CHAPTER 17

Monitoring MPLS Services

The following topics describe how to view and manage aspects of Multiprotocol Label Switching (MPLS) services using Cisco Prime Network Vision (Prime Network Vision), 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. Topics include:

- User Roles Required to Work with MPLS Networks, page 17-1
- Working with MPLS-TP Tunnels, page 17-4
- Viewing VPNs, page 17-19
- Managing VPNs, page 17-22
- Working with VPN Overlays, page 17-25
- Monitoring MPLS Services, page 17-29

User Roles Required to Work with MPLS Networks

This topic identifies the roles that are required to work with MPLS networks. Prime Network determines whether you are authorized to perform a task as follows:

- For GUI-based tasks (tasks that do not affect elements), authorization is based on the default permission that is assigned to your user account.
- For element-based tasks (tasks that do affect elements), authorization is based on the default permission that is assigned to your account. That is, whether the element is in one of your assigned scopes and whether you meet the minimum security level for that scope.

For more information on user authorization, see the *Cisco Prime Network 3.8 Administrator Guide*.

The following tables identify the tasks that you can perform:

- Table 17-1 identifies the tasks that you can perform if a selected element **is not in** one of your assigned scopes.
- Table 17-2 identifies the tasks that you can perform if a selected element **is in** one of your assigned scopes.

By default, users with the Administrator role have access to all managed elements. To change the Administrator user scope, see the topic on device scopes in the *Cisco Prime Network 3.8 Administrator Guide*.

Table 17-1 Default Permission/Security Level Required for Working with MPLS Networks - Element Not in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Working with Elements					
Add tunnels to VPNs	—	X	X	X	X
Add VPNs to a map	—	—	X	X	X
Create VPNs	—	—	X	X	X
Move virtual routers between VPNs	—	X	X	X	X
Remove tunnels from VPNs	X	X	X	X	X
Remove VPNs from a map	—	—	X	X	X
Viewing Element Properties					
View 6RD properties	—	—	—	—	X
View BFD properties	—	—	—	—	X
View cross-VRF routing entries	—	—	—	—	X
View LSE properties	—	—	—	—	X
View MP-BGP information	—	—	—	—	X
View MPLS TE tunnel information	—	—	—	—	X
View MPLS-TP information	—	—	—	—	X
View port configurations	—	—	—	—	X
View pseudowire end-to-end emulation tunnels	—	—	—	—	X
View rate limit information	—	—	—	—	X
View the ARP table	—	—	—	—	X
View the NDP table	—	—	—	—	X
View VPN properties	X	X	X	X	X
View VPNs	X	X	X	X	X
View VRF egress and ingress adjacents	—	—	—	—	X
View VRF properties	—	—	—	—	X
Working with Overlays					
Add VPN overlays	X	X	X	X	X
Display or hide VPN overlays	X	X	X	X	X
Remove VPN overlays	X	X	X	X	X

Table 17-2 Default Permission/Security Level Required for Working with MPLS Networks - Element in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
VPNs and VRFs					
Add tunnels to VPNs	—	X	X	X	X
Add VPNs to a map	—	—	X	X	X
Create VPNs	—	—	X	X	X
Display VRF egress and ingress adjacents	—	—	—	—	X
Move virtual routers between VPNs	—	X	X	X	X
Remove tunnels from VPNs	X	X	X	X	X
Remove VPNs from a map	—	—	X	X	X
View VPN properties	X	X	X	X	X
View VPNs	X	X	X	X	X
View VRF properties	—	—	—	—	X
VPN Overlays					
Add VPN overlays	X	X	X	X	X
Display or hide VPN overlays	X	X	X	X	X
Remove VPN overlays	X	X	X	X	X
Routing Entities					
View the ARP table	X	X	X	X	X
View the NDP table	X	X	X	X	X
View rate limit information	X	X	X	X	X
Other					
View 6RD properties	X	X	X	X	X
View BFD properties	X	X	X	X	X
View cross-VRF routing entries	X	X	X	X	X
View LSE properties	X	X	X	X	X
View MP-BGP information	X	X	X	X	X
View MPLS TE tunnel information	X	X	X	X	X
View MPLS-TP information	X	X	X	X	X
View port configurations	X	X	X	X	X
View pseudowire end-to-end emulation tunnels	X	X	X	X	X

Related Topics

- Viewing VPNs, page 17-19
- Managing VPNs, page 17-22
- Working with VPN Overlays, page 17-25

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 Prime Network Vision 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 Prime Network Vision:

- Adding an MPLS-TP Tunnel, page 17-5
- Viewing MPLS-TP Tunnel Properties, page 17-7
- Viewing LSPs Configured on an Ethernet Link, page 17-12
- Viewing LSP Endpoint Redundancy Service Properties, page 17-14
- Applying an MPLS-TP Tunnel Overlay, page 17-17
- Viewing MPLS-TP BFD session properties—See Viewing BFD Session Properties, page 17-48.

Adding an MPLS-TP Tunnel

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

To add an MPLS-TP tunnel to a map:

Step 1 In Prime Network Vision, 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:

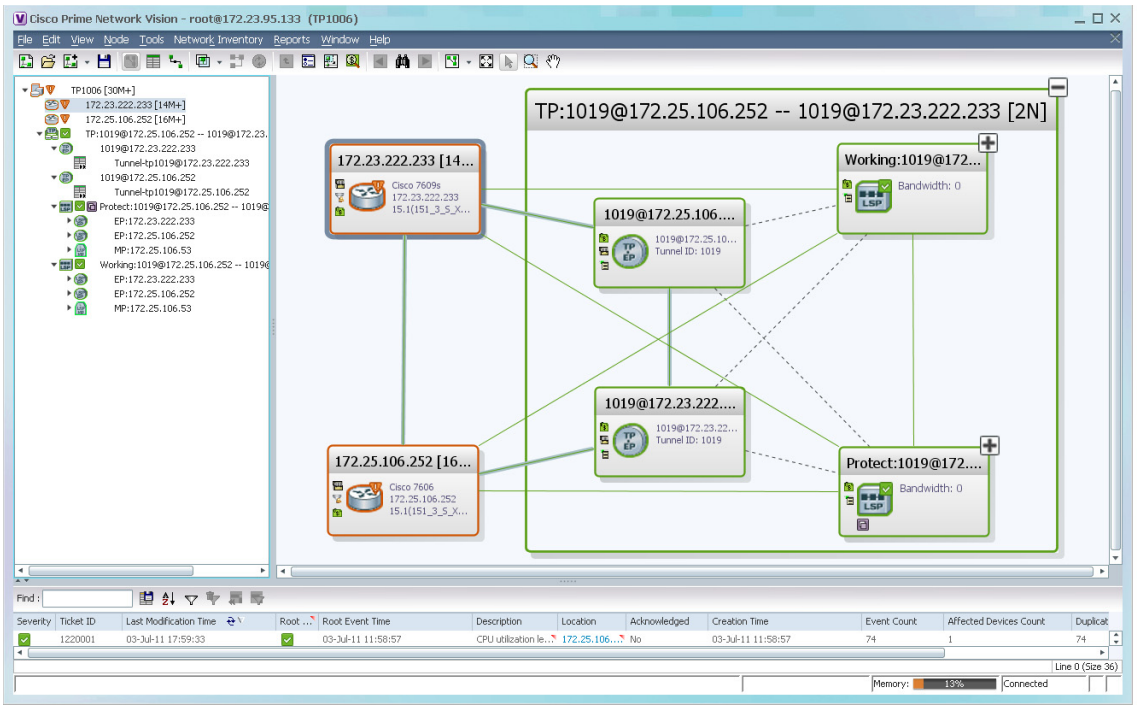
- Choose a search category, enter a search string, then click **Go** to narrow search results to a range of MPLS-TP tunnels or a specific MPLS-TP tunnel. Search categories include:
  - Description
  - Name
  - System Name
- Choose **Show All** to display all the MPLS-TP tunnels.

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.

Figure 17-1 MPLS-TP Tunnel in Prime Network Vision Map



In Figure 17-1:

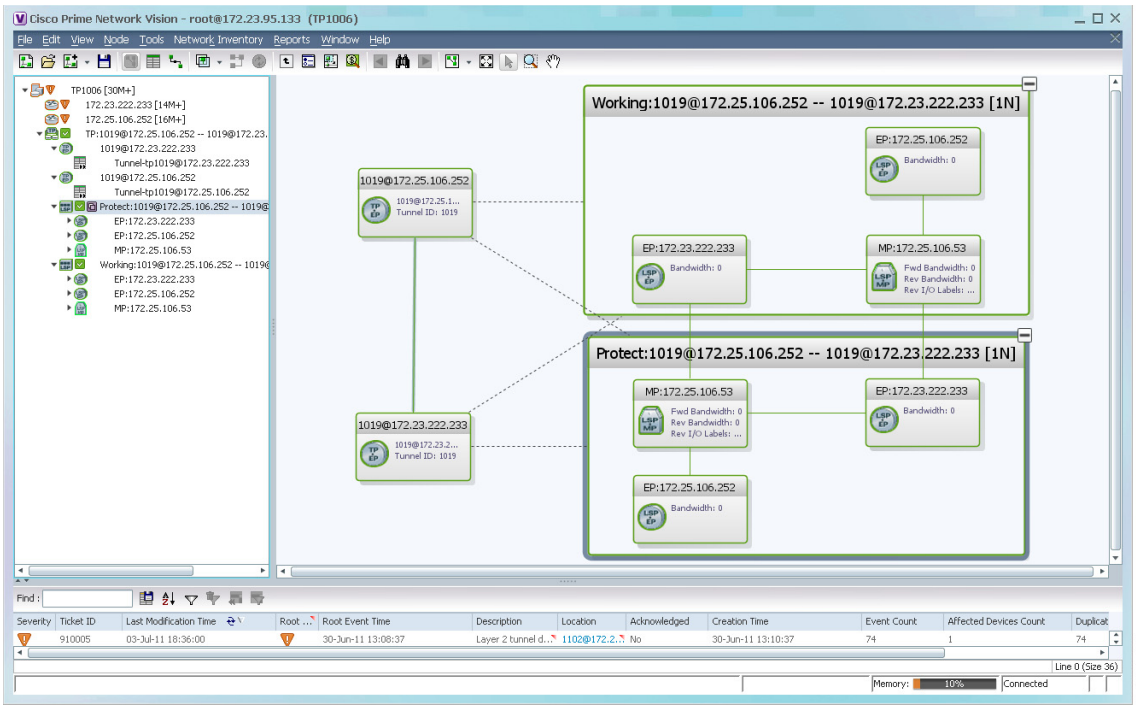
- The devices are on the left side of the map, and the MPLS-TP tunnel is displayed in a thumbnail on the right.
- The devices are connected to each other and to the MPLS-TP tunnel via tunnels.
- Physical links connect the devices to the Working and Protected LSPs.
- A redundancy service badge is displayed 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 17-2), you can see components and links in the MPLS-TP tunnel, including:

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

Figure 17-2 MPLS-TP Tunnel Expanded



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 17-14.

Related Topics

- Viewing MPLS-TP Tunnel Properties, page 17-7
- Applying an MPLS-TP Tunnel Overlay, page 17-17
- Viewing BFD Session Properties, page 17-48

Viewing MPLS-TP Tunnel Properties

Prime Network Vision 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:

- Routing Entities—See Viewing Routing Entities, page 17-34.
- LSEs—See Viewing Label Switched Entity Properties, page 17-42.
- Pseudowires— See Viewing Pseudowire End-to-End Emulation Tunnels, page 17-51.

To view MPLS-TP tunnel properties:

Step 1 Right-click the required device in Prime Network Vision 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 17-3.

Figure 17-3 MPLS-TP Tunnel Properties in Logical Inventory

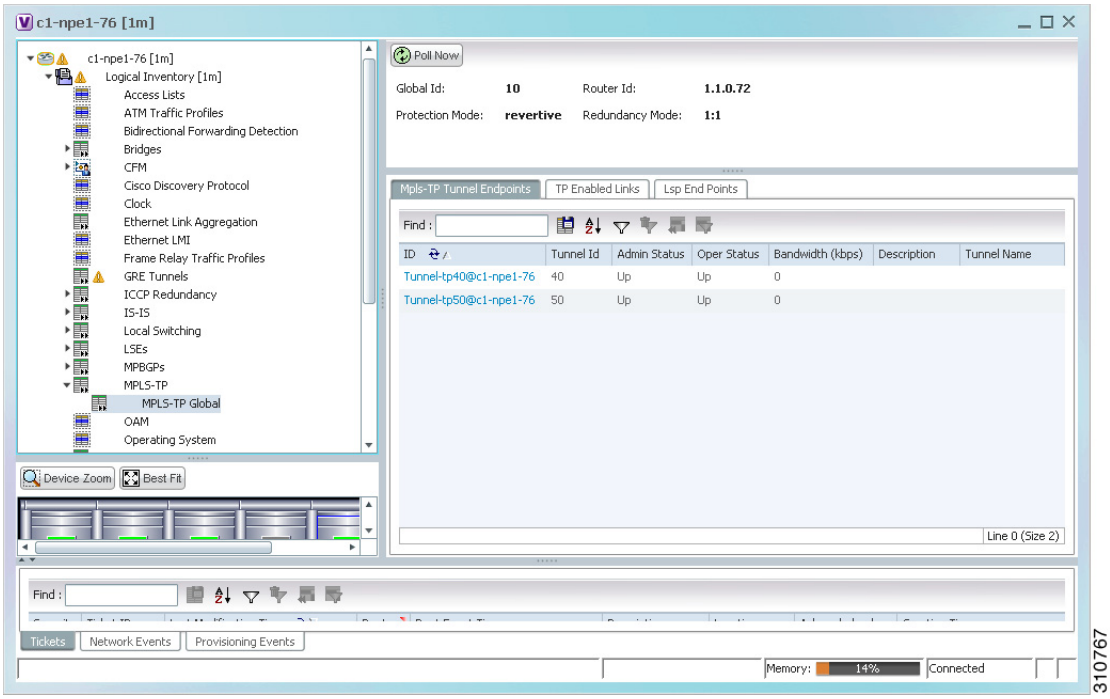


Table 17-3 describes the information that is available for MPLS-TP tunnels. The information that is displayed depends on the configuration.

Table 17-3 MPLS-TP Tunnel Properties in Logical Inventory

Field	Description
Global ID	Globally unique Attachment Interface Identifier (AII) for MPLS-TP derived from the Autonomous System Number (ASN) of the system hosting the PEs.
Router ID	MPLS-TP source node identifier for this element in the form of an IPv4 address.
Protection Mode	Whether the transmitting endpoint is in revertive or nonrevertive mode: • Revertive—If the protection mode is revertive and a failed path is restored, the traffic automatically returns, or reverts, to the original path. • 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.
Redundancy Mode	Level of redundancy for the MPLS-TP tunnel: 1:1, 1+1, or 1:N.

Table 17-3 MPLS-TP Tunnel Properties in Logical Inventory (continued)

Field	Description
MPLS-TP Tunnel Endpoints Tab	
ID	Tunnel endpoint identifier as a Tunnel-tp interface on the selected network element.
Tunnel ID	Unique tunnel identifier.
Admin Status	Administrative status of the tunnel: Up or Down.
Oper Status	Operational status of the tunnel: Up or Down.
Bandwidth (kbps)	Configured bandwidth (in Kb/s) for the tunnel.
Description	Tunnel description.
TP Enabled Links Tab	
Link ID	Identifier assigned to the MPLS-TP interface.
Interface	Hyperlink to the interface in physical inventory.
Next Hop	IP address of the next hop in the path.
LSP End Points Tab	
LSP ID	LSP identifier, derived from both endpoint identifiers and using the format *src-node-ID*::*src-tunnel-number*::*dest-node-ID*::*dest-tunnel-number* where: • *src-node-ID* represents the identifier of the node originating the signal exchange. • *src-tunnel-number* represents source tunnel identifier. • *dest-node-ID* represents the identifier of the target node. • *dest-tunnel-number* represents the destination tunnel identifier.
LSP Type	Indicates whether the LSP is active (Working) or backup (Protect).
In Label	Incoming label identifier.
Out Label	Outgoing label identifier.
Out Interface	Outgoing interface hyperlinked to the relevant entry in physical inventory.
Bandwidth (kbps)	Bandwidth specification in Kb/s.
Role (Oper Status)	Role of the LSP endpoint (Active or Standby) with the operational status (UP or DOWN).

Table 17-3 MPLS-TP Tunnel Properties in Logical Inventory (continued)

Field	Description
LSP Mid Points Tab	
LSP ID	LSP identifier, derived from both endpoint identifiers and using the format *src-node-ID*::*src-tunnel-number*::*dest-node-ID*::*dest-tunnel-number* where: • *src-node-ID* represents the identifier of the node originating the signal exchange. • *src-tunnel-number* represents source tunnel identifier. • *dest-node-ID* represents the identifier of the target node. • *dest-tunnel-number* represents the destination tunnel identifier.
LSP Type	Indicates whether the LSP is active (Working) or backup (Protect).
Forward In Label	Incoming label identifier in the forward direction (source to destination).
Forward Out Label	Label selected by the next hop device in the forward direction.
Reverse In Label	Incoming label identifier in the reverse direction (destination to source).
Reverse Out Label	Label selected by the next hop device in the reverse direction.
Forward Out Interface	Outgoing interface in the forward direction, hyperlinked to its entry in physical inventory.
Forward Bandwidth (kbps)	Bandwidth specification in Kb/s for the forward direction.
Reverse Out Link ID	Link identifier assigned to the outgoing interface in the reverse direction.
Reverse Out Interface	Outgoing interface in the reverse direction, hyperlinked to its entry in physical inventory.
Reverse Bandwidth	Bandwidth specification in Kb/s for the reverse direction.
Internal ID	Identifier associated with the parent entity of the link. Using an internal identifier ensures that individual LSP links do not participate in multiple network LSPs.

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 17-4.

Figure 17-4 MPLS-TP Tunnel Properties Window

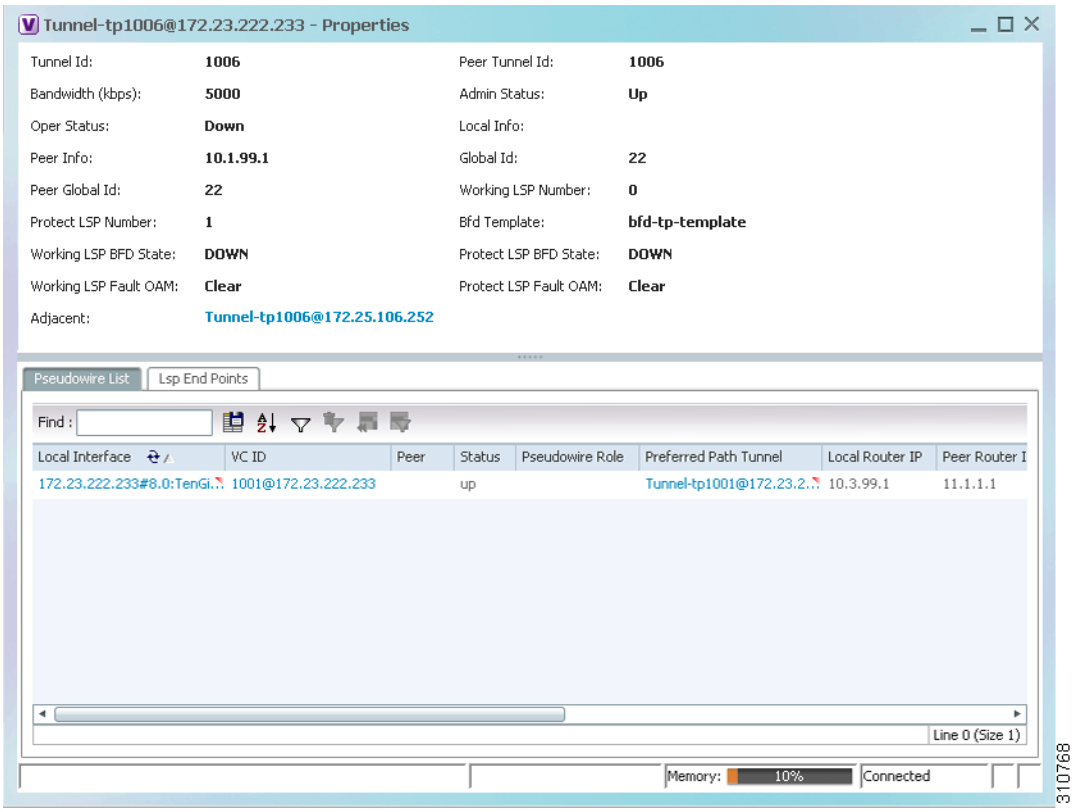


Table 17-4 describes the information available in the top portion of the MPLS-TP Tunnel Properties window. For information about the tabs that are displayed, see Table 17-3.

Table 17-4 MPLS-TP Tunnel Properties Window

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

Table 17-4 MPLS-TP Tunnel Properties Window (continued)

Field	Description
Protect LSP Number	Number assigned to the protected LSP. By default, the working LSP number is 0 and the protected LSP number is 1.
BFD Template	BFD template associated with this MPLS-TP tunnel.
Working LSP BFD State	Configured state of the working LSP BFD template: Up or Down.
Protect LSP BFD State	Configured state of the protected LSP BFD template: Up or Down.
Working LSP Fault OAM	Indicates that a fault has been detected on the working LSP.
Protect LSP Fault OAM	Indicates that a fault has been detected on the protected LSP.
Tunnel Name	Tunnel name.
Adjacent	Hyperlink to the adjacent endpoint in logical inventory.

Related Topics

- Working with MPLS-TP Tunnels, page 17-4
- Adding an MPLS-TP Tunnel, page 17-5
- Applying an MPLS-TP Tunnel Overlay, page 17-17

Viewing LSPs Configured on an Ethernet Link

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

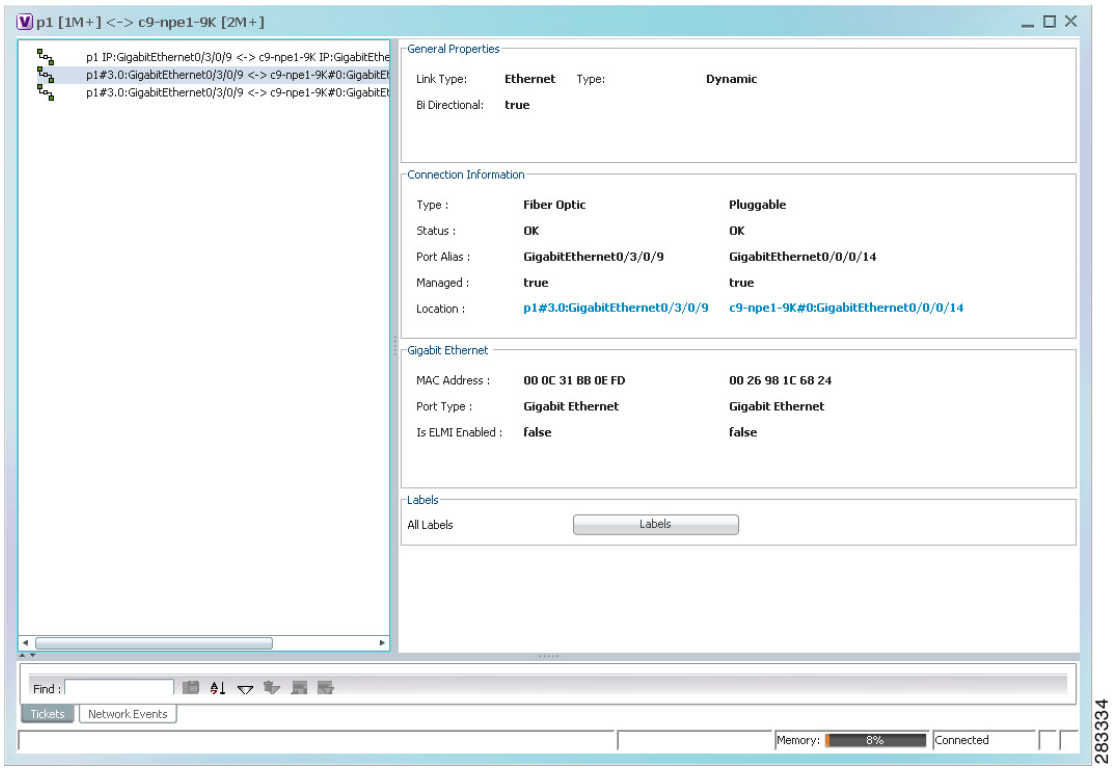
To view LSPs configured on an Ethernet link:

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 17-5.

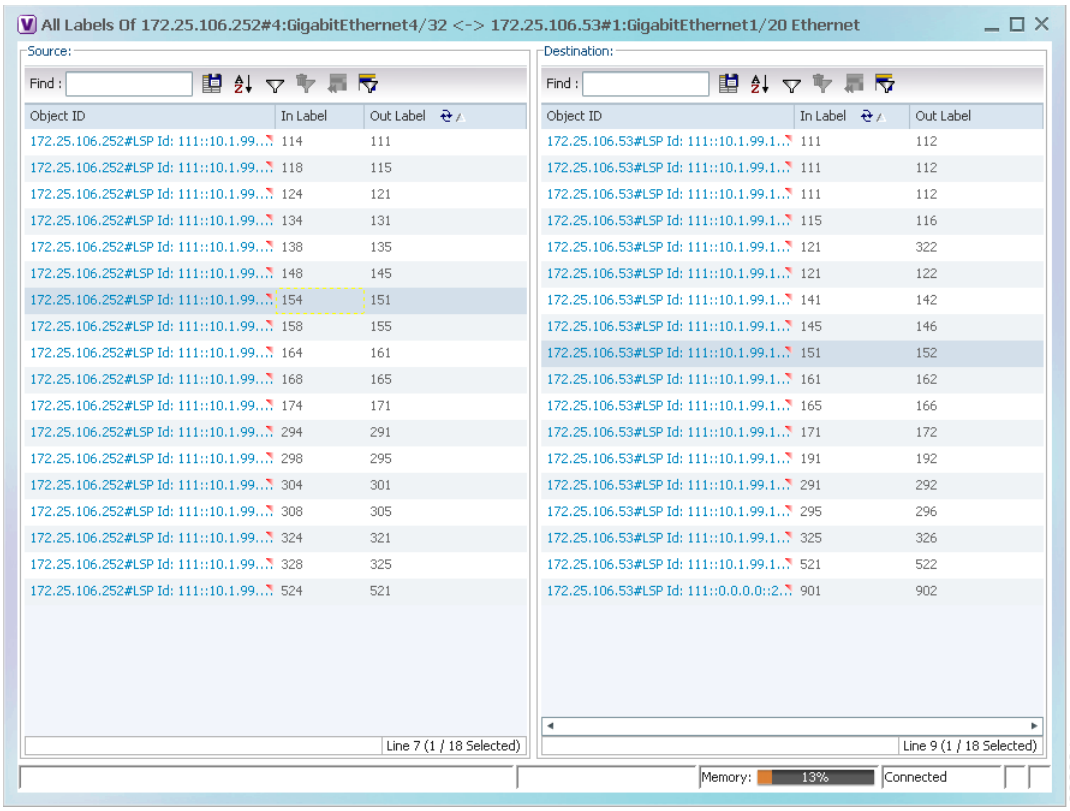
Figure 17-5 Link Properties Window with All Labels Button



Step 3 Click **Labels**.

The All Labels window is displayed as shown in Figure 17-6 with the LSP sources and destinations.

Figure 17-6 All Labels 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.

Related Topics

- Working with MPLS-TP Tunnels, page 17-4
- Viewing MPLS-TP Tunnel Properties, page 17-7
- Applying an MPLS-TP Tunnel Overlay, page 17-17

Viewing LSP Endpoint Redundancy Service Properties

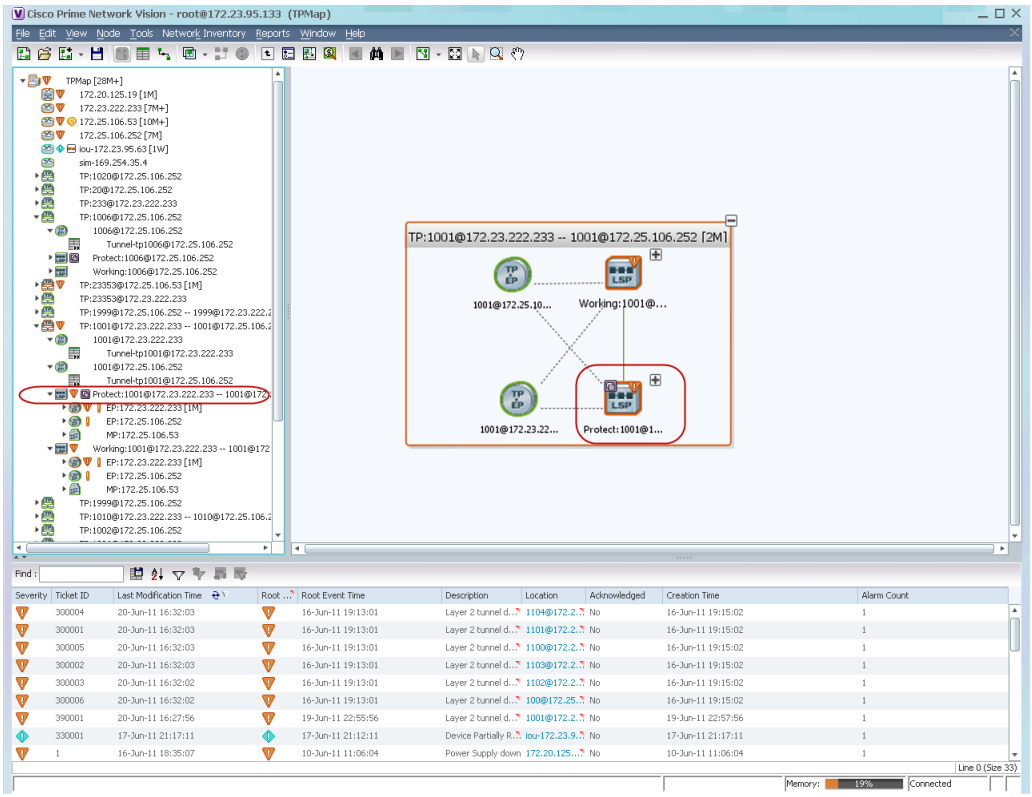
If an LSP endpoint in an MPLS-TP tunnel is configured for redundancy service, a redundancy service badge is applied to the secondary (backup) LSP endpoint in the navigation and map panes in Prime Network Vision. Additional redundancy service details are provided in the LSP endpoint properties window 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 17-7.

Figure 17-7 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 17-8.

Figure 17-8 LSP Endpoint Properties Window

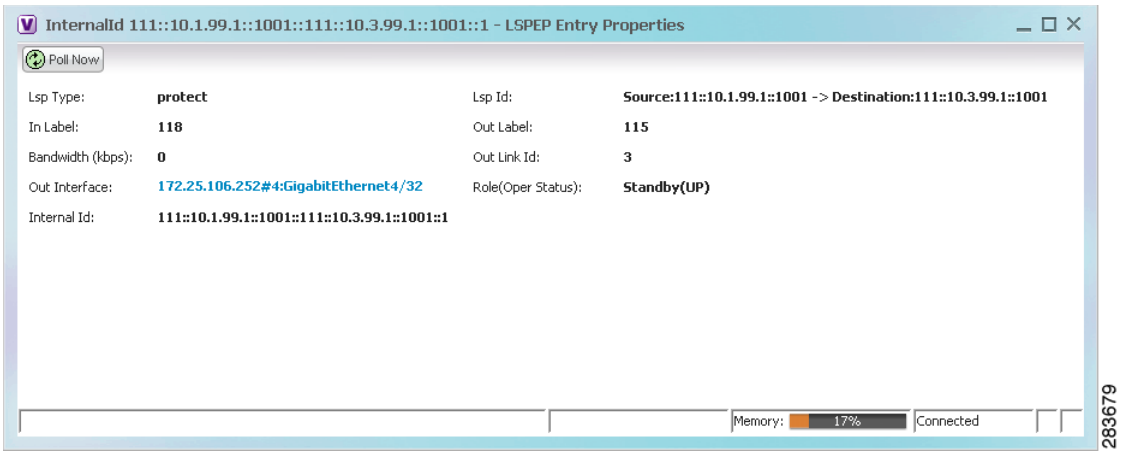


Table 17-5 describes the information displayed in the LSP Endpoint Properties window.

Table 17-5 LSP Endpoint Properties Window

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

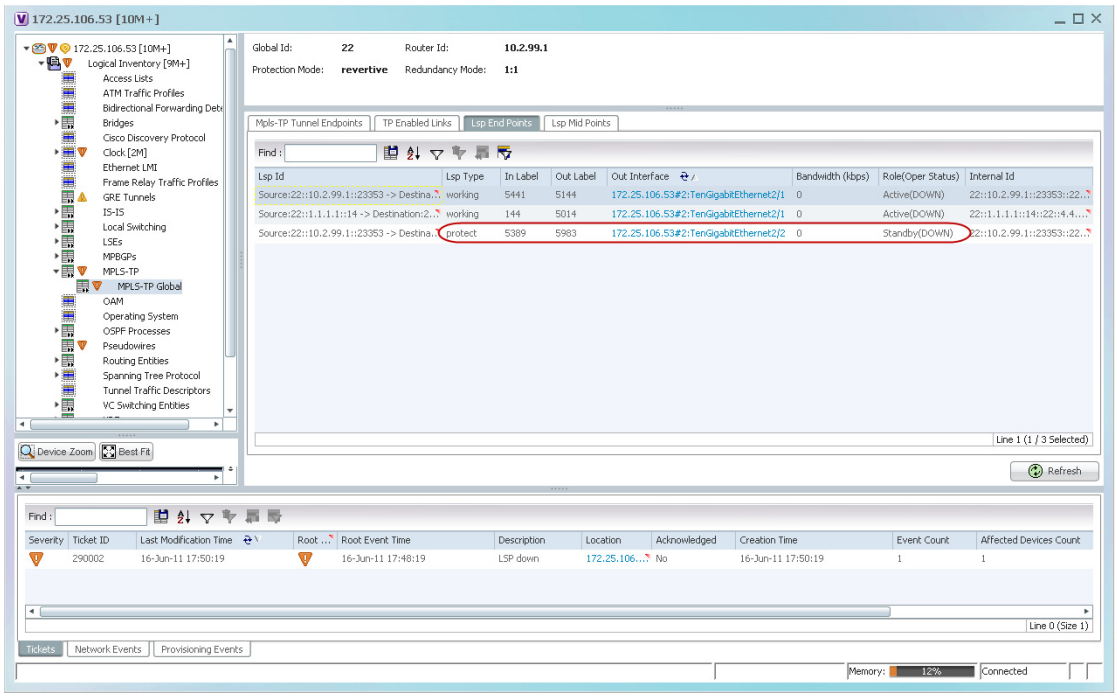
Step 3 To view LSP endpoint redundancy status in inventory, double-click the element on which the MPLS-TP tunnel is configured.

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 17-9):

- 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.

Figure 17-9 LSP End Points Tab in Logical Inventory



Related Topics

- Working with MPLS-TP Tunnels, page 17-4
- Viewing LSPs Configured on an Ethernet Link, page 17-12
- Applying an MPLS-TP Tunnel Overlay, page 17-17

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 Prime Network Vision, 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:

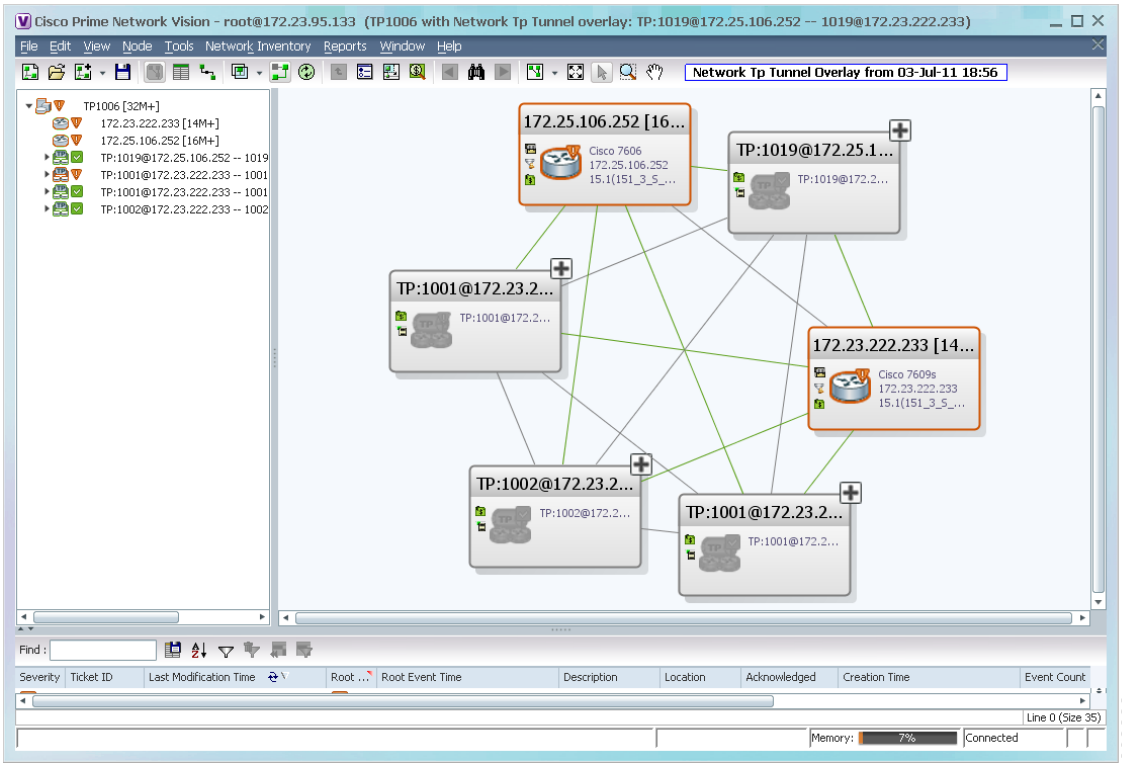
- Choose a search category, enter a search string, then click **Go** to narrow the search results to a range of MPLS-TP tunnels or a specific MPLS-TP tunnel. Search categories include:
  - Description
  - Name
  - System Name

  The search condition is "contains." Search strings are case-insensitive. For example, if you choose the Name category and enter "net," Prime Network Vision 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 17-10.

Figure 17-10 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.

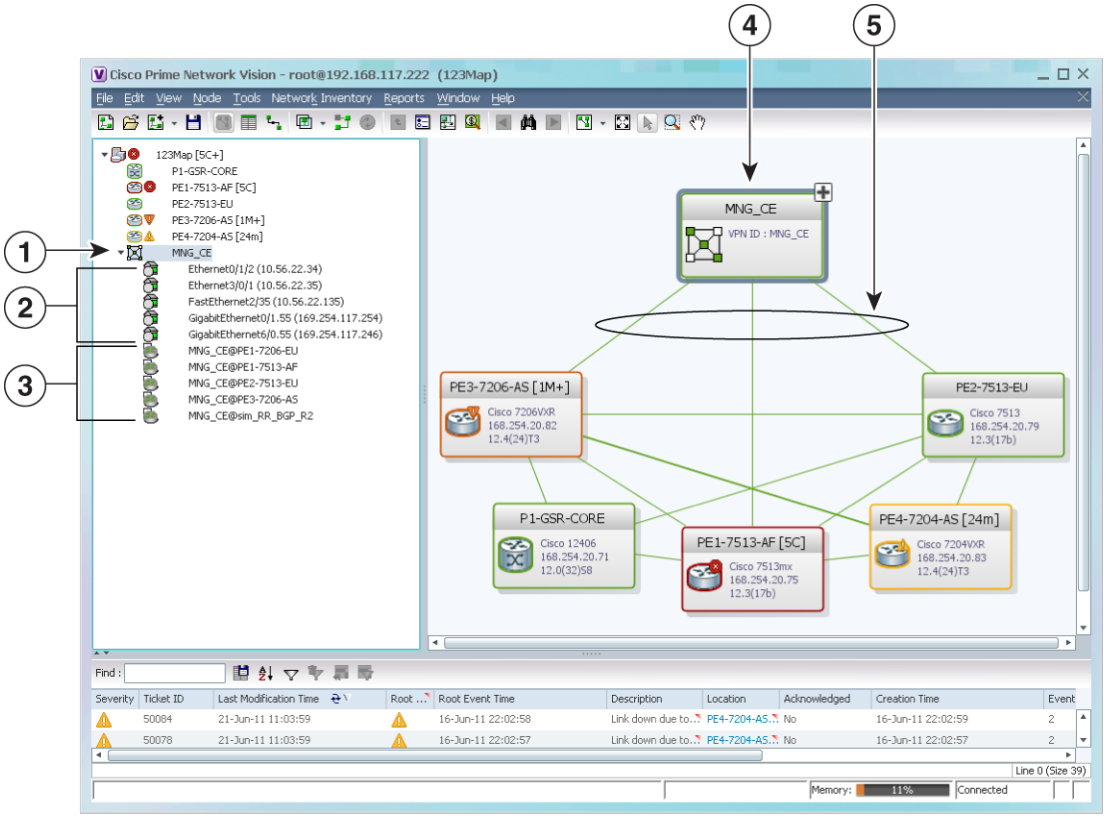
Related Topics

- Working with MPLS-TP Tunnels, page 17-4
- Adding an MPLS-TP Tunnel, page 17-5
- Viewing MPLS-TP Tunnel Properties, page 17-7

Viewing VPNs

Figure 17-11 shows a VPN displayed in the Prime Network Vision 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.

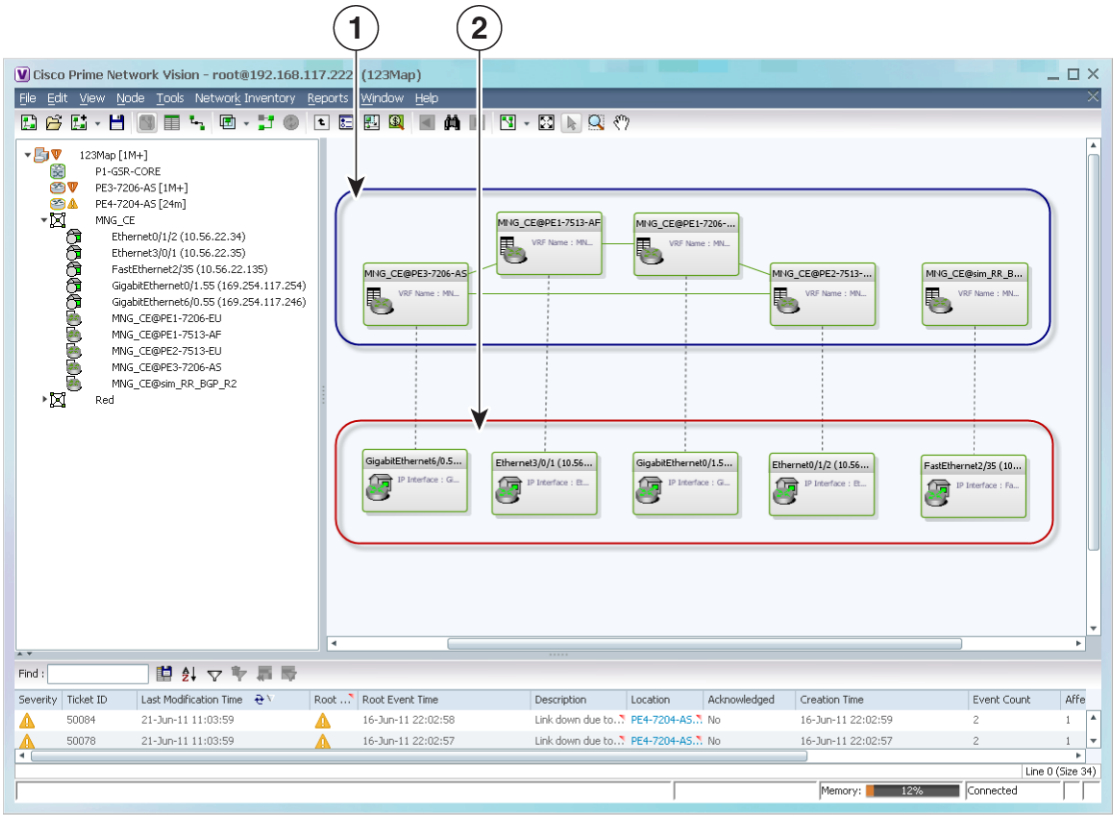
Figure 17-11 VPN in Prime Network Vision Map View



1	VPN in the navigation tree	**5**	VPN in the map view
2	Sites	**6**	VPN links (IPv4 and IPv6 aware)
3	Virtual routers		

Figure 17-12 shows a VPN with details, including virtual routers and sites, in the Prime Network Vision map view.

Figure 17-12 VPN in Prime Network Vision Map View with VRFs and Sites



1	Virtual routers
2	Sites

The Prime Network Vision 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 Prime Network Vision Status Indicators, page 2-30.

Table 17-6 shows the VPN icons in the Prime Network Vision map view.

Table 17-6 VPN Icons in Prime Network Vision Map View

Icon	Description
	Root (map name) or aggregation
	VPN
	Virtual router
	Site

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 Prime Network Vision 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.

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

Related Topics

- Creating a VPN, page 17-22
- Adding a VPN to a Map, page 17-23
- Viewing Additional VPN Properties, page 17-21

Viewing Additional VPN Properties

Prime Network Vision 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 17-7 Displaying Additional VPN Properties

Object	Option	For Additional Information
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 17-29
VRF	Double-click a VRF to view the VRF properties window.	Viewing VRF Properties, page 17-30
Site	Double-click a site to view the IP Interface Properties window	Viewing Site Properties, page 17-30
Link	Double-click a link to view the link properties window. The properties that are depend on the link type.	Chapter 5, "Working with Links"

Managing VPNs

The following topics describe:

- Creating a VPN, page 17-22
- Adding a VPN to a Map, page 17-23
- Removing a VPN from a Map, page 17-24
- Moving a Virtual Router Between VPNs, page 17-25

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 Prime Network Vision 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.

Related Topics

- Adding a VPN to a Map, page 17-23
- Removing a VPN from a Map, page 17-24
- Applying VPN Overlays, page 17-26

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 Vision 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 Prime Network Vision, 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," Prime Network Vision 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 Prime Network Vision window content pane. In addition, any tickets are displayed in the ticket area.

Related Topics

- Managing a VPN Overlay Display in the Map View, page 17-27
- Applying VPN Overlays, page 17-26

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 Vision 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 Prime Network Vision 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.

Related Topics

- Managing a VPN Overlay Display in the Map View, page 17-27
- Viewing VPNs, page 17-19
- Applying VPN Overlays, page 17-26

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:

Step 1 In the Prime Network Vision navigation pane or map, right-click the virtual router and choose **Edit > Move selected**.

Step 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.

Related Topics

- Viewing Additional VPN Properties, page 17-21
- Viewing VPNs, page 17-19

Working with VPN Overlays

The following topics describe:

- Applying VPN Overlays, page 17-26
- Managing a VPN Overlay Display in the Map View, page 17-27
- Displaying VPN Callouts in a VPN Overlay, page 17-27

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 Prime Network Vision, 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," Prime Network Vision 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.

Related Topics

- Managing a VPN Overlay Display in the Map View, page 17-27
- Displaying VPN Callouts in a VPN Overlay, page 17-27
- Viewing VPNs, page 17-19

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**.

Related Topics

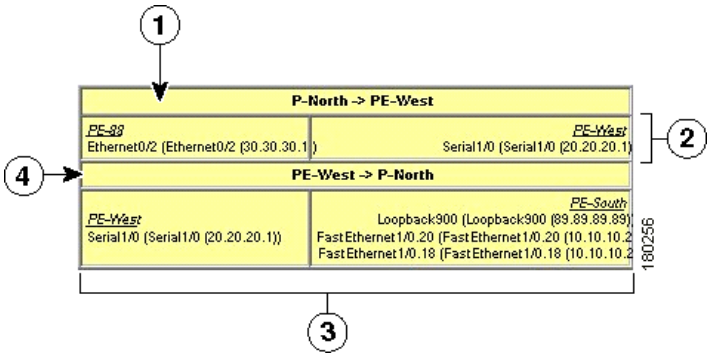
- Viewing VPNs, page 17-19
- Removing a VPN from a Map, page 17-24
- Displaying VPN Callouts in a VPN Overlay, page 17-27

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 17-13) 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 17-13 Callouts Window



1	Link details and direction. In this example, the link is from P-North to 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.
2	Details of the sites using the link and interlinks. In this example, the site PE-88 is linked to site PE-West.	**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 Prime Network Vision 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**.

Related Topics

- Managing a VPN Overlay Display in the Map View, page 17-27
- Viewing VPNs, page 17-19
- Viewing Additional VPN Properties, page 17-21

Monitoring MPLS Services

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

- Viewing VPN Properties, page 17-29
- Viewing Site Properties, page 17-30
- Viewing VRF Properties, page 17-30
- Viewing VRF Egress and Ingress Adjacents, page 17-33
- Viewing Routing Entities, page 17-34
- Viewing Label Switched Entity Properties, page 17-42
- Viewing MP-BGP Information, page 17-45
- Viewing BFD Session Properties, page 17-48
- Viewing Cross-VRF Routing Entries, page 17-51
- Viewing Pseudowire End-to-End Emulation Tunnels, page 17-51
- Viewing MPLS TE Tunnel Information, page 17-53

Viewing VPN Properties

To view the properties of a VPN:

Step 1 In the Prime Network Vision 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.

Related Topics

- Viewing Site Properties, page 17-30
- Viewing VRF Properties, page 17-30
- Viewing Routing Entities, page 17-34

Viewing Site Properties

Prime Network Vision 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 Vision automatically discovered for the device.

To view site properties, in the Prime Network Vision 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 17-8 Router IP Interface Properties Window for Sites

Field	Description
Name	Name of the site, such as FastEthernet4/1.252.
State	Interface state, either Up or Down.
IP Address	IP address of the interface.
Mask	Network mask.
Interface Description	Description applied to the interface.
Associated Entity	Element and interface associated with the site, hyperlinked to its entry in physical inventory.
Addresses Table	
Subnet	IP address and subnet mask. **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, page 16-3.
Type	Address type, such as Primary, Secondary, or IPv6 Unicast.

Related Topics

- Viewing VRF Properties, page 17-30
- Monitoring MPLS Services, page 17-29
- Viewing VPN Properties, page 17-29

Viewing VRF Properties

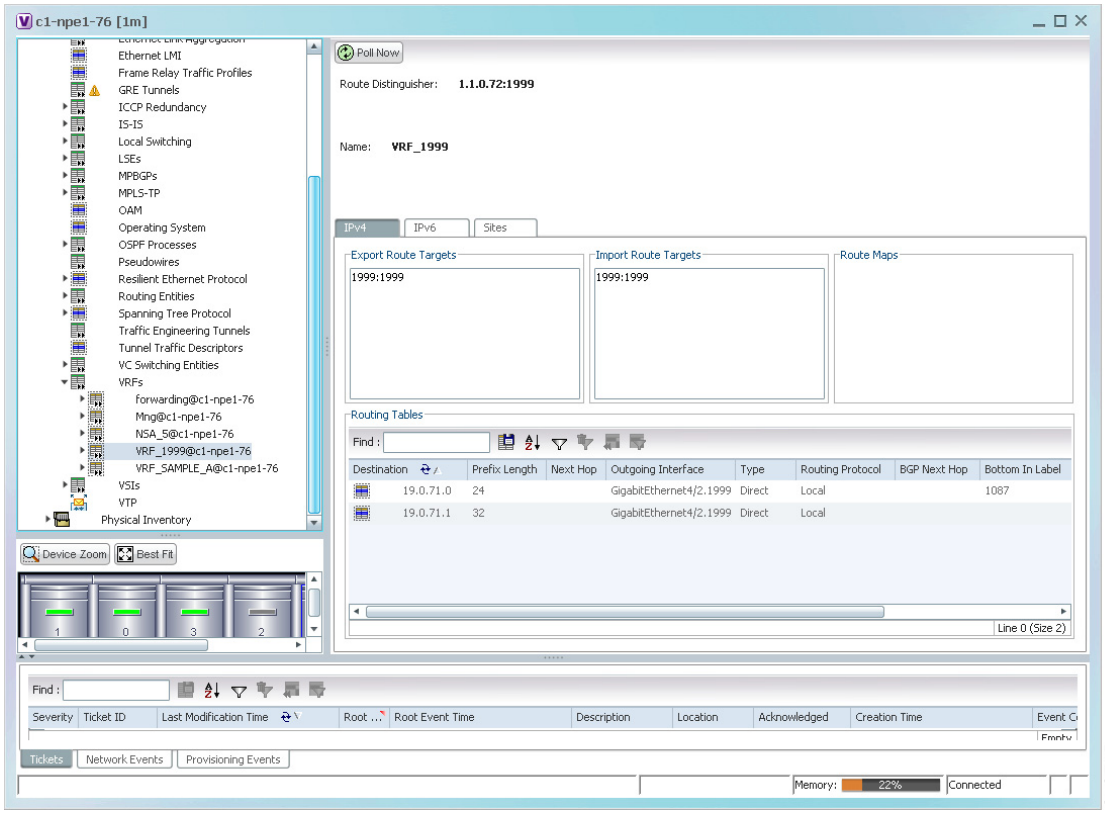
Prime Network Vision enables you to view VRF properties, including the VRF route distinguisher, import and export route targets, and any provisioned sites and VRF routes.

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 17-14.

Figure 17-14 VRF Properties



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 17-9 VRF Properties

Field	Description
Route Distinguisher	Route distinguisher configured in the VRF.
Name	VRF name.
Description	Description of the VRF.
IPv4 Tab	
Export Route Targets	IPv4 export route targets contained by the VRF.
Import Route Targets	IPv4 import route targets contained by the VRF.
Route Maps	Route maps for the VRF.
IPv6 Tab	
Export Route Targets	IPv6 export route targets contained by the VRF.
Import Route Targets	IPv6 import route targets contained by the VRF.
Route Maps	Route maps for the VRF.
Routing Tables	
Destination	Destination of the specific network.
Prefix Length	Length of the network prefix in bits.
Next Hop	Next routing hop.
Outgoing Interface	Name of the outgoing interface; displayed if the Routing Protocol type is local.
Type	Route type: Direct (local), Indirect, or Static.
Routing Protocol	Routing protocol used to communicate with the other sites and VRFs: BGP or local.
BGP Next Hop	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.
Bottom In Label	Innermost label that is expected when MPLS traffic is received.
Bottom Out Label	Innermost label sent with MPLS traffic.
Outer Label	Outermost or top label in the stack used for MPLS traffic.
Sites Tab	
Name	Site name.
IP Address	IP address of the interface.
Mask	Subnet mask.
State	State of the subinterface: Up or Down.
Associated Entity	Element and interface associated with the site, hyperlinked to its entry in physical inventory.
Description	Interface description.
Input Access List	Access list applied to the inbound traffic.
Output Access List	Access list applied to the outbound traffic.

Table 17-9 VRF Properties (continued)

Field	Description
Rate Limits	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. **Note** 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 17-39. **Note** The Input Access, Output Access, and Rate Limits parameters apply only to Cisco IOS devices.
IP Sec Map Name	IP Security (IPsec) map name.
Site Name	Name of the business element to which the interface is attached.

Related Topics

- Viewing VRF Egress and Ingress Adjacents, page 17-33
- Viewing Routing Entities, page 17-34
- Viewing Label Switched Entity Properties, page 17-42

Viewing VRF Egress and Ingress Adjacents

Prime Network Vision 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 17-10 describes the information displayed in the Adjacents window.

Table 17-10 VRF Adjacents Properties Window

Field	Description
Name	VRF name.
Route Distinguisher	Route distinguisher configured in the VRF.
VRF V6 Table	IPv6 route distinguisher if IPv6 is configured.

Related Topics

- Viewing Routing Entities, page 17-34
- Viewing VRF Properties, page 17-30
- Viewing Label Switched Entity Properties, page 17-42

Viewing Routing Entities

To view routing entities:

Step 1 Right-click the required device in Prime Network Vision 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 17-15.

Figure 17-15 Routing Entity Table

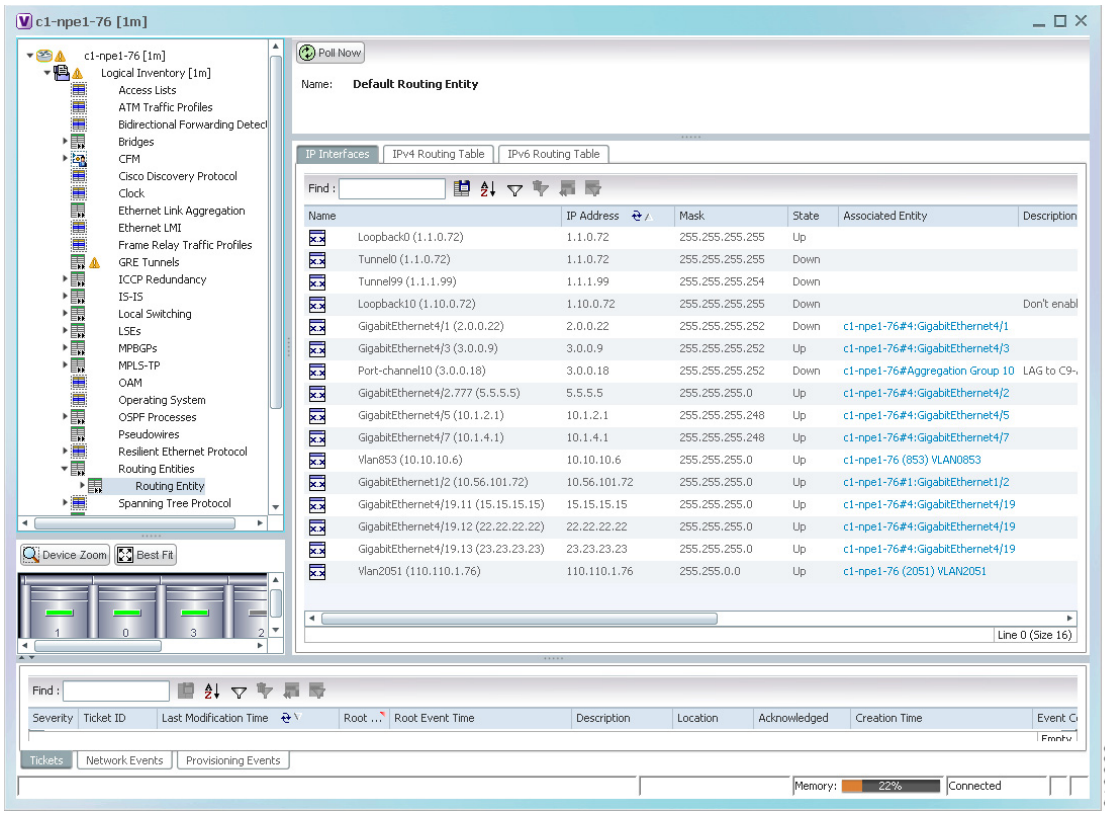


Table 17-11 describes the information that is displayed in the Routing Entity table.

Table 17-11 Routing Entity Table

Field	Description
Name	Name of the routing entity.
IP Interfaces Tab	
Name	Site name.
IP Address	IP address of the interface.
Mask	Network mask.
State	State of the subinterface: Up or Down.
Associated Entity	Interface associated with the routing entity, hyperlinked to its location in physical inventory.
Description	Description of the interface.
Input Access List	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.

Table 17-11 Routing Entity Table (continued)

Field	Description
VRRP Group	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. **Note** 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 17-40.
Output Access List	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.
Rate Limits	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. **Note** 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 17-39. **Note** The Input Access, Output Access, and Rate Limits parameters apply only to Cisco IOS devices.
IP Sec Map Name	IP Security (IPsec) crypto map name.
Site Name	Name of the business element to which the interface is attached.
IPv4 and IPv6 Routing Table Tabs	
Destination	Destination of the specific network.
Outgoing If Name	Name of the outgoing interface; displayed if the Routing Protocol type is local.
Type	Routing type: Direct, Indirect, Static, Other, Invalid, or Unknown.
Next Hop	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.
Prefix Length	Length of the network prefix in bits.
Route Protocol Type	Routing protocol used to communicate with other routers.

Related Topics

- Viewing the ARP Table, page 17-37
- Viewing VRF Properties, page 17-30
- Viewing Label Switched Entity Properties, page 17-42

Viewing the ARP Table

To view the ARP table:

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

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

Table 17-12 describes the information that is displayed in the ARP table.

Table 17-12 ARP Table

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

Related Topics

- Viewing Rate Limit Information, page 17-39
- Viewing the NDP Table, page 17-37
- Viewing Label Switched Entity Properties, page 17-42

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 Prime Network Vision 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 17-16 shows an example of the NDP Table tab.

Figure 17-16 NDP Table in Logical Inventory

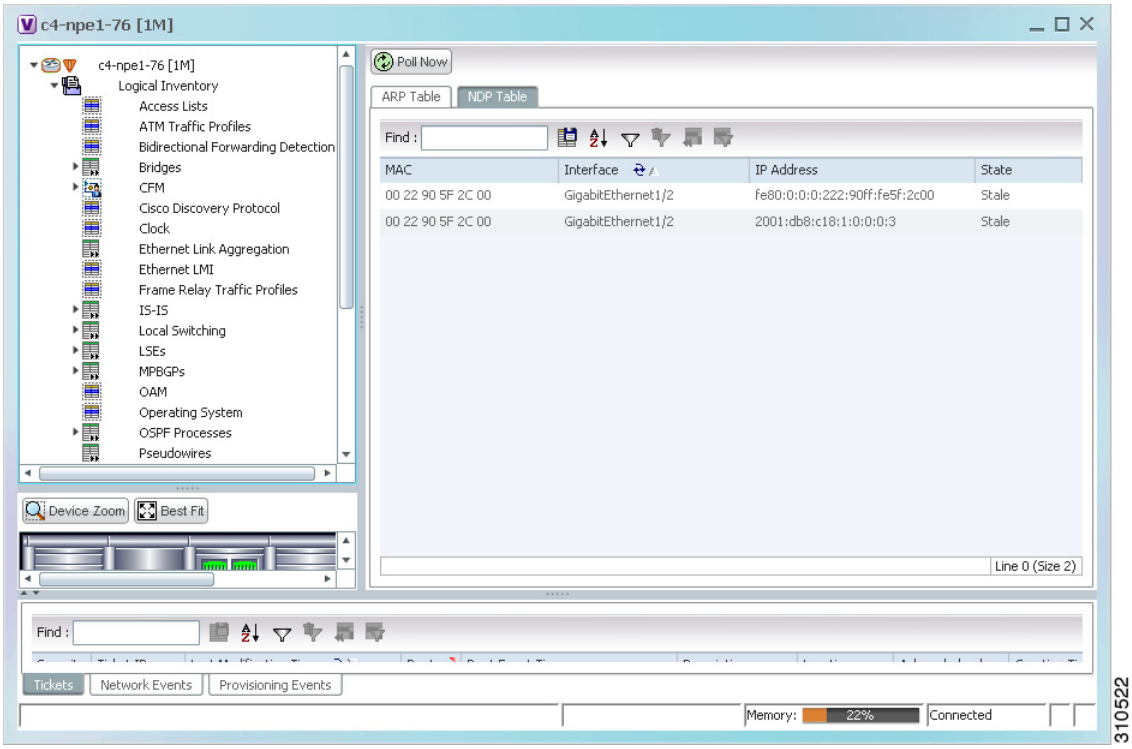


Table 17-13 describes the information displayed for NDP.

Table 17-13 NDP Table

Field	Description
MAC	Interface MAC address.
Interface	Interface name.
IP Address	Interface IPv6 address.
Type	Entry type: • ICMP (Incomplete)—Address resolution is being performed on the entry. A neighbor solicitation (NS) message has been sent to the solicited-node multicast address of the target, but the corresponding neighbor advertisement (NA) message has not yet been received. • REACH (Reachable)—Positive confirmation was received via an NA that the forward path to the neighbor was functioning properly. While in REACH state, the device takes no special action as packets are sent. • STALE—Too much time has elapsed since the last positive confirmation was received that the forward path was functioning properly. While in STALE state, the device takes no action until a packet is sent. • DELAY—Too much time has elapsed since the last positive confirmation was received that the forward path was functioning properly. If no reachability confirmation is received within a specified amount of time, the device sends an NS message and changes the state to PROBE. • PROBE—A reachability confirmation is actively sought by resending neighbor solicitation messages until a reachability confirmation is received. • ????—The state is unknown.

Related Topics

- Viewing Rate Limit Information, page 17-39
- Viewing the ARP Table, page 17-37
- Viewing Label Switched Entity Properties, page 17-42

Viewing Rate Limit Information

To view rate limit information:

Step 1 Right-click the required element in Prime Network Vision 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 is relevant only for Cisco IOS devices.

Table 17-14 describes the information that is displayed in the Rate Limits tab of the IP Interface Properties dialog box.

Table 17-14 Rate Limits Information

Field	Description
Type	Rate limit direction, either Input or Output.
Max Burst	Excess burst size in bytes.
Normal Burst	Normal burst size in bytes.
Bit Per Second	Average rate in bits per second.
Conform Action	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.
Exceed Action	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.
Access List	Hyperlink that highlights the related access list in the Access List table.

Related Topics

- Viewing the ARP Table, page 17-37
- Viewing Routing Entities, page 17-34
- Monitoring MPLS Services, page 17-29

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 Prime Network Vision.

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 17-17 VRRP Properties in IP Interface Properties Window

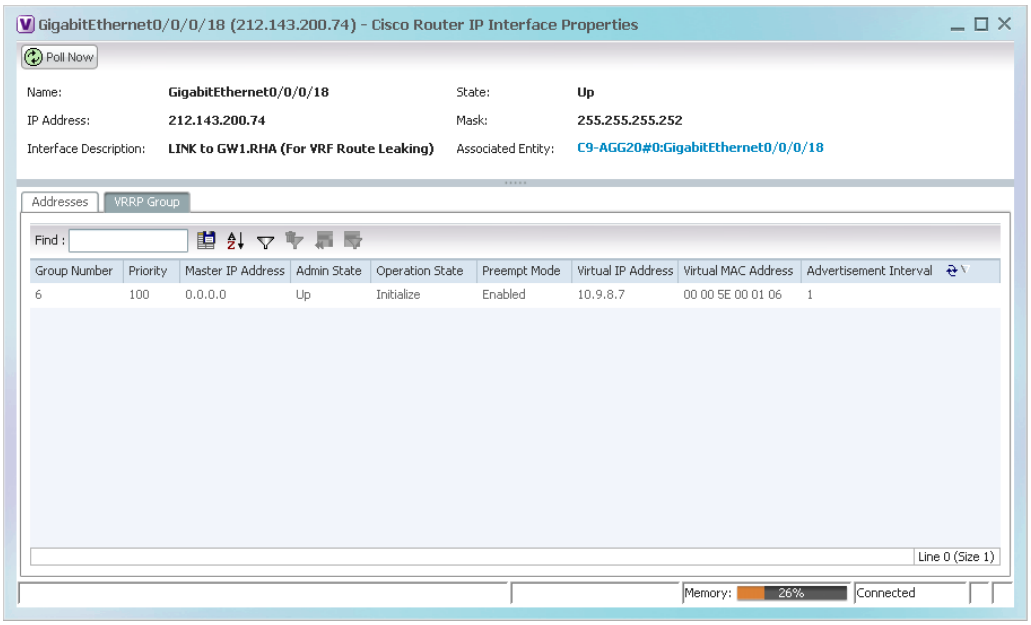


Table 17-15 describes the information in the VRRP Groups tab.

Table 17-15 VRRP Group Properties

Field	Description
Group Number	Number of the VRRP group associated with the interface.
Priority	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.
Master IP Address	IP address of the VRRP group, taken from the physical Ethernet address of the master virtual router.
Admin State	Administrative status of the VRRP group: Up or Down.
Operation State	State of the VRRP group: Master or Backup.
Preempt Mode	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.
Virtual IP Address	IP address of the virtual router.
Virtual MAC Address	MAC address of the virtual router.
Advertisement Interval	Amount of time (in seconds) between successive advertisements by the master virtual router.

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 forwarding 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 Prime Network Vision.

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

Table 17-16 describes the information that is displayed for label switched entities.

Table 17-16 Label Switching Properties in Logical Inventory

Field	Description
Local LDP ID	Local Label Distribution Protocol (LDP) identifier.
LDP Process State	State of the LDP process, such as Running, Down, or Unknown.
MPLS Interfaces	
ID	Identifier for MPLS interface, as a combination of IP address and interface name.
Distribution Protocol Type	Distribution protocol used: Null, LDP, TDP (Tag Distribution Protocol), RSVP, or TDP and LDP.
MPLS TE Properties	Whether or not traffic engineering (TE) properties are configured on the interface: • Checked—MPLS TE properties are configured on the interface. • Unchecked—MPLS TE properties are not configured on the interface.
Discovery Protocols	Discovery protocols used on the interface.
Label Switching Table	
Incoming Label	Incoming MPLS label identifier.
Action	Type of switching action: Null, Pop, Swap, Aggregate, Untagged, or Act. If an action is defined as Pop, an outgoing label is not required. If an action is defined as Untagged, an outgoing label is not present.
Outgoing Label	Outgoing label.
Out Interface	Name of the outgoing interface, displayed as a hyperlink to the port subinterface in physical inventory.
IP Destination	Destination IP address.
Destination Mask	Subnet mask of the destination.
Next Hop	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.
VRF Table	
Incoming Label	Incoming VRF label identifier.
Action	Type of switching action: Null, Pop, Swap, Aggregate, Untagged, or Act.
VRF	VRF name, hyperlinked to its location in logical inventory.
IP Destination	Destination IP address.
Destination Mask	Subnet mask of the destination.
Next Hop	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.
Out Interface	Name of the outgoing interface, displayed as a hyperlink to the port subinterface in physical inventory.

Table 17-16 Label Switching Properties in Logical Inventory (continued)

Field	Description
Traffic Engineering LSPs	
LSP Name	Label switched path (LSP) name.
LSP Type	Segment type: Head, Midpoint, or Tail.
Source Address	Source IP address.
Destination Address	Destination IP address.
In Label	Incoming label, if not a head segment.
In Interface	Incoming interface, if not a head segment.
Out Interface	Outgoing interface, if not a tail segment.
Out Label	Outgoing label, if not a tail segment.
Average Bandwidth (Kbps)	Current bandwidth (in Kb/s) used to automatically allocate the tunnel's bandwidth.
LSP ID	LSP identifier.
Burst (Kbps)	Tunnel bandwidth burst rate, in Kb/s.
Peak (Kbps)	Tunnel bandwidth peak rate, in Kb/s.
FRR TE Tunnel	Fast Reroute (FRR) TE tunnel name, hyperlinked to the routing entity in logical inventory.
FRR TE Tunnel State	State of the FRR TE tunnel: • Active—A failure exists in the primary tunnel and the backup is in use. • Not Configured—The primary tunnel has no designated backup tunnel. • Ready—The primary tunnel is in working condition.
MPLS Label Range	
MPLS Label Type	Type of MPLS label: Dynamic or Static.
Minimum Label Value	Lowest acceptable MPLS label in the range.
Maximum Label Value	Highest acceptable MPLS label in the range.
LDP Neighbors	
LDP ID	Identifier of the LDP peer.
Transport IP Address	IP address advertised by the peer in the hello message or the hello source address.
Session State	Current state of the session: Transient, Initialized, Open Rec, Open Sent, or Operational.
Protocol Type	Protocol used by the peer to establish the session: LDP, TDP, or Unknown.
Label Distribution Method	Method of label distribution: Downstream, Downstream On Demand, Downstream Unsolicited, or Unknown.
Session Keepalive Interval	Length of time (in milliseconds) between keepalive messages.

Table 17-16 Label Switching Properties in Logical Inventory (continued)

Field	Description
Session Hold Time	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.
Discovery Sources	Whether the peer has one or more discovery sources: • Checked—Has one or more discovery sources. • Unchecked—Has no discovery sources. **Note** To see the discovery sources in the LDP Neighbor Properties window, double-click the row of the peer in the table.

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

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

Double-click an entry in this tab...	To display this window...
Label Switching Table	Label Switching Properties
LDP Neighbors	LDP Peer Properties
MPLS Interfaces	MPLS Link Information - MPLS Properties
MPLS Label Range	MPLS Label Range Properties
Traffic Engineering LSPs	Tunnel Properties
VRF Table	MPLS Aggregate Entry Properties

Related Topics

- Viewing MP-BGP Information, page 17-45
- Viewing Cross-VRF Routing Entries, page 17-51
- Viewing Routing Entities, page 17-34

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, Prime Network displays each link in the content pane map view.

To view MP-BGP information:

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

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

Table 17-18 describes the information that is displayed for MP-BGP.

Table 17-18 MP-BGP Information in Logical Inventory

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

Related Topics

- Viewing Label Switched Entity Properties, page 17-42
- Viewing Routing Entities, page 17-34

Viewing 6rd Tunnel Properties

IPv6 rapid deployment (6rd) is a mechanism that allows stateless tunneling of IPv6 over IPv4. In Prime Network Vision 3.8, 6rd is supported on the following devices:

- Cisco 7600 series devices
- Cisco ASR 1000 series devices

To view 6rd tunnel properties:

Step 1 In Prime Network Vision, 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 17-18.

Figure 17-18 6rd Tunnel Properties in Logical Inventory

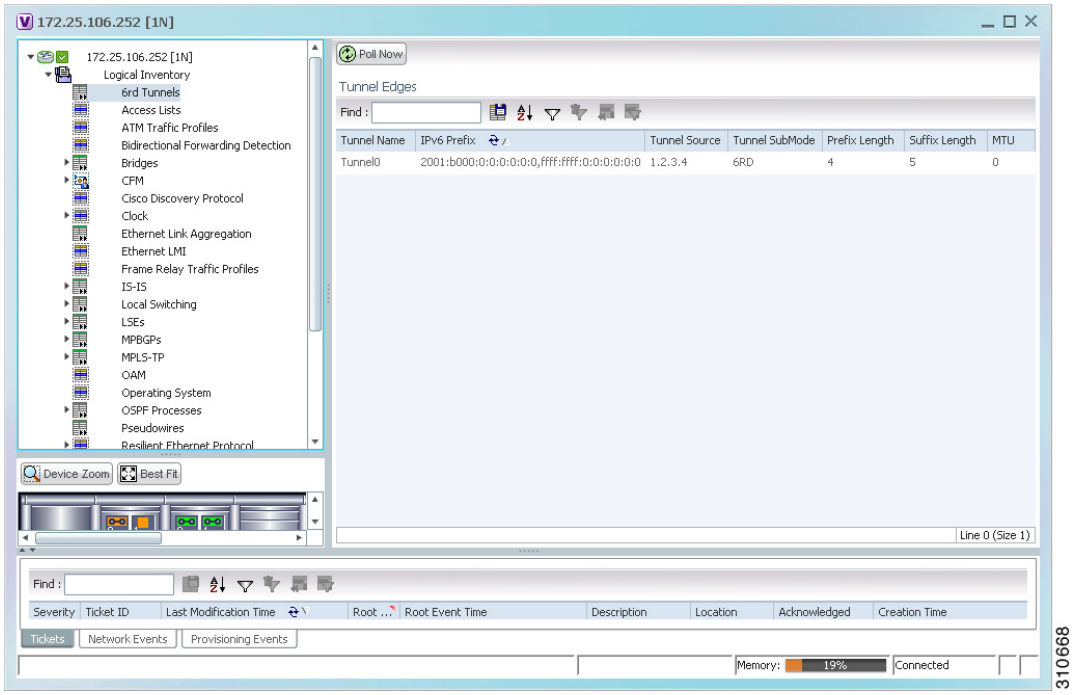


Table 17-19 describes the information displayed for 6rd tunnels.

Table 17-19 6rd Tunnel Properties in Logical Inventory

Field	Description
Tunnel Name	6rd tunnel name.
IPv6 Prefix	IPv6 prefix used to translate the IPv4 address to an IPv6 address.
Source Address	Tunnel IPv4 source IP address.
Tunnel SubMode	Tunnel type: • 6rd—Static IPv6 interface. • 6to4—IPv6 address with the prefix embedding the tunnel source IPv4 address. • Auto-tunnel—IPv4-compatible IPv6 tunnel. • ISATAP—Overlay tunnel using an Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) address.
Prefix Length	IPv4 prefix length used to derive the delegated IPv6 prefix.
Suffix Length	IPv4 suffix length used to derive the delegated IPv6 prefix.
MTU	Maximum transmission unit (MTU) configured on the 6rd IPv4 tunnel.

Related Topics

- Viewing Carrier Grade NAT Properties in Logical Inventory, page 13-2
- Viewing IPv6 Information, page 16-3

Viewing BFD Session Properties

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 Vision 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 Prime Network Vision, 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 17-19.

Figure 17-19 BFD Session Properties

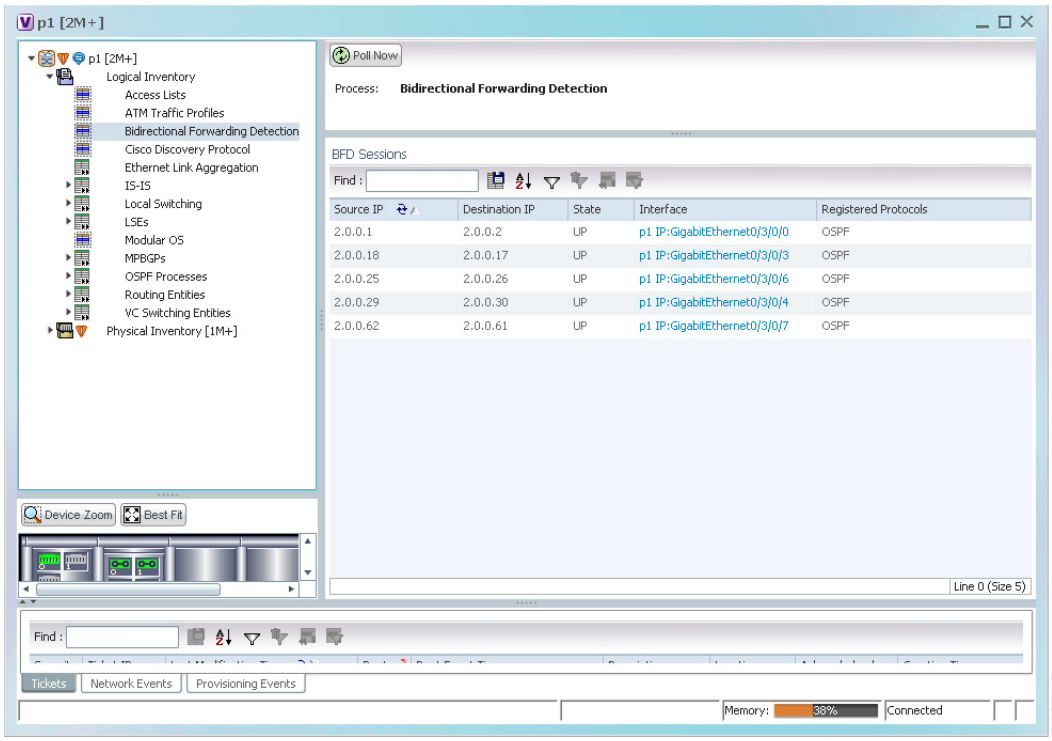


Table 17-20 describes the information displayed for BFD sessions.

Table 17-20 BFD Session Properties

Field	Description
Process	Process name, such as Bidirectional Forwarding Detection.
Process State	Process state, such as Running.
BFD Sessions Table	
Source IP	Source IP address of the session.
Destination IP	Destination IP address of the session.
State	Session state, such as Up or Down.
Interface	Interface used for BFD communications, hyperlinked to the routing entity in logical inventory.
Registered Protocols	Routing protocol being monitored for communication failures, such as BGP or OSPF.

For MPLS-TP BFD sessions, the information in Table 17-21 is displayed.

Table 17-21 MPLS-TP BFD Session Properties in Logical Inventory

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

Step 3 To view additional properties, double-click the required entry in the Sessions table.

Table 17-22 describes the information that is displayed in the Session Properties window.

Table 17-22 Session Properties Window

Field	Description
Source IP	Source IP address of the session.
Destination IP	Destination IP address of the session.
State	Session state: Up or Down.
Interface	Hyperlink to the routing entity in logical inventory.
Registered Protocols	Routing protocol being monitored for communication failures.
Protocols Table	
Protocol	Protocol used for this session.
Interval	Length of time (in milliseconds) to wait between packets that are sent to the neighbor.
Multiplier	Number of times a packet is missed before the neighbor is declared down.

Related Topics

- Viewing Label Switched Entity Properties, page 17-42
- Viewing Routing Entities, page 17-34

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 Prime Network Vision 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 17-23.

Table 17-23 Cross-VRF Properties Window

Field	Description
Name	Cross-VRF name.
Cross VRF Routing Entries Table	
Destination	IP address of the destination network.
Prefix	Length of the network prefix in bits.
Next Hop	IP address of the next hop in the path.
Out Going VRF	Outgoing VRF identifier, hyperlinked to its entry in logical inventory.
Out Tag	Outgoing virtual router tag, such as 50 or no tag.
In Tag	Incoming virtual router tag, such as 97 or no tag.

Related Topics

- Viewing MPLS TE Tunnel Information, page 17-53
- Viewing Pseudowire End-to-End Emulation Tunnels, page 17-51
- Viewing MP-BGP Information, page 17-45

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 Prime Network Vision 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 17-24.

Table 17-24 Pseudowires Branch Tunnel Edges Table

Field	Description
Local Interface	Name of the subinterface or port. Strings, such as Aggregation Group, EFP, VLAN, and VSI, are included in the interface name, and the entry is hyperlinked to the relevant entry in logical or physical inventory: • Aggregation groups are linked to Ethernet Link Aggregation in logical inventory. • ATM interfaces are linked to the port in physical inventory and the ATM interface. • ATM VCs are linked to the port in physical inventory and the Port IP Properties table. • CEM groups are linked to the port in physical inventory and the CEM Group table. • EFPs are linked to the port in physical inventory and the EFPs table. • IMA groups are linked to IMA Groups in logical inventory. • Local switching entities are linked to Local Switching Entity in logical inventory. • VLANs are linked to Bridges in logical inventory. • VSIs are linked to the VSI entry in logical inventory.
VC ID	Tunnel identifier, hyperlinked to the PTP Layer 2 MPLS Tunnel Properties window.
Peer	Details of the selected peer, hyperlinked to the peer pseudowire tunnel in logical inventory.
Status	Operational state of the tunnel: Up or Down.
Pseudowire Role	If the pseudowire is in a redundancy configuration, indicates whether its role is as the primary or secondary pseudowire in the configuration. If the pseudowire is not configured for redundancy, this field is blank.
Preferred Path Tunnel	Path to be used for MPLS pseudowire traffic.
Local Router IP	IP address of this tunnel edge, which is used as the MPLS router identifier.
Peer Router IP	IP address of the peer tunnel edge, which is used as the MPLS router identifier.
Pseudowire Type	Type of pseudowire, such as Ethernet, Ethernet Tagged, CESoPSN Basic, PPP, or SAToP.
Local MTU	Size, in bytes, of the MTU on the local interface.
Remote MTU	Size, in bytes, of the MTU on the remote interface.
Local VC Label	MPLS label that is used by this router to identify or access the tunnel. It is inserted into the MPLS label stack by the local router.
Peer VC Label	MPLS label that is used by this router to identify or access the tunnel. It is inserted into the MPLS label stack by the peer router.
Signaling Protocol	Protocol used by MPLS to build the tunnel, for example, LDP or TDP.

Related Topics

- Viewing MPLS TE Tunnel Information, page 17-53
- Viewing Cross-VRF Routing Entries, page 17-51
- Viewing Label Switched Entity Properties, page 17-42

Viewing MPLS TE Tunnel Information

Prime Network Vision 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 Prime Network Vision and choose **Inventory**.

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

Table 17-25 describes the information that is displayed in the Tunnel Edges table.

Table 17-25 Tunnel Edges Table

Field	Description
Name	Name of the TE tunnel; for Cisco devices it is the interface name.
Tunnel Type	Whether the tunnel is Point-to-Point or Point-to-Multipoint.
Tunnel Destination	IP address of the device in which the tunnel ends.
Administrative Status	Administrative state of the tunnel: Up or Down.
Operational Status	Operational state of the tunnel: Up or Down.
Outgoing Label	TE tunnel's MPLS label distinguishing the LSP selection in the next device.
Description	Description of the tunnel.
Outgoing Interface	Interface through which the tunnel exits the device.
Bandwidth (KBps)	Bandwidth specification for this tunnel in Kb/s.
Setup Priority	Tunnel priority upon path setup.
Hold Priority	Tunnel priority after path setup.
Affinity	Tunnel preferential bits for specific links.
Affinity Mask	Tunnel affinity bits that should be compared to the link attribute bits.
Auto Route	Whether or not destinations behind the tunnel are routed through the tunnel: Enabled or disabled.
Lockdown	Whether or not the tunnel can be rerouted: • Enabled—The tunnel cannot be rerouted. • Disabled—The tunnel can be rerouted.
Path Option	Tunnel path option: • Dynamic—The tunnel is routed along the ordinary routing decisions after taking into account the tunnel constraints such as attributes, priority, and bandwidth. • Explicit—The route is explicitly mapped with the included and excluded links.
Average Rate (Kbps)	Average bandwidth for this tunnel (in Kb/s).
Burst (Kbps)	Burst flow specification (in Kb/s) for this tunnel.
Peak Rate (Kbps)	Peak flow specification (in Kb/s) for this tunnel.
LSP ID	LSP identifier.

Table 17-25 Tunnel Edges Table (continued)

Field	Description
Policy Class	Value of Policy Based Tunnel Selection (PBTS) configured. Values range from 1-7.
FRR	TE Fast Reroute (FRR) status: Enabled or Disabled.
Type	

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 17-44.

Related Topics

- Viewing Label Switched Entity Properties, page 17-42
- Viewing Pseudowire End-to-End Emulation Tunnels, page 17-51
- Monitoring MPLS Services, page 17-29