choose **Add to Map > MPLS-TP Tunnel**.
- In the main toolbar, click **Add to Map**, then choose **Add to Map > MPLS-TP Tunnel**.

The Add MPLS-TP Tunnel dialog box is displayed.

**Step 3**
Do either of the following:

- Choose a search category, enter a search string, then click **Go** to narrow search results to a range of MPLS-TP tunnels or a specific MPLS-TP tunnel. Search categories include:
  - Description
  - Name
  - System Name
- Choose **Show All** to display all the MPLS-TP tunnels.

**Step 4**
Select the MPLS-TP tunnel that you want to add to the map.

**Step 5**
Click **OK**.

The MPLS-TP tunnel is added to the map and to the navigation pane.

In **Figure 17-3**:

- The devices are on the left side of the map, and the MPLS-TP tunnel is displayed in a thumbnail on the right.
- The devices are connected to each other and to the MPLS-TP tunnel via tunnels.
- Physical links connect the devices to the Working and Protected LSPs.
- A redundancy service badge is displayed next to the Protected LSP in the navigation and map panes.
- In the thumbnail:
  - The tunnel endpoints are connected to each other via a tunnel.
  - A physical link connects the Working and Protected LSPs.
  - Business links connect the Working and Protected LSPs to each endpoint.
If an LSP is in lockout state, it is displayed with the lock badge ( ).

By expanding all aggregations in the MPLS-TP tunnel (see Figure 17-4), you can see components and links in the MPLS-TP tunnel, including:

- MPLS-TP tunnel endpoints
- LSP endpoints
- LSP midpoints

If an LSP is configured for redundancy service, a redundancy service badge is applied to the secondary (backup) LSP in the navigation and map panes in the navigation and map panes.
For more information about LSP redundancy service, see Viewing LSP Endpoint Redundancy Service Properties, page 17-15.

Viewing MPLS-TP Tunnel Properties

Prime Network discovers and displays MPLS-TP attributes in the MPLS-TP branch in logical inventory as described in this topic.

Additional information about MPLS-TP tunnel properties are available in the following branches:

- Pseudowires—See Viewing Pseudowire End-to-End Emulation Tunnels, page 17-57.

To view MPLS-TP tunnel properties:

**Step 1** Right-click the required device in the Vision client and choose **Inventory**.

**Step 2** In the logical inventory window, choose **Logical Inventory > MPLS-TP > MPLS-TP Global**.

The routing information is displayed as shown in Figure 17-5.

*Figure 17-5  MPLS-TP Tunnel Properties in Logical Inventory*

Table 17-3 describes the information that is available for MPLS-TP tunnels. The information that is displayed depends on the configuration.
### Table 17-3  MPLS-TP Tunnel Properties in Logical Inventory

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global ID</td>
<td>Globally unique Attachment Interface Identifier (AII) for MPLS-TP derived from the Autonomous System Number (ASN) of the system hosting the PEs.</td>
</tr>
<tr>
<td>Router ID</td>
<td>MPLS-TP source node identifier for this element in the form of an IPv4 address.</td>
</tr>
<tr>
<td>Protection Mode</td>
<td>Whether the transmitting endpoint is in revertive or nonrevertive mode:</td>
</tr>
<tr>
<td></td>
<td>- Revertive—If the protection mode is revertive and a failed path is restored, the traffic automatically returns, or reverts, to the original path.</td>
</tr>
<tr>
<td></td>
<td>- Nonrevertive—If the protection mode is nonrevertive and a failed path is restored, the traffic does not return to the original path. That is, the traffic does not revert to the original path.</td>
</tr>
<tr>
<td>Redundancy Mode</td>
<td>Level of redundancy for the MPLS-TP tunnel: 1:1, 1+1, or 1:N.</td>
</tr>
<tr>
<td><strong>MPLS-TP Tunnel Endpoints Tab</strong></td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Tunnel endpoint identifier as a Tunnel-tp interface on the selected network element.</td>
</tr>
<tr>
<td>Tunnel ID</td>
<td>Unique tunnel identifier.</td>
</tr>
<tr>
<td>Admin Status</td>
<td>Administrative status of the tunnel: Up or Down.</td>
</tr>
<tr>
<td>Oper Status</td>
<td>Operational status of the tunnel: Up or Down.</td>
</tr>
<tr>
<td>Bandwidth (kbps)</td>
<td>Configured bandwidth (in Kb/s) for the tunnel.</td>
</tr>
<tr>
<td>Description</td>
<td>Tunnel description.</td>
</tr>
<tr>
<td><strong>TP Enabled Links Tab</strong></td>
<td></td>
</tr>
<tr>
<td>Link ID</td>
<td>Identifier assigned to the MPLS-TP interface.</td>
</tr>
<tr>
<td>Interface</td>
<td>Hyperlink to the interface in physical inventory.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>IP address of the next hop in the path.</td>
</tr>
<tr>
<td><strong>LSP End Points Tab</strong></td>
<td></td>
</tr>
<tr>
<td>LSP ID</td>
<td>LSP identifier, derived from both endpoint identifiers and using the format src-node-ID::src-tunnel-number::dest-node-ID::dest-tunnel-number where:</td>
</tr>
<tr>
<td></td>
<td>- src-node-ID represents the identifier of the node originating the signal exchange.</td>
</tr>
<tr>
<td></td>
<td>- src-tunnel-number represents source tunnel identifier.</td>
</tr>
<tr>
<td></td>
<td>- dest-node-ID represents the identifier of the target node.</td>
</tr>
<tr>
<td></td>
<td>- dest-tunnel-number represents the destination tunnel identifier.</td>
</tr>
<tr>
<td>LSP Type</td>
<td>Indicates whether the LSP is active (Working) or backup (Protect).</td>
</tr>
<tr>
<td>In Label</td>
<td>Incoming label identifier.</td>
</tr>
<tr>
<td>Out Label</td>
<td>Outgoing label identifier.</td>
</tr>
<tr>
<td>Out Interface</td>
<td>Outgoing interface hyperlinked to the relevant entry in physical inventory.</td>
</tr>
<tr>
<td>Bandwidth (kbps)</td>
<td>Bandwidth specification in Kb/s.</td>
</tr>
<tr>
<td>Role (Oper Status)</td>
<td>Role of the LSP endpoint (Active or Standby) with the operational status (UP or DOWN).</td>
</tr>
</tbody>
</table>
Chapter 17  Managing MPLS Networks

Working with MPLS-TP Tunnels

Step 3

To view additional MPLS-TP tunnel endpoint properties, double-click the required entry in the MPLS-TP Tunnel Endpoints table.

The MPLS-TP Tunnel Properties window is displayed as shown in Figure 17-6.
Table 17-4 describes the information available in the top portion of the MPLS-TP Tunnel Properties window. For information about the tabs that are displayed, see Table 17-3.

**Table 17-4  MPLS-TP Tunnel Properties Window**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel ID</td>
<td>Unique tunnel identifier.</td>
</tr>
<tr>
<td>Peer Tunnel ID</td>
<td>Unique identifier of peer tunnel.</td>
</tr>
<tr>
<td>Bandwidth (kbps)</td>
<td>Configured bandwidth (in Kb/s) for the tunnel.</td>
</tr>
<tr>
<td>Admin Status</td>
<td>Administrative status of the tunnel: Up or Down.</td>
</tr>
<tr>
<td>Oper Status</td>
<td>Operational status of the tunnel: Up or Down.</td>
</tr>
<tr>
<td>Local Info</td>
<td>MPLS-TP source node identifier for this element in the form of an IPv4 address.</td>
</tr>
<tr>
<td>Peer Info</td>
<td>MPLS-TP peer node identifier in the form of an IPv4 address.</td>
</tr>
<tr>
<td>Global ID</td>
<td>Globally unique Attachment Interface Identifier (AII) for MPLS-TP derived from the Autonomous System Number (ASN) of the system hosting the PEs.</td>
</tr>
<tr>
<td>Peer Global ID</td>
<td>Globally unique AII for the peer.</td>
</tr>
<tr>
<td>Working LSP Number</td>
<td>Number assigned to the working LSP. By default, the working LSP number is 0 and the protected LSP number is 1.</td>
</tr>
<tr>
<td>Protect LSP Number</td>
<td>Number assigned to the protected LSP. By default, the working LSP number is 0 and the protected LSP number is 1.</td>
</tr>
<tr>
<td>BFD Template</td>
<td>BFD template associated with this MPLS-TP tunnel.</td>
</tr>
</tbody>
</table>
Viewing LSPs Configured on an Ethernet Link

A single Ethernet link can support a number of LSPs. The Vision client enables you to view all LSPs on a single Ethernet link and to identify the source and destination labels.

To view LSPs configured on an Ethernet link:

**Step 1** In the map view, right-click the required link and choose Properties.

**Step 2** In the link properties window, choose the required Ethernet link.

The link properties window refreshes and displays the Labels button as shown in Figure 17-7.

**Figure 17-7  Link Properties Window with All Labels Button**

**Step 3** Click Labels.
The All Labels window is displayed as shown in Figure 17-8 with the LSP sources and destinations.

**Figure 17-8  All Labels Table**

<table>
<thead>
<tr>
<th>Source</th>
<th>In Label</th>
<th>Out Label</th>
<th>Destination</th>
<th>In Label</th>
<th>Out Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.25.106.252</td>
<td>111</td>
<td>111</td>
<td>172.25.106.110</td>
<td>111</td>
<td>111</td>
</tr>
<tr>
<td>172.25.106.252</td>
<td>115</td>
<td>115</td>
<td>172.25.106.110</td>
<td>111</td>
<td>111</td>
</tr>
<tr>
<td>172.25.106.252</td>
<td>121</td>
<td>121</td>
<td>172.25.106.110</td>
<td>111</td>
<td>111</td>
</tr>
<tr>
<td>172.25.106.252</td>
<td>127</td>
<td>127</td>
<td>172.25.106.110</td>
<td>111</td>
<td>111</td>
</tr>
<tr>
<td>172.25.106.252</td>
<td>130</td>
<td>130</td>
<td>172.25.106.110</td>
<td>111</td>
<td>111</td>
</tr>
<tr>
<td>172.25.106.252</td>
<td>139</td>
<td>139</td>
<td>172.25.106.110</td>
<td>111</td>
<td>111</td>
</tr>
<tr>
<td>172.25.106.252</td>
<td>145</td>
<td>145</td>
<td>172.25.106.110</td>
<td>111</td>
<td>111</td>
</tr>
<tr>
<td>172.25.106.252</td>
<td>153</td>
<td>153</td>
<td>172.25.106.110</td>
<td>111</td>
<td>111</td>
</tr>
<tr>
<td>172.25.106.252</td>
<td>155</td>
<td>155</td>
<td>172.25.106.110</td>
<td>111</td>
<td>111</td>
</tr>
<tr>
<td>172.25.106.252</td>
<td>161</td>
<td>161</td>
<td>172.25.106.110</td>
<td>111</td>
<td>111</td>
</tr>
<tr>
<td>172.25.106.252</td>
<td>165</td>
<td>165</td>
<td>172.25.106.110</td>
<td>111</td>
<td>111</td>
</tr>
<tr>
<td>172.25.106.252</td>
<td>170</td>
<td>170</td>
<td>172.25.106.110</td>
<td>111</td>
<td>111</td>
</tr>
<tr>
<td>172.25.106.252</td>
<td>178</td>
<td>178</td>
<td>172.25.106.110</td>
<td>111</td>
<td>111</td>
</tr>
<tr>
<td>172.25.106.252</td>
<td>190</td>
<td>190</td>
<td>172.25.106.110</td>
<td>111</td>
<td>111</td>
</tr>
<tr>
<td>172.25.106.252</td>
<td>205</td>
<td>205</td>
<td>172.25.106.110</td>
<td>111</td>
<td>111</td>
</tr>
<tr>
<td>172.25.106.252</td>
<td>209</td>
<td>209</td>
<td>172.25.106.110</td>
<td>111</td>
<td>111</td>
</tr>
<tr>
<td>172.25.106.252</td>
<td>209</td>
<td>209</td>
<td>172.25.106.110</td>
<td>111</td>
<td>111</td>
</tr>
<tr>
<td>172.25.106.252</td>
<td>231</td>
<td>231</td>
<td>172.25.106.110</td>
<td>111</td>
<td>111</td>
</tr>
<tr>
<td>172.25.106.252</td>
<td>232</td>
<td>232</td>
<td>172.25.106.110</td>
<td>111</td>
<td>111</td>
</tr>
<tr>
<td>172.25.106.252</td>
<td>232</td>
<td>232</td>
<td>172.25.106.110</td>
<td>111</td>
<td>111</td>
</tr>
</tbody>
</table>

**Step 4** To identify a specific path, click an outgoing label in the Source table. The corresponding in label is selected in the Destination table.

**Viewing MPLS-TE and P2MP-MPLS-TE links in a map**

Using the link filter available in Prime Network, you can view only the MPLS-TE and P2MP-MPLS-TE links in a map.

**Note**

The MPLS Point-to-Multipoint Traffic Engineering (P2MP TE) feature enables you to forward Multiprotocol Label Switching (MPLS) traffic from one source to multiple destinations.

To view the MPLS-TE and P2MP-MPLS-TE links in a map:

**Step 1** Open the required map.

**Step 2** Click the Link filter icon in the navigation menu.

**Step 3** In the Link Filter window, select the **MPLS-TE** and **P2MP MPLS-TE** check boxes.

**Step 4** Click **OK**. The map refreshes and displays only the **MPLS-TE** and **P2MP MPLS-TE** links.

**Step 5** Right-click on the link and choose the **Properties** option.
Step 6 In the Link Properties window, the type of link is displayed in the Link Type field, which can be either MPLS-TE and P2MP MPLS-TE based on the link that you have selected. Additional details about the link such as the MPLS TE tunnel, operational status of the tunnel, TE tunnel type are displayed in the Label Switching section. For more information about the Link Properties window, see Viewing LSPs Configured on an Ethernet Link, page 17-13.

Viewing LSP Endpoint Redundancy Service Properties

If an LSP endpoint in an MPLS-TP tunnel is configured for redundancy service, a redundancy service badge is applied to the secondary (backup) LSP endpoint in the navigation and map panes in the Vision client. Additional redundancy service details are provided in the LSP endpoint properties window and the inventory window for the element on which the MPLS-TP tunnel is configured.

To view LSP endpoint redundancy service properties:

Step 1 To determine if an LSP endpoint on an MPLS-TP tunnel is configured for redundancy service, expand the required MPLS-TP tunnel in the navigation or map pane.

If the LSP endpoint is configured for redundancy service, the redundancy service badge is displayed in the navigation and map panes as shown in Figure 17-9.

Figure 17-9 LSP Endpoint with Redundancy Service Badge

Step 2 To view properties for the LSP endpoint, navigate to and right-click the required endpoint in the map or navigation pane, and choose Properties.

The LSP endpoint properties window is displayed as shown in Figure 17-10.
Table 17-5 describes the information displayed in the LSP Endpoint Properties window.

Table 17-5  LSP Endpoint Properties Window

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSP Type</td>
<td>Indicates whether the LSP is active (Working) or backup (Protected).</td>
</tr>
<tr>
<td>LSP ID</td>
<td>LSP identifier, derived from both endpoint identifiers and using the format</td>
</tr>
<tr>
<td></td>
<td>src-node-ID::src-tunnel-number::dest-node-ID::dest-tunnel-number where:</td>
</tr>
<tr>
<td></td>
<td>• src-node-ID represents the identifier of the node originating the signal</td>
</tr>
<tr>
<td></td>
<td>exchange.</td>
</tr>
<tr>
<td></td>
<td>• src-tunnel-number represents source tunnel identifier.</td>
</tr>
<tr>
<td></td>
<td>• dest-node-ID represents the identifier of the target node.</td>
</tr>
<tr>
<td></td>
<td>• dest-tunnel-number represents the destination tunnel identifier.</td>
</tr>
<tr>
<td>In Label</td>
<td>Incoming label identifier.</td>
</tr>
<tr>
<td>Out Label</td>
<td>Outgoing label identifier.</td>
</tr>
<tr>
<td>Bandwidth (kbps)</td>
<td>Bandwidth specification in Kb/s.</td>
</tr>
<tr>
<td>Out Link ID</td>
<td>Link identifier assigned to the outgoing interface.</td>
</tr>
<tr>
<td>Out Interface</td>
<td>Outgoing interface hyperlinked to the relevant entry in physical inventory.</td>
</tr>
<tr>
<td>Role (Oper Status)</td>
<td>Role of the LSP endpoint (Active or Standby) with the operational status (UP</td>
</tr>
<tr>
<td></td>
<td>or DOWN)</td>
</tr>
</tbody>
</table>

Step 3  To view LSP endpoint redundancy status in inventory, double-click the element on which the MPLS-TP tunnel is configured.

Step 4  Choose Logical Inventory > MPLS-TP > MPLS-TP Global > LSP End Points.

Step 5  The LSP End Points tab contains the following information related to LSP redundancy service (see Figure 17-11):

• Whether the LSP endpoint is Working or Protected.
• The LSP endpoint role, either Active or Standby.
• The operational status of the LSP endpoint, either Up or Down.
Applying an MPLS-TP Tunnel Overlay

You can select and display an overlay of a specific MPLS-TP tunnel on top of the devices displayed in a map view. The overlay is a snapshot of the network that visualizes the flows between the sites and tunnel peers. When an MPLS-TP tunnel is selected in the map, the following elements are highlighted in the map:

- Elements on which TP endpoints and LSPs are configured.
- Links that carry TP traffic.

All elements and links that are not part of the MPLS-TP tunnel are dimmed.

To apply an MPLS-TP tunnel overlay:

**Step 1** In the Vision client, display the network map on which you want to apply an overlay.

**Step 2** From the main toolbar, click **Choose Overlay Type** and choose **MPLS-TP tunnel**.

The Select MPLS-TP tunnel Overlay dialog box is displayed.

**Step 3** Do one of the following:

- Choose a search category, enter a search string, then click **Go** to narrow the search results to a range of MPLS-TP tunnels or a specific MPLS-TP tunnel. Search categories include:
  - Description
  - Name
  - System Name
The search condition is “contains.” Search strings are case-insensitive. For example, if you choose the Name category and enter “net,” the Vision client displays MPLS-TP tunnels that have “net” in their names whether net appears at the beginning of the name, the middle, or at the end: for example, Ethernet.

- Choose **Show All** to display all MPLS-TP tunnels.

**Step 4** Select the MPLS-TP tunnel overlay you want to apply to the map.

The elements and links used by the selected MPLS-TP tunnel are highlighted in the network map, and the MPLS-TP tunnel name is displayed in the window title bar as shown in Figure 17-12.

*Figure 17-12  MPLS-TP Tunnel Overlay*

---

**Note**

An overlay is a snapshot taken at a specific point in time and does not reflect changes that occur in the service. As a result, the information in an overlay can become stale. To update the overlay, click **Refresh Overlay** in the main toolbar.
**Viewing VPNs**

Figure 17-13 shows a VPN displayed in the Vision client map view. In this example, the VPN is selected in the navigation pane, so the VPN details, such as virtual routers and IP interfaces, are not shown in the map view.

![Figure 17-13: VPN in Vision Map](image)

1. VPN in the navigation tree
2. Sites
3. Virtual routers
4. VPN in the map view
5. VPN links
Figure 17-14 shows a VPN with details, including virtual routers and sites, in the Vision client map view.

**Figure 17-14  VPN in Vision Map with VRFs and Sites**

1. Virtual routers
2. Sites

The Vision client navigation pane displays the VPN business elements in a tree-and-branch representation. Each business element is represented by an icon in a color that reflects the highest alarm severity. The icon might also have a management state badge or alarm. For more information about icon severity colors and badges, see Interpreting the Badges and Colors of an NE, page 11-8.
Table 17-6 shows the VPN icons in the Vision client map view.

The highest level of the navigation pane displays the root or map name. The branches display the VPN and aggregated business elements as well as their names. The Layer 3 VPN sub-branch displays the virtual routers and sites contained in the VPN along with the names of the business elements. In addition, CE devices can be displayed in the Layer 2 and Layer 3 VPN sub-branches. If you select an aggregated business element in the navigation pane, the map view displays the business elements contained within the aggregated business element.

The Vision client map view displays the VPN business elements and aggregated business elements loaded in the map view, along with the names of the business elements. In addition, the map view displays the VPN topology (between the virtual routers in the VPNs) and the topology and associations between other business elements. After you select the root in the navigation pane, the map view displays all the VPNs.

The Vision client presents tickets related to the map in the ticket area, which allows you to view and manage the VPN tickets.

### Viewing Additional VPN Properties

The Vision client allows you to select any element in the navigation pane or map view and view additional underlying properties. To view additional properties for an object, either double-click it or right-click it and choose **Properties.** Table 17-7 shows the additional properties available for VPN entities.

<table>
<thead>
<tr>
<th>Object</th>
<th>Option</th>
<th>For Additional Information</th>
</tr>
</thead>
</table>
| VPN    | • Double-click a VPN to view the participating VRFs, sites, and network elements in the navigation pane and map view.  
• Right-click a VPN and choose **Properties** to view the VPN Properties window. | Viewing VPN Properties, page 17-27 |
| VRF    | Double-click a VRF to view the VRF properties window. | Viewing VRF Properties, page 17-28 |

### Table 17-6 VPN Icons in Vision Map

<table>
<thead>
<tr>
<th>Icon Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root (map name) or aggregation</td>
</tr>
<tr>
<td>VPN</td>
</tr>
<tr>
<td>Virtual router</td>
</tr>
<tr>
<td>Site</td>
</tr>
</tbody>
</table>
Creating a VPN

You can change business configurations by manually creating VPNs. The VPNs that are manually created do not contain virtual routers and sites.

To create a VPN:

Step 1  In the Vision client navigation pane, select the map root.

Step 2  From the File menu, choose Add to Map > VPN > New.

Step 3  In the Create VPN dialog box, enter the following:

- Name—A unique name for the new VPN.

Note  VPN business element names are case sensitive.

- Icon—To use a custom icon for the VPN, click the button next to the Icon field and navigate to the icon file.

Note  If a path is not specified to an icon, the default VPN icon is used (for more information about icons, see Table 17-6 on page 17-21).

- Description—(Optional) An additional VPN description.

Step 4  Click OK.

The new VPN is added to the VPN list in the Add VPN dialog box.
For more information about loading the newly created VPN in the service view map, see Adding a VPN to a Map, page 17-23.

Adding a VPN to a Map

You can add a VPN to a map view if the VPN was previously created by a user or discovered by Prime Network and are not currently displayed in the map.

Note

Adding a VPN affects other users if they are working with the same map.

To add an existing VPN to a map:

Step 1
In the Vision client, display the map to which you want to add the VPN.

Step 2
Do either of the following:

- From the File menu, choose Add to Map > VPN > Existing.
- In the main toolbar, click Add to Map, then choose Add to Map > VPN > Existing.

The Add VPN dialog box is displayed.

Step 3
Do either of the following:

- Choose a search category, enter a search string, then click Go to narrow search results to a range of VPNs or a specific VPN. Search categories include:
  - Description
  - Name

  The search condition is “contains.” Search strings are case-insensitive. For example, if you choose the Name category and enter “net,” the Vision client displays VPNs that have “net” in their names whether at the beginning of the name, the middle, or the end.

- Choose Show All to display all the VPNs.

Step 4
Select the VPN that you want to add to the map.

Tip
Press Shift or Ctrl to choose multiple adjoining or nonadjoining VPNs.

Step 5
Click OK.

The VPN is displayed in the navigation pane and the selected map or subnetwork in the Vision client window content pane. In addition, any tickets are displayed in the ticket area.

When a VPN service is added to a map, then a new link is available between the ethernet flow point that represents the pseudowire headend port and the site in the VPN to which it is connected.

If your network has a L3VPN connected to a pseudowire via a PWHe, then EVC will also include the L3VPN in the EVC that contains the pseudowire.
Removing a VPN from a Map

You can remove one or more VPNs from the current active map. This change does not affect other maps. Removing a VPN from a map does not remove it from the Prime Network database. The VPN will appear in the Add VPN dialog box, so you can add it back to the map at any time.

When removing VPNs from maps, keep the following in mind:

- Removing a VPN affects other users if they are working with the same map view.
- This option does not change the business configuration or database.
- You cannot remove virtual routers or sites from the map without removing the VPN.

To remove a VPN, in the Vision client pane or map view, right-click the VPN and choose **Remove from Map**.

The VPN is removed from the map view along with all VPN elements, such as connected CE devices. Remote VPNs (extranets) are not removed.

**Note**

If the routing information changes after an overlay is applied, the changes do not appear in the current overlay. Click **Refresh Overlay** to update the routing information.

Moving a Virtual Router Between VPNs

You can move a virtual router (including its sites) from one VPN to another after you create a VPN and add it to the service view map.

**Note**

Moving a virtual router moves all of its sites as well.

To move a virtual router:

1. In the Vision client navigation pane or map, right-click the virtual router and choose **Edit > Move selected**.
2. Right-click the required VPN in the navigation pane or map to where you want to move the virtual router and choose **Edit > Move here**.

**Caution**

Moving a virtual router from one VPN to another affects all users who have the virtual router loaded in their service view map.

The virtual router and its sites are displayed under the selected VPN in the navigation pane and in the map.
Working with VPN Overlays

The following topics describe:

- Applying VPN Overlays, page 17-25
- Managing a VPN Overlay Display in the Map View, page 17-26
- Displaying VPN Callouts in a VPN Overlay, page 17-26

Applying VPN Overlays

You can select and display an overlay of a specific VPN on top of the devices displayed in a map view. The overlay is a snapshot of the network that visualizes the flows between the sites and tunnel peers. When one network VPN is selected in the network map, the PE routers, MPLS routers, and physical links that carry the LSP used by the VPN are highlighted in the network map. All the devices and links that are not part of the VPN are dimmed.

The VPN service overlay allows you to isolate the parts of a network that are being used by a particular service. This information can then be used for troubleshooting. For example, the overlay can highlight configuration or design problems when bottlenecks occur and all the site interlinks use the same link.

To apply a VPN overlay:

Step 1  In the Vision client, display the network map on which you want to apply an overlay.

Step 2  From the main toolbar, click Choose Overlay Type and choose VPN.

The Select VPN Overlay dialog box is displayed.

Step 3  Do one of the following:

- Choose a search category, enter a search string, then click Go to narrow the search results to a range of VPNs or a specific VPN. Search categories include:
  - Description
  - Name

  The search condition is “contains.” Search strings are case-insensitive. For example, if you choose the Name category and enter “net,” the Vision client displays VPNs that have “net” in their names whether net appears at the beginning of the name, the middle, or at the end: for example, Ethernet.

- Choose Show All to display all the VPNs.

Step 4  Select the VPN overlay that you want to apply to the map.

The PE routers, MPLS routers, and physical links used by the selected VPN are highlighted in the network map. The VPN name is displayed in the title of the window.

Note  An overlay is a snapshot taken at a specific point in time and does not reflect changes that occur in the service. As a result, the information in an overlay can become stale. To update the overlay, click Refresh Overlay in the main toolbar.
Managing a VPN Overlay Display in the Map View

After a VPN overlay is applied to a map, you can manage its display by using the overlay tools in the main toolbar:

- To display the overlay, click **Show Overlay** on the main toolbar.
- To hide an active overlay, click **Hide Overlay** on the main toolbar.

**Note**  The Show Overlay button is a toggle. When clicked, the overlay is displayed. When clicked again, the overlay is hidden.

- To remove the VPN overlay, choose **Show Overlay Type > None**.

Displaying VPN Callouts in a VPN Overlay

You can display or hide the callouts for VPN links displayed in a VPN overlay to show the details of the sites that are interlinked through the selected links. The callouts (see **Figure 17-15**) enable you to view the VPN traffic links for a specific link (either bidirectional or unidirectional).

**Note**  The link must be displayed in the VPN overlay and not dimmed for you to display the link callouts.

**Figure 17-15  Callouts Window**

1. **Link details and direction.** In this example, the link is from P-North to PE-West.
2. **Details of the sites using the link and interlinks.** In this example, the site PE-88 is linked to site PE-West.
3. **Details of sites using the link and interlinks.** In this example, the site PE-West is linked to all sites on PE-South.
4. **Link details and the direction.** In this example, the link is from PE-West to P-North.
To display or hide the callouts:

**Step 1**  In the Vision client window, display the map view with the VPN overlay.
**Step 2**  Right-click the required link in the map view and choose **Show Callouts**.
**Step 3**  To hide the callouts, right-click the link in the map view that is displaying the callouts and choose **Hide Callouts**.

### Monitoring MPLS Services

The following topics provide details for viewing MPLS services and technologies:

- Viewing VPN Properties, page 17-27
- Viewing Site Properties, page 17-28
- Viewing VRF Properties, page 17-28
- Viewing VRF Egress and Ingress Adjacents, page 17-32
- Viewing Routing Entities, page 17-32
- Viewing Label Switched Entity Properties, page 17-41
- Viewing MP-BGP Information, page 17-47
- Viewing BFD Session Properties, page 17-49
- Viewing Cross-VRF Routing Entries, page 17-56
- Viewing Pseudowire End-to-End Emulation Tunnels, page 17-57
- Viewing MPLS TE Tunnel Information, page 17-59

### Viewing VPN Properties

To view the properties of a VPN:

**Step 1**  In the Vision client navigation pane or map view, do either of the following:
- If the VPN icon is of the largest size, click the **Properties** button.
- Right-click the VPN and choose **Properties**.

The VPN Properties window displays the following information:

- Name—Name of the VPN.
- ID—Unique identifier assigned to the VPN.

**Step 2**  Click **Close** to close the VPN Properties dialog box.
Viewing Site Properties

The Vision client enables you to view site properties, including the interfaces that are configured on the PE device. The displayed properties reflect the configuration that Prime Network automatically discovered for the device.

To view site properties, in the Vision client navigation pane or map view, right-click the required site and choose Properties.

Table 17-8 describes the information that is displayed in the Router IP Interface Properties window:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the site, such as FastEthernet4/1.252.</td>
</tr>
<tr>
<td>State</td>
<td>Interface state, either Up or Down.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the interface.</td>
</tr>
<tr>
<td>Mask</td>
<td>Network mask.</td>
</tr>
<tr>
<td>Interface Description</td>
<td>Description applied to the interface.</td>
</tr>
<tr>
<td>Associated Entity</td>
<td>Element and interface associated with the site, hyperlinked to its entry in physical inventory.</td>
</tr>
</tbody>
</table>

**Addresses Table**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet</td>
<td>IP address and subnet mask.</td>
</tr>
</tbody>
</table>

**Note** If the site is an IPv6 VPN over MPLS with IPv6 addresses provisioned, the IPv6 addresses are displayed. For more information, see Viewing IPv6 Information (6VPE), page 17-1.

| Type    | Address type, such as Primary, Secondary, or IPv6 Unicast. |

Viewing VRF Properties

The Vision client enables you to view VRF properties, including the VRF route distinguisher, import and export route targets, and any provisioned sites and VRF routes.

To view VRF properties, do either of the following in map view:

- Double-click the element configured for VRFs.
- Expand the required VPN and double-click the virtual router.
The VRF properties window is displayed as shown in Figure 17-16.

**Figure 17-16  VRF Properties**

![VRF Properties Window](image)

The VRF Properties window contains the VRF routing table for the device. The table is a collection of routes that are available or reachable to all the destinations or networks in the VRF. The forwarding table also contains MPLS encapsulation information.

Table 17-9 describes the information displayed in the VRF Properties window.

> **Note** The VRF Properties window only displays properties and attributes that are provisioned in the VRF. You might not see all the fields and tabs described in Table 17-9.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Distinguisher</td>
<td>Route distinguisher configured in the VRF.</td>
</tr>
<tr>
<td>Name</td>
<td>VRF name.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the VRF.</td>
</tr>
<tr>
<td><strong>IPv4 Tab</strong></td>
<td></td>
</tr>
<tr>
<td>Export Route Targets</td>
<td>IPv4 export route targets contained by the VRF.</td>
</tr>
<tr>
<td>Import Route Targets</td>
<td>IPv4 import route targets contained by the VRF.</td>
</tr>
<tr>
<td>Route Maps</td>
<td>Route maps for the VRF.</td>
</tr>
</tbody>
</table>
### Table 17-9 VRF Properties (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Tab</td>
<td></td>
</tr>
<tr>
<td>Export Route Targets</td>
<td>IPv6 export route targets contained by the VRF.</td>
</tr>
<tr>
<td>Import Route Targets</td>
<td>IPv6 import route targets contained by the VRF.</td>
</tr>
<tr>
<td>Route Maps</td>
<td>Route maps for the VRF.</td>
</tr>
<tr>
<td>Routing Tables</td>
<td></td>
</tr>
<tr>
<td>Destination</td>
<td>Destination of the specific network.</td>
</tr>
<tr>
<td>Prefix Length</td>
<td>Length of the network prefix in bits.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>Next routing hop.</td>
</tr>
<tr>
<td>Outgoing Interface</td>
<td>Name of the outgoing interface; displayed if the Routing Protocol type is local.</td>
</tr>
<tr>
<td>Type</td>
<td>Route type: Direct (local), Indirect, or Static.</td>
</tr>
<tr>
<td>Routing Protocol</td>
<td>Routing protocol used to communicate with the other sites and VRFs: BGP or local.</td>
</tr>
<tr>
<td>BGP Next Hop</td>
<td>Border Gateway Protocol (BGP) next hop. This is the PE address from which to continue to get to a specific address. This field is empty when the routing entry goes to the CE.</td>
</tr>
<tr>
<td>Bottom In Label</td>
<td>Innermost label that is expected when MPLS traffic is received.</td>
</tr>
<tr>
<td>Bottom Out Label</td>
<td>Innermost label sent with MPLS traffic.</td>
</tr>
<tr>
<td>Outer Label</td>
<td>Outermost or top label in the stack used for MPLS traffic.</td>
</tr>
<tr>
<td>MRoute_Table</td>
<td></td>
</tr>
<tr>
<td>Source Address</td>
<td>The source IP address from where the multicast information is sent.</td>
</tr>
<tr>
<td>Group Address</td>
<td>The group IP address of the multicast.</td>
</tr>
<tr>
<td>Flags</td>
<td>The flag information pertaining to the multicast.</td>
</tr>
<tr>
<td>Up Time</td>
<td>The amount of time the interface has been active.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The protocol information, which can be 4 or 6.</td>
</tr>
<tr>
<td>Sites Tab</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Site name.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the interface.</td>
</tr>
<tr>
<td>Mask</td>
<td>Subnet mask.</td>
</tr>
<tr>
<td>State</td>
<td>State of the subinterface: Up or Down.</td>
</tr>
<tr>
<td>Associated Entity</td>
<td>Element and interface associated with the site, hyperlinked to its entry in physical inventory.</td>
</tr>
<tr>
<td>Description</td>
<td>Interface description.</td>
</tr>
<tr>
<td>Input Access List</td>
<td>Access list applied to the inbound traffic.</td>
</tr>
<tr>
<td>Output Access List</td>
<td>Access list applied to the outbound traffic.</td>
</tr>
</tbody>
</table>
Chapter 17  Managing MPLS Networks

Monitoring MPLS Services

Table 17-9  VRF Properties (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate Limits</td>
<td>If a rate limit is configured on an IP interface, the limit is shown as an IP interface property. This option is checked when a rate limit is defined on the IP interface, meaning the access list is a rate limit access list. IP interface traffic is measured and includes the average rate, normal burst size, excess burst size, conform action, and exceed action.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Double-clicking a row displays the properties of the IP interface. When a rate limit is configured on the IP interface, the Rate Limits tab is displayed. For more information about rate limits, see Viewing Rate Limit Information, page 17-38.</td>
</tr>
</tbody>
</table>

| IP Sec Map Name       | IP Security (IPsec) map name. |
| Site Name             | Name of the business element to which the interface is attached. |

Viewing VRF Multicast Configuration details

To view global multicast configuration details for a VRF:

**Step 1**  Right-click on the required device and select **Inventory**.

**Step 2**  In the **Inventory** window, choose **Logical Inventory > VRFs > vrf** (where *vrf* is the required VRF) > **IPV4VRF Multicast Configuration** or **IPV6VRF Multicast Configuration**. The route policies configured on the device are displayed in the content pane.

Table 17-10 describes the information that is displayed in the Router IP Interface Properties window:

Table 17-10  Global Multicast Configuration Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN ID</td>
<td>The VPN ID configured for the VRF.</td>
</tr>
<tr>
<td>RoutePolicy</td>
<td>The name of the multicast route policy.</td>
</tr>
<tr>
<td>BgpAD</td>
<td>The BgpAd enabled on the device.</td>
</tr>
<tr>
<td>MdtSourceif</td>
<td>The Multicast Distribution Tree (MDT) source interface.</td>
</tr>
<tr>
<td>MdtPartitioned</td>
<td>The MDT partitioned permission.</td>
</tr>
<tr>
<td>NSF</td>
<td>The non-stop forwarding (NSF) information configured for the VRF.</td>
</tr>
<tr>
<td>MdtAddress</td>
<td>The MDT address.</td>
</tr>
<tr>
<td>MdtData</td>
<td>The MDT data that can be handled.</td>
</tr>
<tr>
<td>Address Family</td>
<td>The address family, which can be IPV4 or IPV6.</td>
</tr>
<tr>
<td>RP Address</td>
<td>The rendezvous point (RP) address configured for the VRF.</td>
</tr>
</tbody>
</table>
Viewing VRF Egress and Ingress Adjacents

The Vision client enables you to view the exporting and importing neighbors by displaying the VRF egress and ingress adjacents. In addition, you can view the connectivity between the VRFs for the route targets and view their properties. For example, if VRF A retrieved route target import X, you can view all VRFs that export X as a route target whether it is in the same or another VPN.

To display the VRF egress and ingress adjacents, you can use either an element configured for VRFs or a virtual router:

- To use an element configured for VRFs:
  a. Double-click the element configured for VRFs.
  b. In the Inventory window, choose Logical Inventory > VRFs > vrf where vrf is the required VRF.
  c. Right-click the required VRF and choose Show VRF Egress Adjacents or Show VRF Ingress Adjacents.

- To use a virtual router, right-click the required VRF in the navigation pane, and choose Show VRF Egress Adjacents or Show VRF Ingress Adjacents.

Table 17-11 describes the information displayed in the Adjacents window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>VRF name.</td>
</tr>
<tr>
<td>Route Distinguisher</td>
<td>Route distinguisher configured in the VRF.</td>
</tr>
<tr>
<td>VRF V6 Table</td>
<td>IPv6 route distinguisher if IPv6 is configured.</td>
</tr>
</tbody>
</table>

Viewing Routing Entities

To view routing entities:

**Step 1** Right-click the required device in the Vision client and choose Inventory.

**Step 2** In the logical inventory window, choose Logical Inventory > Routing Entities > Routing Entity.

The routing information is displayed as shown in Figure 17-17.
Table 17-12 describes the information that is displayed in the Routing Entity table.

Table 17-12  Routing Entity Table

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the routing entity.</td>
</tr>
</tbody>
</table>

### IP Interfaces Tab

<table>
<thead>
<tr>
<th>Name</th>
<th>Site name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>IP address of the interface.</td>
</tr>
<tr>
<td>Mask</td>
<td>Network mask.</td>
</tr>
<tr>
<td>State</td>
<td>State of the subinterface: Up or Down.</td>
</tr>
<tr>
<td>Associated Entity</td>
<td>Interface associated with the routing entity, hyperlinked to its location in physical inventory.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the interface.</td>
</tr>
<tr>
<td>Input Access List</td>
<td>If an input access list is assigned to an IP interface, the list is shown as an IP interface property, and a hyperlink highlights the related access list in the Access List table. When an access list is assigned to the inbound traffic on an IP interface, the actions assigned to the packet are performed.</td>
</tr>
</tbody>
</table>
Monitoring MPLS Services

Chapter 17      Managing MPLS Networks

Table 17-12 Routing Entity Table (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRRP Group</td>
<td>If a VRRP group is configured on an IP interface, the information is shown as an IP interface property. This option is checked when a rate limit is defined on the IP interface.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Double-clicking a row displays the properties of the IP interface. When a VRRP group is configured on an IP interface, the VRRP Groups tab is displayed in the IP Interface Properties window. For more information, see Viewing VRRP Information, page 17-39.</td>
</tr>
<tr>
<td>Output Access List</td>
<td>If an output access list is assigned to an IP interface, the list is shown as an IP interface property, and a hyperlink highlights the related access list in the Access List table. When an access list is assigned to the outbound traffic on an IP interface, the actions assigned to the packet are performed.</td>
</tr>
<tr>
<td>Rate Limits</td>
<td>If a rate limit is configured on an IP interface, the limit is shown as an IP interface property. This option is checked when a rate limit is defined on the IP interface, meaning the access list is a rate limit access list. IP interface traffic is measured and includes the average rate, normal burst size, excess burst size, conform action, and exceed action.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Double-clicking a row displays the properties of the IP interface. When a rate limit is configured on the IP interface, the Rate Limits tab is displayed. For more information, see Viewing Rate Limit Information, page 17-38.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The Input Access, Output Access, and Rate Limits parameters apply only to certain operating systems, such as Cisco IOS.</td>
</tr>
<tr>
<td>IP Sec Map Name</td>
<td>IP Security (IPsec) crypto map name.</td>
</tr>
<tr>
<td>Site Name</td>
<td>Name of the business element to which the interface is attached.</td>
</tr>
</tbody>
</table>

### IPv4 and IPv6 Routing Table Tabs

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Destination of the specific network.</td>
</tr>
<tr>
<td>Outgoing If Name</td>
<td>Name of the outgoing interface.</td>
</tr>
<tr>
<td>Type</td>
<td>Routing type: Direct, Indirect, Static, Other, Invalid, or Unknown.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>IP address from which to continue to get to a specific address. This field is empty when the routing entry goes to a PE router.</td>
</tr>
<tr>
<td>Prefix Length</td>
<td>Length of the network prefix in bits.</td>
</tr>
<tr>
<td>Route Protocol Type</td>
<td>Routing protocol used to communicate with other routers.</td>
</tr>
</tbody>
</table>

### IPv4 and IPv6 Multicast Routing Tabs

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>The source IP address from where the multicast information is sent.</td>
</tr>
<tr>
<td>Group Address</td>
<td>The group IP address of the multicast.</td>
</tr>
<tr>
<td>Flags</td>
<td>The flag information pertaining to the multicast.</td>
</tr>
<tr>
<td>Up Time</td>
<td>The amount of time the interface has been active.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The protocol information, which can be 4 or 6.</td>
</tr>
</tbody>
</table>

### IPv4 and IPv6 BGP Label Routing Table Tabs

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Destination of the specific network.</td>
</tr>
</tbody>
</table>
Monitoring MPLS Services

Viewing IPv4 Label in BGP Routes

The labeled BGP IPv4 (RFC 3107) enables BGP to distribute MPLS label along the routes it advertises. The label mapping information for a particular route is added in the same BGP update message that is used to distribute the route itself. The label mapping information is carried as a part of the Network Layer Reachability Information (NLRI) in the multiprotocol extension attributes. Hence, the use of any other label distribution protocol is eliminated.

The outer label again identifies the LSP and the inner label identifies the MPLS service. In this case, the RFC 3107 edge device replaces the outer label with two labels, generating a three-label stack.

In Prime Network, the IPv4 BGP Label Routing table displays incoming and outgoing labels. Path tracer follows a service that relies on RFC 3107 and it reflects the BGP label in the MPLS label stack.

RFC3107 is supported on the following device types: ASR9K, ASR901, ASR903, and ME3600/3800X.

To view the BGP label information:

**Step 1** Double-click the required element in the Vision client.

**Step 2** Choose Logical Inventory > Routing Entities > Routing Entity.

**Step 3** In the IPv4 BGP Label Routing table, view the details of incoming and outgoing labels.

Table 17-13 describes the information in the IPv4 BGP Label Routing Table tab.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix Length</td>
<td>Length of the network prefix in bits</td>
</tr>
<tr>
<td>Next Hop</td>
<td>Next routing hop</td>
</tr>
<tr>
<td>Incoming Label</td>
<td>Incoming BGP label identifier</td>
</tr>
<tr>
<td>Outgoing Interfaces</td>
<td>Name of the outgoing interface</td>
</tr>
<tr>
<td>Outgoing label</td>
<td>Outgoing label for the network.</td>
</tr>
<tr>
<td>Type</td>
<td>Route type: Direct (local), Indirect, or Static</td>
</tr>
<tr>
<td>Routing Protocol</td>
<td>Routing protocol used to communicate with the other sites: BGP</td>
</tr>
</tbody>
</table>

Table 17-13 IPv4 BGP Label Routing Table Properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Destination of the specific network</td>
</tr>
<tr>
<td>Prefix Length</td>
<td>Length of the network prefix in bits</td>
</tr>
<tr>
<td>Next Hop</td>
<td>Next routing hop</td>
</tr>
<tr>
<td>Incoming Label</td>
<td>Incoming BGP label identifier</td>
</tr>
<tr>
<td>Outgoing Interfaces</td>
<td>Name of the outgoing interface</td>
</tr>
<tr>
<td>Outgoing label</td>
<td>Outgoing label for the network.</td>
</tr>
</tbody>
</table>
Viewing the ARP Table

To view the ARP table:

**Step 1** Right-click the required device in the Vision client and choose **Inventory**.

**Step 2** In the logical inventory window, choose **Logical Inventory > Routing Entities > Routing Entity > ARP**.

Table 17-14 describes the information that is displayed in the ARP table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Route type: Direct (local), Indirect, or Static</td>
</tr>
<tr>
<td>Routing Protocol</td>
<td>Routing protocol used to communicate with the other sites: BGP</td>
</tr>
</tbody>
</table>

**Table 17-14  ARP Table**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC</td>
<td>Interface MAC address.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface name.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Interface IP address.</td>
</tr>
<tr>
<td>State</td>
<td>Interface state:</td>
</tr>
<tr>
<td></td>
<td>• Dynamic—The entry was learned by the device according to network traffic.</td>
</tr>
<tr>
<td></td>
<td>• Static—The entry was learned by a local interface or from a user</td>
</tr>
<tr>
<td></td>
<td>configuring a static route.</td>
</tr>
<tr>
<td></td>
<td>• Other—The entry was learned by another method not explicitly defined.</td>
</tr>
<tr>
<td></td>
<td>• Invalid—In SNMP, this type is used to remove an ARP entry from the table.</td>
</tr>
</tbody>
</table>

Viewing the NDP Table

Neighbor Discovery Protocol (NDP) is used with IPv6 to discover other nodes, determine the link layer addresses of other nodes, find available routers, and maintain reachability information about the paths to other active neighbor nodes.

NDP functionality includes:

- Router discovery
- Autoconfiguration of addresses (stateless address autoconfiguration [SLAAC])
- IPv6 address resolution (replaces Address Resolution Protocol [ARP])
- Neighbor reachability (neighbor unreachability detection [NUD])
- Duplicate address detection (DAD)
- Redirection
To view the NDP table:

**Step 1**  
Right-click the required device in the Vision client and choose **Inventory**.

**Step 2**  
In the logical inventory window, choose **Logical Inventory > Routing Entities > Routing Entity > ARP Entity**.

**Step 3**  
Click the **NDP Table** tab.

*Figure 17-18* shows an example of the NDP Table tab.

*Figure 17-18  NDP Table in Logical Inventory*

![NDP Table in Logical Inventory](image)

Table 17-15 describes the information displayed for NDP.

**Table 17-15**  Describes the Information Displayed for NDP

<table>
<thead>
<tr>
<th>NDP</th>
<th>Interface</th>
<th>IP Address</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:22:90:6F:2C:00</td>
<td>GigabitEthernet1/2</td>
<td>10.0.0.22/24</td>
<td>State</td>
</tr>
<tr>
<td>00:22:90:6F:2C:00</td>
<td>GigabitEthernet1/2</td>
<td>2001:db8:10:0:0:0:3</td>
<td>State</td>
</tr>
</tbody>
</table>
To view rate limit information:

**Step 1** Right-click the required element in the Vision client and choose **Inventory**.

**Step 2** In the logical inventory window, choose **Logical Inventory > Routing Entities > Routing Entity**.

**Step 3** In the IP Interfaces tab, double-click the required interface to view the IP interface properties. If a rate limit is configured on the IP interface, the Rate Limits tab is displayed.

---

**Note** Rate Limit information applies only to certain operating systems, such as Cisco IOS.
Table 17-16 describes the information that is displayed in the Rate Limits tab of the IP Interface Properties dialog box.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Rate limit direction, either Input or Output.</td>
</tr>
<tr>
<td>Max Burst</td>
<td>Excess burst size in bytes.</td>
</tr>
<tr>
<td>Normal Burst</td>
<td>Normal burst size in bytes.</td>
</tr>
<tr>
<td>Bit Per Second</td>
<td>Average rate in bits per second.</td>
</tr>
<tr>
<td>Conform Action</td>
<td>Action that can be performed on the packet if it conforms to the specified rate limit (rule), for example, continue, drop, change a bit, or transmit.</td>
</tr>
<tr>
<td>Exceed Action</td>
<td>Action that can be performed on the packet if it exceeds the specified rate limit (rule), for example, continue, drop, change a bit, or transmit.</td>
</tr>
<tr>
<td>Access List</td>
<td>Hyperlink that highlights the related access list in the Access List table.</td>
</tr>
</tbody>
</table>

Viewing VRRP Information

Virtual Router Redundancy Protocol (VRRP) is a non-proprietary redundancy protocol that is designed to increase the availability of the static default gateway servicing hosts on the same subnet. This increased reliability is achieved by advertising a virtual router (a representation of master and backup routers acting as a group) as a default gateway to the hosts instead of one physical router. Two or more physical routers are then configured to stand for the virtual router, with only one doing the actual routing at any given time. If the current physical router that is routing the data on behalf of the virtual router fails, another physical router automatically replaces it. The physical router that forwards data on behalf of the virtual router is called the master router; physical routers standing by to take over for the master router if needed are called backup routers.

To view VRRP information:

**Step 1**  Double-click the required element in the Vision client.

**Step 2** In logical inventory, choose Logical Inventory > Routing Entities > Routing Entity.

**Step 3** In the IP Interfaces tab, double-click the required interface to view the IP interface properties. If VRRP is configured on the IP interface, the VRRP Groups tab is displayed.
Figure 17-19  VRRP Properties in IP Interface Properties Window

Table 17-17  VRRP Group Properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Number</td>
<td>Number of the VRRP group associated with the interface.</td>
</tr>
<tr>
<td>Priority</td>
<td>Value that determines the role each VRRP router plays and what happens if the master virtual router fails. Values are 1 through 254, with lower numbers having priority over higher numbers.</td>
</tr>
<tr>
<td>Master IP Address</td>
<td>IP address of the VRRP group, taken from the physical Ethernet address of the master virtual router.</td>
</tr>
<tr>
<td>Admin State</td>
<td>Administrative status of the VRRP group: Up or Down.</td>
</tr>
<tr>
<td>Operation State</td>
<td>State of the VRRP group: Master or Backup.</td>
</tr>
<tr>
<td>Preempt Mode</td>
<td>Whether or not the router is to take over as the master virtual router for a VRRP group if it has a higher priority than the current master virtual router: Enabled or Disabled.</td>
</tr>
<tr>
<td>Virtual IP Address</td>
<td>IP address of the virtual router.</td>
</tr>
<tr>
<td>Virtual MAC Address</td>
<td>MAC address of the virtual router.</td>
</tr>
<tr>
<td>Advertisement Interval</td>
<td>Amount of time (in seconds) between successive advertisements by the master virtual router.</td>
</tr>
</tbody>
</table>
Viewing Label Switched Entity Properties

Logical inventory can display any or all of the following tabs for label switched entities, depending on the configuration:

- **Label Switching Table**—Describes the MPLS label switching entries used for traversing MPLS core networks.
- **LDP Neighbors**—Details all MPLS interface peers that use the Label Distribution Protocol (LDP). LDP enables neighboring provider (P) or PE routers acting as label switch routers (LSRs) in an MPLS-aware network to exchange label prefix binding information, which is required to forward traffic. The LSRs discover potential peers in the network with which they can establish LDP sessions in order to negotiate and exchange the labels (addresses) to be used for forwarding packets.

Two LDP peer discovery types are supported:

- Basic discovery—Used to discover directly connected LDP LSRs. An LSR sends hello messages to the all-routers-on-this-subnet multicast address, on interfaces for which LDP has been configured.
- Extended discovery—Used between indirectly connected LDP LSRs. An LSR sends targeted hello messages to specific IP addresses. Targeted sessions are configured because the routers are not physically connected, and broadcasting would not reach the peers. The IP addresses of both peers are required for extended discovery.

If two LSRs are connected with two separate interfaces, two LDP discoveries are performed.

- **MPLS Interfaces**—Contains information on MPLS interfaces and whether traffic engineering tunnels are configured on an interface.
- **MPLS Label Range**—Identifies whether MPLS uses static or dynamic routing, and the label range.
- **Traffic Engineering LSPs**—Describes the MPLS traffic engineering Label Switched Paths (LSPs) provisioned on the switch entity. MPLS traffic engineering LSP, an extension to MPLS TE, provides flexibility when configuring LSP attributes for MPLS TE tunnels.
- **VRF Table**—Describes MPLS paths that terminate locally at a VRF.

To view information for label switched entities:

**Step 1**
Double-click the required device in the Vision client.

**Step 2**
In the logical inventory window, choose **Logical Inventory > LSEs > Label Switching**.

Table 17-18 describes the information that is displayed for label switched entities.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local LDP ID</td>
<td>Local Label Distribution Protocol (LDP) identifier.</td>
</tr>
<tr>
<td>LDP Process State</td>
<td>State of the LDP process, such as Running, Down, or Unknown.</td>
</tr>
<tr>
<td><strong>MPLS Interaces</strong></td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Identifier for MPLS interface, as a combination of IP address and interface name.</td>
</tr>
<tr>
<td>Distribution Protocol Type</td>
<td>Distribution protocol used: Null, LDP, TDP (Tag Distribution Protocol), RSVP, or TDP and LDP.</td>
</tr>
</tbody>
</table>
### Table 17-18  
*Label Switching Properties in Logical Inventory (continued)*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MPLS TE Properties</strong></td>
<td>Whether or not traffic engineering (TE) properties are configured on the interface:</td>
</tr>
<tr>
<td></td>
<td>• Checked—MPLS TE properties are configured on the interface.</td>
</tr>
<tr>
<td></td>
<td>• Unchecked—MPLS TE properties are not configured on the interface.</td>
</tr>
<tr>
<td><strong>Discovery Protocols</strong></td>
<td>Discovery protocols used on the interface.</td>
</tr>
<tr>
<td><strong>Label Switching Table</strong></td>
<td></td>
</tr>
<tr>
<td>Incoming Label</td>
<td>Incoming MPLS label identifier.</td>
</tr>
<tr>
<td>Action</td>
<td>Type of switching action: Null, Pop, Swap, Aggregate, Untagged, or Act.</td>
</tr>
<tr>
<td>Outgoing Label</td>
<td>Outgoing label.</td>
</tr>
<tr>
<td>Out Interface</td>
<td>Name of the outgoing interface, displayed as a hyperlink to the port subinterface in physical inventory.</td>
</tr>
<tr>
<td>IP Destination</td>
<td>Destination IP address.</td>
</tr>
<tr>
<td>Destination Mask</td>
<td>Subnet mask of the destination.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>IP address of the next hop in the path. The IP address is used for resolving the MAC address of the next MPLS interface that you want to reach.</td>
</tr>
<tr>
<td><strong>VRF Table</strong></td>
<td></td>
</tr>
<tr>
<td>Incoming Label</td>
<td>Incoming VRF label identifier.</td>
</tr>
<tr>
<td>Action</td>
<td>Type of switching action: Null, Pop, Swap, Aggregate, Untagged, or Act.</td>
</tr>
<tr>
<td>VRF</td>
<td>VRF name, hyperlinked to its location in logical inventory.</td>
</tr>
<tr>
<td>IP Destination</td>
<td>Destination IP address.</td>
</tr>
<tr>
<td>Destination Mask</td>
<td>Subnet mask of the destination.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>IP address of the next hop in the path. The IP address is used for resolving the MAC address of the next MPLS interface that you want to reach.</td>
</tr>
<tr>
<td>Out Interface</td>
<td>Name of the outgoing interface, displayed as a hyperlink to the port subinterface in physical inventory.</td>
</tr>
<tr>
<td><strong>Traffic Engineering LSPs</strong></td>
<td></td>
</tr>
<tr>
<td>LSP Name</td>
<td>Label switched path (LSP) name.</td>
</tr>
<tr>
<td>LSP Type</td>
<td>Segment type: Head, Midpoint, or Tail.</td>
</tr>
<tr>
<td>Source Address</td>
<td>Source IP address.</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Destination IP address.</td>
</tr>
<tr>
<td>In Label</td>
<td>Incoming label, if not a head segment.</td>
</tr>
<tr>
<td>In Interface</td>
<td>Incoming interface, if not a head segment.</td>
</tr>
<tr>
<td>Out Interface</td>
<td>Outgoing interface, if not a tail segment.</td>
</tr>
</tbody>
</table>
### Table 17-18  Label Switching Properties in Logical Inventory (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out Label</td>
<td>Outgoing label, if not a tail segment.</td>
</tr>
<tr>
<td>Average Bandwidth (Kbps)</td>
<td>Current bandwidth (in Kb/s) used to automatically allocate the tunnel’s bandwidth.</td>
</tr>
<tr>
<td>LSP ID</td>
<td>LSP identifier.</td>
</tr>
<tr>
<td>Burst (Kbps)</td>
<td>Tunnel bandwidth burst rate, in Kb/s.</td>
</tr>
<tr>
<td>Peak (Kbps)</td>
<td>Tunnel bandwidth peak rate, in Kb/s.</td>
</tr>
<tr>
<td>FRR TE Tunnel</td>
<td>Fast Reroute (FRR) TE tunnel name, hyperlinked to the routing entity in logical inventory.</td>
</tr>
<tr>
<td>FRR TE Tunnel State</td>
<td>State of the FRR TE tunnel:</td>
</tr>
<tr>
<td></td>
<td>• Active—A failure exists in the primary tunnel and the backup is in use.</td>
</tr>
<tr>
<td></td>
<td>• Not Configured—The primary tunnel has no designated backup tunnel.</td>
</tr>
<tr>
<td></td>
<td>• Ready—The primary tunnel is in working condition.</td>
</tr>
</tbody>
</table>

### MPLS Label Range

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS Label Type</td>
<td>Type of MPLS label: Dynamic or Static.</td>
</tr>
<tr>
<td>Minimum Label Value</td>
<td>Lowest acceptable MPLS label in the range.</td>
</tr>
<tr>
<td>Maximum Label Value</td>
<td>Highest acceptable MPLS label in the range.</td>
</tr>
</tbody>
</table>

### LDP Neighbors

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDP ID</td>
<td>Identifier of the LDP peer.</td>
</tr>
<tr>
<td>Transport IP Address</td>
<td>IP address advertised by the peer in the hello message or the hello source address.</td>
</tr>
<tr>
<td>Session State</td>
<td>Current state of the session: Transient, Initialized, Open Rec, Open Sent, or Operational.</td>
</tr>
<tr>
<td>Protocol Type</td>
<td>Protocol used by the peer to establish the session: LDP, TDP, or Unknown.</td>
</tr>
<tr>
<td>Label Distribution Method</td>
<td>Method of label distribution: Downstream, Downstream On Demand, Downstream Unsolicited, or Unknown.</td>
</tr>
<tr>
<td>Session Keepalive Interval</td>
<td>Length of time (in milliseconds) between keepalive messages.</td>
</tr>
<tr>
<td>Session Hold Time</td>
<td>The amount of time (in milliseconds) that an LDP session can be maintained with an LDP peer, without receiving LDP traffic or an LDP keepalive message from the peer.</td>
</tr>
<tr>
<td>Discovery Sources</td>
<td>Whether the peer has one or more discovery sources:</td>
</tr>
<tr>
<td></td>
<td>• Checked—Has one or more discovery sources.</td>
</tr>
<tr>
<td></td>
<td>• Unchecked—Has no discovery sources.</td>
</tr>
</tbody>
</table>

**Note** To see the discovery sources in the LDP Neighbor Properties window, double-click the row of the peer in the table.
Monitoring MPLS Services

Chapter 17      Managing MPLS Networks

Step 3  Double-click an entry in any of the tables to view additional properties for that entry.

Table 17-19   Additional Properties Available from Label Switching in Logical Inventory

<table>
<thead>
<tr>
<th>Double-click an entry in this tab...</th>
<th>To display this window...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label Switching Table</td>
<td>Label Switching Properties</td>
</tr>
<tr>
<td>LDP Neighbors</td>
<td>LDP Peer Properties</td>
</tr>
<tr>
<td>MPLS Interfaces</td>
<td>MPLS Link Information - MPLS Properties</td>
</tr>
<tr>
<td>MPLS Label Range</td>
<td>MPLS Label Range Properties</td>
</tr>
<tr>
<td>Traffic Engineering LSPs</td>
<td>Tunnel Properties</td>
</tr>
<tr>
<td>VRF Table</td>
<td>MPLS Aggregate Entry Properties</td>
</tr>
</tbody>
</table>

Multicast Label Switching (mLADP)

Multicast Label Distribution protocol (mLDP) provides extensions to the Label Distribution Protocol (LDP) for the setup of point-to-multipoint (P2MP) and multipoint-to-multipoint (MP2MP) Label Switched Paths (LSPs) in MPLS networks. A P2MP LSP allows traffic from a single root (or ingress) node to be delivered to a number of leaf (or egress) nodes.

A MP2MP LSP allows traffic from multiple ingress nodes to be delivered to multiple egress nodes. Only a single copy of the packet will be sent on any link traversed by a multipoint LSP. Container is the holder of MPLS mLDP databases and neighbors instances for Multicast.

Viewing MLDP Database Information

To view the MLDP database information:

Step 1  Double-click the required device in the Vision client.

Step 2  In the logical inventory window, choose Logical Inventory > LSEs > Label Switching > Multicast Label Switching > Databases. The database information is displayed in the MLDP Databases content pane.

Step 3  Select a database from the content pane, right-click and choose the Properties option. The MLDP Database Properties dialog box is displayed. You can click on the tabs to view more details.

Table 17-20 describes the information that is displayed for MLDP Database Properties dialog box.
Table 17-20  MLDP Database Properties Dialog Box

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSM ID</td>
<td>The unique ID assigned to a LSP.</td>
</tr>
<tr>
<td>Tunnel Type</td>
<td>The tunnel type.</td>
</tr>
<tr>
<td>FEC Root</td>
<td>The root IP address of the MDT.</td>
</tr>
<tr>
<td>Opaque Value</td>
<td>The stream information that uniquely identifies the tree to the root.</td>
</tr>
<tr>
<td></td>
<td>To receive label switched multicast packets, the Egress Provider Edge (PE)</td>
</tr>
<tr>
<td></td>
<td>indicates to the upstream router (the next hop closest to the root) which</td>
</tr>
<tr>
<td></td>
<td>label it uses for the multicast source by applying the label mapping message.</td>
</tr>
<tr>
<td>Is Root</td>
<td>Indicates whether Forwarding Equivalence Class (FEC) is the root.</td>
</tr>
</tbody>
</table>

**Downstream Clients Tab**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Egress Interface Name</td>
<td>The egress interface name.</td>
</tr>
<tr>
<td>Associated Entity</td>
<td>The entity associated with the LSP. Click this link to view the associated entity details.</td>
</tr>
<tr>
<td>Uptime</td>
<td>The amount of time from when the interface is active.</td>
</tr>
<tr>
<td>Table ID</td>
<td>The unique Table ID of the label through which the packet was received.</td>
</tr>
<tr>
<td>Ingress State</td>
<td>The status of the ingress interface, which can be Enabled or Disabled.</td>
</tr>
<tr>
<td>PPMP State</td>
<td>The status of the Point-to-Point Multipoint, which can be Enabled or Disabled.</td>
</tr>
<tr>
<td>Local Label</td>
<td>The label used to identify the label stack of the route within the local VPN network.</td>
</tr>
</tbody>
</table>

**Viewing the MLDP Neighbors Information**

To view information of MLDP neighbors:

**Step 1** Double-click the required device in the Vision client.

**Step 2** In the logical inventory window, choose **Logical Inventory > LSEs > Label Switching > Multicast Label Switching > MLDP Neighbors**. The MLDP peer information is displayed in the MLDP Peers content pane.

**Step 3** Select a peer id from the content pane, right-click and choose the **Properties** option. The **Peer ID Properties** dialog box is displayed.

**Table 17-21** describes the information that is displayed for **Peer ID Properties** dialog box.
### Table 17-21  Peer ID Properties Dialog Box

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer ID</td>
<td>The IP address of the MLDP peer.</td>
</tr>
<tr>
<td>Capabilities</td>
<td>The capabilities supported by the LDP LSR.</td>
</tr>
<tr>
<td>MLDP GR</td>
<td>Indicates whether graceful restart is enabled for the LDP.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>LDP graceful restart provides a control plane mechanism to ensure high availability and allows detection and recovery from failure conditions while preserving Non Stop Forwarding (NSF) services.</td>
</tr>
<tr>
<td>Path Count</td>
<td>The number of LSP’s configured.</td>
</tr>
<tr>
<td>Uptime</td>
<td>The amount of time from when the peer id is working.</td>
</tr>
</tbody>
</table>

**Peer Paths tab**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address of the MLDP peer.</td>
</tr>
<tr>
<td>Interface Name</td>
<td>The interface name.</td>
</tr>
<tr>
<td>Associated Entity</td>
<td>The link to the associated entity, which when clicked will highlight the associated Default routing entity record under the Routing Entity node.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The protocol type used for communication.</td>
</tr>
</tbody>
</table>

**Peer Adjacent List**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address of the MLDP peer.</td>
</tr>
<tr>
<td>Interface Name</td>
<td>The interface name.</td>
</tr>
<tr>
<td>Associated Entity</td>
<td>The link to the associated entity, which when clicked will highlight the associated Default routing entity record under the Routing Entity node.</td>
</tr>
</tbody>
</table>
Viewing MP-BGP Information

The MP-BGP branch displays information about a router’s BGP neighbors and cross-connect VRFs.

Note
If there are multiple MP-BGP links between two devices, the Vision client displays each link in the content pane map view.

To view MP-BGP information:

Step 1
Right-click the required device in the Vision client and choose Inventory.

Step 2
In the logical inventory window, choose Logical Inventory > MPBGPs > MPBGP.

Table 17-22 describes the information that is displayed for MP-BGP.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local AS</td>
<td>Identifier of the autonomous system (AS) to which the router belongs.</td>
</tr>
<tr>
<td>BGP Identifier</td>
<td>BGP identifier, represented as an IP address.</td>
</tr>
<tr>
<td>Cross VRFs Tab</td>
<td></td>
</tr>
<tr>
<td>VRF Name</td>
<td>Name of the VRF.</td>
</tr>
<tr>
<td>Cross VRF Routing Entries</td>
<td>Group of cross VRFs that share a single destination.</td>
</tr>
<tr>
<td>BGP Neighbors Tab</td>
<td></td>
</tr>
<tr>
<td>Peer AS</td>
<td>Identifier of the AS to which the remote peer belongs.</td>
</tr>
<tr>
<td>Peer State</td>
<td>State of the remote peer: Active, Connect, Established, Open Confirm, Open Sent, or Null.</td>
</tr>
<tr>
<td>Peer Address</td>
<td>Remote peer IP address.</td>
</tr>
<tr>
<td>AFI</td>
<td>Address family identifier: IPv4, IPv6, L2VPN, VPNv4, or VPNv6.</td>
</tr>
<tr>
<td>AF Peer State</td>
<td>Address family peer state: Established or Idle.</td>
</tr>
<tr>
<td>Peer BGP ID</td>
<td>Identifier of the remote peer, represented as an IP address.</td>
</tr>
<tr>
<td>Local BGP ID</td>
<td>Local peer IP address.</td>
</tr>
<tr>
<td>VRF Name</td>
<td>Remote peer VRF name.</td>
</tr>
<tr>
<td>BGP Neighbor Type</td>
<td>Neighbor type: Null, Client, or Non Client.</td>
</tr>
<tr>
<td>Hold Time (secs)</td>
<td>Established hold time in seconds.</td>
</tr>
<tr>
<td>Keepalive (secs)</td>
<td>Established keepalive time in seconds.</td>
</tr>
<tr>
<td>BGP Neighbor Entry</td>
<td>BGP neighbor IP address.</td>
</tr>
</tbody>
</table>
Viewing 6rd Tunnel Properties

IPv6 rapid deployment (6rd) is a mechanism that allows stateless tunneling of IPv6 over IPv4. For information on the devices that support 6rd, refer to Cisco Prime Network 4.1 Supported VNEs.

To view 6rd tunnel properties:

**Step 1** In the Vision client, double-click the required device.

**Step 2** In the **Inventory** window, choose **Logical Inventory > 6rd Tunnels**.

The 6rd tunnel properties are displayed as shown in Figure 17-20.

*Figure 17-20  6rd Tunnel Properties in Logical Inventory*

Table 17-23 describes the information displayed for 6rd tunnels.
Bidirectional Forwarding Detection (BFD) is used to detect communication failures between two elements, or endpoints, that are connected by a link, such as a virtual circuit, tunnel, or LSP. BFD establishes sessions between the two endpoints over the link. If more than one link exists, BFD establishes a session for each link.

Prime Network supports BFD with the following protocols: BGP, IPv4 (static), IPv6 (static), IS-IS, LAG (Ether channel), MPLS TE, MPLS-TP, and OSPF.

To view BFD session properties that are configured on an element:

**Step 1**  
In the Vision client, double-click the required device.

**Step 2**  
In the **Inventory** window, choose **Logical Inventory > Bidirectional Forwarding Detection**.

The properties for BFD sessions are displayed as shown in **Figure 17-21**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel Name</td>
<td>6rd tunnel name.</td>
</tr>
<tr>
<td>IPv6 Prefix</td>
<td>IPv6 prefix used to translate the IPv4 address to an IPv6 address.</td>
</tr>
<tr>
<td>Source Address</td>
<td>Tunnel IPv4 source IP address.</td>
</tr>
<tr>
<td>Tunnel SubMode</td>
<td>Tunnel type:</td>
</tr>
<tr>
<td></td>
<td>• 6rd—Static IPv6 interface.</td>
</tr>
<tr>
<td></td>
<td>• 6to4—IPv6 address with the prefix embedding the tunnel source IPv4 address.</td>
</tr>
<tr>
<td></td>
<td>• Auto-tunnel—IPv4-compatible IPv6 tunnel.</td>
</tr>
<tr>
<td></td>
<td>• ISATAP—Overlay tunnel using an Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) address.</td>
</tr>
<tr>
<td>Prefix Length</td>
<td>IPv4 prefix length used to derive the delegated IPv6 prefix.</td>
</tr>
<tr>
<td>Suffix Length</td>
<td>IPv4 suffix length used to derive the delegated IPv6 prefix.</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit (MTU) configured on the 6rd IPv4 tunnel.</td>
</tr>
</tbody>
</table>
Table 17-24 describes the information displayed for BFD sessions.

### Table 17-24  **BFD Session Properties**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process</td>
<td>Process name, such as Bidirectional Forwarding Detection.</td>
</tr>
<tr>
<td>Process State</td>
<td>Process state, such as Running.</td>
</tr>
<tr>
<td><strong>BFD Sessions Table</strong></td>
<td></td>
</tr>
<tr>
<td>Source IP</td>
<td>Source IP address of the session.</td>
</tr>
<tr>
<td>Destination IP</td>
<td>Destination IP address of the session.</td>
</tr>
<tr>
<td>State</td>
<td>Session state, such as Up or Down.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface used for BFD communications, hyperlinked to the routing entity in logical inventory.</td>
</tr>
<tr>
<td>Registered Protocols</td>
<td>Routing protocol being monitored for communication failures, such as BGP or OSPF.</td>
</tr>
</tbody>
</table>
For MPLS-TP BFD sessions, the information in Table 17-25 is displayed.

**Table 17-25  MPLS-TP BFD Session Properties in Logical Inventory**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process</td>
<td>Process name: Bidirectional Forwarding Detection.</td>
</tr>
<tr>
<td>Process State</td>
<td>Process state, such as Running.</td>
</tr>
<tr>
<td><strong>MPLS-TP BFD Sessions Table</strong></td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>Interface used for BFD communications, hyperlinked to the routing entity in logical inventory.</td>
</tr>
<tr>
<td>LSP Type</td>
<td>Type of LSP: Working or Protected.</td>
</tr>
<tr>
<td>State</td>
<td>Session state: Up or Down.</td>
</tr>
<tr>
<td>Registered Protocols</td>
<td>Routing protocol being monitored for communication failures: MPLS-TP.</td>
</tr>
<tr>
<td>Interface Name</td>
<td></td>
</tr>
</tbody>
</table>

**Step 3**

To view additional properties, double-click the required entry in the Sessions table. **Table 17-26** describes the information that is displayed in the Session Properties window.

**Table 17-26  Session Properties Window**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP</td>
<td>Source IP address of the session.</td>
</tr>
<tr>
<td>Destination IP</td>
<td>Destination IP address of the session.</td>
</tr>
<tr>
<td>State</td>
<td>Session state: Up or Down.</td>
</tr>
<tr>
<td>Interface</td>
<td>Hyperlink to the routing entity in logical inventory.</td>
</tr>
<tr>
<td>Registered Protocols</td>
<td>Routing protocol being monitored for communication failures.</td>
</tr>
<tr>
<td>Offload Host</td>
<td>BFD offload property: Software (applicable when configuring BFD on BVI interface). Displays BFD session hosted in software.</td>
</tr>
<tr>
<td><strong>Protocols Table</strong></td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol used for this session.</td>
</tr>
<tr>
<td>Interval</td>
<td>Length of time (in milliseconds) to wait between packets that are sent to the neighbor.</td>
</tr>
<tr>
<td>Multiplier</td>
<td>Number of times a packet is missed before the neighbor is declared down.</td>
</tr>
</tbody>
</table>
**BFD Single-Hop Authentication**

The BFD Single-Hop Authentication feature enables authentication for single-hop Bidirectional Forwarding Detection (BFD) sessions between two directly connected devices. This feature supports Message Digest 5 (MD5) and Secure Hash Algorithm 1 (SHA-1) authentication types. The BFD templates can be configured only if the BFD sessions are enabled.

**BFD Templates Support**

BFD (Bidirectional Forwarding Detection Templates) are the new features added in CPT devices. Prime Network uses the below Telnet or CLI Command to get the BFD templates in existing CPT devices.

Show running-config|section bfd-template

**Cerent Trap Support**

Cerent traps are alarms supported for CPT devices. There are 170 traps supported. There are various kinds of traps supported which are listed below:

- Communications
- Equipment
- Environmental
- Integrity Violation
- Quality of Service

The alarms can be categorized by their severity such as Critical, Major, Minor, Not Reported and Not Alarmed. Examples of each severity categories are as follows:

- **Critical** - Equipment failure
- **Major** - High Voltage, Battery Failure
- **Minor** - Loss of frame, Loss of signal
- **Not Reported** - Unqualified PPM Inserted
- **Not Alarmed** - Transit Node Clock Traceable

**Change Settings in Cisco Transport Controller (CTC)**

Any configurations settings made in CPT should be done through CTC. To receive traps in a particular server, that server IP needs to be entered in the device through CTC. Most of the traps are on device dependencies.

**CMP Tool**

The default trap format can be used to send the alarms through CMP tool which can be generated in Prime Network. The default trap format is given as follows:

```
<key name="trap"><key name=""></entry name="">sendtrap -V2 10.105.39.217 -ccellbus -r162 -o1.3.6.1.2.1.1.3.0 -mt1166470595 -o1.3.6.1.6.3.1.1.4.1.0 -md1.3.6.1.4.1.3607.6.10.30.0.1670 -o1.3.6.1.4.1.3607.6.10.100.10.20 -mo03/Nov/2001 -o1.3.6.1.4.1.3607.6.10.20.30.20.1.80.1.1670 -mi50 -o1.3.6.1.4.1.3607.6.10.20.30.20.1.60.1.1670 -mi50 -o1.3.6.1.4.1.3607.6.10.20.30.20.1.100.1.1670 -md1.3.6.1.4.1.3607.6.10.30.0.2110
```
Link and Port Parameters

The link and port parameters are scripts which can be navigated from **Device->Port->Interface-> right click Commands->Configuration->Scripts.** The link and port parameters are supported for the following auto populated UI attributes:

**Ethernet Parameter Configuration**
- MTU
- Link State
- Expected Speed
- Expected Duplex
- Operating Flow Control
- Carrier Delays
- Auto Negotiation

**Port Parameter Configuration**
- Port Name
- Admin State
- AINS Soak
- Reach
- Wavelength

**L2 Parameter Configuration**
- CDP
- DOTIX
- DTP
- LACP
- PAGP
- VTP
- STP

The following are the configuration scripts supported,
- Add Loopback
- Remove Loopback
- Configure CDP
- Configure Ethernet
- Configure L2 Control Protocol
- Configure Port Parameters
- Show Ethernet Parameters
• Show L2 Control Parameters
• Show Port Parameters

**Viewing Configuration Scripts in Prime Network**

**Add Loopback**
To view the **Add Loopback** script:

**Step 1** Model the device in **Cisco Prime Network Administration**.
**Step 2** Launch the Cisco Prime Network Vision client and choose **Inventory**
**Step 3** In the physical inventory window, choose **Physical inventory >IPortConnector >Commands >Configuration >Add Loopback**
**Step 4** Select the value **Loopback** from the **Attribute** combo box.
**Step 5** Click on **Execute Now** button.
**Step 6** Verify if **Loopback** is successfully added.

**Remove Loopback**
To view the **Remove Loopback** script:

**Step 1** Model the device in **Cisco Prime Network Administration**.
**Step 2** Launch the Cisco Prime Network Vision client and choose **Inventory**
**Step 3** In the physical inventory window, choose **Physical inventory >IPortConnector >Commands >Configuration >Remove Loopback**
**Step 4** Click on **Execute Now** button.
**Step 5** Verify if **Loopback** is successfully removed.

**Configure CDP**
To view the **Configure CDP** script:

**Step 1** Model the device in **Cisco Prime Network Administration**.
**Step 2** Launch the Cisco Prime Network Vision client and choose **Inventory**
**Step 3** In the physical inventory window, choose **Physical inventory >IPortConnector >Commands >Configuration >Configure CDP**
**Step 4** Select the value **CDP** from the **Attribute** combo box.
**Step 5** Click on **Execute Now** button.
**Step 6** Verify if **CDP** is successfully configured.

**Configure Ethernet**
To view the **Configure Ethernet** script:
Step 1  Model the device in Cisco Prime Network Administration.
Step 2  Launch the Cisco Prime Network Vision client and choose Inventory
Step 3  In the physical inventory window, choose Physical inventory >IPortConnector >Commands > Configuration >Configure Ethernet
Step 4  Select the value Admin Status from the Attribute combo box.
Step 5  Click on Execute Now button.
Step 6  Verify if Ethernet is successfully configured.

Configure L2 Control Protocol
To view the Configure L2 Control Protocol script:

Step 1  Model the device in Cisco Prime Network Administration.
Step 2  Launch the Cisco Prime Network Vision client and choose Inventory
Step 3  In the physical inventory window, choose Physical inventory >IPortConnector >Commands > Configuration >Configure L2 Control Protocol
Step 4  Select the value STP from the Attribute combo box.
Step 5  Click on Execute Now button.
Step 6  Verify if L2 Control Protocol is successfully configured.

Configure Port Parameters
To view the Configure Port Parameters script:

Step 1  Model the device in Cisco Prime Network Administration.
Step 2  Launch the Cisco Prime Network Vision client and choose Inventory
Step 3  In the physical inventory window, choose Physical inventory >IPortConnector >Commands > Configuration >Configure Port Parameters
Step 4  Select the value Reach from the Attribute combo box.
Step 5  Click on Execute Now button.
Step 6  Verify if Port Parameters are successfully added.

Show Port Parameters
To view the Show Port Parameters script:

Step 1  Model the device in Cisco Prime Network Administration.
Step 2  Launch the Cisco Prime Network Vision client and choose Inventory
Step 3  In the physical inventory window, choose Physical inventory >IPortConnector >Commands > Configuration >Show Port Parameters
Step 4  Click on Execute Now button.
Step 5  Verify if all **Port Parameters** are listed.

**Show Ethernet Parameters**
To view the **Show Ethernet Parameters** script:

**Step 1**  Model the device in **Cisco Prime Network Administration**.
**Step 2**  Launch the Cisco Prime Network Vision client and choose **Inventory**.
**Step 3**  In the physical inventory window, choose **Physical inventory >IPortConnector >Commands > Configuration >Show Ethernet Parameters**.
**Step 4**  Click on **Execute Now** button.
**Step 5**  Verify if **Show Ethernet Parameters** are listed.

**Show L2 Control Parameters**
To view the **Show L2 Control Parameters** script:

**Step 1**  Model the device in **Cisco Prime Network Administration**.
**Step 2**  Launch the Cisco Prime Network Vision client and choose **Inventory**.
**Step 3**  In the physical inventory window, choose **Physical inventory >IPortConnector >Commands > Configuration >Show L2 Control Parameters**.
**Step 4**  Click on **Execute Now** button.
**Step 5**  Verify if all **L2 Control Parameters** are listed.

**Show Configure Ethernet**
To view the **Show Configure Ethernet** script:

**Step 1**  Model the device in **Cisco Prime Network Administration**.
**Step 2**  Launch the Cisco Prime Network Vision client and choose **Inventory**.
**Step 3**  In the physical inventory window, choose **Physical inventory >IPortConnector >Commands > Configuration >Show Configure Ethernet**.
**Step 4**  Click on **Execute Now** button.
**Step 5**  Verify if all the **configured Ethernets** are listed.

**Viewing Cross-VRF Routing Entries**
Cross-VRF routing entries display routing information learned from the BGP neighbors (BGP knowledge base).

To view properties for cross-VRF routing entries:

**Step 1** Right-click the required device in the Vision client and choose **Inventory**.

**Step 2** In the logical inventory window, choose **Logical Inventory > MPBGPs > MPBGP**.

**Step 3** Click the **Cross VRFs** tab.

**Step 4** Double-click the required entry in the list of cross-VRFs.

The Cross VRF Properties window is displayed, containing the information described in **Table 17-27**.

**Table 17-27  Cross-VRF Properties Window**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Cross-VRF name</td>
</tr>
</tbody>
</table>

**Cross VRF Routing Entries Table**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>IP address of the destination network.</td>
</tr>
<tr>
<td>Prefix</td>
<td>Length of the network prefix in bits.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>IP address of the next hop in the path.</td>
</tr>
<tr>
<td>Out Going VRF</td>
<td>Outgoing VRF identifier, hyperlinked to its entry in logical inventory.</td>
</tr>
<tr>
<td>Out Tag</td>
<td>Outgoing virtual router tag, such as 50 or no tag.</td>
</tr>
<tr>
<td>In Tag</td>
<td>Incoming virtual router tag, such as 97 or no tag.</td>
</tr>
</tbody>
</table>

**Viewing Pseudowire End-to-End Emulation Tunnels**

The Pseudowires branch in logical inventory displays a list of the Layer 2 tunnel edge properties (per edge), including tunnel status and VC labels.

To view pseudowire properties:

**Step 1** Right-click the required device in the Vision client and choose **Inventory**.

**Step 2** In the logical inventory window, choose **Logical Inventory > Pseudowires**.

The Tunnel Edges table is displayed and contains the information described in **Table 17-28**.
### Table 17-28 Pseudowires Branch Tunnel Edges Table

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Interface Name</td>
<td>Name of the subinterface or port.</td>
</tr>
<tr>
<td></td>
<td>Strings, such as Aggregation Group, EFP, VLAN, and VSI, are included in the</td>
</tr>
<tr>
<td></td>
<td>interface name, and the entry is hyperlinked to the relevant entry in logical or physical inventory:</td>
</tr>
<tr>
<td></td>
<td>• Aggregation groups are linked to Ethernet Link Aggregation in logical</td>
</tr>
<tr>
<td></td>
<td>inventory.</td>
</tr>
<tr>
<td></td>
<td>• ATM interfaces are linked to the port in physical inventory and the ATM</td>
</tr>
<tr>
<td></td>
<td>interface.</td>
</tr>
<tr>
<td></td>
<td>• ATM VCs are linked to the port in physical inventory and the Port IP</td>
</tr>
<tr>
<td></td>
<td>Properties table.</td>
</tr>
<tr>
<td></td>
<td>• CEM groups are linked to the port in physical inventory and the CEM Group</td>
</tr>
<tr>
<td></td>
<td>table.</td>
</tr>
<tr>
<td></td>
<td>• EFPs are linked to the port in physical inventory and the EFPs table.</td>
</tr>
<tr>
<td></td>
<td>• IMA groups are linked to IMA Groups in logical inventory.</td>
</tr>
<tr>
<td></td>
<td>• Local switching entities are linked to Local Switching Entity in logical</td>
</tr>
<tr>
<td></td>
<td>inventory.</td>
</tr>
<tr>
<td></td>
<td>• VLANs are linked to Bridges in logical inventory.</td>
</tr>
<tr>
<td></td>
<td>• VSIs are linked to the VSI entry in logical inventory.</td>
</tr>
<tr>
<td>VC ID</td>
<td>Tunnel identifier, hyperlinked to the PTP Layer 2 MPLS Tunnel Properties</td>
</tr>
<tr>
<td></td>
<td>window.</td>
</tr>
<tr>
<td>SAI II</td>
<td>Specifies the Source Access Individual Identifier (SAII) of the tunnel.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The SAII attribute can be configured only if the Pseudowire type is</td>
</tr>
<tr>
<td></td>
<td>FEC129 TYPE II.</td>
</tr>
<tr>
<td>TAI II</td>
<td>Specifies the Target Attachment Individual Identifier (TAII) of the tunnel.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The TAI II can be configured only if the Pseudowire type is FEC129</td>
</tr>
<tr>
<td></td>
<td>TYPE II.</td>
</tr>
<tr>
<td>Pseudowire Type</td>
<td>Type of pseudowire, such as Ethernet, Ethernet Tagged, CESoPSN Basic, PPP,</td>
</tr>
<tr>
<td></td>
<td>SAToP or FEC129 TYPE II.</td>
</tr>
<tr>
<td>Peer</td>
<td>Details of the selected peer, hyperlinked to the peer pseudowire tunnel in</td>
</tr>
<tr>
<td></td>
<td>logical inventory.</td>
</tr>
<tr>
<td>Status</td>
<td>Operational state of the tunnel: Up or Down.</td>
</tr>
<tr>
<td>Pseudowire Role</td>
<td>If the pseudowire is in a redundancy configuration, indicates whether its</td>
</tr>
<tr>
<td></td>
<td>role is as the primary or secondary pseudowire in the configuration.</td>
</tr>
<tr>
<td></td>
<td>If the pseudowire is not configured for redundancy, this field is blank.</td>
</tr>
<tr>
<td>Preferred Path Tunnel</td>
<td>Path to be used for MPLS pseudowire traffic.</td>
</tr>
<tr>
<td>Local Router IP</td>
<td>IP address of this tunnel edge, which is used as the MPLS router identifier.</td>
</tr>
<tr>
<td>Peer Router IP</td>
<td>IP address of the peer tunnel edge, which is used as the MPLS router</td>
</tr>
<tr>
<td>Local MTU</td>
<td>Size, in bytes, of the MTU on the local interface.</td>
</tr>
<tr>
<td>Remote MTU</td>
<td>Size, in bytes, of the MTU on the remote interface.</td>
</tr>
<tr>
<td>Local VC Label</td>
<td>MPLS label that is used by this router to identify or access the tunnel. It</td>
</tr>
<tr>
<td></td>
<td>is inserted into the MPLS label stack by the local router.</td>
</tr>
<tr>
<td>Peer VC Label</td>
<td>MPLS label that is used by this router to identify or access the tunnel. It</td>
</tr>
<tr>
<td></td>
<td>is inserted into the MPLS label stack by the peer router.</td>
</tr>
</tbody>
</table>
Chapter 17: Managing MPLS Networks

Monitoring MPLS Services

Table 17-28: Pseudowires Branch Tunnel Edges Table (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signaling Protocol</td>
<td>Protocol used by MPLS to build the tunnel, for example, LDP or TDP.</td>
</tr>
<tr>
<td>Peer Status</td>
<td>Status of the peer link.</td>
</tr>
<tr>
<td>Associated EVC</td>
<td>Specifies the name of the associated Ethernet Virtual Circuits (EVC)</td>
</tr>
</tbody>
</table>

Viewing MPLS TE Tunnel Information

Prime Network automatically discovers MPLS TE tunnels and enables you to view MPLS TE tunnel information in inventory.

To view MPLS TE tunnel information:

Step 1 Right-click the required device in the Vision client and choose Inventory.

Step 2 In the logical inventory window, choose Logical Inventory > Traffic Engineering Tunnels.

Table 17-29 describes the information that is displayed in the Tunnel Edges table.

Table 17-29: Tunnel Edges Table

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the TE tunnel; for Cisco devices it is the interface name.</td>
</tr>
<tr>
<td>Tunnel Type</td>
<td>Whether the tunnel is Point-to-Point or Point-to-Multipoint.</td>
</tr>
<tr>
<td>Tunnel Destination</td>
<td>IP address of the device in which the tunnel ends.</td>
</tr>
<tr>
<td>Administrative Status</td>
<td>Administrative state of the tunnel: Up or Down.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>Operational state of the tunnel: Up or Down.</td>
</tr>
<tr>
<td>Outgoing Label</td>
<td>TE tunnel’s MPLS label distinguishing the LSP selection in the next device.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the tunnel.</td>
</tr>
<tr>
<td>Outgoing Interface</td>
<td>Interface through which the tunnel exits the device.</td>
</tr>
<tr>
<td>Bandwidth (KBps)</td>
<td>Bandwidth specification for this tunnel in Kb/s.</td>
</tr>
<tr>
<td>Setup Priority</td>
<td>Tunnel priority upon path setup.</td>
</tr>
<tr>
<td>Hold Priority</td>
<td>Tunnel priority after path setup.</td>
</tr>
<tr>
<td>Affinity</td>
<td>Tunnel preferential bits for specific links.</td>
</tr>
<tr>
<td>Affinity Mask</td>
<td>Tunnel affinity bits that should be compared to the link attribute bits.</td>
</tr>
<tr>
<td>Auto Route</td>
<td>Whether or not destinations behind the tunnel are routed through the tunnel:</td>
</tr>
<tr>
<td></td>
<td>Enabled or disabled.</td>
</tr>
<tr>
<td>Lockdown</td>
<td>Whether or not the tunnel can be rerouted:</td>
</tr>
<tr>
<td></td>
<td>• Enabled—The tunnel cannot be rerouted.</td>
</tr>
<tr>
<td></td>
<td>• Disabled—The tunnel can be rerouted.</td>
</tr>
</tbody>
</table>
### Table 17-29  Tunnel Edges Table (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path Option</td>
<td>Tunnel path option:</td>
</tr>
<tr>
<td></td>
<td>- Dynamic—The tunnel is routed along the ordinary routing decisions after taking into account the tunnel constraints such as attributes, priority, and bandwidth.</td>
</tr>
<tr>
<td></td>
<td>- Explicit—The route is explicitly mapped with the included and excluded links.</td>
</tr>
<tr>
<td>Average Rate (Kbps)</td>
<td>Average bandwidth for this tunnel (in Kb/s).</td>
</tr>
</tbody>
</table>
Configuring VRFs

The following commands configure routes that are available or reachable to all the destinations or networks in the VRF. These commands are launched by right-clicking the VRF node and choosing Commands > Configuration. Your permissions determine whether you can run these commands (see Permissions for Managing MPLS Services, page B-17). To find out if a device supports these commands, see the Cisco Prime Network 4.2.2 Supported Cisco VNEs.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify VRF</td>
<td>Configures VRF properties, including the VRF route distinguisher, import and export route targets, and any provisioned sites and VRF routes.</td>
</tr>
<tr>
<td>Delete VRF</td>
<td></td>
</tr>
</tbody>
</table>

The Traffic Engineering LSPs tab in the LSEs branch in logical inventory displays TE tunnel LSP information.

For details about the information displayed for TE tunnel LSPs, see Traffic Engineering LSPs, page 17-42.

### Table 17-29 Tunnel Edges Table (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Burst (Kbps)</td>
<td>Burst flow specification (in Kb/s) for this tunnel.</td>
</tr>
<tr>
<td>Peak Rate (Kbps)</td>
<td>Peak flow specification (in Kb/s) for this tunnel.</td>
</tr>
<tr>
<td>LSP ID</td>
<td>LSP identifier.</td>
</tr>
<tr>
<td>Policy Class</td>
<td>Value of Policy Based Tunnel Selection (PBTS) configured. Values range from 1-7.</td>
</tr>
<tr>
<td>FRR</td>
<td>TE Fast Reroute (FRR) status: Enabled or Disabled.</td>
</tr>
<tr>
<td>Type</td>
<td></td>
</tr>
</tbody>
</table>
Configuring IP Interfaces

The following IP interface commands are launched by right-clicking Routing Entities > routing entity and choosing Commands > Configuration. Your permissions determine whether you can run these commands (see Permissions for Managing IP and MPLS Multicast, page B-19). To find out if a device supports these commands, see the Cisco Prime Network 4.2.2 Supported Cisco VNEs.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Interface</td>
<td>Configures an IP interface for the selected routing entity</td>
</tr>
<tr>
<td>Modify Interface</td>
<td></td>
</tr>
<tr>
<td>Delete Interface</td>
<td></td>
</tr>
<tr>
<td>Configure Secondary IP Address</td>
<td></td>
</tr>
<tr>
<td>Delete Secondary IP Address</td>
<td></td>
</tr>
</tbody>
</table>

Auto-IP in PN

Prime network supports AUTO-IP feature in 4.2.2.2 Release. Auto-IP is an IP address configured on the interface using the Auto-IP ring command. The Auto-IP feature enables node insertion, removal and movement to any location within a ring without the need for reconfiguring the existing nodes manually. When enabled on the physical interface or the sub interface, you can discover the devices in the Auto-IP ring automatically.

Configuring Auto-IP

To configure Auto-IP, configure one of the routers in the ring as a seed router. Normally an edge router is configured as a seed router, and the Auto-IP address of the seed router is same as the IP address of the router interface in which the Auto-IP is enabled. The device, in which the Auto-IP configured with priority value 2, becomes the owner interface and assigns the IP address to the non-owner interface (Priority value for non-owner interface is 0) in the ring topology. The Link Layer Discovery Protocol (LLDP) must be enabled on the device before enabling the auto-IP functionality on a node interface.

Note

When you configure Auto-IP feature on the devices, by default, the priority value is 1.

Configuring MPLS-TP

The following MPLS-TP commands are launched by right-clicking the appropriate node and choosing MPLS-TP Global > Commands > Configuration. Your permissions determine whether you can run these commands (see Permissions for Managing MPLS Services, page B-17). To find out if a device supports these commands, see the Cisco Prime Network 4.2.2 Supported Cisco VNEs.

Note

To run the Global Configuration, BFD Configuration, and Link Configuration commands on the Cisco Carrier Packet Transport (CPT) System, right-click the device in the Vision client list or map view, and click Logical Inventory > CPT Context Container.
Locking/Unlocking MPLS-TP Tunnels in Bulk

An MPLS-TP network has one or multiple LSPs running between endpoint devices. If you want to shutdown one of the interfaces in the network, the MPLS-TP packet must be diverted through an alternative LSP. This can be achieved by locking the interface. Before attempting to lock or unlock a tunnel, ensure that MPLS-TP tunnels have been configured for the link. Also, ensure that you have the appropriate rights (Configurator and above) to lock or unlock a tunnel.

The MPLS-TP bulk lockout/unlock option in Prime Network allows you to lock or unlock multiple MPLS-TP tunnels on different VNEs at the same time.

Your permissions determine whether you can run these commands (see Permissions for Managing MPLS Services, page B-17). To find out if a device supports these commands, see the Cisco Prime Network 4.2.2 Supported Cisco VNEs.

Locking MPLS-TP Tunnels

To lock MPLS-TP tunnels in bulk:

Step 1  In the map view, right-click the required link and choose Properties.
Chapter 17      Managing MPLS Networks

Configuring MPLS-TP

Step 2  In the link properties window, right-click on the required physical link and choose the Show MPLS-TP tunnels option. The MPLS-TP tunnels’ commands dialog box is displayed, which lists all the tunnels in the selected link.

Step 3  In the MPLS-TP tunnels’ commands dialog box, choose the tunnels that you want to lock and select the Lock Out option in the Commands field.

Step 4  Click Execute Now. You are prompted to confirm the lockout operation.

Step 5  Click Yes to confirm. A message is displayed confirming that the selected tunnels have been locked. The status of the tunnel is automatically updated as Lockout(UP) after this operation.

Unlocking MPLS-TP Tunnels

To unlock MPLS-TP tunnels in bulk:

Step 1  In the map view, right-click the required link and choose Properties.

Step 2  In the link properties window, right-click on the required physical link and choose the Show MPLS-TP tunnels option. The MPLS-TP tunnels’ commands dialog box is displayed, which lists all the tunnels in the selected link.

Step 3  In the MPLS-TP tunnels’ commands dialog box, select the locked tunnels that you want to unlock and select the Unlock option in the Commands field.

Step 4  Click Execute Now. You are prompted to confirm the unlock operation.

Step 5  Click Yes to confirm. A message is displayed confirming that the selected tunnels have been unlocked. The status of the tunnels is automatically updated as Active(UP) after this operation.

Note  If you attempt to unlock a tunnel that is not locked, a message is displayed indicating that there are no valid tunnels to perform the unlock operation.

Linear Protection for MPLS-TP

As explained earlier, MPLS-TP is the transport profile that fulfills the deployment in the network for the MPLS technology. This technology provides fast protection switching for end-to-end segments wherein the protection switching time is generally less than 50 milliseconds.

Protection switching is a mechanism wherein route and resources of a protection path are reserved for a selected working path or set of working paths.

Linear protection provides rapid and simple protection switching because it can operate between any pair of points within the network. For every working Label Switched Paths (LSP) in the network, there is a protected LSP that is not related to any other working entity. When a working LSP fails, the protected LSP is ready to take up transmission of data.

In Prime Network, the following commands are available for linear protection:
- **Force Switch (Lockout)**—This command is used to switch normal traffic from a working LSP to a protected LSP. This command can only be applied on a working LSP. If Force Switch is enabled, then the Working LSP becomes standby and the Protected LSP becomes active.

- **Manual Switch**—This command is used to switch normal traffic from a working LSP to a protected LSP. This command can be applied only on a working LSP. If Manual Switch is enabled, then the working LSP becomes standby and the protected LSP becomes active.

  **Note** The Force Switch and Manual Switch commands are both used to switch traffic from the working LSP to the protected LSP. However, if the Manual Switch command is used, and there is a failure in the protecting LSP, then the working LSP becomes active. In case of the Force Switch command, then the working LSP does not become active if there is a failure in the protecting LSP.

- **Lockout of Protecting (Lockout)**—This command is used to switch traffic from the protected LSP to the working LSP. This command can be applied only on a protected LSP. If Lockout of Protecting is enabled, then the working LSP becomes active and the protected LSP becomes standby.

- **Clear Force Switch (no Lockout)**—This command is used to clear the force switch on a working LSP after which the working LSP becomes active and the protected LSP becomes standby.

- **Clear Manual Switch**—This command is used to clear the manual switch made on a working LSP, after which the working LSP becomes active and the protected LSP becomes standby.

- **Clear Lockout of Protecting (no Lockout)**—This command is used to clear the lockout of protecting made on a protected LSP. The working LSP becomes standby and the protected LSP becomes active after this command is executed.

**Figure 17-22** depicts the MPLS-TP topology along with the working and protected LSPs:

![Linear Protection for MPLS-TP](image)

**Note** In the above figure, you can find working and protected LSPs between two routers. In case of maintenance or network upgrade, the Force Switch and Manual Switch commands can be used to shut down the working LSP link. Similarly, the Lockout of Protecting command can be used to shut down the protected LSP link.

To switch traffic using the Force Switch or Manual Switch command:
Step 1 In the map view, right-click the required link and choose **Properties**. A list of tunnels for the selected link is displayed.

Step 2 Right-click on the required physical link and choose the **Manage MPLS-TP tunnels** option. The MPLS-TP tunnels’ commands dialog box is displayed.

**Note** If there are no MPLS-TP tunnels configured for the selected link, then a message indicating the absence of MPLS-TP tunnels is displayed.

Step 3 In the MPLS-TP tunnels’ commands dialog box, select the working LSP tunnel and select **Force Switch (Lockout)** or **Manual Switch** in the **Commands** field.

Step 4 Click **Execute Now**. You are prompted to confirm the operation.

Step 5 Click **Yes** to confirm. The status of the working LSP is updated as **Standby** and the status of the protected LSP is updated as **Active** after this operation.

To switch traffic using the Lockout of Protecting command:

Step 1 In the map view, right-click the required link and choose **Properties**. A list of tunnels for the selected link is displayed.

Step 2 Right-click on the required physical link and choose the **Manage MPLS-TP tunnels** option. The MPLS-TP tunnels’ commands dialog box is displayed.

Step 3 In the MPLS-TP tunnels’ commands dialog box, select the protected LSP tunnel and select **Lock of Protecting** in the **Commands** field.

Step 4 Click **Execute Now**. You are prompted to confirm the operation.

Step 5 Click **Yes** to confirm. The status of the working LSP is updated as **Active** and the status of the protected LSP is updated as **Standby** after this operation.

To clear the Force Switch or Manual switch on a working LSP:

Step 1 In the map view, right-click the required link and choose **Properties**. A list of tunnels for the selected link is displayed.

Step 2 Right-click on the required physical link and choose the **Manage MPLS-TP tunnels** option. The MPLS-TP tunnels’ commands dialog box is displayed.

Step 3 In the MPLS-TP tunnels’ commands dialog box, select the working LSP tunnel that has been locked and select **Clear Force Switch** or **Clear Manual Switch** in the **Commands** field.

Step 4 Click **Execute Now**. You are prompted to confirm the operation.

Step 5 Click **Yes** to confirm. The status of the working LSP is updated as **Active** and the status of the protected LSP is updated as **Standby** after this operation.

To clear the Lockout of Protecting on a protected LSP:

Step 1 In the map view, right-click the required link and choose **Properties**. A list of tunnels for the selected link is displayed.
Step 2 Right-click on the required physical link and choose the Manage MPLS-TP tunnels option. The MPLS-TP tunnels’ commands dialog box is displayed.

Step 3 In the MPLS-TP tunnels’ commands dialog box, select the protected LSP tunnel that has been locked and select Clear Lockout of Protecting in the Commands field.

Step 4 Click Execute Now. You are prompted to confirm the operation.

Step 5 Click Yes to confirm. The status of the protected LSP is updated as Active and the status of the working LSP is updated as Standby after this operation.

Visualization Status Enhancements- MPLS TP Tunnel

In the MPLS TP Tunnel, the following visualization status enhancements have been carried out:

Non Eligible LSPs

If the tunnel is not configured with protected LSP, i.e., the tunnel is configured with working LSP (Active-UP), the information column displays the value as Protected LSP is not configured. See Figure 17-24. This information is displayed for all non-eligible LSPs which are not eligible for bulk flow operations like FS, LOP, MS, LOCK.

Figure 17-23 Viewing the Working LSPs and Protected LSPs
In the above Figure 17-23, both the status of **Working LSP** and the **Protected LSP** are in up state. So, the **Information** field is blank.

### Lockout State

In the Lockout State, information value has been changed. If the **Working LSP** is down, it displays **Working LSP is Locked Out**. If the **Protected LSP** is down, it displays that the **Protected LSP is Locked Out**.

*Figure 17-24  Viewing the Lockout States of LSP*
In the above Figure 17-25 the commands that are executed on LSPs on the link are displayed. It will be enabled only when an eligible LSP is working/protected on the link.
Configuring MPLS-TE

The following table lists commands you can use to configure MPLS-TE and how to launch these commands. You can preview a command before executing it, or schedule it to run at a later time. You may be prompted to enter your device access credentials while executing a command.

Your permissions determine whether you can run these commands (see Permissions for Managing MPLS Services, page B-17). To find out if a device supports these commands, see the Cisco Prime Network 4.2.2 Supported Cisco VNEs. (You can also add support for new commands by downloading and installing Prime Network Device Packages (DPs); see the Cisco Prime Network 4.2.2 Administrator Guide.)

<table>
<thead>
<tr>
<th>Command</th>
<th>Navigation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure MPLS-TE</td>
<td>LSEs &gt; right-click Label Switching &gt; Commands &gt;</td>
<td>Configures MPLS at the device level or an interface level. Contains information on MPLS interfaces and</td>
</tr>
<tr>
<td>Global</td>
<td>Configuration</td>
<td>whether traffic engineering tunnels are configured.</td>
</tr>
<tr>
<td>Configure MPLS-TE</td>
<td>Routing Entities &gt; Routing Entity &gt; IP Interfaces</td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>tab, right-click the required interface &gt; Commands</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configuration</td>
<td></td>
</tr>
</tbody>
</table>

Configuring MPLS

The following table lists commands you can use to configure MPLS and how to launch these commands. You can preview a command before executing it, or schedule it to run at a later time. You may be prompted to enter your device access credentials while executing a command.

Your permissions determine whether you can run these commands (see Permissions for Managing MPLS Services, page B-17). To find out if a device supports these commands, see the Cisco Prime Network 4.2.2 Supported Cisco VNEs. (You can also add support for new commands by downloading and installing Prime Network Device Packages (DPs); see the Cisco Prime Network 4.2.2 Administrator Guide.)

<table>
<thead>
<tr>
<th>Command</th>
<th>Navigation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure MPLS</td>
<td>LSEs &gt; right-click Label Switching &gt; Commands &gt;</td>
<td>Configures MPLS LDP discovery parameters to discover core MPLS networks. This also includes</td>
</tr>
<tr>
<td>Discovery</td>
<td>Configuration</td>
<td>specifying the discovery method.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure MPLS</td>
<td>LSEs &gt; Label Switching &gt; right-click on a selected ID in the MPLS Interface tab &gt; Commands &gt; Command</td>
<td>Configures MPLS static and dynamic label range.</td>
</tr>
<tr>
<td>Label Range</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable MPLS on Interface</td>
<td>LSEs &gt; Label Switching &gt; right-click on a selected ID in the MPLS Interface tab &gt; Commands &gt; Configuration</td>
<td>Enables/disables MPLS protocol on an interface. Contains information on MPLS interfaces and whether traffic engineering tunnels are configured on an interface.</td>
</tr>
<tr>
<td>Disable MPLS on Interface</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 17      Managing MPLS Networks

Configuring RSVP

The following RSVP commands manage a reserved-bandwidth path between hosts or the end systems to predetermine and ensure Quality of Service (QoS) for their data transmission. You can preview a command before executing it, or schedule it to run at a later time. You may be prompted to enter your device access credentials while executing a command.

Your permissions determine whether you can run these commands (see Permissions for Vision Client NE-Related Operations, page B-4). To find out if a device supports these commands, see the Cisco Prime Network 4.2.2 Supported Cisco VNEs. (You can also add support for new commands by downloading and installing Prime Network Device Packages (DPs); see the Cisco Prime Network 4.2.2 Administrator Guide.)

<table>
<thead>
<tr>
<th>Command</th>
<th>Navigation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure RSVP</td>
<td>LSEs &gt; right-click Label Switching &gt; Commands &gt; Configuration</td>
<td>Configures RSVP on a device or an interface.</td>
</tr>
<tr>
<td>Delete RSVP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable RSVP On Interface</td>
<td>Routing Entities &gt; Routing Entity &gt; IP Interfaces tab, right-click the required interface &gt; Commands &gt; Configuration</td>
<td></td>
</tr>
<tr>
<td>Disable RSVP On Interface</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Configuring BGP

The following BGP commands configure the routing protocol to communicate with the other sites and VRFs. BGP neighbors should be configured as part of BGP routing. At least one neighbor and at least one address family must be configured to enable BGP routing.

You can preview a command before executing it, or schedule it to run at a later time. You may be prompted to enter your device access credentials while executing a command.

Your permissions determine whether you can run these commands (see Permissions for Vision Client NE-Related Operations, page B-4). To find out if a device supports these commands, see the Cisco Prime Network 4.2.2 Supported Cisco VNEs. (You can also add support for new commands by downloading and installing Prime Network Device Packages (DPs); see the Cisco Prime Network 4.2.2 Administrator Guide.)
Configuring VRRP

The following VRRP commands configure the VRRP protocol on routers. These commands configure transparent failover at the first-hop IP router, enabling a group of routers to form a single virtual router. You can preview a command before executing it, or schedule it to run at a later time. You may be prompted to enter your device access credentials while executing a command.

Your permissions determine whether you can run these commands (see Permissions for Vision Client NE-Related Operations, page B-4). To find out if a device supports these commands, see the Cisco Prime Network 4.2.2 Supported Cisco VNEs. (You can also add support for new commands by downloading and installing Prime Network Device Packages (DPs); see the Cisco Prime Network 4.2.2 Administrator Guide.)

<table>
<thead>
<tr>
<th>Command</th>
<th>Navigation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create BGP Router</td>
<td>MPBGP &gt; right-click</td>
<td>Configures BGP routing and establish a BGP routing process with AS number and Router ID</td>
</tr>
<tr>
<td>Modify BGP Router</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete BGP Router</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create BGP Address Family</td>
<td></td>
<td>Enter various address family configuration modes that uses IPv4, IPv6, L2VPN, VPNV4 or VPNV6 address prefixes.</td>
</tr>
<tr>
<td>Modify BGP Address Family</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete BGP Address Family</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create BGP Neighbor</td>
<td>MPBGP &gt; MPBGP &gt; right-click on the BGP neighbour in the content pane &gt; Commands &gt; Configuration</td>
<td>Places the router in neighbor configuration mode for BGP routing and configures the neighbor IP address as a BGP peer.</td>
</tr>
<tr>
<td>Modify BGP Neighbor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete BGP Neighbor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Show VRRP</td>
<td>Routing Entities &gt; Routing Entity &gt; IP Interfaces tab, right-click the required interface &gt; Commands &gt; Configuration</td>
<td></td>
</tr>
</tbody>
</table>

Configuring Bundle Ethernet

Configure a bundle of one or more ports to form a single link using bundle ethernet commands.
The following table lists the supported bundle ethernet commands. You can preview a command before executing it, or schedule it to run at a later time. You may be prompted to enter your device access credentials while executing a command.

Your permissions determine whether you can run these commands (see Appendix B, “Permissions Required to Perform Tasks Using the Prime Network Clients”). To find out if a device supports these commands, see the Cisco Prime Network 4.2.2 Supported Cisco VNEs. (You can also add support for new commands by downloading and installing Prime Network Device Packages (DPs); see the Cisco Prime Network 4.2.2 Administrator Guide.)

<table>
<thead>
<tr>
<th>Command</th>
<th>Navigation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Bundle</td>
<td>Physical Inventory &gt; Chassis &gt; Slot &gt; Ethernet Port &gt; Commands &gt; Configuration</td>
<td>Configuring an Ethernet link bundle involves creating a bundle and adding member interfaces to that bundle.</td>
</tr>
</tbody>
</table>

**Viewing MPLS LDP, Static Information**

The Multi-Protocol Label Switching (MPLS) is a scalable, protocol-independent transport. In an MPLS network, data packets are assigned labels. The packet-forwarding decisions are made solely based on the contents of this label, without the need of examining the packet itself. This enables creating end-to-end circuits across any type of transport medium using any protocol.

Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) enables peer label switch routers (LSRs) in an MPLS network to exchange label binding information for supporting hop-by-hop forwarding in an MPLS network.

As part of the topological link support, Prime Network started supporting two new service alarms MPLS Link down and MPLS Link up, besides MPLS-TP inventory information. These alarms are raised on the MPLS links during misconfigurations of physical links or shut down of physical interfaces. To view the service alarms supported by Prime Network, refer Cisco Prime Network Supported Service Alarms.
Figure 17-26  Viewing MPLS link configured with LDP and Static