Monitoring Carrier Ethernet Services

The following topics describe how you can use Cisco Prime Network Vision (Prime Network Vision) to monitor Carrier Ethernet services:

- User Roles Required to Work with Carrier Ethernet Services, page 12-2
- Viewing CDP Properties, page 12-6
- Viewing Link Layer Discovery Protocol Properties, page 12-8
- Viewing Spanning Tree Protocol Properties, page 12-10
- Viewing Resilient Ethernet Protocol Properties (REP), page 12-14
- Viewing HSRP Properties, page 12-18
- Viewing Access Gateway Properties, page 12-19
- Working with Ethernet Link Aggregation Groups, page 12-23
- Viewing mLACP Properties, page 12-29
- Viewing Provider Backbone Bridge Properties, page 12-32
- Viewing EFP Properties, page 12-33
- Connecting a Network Element to an EFP, page 12-38
- Understanding EFP Severity and Ticket Badges, page 12-38
- Viewing EVC Service Properties, page 12-40
- Viewing and Renaming Ethernet Flow Domains, page 12-42
- Working with VLANs, page 12-45
- Understanding Unassociated Bridges, page 12-73
- Working with Ethernet Flow Point Cross-Connects, page 12-75
- Working with VPLS and H-VPLS Instances, page 12-78
- Working with Pseudowires, page 12-90
- Working with Ethernet Services, page 12-106
- Viewing IP SLA Responder Service Properties, page 12-112
- Viewing IS-IS Properties, page 12-114
- Viewing OSPF Properties, page 12-117
- Configuring REP and mLACP, page 12-119
- Using Pseudowire Ping and Show Commands, page 12-120

- Configuring IS-IS, page 12-121

User Roles Required to Work with Carrier Ethernet Services

This topic identifies the roles that are required to work with to Carrier Ethernet services in Prime Network Vision. 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 4.0 Administrator Guide*.

The following tables identify the tasks that you can perform:

- Table 12-1 identifies the tasks that you can perform if a selected element **is not in** one of your assigned scopes.
- Table 12-2 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 4.0 Administrator Guide*.

Table 12-1 Default Permission/Security Level Required for Working with Carrier Ethernet Services - Element Not in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Adding Elements to Maps					
Add associated VLANs to a map	—	—	X	X	X
Add EFP cross-connects	—	—	X	X	X
Add Ethernet services to a map	—	—	X	X	X
Add pseudowires to a map	—	—	X	X	X
Add unassociated bridges	—	—	X	X	X
Add VLANs to a map	—	—	X	X	X
Add VPLS instances to a map	—	—	X	X	X
Viewing Element Properties					
View access gateway properties	—	—	—	—	X
View associated network VLAN service links and VLAN mapping properties	—	—	—	—	X
View CDP properties	—	—	—	—	X
View EFD properties	—	—	—	—	X
View EFP cross-connect properties	Partial[1]	Partial[1]	Partial[1]	Partial[1]	X
View EFP properties	Partial[1]	Partial[1]	Partial[1]	Partial[1]	X

Table 12-1 Default Permission/Security Level Required for Working with Carrier Ethernet Services - Element Not in User's Scope (continued)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View Ethernet flow domains	X	X	X	X	X
View Ethernet LAG properties	—	—	—	—	X
View Ethernet service properties	X	X	X	X	X
View EVC service properties	—	—	—	—	X
View IP SLA responder service properties	—	—	—	—	X
View IS-IS properties	—	—	—	—	X
View Link Layer Discovery Protocol (LLDP) properties	—	—	—	—	X
View mLACP properties	—	—	—	—	X
View OSPF properties	—	—	—	—	X
View Provider Backbone Bridge (PBB) properties	—	—	—	—	X
View pseudowire properties	Partial[1]	Partial[1]	Partial[1]	Partial[1]	X
View pseudowire redundancy service properties	Partial[2]	Partial[2]	Partial[2]	Partial[2]	
Viewing the PW-HE configuration	—	—	—	—	X
View REP properties	—	—	—	—	X
View REP properties for VLAN service links	—	—	—	—	X
View STP properties	—	—	—	—	X
View STP properties for VLAN service links	—	—	—	—	X
View HSRP properties	—	—	—	—	X
View virtual service instance properties	—	—	—	—	X
View VLAN bridge properties	—	—	—	—	X
View VLAN links between VLAN elements and devices	Partial[3]	Partial[3]	Partial[3]	Partial[3]	X
View VLAN mappings	—	—	—	—	X
View VLAN service link properties	—	—	—	—	X
View VLAN trunk group properties	—	—	—	—	X
View VPLS access EFP properties	—	—	—	—	X
View VPLS core or access pseudowire endpoint properties	—	—	—	—	X
View VPLS instance properties	X	X	X	X	X

Table 12-1 Default Permission/Security Level Required for Working with Carrier Ethernet Services - Element Not in User's Scope (continued)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Working with Overlays					
Apply overlays	X	X	X	X	X
Display or hide overlays	X	X	X	X	X
Remove overlays	X	X	X	X	X
View pseudowire tunnel links in VPLS overlays	—	—	—	—	X
View REP information in VLAN domain views and VLAN overlays	—	—	—	—	X
View STP information in VLAN domain views and VLAN overlays	—	—	—	—	X
Other Tasks					
Display pseudowire information	—	—	—	—	X
Ping a pseudowire	—	—	—	—	X
Remove VLANs from a map	—	—	X	X	X
Rename Ethernet flow domains	X	X	X	X	X
Using REP and mLACP Show Commands	—	—	—	X	X
Using Pseudowire Ping and Show Commands	—	—	—	X	X

1. The user can view properties available via **Node > Properties** but not those available via the right-click Properties option or in logical inventory.
2. The user can view the pseudowire redundancy icon in the navigation and map panes, but not the inventory or properties window.
3. The user can view links, but the links are dimmed and do not indicate their status.

Table 12-2 Default Permission/Security Level Required for Working with Carrier Ethernet Services - Element in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Adding Elements to a Map					
Add associated VLANs to a map	—	—	X	X	X
Add EFP cross-connects	—	—	X	X	X
Add Ethernet services to a map	—	—	X	X	X
Add pseudowires to a map	—	—	X	X	X
Add unassociated bridges	—	—	X	X	X
Add VLANs to a map	—	—	X	X	X
Add VPLS instances to a map	—	—	X	X	X
Viewing Element Properties					
View access gateway properties	X	X	X	X	X

Table 12-2 Default Permission/Security Level Required for Working with Carrier Ethernet Services - Element in User's Scope (continued)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View associated network VLAN service links and VLAN mapping properties	X	X	X	X	X
View CDP properties	X	X	X	X	X
View EFD properties	X	X	X	X	X
View EFP cross-connect properties	X	X	X	X	X
View EFP properties	X	X	X	X	X
View Ethernet flow domains	X	X	X	X	X
View Ethernet LAG properties	X	X	X	X	X
View Ethernet service properties	X	X	X	X	X
View EVC service properties	X	X	X	X	X
View IP SLA responder service properties	X	X	X	X	X
View IS-IS properties	X	X	X	X	X
View Link Layer Discovery Protocol (LLDP) properties	X	X	X	X	X
View mLACP properties	X	X	X	X	X
View OSPF properties	X	X	X	X	X
View Provider Backbone Bridge (PBB) properties	X	X	X	X	X
View pseudowire properties	X	X	X	X	X
View pseudowire redundancy service properties	X	X	X	X	X
Viewing the PW-HE configuration	X	X	X	X	X
View REP properties	X	X	X	X	X
View REP properties for VLAN service links	X	X	X	X	X
View HSRP properties	X	X	X	X	X
View STP properties	X	X	X	X	X
View STP properties for VLAN service links	X	X	X	X	X
View VLAN bridge properties	X	X	X	X	X
View VLAN links between VLAN elements and devices	X	X	X	X	X
View VLAN mappings	X	X	X	X	X
View VLAN service link properties	X	X	X	X	X
View VLAN trunk group properties	X	X	X	X	X
View VPLS access EFP properties	X	X	X	X	X

Table 12-2 Default Permission/Security Level Required for Working with Carrier Ethernet Services - Element in User's Scope (continued)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View VPLS core or access pseudowire endpoint properties	X	X	X	X	X
View VPLS instance properties	X	X	X	X	X
View VSI properties	X	X	X	X	X
Working with Overlays					
Apply overlays	X	X	X	X	X
Display or hide overlays	X	X	X	X	X
Remove overlays	X	X	X	X	X
View pseudowire tunnel links in VPLS overlays	X	X	X	X	X
View REP information in VLAN domain views and VLAN overlays	X	X	X	X	X
View STP information in VLAN domain views and VLAN overlays	X	X	X	X	X
Other Tasks					
Display pseudowire information	—	—	—	X	X
Ping a pseudowire	—	—	—	X	X
Remove VLANs from a map	—	—	X	X	X
Rename Ethernet flow domains	X	X	X	X	X
Using REP and mLACP Show Commands	—	—	—	X	X
Using Pseudowire Ping and Show Commands	—	—	—	X	X

Viewing CDP Properties

Cisco Discovery Protocol (CDP) is primarily used to obtain protocol addresses of neighboring devices and discover the platform of those devices.

In Logical Inventory

To view CDP properties:

Step 1 In Prime Network Vision, double-click the device whose CDP properties you want to view.

Step 2 In the inventory window, click **Logical Inventory > Cisco Discovery Protocol**.

The CDP properties are displayed in logical inventory as shown in Figure 12-1.

Figure 12-1 CDP in Logical Inventory

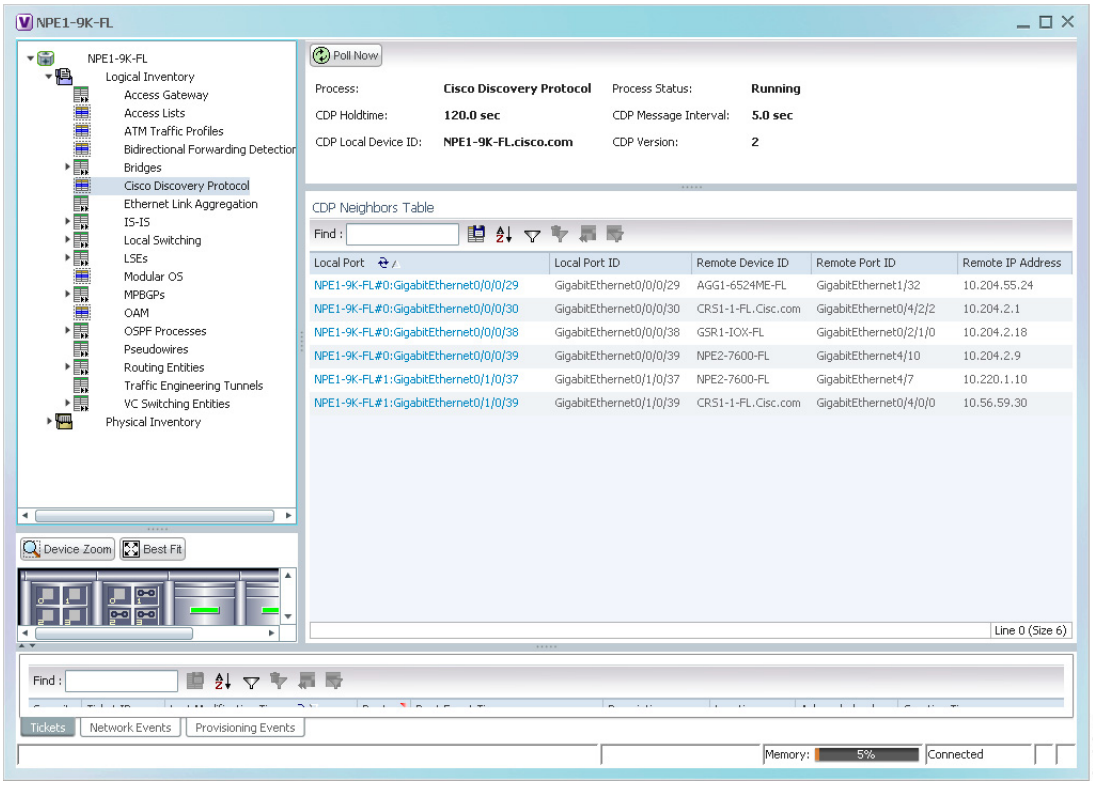


Table 12-3 describes the CDP instance properties that are displayed.

Table 12-3 CDP Properties in Logical Inventory

Field	Description
Process	Process name; in this case, Cisco Discovery Protocol
Process Status	Process status: Running or Disabled.
CDP Holdtime	Specifies the amount of time a receiving device should hold the information sent by a device before discarding it.
CDP Message Interval	Interval between CDP advertisement transmissions.
CDP Local Device ID	Local device identifier.
CDP Version	CDP version: 1 or 2.
CDP Neighbors Table	
Local Port	Local port name.
Local Port ID	Local port identifier.
Remote Device ID	Remote device identifier.
Remote Port ID	Remote port identifier.
Remote IP Address	Remote IP address.

In Physical Inventory

To view CDP on a Layer 2 port:

Step 1 In Prime Network Vision, double-click the device with the Layer 2 port with the CDP information you want to view.

Step 2 In the inventory window, select the required port under Physical Inventory.

The CDP information is displayed in the Discovery Protocols area in the Prime Network Vision content pane:

- Discovery Protocol Type—CDP
- Info—Up or Down

Viewing Link Layer Discovery Protocol Properties

Link Layer Discovery Protocol (LLDP) stores and maintains the local device information, including a list of devices directly connected to the device.

In Logical Inventory

To view LLDP properties:

Step 1 In Prime Network Vision, double-click the device with the LLDP information you want to view.

Step 2 In the inventory window, choose **Logical Inventory > Link Layer Discovery Protocol**.

The LLDP properties are displayed in logical inventory as shown in Figure 12-2.

Figure 12-2 LLDP in Logical Inventory

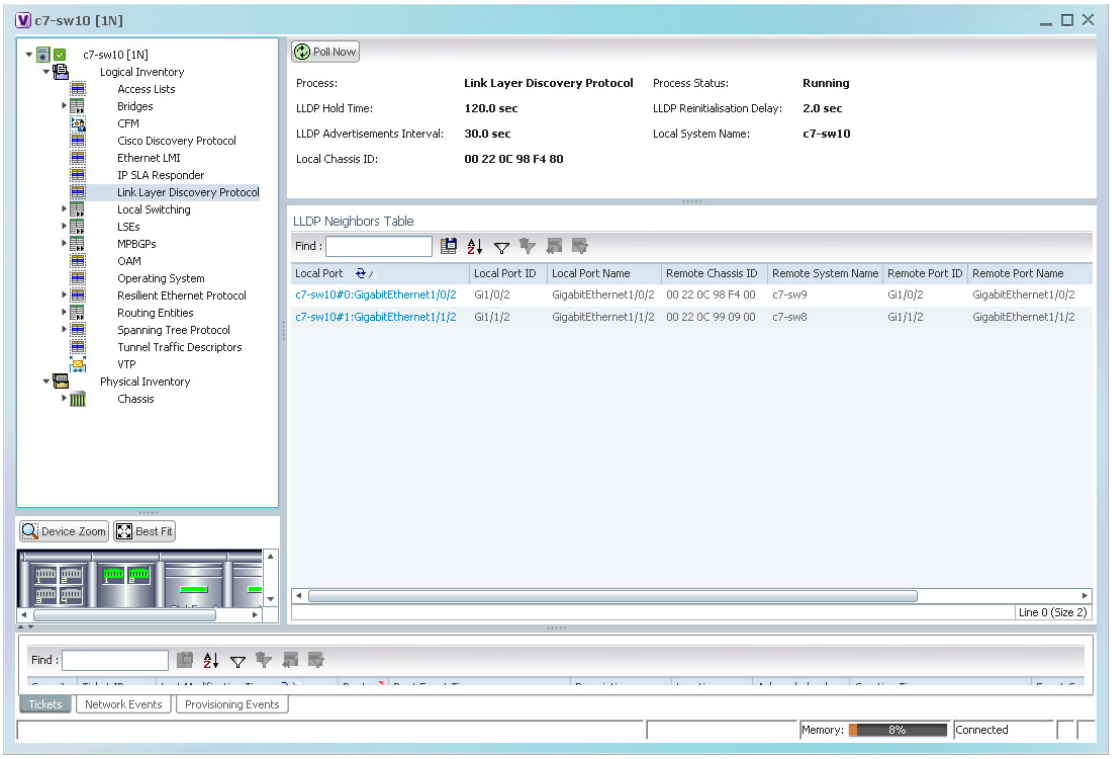


Table 12-4 describes the properties that are displayed for LLDP.

Table 12-4 Link Layer Discovery Protocol Properties

Field	Description
Process	Process; in this case, Link Layer Discovery Protocol
Process Status	Process status: Running or Disabled.
LLDP Hold Time	LLDP advertised hold time in seconds.
LLDP Reinitialization Delay	LLDP interface reinitialization delay in seconds
LLDP Advertisements Interval	LLDP advertisements interval in seconds.
Local System Name	Local system name.
Local Chassis ID	Local chassis identifier.

Table 12-4 Link Layer Discovery Protocol Properties (continued)

Field	Description
LLDP Neighbors Table	
Local Port	Local port.
Local Port ID	Local port identifier.
Local Port Name	Local port name.
Remote System Name	Remote system name.
Remote Chassis ID	Remote chassis identifier.
Remote Port ID	Remote port identifier.
Remote Port Name	Remote port name.
Remote Management IP	Remote management IP address.

In Physical Inventory

To view LLDP on a Layer 2 port:

Step 1 In Prime Network Vision, double-click the device with the Layer 2 port with LLDP information you want to view.

Step 2 In the inventory window, select the required port under Physical Inventory.

The LLDP information is displayed in the Discovery Protocols area in the Prime Network Vision content pane:

- Discovery Protocol Type—LLDP
- Info—Tx (Enabled or Disabled), Rx (Enabled or Disabled).

Viewing Spanning Tree Protocol Properties

Spanning Tree Protocol (STP) is a link management protocol that provides path redundancy while preventing undesirable loops in the network.

To view Spanning Tree properties:

Step 1 In Prime Network Vision, double-click the element whose STP properties you want to view.

Step 2 In the inventory window, choose **Logical Inventory > Spanning Tree Protocol**.

Step 3 STP properties are displayed in logical inventory as shown in Figure 12-3.

Figure 12-3 STP in Logical Inventory

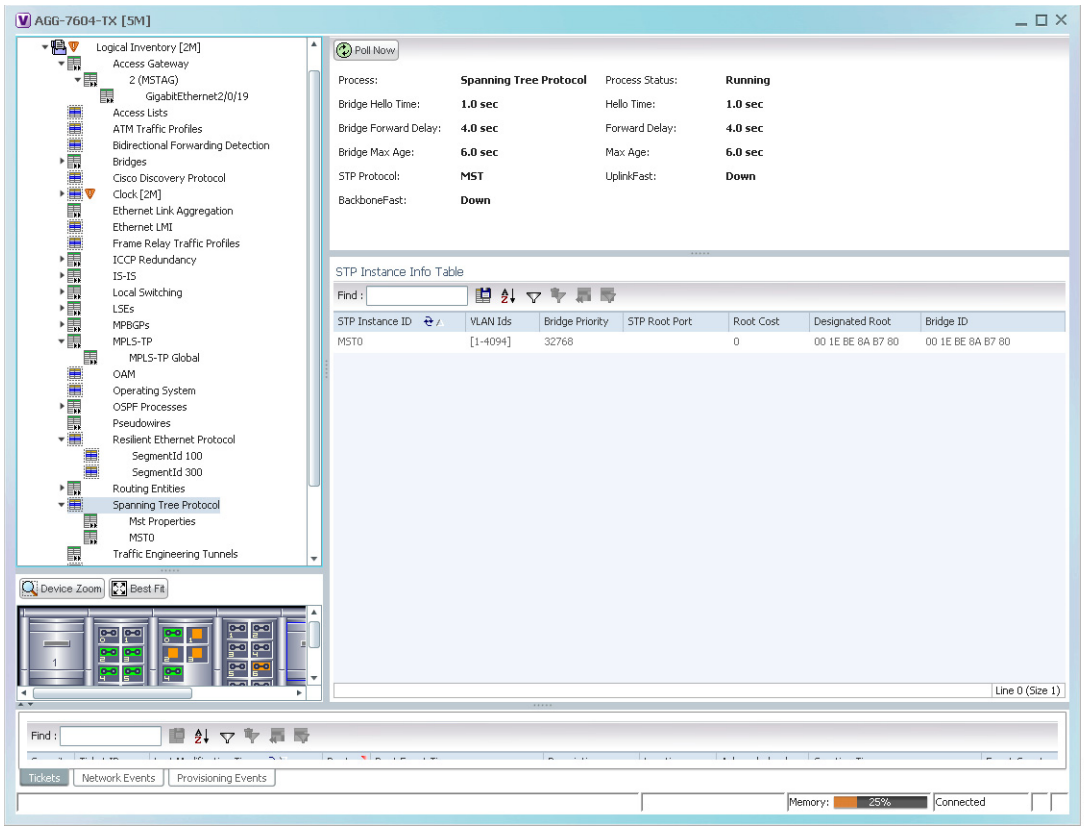


Table 12-5 describes the properties that are displayed for STP.

Table 12-5 STP Properties

Field	Description
Process	Process; in this case, Spanning Tree Protocol.
Process Status	Process status: Running or Disabled.
Bridge Hello Time	Hello message keepalive interval (in seconds) when the port is the root.
Hello Time	Current hello time (in seconds).
Bridge Forward Delay	When the port is the root and in listening or learning state, amount of time to wait (in seconds) before proceeding to the forwarding state.
Forward Delay	Current bridge forward delay (in seconds).
Bridge Max Age	When the port is the root, maximum age of learned Spanning Tree Protocol port information (in seconds).
Max Age	Current maximum age (in seconds).
STP Protocol	STP version: MST, RSTP, PVSTP, MSTP, or RPVST.
UplinkFast	PVSTP Uplink Fast function status: Up or Down.
BackboneFast	PVSTP BackboneFast function status: Up or Down.

Table 12-5 STP Properties (continued)

Field	Description
STP Instance Info Table	
STP Instance ID	STP instance name.
VLAN IDs	VLAN identifiers.
Bridge Priority	Bridge priority.
STP Root Port	Hyperlinked entry to the STP port in logical or physical inventory.
Root Cost	Root cost value for this bridge.
Designated Root	MAC address of the designated root.
Bridge ID	Bridge identifier (MAC address).
Bridge Hello Time	Hello message keepalive interval (in seconds) when the port is the root.
Hello Time	Current hello time (in seconds).
Bridge Forward Delay	When the port is the root and in the listening or learning state, amount of time to wait (in seconds) before proceeding to the forwarding state.
Forward Delay	Current bridge forward delay (in seconds).
Bridge Max Age	When the port is the root, maximum age of learned Spanning Tree Protocol port information (in seconds).
Max Age	Current maximum age (in seconds).

Step 4 To view the properties of an STP instance, do one of the following:

- Double-click the required instance.
- Click the required entry in logical inventory under the Spanning Tree Protocol branch.

Table 12-6 describes the information that is displayed in the STP Instance Information Properties window.

Table 12-6 STP Instance Information Properties

Field	Description
STP Instance ID	STP instance identifier.
VLAN ID	VLAN identifier.
Bridge Priority	Bridge priority.
Bridge ID	Bridge identifier (MAC address).
Root Cost	Root cost value for this bridge.
Designated Root	MAC address of the designated root.
Bridge Hello Time	Hello message keepalive interval (in seconds) when the port is the root.
Hello Time	Current hello time (in seconds).
Bridge Forward Delay	When the port is the root and in listening or learning state, amount of time to wait (in seconds) before proceeding to the forwarding state.
Forward Delay	Current bridge forward delay (in seconds).
Bridge Max Age	When the port is the root, the maximum age of learned Spanning Tree Protocol port information (in seconds).

Table 12-6 STP Instance Information Properties (continued)

Field	Description
Max Age	Current maximum age (in seconds).
STP Protocol Specification	Specific STP protocol type or variant used for this instance, such as Rapid PvSTP.
Is Root	Whether or not the port is the root: True or False.
Ports Info Table	
STP Port	Hyperlinked entry to the STP port in physical inventory.
Port State	STP port state: Disabled, Blocking, Listening, Learning, or Forwarding,
Port Role	Port role: Unknown, Backup, Alternative, Designated, Root, or Boundary.
Port Priority	Default 802.1p priority assigned to untagged packets arriving at the port.
Port Path Cost	Port path cost, which represents the media speed for this port.
Point To Point Port	Whether or not the port is linked to a point-to-point link: True or False.
Edge Port	Whether or not the port is an edge port; that is, whether it is connected to a nonbridging device: True or False.
MST Port Hello Time	This field is displayed in the Ports Info Table only for MST. In seconds, the interval between hello BPDUs sent by root switch configuration messages. The range is 1 to 10 seconds.
Port Identifier	STP port identifier.
Portfast	Whether or not STP PortFast is enabled on the port: Up or Down.
Designated Port Identifier	Designated STP port identifier.
Designated Bridge	STP designated bridge.
BPDU Filter	BPDU Filter status: Up or Down.
BPDU Guard	BPDU Guard status: Up or Down.

Step 5 To view MSTP properties, choose the required MSTP entry in logical inventory under Spanning Tree Protocol.

Table 12-7 describes the information that is displayed for MSTP.

Table 12-7 MSTP Properties in Logical Inventory

Field	Description
MST Force Version	Force version used: MST, PVSTP, RSTP, STP, or Unknown.
MST Cfg ID Rev Level	Revision level used by the selected device and negotiated with other devices.
MST Cfg ID Name	MSTP instance name.
MST Max Instances	Maximum number of MSTP instances.
MST Cfg ID Fmt Sel	Configuration format used by this device and negotiated with other devices.
MST External Root Cost	External root cost of the MSTP instance.

The following topics describe how to view STP properties related to:

- VLAN domain views and overlays—See Viewing STP Information in VLAN Domain Views and VLAN Overlays, page 12-66.
- VLAN service link properties—See Viewing STP Properties for VLAN Service Links, page 12-67.

Viewing Resilient Ethernet Protocol Properties (REP)

Cisco Resilient Ethernet Protocol (REP) technology is implemented on Cisco Carrier Ethernet switches and intelligent service edge routers. REP is a segment protocol, and a REP segment is a chain of ports connected to each other and configured with the same segment identifier. Each end of a segment terminates on an edge switch. The port where the segment terminates is called the edge port.

Cisco Prime Network discovers and displays REP Segments (identified by a REP segment identifier that is locally configured on the network element) along with Global REP configuration details.

You can also view the REP port roles (open, alternate, and failed) in the Cisco Prime Network Vision map. The REP port role is displayed as a tool-tip between the REP enabled trunk ports in the Ethernet links. Using the Cisco Prime Network Vision map, you can identify if the segment is open or closed.

The map displays the forwarding direction (REP port roles) along the Physical links within VLAN overlays. It also displays the forwarding direction along the VLAN links among the switching elements within the VLAN logical domain topology.

REP implementation supports the following faults:

- A REP Port Role change to Failed service event will be generated when a REP port role is change from Alternate or Open to Failed.
- A REP Port Role change to OK clearing service event will be generated when a REP port role is change from Failed to Alternate or Open.

Correlation to these service events to physical layer events (for example Link down or Port down) is also performed.

You can view REP properties in logical inventory.

Step 1 In Prime Network Vision, double-click the device configured for REP.

Step 2 In the inventory window, choose **Logical Inventory > Resilient Ethernet Protocol**.

Figure 12-4 shows an example of REP in logical inventory.

Figure 12-4 REP in Logical Inventory

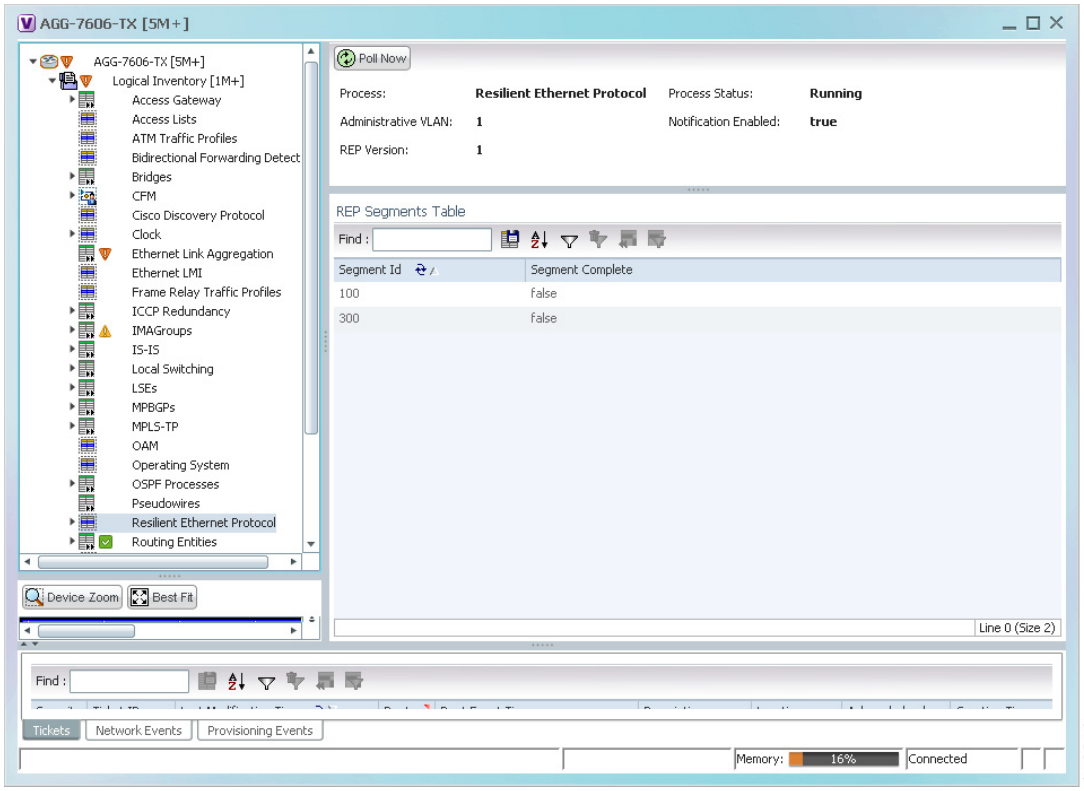


Table 12-8 describes the information that is displayed for REP.

Table 12-8 REP Properties

Field	Description
Process	Process name; in this case, Resilient Ethernet Protocol.
Process Status	State of the REP process, such as Running or Down.
Administrative VLAN	Administrative VLAN used by REP to transmit its hardware flooding layer messages. Values range from 1 to 4094.
Notification Enabled	Whether or not notification is enabled: True or False.
REP Version	Version of REP being used.
REP Segments Table	
Segment ID	Segment identifier.
Segment Complete	Whether the segment is complete; that is, that no port in the segment is in a failed state: True or False.

Step 3 To view REP segment properties, double-click the required entry in the REP Segments table.

Figure 12-5 shows an example of REP segment properties in logical inventory.

Figure 12-5 REP Segment Properties

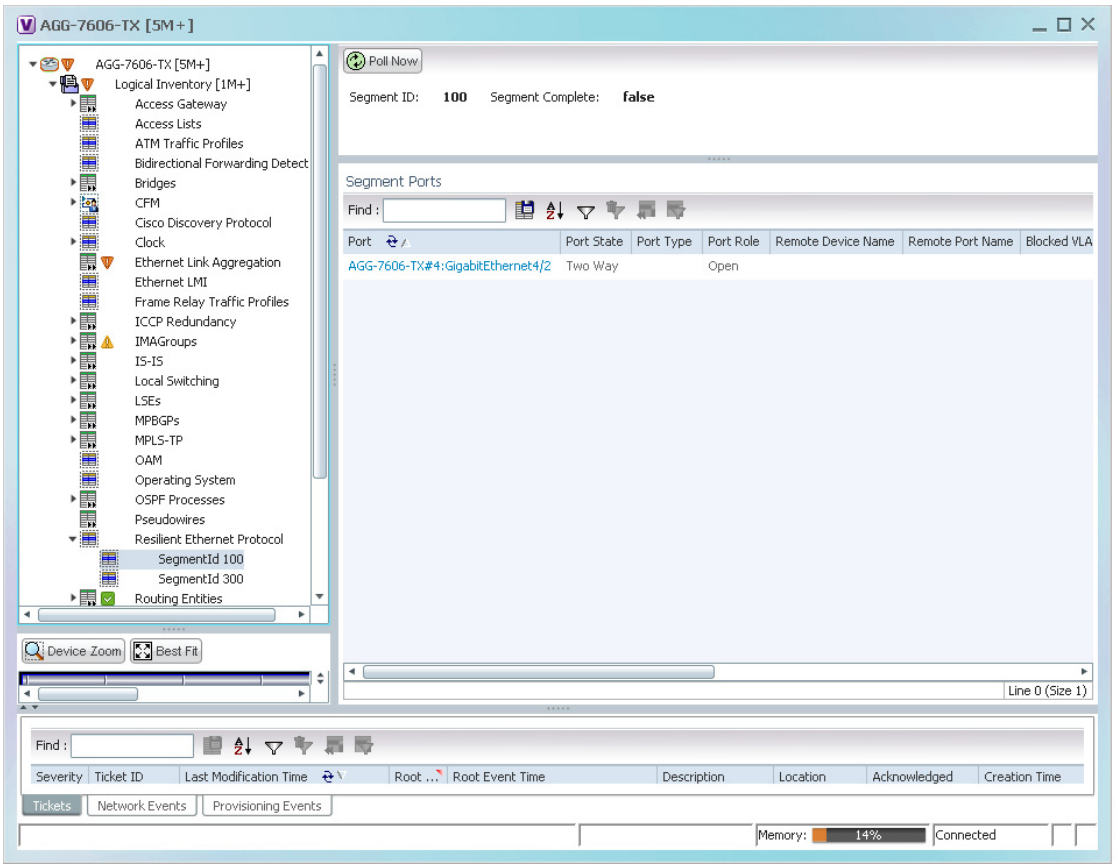


Table 12-9 describes the information that is displayed for REP segments.

Table 12-9 REP Segment Properties

Field	Description
Segment ID	Segment identifier.
Segment Complete	Whether the segment is complete; that is, that no port in the segment is in a failed state: True or False.
Segment Ports Table	
Port	Hyperlinked entry to the port in physical inventory.
Port State	Current operational link state of the REP port: None, Init Down, No Neighbor, One Way, Two Way, Flapping, Wait, or Unknown.
Port Type	Port type: Primary Edge, Secondary Edge, or Intermediate.
Port Role	Role or state of the REP port depending on its link status and whether it is forwarding or blocking traffic: Failed, Alternate, or Open.
Remote Device Name	Name of the neighbor device that this port is connected to on this segment. This value can be null.
Remote Port Name	Name of the neighbor port on the neighbor bridge that this port is connected to on this segment. This value can be null.
Blocked VLANs	VLANs that are blocked on this port.
Configured Load Balancing Blocked VLANs	List of VLANs configured to be blocked at this port for REP VLAN load balancing.
Preemptive Timer	Amount of time, in seconds, that REP waits before triggering preemption after the segment is complete. The entry can range from 0 to 300, or be Disabled. The value Disabled indicates that no time delay is configured, and that the preemption occurs manually. This property applies only to REP primary edge ports.
LSL Ageout Timer	Using the Link Status Layer (LSL) age-out timer, the amount of time, in milliseconds, that the REP interface remains up without receiving a hello from a neighbor.
Remote Device MAC	MAC address of the neighbor bridge that this port is connected to on this segment. This value can be null.

The following topics describe how to view REP properties related to VLANs:

- VLAN domain views and overlays—See Viewing REP Information in VLAN Domain Views and VLAN Overlays, page 12-63.
- VLAN service link properties—See Viewing REP Properties for VLAN Service Links, page 12-64.

Viewing HSRP Properties

Hot Standby Router Protocol (HSRP) is a protocol that provides backup to a router in case of failure. Using HSRP, several routers are connected to the same Ethernet network segment and work together to present the appearance of a single virtual router. The routers share the same IP and MAC addresses; therefore in the event of failure of one router, the hosts on the LAN will be able to continue forwarding packets to a consistent IP and MAC address.

HSRP groups are configured on IP interfaces. An IP interface is modeled by the VNE through the IPInterface DC. The IPInterface DC maintains the HSRP related information by the use of HSRP group entries. Ethernet DCs, which are used to model Ethernet ports, maintain MAC addresses of the HSRP groups.

To view HSRP properties:

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 HSRP is configured on the IP interface, the HSRP Group tab is displayed as shown in Figure 12-6.

Figure 12-6 HSRP Group Information

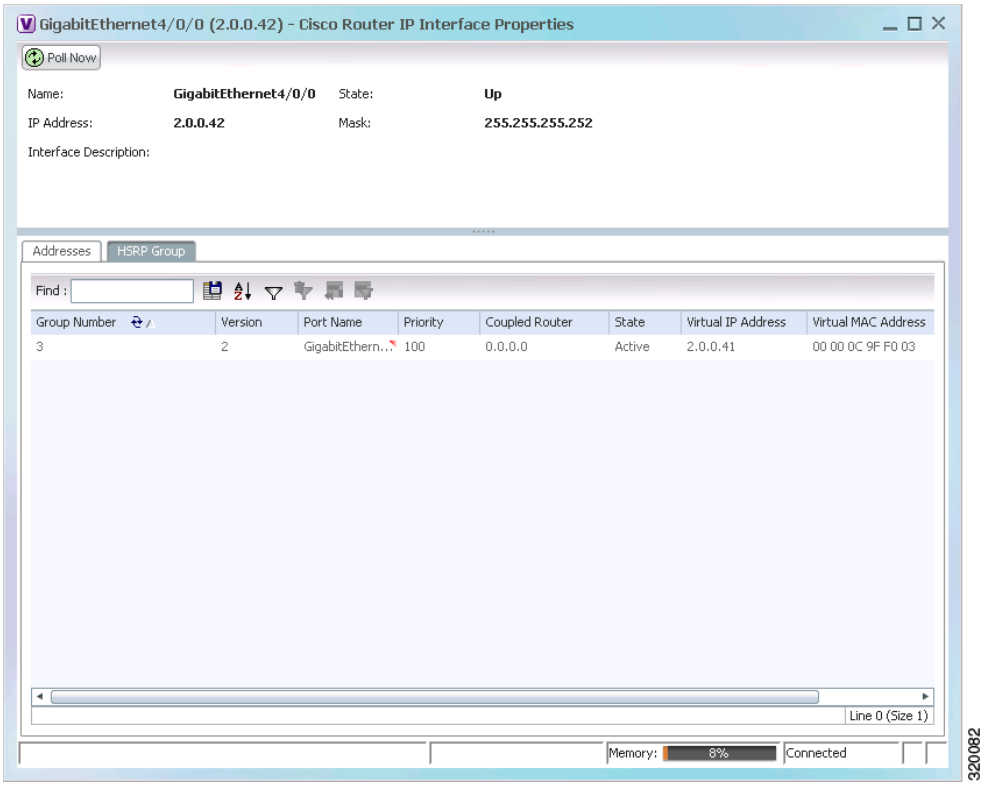


Table 12-10 describes the information in the HSRP Group tab.

Table 12-10 HSRP Group Properties

Field	Description
Group Number	Number of the HSRP group associated with the interface.
Version	Version of the HSRP group.
Port Name	Port on which the HSRP is configured.
Priority	Value that determines the role each HSRP router plays. Values are 1 through 254, with higher numbers having priority over lower numbers.
Coupled Router	The partnet router.
State	State of the HSRP group: Active or Standby.
Virtual IP Address	Virtual IP address assigned to the active router.
Virtual MAC Address	Virtual MAC address assigned to the active router.

Viewing Access Gateway Properties

In an access network, an access gateway configuration ensures loop-free connectivity in the event of various failures by sending statically configured bridge protocol data units (BPDUs) toward the access network. Using statically configured BPDUs enables the gateway device to act appropriately when notified of the following topology changes:

- Failure of a link in the access network.
- Failure of a link between the access network and the gateway device.
- Failure of an access device.
- Failure of a gateway device.

To view access gateway properties:

Step 1 Double-click the element configured for access gateway.

Step 2 In the inventory window, choose **Logical Inventory > Access Gateway >** *access-gateway*. The group name is appended by either MSTAG or REPAG, indicating the group type Multiple Spanning Tree Access Gateway or Resilient Ethernet Protocol Access Gateway.

Figure 12-7 shows an example of an access gateway entry in logical inventory.

Figure 12-7 Access Gateway in Logical Inventory

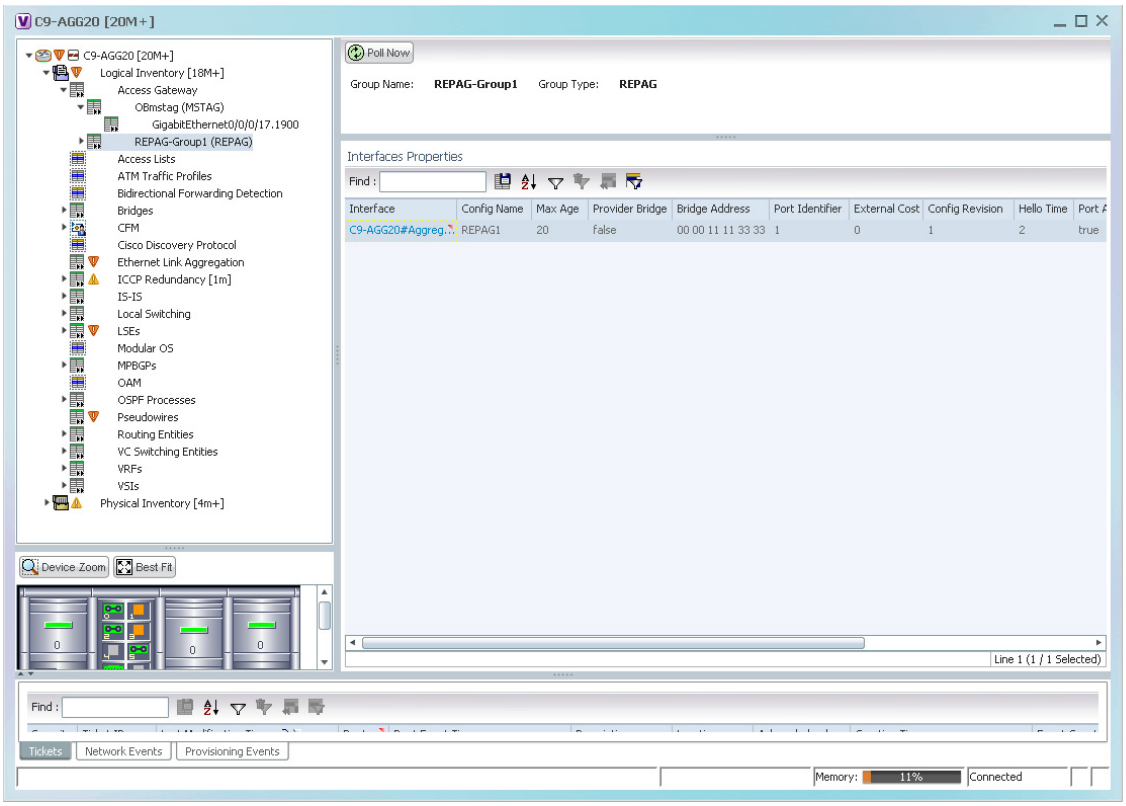


Table 12-11 describes the information that is displayed for an access gateway.

Table 12-11 Access Gateway Properties in Logical Inventory

Field	Description
Group Name	Access gateway group name.
Group Type	Group type: MSTAG or REPAG.
Interface Properties	
Interface	Hyperlink to the interface in physical inventory on which access gateway is configured.
Config Name	Name of the MSTP region. The default value is the MAC address of the switch, formatted as a text string using the hexadecimal representation specified in IEEE Standard 802.
Max Age	In seconds, the maximum age for the bridge. Values range from 6 to 40 seconds.
Provider Bridge	Whether the current instance of the protocol is in 802.1ad mode: True or False.
Bridge Address	Bridge identifier for the interface.
Port Identifier	Port identifier for the interface.
External Cost	External path cost on the current port. Values range from 1 to 200000000.
Config Revision	Number of the configuration revision.
Hello Time	Current hello time (in seconds)
Port Active	Whether or not the port is active: True or False.
BPDUs Sent	Number of BPDUs sent.
Reversion Control Enabled	Whether reversion control is enabled: True or False.

Step 3 Choose an access gateway instance to view instance properties.

Figure 12-8 shows an example of the information displayed for an access gateway instance.

Figure 12-8 Access Gateway Instance in Logical Inventory

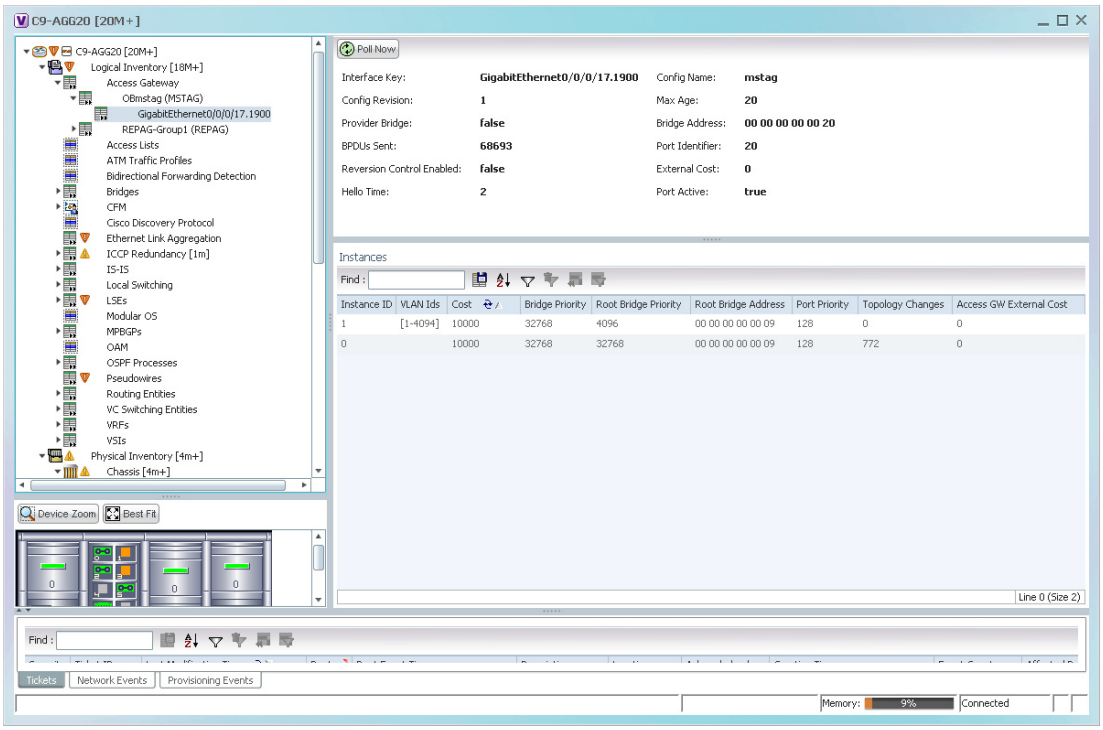


Table 12-12 describes the information that is displayed for an access gateway instance.

Table 12-12 Access Gateway Instance Properties

Field	Description
Interface Key	Hyperlink to the interface in physical inventory on which access gateway is configured.
Config Name	Name of the MSTP region. The default value is the MAC address of the switch, formatted as a text string using the hexadecimal representation specified in IEEE Standard 802.
Config Revision	Number of the configuration revision.
Max Age	In seconds, the maximum age for the bridge. Values range from 6 to 40 seconds.
Provider Bridge	Whether the current instance of the protocol is in 802.1ad mode: True or False.
Bridge Address	Bridge identifier for the current switch.
BPDUs Sent	Number of BPDUs sent.
Port Identifier	Port identifier for the interface.
Reversion Control Enabled	Whether reversion control is enabled: True or False.
External Cost	External path cost on the current port. Values range from 1 to 200000000.

Table 12-12 Access Gateway Instance Properties (continued)

Field	Description
Hello Time	Current hello time (in seconds)
Port Active	Whether or not the port is active: True or False.
Instances Table	
Instance ID	Access gateway instance identifier.
VLAN IDs	VLAN identifiers.
Cost	Path cost for this instance.
Bridge Priority	Priority associated with current bridge.
Root Bridge Priority	Priority associated with the root bridge.
Root Bridge Address	Address of the root bridge.
Port Priority	Priority of the interface for this instance.
Topology Changes	Number of times the topology has changed for this instance.
Access GW External Cost	External root cost of this instance.

Working with Ethernet Link Aggregation Groups

Ethernet link aggregation groups (LAGs) provide the ability to treat multiple switch ports as one switch port. The port groups act as a single logical port for high-bandwidth connections between two network elements. A single link aggregation group balances the traffic load across the links in the channel.

LAG links are discovered automatically for devices that support LAG technology and use VNEs that model Link Aggregation Control Protocol (LACP) attributes.

You can create static links between Ethernet LAGs by choosing a LAG and the desired port channel for the A or Z side as described in Adding Static Links, page 6-15.

If a physical link within the link aggregation group fails, the following actions occur:

- Traffic that was previously carried over the failed link is moved to the remaining links.

  Most protocols operate over single ports or aggregated switch ports and do not recognize the physical ports within the port group.

- An aggregation service alarm is generated.

  The aggregation service alarm indicates the percentage of links within the aggregation that have failed. For example, if an Ethernet link aggregation group contains four Ethernet links and one fails, the aggregation service alarm indicates that 25% of the links are down.

Viewing Ethernet LAG Properties

Note Cisco CRS devices must be configured to receive SNMP traps in order to view Ethernet LAG properties. For more information on required SNMP settings, see the *Cisco Prime Network4.0 Administrator Guide*.

To view properties for Ethernet link aggregation groups:

Step 1 In Prime Network Vision, double-click the device with the link aggregation group you want to view.

Step 2 In the inventory window, choose **Logical Inventory > Ethernet Link Aggregation**.

The link aggregation properties are displayed as shown in Figure 12-9.

Figure 12-9 Ethernet Link Aggregation in Logical Inventory

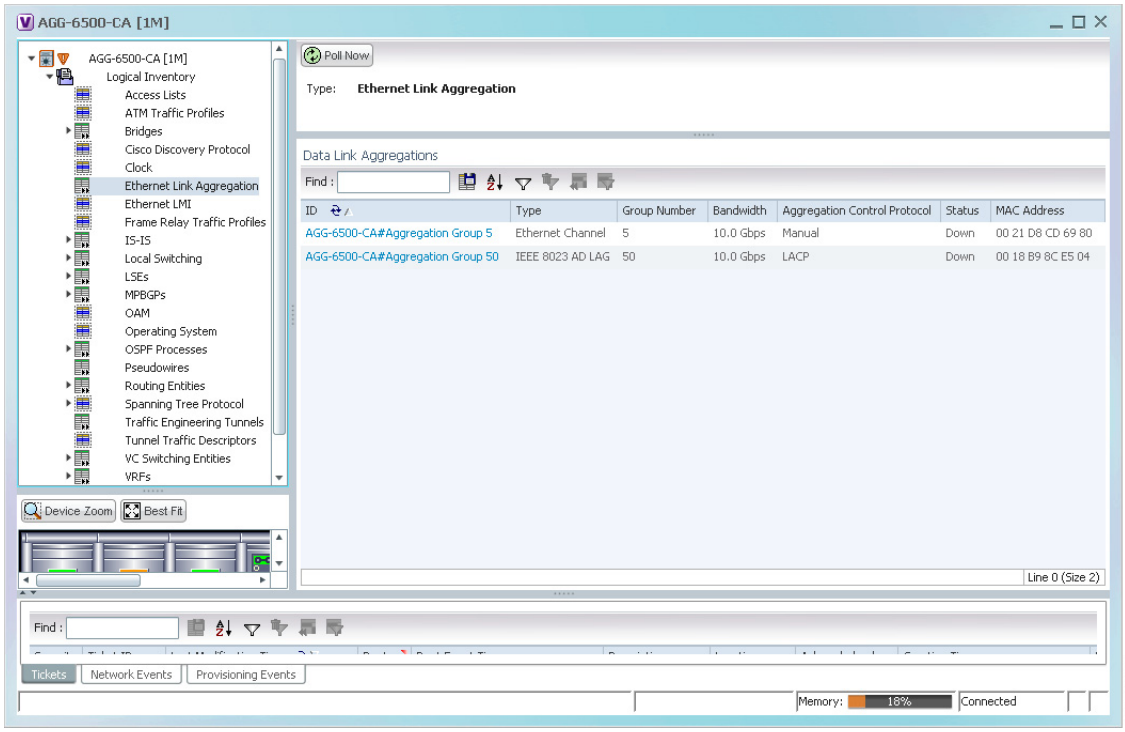


Table 12-13 describes the aggregation group properties that are displayed in the Data Link Aggregations table.

Table 12-13 Data Link Aggregations Table

Field	Description
ID	Aggregation identifier. Double-click the entry to view the properties for that aggregation.
Type	Aggregation group type: Ethernet Channel or IEEE 8023 AD LAG.
Group Number	Aggregation group number.
Bandwidth	Aggregation bandwidth.
Aggregation Control Protocol	Aggregation control protocol: Manual, Link Aggregation Control Protocol (LACP), or Port Aggregation Protocol (PagP).
Status	Aggregation status: Up or Down.
MAC Address	Aggregation MAC address.

Step 3 To view properties for a specific aggregation, double-click the group identifier.

The information that is displayed depends on the type of aggregation:

- For Ethernet Channel aggregations, see Table 12-14.
- For IEEE 802.3 AD aggregations, see Table 12-15.

Table 12-14 LAG Ethernet Channel Properties

Field	Description
Group Number	Aggregation group number.
Bandwidth	Aggregation bandwidth in b/s.
Control Protocol	Aggregation control protocol: Manual, Link Aggregation Control Protocol (LACP), or Port Aggregation Protocol (PagP).
MAC Address	Aggregation MAC address.
Administrative State	Aggregation administrative status: Up or Down.
Operational State	Aggregation operational status: Up or Down.
Adjacent	Adjacent group, hyperlinked to the group in logical inventory.
mLACP Properties	mLACP properties are displayed if the aggregation group is associated with an ICCP redundancy group.
ICCP Redundancy Group	ICCP redundancy group associated with this aggregation group, hyperlinked to the relevant entry in logical inventory.
mLACP Role	Role of the LAG in the redundancy group: Active or Standby.
mLACP Operational System MAC	MAC address used in a dual-homed environment that is selected by ICCP from one of the configured system MAC addresses for one of the points of attachment (PoAs).
mLACP Operational System Priority	Priority used in a dual-homed environment that is selected by ICCP from the configured system priority on one of the PoAs.
mLACP Failover Option	Configured mLACP failover mode: Revertive or Nonrevertive.
mLACP Max Bundle	Maximum number of links allowed per bundle.
Aggregated Ports Table	
ID	Aggregated port identifier, hyperlinked to the interface in physical inventory.
Type	Aggregation type, such as Layer 2 VLAN.
Mode	VLAN mode, such as Trunk.
Native VLAN ID	VLAN identifier (VID) associated with this VLAN. The range of VLANs is 1 to 4067.
VLAN Encapsulation Type	Type of encapsulation configured on the VLAN, such as IEEE 802.1Q.
Allowed VLANs	List of VLANs allowed on this interface.
VLAN Encapsulation Admin Type	VLAN administration encapsulation type, such as IEEE 802.1Q.
Subinterfaces Table	
Address	IP address of the subinterface.
Mask	Subnet mask applied to the IP address.
VLAN Type	Type of VLAN, such as Bridge or IEEE 802.1Q.

Table 12-14 LAG Ethernet Channel Properties (continued)

Field	Description
Operational State	Operational state of the subinterface: Up or Down.
VLAN ID	VLAN identifier.
Inner VLAN	CE-VLAN identifier.
IP Interface	IP interface configured as part of the subinterface, hyperlinked to the routing entity or VRF in logical inventory.
VRF Name	VRF associated with the subinterface.
Is MPLS	Whether the subinterface is enabled for MPLS: True or False. This column is displayed when at least one interface is MPLS-enabled.
Tunnel Edge	Whether this is a tunnel edge: True or False.
VC	Virtual circuit identifier, hyperlinked to the VC Table when the subinterface is configured for ATM VC.
Binding	Hyperlinked entry to the specific bridge in logical inventory.
EFPs Table	
EFP ID	EFP identifier.
Operational State	EFP operational state: Up or Down.
VLAN	VLAN associated with this EFP.
Inner VLAN	CE-VLAN identifier.
Translated VLAN	Translated, or mapped, VLAN identifier.
Translated Inner VLAN	Translated, or mapped, inner VLAN identifier.
Binding	Hyperlinked entry to the specific bridge in logical inventory.
Description	Description for the EFP.

Table 12-15 LAG IEEE 802.3 AD Properties

Field	Description
Group Number	Aggregation group number.
Bandwidth	Aggregation bandwidth.
Control Protocol	Aggregation control protocol: Manual, Link Aggregation Control Protocol (LACP), or Port Aggregation Protocol (PagP).
MAC Address	Aggregation MAC address.
Administrative State	Aggregation administrative status: Up or Down.
Operational State	Aggregation operational status: Up or Down.
Dot3ad Agg Partner System Priority	Priority of the partner system.
Dot3ad Agg MAC Address	Aggregation MAC address.
Dot3ad Agg Actor Admin Key	Actor administrative key.
Dot3ad Agg Actor System Priority	Actor system priority.
Dot3ad Agg Partner Oper Key	Partner operational key.
Dot3ad Agg Actor Oper Key	Actor operational key.
Dot3ad Agg Collector Max Delay	Maximum delay (in microseconds) for either delivering or discarding a received frame by the frame collector.
Dot3ad Agg Actor System ID	Actor system identifier, in the form of a MAC address.
Dot3ad Agg Partner System ID	Partner system identifier, in the form of a MAC address.
mLACP Properties	mLACP properties are displayed if the aggregation group is associated with an ICCP redundancy group.
ICCP Redundancy Group	ICCP redundancy group associated with this aggregation group, hyperlinked to the relevant entry in logical inventory.
mLACP Role	Role of the LAG in the redundancy group: Active or Standby.
mLACP Operational System MAC	MAC address used in a dual-homed environment that is selected by ICCP from one of the configured system MAC addresses for one of the points of attachment (PoAs).
mLACP Operational System Priority	Priority used in a dual-homed environment that is selected by ICCP from the configured system priority on one of the PoAs.
mLACP Failover Option	Configured mLACP failover mode: Revertive or Nonrevertive.
mLACP Max Bundle	Maximum number of links allowed per bundle.
Aggregated Ports Table	
ID	Port identifier, hyperlinked to the interface in physical inventory.
Type	Type of VLAN, such as Layer 2 VLAN.
Discovery Protocols	Discovery protocols used on this port.

Table 12-15 LAG IEEE 802.3 AD Properties (continued)

Field	Description
Subinterfaces Table	
Address	IP address of the subinterface.
Mask	Subnet mask applied to the IP address.
VLAN Type	Type of VLAN, such as Bridge or IEEE 802.1Q.
Operational State	Operational state of the subinterface: Up or Down.
VLAN ID	VLAN identifier.
Inner VLAN	CE-VLAN identifier.
IP Interface	IP interface configured as part of the subinterface, hyperlinked to the routing entity or VRF in logical inventory.
VRF Name	VRF associated with the subinterface.
VC	Virtual circuit identifier, hyperlinked to the VC Table when the subinterface is configured for ATM VC.
Binding	Hyperlinked entry to the specific bridge in logical inventory.
EFPs Table	
EFP ID	EFP identifier.
Operational State	EFP operational state: Up or Down.
VLAN	VLAN associated with this EFP.
Inner VLAN	CE-VLAN identifier.
Translated VLAN	Translated, or mapped, VLAN identifier.
Translated Inner VLAN	Translated, or mapped, inner VLAN identifier.
Binding	Hyperlinked entry to the specific bridge in logical inventory.
Description	Description for the EFP.
LACP Port Entries	
Aggregated Port	Port on which the aggregation is configured, hyperlinked to the entry in physical inventory.
Dot3ad Agg Port Partner Admin Port Priority	Administrative port priority for the partner.
Dot3ad Agg Port Partner Admin Key	Administrative key for the partner port.
Dot3ad Agg Port Partner Oper Port Priority	Priority assigned to the aggregation port by the partner.
Dot3ad Agg Port Actor Oper State	Local operational state for the port.
Dot3ad Agg Port Actor Admin State	Local administrative state as transmitted by the local system in LACP data units (LACPDUs).
Dot3ad Agg Port Selected Agg ID	Selected identifier for the aggregation port.
Dot3ad Agg Port Partner Oper Key	Operational key for the partner port.
Dot3ad Agg Port Partner Admin State	Partner administrative state.
Dot3ad Agg Port Actor Port Priority	Priority assigned to the local aggregation port.
Dot3ad Agg Port Partner Oper State	Partner administrative state as transmitted by the partner in the most recently transmitted LAPCDU.
Dot3ad Agg Port Attached Agg ID	Identifier of the aggregator that the port is attached to.

Table 12-15 LAG IEEE 802.3 AD Properties (continued)

Field	Description
Dot3ad Agg Port Actor Admin Key	Administrative key for the local port.
Dot3ad Agg Port Actor Port	Number assigned to the local aggregation port.
Dot3ad Agg Port Partner Oper Port	Number assigned to the aggregation port by the partner.
Dot3ad Agg Port Actor Oper Key	Operational for the local port.
Dot3ad Agg Port Partner Admin Port	Administrative value of the port for the partner.

Viewing mLACP Properties

Prime Network Vision supports the discovery of Multichassis LACP (mLACP) configurations on devices configured for them, and displays mLACP configuration information, such as redundancy groups and properties, in inventory.

To view mLACP properties:

Step 1 In Prime Network Vision, double-click the element configured for mLACP.

Step 2 In the inventory window, choose **Logical Inventory > ICCP Redundancy**.

In response, Prime Network Vision lists the Inter-Chassis Communication Protocol (ICCP) redundancy groups configured on the device as shown in Figure 12-10.

Figure 12-10 ICCP Redundancy in Logical Inventory

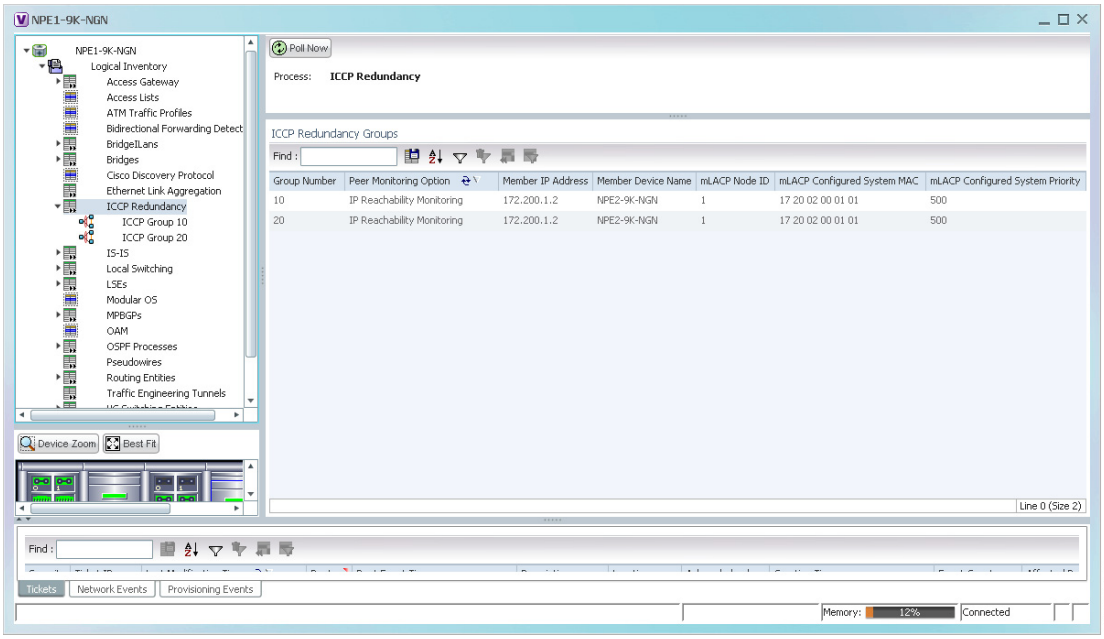


Table 12-16 describes the information displayed in the ICCP Redundancy Groups table.

Table 12-16 ICCP Redundancy Groups in Logical Inventory

Field	Description
Group Number	ICCP group identifier.
Peer Monitoring Option	Method used to monitor the peer: BFD or IP Reachability Monitoring.
Member IP Address	IP address of the neighbor PoA device.
Member Device Name	Name of the neighbor PoA device.
mLACP Node ID	Identifier used by this member of the mLACP redundancy group.
mLACP Configured System MAC	System MAC address of the redundancy group advertised to other members of the mLACP redundancy group and used for arbitration.
mLACP Configured System Priority	System priority advertised to other mLACP members of the redundancy group.

Step 3 To view additional information about an ICCP redundancy group, do either of the following:

- In the logical inventory window navigation pane, choose **Logical Inventory ICCP Redundancy >** *ICCP-group*.
- In the logical inventory content pane, right-click the required group in the ICCP Redundancy Groups table and choose **Properties**.

The ICCP Redundancy Group Properties window is displayed with the Backbone Interfaces and Data Link Aggregations tabs as shown in Figure 12-11.

Figure 12-11 ICCP Redundancy Group Properties Window

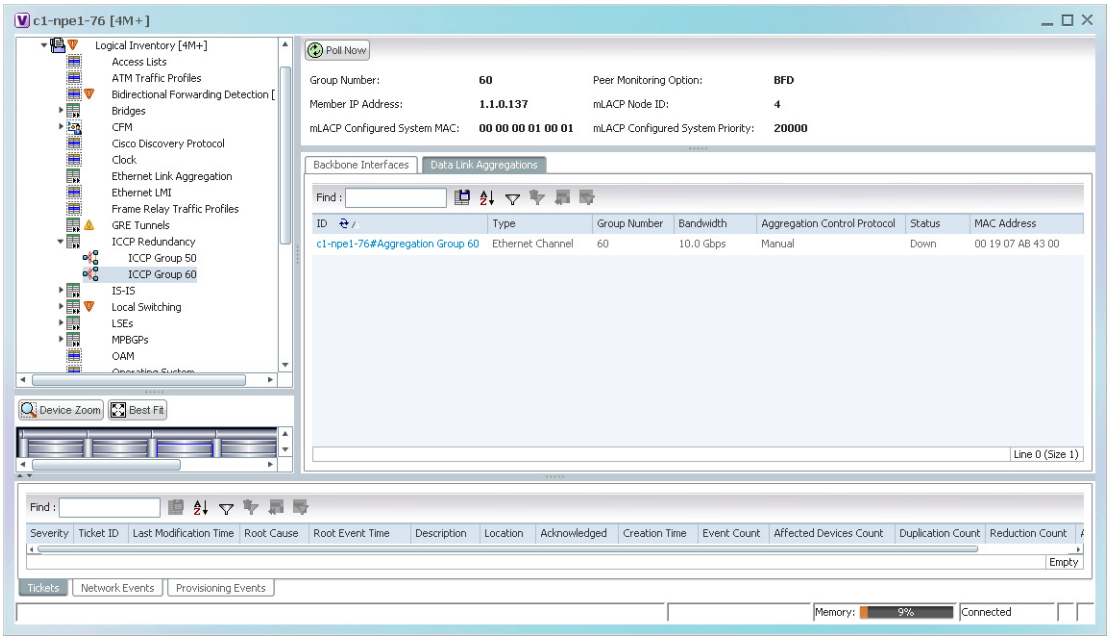


Table 12-17 describes the information available in the ICCP Redundancy Group Properties window.

Table 12-17 ICCP Redundancy Group Properties Window

Field	Description
Group Number	ICCP group identifier.
Peer Monitoring Option	Method used to monitor the peer: BFD or IP Reachability Monitoring.
Member IP Address	IP address of the neighbor PoA device.
Member device name	Name of the neighbor PoA device.
mLACP Node ID	Identifier used by this member of the mLACP redundancy group.
mLACP Configured System MAC	System MAC address of the redundancy group advertised to other members of the mLACP redundancy group and used for arbitration.
mLACP Configured System Priority	System priority advertised to other mLACP members of the redundancy group.
Backbone Interfaces Tab	
ID	Backbone interface defined for the redundancy group, hyperlinked to the relevant entry in logical inventory.
Status	Status of the backbone interface: Up, Down, or Unknown.
Data Link Aggregations Tab	
ID	Link aggregation group associated with the redundancy group, hyperlinked to the relevant entry in logical inventory.
Type	Aggregation group type: Ethernet Channel or IEEE 8023 AD LAG.
Group Number	Aggregation group number.
Bandwidth	Aggregation bandwidth.
Aggregation Control Protocol	Aggregation control protocol: Manual, LACP, or PAgP.
Status	Aggregation status: Up or Down.
MAC Address	Aggregation MAC address.

Step 4 To view additional mLACP properties, double-click the entry for the required link aggregation group in the Data Link Aggregations tab.

mLACP information is displayed in the Link Aggregation Group Properties window, as described in the following tables:

- Table 12-14—LAG Ethernet Channel Properties
- Table 12-15—LAG IEEE 802.3 AD Properties

Viewing Provider Backbone Bridge Properties

Provider backbone bridges (PBBs), specified by IEEE 802.1ah-2008, provide a way to increase the number of service provider supported Layer 2 service instances beyond the number supported by QinQ and VPLS. PBB adds a backbone VLAN tag and backbone destination and source MAC addresses to encapsulate customer Ethernet frames and create a MAC tunnel across core switches.

Prime Network supports PBB inventory discovery and modeling for the following devices:

- Cisco 7600-series devices running Cisco IOS version 12.2(33)SRE1
- Cisco ASR 9000-series devices running Cisco IOS XR version 3.9.1

Prime Network models the IB type of Backbone edge bridges which includes both I-type and B-type components.

To view PBB properties:

Step 1 In Prime Network Vision, double-click the element configured for PBB.

Step 2 In the inventory window, choose **Logical Inventory > BridgeILans >** *PBB-bridge*.

Figure 12-12 shows an example of PBB properties in logical inventory.

Figure 12-12 PBB Properties in Logical Inventory

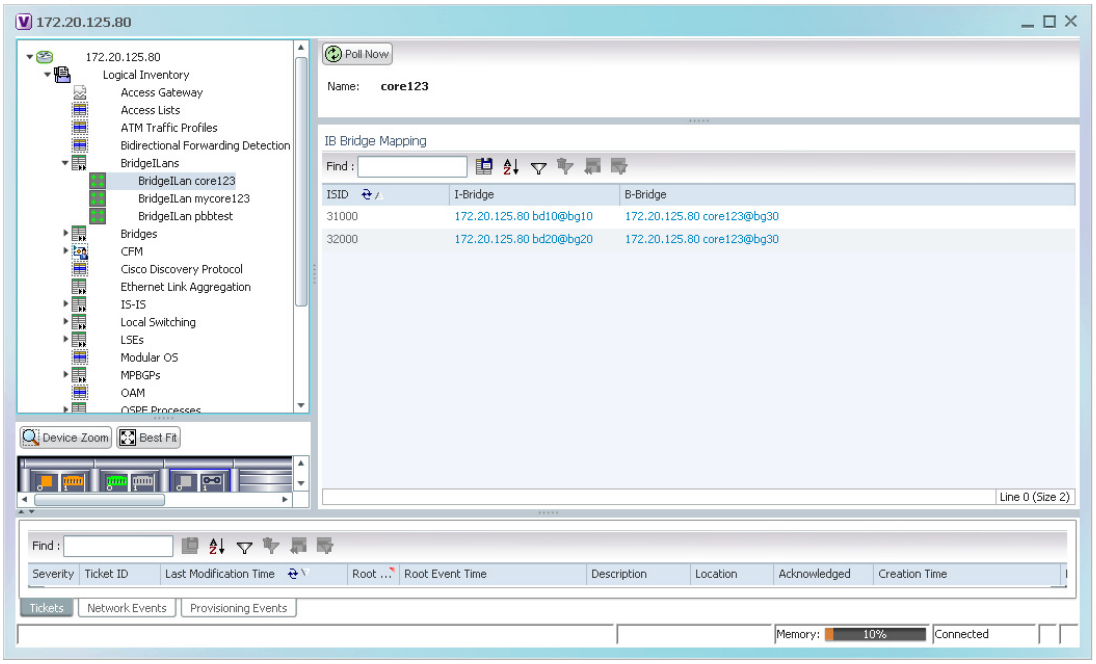


Table 12-18 describes the information displayed for PBB.

Table 12-18 PBB Properties in Logical Inventory

Field	Description
Name	Identifier of the bridge as follows: • For Cisco 7600 devices, the identifier of the MAC tunnel created. • For Cisco ASR 9000-series devices, the identifier is a combination of the bridge group and the bridge domain on the B-Bridge component.
IB Bridge Mapping Table	
ISID	24-bit entry representing the Backbone service instance.
I-Bridge	XID of the I-Bridge component, hyperlinked to the relevant bridge in logical inventory.
B-Bridge	XID of the B-Bridge component, hyperlinked to the relevant bridge in logical inventory.

Viewing EFP Properties

Prime Network Vision provides information about EFPs in a number of ways. For example:

- EFP names displayed in Prime Network Vision maps add EFP and the managed element name to the interface name, such as GigabitEthernet4/0/1 EFP: 123@c4-npe5-67.
- If you select an EFP in the navigation pane in Prime Network Vision and then click **Show List View**, an Ethernet Flow Points table lists the network element, port, and network VLAN associated with the EFP.

To view additional EFP properties:

Step 1 In the Prime Network Vision map view, select the required EFP in the navigation pane or in the map pane and then do either of the following:

- Right-click the EFP and choose **Properties**.
- Choose **Node > Properties**.

Figure 12-13 shows an example of the EFP Properties window.

Figure 12-13 EFP Properties Window

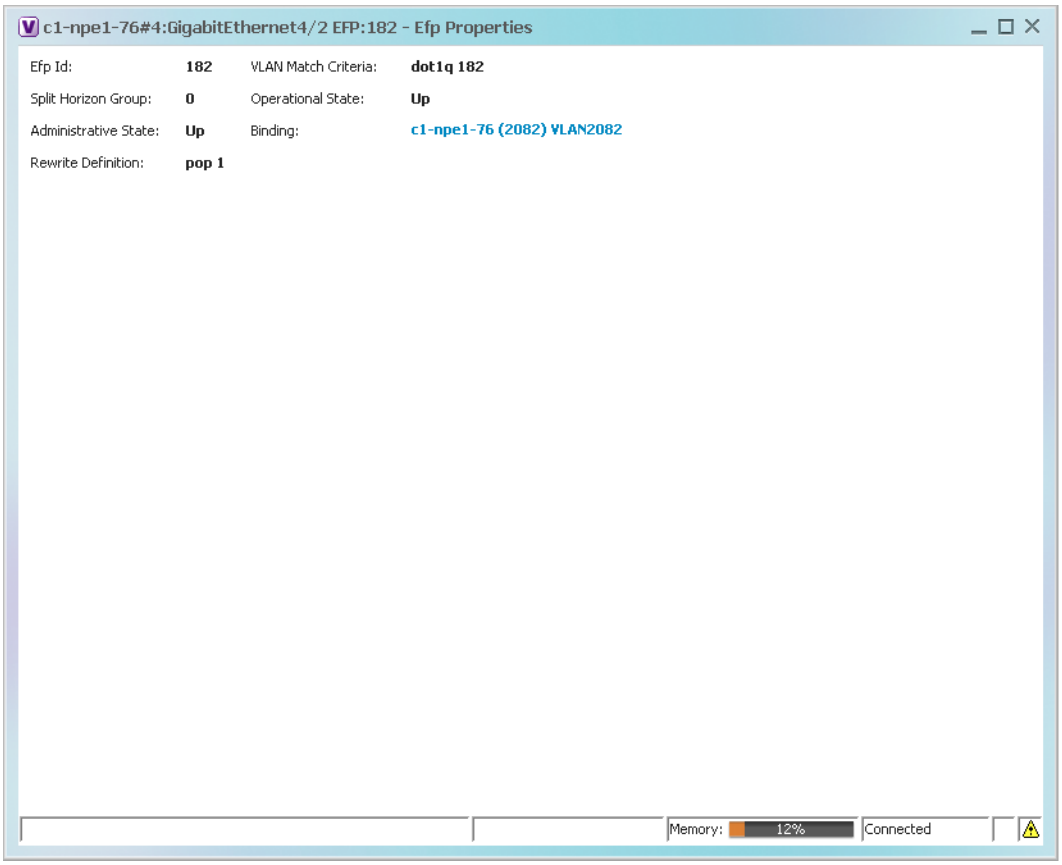


Table 12-19 describes the information displayed in the EFP Properties window.

Table 12-19 EFP Properties Window

Field	Description
EFP ID	Identifier for the EFP.
VLAN Match Criteria	Match criteria configured on the EFP for forwarding decisions.
Split Horizon Group	Split horizon group to which the EFP is associated. If no split horizon group is defined, the value is null. If only one split horizon group exists and it is enabled for the EFP, the value is the default group 0.
Operational State	Operational status of the EFP: Up or Down.
Administrative State	Administrative status of the EFP: Up or Down.
Binding	Hyperlinked entry to the relevant item in logical inventory, such as a pseudowire or bridge.
Rewrite Definition	Rewrite command configured on the EFP: **pop**, **push**, or **translate**.

Step 2 Click the hyperlink entry in the Binding field to view the related properties in logical inventory.

In this example, clicking the hyperlink displays the relevant bridge in logical inventory, as shown in Figure 12-14.

Figure 12-14 Bridge Associated with EFP in Logical Inventory

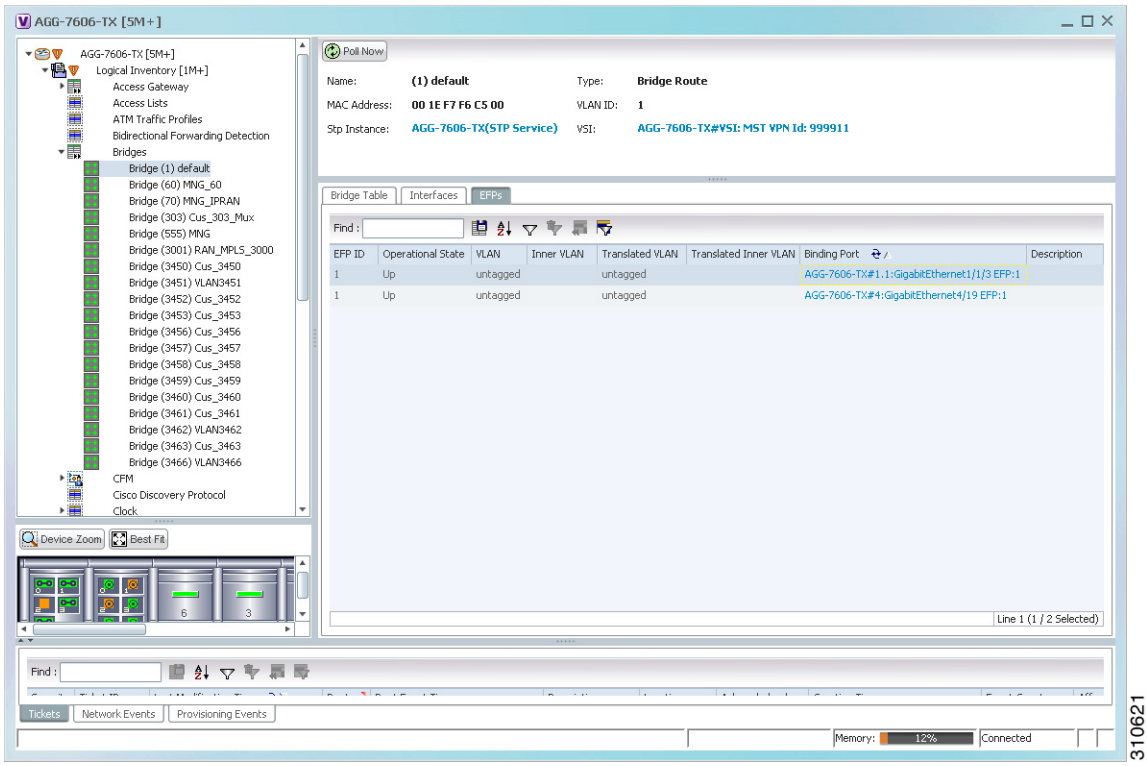


Table 12-20 describes the information displayed for an EFP associated with a bridge.

Table 12-20 EFP Associated with a Bridge in Logical Inventory

Field	Description
Name	VLAN bridge name.
Type	VLAN bridge type.
MAC Address	VLAN bridge MAC address.
VLAN ID	VLAN bridge VLAN identifier.
STP Instance	STP instance information, hyperlinked to the STP entry in logical inventory.
VSI	VSI information, hyperlinked to the VSI entry in logical inventory.

Table 12-20 EFP Associated with a Bridge in Logical Inventory (continued)

Field	Description
EFPs Table	
EFP ID	EFP identifier.
Operational State	EFP operational state: Up or Down.
VLAN	VLAN associated with this EFP.
Inner VLAN	CE-VLAN identifier.
Translated VLAN	Translated, or mapped, VLAN identifier.
Translated Inner VLAN	Translated, or mapped, inner VLAN identifier.
Binding	Hyperlinked entry to the specific interface and EFP entry in physical inventory.
Description	Description for the EFP.

Step 3 To view EFP properties in physical inventory, navigate to the required interface in one of the following ways:

- In the bridge entry in logical inventory, click the hyperlinked entry in the Binding field.
- Use the procedure described in Viewing and Renaming Ethernet Flow Domains, page 12-42 to navigate to the individual interface.
- In physical inventory, navigate to and then select the required interface.

The EFPs tab is displayed in the content pane next to the Subinterfaces tab as shown in Figure 12-15.

Figure 12-15 EFPs Tab in Physical Inventory

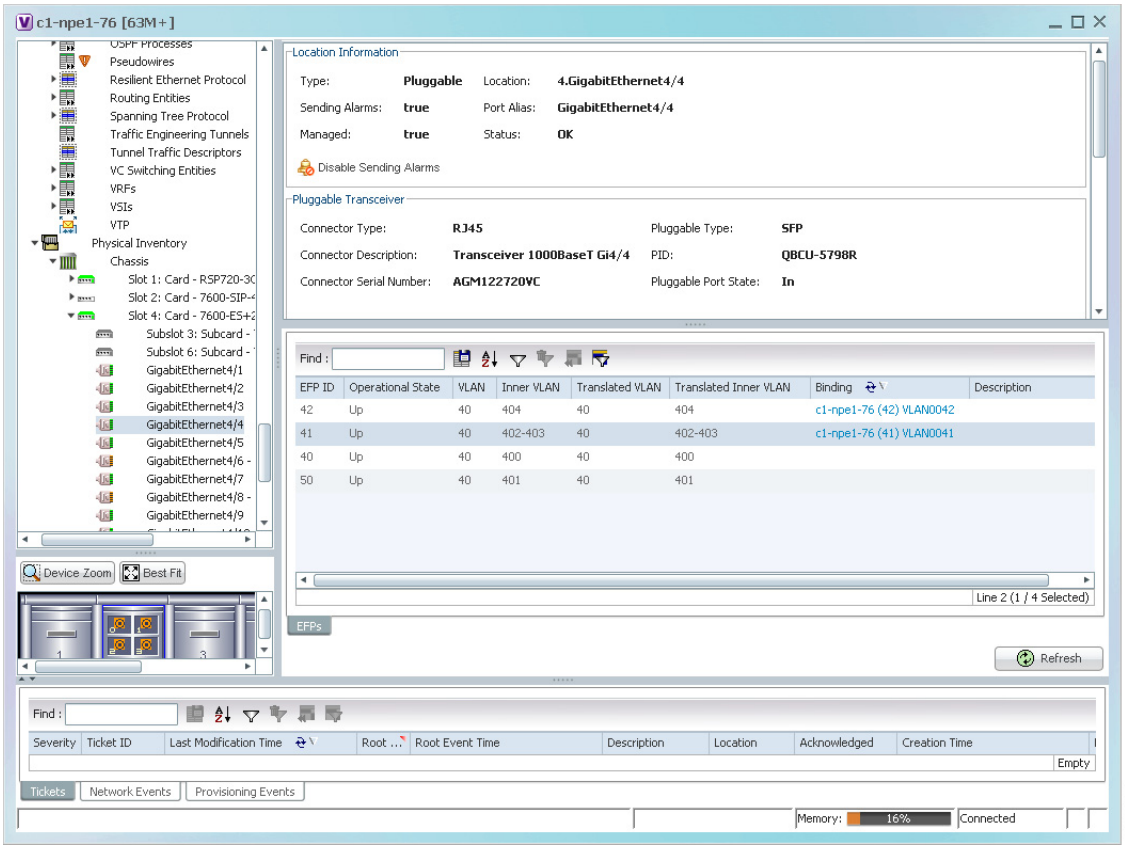


Table 12-21 describes the information displayed in the EFPs tab.

Table 12-21 EFPs Tab

Field	Description
EFP ID	EFP identifier.
Operational State	EFP operational state.
VLAN	VLAN identifier.
Inner VLAN	CE-VLAN identifier.
Translated VLAN	Translated VLAN identifier.
Translated Inner VLAN	Translated CE-VLAN identifier.
Binding	Hyperlinked entry to the specific bridge or pseudowire in logical inventory.
Description	Configured description for the EFP.

Connecting a Network Element to an EFP

You can add and connect network elements to an EFP under an existing aggregation for VLAN, VPLS, Pseudowire, and Ethernet Service.

To connect network elements to an EFP:

Step 1 Select an EFP node under the VLAN/VPLS/Pseudowire/Ethernet Service aggregation node and choose **File > Add to Map > Network Element**.

Step 2 In the Add Network Element dialog box, search for the desired network elements and choose the network element that you want to add.

The selected network element appears under the aggregation node in the navigation pane.

Step 3 Right-click the EFP node and choose **Topology > Connect CE Device**.

Step 4 Right-click the network element that you added and choose **Topology > Connect to** *EFP*.

The map view displays a link between the EFP and the added network element. If required, you can remove the link, by right-clicking the link and choosing **Remove Link**.

Step 5 To hide or show the connected network elements, right-click the EFP node and choose **Hide Connected Devices** or **Show CE device**.

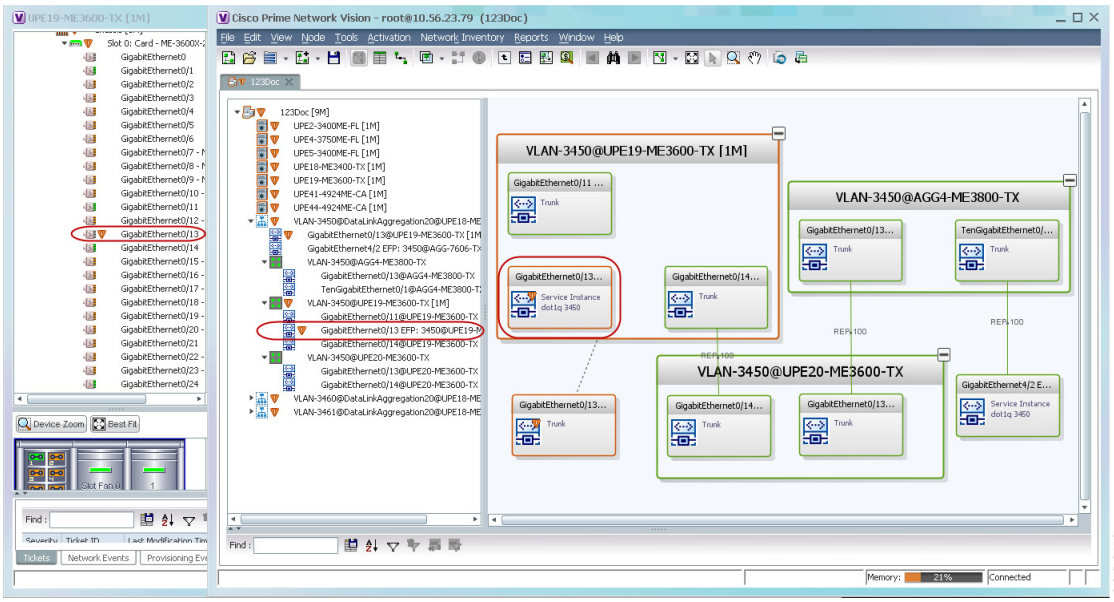
Understanding EFP Severity and Ticket Badges

Severity and ticket badges are displayed on EFP icons as follows:

- If the VLAN EFP element represents a configuration, such as a service instance on a Cisco 7600 device or an enhanced port on a Cisco ASR 9000 device, and is associated directly with a network VLAN or a bridge domain switching entity, the severity and ticket badges are based on the underlying service instance or enhanced port configuration.

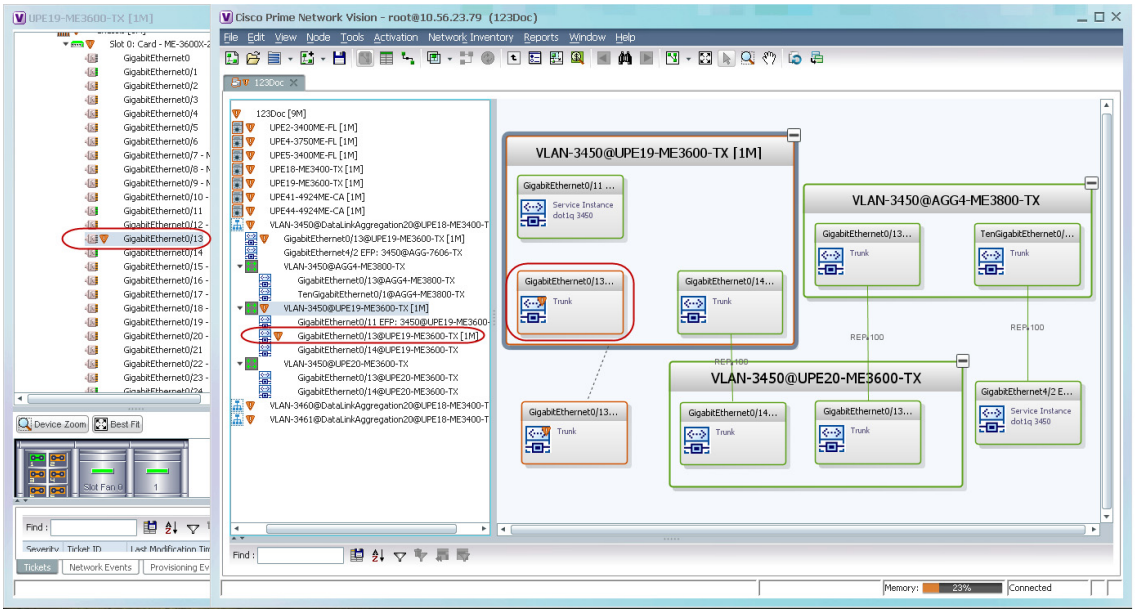
  Figure 12-16 shows an example of a ticket badge based on a service instance.

Figure 12-16 EFP Severity and Ticket Badges Based on Underlying Service Instance



- If the Ethernet flow point element represents a VLAN interface for a regular switch port, the severity and ticket badges are based on the corresponding port, as shown in Figure 12-17.

Figure 12-17 EFP Severity and Ticket Badges Based on Corresponding Port



Viewing EVC Service Properties

Certain EVC service properties are configured as port attributes. These attributes determine the degree of service transparency and protect the service provider's network from protocol control traffic. Prime Network Vision discovers these key EVC service properties and displays this information in physical inventory for the following devices:

- Cisco ME3400- and Cisco ME3400E-series devices running Cisco IOS versions 12.2(52)SE to 12.2(54)SE.
- Cisco 3750 Metro devices running Cisco IOS versions 12.2(52)SE to 12.2(54)SE.

Shared Switching Entities and EVC Service View

Some switching entities that Prime Network Vision discovers are concurrently part of a network VLAN and VPLS/EoMPLS instance. These switching entities are referred to as *shared switching entities*.

Prime Network Vision displays the switching entity information for shared switching entities only under the VPLS instances in the EVC service view.

To view EVC port-related properties for the supported devices and software versions:

Step 1 In Prime Network Vision, double-click the required device.

Step 2 In the inventory window, choose **Physical Inventory > Chassis >** *module* **>** *port*.

Figure 12-18 shows an example of a port in physical inventory configured with these EVC properties.

Figure 12-18 EVC Port Properties in Physical Inventory

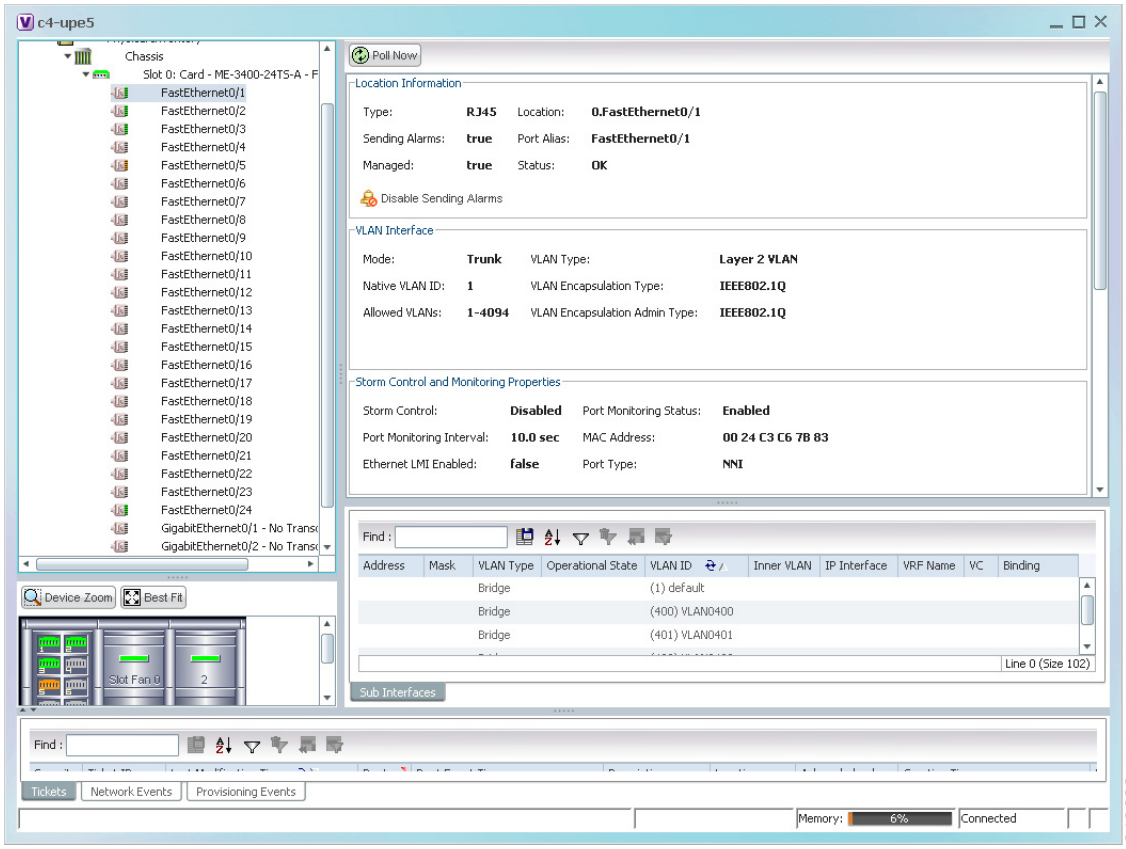


Table 12-22 describes the information displayed for these properties.

Table 12-22 EVC Port Properties in Physical Inventory

Field	Description
Storm Control and Monitoring Properties Area	
Storm Control	Status of storm control on the port: Enabled or Disabled.
Port Monitoring Status	Status of port monitoring: • Enabled—The switch sends keepalive messages on user network interfaces (UNIs) and enhanced network interfaces (ENIs) and does not send keep alive messages on network node interfaces (NNIs). • Disabled—The switch does not send keepalive messages.
Port Monitoring Interval	Keepalive interval in seconds. The default value is ten seconds.
Storm Control Level	Representing a percentage of the total available bandwidth of the port, the threshold at which additional traffic of the specified type is suppressed until the incoming traffic falls below the threshold.
Storm Control Type	Type of storm the port is configured for protection from: Broadcast, Multicast, or Unicast.

Table 12-22 EVC Port Properties in Physical Inventory (continued)

Field	Description
Security Properties Areas	
Port Security	Status of security on the port: Enabled or Disabled.
MAC Address Limit	Maximum number of MAC addresses allowed on the interface.
Aging Type	Type of aging used for automatically learned addresses on a secure port: • Absolute—Times out the MAC address after the specified age-time has been exceeded, regardless of the traffic pattern. This is the default for any secured port, and the age-time value is set to 0. • Inactivity—Times out the MAC address only after the specified age-time of inactivity from the corresponding host has been exceeded.
Aging Time	Length of time, in minutes, that a MAC address can remain on the port security table.
Violation Mode	Action that occurs when a new device connects to a port or when a new device connects to a port after the maximum number of devices are connected: • Protect—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value • Restrict—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment. • Shutdown—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.

Viewing and Renaming Ethernet Flow Domains

An Ethernet flow domain represents an Ethernet access domain. The Ethernet flow domain holds all network elements between the CE (inclusive, if managed by the SP), up to the SP core (exclusive). This includes CE, access, aggregation, and distribution network elements.

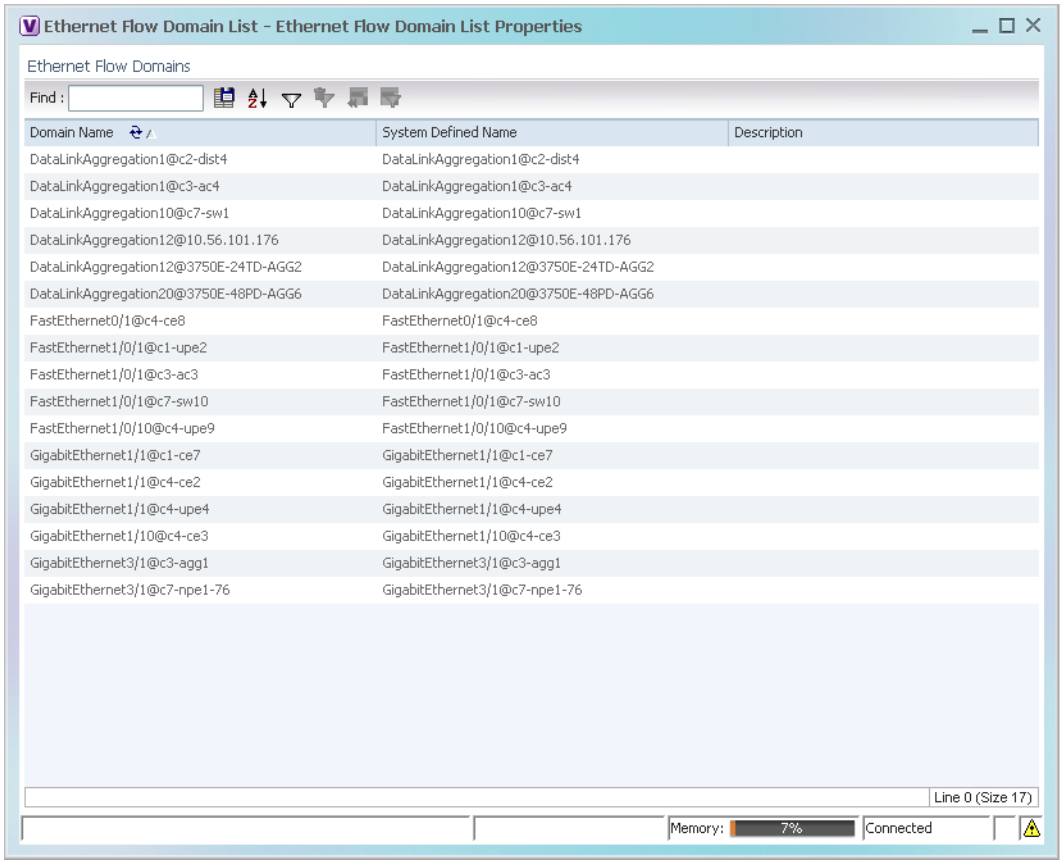
An Ethernet flow domain can have no N-PEs (flat VLAN) or one or more N-PEs (N-PE redundancy configuration). The Ethernet flow domain is defined using physical connectivity at the port level, and not at the network element level. STP is used to mark the root bridge, root or blocked ports, and blocked VLAN links.

To view Ethernet flow domains:

Step 1 In Prime Network Vision, choose **Network Inventory > Ethernet Flow Domains**.

The Ethernet Flow Domain List window is displayed with the domain name, the system-defined domain name, and a brief description for each Ethernet flow domain as shown in Figure 12-19.

Figure 12-19 Ethernet Flow Domain List Properties Window



Step 2 To rename an Ethernet flow domain:

a. Right-click the required domain, then choose **Rename**.

b. In the Rename Node dialog box, enter a new name for the domain.

c. Click **OK**.

The window is refreshed, and the new name is displayed.

Step 3 To view Ethernet flow domain properties, do either of the following:

- Right-click the required domain, then choose **Properties**.
- Double-click the required domain.

The Ethernet Flow Domain Properties window is displayed as shown in Figure 12-20.

Figure 12-20 Ethernet Flow Domain Properties Window

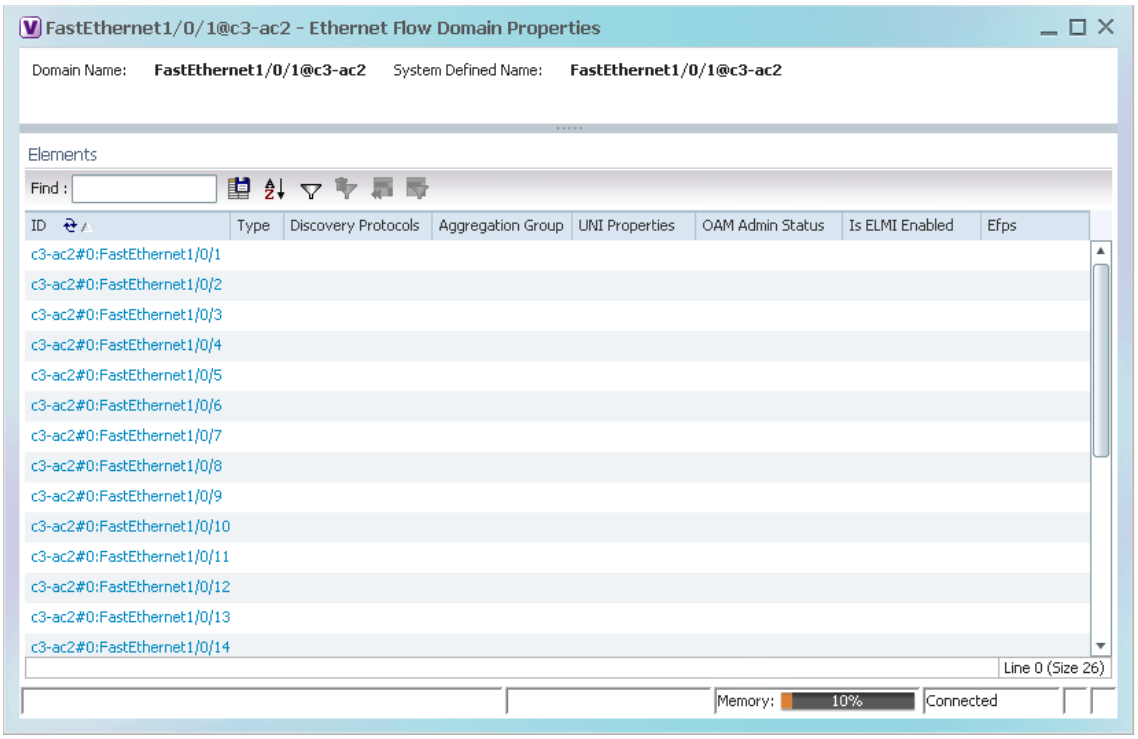


Table 12-23 describes the information displayed in the Ethernet Flow Domain Properties window.

Note Not all fields are available in all tables. The table contents depend on the domain type, such as FastEthernet.

Table 12-23 Ethernet Flow Domain Properties Window

Field	Description
Domain Name	Name of the selected domain.
System Defined Name	Domain name as identified by the most dominant device and its lowest port name lexicographically.
Elements Table	
ID	Interface identifier, hyperlinked to the interface in physical inventory.
Type	Aggregation group type: Ethernet Channel (EtherChannel), or IEEE 8023 AD LAG (IEEE 802.3 link aggregation group).
Discovery Protocols	Discovery protocols used on the interface.
Is ELMI Enabled	Whether or not Ethernet LMI is enabled on the interface: True or False.

Step 4 To navigate to the individual interface or link aggregation group, click an interface identifier or group.

The interface or link aggregation group properties are displayed in the inventory window.

Working with VLANs

The following topics provide information and procedures for working with VLANs. The Vision GUI client supports a VLAN overlay which, when applied, highlights the network elements and links that a VLAN (and its associated VLANs) traverse. The overlay displays STP and REP link and port information. Using overlays is described in Displaying VLANs By Applying VLAN Overlays to a Map45, page 12-61.

- Understanding VLAN and EFD Discovery, page 12-45
- Understanding VLAN Elements, page 12-46
- Switching Entities Containing Termination Points, page 12-50
- Adding and Removing VLANs from a Map, page 12-50
- Viewing VLAN Mappings, page 12-53
- Working with Associated VLANs, page 12-55
- Viewing VLAN Links Between VLAN Elements and Devices, page 12-58
- Displaying VLANs By Applying VLAN Overlays to a Map45, page 12-61
- Viewing VLAN Service Link Properties, page 12-63
- Viewing REP Information in VLAN Domain Views and VLAN Overlays, page 12-63
- Viewing REP Properties for VLAN Service Links, page 12-64
- Viewing STP Information in VLAN Domain Views and VLAN Overlays, page 12-66
- Viewing STP Properties for VLAN Service Links, page 12-67
- Viewing VLAN Trunk Group Properties, page 12-68
- Viewing VLAN Bridge Properties, page 12-70
- Using Commands to Work With VLANs, page 12-72

Understanding VLAN and EFD Discovery

When you start the Prime Network gateway the first time, Prime Network Vision waits for two topology cycles to complete before discovering new VLANs, VLAN associations, and EFDs. The default configured time for two topology cycles to complete is one hour, but might be configured for longer periods of time on large setups. This delay allows the system to stabilize, and provides the time needed to model devices and discover links.

During this delay, Prime Network Vision does not add VNEs or apply updates to existing VLANs or EFDs.

After the initial delay has passed, Prime Network Vision discovers new VLANs, VLAN associations, and EFDs, applies updates to existing VLANs, VLAN associations, and EFDs, and updates the database accordingly.

When you restart the gateway, Prime Network Vision uses the persisted topology information instead of waiting two topology cycles, thus improving the discovery time for new VLANs, VLAN associations, and EFDs.

Understanding VLAN Elements

The following concepts are important to understand when working with the representation of edge EFPs inside VLANs:

- VLAN Elements in Prime Network Vision, page 12-46
- VLANs, page 12-46
- Switching Entities, page 12-46
- Ethernet Flow Points, page 12-47

VLAN Elements in Prime Network Vision

Table 12-24 describes the icons that Prime Network Vision uses to represent VLAN elements.

Table 12-24 VLAN Elements and Icons in Prime Network Vision

Element	Associated Network Element	Icon
Network VLAN	None	
Switching entity	Bridge	
Ethernet Flow Point (EFP)	Ethernet port	

VLANs

Prime Network Vision discovers and allows you to display maps with a network-level view of VLANs.

In Prime Network, a VLAN entity consists of one or more switching entities and the corresponding EFP elements.

A network VLAN represents the virtual LAN. The network VLAN holds its contained switching entities and can be associated to a customer. The network VLAN also holds the Ethernet flow points that are part of the network VLAN but not part of any switching entity. For example, a port that tags ingress flows after which the flow moves to a different VLAN.

Switching Entities

A switching entity represents a device-level Layer 2 forwarding entity (such as a VLAN or bridge domain) that participates in a network VLAN. A switching entity is associated to a network VLAN according to its relationship to the same Ethernet Flow Domain (EFD) and the VLAN identifier.

If you right-click a switching entity in Prime Network Vision and then choose **Inventory**, the inventory window is displayed with the corresponding bridge selected in Logical Inventory.

A switching entity typically contains EFP elements.

Ethernet Flow Points

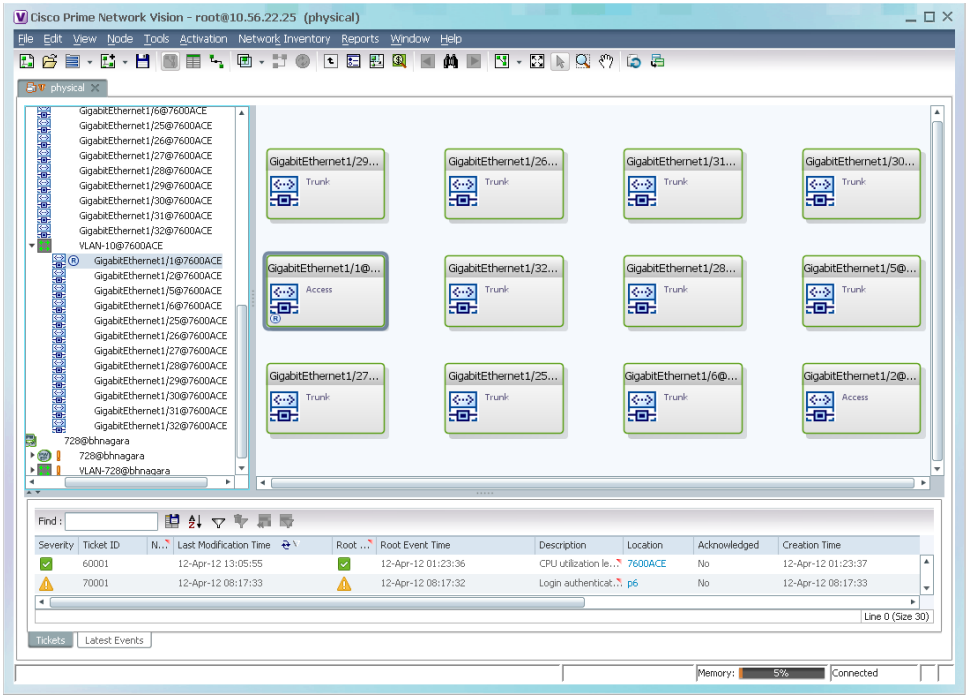
An Ethernet flow point (EFP) can represent a port that is configured for participation in a specific VLAN.

If you right-click an EFP in Prime Network Vision and then choose **Inventory**, the inventory window is displayed with the corresponding port selected in Physical Inventory.

EFPs that are located in a switching entity represent Ethernet ports that are configured as switch ports (in either Access, Trunk, or Dot1Q tunnel mode).

Figure 12-21 shows an example of EFPs configured as switch ports in Prime Network Vision.

Figure 12-21 EFPs Configured as Switch Ports

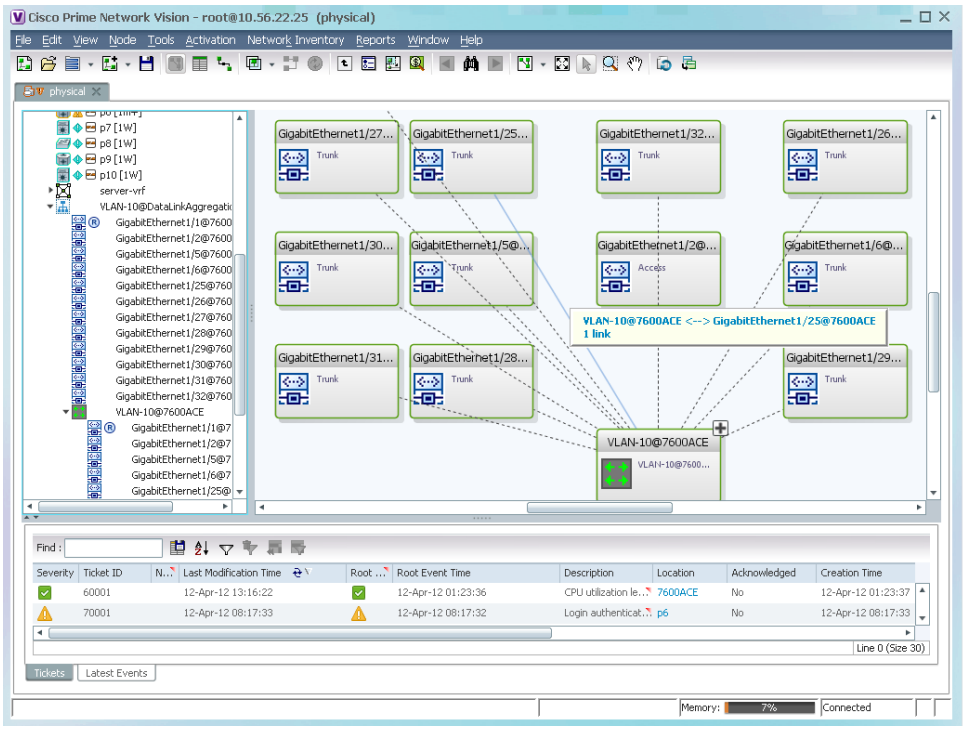


EFPs that are located directly inside a VLAN represent one of the following:

- Termination point EFPs—Ethernet ports that are at the edge of a Layer 2 domain flow, such as a VLAN, on which traffic enters a Layer 3 domain or a different Layer 2 domain, such as EoMPLS. These ports are found on such devices as the Cisco 7600 series, Cisco GSR, and Cisco ASR 9000 series devices.

  These EFPs are typically connected to a switching entity inside the VLAN by a VLAN link, as shown in Figure 12-22.

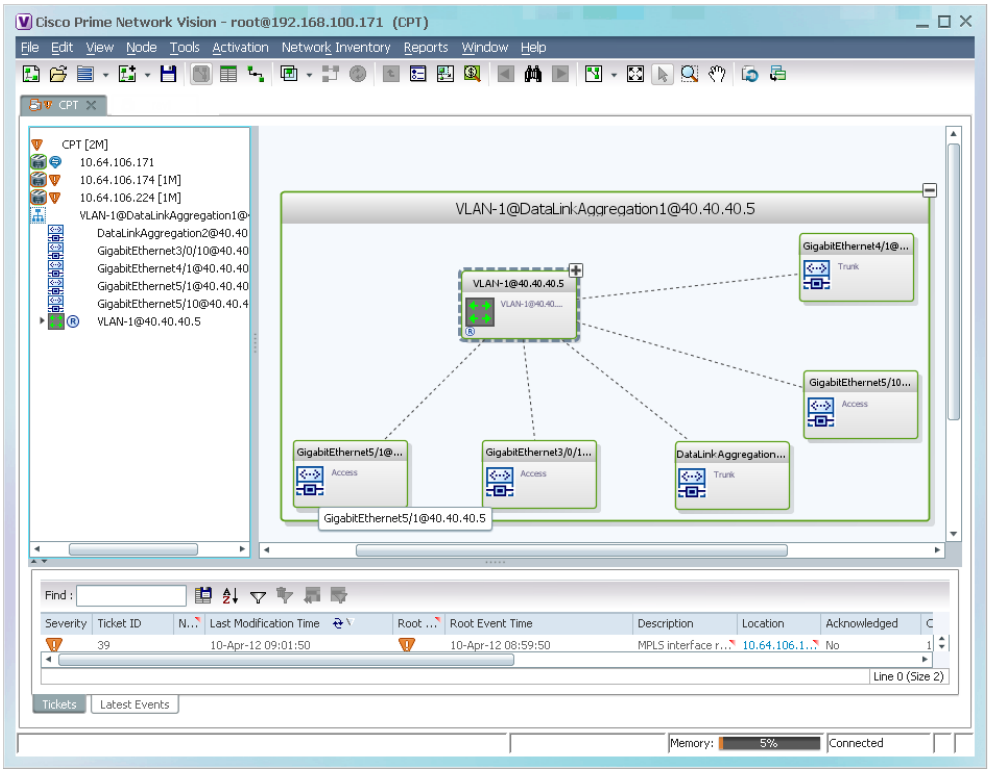
Figure 12-22 Termination Point EFP Inside a VLAN



- Edge EFPs—A subset of EFPs that exist inside a switching entity but that are not connected to other EFPs and that represent edge EFPs in the context of the VLAN.

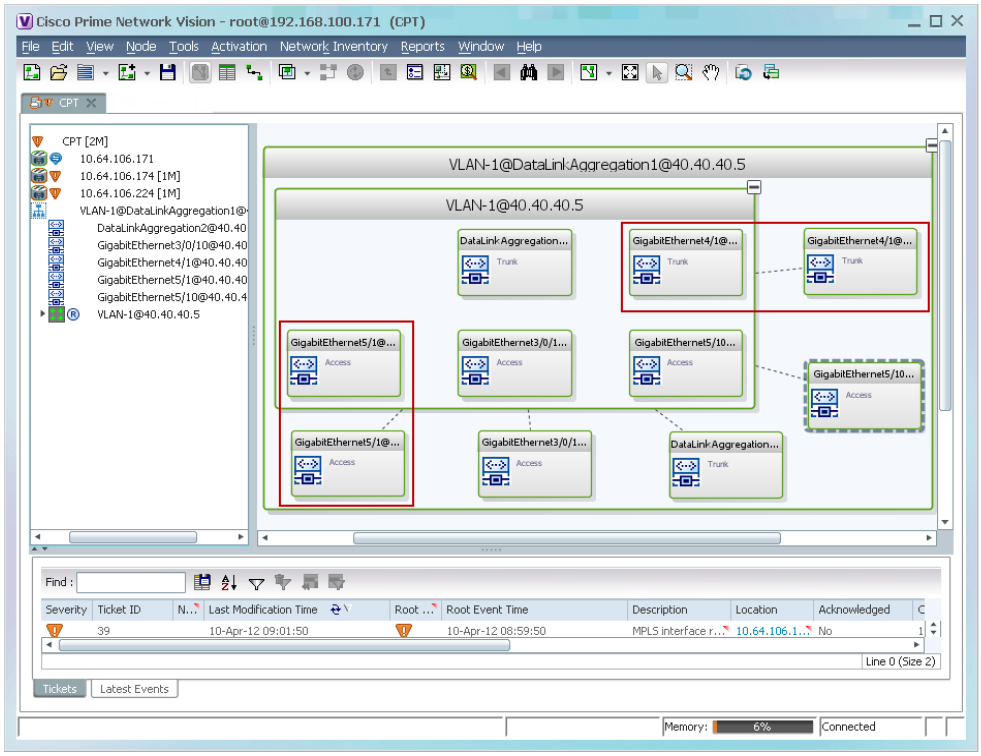
In Prime Network Vision, edge EFPs are displayed directly under the VLAN at the same level as their switching entities and are connected to their corresponding switching entities by a dotted link, as shown in Figure 12-23.

Figure 12-23 Edge EFP Inside a VLAN



An edge EFP can be displayed both inside and outside of its switching entity, as shown (highlighted with a red outline) in Figure 12-24:

Figure 12-24 Edge EFPs Displayed Inside and Outside of Switching Entities



You can delete EFPs and switching entities that have a reconciliation icon by right-clicking them and choosing **Delete**. After all switching entities and EFPs are deleted from a network VLAN, the empty network VLAN is automatically deleted from Prime Network Vision after a few minutes.

Switching Entities Containing Termination Points

For some devices, such as Cisco 7600 series, Cisco GSR, and Cisco ASR 9000 series devices, the related switching entities can contain Ethernet flow point elements that serve as termination points on different network VLANs. If a single map contains both the switching entities and the network VLANs, a link is displayed between them.

Adding and Removing VLANs from a Map

Adding VLANs to a Map

You can add VLANs to a map if the VLANs were previously discovered by Prime Network Vision and are not currently displayed in the map.

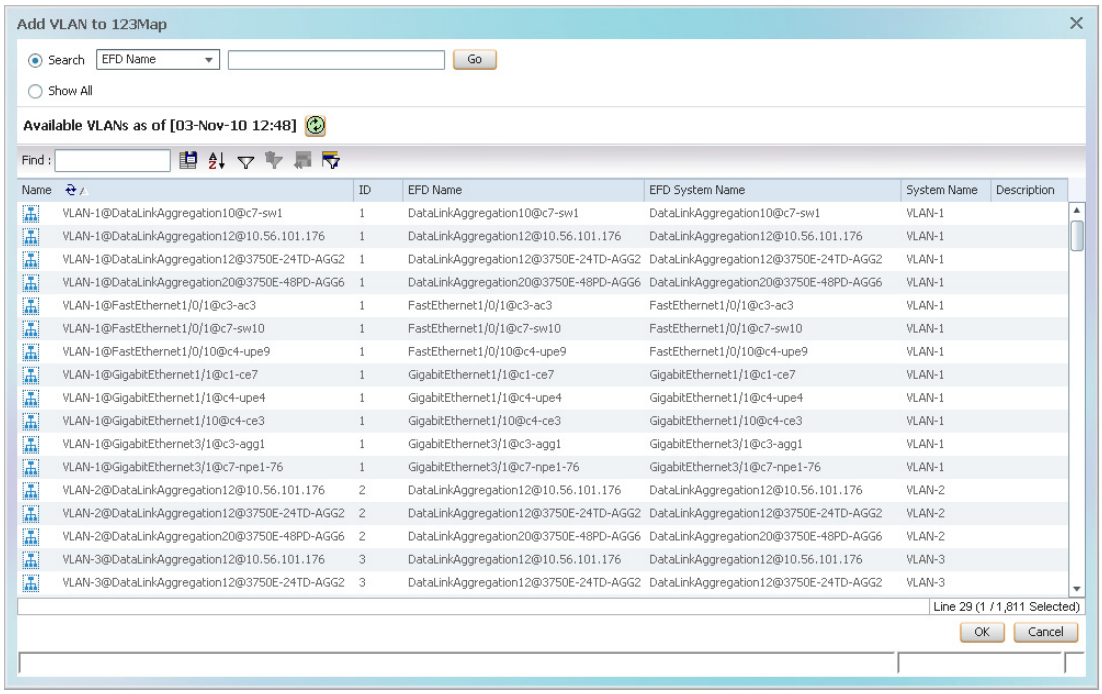
Note Adding VLANs affects other users if they are working with the same map.

To add VLANs to a map:

Step 1 In Prime Network Vision, display the map to which you want to add the VLANs.

Step 2 Choose **File > Add to Map > VLAN**. The Add VLAN to *map* dialog box is displayed as shown in Figure 12-25.

Figure 12-25 Add VLAN Dialog Box



Step 3 In the Add VLAN dialog box, do either of the following:

- Choose a search category, enter a search string, then click **Go** to narrow the VLAN display to a range of VLANs or a specific VLAN.

  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 VLANs that have “net” anywhere in their names. The string “net” can be at the beginning, the middle, or end of the name, such as Ethernet.

- Choose **Show All** to display all the VLANs.

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

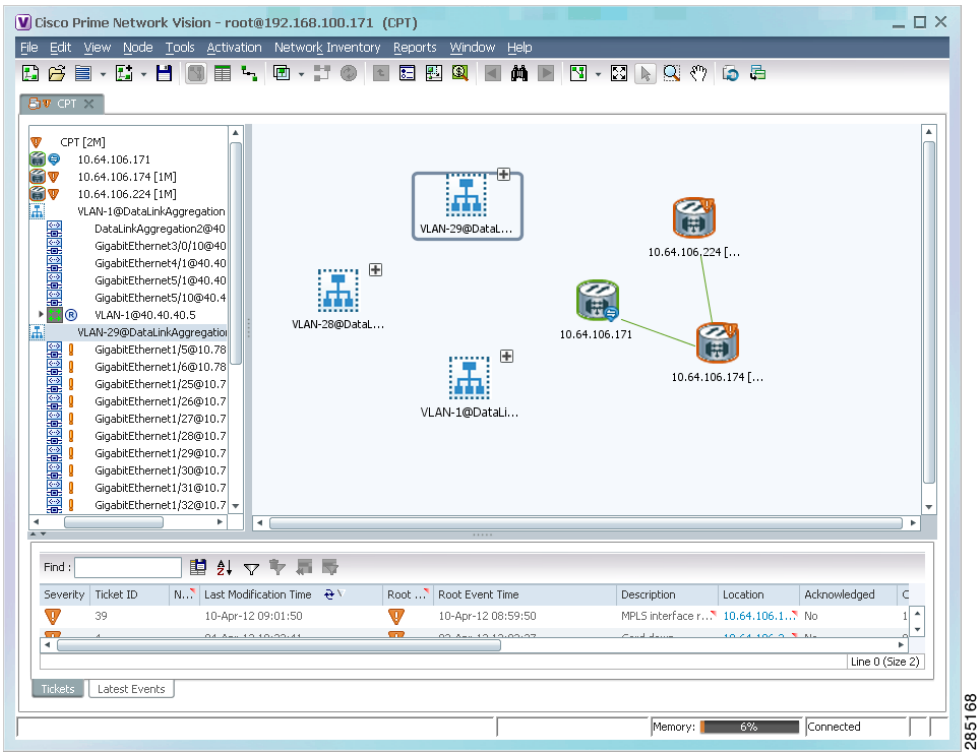
Tip Press **Shift** or **Ctrl** to choose multiple adjoining or nonconsecutive VLANs.

Step 5 Click **OK**.

The VLANs are displayed in the Prime Network Vision content pane as shown in Figure 12-26.

Any tickets that apply to the VLANs are displayed in the ticket pane.

Figure 12-26 VLANs in Map View



After you add a VLAN to a map, you can use Prime Network Vision to view its switching entities and Ethernet flow points. For more information, see:

- Viewing and Renaming Ethernet Flow Domains, page 12-42
- Viewing EFP Properties, page 12-33

You can view additional information about REP and STP in logical inventory, VLAN domain views, and VLAN overlays.

For REP, see:

- Viewing Resilient Ethernet Protocol Properties (REP), page 12-14
- Viewing REP Information in VLAN Domain Views and VLAN Overlays, page 12-63
- Viewing REP Properties for VLAN Service Links, page 12-64

For STP, see:

- Viewing Spanning Tree Protocol Properties, page 12-10
- Viewing STP Information in VLAN Domain Views and VLAN Overlays, page 12-66
- Viewing STP Properties for VLAN Service Links, page 12-67

Removing VLANs From a Map

You can remove one or more VLANs from the current map. This change does not affect other maps. Removing a VLAN from a map does not remove it from the Prime Network database. You can add the VLAN to the map at any time.

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

- Removing a VLAN affects other users who 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 VLAN.

To remove a VLAN, in the Prime Network Vision navigation pane or map view, right-click the VLAN and choose **Remove from Map**.

The VLAN is removed from the navigation pane and map view along with all VLAN elements such as connected CE devices. Remote VLANs (extranets) are not removed.

Viewing VLAN Mappings

VLAN mapping, or VLAN ID translation, is used to map customer VLANs to service provider VLANs. VLAN mapping is configured on the ports that are connected to the service provider network. VLAN mapping acts as a filter on these ports without affecting the internal operation of the switch or the customer VLANs.

If a customer wants to use a VLAN number in a reserved range, VLAN mapping can be used to overlap customer VLANs by encapsulating the customer traffic in IEEE 802.1Q tunnels.

To view VLAN mappings:

Step 1 In Prime Network Vision, double-click the device with VLAN mappings configured.

Step 2 In the inventory window, choose **Physical Inventory > Chassis >** *slot* **>** *port*.

Step 3 Click **VLAN Mappings** next to the Subinterfaces tab in the lower portion of the content pane.

The VLAN Mappings tab is displayed as shown in Figure 12-27.

Figure 12-27 VLAN Mappings Tab in Physical Inventory

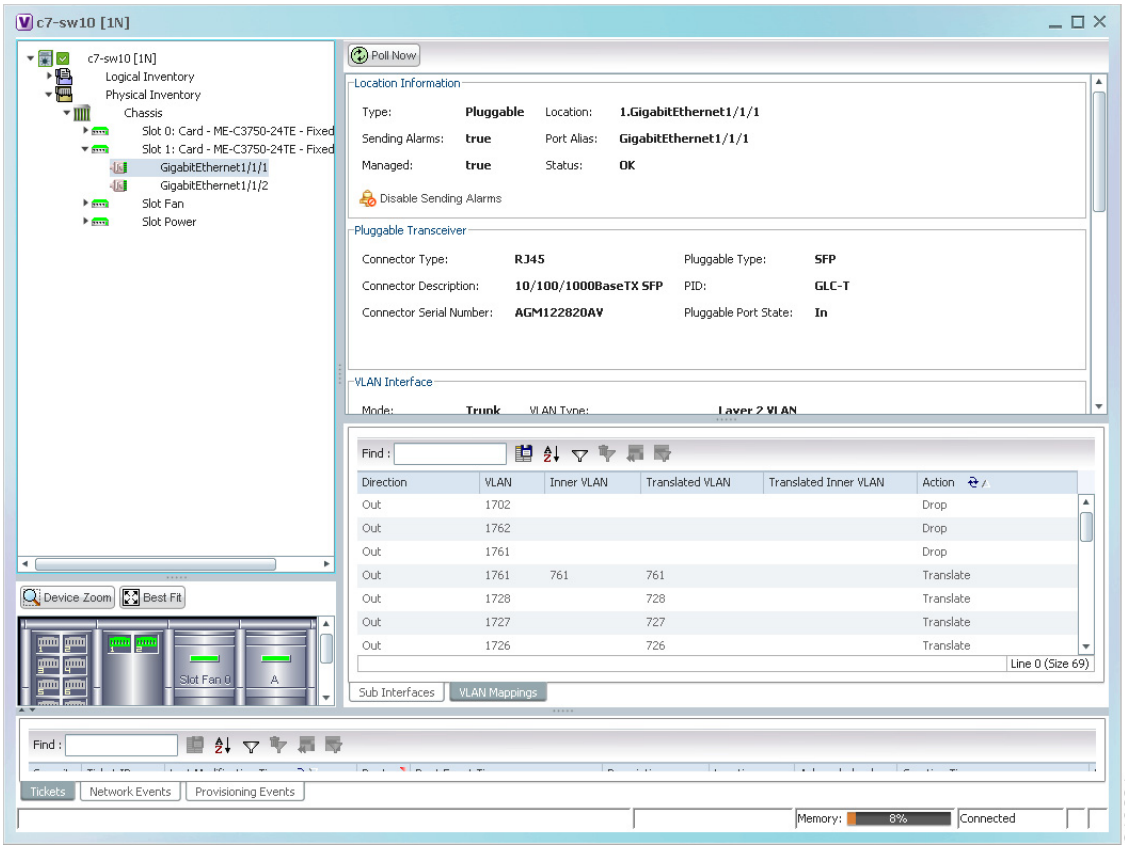


Table 12-25 describes the information that is displayed in the VLAN Mappings table.

Table 12-25 VLAN Mappings Table

Field	Description
Direction	Whether the VLAN mapping is defined in the incoming or outgoing direction: In or Out.
VLAN	Customer-side VLAN identifier.
Inner VLAN	Used for two-to-one mappings, the customer-side inner VLAN identifier.
Translated VLAN	Translated, or mapped, service-provider side VLAN identifier.
Translated Inner VLAN	Translated, or mapped, service-provider side inner VLAN identifier.
Action	Action taken if the VLAN traffic meets the specified mapping: Translate or Drop.

Working with Associated VLANs

Prime Network Vision discovers associations between network VLANs and displays the information in Prime Network Vision. Network VLAN associations are represented by VLAN service links, and can be any of the tag manipulation types described in Table 12-26.

Table 12-26 Types of Tag Manipulations in VLAN Associations

VLAN Tag Manipulation	Description	Example
One-to-one	One VLAN tag is translated to another VLAN tag.	VLAN tag 100 > VLAN tag 200
Two-to-two	• Two VLAN tags exist and both are translated to other tags. • Two VLAN tags exist, but tag manipulation is applied only to the outer tag.	• Inner tag 100, Outer tag 101 > Inner tag 200, Outer tag 201 • Inner tag 100, Outer tag 101 > Inner tag 100, Outer tag 201
One-to-two	One VLAN tag exists and an additional tag is inserted into the packet.	VLAN tag 100 > Inner tag 100, Outer tag 101

When working with VLANs, you can:

- Add an associated VLAN—See Adding an Associated VLAN, page 12-55.
- View properties for associated VLANs—See Viewing Associated Network VLAN Service Links and VLAN Mapping Properties, page 12-57.

Adding an Associated VLAN

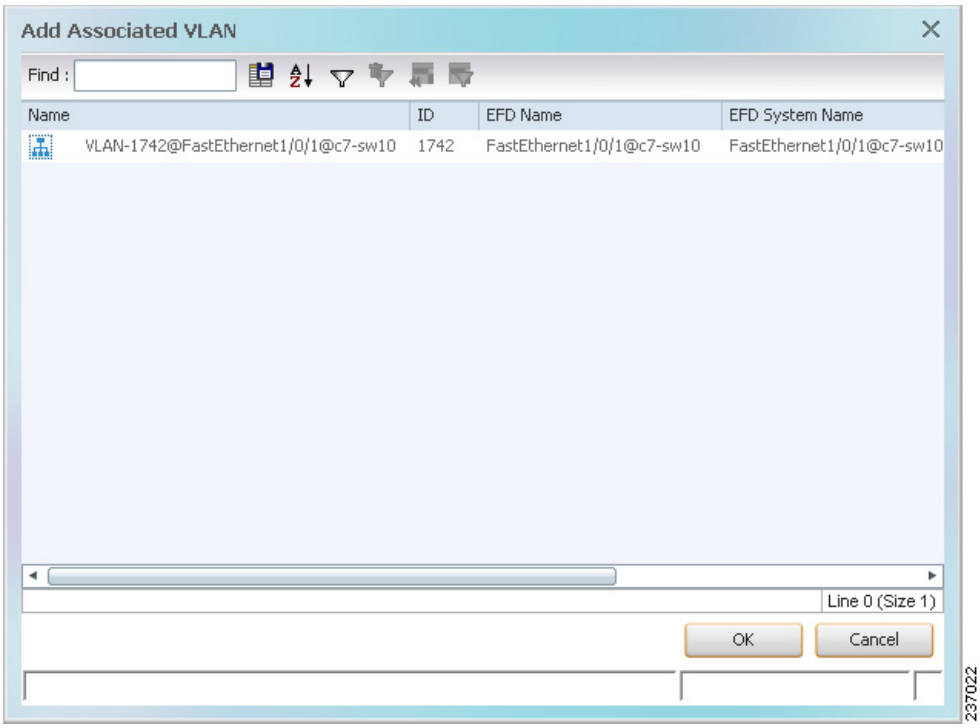
To add an associated VLAN to an existing VLAN in a map:

Step 1 In Prime Network Vision, select the required VLAN in the map view.

Step 2 Right-click the VLAN and choose **Add Associated VLAN**.

The Add Associated VLAN table is displayed as shown in Figure 12-28.

Figure 12-28 Add Associated VLAN Window



In this example, the selected network VLAN has one associated VLAN: VLAN-1742.

Table 12-27 describes the information displayed in the Add Associated VLAN table.

Table 12-27 Add Associated VLAN Table

Field	Description
Name	Name of the VLAN.
ID	VLAN identifier.
EFD Name	Name of the Ethernet flow domain.
EFD System Name	Name that Prime Network assigns to the EFD.
System Name	Name that Prime Network assigns to the VLAN.
Description	Brief description of the VLAN.

Step 3 Select the required VLAN in the Add Associated VLAN table, then click **OK**.

The associated network VLAN is added to the map in Prime Network Vision.

Viewing Associated Network VLAN Service Links and VLAN Mapping Properties

After you add an associated network VLAN, you can:

- View the associated network VLAN service links in Prime Network Vision in the thumbnail view.
- View VLAN mapping properties in the Link Properties window.

To view associated network VLAN service links and VLAN mapping properties:

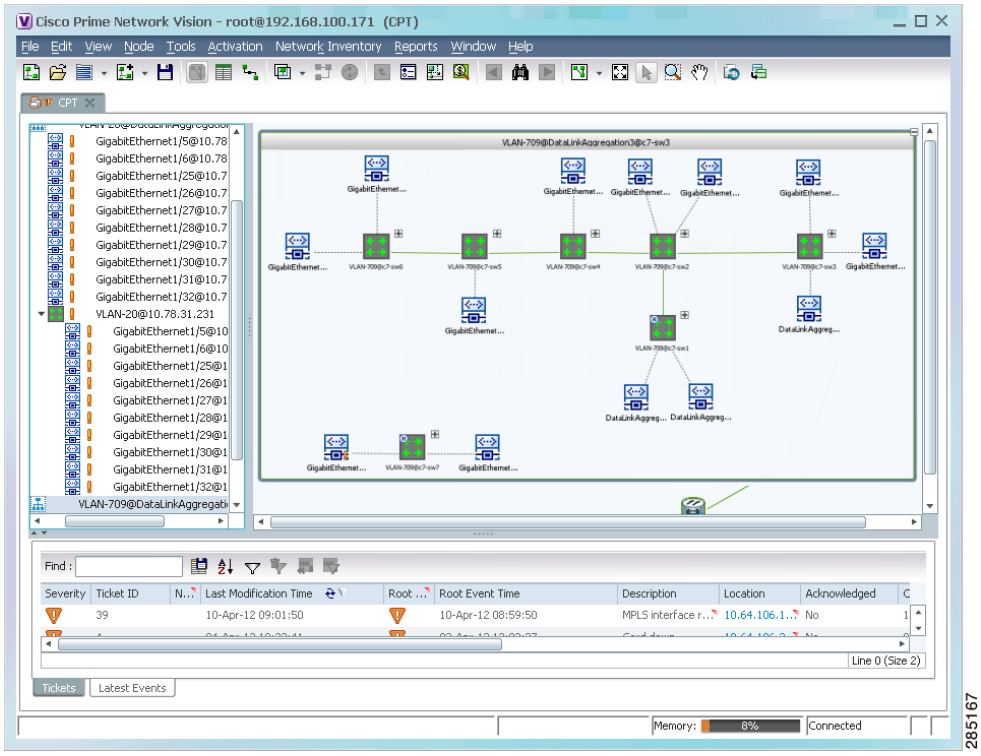
Step 1 Select the required network VLAN in the map view.

Step 2 Right-click the VLAN, then choose **Show Thumbnail**.

Figure 12-29 shows an example of a network VLAN in a thumbnail.

The VLAN service links are displayed as lines between the associated network VLANs. The links represent the connections between the Ethernet flow points that are part of each network VLAN.

Figure 12-29 VLAN Service Links Between Associated Network VLANs

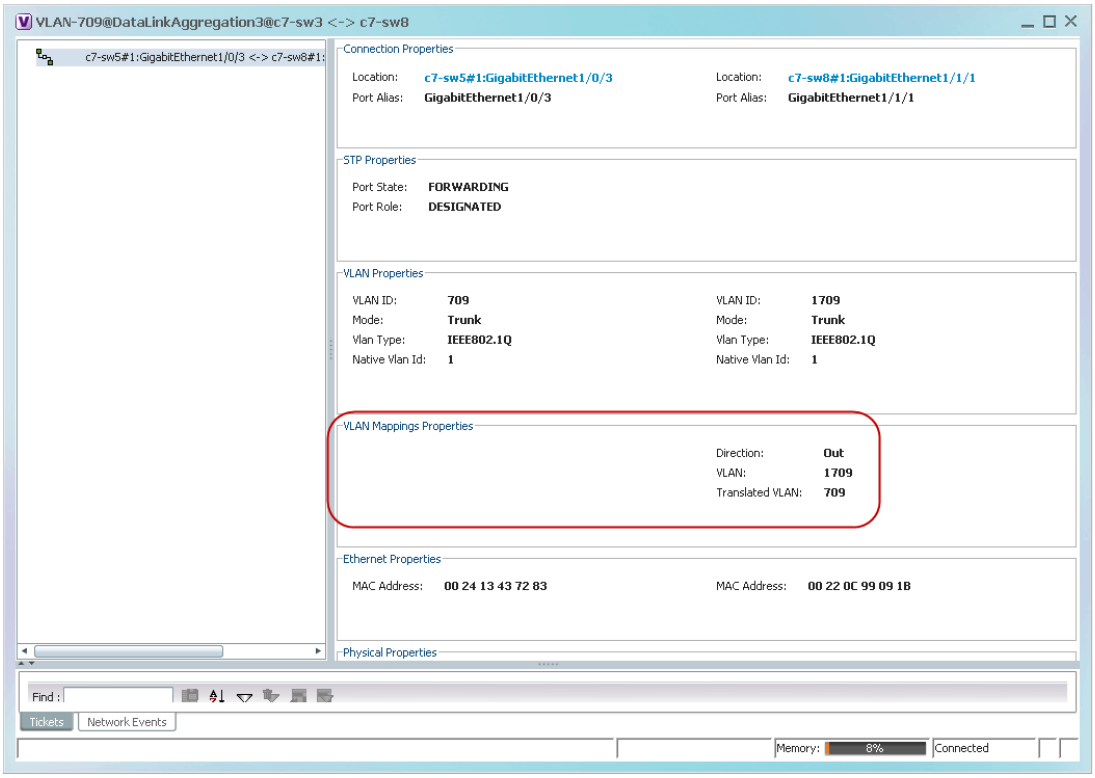


Step 3 To view additional information, right-click a link, and choose **Properties**.

The Link Properties window is displayed as shown in Figure 12-30.

If VLAN tag manipulation is configured on the link, the VLAN Mapping Properties area in the Link Properties window displays the relevant information. For example, in Figure 12-30, the VLAN Mapping Properties area shows that a one-to-one VLAN mapping for VLAN tag 1709 to VLAN tag 709 is configured on GigabitEthernet1/1/1 on c7-sw8 on the egress direction.

Figure 12-30 VLAN Mapping Properties in Link Properties Window



For additional information about viewing network VLAN service link properties, see:

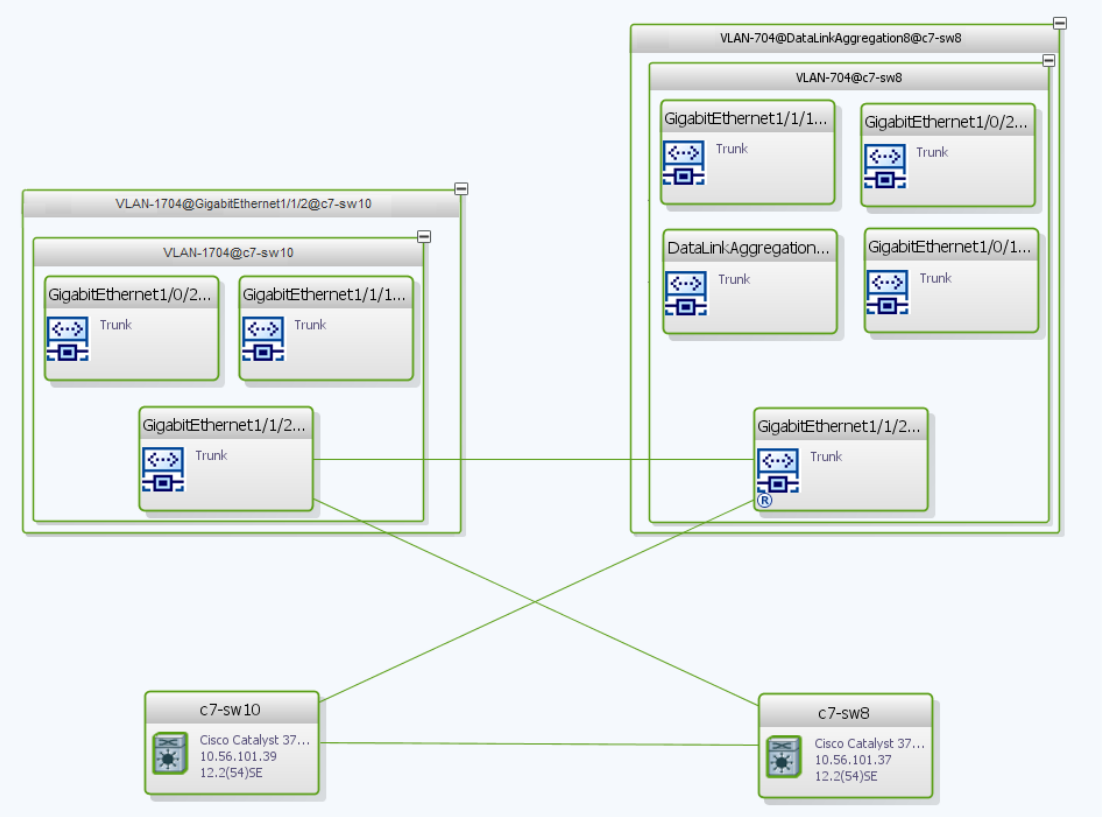
- Viewing REP Properties for VLAN Service Links, page 12-64
- Viewing STP Properties for VLAN Service Links, page 12-67

Viewing VLAN Links Between VLAN Elements and Devices

If a Prime Network Vision map contains a VLAN and the network element on which the VLAN is configured, along with EFPs, switching entities, or network VLANs, you might see what appear to be multiple associations between the logical and physical entities. Actually, however, you are seeing other views of the original VLAN link.

For example, assume that you have the following situation, as shown in Figure 12-31 and described in the following paragraphs.

Figure 12-31 VLAN Elements and Devices in Prime Network Vision



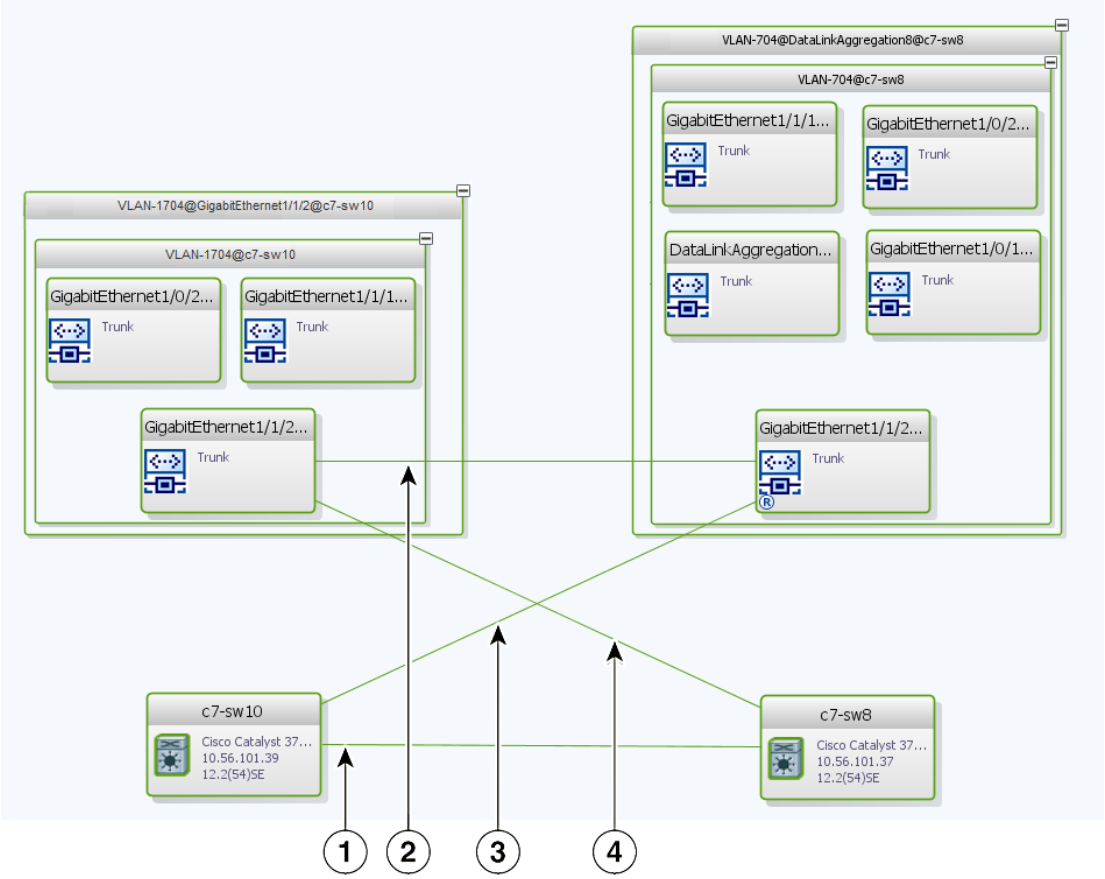
The elements are configured as follows:

- Port GigabitEthernet1/1/2 on element c7-sw10 is connected to port GigabitEthernet1/1/2 on element c7-sw8 by an Ethernet topology link.
- Port GigabitEthernet1/1/2 on element c7-sw10 is a trunk port associated with VLAN-1704 which is configured on element c7-sw10.
- Port GigabitEthernet1/1/2 on element c7-sw8 is a trunk port associated with VLAN-704 which is configured on element c7-sw8.
- Port GigabitEthernet1/1/2 on element c7-sw8 has a VLAN mapping to tunnel VLAN-1704 (C-VLAN) in VLAN-704 (SP-VLAN).

In this example, VLAN discovery identified two network VLANs: VLAN-1704 and VLAN-704. Each of these network VLANs contains a switching entity and an EFP that represent the connected ports, GigabitEthernet1/1/2@c7-sw10 and GigabitEthernet1/1/2@c7-sw8, respectively.

The four links in the map are identified in Figure 12-32 and described in the following table.

Figure 12-32 Links Between VLAN Elements and Devices



1	The Ethernet topological link between port GigabitEthernet1/1/2 on VNE c7-sw10 and GigabitEthernet1/1/2 on VNE c7-sw8.
2	The VLAN link between GigabitEthernet1/1/2@c7-sw10 EFP and GigabitEthernet1/1/2@c7-sw8 EFP.
3	Another view of the VLAN link (link 2), shown as a link between GigabitEthernet1/1/2@c7-sw10 EFP and GigabitEthernet1/1/2@c7-sw8 EFP.
4	Another view of the VLAN link (link 2), shown as a link between GigabitEthernet1/1/2@c7-sw10 EFP and GigabitEthernet1/1/2@c7-sw8 EFP.

The key point is that a link between a VNE and EFP, switching entity, or network VLAN **does not** represent an association between the VNE and the logical element. Such a link is simply another view of the VLAN link.

If the thumbnail view is closed, instead of a link between the VNE and EFP, you will see a link between the VNE and the switching entity or network VLAN.

Displaying VLANs By Applying VLAN Overlays to a Map45

You can create an overlay of a specific VLAN on top of the physical network elements displayed in a map view. The overlay highlights the network elements and links that the selected VLAN and its associated VLANs traverse. Network elements and links that are not part of the VLAN are dimmed in the map view.

The VLAN overlay is a snapshot of the network to help you visualize the network elements and links connected to a VLAN. The overlay displays STP and REP link and port information.

If you select a network VLAN that is associated with other VLANs, the associated VLANs are included in the overlay.

The VLAN 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 site interconnections use the same link.

Adding a VLAN Overlay

To add a VLAN overlay:

Step 1 Display the network map for which you want to create an overlay in Prime Network Vision.

Step 2 In the toolbar, choose **Choose Overlay Type > VLAN**.

Step 3 In the Select VLAN Overlay dialog box, do either of the following:

- Choose a search category, enter a search string, then click **Go** to narrow the selection to a set of overlays or a specific overlay.

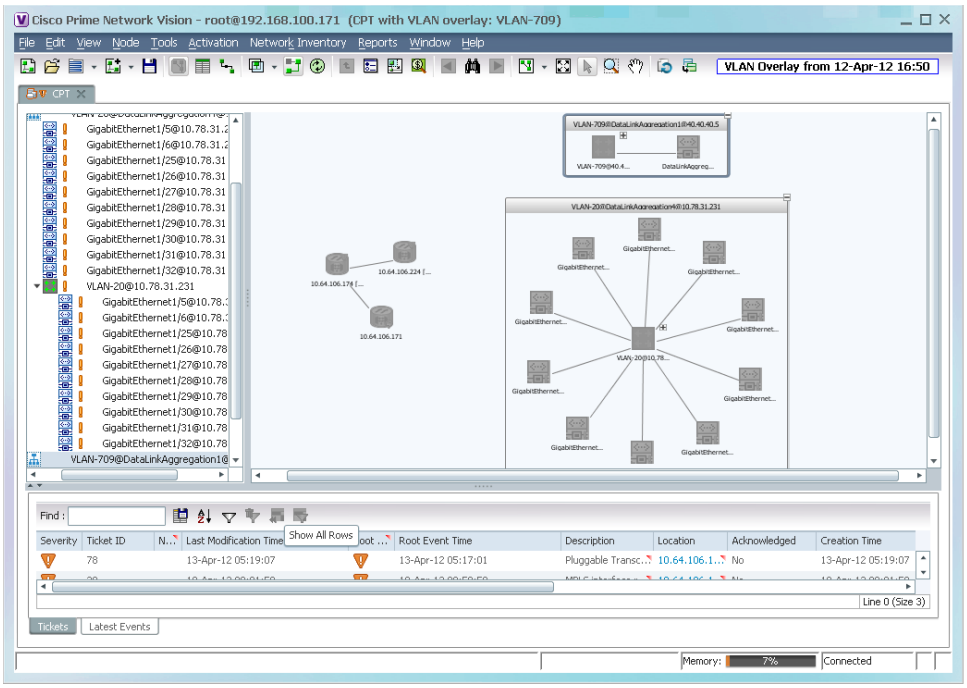
  The search condition is “contains.” Search strings are case-insensitive. For example, if you choose the Name category and enter “net,” Prime Network Vision displays overlays that have “net” in their names. The string “net” can be at the beginning, middle, or end of the name, such as Ethernet.

- Choose **Show All** to view all overlays.

Step 4 Select an overlay, then click **OK**.

The network elements and physical links used by the selected VLAN overlay are highlighted in the network map. All other network elements and links are dimmed. The VLAN name is displayed in the title of the window. See Figure 12-33.

Figure 12-33 VLAN Overlay Example



Note The overlay is a snapshot taken at a specific point in time. As a result, the information in the overlay might become stale. To update the overlay, click **Refresh the Last Selected Overlay** in the toolbar.

The VLAN overlay service also supports multi-chassis devices. If a network element in the overlay is dimmed, then all the hosts of the network element along with the Inter Rack Links (IRL) and the Inter Chassis Links (ICL) used for transportation will also be dimmed. Apart from these, the chassis that holds the configured port will also be dimmed.

Displaying or Hiding VLAN Overlays

After you create a VLAN overlay, you can hide it by clicking **Hide Overlay** in the toolbar. All previously dimmed network elements and links are displayed. To display the overlay, click **Show Overlay**.

Note The Overlay icon toggles between Show Overlay and Hide Overlay. When selected, the VLAN overlay is displayed and the Hide Overlay tool is active. When deselected, the VLAN overlay is hidden and the Show Overlay tool is active.

Removing a VLAN Overlay

To remove a VLAN overlay from a map, choose **Choose Overlay Type > None** in the toolbar. The overlay is removed from the map, and the Show Overlay/Hide Overlay icon is dimmed.

Viewing VLAN Service Link Properties

See the following topics for information on viewing VLAN service link properties:

- Viewing REP Properties for VLAN Service Links, page 12-64
- Viewing STP Properties for VLAN Service Links, page 12-67
- Viewing Associated Network VLAN Service Links and VLAN Mapping Properties, page 12-57

Viewing REP Information in VLAN Domain Views and VLAN Overlays

You can view REP segment and port information in Prime Network Vision in the map view. The icons displayed depend on whether you view the REP information in the VLAN domain view or in a VLAN overlay. Table 12-28 describes the icons and badges used to represent REP segment and port information.

Table 12-28 REP Icons and Badges in VLAN Domain Views and Overlays

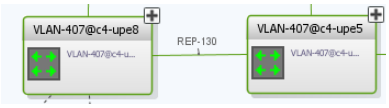
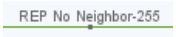
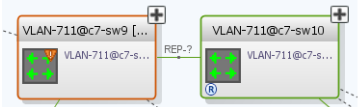
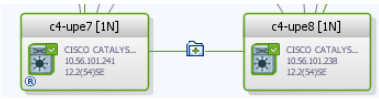
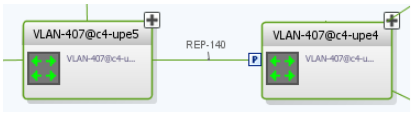
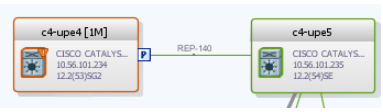
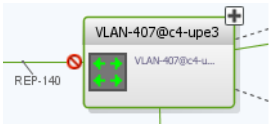
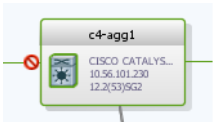
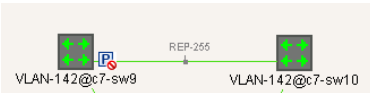
Item	Description	VLAN Domain View	VLAN Overlay
	REP identifier—Uses the format REP-*id* where *id* represents the REP segment identifier.	 The REP identifier is displayed in the domain view if the visual link represents only one link. f the visual link represents more than one link, no REP identifier is displayed.	The REP identifier is displayed in a VLAN overlay view if all the links represented by the visual link are from the same source to the same destination.
	REP No Neighbor *segment*— Indicates that the specified segment has no neighbor.		
	REP identifier for incorrect configuration—Indicates that the two sides of the link are configured differently or incorrectly.		

Table 12-28 REP Icons and Badges in VLAN Domain Views and Overlays (continued)

Item	Description	VLAN Domain View	VLAN Overlay
	Multiple links with badges icon—Indicates that one or more link is represented by the visual link and at least one of the links contains a badge.	The multiple links icon is displayed in the domain view if more than one link is represented by the visual link and at least one of the links contains a badge.	 The multiple links icon is displayed in a VLAN overlay view if either of the following is true: • More than one link is represented by the visual link and the links have different sources or destinations. • A badge or REP identifier exists on a sublink.
	REP primary badge—Indicates a REP primary port.		
	Blocking badge—Indicates a REP alternate port.		
	Primary and blocking badge—Indicates a REP primary port that is also blocking.		

Viewing REP Properties for VLAN Service Links

To view REP properties for a VLAN service link, open the Link Properties window in either of the following ways:

- Double-click the VLAN service link.
- Right-click the VLAN service link, and choose **Properties**.

Figure 12-34 shows an example of the Link Properties window with REP information.

Figure 12-34 VLAN Service Link Properties Window with REP Information

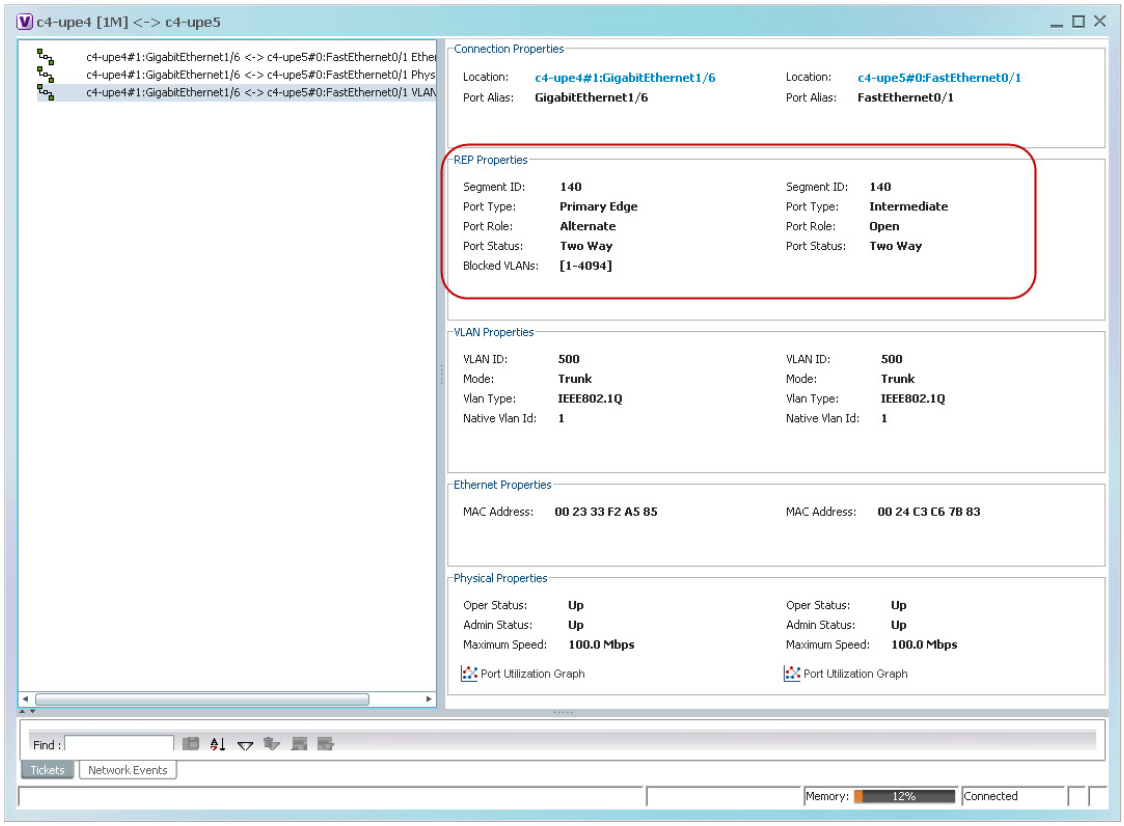


Table 12-29 describes the information that is displayed for REP for each end of the link.

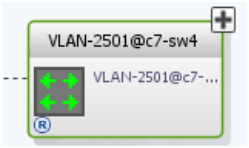
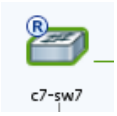
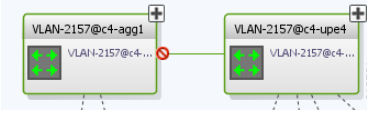
Table 12-29 REP Properties in VLAN Service Link Properties Window

Field	Description
Segment ID	REP segment identifier.
Port Type	Port type: Primary Edge, Secondary Edge, or Intermediate.
Port Role	Role or state of the REP port depending on its link status and whether it is forwarding or blocking traffic: Failed, Alternate, or Open.
Port Status	Operational link state of the REP port: None, Init Down, No Neighbor, One Way, Two Way, Flapping, Wait, or Unknown.

Viewing STP Information in VLAN Domain Views and VLAN Overlays

You can view STP segment and port information in Prime Network Vision in the map view. The icons displayed depend on whether you view the STP information in the VLAN domain view or in a VLAN overlay. Table 12-30 describes the icons and badges used to represent STP link and port information.

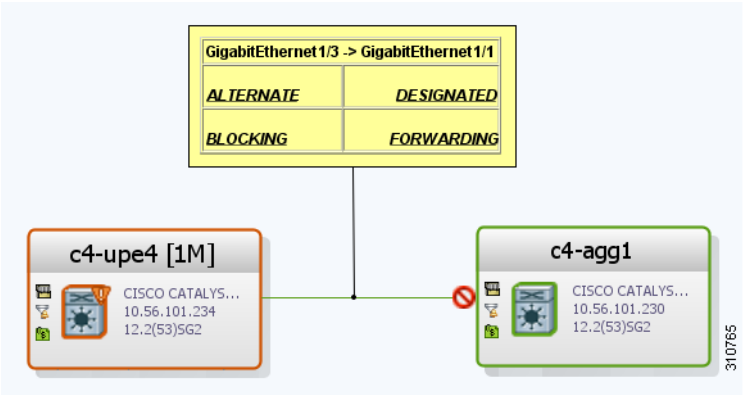
Table 12-30 STP Information in VLAN Domain Views and Overlays

Item	Description	VLAN Domain View	VLAN Overlay
	The STP root bridge, or root of the STP tree, is indicated by an uppercase R.		
	An STP root port is the port at the root of the STP tree. Each switching entity in the network VLAN should have a port designated as the root port. The STP root port is indicated by an uppercase R on the Ethernet flow point that is designated the root port.		
	STP blocks some VLAN ports to ensure a loop-free topology. The blocked port is marked with a red deny badge on the side on which traffic is denied.		

To view additional STP information in a VLAN overlay, right-click an STP link and choose **Show Callouts**. The following STP port information is displayed as shown in Figure 12-35:

- Port name
- Port role
- Port state

Figure 12-35 STP Link Information in a VLAN Overlay



Viewing STP Properties for VLAN Service Links

To view STP properties for a VLAN service link, open the Link Properties window in one of the following ways:

- Double-click the VLAN service link.
- Right-click the VLAN service link, and choose **Properties**.

Figure 12-36 shows an example of the Link Properties window with STP information.

Figure 12-36 STP Properties in VLAN Service Link Properties Window

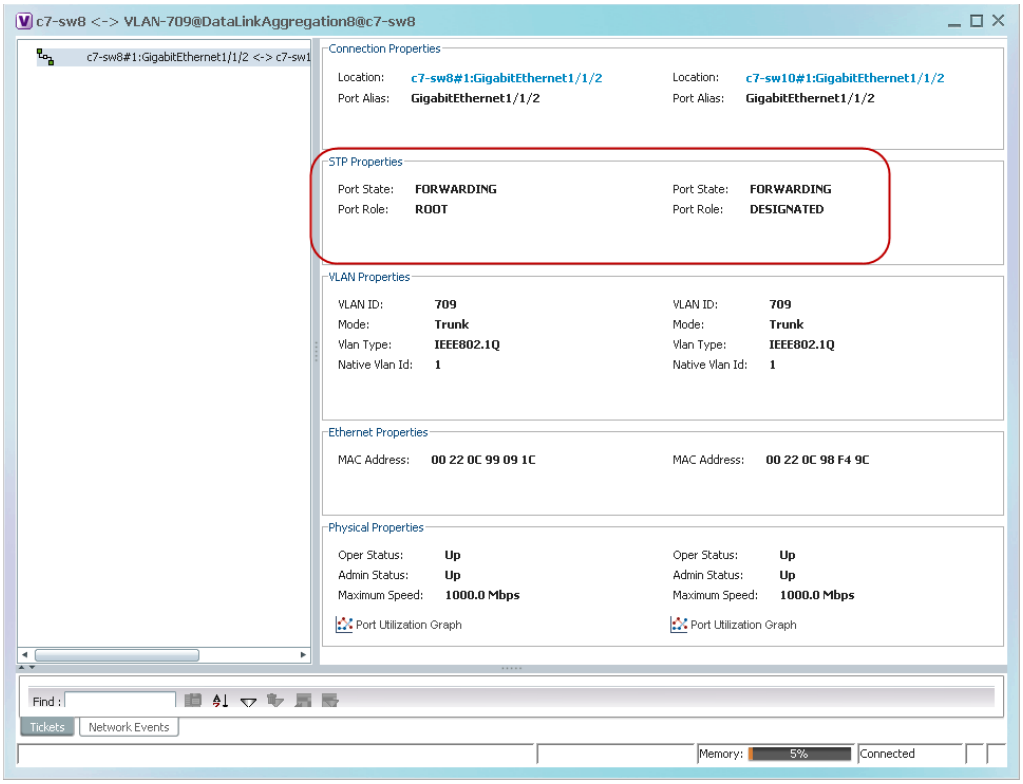


Table 12-31 describes the information that is displayed for STP for the VLAN service link.

Table 12-31 STP Properties in VLAN Service Link Properties Window

Field	Description
Port State	STP port state: Disabled, Blocking, Listening, Learning, or Forwarding,
Port Role	STP port role: Unknown, Backup, Alternative, Designated, Root, or Boundary.

Viewing VLAN Trunk Group Properties

VTP is a Layer 2 multicast messaging protocol that manages the addition, deletion, and renaming of VLANs on a switched network-wide basis.

Prime Network Vision displays VTP information in the logical inventory. VTP information is shown only for Cisco devices that support VTP, and support is provided only for VTP Version 1 and 2. Support for Version 3 is limited to the additional attributes that are supported by the version, such as primary and secondary server. No support is provided for the display of VTP information at the port (trunk) level.

Prime Network Vision shows all VTP modes: Server, Client, Transparent, and Off. For each mode, Prime Network Vision displays the relevant mode information such as VTP domain, VTP mode, VTP version, VLAN trunks, and the trunk encapsulation. Prime Network Vision also displays VTP domain information in a view that includes a list of all switches that are related to these domains, their roles (server, client, and so on), and their VTP properties.

To view VTP properties:

Step 1 In Prime Network Vision, choose **Network Inventory > VTP Domains**.

Step 2 Double-click the VTP domain you want to view.

The VTP Domain Properties window is displayed as shown in Figure 12-37.

Figure 12-37 VTP Domain Properties Window in Logical Inventory

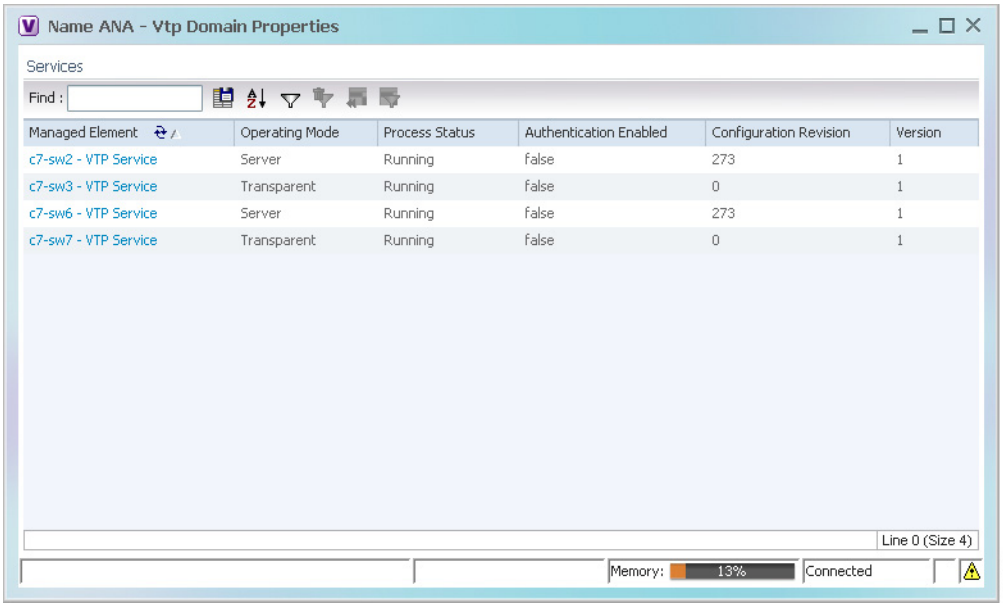


Table 12-32 describes the information that is displayed in the VTP Domain Properties window.

Table 12-32 VTP Domain Properties Window

Field	Description
Managed Element	Managed element name, hyperlinked to VTP in logical inventory.
Operating Mode	VTP operating mode: • Server—Allows VLAN creation, modification, and deletion, and specification of other configuration parameters for the entire VTP domain. Server is the default mode. • Client—Same behavior as VTP server, except VLANs cannot be created, changed, or deleted. • Transparent—The device does not participate in the VTP. The device does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, the device forwards received VTP advertisements out of their trunk ports in VTP Version 2. • Off—The device does not participate in VTP and does not forward VTP advertisements.
Process Status	Status of the VTP process: Running or Disabled.
Authentication Enabled	Whether or not VTP authentication is enabled: True or False. Authentication ensures authentication and integrity of switch-to-switch VTP messages. VTP Version 3 introduces an additional mechanism to authenticate the primary VTP server as the only device allowed to change the VLAN configuration on a network-wide basis.
Configuration Revision	32-bit number that indicates the level of revision for a VTP packet. Each VTP device tracks the VTP configuration revision number that is assigned to it. Most VTP packets contain the VTP configuration revision number of the sender.
Version	VTP version: 1, 2, or 3.

Step 3 To view the VTP properties at the device, double-click the VTP domain.

Table 12-33 describes the VTP information that is displayed in the inventory window content pane.

Table 12-33 VTP Properties in Inventory

Field	Description
Operating Mode	VTP operating mode: Server, Client, Transparent, or Off.
Domain Name	VTP domain name.
Version	VTP version: 1, 2, or 3.
Pruning	Whether or not VTP pruning is enabled: True or False. VTP pruning increases available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to access the appropriate network devices.

Table 12-33 VTP Properties in Inventory (continued)

Field	Description
Configuration Revision	32-bit number that indicates the level of revision for a VTP packet.
Authentication	Whether or not VTP authentication is enabled: True or False.

Step 4 When finished, press **Ctrl + F4** to close each VTP properties window.

Viewing VLAN Bridge Properties

You can view VLAN bridges provisioned on a device by displaying the device in the Prime Network Vision inventory window and choosing Bridges in logical inventory.

To view VLAN bridge properties:

Step 1 In Prime Network Vision, double-click the device containing the VLAN bridges you want to view.

Step 2 In the inventory window, choose **Logical Inventory > Bridges >** *bridge*.

VLAN bridge properties are displayed as shown in Figure 12-38.

Figure 12-38 VLAN Bridge Properties in Logical Inventory

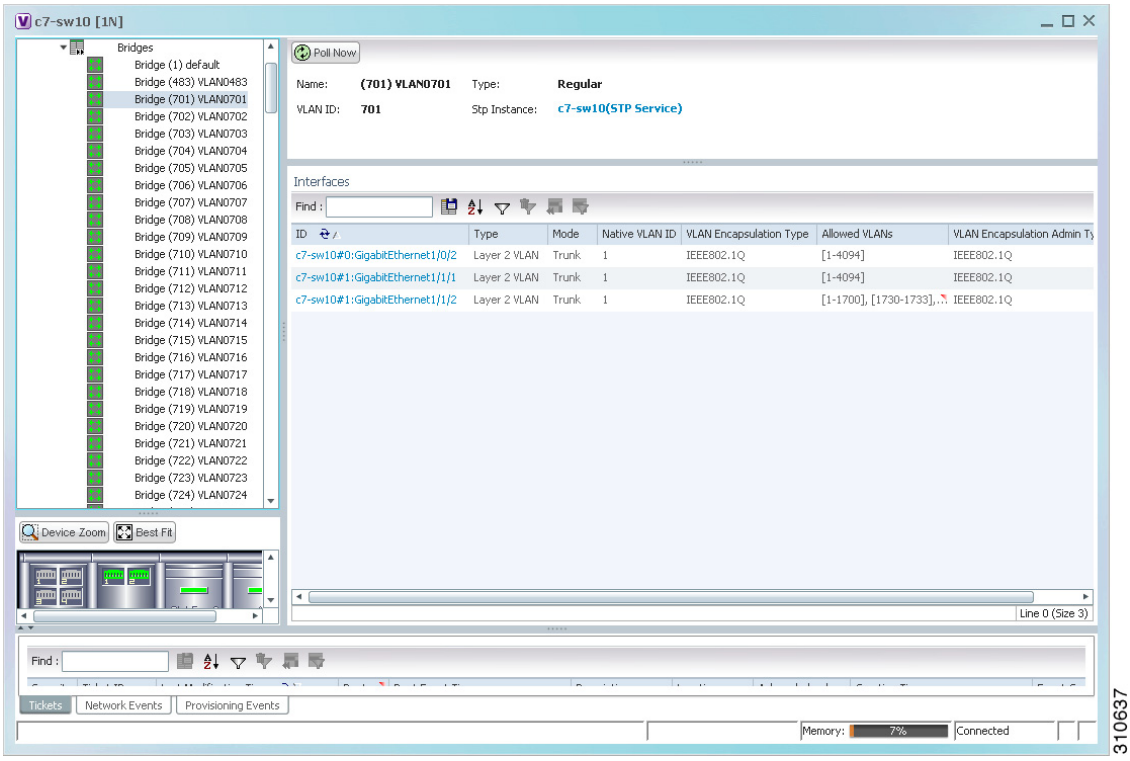


Table 12-34 describes the information that is displayed. Depending on the bridge configuration, any of the tabs might be displayed for the selected bridge.

Table 12-34 VLAN Bridge Properties

Field	Description
Name	VLAN bridge name.
Type	VLAN bridge type.
MAC Address	VLAN bridge MAC address.
VLAN ID	VLAN bridge VLAN identifier.
STP Instance	STP instance information, hyperlinked to the STP entry in logical inventory.
Bridge Table Tab	
MAC Address	Bridge MAC address.
Port	Port associated with the bridge, hyperlinked to the interface in physical inventory.
Interfaces Tab	
ID	VLAN interface identifier, hyperlinked to the interface in physical inventory.
Type	VLAN interface type, such as Layer 2 VLAN.
Mode	VLAN interface configuration mode: • Unknown—The interface is not VLAN aware. • Access—Puts the interface into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The interface becomes nontrunking. • Dynamic Auto—The interface can convert the link to a trunk link. The interface becomes a trunk if the neighbor interface is set to Trunk or Dynamic Desirable mode. • Dynamic Desirable—The interface actively attempts to convert the link to a trunk link. The interface becomes a trunk if the neighboring interface is set to Trunk, Dynamic Desirable, or Dynamic Auto mode. Dynamic Desirable is the default mode for all Ethernet interfaces. • Trunk—Puts the interface into permanent trunking mode and negotiates to convert the link into a trunk link. The interface becomes a trunk interface even if the neighbor interface is not a trunk interface. • Dot1Q Tunnel—Configures the interface as a tunnel (nontrunking) port to be connected in an asymmetric link with an 802.1Q trunk port. 802.1Q tunneling is used to maintain customer VLAN integrity across a service provider network.
Native VLAN ID	VLAN Identifier (VID) associated with this VLAN. The range of the VLAN ID is 1 to 4067.
VLAN Encapsulation Type	Type of encapsulation configured on the VLAN, such as IEEE 802.1Q.

Table 12-34 VLAN Bridge Properties (continued)

Field	Description
Allowed VLANs	List of the VLANs allowed on this VLAN interface.
VLAN Encapsulation Admin Type	VLAN administration encapsulation type, such as IEEE 802.1Q.
EFPs Tab	
EFP ID	EFP identifier.
Operational State	EFP operational state.
VLAN	VLAN identifier.
Inner VLAN	CE-VLAN identifier.
Translated VLAN	Translated VLAN identifier.
Translated Inner VLAN	Translated CE-VLAN identifier.
Binding Port	Hyperlinked entry to the port in physical inventory.
Description	Brief description of the EFP.
Pseudowires Tab	
ID	Pseudowire identifier, hyperlinked to the VLAN entry in Bridges in logical inventory.
Peer	Identifier of the pseudowire peer, hyperlinked to the entry in the Pseudowire Tunnel Edges table in logical inventory.
Tunnel ID	Tunnel identifier.
Tunnel Status	Status of the tunnel: Up or Down.
Peer Router IP	IP address of the peer router for this pseudowire.
Sub Interfaces Tab	
BER	VLAN bit error rate.
Interface Name	Interface on which the VLAN is configured.
VLAN Type	Type of VLAN, such as Bridge or IEEE 802.1Q.
Operational State	Subinterface operational state.
VLAN ID	VLAN identifier.
Inner VLAN	CE-VLAN identifier.

Step 3 When finished, press **Ctrl + F4** to close each VLAN Bridge properties window.

Using Commands to Work With VLANs

The following commands can be launched from the physical inventory by right-clicking an Ethernet slot and choosing **Commands > Configuration**. Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 4.0 Supported Cisco VNEs*.

These commands are applicable only for Cisco ASR 5000 series network elements.

Note You might be prompted to enter your device access credentials while executing a command. Once you have entered them, these credentials will be used for every subsequent execution of a command in the same GUI client session. If you want to change the credentials, click **Edit Credentials**. The Edit Credentials button will not be available for SNMP commands or if the command is scheduled for a later time.

Table 12-35 VLAN Commands

Command	Inputs Required and Notes
Create VLAN	VLAN ID, VLAN Context Name, Bind Interface Name, Status
Modify VLAN	VLAN ID, Delete Bind Interface, Context Name, Bind Interface Name, Status
Delete VLAN	VLAN ID

Understanding Unassociated Bridges

Some switching entities might not belong to a flow domain, such as a network VLAN, a VPLS instance, or a network pseudowire. These switching entities are referred to as *unassociated bridges*.

In addition, a switching entity that belongs to a network VLAN is considered an unassociated bridge if it meets both of the following criteria:

- The network VLAN contains a null Ethernet flow domain (EFD).
- The switching entity contains no switch ports.

Unassociated bridge switching entities can hold Ethernet flow points that serve as termination points on different network VLANs. If these switching entities are added to a map with the relevant VLANs, the links are displayed in the Prime Network Vision map.

Adding Unassociated Bridges

Prime Network Vision enables you to add unassociated bridges to maps and to view their properties.

To add an unassociated bridge to a map:

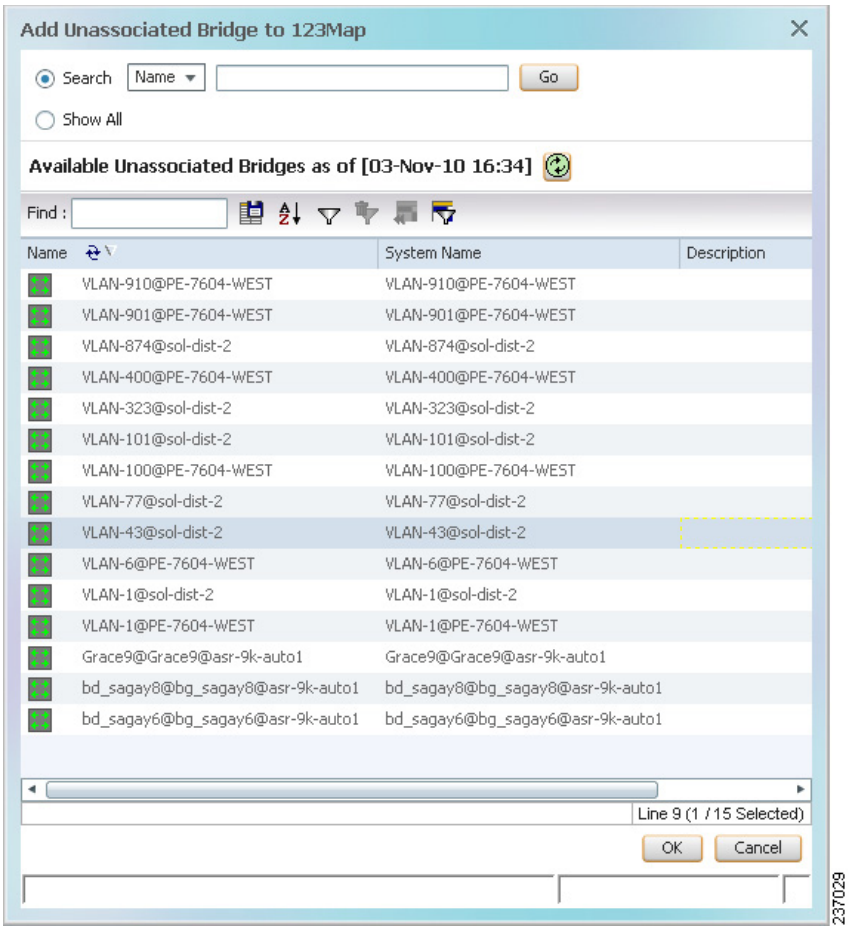
Step 1 In Prime Network Vision, select the required map or domain.

Step 2 Open the Add Unassociated Bridge dialog box in one of the following ways:

- Choose **File Add to Map > Unassociated Bridge**.
- In the toolbar, click **Add to Map** and choose **Unassociated Bridge**.

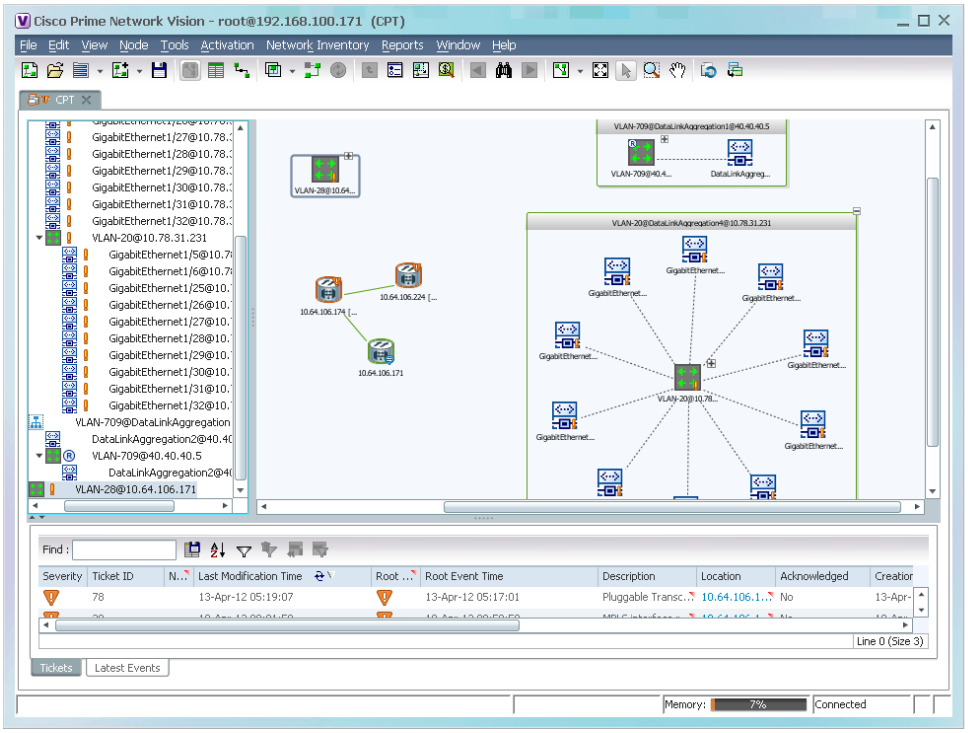
Figure 12-39 shows an example of the Add Unassociated Bridge dialog box.

Figure 12-39 Add Unassociated Bridge Dialog Box



Step 3 In the Add Unassigned Bridge to *domain* dialog box, select the required bridge and click **OK**. The map is refreshed and displays the newly added bridge as shown in Figure 12-40.

Figure 12-40 Unassociated Bridge in Prime Network Vision



Working with Ethernet Flow Point Cross-Connects

Prime Network Vision automatically discovers Ethernet flow point (EFP) cross-connects, also known as locally switched EFPs. Prime Network Vision also identifies changes in already identified EFP cross-connects, such as cross-connect deletions or changes. Cross-connect changes can occur when one side of the cross-connect is removed or replaced.

Prime Network Vision also associates the VLANs that contain the EFPs that are part of the cross-connects. If the cross-connect contains a range EFP, which represents a range of VLANs, and you add the related VLANs to a map, Prime Network Vision displays the links between them and the cross-connect as well.

Prime Network Vision enables you to add EFP cross-connects to maps and to view their properties in inventory, as described in the following topics:

- Adding EFP Cross-Connects, page 12-76
- Viewing EFP Cross-Connect Properties, page 12-76

Adding EFP Cross-Connects

To add an EFP cross-connect to a map:

Step 1 In Prime Network Vision, select the map to which you wish to add the cross-connect.

Step 2 Open the Add EFP Cross-Connect dialog box in one of the following ways:

- Choose **File Add to Map > Cross Connect**.
- In the toolbar, click **Add to Map** and choose **Cross Connect**.

Step 3 In the Add EFP Cross Connect to *domain* dialog box, select the required EFP cross-connect and click **OK**.

The map is refreshed and displays the newly added EFP cross-connect.

Viewing EFP Cross-Connect Properties

To view EFP cross-connect properties in Prime Network Vision, do either of the following:

- Select the EFP cross-connect with the properties you want to view, and choose **Node > Properties**.
- Double-click the device configured with an EFP cross-connect and, in the inventory window, choose **Logical Inventory > Local Switching > Local Switching Entity**.

The information that is displayed for EFP cross-connects is the same in both the Local Switching Entry Properties window and in the Local Switching Table in logical inventory (as shown in Figure 12-41).

Figure 12-41 Local Switching Table in Logical Inventory

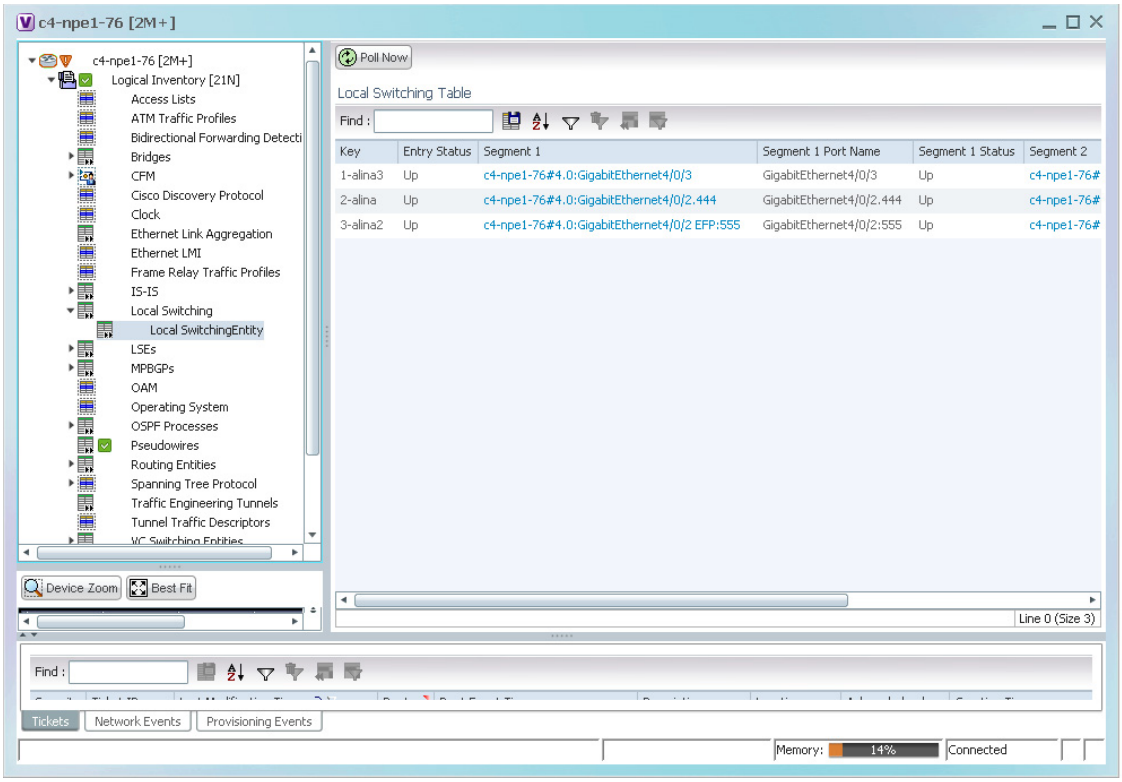


Table 12-36 describes the information displayed for the EFP cross-connects in the Local Switching Table.

Table 12-36 EFP Cross-Connect Properties in Local Switching Table

Field	Description
Key	Entry key for the cross-connect group.
Entry Status	Status of the cross-connect: Down, Unresolved, or Up.
Segment 1	Identifier of the first cross-connect segment, hyperlinked to the relevant entry in physical inventory.
Segment 1 Port Name	Identifier of the first cross-connect segment port.
Segment 1 Status	Status of the first cross-connect segment, such as Admin Up, Admin Down, Oper Down, or Up.
Segment 2	Identifier of the second cross-connect segment, hyperlinked to the relevant entry in physical inventory.
Segment 2 Port Name	Identifier of the second cross-connect segment port.
Segment 2 Status	Status of the second cross-connect segment, such as Admin Up, Admin Down, Oper Down, or Up.

Working with VPLS and H-VPLS Instances

Virtual Private LAN Service (VPLS) is a Layer 2 VPN technology that provides Ethernet-based multipoint-to-multipoint communication over MPLS networks. VPLS allows geographically dispersed sites to share an Ethernet broadcast domain by connecting sites through pseudowires. The network emulates a LAN switch or bridge by connecting customer LAN segments to create a single bridged Ethernet LAN.

Hierarchical VPLS (H-VPLS) partitions the network into several edge domains that are interconnected using an MPLS core. The edge devices learn only of their local N-PE devices and therefore do not need large routing table support. The H-VPLS architecture provides a flexible architectural model that enables Ethernet multipoint and point-to-point Layer 2 VPN services, as well as Ethernet access to Layer 3 VPN services, enabling service providers to offer multiple services across a single high-speed architecture.

Prime Network Vision discovers the following VPLS-related information from the network and constructs VPLS instances:

- VSIs
- Pseudowires
- EFPs
- Switching entities

Prime Network Vision enables you to:

- Add VPLS instances to a map—See Adding VPLS Instances to a Map, page 12-79.
- Apply VPLS overlays—See Applying VPLS Instance Overlays, page 12-80.
- View link details in VPLS overlays—See Viewing Pseudowire Tunnel Links in VPLS Overlays, page 12-82.
- View VPLS-related properties—See the following topics:
  - Viewing VPLS Instance Properties, page 12-84
  - Viewing Virtual Switching Instance Properties, page 12-85
  - Viewing VPLS Core or Access Pseudowire Endpoint Properties, page 12-87
  - Viewing VPLS Access Ethernet Flow Point Properties, page 12-89

You can delete a VPLS forward from Prime Network Vision if it is displayed with the reconciliation icon.

Adding VPLS Instances to a Map

You can add the VPLS instances that Prime Network Vision discovers to maps as required.

To add a VPLS instance to a map:

Step 1 In Prime Network Vision, select the required map or domain.

Step 2 Open the Add VPLS Instance to *map* dialog box in either of the following ways:

- In the toolbar, choose **Add to Map > VPLS**.
- In the menu bar, choose **File > Add to Map > VPLS**.

Step 3 In the Add VPLS Instance dialog box, do either of the following:

- To search for specific elements:

  a. Choose **Search**.

  b. To narrow the display to a range of VPLS instances or a group of VPLS instances, enter a search string in the search field.

  c. Click **Go**.

  For example, if you enter **`VPLS1`**, the VPLS instances that have names containing the string VPLS1 are displayed.

- To view all available VPLS instances, choose **Show All** and click **Go**.

The VPLS instances that meet the specified search criteria are displayed in the Add VPLS Instance dialog box in table format. The dialog box also displays the date and time at which the list was generated. To update the list, click **Refresh**.

Note If an element is not included in your scope, it is displayed with the locked device icon.

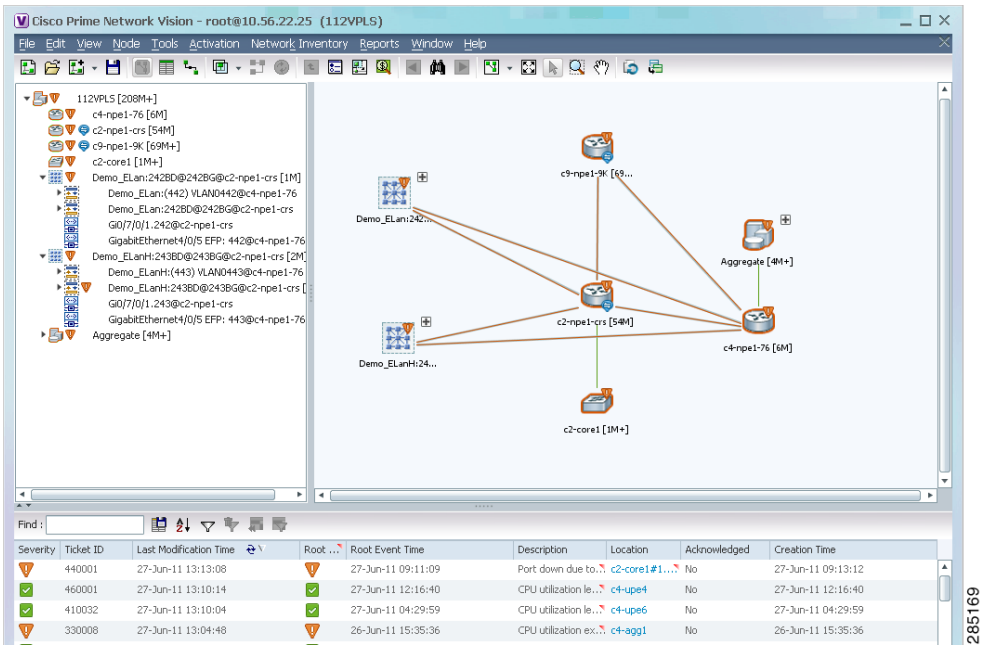
For information about sorting and filtering the table contents, see Filtering and Sorting Tabular Content, page 2-42.

Step 4 In the Add VPLS Instance dialog box, select the instances that you want to add. You can select and add multiple instances by pressing **Ctrl** while selecting individual instances or by pressing **Ctrl +Shift** to select a group of instances.

Step 5 Click **OK**.

The VPLS instance is displayed in the navigation pane and in the content area. In addition, any associated tickets are displayed in the ticket pane. See Figure 12-42.

Figure 12-42 VPLS Instance in Prime Network Vision Map



The VPLS instance information is saved with the map in the Prime Network database.

Applying VPLS Instance Overlays

An VPLS instance overlay allows you to isolate the parts of a network that are being used by a specific VPLS instance.

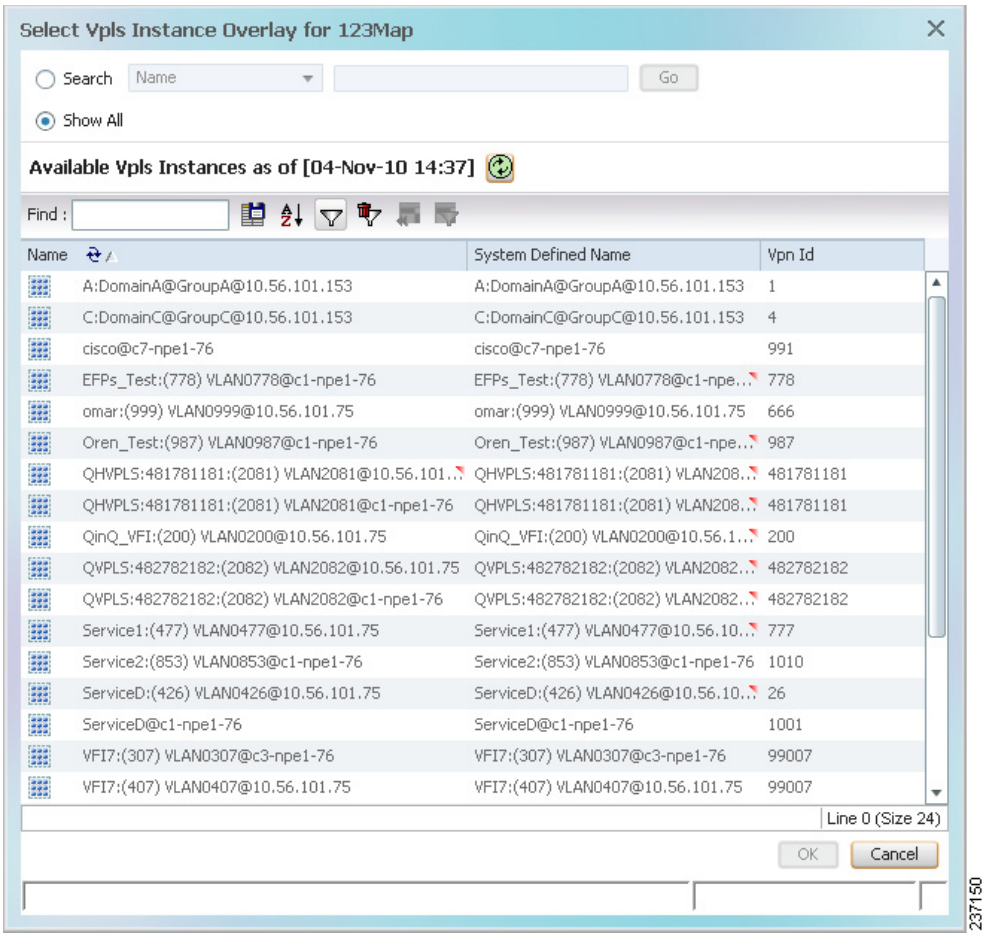
To apply a VPLS instance overlay:

Step 1 In Prime Network Vision, choose the map in which you want to apply an overlay.

Step 2 From the toolbar, choose **Choose Overlay Type > VPLS**.

Figure 12-43 shows an example of the Select VPLS Instance Overlay for *map* dialog box.

Figure 12-43 Select VPLS Instance Overlay Dialog Box

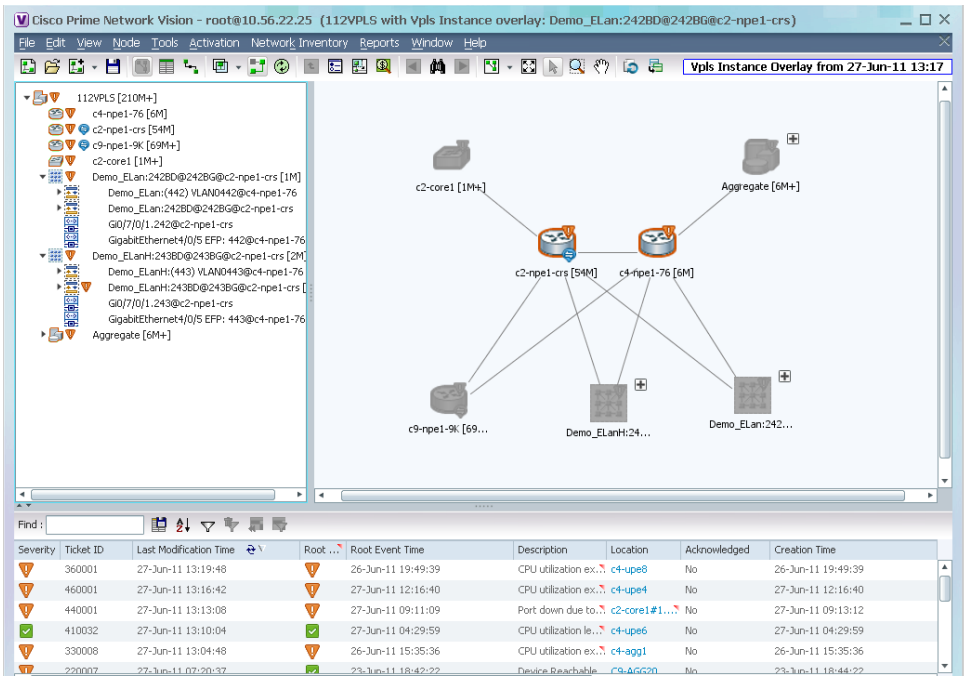


Step 3 Select the required VPLS instance for the overlay.

Step 4 Click **OK**.

The elements being used by the selected VPLS instance are highlighted in the map while the other elements are dimmed, as shown in Figure 12-44.

Figure 12-44 VPLS Instance Overlay in Prime Network Vision



Step 5 To hide and view the overlay, click **Hide Overlay/Show Overlay** in the toolbar. The button toggles depending on whether the overlay is currently displayed or hidden.

Step 6 To remove the overlay, choose **Choose Overlay Type > None**.

Viewing Pseudowire Tunnel Links in VPLS Overlays

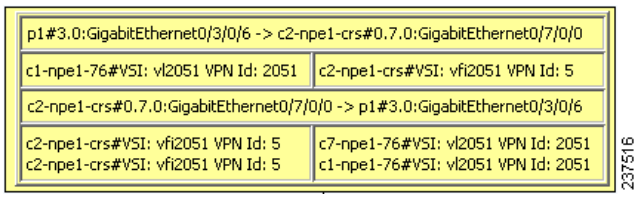
When a VPLS overlay is applied to a map in Prime Network Vision, you can view the details of the pseudowires that are interconnected through selected links.

To view unidirectional or bidirectional pseudowire traffic links when a VPLS overlay is applied to a map:

Step 1 Right-click the required link in the overlay, and choose **Show Callouts**. The link must be visible (not dimmed) in the map.

Link information is displayed as shown in Figure 12-45.

Figure 12-45 Link Callout Window for a VPLS Overlay



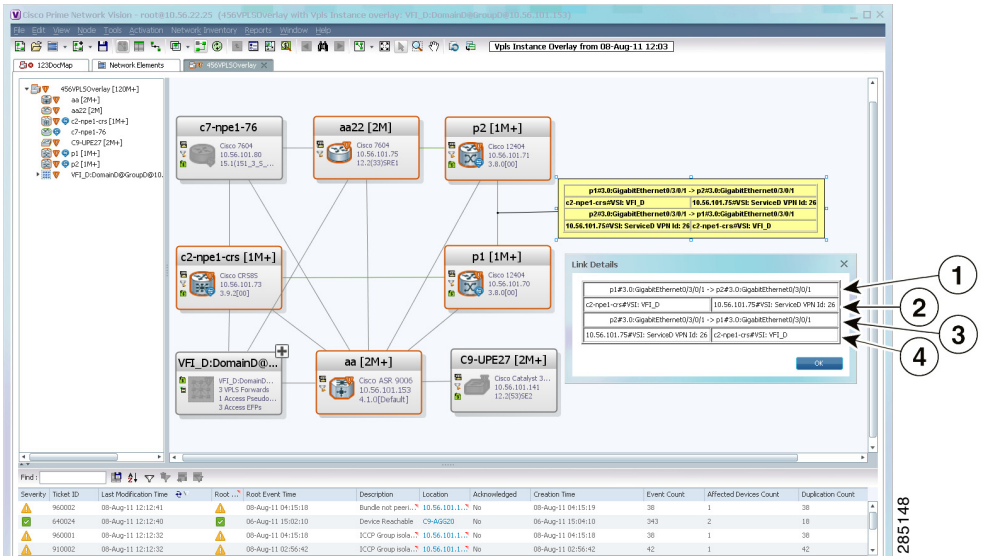
The callout window displays the following information for each link represented by the selected link:

- Link details and direction.
- Details of the sites using the link and the interlinks.

Step 2 To view the pseudowire link details, double-click the yellow callout window.

The details about the link are displayed in the Link Details window as shown in Figure 12-46.

Figure 12-46 Link Details Window for a VPLS Overlay



The Link Details window provides the following information:

1	Link details and direction. In this example, the link is from p1 to p2.
3	Link details and direction. In this example, the link is from p2 to p1.
2 and 4	Details of the pseudowire tunnel traversing this link.

Step 3 Click **OK** to close the Link Details window.

Step 4 To close the link callout window, right-click the selected link, then choose **Hide Callouts**.

Viewing VPLS-Related Properties

Prime Network Vision enables you to view the properties of the following VPLS-related elements:

- VPLS instances—See Viewing VPLS Instance Properties, page 12-84.
- Virtual Switching Instances—Viewing Virtual Switching Instance Properties, page 12-85
- Tunnels—See Viewing VPLS Core or Access Pseudowire Endpoint Properties, page 12-87.
- Port connectors—See Viewing VPLS Access Ethernet Flow Point Properties, page 12-89.

Viewing VPLS Instance Properties

To view the properties of a VPLS instance in Prime Network Vision, open the VPLS Instance Properties window in either of the following ways:

- In the navigation pane or the map pane, right-click the VPLS instance and choose **Properties**.
- In the navigation pane or the map pane, select the VPLS instance and choose **Node > Properties**.

Figure 12-47 shows an example of the VPLS Instance Properties window.

Figure 12-47 VPLS Instance Properties Window

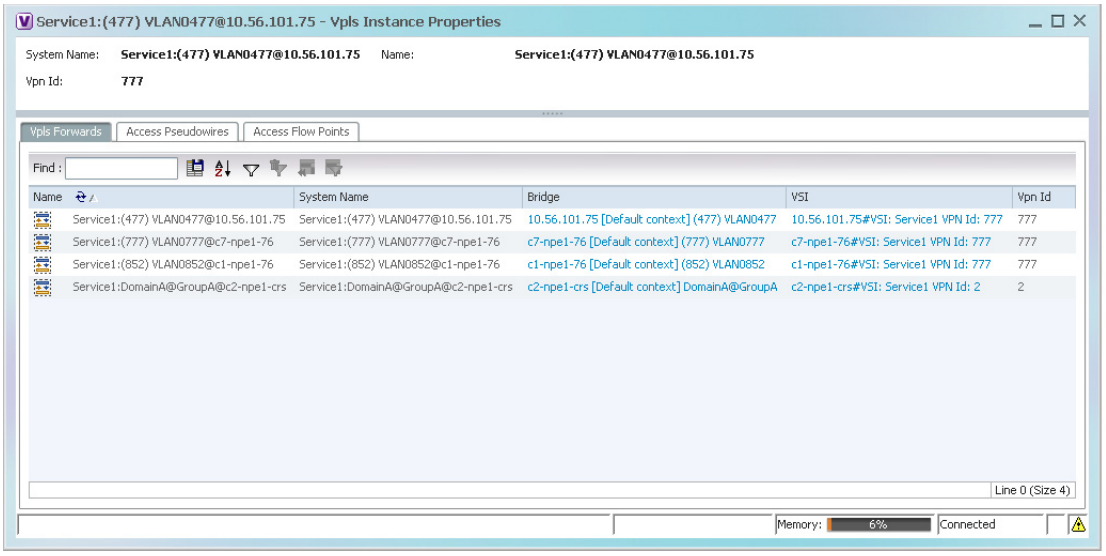


Table 12-37 describes the information that is displayed for VPLS instance properties.

The tabs that appear in the window depend on the VPLS instance and its configuration.

Table 12-37 VPLS Instance Properties

Field	Description
System Name	Name that Prime Network Vision assigns to the VPLS instance.
Name	User-defined name of the VPLS instance. When the VPLS instance is created, the system name and this name are the same. If you change the name of the VPLS instance (right-click, then choose **Rename**), the changed name appears in this field whereas the system name retains the original name.
VPN ID	VPN identifier used in an MPLS network to distinguish between different VPLS traffic.
VPLS Forwards Tab	
Name	User-defined name of the VPLS forward.
System Name	Name that Prime Network Vision assigns to the VPLS forward.
Bridge	Bridge that the VSI is configured to use, hyperlinked to the bridge table in logical inventory.
VSI	VSI hyperlinked to the relevant entry in logical inventory.

Table 12-37 VPLS Instance Properties (continued)

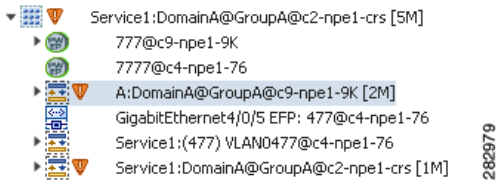
Field	Description
VPN ID	VPN identifier for the VSI.
Access Pseudowires Tab	
Name	Pseudowire name.
Port	VSI on which the pseudowire is configured, hyperlinked to the entry in logical inventory.
Local Router IP	Local router IP address on which the pseudowire is configured.
Tunnel ID	Virtual circuit identifier of the pseudowire.
PTP Tunnel	Hyperlinked entry to the pseudowire properties in logical inventory.
Peer Router IP	Peer router IP address on which the pseudowire is configured.
Peer OID	Hyperlinked entry to the pseudowire properties of the peer.
Pseudowire Type	Type of pseudowire, such as Ethernet, Ethernet Tagged, CESoPSN Basic, PPP, or SAToP.
Pseudowire Edge Binding Type	Pseudowire endpoint association: • 0—Unknown • 1—Connection termination point • 2—Ethernet flow point • 3—Switching entity • 4—Pseudowire switching entity • 5—VPLS forward
Access Flow Points Tab	
Name	Access flow point name. Double-click to view port connector properties.
Port	Interface configured as a flow point, hyperlinked to the interface in physical inventory.

Viewing Virtual Switching Instance Properties

To view VSI properties in Prime Network Vision, open the VSI properties window in either of the following ways:

- Double-click the required device and, in the inventory window, choose **Logical Inventory > VSIs >** *vsi*.
- In the navigation pane, expand the VPLS instance, right-click the required VPLS forward, and choose **Inventory** or **Properties**. (See Figure 12-48.)

Figure 12-48 VPLS Forward in Prime Network Vision Navigation Pane



If you right-click the VPLS forward and choose **Inventory**, the inventory window is displayed. If you right-click the VPLS forward and choose **Properties**, the VSI Properties window is displayed. The information displayed is the same for both options.

VSI properties are displayed as shown in Figure 12-49.

Figure 12-49 VSI Properties in Logical Inventory

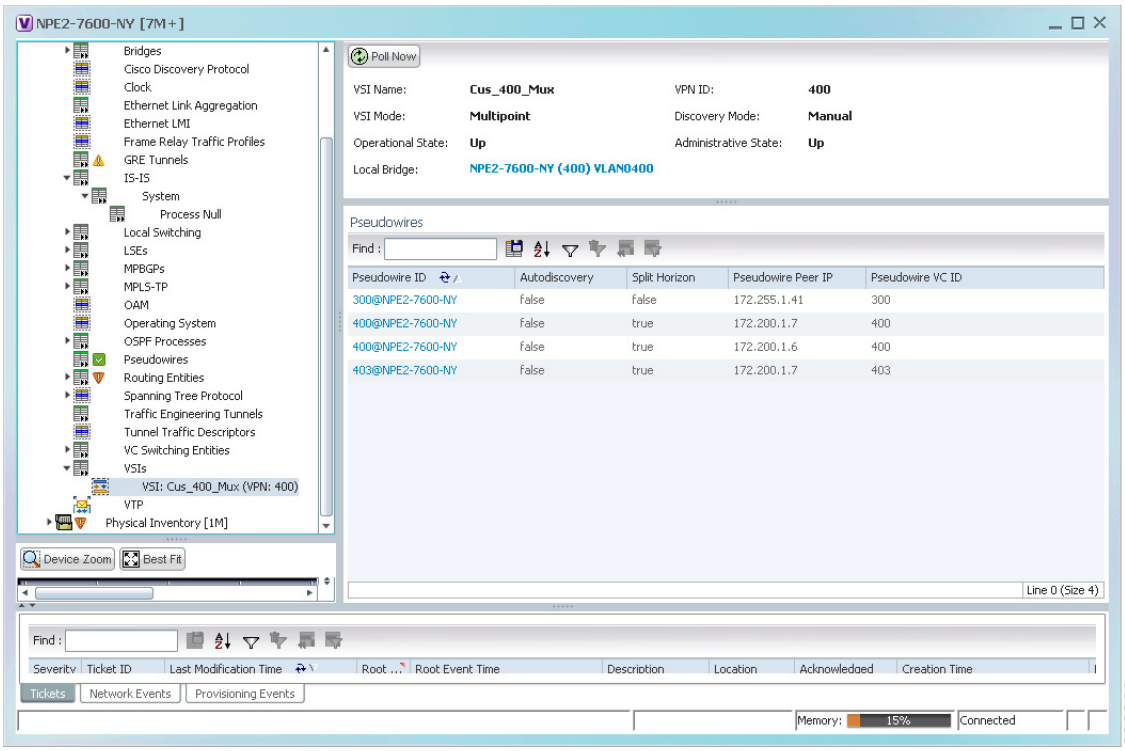


Table 12-38 describes the information that is displayed for the selected VSI.

Table 12-38 VSI Properties in Logical Inventory

Field	Description
VSI Name	VSI name.
VPN ID	VPN identifier used in an MPLS network to distinguish between different VPLS traffic.
VSI Mode	VSI mode: Point-to-Point (default) or Multipoint.
Discovery Mode	VSI discovery mode: Manual, BGP, LDP, RADIUS, DNS, MSS/OSS, or Unknown.
Operational State	VSI operational status: Up or Down.
Administrative State	VSI administrative status: Up or Down.
Local Bridge	Local bridge, hyperlinked to the bridge in logical inventory.
Pseudowires Table	
Pseudowire ID	Pseudowire identifier, hyperlinked to the Tunnel Edges table under Pseudowires in logical inventory.
Autodiscovery	Whether the pseudowire was automatically discovered: True or False.
Split Horizon	SSH pseudowire policy that indicates whether or not packets are forwarded to the MPLS core: True or False.
Pseudowire Peer IP	IP address of the pseudowire peer.
Pseudowire VC ID	Pseudowire virtual circuit identifier.

Viewing VPLS Core or Access Pseudowire Endpoint Properties

Pseudowire endpoints are displayed under VPLS Instance (Access) or VPLS Forward (Core) in the Prime Network Vision navigation pane.

To view pseudowire endpoint properties for a VPLS instance, right-click the required pseudowire endpoint in the navigation pane, and choose **Properties**. (See Figure 12-50.)

Figure 12-50 VPLS Pseudowire in Prime Network Vision Navigation Pane

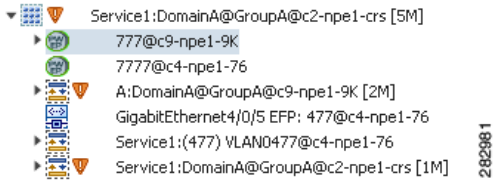


Figure 12-51 shows an example of the Tunnel Properties window that is displayed.

Figure 12-51 VPLS Tunnel Properties Window

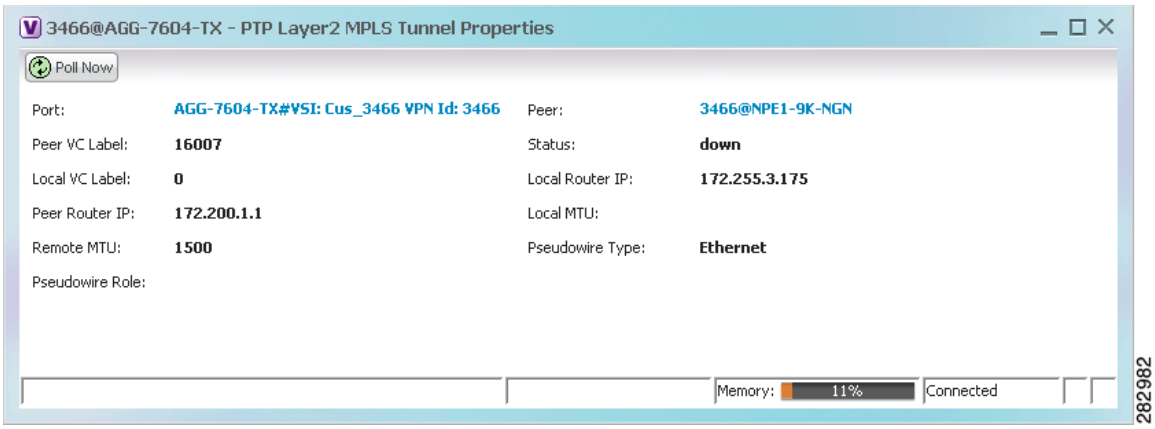


Table 12-39 describes the information that is displayed for pseudowire endpoint properties.

Table 12-39 Tunnel Properties Window

Field	Description
Port	VSI on which the pseudowire is configured, hyperlinked to the VSI in logical inventory.
Peer	Hyperlinked entry to the pseudowire endpoint peer pseudowires in logical inventory.
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.
Tunnel Status	Operational state of the tunnel: Up or Down.
Local VC Label	MPLS label that is used to identify or access the tunnel. It is inserted into the MPLS label stack by the local router.
Local Router IP	IP address of this tunnel edge, which is used as the MPLS router identifier.
Tunnel ID	Identifier that, along with the router IP addresses of the two pseudowire endpoints, identifies the PWE3 tunnel.
Peer Router IP	IP address of the peer tunnel edge, which is used as the MPLS router identifier.
Local MTU	Size, in bytes, of the MTU on the local interface.
Remote MTU	Size, in bytes, of the MTU on the remote interface.
Signaling Protocol	Protocol used by MPLS to build the tunnel, such as LDP or TDP.
Pseudowire Type	Type of pseudowire, such as Ethernet, Ethernet Tagged, CESoPSN Basic, PPP, or SAToP.

Viewing VPLS Access Ethernet Flow Point Properties

The ports that represent the attachment circuits to VPLS instances are displayed under VPLS instances in the Prime Network Vision navigation pane.

To view the properties for the Access Ethernet Flow Points configured for a VPLS instance, right-click the required interface in the navigation pane, and choose **Inventory**. (See Figure 12-52.)

Figure 12-52 VPLS Interface in Prime Network Vision Navigation Pane

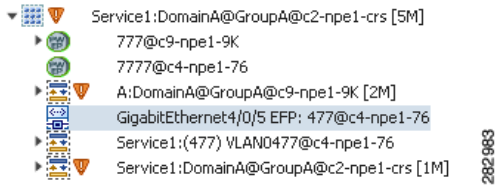
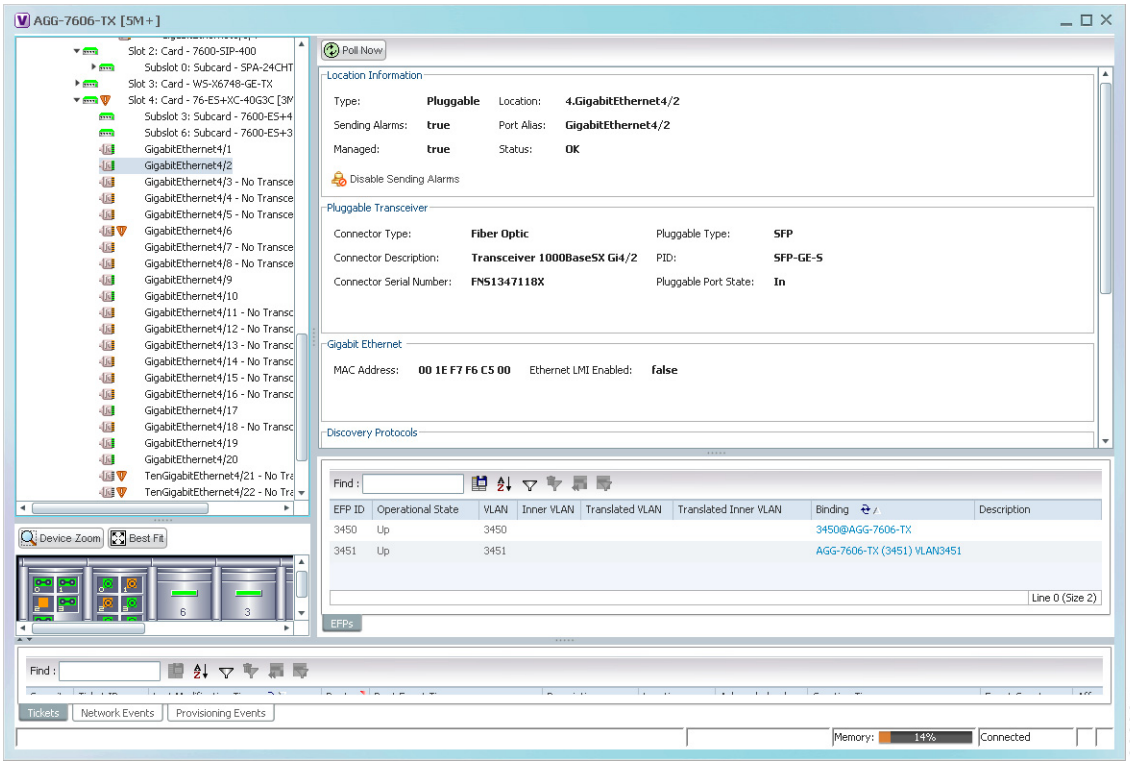


Figure 12-53 shows an example of the information displayed for the interface in physical inventory.

Figure 12-53 EFP Properties in Physical Inventory



The information displayed in this window is the same as that displayed when the interface is selected in physical inventory.

The following information is displayed, depending on the interface and its configuration:

- Location and interface details.
- Technology-related information, such as Ethernet CSMA/CD or ATM IMA properties.
- VLAN configuration details.

- List of the configured subinterfaces on the port. For more information on the Subinterfaces table, see Viewing a Port Configuration, page 3-25.
- List of the configured EFPs on the port. For more information on the EFPs table, see Viewing EFP Properties, page 12-33.
- List of VLAN mappings configured on the port. For more information about the VLAN Mappings table, see Viewing VLAN Mappings, page 12-53.

Working with Pseudowires

Prime Network supports the discovery and modeling of Any Transport over MPLS (AToM) and Ethernet over MPLS (EoMPLS) domains that span multisegment pseudowires. After discovery is complete, you can add any of the pseudowires to a map, view their properties in logical inventory, or view their redundancy status.

You can run the psuedowire commands on all Cisco IOS and Cisco IOS XR devices that support pseudowire technology, such as

- Cisco 7200 series routers
- Cisco 7600 series routers
- Cisco ASR 9000 series aggregation services routers
- Cisco XR 12000 series routers
- Cisco ME 3600X and Cisco ME 3800X Carrier Ethernet Switches
- Cisco Carrier Packet Transport (CPT) System

For details on the software versions Prime Network supports for these network elements, see the *Cisco Prime Network 4.0 Supported Cisco VNEs*. To run the pseudowire commands, the software on the network element must support the pseudowire technology.

The following topics describe the options available to you for working with pseudowires in Prime Network:

- Adding Pseudowires to a Map, page 12-90
- Viewing Pseudowire Properties, page 12-93
- Displaying Pseudowire Information, page 12-95
- Viewing Pseudowire Redundancy Service Properties, page 12-96
- Applying Pseudowire Overlays, page 12-98
- Monitoring the Pseudowire Headend, page 12-100

Adding Pseudowires to a Map

You can add a pseudowire that Prime Network discovers to maps as required.

To add a pseudowire to a map:

Step 1 In Prime Network Vision, select the required map or domain.

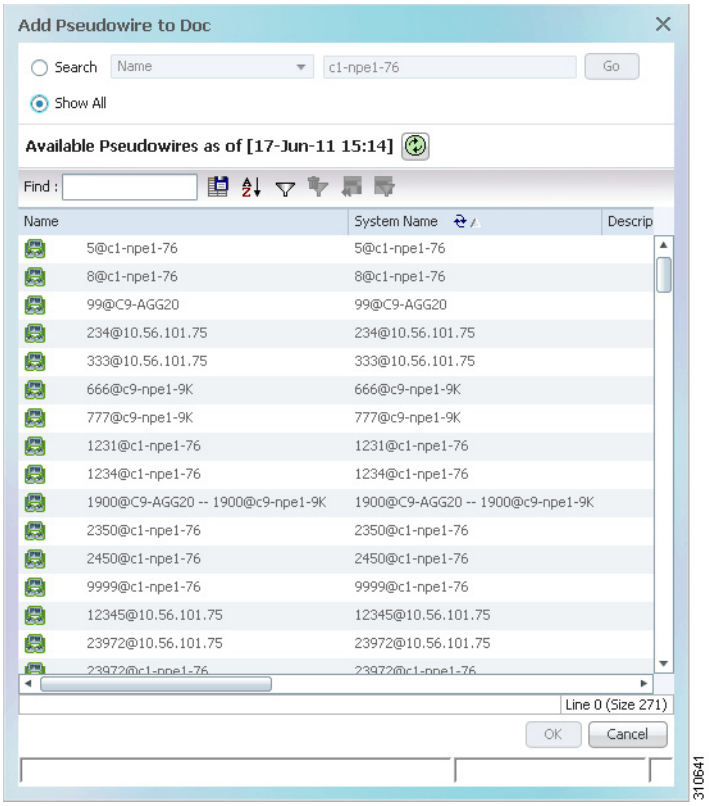
Step 2 Open the Add Pseudowire to *map* dialog box in either of the following ways:

- In the toolbar, choose **Add to Map > Pseudowire**.

- In the menu bar, choose **File > Add to Map > Pseudowire**.

Figure 12-54 shows an example of the Add Pseudowire dialog box.

Figure 12-54 Add Pseudowire Dialog Box



Step 3 In the Add Pseudowire dialog box, do either of the following:

- To search for specific elements:

  a. Choose **Search**.

  b. To narrow the display to a range of pseudowire or a group of pseudowires, enter a search string in the search field.

  c. Click **Go**.

  For example, if you enter `pseudo1`, the pseudowires that have names containing the string "pseudo1" are displayed.

- To view all available pseudowires, choose **Show All** and click **Go**.

The pseudowires that meet the specified search criteria are displayed in the Add Pseudowire dialog box in table format. The dialog box also displays the date and time at which the list was generated. To update the list, click **Refresh**.

Note If an element is not included in your scope, it is displayed with the locked device icon.

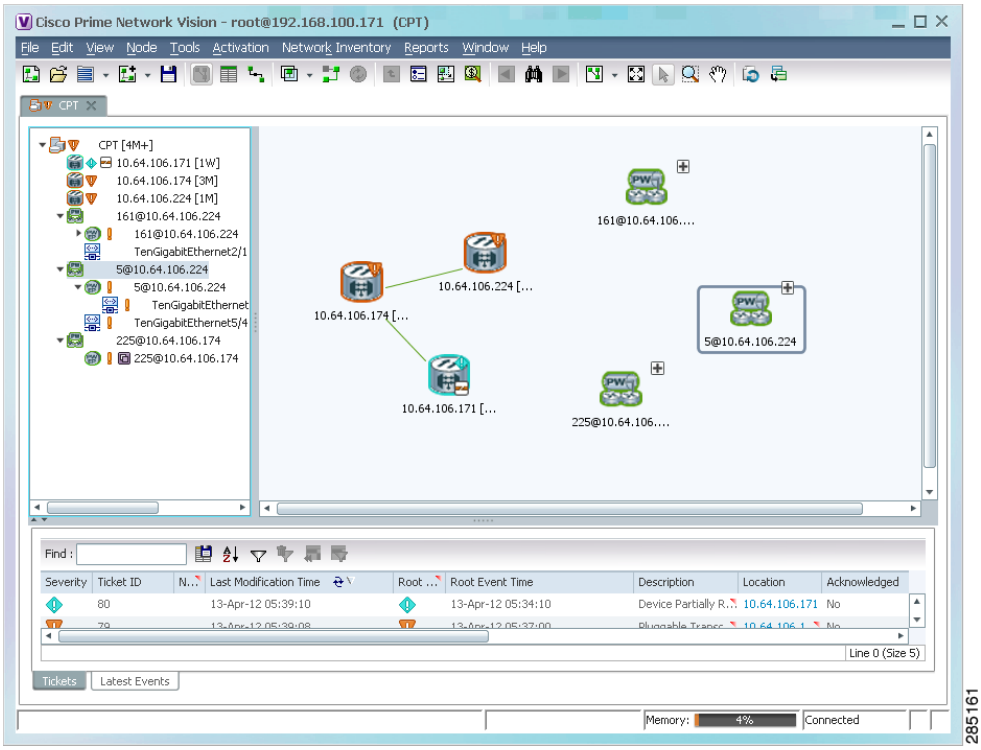
For information about sorting and filtering the table contents, see Filtering and Sorting Tabular Content, page 2-42.

Step 4 In the Add Pseudowire dialog box, select the pseudowires that you want to add. You can select and add multiple pseudowires by pressing **Ctrl** while selecting individual pseudowires or by pressing **Ctrl +Shift** to select a group of pseudowires.

Step 5 Click **OK**.

The pseudowire is displayed in the navigation pane and in the content area. In addition, any associated tickets are displayed in the ticket pane. See Figure 12-55.

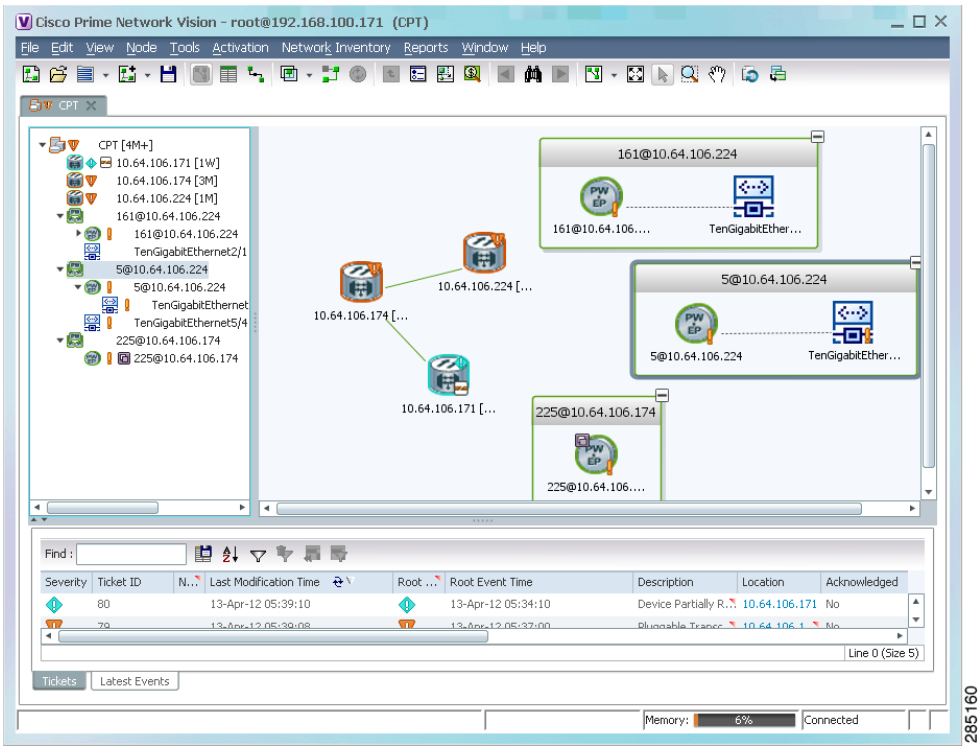
Figure 12-55 Pseudowire in Prime Network Vision Map



Step 6 Click the pseudowire in the navigation pane or double-click the pseudowire in the map pane to view the pseudowire components, such as pseudowire endpoints, pseudowire switching entities, and terminating interfaces.

Figure 12-56 shows an example of an expanded pseudowire in Prime Network Vision.

Figure 12-56 Pseudowire Components in Prime Network Vision Maps



The pseudowire information is saved with the map in the Prime Network database.

Viewing Pseudowire Properties

To view pseudowire properties:

Step 1 In Prime Network Vision, select the required map or domain.

Step 2 To view pseudowire endpoint properties configured on an element:

a. In the navigation or map pane, right-click the required element and then choose **Inventory**.

b. In the inventory window, choose **Logical Inventory > Pseudowires**.

The Tunnel Edges table is displayed, listing the pseudowire endpoints configured on the selected element. For a description of the information contained in the Pseudowires Tunnel Edges table, see Table 18-27.

Step 3 To view the properties of a pseudowire that you added to a map, do either of the following:

- If the pseudowire icon is of the largest size, click the **Properties** button.
- Right-click the element, and then choose **Properties**.

The Pseudowire Properties window is displayed as shown in Figure 12-57.

Figure 12-57 Pseudowire Properties Window

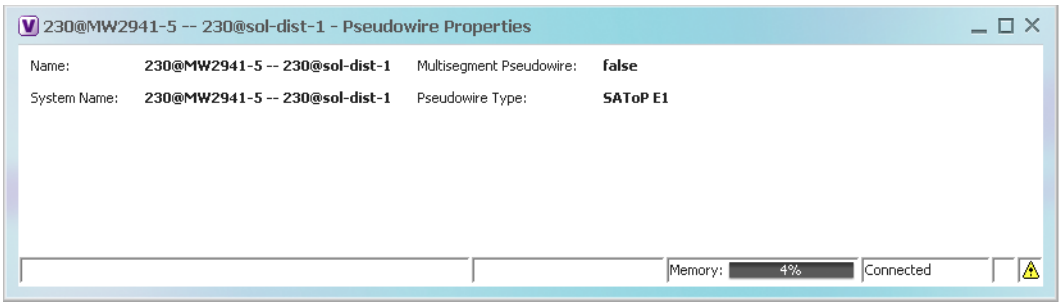


Table 12-40 describes the information presented in the Pseudowire Properties window.

Table 12-40 Pseudowire Properties Window

Field	Description
Name	Name of the pseudowire.
Multisegment Pseudowire	Whether or not the pseudowire is multisegment: True or False.
System Name	Internal or system-generated name of the pseudowire.
Pseudowire Type	Type of pseudowire, such as Ethernet, Ethernet Tagged, CESoPSN Basic, PPP, or SAToP.

Step 4 To view the properties of a pseudowire endpoint associated with a pseudowire, right-click the required pseudowire endpoint, and then choose **Properties**.

The Tunnel Properties window containing the pseudowire endpoint properties is displayed as shown in Figure 12-51 and described in Table 12-39.

Step 5 To view the properties of a pseudowire switching entity associated with the pseudowire, select the switching entity, and then choose **Node > Inventory**.

The Local Switching table is displayed as shown in Figure 12-41.

Table 12-36 describes the information displayed in the Local Switching table.

Step 6 To view the properties of the pseudowire endpoint that terminates on the subinterface, right-click the required interface, and then choose **Properties**.

Note The selected port must be an Ethernet subinterface for the Contained Current CTPs table to be displayed.

Table 12-41 describes the information displayed in the Contained Current CTPs table.

Table 12-41 Contained Current CTPs Table

Field	Description
Local Interface	The name of the subinterface or port, hyperlinked to the interface in physical inventory.
ID	The tunnel identifier, hyperlinked to Pseudowires Tunnel Edges table in logical inventory.
Peer	The peer tunnel identifier, hyperlinked to the peer pseudowire tunnel in logical inventory.
Tunnel ID	The identifier that, along with the router IP addresses of the two tunnel edges, identifies the tunnel.
Tunnel Status	The operational state of the tunnel: Up or Down.
Local Router IP	The IP address of this tunnel edge, which is used as the router identifier.
Peer Router IP	The IP address of the peer tunnel edge, which is used as the router identifier.
Pseudowire Type	Type of pseudowire, such as Ethernet, Ethernet Tagged, CESoPSN Basic, PPP, or SAToP.
Local MTU	The size, in bytes, of the MTU on the local interface.
Remote MTU	The size, in bytes, of the MTU on the remote interface.
Local VC Label	The MPLS label that is used by this router to identify or access the tunnel. It is inserted in the MPLS label stack by the local router.
Peer VC Label	The MPLS label that is used by this router to identify or access the tunnel. It is inserted in the MPLS label stack by the peer router.
Signaling Protocol	The protocol used to build the tunnel, such as LDP or TDP.
Preferred Path Tunnel	The path to be used for pseudowire traffic.

Step 7 To view the properties of an Ethernet flow point associated with the pseudowire, right-click the EFP and then choose Properties.

See Viewing EFP Properties, page 12-33 for the information that is displayed for EFPs.

Displaying Pseudowire Information

Note You might be prompted to enter your device access credentials while exectuing the command. Once you have entered them, these credentials will be used for every subsequent execution of a command in the same GUI client session. If you want to change the credentials, click **Edit Credentials**. The Edit Credentials button will not be available for SNMP commands or if the command is scheduled for a later time.

To To view Virtual Circuit Connectivity Verification (VCCV) and Control Channel (CC) information for a pseudowire endpoint:

Step 1 In the require map, double-click the required device configured for pseudowire.

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

Step 3 In the Tunnel Edges table, right-click the required interface and choose **Commands > Show > Display Pseudowire**.

Step 4 In the Display Pseudowire dialog box, do either of the following:

- To view the command before running it, click **Preview**.
- To run the command, click **Execute**.

When you click **Execute**, the results are displayed in the dialog box.

Step 5 The following information is displayed:

- The element name.
- The command issued.
- The results, including:
  - VCCV: CC Type—The types of CC processing that are supported. The number indicates the position of the bit that was set in the received octet. The available values are:

    - CW [1]—Control Word
    - RA [2]—Router Alert
    - TTL [3]—Time to Live
    - Unkn [x]—Unknown
  - Elapsed time—The elapsed time, in seconds.

Step 6 Click **Close** to close the Display Pseudowire dialog box.

Viewing Pseudowire Redundancy Service Properties

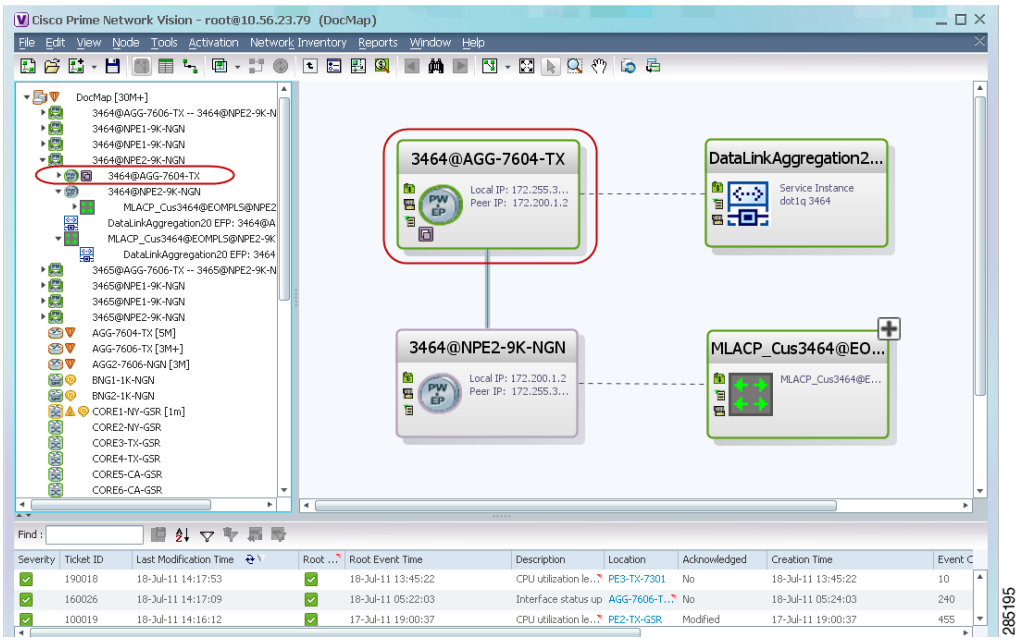
If a pseudowire is configured for redundancy service, a redundancy service badge is applied to the secondary (backup) pseudowire in the navigation and map panes in the Prime Network Vision window. Additional redundancy service details are provided in the inventory window for the device on which the pseudowire is configured.

To view redundancy service properties for pseudowires:

Step 1 To determine if a pseudowire is configured for redundancy service, expand the required pseudowire in the navigation or map pane.

If the pseudowire is configured for redundancy service, the redundancy service badge appears in the navigation and map panes as shown in Figure 12-58.

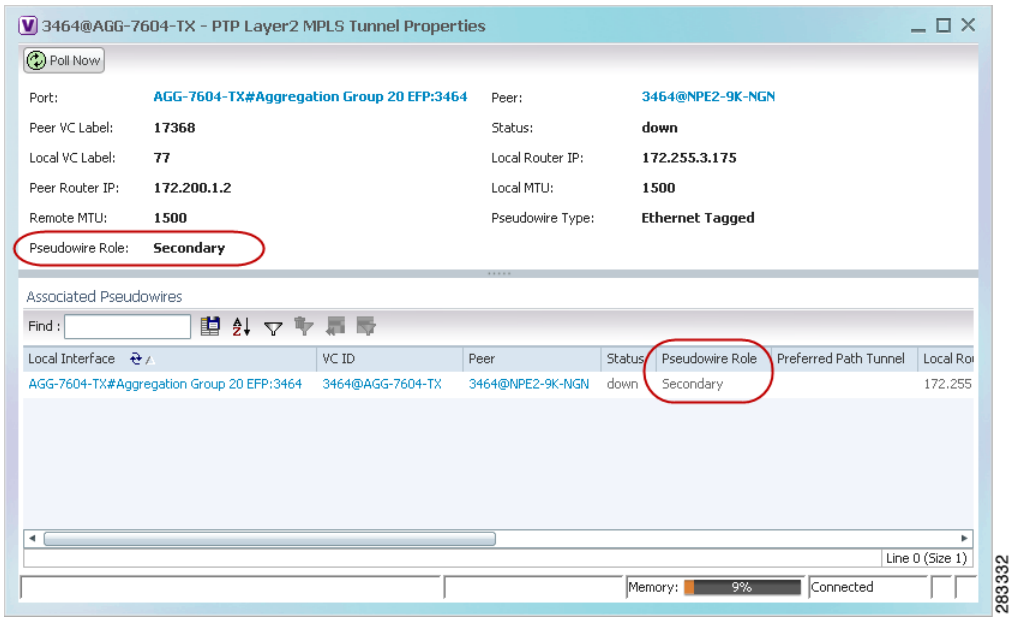
Figure 12-58 Pseudowire Redundancy Service Badge in a Map



Step 2 To view additional details, in the map, double-click the element with the redundancy service badge.

The PTP Layer 2 MPLS Tunnel Properties window is displayed as shown in Figure 12-59 and shows that the selected pseudowire has a Secondary role in a redundancy service.

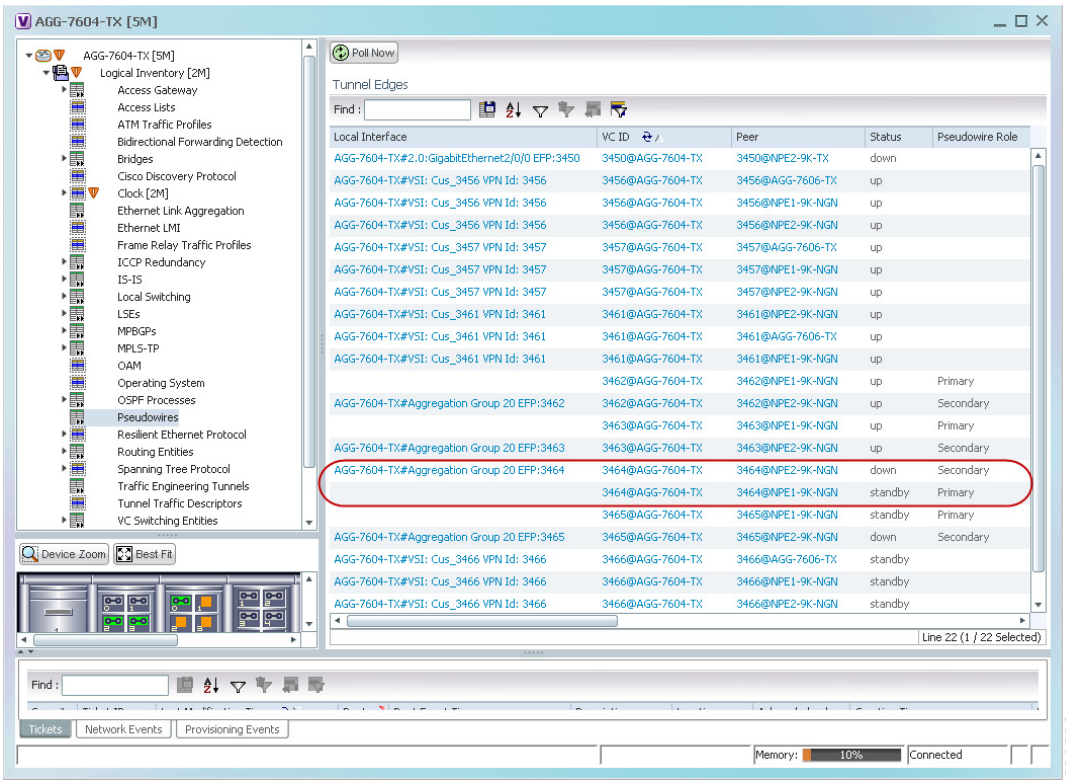
Figure 12-59 Layer 2 MPLS Tunnel Properties for Pseudowire Redundancy Service



Step 3 In the PTP Layer 2 MPLS Tunnel Properties window, click the VC ID hyperlink.

The Tunnel Edges table in logical inventory is displayed, with the local interface selected in the table. (See Figure 12-60.)

Figure 12-60 Pseudowire Redundancy Service in Logical Inventory



The entries indicate that the selected tunnel edge has a Secondary role in the first VC and a Primary role in the second VC.

For more information about the Pseudowires Tunnel Edges table, see Table 18-27.

Applying Pseudowire Overlays

A pseudowire overlay allows you to isolate the parts of a network that are used by a specific pseudowire.

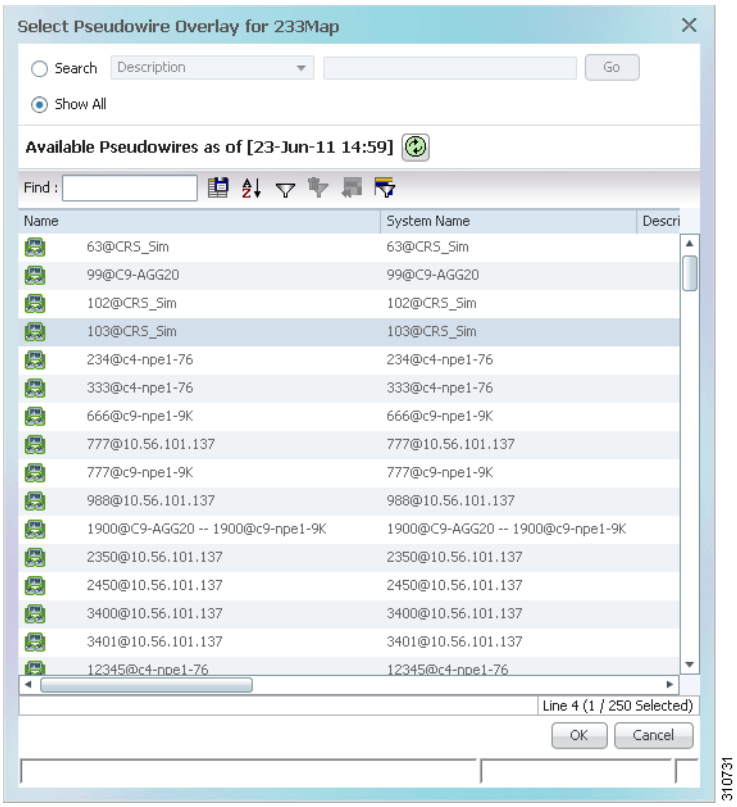
To apply a pseudowire overlay:

Step 1 In Prime Network Vision, choose the map in which you want to apply an overlay.

Step 2 From the toolbar, choose **Choose Overlay Type > Pseudowire**.

Figure 12-61 shows an example of the Select Pseudowire Overlay for *map* dialog box.

Figure 12-61 Select Pseudowire Overlay Dialog Box

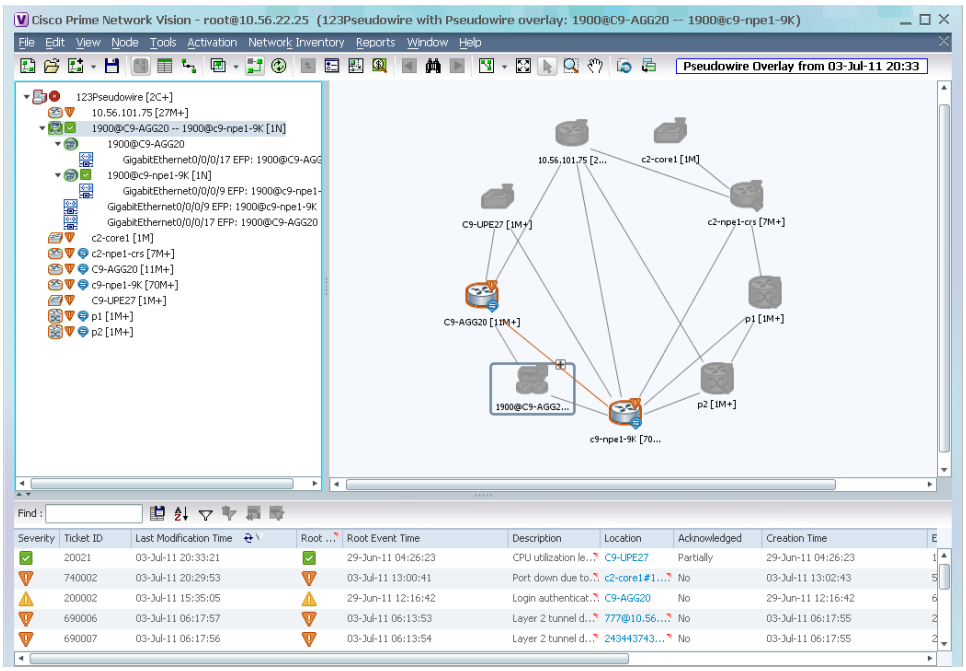


Step 3 Select the required pseudowire for the overlay.

Step 4 Click **OK**.

The elements being used by the selected pseudowire are highlighted in the map while the other elements are dimmed, as shown in Figure 12-62.

Figure 12-62 Pseudowire Overlay in Prime Network Vision



Step 5 To hide and view the overlay, click **Hide Overlay/Show Overlay** in the toolbar. The button toggles depending on whether the overlay is currently displayed or hidden.

Step 6 To remove the overlay, choose **Choose Overlay Type > None**.

Monitoring the Pseudowire Headend

A pseudowire (PW) is an emulation of a point-to-point connection over a packet-switching network (PSN). It operates over a uniform packet-based access/aggregation network. The composite L2 AC and the PW segment together form a point-to-point virtual CE-PE link that functions like a traditional CE-PE link technology.

Figure 12-63 displays a typical pseudowrie deployment over core network and Figure 12-64 displays a pseduowire deployment over access network.

Figure 12-63 Pseudowire Deployment Over Core Network

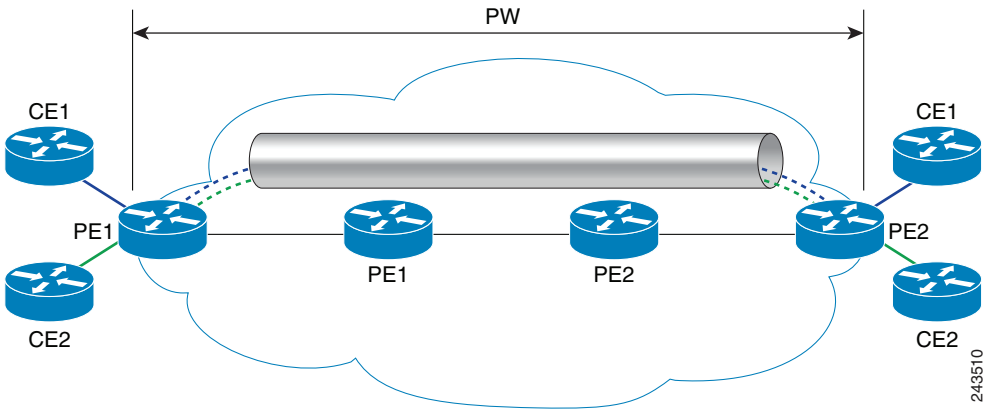
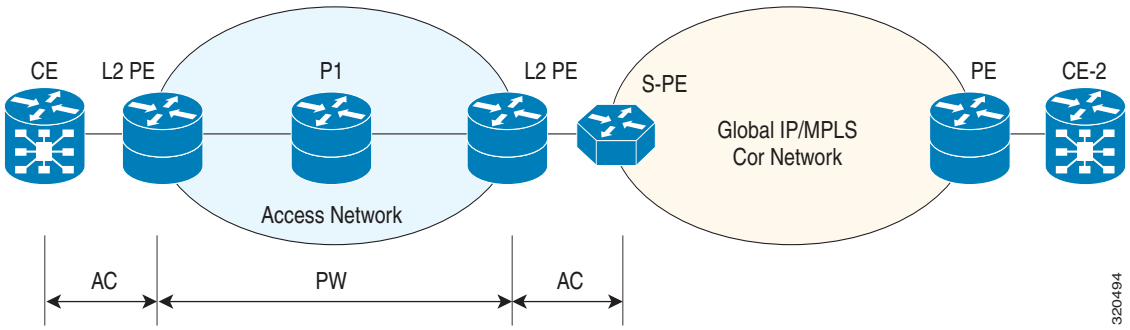


Figure 12-64 Pseudowire Deployment Over Access Network

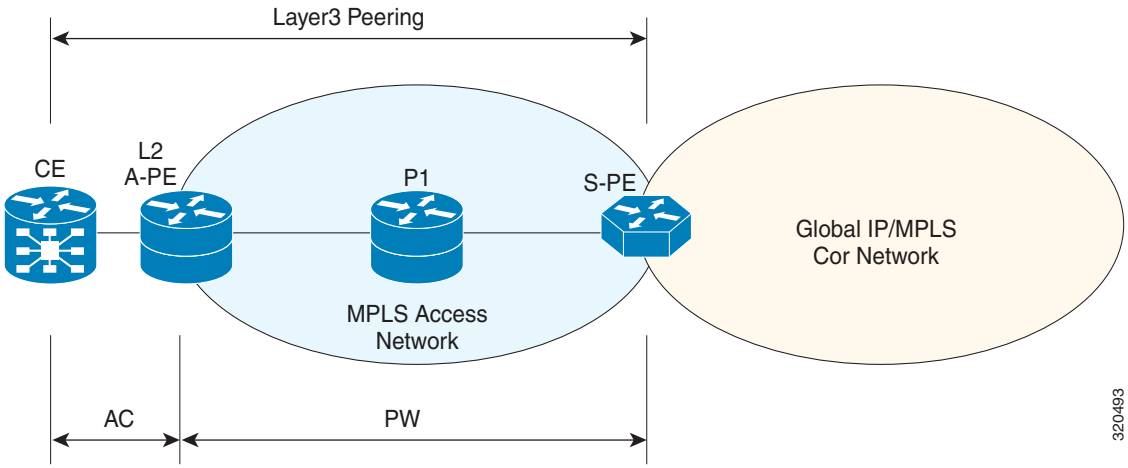


A pseudowire headend (PW-HE) virtual interface originates as a PW on an access node and terminates on a Layer 3 service instance on the service provider router. For example, a PWHE can originate on the Layer 2 PW feeder node and terminate on a VRF instance on the Cisco CRS Router. You can configure all ingress and egress QoS function on the PW-HE interface, including policing, shaping, queuing, and hierarchical policies.

In other words, the PW-HE is a technology that allows termination of access or aggregation pseduowires into an L2 or L3 domain. It allows us to replace a 2-node solution with a 1-node solution. Without a PW-HE, a L2 PE node must terminate a PW and then handoff the data to a S-PE via an Access Circuit.

The following figure displays the PW-HE interface:

Figure 12-65 PW-HE Interface



The PW-HE interface is treated like any existing L3 interface and operates on one of the following nodes:

- Bridged interworking (VC type 5 or 4) node—PW will carry customer Ethernet frames with IP payload. The S-PE device must perform ARP resolution for customer IP addresses learnt over PW-HE, which acts as a broadcast interface.
- IP interworking node (VC type 11)—The PW-HE acts as a point-to-point interface. Hence, there will be two types of PW-HE interface-PW-Ether and PW-IW. These PW's can terminate into a VRF or the IP global table on SP-E.

Viewing the PW-HE configuration

To view the PW-HE configuration:

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

Step 2 In the logical inventory window, choose **Logical Inventory > PW-HE**. The list of PW-HE interfaces configured in Prime Network are displayed in the content pane.

Step 3 From the **PW-HE** node, choose a PW-HE interface. The PW-HE interface details are displayed in the content pane as shown in Figure 12-66.

Figure 12-66 PW-HE Configuration Details

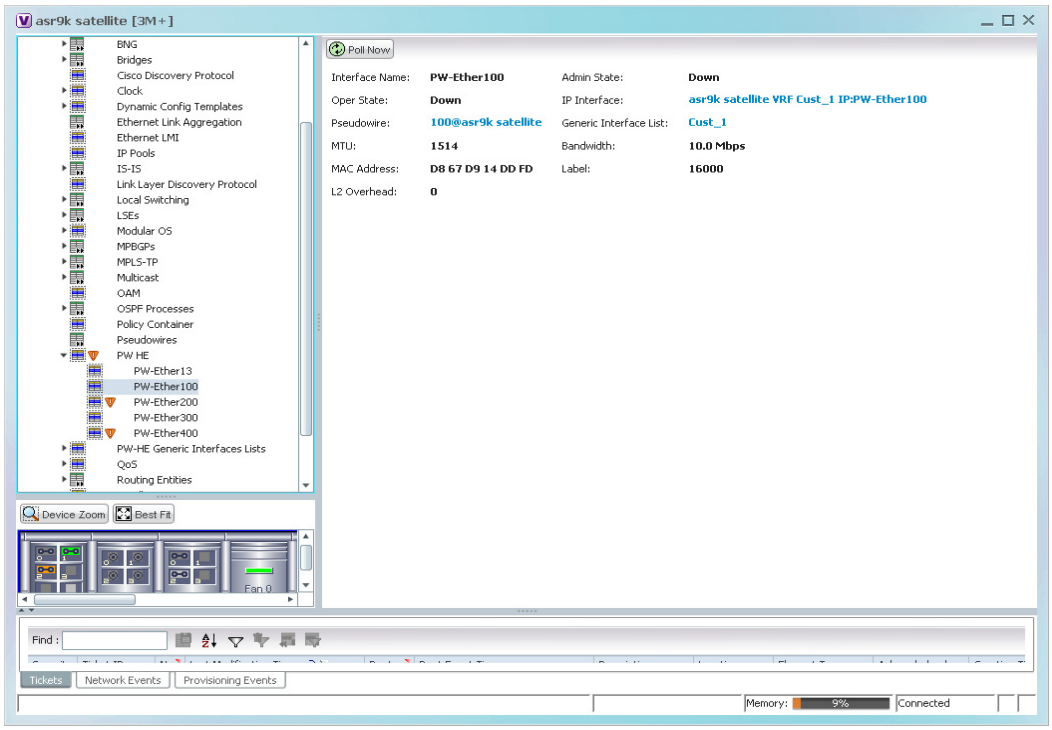


Table 12-42 displays the PW-HE interface details.

Table 12-42 PW-HE Interface Details

Field	Description
Interface Name	The unique name to identify the PW-HE interface.
Admin State	The administrative state of the PW-HE, which can be any one of the following: • Up • Down
Oper State	The operational state of the PW-HE, which can be any one of the following: • Up • Down
IP Interface	The IP interface for the PW-HE, which when clicked will take you either to the associated VRF interface site under the VRF node or the associated IP Interface under the Routing Entity node.
Pseudowire	The pseudowire to which the PW-HE is associated with, which when clicked will take you to the **Pseudowire** node.
Generic Interface List	The generic interface list linked to the PW-HE, which when clicked will take you to the relevant node under the **PW-HE Generic Interfaces Lists** node.
MTU	The maximum number of transmission units (in bytes) for the PW-HE interface.
Bandwidth	The bandwidth (in kbits) for the PW-HE interface.
MAC Address	The MAC address specified for the PW-HE interface, which is generally in the xxx.xxx.xxx format.
Label	The MPLS label for the PW-HE interface.
L2 Overhead	The layer 2 overhead (in bytes) configured on the PW-HE interface, which can be any value between 0 and 64. This field defaults to 0.

You can also view the following configuration details for a PW-HE interface:

- Viewing PW-HE Configured as a Local Interface under Pseudowire, page 12-104
- Viewing PW-HE Generic Interface List, page 12-105
- Viewing PW-HE as an Associated Entity for a Routing Entity, page 12-105
- Viewing PW-HE as an Associated Entity for a VRF, page 12-105

Viewing PW-HE Configured as a Local Interface under Pseudowire

To view the local interface details:

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

Step 2 In the logical inventory window, choose **Logical Inventory > Pseudowire**. The list of Pseudowire interfaces configured in Prime Network are displayed in the content pane. For more information on Pseudowire properties, see Viewing Pseudowire Properties, page 12-93.

Viewing PW-HE Generic Interface List

To view the PW-HE generic interface list:

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

Step 2 In the logical inventory window, choose **Logical Inventory > PW-HE Generic Interface List**. The list of generic interfaces configured in Prime Network are displayed in the content pane.

Step 3 From the **PW-HE Generic Interface List** node, choose a generic interface list. The interface details are displayed in the content pane.

Table 12-43 displays the PW-HE Generic Interface List details.

Table 12-43 PW-HE Generic Interface List Details

Field	Description
Generic Interface	The name of the generic interface list.
Interfaces tab	
Interface	The Ethernet Link Aggregation Group (LAG) for the PW-HE service, which when clicked will take you to the **LAG** node.

Viewing PW-HE as an Associated Entity for a Routing Entity

To view the routing entity details for a PW-HE:

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 entity details for the PW-HE is displayed in the content pane. For more information on Routing entity details, see Viewing Routing Entities, page 18-31.

Viewing PW-HE as an Associated Entity for a VRF

To view the VRF details for a PW-HE:

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

Step 2 In the logical inventory window, choose **Logical Inventory > VRF >** *PW-HE node*. The VRF details for the PW-HE is displayed in the content pane. For more information on VRF details, see Viewing VRF Properties, page 18-27.

Working with Ethernet Services

Ethernet services are created when the following business elements are linked to one another:

- Network VLAN and bridge domain are linked through a shared EFP.
- Network VLAN and VPLS instance are linked through either of the following:
  - A shared, standalone EFP.
  - A shared switching entity.
- Network VLAN and network pseudowire (single or multi-segment) are linked through either of the following:
  - A shared, standalone EFP.
  - A shared switching entity.
- VPLS-EoMPLS connected via a shared access pseudowire endpoint.
- Network VLAN and cross-connect are connected by a shared EFP.
- Network VLAN and service link are connected by a shared EFP.

If a VPLS, network pseudowire, cross-connect, or network VLAN object is not connected to another business element, it resides alone in an Ethernet service.

In releases prior to Prime Network Vision 3.8, EVC multiplex was discovered by means of Ethernet flow point associations. Beginning with Prime Network Vision 3.8, multiplex capabilities were enhanced to distinguish multiplexed services based on the Customer VLAN ID; that is, Prime Network Vision 3.9 is Inner Tag-aware.

As a result, in environments in which service providers have customers with multiplexed services, an EVC can distinguish each service and create its own EVC representation.

Prime Network Vision discovers Ethernet services and enables you to add them to maps, apply overlays, and view their properties. See the following topics for more information:

- Adding Ethernet Services to a Map, page 12-106
- Applying Ethernet Service Overlays, page 12-108
- Viewing Ethernet Service Properties, page 12-109

Adding Ethernet Services to a Map

You can add the Ethernet services that Prime Network Vision discovers to maps as required.

To add an Ethernet service to a map:

Step 1 In Prime Network Vision, select the required map or domain.

Step 2 Open the Add Ethernet Service to *map* dialog box in either of the following ways:

- In the toolbar, choose **Add to Map > Ethernet Service**.
- In the menu bar, choose **File > Add to Map > Ethernet Service**.

Step 3 In the Add Ethernet Service dialog box, do either of the following:

- To search for specific elements:

  a. Choose **Search**, and then choose a search category: EVC Terminating EFPs, Name, or System Name.

b. To narrow the display to a range of Ethernet services or a group of Ethernet services, enter a search string in the search field.

c. Click **Go**.

For example, if you choose Name and enter **EFP1**, the network elements that have names beginning with EFP1 are displayed.

- To view all available Ethernet services, choose **Show All** and click **Go**.

The available elements that meet the specified search criteria are displayed in the Add Ethernet Service dialog box in table format. The dialog box also displays the date and time at which the list was generated. To update the list, click **Refresh**.

Note If an element is not included in your scope, it is displayed with the locked device icon.

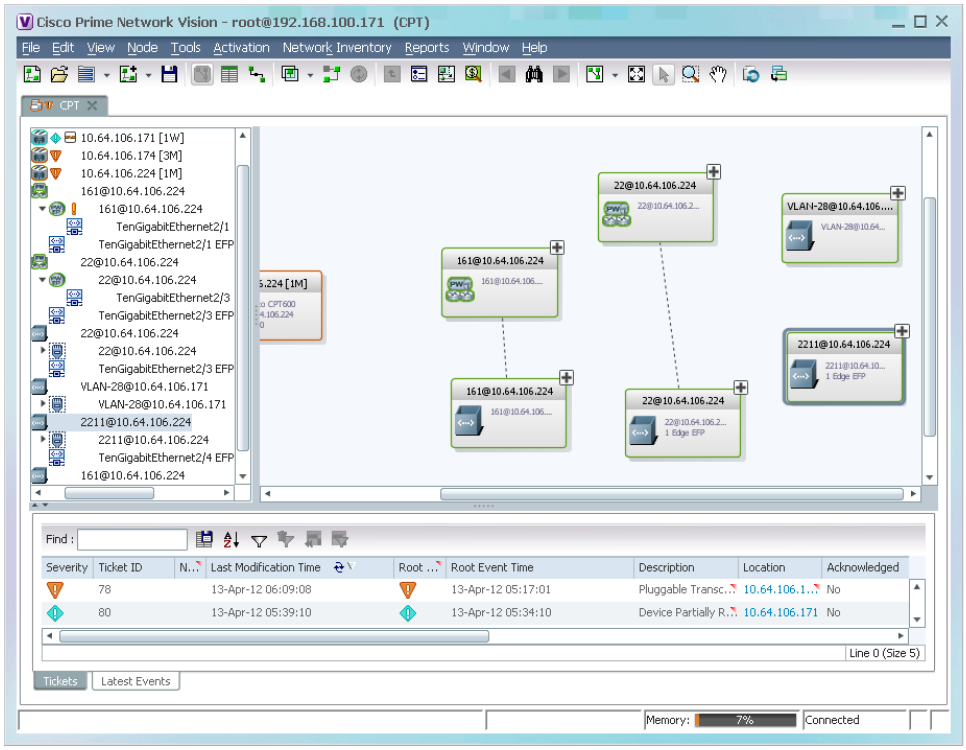
For information about sorting and filtering the table contents, see Filtering and Sorting Tabular Content, page 2-42.

Step 4 In the Add Ethernet Service dialog box, select the elements that you want to add. You can select and add multiple elements by pressing **Ctrl** while selecting individual elements or by pressing **Ctrl +Shift** to select a group of elements.

Step 5 Click **OK**.

The Ethernet service is displayed in the navigation pane and in the content area. In addition, any associated tickets are displayed in the ticket pane. See Figure 12-67.

Figure 12-67 Ethernet Service in Prime Network Vision



The Ethernet service information is saved with the map in the Prime Network database.

Applying Ethernet Service Overlays

An Ethernet service overlay allows you to isolate the parts of a network that are being used by a specific Ethernet service.

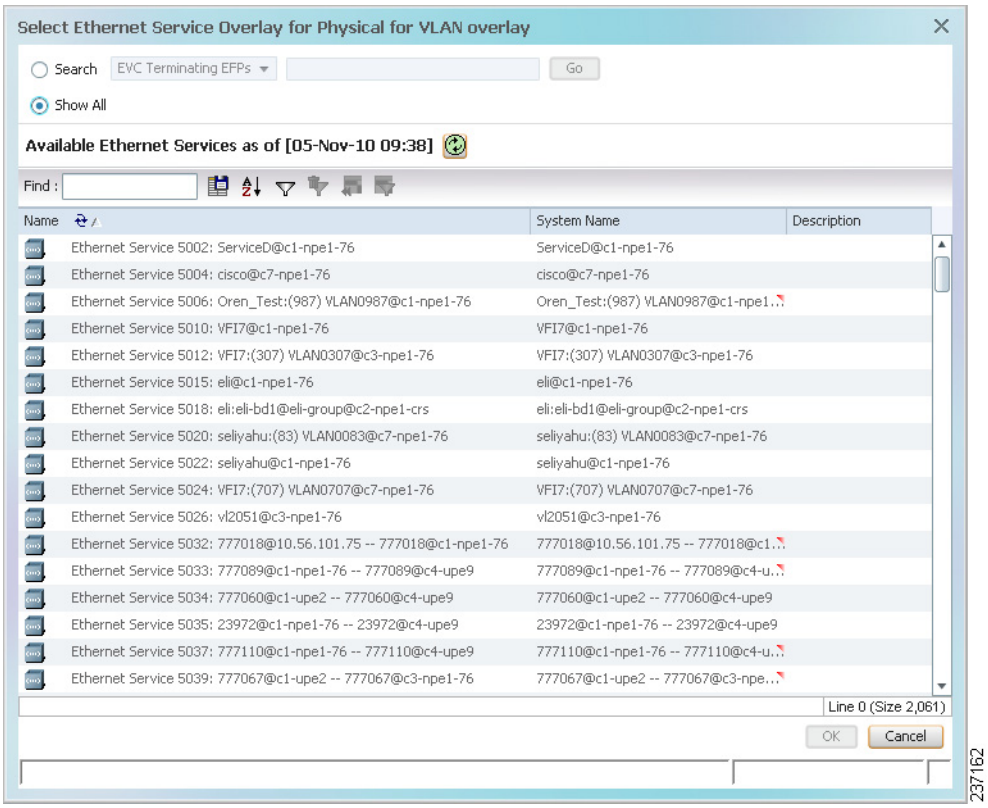
To apply an Ethernet service overlay:

Step 1 In Prime Network Vision, choose the map in which you want to apply an overlay.

Step 2 From the toolbar, choose **Choose Overlay Type > Ethernet Service**.

Figure 12-68 shows an example of the Select Ethernet Service Overlay for *map* dialog box.

Figure 12-68 Select Ethernet Service Overlay Dialog Box

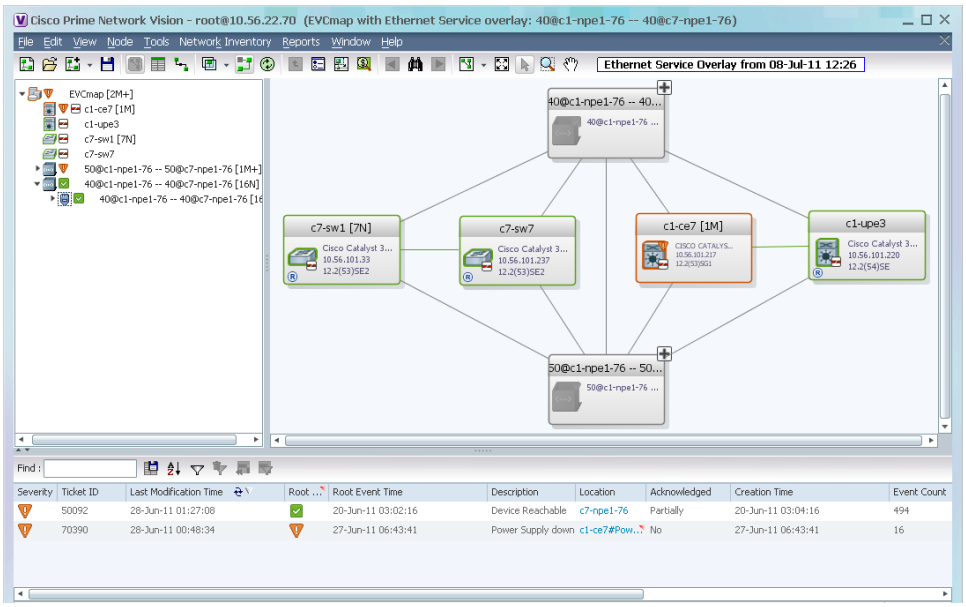


Step 3 Select the required Ethernet Service for the overlay.

Step 4 Click **OK**.

The elements being used by the selected Ethernet service are highlighted in the map while the other elements are dimmed, as shown in Figure 12-69.

Figure 12-69 Ethernet Service Overlay in Prime Network Vision



Step 5 To hide and view the overlay, click **Hide Overlay/Show Overlay** in the toolbar. The button toggles depending on whether the overlay is currently displayed or hidden.

Step 6 To remove the overlay, choose **Choose Overlay Type > None**.

Viewing Ethernet Service Properties

To view Ethernet service properties:

Step 1 In Prime Network Vision, select the map containing the required Ethernet service.

Step 2 In the navigation or map pane, right-click the Ethernet service and choose **Properties**.

Figure 12-70 shows an example of an Ethernet Service Properties window with the EVC Terminating table. Depending on the types of service in the EVC, tabs might be displayed. For example, if the EVC contains two network VLANs and a VPLS, tabs are displayed for the following:

- EVC Terminating table
- Network VLANs
- VPLS

Figure 12-70 Ethernet Service Properties Window

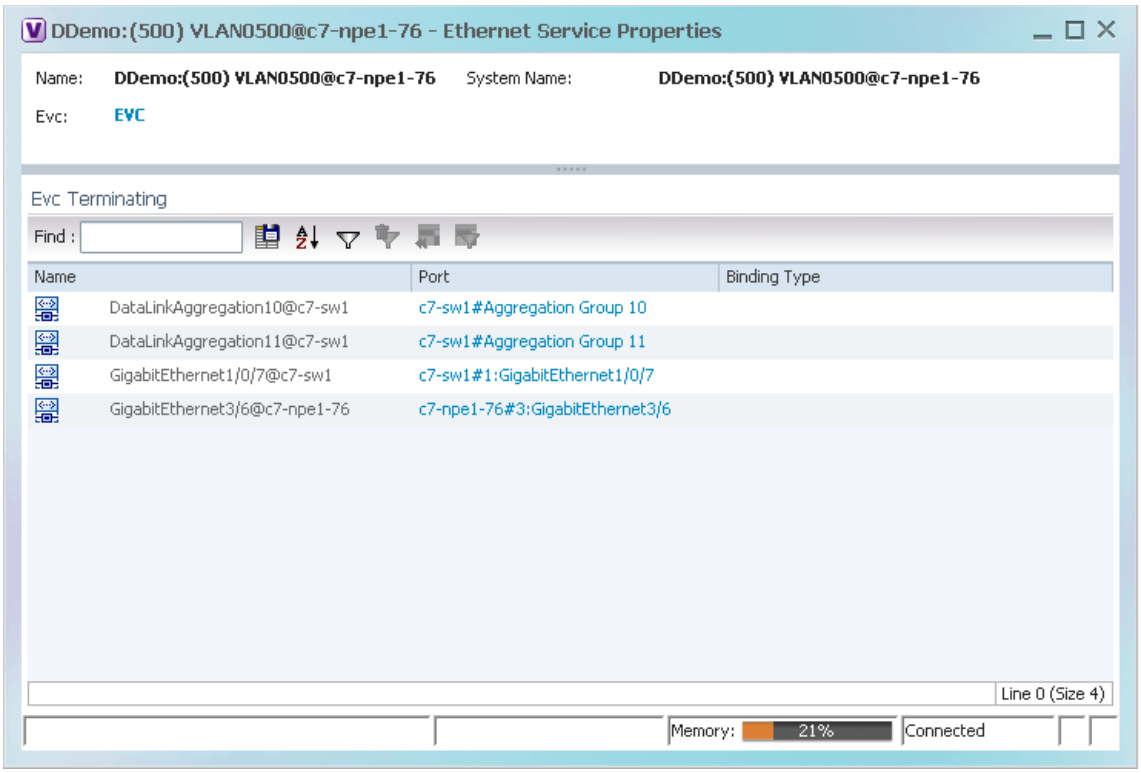


Table 12-44 describes the information that is displayed for an Ethernet service.

Table 12-44 Ethernet Service Properties Window

Field	Description
Name	Ethernet service name.
System Name	Name that Prime Network Vision assigns to the Ethernet service.
EVC	Name of the EVC associated with the Ethernet service, hyperlinked to the EVC Properties window.
EVC Terminating Table	
Name	EVC name, represented by the interface name, EFP, and the EFP name.
Network Element	Hyperlinked entry to the specific interface and EFP in physical inventory.
Port	Hyperlinked entry to the specific interface in physical inventory.

Step 3 To view the EVC Properties window, click the hyperlink in the EVC field.

Figure 12-71 shows an example of the EVC Properties window.

Figure 12-71 EVC Properties Window

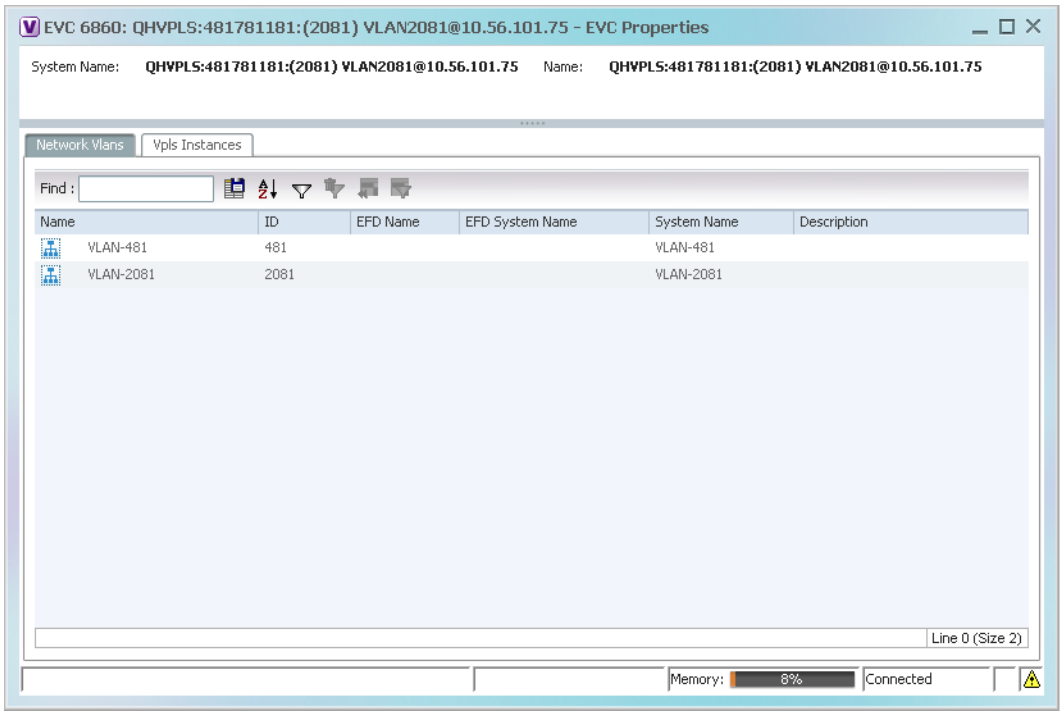


Table 12-45 describes the information that is displayed in the EVC Properties window. The tabs that are displayed depend on the services included in the EVC. For example, if the EVC contains two network VLANs and a VPLS, tabs are displayed for the following:

- EVC Terminating table
- Network VLANs
- VPLS

Table 12-45 EVC Properties Window

Field	Description
System Name	Name of the system on which the EVC is configured.
Name	EVC name.
Cross-Connects Table	
Name	Cross-connect name.
Segment 1	Identifier of the first cross-connect endpoint.
Segment 2	Identifier of the second cross-connect endpoint.
System Name	Cross-connect system name.

Table 12-45 EVC Properties Window (continued)

Field	Description
Network VLANs Tab	
Name	VLAN name.
ID	VLAN identifier.
EFD Name	Name of the Ethernet flow domain.
EFD System Name	Name that Prime Network Vision assigns to the EFD.
System Name	VLAN system name.
Description	Brief description of the VLAN.
Network Pseudowires Tab	
Name	Pseudowire name.
System Name	System on which the pseudowire is configured.
Description	Brief description of the pseudowire.
Pseudowire Type	Type of pseudowire.
Is Multisegment Pseudowire	Whether or not the pseudowire is multisegment: True or False.
VPLS Instances Tab	
Name	VPLS instance name.
System Defined Name	Name that Prime Network Vision assigns to the VPLS instance.
VPN ID	Identifier of associated VPN.

Viewing IP SLA Responder Service Properties

Cisco IOS Service Level Agreements (SLAs) software allows you to analyze IP service levels for IP applications and services by using active traffic monitoring to measure network performance.

The IP SLA responder is a component embedded in the destination Cisco device that allows the system to anticipate and respond to IP SLAs request packets. The responder provides accurate measurements without requiring dedicated probes. The responder uses the Cisco IOS IP SLAs Control Protocol to provide a mechanism through which it can be notified on which port it should listen and respond.

Two-Way Active Measurement Protocol (TWAMP) defines a standard for measuring round-trip network performance between any two devices that support the protocol.

Prime Network Vision supports IP SLA Responder service on the following devices:

- Cisco 3400ME and 3750ME devices running Cisco IOS 12.2(52)SE.
- Cisco MWR2941 devices running Cisco CSR 3.2.

To view IP SLA Responder service properties:

Step 1 In Prime Network Vision, double-click the device configured for IP SLA Responder service.

Step 2 In the inventory window, choose **Logical Inventory > IP SLA Responder**.

IP SLA Responder properties are displayed as shown in Figure 12-72.

Figure 12-72 IP SLA Responder in Logical Inventory

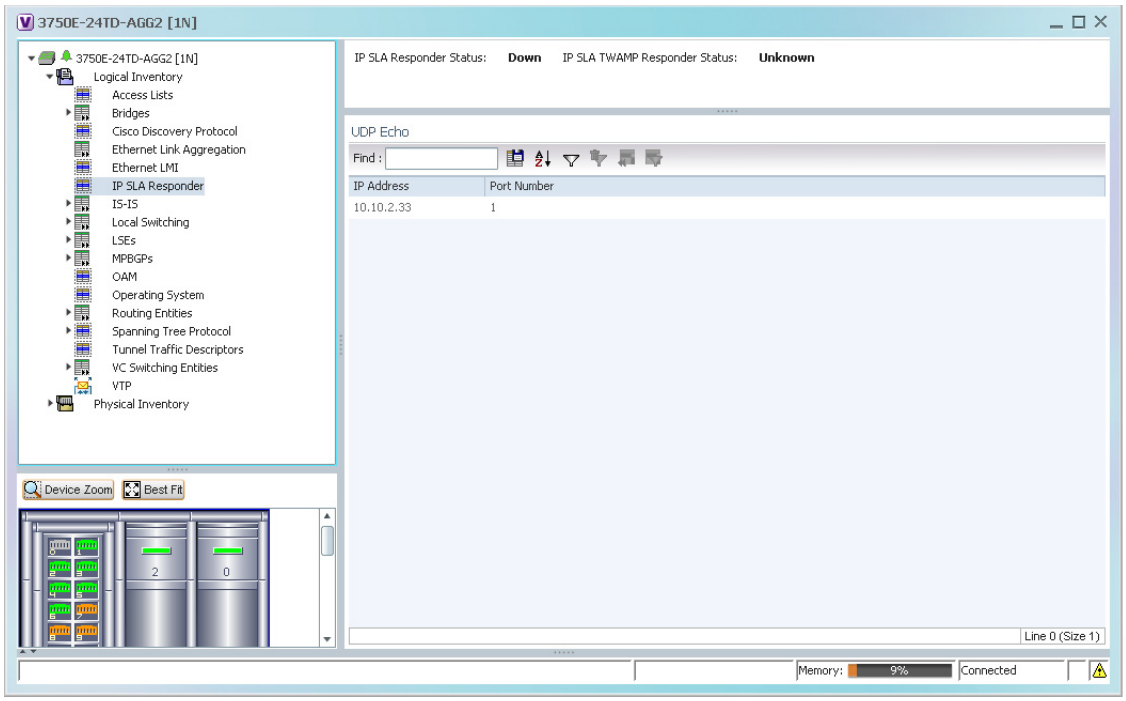


Table 12-46 describes the properties displayed for IP SLA Responder service.

Table 12-46 IP SLA Responder Properties in Logical Inventory

Field	Description
IP SLA Responder Status	Status of the IP SLA Responder: Up or Down.
IP SLA TWAMP Responder Status	Status of the IP SLA TWAMP responder: Up or Down.
UDP Echo Tab	
IP Address	Destination IP address used for the UDP echo operation.
Port Number	Destination port number used for the UDP echo operation.
TCP Connect Tab	
IP Address	Destination IP address used for the TCP connect operation.
Port Number	Destination port number used for the TCP connect operation.

Viewing IS-IS Properties

Intermediate System-to-Intermediate System (IS-IS) protocol is a routing protocol developed by the ISO. It is a link-state protocol where IS routers exchange routing information based on a single metric to determine network topology. It behaves in a manner similar to OSPF in the TCP/IP network.

IS-IS networks contain end systems, intermediate systems, areas, and domains. End systems are user devices. Intermediate systems are routers. Routers are organized into local groups called areas, and areas are grouped into a domain. For configuring IS-IS, see Configuring IS-IS, page 12-121.

To view IS-IS properties:

Step 1 In Prime Network Vision, double-click the device configured for IS-IS.

Step 2 In the inventory window, choose **Logical Inventory > IS-IS > System**.

Figure 12-73 shows an example of the IS-IS window with the Process table in logical inventory.

Figure 12-73 IS-IS Window in Logical Inventory

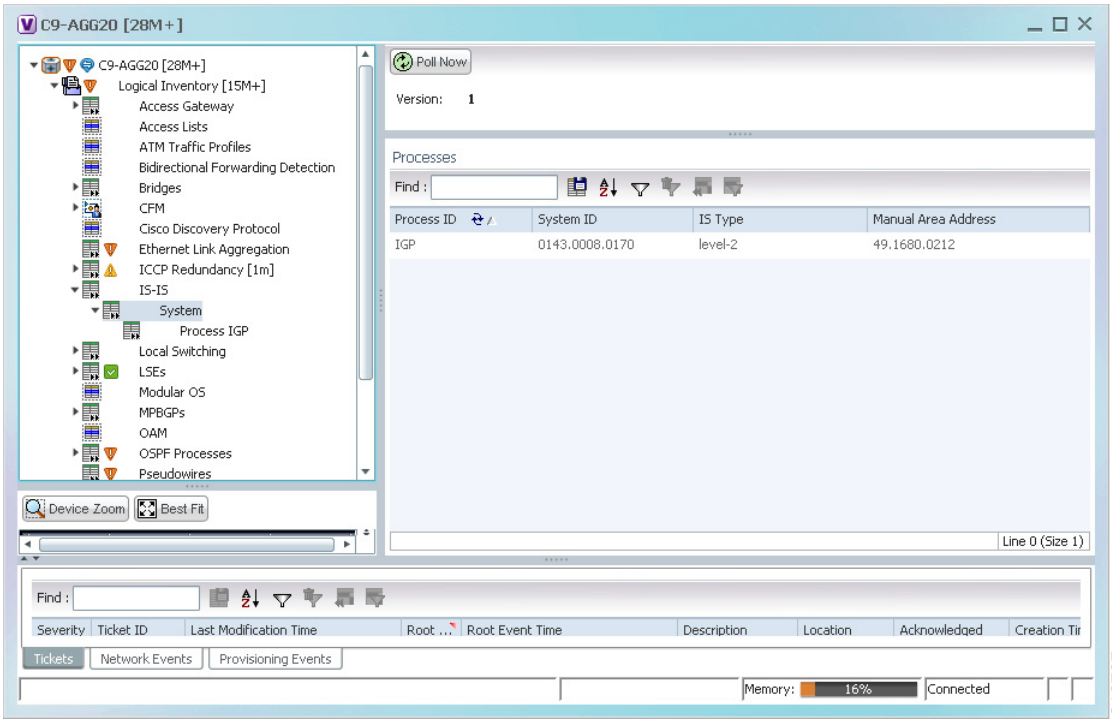


Table 12-47 describes the information that is displayed in this window and the Processes table.

Table 12-47 IS-IS Properties in Logical Inventory - Processes Table

Field	Description
Version	Version of IS-IS that is implemented.
Processes Table	
Process ID	Identifier for the IS-IS process.
System ID	Identifier for this Intermediate System.
IS Type	Level at which the Intermediate System is running: Level 1, Level 2, or Level 1-2.
Manual Area Address	Address assigned to the area.

Step 3 To view IS-IS process information, choose **Logical Inventory > IS-IS > Process** *nnn*.

Figure 12-74 shows an example of the information that is displayed for the IS-IS process.

Figure 12-74 IS-IS Process Properties in Logical Inventory

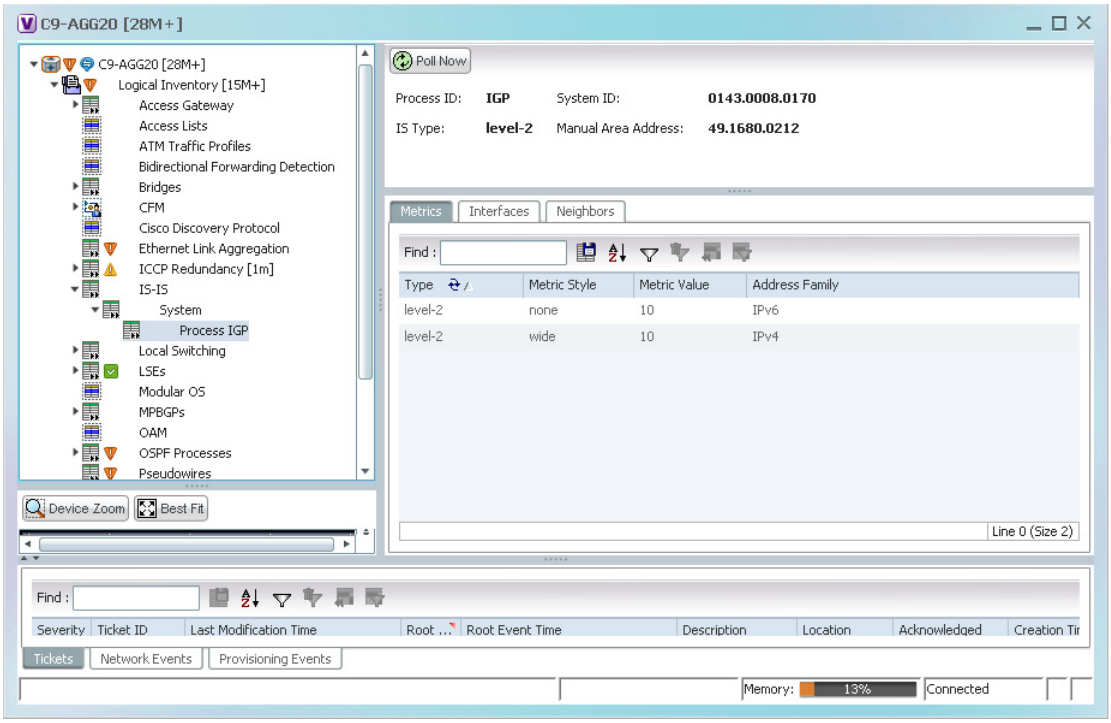


Table 12-48 describes the information that is displayed for the selected IS-IS process.

Table 12-48 IS-IS Process Properties in Logical Inventory

Field	Description
Process	Unique identifier for the IS-IS process.
System ID	Identifier for this Intermediate System.
IS Type	Level at which the Intermediate System process is running: Level 1, Level 2, or Level 1-2.
Manual Area Address	Address assigned to the area.
Metrics Tab	
IS Type	Level at which the Intermediate System is running: Level 1, Level 2, or Level 1-2.
Metric Style	Metric style used: Narrow, Transient, or Wide.
Metric Value	Metric value assigned to the link. This value is used to calculate the path cost via the links to destinations. This value is available for Level 1 or Level 2 routing only. If the metric style is Wide, the value can range from 1 to 16777214. If the metric style is Narrow, the value can range from 1 to 63. The default value for active IS-IS interfaces is 10, and the default value for inactive IS-IS interfaces is 0.
Address Family	IP address type used: IPv4 or IPv6.
Interfaces Tab	
Interface Name	Interface name.
Neighbors Tab	
System ID	Identifier for the neighbor system.
Interface	Neighbor interface name.
IP Address	Neighbor IP address.
Type	IS type for the neighbor: Level 1, Level 2, or Level 1-2.
SNPA	Subnetwork point of attachment (SNPA) for the neighbor.
Hold Time	Holding time, in seconds, for this adjacency. The value is based on received IS-to-IS Hello (IIH) PDUs and the elapsed time since receipt.
State	Administrative status of the neighbor system: Up or Down.
Address Family	IP address type used by the neighbor: IPv4 or IPv6.

Viewing OSPF Properties

Prime Network Vision supports the following versions of OSPF:

- OSPFv1
- OSPFv2
- OSPFv3

Using Prime Network Vision you can view OSPF properties for:

- OSPF processes, including the process identifier and OSPF version.
- OSPF network interfaces, such as the area identifier, network type, and status.
- OSPF neighbors, including the neighbor identifier, neighbor interface address, and status.

To view OSPF properties:

Step 1 In Prime Network Vision, double-click the device configured for OSPF.

Step 2 To view OSPF processes, choose **Logical Inventory > OSPF Processes > OSPF Process (v*n*)** *ID* where **v***n* represents the OSPF version and *ID* is the OSPF process identifier.

For example, in Figure 12-75, the entry in the navigation tree is OSPF Process (v2) 10.

Figure 12-75 OSPF Processes in Logical Inventory

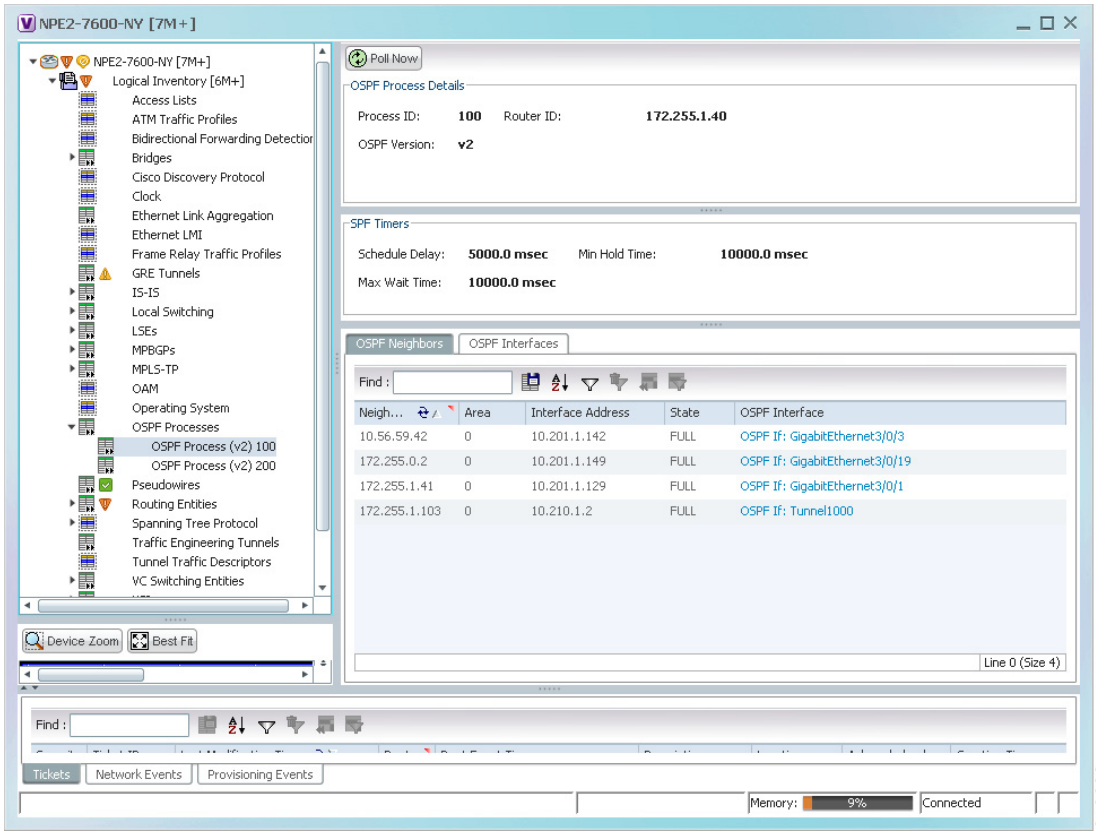


Table 12-49 describes the information that is displayed for OSPF processes.

Table 12-49 OSPF Processes in Logical Inventory

Field	Description
OSPF Process Details	
Process ID	Unique process identifier.
Router ID	Router IP address.
OSPF Version	OSPF version: v1, v2, or v3.
SPF Timers	
Schedule Delay	Number of milliseconds to wait after a change before calculating the shortest path first (SPF).
Min Hold Time	Minimum number of milliseconds to wait between two consecutive SPF calculations.
Max Wait Time	Maximum number of milliseconds to wait between two consecutive SPF calculations.
OSPF Neighbors Table	
Neighbor ID	OSPF neighbor IP address.
Area	OSPF area identifier.
Interface Address	IP address of the interface on the neighbor configured for OSPF.
State	State of the communication with the neighbor: Down, Attempt, Init, 2-Way, Exstart, Exchange, Loading, and Full.
OSPF Interface	Hyperlinked entry to the OSPF Interface Properties window. The OSPF Interfaces window displays the same information as the OSPF Interfaces Table below.
OSPF Interfaces Table	
IP Interface	OSPF interface, hyperlinked to the relevant entry in the routing entity IP Interfaces table in logical inventory. For more information about the IP Interfaces table, see Table 18-12.
Internet Address	OSPF interface IP address.
Area ID	OSPF area identifier.
Priority	Eight-bit unsigned integer that specifies the priority of the interface. Values range from 0 to 255. Of two routers, the one with the higher priority takes precedence.
Cost	Specified cost of sending a packet on the interface, expressed as a metric. Values range from 1 to 65535.
Status	State of the interface: Up or Down.
State	OSPF state: BDR, DR, DR-Other, Waiting, Point-to-Point, or Point-to-Multipoint.
Network Type	Type of OSPF network: Broadcast, Nonbroadcast Multiple Access (NBMA), Point-to-Multipoint, Point-to-Point, or Loopback.
DR Address	Designated router IP address.
BDR Address	Backup designated router IP address.

Configuring REP and mLACP

The following commands can be launched from the inventory by right-clicking the appropriate node and selecting **Commands.** Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. For details on the software versions Prime Network supports for these network elements, see the *Cisco Prime Network 4.0 Supported Cisco VNEs*. To run the REP and mLACP commands, the software on the network element must support these technology.

Additional commands may be available for your devices. New commands are often provided in Prime Network Device Packages, which can be downloaded from the Prime Network software download site. For more information on how to download and install DPs and enable new commands, see the information on "Adding Additional Device (VNE) support" in the *Cisco Prime Network 4.0 Administrator Guide*.

Note You might be prompted to enter your device access credentials while executing a command. Once you have entered them, these credentials will be used for every subsequent execution of a command in the same GUI client session. If you want to change the credentials, click **Edit Credentials**. The Edit Credentials button will not be available for SNMP commands or if the command is scheduled for a later time.

Command	Navigation	Description
REP Command		
Show REP Segment Information	**Commands > Show**	This action performed at the command the launch point.
mLACP Commands		
Show Group **Show MPLS LDP** **Show Channel** **Show LACP Internal**	**Commands > Show**	These actions are performed at the command the launch point.

Using Pseudowire Ping and Show Commands

The **Ping Pseudowire** and **Display Pseudowire** commands can be launched from the inventory by right-clicking the appropriate node and selecting **Commands.** Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands.

Additional commands may be available for your devices. New commands are often provided in Prime Network Device Packages, which can be downloaded from the Prime Network software download site. For more information on how to download and install DPs and enable new commands, see the information on "Adding Additional Device (VNE) support" in the *Cisco Prime Network 4.0 Administrator Guide*.

Note You might be prompted to enter your device access credentials while executing a command. Once you have entered them, these credentials will be used for every subsequent execution of a command in the same GUI client session. If you want to change the credentials, click **Edit Credentials**. The Edit Credentials button will not be available for SNMP commands or if the command is scheduled for a later time.

Command	Navigation	Description
Ping Pseudowire	**Logical Inventory** > **Pseudowires** > right-click the interface > **Commands** > **Configure** >	Use the **Ping Pseudowire** command to ping the peer router with a tunnel ID from a single or multisegment pseudowire. This command can be used to verify connectivity between any set of PE routers in the pseudowire path. For a multisegment pseudowire this command can be used to verify that all the segments of the multisegment pseudowire are operating. You can use this command to verify connectivity at the following pseudowire points: • From one end of the pseudowire to the other • From one of the pseudowires to a specific segment • The segment between two adjacent PE routers You can choose to ping the peer router by default or provide the IP of the required destination router to ping.
Display Pseudowire	**Logical Inventory** > **Pseudowire** > right-click the required interface > **Commands** > **Show** > **Display Pseudowire**	Use the Display Pseudowire command to show the MPLS Layer 2 (L2) transport binding using tunnel identifier. MPLS L2 transport binding allows you to identify the VC label binding information. This command can be used to display information about the pseudowire switching point.

Configuring IS-IS

In order to enable IS-IS for IP on a Cisco router and have it exchange routing information with other IS-IS enabled routers, you must perform these two tasks:

- Enable the IS-IS process and assign area
- Enable IS-IS for IP routing on an interface

You can configure the router to act as a Level 1 (intra-area) router, as Level 1-2 (both a Level 1 router and a Level 2 router), or as Level 2 (an inter-area router only).

The IS-IS commands helps you to configure the IS-IS on a Cisco router. These commands can be launched from the logical inventory. Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands.

The table below lists the IS-IS configuration commands. To run the ISIS commands, the software on the network element must support ISIS technology. For details on the software versions Prime Network supports for the ISIS supported network elements, see the *Cisco Prime Network 4.0 Supported Cisco VNEs*.

Additional commands may be available for your devices. New commands are often provided in Prime Network Device Packages, which can be downloaded from the Prime Network software download site. For more information on how to download and install DPs and enable new commands, see the information on "Adding Additional Device (VNE) support" in the *Cisco Prime Network 4.0 Administrator Guide*.

Note You might be prompted to enter your device access credentials while executing a command. Once you have entered them, these credentials will be used for every subsequent execution of a command in the same GUI client session. If you want to change the credentials, click **Edit Credentials**. The Edit Credentials button will not be available for SNMP commands or if the command is scheduled for a later time.

Command	Navigation	Description
Create ISIS Router	**ISIS** > *right-click System* > **Commands** > **Configuration**	Use this command to create an IS-IS routing process and specify the area for each instance of the IS-IS routing process. An appropriate Network Entity Title (NET) must be configured to specify the area address for the IS-IS area and system ID of the router. Multiple IS-IS processes can be configured. Up to eight processes are configurable. A maximum of five IS-IS instances on a system are supported.
Modify ISIS Router **Delete ISIS Router**	**ISIS** > **System** > *right-click Process ID in content pane* > **Commands** > **Configuration** >	Use this command to modify or delete an exisiting IS-IS routing configuration for the specified routing process.

Command	Navigation	Description
Create ISIS Interface	**ISIS > System >** *right-click Process ID in content pane* **> Commands > Configuration >**	Use these command to create or modify an IS-IS routing process and assign it to a specific interface, rather than to a network.
Modify ISIS Interface **Delete ISIS Interface**	**ISIS >** *expand* **System >** *select a Process* **>** *select* **Interfaces** *tab***>** *right-click on a Interface Name* **> Commands > Configuration >**	
Create ISIS Address Family **Modify ISIS Address Family** **Delete ISIS Address Family**	**ISIS > System >** *right-click Process ID in content pane* **> Commands > Configuration**	Configure or modify IS-IS routing to use standard IP Version 4 (IPv4) and IP Version 6 (IPv6) address prefixes.
Create ISIS Interface Address Family **Modify ISIS Interface Address Family** **Delete ISIS Interface Address Family**	**ISIS >** expand **System >** *select a Process* **>** *select* **Interfaces** *tab***>** *right-click on a Interface Name* **> Commands > Configuration >**	Configure IS-IS routing to use standard IP Version 4 (IPv4) and IP Version 6 (IPv6) address prefixes on an interface.
Show ISIS Configuration	**ISIS >** *right-click* **System > Commands > Show**	The **show isis** command displays general information about an IS-IS instance and protocol operation.