



Managing Carrier Ethernet Configurations

The following topics describe how you can use the Vision client to monitor Carrier Ethernet services. If you cannot perform an operation that is described in these topics, you may not have sufficient permissions; see [Permissions for Managing Carrier Ethernet](#), page B-12.

- [Viewing CDP Properties](#), page 18-2
- [Viewing Link Layer Discovery Protocol Properties](#), page 18-3
- [Viewing Spanning Tree Protocol Properties](#), page 18-5
- [Viewing Resilient Ethernet Protocol Properties \(REP\)](#), page 18-9
- [Viewing HSRP Properties](#), page 18-13
- [Viewing Access Gateway Properties](#), page 18-14
- [Working with Ethernet Link Aggregation Groups](#), page 18-17
- [Viewing mLACP Properties](#), page 18-24
- [Monitoring Provider Backbone Bridges](#), page 18-27
- [Monitoring PBB-based Support Service Discovery](#), page 18-47
- [Viewing EFP Properties](#), page 18-51
- [Connecting a Network Element to an EFP](#), page 18-54
- [Understanding EFP Severity and Ticket Badges](#), page 18-55
- [Viewing EVC Service Properties](#), page 18-56
- [Viewing and Renaming Ethernet Flow Domains](#), page 18-60
- [Working with VLANs](#), page 18-62
- [Working with VXLANs](#), page 18-90
- [Understanding Unassociated Bridges](#), page 18-92
- [Working with Ethernet Flow Point Cross-Connects](#), page 18-94
- [Working with VPLS and H-VPLS Instances](#), page 18-96
- [Working with Pseudowires](#), page 18-107
- [Working with Ethernet Services](#), page 18-124
- [Viewing IP SLA Responder Service Properties](#), page 18-131
- [Viewing IS-IS Properties](#), page 18-132
- [Viewing OSPF Properties](#), page 18-135

- [Monitoring the CPT 50 Ring Support, page 18-140](#)
- [Configuring REP and mLACP, page 18-149](#)
- [Viewing the Remote Loop Free Alternate Configurations, page 18-150](#)
- [Using Pseudowire Ping and Show Commands, page 18-155](#)
- [Configuring IS-IS, page 18-156](#)

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 the Vision client, 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 18-1](#).

Figure 18-1 CDP in Logical Inventory

Local Port	Local Port ID	Remote Device ID	Remote Port ID	Remote IP Address
NPE1-9K-FL#0:GigabitEthernet0/0/29	GigabitEthernet0/0/29	AGG1-6524ME-FL	GigabitEthernet1/32	10.204.55.24
NPE1-9K-FL#0:GigabitEthernet0/0/30	GigabitEthernet0/0/30	CRS1-1-FL.Cisc.com	GigabitEthernet0/4/2/2	10.204.2.1
NPE1-9K-FL#0:GigabitEthernet0/0/38	GigabitEthernet0/0/38	GSR1-10X-FL	GigabitEthernet0/2/1/0	10.204.2.18
NPE1-9K-FL#0:GigabitEthernet0/0/39	GigabitEthernet0/0/39	NPE2-7600-FL	GigabitEthernet4/10	10.204.2.9
NPE1-9K-FL#1:GigabitEthernet0/1/0/37	GigabitEthernet0/1/0/37	NPE2-7600-FL	GigabitEthernet4/7	10.220.1.10
NPE1-9K-FL#1:GigabitEthernet0/1/0/39	GigabitEthernet0/1/0/39	CRS1-1-FL.Cisc.com	GigabitEthernet0/4/0/0	10.56.59.30

[Table 18-1](#) describes the CDP instance properties that are displayed.

Table 18-1 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 the Vision client, 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 Vision client 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.

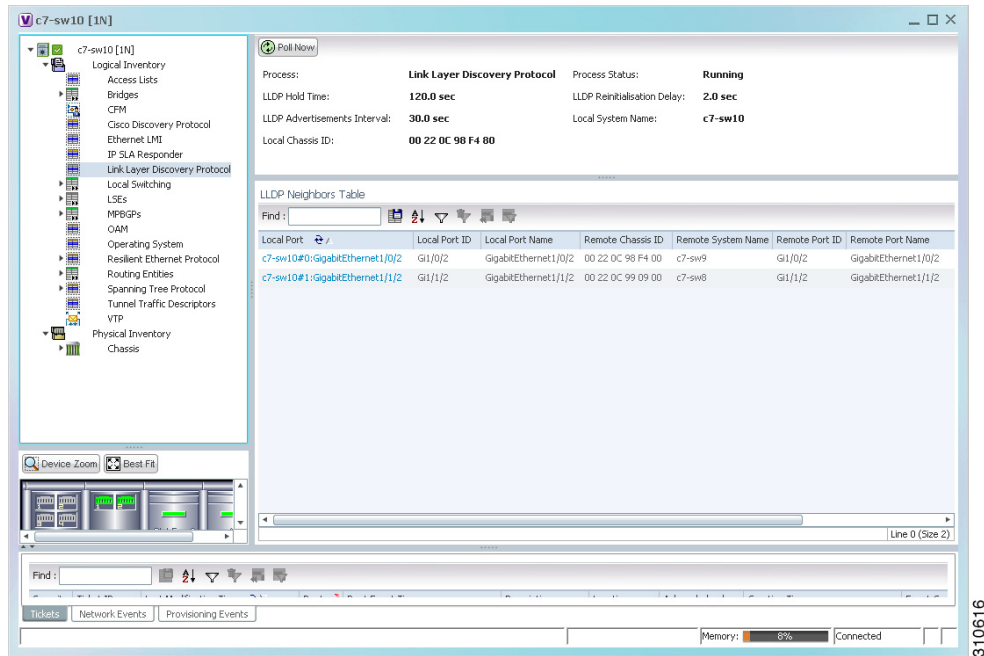
In Logical Inventory

To view LLDP properties:

-
- Step 1** In the Vision client, 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 18-2](#).

Figure 18-2 LLDP in Logical Inventory



[Table 18-2](#) describes the properties that are displayed for LLDP.

Table 18-2 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 18-2 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 the Vision client, 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 Vision client content pane:
- Discovery Protocol Type—LLDP
 - Info—Tx (Enabled or Disabled), Rx (Enabled or Disabled).



Note If the LLDP transmit is disabled on the interface using CLI and you click the Poll Now button, the LLDP **Info-Tx** field is 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 the Vision client, 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 18-3](#).

Figure 18-3 STP in Logical Inventory

Table 18-3 describes the properties that are displayed for STP.

Table 18-3 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.
STP Instance Info Table	
STP Instance ID	STP instance name.
VLAN ID	VLAN identifiers.
Bridge Priority	Bridge priority.

Table 18-3 STP Properties (continued)

Field	Description
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 18-4](#) describes the information that is displayed in the STP Instance Information Properties window.

Table 18-4 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).
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.

Table 18-4 STP Instance Information Properties (continued)

Field	Description
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 18-5](#) describes the information that is displayed for MSTP.

Table 18-5 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 18-83.
- VLAN service link properties—See [Viewing STP Properties for VLAN Service Links](#), page 18-84.

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.

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 Vision client map. The REP port role is displayed as a tool-tip between the REP enabled trunk ports in the Ethernet links. Using the Vision client, 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 the Vision client, double-click the device configured for REP.

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

[Figure 18-4](#) shows an example of REP in logical inventory.

Figure 18-4 REP in Logical Inventory

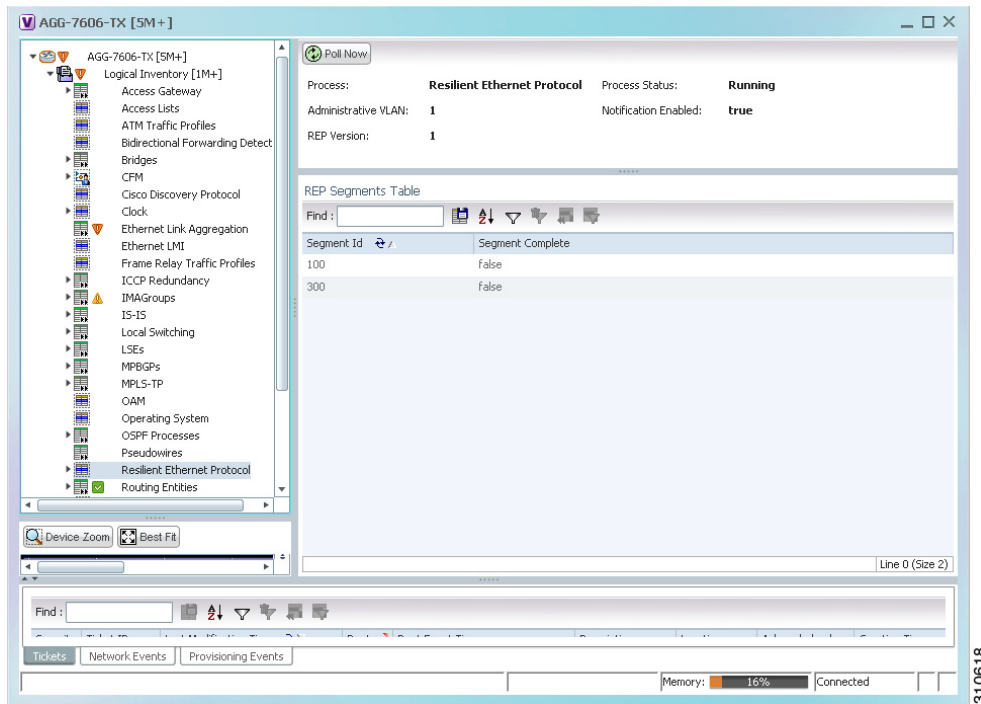


Table 18-6 describes the information that is displayed for REP.

Table 18-6 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 18-5 shows an example of REP segment properties in logical inventory.

Figure 18-5 REP Segment Properties

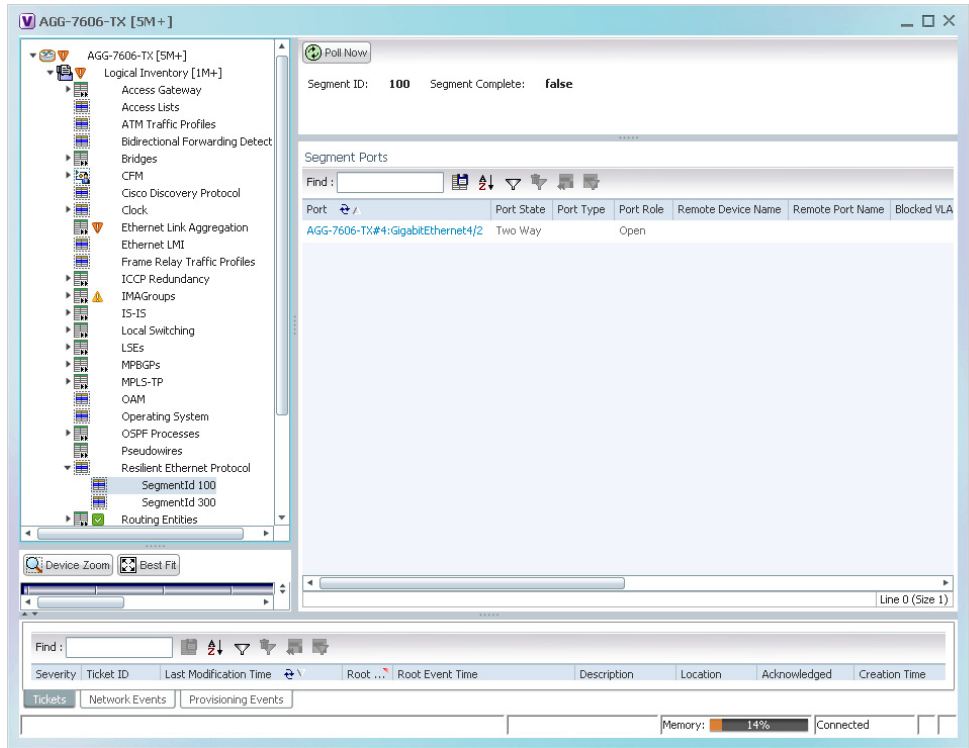


Table 18-7 describes the information that is displayed for REP segments.

Table 18-7 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 18-80](#).
- VLAN service link properties—See [Viewing REP Properties for VLAN Service Links, page 18-81](#).

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 the Vision client.
- Step 2** In logical inventory, choose **Logical Inventory > Routing Entities > Routing Entity**.
- Step 3** In the IP Interfaces tab, double-click the required interface to view the IP interface properties. If HSRP is configured on the IP interface, the HSRP Group tab is displayed as shown in [Figure 18-6](#).

Figure 18-6 HSRP Group Information

The screenshot shows the Cisco Prime Network 5.2 Vision client interface. On the left is a tree view of the Logical Inventory, showing the path: Logical Inventory [134] > Compute Virtualization > Virtual DataCenter - Bangalore Datacenter-1 > Data Stores > Host Clusters > Host Servers > Virtual DataCenter - Bangalore Datacenter-2 > Data Stores > Host Clusters > NMTG-PRIME-CLUSTER > Host Servers > 10.105.172.233 (Hypervisor) > 10.105.172.140 (Hypervisor) > 10.105.172.160 (Hypervisor) > 10.105.172.162 (Hypervisor) > 10.105.172.200 (Hypervisor) > 10.105.172.232 (Hypervisor) > 10.105.172.233 (Hypervisor) > Virtual Machines (All Datacenters) > Routing Entities > Physical Entities.

The main pane shows the HSRP Group Information for the IP interface 10.105.172.233. The configuration details are as follows:

Name:	10.105.172.233	IP Address:	10.105.172.233
DNS Name:	nmtg-dell-esvi	State:	Connected
EVC Mode:	Disabled	vMotion Enabled:	false
Fault Tolerance Enabled:	false	Fault Tolerance Version:	2.0.1-3.0.0-3.0.0
MAC Address:	00 1E 4F 3A 25 85	System Up Time:	18-Mar-13 12:19:49
UUID:	44454c4c-3600-104e-804d-c3c04f563153	Hardware Model:	PowerEdge 2950
Vendor:	Dell Inc.		

Below the configuration details, there are tabs for Hypervisor, Processor, Statistics, CPU Allocation, and Memory Allocation. The Processor tab is selected, showing the following information:

Name:	Intel(R) Xeon(R) CPU	Description:	Intel(R) Xeon(R) CPU E5405 @ 2.00GHz
CPU:	1	Cores Per CPU:	4
Rated Speed:	1.99 GHz	Used Speed:	0.04 GHz (0 %)
HyperThreading Enabled:	false	RAM Size:	7.99 GB

At the bottom, there is a table for Virtual Machines:

Resource Pool	Provider Name	Status	Root Pool
host-pool-prnt	10.105.172.233	Normal	false
test-parent1	10.105.172.233	Normal	false

At the very bottom, there is a table for Tickets:

Severity	Ticket ID	Last Modification Time	Root	Root Event Time	Description	Location	Element Type	Acknow
Warning	20002	14-May-13 18:08:34	Warning	14-May-13 18:06:26	Virtual machine memory usage crossed threshold	BLR-VCenter#migration-test-vm-123	VMware vCenter Server	No
Warning	20001	14-May-13 18:08:34	Warning	14-May-13 18:06:26	Virtual machine cpu usage crossed threshold	BLR-VCenter#migration-test-vm-123	VMware vCenter Server	No
Warning	10003	14-May-13 18:06:26	Warning	14-May-13 18:06:26	VM Powered Off	BLR-VCenter#migration-test-vm-123	VMware vCenter Server	No

Table 18-8 describes the information in the HSRP Group tab.

Table 18-8 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 partner 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 18-7](#) shows an example of an access gateway entry in logical inventory.

Figure 18-7 Access Gateway in Logical Inventory

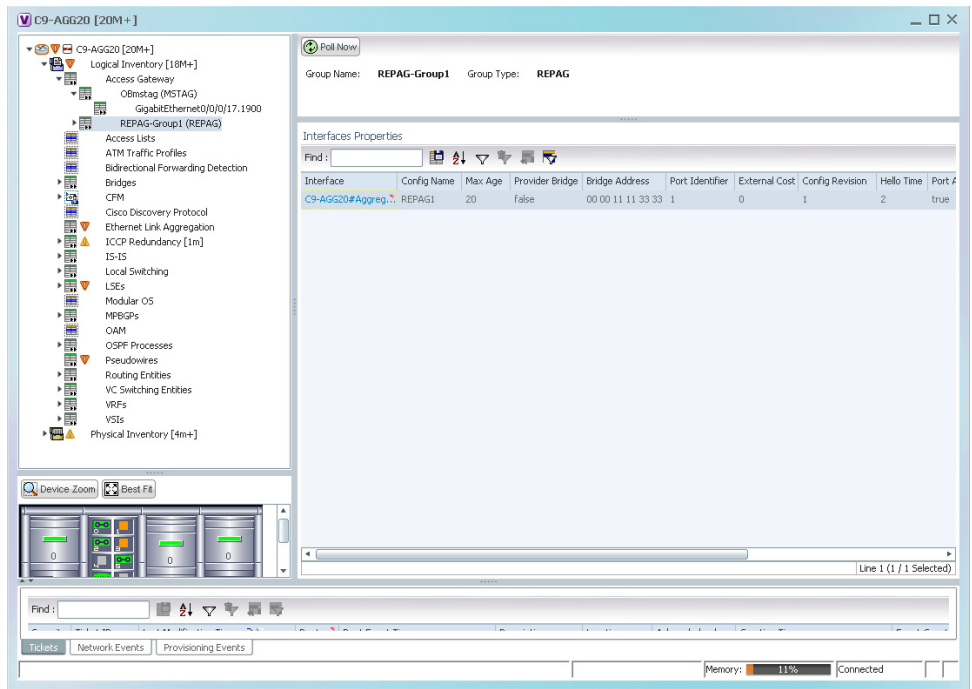


Table 18-9 describes the information that is displayed for an access gateway.

Table 18-9 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.

Table 18-9 Access Gateway Properties in Logical Inventory (continued)

Field	Description
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 18-8 shows an example of the information displayed for an access gateway instance.

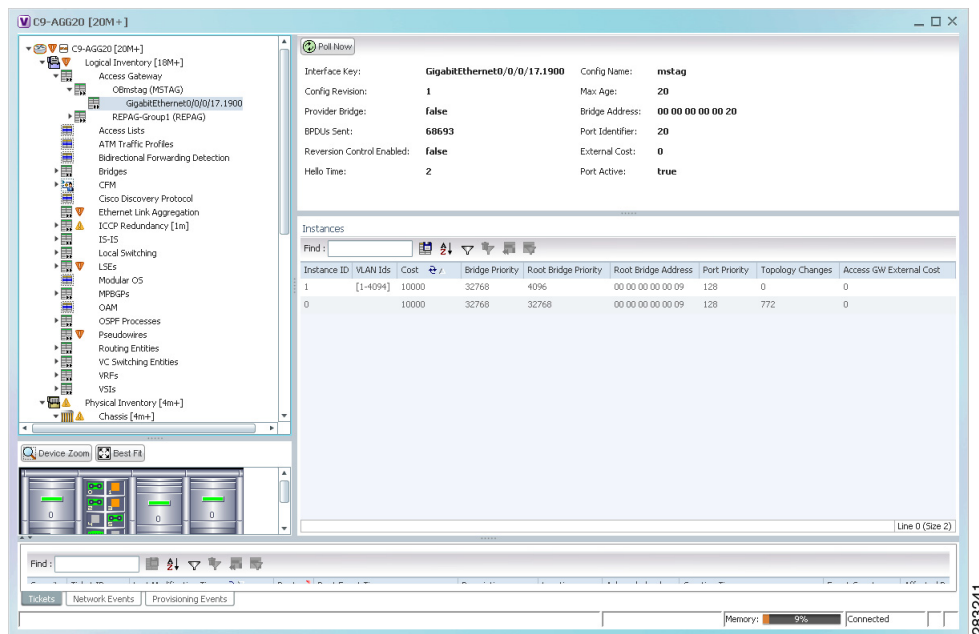
Figure 18-8 Access Gateway Instance in Logical Inventory

Table 18-10 describes the information that is displayed for an access gateway instance.

Table 18-10 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.

Table 18-10 Access Gateway Instance Properties (continued)

Field	Description
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.
BPDU 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.
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 ID	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 a Static Link When a Network Link is Missing, page 4-13](#).

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

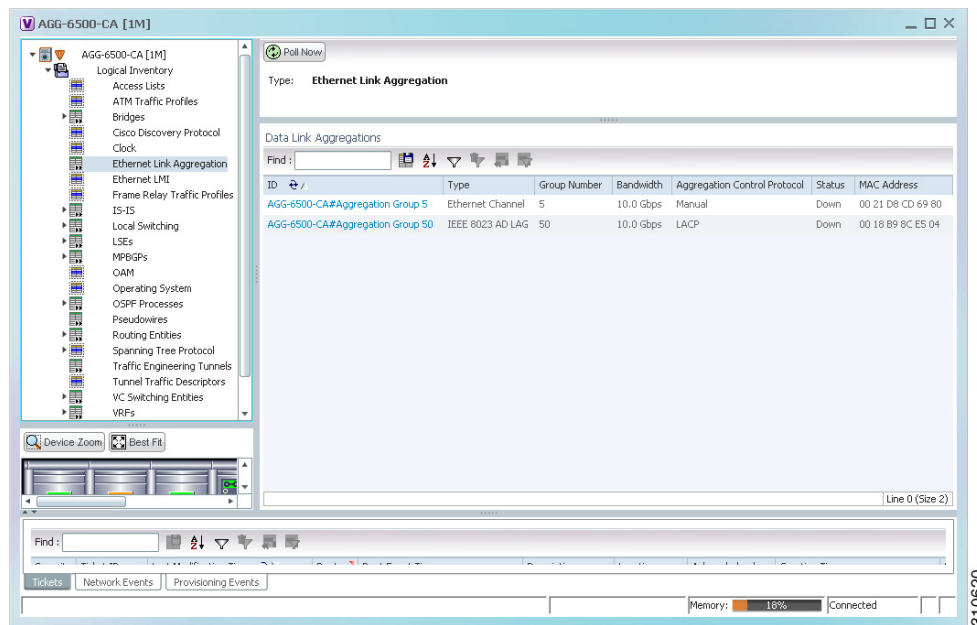
To view a device's Ethernet LAG properties, the device must be configured to receive SNMP traps as described in the *Cisco Prime Network 5.2 Administrator Guide*. To view properties for Ethernet link aggregation groups:

Step 1 In the Vision client, 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 18-9](#).

Figure 18-9 Ethernet Link Aggregation in Logical Inventory



[Table 18-11](#) describes the aggregation group properties that are displayed in the Data Link Aggregations table.

Table 18-11 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 802.3 AD LAG.
Group Number	Aggregation group number.
Bandwidth	Aggregation bandwidth.

Table 18-11 Data Link Aggregations Table (continued)

Field	Description
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.
Link Type	The type of ethernet bundle link, namely ICL and transport. <ul style="list-style-type: none"> ICL link type represents the ethernet link bundle between Cisco ASR 9000 device and satellite chassis or between two satellite chassis. Transport link type represents the ethernet link bundle between two Cisco ASR 9000 devices.
Non Revertive	Specifies the currently active but a lower priority port to remain active port even after a higher priority port is capable of being operational (if non revertive is enabled). By default, non revertive is disabled.
Load Balance	Load balance type which uses Source and Destination MAC address, Source IP address, or Destination IP 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 18-12](#).
- For IEEE 802.3 AD aggregations, see [Table 18-13](#).

Table 18-12 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).

Table 18-12 LAG Ethernet Channel Properties (continued)

Field	Description
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.
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.

Table 18-12 LAG Ethernet Channel Properties (continued)

Field	Description
Binding	Hyperlinked entry to the specific bridge in logical inventory.
Description	Description for the EFP.

Table 18-13 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.
Adjacent	Displays the adjacent ethernet link aggregation for the selected Data Link Aggregation ID.
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 18-13 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 LACPDUs.
Dot3ad Agg Port Attached Agg ID	Identifier of the aggregator that the port is attached to.

Table 18-13 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

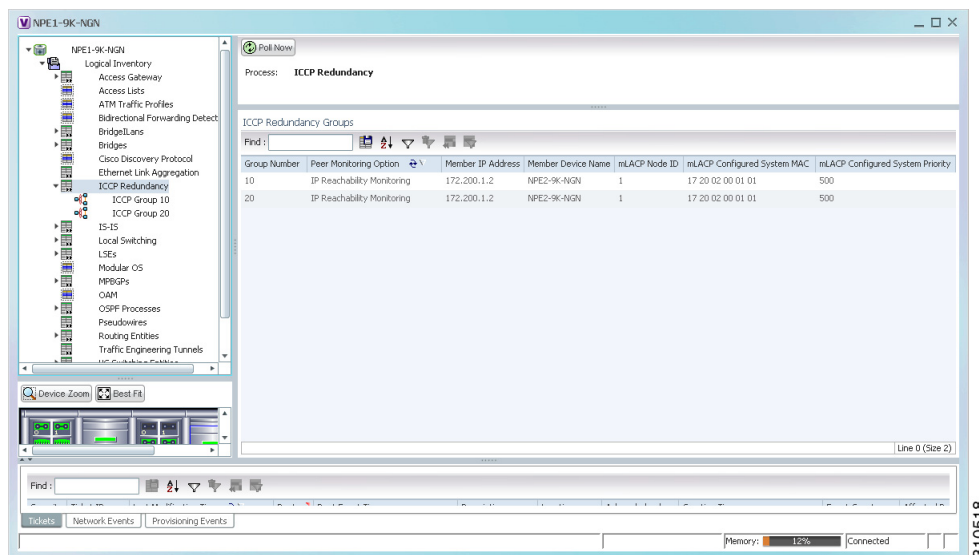
The Vision client supports the discovery of Multichassis LACP (mLACP) configurations on devices configured for them, and displays mLACP configuration information, such as redundancy groups and properties, in inventory.

To view mLACP properties:

- Step 1** In the Vision client, double-click the element configured for mLACP.
- Step 2** In the **Inventory** window, choose **Logical Inventory > ICCP Redundancy**.

In response, the Vision client lists the Inter-Chassis Communication Protocol (ICCP) redundancy groups configured on the device as shown in [Figure 18-10](#).

Figure 18-10 ICCP Redundancy in Logical Inventory



310518

Table 18-14 describes the information displayed in the ICCP Redundancy Groups table.

Table 18-14 ICCP Redundancy Groups in Logical Inventory

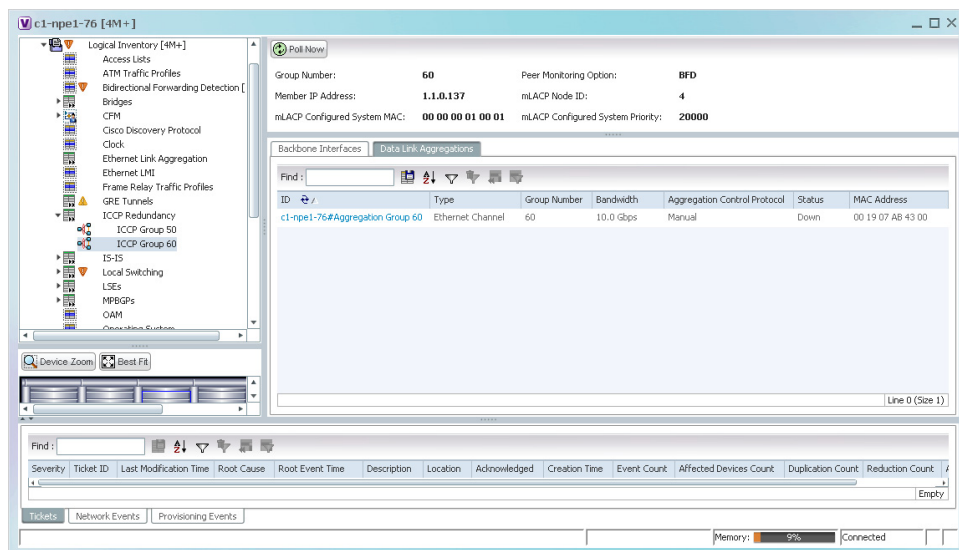
Field	Description
Group Number	ICCP group identifier.
Peer Monitoring Option	Method used to monitor the peer: BFD or IP Reachability Monitoring.
Member IP Address	IP address of the neighbor PoA device.
Member Device Name	Name of the neighbor PoA device.
mLACP Node ID	Identifier used by this member of 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 18-11.

Figure 18-11 ICCP Redundancy Group Properties Window



310519

Table 18-15 describes the information available in the ICCP Redundancy Group Properties window.

Table 18-15 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 802.3 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 18-12—LAG Ethernet Channel Properties](#)
- [Table 18-13—LAG IEEE 802.3 AD Properties](#)

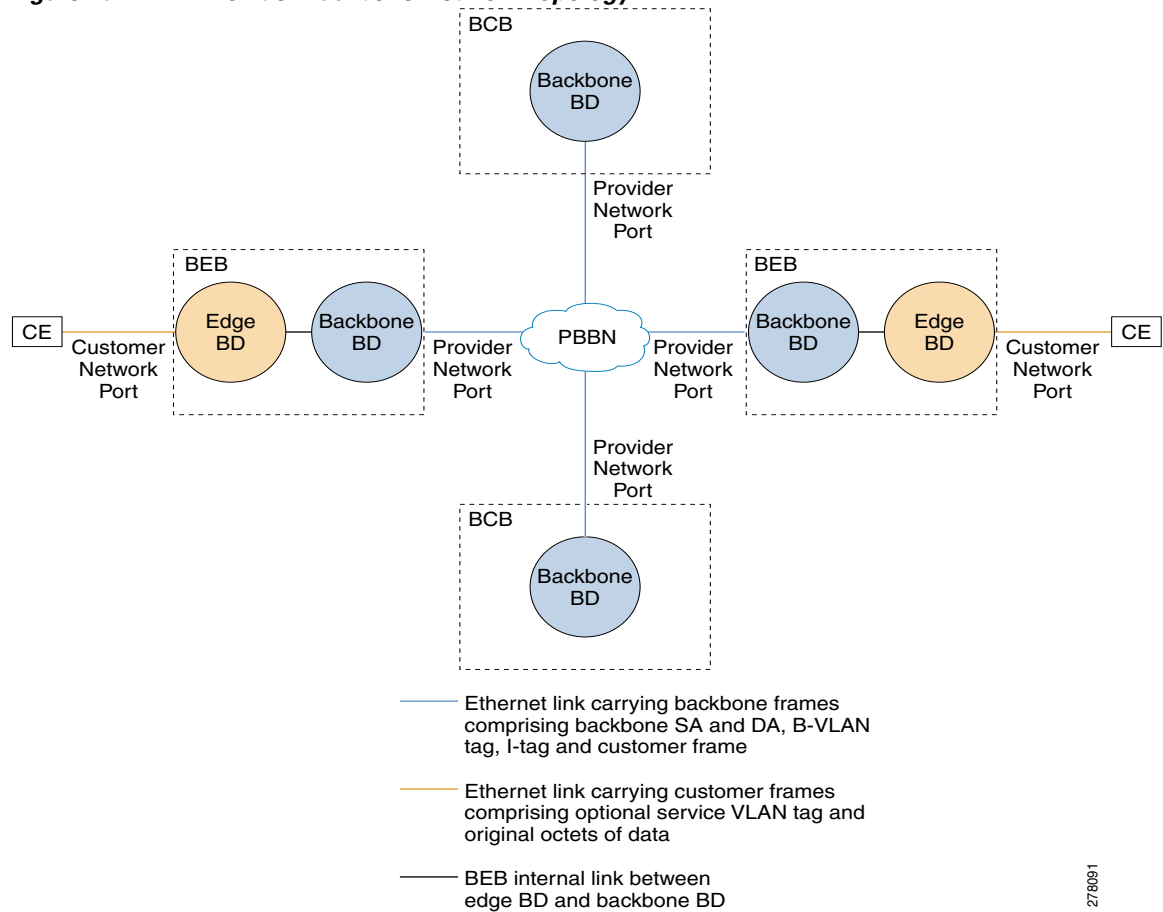
Monitoring Provider Backbone Bridges

The Provider Backbone Bridge (PBB) 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.

The PBB network comprises of a set of architecture and protocols for routing over a provider's network. The PBB network interconnects multiple provider bridge networks without losing each customer's individual VLANs. The PBB network encapsulates and decapsulates end-user traffic on a Backbone Edge Bridge (BEB) at the edge of the Provider Backbone Bridged Network (PBBN). A Backbone Core Bridge (BCB)-based network provides internal transport of the IEEE 802.1ah encapsulated frames within the PBBN.

Figure 18-12 shows a typical provider backbone network topology.

Figure 18-12 Provider Backbone Network Topology



278091

BFD Templates Support

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

Telnet /CLI Command for listing the BFD template

Show running-config|section bfd-template

Cerent Trap Support

Cerent trap alarms are supported for CPT devices. There are 170 traps supported.

Change Settings in CTC (Cisco Transport Controller)

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

Link and Port Parameters

Configuration of Ethernet loopback is used to add and remove loopback. Link and Port parameters have been used for Prime Network configuration scripts in both TLI and Telnet. The link and port parameters are supported for the following: Ethernet Parameter Configuration

- MTU
- Link State
- Expected Speed
- Expected Duplex
- Operating Flow Control
- Carrier Delays
- Auto Negotiation

Port Parameter Configuration

- Port Name
- Admin State
- AINS Soak
- Reach
- Wavelength

L2 Parameter Configuration

- CDP
- DOTIX
- DTP
- LACP
- PAGP
- VTP
- STP

The following are the configuration scripts supported,

- Add Loopback
- Remove Loopback
- Configure CDP
- Configure Ethernet
- Configure L2 Control Protocol
- Configure Port Parameters
- Show Ethernet Parameters
- Show L2 Control Parameters
- Show Port Parameters

This chapter describes the following topics:

- [Working with PBB-EVPN, page 18-29](#)
- [Working with PBB-VPLS, page 18-40](#)
- [Working with PBB-MMRP, page 18-44](#)

Working with PBB-EVPN

Ethernet Virtual Private Network (EVPN) is a solution for secure and private connectivity of multiple sites within an organization. The EVPN service extends the benefits of Ethernet technology to the WAN. This service is delivered over Multiprotocol Label Switching (MPLS) networks.

EVPN allows you to manage routing over a virtual private network, providing complete control and security. EVPN introduces a solution for multipoint L2VPN services with advanced multi-homing capabilities, using BGP for distributing customer or client MAC address reachability information over the MPLS/IP network. EVPN advertises each customer MAC address as BGP routes, therefore allowing BGP policy control over MAC addresses.

The PBB-EVPN solution combines Ethernet Provider Backbone Bridging (PBB - IEEE 802.1ah) with Ethernet VPN, where provider edges (PEs) perform as PBB Backbone Edge Bridge (BEB). The PEs receive 802.1Q Ethernet frames from their attachment circuits. These frames are encapsulated in the PBB header and forwarded over the Internet Protocol / Multi-protocol label switching (IP/MPLS) core. On the egress side (EVPN PE), the PBB header is removed after MPLS disposition, and the original 802.1Q Ethernet frame is delivered to the customer equipment.

The PE routers perform these functions:

- Learns customer or client MAC addresses (C-MACs) over the attachment circuits in the data-plane, per normal bridge operation.
- Learns remote C-MAC to backbone MAC (B-MAC) bindings in the data-plane from traffic ingress from the core.
- Advertises local B-MAC address reachability information in BGP to all other PE nodes in the same set of service instances. Note that every PE has a set of local B-MAC addresses that uniquely identify the device.

- Builds a forwarding table from the received remote BGP advertisements, associating remote B-MAC addresses with remote PE IP addresses.

PBB-EVPN scales well for large network with millions of customer MAC addresses by constraining customer MAC address in access. Only B-MAC addresses are advertised in core, making the number of BGP routes exchanged manageable.

This section describes the following topics:

- [EVPN Instance, page 18-30](#)
- [Ethernet Segment, page 18-30](#)

EVPN Instance

E-VPN Instance (EVI) identifies a VPN in the MPLS/IP network. There can only be one EVI per core bridge.

Ethernet Segment

Ethernet Segment is a site connected to one or more PEs. The Ethernet Segment can be a single device like a Customer Edge (CE) or an entire network, such as:

- Single-Homed Device (SHD)
- Multi-Homed Device (MHD) using Ethernet Multi-chassis Link Aggregation Group
- Single-Homed Network (SHN)
- Multi-Homed Network (MHN)

The Ethernet segment is uniquely identified by a 10-byte global Ethernet Segment Identifier (ESI).

You can view the following properties in the PBB-EVPN network:

- [Viewing PBB-EVPN Core Bridge Properties, page 18-30](#)
- [Viewing EVPN Container Properties, page 18-34](#)
- [Viewing EVPN Properties, page 18-35](#)
- [Viewing Ethernet Segment Container Properties, page 18-36](#)
- [Viewing Ethernet Segment Properties, page 18-38](#)

Viewing PBB-EVPN Core Bridge Properties

To view the PBB-EVPN core bridge properties:

-
- Step 1** Double-click the required device in the Vision client.
 - Step 2** In the **Inventory** window, choose **Logical Inventory** > **Bridges** to view the list of bridges.
 - Step 3** Select a PBB-EVPN bridge to view the properties.

[Table 18-16](#) describes the information displayed for PBB-EVPN bridge properties.

Table 18-16 PBB-EVPN Core Bridge Properties




Field	Description
Name	PBB bridge name.
Type	Specifies the type of bridge. There can be two types of bridges: <ul style="list-style-type: none"> I-Bridge—Interfaces with the customer edge. B-bridge—Interfaces with the core network. The PBB-EVPN core bridge is a B-bridge
VLAN ID	VLAN identifier configured for the subscriber.
VSI	VSI information, hyperlinked to the VSI entry in logical inventory.
Evi	Specifies an unique route distinguisher per customer. There can only be one Evi per core bridge.
MMRP Enabled	Denotes Multiple MAC Registration Protocol (MMRP). It allows multicast traffic in bridged LANs.
	 Note The MMRP is disabled by default in the EVPN network.
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.
SAII	Specifies the Source Access Individual Identifier (SAII) of the tunnel.
	 Note The SAI attribute can be configured only if the Pseudowire type is FEC129 TYPE II.
Tunnel Status	Operational state of the tunnel: Up or Down.
TAII	Specifies the Target Attachment Individual Identifier (TAII) of the tunnel.
	 Note The TAI attribute can be configured only if the Pseudowire type is FEC129 TYPE II.
Peer Router IP	IP Address of the peer router for this pseudowire.
Pseudowire Type	Type of pseudowire, such as Ethernet, Ethernet Tagged, CESoPSN Basic, PPP, SAToP or FEC129 TYPE II.
Pseudowire Role	If the pseudowire is in a redundancy configuration, then the pseudowire role indicates whether its a primary pseudowire or a secondary pseudowire in the configuration. If the pseudowire is not configured for redundancy, the field is blank.
Preferred Path Tunnel	Specifies the path that has to be used for MPLS pseudowire traffic.

Table 18-16 PBB-EVPN Core Bridge Properties (continued)

Field	Description
Local Router IP	Specifies the IP address of the tunnel edge, which is used as the router identifier.
Local MTU	Specifies the byte size of the MTU on the local interface.
Remote MTU	Specifies the byte size of the MTU on the remote interface.
Local VC Label	Specifies the MPLS label that is used by the local router to identify or access the tunnel. It is inserted in the MPLS label stack by the local router.
Peer VC Label	Specifies the MPLS label that is used by the peer router to identify or access the tunnel. It is inserted in the MPLS label stack by the peer router.
Signaling Protocol	Specifies the protocol that is used to build the tunnel, such as the LDP or TDP.
Peer Status	Specifies the status of the peer link.
Associated EVC Name	Specifies the name of the associated Ethernet Virtual Circuits (EVC).
I-Bridge Associations Tab	
I-SID	Specifies a 24-bit identifier that represents the backbone service instance.
I-Bridge	Specifies the exchange identification (XID) in the I-Bridge component. The XID is hyperlinked to the relevant bridge in the logical inventory.

Viewing PBB-EVPN Customer Bridge Properties

To view the PBB-EVPN customer bridge properties:

- Step 1** Double-click the required device in the Vision client.
- Step 2** In the **Inventory** window, choose **Logical Inventory > Bridges** to view the list of bridges.
- Step 3** Select a PBB-EVPN customer bridge to view the properties.

[Table 18-17](#) describes the information displayed for PBB-EVPN customer bridge properties.

Table 18-17 PBB-EVPN Customer Bridge Properties

Field	Description
Name	PBB bridge name.
Type	Specifies the type of bridge. The PBB-EVPN customer bridge is an I-bridge
VLAN ID	VLAN identifier configured for the subscriber.

Table 18-17 PBB-EVPN Customer Bridge Properties (continued)



Field	Description
I-SID	Specifies a 24-bit identifier that represents the backbone service instance.
B-Bridge	Specifies the XID of the B-Bridge component. The XID is hyperlinked to the relevant bridge in logical inventory.
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.
SAII	Specifies the Source Access Individual Identifier (SAII) of the tunnel.  Note The SAI attribute can be configured only if the Pseudowire type is FEC129 TYPE II.
Tunnel Status	Operational state of the tunnel: Up or Down.
TAII	Specifies the Target Attachment Individual Identifier (TAII) of the tunnel.  Note The TAI can be configured only if the Pseudowire type is FEC129 TYPE II.
Peer Router IP	IP address of the peer router for this pseudowire.
Pseudowire Type	Type of pseudowire, such as Ethernet, Ethernet Tagged, CESoPSN Basic, PPP, SAToP or FEC129 TYPE II.
Pseudowire Role	If the pseudowire is in a redundancy configuration, then the pseudowire role indicates whether its a primary pseudowire or a secondary pseudowire in the configuration. If the pseudowire is not configured for redundancy, the field is blank.
Preferred Path Tunnel	Specifies the path that has to be used for MPLS pseudowire traffic.
Local Router IP	Specifies the IP address of the tunnel edge, which is used as the router identifier.
Local MTU	Specifies the byte size of the MTU on the local interface.
Remote MTU	Specifies the byte size of the MTU on the remote interface.
Local VC Label	Specifies the MPLS label that is used by the local router to identify or access the tunnel. It is inserted in the MPLS label stack by the local router.
Peer VC Label	Specifies the MPLS label that is used by the peer router to identify or access the tunnel. It is inserted in the MPLS label stack by the peer router.
Signaling Protocol	Specifies the protocol that is used to build the tunnel, such as the LDP or TDP.
Peer Status	Specifies the status of the peer link.

Table 18-17 PBB-EVPN Customer Bridge Properties (continued)

Field	Description
Associated EVC Name	Specifies the name of the associated EVC.
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.
Ingress Policy	The name of the ingress service policy associated with the subscriber template. This field is applicable only for IP Subscriber and Service templates.
Egress Policy	The name of the egress service policy associated with the subscriber template. This field is applicable only for IP Subscriber and Service templates.
Service Control Policy	Specifies the policy for a port or operation.
MMRP Participants	
Associated MMRP Participant	Specifies an entry that is hyperlinked to an associated MMRP service for that bridge.

Viewing EVPN Container Properties

To view the EVPN container properties:

-
- Step 1** Right-click the required device in the Vision client and choose **Inventory**.
 - Step 2** In the **Inventory** window, choose **Logical Inventory** > **EVPN** to view the EVPN container properties. [Table 18-18](#) describes the information displayed for the EVPN container properties.

Table 18-18 EVPN Container Properties

Field	Description
EVI	The EVI identifies a VPN (Virtual Private Network) in the MPLS/IP network. There can only be one EVI per core bridge.
Bridge Domain	Maintains a forwarding database of MAC addresses from packets received from its interfaces. The bridge domain is hyperlinked to the relevant core bridge in the logical inventory.

Table 18-18 *EVPN Container Properties (continued)*

Field	Description
EVPN Type	Specifies the type of bridges. There can be two types of bridges: <ul style="list-style-type: none"> • PBB-EVPN • BD
Route Distinguisher	Creates a unique 96-bit VPNv4 address to distinguish routes within a single internet service provider's (ISP) MPLS network.
Multicast Label	Specifies a 20-bit multicast label in the MPLS packet to make forwarding decisions and to pre-establish a path for switch-labeled packets at the Layer 2.
Unicast Label	Specifies a 20-bit unicast label in MPLS packet to make forwarding decisions and to pre-establish a path for switch-labeled packets at the Layer 2.
Route Distinguisher (Auto)	The Route Distinguisher (Auto) is generated by default as a combination of Loopback IP Address and EVI.
Route Target (Auto)	Communicates the VPN route to the PE routers.

Viewing EVPN Properties

To view the EVPN properties:

- Step 1** Right-click the required device in the Vision client and choose **Inventory**.
- Step 2** In the **Inventory** window, choose **Logical Inventory > EVPN** to display the EVPN container properties.
- Step 3** Double-click an EVI to view its EVPN properties.

[Table 18-19](#) describes the information displayed for EVPN properties.

Table 18-19 *EVPN Properties*

Field	Description
EVI	The EVI identifies a VPN in the MPLS/IP network. There can only be one EVI per core bridge.
Bridge Domain	Maintains a forwarding database of MAC addresses from packets received from its interfaces. The bridge domain is hyperlinked to the relevant core bridge in the logical inventory.
EVPN Type	Specifies the type of bridges. There can be two types of bridges: <ul style="list-style-type: none"> • PBB-EVPN • BD
Route Distinguisher	Creates a unique 96-bit VPNv4 address to distinguish routes within a single ISP-MPLS network.

Table 18-19 *EVPN Properties*

Field	Description
Multicast Label	Specifies a 20-bit multicast label in MPLS packet to make forwarding decisions and to pre-establish a path for switch-labeled packets at the Layer 2.
Unicast Label	Specifies a 20-bit unicast label in MPLS packet to make forwarding decisions and to pre-establish a path for switch-labeled packets at the Layer 2.
Route Distinguisher (Auto)	The Route Distinguisher (Auto) is generated by default as a combination of Loopback IP Address and EVI.
Route Target (Auto)	Communicates the VPN route to the PE routers.
EVPN BMAC Address Entries Tab	
MAC Address	It is a unique identifier of the bridge clients in a PE router for an EVPN instance.
Next HOP	Specifies the peer router associated to each EVPN instance.
MPLS Label	Enables the MPLS network data packets to make packet forwarding decisions. This allows the data packets to create end-to-end circuits across any type of transport medium, using any protocol.
Import Route Targets Tab	
Route Target	The PE imports routes with specific prefixes or subnet masks based on the Route Target.
Export Route Targets Tab	
Route Target	The Route Target attribute defines the prefixes that are exported on the PE routers.

Viewing Ethernet Segment Container Properties

The Ethernet segment is a site that is connected to one or more Provider Edge Switches (PEs). The Ethernet segment can be a single device such as a customer edge or an entire network. The Ethernet segment in a network can be of the following types:

- Single-homed device (SHD)
- Multi-homed device (MHD)
- Single-homed network (SHN)
- Multi-homed network (MHN)

The Ethernet segment is unique and identified by a 10-byte global Ethernet Segment Identifier (ESI).

To view the Ethernet segment container properties:

-
- Step 1** Right-click the required device in the Vision client and choose **Inventory**.
- Step 2** In the **Inventory** window, choose **Logical Inventory > Ethernet Segments** to view the Ethernet segment container properties.

Table 18-20 describes the information displayed for PBBE VPN Ethernet segment container properties.

Table 18-20 Ethernet Segment Container Properties

Field	Description
Interface Name	Name of the interface that is connected to the Ethernet segment.
Associated Interface	Associated Name of the interface that is connected to the Ethernet segment.
ES ID	The Ethernet Segment Identifier (ES ID) is a 10-byte field. It identifies the unique Ethernet segment in the core network of the PE routers.
Source MAC Address	Specifies the Ethernet Segment MAC Address.
Access Topology Mode	Specifies one of the following network types: <ul style="list-style-type: none"> • Single Home Device (SH) • Single Home Network (SHN) • Dual Home Device (DHD) • Dual Home Network (DHN) • Multi Home Network (MHN) The default value is MHN.
Access Topology Flow Mode	Specifies the flow of traffic in a network. The flow mode can be one of the following options: <ul style="list-style-type: none"> • Active/Active per-flow • Active/Active per-service
I-SID Primary Services	Specifies the type of primary customer service interfaces provided by the I-Bridge Backbone Edge Bridge (IB-BEB). The primary customer service interfaces can be one of the following types: <ul style="list-style-type: none"> • Port based • S-tagged • I-tagged
I-SID Secondary Services	Specifies the type of secondary customer service interfaces provided by the IB-BEB bridge. The secondary customer service interfaces can be one of the following types: <ul style="list-style-type: none"> • Port based • S-tagged • I-tagged
Total I-SID Count	Specifies the total number of elected and non-elected ports.
Elected I-SIDs	Specifies the Elected Service Identifiers (I-SID) list.
Non-Elected I-SIDs	Specifies the Non-Elected Service Identifiers (I-SID) list.

Table 18-20 Ethernet Segment Container Properties (continued)

Field	Description
MAC Flushing Mode	Specifies the MAC flush over Multiple VLAN Registration Protocol (MVRP). The possible values in the MAC Flushing Mode field can be one of the following: <ul style="list-style-type: none"> Spanning Tree Protocol - Topology Change Notification (STP-TCN) MVRP The default value is STP-TCN.
Peering Timer	Specifies the interface-specific peering timer in seconds. The default value is 45 seconds.
Recovery Timer	Specifies the interface-specific recovery timer in seconds. The range is 20 to 3600 seconds. The default value is 20 seconds.
Flush Again Timer	Specifies the interface-specific MAC flush again timer in seconds. The range is 0 to 120 seconds. The default value is 60 seconds.

Viewing Ethernet Segment Properties

To view the Ethernet segment properties:

-
- Step 1** Right-click the required device in the Vision client and choose **Inventory**.
- Step 2** In the **Inventory** window, choose **Logical Inventory > Ethernet Segments** to view the Ethernet segment container properties.
- Step 3** Double-click an interface to view its PBBE VPN Ethernet segment properties.

[Table 18-21](#) describes the information displayed for PBBE VPN Ethernet segment properties.

Table 18-21 Ethernet Segment Properties

Field	Description
Interface Name	Name of the interface that is connected to the Ethernet segment.
Associated Interface	Associated Name of the interface that is connected to the Ethernet segment.
ES ID	The Ethernet Segment Identifier (ES ID) is a 10-byte field. It identifies the unique Ethernet segment in the core network of the PE routers.
Source MAC Address	Specifies the Ethernet Segment MAC Address.
Access Topology Mode	Specifies one of the following network types: <ul style="list-style-type: none"> Single Home Device (SH) Single Home Network (SHN) Dual Home Device (DHD) Dual Home Network (DHN) Multi Home Network (MHN) The default value is MHN.

Table 18-21 Ethernet Segment Properties (continued)

Field	Description
Access Topology Flow Mode	Specifies the flow of traffic in a network. The flow mode can be one of the following options: <ul style="list-style-type: none"> Active/Active per-flow Active/Active per-service
I-SID Primary Services	Specifies the type of primary customer service interfaces provided by the IB-BEB bridge. The primary customer service interfaces can be one of the following types: <ul style="list-style-type: none"> Port based S-tagged I-tagged
I-SID Secondary Services	Specifies the type of secondary customer service interfaces provided by the IB-BEB bridge. The secondary customer service interfaces can be one of the following types: <ul style="list-style-type: none"> Port based S-tagged I-tagged
Total I-SID Count	Specifies the total number of elected and non-elected ports.
Elected I-SIDs	Specifies the Elected Service Identifiers (I-SID) list.
Non-Elected I-SIDs	Specifies the Non-Elected Service Identifiers (I-SID) list.
MAC Flushing Mode	Specifies the MAC flush over MVRP. The possible values in the MAC Flushing Mode field can be one of the following: <ul style="list-style-type: none"> STP-TCN MVRP <p>The default value is STP-TCN.</p>
Peering Timer	Specifies the interface-specific peering timer in seconds. The default value is 45 seconds.
Recovery Timer	Specifies the interface-specific recovery timer in seconds. The range is 20 to 3600 seconds. The default value is 20 seconds.
Flush Again Timer	Specifies the interface-specific MAC flush again timer in seconds. The range is 0 to 120 seconds. The default value is 60 seconds.
Redundancy Group Entries	
IP Address	Identifies the redundancy group IP address that is associated to an Ethernet segment.
Is Self	Specifies whether the redundancy group IP Address belongs to a local border gateway protocol (BGP).

Working with PBB-VPLS

The Virtual Private LAN service (VPLS) is a class of VPN that supports the connection of multiple sites in a single bridged domain over a managed MPLS network. The VPLS is a multipoint service and it can also transport non-IP traffic. All customer premises at a VPLS instance appear to be on the same local area network regardless of their actual locations. The VPLS uses an Ethernet interface to the customer.

A VPLS network consists of the following three main components.

- Customer Edges
- Provider Edges
- IP/MPLS core network

This section consists of the following topics:

- [Viewing PBB-VPLS Core Bridge Properties, page 18-40](#)
- [Viewing PBB-VPLS Customer Bridge Properties, page 18-42](#)
- [Working with PBB-MMRP, page 18-44](#)

Viewing PBB-VPLS Core Bridge Properties

To view the PBB-VPLS bridge properties:

-
- Step 1** Double-click the required device in the Vision client.
- Step 2** In the **Inventory** window, choose **Logical Inventory > Bridges** to view the list of bridges.
- Step 3** Select a PBB-VPLS bridge to view the properties.

[Table 18-22](#) describes the information displayed for PBB-VPLS bridge properties.

Table 18-22 PBB-VPLS Bridge Properties


Field	Description
Name	PBB bridge name.
Type	Specifies the type of bridge. There can be two types of bridges: I-Bridge—Interfaces with the customer edge. B-bridge—Interfaces with the core network.
VLAN ID	Specifies the VLAN identifier of the subscriber.
VSI	VSI information, hyperlinked to the VSI entry in logical inventory.
Evi	Specifies a unique route distinguisher per customer. There can only be one EVI per core bridge.
MMRP Enabled	Denotes Multiple MAC Registration Protocol (MMRP). It allows multicast traffic in bridged LANs.
	 Note The MMRP is enabled in the VPLS network.
Pseudowires Tab	

Table 18-22 PBB-VPLS Bridge Properties (continued)



Field	Description
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.
SAII	Specifies the Source Access Individual Identifier (SAII) of the tunnel.  Note The SAII attribute can be configured only if the Pseudowire type is FEC129 TYPE II.
Tunnel Status	Operational state of the tunnel: Up or Down.
TAII	Specifies the Target Attachment Individual Identifier (TAII) of the tunnel.  Note The TAI can be configured only if the Pseudowire type is FEC129 TYPE II.
Peer Router IP	IP address of the peer router for this pseudowire.
Pseudowire Type	Type of pseudowire, such as Ethernet, Ethernet Tagged, CESoPSN Basic, PPP, SAToP or FEC129 TYPE II.
Pseudowire Role	If the pseudowire is in a redundancy configuration, then the pseudowire role indicates whether its a primary pseudowire or a secondary pseudowire in the configuration. If the pseudowire is not configured for redundancy, the field is blank.
Preferred Path Tunnel	Specifies the path that has to be used for MPLS pseudowire traffic.
Local Router IP	Specifies the IP address of the tunnel edge, which is used as the router identifier.
Local MTU	Specifies the byte size of the MTU on the local interface.
Remote MTU	Specifies the byte size of the MTU on the remote interface.
Local VC Label	Specifies the MPLS label that is used by the local router to identify or access the tunnel. It is inserted in the MPLS label stack by the local router.
Peer VC Label	Specifies the MPLS label that is used by the peer router to identify or access the tunnel. It is inserted in the MPLS label stack by the peer router.
Signaling Protocol	Specifies the protocol that is used to build the tunnel, such as the LDP or TDP.
Peer Status	Specifies the status of the peer link.
Associated EVC Name	Specifies the name of the associated EVC.
VPLS I-Bridge Associations Tab	

Table 18-22 PBB-VPLS Bridge Properties (continued)

Field	Description
I-SID	Specifies a 24-bit identifier that represents the backbone service instance.
I-Bridge	Specifies the exchange identification (XID) in the I-Bridge component. The XID is hyperlinked to the relevant bridge in the logical inventory.

Viewing PBB-VPLS Customer Bridge Properties

The PBB-VPLS customer bridges communicates directly with the customer edge. Multiple customer bridges can communicate with the core bridge.

To view the PBB-VPLS customer bridge properties:

-
- Step 1** Double-click the required device in the Vision client.
 - Step 2** In the **Inventory** window, choose **Logical Inventory > Bridges**.
 - Step 3** Select a PBB-VPLS customer bridge to view the properties.

[Table 18-22](#) describes the information displayed for PBB-VPLS bridge properties.

Table 18-23 PBB-VPLS Customer Bridge Properties

Field	Description
Name	PBB customer bridge name.
Type	Specifies the type of bridge. There can be two types of bridges: I-Bridge—Interfaces with the customer edge. B-bridge—Interfaces with the core network.
VLAN ID	Specifies the VLAN identifier of the subscriber.
I-SID	Specifies a 24-bit identifier that represents the backbone service instance.
B-Bridge	Specifies the XID of the B-Bridge component. The XID is hyperlinked to the relevant bridge in logical inventory.
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.

Table 18-23 PBB-VPLS Customer Bridge Properties



Field	Description
SAII	Specifies the Source Access Individual Identifier (SAII) of the tunnel.  Note The SAI attribute can be configured only if the Pseudowire type is FEC129 TYPE II.
Tunnel Status	Operational state of the tunnel: Up or Down.
TAII	Specifies the Target Attachment Individual Identifier (TAII) of the tunnel.  Note The TAI attribute can be configured only if the Pseudowire type is FEC129 TYPE II.
Peer Router IP	IP address of the peer router for this pseudowire.
Pseudowire Type	Type of pseudowire, such as Ethernet, Ethernet Tagged, CESoPSN Basic, PPP, SAToP or FEC129 TYPE II.
Pseudowire Role	If the pseudowire is in a redundancy configuration, then the pseudowire role indicates whether its a primary pseudowire or a secondary pseudowire in the configuration. If the pseudowire is not configured for redundancy, the field is blank.
Preferred Path Tunnel	Specifies the path that has to be used for MPLS pseudowire traffic.
Local Router IP	Specifies the IP address of the tunnel edge, which is used as the router identifier.
Local MTU	Specifies the byte size of the MTU on the local interface.
Remote MTU	Specifies the byte size of the MTU on the remote interface.
Local VC Label	Specifies the MPLS label that is used by the local router to identify or access the tunnel. It is inserted in the MPLS label stack by the local router.
Peer VC Label	Specifies the MPLS label that is used by the peer router to identify or access the tunnel. It is inserted in the MPLS label stack by the peer router.
Signaling Protocol	Specifies the protocol that is used to build the tunnel, such as the LDP or TDP.
Peer Status	Specifies the status of the peer link.
Associated EVC Name	Specifies the name of the associated EVC.
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.

Table 18-23 PBB-VPLS Customer Bridge Properties

Field	Description
Binding Port	Hyperlinked entry to the port in physical inventory.
Description	Brief description of the EFP.
Ingress Policy	The name of the ingress service policy associated with the subscriber template. This field is applicable only for IP Subscriber and Service templates.
Egress Policy	The name of the egress service policy associated with the subscriber template. This field is applicable only for IP Subscriber and Service templates.
Service Control Policy	Specifies the policy for a port or operation.
MMRP Participants Tab	
Associated MMRP Participant	Specifies an entry that is hyperlinked to an associated MMRP service for that bridge.

Working with PBB-MMRP

Multiple MAC registration protocol (MMRP) is a data link layer 2 protocol that registers group MAC addresses on multiple switches. The MMRP allows multicast traffic in bridged LANs and provides a mechanism to achieve the following:

- Register or unregister group membership information across the bridges attached to the same LAN.
- Register or unregister individual MAC address information across the bridges attached to the same LAN.
- Communicate the registration information across all the bridges that support extended filtering services in the bridged network.

MMRP operates on the services provided by the Multiple Registration Protocol (MRP). It allows bridges, switches or other similar devices to register or unregister attribute values such as VLAN identifiers and multicast the group membership information across a large LAN.

You can view the following properties in the PBB-MMRP network:

- [Viewing MMRP Container Properties, page 18-44](#)
- [Viewing MMRP Registration Properties, page 18-46](#)

Viewing MMRP Container Properties

To view MMRP container properties:

-
- Step 1** Right-click the required device in the Vision client and choose **Inventory**.
 - Step 2** In the **Inventory** window, choose **Logical Inventory > MMRP** to view the container properties. [Table 18-24](#) describes the information displayed for the MMRP container properties.

Table 18-24 MMRP Container Properties

Field	Description
Flood Time	Specifies the flood time to enable the flooding of traffic for the whole core bridge when the MMRP feature is first enabled on the core bridge. The range is 3 to 600 seconds.
Leave All Time	Specifies the minimum time in seconds for the Leave All timer parameter to check how often Leave All messages are sent for all the active ports. The range is 5 to 30 seconds. The default value is 10 seconds.
Leave Time	Specifies the leave time for all the active ports. The range is 1 to 90 seconds. The default value is 30 seconds.
Join Time	Specifies the maximum time for controlling the interval between transmit opportunities that are applied to the applicant state machine for all active ports.
Periodic Transmit	Specifies the periodic transmit interval of Multiple MAC Registration Protocol Data Units (MMRPDU) on all active ports. The range is 2 to 10 seconds.

MMRP Participants Tab

Peer IP Address	Specifies the neighbor Peer IP address.
PW ID	Specifies the associated Pseudowire ID.
Bridge Domain	Specifies the associated B-Bridge domain.
Participant Type	Specifies the node participating in MMRP. In PBB-MMRP, each IB-PE router in B-domain is a participant. The possible value is FULL.
Flood Optimization	Specifies if the flood optimization is enabled between two point-to-point peers. The possible value is Yes.
Participant State	Specifies the state of the Participant. The possible value is Normal.
Registrar State	Specifies the state of the Registrar. The Registrar listens to the MRPDUs and registers the applicants. The possible value is Normal.
Leave State	Specifies the state of one or more remote IB-PE routers that must leave the group B-MAC address flooding tree.
Join State	Specifies the state of one or more remote IB-PE routers that must join the group B-MAC address flooding tree.
Last Peer	Specifies the last peer.
Failed Registrations	Specifies the number of failed registrations when the PE bridges join the network.

Viewing MMRP Registration Properties

To view the MMRP registration properties:

- Step 1** Right-click the required device in the Vision client and choose **Inventory**.
- Step 2** In the **Inventory** window, choose **Logical Inventory > MMRP** to view the container properties.
- Step 3** Double-click any row to view its registration properties.

[Table 18-25](#) describes the information displayed for MMRP registration properties.

Table 18-25 MMRP Registration Properties

Field	Description
Peer IP Address	Specifies the neighbor peer IP address.
PW ID	Specifies the associated pseudowire ID.
Bridge Domain	Specifies the associated B-Bridge domain
Participant Type	Specifies the participating node in MMRP. In PBB-MMRP, each IB-PE router in B-domain is a participant. The possible value is FULL.
Point To Point	Specifies if flood optimization is enabled between two point-to-point peers. The possible value is Yes.
Applicant State	Announces the group B-MAC address and triggers MRPDUs propagation. The possible values can be one of the following: <ul style="list-style-type: none"> • Normal • Quiet Active
Registrar State	Specifies the state of the Registrar. The Registrar listens to the MRPDUs and registers the applicants. The possible value is Normal.
Leave	Specifies the state of one or more remote IB-PE routers that must leave the group B-MAC address flooding tree.
Join	Specifies the state of one or more remote IB-PE routers that must join the group B-MAC address flooding tree.
Last Peer	Specifies the last peer.
Failed Registrations	Specifies the number of failed registrations when the PE bridges join the network.
Registered Neighbours Tab	
I-SID	Specifies a 24-bit identifier that represents the backbone service instance.
B-MAC	Specifies the bridge MAC Address.
Participant State	Specifies the state of the Participant. The default value is Normal.
Registrar State	Specifies the state of the Registrar. The Registrar listens to the MRPDUs and registers the applicants. The possible value is In.

Monitoring PBB-based Support Service Discovery

The Cisco Prime Network delivers PBB-based discovery for various support services over VLAN, VPLS, EVC, and pseudowires.

The Cisco Prime Network supports the following service discoveries:

- **VLAN Discovery**—Discovers bridges domains such as I-Bridges, B-Bridges, and regular bridges that are unassociated.
- **VPLS Discovery**—Discovers VFIs and their associations between I-Bridges and B-Bridges.
- **Pseudowire Discovery**—Discovers pseudowires and their associations between I-Bridges and B-Bridges.
- **EVC Discovery**—Creates an end-to-end complex circuit representing the network associations in the core network of the above discovered elements.

The PBB specified by IEEE 802.1ah-2008, provides 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. The PBB network interconnects multiple provider bridge networks without losing each customer's individual VLANs.

The Prime Network PBB-based support service discovery recognizes service entities in the network. Service discovery are either network data discovered by Prime Network VNEs or other underlying services discovered by other service discoveries. The network data is stored and cached (in memory) in Snapshots on the Prime Network gateway machine. After which, the data is transformed into service data, and then stored in the Prime Network database.

The Prime Network PBB-based support services can be discovered either by using a full discovery mode or a notification-based discovery mode.

The Prime Network supports the following PBB-based support services:

- [PBB-based VLAN Discovery, page 18-47](#)
- [PBB-based EVC Discovery, page 18-48](#)
- [Discovering PBB-links Between I-Bridge and B-Bridge, page 18-49](#)
- [PBB-based Pseudowire Discovery, page 18-49](#)
- [PBB-based VPLS Discovery, page 18-50](#)

PBB-based VLAN Discovery

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

A VLAN entity consists of one or more bridges and the corresponding EFP elements. When the VLAN discovery is initiated, it identifies VLANs that are considered as part of a switching entity.

Associated and Unassociated Bridges

Generally, all the bridges are categorized as associated or unassociated based on their association with the type of switching entities such as pseudowire and VPLS. In the Provider Backbone configuration, the VLANs identified by VLAN discovery are considered as a part of associated bridges and the VLANs that are not identified are considered as a part of unassociated bridges. For example, if a regular bridge

is associated with a pseudowire or a VPLS, then it is classified as an associated bridge. Otherwise, it is classified as an unassociated bridge. However, the I-Bridges and B-Bridges are always considered as a part of unassociated bridges irrespective of their association with the switching entities.

Discovering Unassociated Domains

To discover the VLAN service configured in a network, a component called VLAN data plug-in collects information related to VLAN from various devices. The data plug-in holds all the data related to the bridges in a centralized location. To discover an unassociated bridge, for example, an I-bridge or a B-bridge, it is essential to verify whether the plug-in has information related to the I-bridge or the B-bridge, or any other additional I-bridge PBB information. To verify, see [Verifying Bridge domains, page 18-48](#). Based on the information collected, a discovery plug-in is created, and the plug-in receives the necessary data from the VLAN plug-in to create the VLAN instances.

Verifying Bridge domains

To verify the bridge domains, follow the steps provided below:

-
- Step 1** Create a new map in the **Vision** client. For example, VLAN.
 - Step 2** Add bridges to the map.
 - Step 3** Right-click one of the bridges and choose **Inventory**.
 - Step 4** Verify the bridge type in the **Inventory** window.
 - Step 5** Open the **Add Bridge Domain** dialog box in one of the following ways:
 - Choose **File Add to Map > Bridge Domain**.
 - In the toolbar, click **Add to Map** and choose **Bridge Domain**.
 - Step 6** In the **Add Bridge Domain** dialog box, select **Show All** to display the list of bridge domains.
 - Step 7** Verify whether the bridge that you identified in the **Inventory** window is listed in the Bridge Domain list.



Note

The bridges of type I-Bridges or B-Bridges are considered as the bridge domains. These I-Bridges or B-Bridges are added in the Bridge Domain list.

PBB-based EVC Discovery

PBB-based EVC discovery is dependent on the following discovery processes:

- VPLS Discovery
- Network VLAN Discovery
- Network Pseudowire Discovery
- Bridge Domain Discovery

EVC discovery plug-in is responsible for handling Carrier Ethernet technologies such as VPLS, VLAN, bridge domains, cross connect, and pseudowires. This plug-in connects all the domains together in a map from the Vision client.

For more information on the Ethernet services, refer to [Working with Ethernet Services](#) in the Cisco Prime Network 5.2 User Guide.

PBB-based EVC Multiplexing

Every EVC should be created with the following rules:

- Every network element, for example, I-Bridge, B-Bridge, pseudowire, or VPLS that is discovered in the inventory should definitely be part of at least one EVC.
- If a network element is associated with the I-Bridge, EVC is created for each I-SID (I-Bridge unique identifier).
- If no I-Bridges are associated, then the EVC is created based on the association between the B-Bridge and VPLS.
- EVC creation for regular bridges works in the same way as that of Prime Network 5.2.

Prime Network supports EVC multiplexing to create an EVC. EVC creation involves the following processes:

- Discovers all dependent discoveries such as VLAN, VPLS, or pseudowires.
- Notifications for each discovery are received by related processors and the Information Model Objects (IMOs) are processed to loaders for creating building blocks based on the associations between the network elements.
- Segmenter collects building blocks from all the above mentioned discoveries and creates segments based on the associations.
- Every segment created is processed based on the rules specified above and creates a complex virtual circuit.

Discovering PBB-links Between I-Bridge and B-Bridge

The PBB I-Bridge interfaces with the customer edge and the B-bridge interfaces with the core network. To discover the link between the I-Bridge and the B-Bridge, follow the steps provided below:

-
- Step 1** Create a new map in the Vision client. For example, VLAN.
 - Step 2** Open the **Add Bridge Domain** dialog box in one of the following ways:
 - Choose **File Add to Map > Bridge Domain**.
 - In the toolbar, click **Add to Map** and choose **Bridge Domain**.
 - Step 3** In the **Add Bridge Domain** dialog box, select **Show All** to display the list of bridge domains.
 - Step 4** From the bridge domains, select an I-Bridge and a B-Bridge and click **OK**.
 - Step 5** Add the selected bridges to the map. The map displays the PBB links between the newly added bridges.

PBB-based Pseudowire Discovery

A pseudowire is a point-to-point connection between pairs of provider edge (PE) routers.

Discovering PBB-links Between Pseudowire and I-Bridge/B-Bridge

To discover the link between the pseudowire and the I-Bridge or B-Bridge, follow the steps provided below:

-
- Step 1** Create a new map in the Vision client. For example, Pseudowire.
- Step 2** Open the **Add Bridge Domain** to *domain* dialog box in one of the following ways:
- Choose **File Add to Map > Bridge Domain**.
 - In the toolbar, click **Add to Map** and choose **Bridge Domain**.
- Step 3** In the **Add Bridge Domain** dialog box, select **Show All** to display the list of bridge domains.
- Step 4** From the bridge domains, select an I-Bridge and a B-Bridge and click **OK** to add the selected bridges to the map.
- Step 5** Choose **Add to Map > Pseudowire** to open the **Add Pseudowire** to *map* dialog box.
- Step 6** In the **Add Pseudowire** to *map* dialog box, select **Show All** to display the list of pseudowires.
- Step 7** Add any pseudowire from the list to the map.
- Step 8** The map displays the link between the pseudowires and the bridge domains.

PBB-based VPLS Discovery

Prime Network provides Virtual Private LAN Service (VPLS) plug-in to gather VPLS relevant information in a network.

The VPLS plug-in gathers VPLS relevant information from all the VNEs, including the VFIs or VSIs, to create a VPLS service. A VPLS instance representing the VPLS configuration is created on the network. The VPLS snapshot finds out VNEs that are running to retrieve potential VFIs and VSIs. The bridge domains that are connected to the VSIs are attached to VPLS instances to create connection between the VPLS and the Network VLANs.

Based on data gathered, the VPLS discovery constructs the VPLS instances. This discovery can be viewed from the client GUI. A map in the GUI represents VPLS instances in addition to regular VNEs. Thereby, the bridges connected to VSI or VFI are discovered and connected. The VPLS container sends notifications when an VPLS instance is added, modified, or deleted.

Discovering PBB-links Between VPLS and I-Bridge/B-Bridge

To discover the link between the VPLS and the I-Bridge or B-Bridge, follow the steps provided below:

-
- Step 1** Create a new map in the Vision client. For example, VPLS.
- Step 2** Open the **Add Bridge Domain** to *domain* dialog box in one of the following ways:
- Choose **File Add to Map > Bridge Domain**.
 - In the toolbar, click **Add to Map** and choose **Bridge Domain**.
- Step 3** In the **Add Bridge Domain** dialog box, select **Show All** to display the list of bridge domains.
- Step 4** From the bridge domains, select an I-Bridge and a B-Bridge and click **OK** to add the selected bridges to the map.
- Step 5** Choose **Add to Map > VPLS** to open the **Add Vpls Instance** to *map* dialog box.
- Step 6** In the **Add Vpls Instance** to *map* dialog box, select **Show All** to display the list of VPLS instances.
- Step 7** Add a VPLS instance from the VPLS instances list.
The map displays the link between the VPLS instance and bridge domains.

Viewing EFP Properties

The Vision client provides information about EFPs in a number of ways. For example:

- EFP names displayed in Vision client 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 the Vision client 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 Vision client 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 18-13 shows an example of the EFP Properties window.

Figure 18-13 EFP Properties Window

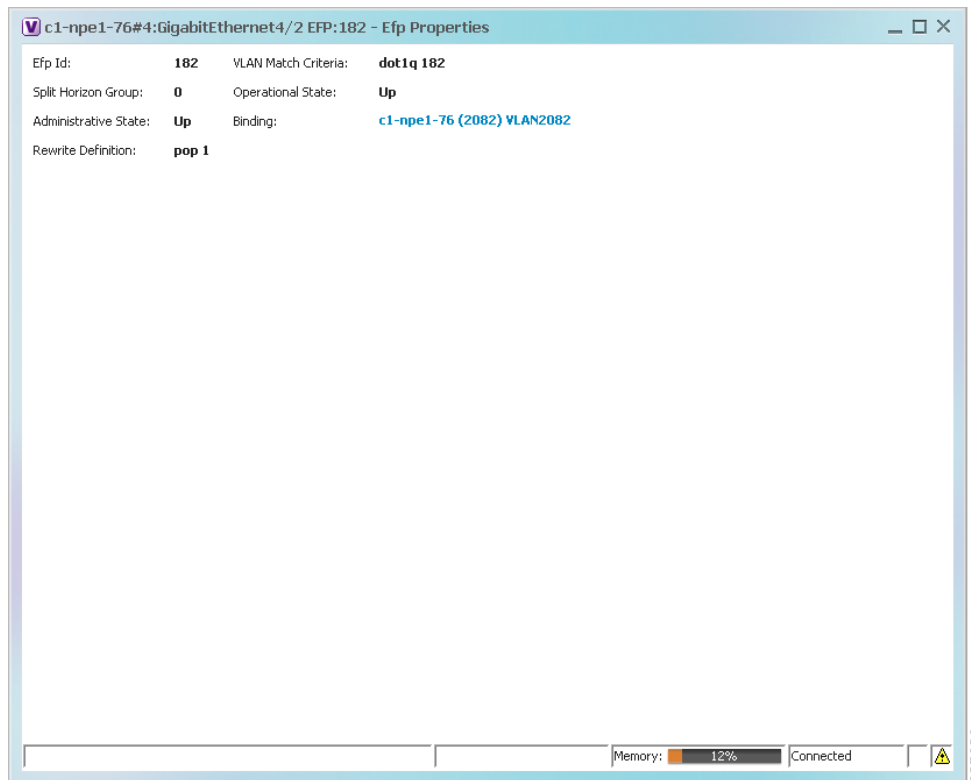


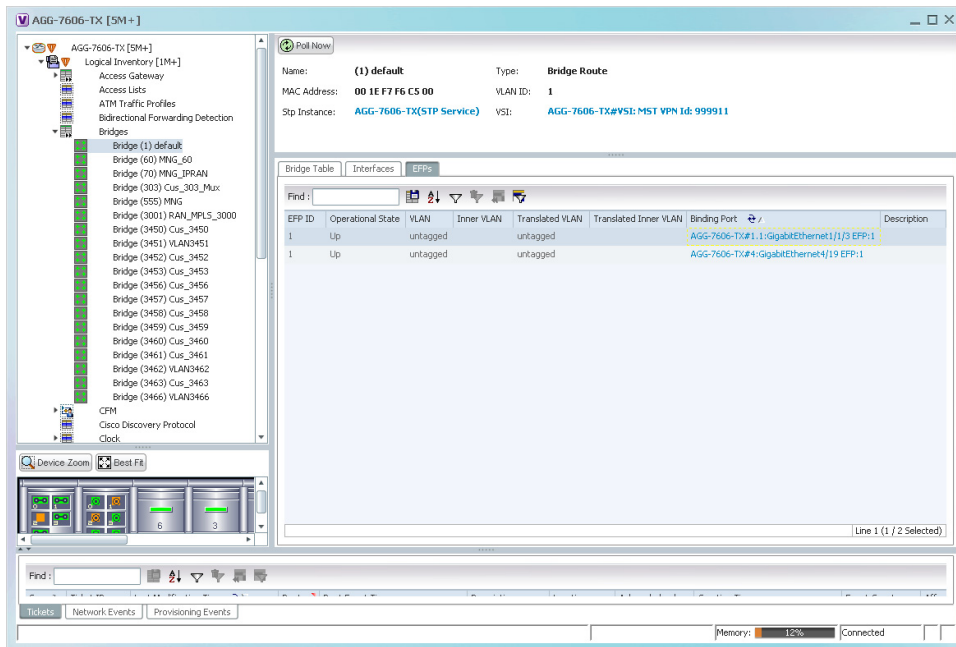
Table 18-26 describes the information displayed in the EFP Properties window.

Table 18-26 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 18-14.

Figure 18-14 Bridge Associated with EFP in Logical Inventory



310621

Table 18-27 describes the information displayed for an EFP associated with a bridge.

Table 18-27 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.
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 18-60](#) 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 18-15](#).

Figure 18-15 EFPs Tab in Physical Inventory

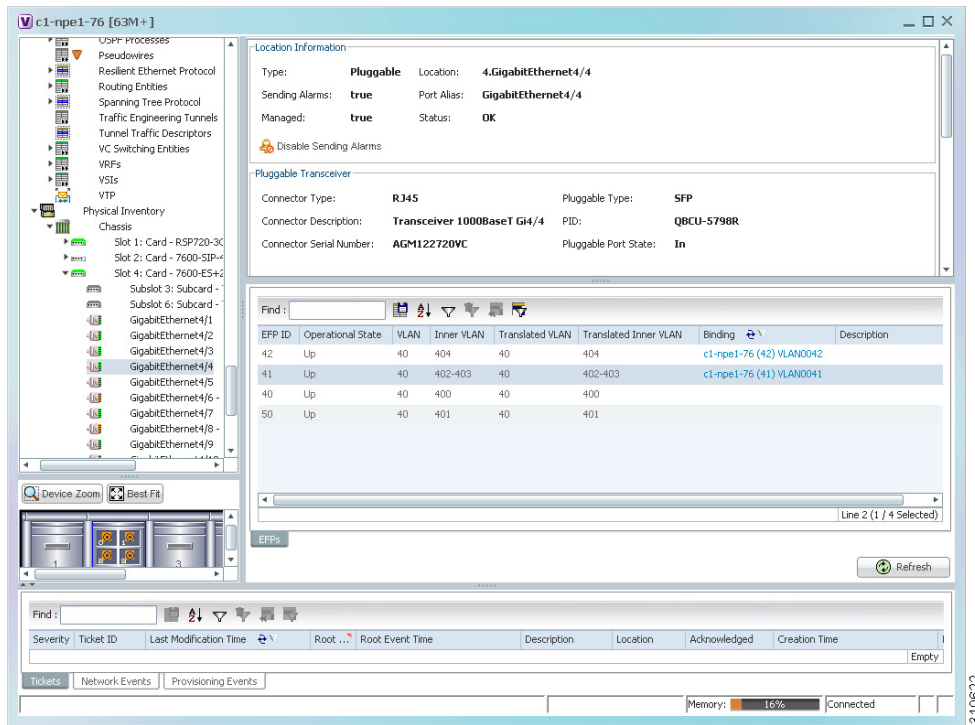


Table 18-28 describes the information displayed in the EFPs tab.

Table 18-28 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**.

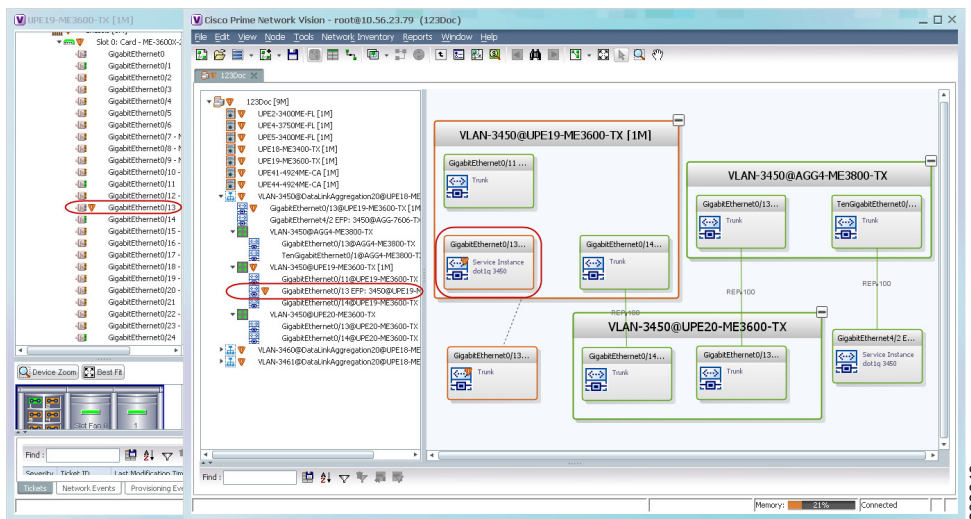
Understanding EFP Severity and Ticket Badges

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.

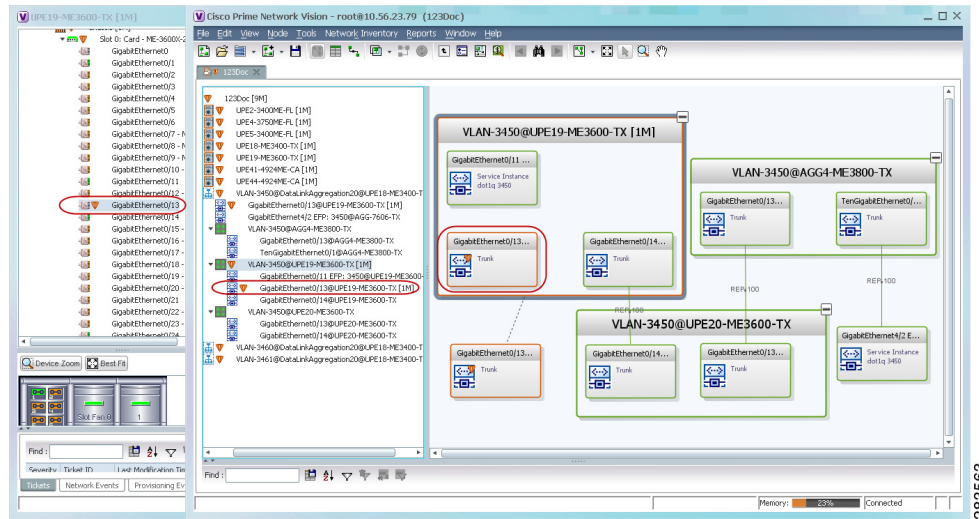
Figure 18-16 shows an example of a ticket badge based on a service instance.

Figure 18-16 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 18-17.

Figure 18-17 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. For information on the devices for which Prime Network discovers and models these key EVC service properties, refer to *Cisco Prime Network 4.1 Supported VNEs*.

Shared Switching Entities and EVC Service View

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

The Vision client 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 the Vision client, double-click the required device.
- Step 2** In the **Inventory** window, choose **Physical Inventory** > **Chassis** > *module* > *port*.

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

Figure 18-18 EVC Port Properties in Physical Inventory

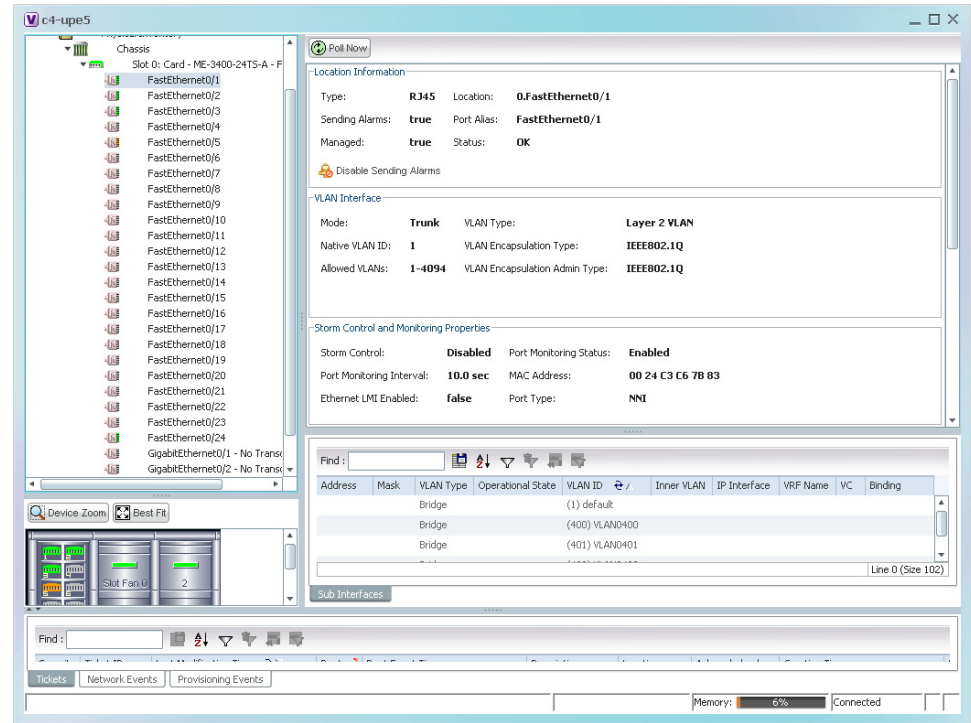


Table 18-29 describes the information displayed for these properties.

Table 18-29 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: <ul style="list-style-type: none"> 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.
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.

Table 18-29 EVC Port Properties in Physical Inventory (continued)

Field	Description
Aging Type	Type of aging used for automatically learned addresses on a secure port: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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.

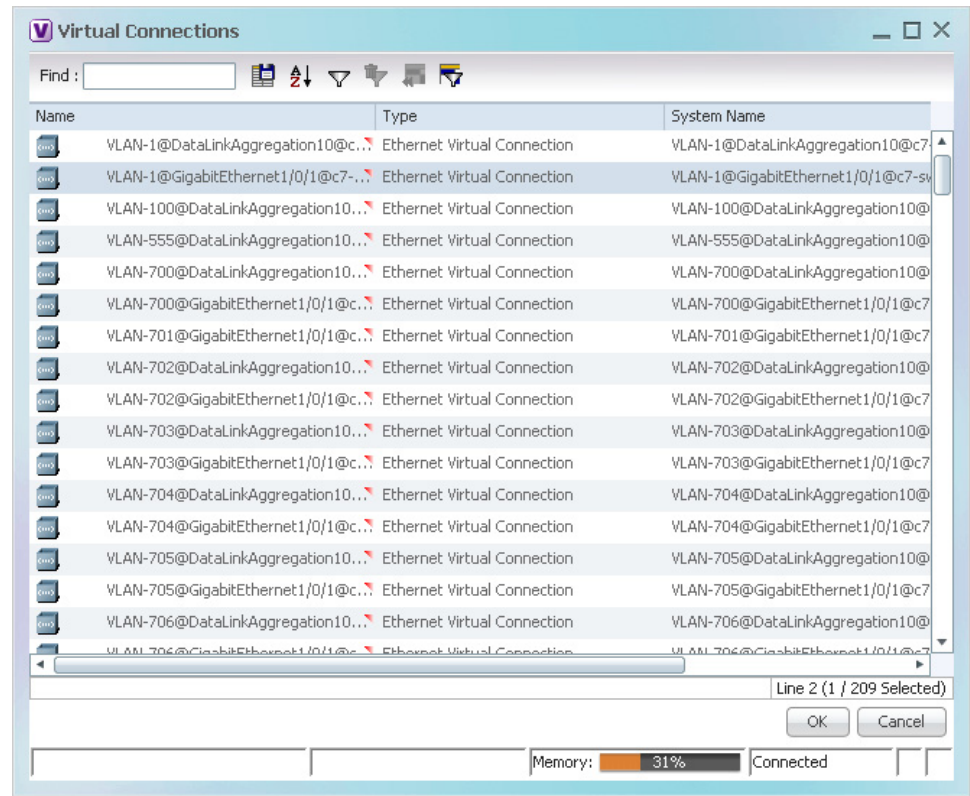
Viewing the Virtual Connections for a Port

In Prime Network, you can view the related virtual connections for an ethernet port or LAG port. In other words, you can view a list of Ethernet Virtual Connections (EVCs) to which the selected port is linked to. The virtual connections can be of type L2 (if the virtual connection is a L2 service) or L3 (if the virtual connection is an L3 service or combination of L2 and L3 service).

To view the related virtual connections for an ethernet port:

-
- Step 1** Right-click on the required device and choose the **Inventory** option.
 - Step 2** In the **Inventory** window, choose **Physical Inventory > Chassis > slot > port**.
 - Step 3** Right-click on the selected port and choose **Get Virtual Connections**. The **Virtual Connections** window is displayed as shown in [Figure 18-19](#).

Figure 18-19 Virtual Connections

**Note**

If no related virtual connections are available for a port, then a message indicating that there are no virtual connections for the port is displayed.

- Step 4** In the Virtual Connections window, select the relevant connections and click **OK**. A temporary map that contains the selected connections is created and displayed in the Prime Network Vision window.
- You can also view the virtual connections for an ethernet link aggregation.

To view the related virtual connections for an ethernet link aggregation:

- Step 1** Right-click on the required device and choose the **Inventory** option.
- Step 2** In the **Inventory** window, choose **Logical Inventory** > **Ethernet Link Aggregation**. The link aggregation details are displayed in the content pane.
- Step 3** In the Data Link Aggregations section, Right-click the ID and select **Get Virtual Connections**. The Virtual Connections window is displayed.
- Step 4** Select the relevant connections and click **OK** to create a temporary map for the connections.

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.

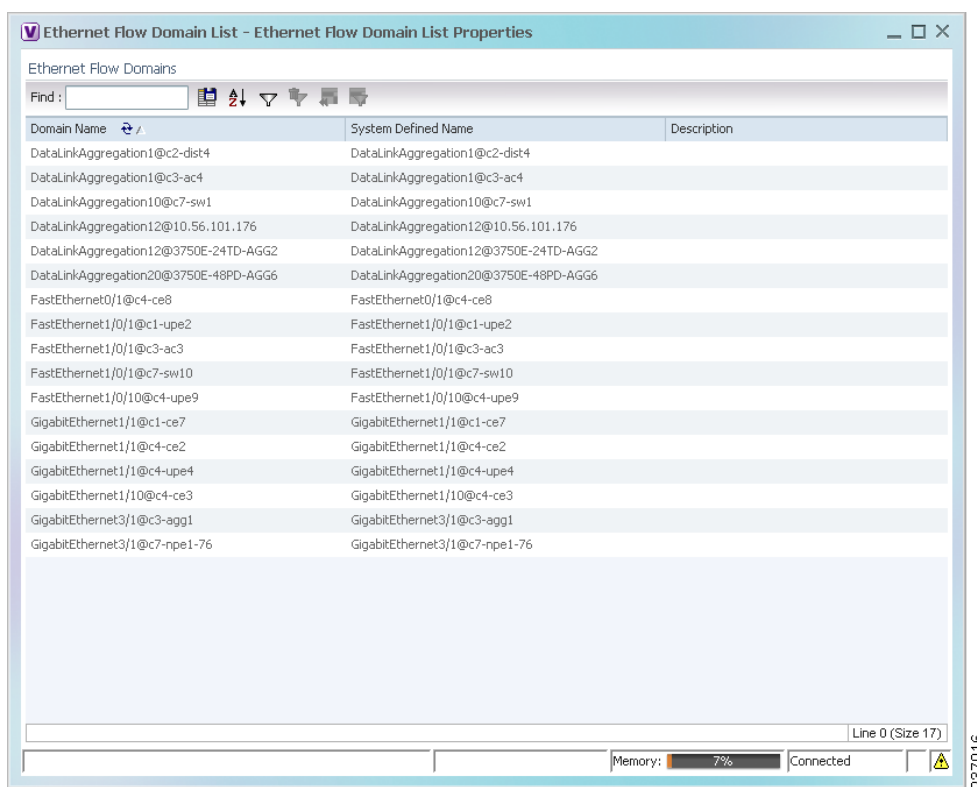
An Ethernet flow domain can have no N-PEs (flat VLAN) or one or more N-PEs (N-PE redundancy configuration). The Ethernet flow domain is defined using physical connectivity at the port level, and not at the network element level. STP is used to mark the root bridge, root or blocked ports, and blocked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

To view Ethernet flow domains:

Step 1 In the Vision client, 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 18-20](#).

Figure 18-20 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 18-21.

Figure 18-21 Ethernet Flow Domain Properties Window

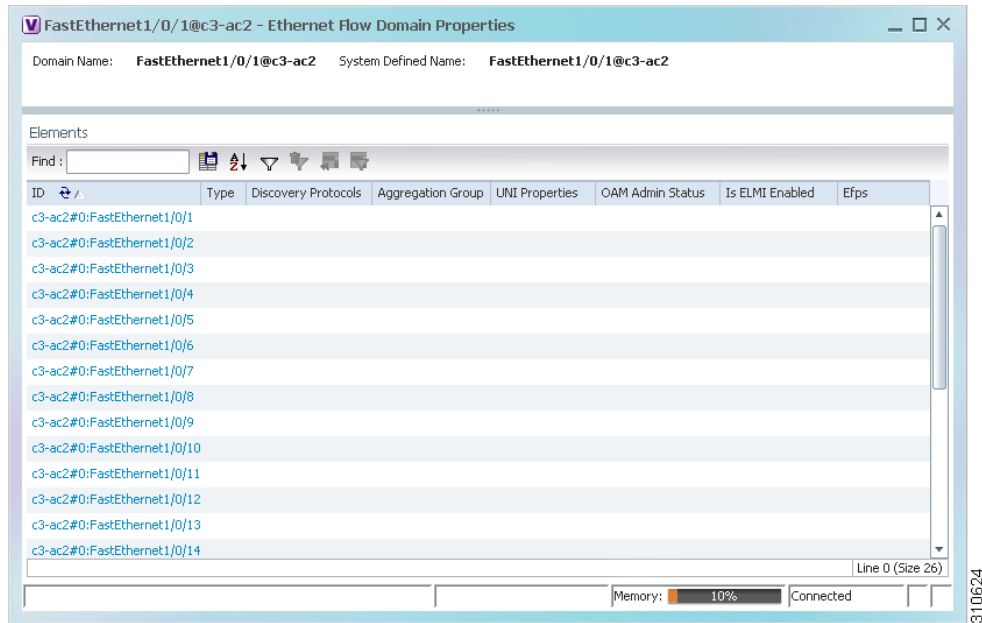


Table 18-30 describes the information displayed in the Ethernet Flow Domain Properties window.



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

Table 18-30 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 802.3 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 Map](#), page 18-77.

- [Understanding VLAN and EFD Discovery](#), page 18-62
- [Understanding VLAN Elements](#), page 18-63
- [Switching Entities Containing Termination Points](#), page 18-67
- [Adding and Removing VLANs from a Map](#), page 18-67
- [Viewing VLAN Mappings](#), page 18-70
- [Working with Associated VLANs](#), page 18-71
- [Viewing VLAN Links Between VLAN Elements and Devices](#), page 18-75
- [Displaying VLANs By Applying VLAN Overlays to a Map](#), page 18-77
- [Viewing VLAN Service Link Properties](#), page 18-80
- [Viewing REP Information in VLAN Domain Views and VLAN Overlays](#), page 18-80
- [Viewing REP Properties for VLAN Service Links](#), page 18-81
- [Viewing STP Information in VLAN Domain Views and VLAN Overlays](#), page 18-83
- [Viewing STP Properties for VLAN Service Links](#), page 18-84
- [Viewing VLAN Trunk Group Properties](#), page 18-85
- [Viewing VLAN Bridge Properties](#), page 18-87
- [Using Commands to Work With VLANs](#), page 18-89

Understanding VLAN and EFD Discovery

When you start the Prime Network gateway the first time, the Prime Network 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 does not add VNEs or apply updates to existing VLANs or EFDs.

After the initial delay has passed, Prime Network 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 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 the Vision Client](#), page 18-63
- [VLANs](#), page 18-63
- [Switching Entities](#), page 18-63
- [Ethernet Flow Points](#), page 18-64

VLAN Elements in the Vision Client

Table 18-31 describes the icons that the Vision client uses to represent VLAN elements.

Table 18-31 VLAN Elements and Icons in the Vision Window

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

VLANs

Prime Network 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 the Vision client 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

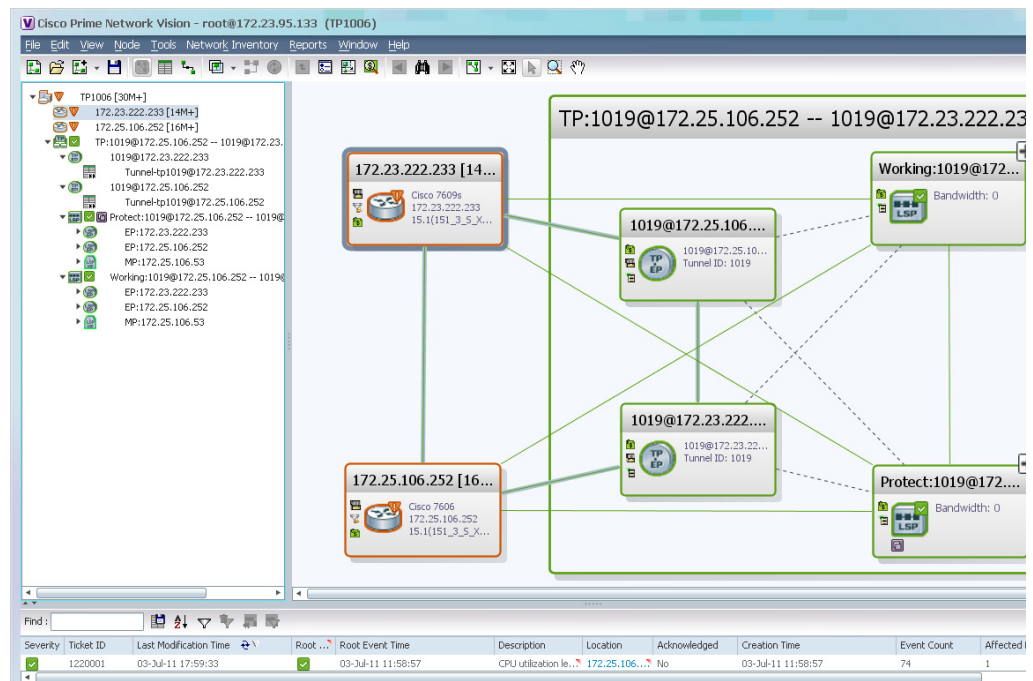
An Ethernet flow point (EFP) can represent a port that is configured for participation in a specific VLAN.

If you right-click an EFP in the Vision client 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 18-22 shows an example of EFPs configured as switch ports in the Vision client.

Figure 18-22 EFPs Configured as Switch Ports

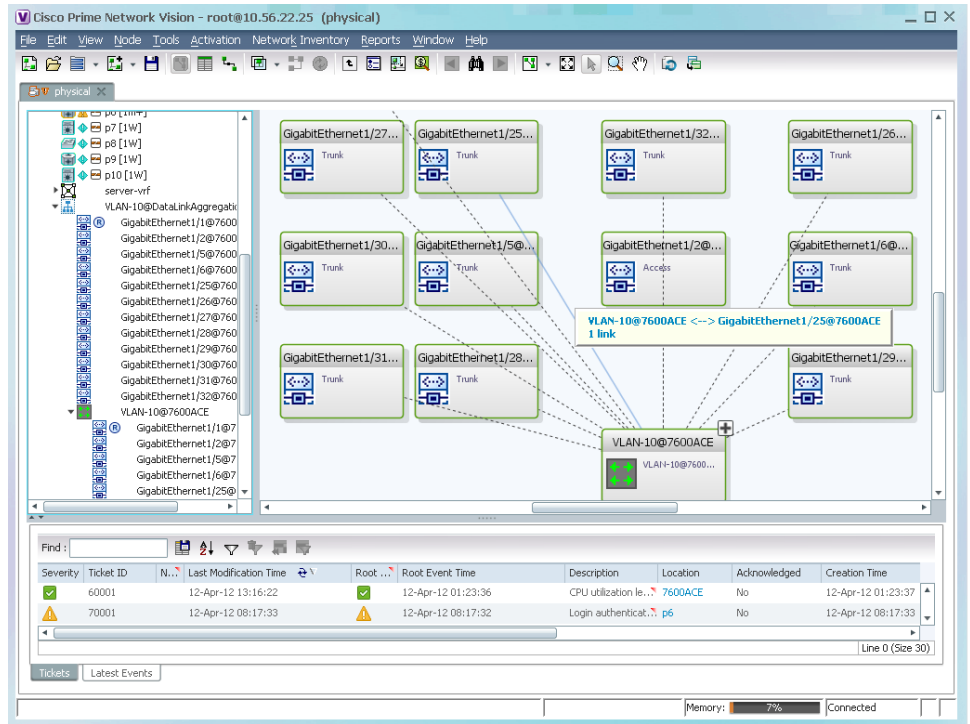


EFPs that are located directly inside a VLAN represent one of the following:

- 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 (for example, in 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 18-23.

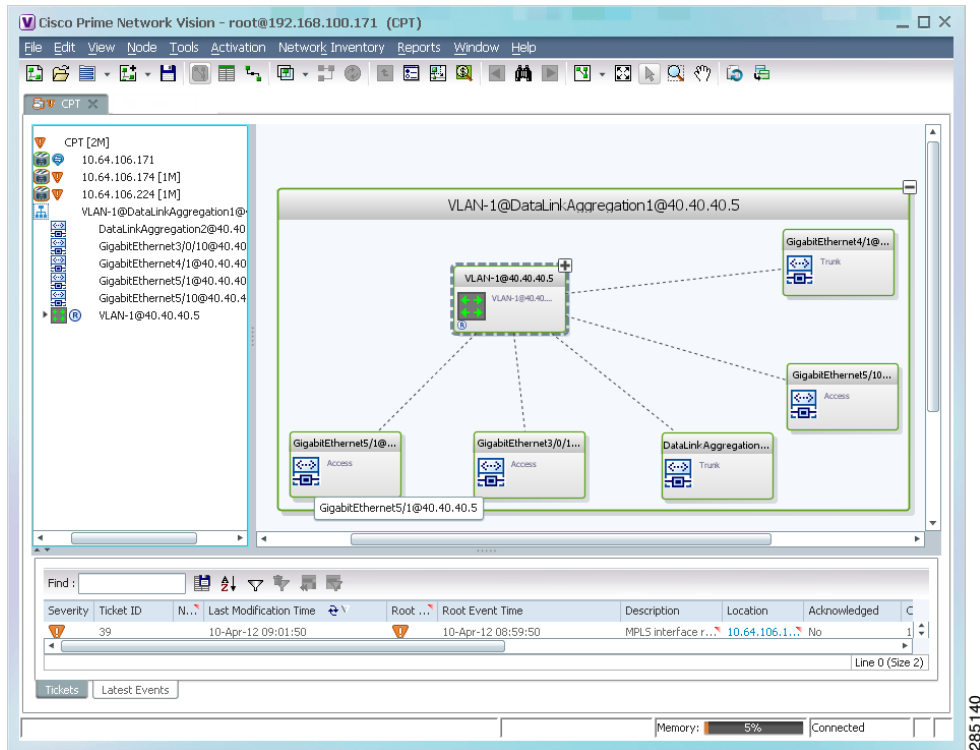
Figure 18-23 Termination Point EFP Inside a VLAN



- **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.

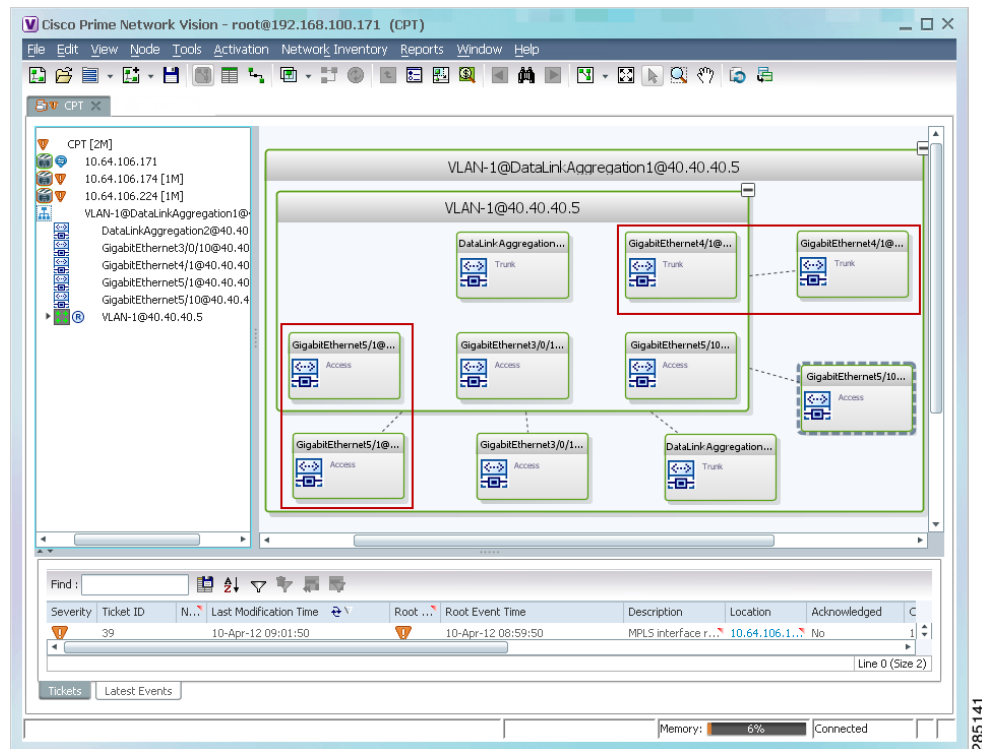
In the Vision client, edge EFPs are displayed directly under the VLAN at the same level as their switching entities and are connected to their corresponding switching entities by a dotted link, as shown in Figure 18-24.

Figure 18-24 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 18-25:

Figure 18-25 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 the Vision client after a few minutes.

Switching Entities Containing Termination Points

For certain devices (for example, the Cisco 7600 series, Cisco GSR series, 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 and are not currently displayed in the map.



Note

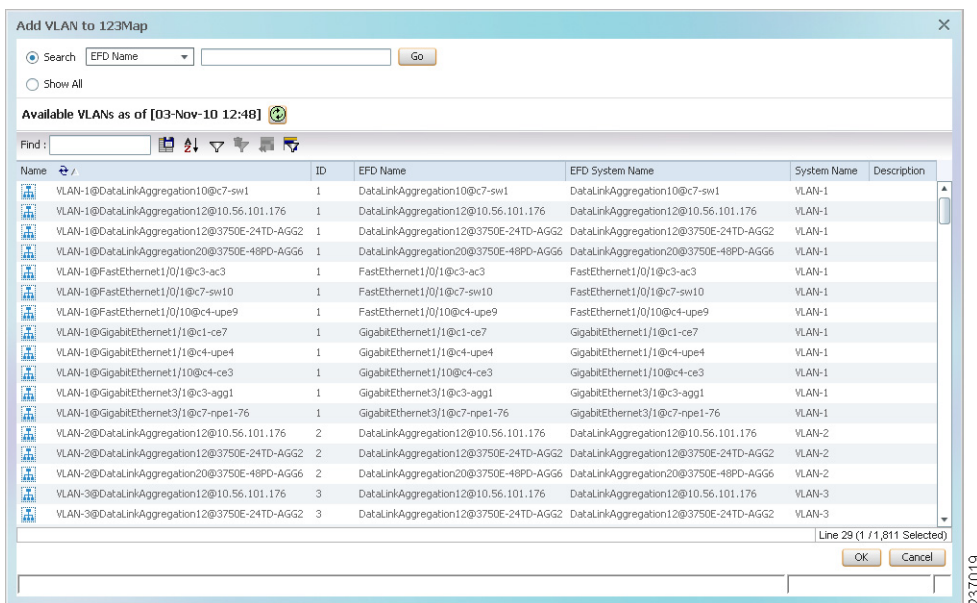
Adding VLANs affects other users if they are working with the same map.

To add VLANs to a map:

Step 1 In the Vision client, 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 18-26](#).

Figure 18-26 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,” the Vision client displays VPNs “net” and “NET” in the names whether net appears at the beginning, middle, or at the end of the name: for example, Ethernet.
- Choose **Show All** to display all the VLANs.

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



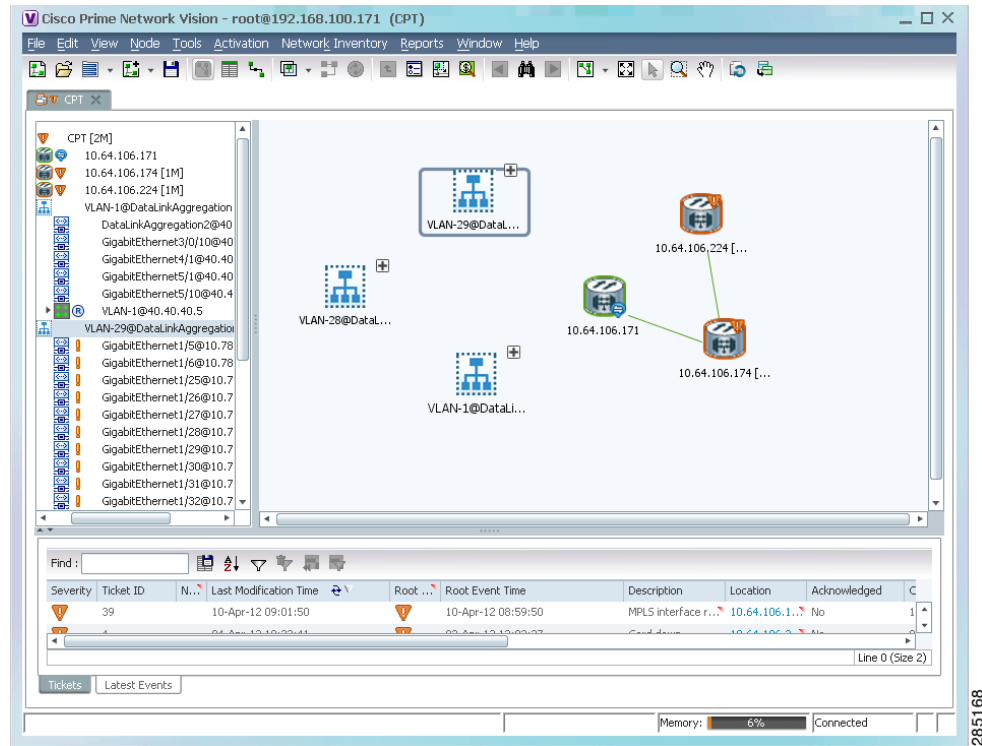
Tip Press **Shift** or **Ctrl** to choose multiple adjoining or nonconsecutive VLANs.

Step 5 Click **OK**.

The VLANs are displayed in the Vision client content pane as shown in [Figure 18-27](#).

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

Figure 18-27 VLANs in Map View



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

- [Viewing and Renaming Ethernet Flow Domains, page 18-60](#)
- [Viewing EFP Properties, page 18-51](#)

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 18-9](#)
- [Viewing REP Information in VLAN Domain Views and VLAN Overlays, page 18-80](#)
- [Viewing REP Properties for VLAN Service Links, page 18-81](#)

For STP, see:

- [Viewing Spanning Tree Protocol Properties, page 18-5](#)
- [Viewing STP Information in VLAN Domain Views and VLAN Overlays, page 18-83](#)
- [Viewing STP Properties for VLAN Service Links, page 18-84](#)

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 Vision client 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 the Vision client, 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 18-28](#).

Figure 18-28 VLAN Mappings Tab in Physical Inventory

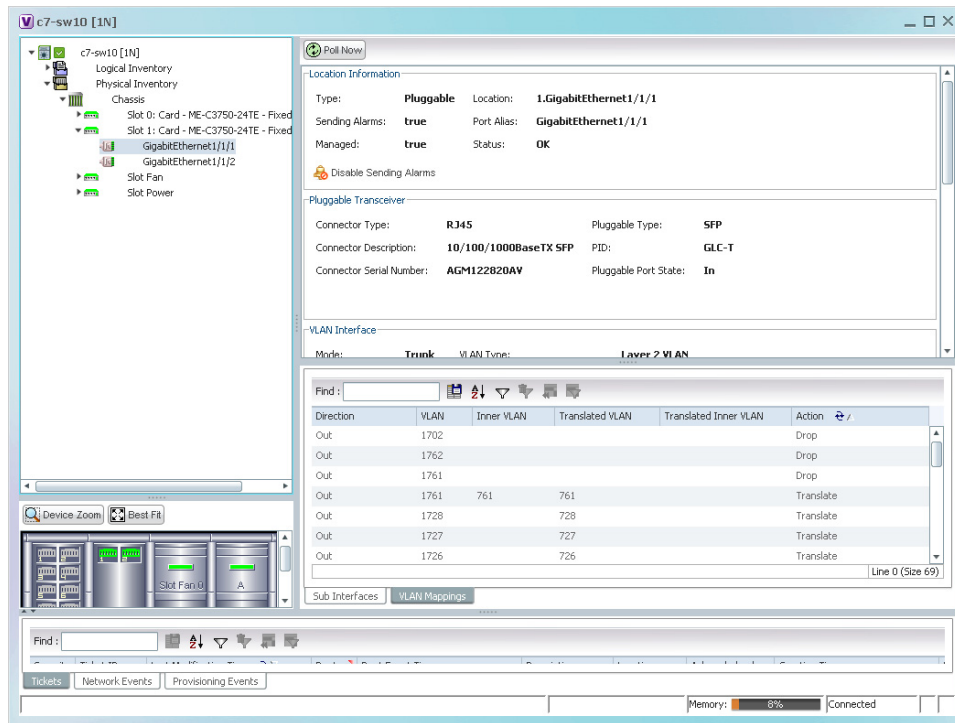


Table 18-32 describes the information that is displayed in the VLAN Mappings table.

Table 18-32 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 discovers associations between network VLANs and displays the information in the Vision client. Network VLAN associations are represented by VLAN service links, and can be any of the tag manipulation types described in Table 18-33.

Table 18-33 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	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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:

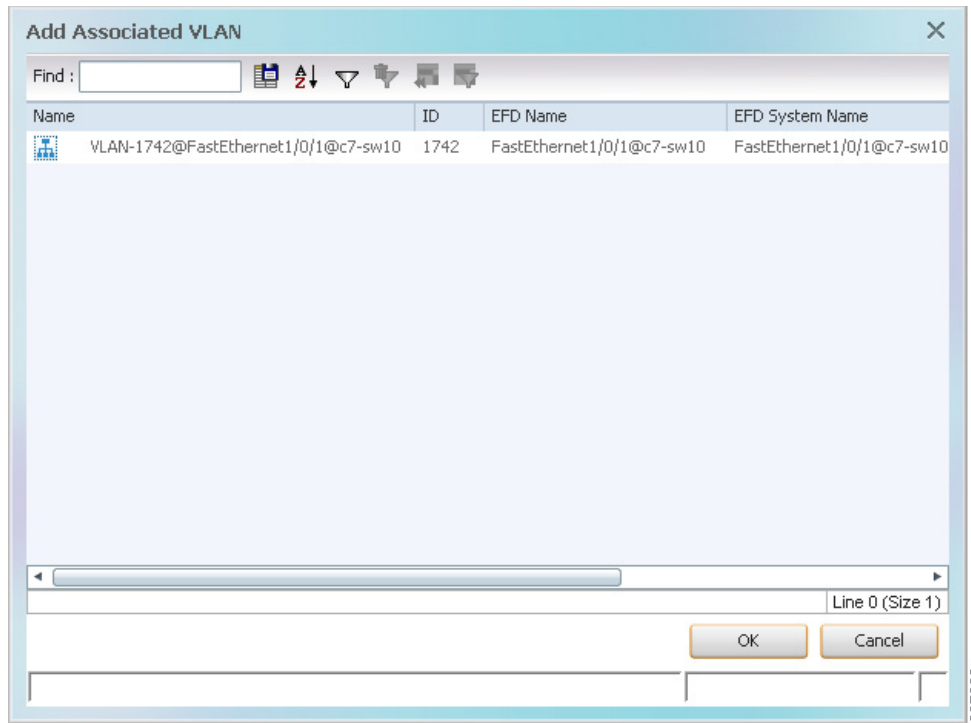
- Add an associated VLAN—See [Adding an Associated VLAN, page 18-72](#).
- View properties for associated VLANs—See [Viewing Associated Network VLAN Service Links and VLAN Mapping Properties, page 18-74](#).

Adding an Associated VLAN

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

-
- Step 1** In the Vision client, 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 18-29](#).

Figure 18-29 Add Associated VLAN Window

In this example, the selected network VLAN has one associated VLAN: VLAN-1742. [Table 18-34](#) describes the information displayed in the Add Associated VLAN table.

Table 18-34 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 the Vision client.

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 the Vision client in the thumbnail view.
- View VLAN mapping properties in the Link Properties window.

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

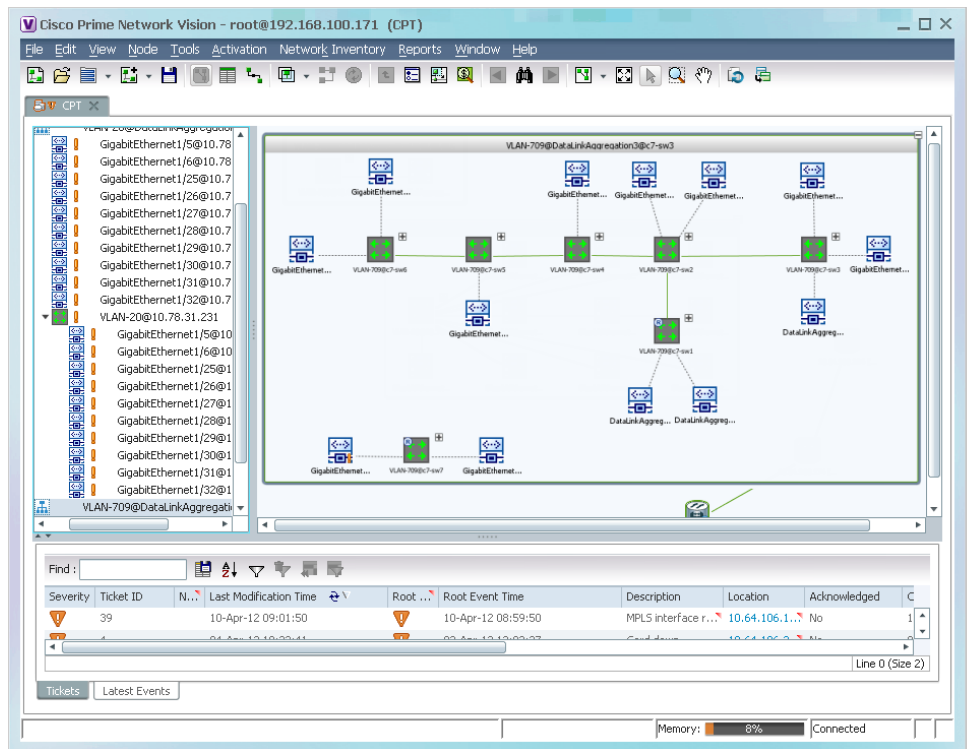
Step 1 Select the required network VLAN in the map view.

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

Figure 18-30 shows an example of a network VLAN in a thumbnail.

The VLAN service links are displayed as 5.2 between the associated network VLANs. The links represent the connections between the Ethernet flow points that are part of each network VLAN.

Figure 18-30 VLAN Service Links Between Associated Network VLANs

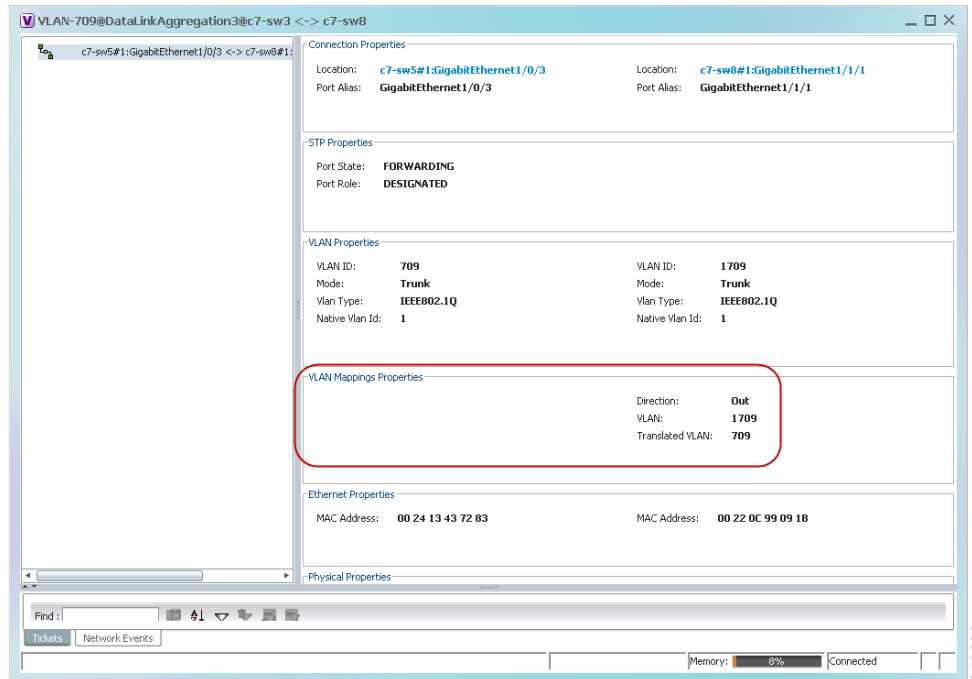


Step 3 To view additional information, right-click a link, and choose **Properties**.

The Link Properties window is displayed as shown in Figure 18-31.

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 18-31](#), 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 18-31 VLAN Mapping Properties in Link Properties Window



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

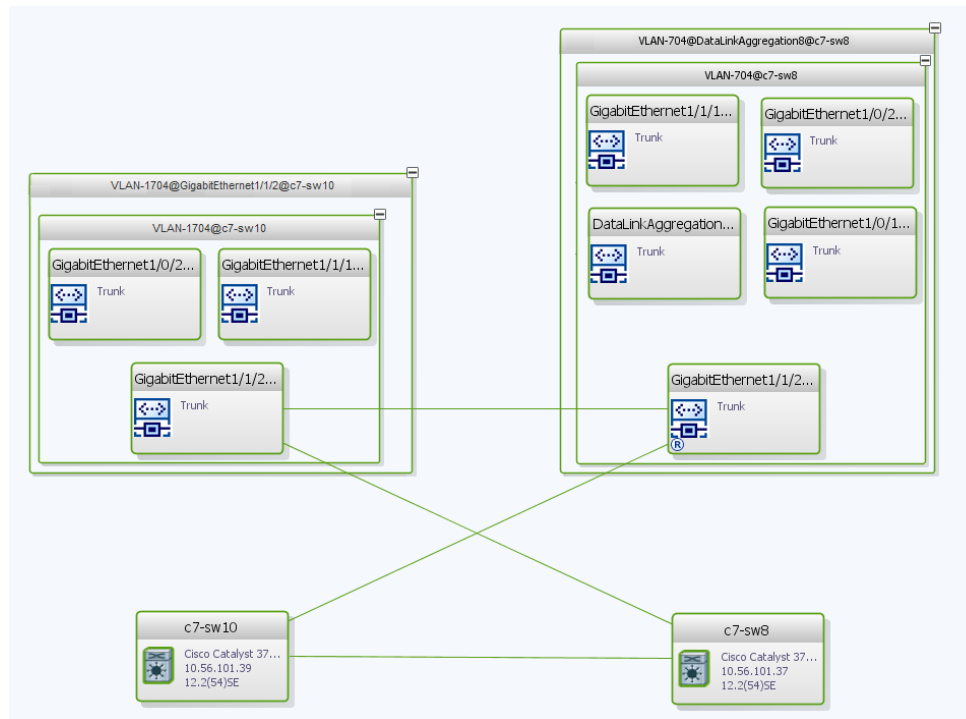
- [Viewing REP Properties for VLAN Service Links, page 18-81](#)
- [Viewing STP Properties for VLAN Service Links, page 18-84](#)

Viewing VLAN Links Between VLAN Elements and Devices

If a Vision client 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 18-32](#) and described in the following paragraphs.

Figure 18-32 VLAN Elements and Devices in the Vision Window



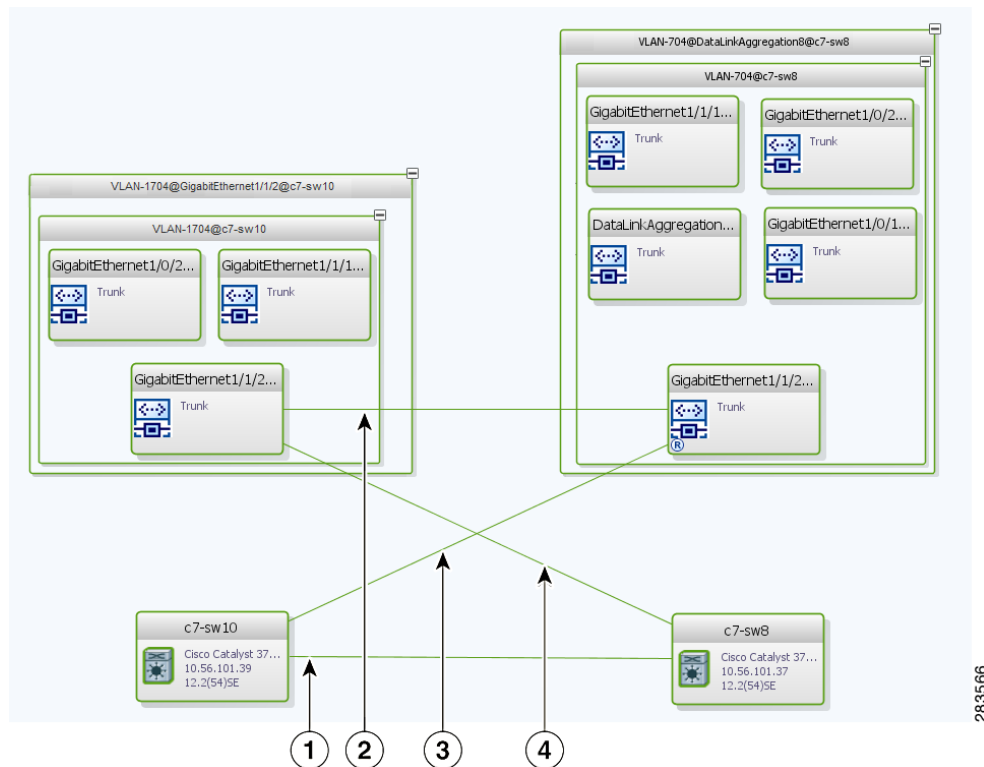
The elements are configured as follows:

- 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 18-33](#) and described in the following table.

Figure 18-33 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 Map

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

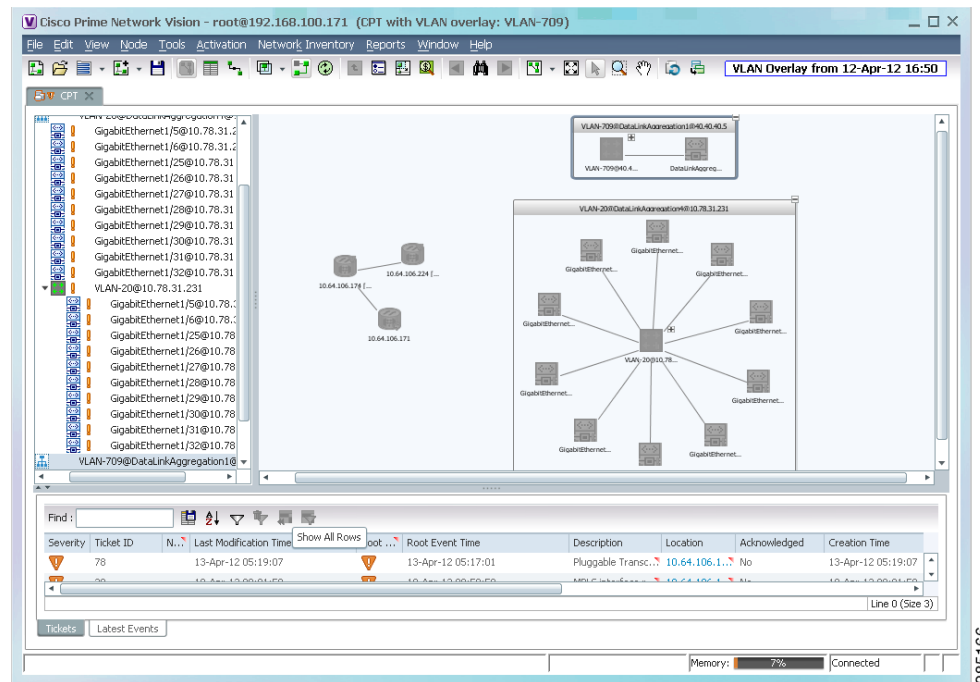
To add a VLAN overlay:

-
- Step 1** Display the network map for which you want to create an overlay in the Vision client.
 - 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,” the Vision client 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 18-34](#).

Figure 18-34 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 18-81
- [Viewing STP Properties for VLAN Service Links](#), page 18-84
- [Viewing Associated Network VLAN Service Links and VLAN Mapping Properties](#), page 18-74

Viewing REP Information in VLAN Domain Views and VLAN Overlays

You can view REP segment and port information in the Vision client 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 18-35](#) describes the icons and badges used to represent REP segment and port information.

Table 18-35 REP Icons and Badges in VLAN Domain Views and Overlays




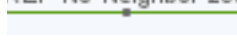



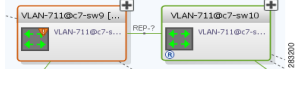


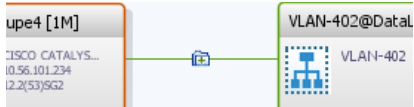
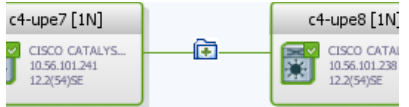

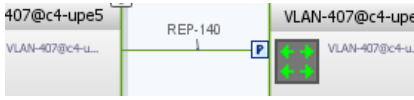



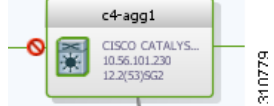


Item	Description	VLAN Domain View	VLAN Overlay
	REP identifier—Uses the format REP- <i>id</i> where <i>id</i> represents the REP segment identifier.	 The REP identifier is displayed in the domain view if the visual link represents only one link. If the visual link represents more than one link, no REP 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 <i>segment</i> —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 18-35 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 a VLAN overlay view if either of the following is true: <ul style="list-style-type: none"> • 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 18-35 shows an example of the Link Properties window with REP information.

Figure 18-35 VLAN Service Link Properties Window with REP Information

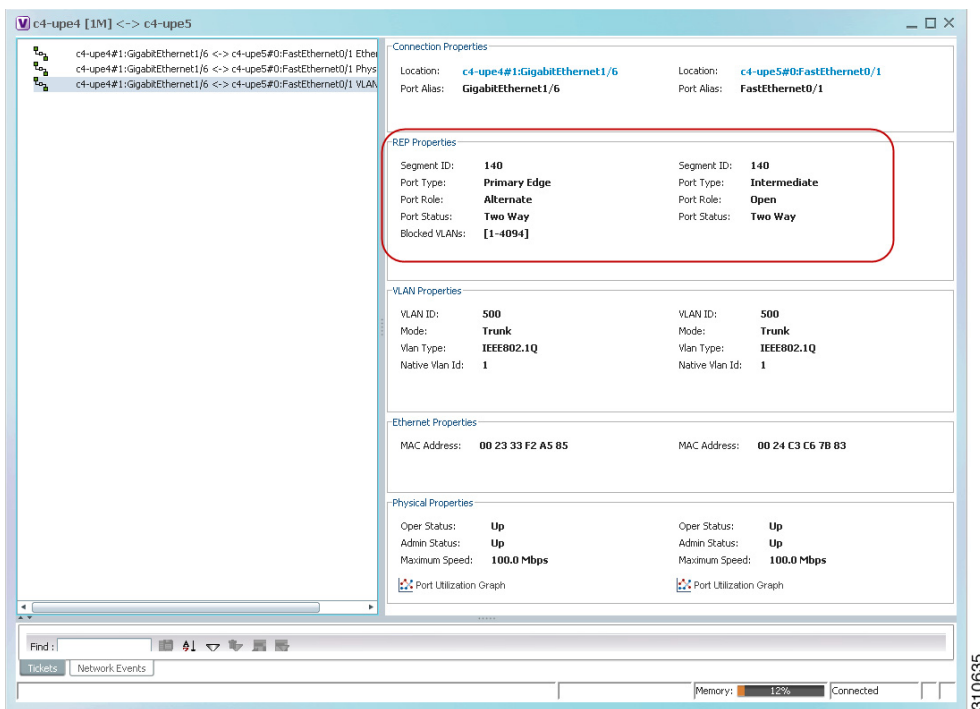


Table 18-36 describes the information that is displayed for REP for each end of the link.








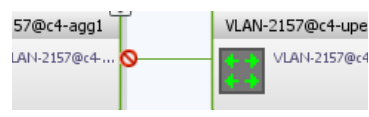

Table 18-36 REP Properties in VLAN Service Link Properties Window

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 the Vision client 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 18-37](#) describes the icons and badges used to represent STP link and port information.

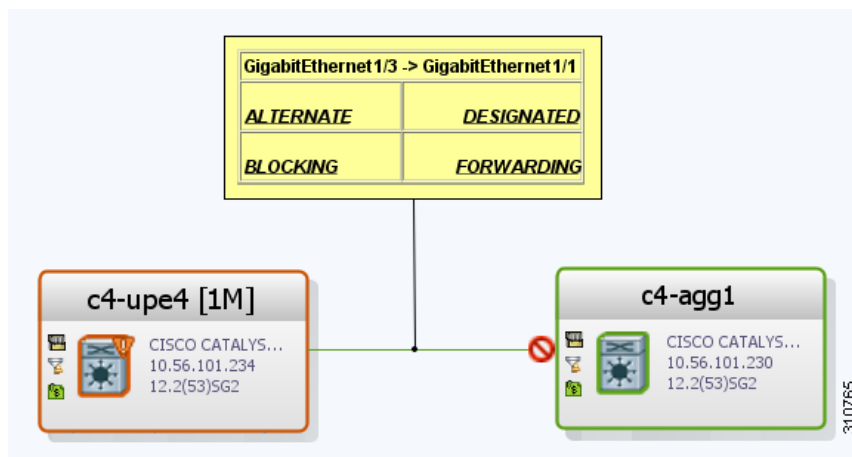
Table 18-37 STP Information in VLAN Domain Views and Overlays

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 18-36](#):

- Port name
- Port role
- Port state

Figure 18-36 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 18-37 shows an example of the Link Properties window with STP information.

Figure 18-37 STP Properties in VLAN Service Link Properties Window

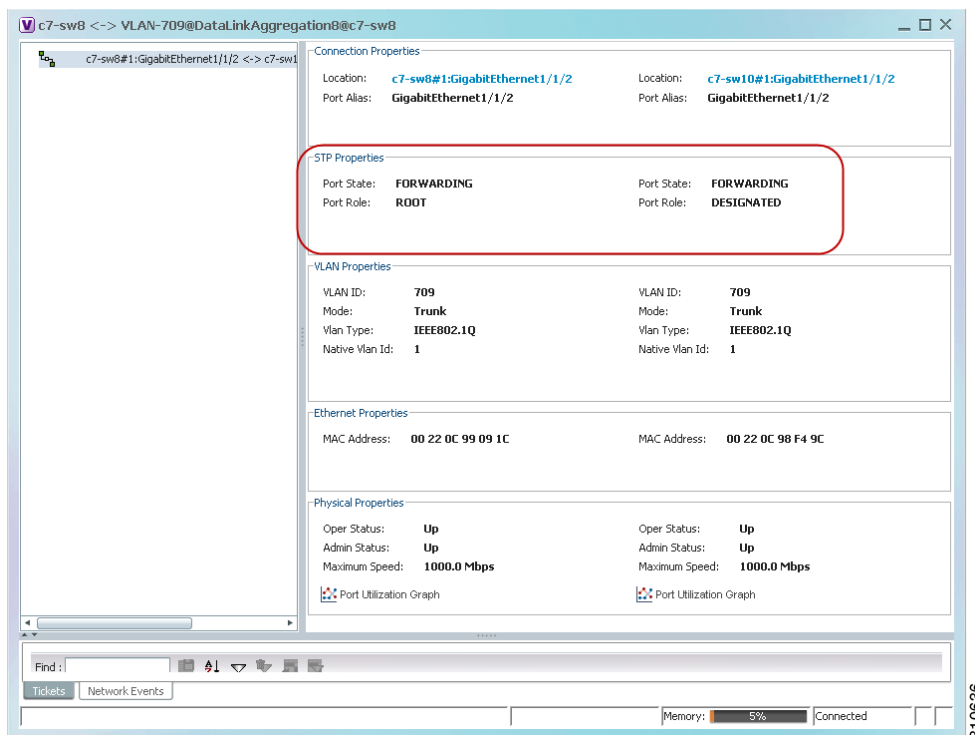


Table 18-38 describes the information that is displayed for STP for the VLAN service link.

Table 18-38 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.

The Vision client 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.

The Vision client shows all VTP modes: Server, Client, Transparent, and Off. For each mode, the Vision client displays the relevant mode information such as VTP domain, VTP mode, VTP version, VLAN trunks, and the trunk encapsulation. The Vision client 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 the Vision client, 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 18-38](#).

Figure 18-38 VTP Domain Properties Window in Logical Inventory

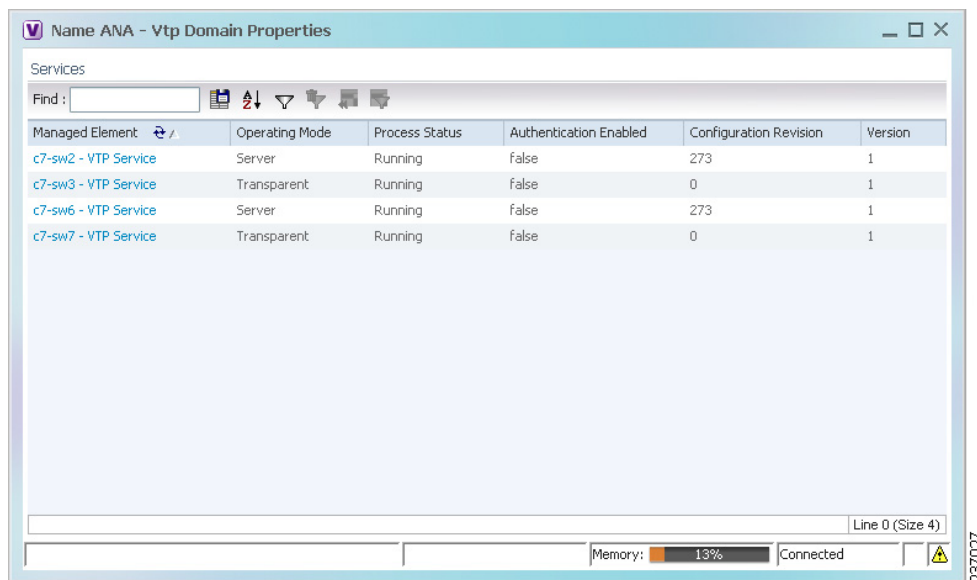


Table 18-39 describes the information that is displayed in the VTP Domain Properties window.

Table 18-39 VTP Domain Properties Window

Field	Description
Managed Element	Managed element name, hyperlinked to VTP in logical inventory.
Operating Mode	<p>VTP operating mode:</p> <ul style="list-style-type: none"> • 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	<p>Whether or not VTP authentication is enabled: True or False.</p> <p>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.</p>
Configuration Revision	<p>32-bit number that indicates the level of revision for a VTP packet.</p> <p>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.</p>
Version	VTP version: 1, 2, or 3.

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

Table 18-40 describes the VTP information that is displayed in the inventory window content pane.

Table 18-40 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	<p>Whether or not VTP pruning is enabled: True or False.</p> <p>VTP pruning increases available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to access the appropriate network devices.</p>

Table 18-40 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 Vision client inventory window and choosing Bridges in logical inventory.

To view VLAN bridge properties:

Step 1 In the Vision client, 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 18-39](#).

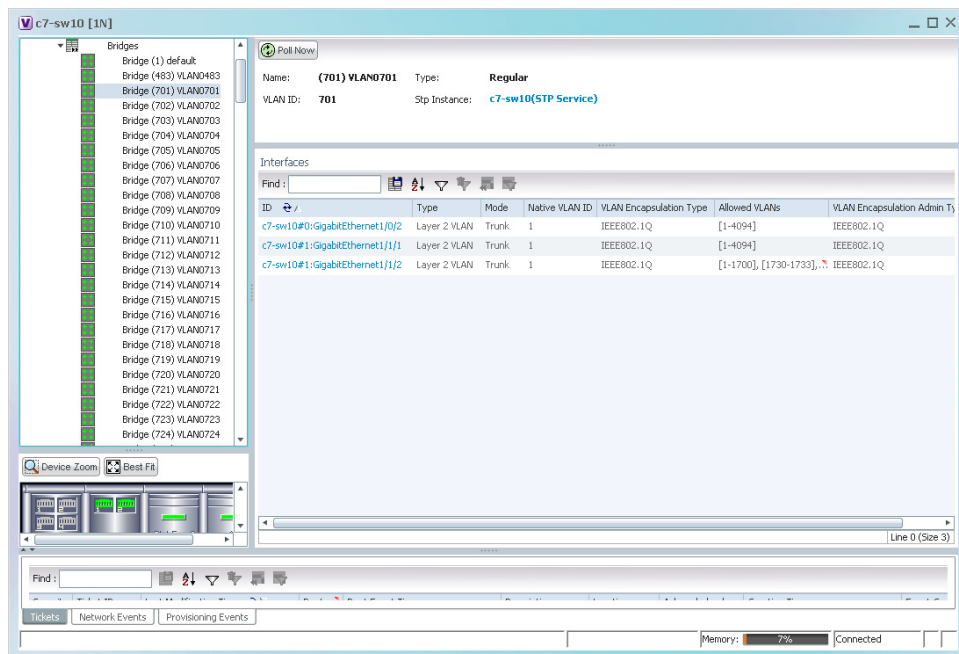
Figure 18-39 VLAN Bridge Properties in Logical Inventory

Table 18-41 describes the information that is displayed. Depending on the bridge configuration, any of the tabs might be displayed for the selected bridge.

Table 18-41 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: <ul style="list-style-type: none"> 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 18-41 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**. Your permissions determine whether you can run these commands (see [Permissions for Managing Carrier Ethernet, page B-12](#)). To find out if a device supports these commands, see the [Cisco Prime Network 5.2 Supported Cisco VNEs](#).

Table 18-42 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

Working with VXLANs

The following topics provide information and properties for working with VXLANs.

[Understanding Virtual Extensible LAN \(VXLAN\) and BGP EVPN Address Family, page 18-90](#)

[Viewing VXLAN Properties, page 18-91](#)

Understanding Virtual Extensible LAN (VXLAN) and BGP EVPN Address Family

Virtual Extensible LAN (VXLAN) is an overlay virtual network technology that is built on top of existing network Layer 2 and Layer 3 technologies to support elastic compute architectures. VXLAN uses VXLAN Identifier (VNI) that is similar to a VLAN ID to identify a user. VNI is a 24 bit ID which enables scalability of up to 16 million VNIs. Also, it is interchangeable with VXLAN Segment ID.

VXLAN architecture consists of following devices.

- Spine Devices— Spine devices are responsible for learning infrastructure routes and end-host subnet routes. Leaf devices communicate with their peers through Spine devices. Spine layer is the backbone of the network and is responsible for interconnecting all leaf switches fabric.
- Access Leaf Devices—Consists of access switches that connect to Ethernet devices such as servers (host interfaces)
- Border Leaf Devices—Connects to external network devices or services like router ports.



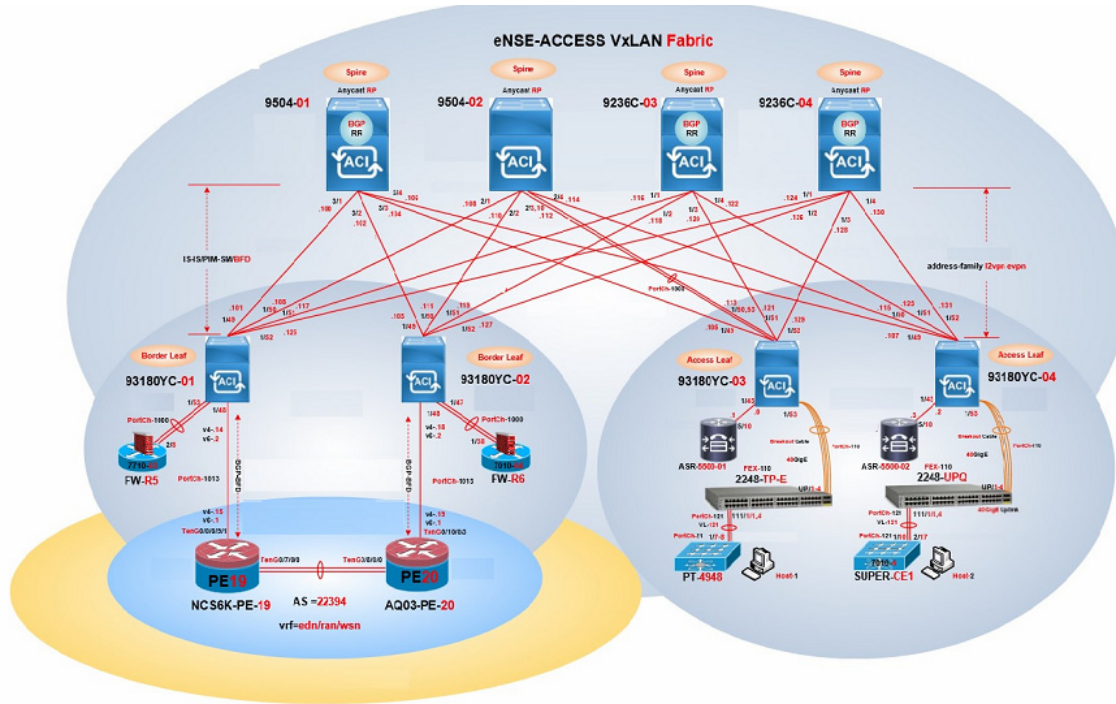
Note

VXLAN is enabled only on Leaf devices and not on Spine devices. BGP is used as an underlay protocol in Spine devices.

Prime Network 5.2 supports VXLAN and BGP EVPN Address Family in inventory and fault. You can find associated VNIs information in logical inventory.

VXLAN Architecture

Figure 18-40 VXLAN Architecture



Viewing VXLAN Properties

To view VXLAN information:

- Step 1** Right-click the required device in the Vision client and choose **Inventory**.
- Step 2** In the logical inventory window, choose **Logical Inventory > VXLANs > VXLAN**.
Table 18-43 describes the information that is displayed for VXLAN.

Table 18-43 VXLAN Information in Logical Inventory

Field	Description
Name	Name of the VXLAN.
VNI Details Tab	
VNI	VXLAN identifier used to identify a user.
NVE Interface	The name of the endpoint interface.
Multicast Group	The IP address of the multicast group.
State	The state of the VNI.
Mode	The mode of the VNI (For example, Control Plane or Data Plane)

Table 18-43 VXLAN Information in Logical Inventory (continued)

Field	Description
Layer Type	The type of the layer of the VNI. For example, L2 for a bridge/VLAN and L3 for a VRF.
Associated VLAN	The link to the associated entity, which when clicked will highlight the associated Bridges record under the Bridges node .
Associated VRF	The link to the associated entity, which when clicked will highlight the Associated VRF record under the VRF node .
Flags	Displays the flag information pertaining to the VNI.
VNI Neighbors Tab	
NVE Interface	The name of the endpoint interface.
Peer IP	Remote peer IP address.
Peer State	State of the remote peer. For example, Up or Down.
Learn Type	The learn type of the peer (For example, Control or Data Plane).
Peer UP Time	The amount of time the interface has been active.
Router MAC Address	MAC address of the router.

Mapping Associated VNI to Bridges

To view the VXLAN ID associated with a bridge:

1. Double-click the required device in the Vision client.
2. In the **Logical Inventory** window, choose **Logical Inventory** > Context > **Bridges** > **Bridge**.
3. Click the required bridge. The **Associated VNI** field in the content pane displays the VXLAN ID associated with the bridge or VLAN. You can click the link to go to the corresponding VNI row in the VNI Details pane.

**Note**

The **Associated VNI** field is not visible in the content pane if there is no VNI associated with the bridge.

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 Vision client map.

Adding Unassociated Bridges

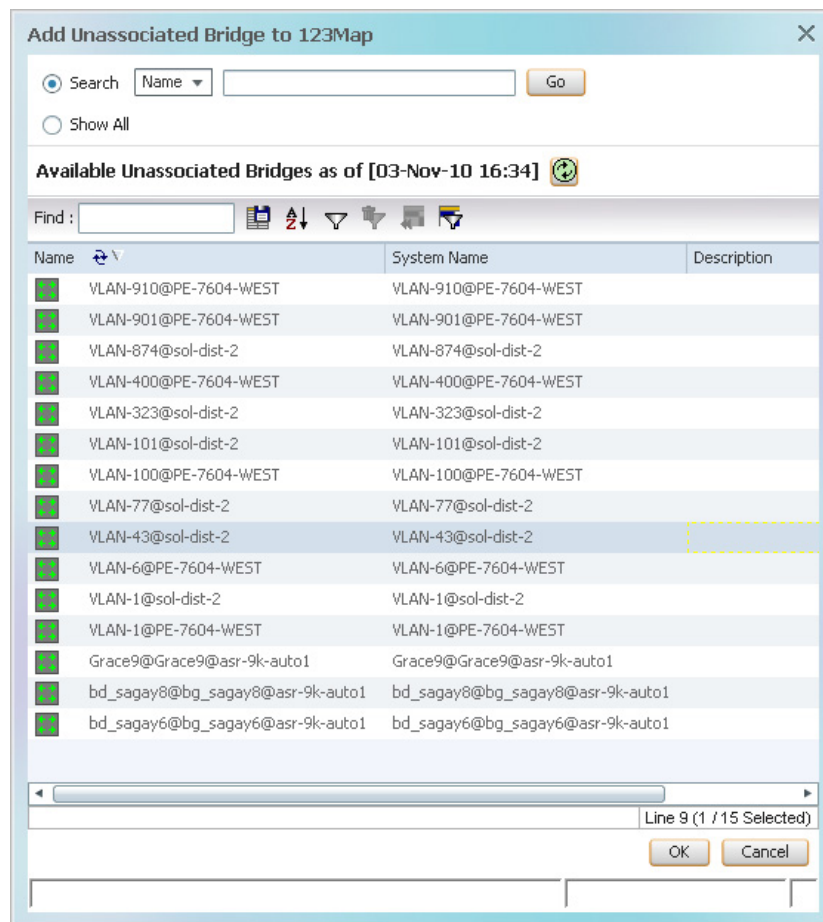
The Vision client enables you to add unassociated bridges to maps and to view their properties.

To add an unassociated bridge to a map:

- Step 1** In the Vision client, 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**.

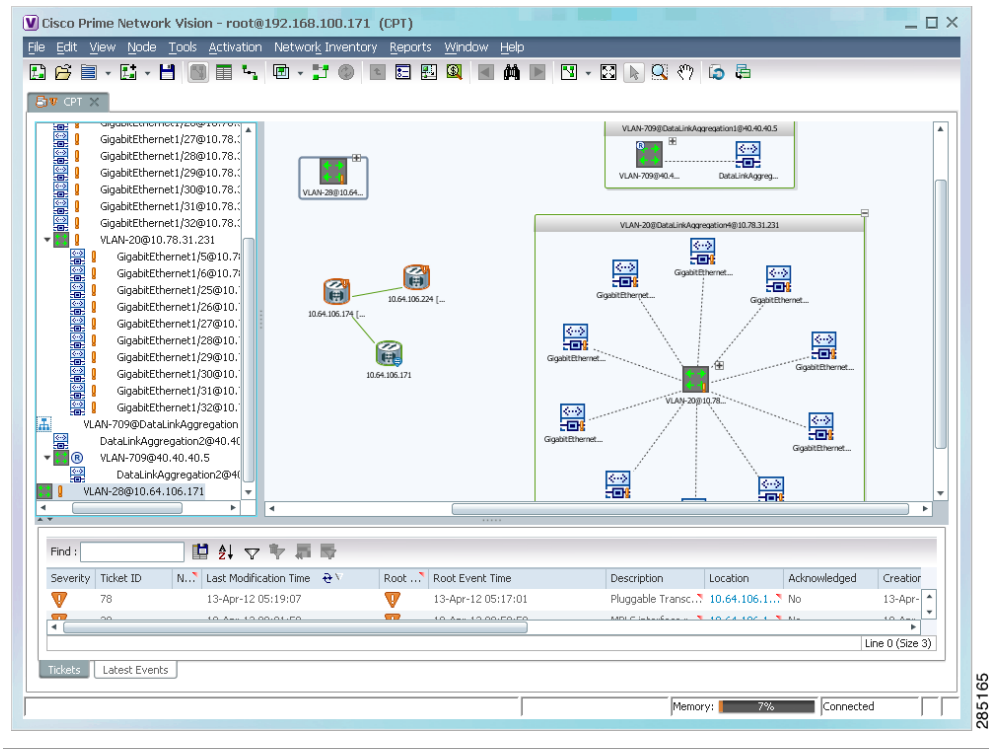
Figure 18-41 shows an example of the Add Unassociated Bridge dialog box.

Figure 18-41 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 18-42.

Figure 18-42 Unassociated Bridge in the Vision Window



Working with Ethernet Flow Point Cross-Connects

Prime Network automatically discovers Ethernet flow point (EFP) cross-connects, also known as locally switched EFPs. Prime Network 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 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, the Vision client displays the links between them and the cross-connect as well.

The Vision client 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 18-94](#)
- [Viewing EFP Cross-Connect Properties, page 18-95](#)

Adding EFP Cross-Connects

To add an EFP cross-connect to a map:

- Step 1** In the Vision client, 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 the Vision client, 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 18-43](#)).

Figure 18-43 Local Switching Table in Logical Inventory

Key	Entry Status	Segment 1	Segment 1 Port Name	Segment 1 Status	Segment 2
1-alna3	Up	c4-npe1-76#4.0:GigabitEthernet4/0/3	GigabitEthernet4/0/3	Up	c4-npe1-76#
2-alna	Up	c4-npe1-76#4.0:GigabitEthernet4/0/2.444	GigabitEthernet4/0/2.444	Up	c4-npe1-76#
3-alna2	Up	c4-npe1-76#4.0:GigabitEthernet4/0/2:EFP:555	GigabitEthernet4/0/2:555	Up	c4-npe1-76#

[Table 18-44](#) describes the information displayed for the EFP cross-connects in the Local Switching Table.

Table 18-44 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.

Table 18-44 EFP Cross-Connect Properties in Local Switching Table (continued)

Field	Description
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 discovers the following VPLS-related information from the network and constructs VPLS instances:

- VSIs
- Pseudowires
- EFPs
- Switching entities

The Vision client enables you to:

- Add VPLS instances to a map—See [Adding VPLS Instances to a Map](#), page 18-97.
- Apply VPLS overlays—See [Applying VPLS Instance Overlays](#), page 18-98.
- View link details in VPLS overlays—See [Viewing Pseudowire Tunnel Links in VPLS Overlays](#), page 18-99.
- View VPLS-related properties—See the following topics:
 - [Viewing VPLS Instance Properties](#), page 18-101
 - [Viewing Virtual Switching Instance Properties](#), page 18-102

- [Viewing VPLS Core or Access Pseudowire Endpoint Properties](#), page 18-104
- [Viewing VPLS Access Ethernet Flow Point Properties](#), page 18-106
- Configure VFI Autodiscovery and Signaling—[Configuring VFI Autodiscovery and Signaling](#), page 18-107

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

Adding VPLS Instances to a Map

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

To add a VPLS instance to a map:

-
- Step 1** In the Vision client, 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 [Viewing a Table of NEs and Their Properties \(List View\)](#), page 7-7.

- 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.

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

Applying VPLS Instance Overlays

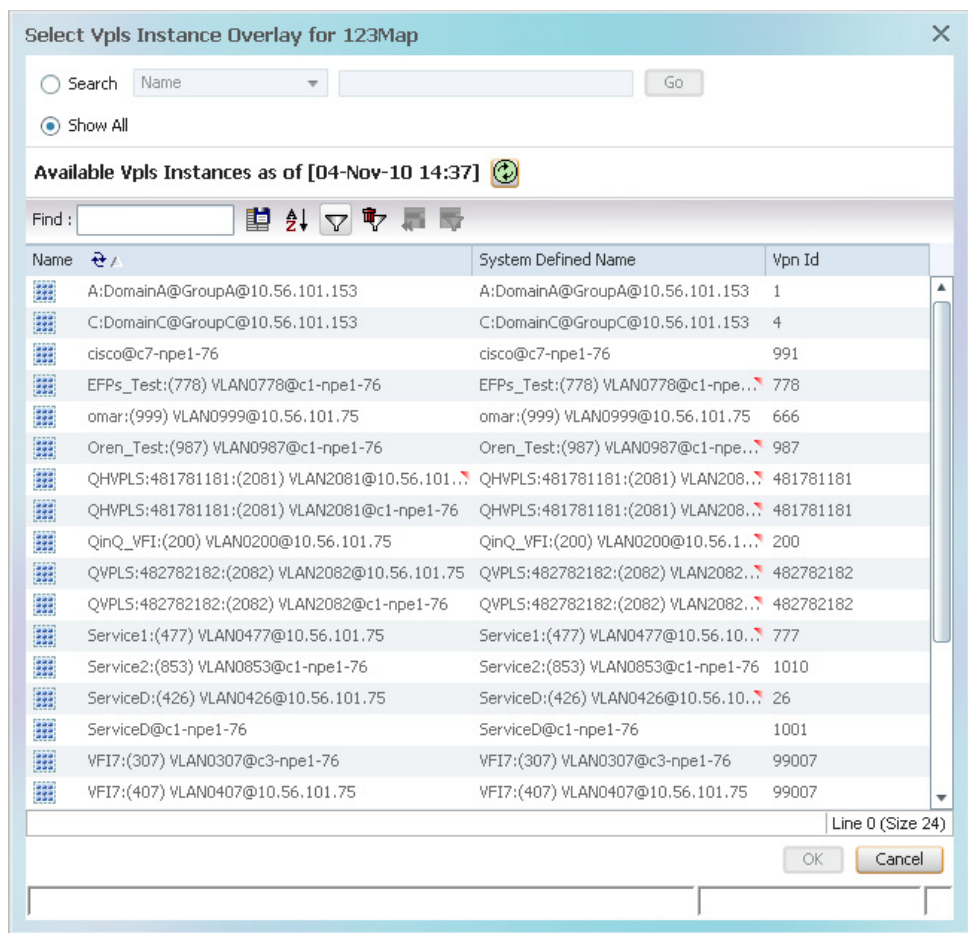
An VPLS instance overlay allows you to isolate the parts of a network that are being used by a specific VPLS instance.

To apply a VPLS instance overlay:

- Step 1** In the Vision client, choose the map in which you want to apply an overlay.
- Step 2** From the toolbar, choose **Choose Overlay Type > VPLS**.

Figure 18-44 shows an example of the Select VPLS Instance Overlay for *map* dialog box.

Figure 18-44 Select VPLS Instance Overlay Dialog Box

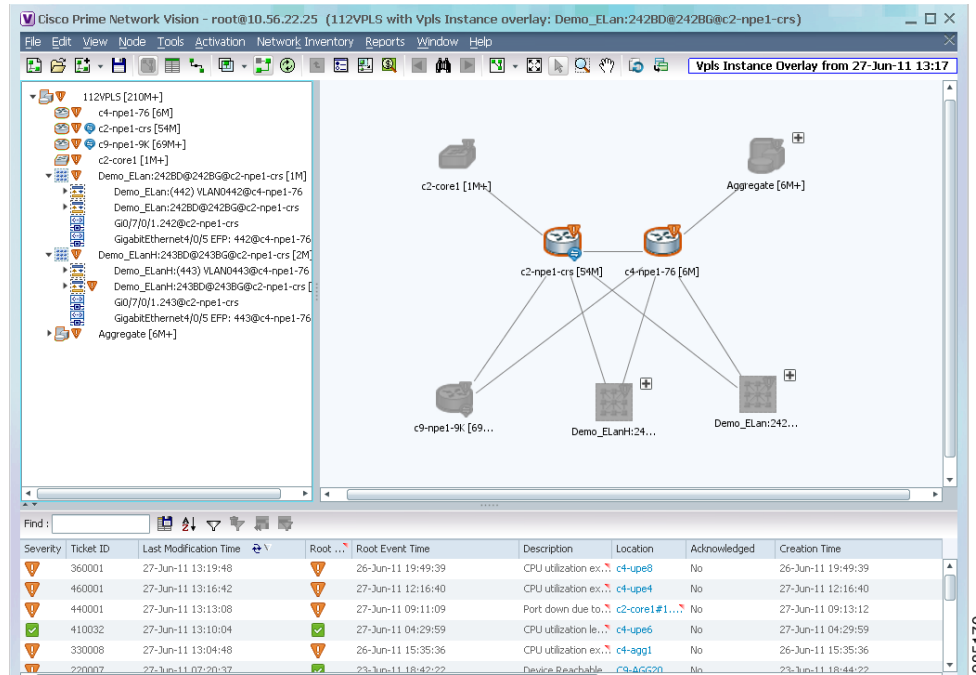


- Step 3** Select the required VPLS instance for the overlay.

- 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 18-45.

Figure 18-45 VPLS Instance Overlay in Vision Window



- 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**.

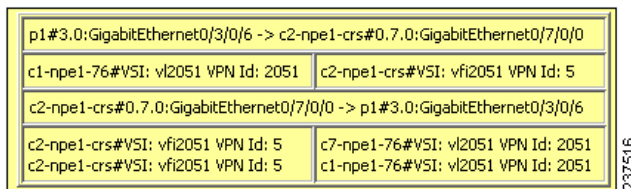
Viewing Pseudowire Tunnel Links in VPLS Overlays

When a VPLS overlay is applied to a map in the Vision client, 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 18-46.

Figure 18-46 Link Callout Window for a VPLS Overlay



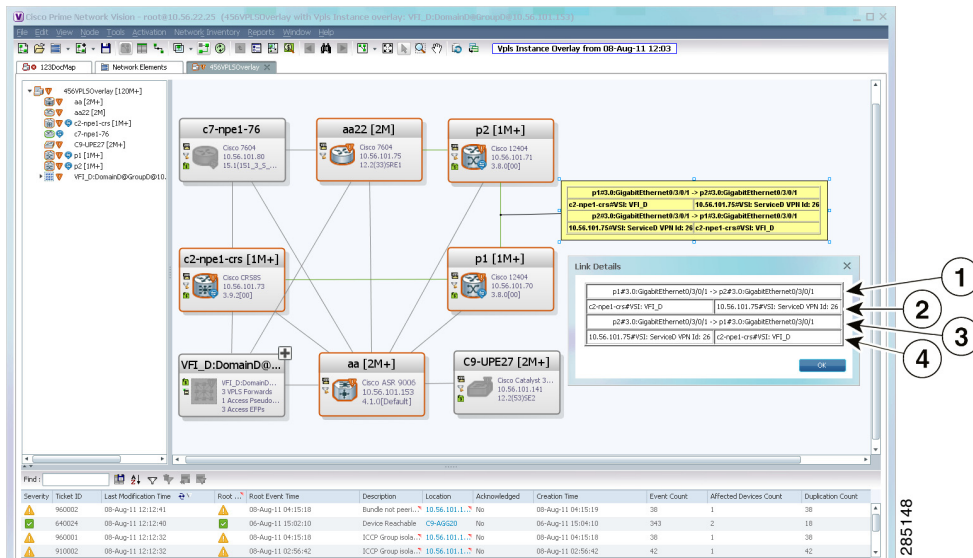
The callout window displays the following information for each link represented by the selected link:

- 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 18-47](#).

Figure 18-47 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

The Vision client enables you to view the properties of the following VPLS-related elements:

- VPLS instances—See [Viewing VPLS Instance Properties](#), page 18-101.
- Virtual Switching Instances—[Viewing Virtual Switching Instance Properties](#), page 18-102
- Tunnels—See [Viewing VPLS Core or Access Pseudowire Endpoint Properties](#), page 18-104.
- Port connectors—See [Viewing VPLS Access Ethernet Flow Point Properties](#), page 18-106.

Viewing VPLS Instance Properties

To view the properties of a VPLS instance in the Vision client, 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 18-48 shows an example of the VPLS Instance Properties window.

Figure 18-48 VPLS Instance Properties Window

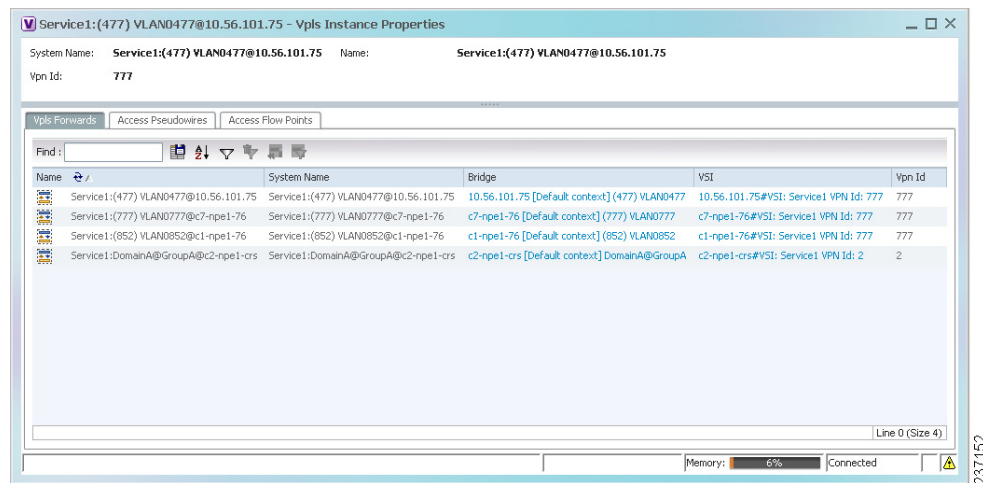


Table 18-45 describes the information that is displayed for VPLS instance properties.

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

Table 18-45 VPLS Instance Properties

Field	Description
System Name	Name that Prime Network 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 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.
VPN ID	VPN identifier for the VSI.

Table 18-45 VPLS Instance Properties (continued)

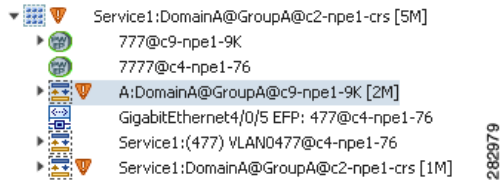
Field	Description
Access Pseudowires Tab	
Name	Pseudowire name.
Port	VSI on which the pseudowire is configured, hyperlinked to the entry in logical inventory.
Local Router IP	Local router IP address on which the pseudowire is configured.
Tunnel ID	Virtual circuit identifier of the pseudowire.
PTP Tunnel	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: <ul style="list-style-type: none"> • 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 the Vision client, 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 18-49](#).)

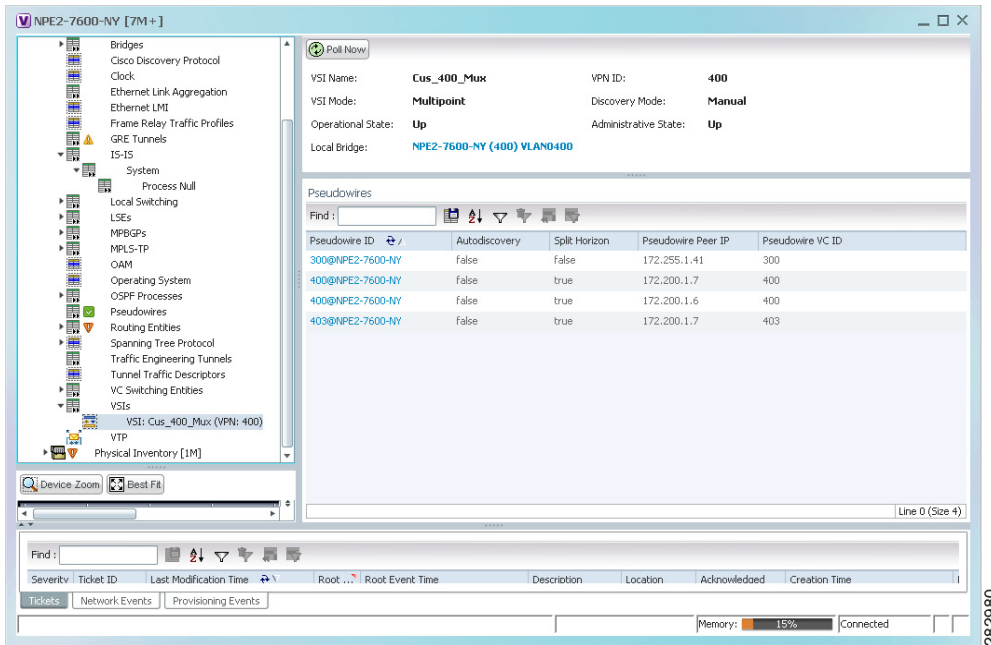
Figure 18-49 VPLS Forward in Vision Window Navigation Pane



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 18-50.

Figure 18-50 VSI Properties in Logical Inventory



282980

Table 18-46 describes the information that is displayed for the selected VSI.

Table 18-46 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 Vision client 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 18-51.)

Figure 18-51 VPLS Pseudowire in Vision Window Navigation Pane



Figure 18-52 shows an example of the Tunnel Properties window that is displayed.

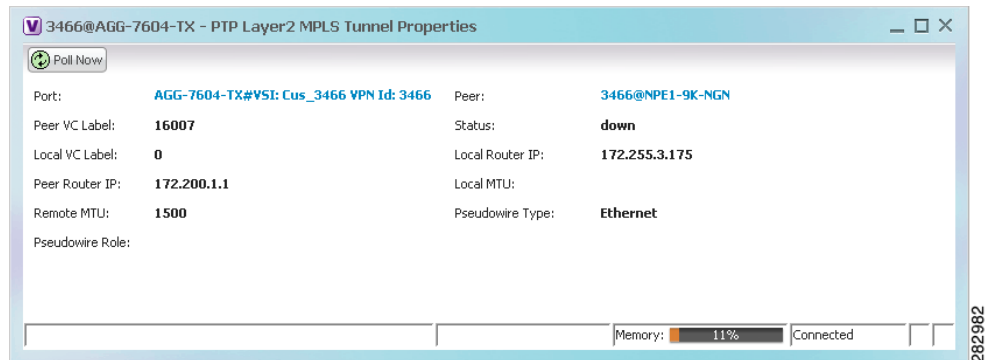
Figure 18-52 VPLS Tunnel Properties Window

Table 18-47 describes the information that is displayed for pseudowire endpoint properties.

Table 18-47 Tunnel Properties Window

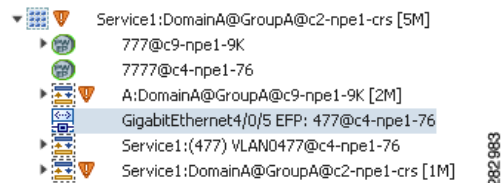
Field	Description
Port	VSI on which the pseudowire is configured, hyperlinked to the VSI in logical inventory.
Peer	Hyperlinked entry to the pseudowire endpoint peer pseudowires in logical inventory.
Peer VC Label	MPLS label that is used by this router to identify or access the tunnel. It is inserted 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 Vision client navigation pane.

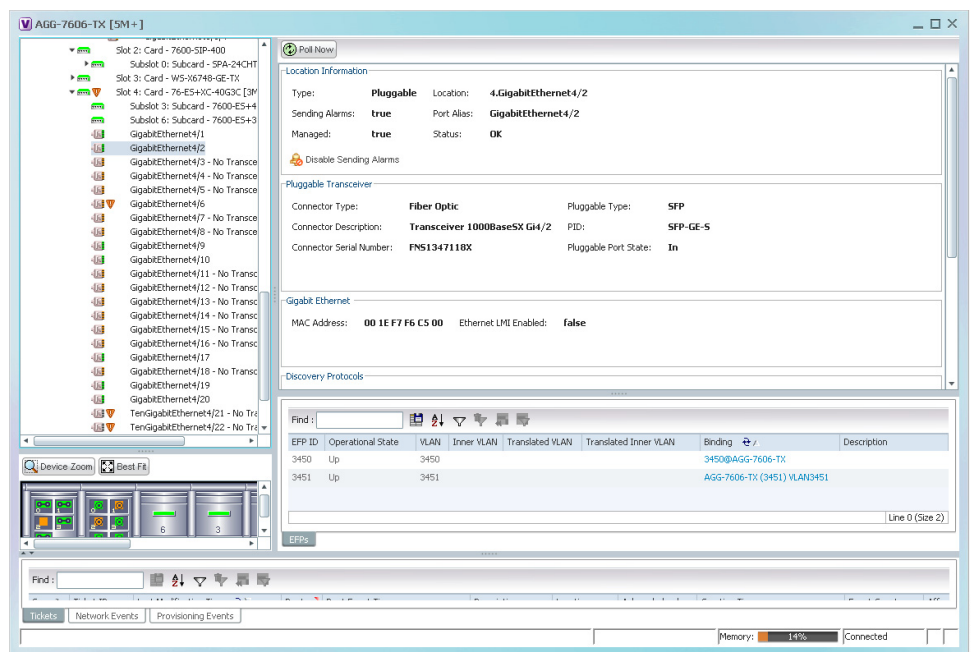
To view the properties for the Access Ethernet Flow Points configured for a VPLS instance, right-click the required interface in the navigation pane, and choose **Inventory**. (See [Figure 18-53](#).)

Figure 18-53 VPLS Interface in Vision Window Navigation Pane



[Figure 18-54](#) shows an example of the information displayed for the interface in physical inventory.

Figure 18-54 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 [Drilling Down Into a Port's Configuration Details \(Including Services and Subinterfaces\)](#), page 8-17.

- List of the configured EFPs on the port. For more information on the EFPs table, see [Viewing EFP Properties, page 18-51](#).
- List of VLAN mappings configured on the port. For more information about the VLAN Mappings table, see [Viewing VLAN Mappings, page 18-70](#).

Configuring VFI Autodiscovery and Signaling

The following commands enable you to configure VFI autodiscovery and signalling at the device level or at the VSI Level. To find out if a device supports these commands, see the [Cisco Prime Network 5.2 Supported Cisco VNEs](#).

Command	Navigation	Description
Configure VFI Autodiscovery and Signaling	Logical Inventory > <i>right-click the VSI</i> > Commands > Configuration > Configure VFI Autodiscovery and Signaling	Use this command to configure Autodiscovery and Signaling at the VFI level.
	Right-click the <i>ASR 9000 series device</i> > Commands > Configuration > Configure VFI Autodiscovery and Signaling	Use this command to configure Autodiscovery and Signaling at the device level.

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. For information on the devices that support pseudowire technology, refer to [Cisco Prime Network 5.2 Supported Cisco VNEs](#).

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

- [Adding Pseudowires to a Map, page 18-108](#)
- [Viewing Pseudowire Properties, page 18-110](#)
- [Displaying Pseudowire Information, page 18-112](#)
- [Viewing Pseudowire Redundancy Service Properties, page 18-113](#)
- [Applying Pseudowire Overlays, page 18-115](#)
- [Monitoring the Pseudowire Headend, page 18-117](#)

Adding Pseudowires to a Map

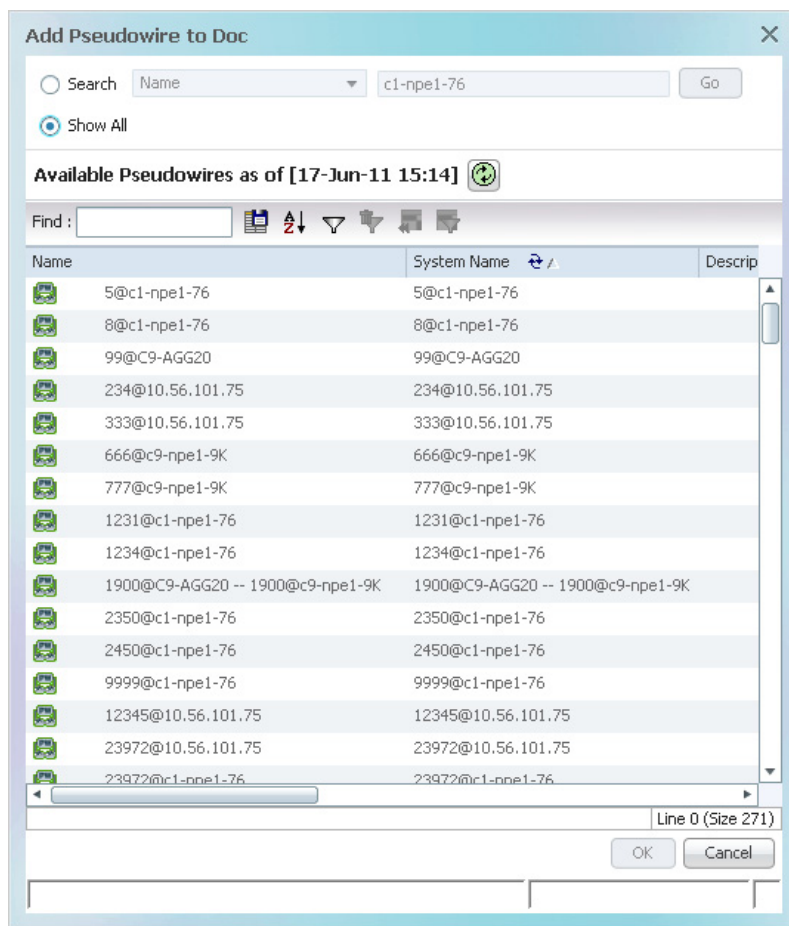
You can add a pseudowire that Prime Network discovers to maps as required.

To add a pseudowire to a map:

- Step 1** In the Vision client, 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 18-55 shows an example of the Add Pseudowire dialog box.

Figure 18-55 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.

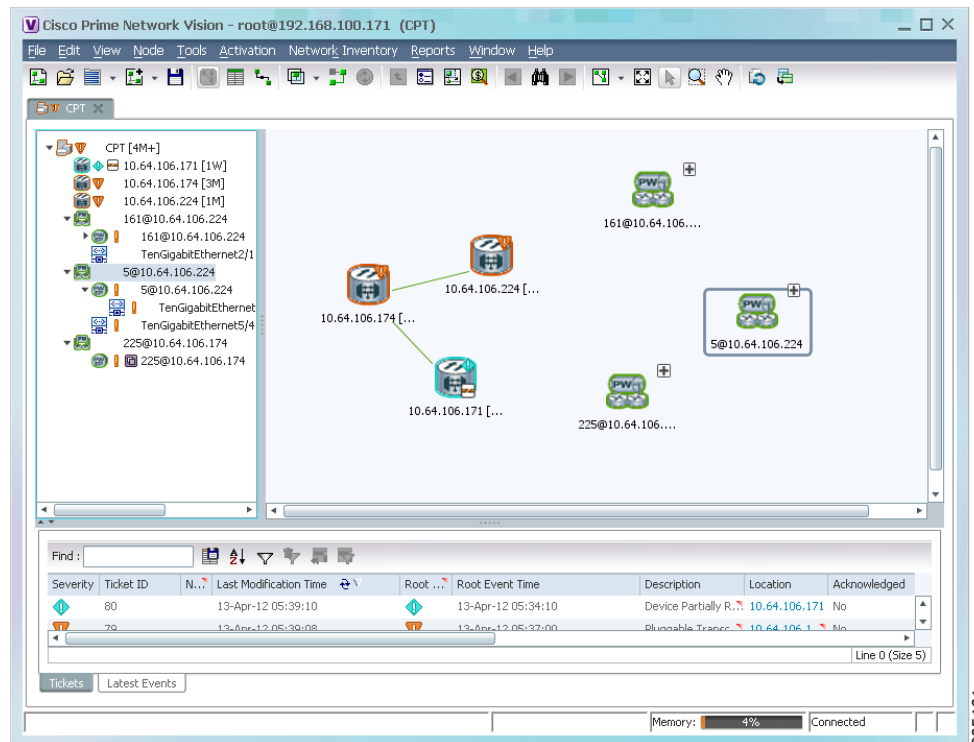
For information about sorting and filtering the table contents, see [Viewing a Table of NEs and Their Properties \(List View\)](#), page 7-7.

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 18-56](#).

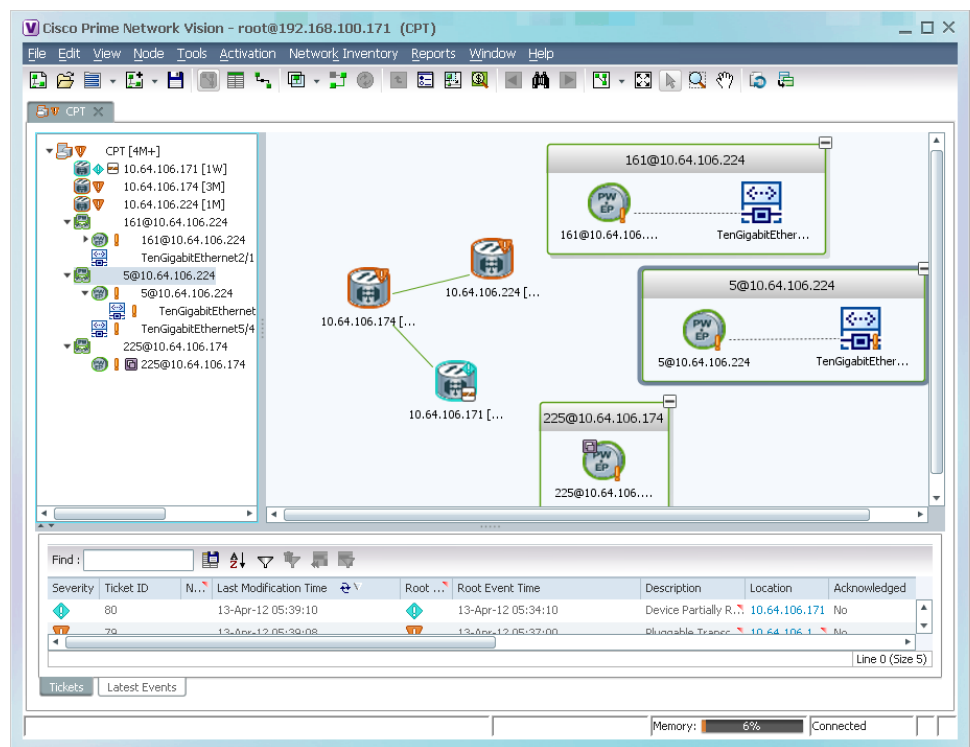
Figure 18-56 Pseudowire in Vision Map



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 18-57](#) shows an example of an expanded pseudowire in the Vision client.

Figure 18-57 Pseudowire Components in Vision Maps



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

Pseudowire discovery

As explained earlier, a pseudowire is a point-to-point connection between pairs of provider edge (PE) routers.

In a PW-HE configuration, the network PseudoWire service will include pseudowire edges. One of these edges will be connected to a dedicated ethernet flow point that will represent the pseudowire headend port.

Viewing Pseudowire Properties

To view pseudowire properties:

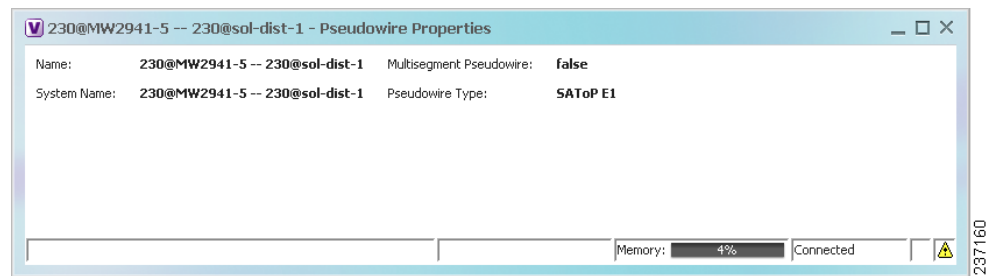
- Step 1** In the Vision client, select the required map or domain.
- Step 2** To view pseudowire endpoint properties configured on an element:
 - a. In the navigation or map pane, right-click the required element and then choose **Inventory**.
 - b. In the **Inventory** window, choose **Logical Inventory > 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 17-29](#).

- 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 18-58](#).

Figure 18-58 Pseudowire Properties Window



[Table 18-48](#) describes the information presented in the Pseudowire Properties window.

Table 18-48 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 18-52](#) and described in [Table 18-47](#).

- 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 18-43](#).

[Table 18-44](#) 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 18-49](#) describes the information displayed in the Contained Current CTPs table.

Table 18-49 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 18-51](#) for the information that is displayed for EFPs.

Displaying Pseudowire Information

Use the following procedure to view Virtual Circuit Connectivity Verification (VCCV) and Control Channel (CC) information for a pseudowire endpoint. Your permissions determine whether you can run these commands (see [Permissions for Managing Carrier Ethernet, page B-12](#)). To find out if a device supports these commands, see the [Cisco Prime Network 5.2 Supported Cisco VNEs](#).

-
- 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, preview or execute the command. 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 5** Click **Close** to close the Display Pseudowire dialog box.
-

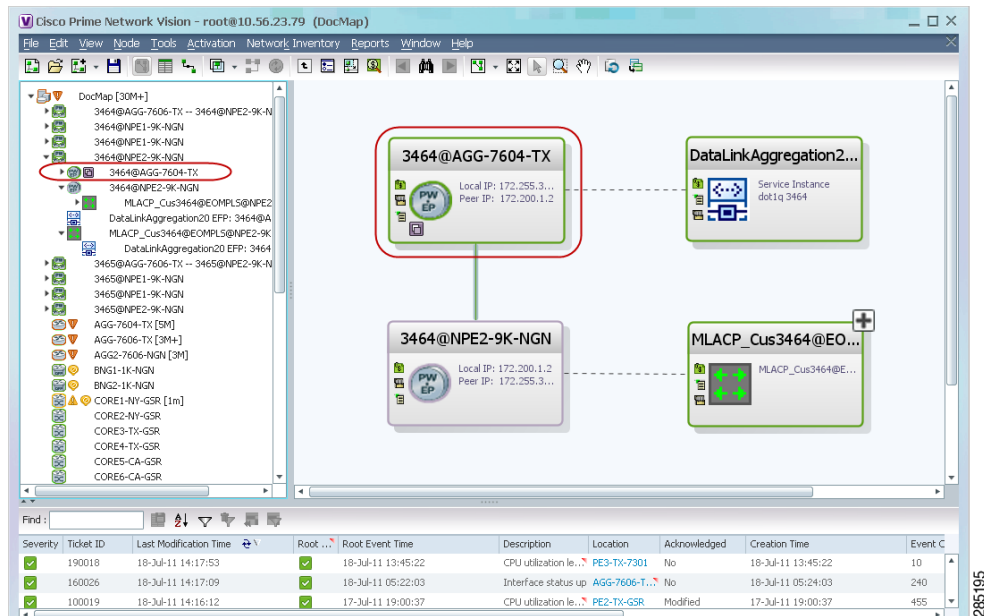
Viewing Pseudowire Redundancy Service Properties

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 Vision client. 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 18-59](#).

Figure 18-59 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 18-60 and shows that the selected pseudowire has a Secondary role in a redundancy service.

Figure 18-60 Layer 2 MPLS Tunnel Properties for Pseudowire Redundancy Service

The screenshot shows the '3464@AGG-7604-TX - PTP Layer2 MPLS Tunnel Properties' window. It displays the following information:

- Port: AGG-7604-TX#Aggregation Group 20 EFP:3464
- Peer: 3464@NPE2-9K-NGN
- Peer VC Label: 17368
- Status: down
- Local VC Label: 77
- Local Router IP: 172.255.3.175
- Peer Router IP: 172.200.1.2
- Local MTU: 1500
- Remote MTU: 1500
- Pseudowire Type: Ethernet Tagged
- Pseudowire Role: **Secondary** (circled in red)

Below this information is a table titled 'Associated Pseudowires':

Local Interface	VC ID	Peer	Status	Pseudowire Role	Preferred Path Tunnel	Local Ro
AGG-7604-TX#Aggregation Group 20 EFP:3464	3464@AGG-7604-TX	3464@NPE2-9K-NGN	down	Secondary		172.255

The 'Pseudowire Role' column in the table is circled in red. At the bottom of the window, there is a 'Memory' indicator showing 9% usage and a 'Connected' status.

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 18-61.)

Figure 18-61 Pseudowire Redundancy Service in Logical Inventory

Local Interface	VC ID	Peer	Status	Pseudowire Role
AGG-7604-TX#2.0:GigabitEthernet2/0/0 EFP:3450	3450@AGG-7604-TX	3450@NPE2-9K-TX	down	
AGG-7604-TX#VSI: Cus_3456 VFN Id: 3456	3456@AGG-7604-TX	3456@AGG-7606-TX	up	
AGG-7604-TX#VSI: Cus_3456 VFN Id: 3456	3456@AGG-7604-TX	3456@NPE1-9K-NGN	up	
AGG-7604-TX#VSI: Cus_3456 VFN Id: 3456	3456@AGG-7604-TX	3456@NPE2-9K-NGN	up	
AGG-7604-TX#VSI: Cus_3457 VFN Id: 3457	3457@AGG-7604-TX	3457@AGG-7606-TX	up	
AGG-7604-TX#VSI: Cus_3457 VFN Id: 3457	3457@AGG-7604-TX	3457@NPE1-9K-NGN	up	
AGG-7604-TX#VSI: Cus_3457 VFN Id: 3457	3457@AGG-7604-TX	3457@NPE2-9K-NGN	up	
AGG-7604-TX#VSI: Cus_3461 VFN Id: 3461	3461@AGG-7604-TX	3461@NPE2-9K-NGN	up	
AGG-7604-TX#VSI: Cus_3461 VFN Id: 3461	3461@AGG-7604-TX	3461@AGG-7606-TX	up	
AGG-7604-TX#VSI: Cus_3461 VFN Id: 3461	3461@AGG-7604-TX	3461@NPE1-9K-NGN	up	
AGG-7604-TX#Aggregation Group 20 EFP:3462	3462@AGG-7604-TX	3462@NPE1-9K-NGN	up	Primary
AGG-7604-TX#Aggregation Group 20 EFP:3462	3462@AGG-7604-TX	3462@NPE2-9K-NGN	up	Secondary
AGG-7604-TX#Aggregation Group 20 EFP:3463	3463@AGG-7604-TX	3463@NPE1-9K-NGN	up	Primary
AGG-7604-TX#Aggregation Group 20 EFP:3463	3463@AGG-7604-TX	3463@NPE2-9K-NGN	up	Secondary
AGG-7604-TX#Aggregation Group 20 EFP:3464	3464@AGG-7604-TX	3464@NPE2-9K-NGN	down	Secondary
AGG-7604-TX#Aggregation Group 20 EFP:3464	3464@AGG-7604-TX	3464@NPE1-9K-NGN	standby	Primary
AGG-7604-TX#Aggregation Group 20 EFP:3465	3465@AGG-7604-TX	3465@NPE1-9K-NGN	standby	Primary
AGG-7604-TX#Aggregation Group 20 EFP:3465	3465@AGG-7604-TX	3465@NPE2-9K-NGN	down	Secondary
AGG-7604-TX#VSI: Cus_3466 VFN Id: 3466	3466@AGG-7604-TX	3466@AGG-7606-TX	standby	
AGG-7604-TX#VSI: Cus_3466 VFN Id: 3466	3466@AGG-7604-TX	3466@NPE1-9K-NGN	standby	
AGG-7604-TX#VSI: Cus_3466 VFN Id: 3466	3466@AGG-7604-TX	3466@NPE2-9K-NGN	standby	

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 17-29](#).

Applying Pseudowire Overlays

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

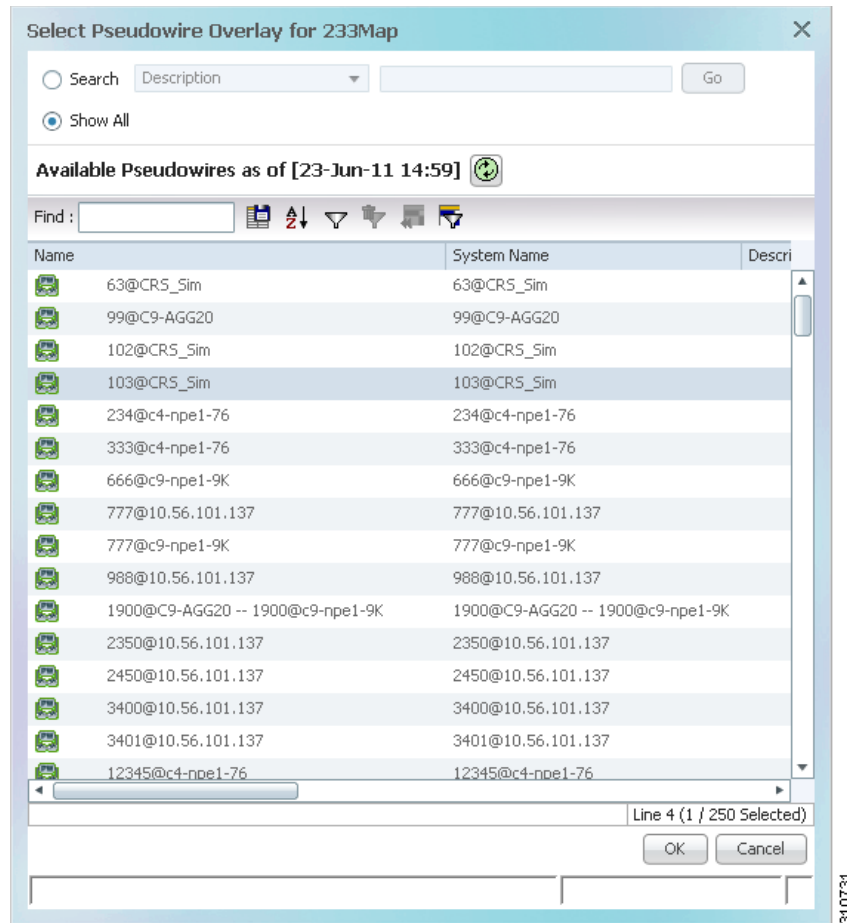
To apply a pseudowire overlay:

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

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

[Figure 18-62](#) shows an example of the Select Pseudowire Overlay for *map* dialog box.

Figure 18-62 Select Pseudowire Overlay Dialog Box

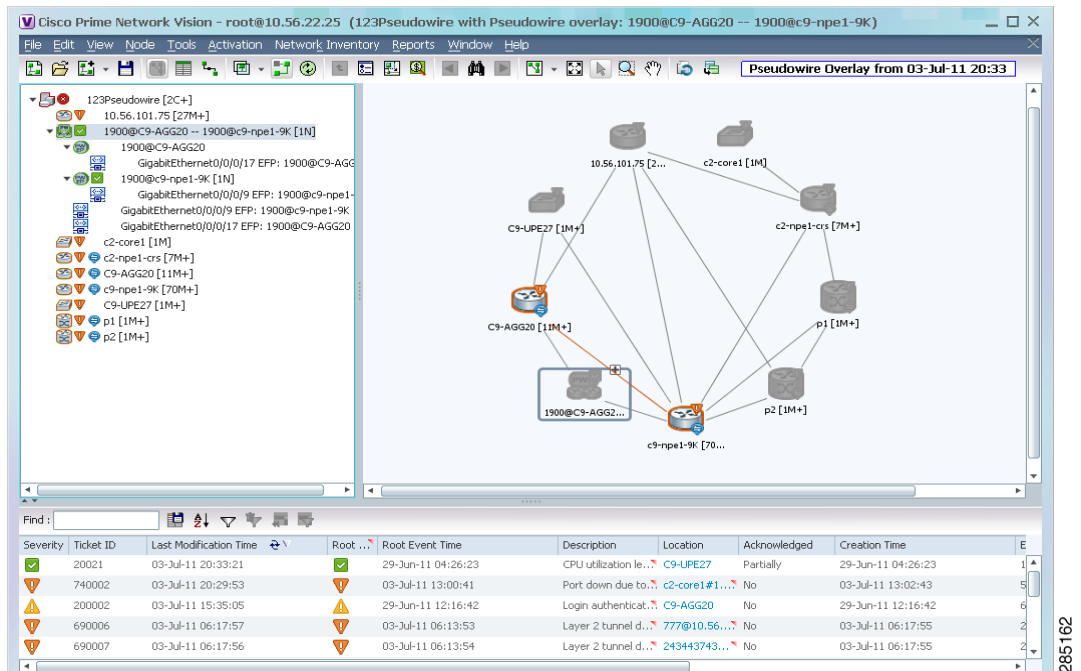


Step 3 Select the required pseudowire for the overlay.

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 18-63](#).

Figure 18-63 Pseudowire Overlay in Vision Window



- 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 18-64 displays a typical pseudowire deployment over core network and Figure 18-65 displays a pseudowire deployment over access network.

Figure 18-64 Pseudowire Deployment Over Core Network

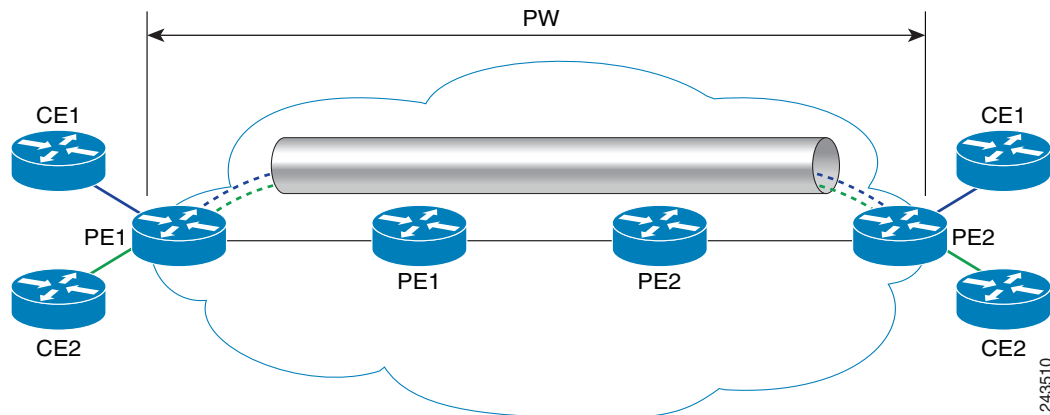
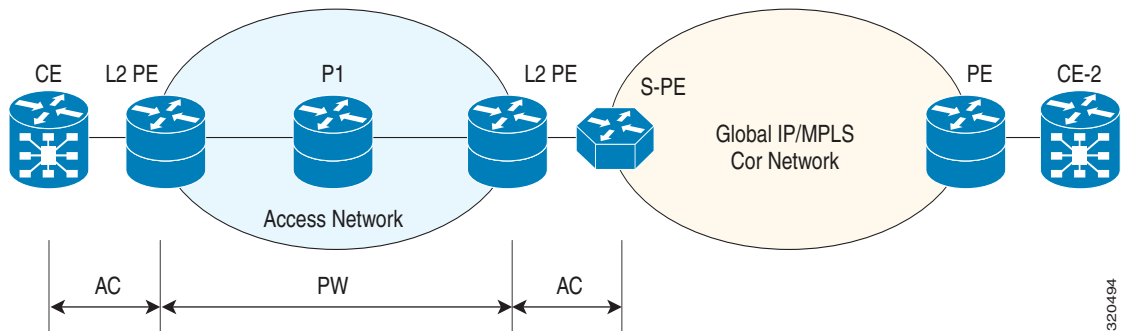


Figure 18-65 Pseudowire Deployment Over Access Network

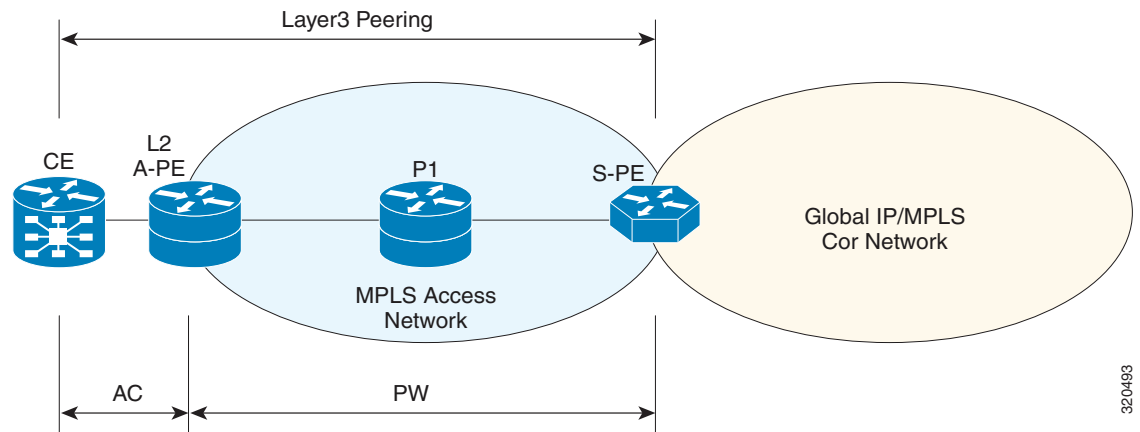


A pseudowire headend (PW-HE) virtual interface originates as a PW on an access node and terminates on a Layer 3 service instance on the service provider router. For example, a PWHE can originate on the Layer 2 PW feeder node and terminate on a VRF instance on the Cisco CRS Router. You can configure all 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 pseudowires 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 18-66 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 the Vision client 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 18-67](#).

Figure 18-67 PW-HE Configuration Details

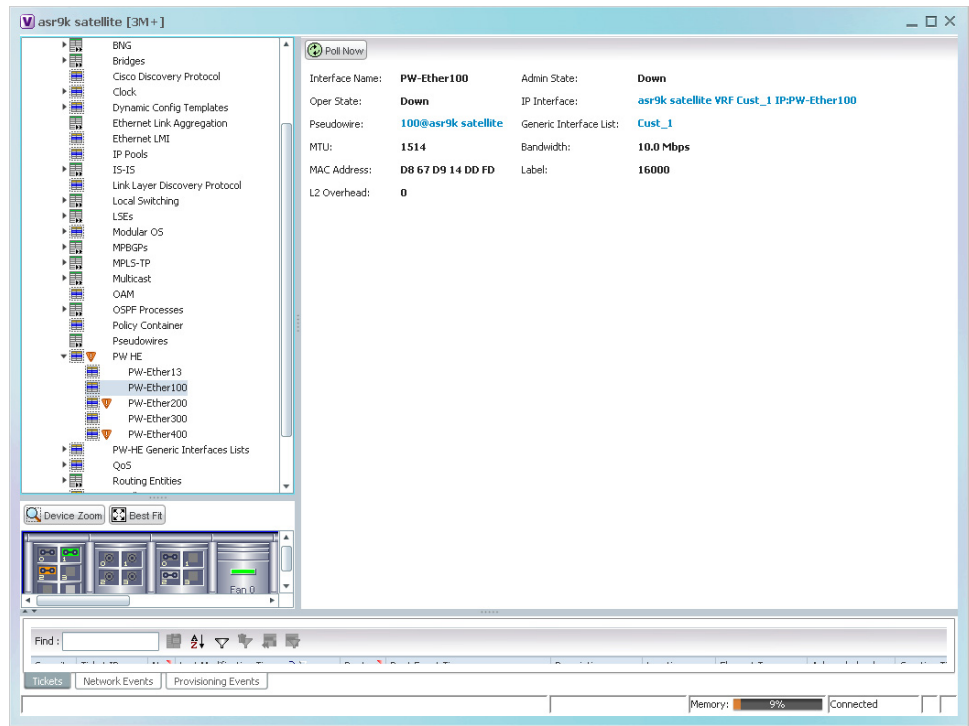


Table 18-50 displays the PW-HE interface details.

320486

Table 18-50 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: <ul style="list-style-type: none"> Up Down
Oper State	The operational state of the PW-HE, which can be any one of the following: <ul style="list-style-type: none"> 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 18-121](#)
- [Viewing PW-HE L2 Sub-Interface Properties, page 18-122](#)
- [Viewing PW-HE L3 Sub-interface Properties, page 18-122](#)
- [Viewing PW-HE Generic Interface List, page 18-123](#)
- [Viewing PW-HE as an Associated Entity for a Routing Entity, page 18-124](#)
- [Viewing PW-HE as an Associated Entity for a VRF, page 18-124](#)

Viewing PW-HE Configured as a Local Interface under Pseudowire

To view the local interface details:

- Step 1** Right-click the required device in the Vision client 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 18-110](#).

Viewing PW-HE L2 Sub-Interface Properties

To view the L2 Sub-Interface details:

- Step 1** Right-click the required device in the Vision client and choose **Inventory**.
- Step 2** In the logical inventory window, choose **Logical Inventory > PW HE > PW-Ether interface**. The list of PW-HE interfaces configured in Prime Network are displayed in the content pane.
- Step 3** Choose the EFPs tab of an interface to view the details.

[Table 18-51](#) displays the PW-HE L2 Sub-Interface details.

Table 18-51 PW-HE L2 Sub-Interface Details

Field	Description
EFPs tab	
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.
Ingress Policy	The name of the ingress service policy associated with the subscriber template. This field is applicable only for IP Subscriber and Service templates.
Egress Policy	The name of the egress service policy associated with the subscriber template. This field is applicable only for IP Subscriber and Service templates.
Service Control Policy	Specifies the policy for a port or operation.

Viewing PW-HE L3 Sub-interface Properties

To view the L3 Sub-Interface details:

- Step 1** Right-click the required device in the Vision client and choose **Inventory**.
- Step 2** In the logical inventory window, choose **Logical Inventory > PW HE > PW-Ether interface**. The list of PW-HE interfaces configured in Prime Network are displayed in the content pane.
- Step 3** Choose the Sub Interfaces tab of an interface to view the details.

[Table 18-52](#) displays the PW-HE L3 Sub-Interface details.

Table 18-52 PW-HE L3 Sub-Interface Details

Field	Description
Sub Interfaces tab	
Address	EFP identifier.
Mask	The mask of the specific network.
VLAN Type	The VLAN interface type, such as Layer 2 VLAN.
Operational State	EFP operational state: Up or Down.
VLAN ID	VLAN identifier.
Inner VLAN	CE-VLAN identifier.
IP Interface	IP interface, hyperlinked to the VRF properties in the inventory window.
VRF Name	Virtual Routing and Forwarding (VRF) name, if the pool belongs to a VRF.
VC	Virtual connection identifier.
Binding	Hyperlinked entry to the specific bridge in logical inventory.
Description	Description for the EFP.
Ingress Policy	The name of the ingress service policy associated with the subscriber template. This field is applicable only for IP Subscriber and Service templates.
Egress Policy	The name of the egress service policy associated with the subscriber template. This field is applicable only for IP Subscriber and Service templates.
Service Control Policy	Specifies the policy for a port or operation.

Viewing PW-HE Generic Interface List

To view the PW-HE generic interface list:

- Step 1** Right-click the required device in the Vision client 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 18-53](#) displays the PW-HE Generic Interface List details.

Table 18-53 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 the Vision client 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 17-32](#).
-

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 the Vision client 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 17-28](#).
-

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 3.8, EVC multiplex was discovered by means of Ethernet flow point associations. Beginning with Prime Network 3.9, multiplex capabilities were enhanced to distinguish multiplexed services based on the Customer VLAN ID; that is, Prime Network 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 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 Virtual Connections to a Map, page 18-125](#)
- [Applying Ethernet Service Overlays, page 18-126](#)
- [Viewing Ethernet Service Properties, page 18-128](#)

Adding Virtual Connections to a Map

You can add the virtual connections that Prime Network discovers to maps as required.

To add a virtual connection to a map:

-
- Step 1** In the Vision client, 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 > Virtual Connection**.
 - In the menu bar, choose **File > Add to Map > Virtual Connection**.
- Step 3** In the Add Virtual Connection 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 virtual connection or a group of virtual connections, 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 virtual connections, choose **Show All** and click **Go**.

The available elements that meet the specified search criteria are displayed in the Add Virtual Connections 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**.



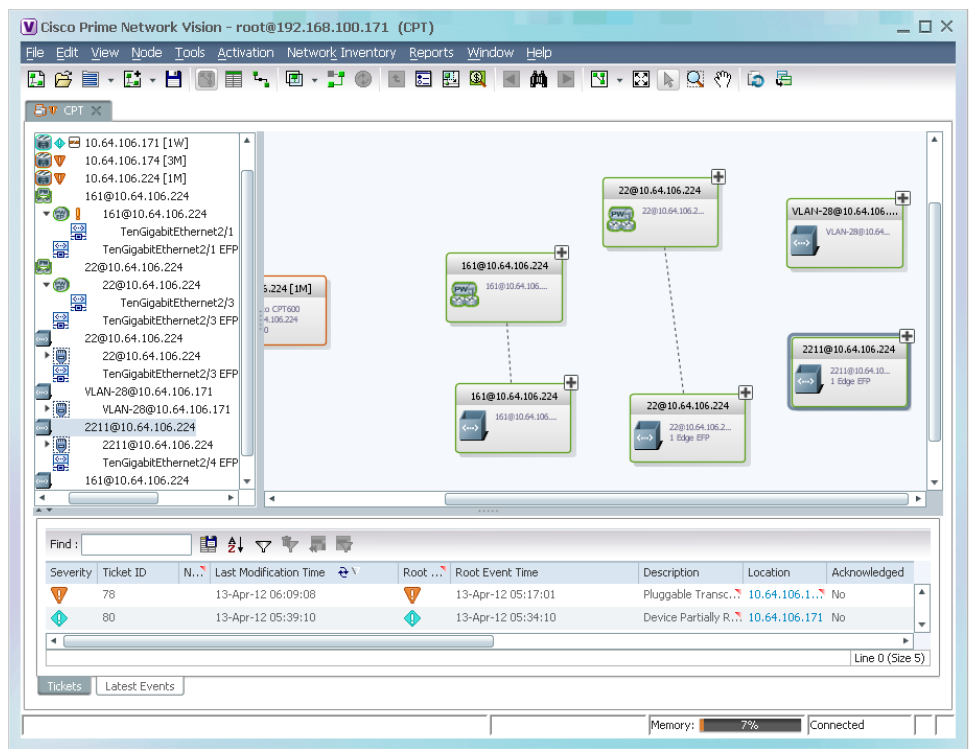
Note If an element is not included in your scope, it is displayed with the locked device icon.

For information about sorting and filtering the table contents, see [Viewing a Table of NEs and Their Properties \(List View\), page 7-7](#).

- Step 4** In the Add Virtual Connections 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 virtual connection is displayed in the navigation pane and in the content area. In addition, any associated tickets are displayed in the ticket pane. See [Figure 18-68](#).

Figure 18-68 Ethernet Service in Prime Vision Window



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

Applying Ethernet Service Overlays

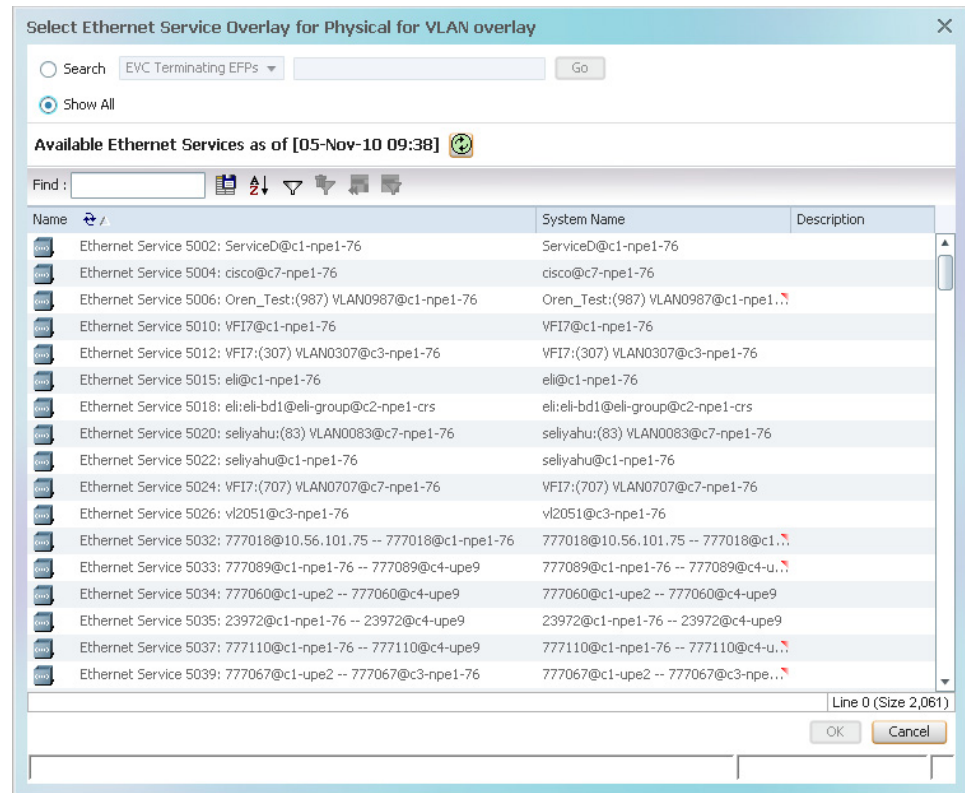
An Ethernet service overlay allows you to isolate the parts of a network that are being used by a specific Ethernet service.

To apply an Ethernet service overlay:

- Step 1** In the Vision client, choose the map in which you want to apply an overlay.
- Step 2** From the toolbar, choose **Choose Overlay Type > Ethernet Service**.

Figure 18-69 shows an example of the Select Ethernet Service Overlay for *map* dialog box.

Figure 18-69 Select Ethernet Service Overlay Dialog Box

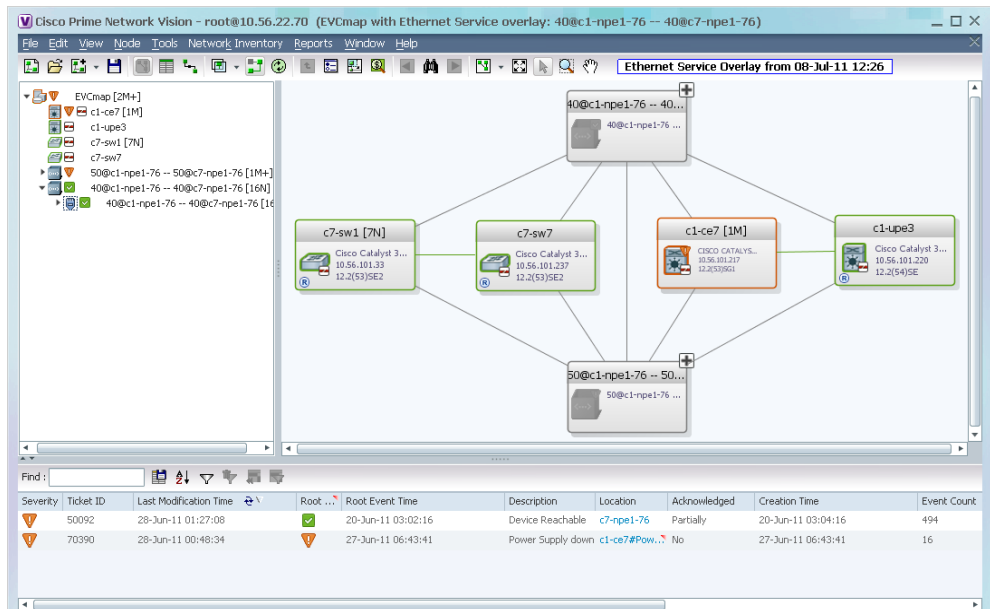


Step 3 Select the required Ethernet Service for the overlay.

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 18-70.

Figure 18-70 Ethernet Service Overlay in Vision Window



- 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 the Vision client, 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 18-71 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

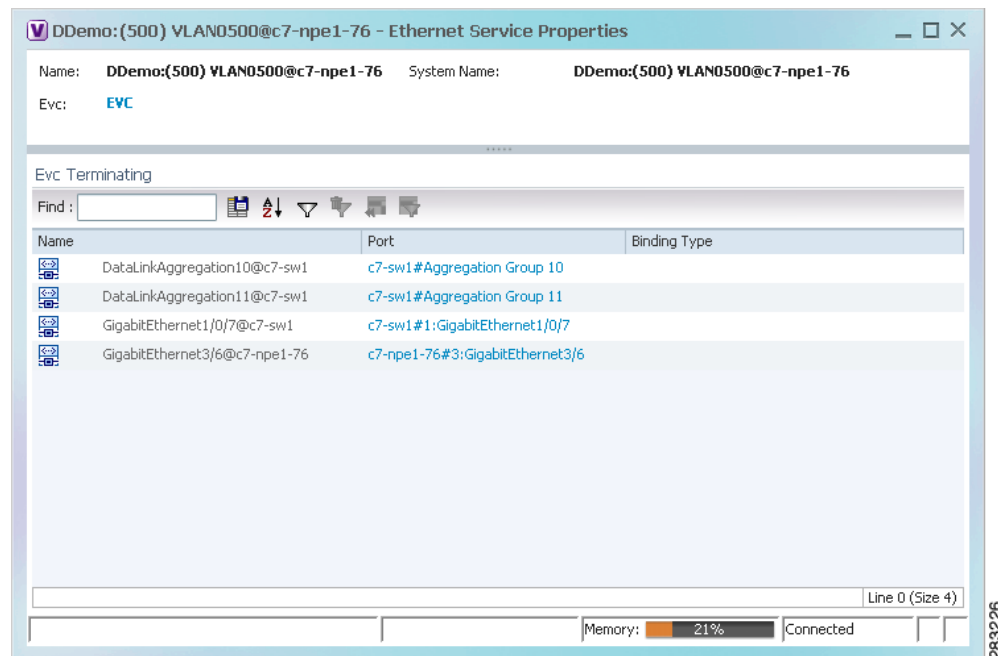
Figure 18-71 Ethernet Service Properties Window

Table 18-54 describes the information that is displayed for an Ethernet service.

Table 18-54 Ethernet Service Properties Window

Field	Description
Name	Ethernet service name.
System Name	Name that Prime Network 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 18-72 shows an example of the EVC Properties window.

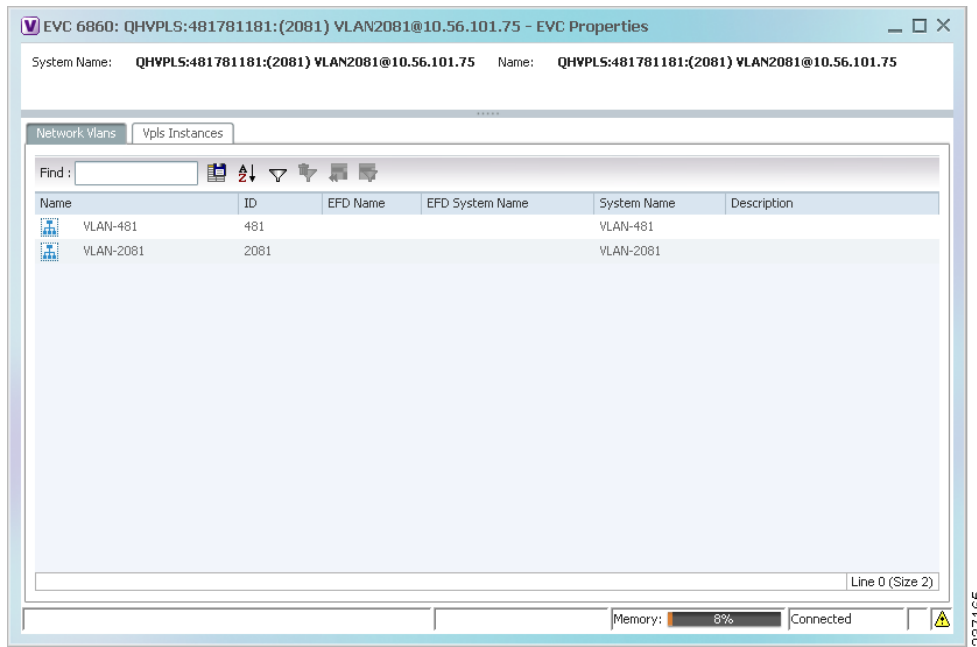
Figure 18-72 EVC Properties Window

Table 18-55 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 18-55 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 18-55 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 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 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.

For information on the devices that support IP SLA Responders, refer to [Cisco Prime Network 4.1 Supported VNEs](#).

To view IP SLA Responder service properties:

-
- Step 1** In the Vision client, 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 18-73](#).

Figure 18-73 IP SLA Responder in Logical Inventory

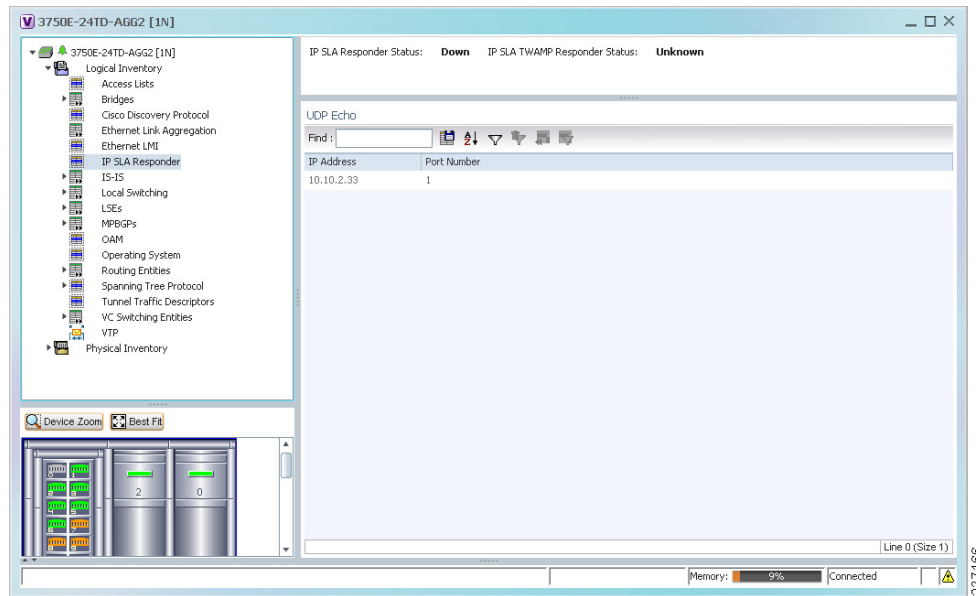


Table 18-56 describes the properties displayed for IP SLA Responder service.

Table 18-56 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 18-156](#).

To view IS-IS properties:

- Step 1** In the Vision client, double-click the device configured for IS-IS.
- Step 2** In the **Inventory** window, choose **Logical Inventory > IS-IS > System**.

Figure 18-74 shows an example of the IS-IS window with the Process table in logical inventory.

Figure 18-74 IS-IS Window in Logical Inventory

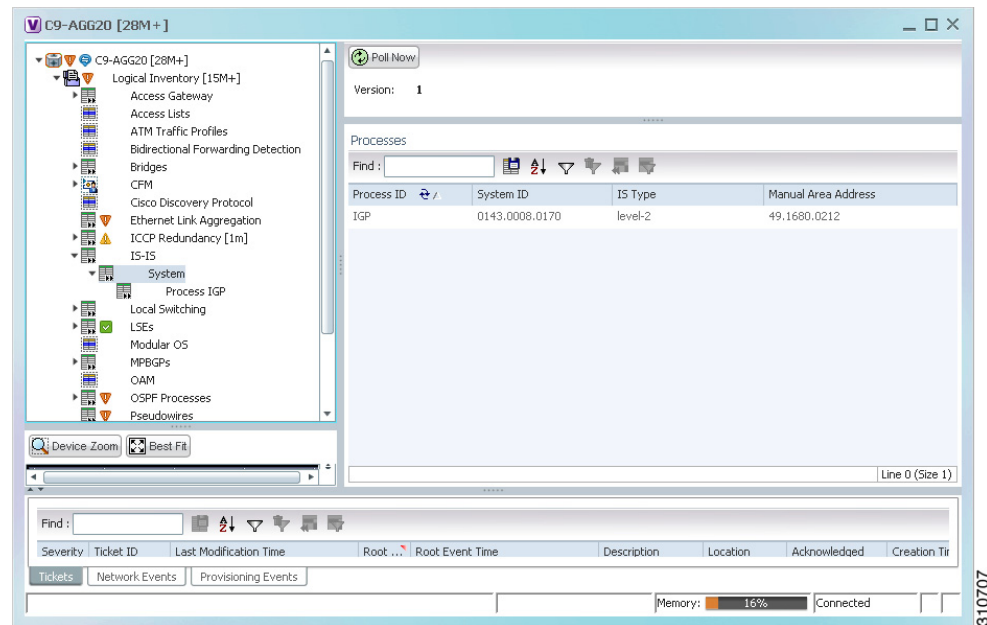


Table 18-57 describes the information that is displayed in this window and the Processes table.

Table 18-57 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 18-75 shows an example of the information that is displayed for the IS-IS process.

Figure 18-75 IS-IS Process Properties in Logical Inventory

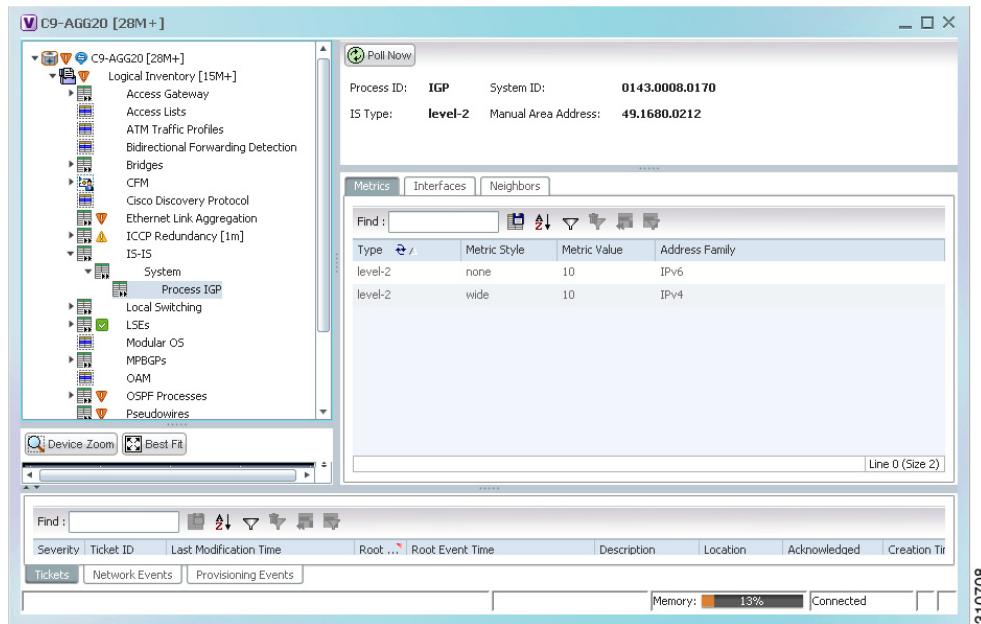


Table 18-58 describes the information that is displayed for the selected IS-IS process.

Table 18-58 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	

Table 18-58 IS-IS Process Properties in Logical Inventory (continued)

Field	Description
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

Open Shortest Path First (OSPF) is a link-state routing protocol for IP networks. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS). It uses the Shortest Path First (SPF) algorithm to calculate the best path for a given destination. OSPF is perhaps the most widely used interior gateway protocol (IGP) in large enterprise networks.

The OSPF topology is a multilink topology, i.e. there can be multiple links from the same OSPF process. It is also a single layer and dynamic topology.

Prime Network supports the following versions of OSPF:

- OSPFv2
- OSPFv3

Using the Vision client 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.

You can view the OSPF topological links for neighbors whose status is Full or Two Way.

To view OSPF properties:

-
- Step 1** In the Vision client, double-click the device configured for OSPF.
- Step 2** To view OSPF processes, choose **Logical Inventory > OSPF Processes > OSPF Process (vn) ID** where *vn* represents the OSPF version and *ID* is the OSPF process identifier.
- For example, in [Figure 18-76](#), the entry in the navigation tree is OSPF Process (v2) 10.

Figure 18-76 OSPF Processes in Logical Inventory

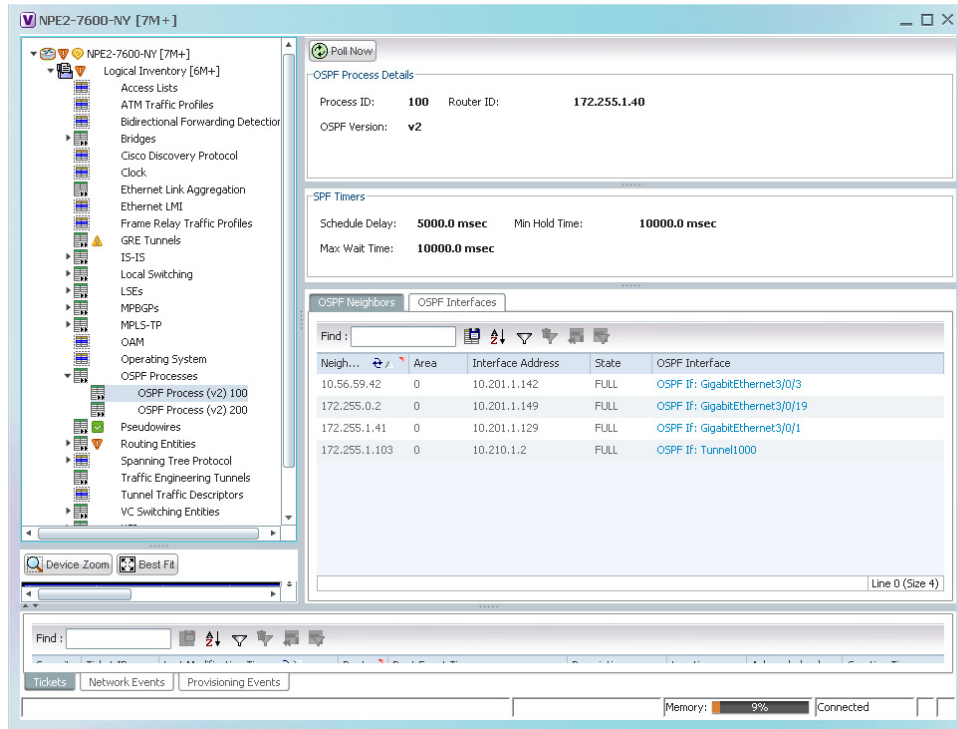


Table 18-59 describes the information that is displayed for OSPF processes.

Table 18-59 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.

Figure 18-77 Viewing OSPF Interface

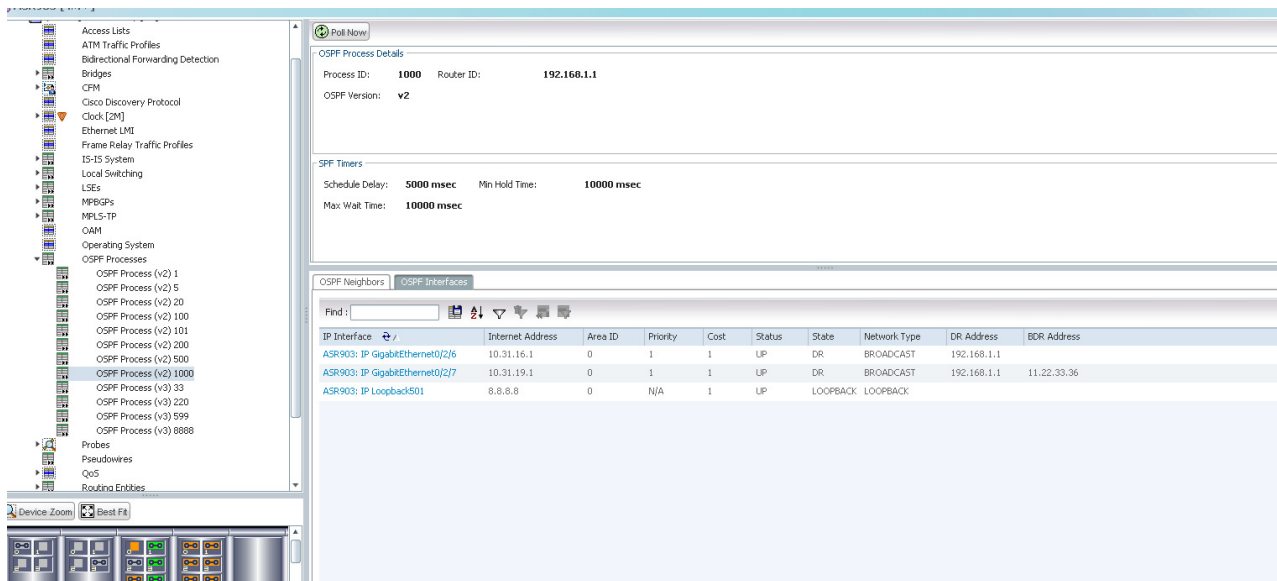


Table 18-60 OSPF Processes in Logical Inventory (continued)

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 17-8 .
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	The displayed OSPF state will be either BDR, DR, DR-Other, or LOOPBACK.
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.

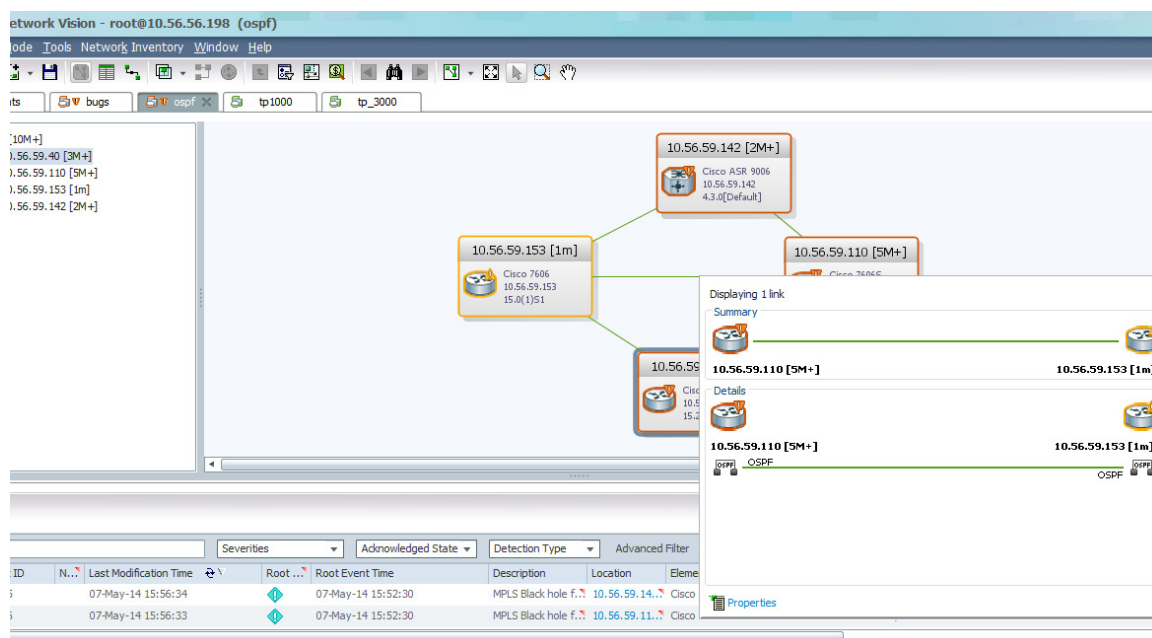
OSPF Topology

In OSPF topology, the links will be formed among the OSPF Process Device Components even though the link signifies the neighborhood among them. The OSPF is a multilink topology, thus enabling the creation of multiple links from the same OSPF process. From Prime Network 5.1, the OSPF topology will be added along with the existing support.

The various types of topologies that can be formed under OSPF are

- Single layer topology
- Dynamic topology

The OSPF topological links are shown for the neighbors which has the Neighbor State as either FULL or TWOWAY. For neighbors with TWOWAY state, the OSPF interface's network type should be either BROADCAST or NBMA.



Viewing OSPF Link Properties

To view the OSPF link properties:

- Step 1** In the Vision client, right-click on the link between the devices and select **Properties** to view the link properties.
- Step 2** In the link properties window, the left pane displays the selected link and the right pane displays the link properties.

Figure 18-78 Viewing OSPF Link Properties

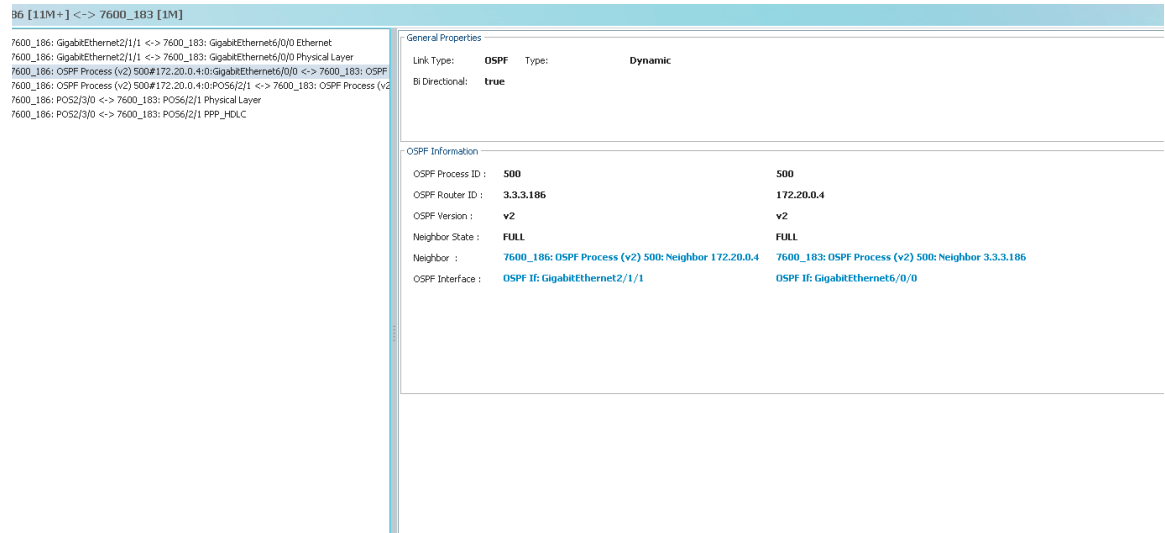


Table 18-61 describes the information that is displayed in link properties window.

Table 18-61 OSPF Link Properties window

Field	Description
Link Type	The link protocol, which is OSPF in this instance.
Type	The type of link, which is Dynamic .
Bi Directional	Indicates whether the link is bidirectional.
OSPF Information tab	
OSPF Process ID	The unique code to identify the OSPF process.
OSPF Router ID	The IP address of the OSPF router.
OSPF Version	The OSPF version, which can be v1, v2, or v3.
Neighbor State	The status of the OSPF neighbor, which can be Full and Two-Way.
Neighbor	Provides IP address of the OSPF Neighbor
OSPF Interface	The link to the OSPF interface.

Service Alarms

As part of the topological link support, two new service alarms **OSPF link down** and **OSPF link up** are introduced. These alarms are generated on the OSPF links in cases such as misconfigurations, shutting down of physical interfaces or any other scenario that might break the OSPF neighborship.

Correlation

The **OSPF link down** alarm is a ticketable event. It also can be correlated under the physical link alarms. If OSPF configured interface goes down, the OSPF link also goes down. For e.g, In case of interface shut down, the **OSPF link down** alarm is generated and correlated to the **Link down due to admin** service alarm.

Monitoring the CPT 50 Ring Support

The Cisco Carrier Packet Transport (CPT) Product Family with CPT600, CPT200 and CPT50 Series sets the industry benchmark as a compact carrier-class converged access and aggregation platform for Unified Packet Transport architectures.

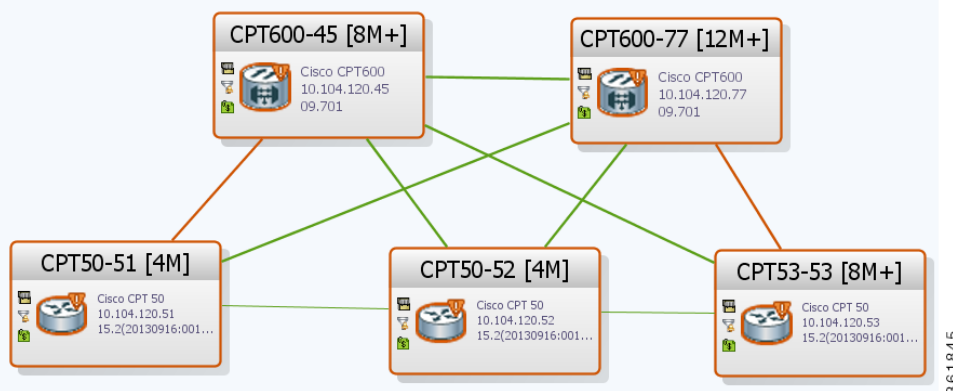
The CPT 50 is a compact and operationally simple, yet highly scalable and flexible platform optimized for delivering TDM like Ethernet Private 5.2 as well as multipoint capabilities for Business, Residential, Mobile Backhaul, Data Center, and Video Services. Its unique satellite architecture is designed to scale, simplify and enhance the operational and deployment aspects of service-delivery networks.

The CPT system also provides the ability to operate CPT 50 in a physical ring homed back to a single CPT 600 or CPT 200 chassis. This feature provides the flexibility of connecting CPT 50 in a closed-ended ring or an open-ended ring. As a result, the failure of a line or uplink card does not impact the traffic in a ring. CPT 50 in a ring works like a route processor and each CPT 50 interacts with Transport Node Controller (TNC) directly.

CPT 50 supports the following types of rings:

- Single Homed—A ring that is subtending from a single CPT-600 or CPT 200. There are two types of single home rings:
 - Open Ended Ring—Connects to the CPT-600 or CPT-200 through one interface only. Hence, there is only one unprotected path available to the traffic on the ring.
 - Closed—Connects to the CPT-600/200 through two interfaces. Hence there is a protected path available for the traffic either through the east or west interface on the ring.
- Dual Homed—A ring whose east port exists on one CPT 200 or CPT 600 (Working Ring Controller) and west port exists on another CPT 200 or CPT 600 (Protected Ring Controller). If WRC fails, this type of ring provides access to all the CPT 50s in the ring by switching the traffic to the other controller.

The following figure depicts the CPT 50 dual homed in Prime Network:





In the above figure, the dual ring home starts in one CPT 600 device and ends in another CPT 600 device. The CPT 600 device from which the dual ring starts is the Working Ring Controller (WRC) and the other CPT 600 device is the Protected Ring Controller (PRC).

**Note**

To view more details about the device, right-click the device and choose **Inventory** to view the inventory details. The Node Role field in the content pane denotes whether the CPT device is WRC or PRC.

Configuring CPT

The following commands can be launched from the inventory by right-clicking the appropriate node and choosing **Commands > Configuration**. Your permissions determine whether you can run these commands. To find out if a device supports these commands, see the [Cisco Prime Network 5.2 Supported Cisco VNEs](#).

Command	Navigation	Description
Configure L2 Control Protocol	Physical Inventory > Chassis > Backplane > slot > right-click on the Ethernet card > Commands > Configuration	Use this command to configure the L2 Control Protocol.
Show L2 Control Protocol	Physical Inventory > Chassis > Backplane > slot > right-click on the Ethernet card > Commands > Show	Use this command to view details of the L2 Control protocol parameters configured for the selected port.
Add Loopback Remove Loopback	Physical Inventory > Chassis > Backplane > slot > right-click on the Ethernet card > Commands > Configuration	Use these commands to add and remove a loop-back respectively.  Note Loop-back refers to the process of routing electronic signals or digital data streams, back to their source with processing or modifying it.
Configure CDP	Physical Inventory > Chassis > Backplane > slot > right-click on the Ethernet card > Commands > Configuration	Use this command to configure CDP.  Note Cisco Discovery Protocol (CDP) is used to obtain protocol addresses of neighboring devices and discover the platform of those devices. It can also be used to show information about the interfaces your router uses.
Configure Ethernet		Use this command to configure Ethernet parameters.

Command	Navigation	Description
Show Ethernet Parameters	Physical Inventory > Chassis > Backplane > slot > right-click on the Ethernet card > Commands > Show	Use this command to view details of the Ethernet parameters configured for the selected Ethernet port.
Configure Port Parameters	Physical Inventory > Chassis > Backplane > slot > right-click on the Ethernet card > Commands > Configuration	Use this command to configure port parameters.
Show Port Parameters	Physical Inventory > Chassis > Backplane > slot > right-click on the Ethernet card > Commands > Show	Use this command to view the port parameters configured for the selected port.

Viewing the G8032 ERPS Configuration

Ethernet Ring Protection Switching is an effort at ITU-T under G.8032 Recommendation to provide sub-50ms protection and recovery switching for Ethernet traffic in a ring topology and at the same time ensuring that there are no loops formed at the Ethernet layer.

Ring Protection Switching Architecture works based on the following fundamentals:

- **Principle of Loop Avoidance**—Loop avoidance is achieved by guaranteeing that traffic flows on all but one of the ring links at any point of time. The one ring link from which traffic does not flow is called the Ring Protection Link (RPL), which is generally blocked. A designated Ethernet ring node—the RPL owner node—is responsible for blocking traffic at one end of the RPL. In the event of an Ethernet ring failure, the RPL owner node must unblock its end of the RPL and allow the RPL to be used for traffic.
- **Utilization of learning, forwarding, and filtering database mechanisms defined in the Ethernet Flow Forwarding Function**—Failure of Ethernet ring results in protection switching of traffic, which is controlled by the Ethernet Flow Forwarding Function. An APS protocol is used to coordinate the protection action over the ring, which transmits Ring Automatic Protection Switching (R-APS) messages.

Ethernet rings also supports multi ring/ladder network that consists of conjoined Ethernet rings by one or more interconnection points. The protection switching mechanisms and protocol are also applicable for multi ring/ladder network on adherence of certain principles.

The G8032 technology also supports multiple ERP instances over a ring. An ERP instance is an entity that is responsible for the protection of subset of VLANs carried over the physical ring and it should configure its own R-APS channel, RPL, RPL Owner and RPL Neighbor nodes.

Ring protection switching process also occurs based on the detection of defects on the transport entity on the ring link, and the transport entity can have a failed or non-failed condition. To monitor these defects, Ethernet ring protection may use any one of the following methods:

- **Inherent**—The fault condition status of each link connection is derived from the status of the underlying server layer trail.

- Sub-layer—Each ring link is monitored using Tandem Connection Monitoring (TCM).
- Test trail—An extra test trail is used to detect defects, which is setup along each ring link.

In Prime Network, the G8032 Ethernet Ring Protection Switching configuration can be viewed in the following nodes:

- Profile—This node displays the G8032 profile details. Each G8032 ring is associated to a profile, which consists of several timers. The timer displays details of the time frame the ring needs to wait before, during and after performing an action to avoid race conditions and unnecessary switching operations. If a ring is not associated to a profile, the default profile is automatically associated to it.
- Ring—This node displays the properties of the ring as well as the properties that are shared across all ERP instances

To view the G8032 Ethernet Ring Protection Switching Profile configuration:

-
- Step 1** Right-click on the required device and choose the **Inventory** option.
- Step 2** In the **Inventory** window, choose **Logical Inventory > G8032 > Profiles**. A list of all the G8032 profiles are displayed in the content pane.
- Step 3** In the content pane, right-click on the profile name to view the **G8032 Profile Properties** window. [Table 18-62](#) describes the information displayed in the G8032 Profile Properties window.

Table 18-62 G8032 Profile Properties

Field	Description
Profile Name	The unique name of the profile associated to the G8032 ring.
WTR Interval	The Wait-to-Restore interval (in minutes) applicable to the G8032 ring. This interval refers to the duration before traffic is restored to the state, when it is found that a failure is no longer occurring. This interval also avoids toggling protection states in case of intermittent defects. This field defaults to 5 minutes.
Guard Interval	The Guard Interval (in milliseconds) that denotes the duration the node waits before performing a node state transition. This is done to block outdated R-APS messages from causing unnecessary node state changes. This field defaults to 500.
Holdoff Timer	The duration (in seconds) applicable for the G8032 ring. The node waits for the specified duration to expire before reporting faults to the ring protection mechanism.
Mode Type	The operating mode applicable for the G8032 ring, which can be any one of the following: <ul style="list-style-type: none"> • Revertive—In case the condition causing the switch is cleared, the traffic channel is restored to the working transport entity. • Non revertive—In case the condition causing the switch is cleared, the traffic channel continues to use the RPL. This field defaults to Revertive .

To view the G8032 Ethernet Ring Protection Switching Ring configuration:

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

Step 2 In the **Inventory** window, choose **Logical Inventory > G8032 > Ring > ring name**. The details of the ring are displayed in the content pane.

Table 18-63 describes the Ring properties.

Table 18-63 G8032 Ring Properties

Field	Description
Ring Name	The name of the ring.
Ring Type	The ring type, which can be any one of the following: <ul style="list-style-type: none"> • Open—When the ring is terminated by an Ethernet access such as VPLS. • Closed—When the arcs or links in the ring are simple Ethernet links.
Excluded VLAN ID	The range of VLAN ID that are excluded by the ring. In other words, the VLAN ID included in this range are not serviced by the ring and not blocked by the ring switching mechanism.
Untagged in Excluded VLANs	Indicates whether untagged Ethernet traffic is also blocked by the VLAN exclusion list.
Ring Ports Entries tab	
Port Number	The port number associated to the ring.
Local Port	The link to the local physical port that is used for this ring port.
Monitor Interface	The link to the interface that is used as the monitor interface. A monitor interface is used to monitor the ring port and detect ring failures.
Blocked VLAN IDs	The range of VLAN IDs that are blocked by the ring port.
Untagged in Blocked VLANs	Indicates whether untagged traffic is blocked by the ring port.
Unblocked VLAN IDs	The list of VLAN IDs that are not blocked by the ring port.
Untagged in Unblocked VLANs	Indicates whether untagged traffic is unblocked by the ring port.
Ring Instance Entries tab	
Instance	The unique code assigned to the instance.
Node Type	The node type that determines the node's responsibility towards the instance. This can be Normal, Owner, Neighbor, or Next Neighbor.
Node State	The state of the node for a specific instance, which can be any one of the following: Idle, Pending, Protection, Forced Switch, and Manual Switch. This state is configured by the administrator or determined by the APS as part of the G8032 protection protocol.
Port 0 State	The status of the port that is configured as Port 0, which can be N/A, RPL-Link, Faulty, Blocked, Local Forced Switch, or Local Manual Switch.
Port 1 State	The status of the port that is configured as Port 1, which can be N/A, RPL-Link, Faulty, Blocked, Local Forced Switch, or Local Manual Switch.
Instances tab	







Table 18-63 G8032 Ring Properties

Field	Description
ID	The unique code assigned to the instance.
Instance Description	The description of the instance.
Profile	The link to the ring profile associated to the instance.
Included VLAN IDs	The list of VLAN IDs included or served by this instance, which includes all VLANs associated with the ring instance.
RPL Port Role	The Ring Protection Link (RPL) port in charge of the RPL, which enables it to turn the RPL on or off according to the ring instance functionality. This port can be Port 0 or Port 1.
APS Channel Level	The APS Channel Level for the ring instance, which can be any value between 0 and 7. This value is defined by the Maintenance Entity group Level (MEL) and is used to differentiate various Ethernet problems and to signal them.
Configuration State	The configuration status of the ring instance, which can be Resolved or Unresolved.
Unresolved Reason	The feedback to the configurator that explains the reason for the unresolved configuration state.

Viewing Ring Topology Properties from Topology View

An Ethernet ring consists of multiple Ethernet ring nodes. Each Ethernet ring node is connected to adjacent Ethernet ring nodes using two independent ring links. A ring link prohibits formation of loops that affect the network. The Ethernet ring uses a specific link to protect the entire Ethernet ring. This specific link is called the Ring Protection Link (RPL). A ring link is bound by two adjacent Ethernet ring nodes and a port for a ring link (also known as a ring port). There must be at least two Ethernet ring nodes in an Ethernet ring.

Prime Network uses the following color and pattern conventions to denote the types of links based on their ring type, ring state, and link state:

	RPL,Blocked - Idle
	NonRPL-Idle
	RPL-Protected
	NonRPL-Protected
	NonRPL,Faulty,Blocked-Protected
	RPL,Faulty,Blocked-Protected

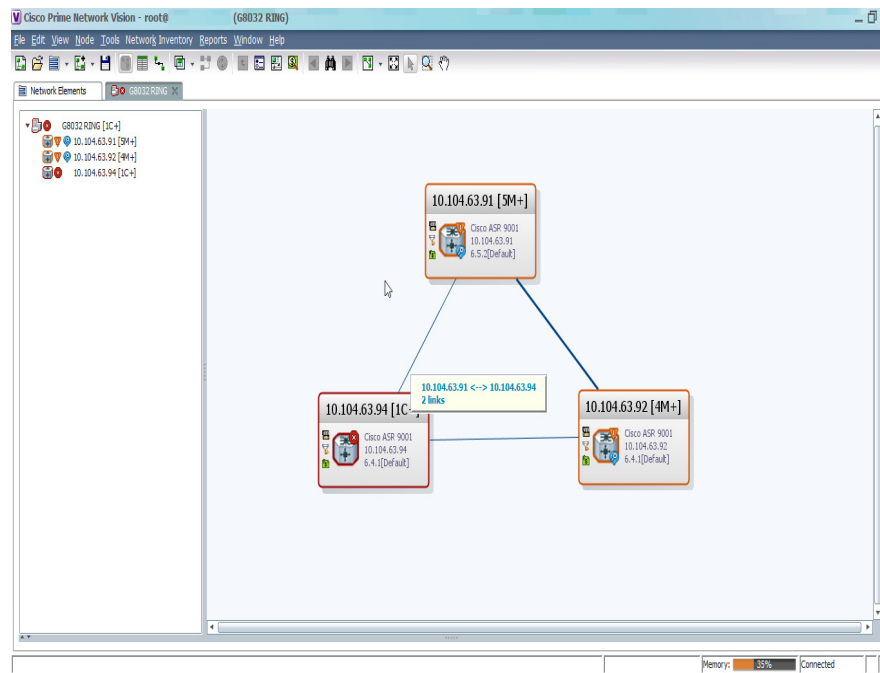
Links are displayed in the map based on the following propagation priority rules:

1. The critical events have first priority and are displayed in the map with corresponding color and pattern of the link (refer Image below) between the devices.
2. If there are no critical events, then faulty events are prioritized.
3. If there are no critical, faulty, or major events, then events with RPL Link color and pattern are prioritized.
4. If there are no RPL links, then the Non RPL link are prioritized.
5. RPL-Protected and Non RPL-Protected are prioritized over RPL,Blocked-Idle and Non RPL-Idle respectively.

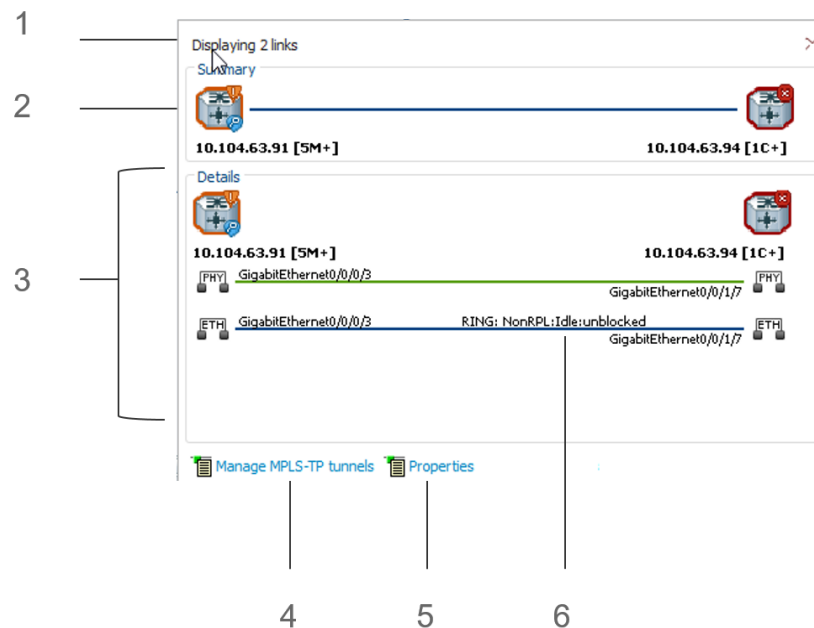
Viewing Ring Link Properties

To view link properties:

- Step 1** In the Vision client map view, hover your mouse cursor over the link to display the link tool tip.



- Step 2** Click the tooltip. The **Link Quick View** opens.



The Link Quick View provides the following information:

1	Number of links represented by the ring link in the map (in this example, two links).
2	Link endpoints.
3	List of all links represented by the ring link, including the link type, detail, and alarm status (color).
4	Opens the Manage MPLS-TP tunnels commands dialog box.
5	Opens the topological link properties window.
6	Ring information - ring type, ring state, and link state



Note

The propagation priority rules of map mentioned above are applicable to Link Quick View too in case of two instances of same interface.

Step 3 Click **Properties** at the bottom of the **Link Quick View**. The **Topological Link Properties** window opens.

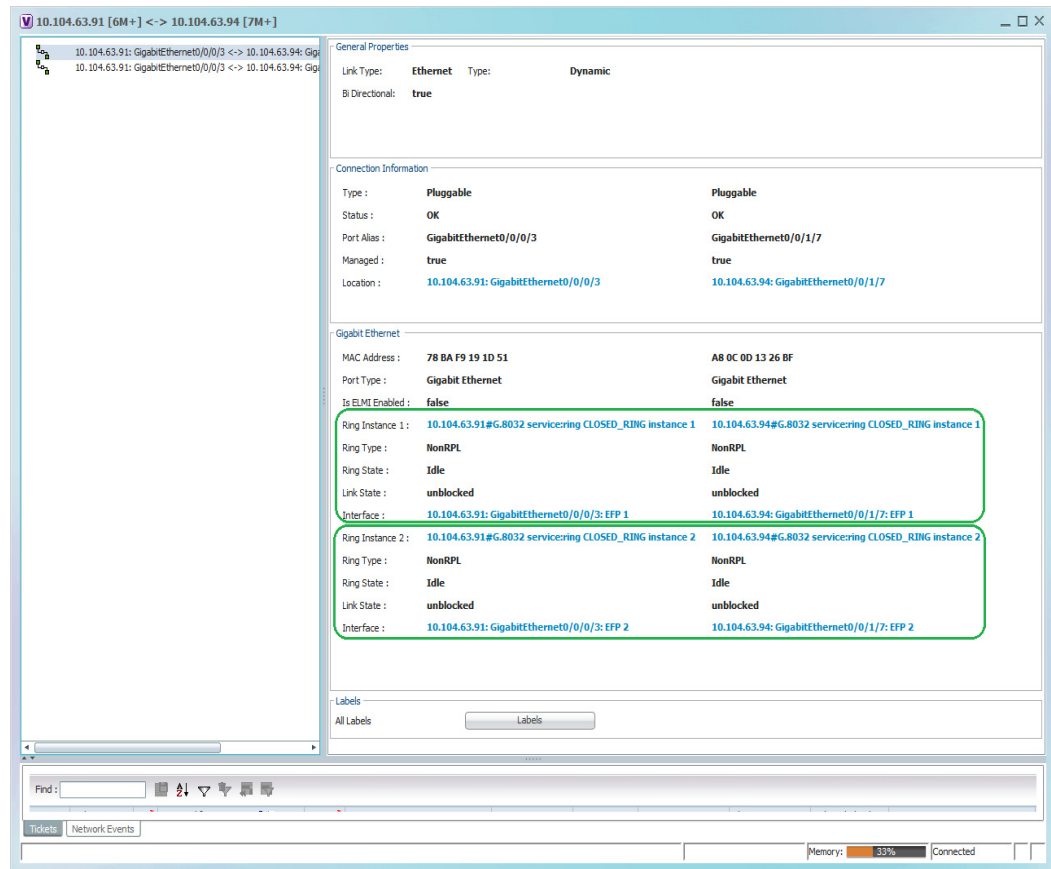


Table 18-64 describes the information that is displayed in the above window for the ring topology instances:

Table 18-64 Ring Instance properties

Field	Description
Gigabit Ethernet	
Ring Instance 1	Link to the Logical Inventory listing of the first ring instance
Ring Type	Type of the ring link of the first ring instance: <ul style="list-style-type: none"> RPL Non RPL
Ring State	State of the ring link of the first ring instance: <ul style="list-style-type: none"> Protection Idle
Link State	State of the link of the first ring instance: <ul style="list-style-type: none"> Blocked Unblocked Faulty, blocked

Table 18-64 Ring Instance properties

Field	Description
Interface	Link to the Physical Inventory listing of the first ring instance
Ring Instance 2	Link to the Logical Inventory listing of the second ring instance
Ring Type	Type of the ring link of the second ring instance: <ul style="list-style-type: none"> • RPL • Non RPL
Ring State	State of the ring link of the second ring instance: <ul style="list-style-type: none"> • Protection • Idle
Link State	State of the link of the second ring instance: <ul style="list-style-type: none"> • Blocked • Unblocked • Faulty, blocked
Interface	Link to the Physical Inventory listing of the second ring instance



Note If there is only one ring instance in a ring topology, the properties of the second ring instance are not displayed.

Configuring REP and mLACP

The following commands can be launched from the inventory by right-clicking the appropriate node and choosing **Commands > Configuration**. Your permissions determine whether you can run these commands (see [Permissions for Managing Carrier Ethernet, page B-12](#)). To find out if a device supports these commands, see the [Cisco Prime Network 5.2 Supported Cisco VNEs](#).

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

Viewing the Remote Loop Free Alternate Configurations

When a link or router in the network fails, there is loss of data during the time it takes for the routers to converge after a topology change. Since it takes hundreds of milliseconds for the router to converge, the application traffic is sensitive to losses especially in the case of interactive multimedia services such as VoIP and pseudowires.

The Loop Free Alternate Fast ReRoute (LFA-FRR) technology helps reduce the packet loss that happens in the event of link or router failure. It reduces the failure reaction time to tens of milliseconds. This is achieved by using a pre-computed alternate next-hop. If the currently selected primary next-hop fails, then the alternate next-hop is used in the event of failure. A network that is configured with the LFA-FRR experiences less traffic loss and micro-looping of packets when compared to a network without LFA-FRR.

The Remote LFA-FRR technology is an extension of LFA that covers all topologies. It can dynamically compute its LFA node and forward traffic around a failed node to a remote LFA that is more than one hop away. After a node dynamically determines an alternate node (which is not directly connected to it), it establishes a directed Label Distribution Protocol (LDP) session to the alternate node. The directed LDP session exchanges labels for the particular forward error correction (FEC). When the network experiences link failure, the node manages to forward the data to the destination by using label stacking.

By configuring Remote LFA-FRR on your network, you can eliminate additional traffic engineering protocols, simplify operations with minimum configuration, prevent hair-pinning that occurs in TE-FRR, and compute node dynamically without manual provision.

In Prime Network, Remote LFA-FRR is configured using IS-IS and OSPF configurations.

To view the OSPF Remote LFA configuration:

-
- Step 1** Right-click on the required device and choose the **Inventory** option.
 - Step 2** In the **Inventory** window, choose **Logical Inventory > OSPF Processes > OSPF Process (version) ID**. The OSPF process details are displayed in the content pane. For more information, see [Viewing IS-IS Properties, page 18-132](#).
 - Step 3** In the content pane, click the **RLFA Tunnels** tab as shown in [Figure 18-79](#).

Figure 18-79 RLFA Tunnels tab

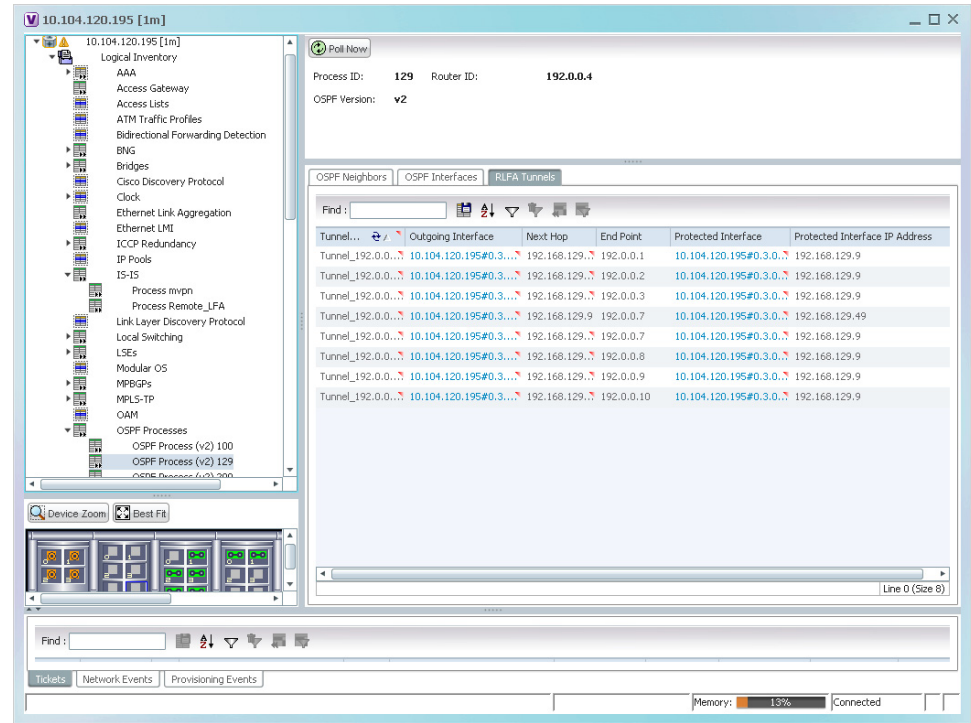


Table 18-65 describes the information that is displayed in the RLFA Tunnels tab.

Table 18-65 OSPF Processes - RLFA Tunnels tab

Field	Description
Tunnel Name	The name of the RLFA tunnel.
Out-Interface	The outgoing interface of the tunnel, which is used to reach the end point. Clicking this link will take you to the relevant entry in the physical inventory node.
Next Hop	The IP address of the next hop in the path.
End Point	The end point of the RLFA tunnel.
Protected Interface	The interface protected by the Remote RLFA tunnel.
Protected Interface IP Address	The IP Address of the interface protected by the Remote RLFA tunnel.

To view the IS-IS Remote LFA configuration:

- Step 1** Right-click on the required device and choose the **Inventory** option.
- Step 2** In the **Inventory** window, choose **Logical Inventory** > **IS-IS** > *Process*. The IS-IS process details are displayed in the content pane. For more information, see [Viewing IS-IS Properties, page 18-132](#).
- Step 3** In the content pane, click the **RLFA Tunnels** tab. For more information, see [Table 18-65](#).

Tie-Breaking Rules for Remote LFA

A primary path can have multiple LFAs. A routing protocol is used to implement tie-breaking rules. When the primary path fails, then these rules help to eliminate multiple candidate LFAs, select one LFA per primary path, and distribute the traffic over multiple LFAs.





Note




The tie-breaking rule has certain conditions and attributes based on which multiple candidate LFAs are eliminated. If a rule eliminates all candidate LFAs, then the rule is omitted.

Configuring OSPF and ISIS with Remote LFA

The following can be launched from the inventory by right-clicking on the appropriate node and choosing **Commands > Configuration**. Your permissions determine whether you can run these commands (see [Permissions for Managing Carrier Ethernet, page B-12](#)). To find out if a device supports these commands, see the [Cisco Prime Network 5.2 Supported Cisco VNEs](#).

Command	Navigation	Description
Create OSPF Process	In the Inventory window, right-click on the device > Commands > Configuration > OSPF .	Create a new OSPF process. The new OSPF process created here will be available under the OSPF Processes node in the Logical Inventory.
Show OSPF Database		View the OSPF database details.
Create OSPF Network	Logical Inventory > OSPF Processes > OSPF Process . Right-click on the process and choose Commands > Configuration .	Create one or more of the following OSPF Networks—Broadcast, Non-broadcast, Point-to-multipoint, and Point-to-point.
Delete OSPF Network		Delete an OSPF Network created using the Create OSPF Network command.
Delete OSPF Process		Delete an OSPF process created using the Create OSPF Process command.
Modify OSPF Process		Modify details of the OSPF process created using the Create OSPF Process command.
Create OSPF Passive Interface		Create a passive interface for an OSPF process.
Delete OSPF Passive Interface		Delete a passive interface for an OSPF process.

Command	Navigation	Description
Show OSPF Neighbor	Logical Inventory > OSPF Processes > <i>OSPF process</i> . Right-click and choose Commands > Show.	View the OSPF neighbor details.  Note This command is available only for ASR 9000 devices.
Show OSPF Process	Logical Inventory > OSPF Processes > <i>OSPF process</i> . Right-click and choose Commands > Show	View the OSPF process details.
Create OSPF on Interface	Logical Inventory > Routing Entities > Routing Entity. In the content pane, right-click the name in the IP Interfaces tab and choose Commands > Configuration.	Create a new IP interface on an existing OSPF process. The new interface details can be viewed under the OSPF Interfaces section in the content pane on selection of an OSPF process.
Modify OSPF on Interface	Logical Inventory > OSPF Processes > <i>OSPF process</i> . In the OSPF Interfaces section in the content pane, right-click the IP Interface > Commands > Configuration.	Modify the OSPF interface details for a selected OSPF process.  Note This command is available only for ASR 9000 devices.
Delete OSPF from Interface		Delete the OSPF interface details for a selected OSPF process.  Note This command is available only for ASR 9000 devices.
Show OSPF On Interface	Logical Inventory > Routing Entities > Routing Entity. In the content pane, Right-click the name in the IP Interfaces tab and choose Commands > Configuration.	View the OSPF interface details.
Create ISIS Router	Logical Inventory > IS-IS > System. Right-click and choose Commands > Configuration.	Create a new ISIS process.

Command	Navigation	Description
Create ISIS Address Family	Logical Inventory > IS-IS. In the content pane, Right-click the process and choose Commands > Configuration.	Create an Address Family (IPV4 or IPV6)for a selected ISIS process.
Create ISIS Interface		Create an ISIS interface for the selected process.
Delete ISIS Address Family		Delete the Address Family (IPV4 or IPV6) created for the selected ISIS process.
Delete ISIS Router		Delete the ISIS process.
Modify ISIS Address Family		Modify the Address Family (IPV4 or IPV6) details created for the ISIS process.
Modify ISIS Router		Modify the ISIS process details.
Create ISIS Interface Address Family		Create an Address Family for an ISIS interface. 
		Note This command is applicable only for ASR 9000.
Modify ISIS Interface Address Family		Modify the Address Family details created for an ISIS interface. 
		Note This command is applicable only for ASR 9000 devices.
Delete ISIS Interface Address Family	Delete the Address Family details created for an ISIS interface. 	
	Note This command is applicable only for ASR 9000 devices.	

Using Pseudowire Ping and Show Commands

The following commands can be launched from the inventory by right-clicking the appropriate node and choosing **Commands > Configuration**. Your permissions determine whether you can run these commands (see [Permissions for Managing Carrier Ethernet, page B-12](#)). To find out if a device supports these commands, see the [Cisco Prime Network 5.2 Supported Cisco VNEs](#).

Command	Navigation	Description
Ping Pseudowire	Logical Inventory > Pseudowires > right-click the interface > Commands > Configure >	<p>Pings 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:</p> <ul style="list-style-type: none"> • 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 <p>You can choose to ping the peer router by default or provide the IP of the required destination router to ping.</p>
Display Pseudowire	Logical Inventory > Pseudowire > right-click the required interface > Commands > Show > Display Pseudowire	Shows 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 following IS-IS commands can be launched from the inventory by right-clicking on the appropriate node and choosing **Commands > Configuration**. Your permissions determine whether you can run these commands (see [Permissions for Managing Carrier Ethernet](#), page B-12). To find out if a device supports these commands, see the [Cisco Prime Network 5.2 Supported Cisco VNEs](#).

Command	Navigation	Description
Create ISIS Router	ISIS > right-click System > Commands > Configuration	Creates 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. 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	Modifies or deletes an existing IS-IS routing configuration for the specified routing process.
Create ISIS Interface	ISIS > System > right-click Process ID in content pane > Commands > Configuration	Creates or modifies 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 the 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.