

Cisco Prime Network 3.9 User Guide

June 13, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-26486-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco Prime Network 3.9 User Guide
© 1999-2012 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface xvii

Audience xvii

Document Organization xviii

Conventions xx

Related Documentation xxi

Obtaining Documentation and Submitting a Service Request xxi

CHAPTER 1 **Cisco Prime Network Client Overview** 1-1

Basic Prime Network Terminology 1-1

Prime Network Security: Permissions, Roles, and Scopes 1-3

Prime Network Vision 1-4

Prime Network Events 1-7

CHAPTER 2 **Working with the Cisco Prime Network Vision Client** 2-1

User Roles Required to Work with Prime Network Vision 2-1

Launching Prime Network Vision 2-2

Launching Prime Network Vision from Prime Central 2-2

Launching Prime Network Vision as a Standalone Application 2-3

Prime Network Vision Window 2-4

Prime Network Vision Inventory Tabs 2-5

Opening Inventory Tabs 2-6

Working with Inventory Tabs 2-7

Prime Network Vision Maps 2-7

Opening Maps 2-8

Working with Multiple Tabs 2-9

Navigation Pane 2-9

Content Pane: Map, List, and Links Views 2-10

Ticket Pane 2-24

Prime Network Vision Status Indicators 2-24

Severity 2-24

VNE Management State 2-25

Tickets 2-29

Prime Network Vision Toolbar 2-29

Prime Network Vision Menu Bar 2-31
File Menu 2-32
Edit Menu 2-33
View Menu 2-33
Node Menu 2-34
Tools Menu 2-35
Activation Menu 2-35
Network Inventory Menu 2-36
Reports Menu 2-36
Window Menu 2-36
Help Menu 2-37
Prime Network Vision Right-Click Menus 2-37
Map Right-Click Menu 2-38
Element Right-Click Menu 2-38
Aggregation Right-Click Menu 2-42
Link Right-Click Menu 2-42
List View Right-Click Menu 2-43
Links View Right-Click Menu 2-45
Ticket Right-Click Menu 2-46
Changing a User Password in Prime Network Vision 2-47
Selecting Prime Network Vision Options 2-47
Working with Prime Network Tables 2-49
Table Toolbar Options 2-50
Using Keyboard Shortcuts in Tables 2-51
Finding Text in a Table 2-51
Sorting a Table 2-51
Filtering Table Contents 2-53
Viewing Selected Rows 2-54
Exporting Tables to a File 2-55

CHAPTER 3 **Viewing Network Element Properties** 3-1
User Roles Required to Work with Prime Network Vision 3-2
Information Available in Element Icons 3-3
Viewing the Properties of a Network Element 3-5
Network Element Badges 3-8
Viewing and Modifying VNE Properties 3-9
Viewing VNE Communication Status 3-11
Updating VNE Information 3-12

Opening the Inventory Window 3-12
Navigation Pane 3-15
Content Pane 3-16
Device View Pane 3-16
Device View Pane Toolbar 3-17
Ticket and Events Pane 3-18
Viewing the Physical Properties of a Device 3-19
Working with Ports 3-22
Viewing Port Status and Properties 3-22
Viewing a Port Configuration 3-24
Disabling Alarms 3-26
Enabling Alarms 3-26
Generating the Port Utilization Graph 3-27
Viewing the Logical Properties of a Network Element 3-27
Logical Inventory Window 3-28
Logical Inventory Navigation Pane Branches 3-29
Logical Inventory Navigation Pane Icons 3-30
Logical Inventory Content Pane Tabs 3-32
Viewing Device Operating System Information 3-33

CHAPTER 4 **Working with Prime Network Vision Maps** 4-1
User Roles Required for Working with Prime Network Vision Maps 4-2
Using Chinese Characters 4-5
Opening and Closing Maps 4-5
Opening Previously Viewed Maps 4-6
Opening a Map from the Open Map Dialog Box 4-6
Closing a Map 4-8
Creating a New Map 4-8
Working with Elements in a Map 4-9
Adding Elements to a Map 4-9
Resizing Map Elements 4-14
Using Your Mouse 4-14
Using the Resize Option 4-14
Using Zoom 4-15
Removing Elements from a Map 4-15
Managing Maps 4-16
Selecting Map Viewing Options 4-16
Defining a Map Layout 4-17

Applying a Background Image 4-17
Using the Overview Window 4-19
Renaming a Map 4-20
Saving Maps 4-20
Saving a Map with Information 4-20
Saving a Map as a New Map 4-21
Saving a Map as an Image 4-21
Previewing and Printing a Map 4-23
Deleting a Map from the Prime Network Vision Database 4-25
Finding Items in a Map 4-26
Finding a Network Element or Service 4-26
Finding and Selecting Links in Maps 4-27
Finding Elements Affected by a Ticket 4-27
Working with Aggregations 4-28
Grouping Network Elements into Aggregations 4-29
Adding Elements to an Existing Aggregation 4-30
Viewing an Aggregation Thumbnail 4-30
Renaming Aggregations 4-32
Ungrouping Aggregations 4-33
Working with Overlays 4-33
Applying an Overlay 4-34
Hiding or Viewing an Overlay 4-37
Removing an Overlay 4-37
Filtering Links in a Map 4-38
Filtering Links During Map Creation 4-38
Filtering Links in an Existing Map 4-40
Opening the CPU Usage Graph 4-40
Communicating with Devices Using Ping and Telnet 4-41

CHAPTER 5 **Working with Links** 5-1
User Roles Required to Work with Links 5-1
Understanding Dynamic and Static Links 5-3
Link Discovery and Flickering Ethernet Topology Links 5-3
Viewing Link Properties 5-4
Viewing Link Properties in Prime Network Vision Maps 5-4
Viewing Link Properties in the Links View 5-8
Viewing Link Properties in the Link Properties Window 5-10
Link List Pane 5-11

Properties Pane 5-11
Ticket and Events Pane 5-12
Viewing Link Impact Analysis 5-13
Adding Static Links 5-15
Filtering Links Using the Collection Method 5-18
Selecting a Link 5-18

CHAPTER 6 **Working with Business Tags and Business Elements** 6-1
User Roles Required to Work with Business Tags and Business Elements 6-1
Using Chinese Characters 6-3
Attaching and Detaching Business Tags 6-3
Searching for Business Tags and Viewing Their Properties 6-5
Renaming a Business Element 6-8
Deleting a Business Element 6-8

CHAPTER 7 **Working with the Prime Network Events Client** 7-1
User Roles Required to Work with Prime Network Events 7-1
Launching Prime Network Events 7-2
Launching Prime Network Events from Prime Central 7-3
Launching Prime Network Events as a Standalone Application 7-3
Prime Network Events Window 7-3
Prime Network Events Toolbar 7-7
Prime Network Events Menu Bar 7-8
Prime Network Events Right-Click Options 7-9
Selecting Prime Network Events Viewing Options 7-10

CHAPTER 8 **Tracking Faults Using Prime Network Events** 8-1
User Roles Required to Work with Prime Network Events 8-1
Viewing Events and Tickets in Cisco Prime Network Events 8-2
All Tab 8-3
System Event Tabs 8-3
Audit Tab 8-3
Provisioning Tab 8-5
Security Tab 8-5
System Tab 8-6
Network Event Tabs 8-6
Service Tab 8-7

Syslog Tab 8-7
Ticket Tab 8-8
V1 Trap Tab 8-10
V2 Trap Tab 8-10
V3 Trap Tab 8-11
Viewing 3.6.x Tabs 8-12
Working with Cisco Prime Network Events 8-14
Viewing Event Properties 8-14
Viewing Ticket Properties 8-19
Refreshing Cisco Prime Network Events Information 8-21
Filtering Events 8-22
Defining Filters 8-23
Removing Filters 8-24
Exporting Displayed Data 8-25

CHAPTER 9 **Working with Tickets in Cisco Prime Network Vision** 9-1
Tickets - Overview 9-1
User Roles Required to Work with Tickets in Prime Network Vision 9-1
Viewing Tickets and Network Events for Elements in a Map 9-3
Managing Tickets in the Tickets Tab 9-4
Understanding Ticket Status 9-6
Filtering Tickets by Network Element 9-8
Filtering Tickets by Criteria 9-8
Viewing Ticket Properties 9-10
Ticket Properties Toolbar 9-12
Details Tab 9-12
History Tab 9-13
Affected Parties Tab 9-14
Correlation Tab 9-17
Advanced Tab 9-18
Notes Tab 9-18
User Audit Tab 9-19
Managing Tickets 9-19
Finding Affected Elements 9-19
Acknowledging a Ticket 9-19
Clearing a Ticket 9-20
Removing a Ticket 9-21
Clearing and Removing Tickets 9-21
Impact Analysis in Prime Network 9-22

Status Values for Affected Parties 9-22
Accumulating Affected Parties 9-23
Accumulating the Affected Parties in an Alarm 9-23
Accumulating the Affected Parties in the Correlation Tree 9-23
Updating Affected Severity over Time 9-24

CHAPTER 10 **Working with Reports** 10-1
User Roles Required to Manage Reports 10-1
Using the Report Manager 10-4
Menu Options 10-6
Report Manager Toolbar 10-6
Navigation Tree 10-7
Content Pane 10-7
Right-Click Options 10-9
Report Categories 10-11
Events Reports 10-11
Inventory Reports 10-18
Network Service Reports 10-20
Generating Reports 10-22
Database Load and Report Generation 10-23
Report Generation Failure 10-23
Report Generation Canceled 10-23
Generating Reports from Report Manager 10-23
Generating Events Reports 10-23
Generating Inventory Reports 10-31
Generating Network Service Reports 10-34
Generating Reports from the Reports Menu 10-37
Generating Reports from Prime Network Vision 10-38
Scheduling Reports 10-38
Managing Reports 10-39
Managing the Maximum Number of Concurrent Reports 10-39
Viewing and Saving Reports 10-40
Renaming Reports 10-41
Sharing Reports 10-42
Moving Reports Between Folders 10-43
Deleting Reports 10-43
Viewing Report Properties 10-44
Defining Report Types 10-46
Working with Report Folders 10-46

Creating Folders 10-46
Moving Folders 10-47
Renaming Folders 10-47
Deleting Folders 10-48
Viewing Folder and Report Type Properties 10-48
Viewing Report Folder Properties 10-48
Viewing Report Type Properties 10-50

CHAPTER 11 **Using Cisco PathTracer to Diagnose Problems** 11-1
User Roles Required to Work with Cisco PathTracer 11-1
Cisco PathTracer Overview 11-2
Launching Path Traces 11-3
Cisco PathTracer Right-Click Menu Options 11-4
Starting a Path Trace 11-5
From the Map View 11-5
From Logical or Physical Inventory 11-7
Examples of Launching Cisco PathTracer 11-7
Viewing Path Traces in Cisco PathTracer 11-14
Menus 11-16
Toolbar 11-17
Trace Tabs 11-18
Paths Pane 11-18
Path Trace Pane 11-18
Right-Click Menu Options 11-19
Viewing Path Trace Details 11-21
Menus 11-22
Cisco PathTracer Details Window Toolbar 11-23
Path Trace Pane 11-23
Details Pane 11-25
Saving and Opening Cisco PathTracer Map Files 11-26
Saving Cisco PathTracer Counter Values 11-27
Rerunning a Path and Comparing Results 11-27
Viewing Q-in-Q Path Information 11-28
Viewing L2TP Path Information 11-29
Using Cisco PathTracer in MPLS Networks 11-29
Cisco PathTracer MPLS Start and Endpoints 11-30
Using Cisco PathTracer for CSC Configurations 11-31
Using Cisco PathTracer for Layer 3 VPNs 11-32

Using Cisco PathTracer for Layer 2 VPNs 11-33
Using Cisco PathTracer for MPLS TE Tunnels 11-34

CHAPTER 12 **Monitoring Carrier Ethernet Services** 12-1
User Roles Required to Work with Carrier Ethernet Services 12-2
Viewing CDP Properties 12-6
Viewing Link Layer Discovery Protocol Properties 12-8
Viewing Spanning Tree Properties 12-10
Viewing Resilient Ethernet Protocol Properties 12-14
Viewing Access Gateway Properties 12-18
Working with Ethernet Link Aggregation Groups 12-21
Viewing Ethernet LAG Properties 12-22
Viewing mLACP Properties 12-27
Viewing Provider Backbone Bridge Properties 12-30
Viewing EFP Properties 12-31
Understanding EFP Severity and Ticket Badges 12-36
Viewing EVC Service Properties 12-37
Viewing and Renaming Ethernet Flow Domains 12-39
Working with VLANs and VLAN Overlays 12-42
Understanding VLAN and EFD Discovery 12-42
Understanding VLAN Elements 12-43
Switching Entities Containing Termination Points 12-48
Adding VLANs to a Map 12-48
Removing VLANs from a Map 12-50
Viewing VLAN Mappings 12-50
Working with Associated VLANs 12-52
Adding an Associated VLAN 12-52
Viewing Associated Network VLAN Service Links and VLAN Mapping Properties 12-54
Viewing VLAN Links Between VLAN Elements and Devices 12-55
Applying VLAN Overlays 12-58
Displaying or Hiding VLAN Overlays 12-59
Removing a VLAN Overlay 12-59
Viewing VLAN Service Link Properties 12-60
Viewing REP Information in VLAN Domain Views and VLAN Overlays 12-60
Viewing REP Properties for VLAN Service Links 12-61
Viewing STP Information in VLAN Domain Views and VLAN Overlays 12-63
Viewing STP Properties for VLAN Service Links 12-64
Viewing VLAN Trunk Group Properties 12-65

Viewing VLAN Bridge Properties 12-67
Understanding Unassociated Bridges 12-70
Adding Unassociated Bridges 12-70
Working with Ethernet Flow Point Cross-Connects 12-72
Adding EFP Cross-Connects 12-73
Viewing EFP Cross-Connect Properties 12-73
Working with VPLS and H-VPLS Instances 12-75
Working with VPLS and H-VPLS in Prime Network Vision 12-75
Adding VPLS Instances to a Map 12-76
Applying VPLS Instance Overlays 12-77
Viewing Pseudowire Tunnel Links in VPLS Overlays 12-79
Viewing VPLS-Related Properties 12-81
Viewing VPLS Instance Properties 12-81
Viewing Virtual Switching Instance Properties 12-83
Viewing VPLS Core or Access Pseudowire Endpoint Properties 12-85
Viewing VPLS Access Ethernet Flow Point Properties 12-87
Working with Pseudowires 12-88
Adding Pseudowires to a Map 12-88
Viewing Pseudowire Properties 12-91
Pinging a Pseudowire 12-94
Displaying Pseudowire Information 12-96
Viewing Pseudowire Redundancy Service Properties 12-98
Applying Pseudowire Overlays 12-100
Working with Ethernet Services 12-101
Adding Ethernet Services to a Map 12-102
Applying Ethernet Service Overlays 12-104
Viewing Ethernet Service Properties 12-105
Viewing IP SLA Responder Service Properties 12-108
Viewing IS-IS Properties 12-110
Viewing OSPF Properties 12-113

CHAPTER 13 **Monitoring Carrier Grade NAT Properties** 13-1
User Roles Required to View Carrier Grade NAT Properties 13-1
Viewing Carrier Grade NAT Properties in Logical Inventory 13-2
Viewing Carrier Grade NAT Properties in Physical Inventory 13-5

CHAPTER 14 **Monitoring DWDM Properties** 14-1
User Roles Required to View DWDM Properties 14-1

Viewing DWDM in Physical Inventory 14-2
Viewing G.709 Properties 14-4
Viewing Performance Monitoring Configuration 14-10

CHAPTER 15 **Viewing Ethernet Operations, Administration, and Maintenance Tool Properties** 15-1
User Roles Required to View Ethernet OAM Tool Properties 15-1
Ethernet OAM Overview 15-2
Viewing Connectivity Fault Management Properties 15-3
Viewing Ethernet LMI Properties 15-9
Viewing Link OAM Properties 15-13

CHAPTER 16 **IPv6 and IPv6 VPN over MPLS** 16-1
User Roles Required to Work with IPv6 and 6VPE 16-2
Viewing IPv6 Information 16-3

CHAPTER 17 **Monitoring MPLS Services** 17-1
User Roles Required to Work with MPLS Networks 17-1
Working with MPLS-TP Tunnels 17-4
Adding an MPLS-TP Tunnel 17-5
Viewing MPLS-TP Tunnel Properties 17-7
Viewing LSPs Configured on an Ethernet Link 17-11
Viewing LSP Endpoint Redundancy Service Properties 17-13
Applying an MPLS-TP Tunnel Overlay 17-16
Viewing VPNs 17-18
Viewing Additional VPN Properties 17-20
Managing VPNs 17-21
Creating a VPN 17-21
Adding a VPN to a Map 17-22
Removing a VPN from a Map 17-23
Moving a Virtual Router Between VPNs 17-23
Working with VPN Overlays 17-24
Applying VPN Overlays 17-24
Managing a VPN Overlay Display in the Map View 17-25
Displaying VPN Callouts in a VPN Overlay 17-25
Monitoring MPLS Services 17-26
Viewing VPN Properties 17-26
Viewing Site Properties 17-27
Viewing VRF Properties 17-27

Viewing VRF Egress and Ingress Adjacents 17-30
Viewing Routing Entities 17-31
Viewing the ARP Table 17-33
Viewing the NDP Table 17-34
Viewing Rate Limit Information 17-35
Viewing VRRP Information 17-36
Viewing Label Switched Entity Properties 17-38
Viewing MP-BGP Information 17-42
Viewing 6rd Tunnel Properties 17-43
Viewing BFD Session Properties 17-44
Viewing Cross-VRF Routing Entries 17-47
Viewing Pseudowire End-to-End Emulation Tunnels 17-47
Viewing MPLS TE Tunnel Information 17-49

CHAPTER 18 **Monitoring MToP Services** 18-1
User Roles Required to Work with MToP 18-1
Viewing SAToP Pseudowire Type in Logical Inventory 18-2
Viewing CESoPSN Pseudowire Type in Logical Inventory 18-3
Viewing Virtual Connection Properties 18-5
Viewing ATM Virtual Connection Cross-Connects 18-6
Viewing ATM VPI and VCI Properties 18-10
Viewing Encapsulation Information 18-11
Viewing IMA Group Properties 18-13
Viewing TDM Properties 18-16
Viewing Channelization Properties 18-17
Viewing SONET/SDH Channelization Properties 18-18
Viewing T3 DS1 and DS3 Channelization Properties 18-21
Viewing MLPPP Properties 18-26
Viewing MLPPP Link Properties 18-29
Viewing MPLS Pseudowire over GRE Properties 18-31
Network Clock Service Overview 18-34
Monitoring Clock Service 18-34
Monitoring PTP Service 18-36
Viewing Pseudowire Clock Recovery Properties 18-41
Viewing SyncE Properties 18-45
Applying a Network Clock Service Overlay 18-48
Viewing CEM and Virtual CEM Properties 18-50
Viewing CEM Interfaces 18-50

Viewing Virtual CEMs 18-51
Viewing CEM Groups 18-51
Viewing CEM Groups on Physical Interfaces 18-51
Viewing CEM Groups on Virtual CEM Interfaces 18-53

CHAPTER 19 **Viewing SBC Properties** 19-1
User Roles Required to View SBC Properties 19-2
Viewing SBC Properties in Logical Inventory 19-3
Viewing SBC DBE Properties 19-4
Viewing Media Address Properties 19-4
Viewing VDBE H.248 Properties 19-5
Viewing SBC SBE Properties 19-6
Viewing AAA Properties 19-6
Viewing H.248 Properties 19-7
Viewing Policy Properties 19-8
Viewing SIP Properties 19-11

CHAPTER 20 **Viewing Mobile Technologies in Prime Network** 20-1
User Roles Required to View GGSN, GTPU, and APN Parameters 20-2
GGSN Overview 20-3
Viewing GGSN Properties 20-4
GTPU Overview 20-6
Viewing GTPU Properties 20-6
APN Overview 20-8
Viewing APN Properties 20-9
Viewing Additional Characteristics of an APN 20-12

APPENDIX A **Icon and Button Reference** A-1
Icons A-1
Network Element Icons A-2
Business Element Icons A-4
Logical Inventory Icons A-6
Physical Inventory Icons A-8
Links A-8
Link Icons A-9
Link Colors A-10
Link Characteristics A-10
Severity Icons A-11

Buttons A-12
Prime Network Vision Buttons A-12
Table Buttons A-15
Link Filtering Buttons A-15
Prime Network Events Buttons A-16
Ticket Properties Buttons A-16
Report Manager Buttons A-17
Badges A-17
VNE Communication State Badges A-18
VNE Investigation State Badges A-18
Network Element Technology-Related Badges A-20
Alarm and Ticket Badges A-20

INDEX



Preface

This document describes Cisco Prime Network (Prime Network) 3.9. Prime Network serves as an extensible integration platform for network and service management. At its core is a virtual network mediation model that is rich, open, and vendor-neutral, and supports the management of diverse multiservice and multivendor networks. Additionally, Prime Network provides the following mature NMS functionality:

- Network topology discovery and visualization.
- Element management, providing near real-time inventory.
- Fault management, event correlation, root cause analysis and troubleshooting.
- Network service support.

This preface contains the following sections:

- Audience, page xvii
- Document Organization, page xviii
- Conventions, page xx
- Related Documentation, page xxi
- Obtaining Documentation and Submitting a Service Request, page xxi

Audience

The intended audience for this documentation includes:

- Network viewers who monitor the network and perform basic (nonprivileged) system functions.
- Network operators who perform day-to-day operations such as creating business tags and maps, and managing alarms.
- Network configurators who activate services and configure network elements.
- System administrators who manage and configure users, network elements, the Prime Network system, and overall security.
- System managers or administrators who periodically review and manage the events list using Cisco Prime Network Events (Prime Network Events).
- Networking engineers who are interested in understanding how the Prime Network Events fault and root cause analysis mechanism works. These engineers should have networking knowledge at Cisco Certified Network Associate (CCNA) level, and should have received Cisco Prime Network Vision (Prime Network Vision) basic and administrative training.

Document Organization

This guide contains the following sections:

Section and Title	Description
Chapter 1, “Cisco Prime Network Client Overview”	Describes the suite of GUI tools that offer an intuitive interface for managing the network and services, and for performing required system administration activities.
Chapter 2, “Working with the Cisco Prime Network Vision Client”	Describes the user access roles required to use Prime Network Vision, the Prime Network Vision working environment, and how to access Prime Network Vision tools and commands.
Chapter 3, “Viewing Network Element Properties”	Describes the user access roles required to use Prime Network Vision and how to view network element physical and logical properties in any mapped network.
Chapter 4, “Working with Prime Network Vision Maps”	Describes how to work with the topological maps displayed in the content pane of the Prime Network Vision window.
Chapter 5, “Working with Links”	Describes how to view information about static and dynamic links using the Prime Network Vision user interface.
Chapter 6, “Working with Business Tags and Business Elements”	Describes how to manage and view Prime Network Vision business tags and business elements.
Chapter 7, “Working with the Prime Network Events Client”	Describes the Prime Network Events application and the options you can use to view system events and tickets that are generated within the Prime Network system.
Chapter 8, “Tracking Faults Using Prime Network Events”	Describes how to use Prime Network Events to track faults.
Chapter 9, “Working with Tickets in Cisco Prime Network Vision”	Describes viewing tickets in Prime Network Vision, how to manage tickets that represent fault scenarios of selected devices or network elements, and fault impact analysis.
Chapter 10, “Working with Reports”	Describes how to use Prime Network Report Manager to generate, customize, view, and export a variety of reports about events, traps, tickets, syslogs, software versions, elements, and network services.
Chapter 11, “Using Cisco PathTracer to Diagnose Problems”	Describes how to perform end-to-end route tracing and the performance information displayed simultaneously for the multiple networking layers.

Section and Title	Description
Chapter 12, “Monitoring Carrier Ethernet Services”	Describes how to view Carrier Ethernet services in Prime Network Vision and how to work with VLANs, pseudowires, overlays, VPLS instances, and Ethernet services.
Chapter 13, “Monitoring Carrier Grade NAT Properties”	Describes the Carrier Grade Name Address Translation (NAT) properties available in Prime Network Vision.
Chapter 14, “Monitoring DWDM Properties”	Describes how to view and monitor IP over dense wavelength division multiplexing (DWDM) properties in Prime Network Vision.
Chapter 15, “Viewing Ethernet Operations, Administration, and Maintenance Tool Properties”	Describes how to use Prime Network Vision to monitor Ethernet operations, administration, and maintenance (OAM) tools.
Chapter 16, “IPv6 and IPv6 VPN over MPLS”	Describes how to use Prime Network Vision to view IPv6 and 6PVE properties.
Chapter 17, “Monitoring MPLS Services”	Describes how to view and manage aspects of Multiprotocol Label Switching (MPLS) services using Prime Network Vision, including the MPLS service view, business configuration, and maps. This section also describes the inventory properties specific to MPLS VPNs, including routing entities, label switched entities (LSEs), BGP neighbors, Multiprotocol BGP (MP-BGP), VRF instances, pseudowires, and traffic engineering (TE) tunnels.
Chapter 18, “Monitoring MToP Services”	Describes Mobile Transport over Packet (MToP) services and how to view their properties in Prime Network Vision.
Chapter 19, “Viewing SBC Properties”	Describes the Session Border Controller (SBC) properties available in Prime Network Vision.
Chapter 20, “Viewing Mobile Technologies in Prime Network”	Describes how to view the mobile technologies in Prime Network Vision.
Appendix A, “Icon and Button Reference”	Identifies the icons and buttons used in Prime Network Events and Prime Network Vision.

Conventions

This document uses the following conventions:

Table 1 Conventions

Convention	Description
string	A string is a nonquoted set of characters. For example, when setting an SNMP community string to public, do not use quotation marks around the string, or the string will include the quotation marks.
^ or Ctrl	^ or Ctrl represents the Control key. For example, the key combination ^D or Ctrl-D means hold down the **Control** key while you press the **D** key. Alphabetic character keys are indicated in capital letters but are not case sensitive.
< >	Angle brackets show nonprinting characters, such as passwords.
!	An exclamation point at the beginning of a line indicates a comment line.
[ ]	Square brackets show optional elements.
{ }	Braces group alternative, mutually exclusive elements that are part of a required choice.
|	A vertical bar, also known as a pipe, separates alternative, mutually exclusive elements of a choice.
boldface font	Button names, commands, keywords, and menu items.
boldface screen font	Courier bold shows an example of text that you must enter.
italic font	Variables for which you supply values.
italic screen font	Variables you enter.
screen font	Courier plain shows an example of information displayed on the screen.
Option > Network Preferences	Choosing a menu item.

Related Documentation

Note We sometimes update the documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

For a complete list of Prime Network 3.9 documentation, see the *Cisco Prime Network 3.9 Documentation Guide*.

Cisco Prime Network 3.9 Integration Developer Guide is available on the Cisco Prime Network Technology Center website. This guide describes how to use Prime Network integration interfaces.

The Prime Network Technology Center is an online resource for additional downloadable Prime Network support content, including help for integration developers who use Prime Network application programming interfaces (APIs). It provides information, guidance, and examples to help you integrate your applications with Prime Network. It also provides a platform for you to interact with subject matter experts. To view the information on the Prime Network Technology Center website, you must have a Cisco.com account with partner level access, or you must be a Prime Network licensee. You can access the Prime Network Technology Center at http://developer.cisco.com/web/prime-network/home.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.



CHAPTER 1

Cisco Prime Network Client Overview

Cisco Prime Network (Prime Network) provides a suite of GUI tools that offer an intuitive interface for managing the network and services, and for performing required system administration activities. The Prime Network client application suite comprises Prime Network Vision, Prime Network Events, and Prime Network Administration.

The following topics provide an introduction to Prime Network terminology and client applications:

- Basic Prime Network Terminology, page 1-1
- Prime Network Security: Permissions, Roles, and Scopes, page 1-3
- Prime Network Vision, page 1-4
- Prime Network Events, page 1-7

Note For information about the Prime Network Administration application, see the *Cisco Prime Network 3.9 Administrator Guide*.

Basic Prime Network Terminology

Table 1-1 provides a brief explanation of the terms used in the Prime Network clients and documentation.

Table 1-1 Definitions

Term	Description
aggregation	A user-defined collection of network elements. For example, an aggregation can contain devices, links, VPNs, and other aggregations.
alarm	Sequence of event notifications that share the same source, cause, or fault. For example, if a single port goes up and then down, these two events in a related sequence may result in a single alarm. An alarm is stateful and is opened when a fault is first detected. Event notifications may be added to the alarm, and it is archived when it is fixed.

Table 1-1 Definitions (continued)

Term	Description
association	A relationship between the following types of network elements: • A logical (protocol-oriented) network element and a physical network element • A logical network element and another logical network element • An existing association and anything else An example for a VPN would be an association between the physical IP interface and Virtual Routing and Forwarding (VRF) table, which is the associated routing table. An association is not considered a topological link.
business element	Construction or organization of certain network elements and their properties into a logical entity, to provide the ability to track them in a way that makes sense from a business perspective. A virtual private network (VPN) is a business element, which represents a set of interconnected sites that form a single network over a public network. Prime Network organizes the business elements in a way that creates a containment hierarchy that reflects the VPN structure.
business tag	A string that is meaningful to the business, and that can be used to label a component of a network element for use in Prime Network screens and reports. There are three types of business tags: subscriber, provider, and label. Business tags are stored in the Prime Network gateway database.
event	In the context of network management, a discrete activity that occurred at a specific point in time.
link	A physical or logical connection between: • Two devices in the network • A device and an aggregation • Two aggregations
logical link	An association between two network elements (based on a chain of physical links between the elements); for example, a tunnel.
managed element	A network element that is managed by Prime Network; for example, a device, cloud, or Internet Control Message Protocol (ICMP) VNE.
network element	Any physical component or device in the network that can be managed through an IP address.
physical link	A link between physical network objects; for example, a connection between two physical ports.
provider	The party providing a service.
subscriber	The party receiving a service.

Table 1-1 Definitions (continued)

Term	Description
ticket	Object that represents an attention-worthy root alarm whose type is marked in the registry as "ticketable." A ticket has the same type as the root alarm it represents, and it has a status, which represents the entire correlation tree. A ticket can be acknowledged by the user. Both Prime Network Vision and Cisco Prime Network Events display tickets and allow you to navigate down to view the consequent alarm hierarchy. From an operator's point of view, a fault is always represented by a complete ticket. Operations such as Acknowledge or Remove are applied to the whole ticket.
virtual cloud or unmanaged network	Network, or part of a network, that is not managed by Prime Network. An unmanaged network is often represented in network diagrams by a cloud symbol or image.
VLAN	Virtual local-area network (LAN). Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.
VPN	Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses *tunneling* to encrypt all information at the IP level.

Prime Network Security: Permissions, Roles, and Scopes

Prime Network provides enhanced security when working with and managing the Prime Network system. Users are assigned permission levels for an operational scope, enabling them to perform only the functions assigned to the scope and defined security level. A user can be assigned more than one security level.

Permission

The user's ability to perform certain tasks. There are two types of permissions: GUI-related and element-related.

- GUI-related—Applies only to the activities that are related to GUI functionality, and not the activities related to network elements. For example, a user with the default permission Viewer can view maps and the element list. For more information, see the *Cisco Prime Network 3.9 Administrator Guide*.
- Element-related—Enables the administrator to group a collection of managed elements (in Prime Network Administration) to allow the user to view and manage the elements based on the user's role or permission. After the user is allocated a scope (group of elements) and a role, the user can then perform various activities on the allocated elements, such as viewing maps or generating reports on the elements using Report Manager. For more information, see the *Cisco Prime Network 3.9 Administrator Guide*.

Roles

Prime Network implements a security engine that combines a role-based security mechanism that is applied on scopes of network elements granted per user. The system supports:

- User account creation
- Network element scope definition
- A set of five predefined roles for security and access control that allow different system functions. The roles, listed from the lowest security level to the highest security level, are:
  - Viewer—Have read-only access to the network and to nonprivileged system functions.
  - Operator—Configure business tags and perform most day-to-day operations.
  - Operator Plus—Fully control alarm life cycle and create maps.
  - Configurator—Activate services and configure the network.
  - Administrator—Manage the system configuration and security.

Note Viewer is the lowest security level, and Administrator is the highest. A user with a higher security level can perform all the Prime Network functions assigned to a user with a lower security level.

Each user is assigned a permission level for an operational scope, which enables the user to perform certain tasks. Every user has a private username and password. A user can log in from any workstation with their own set of permissions and operational scope. When a user does not have the required permission level to perform a function, the appropriate menu option or button is disabled.

The administrator is responsible for defining the types of activities that the user can view and perform using Prime Network Administration. For more information about user security and defining operational scopes, see the *Cisco Prime Network 3.9 Administrator Guide*.

A user's role (their default permissions) applies only to the activities that are related to GUI functionality, not the activities related to network elements (which are controlled by scopes). Default permissions control Prime Network functions.

Scopes

A scope is a named collection of managed network elements that have been grouped together to allow a user to view or manage the network elements, based on their access role. Grouping can be based on geographical location, network element type (such as DSLAM, router, or software), network element category (such as access or core), or any other division according to the network administrator's requirements.

For example, using Prime Network Vision, a user who has been assigned a scope can view or manage the network elements within this scope, according to the role assigned to the user for that scope. The user cannot view any information regarding network elements that are outside their scope, including basic properties, inventory, and alarms.

Prime Network Vision

Prime Network Vision is the main GUI application used to visualize the network through network and service maps, to view element physical and logical inventories and connectivity, and to manage device configuration and software images. It provides total visibility for multiple-tier, multiple-technology networks, and supports fault and configuration functionality. The highly optimized, customizable GUIs enable constant, system-wide surveillance of the network and service states, down to the node level.

Prime Network Vision supports the creation of multiple network maps to represent specific network views. Views can cover specific network segments, customer networks, or any other mix of network elements desired. Once the maps have been created, they are available for all connecting clients (with support for fine-grained access privileges).

Prime Network Vision enables you to:

- View network inventory and multiple-layer connectivity.
- Troubleshoot, monitor, and manage network elements.
- Model and view network maps, maintaining up-to-date topological information on connections, traffic, and routes.

Prime Network Vision maps based on Prime Network's representation of VNEs provide a graphic display of active faults and alarms, and serve as an easy access point for activation of services. Prime Network provides rich functionality for displaying and managing network maps by providing:

- Multiple concurrent maps per user.
- Easily customizable hierarchy of nested submaps, aggregations, and business tags with easy navigation up and down the hierarchy.
- Dual views of the network in a hierarchical tree, as well as in topological maps, including all network connections.
- Network elements and links using color cues and graphic symbols to indicate status and alarms.
- Mouse point-and-click drill-down from every element (either from the tree or map), providing detailed internal physical and logical inventory information.

For details on using Prime Network Vision when working with specific technologies, see the following topics:

- Carrier Ethernet services—Chapter 12, "Monitoring Carrier Ethernet Services"
- Carrier Grade NAT properties—Chapter 13, "Monitoring Carrier Grade NAT Properties"
- Dense wavelength division multiplexing (DWDM) services—Chapter 14, "Monitoring DWDM Properties"
- Ethernet Operations, Administration, and Maintenance (E-OAM) tool properties—Chapter 15, "Viewing Ethernet Operations, Administration, and Maintenance Tool Properties"
- IPv6 and 6VPE technologies—Chapter 16, "IPv6 and IPv6 VPN over MPLS"
- Multiprotocol Label Switching (MPLS) services—Chapter 17, "Monitoring MPLS Services"
- Mobile Transport over Packet services—Chapter 18, "Monitoring MToP Services"
- Session Border Controller properties—Chapter 19, "Viewing SBC Properties"

Prime Network Vision is also the launch point for:

- Cisco PathTracer
- Prime Network Soft Properties Manager
- Prime Network Command Builder
- Prime Network Report Manager
- Prime Network Change and Configuration Management
- Prime Network Activation

Cisco PathTracer

Cisco PathTracer enables you to perform end-to-end route tracing with pertinent performance information displayed simultaneously for the multiple networking layers. Upon receiving a path's starting point and end point, Cisco PathTracer visually traces the route through the network. For more information about Cisco PathTracer, see Chapter 11, "Using Cisco PathTracer to Diagnose Problems."

Prime Network Soft Properties Manager

The Prime Network Soft Properties Manager enables you to manage soft properties and threshold-crossing alarms (TCAs).

The Prime Network Soft Properties Manager allows you to extend the set of supported properties for each network element by adding soft properties to the VNEs. These properties extend the Prime Network Information Model Object (IMO) and are available through the client GUI as well as through the Broadband Query Language (BQL) API.

Soft properties are retrieved from the network element using Simple Network Management Protocol (SNMP), Telnet, Secure Shell Protocol (SSH), or Transaction Language One (TL-1).

In addition, alarm thresholding enables you to constantly monitor selected properties and generate an alarm each time they cross a user-defined threshold or violate a condition.

The Prime Network Soft Properties Manager tool is typically used by integrators or other users who want to manage the soft properties and TCAs that are executed within the Prime Network platform.

For more information on the Prime Network Soft Properties Manager, see the *Cisco Prime Network 3.9 Administrator Guide*.

For more information about using BQL with Prime Network, see the *Cisco Prime Network 3.9 Integration Developer Guide.*

Prime Network Command Builder

The Prime Network Command Builder enables you to execute a programmable sequence of SNMP or Telnet command lines. These command lines can include data properties taken from the Prime Network information model (built-in) or user-defined input parameters entered during runtime.

The Prime Network Command Builder is launched from a managed element (Prime Network-modeled VNE) such as a port, typically from the Prime Network Vision inventory window. The managed element is then used to develop and test the command. Once the command has been completed, you can publish it and attach it to a wider scope of managed elements.

For more information on the Prime Network Command Builder, see the *Cisco Prime Network 3.9 Customization User Guide*.

Prime Network Report Manager

The Prime Network Report Manager enables you to generate, customize, view, and export a variety of reports about events, traps, tickets, syslogs, software versions, elements, and network services. The Report Manager, available from Prime Network Administration, Prime Network Vision, and Prime Network Events, provides out-of-the-box reports for events, inventory, and networks services.

The Report Manager enables you to:

- Produce reports on demand.
- Save generated reports in PDF, CSV, HTML, XLS, or XML format.
- Customize reports for your environment.
- Generate reports for the nonactionable events that are not displayed in Prime Network Events.

For information about reports and Report Manager, see Chapter 10, "Working with Reports."

You can also retrieve reports using BQL. For more information, see the *Cisco Prime Network 3.9 Integration Developer Guide.*

Cisco Prime Network Change and Configuration Management

Prime Network Change and Configuration Management provides tools that allow you to manage the software and device configuration changes that are made to devices in your network. Device configuration management tools are provided by the Configuration Management (CM) function, and software image management tools are provided by the Network Element Image Management (NEIM) function.

For more information on Prime Network Change and Configuration Management, see the *Cisco Prime Network 3.9 Change and Configuration Management User and Administration Guide*.

Cisco Prime Network Activation

Prime Network Activation is a GUI client that you can use to create Activation wizards. Activation wizards are GUI wizards that are added to the Prime Network Vision GUI client. Operators can launch these wizards to create, modify, and delete activations on network devices. The Activation Wizard Builder (AWB) provides a user-friendly interface for creating wizards according to the needs of your network. For more information, see the *Cisco Prime Network 3.9 Customization User Guide*.

Prime Network Events

Prime Network Events is the interface used by administrators for viewing system events and tickets that are generated within the Prime Network system.

Prime Network Events is a GUI application that serves as a browser for viewing and retrieving detailed information about the different types of system events and tickets that are generated. Monitoring with Prime Network Events helps predict and identify the sources of system problems, which in turn assists in preventing future problems.

You can configure Prime Network Events to display the following information:

- Number of events per page.
- Number of events to be exported to a file.
- Previous dated events (in weeks).
- Filter options.
- The information that appears in Prime Network Events tabs, such as the Audit tab.

System managers or administrators periodically review and manage the events list using Prime Network Events. In addition, when an event occurs in the Prime Network system, the details become available in Prime Network Events.

All administrator activities in Prime Network Administration are logged and available in Prime Network Events. For more information on Prime Network Administration, see the *Cisco Prime Network 3.9 Administrator Guide*.



CHAPTER 2

Working with the Cisco Prime Network Vision Client

The following topics describe the user access roles required to use Cisco Prime Network Vision (Prime Network Vision), the Prime Network Vision working environment, and how to access the Prime Network Vision tools and commands:

- User Roles Required to Work with Prime Network Vision, page 2-1
- Launching Prime Network Vision, page 2-2
- Prime Network Vision Window, page 2-4
- Prime Network Vision Status Indicators, page 2-24
- Prime Network Vision Toolbar, page 2-29
- Prime Network Vision Menu Bar, page 2-31
- Prime Network Vision Right-Click Menus, page 2-37
- Changing a User Password in Prime Network Vision, page 2-47
- Selecting Prime Network Vision Options, page 2-47
- Working with Prime Network Tables, page 2-49

User Roles Required to Work with Prime Network Vision

Table 2-1 identifies the GUI default permission or device scope security level that is required to work with Prime Network Vision. Prime Network Vision determines whether you are authorized to perform a task as follows:

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

For more information on user authorization, see the *Cisco Prime Network 3.9 Administrator Guide*.

By default, users with the Administrator role have access to all managed elements. To change the Administrator user scope, see the topic on device scopes in the *Cisco Prime Network 3.9 Administrator Guide*.

Table 2-1 Default Permission/Security Level Required for Prime Network Vision Functions

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Start Prime Network Vision	X	X	X	X	X
Change a user password in Prime Network Vision	—[1]	—[1]	—[1]	—[1]	X[1]
Set Prime Network Vision options	X	X	X	X	X
Work with Prime Network Vision tables	X	X	X	X	X

1. Each user can change their own password, but only the Administrator role can change another user's password.

Launching Prime Network Vision

Prime Network provides two methods for launching Prime Network Vision:

- From the Cisco Prime Central portal
- As a standalone application

Prime Network Vision is password protected to ensure security. Before you start working with Prime Network Vision, make sure you know your username and password. If you use the standalone application, you also need to know the Prime Network Vision gateway IP address or hostname.

Note If you do not log into Prime Network Administration, Prime Network Vision, or Prime Network Events during a specified period of time (the default is one month) from the standalone application, your account is automatically locked. The default period can be changed per user in Prime Network Administration. The period of time is measured from the time you last logged out of any of the Prime Network client applications. For more information about changing the default period and unlocking an account, see the *Cisco Prime Network 3.9 Administrator Guide*.

The following topics describe how to launch Prime Network Vision:

- Launching Prime Network Vision from Prime Central, page 2-2
- Launching Prime Network Vision as a Standalone Application, page 2-3

Launching Prime Network Vision from Prime Central

If Prime Central is available in your environment, you can launch Prime Network applications from the main Prime Central page.

To launch Prime Network Vision from Prime Central, choose **Assure > Prime Network > Vision** in the menu bar.

The Prime Network Vision application is opened in a separate window.

For more information about using Prime Network Vision with the Prime Central suite of products, see:

- *Cisco Prime Central 1.0 User Guide*
- Prime Network Vision Right-Click Menus, page 2-37

Launching Prime Network Vision as a Standalone Application

To launch Prime Network Vision as a standalone application:

Step 1 Choose **Start > Programs > Cisco Prime Network > gateway hostname/IP address >** Cisco Prime Network Vision.

Note The hostname/IP address corresponds to the gateway on which Prime Network was configured.

The Cisco Prime Network Vision login dialog box is displayed.

Step 2 Enter your username and password.

The Server field should already be populated with the hostname/IP address of the Prime Network gateway.

Step 3 Click **OK**.

If any client updates are available, Prime Network automatically installs them.

When you launch Prime Network Vision, messages are displayed if the server and client have different versions of the application that launches the client. For more information about these messages, see the *Cisco Prime Network 3.9 Installation Guide*.

The Prime Network Vision window appears empty when it is opened for the first time. You can create a new map or open a map that has been previously saved; see Chapter 4, "Working with Prime Network Vision Maps," for information on network maps. You can also open inventory tabs such as the Network Elements tab, which provides the available network element inventory. For more information on inventory tabs, see Prime Network Vision Inventory Tabs, page 2-5.

After logging into Prime Network Vision and launching the application, you can customize the Prime Network Vision settings. For example, you can:

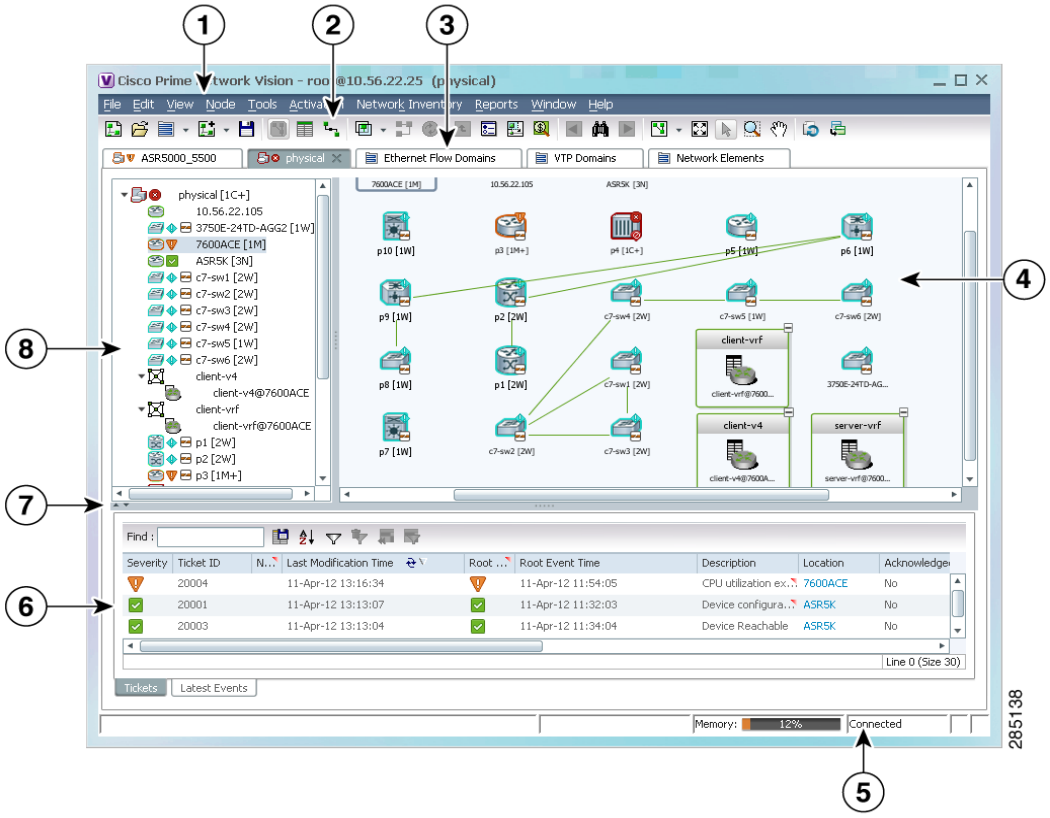
- Load the content pane with information when starting Prime Network Vision.
- Display network elements in the Prime Network Vision content pane and navigation pane.
- Configure audio responses when different alarms are triggered.
- Specify the length of time that events should be displayed in the inventory window.

For more information on customizing Prime Network Vision startup and display options, see Selecting Prime Network Vision Options, page 2-47.

Prime Network Vision Window

Figure 2-1 displays the Prime Network Vision window with an open map.

Figure 2-1 Prime Network Vision Window



1	Menu bar	**5**	Status bar
2	Toolbar	**6**	Ticket pane
3	Inventory and map tabs	**7**	Hide/display ticket pane
4	Content pane (showing the map view)	**8**	Navigation pane

The Prime Network Vision window can display either inventory tabs or maps. For more information, see the following topics:

- Prime Network Vision Inventory Tabs, page 2-5
- Prime Network Vision Maps, page 2-7

The Prime Network Vision window enables you to:

- View network element inventory.
- View maps.
- Display network element properties.
- Link to element physical and logical inventory information.
- View complete or filtered lists of links in a map and link status.
- View link properties.
- View and manage tickets.

Tip The ticket pane can be displayed or hidden by clicking the arrows below the navigation pane (see Callout 7 in Figure 2-1).

The status bar at the bottom of the window provides information about the current connection status for the view. The status bar also displays information about the command that was sent while the application waits for an answer.

The memory utilization bar in the status bar displays the amount of memory used by the client. By default, if memory utilization exceeds 60%, it is colored yellow, and if it exceeds 80%, it is colored red.

Dragging the borders of the Prime Network Vision window adjusts the size of each pane. The navigation pane and content pane are correlated; this means that selecting an option in the navigation pane affects the information displayed in the content pane.

Prime Network Vision Inventory Tabs

The Prime Network Vision interface includes inventory tabs that enable you to access many Prime Network Vision features and functions without opening a map. For example, by opening the Network Elements inventory tab, you can:

- View the available network element inventory, including an element's:
  - VNE communication and investigation states.
  - Severity status and whether any tickets that are not cleared or acknowledged are associated with the element.
  - Logical or physical inventory.
  - Tickets and events, with the ability to clear, acknowledge, or clear and remove tickets.
- Identify and open maps that contain a selected element.
- Search and filter the network element inventory for elements that meet your specific criteria.

Prime Network Vision includes the following inventory tabs:

- Network Elements—Lists all network elements with the information described in Table 2-8, Network Element Information Displayed in List View, and the following two columns:
  - Severity—Displays an icon that indicates the highest severity ticket associated with the element.
  - Unacknowledged—Displays a severity icon that indicates the severity of the highest severity ticket associated with the element that is not acknowledged.

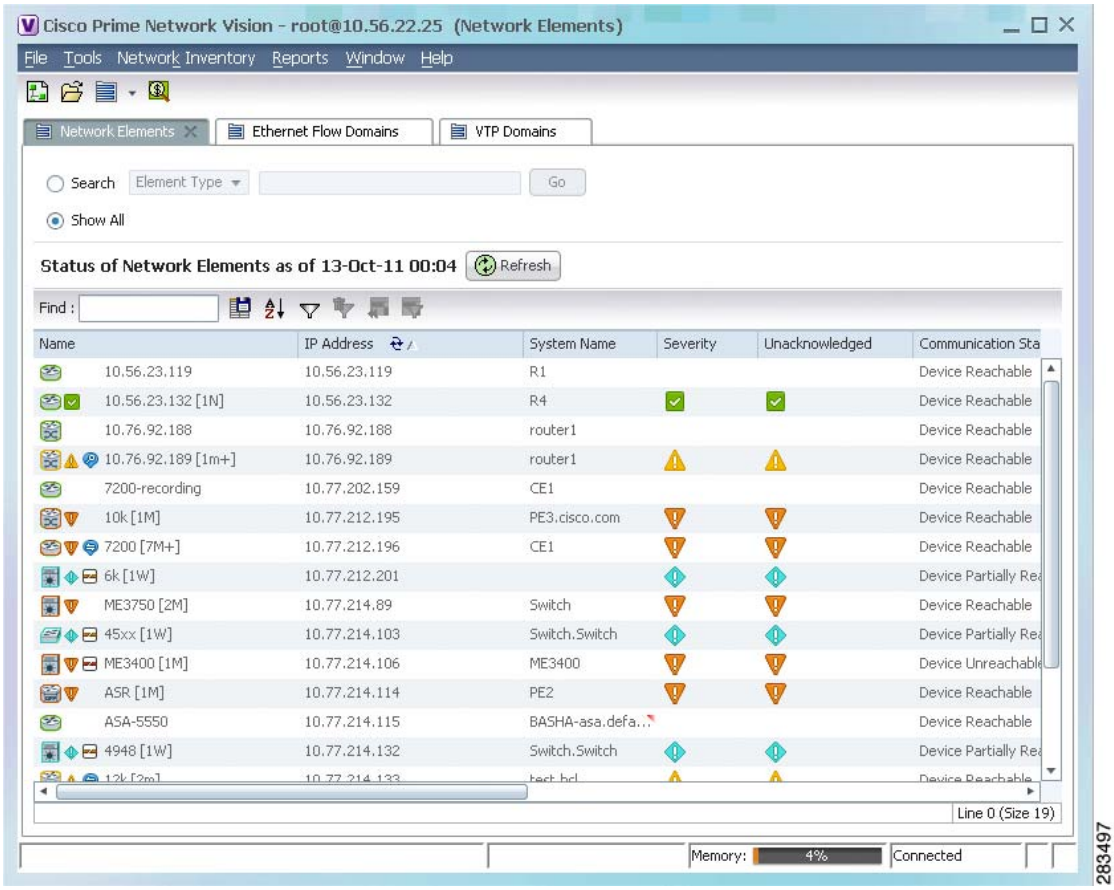
- Ethernet Flow Domains—Lists all Ethernet flow domains, including the domain name, the system-defined domain name, and a brief description for each domain. For more information about Ethernet flow domains, see Viewing and Renaming Ethernet Flow Domains, page 12-39.
- VTP Domains—Lists all VTP domains. For more information about VTP domains, see Viewing VLAN Trunk Group Properties, page 12-65.

Opening Inventory Tabs

To open an inventory tab, either click the **Network Elements** icon in the toolbar or choose **Network Elements** in the menu bar, and choose the required option.

The selected inventory table is displayed as shown in Figure 2-2.

Figure 2-2 Prime Network Vision Inventory Tabs



The inventory tabs display the network inventory icon and name. If a tab is selected, it also displays an X for closing the tab. To close a tab that is not selected, place your cursor over that tab and click the X once it appears.

Working with Inventory Tabs

Table 2-2 describes the functions that are available for working with inventory tabs.

Table 2-2 Working with Inventory Tabs

Function	Description
Filter	Click **Filter** in the table toolbar and specify filter criteria. For more information, see Filtering Table Contents, page 2-53.
Scroll	If the number of entries exceeds the current viewing area, use your mouse scroll wheel to move up and down through the table.
Search	This option is available only for the Network Elements tab. To search for specific elements: 1. Click **Search**. 2. In the drop-down list, select the category to search. 3. In the search field, enter the string to search for. 4. Click **Go**.
Sort	To sort: • By a single column, click the column heading. Click the heading again to sort in the reverse order. • Using multiple sort criteria, click **Sort Table Values** in the toolbar and select the required criteria. For more information, see Sorting a Table, page 2-51.

Prime Network Vision Maps

Prime Network Vision enables you to visualize networks through network and service maps. These maps provide access to element physical and logical inventories, connectivity, and the current network and service states.

You can create as many maps as required to represent the network views you need. For example, maps can include specific network segments, customer networks, or the particular network elements and services that you require.

Each map is displayed in a tab that contains the following panes (as shown in Figure 2-1):

- Navigation pane—Tree-and-branch representation of the network elements and aggregations in the current map. For more information, see Navigation Pane, page 2-9.
- Content pane—Representation of map elements and links in a map (topological layout) or in list format. For more information, see Content Pane: Map, List, and Links Views, page 2-10.
- Ticket pane—Tickets associated with elements currently displayed in the map and ticket status. For more information, see Ticket Pane, page 2-24.

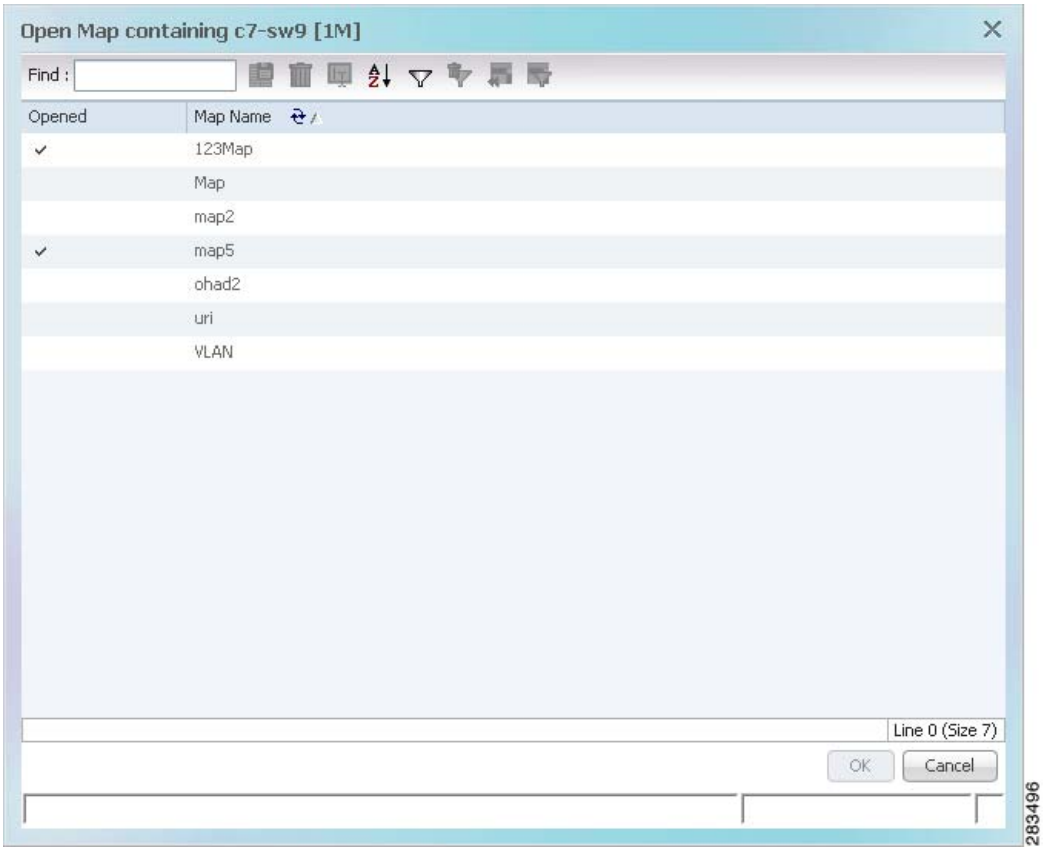
Opening Maps

You can open an existing map in any of the following ways:

- In the menu bar, choose **File > Open Map**.
- In the toolbar, click **Open Map**.
- In the Network Elements tab, right-click the required element and choose **Open Relevant Maps**.
- In either the navigation pane or content pane, right-click the required element and choose **Open Relevant Maps**.

The Open Map dialog box is displayed (see Figure 2-3).

Figure 2-3 Open Map Dialog Box



Depending on the method you use to open this dialog box, the Open Map dialog box lists either all maps or only those maps that contain the selected network element.

A check mark in the Opened column indicates that the map is already open.

Select the required maps and click **OK**.

Map tabs display the root node icon and name.

In addition, the icon color reflects the highest severity ticket that is not cleared in the map, and an alarm icon indicates the severity of the highest severity ticket that is not acknowledged. If a tab is selected, it also displays an X for closing the tab. To close a tab that is not selected, place your cursor over that tab and click the X once it appears.

For more information about maps, see Working with Prime Network Vision Maps, page 4-1.

Working with Multiple Tabs

Prime Network Vision enables you to open up to eight tabs at a time:

- One each of the three inventory tabs
- Up to five maps, each with their own tab

The following features can help you navigate multiple tabs more quickly:

- Use the following keyboard shortcuts to move between tabs:
  - **Ctrl+Tab**—Moves to the next tab to the right.
  - **Ctrl+Shift+Tab**—Moves to the next tab to the left.
- If a name is cropped in a tab, hover your cursor over the tab to view a tooltip with the complete name.
- If the number of tabs exceeds the window width, use the scroll arrows to the right of the tabs to move through the tabs.
- To view all tabs that are open and optionally select one, click **Window** in the menu bar and choose the required tab.

Navigation Pane

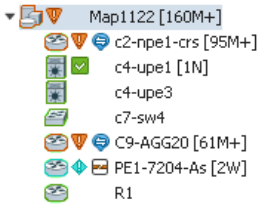
The navigation pane displays a tree-and-branch representation of the network elements and aggregations defined for the loaded map.

The highest level in the navigation tree displays root node icon with the map name. When the map name is changed, the Prime Network Vision window is updated, and the new map name is displayed at the top of the navigation tree and in the window title bar.

The lowest level of the navigation tree displays a single network element or service, such as a port, Ethernet flow point, or bridge.

The navigation pane can include up to two icons for each element. These icons can include alarm icons, communication or investigation state icons, and badges, as shown in Figure 2-4. Alarm icons are always displayed next to the element icon.

Figure 2-4 Navigation Pane with Icons



For information about the status of network objects, see Prime Network Vision Status Indicators, page 2-24.

Content Pane: Map, List, and Links Views

The content pane enables you to view and modify low-level information. It supports the following views:

- Map view—Displays managed network elements on a geographical map. For more information, see Map View, page 2-10.
- List view—Displays the details of the network elements contained in the currently selected hierarchy or subnetwork (map), such as the IP address and system name. For more information, see List View, page 2-18.
- Links view—Displays a complete list of the links in the map view and their status. For more information, see Links View, page 2-22.

When you switch between the map, list, and links views, the following are preserved:

- The currently selected network elements or links.
- The sorting preferences.
- The filtering preferences, as defined using:
  - The Link Filter dialog box—See Filtering Links in a Map, page 4-38.
  - The Filter dialog box—See Filtering Table Contents, page 2-53.
  - The links view collection method—See Filtering Links Using the Collection Method, page 5-18.

Map View

Click **Show Map View** on the toolbar to display the map view in the Prime Network Vision window.

In the map view, Prime Network Vision displays:

- Aggregations
- Managed network elements
  - Each network element is displayed as an icon, the color of which reflects severity, as described in Alarm Indicators, page 2-17.
  - Depending on the size of the icon, additional information can be displayed. For more information, see Information Available in Element Icons, page 3-3.
- Ethernet flow point cross-connects
- Ethernet services
- MPLS-TP tunnels
- Pseudowires
- VLANs
- VPLS instances
- VPNs
- Links
  - Service and business links are represented as well as physical and topological links.
  - Unidirectional links include arrowheads that indicate the direction of the flow, while bidirectional links do not have arrowheads.
- Relationships between network elements, aggregations, and networks

The map view enables you to view network objects down to the device level. An example of the map view is displayed in Figure 2-1.

You can move network elements manually on the map by dragging the required icon. You can also click **Layout Map** in the toolbar or use your mouse to change the way the elements are displayed on the map. For more information about working with maps, see Chapter 4, "Working with Prime Network Vision Maps."

Element Icons

Prime Network Vision enables you to:

- Zoom in and out on maps with your mouse.
- Apply one of four icon sizes to icons.
- View more or less information about the element in the icon, depending on the icon size.
- Access common functions from the icons, such as attaching business tags or viewing properties.

Table 2-3 provides examples of the four icons sizes and describes the information that is available with each.

Table 2-3 Prime Network Vision Element Icon Sizes

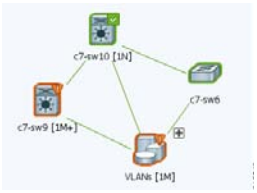
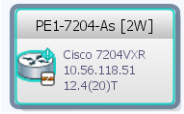
Example Icon	Name and Description
	Tiny • Displays the element as a dot. • Alarm severities are indicated by dot and link colors.
	Normal • Displays the element as an icon with the element name below the icon. • Alarm severities are indicated by badge, element icon outline, and link colors.

Table 2-3 Prime Network Vision Element Icon Sizes (continued)

Example Icon	Name and Description
	Large • Displays the element as a card with: – Element name in the title bar – Up to three additional properties • Alarm severities are indicated by card outline, element icon outline, and badge colors. • Property text can be selected for cut-and-paste operations by pressing and dragging the mouse scroll wheel over the text.
	Huge • Displays the element as a card with: – Element name in the title bar – Up to four additional properties – Up to four action buttons • Alarm severities are indicated by card outline, element icon outline, and badge colors. • Property text can be selected for cut-and-paste operations by pressing and dragging the mouse scroll wheel over the text.

For more information about using these features, see:

- Resizing Map Elements, page 4-14
- Information Available in Element Icons, page 3-3

Prime Network Vision also provides additional features for working with aggregations. For more information, see Working with Aggregations, page 4-28.

The following tables identify some of the icons used to represent network elements and business elements in the Prime Network Vision window's navigation pane and content pane:

- Table 2-4, Prime Network Vision Network Element Icons
- Table 2-5, Prime Network Vision Business Element Icons

For a complete list of the icons and their descriptions, see Appendix A, "Icon and Button Reference."

Table 2-4 Prime Network Vision Network Element Icons

Icon	Network Element
	Access pseudowire Router
	ATM switch
	Basic rate access (BRA)
	Cisco 7600 series router
	Cisco ASR 1000 series router
	Cisco ASR 5000 series router
	Cisco ASR 9000 series router
	Cisco CRS series router
	Cisco MWR 3941
	Cisco Nexus 1000 series devices
	Cisco IOS XR 12000 series router
	Cisco Unified Computing System (UCS)
	Cloud
	Digital subscriber line access multiplexer (DSLAM)

Table 2-4 Prime Network Vision Network Element Icons (continued)

Icon	Network Element
	Ethernet switch
	Generic SNMP device
	Ghost, or unknown device
	ICMP device
	Lock, or security violation; viewable by a user with a higher permission level
	Missing icon, displayed in either of the following situations: • A device has been deleted via Cisco Prime Network Administration, but remains in the map. • A unique icon for an element (physical or logical) does not exist.
	Sun Netra server
	Service control switch
	WiFi element

Note When Prime Network Vision detects a network element for which it does not have enough information available, Prime Network Vision displays as a ghost element on the map. When this occurs, you cannot view the ghost element properties or communicate with it. When the information for the ghost element becomes available, Prime Network Vision replaces its icon with the relevant element icon, and updates the related element and communication information.

Table 2-5 Prime Network Vision Business Element Icons

Icon	Business Element
	Aggregation or root node
	Backup pseudowire edge

Table 2-5 Prime Network Vision Business Element Icons (continued)

Icon	Business Element
	Connection termination point (TP) Ethernet flow point (EFP) MToP service
	EFP cross-connect
	Ethernet service
	Ethernet virtual connection (EVC)
	Label-Switched Path (LSP) end point
	LSP mid point
	Missing icon, displayed in either of the following situations: • A device has been deleted via Cisco Prime Network Administration, but remains in the map. • A unique icon for an element (physical or logical) does not exist.
	Network LSP Protected LSP Working LSP
	Network pseudowire
	Network Traffic Profile (TP) tunnel
	Network VLAN
	Pseudowire edge
	Pseudowire switching entity

Table 2-5 Prime Network Vision Business Element Icons (continued)

Icon	Business Element
	Subnet
	Switching entity
	TP tunnel endpoint
	VPLS forward
	VPLS instance
	VPN

Links

Prime Network Vision maps contain *graphical links* that can represent multiple physical, topological, service, and business links.

The maximum number of graphical links that can be displayed is specified in the registry. If the number of graphical links exceeds the specified limit, a warning message with a Refresh button is displayed, and the map is surrounded by a red border. The presence of a red border around a map indicates that some links exist that are not displayed in the map.

Note Changes to the registry should only be carried out with the support of Cisco. For details, contact your Cisco account representative.

To reduce the number of graphical links in a map:

Step 1 Remove the links in any of the following ways:

- Use the links view:

  a. Click **Show Links View** in the toolbar. The links view includes all links, even if the number of links exceeds the number of graphical links that can be displayed in a map.

  b. Filter the links so that the map contains only the required links. For more information on filtering links, see Filtering Links in an Existing Map, page 4-40.

- Click **Link Filter** in the toolbar, uncheck the check boxes for the links you do not need to view, and click **OK**.

  Only the links selected appear in the map and the Link Filter icon in the toolbar changes to indicate that a link filter is applied.

- Right-click linked devices and choose **Remove from Map**.

Step 2 After you remove the links, click **Refresh** to refresh the map contents and to see if the red border has been removed, indicating that all links are displayed in the map.

Links in maps have tooltips that provide you with information regarding the link endpoints and the number of links represented by the selected link in the map. Click the link tooltip to view additional information about the link in a link *quick view* window. Click **Properties** in the link quick view window to open the link properties window. For more information about viewing link properties, see Viewing Link Properties in Prime Network Vision Maps, page 5-4.

Note If you apply a link filter to the map, the link tooltip displays only the relevant links.

Alarm Indicators

Table 2-6 shows the colors that are used to display the severity (or propagated severity) of a network element in the navigation, content, and ticket panes.

Table 2-6 Severity Indicators

Icon	Color	Severity
	Red	Critical
	Orange	Major
	Yellow	Minor
	Light Blue	Warning
	Green	Cleared, Normal, or OK

Table 2-6 Severity Indicators (continued)

Icon	Color	Severity
	Medium Blue	Information
	Dark blue	Indeterminate

The same coloring conventions apply to the link severities displayed in the map view, links view, and link quick view.

Note The color of a selected link can be customized. The default color is blue.

When you select an aggregation in the navigation tree, you can view the elements that belong to that aggregation in the map pane by either double-clicking its icon or clicking the plus sign in the upper right corner of its icon.

For more information about how the status of a network element is displayed in a map, see Prime Network Vision Status Indicators, page 2-24.

Right-Click Functions

Many functions can be performed by using the right-click menu in the map view, including launching external applications or tools. Some of these functions are also available in the navigation pane, links view, and ticket pane.

The specific options that are available in the right-click menu depend on whether you select a network element, click in the map background, select an aggregation, or select a ticket in the ticket pane. For details on the specific right-click options that are available for each scenario, see Prime Network Vision Right-Click Menus, page 2-37.

List View

Click **Show List View** in the toolbar to display the Prime Network Vision list view. The list view displays the tabs described in Table 2-7, depending on the items included in the current map and the item selected in the navigation tree.

Table 2-7 Prime Network Vision List View Tabs

Tab	Description
Aggregations	Aggregations in the current map.
Connection TP	Connection termination points (TPs) in the current map.
EFP Cross-Connect	EFP cross-connects in the current map.
Ethernet Flow Points	EFPs in the current map.
Ethernet Services	Ethernet services in the current map.
EVCs	EVCs in the current map.
Network Elements	Network elements in the current map that are in the user's scope.
Network Pseudowire	Network pseudowires in the current map.

Table 2-7 Prime Network Vision List View Tabs (continued)

Tab	Description
Network TP Tunnel	Network Traffic Profile (TP) tunnels in the current map.
Pseudowires	Pseudowires in the current map.
Pseudowire Edge	Pseudowire endpoints in the current map.
PW Switching Entity	Pseudowire switching entities in the current map.
Restricted Elements	Network elements in the current map that are not in the user's scope.
Sites	Sites for the selected VLAN. Site properties include site name, description, location, and IP interface.
Switching Entities	Switching entities in the current map.
Virtual Routers	Virtual routers on the selected VLAN. Virtual router properties include the virtual router name and description.
VLANs	VLANs in the current map. VLAN properties include VLAN name, identifier, description, and Ethernet flow points.
VPLS Forward	VPLS forwards in the current map.
VPLS Instance	VPLS instances in the current map.
VPNs	VPNs in the current map. VPN properties include VPN name and description

Table 2-8 describes the network element properties displayed in the Network Elements tab. (Locked network elements display only managed element information and the locked element icon.) To ensure that you are viewing the latest information, either perform a new search or click the Refresh button.

Table 2-8 Network Element Information Displayed in List View

Field Name	Description
Name	Name of the network element managed by Cisco, as defined in Cisco Prime Network Administration. The Name property also displays a network element icon. The icon color reflects the highest network element alarm severity. In addition, the management state or an alarm icon is displayed.
IP Address	IP address used for managing the network element.
System Name	System name of the network element, as defined in the network element's MIB. If the network element is configured for Telnet access, the prompt is displayed.
Severity	Current operational health of the network element.
Unacknowledged	Severity of the most severe unacknowledged ticket.
Communication State	Ability of the VNE to reach the network element, according to the health of the element. For more information about communication states, see the *Cisco Prime Network 3.9 Administrator Guide*.
Investigation State	Level of network element discovery that has been performed or is being performed by the VNE. For more information about investigation states, see the *Cisco Prime Network 3.9 Administrator Guide.*
Vendor	Vendor name.
Product	Network element category, such as Router or Eth-Switch (Ethernet switch).

Table 2-8 Network Element Information Displayed in List View (continued)

Field Name	Description
Device Series	Device series, such as Cisco 7600 Series Routers.
Element Type	Network element type including the manufacturer's name, such as Cisco 7200.
Software Version	Cisco IOS software version running on the network element.
Location	Location of the network element.
Up Since	Date and time the network element was last reset.

Tip Click the red triangle in a cell to expand the cell and view all the information it contains. You can also use a tooltip to view all the information.

Table 2-9 identifies the buttons that are displayed in the list view toolbar.

Table 2-9 List View Toolbar

Icon	Name	Description
	Find	Searches the table for the string you enter. For more information, see Finding Text in a Table, page 2-51.
	Export to CSV	Exports the information displayed in the table, or selected portions, to a CSV file. For more information, see Exporting Tables to a File, page 2-55
	Sort Table Values	Sorts the information displayed in the table by the criteria you specify. For more information, see Sorting a Table, page 2-51.
	Filter	Filters the information displayed in the table by the criteria you specify. For more information, see Filtering Table Contents, page 2-53.
	Clear Filter	Clears the existing filter.
	Show All Rows	Displays all table rows that meet the current filtering criteria.
	Show Only Selected Rows	Displays only the rows that you select. For more information, see Viewing Selected Rows, page 2-54.

See Working with Prime Network Tables, page 2-49 for more information about filtering, finding details about a network element in Prime Network Vision tables, and keyboard shortcuts available for accessing table functionality.

Table 2-10 describes some of the functions that are available from the right-click menu in the list view. You must select an item for the right-click menu to appear. Not all options are available for all selections.

Table 2-10 List View Right-Click Options

Right-Click Option	Function	Related Documentation
Inventory	View network element inventory	Opening the Inventory Window, page 3-12
Poll Now	Poll the selected element	
Attach / Detach / Edit Business Tag	Configure and view business tag information	Chapter 6, "Working with Business Tags and Business Elements"
Config Mgmnt	View the Configuration Management page in Prime Network Change and Configuration Management	*Cisco Prime Network 3.9 Change and Configuration Management User and Administration Guide*
Image Mgmnt	View the Image Management page in Prime Network Change and Configuration Management	*Cisco Prime Network 3.9 Change and Configuration Management User and Administration Guide*
Run Report	Generate reports	Chapter 10, "Working with Reports"
Show Only Selected Rows / Show All Rows	View selected rows or all rows	Viewing Selected Rows, page 2-54
Tools	Ping or telnet a VNE, or check VNE CPU usage	List View Right-Click Menu, page 2-43
Topology	Configure the topology	Adding Static Links, page 5-15
Properties	View network element properties	Viewing the Properties of a Network Element, page 3-5
Commands	Launch any of the commands that are included with Prime Network Vision	*Cisco Prime Network 3.9 Reference Guide*
Management	Access Command Builder and Soft Properties Management	*Cisco Prime Network 3.9 Customization User Guide*
VNE Tools	Poll a VNE, or start or stop a VNE	Updating VNE Information, page 3-12

Tip Click a column heading in a table to sort the information by that property.

Links View

Click **Show Links View** in the toolbar to display the links view in the Prime Network Vision window.

Maps can contain many graphical links, each of which can represent multiple physical, topological, service, and business links. This can make it difficult for you to view the links you are interested in. In addition, if the number of graphical links exceeds the number that can be displayed in a map, not all links are displayed. By using the links view, you can view all links in the map, as well as search for a specific link and view the status of a link.

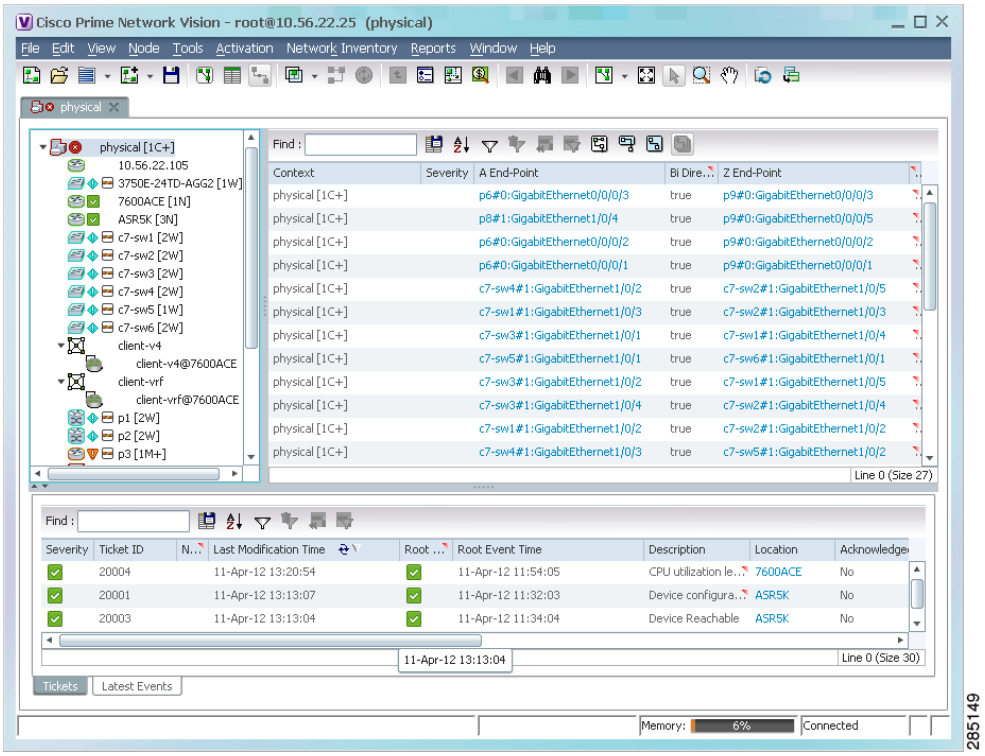
Note You can view and filter the links according to type by using the Link Filter dialog box. For more information, see Filtering Links in a Map, page 4-38.

Any links that are added or removed from the map are automatically added or removed from the links view, provided they have not been filtered out.

The links view is selection sensitive; that is, the links displayed in the links view depend on the context selected in the navigation pane or map. For example, if an aggregation is selected, the links in the selected aggregation are displayed in the links view.

Figure 2-5 shows a links view.

Figure 2-5 Links View



Note An external link has a blue cell background in the table, and you can open the inventory window by clicking the hyperlink. For more information about external links, see Viewing Link Properties in the Links View, page 5-8.

Table 2-11 describes the information that is displayed in the links view.

Table 2-11 Information Displayed in the Links View

Field Name	Description
Context	Name of the map or aggregation containing the link. This field can be empty for either of the following reasons: • One side of the link is not included in the map. • The link is filtered out of all contexts.
Severity	Link alarm severity, represented by an icon. The icon and its color indicate the alarm severity and thereby the impact of the alarm on the network. For more information about severity, see Map View, page 2-10.
A End-Point	Element or site that is the source of the link as a hyperlink to the inventory of the element or site.
Bi Directional	Whether the link is bidirectional or unidirectional: true (bidirectional) or false (unidirectional). If the link is unidirectional (false), the traffic is from A to Z.
Z End-Point	Element or site that is the destination of the link as a hyperlink to the inventory of the element or site.
Link Type	Type of link, such as Physical Layer, LAG, MPLS TE Tunnel, pseudowire (PW) or VPN.

Note Clicking a column heading in the links view sorts the information by that header value.

The links view toolbar includes the tools described in Table 2-9 and the link filtering buttons described in Table 2-12.

Table 2-12 Link Filtering Buttons

Button	Name	Description
	All Links	Displays the complete list of links for the selected context (map or aggregation). In other words, the list is not filtered and all the links are displayed, including external links.
	External Links	Displays links with only one side of the link in this context (map or aggregation) and the other side either not in the map or outside the selected context.
	Flat Links	Displays the links currently visible on the map for the selected context (map or aggregation), excluding any thumbnails.
	Deep Links	Displays the links for the current aggregation where both endpoints are within the currently selected context.

For more information about filtering and sorting links in the links view, see Viewing Link Properties in the Links View, page 5-8.

For information about the right-click options available in the links view, see Links View Right-Click Menu, page 2-45.

Ticket Pane

The ticket pane shows the tickets that relate to the elements in the displayed map. It also contains the Latest Events tab that shows the latest incoming events for the elements in the map from the time the map was opened. See Chapter 9, "Working with Tickets in Cisco Prime Network Vision" for more information.

Prime Network Vision Status Indicators

The following topics describe the ways in which the status of an element is displayed in Prime Network Vision:

- Severity, page 2-24
- VNE Management State, page 2-25
- Tickets, page 2-29

Severity

Severity indicates the operational health of the element. An element has only one severity value at any given time, and this value is displayed using a severity color. For more information about the colors used to display the severity (or propagated severity) of network elements and links, see Alarm Indicators, page 2-17.

Propagation

Severity is propagated upward in the network hierarchy, displaying the top-most severity of the network element's children and thereby ensuring that every single problem in the network is propagated and visible.

The same severity propagation rules that are used for network elements apply to links. A link is a child object of an aggregation *only* if it is fully contained in the aggregation; that is, the network elements on both sides of the link are part of the aggregation, as shown in Figure 2-6 and Figure 2-7.

Figure 2-6 Link Severity Example 1

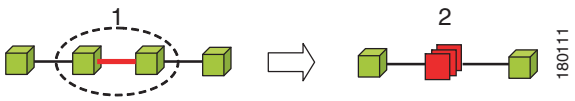


Figure 2-6 shows critical link 1 between two network elements in an aggregation. This critical link affects the severity of aggregation 2. That is, the aggregation is critical because it contains a link with a critical severity. Link severity affects the context.

Figure 2-7 Link Severity Example 2

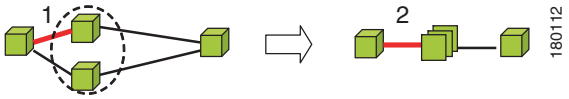


Figure 2-7 shows critical link 1 that forms part of a link aggregation. This affects the severity of link 2 because it contains a link with a critical severity.

New Ticket Propagation

A new ticket indicates a new local fault or accumulates and propagates the number of new faults in its children. New tickets are propagated upward, displaying the number of new tickets and the top-most severity.

When new tickets are accumulated, a label is displayed in the navigation pane and map, based on the following formula:

n s [+]

where:

Symbol	Description
n	The number of tickets with the highest severity in the new ticket count.
s	The highest severity level in the new tickets: • C = Critical • M = Major • m = Minor • W = Warning • N = Normal (cleared alarm) • i = Informational
+	Additional, less severe tickets (optional) exist.

For example:

- An object with three critical new alarms, two major alarms, and one warning alarm is labeled 3C+.
- An object with five minor new alarms is labeled 5m.

An icon represents unacknowledged tickets, and the icon color is that of the most severe, unacknowledged ticket. For more information about severity colors and icons, see Alarm Indicators, page 2-17.

If all relevant tickets are acknowledged, no bell is displayed.

VNE Management State

The management state indicates the state or mode of the software component (a VNE) managing a network element and the communication with it. This enables you to determine the accuracy of the network information and the availability of VNEs to carry out network operations.

Management states are always local indications and are not propagated. A partial exception to this rule is the propagation of unreachable VNEs.

The management state indication applies only to VNE and its components. A VNE can have only one state at a time (for example, Unsupported or Connecting).

A managed VNE icon consists of a managed element icon and one or two overlay icons, or *badges*:

- The managed element icon displays a symbol of the element, and the color of the symbol indicates the highest severity ticket that is *not cleared* for the element.

  An element icon is colored green if either of the following is true:

  – No ticket of any severity exists for the element.

  – All tickets that exist for the element have the severity Cleared or Informational.

  For more information about network element icons, see Element Icons, page 2-11. For more information about severity colors, see Alarm Indicators, page 2-17.

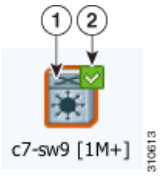
- An alarm badge is displayed on top of a managed element icon, and the color of the alarm badge indicates the severity of the highest severity ticket that is *not acknowledged* for the element. If all tickets are acknowledged, no alarm icon appears.

  Figure 2-8 shows an example of an element with the following ticket and alarm severities:

  – The highest severity ticket that is not cleared for the element is Major, as indicated by the orange color applied to the element icon.

  – The highest severity alarm that is not acknowledged for the element is Cleared or OK, as indicated by the green alarm badge.

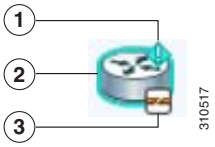
Figure 2-8 Element with Ticket and Alarm Severity Indicators



1	Element icon with severity Major (orange)
2	Alarm badge with severity Cleared or OK (green)

- A VNE management state badge is displayed on top of the managed element icon to indicate the management state of the VNE in the navigation tree and map. For example, a router that is partially reachable by Prime Network Vision is displayed as illustrated in Figure 2-9.

Figure 2-9 Element with Overlay Badges



1	Alarm badge with severity Warning.
2	Managed element icon with severity Warning.
3	VNE management state badge of Device Partially Reachable.

Table 2-13 and Table 2-14 describe network element communication and investigation states and shows the related badge for each state.

Table 2-13 VNE Communication States

State Name	Description	Badge
Agent Not Loaded	The VNE is not responding to the gateway because it was stopped, or it was just created. This communication state is the equivalent of the Defined Not Started investigation state.	None
VNE/Agent Unreachable	The VNE is not responding to the gateway. This can happen if the unit or AVM is overutilized, the connection between the gateway and unit or AVM was lost, or the VNE is not responding in a timely fashion. (A VNE in this state does not mean the device is down; it might still be processing network traffic.)	
Connecting	The VNE is starting and the initial connection has not yet been made to the device. This is a momentary state. Because the investigation state decorator (the hourglass) will already be displayed, a special GUI decorator is not required.	None
Device Partially Reachable	The VNE is not fully reachable because at least one protocol is not operational. **Note** This is the default behavior. You can change the settings that determine when Cisco Prime Network moves a VNE to Device Unreachable. For more information, see the *Cisco Prime Network 3.9 Administrator Guide*.	
Device Unreachable	The connection between the VNE and the device is down because all of the protocols are down (though the device might be sending traps or syslogs). **Note** This is the default behavior. You can change the settings that determine when Cisco Prime Network moves a VNE to Device Unreachable. For more information, see the *Cisco Prime Network 3.9 Administrator Guide*.	
Tracking Disabled	The reachability detection process is not enabled for any of the protocols used by the VNE. The VNE will not perform reachability tests nor will Cisco Prime Network generate reachability-related events. In some cases this is desirable; for example, tracking for Cloud VNEs should be disabled because Cloud VNEs represent unmanaged network segments. Because this is a user-defined mode (rather than an error or transitional mode), Cisco Prime Network does not display a decorator for this state. To troubleshoot a VNE that is in this state, see the *Cisco Prime Network 3.9 Administrator Guide*.	None

Table 2-14 VNE Investigation States

State Name	Description	Badge
Defined Not Started	A new VNE was created (and is starting); or an existing VNE was stopped. In this state, the VNE is managed and is validating support for the device type. (This investigation state is the equivalent of the Agent Not Loaded communication state.) A VNE remains in this state until it is started (or restarted).	None
Unsupported	The device type is either not supported by Prime Network or is misconfigured (it is using the wrong scheme, or is using reduced polling but the device does not support it). To extend Cisco Prime Network functionality so that it recognizes unsupported devices, use the VNE Customization Builder. See the *Cisco Prime Network 3.9 Customization User Guide*.	

Table 2-14 VNE Investigation States (continued)

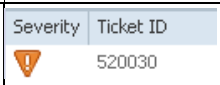
State Name	Description	Badge
Discovering	The VNE is building the model of the device (the device type was found and is supported by Cisco Prime Network). A VNE remains in this state until all device commands are successfully executed at least once, or until there is a discovery timeout.	
Operational	The VNE has a stable model of the device. Modeling may not be fully complete, but there is enough information to monitor the device and make its data available to other applications, such as activation scripts. A VNE remains in this state unless it is stopped or moved to the maintenance state, or there are device errors.	None
Currently Unsynchronized	The VNE model is inconsistent with the device. This can be due to a variety of reasons; for a list of these reasons along with troubleshooting tips, see the topic on troubleshooting VNE investigation state issues in the *Cisco Prime Network 3.9 Administrator Guide*.	
Maintenance	VNE polling was suspended because it was manually moved to this state (by right-clicking the VNE and choosing **Actions > Maintenance**). The VNE remains in this state until it is manually restarted. A VNE in the maintenance state has the following characteristics: • Does not poll the device, but handles syslogs and traps. • Maintains the status of any existing links. • Does not fail on VNE reachability requests. • Handles events for correlation flow issues. It does not initiate new service alarms, but does receive events from adjacent VNEs, such as in the case of a Link Down alarm. The VNE is moved to the Stopped state if: it is VNE is moved, the parent AVM is moved or restarted, the parent unit switches to a standby unit, or the gateway is restarted.	
Partially Discovered	The VNE model is inconsistent with the device because a required device command failed, even after repeated retries. A common cause of this state is that the device contains an unsupported module. To extend Cisco Prime Network functionality so that it recognizes unsupported modules, use the VNE Customization Builder. See the *Cisco Prime Network 3.9 Customization User Guide*.	
Shutting Down	The VNE has been stopped or deleted by the user, and the VNE is terminating its connection to the device.	
Stopped	The VNE process has terminated; it will immediately move to Defined Not Started.	None

More than one management state can occur at the same time. For example, a single overlay icon can be displayed, reflecting the device status based on the following priorities: Unsupported > Discovering > VNE/Agent Unreachable > Device Unreachable > Partially Discovered > Operational.

For more information about each of these states and how to troubleshoot any issues, see the *Cisco Prime Network 3.9 Administrator Guide.*

Tickets

Cisco Prime Network Vision displays an icon with a ticket to indicate the severity of the top-most alarm on the ticket. The icons are the same as those used with network elements (see Table 2-6) and are displayed in Cisco Prime Network Vision as follows:

Value	Navigation Pane	Map	Ticket Pane
Element with ticket of Major severity			

Prime Network Vision Toolbar

The Prime Network Vision toolbar is context-sensitive and the options vary depending on your selection in the application.

Note The functionality that a user can access in Prime Network Vision depends on the user role and the security level of the scopes assigned to the user. For more information, see User Roles Required for Working with Prime Network Vision Maps, page 4-2.

Table 2-15 identifies the toolbar buttons and describes the functions that are available in the Prime Network Vision toolbar.

Table 2-15 Prime Network Vision Toolbar

Button	Name	Function
	Open Network Inventory	Opens the Network Elements tab.
Map Options		
	New Map	Creates a new map in the database.
	Open Map	Opens a map saved in the database using the Open dialog box.
	Add to Map	Adds an element to the map or to the subnetwork selected in the navigation pane and displayed in the content pane.
	Save Map Appearance	Saves the current map (the background and the location of devices) to the database.

Table 2-15 Prime Network Vision Toolbar (continued)

Button	Name	Function
Viewing Options		
	Show Map View	Displays the map view in the Prime Network Vision content pane (the button toggles when selected or deselected).
	Show List View	Displays the list view in the Prime Network Vision content pane (the button toggles when selected or deselected).
	Show Links View	Displays the links view in the Prime Network Vision content pane (the button toggles when selected or deselected).
Overlay Tools		
	Choose Overlay Type	Chooses and displays an overlay of a specific type on top of the elements displayed in the content pane in a map view. Available overlay options are: • Ethernet Service • MPLS-TP Tunnel • Network Clock • Pseudowire • VLAN • VPLS • VPN • None—Removes the existing overlays.
	Show Overlay / Hide Overlay	Displays or hides a previously defined overlay on top of the elements displayed in the map view. **Note** Overlays do not reflect changes that occur in the selected service. As a result, the information in an overlay can become stale.
	Refresh Overlay	Refreshes the overlay that was last selected.
Viewing Tools		
	Go to Parent	Moves up one level in the navigation pane and content pane so you can view different information.
	Link Filter	Opens the Link Filter dialog box, enabling you to display or hide different types of links in the map and links views. If a link filter is applied to the map, the Link Filter Applied button is displayed instead.
	Link Filter Applied	Indicates a link filter is currently applied to the map and opens the Link Filter dialog box so you can remove or modify the existing link filter. If no link filter is applied to the map, the Link Filter button is displayed instead.

Table 2-15 Prime Network Vision Toolbar (continued)

Button	Name	Function
	Overview	Opens a window displaying an overview of the network.
	Find Business Tag	Opens the Find Business Tag dialog box, enabling you to find and delete a business tag according to name, key, or type.
Search Tools		
	Find Previous	Finds the previous instance of the search string entered in the Find in Map dialog box.
	Find	Opens the Find in Map dialog box, enabling you to find an element in the map by its name or IP address.
	Find Next	Finds the next instance of the search string entered in the Find in Map dialog box.
Map Zoom and Layout Tools		
	Layout Map	Defines the way in which the elements are arranged in the Prime Network Vision window: Circular, hierarchical, orthogonal, or symmetric.
	Fit in Window	Fits all elements in the map in the content pane.
	Normal Selection Mode	Activates the normal selection mode.
	Zoom Selection Mode	Activates the zoom selection mode, which enables you to zoom in on a section of the map by clicking and dragging the required area.
	Pan Mode	Activates the pan mode, which enables you to view different areas of the map by clicking and dragging the map.
Application-Specific Tools		
	Open Activation	Opens the Activation dialog box. For more information, see the *Cisco Prime Network 3.9 Customization User Guide.*
	Activation History	Opens the Activation History dialog box. For more information, see the *Cisco Prime Network 3.9 Customization User Guide.*

Prime Network Vision Menu Bar

The following topics describe the options that are available in each Prime Network Vision menu:

- File Menu, page 2-32
- Edit Menu, page 2-33
- View Menu, page 2-33

- Node Menu, page 2-34
- Tools Menu, page 2-35
- Activation Menu, page 2-35
- Network Inventory Menu, page 2-36
- Reports Menu, page 2-36
- Window Menu, page 2-36
- Help Menu, page 2-37

Note The functionality that a user can access in Prime Network Vision depends on the user role and the security level of the scopes assigned to the user. For more information, see User Roles Required for Working with Prime Network Vision Maps, page 4-2.

Note The menus are context-sensitive and the options vary depending on your selection in the application.

File Menu

Table 2-16 describes the options that are available in the Prime Network Vision File menu. For more information, see Chapter 4, "Working with Prime Network Vision Maps."

Table 2-16 File Menu Options

File Menu Option	Description
New Map	Creates a new empty map in the database.
Open Map	Opens a map saved in the database using the Open dialog box.
Add to Map[1]	Opens the Add dialog box and enables you to add any of the following to the map or to the subnetwork selected in the navigation pane and displayed in the content pane: • Cross Connect • Ethernet Service • MPLS-TP Tunnel • Network Element • Pseudowire • Unassociated Bridge • VLAN • VPLS • VPN
Save Map[1]	Saves the appearance of the map (the background and the location of devices) to the database.
Save As Image[1]	Saves the active map as an image and automatically displays the Save as Image dialog box. Use this dialog box to save an image using a different file format or name.

Table 2-16 File Menu Options (continued)

File Menu Option	Description
Print Preview[1]	Displays how the map will look when it is printed.
Print[1]	Prints the active map as displayed in the Print Preview dialog box.
Load MultiPath	Loads a Cisco PathTracer multiple-path trace from a file that was previously saved in Cisco PathTracer.
Close	Closes the selected map or tab.
Exit	Exits the Prime Network Vision application and saves the content pane.

1. This option is available only when a map is displayed in the content pane.

Edit Menu

Table 2-17 identifies the options available in the Prime Network Vision Edit menu. For more information, see Chapter 4, "Working with Prime Network Vision Maps."

Table 2-17 Edit Menu Options

Edit Menu Option	Description
Find in Map	Searches for a device in the map that contains the specified text in the name or the IP address fields.
Find Business Tag	Searches for business tag information in the database.
Resize	This option is displayed only when element icons or aggregations are selected. Displays the Resize dialog box, enabling you to specify the size of selected icons or aggregations in the map, either by percentage or size.
Select All	Selects all elements in the map.

View Menu

Table 2-18 identifies the options available in the Prime Network Vision View menu. For more information, see Using the Overview Window, page 4-19.

Table 2-18 View Menu Options

View Menu Option	Description
Layout	Defines the way in which the map is displayed in the Prime Network Vision content pane: Circular, hierarchical, orthogonal, or symmetric.
Overview	Opens a window displaying an overview of the network map.
Zoom In	Zooms in on the network map.
Zoom Out	Zooms out of the network map.
Fit In Window	Displays the entire network map in the content pane.
Normal Select	Activates the normal selection mode. The selected option is dimmed.

Table 2-18 View Menu Options (continued)

View Menu Option	Description
Pan	Activates the pan mode, which enables you to move around in a map by clicking and dragging. The selected option is dimmed.
Zoom Selection	Activates the zoom selection mode, which enables you to select an area in a map to zoom in on by clicking and dragging. The selected option is dimmed.

Node Menu

Table 2-19 describes the Node menu options.

Note Most of the functionality available in this menu is available only when an element icon or an aggregation is selected in the navigation pane or a map.

Table 2-19 Node Menu Options

Node Menu Option	Description
Inventory	Displays a dialog box that enables you to view the physical and logical inventory. For physical inventory, you can view all the components of the device, such as modules and ports. In addition, you can view the status of each component. For logical inventory, you can view all the profiles and virtual channels or routing tables of the device. For more information, see Chapter 3, "Viewing Network Element Properties."
Mark as A Side	Starts the process of creating a new static link. This option is enabled when a device, port, or unmanaged network is selected.
Mark as Z Side	Launches the Add Static Link dialog box, enabling you to create a static link between the two selected nodes. This option is enabled after a device, port, or unmanaged network is selected and after the Mark as A Side option is selected. **Note** If you select two ports, the Add Static Link dialog box is not displayed.
Properties	Displays a dialog box enabling you to view the properties of the selected device, such as the severity, IP address, and communication state. For more information, see Chapter 3, "Viewing Network Element Properties."

Tools Menu

Table 2-20 describes the Tools menu options.

Table 2-20 Tools Menu Options

Tools Menu Option	Description
Change User Password	Enables you to change the password used when logging into the Prime Network client application suite. The change takes effect the next time you log into the application. **Note** The administrator can also change a user password in Cisco Prime Network Administration.
Options	Enables you to customize several of Prime Network's options, such as whether or not to load the content upon startup. For more information, see Selecting Prime Network Vision Options, page 2-47.
Change and Config Mgmnt	Displays the Prime Network Change and Configuration Management dashboard. For more information, see the *Cisco Prime Network 3.9 Change and Configuration Management User and Administration Guide*.
Command Jobs	Displays all Command Builder jobs that have been scheduled and their details. For more information, see the *Cisco Prime Network 3.9 Customization User Guide.*

Activation Menu

See the *Cisco Prime Network 3.9 Customization User Guide* for more information about any of the options in this menu.

Table 2-21 describes the Activation menu options.

Table 2-21 Activation Menu Options

Activation Menu Option	Description
Activation	Opens the Activation dialog box.
Activation History	Opens the Activation History dialog box.
Activation Modification Utility	Opens the Activation Modification Utility dialog box.

Network Inventory Menu

Table 2-22 describes the Network Inventory menu options.

Table 2-22 Network Inventory Menu Options

Network Inventory Menu Option	Description
Network Elements	Displays a list of the available network elements in the Network Elements tab. For more information, see Prime Network Vision Inventory Tabs, page 2-5.
Ethernet Flow Domains	Displays a list of the current Ethernet flow domains in the Ethernet Flow Domains tab. For more information, see Viewing and Renaming Ethernet Flow Domains, page 12-39
VTP Domains	Displays a list of the current of the VLAN Trunk Protocol (VTP) domains in the VTP Domains tab. For more information, see Viewing VLAN Trunk Group Properties, page 12-65.

Reports Menu

Table 2-23 describes the Reports menu options.

Table 2-23 Reports Menu Options

Reports Menu Option	Description
Report Manager	Opens the Reports Manager window so you can create, run, and manage reports.
Run Report	Enables you to run standard or user-defined events, inventory, and network service reports on demand.

For more information about Report Manager and reports, see Chapter 10, "Working with Reports."

Window Menu

The Prime Network Vision Window menu lists all maps open in the Prime Network Vision content pane, enabling you to move between the maps. The menu also lists any network element inventory tabs that are open.

Help Menu

Table 2-24 describes the Help menu options.

Table 2-24 Help Menu Options

Help Menu Option	Description
Cisco Prime Network Vision Help	Opens the online help for Prime Network Vision and Prime Network Events.
Icon Reference	Opens a window that identifies and describes the icons and buttons used in Prime Network Vision and Prime Network Events.
Cisco.com	This option is unavailable.
About Cisco Prime Network Vision	Displays the Prime Network version and any additionally installed applications.

Prime Network Vision Right-Click Menus

If you right-click a specific area, link, network element, device, or alarm in a Prime Network Vision window, a context-sensitive right-click menu is displayed that contains options available for the selected item or items.

Right-click menus are also available in many of the inventory and property windows. For example, if you right-click an entry in a logical inventory table, you can view properties specific to that entry. The options that are available depend on the window or table currently displayed and the item selected.

The menus are context-sensitive and the options vary according to your selection in the application. For example, the right-click menus for network elements and aggregations are different.

Additional right-click options are displayed in the following situations:

- If Prime Network is installed as part of the Cisco Prime suite of applications, right-click menus in Prime Network Vision include options for accessing the other Cisco Prime applications.
- If Prime Performance Manager is installed in your environment, Prime Network Vision includes right-click options that allow you to generate device, interface, and VRF-related reports using Prime Performance Manager.
- The Prime Network Vision installation includes a number of scripts. When these scripts are installed, they are displayed as options in the right-click menus of the devices that support them. For more information about these scripts, see the Commands section of the *Cisco Prime Network 3.9 Reference Guide*.

The functionality that you can access in Prime Network Vision depends on your user role and the security level of the scopes that you can access. For more information, see User Roles Required for Working with Prime Network Vision Maps, page 4-2.

See the following topics for the default options available in Prime Network Vision right-click menus:

- Map Right-Click Menu, page 2-38
- Element Right-Click Menu, page 2-38
- Aggregation Right-Click Menu, page 2-42
- Link Right-Click Menu, page 2-42

- List View Right-Click Menu, page 2-43
- Links View Right-Click Menu, page 2-45
- Ticket Right-Click Menu, page 2-46

Map Right-Click Menu

The map right-click menu is displayed when you right-click anywhere on a map in the content pane and no elements are selected.

Table 2-25 describes the map right-click menu options.

Table 2-25 Map Right-Click Menu Options

Option	Description
Go to Parent	Moves up one level in the navigation pane and content pane to enable you to view different information.
Go to Root	Moves to the root level in the navigation pane and content pane to enable you to view different information.
Set Map Background	Displays a background image for the map in the content pane. For more information, see Applying a Background Image, page 4-17.

Element Right-Click Menu

The element right-click menu is displayed when you right-click an element in the navigation pane, the content pane, or in the Network Elements inventory tab.

Note The element right-click menu is context-sensitive and the options vary depending on your selection in the application. Also, some options might not be available if multiple elements are selected.

Table 2-26 describes the options available in the element right-click menu.

Table 2-26 Element Right-Click Menu Options

Option	Description
Add Associated VLAN	Opens the Add Associated VLAN dialog box so that you can add an associated VLAN to the selected VLAN. For more information, see Adding an Associated VLAN, page 12-52.
Aggregate	Groups the selected devices into an aggregation in the Prime Network Vision content pane, and enables you to define a name for the new aggregation. For more information, see Chapter 4, "Working with Prime Network Vision Maps." **Note** You cannot aggregate service entities that exist within services. For example, you cannot aggregate VRFs that exist in a VLAN.

Table 2-26 Element Right-Click Menu Options (continued)

Option	Description
Attach / Detach / Edit Business Tag	Allows you to perform the following actions: • Attach a business tag to the selected network element. • Detach a business tag from a network element. • Edit a business tag for a network element. **Note** The Detach and Edit options are displayed only when a business tag is attached to a network element. For more information, see Chapter 6, "Working with Business Tags and Business Elements."
Commands	Enables you to launch any of the commands that are included with Prime Network Vision. For more information on the available commands and how to implement them, see the "Using the Prime Network Basic Operation Commands" chapter in the *Cisco Prime Network 3.9 Reference Guide*.
Config Mgmnt	This option is available only if Prime Network Change and Configuration Management is installed. Displays the Configuration Management page for the selected device in Prime Network Change and Configuration Management. For more information, see the *Cisco Prime Network 3.9 Change and Configuration Management User and Administration Guide.*
Delete	Deletes the selected item from the map.
Disaggregate	Ungroups the devices in the selected aggregation in the navigation and map panes. For more information, see Chapter 4, "Working with Prime Network Vision Maps." **Note** This option is available only when an aggregation is selected in the navigation pane or map.
Edit	Move the selected virtual router to the location you specify.
Filter Tickets	Displays only those tickets that have the selected VNE as the root cause. This option is available only for VNEs that have not been deleted by Prime Network Administration.
Hide Connected Devices	Hides the devices for sites with one or more connected devices.
Image Mgmnt	This option is available only if Prime Network Change and Configuration Management is installed. Displays the Image Management page for the selected device in Prime Network Change and Configuration Management. For more information, see the *Cisco Prime Network 3.9 Change and Configuration Management User and Administration Guide.*

Table 2-26 Element Right-Click Menu Options (continued)

Option	Description
Inventory	Displays a window enabling you to view the physical and logical inventory. For physical inventory, you can view all the components of the device, such as the modules, ports, and its IP address or configured VLANs. In addition, you can view the status of each component. For logical inventory, you can view all the profiles and VC tables of the device. For more information, see Chapter 3, "Viewing Network Element Properties."
Launch external applications	Starts an external application or tool that has been configured for access via the right-click menu. For more information, see the *Cisco Prime Network 3.9 Customization User Guide.*
Management	Contains the following submenu options: • Command Builder—Defines commands and scripts using the Prime Network Command Builder tool (Configurator security level required). • Soft Properties Management—Extends VNEs by adding SNMP MIB or Telnet/SHH/TL-1 properties to the device's collected information model using the Prime Network Soft Properties Manager (Administrator security level required). For more information about Command Builder and Soft Properties Manager, see the *Cisco Prime Network 3.9 Customization User Guide.*
Modify	Displays the Modify dialog box so that you can change the selected item's name, description, or icon.
Open Relevant Maps	Displays the Open Map dialog box so that you can view and open maps that contain the selected element.
PathTracer	Launches a path trace from the selected item.
Poll Now	Polls the selected element.
Properties	Displays the properties of the selected item, such as the IP address and system name. In addition, you can open the VNE Properties dialog box and manage VNE properties. For more information, see Chapter 3, "Viewing Network Element Properties."
Remove from Map	Removes the selected device and all its children from the map (navigation pane and content pane). The device that has been removed is still maintained in the network.
Rename	Renames the selected item.
Resize	Enables you to resize an object on the map by percentage or size.
Run Report	Enables you to run standard or user-defined events, inventory, and network service reports on demand.
Save as New Map	Creates a new map and places the selected aggregation as the root, while leaving the original map intact.
Script names	Launches available activation and configuration scripts. This can include the commands documented in Commands part of the *Cisco Prime Network 3.9 Reference Guide*, and those you create using Command Builder (can be launched against multiple network elements). For more information, see the *Cisco Prime Network 3.9 Customization User Guide.*

Table 2-26 Element Right-Click Menu Options (continued)

Option	Description
Show as Aggregation / Thumbnail	Displays the selected aggregation as a single entity or as a collection of items. The options toggle, depending on whether the aggregation is in a thumbnail or aggregated view.
Show CE Device	Displays devices for sites or LCPs with one or more hidden, connected devices.
Tools	The Tools option contains the following choices: • CPU Usage—Displays memory and CPU usage information for a device or network element. • Ping—Pings the device from the client station. • Telnet—Communicates with the device using the Telnet window from the client station. **Note** If you are using a Windows 7 system and want to use the Prime Network Telnet option, you need to set up Telnet on the Windows 7 system as follows: - For Windows 7 32-bit systems, enable the Windows Telnet Client to use the Prime Network Telnet option. - For Windows 7 64-bit systems, a solution is available on the Cisco Developer Network at http://developer.cisco.com/web/ana/forums/-/message_boards/message/2780108.
Topology	The Topology option enables you to add: • A static link between two devices. • A static topology between a device and an unmanaged network. • A tunnel to a VPN. When working with static links, the following submenu options enable you to define the A Side and Z Side of the link: • Mark as A Side • Mark as Z Side When working with VPNs in VPN Service View, the Add Tunnel submenu option allows you define and configure tunnels.
VNE Tools	Contains the following submenu options: • Poll Now—Updates the VNE information. • Stop VNE—Stops the VNE. • Start VNE—Starts the VNE. For more information, see Chapter 3, "Viewing Network Element Properties."

Aggregation Right-Click Menu

The aggregation right-click menu is displayed when you right-click an aggregation in a map.

Table 2-27 describes the aggregation right-click menu options.

Table 2-27 Aggregation Right-Click Menu Options

Option	Description
Aggregate	Groups the selected aggregations into an aggregation in the Prime Network Vision content pane, and enables you to define a name for the new aggregation. For more information, see Chapter 4, "Working with Prime Network Vision Maps."
Disaggregate	Ungroups the selected aggregation in the navigation pane and map in the Prime Network Vision window. All the aggregations in the selected node move up one level, and the original aggregation is removed. For more information, see Chapter 4, "Working with Prime Network Vision Maps."
Rename	Renames the selected aggregation.
Resize	Defines the size of selected aggregations in a map according to one of four sizes or according to a percentage of the current size.
Remove from Map	Removes the selected aggregation and all its children from the navigation pane and the map.
Save as New Map	Creates a new map and places the selected aggregation as the root, while leaving the original map intact.
Run Report	Enables you to run standard or user-defined events, inventory, and network service reports.
Show as Aggregation / Thumbnail	Displays the aggregation as a single entity or as a collection of items. The options toggle, depending on whether the aggregation is in a thumbnail or aggregated view.
Delete	Deletes the selected item. This option is available when the item is marked with the reconciliation icon.

Link Right-Click Menu

The Link right-click menu is displayed when you right-click a link in the map view. For more information, see Chapter 5, "Working with Links."

Table 2-28 describes the link right-click menu options.

Table 2-28 Link Right-Click Menu Option

Option	Description
Properties	Displays the properties of the selected link.

List View Right-Click Menu

The list view right-click menu is displayed when you right-click an entry in the Network Elements tab in the list view table. For more information, see List View, page 2-18.

Table 2-29 describes the list view right-click menu options.

Table 2-29 List View Right-Click Menu Options - Network Elements Tab

Option	Description
Inventory	Displays a window enabling you to view the physical and logical inventory. For physical inventory, you can view all the components of the device, such as the modules, ports, and its IP address or configured VLANs. In addition, you can view the status of each component. For logical inventory, you can view all the profiles and VC tables of the device. For more information, see Chapter 3, "Viewing Network Element Properties."
Attach / Detach / Edit Business Tag	Allows you to perform the following actions: • Attach a business tag to the selected element. • Remove a business tag from the selected element. • Edit an existing business tag for the selected element. **Note** The Detach and Edit options are available only when a business tag is attached to a link. For more information, see Chapter 6, "Working with Business Tags and Business Elements."
Config Mgmnt	Displays the Configuration Management page for the selected device in Prime Network Change and Configuration Management. For more information, see the *Cisco Prime Network 3.9 Change and Configuration Management User and Administration Guide.*
Image Mgmnt	Displays the Image Management page for the selected device in Prime Network Change and Configuration Management. For more information, see the *Cisco Prime Network 3.9 Change and Configuration Management User and Administration Guide.*
Run Report	Enables you to run standard or user-defined events, inventory, and network service reports.
Show Only Selected Rows	Displays only the rows that you select. For more information, see Viewing Selected Rows, page 2-54.
Show All Rows	Displays all table rows that meet the current filtering criteria.

Table 2-29 List View Right-Click Menu Options - Network Elements Tab (continued)

Option	Description
Tools	Contains the following submenu options: • CPU Usage—Displays memory and CPU usage information for a device or network element. • Ping—Pings the device from the client station. • Telnet—Communicates with the device using the Telnet window from the client station. **Note** If you are using a Windows 7 system and want to use the Prime Network Telnet option, you need to set up Telnet on the Windows 7 system as follows: - For Windows 7 32-bit systems, enable the Windows Telnet Client to use the Prime Network Telnet option. - For Windows 7 64-bit systems, a solution is available on the Cisco Developer Network at http://developer.cisco.com/web/ana/forums/-/message_boards/message/2780108.
Topology	Enables you to add: • A static link between two devices. • A static topology between a device and an unmanaged network. • A tunnel to a VPN. When working with static links, the following submenu options enable you to define the A Side and Z Side of the link: • Mark as A Side • Mark as Z Side When working with VPNs in VPN Service View, the Add Tunnel submenu option allows you define and configure tunnels.
Launch external applications	Launches external applications or tools, such as an SSH client. See the *Cisco Prime Network 3.9 Customization User Guide.*
Properties	Displays the properties of the selected item, such as the IP address and system name. In addition, you can open the VNE Properties dialog box and manage VNE properties. For more information, see Chapter 3, "Viewing Network Element Properties."
Commands	Enables you to launch any of the commands that are included with Prime Network Vision. For a complete list of the available commands, see the *Cisco Prime Network 3.9 Reference Guide*.
Script names	Launches available activation and configuration scripts. This can include the commands documented in Commands part of the *Cisco Prime Network 3.9 Reference Guide*, and those you create using Command Builder (can be launched against multiple network elements). For more information, see the *Cisco Prime Network 3.9 Customization User Guide.*

Table 2-29 List View Right-Click Menu Options - Network Elements Tab (continued)

Option	Description
Management	Contains the following submenu options: • Command Builder—Defines commands and scripts using the Prime Network Command Builder tool (Configurator security level required). • Soft Properties Management—Extends VNEs by adding SNMP MIB or Telnet/SHH/TL-1 properties to the device's collected information model using the Prime Network Soft Properties Manager (Administrator security level required). For more information about Command Builder and Soft Properties Manager, see the *Cisco Prime Network 3.9 Customization User Guide.*
VNE Tools	Contains the following submenu options: • Poll Now—Updates the VNE information. • Stop VNE—Stops the VNE. • Start VNE—Starts the VNE. For more information, see Chapter 3, "Viewing Network Element Properties."

Links View Right-Click Menu

The links view right-click menu is displayed when you right-click a link in the links view table. For more information, see Chapter 5, "Working with Links."

Table 2-30 describes the links view right-click menu options.

Table 2-30 Links View Right-Click Menu Options

Option	Description
Attach Business Tag	Attaches a business tag to the selected link. For more information, see Chapter 6, "Working with Business Tags and Business Elements."
Detach/Edit Business Tag	Detaches or edits a business tag from the selected link. For more information, see Chapter 6, "Working with Business Tags and Business Elements." The Detach and Edit options are available only when a business tag is attached to a link.
Select Link in Map	Highlights the selected link in the content pane.
Show Only Selected Rows	Displays only the rows that you select. For more information, see Viewing Selected Rows, page 2-54.
Show All Rows	Displays all table rows that meet the current filtering criteria.
Properties	Displays the properties of the selected link.

Ticket Right-Click Menu

The Ticket right-click menu is displayed when you right-click a ticket in the ticket pane. The Ticket right-click menu enables you to view ticket properties and highlights the links or elements that are affected by a ticket. The Ticket menu also enables you to acknowledge, clear, and remove a ticket. For more information, see Chapter 9, "Working with Tickets in Cisco Prime Network Vision."

Table 2-31 describes the ticket right-click menu options.

Table 2-31 Ticket Right-Click Menu Options

Option	Description
Acknowledge	Acknowledges that the ticket is being handled; the ticket is displayed as true in the ticket pane. Acknowledging an alarm removes the alarm icon from the device icon. Multiple tickets can be acknowledged at the same time.
Clear	Approves the reported faulty ticket and clears the faulty networking entity from Prime Network. The ticket is displayed as Clear in the ticket pane. **Note** When a Card Out or Link Down alarm occurs, the relevant information is displayed in the inventory and maintained in the VNE.
Remove	Removes the ticket and all its active subtickets from the ticket pane (this option is only available after the ticket has been cleared). The deleted tickets can be viewed using Cisco Prime Network Events. Multiple tickets can be removed at the same time. **Note** When a ticket is removed, the information is no longer displayed in the inventory and is removed from the VNE.
Clear and Remove	Approves the reported faulty ticket and clears the faulty networking entity from Prime Network. In addition, the ticket and all its active subtickets are removed from the ticket pane.
Find Affected Elements	Finds any elements affected by the selected ticket: • If only one element is affected, it is selected in the Prime Network navigation pane and content area. • If multiple elements are affected, they are displayed in the Affected Elements window.
Show Only Selected Rows	Displays only the rows that you select. For more information, see Viewing Selected Rows, page 2-54.
Show All Rows	Displays all table rows that meet the current filtering criteria.
Properties	Displays the Ticket Properties dialog box, enabling you to view ticket information, including impact analysis details of the affected parties and correlated alarms. See Viewing Ticket Properties, page 9-10.

Changing a User Password in Prime Network Vision

Prime Network enables you to provide authentication by Prime Network or an external Lightweight Directory Access Protocol (LDAP) server. The method used to change your password depends on whether authentication is provided by Prime Network or an LDAP server:

- If Prime Network provides login authentication, Prime Network Vision enables you to change your login password. If needed, the administrator can also change your password in Cisco Prime Network Administration.
- If Prime Network uses an LDAP server for authentication, you cannot change your password in Prime Network Vision. Only users with Administrator privileges can change your password, which must be done on the LDAP server.
  - For more information about external authentication, see the *Cisco Prime Network 3.9 Customization User Guide*.
  - For more information about password guidelines, see the *Cisco Prime Network 3.9 Administrator Guide*.

To change your password:

Step 1 Choose **Tools > Change User Password**. The Change User Password dialog box is displayed.

Note If Prime Network uses an LDAP server for authentication, the Change User Password option is dimmed. Contact your administrator to change your password on the LDAP server.

Step 2 Enter the following information:

- Old password—Enter the old user password.
- New password—Enter the new user password.
- Confirm password—Enter the new password again to confirm the entry.

Step 3 Click **OK**. The change takes effect the next time you log into the application.

Selecting Prime Network Vision Options

Prime Network Vision enables you to select map, display, audio, event history size options.

To select Prime Network Vision options:

Step 1 Choose **Tools > Options** from the main menu.

Step 2 In the Startup tab, check the Load Workspace on Startup check box to automatically view the content pane when you log in. Uncheck the check box if you do not want to view the content pane when you log in.

Step 3 Click the **Display** tab. Set the display options using the information in Table 2-32.

Table 2-32 Prime Network Vision Display Options

Field	Description
Preferences	
Map Labels Font Size	In the drop-down list, choose the preferred font size for labels on maps. Font sizes are 26, 28, 30, 32, and 34, with a default of 30.
Severity	
Show Severity Text (e.g. [3M+]	Check the check box to view severity labels in the navigation pane and maps, using the formula described in New Ticket Propagation, page 2-25. Uncheck the check box to hide severity labels.
Show Acknowledged	Check the check box to view the number of both acknowledged and unacknowledged alarms in the network element display name. Uncheck the check box to view only the number of unacknowledged alarms in the network element display name. For example, assume that device NE1 has two alarms with the severity M. One of these two alarms is acknowledged, and the other is not. If you check the Show Acknowledged check box, the display name will be NE1 [2M]. If you uncheck the Show Acknowledged check box, the display name will be NE1 [1M].
Show Propagated	Check the check box to view propagated alarms on the specific entity. Uncheck the check box to view only the alarms on the specific entity.
Display Name	
Display Name	Select the preferred setting for network element names: • Do not use Business Tag—Displays the original network element name only. • Add Business Tag to name—Displays the original network element name and the name of the business tag. • Replace name with Business Tag—Replaces the network element name with the business tag name. When a subscriber is attached to a port, the subscriber name is also added.

Step 4 Click the **Audio** tab and select your preferences for audio notifications using the information in Table 2-33.

Table 2-33 Prime Network Vision Audio Options

Field	Description
Enable Audio Response for Alarm	Select the preferred setting for audio notifications: • To indicate that a sound is to be issued when an alarm is triggered, check the check box. • To prevent a sound from being issued when an alarm is triggered, uncheck the check box. If you uncheck the check box, continue with Step 6.
Critical	Specify the .wav file to use for critical alarms.
Major	Specify the .wav file to use for major alarms.
Minor	Specify the .wav file to use for minor alarms.
Loop Sound on Critical Alarm	Specify whether or not the critical alarm sound should sound continuously when a critical alarm is triggered: • To play the critical alarm sound continuously when a critical alarm is triggered, check the check box. • To play the critical alarm sound only once when a critical alarm is triggered, uncheck the check box.

Step 5 Click the **Events** tab and, in the Events History Size in Hours field, enter the length of time in hours that Cisco Prime Network Vision should use when determining the events to display in the Network Events and Provisioning Events tab in the inventory window (see Ticket and Events Pane, page 3-18). If you enter a value of 0 (zero), only active events are displayed in the Network Events tab in inventory. The default value of six hours can be changed in Prime Network Administration.

Step 6 Click **Apply** to apply your selections.

Step 7 Click **OK**.

Working with Prime Network Tables

Prime Network uses tables to display different types of information. The following topics describe how to work with Prime Network tables so that you can view the information that you want and, optionally, save the information to a file:

- Table Toolbar Options, page 2-50
- Finding Text in a Table, page 2-51
- Sorting a Table, page 2-51
- Filtering Table Contents, page 2-53
- Viewing Selected Rows, page 2-54
- Exporting Tables to a File, page 2-55

To view all text in a table cell, you can do either of the following:

- Click the red triangle in the cell to automatically expand the cell to the size of the cell's contents.
- Hover your mouse cursor over the cell.

Table Toolbar Options

Table 2-34 describes the options available in table toolbars.

Table 2-34 Table Toolbar Options

Option	Name	Description
	Find	Searches the current table for the string you enter. For more information, see Finding Text in a Table, page 2-51.
	Export to CSV	Exports the information displayed in the table, or selected portions, to a CSV file. For more information, see Exporting Tables to a File, page 2-55
	Sort Table Values	Sorts the information displayed in the table by the criteria you specify. For more information, see Sorting a Table, page 2-51.
	Filter	Filters the information displayed in the table by the criteria you specify. For more information, see Filtering Table Contents, page 2-53.
	Clear Filter	Clears the existing filter.
	Show All Rows	Displays all table rows that meet the current filtering criteria.
	Show Only Selected Rows	Displays only the rows that you select. For more information, see Viewing Selected Rows, page 2-54.

Using Keyboard Shortcuts in Tables

Table 2-35 lists the keyboard shortcuts that you can use when working with tables.

Table 2-35 Keyboard Shortcuts for Tables

Keyboard Shortcut	Description
Ctrl + A	Selects all the rows in the table.
Ctrl + Space	Deselects all the rows in the table.
Enter	On a selected row, opens the default action.
Arrow Navigation Keys	Navigates up and down in the rows.
Ctrl + Up/Down	Keeps the selected row and moves up or down.
Ctrl + Up/Down + Space	Keeps the selected row and moves up or down. The space selects the required row.
Shift + Up/Down	Keeps the selected row and selects all the rows that are above or below it.
Shift + F10	Opens the right-click menu.
F3	Finds next.
Shift + F3	Finds previous.

Finding Text in a Table

Prime Network Vision enables you to search for information about a specific entry in a table by entering search criteria, such as a partial IP address.

To find text in a table:

Step 1 In the Find field on the toolbar, enter the search criterion for the entity that you want to find and press **Enter**.

Step 2 Press **F3** to continue searching the table or press **Ctrl + F** to return to the Find field.

Sorting a Table

Prime Network Vision enables you to sort a table in the following ways:

- According to a column, by clicking the required column heading.
- In ascending or descending order, by clicking a column heading.
- By clicking **Sort Table Values** in the toolbar and specifying sort criteria.

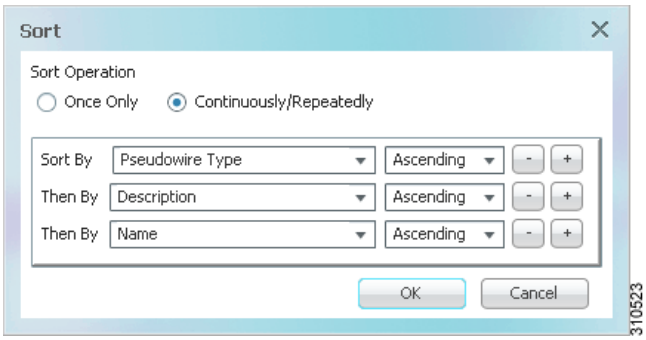
A triangle next in the column heading indicates the sort order:

- indicates the column is sorted in ascending order.
- indicates the column is sorted in descending order.

To sort a table using the Sort Table Values option:

Step 1 In the table toolbar, click **Sort Table Values**. The Sort dialog box is displayed.

Figure 2-10 Sort Dialog Box



Step 2 In the Sort Operation field, specify the frequency of the sort operation:

- Only Once—Sorts the information in the table only once according to the specified criteria. When this option is selected, newly added rows will always be listed at the bottom of the table, regardless of their sort criteria value. Also, if an existing row's value changes, the row will remain where it is.
- Continuously/Repeatedly—Sorts the information in the table continuously according to the specified criteria.

  If you select this option, the icon is displayed next to the selected column heading.

Step 3 In the Sort By field, specify the first sort criterion:

a. In the first drop-down list, choose the column to use for the first sort criterion.

b. In the second drop-down list, choose **Ascending** or **Descending** to indicate the sort order.

Step 4 If needed, click + to add another sort criterion.

Step 5 Adjust the sort criteria as needed:

- To add additional criteria, click +.
- To remove a criterion, click -.

Step 6 Click **OK** to sort the table using the specified criteria.

Filtering Table Contents

You can view only those items that are of interest to you by filtering a table's contents. This feature can be extremely helpful when working with tables that contain many entries.

Note If you load a table with many entries, (for example, thousands of entries), it can take a while for the complete table to load. The filtering options in the table toolbar are unavailable until the table has completely loaded.

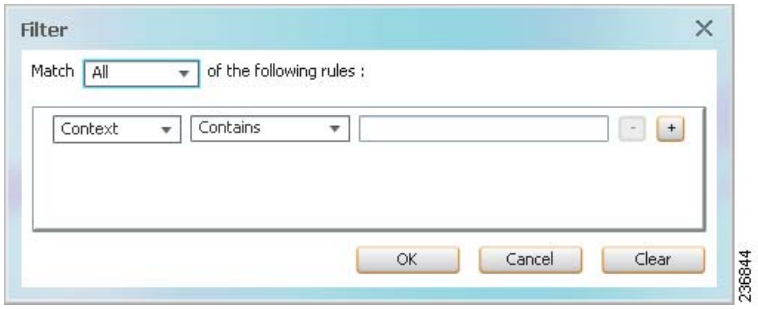
The following changes in the GUI indicate that a filter has been applied:

- The Filter button is slightly shaded.
- The Clear Filter button is active.
- The filter details are displayed:
  - In the status line below the table.
  - When you hover the mouse cursor over the Filter button.

To define a filter:

Step 1 In the toolbar above the table, click **Filter**. The Filter dialog box is displayed as shown in Figure 2-11.

Figure 2-11 Table Filter Dialog Box



Step 2 In the Match drop-down list, choose the rule for including items that meet the specified criteria:

- All—All of the following criteria are to be met.
- Any—Any of the following criteria are to be met.

Step 3 For each criterion, specify the following information:

a. In the first drop-down list, choose the primary match category. The drop-down list contains all columns in the current table.

b. In the second drop-down list, choose the rule to use for this criterion. The options are:

- Contains
- Does not contain
- Equals
- Does not equal
- Greater than
- Less than

c. The third field either lists the available values or allows you to enter text:
   - If a drop-down list is displayed, choose the required entry.
   - If an entry field is displayed, enter a string or regular expression for the criterion.

   Any entry that is not a regular expression is treated as a string.

Tip You can use the "Greater than" or "Less than" rule with a string for filtering. For example, if you want to include all interfaces above Ethernet0/0/3, you can select **Greater than** and enter the string `Ethernet0/0/3` to view interfaces Ethernet0/0/4, Ethernet0/0/5, and so on.

Step 4 Click  to add another criterion for this filter.

Step 5 Add additional criteria as required. To remove a criterion, click  .

Step 6 When you have specified all criteria for the filter, click **OK**.

The table data is displayed using the defined filter.

Step 7 To clear a filter, click **Clear Filter** in the table toolbar.

The table is refreshed and all entries are displayed.

The following tables have additional filtering capabilities:

- Prime Network Vision ticket pane. For more information, see Filtering Tickets by Criteria, page 9-8.
- Links view in the content pane. For more information, see Links View, page 2-22.

Viewing Selected Rows

Prime Network enables you to select a line or a specific set of lines, and display them in the table. The lines that you do not select are hidden from view.

You can use this feature with the filtering mechanism to view the specific entries that you need. You can either select specific rows and then apply a filter, or you can filter the table's contents and then select specific rows to view.

If you apply a filter, the details of the filter are displayed below the table. For example, if you apply a filter that specifies all elements with names containing ME are to be displayed, the following appears in the table status line:

```
Filter: Name Contains ME
```

The status bar below the table also displays the:

- Number of the selected row, if a row is selected.
- Number of rows selected, if any.
- Total number of rows currently displayed in the table.

For example, if you select line four in a table with six rows, the following information is displayed:

```
Line 4 (1/6 Selected)
```

If no rows are selected, the value for the line defaults to 0, such as:

```
Line 0 (Size 6)
```

To view selected rows:

Step 1 Select the appropriate line or lines in the table using standard Windows mouse or keystroke operations.

Step 2 Click **Show Only Selected Rows**.

The table displays the selected rows, and the Show All Rows option becomes active.

Step 3 Click **Show All Rows** to view all rows in the table.

Exporting Tables to a File

Prime Network Vision enables you to export the currently displayed data from a table. You can either select specific rows to export, or clear all selections in the table to export the entire table. The data can then be imported and viewed at a later stage.

To export a table to a file:

Step 1 Press **Ctrl + Space** to clear any existing selection.

Step 2 Identify the content you want to export:

- To export specific rows, select the required rows.
- To export the entire table, ensure that nothing is selected.

Step 3 In the table toolbar, click **Export to CSV**. The Export Table to File dialog box is displayed.

Step 4 Navigate to the directory where you want to save the table.

Step 5 In the File name field, enter a name for the file.

Step 6 Click **Save**. The content specified in Step 2 is saved in the specified file and directory.



CHAPTER 3

Viewing Network Element Properties

The following topics describe the user access roles required to use Cisco Prime Network Vision (Prime Network Vision) and how to view network element physical and logical properties in any mapped network:

- User Roles Required to Work with Prime Network Vision, page 3-2
- Information Available in Element Icons, page 3-3
- Viewing the Properties of a Network Element, page 3-5
- Viewing and Modifying VNE Properties, page 3-9
- Viewing VNE Communication Status, page 3-11
- Updating VNE Information, page 3-12
- Opening the Inventory Window, page 3-12

Note The inventory window also enables you to view all the tickets that are collected on the selected element in the ticket and events pane. For more information, see Ticket and Events Pane, page 3-18.

- Viewing the Physical Properties of a Device, page 3-19
- Working with Ports, page 3-22
- Viewing the Logical Properties of a Network Element, page 3-27
- Viewing Device Operating System Information, page 3-33

Note Prime Network Vision maintains continuous, real-time discovery of all the physical and logical entities of the network inventory and the relationships among them. The Prime Network Vision distributed system inventory automatically reflects every addition, deletion, and modification that occurs in the network.

User Roles Required to Work with Prime Network Vision

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

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

For more information on user authorization, see the *Cisco Prime Network 3.9 Administrator Guide*.

The following tables identify the tasks that you can perform:

- Table 3-1 identifies the tasks that you can perform if a selected element **is not in** one of your assigned scopes.
- Table 3-2 identifies the tasks that you can perform if a selected element **is in** one of your assigned scopes.

By default, users with the Administrator role have access to all managed elements. To change the Administrator user scope, see the topic on device scopes in the *Cisco Prime Network 3.9 Administrator Guide*.

Table 3-1 Default Permission/Security Level Required for Prime Network Vision Functions - Element Not in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View maps	X	X	X	X	X
View network element properties	—	—	—	—	X
View network element properties in logical and physical inventory	—	—	—	—	X
View port status and properties	—	—	—	—	X
View VNE properties	—	—	—	—	X
Open the Port Utilization Graph	—	—	—	—	X
Enable and disable port alarms	—	—	—	—	X[1]
View tickets in inventory window	—	—	—	—	X
View network events in inventory window	—	—	—	—	X
View provisioning events in inventory window	—	—	—	—	X

Table 3-2 Default Permission/Security Level Required for Prime Network Vision Functions - Element in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View maps	X	X	X	X	X
View network element properties	X	X	X	X	X
View network element properties in logical and physical inventory	X	X	X	X	X
View port status and properties	—	X	X	X	X
View VNE properties	X	X	X	X	X
Open the Port Utilization Graph	X	X	X	X	X
Enable and disable port alarms	—	—	—	X[1]	X[1]
View tickets in inventory window	X	X	X	X	X
View network events in inventory window	X	X	X	X	X
View provisioning events in inventory window	X	X	X	X	X

1. To enable and disable port alarms on a device, the Administrator scope level must also be configured for that device.

Information Available in Element Icons

Element icons in Prime Network Vision maps display different amounts of information according to their size as shown in Table 2-3. Table 3-3 identifies the information that is available for different types of elements for the four icons sizes.

Table 3-3 Information Displayed in Element Icons by Size

	Icon Size			
Element Type	Tiny (Dot)	Normal	Large	Huge
Aggregation	Color representing the associated alarm severity	Name	Name in card title	Name in card title
Bridge	Color representing the associated alarm severity	Name	• Name in card title and body • Number of Ethernet flow points	• Name in card title and body • Number of Ethernet flow points
EFP cross-connect	Color representing the associated alarm severity	Name	Name in card title	Name in card title
Ethernet flow point	Color representing the associated alarm severity	Name	• Name in card title • Type, such as Trunk, Access, Dot1Q Tunnel, and so on • Match criteria	• Name in card title • Type, such as Trunk, Access, Dot1Q Tunnel, and so on • Match criteria
Ethernet service	Color representing the associated alarm severity	Name	• Name in card title • Number of edge EFPs	• Name in card title • Number of edge EFPs

Table 3-3 Information Displayed in Element Icons by Size (continued)

Element Type	Icon Size			
	Tiny (Dot)	Normal	Large	Huge
EVC	Color representing the associated alarm severity	Name	• Name in card title • Number of instances of domains (VPLS, EoMPLS, bridge, or cross-connect) with a maximum of three lines	• Name in card title • Number of instances of domains (VPLS, EoMPLS, bridge, or cross-connect) with a maximum of four lines
LSP Endpoint (Working or Protected)	Color representing the associated alarm severity	Name	• Name in card title • Bandwidth	• Name in card title • Bandwidth • Attach Business Tag button • Properties button
LSP Midpoint	Color	Name	• Name in card title • Forward bandwidth • Reverse bandwidth • Reverse in and out labels	• Name in card title • Forward bandwidth • Reverse bandwidth • Reverse in and out labels • Attach Business Tag button • Inventory button • Properties button
MPLS-TP Tunnel	Color representing the associated alarm severity	Name	Name in card title and body	• Name in card title and body • Attach Business Tag button • Properties button
MPLS-TP Tunnel Endpoint	Color representing the associated alarm severity	Name	• Name in card title and body • Tunnel identifier	• Name in card title and body • Tunnel identifier • Attach Business Tag button • Inventory button • Properties button
Network element	Color representing the associated alarm severity	Name	• Name in card title • Element model • IP address • Software version	• Name in card title • Element model • IP address • Software version • Inventory button • Filter Tickets button • Attach Business Tag button
Pseudowire	Color representing the associated alarm severity	Name	Name in card title and body	• Name in card title and body • Attach Business Tag button • Properties button

Table 3-3 Information Displayed in Element Icons by Size (continued)

Element Type	Icon Size			
	Tiny (Dot)	Normal	Large	Huge
Pseudowire edge	Color representing the associated alarm severity	Name	• Name in card title • Local IP address • Peer IP address	• Name in card title • Local IP address • Peer IP address • Attach Business Tag button • Inventory button • Properties button
VLAN	Color representing the associated alarm severity	Name	Name in card title and body	• Name in card title • Name in card body • Number of switching entities • Number of edge EFPs
VPLS	Color representing the associated alarm severity	Name	• Name in card title • Number of access EFPs • Number of access pseudowires • Number of VPLS forwards	• Name in card title • Number of access EFPs • Number of access pseudowires • Number of VPLS forwards
VPLS Forward	Color representing the associated alarm severity	Name	• Name in card title • VPN identifier • Number of core pseudowires	• Name in card title • VPN identifier • Number of core pseudowires
VPN	Color representing the associated alarm severity	Name	Name in card title and body	• Name in card title and body • Attach Business Tag button • Properties button

Viewing the Properties of a Network Element

You can view the general information about a selected network element in the Prime Network Vision map view and view more detailed information by viewing the Properties window for the selected element.

To view network element properties:

Step 1 To view general information about a network element, do either of the following:

- Zoom in to view the required information:
  1. Position your mouse cursor on or near the required element.
  2. Use the mouse scroll wheel to zoom in or out.

- Resize the element icon as follows:

  1. Click the required element in the Prime Network Vision map. The element displays a gray outline to indicate that it is selected.

  2. Position the cursor on the gray outline and, while pressing the left mouse button, drag the mouse to resize the element in the map.

As the element size increases, additional information is displayed. For network elements, the available information is the following:

- IP address
- Model, such as Cisco 7606
- Software version

Step 2 To view more detailed information, open the Properties or inventory window for the element in any of the following ways:

- Right-click the element in the navigation pane, map view, or list view, and choose **Properties**.
- Select the element in the map view or list view, and choose **Node > Properties**.
- Double-click an element in the navigation pane or map view.
- If the element icon is at the largest size, click the **Inventory** icon.
- Select the element in the map view or list view, and choose **Node > Inventory**.

Depending on your selection, either the Properties window or inventory window is displayed with the inventory window providing slightly more information than the Properties window. Figure 3-1 shows the Properties window.

Figure 3-1 Properties Window

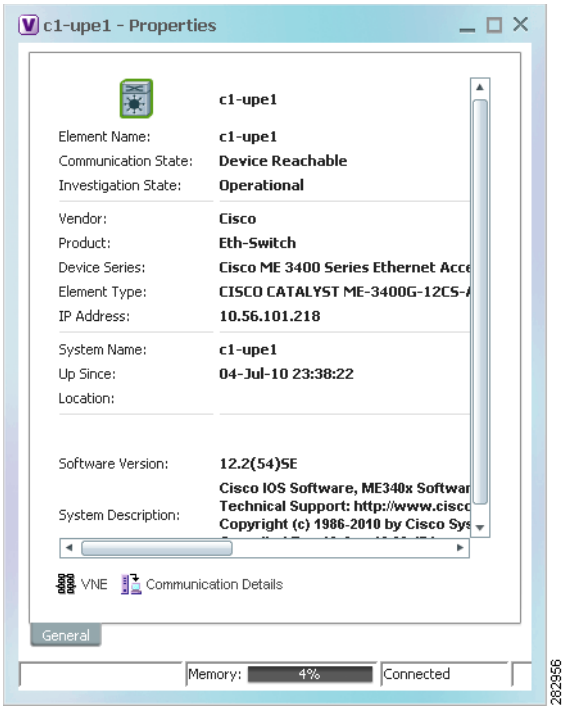


Table 3-4 describes the information displayed in both the Properties and inventory windows.

Table 3-4 Properties and Inventory Windows

Field	Description
General Tab	
Element icon	Icon representing the element in Prime Network Vision and displaying the current color associated with the element operational health. For more information on severity colors, see Prime Network Vision Status Indicators, page 2-24. The icon might include a badge that indicates an alarm or another item of interest associated with the element. For more information about badges, see Network Element Badges, page 3-8.
Element Name	Name assigned to the element for ease of identification.
Communication State	Ability of the VNE to reach the network element, according to the health of the element. For more information about communication states, see the *Cisco Prime Network 3.9 Administrator Guide*.
Investigation State	Level of network element discovery that has been performed or is being performed by the VNE. For more information about investigation states, see the *Cisco Prime Network 3.9 Administrator Guide*.
Vendor	Vendor name, as defined in the device MIB.
Product	Product name of the element, as defined in the device MIB; for example, Router.
Device Series	Product series that the device belongs to, such as Cisco 7600 Series Routers.
Element Type	Element model, such as Cisco 7606.
Serial Number[1]	Serial number of the element.
CPU Usage[1]	Percentage of CPU currently in use by the element.
Memory Usage[1]	Amount of memory currently in use by the element.
IP Address	IP address used for managing the element.
System Name	Name of the device, as defined in the device MIB.
Up Since	Date and time the element was last reset.
Contact	Email address of the person responsible for the element.
Location	Physical location of the element, as defined in the device MIB.
DRAM Usage[1]	Percentage of available DRAM currently in use by the element.
Flash Device Size[1]	Amount of flash memory available on the element.
NVRAM Size[1]	Amount of NVRAM available on the element.
Software Version	Software version running on the element.
Software Description	Description of the system taken from the element.
Processor DRAM[1]	Amount of DRAM currently in use by the element's processor.
Sending Alarms[1]	Whether or not the element is configured for sending alarms: True or False.

Table 3-4 Properties and Inventory Windows (continued)

Field	Description
Buttons	
VNE Details	Opens the Properties dialog box, where you can edit the VNE's properties, perform maintenance, configure polling rates, and identify IP addresses for which SNMP syslog and trap events are to be generated. For more information, see: • Viewing and Modifying VNE Properties, page 3-9 • *Cisco Prime Network 3.9 Administrator Guide*
VNE Status	Opens the Communication Details window, which displays the status of the device protocols and whether the device is sending traps and syslogs. For more information, see Viewing VNE Communication Status, page 3-11.

1. Displayed only in the inventory window.

Network Element Badges

Network elements and links can also display badges that are technology-specific, such as a Protected LSP or an STP root. Table 3-5 describes some of the badges that are available in Prime Network Vision. For more information, see the related topics.

Table 3-5 Network Element Badges

Icon	Name	Description	Related Topic
	Access gateway	An MST or REP access gateway is associated with the element.	Viewing Access Gateway Properties, page 12-18
	Blocking	The element associated with this badge has a REP alternate port.	Viewing REP Information in VLAN Domain Views and VLAN Overlays, page 12-60
	Clock service	A clocking service is running on the associated element.	Applying a Network Clock Service Overlay, page 18-48
	Lock	The associated network LSP is in lockout state.	Viewing MPLS-TP Tunnel Properties, page 17-7
	Multiple links	One or more links is represented by the visual link and at least one of the links contains a badge.	Viewing REP Information in VLAN Domain Views and VLAN Overlays, page 12-60

Table 3-5 Network Element Badges (continued)

Icon	Name	Description	Related Topic
	Reconciliation	The element with this badge is associated with a network element that does not exist. For example, the device configuration has changed and a network problem exists. Some elements can be deleted only if their components, such as EFPs, VPLS forwards, or VRFs, display the reconciliation icon.	Deleting a Business Element, page 6-8
	REP primary blocking	The element associated with this badge has a REP primary port that is also blocking.	Viewing REP Information in VLAN Domain Views and VLAN Overlays, page 12-60
	REP primary	The element associated with this badge has a REP primary port.	Viewing REP Information in VLAN Domain Views and VLAN Overlays, page 12-60
	Redundancy service	The element associated with this badge is a backup pseudowire or a protected LSP.	• Adding an MPLS-TP Tunnel, page 17-5 • Viewing Pseudowire Redundancy Service Properties, page 12-98
	STP root	The element associated with this badge is a STP root bridge or the root of an STP tree.	Viewing STP Information in VLAN Domain Views and VLAN Overlays, page 12-63

Viewing and Modifying VNE Properties

To view and optionally modify VNE properties:

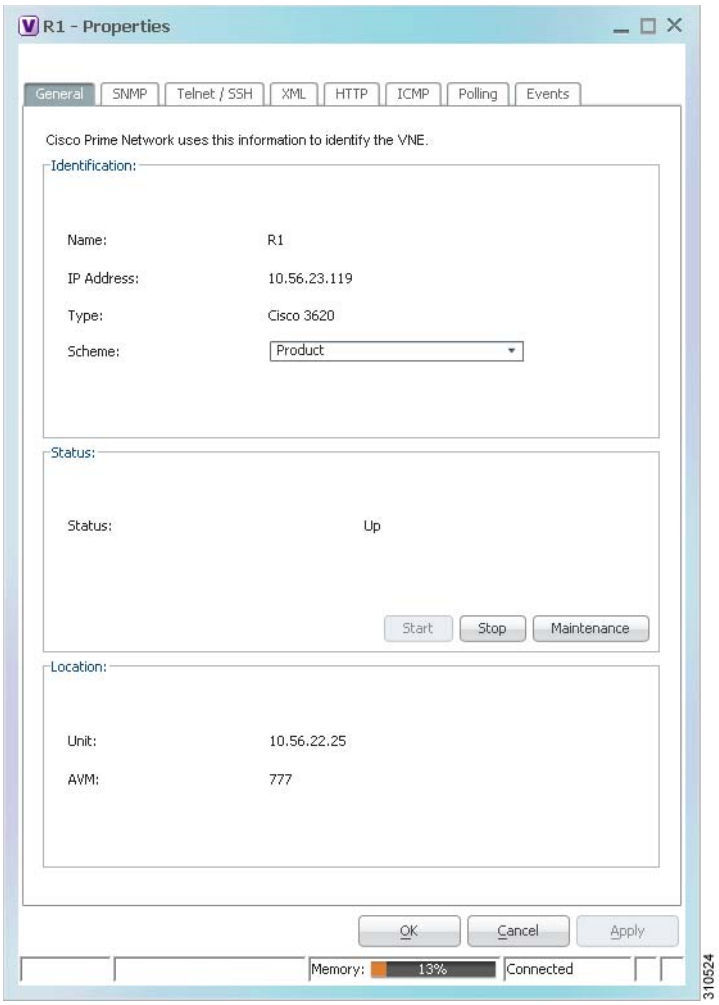
Step 1 Select the required element in Prime Network Vision and open the inventory window or Properties window in one of the following ways:

- If the element icon is at the largest size, click the **Inventory** icon.
- Select an element in the map view or list view, and choose **Node > Inventory**.
- Right-click a device in the navigation pane, map view, or list view, and choose **Properties**.
- Select an element in the map view or list view, and choose **Node > Properties**.

Step 2 Click **VNE**.

Figure 3-2 shows an example of the VNE Properties window.

Figure 3-2 VNE Properties Window



If the VNE for the element has been stopped, a message is displayed at the top of the inventory window letting you know that the VNE was stopped. The message includes a Refresh button so that you can refresh the information if the VNE has restarted. If the VNE is still down when you click **Refresh**, a VNE Unreachable message is displayed and the inventory window is closed. For more information about starting VNEs, stopping VNEs, adding new VNEs to a network, or modifying the status of a VNE, see the *Cisco Prime Network 3.9 Administrator Guide*.

Step 3 Click the required tab to view or modify the desired information. For more information about these options and configuring a VNE, see the *Cisco Prime Network 3.9 Administrator Guide.*

Step 4 If you change any of the settings, click **Apply** and then **OK**.

If you do not change any of the settings, click **OK** or **Cancel**.

Viewing VNE Communication Status

To view the status of VNE communication:

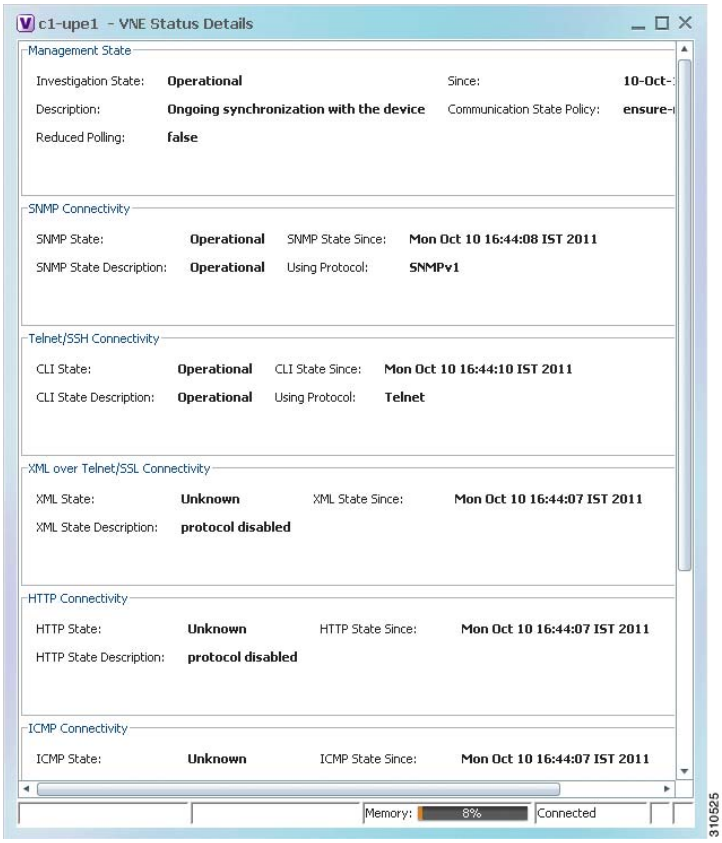
Step 1 In Prime Network Vision, select the required element.

Step 2 Open the inventory window (**Node > Inventory**) or Properties window (**Node > Properties**) for the selected item.

Step 3 Click **VNE Status**.

The VNE Status Details window is displayed as shown in Figure 3-3.

Figure 3-3 VNE Status Details Window



The VNE Status Details window provides information about:

- Management connectivity state
- SNMP connectivity
- Telnet/SSH connectivity
- XML over Telnet/SSH connectivity
- HTTP connectivity
- ICMP connectivity
- Syslog connectivity
- Trap connectivity

For more information about the VNE Status Details window, see the *Cisco Prime Network 3.9 Administrator Guide*.

Updating VNE Information

Some VNEs use the reduced polling mechanism which automatically polls the device when a configuration change syslog is received and immediately updates the VNE information accordingly.

The risk of using reduced polling applies mostly to situations in which events are dropped. In those situations, changes might be detected later than they would have if regular polling were used.

If an event is dropped, the network element shows a Currently Unsynchronized investigation state. If you notice this VNE state, you can initiate polling to update the VNE information in either of the following ways:

- Right-click the element and choose **VNE Tools > Poll Now**.
- Double-click the element to open the inventory window and click **Poll Now**.

Prime Network polls the selected element and updates the VNE information.

For more information about reduced polling, see the *Cisco Prime Network 3.9 Administrator Guide*.

Opening the Inventory Window

Table 3-6 describes the tasks that you can perform from the inventory window and related topics.

Table 3-6 Tasks Available from Inventory and Related Topics

Task	Related Topic
Add or remove links.	Adding Static Links, page 5-15
Generate the Port Utilization graph for physical ports.	Generating the Port Utilization Graph, page 3-27
Manage the alarms being sent on a port.	Working with Ports, page 3-22
Open Cisco PathTracer and launch a path trace.	Using Cisco PathTracer to Diagnose Problems, page 11-1

Table 3-6 Tasks Available from Inventory and Related Topics (continued)

Task	Related Topic
Open the Prime Network Command Builder to create customized commands.	*Cisco Prime Network 3.9 Customization User Guide*
Open the Prime Network Soft Properties Manager to extend the amount of information displayed.	*Cisco Prime Network 3.9 Customization User Guide*
Update the VNE information.	Updating VNE Information, page 3-12
View and optionally modify VNE properties.	Viewing and Modifying VNE Properties, page 3-9
View physical and logical inventory information.	• Viewing the Physical Properties of a Device, page 3-19 • Viewing the Logical Properties of a Network Element, page 3-27
View tickets or events for a device, service, or component.	Ticket and Events Pane, page 3-18
View VNE communication details.	Viewing VNE Communication Status, page 3-11

The inventory window also allows you to view technology-specific information. For more information on viewing technology-specific information in logical inventory or physical inventory, see:

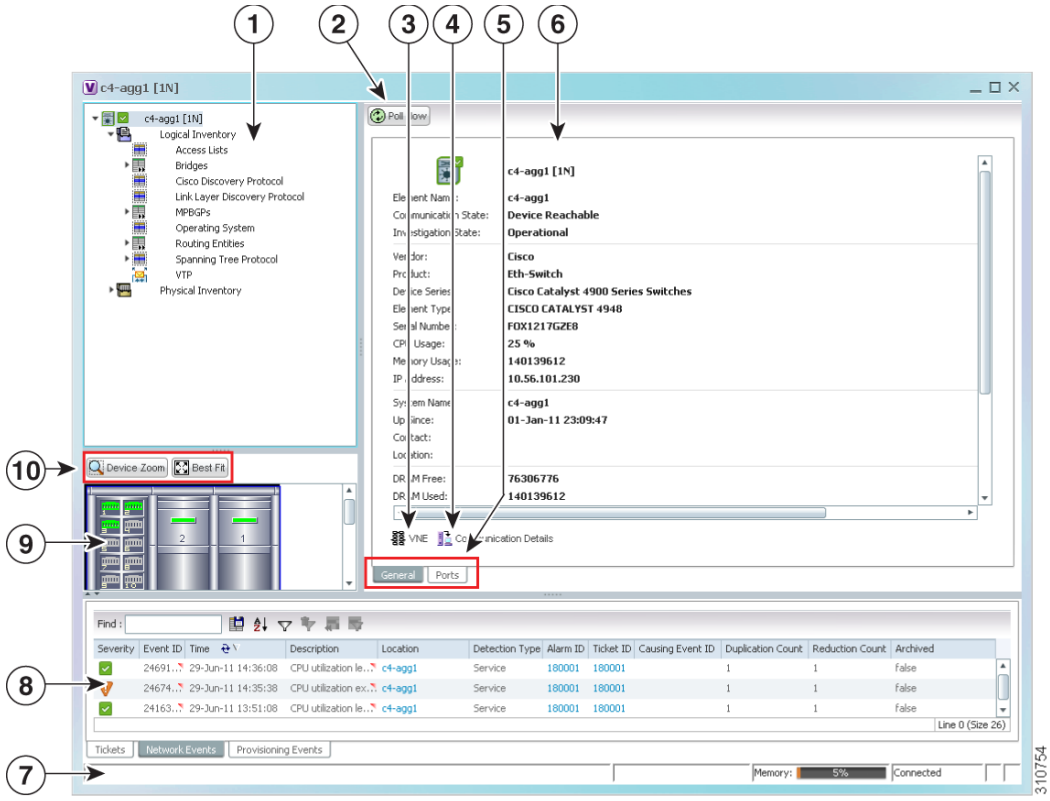
- Chapter 12, “Monitoring Carrier Ethernet Services”
- Chapter 13, “Monitoring Carrier Grade NAT Properties”
- Chapter 14, “Monitoring DWDM Properties”
- Chapter 15, “Viewing Ethernet Operations, Administration, and Maintenance Tool Properties”
- Chapter 16, “IPv6 and IPv6 VPN over MPLS”
- Chapter 17, “Monitoring MPLS Services”
- Chapter 18, “Monitoring MToP Services”
- Chapter 19, “Viewing SBC Properties”

To open the inventory window, do one of the following:

- If the element icon is at the largest size, click the **Inventory** icon.
- Double-click an item in the navigation pane or map.
- Right-click an element in the navigation pane or map and choose **Inventory**.

Figure 3-4 shows an example of an inventory window.

Figure 3-4 Inventory Window



1	Navigation pane	**6**	Content pane
2	Poll Now button	**7**	Status bar
3	VNE button	**8**	Ticket and events pane
4	Communications Details button	**9**	Device view pane
5	Content pane tabs	**10**	Device view pane toolbar

The inventory window displays the physical and logical inventory for the selected item. For more information about the options in the inventory window, see:

- Navigation Pane, page 3-15
- Device View Pane, page 3-16
- Device View Pane Toolbar, page 3-17
- Ticket and Events Pane, page 3-18
- Content Pane, page 3-16
- Working with Ports, page 3-22
- Updating VNE Information, page 3-12
- Viewing the Properties of a Network Element, page 3-5
- Viewing VNE Communication Status, page 3-11

All areas displayed in the inventory window are correlated; this means that selecting an option in one area affects the information displayed in the other areas.

The information displayed in the inventory window varies according to the item selected in the navigation pane.

To view logical inventory information, expand the Logical Inventory branch. For more information about logical inventory information, see Viewing the Logical Properties of a Network Element, page 3-27.

To view physical inventory information, expand the Physical Inventory branch. For more information about physical inventory information, see Viewing the Physical Properties of a Device, page 3-19.

Click **Poll Now** to update the display with the current VNE information.

Click the top right corner to close the inventory window.

Navigation Pane

The navigation pane in the inventory window displays a tree-and-branch representation of the selected device and its modules. The navigation pane contains two main branches:

- Logical Inventory—Includes logical items related to the selected element, such as access lists, ATM traffic profiles, and routing entities.
- Physical Inventory—Includes the various device components, such as chassis, cards, subslots, and so on.

When you select an item in the navigation pane, the information displayed in the content pane is updated. You can expand and collapse the branches in the navigation pane to display and hide information as needed.

The window heading and the highest level in the navigation pane display the name of the VNE given to the element as defined in Cisco Prime Network Administration. The element icon and status are displayed at the top of the navigation and content panes.

The color of the element icon reflects the element operational status. For more information about indicators of operational health and status, see:

- Prime Network Vision Status Indicators, page 2-24
- VNE Management State, page 2-25

Status Indicators

A status indicator icon appears next to the element icon for any unacknowledged tickets associated with the element. In addition, status indicator icons are displayed next to the specific logical or physical inventory branches that are associated with the ticket.

If you click a branch in the navigation pane that contains a status icon, the associated tickets and events are displayed in the tickets and events pane at the bottom of the inventory window.

Communication and Investigation State Icons

The navigation pane can also display a communication or investigation state icon next to the element icon in the navigation and content panes.

For more information about communication and investigation state icons, see VNE Management State, page 2-25.

Content Pane

The content pane contains two tabs:

- General—Contains physical or logical information specific to the item you select in the navigation pane or device view panel; for example, information about pseudowires or the chassis.

  The General tab can also display context-sensitive tabs and buttons; the buttons displayed depend on your selection in the navigation pane or device view panel. For example, if an ATM port is selected, the Show VC Table, Show Cross-Connect, or Show Encapsulation button might be displayed.

- Ports—Lists all ports on the device with their current alarm status, location, and other properties, and enables you to change their status by using a right-click menu. For more information, see Working with Ports, page 3-22.

The content pane can also display context-sensitive tabs and buttons; the buttons displayed depend on your selection in the navigation pane or device view panel. For example, if an ATM port is selected, the Show VC Table, Show Cross-Connect, or Show Encapsulation button might be displayed.

In addition, you can view the properties of a row in a table by double-clicking the row or by right-clicking the row and choosing **Properties**.

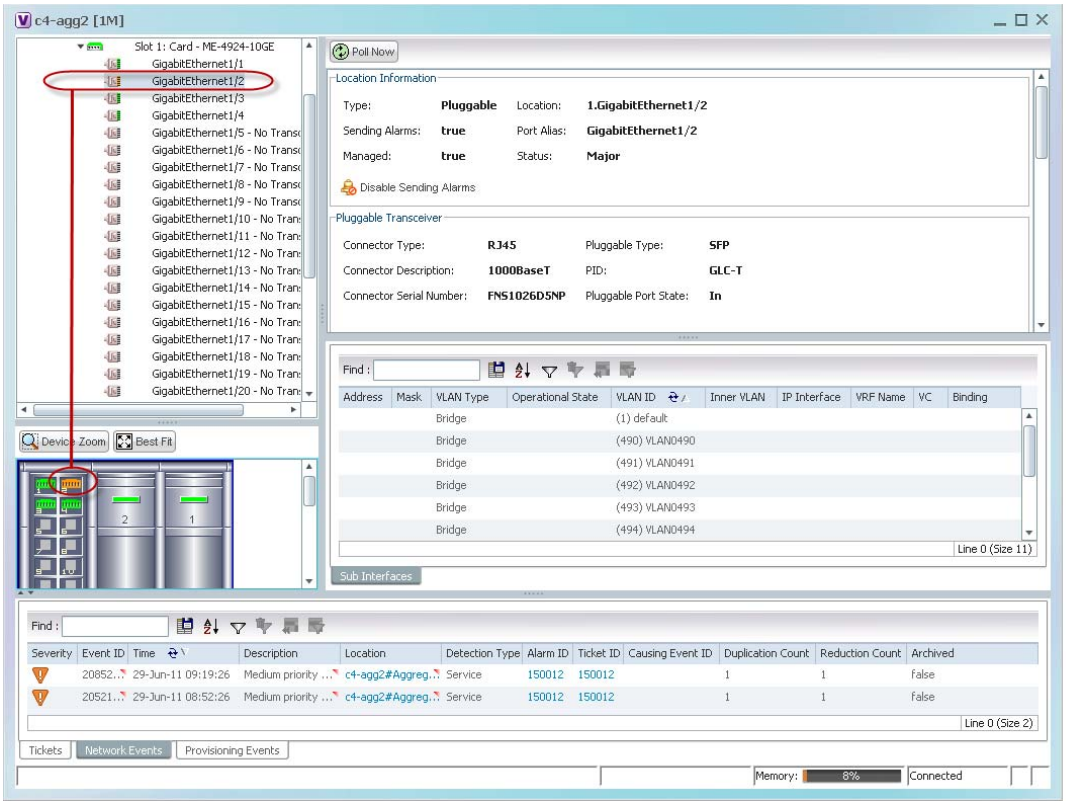
For information about tables that appear in the content pane, see Working with Prime Network Tables, page 2-49.

Device View Pane

The device view pane enables you to visually locate elements in the chassis and identify their status. All occupied slots in the chassis are rendered in the device view pane. If a port is down, it is shown in red in both the navigation pane and the device view pane, allowing you to quickly pinpoint the problem.

Figure 3-5 provides an example of the device view pane for a Cisco device. The circled slot in the device view pane corresponds to the circled slot in the physical inventory navigation pane. If you click a port in the device view pane (see the circled port), Prime Network Vision displays both the properties of the element and its location in the navigation pane and content pane.

Figure 3-5 Device View Pane



Device View Pane Toolbar

The following tools for working with the device view pane:

Icon	Description
	Displays an enhanced view of the components within the device in a browse box as you move over the device view panel with the selection tool.
	Fits the entire view of the element in the device view panel.

Ticket and Events Pane

The ticket and events pane is displayed at the bottom of the inventory window and contains the following tabs:

- Tickets—Displays the tickets that are collected on the selected element, service, or component in the navigation pane.

  Table 9-3 on page 9-5 describes the information that is available in the Tickets tab.

- Network Events—Displays all active network events associated with tickets and alarms, and all archived events with a timestamp that falls within the specified events history size (see Selecting Prime Network Vision Options, page 2-47).

  Table 3-7 describes the information that is available in the Network Events tab.

Table 3-7 Network Events Tab in Logical Inventory

Field	Description
Severity	Icon indicating the severity of the alarm on the event
Event ID	Event identifier, assigned sequentially.
Time	Date and time when the event occurred and was logged and recorded.
Description	Description of the event.
Location	Entity that triggered the event.
Detection Type	Method by which the event was detected, such as Service or Syslog.
Alarm ID	Identifier of the alarm associated with the event.
Ticket ID	Identifier of the ticket associated with the event.
Causing Event ID	Identifier of the causing event.
Duplication Count	For network events, the duplication count is calculated by the VNE and pertains only to flapping events. The duplication count represents the number of noncleared events aggregated by the flapping event.
Reduction Count	For network events, the reduction count is calculated by the VNE and pertains only to flapping events. The reduction count represents the number of events that are aggregated by the flapping event.
Archived	Whether the event is archived: True or False.

- Provisioning Events—Available to users with the Configurator role or higher for the selected element. This tab displays provisioning events with their source in the selected element and with a timestamp that falls within the specified events history size (see Selecting Prime Network Vision Options, page 2-47).

  All activations that occur are also included in this tab.

  Table 8-4 on page 8-5 describes the information that is available in the Provisioning Events tab.

Note Provisioning events that are caused by workflows (AVM 66) are not displayed in this table even if the element is affected by the workflow.

When displaying network and provisioning events, Prime Network Vision monitors the history size value defined in the Events tab of the Options dialog box (**Tools > Options > Events**). The default value is six hours and can be changed in Prime Network Administration. In addition, Prime Network Vision limits the maximum number of network and provisioning events that are sent from the server to client to 15,000 each. If the number of network or provisioning events exceeds the limit specified in the Options Events tab or the 15,000 maximum limit, Prime Network Vision purges the oldest events from table. The purging mechanism runs once per minute.

Tip You can display or hide the ticket and events pane by clicking the arrows displayed below the device view panel.

Viewing the Physical Properties of a Device

Each device that is managed by Prime Network is modeled in the same manner. The physical inventory reflects the physical components of the managed network element. Prime Network enables you to view physical inventory information for the following entities:

- Device
- Chassis
- Shelves
- Cards
- Subcards
- Ports, including logical ports and pluggable transceivers

Table 3-8 identifies the icons used to display physical inventory components in the navigation pane.

Table 3-8 Physical Inventory Icons

Icon	Device
	Chassis
	Shelf
	Card/Subcard
	Port/Logical Port Pluggable Transceiver
	Unmanaged Port

Physical inventory is continuously updated for both status and configuration. The addition of a new card, the removal of a card, or any change to the device is reflected by the VNE and updated instantly.

If you physically remove an item that Prime Network Vision is managing, the following changes occur in physical inventory, depending on the item removed:

- Removing an item other than a pluggable transceiver results in the following changes:
  - The color of the icon in physical inventory changes to black.
  - The item's status changes to Out.

  The other properties of the removed item reflect the most recent value that was updated from the device with the following exceptions:
  - Cards—If the card was participating in a card redundancy configuration, the redundancy state changes to None.
  - Port—The operational status of the port changes to Down.
- Removing a pluggable transceiver results in the following changes:
  - The color of the pluggable transceiver icon changes to gray.
  - The pluggable transceiver status changes to Disabled.
  - In the Pluggable Transceiver panel:
    - The properties are no longer displayed.
    - The connector type changes to Unknown.
    - The pluggable port state changes to Out.

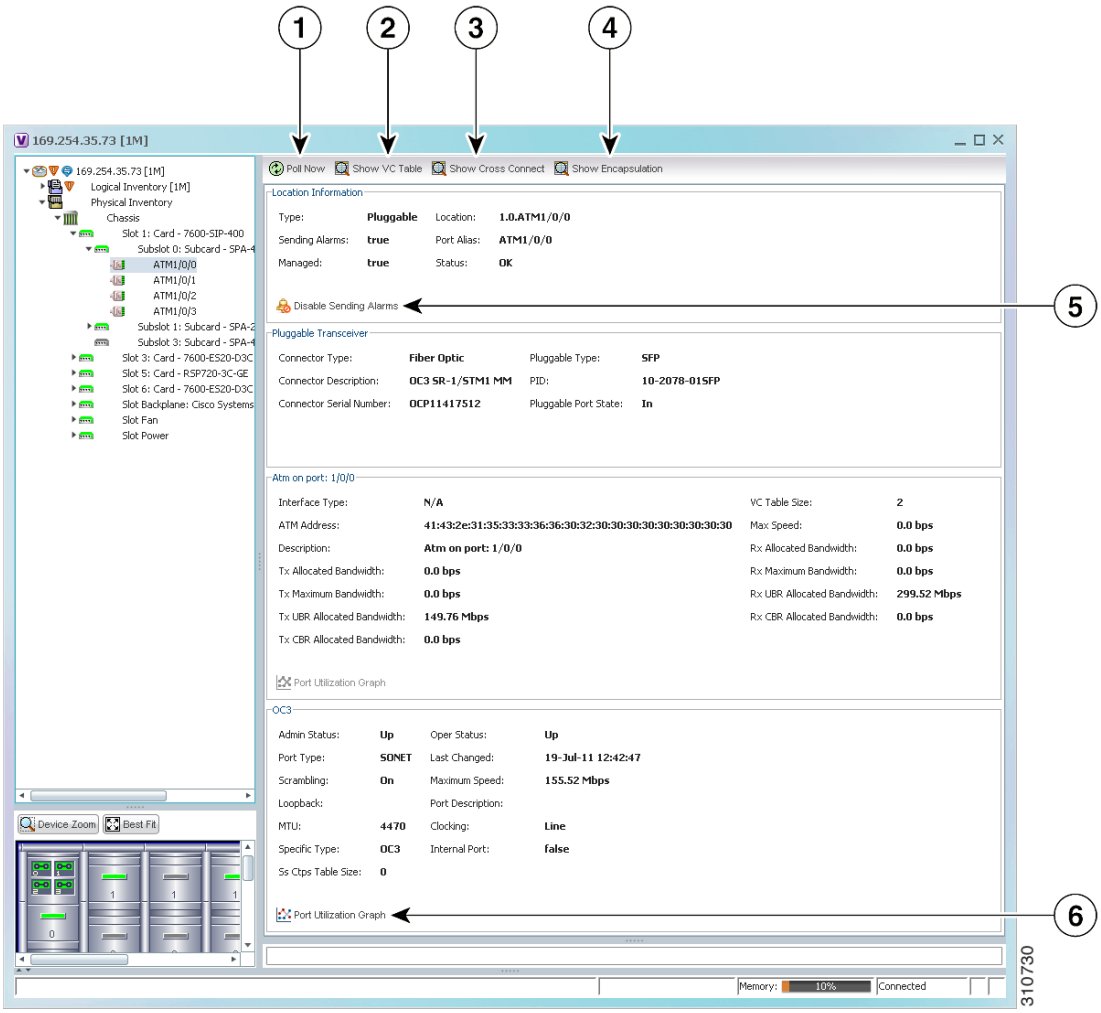
Fans and power supplies are displayed in physical inventory if they are field replacable units (FRUs). The manner in which the fans are displayed depends on whether the fans can be separated or not:

- If the fans under the fan trays are inseparable, only the fan trays are represented.
- If the fans under the fan trays can be separated, they are shown as separate items in physical inventory.

The window displayed for all the devices is similar in appearance. However, the individual sections that are displayed depends on the selected item. For example, when a port that supports pluggable transceivers is selected, the Pluggable Transceiver section is displayed. This section provides information such as the port connector's type and serial number, as well as an indication whether a transceiver is currently plugged in.

Figure 3-6 shows an example of a selection in physical inventory and the available buttons.

Figure 3-6 Physical Inventory Example



1	Poll Now button	Poll the VNE and update the information as needed. For more information, see Updating VNE Information, page 3-12.
2	Show VC Table button	Displays virtual circuit (VC) information for the selected port. For more information, see Viewing ATM VPI and VCI Properties, page 18-10.
3	Show Cross Connect button	Displays cross-connect information for incoming and outgoing ports. For more information, see Viewing ATM Virtual Connection Cross-Connects, page 18-6.
4	Show Encapsulation button	Displays encapsulation information for incoming and outgoing traffic for the selected item. For more information, see Viewing Encapsulation Information, page 18-11.

5	Disable Sending Alarms button	Enables you to manage the alarms on a port. For more information, see Working with Ports, page 3-22.
6	Port Utilization Graph button	Displays the selected port traffic statistics: Rx/Tx Rate and Rx/Tx Rate History. For more information, see Generating the Port Utilization Graph, page 3-27.
—	Show DLCI Table button (not displayed)	Displays data-link connection identifier (DCLI) information for the selected port.

The buttons that are displayed in the physical inventory content pane depend on the selected port.

For information about configuring topology from a port, see Adding Static Links, page 5-15.

For a detailed description of device properties, see Viewing the Properties of a Network Element, page 3-5.

Working with Ports

The following topics describe some of the options available for working with ports:

- Viewing Port Status and Properties, page 3-22
- Viewing a Port Configuration, page 3-24
- Disabling Alarms, page 3-26
- Enabling Alarms, page 3-26
- Generating the Port Utilization Graph, page 3-27

Viewing Port Status and Properties

Prime Network Vision displays all ports on a device in the Ports tab in the inventory window.

This information is available to users with an Operator or higher role on the selected device. Users with a Configurator or higher role can modify the status of a single port or a selected group of ports as described in the following sections:

- Disabling Alarms, page 3-26
- Enabling Alarms, page 3-26

You can export the port list from Prime Network Vision by using the Export to CSV option in the toolbar.

Figure 3-7 shows an example of the Ports tab in the inventory window.

Figure 3-7 Ports Tab in the Inventory Window

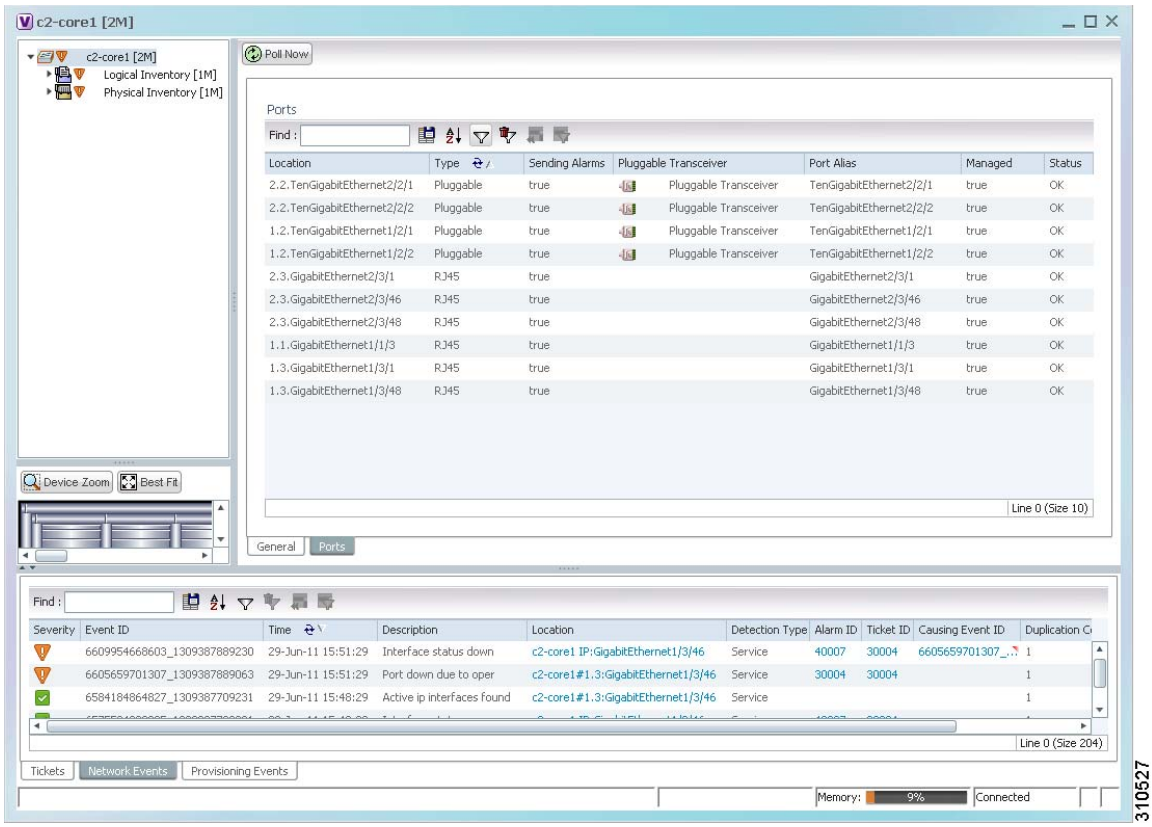


Table 3-9 describes the information that is displayed in the Ports tab.

Table 3-9 Ports Tab in the Inventory Window

Field	Description
Location	Location of the port in the device, using the format *slot.module/port*, such as 1.GigabitEthernet1/14.
Type	Port type, such as RJ45 or Pluggable.
Sending Alarms	Whether or not the port is configured for sending alarms: True or False.
Pluggable Transceiver	For the Pluggable port type, indicates that the port can hold a pluggable transceiver.
Port Alias	Name used in the device CLI or EMS for the port.
Managed	Whether or not the port is managed: True or False.
Status	Port status, such as OK, Major, or Disabled.

Viewing a Port Configuration

In addition to viewing logical inventory information from the logical inventory branch, you can view services provisioned on physical ports by clicking a physical port in the physical inventory branch. Information that is displayed includes:

- Physical layer information.
- Layer 2 information, such as ATM and Ethernet.
- Subinterfaces used by a VRF.

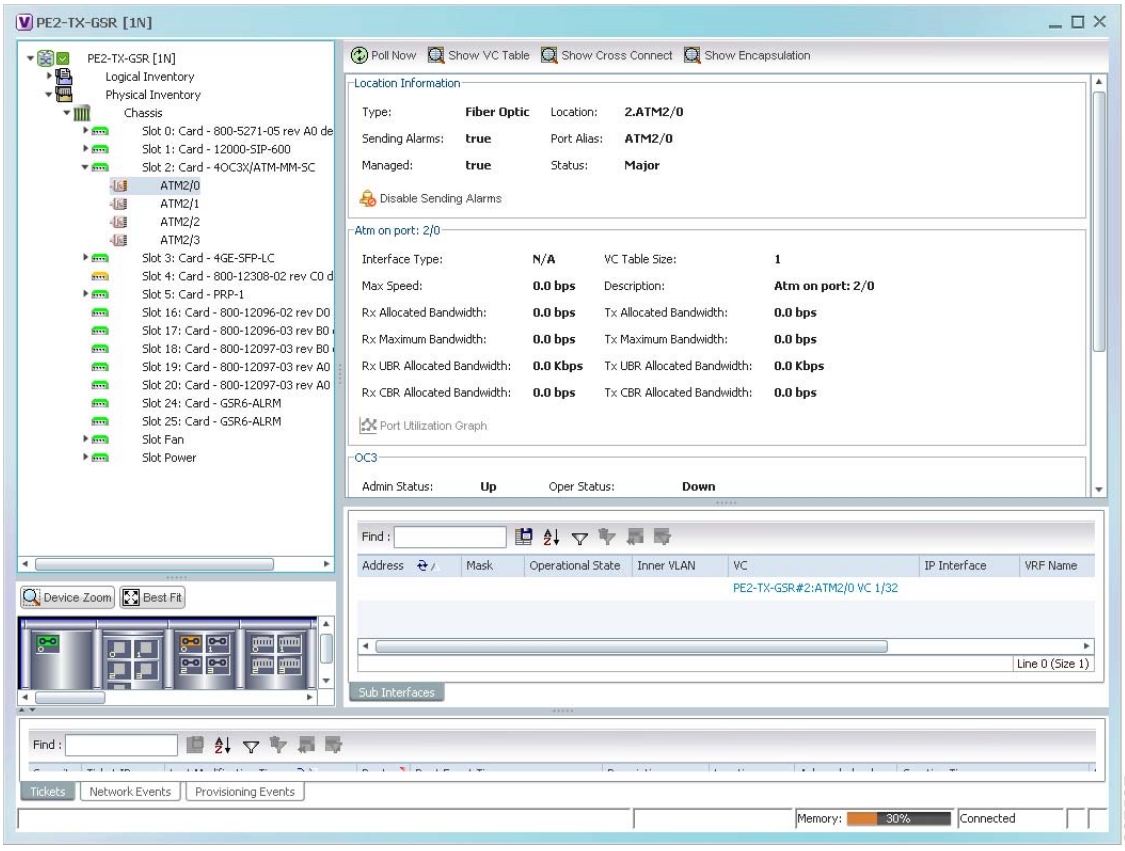
To view a port's configuration:

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

Step 2 In the inventory window, choose **Physical Inventory > Chassis >** *Slot* **>** *Subslot* **>** *Port*.

Figure 3-8 shows an example of the information (including the subinterfaces) displayed when a port is selected in the physical inventory branch of the inventory window.

Figure 3-8 Port Information in the Inventory Window



The subinterface is a logical interface defined in the device; all of its parameters can be part of its configuration. Table 3-10 describes the information that can be displayed in the Subinterfaces table. Not all fields appear in all Subinterfaces tables.

Table 3-10 Subinterfaces Table

Field	Description
Address	IP address defined in the subinterface.
Mask	Subnet mask.
VLAN Type	Type of VLAN, such as Bridge or IEEE 802.1Q. Double-click the entry to view the Port IP VLAN Properties window containing: • VLAN type • VLAN identifier • Operational status • A brief description of the VLAN
Operational State	Operational state of the subinterface.
VLAN ID	VLAN identifier.
Inner VLAN	CE-VLAN identifier.
IP Interface	IP interface, hyperlinked to the VRF properties in the inventory window.
VRF Name	Name of the VRF.
Is MPLS	Whether this is an MPLS interface: True or False.
VC	Virtual connection (VC) configured on the interface, hyperlinked to the VC Table window. For more information about VC properties, see Viewing ATM Virtual Connection Cross-Connects, page 18-6.
Tunnel Edge	Hyperlinked entry to the specific tunnel edge in logical inventory.
Binding	Hyperlinked entry to the specific bridge or pseudowire in logical inventory.

Disabling Alarms

By default, alarms are enabled on all ports. When the alarms are disabled on a port, no alarms are generated for the port and they are not displayed in the ticket and events pane.

To disable alarms on ports:

Step 1 Open the inventory window for the required device.

Step 2 To disable alarms on individual ports, do one of the following:

- In the navigation pane:
  1. Navigate to the required port.
  2. Right-click the required port and choose **Disable Sending Alarms**.
- In the content pane:
  1. Click the **Ports** tab.
  2. Right-click the required port and choose **Disable Sending Alarms**.

In response:

- The Sending Alarms field displays the value *false*, indicating that the alarm for the required port has been disabled.
- The content pane displays the Enable Sending Alarms button.

Step 3 To disable alarms on one or more ports at the same time:

a. In the inventory window, click the **Ports** tab.

b. In the Ports table, select the required ports. You can select multiple ports by using the Ctrl and Shift keys.

c. Right-click one of the selected ports, and choose **Disable Sending Alarms**. In response, the Sending Alarms field displays the value *false* for the selected ports.

Enabling Alarms

You can enable the alarms on a port at any time.

To enable alarms:

Step 1 Open the inventory window for the required device.

Step 2 To enable alarms on individual ports, do one of the following:

- In the navigation pane:
  1. Navigate to the required port.
  2. Right-click the required port and choose **Enable Sending Alarms**.
- In the content pane:
  1. Click the **Ports** tab.
  2. Right-click the required port and choose **Enable Sending Alarms**.

In response:

- The Sending Alarms field displays the value *true*, indicating that the alarm for the required port has been enabled.
- The content pane displays the Disable Sending Alarms button.

Step 3 To enable alarms on one or more ports at the same time:

a. In the inventory window, click the **Ports** tab.

b. In the Ports table, select the required ports. You can select multiple ports by using the Ctrl and Shift keys.

c. Right-click one of the selected ports, and choose **Enable Sending Alarms**. In response, the Sending Alarms field displays the value *true* for the selected ports.

Generating the Port Utilization Graph

Prime Network Vision enables you to view the Rx/Tx Rate and Rx/Tx Rate History of a port.

Note Port utilization graphs are for physical ports only. Port utilization graphs are not available for ATM, E1/T1, or ATM IMA interfaces that are included in an IMA group.

To view port utilization statistics:

Step 1 Open the inventory window and select the required port in physical inventory.

Step 2 In the Ethernet CSMA/CD section, click **Port Utilization Graph**.

The following information is displayed in the Port Statistics dialog box:

- Rx Rate—The reception rate as a percentage.
- Rx Rate History—The reception rate history is displayed as a graph.
- Tx Rate—The transmission rate as a percentage.
- Tx Rate History—The transmission rate history is displayed as a graph.

Step 3 Click  to close the Port Statistics dialog box.

Viewing the Logical Properties of a Network Element

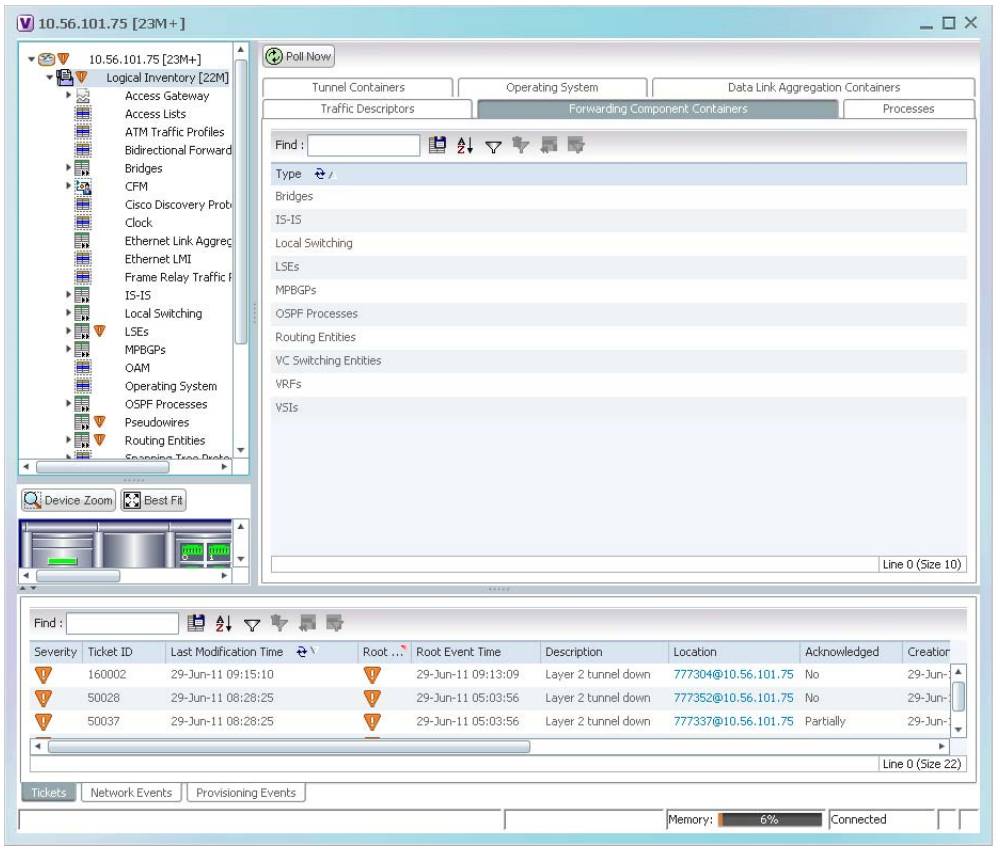
Prime Network Vision enables you to view logical inventory information. Prime Network Vision maintains logical inventory for each network element. The logical inventory reflects dynamic data such as configuration data, forwarding, and service-related components that affect traffic handling in the element.

The information displayed in the inventory window changes according to the type of element and branch selected in the navigation pane.

Logical Inventory Window

Logical inventory information is displayed in the inventory window as shown in Figure 3-9.

Figure 3-9 Logical Inventory Information Displayed in the Inventory Window



Note For more information about opening the inventory window, see Opening the Inventory Window, page 3-12.

Logical Inventory Navigation Pane Branches

Table 3-11 describes the branches that appear in the logical inventory navigation pane.

Table 3-11 Logical Inventory Navigation Pane Branches

This branch...	Provides information about...
6rd	IPv6 rapid development (6rd) tunnels
Access Gateway	Multiple Spanning Tree (MST) and Resilient Ethernet Protocol (REP) access gateways (AGs)
Access Lists	Access lists
ATM Traffic Profiles	Traffic profiles for ATM
Bidirectional Forwarding Detection	Bidirectional Forwarding Detection
BridgeILans	Provider Backbone Bridge (PPB)
Bridges	Configured VLANs
Carrier Grade NAT	Carrier Grade Name Address Translation (NAT)
CFM	Connectivity Fault Management (CFM)
Cisco Discovery Protocol	Cisco Discovery Protocol (CDP)
Clock	Network clock service, clock recovery, and Precision Time Protocol (PTP) configuration
Context Name	Context that is configured on devices that support multiple virtual contexts
Ethernet Link Aggregation	Ethernet aggregation groups
Ethernet LMI	Ethernet Local Management Interface (LMI)
Frame Relay Traffic Profiles	Traffic profiles for Frame Relay
GRE Tunnels	Generic routing encapsulation (GRE) tunneling protocol for IP tunnels
ICCP Redundancy	Inter-Chassis Communication Protocol (ICCP) redundancy groups
IMA Groups	Inverse Multiplexing over ATM (IMA) groups
IP SLA Responder	Cisco IOS Service Level Agreements (SLAs)
IS-IS	Intermediate System-to-Intermediate System (IS-IS) protocol
Link Layer Discovery Protocol	Link Layer Discovery Protocol (LLDP)
Local Switching	Local switching
LSEs	Local switching for MPLS interfaces
MLPPP	Multilink Point-to-Point (MLPPP) configurations
Modular OS	Modular operating systems for Cisco IOX XR devices
MPBGPs	Properties associated with provider edge (PE) network elements. The Multiprotocol Border Gateway Protocols (MP-BGPs) inventory folder contains information such as BGP identifier, local and remote Autonomous System (AS), VRF name, cross-VRF routing, and so on.

Table 3-11 Logical Inventory Navigation Pane Branches (continued)

This branch...	Provides information about...
MPLS-TP	MPLS Transport Profile (MPLS-TP).
OAM	Link operations, administration, and maintenance (OAM).
Operating System	Operating systems for Cisco IOS devices.
OSPF Processes	OSPF processes, such as the Shortest Path First (SPF) timer settings, OSPF neighbors, and OSPF interfaces.
Pseudowires	Pseudowire end-to-end emulation (PW3E) tunnels.
Resilient Ethernet Protocol	Resilient Ethernet Protocol (REP).
Routing Entities	Routing table entries and IP interfaces.
Session Border Controller	Session Border Controller (SBC) configuration.
Spanning Tree Protocol	Spanning Tree Protocol (STP) and Multiple Spanning Tree Protocol (MSTP) configurations.
Traffic Engineering Tunnels	Traffic engineering (TE) tunnels.
Tunnel Traffic Descriptors	Tunnel traffic descriptors associated with the element.
VC Switching Entities	Cross-connects and VC traffic.
VRFs	Virtual Routing and Forwarding (VRF).
VSIs	Virtual Switch Interface (VSI) instance names, associated pseudowire information, virtual circuit IDs, and so on.
VTP	VLAN Trunk Protocol (VTP) domain names, modes, version numbers, and so on.

Logical Inventory Navigation Pane Icons

Each branch in the logical inventory navigation pane is represented by an icon and, if appropriate, includes an icon indicating

Table 3-12 describes the icons used in the logical inventory navigation pane.

Table 3-12 Logical Inventory Navigation Pane Icons

Icon	Logical Inventory Item	
	Access Lists	Modular OS
	ATM Traffic Profiles	OAM
	Bidirectional Forwarding Detection (BFD)	Operating System
	Cisco Discovery Protocol (CDP)	Pseudowire Clock Recovery
	Clock	PTP Service
	Ethernet LMI	Resilient Ethernet Protocol (REP)
	Frame Relay Traffic Profiles	Session Border Controller
	IP SLA Responder	Spanning Tree Protocol
	Link Layer Discovery Protocol (LLDP)	Tunnel Traffic Descriptors

Table 3-12 Logical Inventory Navigation Pane Icons (continued)

Icon	Logical Inventory Item	
	ARP Entity Bridges Ethernet Link Aggregation GRE Tunnels ICCP Redundancy Container IMA Groups IS-IS Local Switching LSEs MLPPP	MP-BGPs Multiple Spanning Tree protocol (MST) instance OSPF Processes Pseudowires Routing Entities Traffic Engineering Tunnels VC Switching Entities VRFs VSIs
	Carrier Grade NAT service VRF	
	Bridge	
	Connectivity Fault Management (CFM)	
	CFM Maintenance Association	
	CFM Maintenance Domain	
	Context, for devices that support multiple contexts	
	Cross-VRF	
	Encapsulation	
	ICCP Redundancy group	
	Inverse Multiplexing over ATM (IMA) group	

Table 3-12 Logical Inventory Navigation Pane Icons (continued)

Icon	Logical Inventory Item
	Label switching
	Layer 2 Tunnel Protocol (TP) peer
	Logical inventory
	Virtual Switch Interface (VSI)
	VLAN Trunk Protocol (VTP)

Logical Inventory Content Pane Tabs

Table 3-13 describes the tabs that are displayed in the logical inventory content pane when you select **Logical Inventory**, depending on the device configuration.

Note Prime Network Vision does not display the tabs in Table 3-13 for devices that support multiple contexts. Instead, when you select **Logical Inventory** for a device that contains multiple contexts, Prime Network Vision displays a Contexts table that lists the contexts configured on the device.

Table 3-13 Logical Inventory Content Pane Tabs

Tab	Description
Data Link Aggregation Containers	Lists the data link aggregations configured on the selected entity, such as Ethernet link aggregations.
Encapsulation Aggregation Containers	Lists the encapsulation aggregations configured on the selected entity.
Forwarding Component Containers	Lists the context profiles for which logical inventory information can be displayed, such as routing entities and bridges.
Operating System	Provides information about the operating system on the selected entity.
Physical Layer Aggregation Containers	Lists aggregations configured at the physical layer for the selected entity, such as IMA groups.
Processes	Lists the processes running on the selected entity, such as Clock or CDP.

Table 3-13 Logical Inventory Content Pane Tabs (continued)

Tab	Description
Traffic Descriptors	Lists the profiles for which logical inventory information can be displayed, such as Frame Relay traffic profiles and Address Resolution Protocol (ARP) entities.
Tunnel Containers	Lists the types of tunnels that are configured on the selected entity, such as pseudowires or GRE tunnels.

Viewing Device Operating System Information

Prime Network Vision discovers and automatically displays operating system information for Cisco IOS, Cisco IOS XR, and Cisco IOS XE devices in logical inventory. For other devices, choose the element name at the top of the inventory window navigation pane.

To view operating system information for Cisco IOS, Cisco IOS XR, or Cisco IOS XE devices:

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

Step 2 For a Cisco IOS device, view information about the operating system in one of the following ways:

- In the inventory window, choose **Logical Inventory > Operating System**.

  Table 3-14 describes the information that is displayed for the Cisco IOS operating system.

Table 3-14 Operating System Information in Logical Inventory

Field	Description
Boot Software	Cisco IOS system image information.
Is K9Sec	Whether or not the K9 security feature is enabled on the operating system: True or False
ROM Version	Cisco IOS bootstrap software version, such as 12.2(33r)SRC3.
OS Version	Cisco IOS software version, such as 12.2(33)SRE, Release Software (fc1).

- Click **Logical Inventory** and choose the **Operating System** tab.

  Figure 3-10 shows an example of the Operating System tab.

Figure 3-10 Operating System Tab in Logical Inventory

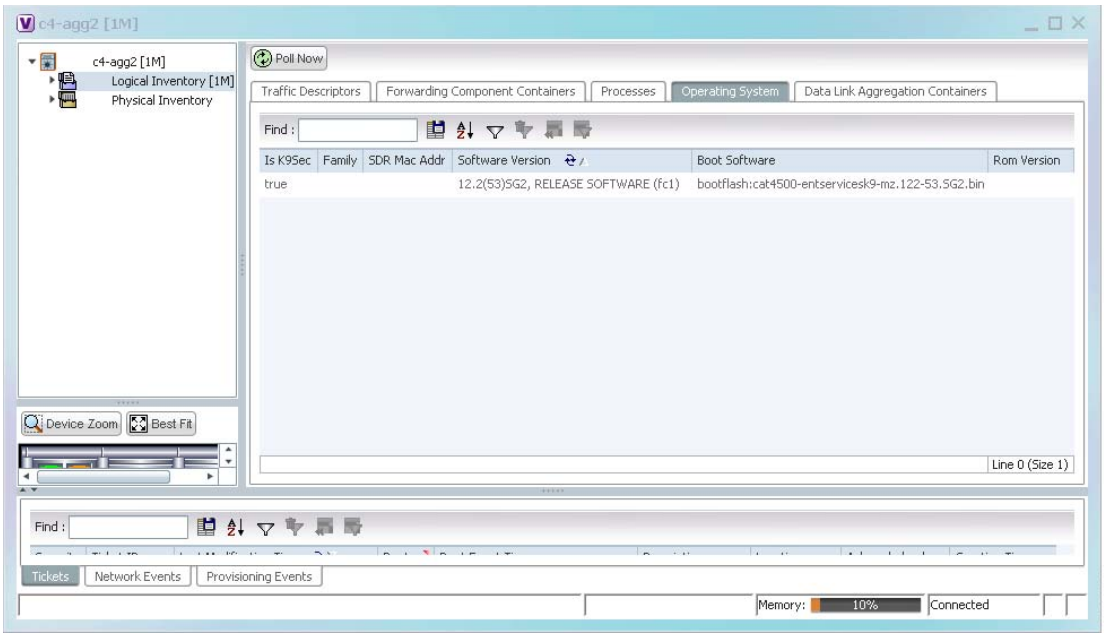


Table 3-15 describes the information that is displayed in the Operating System tab.

Table 3-15 Operating System Information in Logical Inventory

Field	Description
Is K9Sec	Whether or not the K9 security feature is enabled on the operating system: True or False
Family	Cisco family, based on the device platform, such as CRS_IOS or C12K_IOS_XR.
SDR Mac Addr	Secure Domain Router (SDR) MAC address. This field applies to Cisco IOS XR devices only.
Software Version	Cisco IOS software version, such as 12.2(33)SRC3, Release Software (fc2).
Boot Software	Cisco IOS system image information.
ROM Version	Cisco IOS bootstrap software version, such as 12.2(17r)SX3.

Step 3 For a Cisco IOS XR device, view information about the operating system in one of the following ways:

- In the inventory window, choose **Logical Inventory > Modular OS**.

  Figure 3-11 shows an example of the information that is displayed for Cisco IOS XR devices.

Figure 3-11 Modular OS Information in Logical Inventory

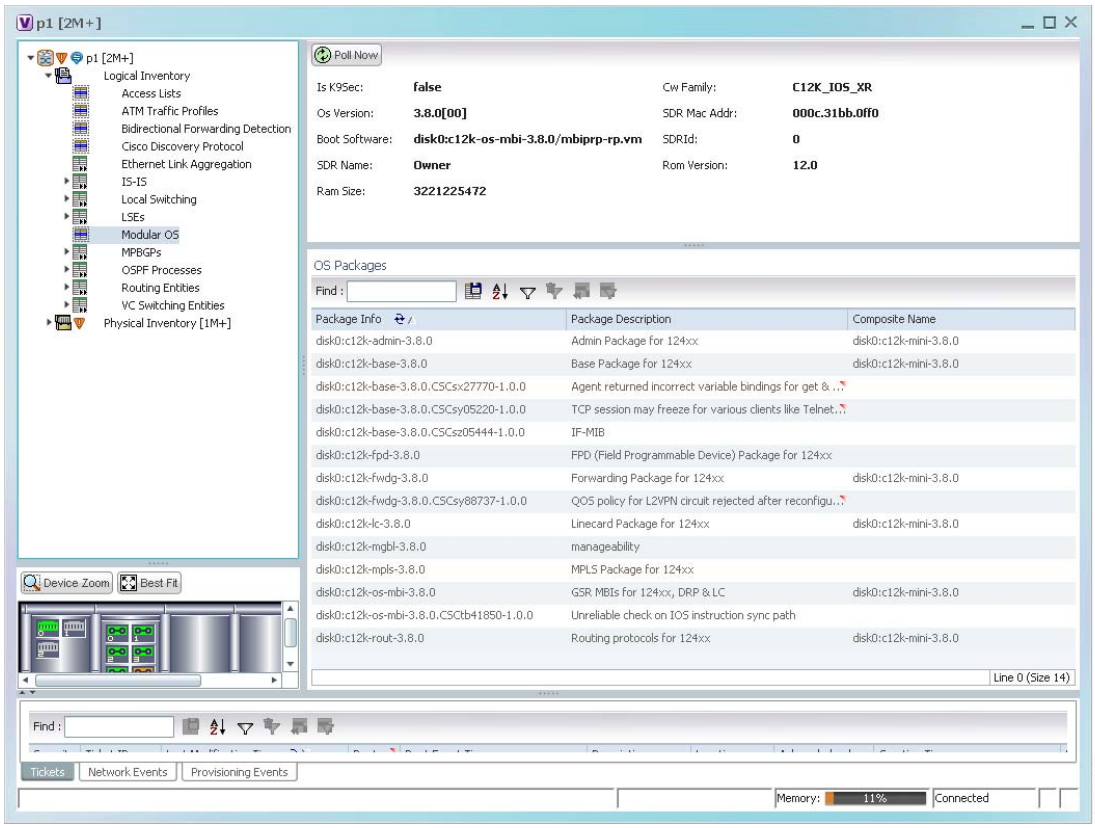


Table 3-16 describes the information that is displayed for Cisco IOS XR system.

Table 3-16 Modular OS Information in Logical Inventory

Field	Description
Is K9Sec	Whether or not the K9 security feature is enabled on the operating system: True or False
Cw Family	Cisco family, based on the device platform, such as CRS_IOS_XR or C12K_IOS_XR.
SDR Mac Addr	Secure Domain Router (SDR) MAC address.
OS Version	Cisco IOS XR software version, such as 3.8.0[00].
Boot Software	Cisco IOS XR system image information.
SDR Name	SDR name.
SDR Id	SDR identifier.
ROM Version	Cisco IOS XR bootstrap software version, such as 1.51.
RAM Size	Size, in kilobytes, of the device processor RAM.

Table 3-16 Modular OS Information in Logical Inventory (continued)

Field	Description
OS Packages Table	
Package Info	Information on the individual package and its version, such as disk0:hfr-admin-3.9.3.14
Package Description	Description of the package, such as FPD (Field Programmable Device) Package.

Composite Name	Composite package name of the package with the date and time, such as:
	`Tues Feb 8 20:37:07.966 UTC`
	`disk0:comp-hfr-mini-3.9.3.14`

- Click **Logical Inventory** and choose the **Operating System tab**.

  Figure 3-12 shows an example of the Operating System tab with information for a device with a modular operating system.

Figure 3-12 Modular OS Information in Operating System Tab

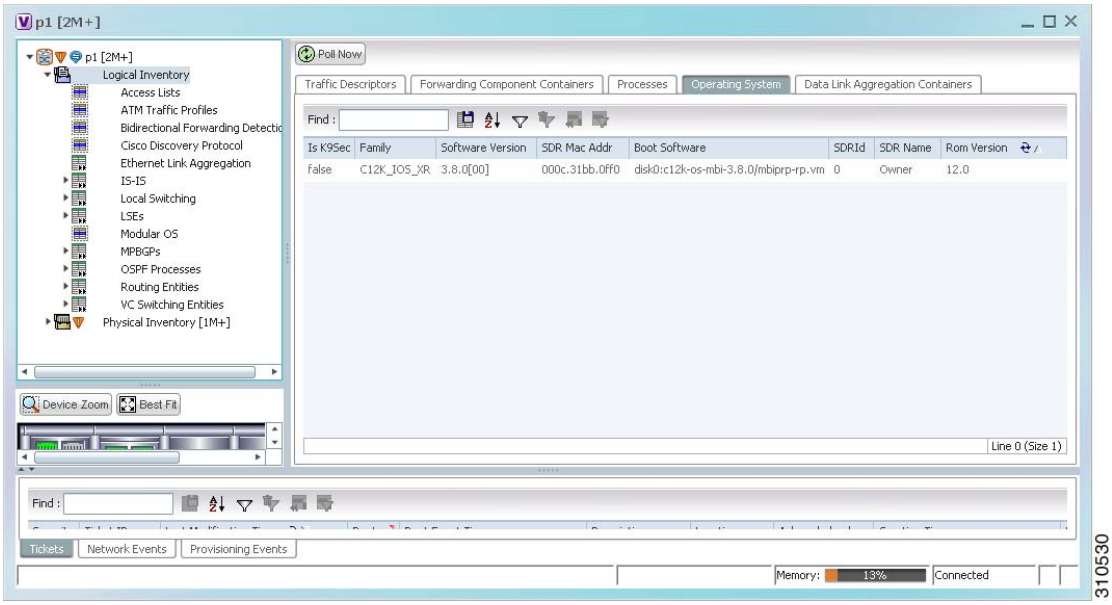


Table 3-17 describes the information that is displayed for modular operating systems in the Operating System tab.

Table 3-17 Modular OS Information in Operating System Tab

Field	Description
Is K9Sec	Whether or not the K9 security feature is enabled on the operating system: True or False
Family	Cisco family, based on the device platform, such as CRS_IOS_XR or C12K_IOS_XR.
Software Version	Cisco IOS XR software version, such as 4.0.0[Default].
SDR Mac Addr	Secure Domain Router (SDR) MAC address.
Boot Software	Cisco IOS XR system image information.
SDR ID	SDR identifier.
SDR Name	SDR name.
ROM Version	Cisco IOS XR bootstrap software version, such as 1.54.



CHAPTER 4

Working with Prime Network Vision Maps

The topological map is the main tool used by Cisco Prime Network Vision (Prime Network Vision) to display the links and relationships between the network elements and aggregations. The following topics describe how to work with the topological maps displayed in the content pane of the Prime Network Vision window:

- User Roles Required for Working with Prime Network Vision Maps, page 4-2
- Using Chinese Characters, page 4-5
- Opening and Closing Maps, page 4-5
- Creating a New Map, page 4-8
- Working with Elements in a Map, page 4-9
- Managing Maps, page 4-16
- Finding Items in a Map, page 4-26
- Working with Aggregations, page 4-28
- Working with Overlays, page 4-33
- Filtering Links in a Map, page 4-38
- Opening the CPU Usage Graph, page 4-40
- Communicating with Devices Using Ping and Telnet, page 4-41

You can also perform the following functions from the map and list views if they are configured for your client:

- Launch external applications or tools, such as an SSH client.
- Launch available activation and configuration scripts. This can include the commands documented in Commands part of the *Cisco Prime Network 3.9 Reference Guide*, and those you create using Command Builder. These scripts can be launched against multiple network elements at the same time.

For more information on these functions, see the *Cisco Prime Network 3.9 Customization User Guide*.

User Roles Required for Working with Prime Network Vision Maps

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

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

For more information on user authorization, see the *Cisco Prime Network 3.9 Administrator Guide*.

The following tables identify the tasks that you can perform:

- Table 4-1 identifies the tasks that you can perform if a selected element **is not in** one of your assigned scopes.
- Table 4-2 identifies the tasks that you can perform if a selected element **is in** one of your assigned scopes.

By default, users with the Administrator role have access to all managed elements. To change the Administrator user scope, see the topic on device scopes in the *Cisco Prime Network 3.9 Administrator Guide*.

Table 4-1 Default Permission/Security Level Required for Working with Prime Network Vision Maps - Element Not in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Map-Related Tasks					
Apply a background image	—	—	—	X	X
Create maps	—	—	X	X	X
Define a map layout	X	X	X	X	X
Delete maps	—	—	X	X	X
Open maps	X	X	X	X	X
Preview and print maps	X	X	X	X	X
Rename maps	—	—	X	X	X
Save as a new map	—	—	X	X	X
Save as an image	X	X	X	X	X
Save map appearance	—	—	X	X	X
Select viewing options	X	X	X	X	X
Use Overview window	X	X	X	X	X
View maps	X	X	X	X	X

Table 4-1 Default Permission/Security Level Required for Working with Prime Network Vision Maps - Element Not in User's Scope (continued)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Element-Related Tasks					
Add elements to a map	—	—	X	X	X
Remove elements from a map	—	—	X	X	X
Resize elements in a map	X	X	X	X	X
Aggregation-Related Tasks					
Group and ungroup aggregations	—	—	X	X	X
Rename aggregations	X	X	X	X	X
View aggregation thumbnails	X	X	X	X	X
Finding Items in Maps					
Find affected elements	—	—	—	—	X
Find an element or service	X	X	X	X	X
Find and select a link in a map[1]	X	X	X	X	X
Link-Related Task					
Filter links	X	X	X	X	X
Overlay-Related Tasks					
Apply an overlay	X	X	X	X	X
Hide or view an overlay	X	X	X	X	X
Remove an overlay	X	X	X	X	X
Other Tasks					
Open the CPU Usage Graph	—	—	—	—	X
Use Ping and Telnet to communicate with elements	—	—	—	—	X

1. This applies to links within the selected context, and not links identified as network links.

Table 4-2 Default Permission/Security Level Required for Working with Prime Network Vision Maps - Element in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Map-Related Tasks					
Apply a background image	—	—	—	X	X
Create maps	—	—	X	X	X
Define a map layout	X	X	X	X	X
Delete maps	—	—	X	X	X
Open maps	X	X	X	X	X
Preview and print maps	X	X	X	X	X
Rename maps	—	—	X	X	X
Save as a new map	—	—	X	X	X
Save as an image	X	X	X	X	X
Save map appearance	—	—	X	X	X
Select viewing options	X	X	X	X	X
Use Overview window	X	X	X	X	X
View maps	X	X	X	X	X
Element-Related Tasks					
Add elements to a map	—	—	X	X	X
Remove elements from a map	—	—	X	X	X
Resize elements in a map	X	X	X	X	X
Aggregation-Related Tasks					
Group and ungroup aggregations	—	—	X	X	X
Rename aggregations	X	X	X	X	X
View aggregation thumbnails	X	X	X	X	X
Finding Items in Maps					
Find affected elements	X	X	X	X	X
Find an element or service	X	X	X	X	X
Find and select a link in a map[1]	X	X	X	X	X

Table 4-2 Default Permission/Security Level Required for Working with Prime Network Vision Maps - Element in User's Scope (continued)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Link-Related Task					
Filter links	X	X	X	X	X
Overlay-Related Tasks					
Apply an overlay	X	X	X	X	X
Hide or view an overlay	X	X	X	X	X
Remove an overlay	X	X	X	X	X
Other Tasks					
Open the CPU Usage Graph	—	—	X	X	X
Use Ping and Telnet to communicate with devices	—	—	—	X	X

1. This applies to links within the selected context, and not links identified as network links.

Using Chinese Characters

Prime Network Vision supports Chinese characters in map and aggregation names, enabling you to name or rename maps or aggregations using Chinese characters. For information on setting up Prime Network to use Chinese characters, see the *Cisco Prime Network 3.9 Installation Guide*.

Opening and Closing Maps

Prime Network Vision provides two methods for opening maps:

- You can open previously viewed maps (if you left the maps open when you last exited Prime Network Vision). See Opening Previously Viewed Maps, page 4-6.
- You can list all existing maps and choose the ones you want to open. See Opening a Map from the Open Map Dialog Box, page 4-6.

For information on how to close a map, see Closing a Map, page 4-8.

When you open a map, the network information is automatically refreshed. For example, if a device was up the last time that the map was saved and closed, and then the device is moved to maintenance, the next time you open the map the management status of the device is updated accordingly and the device displays a maintenance status.

Opening Previously Viewed Maps

When you launch Prime Network Vision, it lists the maps you recently viewed but did not close when you exited the client session. This list of recently viewed maps prevents you from having to view the complete list of available maps, which can be lengthy.

Note This list is not available to first-time users or users who closed their maps before closing the application.

To open a map that you viewed previously but did not close when you last logged out:

Step 1 Launch Prime Network Vision as described in Launching Prime Network Vision, page 2-2. The Prime Network Vision window opens, and the Last Open Maps dialog box is displayed.

Step 2 Check the check boxes for the maps you want to open, and uncheck the check boxes for the maps you do not want to open.

Step 3 Click **OK**.

Opening a Map from the Open Map Dialog Box

You can open any map that is displayed in the Open Map dialog box, even if you have never accessed it before.

To open a map using the Open Map dialog box:

Step 1 Display the Open Map dialog box by doing one of the following:

- Click **Open Map** in the main toolbar.
- Choose **File > Open**.

The Open Map dialog box lists the existing maps, and indicates which maps are currently open in your view.

The Find field enables you to search for a map containing the string that you enter. For more information, see Finding Text in a Table, page 2-51.

You can use the tools described in Table 4-3 to manage maps in the Open Map dialog box.

Table 4-3 Open Map Dialog Box Options

Tool	Name	Description
	Export to CSV	Exports the information displayed in the table. For more information, see Exporting Tables to a File, page 2-55.
	Delete Map	Deletes the selected map from the Open Map dialog box, the Prime Network Vision window, and the database. If a map that is opened is deleted, the map closes. For more information, see Deleting a Map from the Prime Network Vision Database, page 4-25.
	Rename Map	Renames the selected map in the Open Map dialog box and Prime Network Vision window. For more information, see Renaming a Map, page 4-20.
	Sort Table Values	Sorts the information displayed in the table. For more information, see Sorting a Table, page 2-51.
	Filter	Defines a filter for the information displayed in the table. For more information, see Filtering Table Contents, page 2-53. **Note** When a filter is applied, the Clear Filter button is activated.
	Clear Filter	Clears the existing filter.
	Show All Rows	Displays all table rows that meet the current filtering criteria.
	Show Only Selected Rows	Displays only the rows that you select. For more information, see Viewing Selected Rows, page 2-54.

Step 2 Select the maps you want to open using one of the following methods. You can select multiple maps by pressing **Ctrl** while you select individual maps.

- Select the maps in which you are interested, and then click **Open**.
- Right-click the required maps and choose **Open**.
- Double-click the required maps.



Note By default, you can view and work on a maximum of five maps at any given time (per client instance) in the Prime Network Vision window. To change this default setting, contact your Cisco account representative. To create a new map or select a new map, close the required number of maps.

Closing a Map

When you close a map, Prime Network Vision saves basic map information whether or not you manually save the map. This default information includes device and link additions, device and link removals, aggregations, and disaggregations. However, you must use the Save Map option if you want to retain the following information in the database:

- The location of the devices on the map
- Thumbnails
- The size of the devices

To close a map:

Step 1 (Optional) To save more than the default map information, use one of the following methods:

- Click **Save Map Appearance** in the main toolbar.
- Choose **File > Save Map** from the main menu.

Step 2 Do one of the following:

- Choose **File > Close**.
- Click  in the upper right corner of the content pane.

If changes have been made to the map, an information message is displayed.

Step 3 Click **Yes**. The map is saved and closed. An empty Prime Network Vision window is displayed, or the map that was last opened is displayed.

Creating a New Map

Prime Network Vision enables you to create multiple network maps to represent specific network views. Maps can cover specific network segments, customer networks, or any other mix of network elements required. When you create a map, it is available to other users if they have sufficient access and security privileges.

Network maps provide a graphic display of active faults and alarms, and serve as access points for activating services.



Note You cannot specify the same name for two or more maps.

To create a new map:

Step 1 Do one of the following:

- Click **New Map** in the main toolbar.
- Choose **File > New Map** in the main menu.

The Create Map dialog box is displayed.

The Advanced button enables you to filter the links displayed in the map pane. For more information, see Filtering Links in a Map, page 4-38.

Step 2 Enter a name for the new map and click **OK**.

A new empty map is displayed in the navigation pane and map pane.

Step 3 Add elements to your new map as described in Adding Elements to a Map, page 4-9.

For information on removing elements from a map, see Removing Elements from a Map, page 4-15.

Working with Elements in a Map

The following topics describe how to work with elements in a map:

- Adding Elements to a Map, page 4-9
- Resizing Map Elements, page 4-14
- Removing Elements from a Map, page 4-15

Adding Elements to a Map

When you add an element to a map, the map is automatically saved in the Prime Network Vision database.

Note Based on the security level and access permissions assigned, this option might not be available to all users.

To add an element to a map:

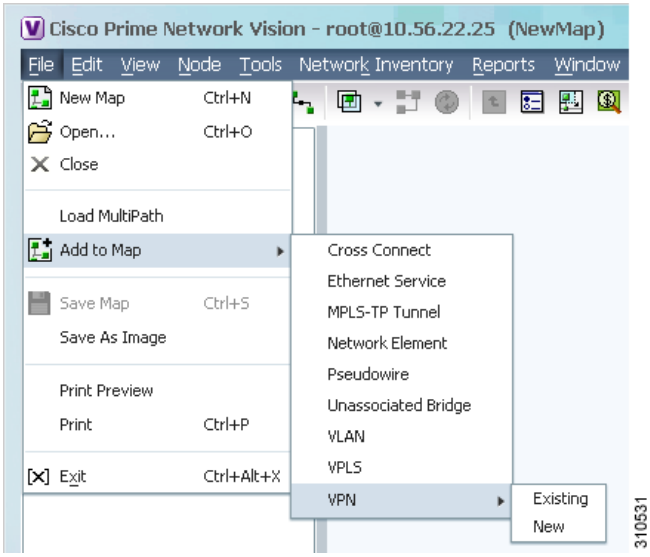
Step 1 Do one of the following:

- Click **Add to Map** in the main toolbar, and choose the required element.
- Choose **File > Add to Map >** *element*.

You can add the following types of elements to maps, as shown in Figure 4-1:

- EFP cross-connects
- Ethernet services
- MPLS-TP tunnels
- Network elements
- Pseudowires
- Unassociated bridges
- VLANs
- VPLS instances
- Existing or new VPNs

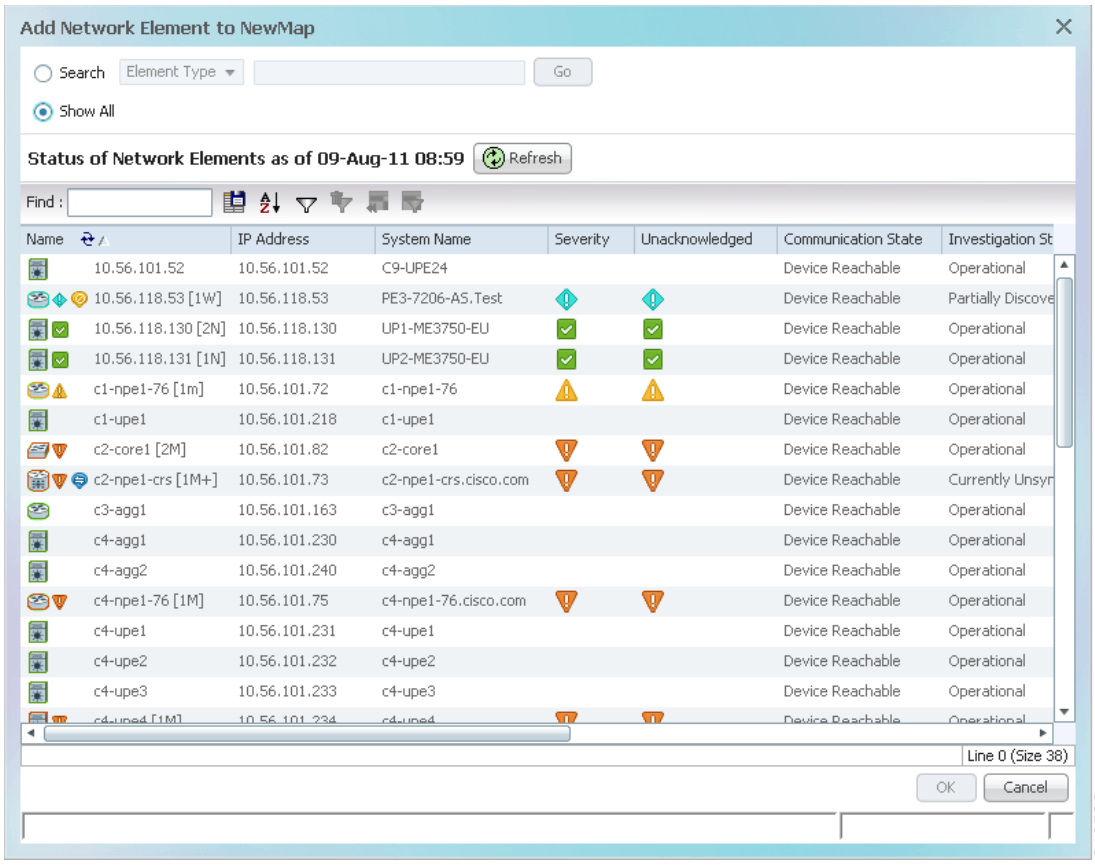
Figure 4-1 Available Elements to Add to Maps



If you choose to add a new VPN, the Create VPN dialog box is displayed. For information on creating a VPN, see Creating a VPN, page 17-21

In all other instances, the Add *element* to *map* dialog box is displayed, as shown in Figure 4-2.

Figure 4-2 Add Element Dialog Box



Step 2 In the Add *element* dialog box, do one of the following:

Note If the element you want to add is outside of your scope, it is not displayed if you enter a search string. Choose **Show All** to view all available elements, both in and out of your scope.

- To view elements that meet specific criteria:

  a. In the Search field, choose a search category. Table 4-4 identifies the search categories available for each element type.

Table 4-4 Network Elements to Add to Maps

Name	Available Search Criteria
Cross-Connect	Name
Ethernet Service	• EVC Terminating EFPs • Name • System Name
MPLS-TP Tunnel	• Description • Name • System Name

Table 4-4 Network Elements to Add to Maps (continued)

Name	Available Search Criteria
Network Element	• Element Category • Element Type • IP Address • Name • System Name • Vendor
Pseudowire	• Description • Is Multisegment Pseudowire • Name • Pseudowire Role • Pseudowire Type • System Name
Unassociated Bridge	Name
VLAN	• EFD Name • EFD System Name • ID • Name • System Name
VPLS	• Name • System Defined Name • VPN ID
VPN > Existing	• Description • Name

b. Enter a search string to narrow the display to a range of elements or to a specific element.

c. Click **Go**.

For example, if you add a network element, choose IP Address, and enter `254`, the network elements with IP addresses containing the string 254 are displayed. If you choose Vendor and enter `Cisco`, only Cisco network elements are displayed.

- To view all available elements, choose **Show All**.

  The following conditions apply when working with large numbers of elements:

  - If the number of elements to be displayed is large, it can take a while for all elements to appear.
  - If the retrieval time for displaying all elements is expected to take a significant amount of time, the Show All button is disabled and the following message is displayed:

    ```
    The Show All option is disabled because the retrieval time is expected to be
    excessive.
    Please define a search that is as specific as possible to minimize the data
    retrieval time.
    ```

    As recommended, use the Search option to specify search criteria and thereby limit the number of elements displayed.

    The number of elements that can be displayed in the Add *element* dialog box is configured in the registry.

    Note Changes to the registry should only be carried out with the support of Cisco. For details, contact your Cisco account representative.

The available elements are displayed in the Add *element* 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**.

If a network 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 Working with Prime Network Tables, page 2-49.

Step 3 In the Add *element* dialog box, select the elements that you want to add. You can select and add multiple elements by pressing **Ctrl** while selecting individual network elements or by pressing **Ctrl + Shift** to select a group of elements.

Step 4 Click **OK**.

If you select more than 25 business elements (such as VLANs or VPLS instances) to add, a message is displayed, stating that the action can take a while to complete and asking if you want to continue. Click **OK** to continue or **Cancel** to change your selection.

The elements are displayed in the navigation pane and content area. In addition, any associated tickets are displayed in the ticket pane.

The network element information is saved with the map in the Prime Network Vision database.

Resizing Map Elements

Prime Network Vision can display network element icons in four sizes. The size that is used when you add elements to a map depends on the number of elements in the map, the map layout, and the size of the content pane.

Icons at the top level of a map have a solid gray border when selected whereas element icons within an aggregation thumbnail have a dashed gray border when they are selected. However, if you double-click the thumbnail frame so that the aggregation fills the map pane and then select an element in the aggregation, the selected element displays a solid gray border.

You can resize element icons in the following ways:

- Using Your Mouse, page 4-14
- Using the Resize Option, page 4-14

Using Your Mouse

To resize a single icon in a map using your mouse:

Step 1 Click the icon you want to resize.

The icon displays a gray border to indicate that it is selected.

Step 2 Position your mouse cursor on the gray border and click and drag the border until the icon is the required size.

Using the Resize Option

Note The Resize option is enabled only when element icons are selected. Links cannot be resized.

To resize icons with the Resize option:

Step 1 In the map, select the icons you want to resize.

Step 2 Do one of the following:

- Choose **Edit > Resize** from the main menu.
- Right-click the required icons in the map, and choose **Resize**.

Step 3 In the Resize Nodes dialog box, set the size of the selected icons in one of the following ways:

- In the By Percentage field, choose the required percentage for resizing the icons from the drop-down list. The available values are 10, 20, 50, 150, and 200.
- In the By Size Category field, choose the required size from the drop-down list. The available sizes are Tiny, Normal, Large, and Huge. To see examples of these sizes, see Table 2-3.

Step 4 Click **OK**. The selected icons are resized.

For more information about the information that is displayed in the element icons, see Information Available in Element Icons, page 3-3.

Using Zoom

Prime Network Vision enables you zoom in or out of maps so that you can use the viewing level that meets your needs. Zooming differs from resizing in that zooming does not change the size of the icon itself.

You can zoom in or out on a map by using either of the following methods:

- Position your mouse cursor in the map pane and use your mouse scroll wheel, as follows:
  - Roll the wheel forward to zoom in on the map.
  - Roll the wheel backward to zoom out on the map.
- Click **Zoom Selection Mode** in the and zoom in and out, as follows:
  - To zoom in, press and hold the mouse button while selecting the area that you want to view in greater detail. Prime Network Vision zooms in on the selected area and centers it in the map pane.
  - To zoom out, click **Normal Selection Mode** in the and do either of the following:

    - Position your mouse cursor in the map pane and use the mouse scroll wheel to zoom out.

    - Click **Fit in Window** to view the entire map in the map pane.

Removing Elements from a Map

When you delete an element or aggregation from a map, it is removed from the map in the database, but the elements are still managed by Prime Network Vision.

Note Based on the security level and access permissions assigned, this option might not be available to all users.

To remove a network element or aggregation from a map:

Step 1 In the navigation pane or map, select the element or aggregation that you want to delete.

Step 2 Right-click to display the right-click menu and choose **Remove from Map**. The selected element or aggregation is removed from the map.

The element is removed from the map in the database, but is still managed by Prime Network Vision and can be added again.

Managing Maps

The following topics describe how to manage maps in Prime Network Vision:

- Selecting Map Viewing Options, page 4-16
- Defining a Map Layout, page 4-17
- Applying a Background Image, page 4-17
- Using the Overview Window, page 4-19
- Renaming a Map, page 4-20
- Saving Maps, page 4-20
- Previewing and Printing a Map, page 4-23
- Deleting a Map from the Prime Network Vision Database, page 4-25

Selecting Map Viewing Options

Table 4-5 describes the tools that you can use to view and manipulate maps in the Prime Network Vision map pane.

Table 4-5 Prime Network Vision Map Viewing Options

Button	Name	Function
	Layout Map	Defines the way in which the map is displayed in the map pane of the Prime Network Vision window: Circular, hierarchical, orthogonal, or symmetric.
	Fit in Window	Fits an entire aggregation or map in the map pane.
	Normal Selection Mode	Activates the normal selection mode.
	Zoom Selection Mode	Activates the zoom selection mode, which enables you to select an area in the map pane to enlarge by clicking and dragging the zoom mode cursor.
	Pan Mode	Activates the pan mode, which enables you to move around in the map pane by clicking and dragging the pan mode cursor.

To select a tool, do one of the following:

- From the View menu, choose the required selection tool.
- In the toolbar, click the required tool icon.

Defining a Map Layout

Prime Network Vision enables you to select the way in which the network object topology is displayed with the following options: Circular, hierarchical, orthogonal, or symmetric.

Select the map layout by using either of the following methods:

- In the toolbar, click the **Layout Map drop-down button**, and choose one of the options.
- Choose **View > Layout** from the main menu and select one of the layout options.

When you choose a map layout, the elements align accordingly, using animation by default. Related characteristics, such as the speed of the animation and whether an expanded node causes sibling nodes to move aside, are also configured by settings in the registry.

Note Changes to the registry should only be carried out with the support of Cisco. For details, contact your Cisco account representative.

By default, Prime Network Vision uses the circular layout for maps. If you click **Layout Map** in the main toolbar, Prime Network Vision displays the map according to the option last selected.

Applying a Background Image

Prime Network Vision allows you to apply a background image to the map view. You can also choose the same background image or different images for other subordinate windows, such as detailed views of aggregations, VLANs, and VPNs.

The supported file formats are GIF, JPG/JPEG, and PNG.

Note Background images are not supported in thumbnail views.

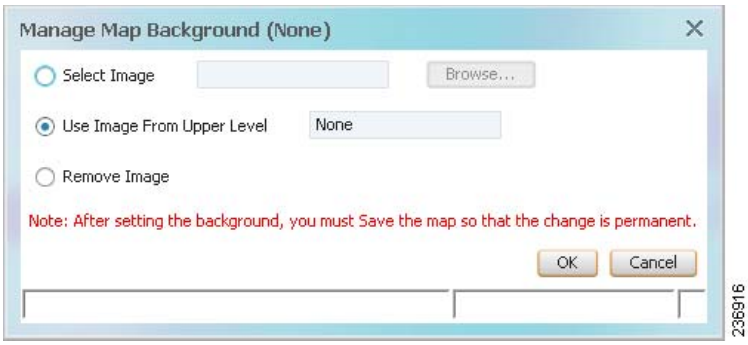
To apply a background image to a map:

Step 1 Navigate to the required map in Prime Network Vision. The map can reside at the top level or in a subordinate window.

Step 2 Right-click the map background and choose **Set Map Background**.

The Manage Map Background dialog box is displayed, as shown in Figure 4-3.

Figure 4-3 Manage Map Background Dialog Box



Step 3 Enter the required information as described in Table 4-6.

Table 4-6 Manage Map Background Options

Field	Description
Select Image	Applies the selected image to the current map background: 1. Choose **Select Image**. 2. Click **Browse**. 3. In the Open dialog box, select the desired image and click **OK**. The name of the selected image is displayed in the Manage Map Background dialog box. 4. Click **OK**. The selected image is displayed as the map background.
Use Image From Upper Level	Indicates whether the selected subordinate map should use the same image as the parent map or a different image: • To use the same image that is used by the parent map, choose **Use Image from Upper Level**. The name of the image used by the parent map is displayed by default. • To use a different image than that used by the parent map, choose **Select Image** and complete the steps described for that option.
Remove Image	Removes the current image from the map background. To remove an image from the current map, click **Remove Image**.

Step 4 Click **OK**. The current map background is updated as specified.

Step 5 To retain the background image for subsequent logins, do one of the following:

- Click **Save** in the toolbar.
- Choose **File > Save**.

Using the Overview Window

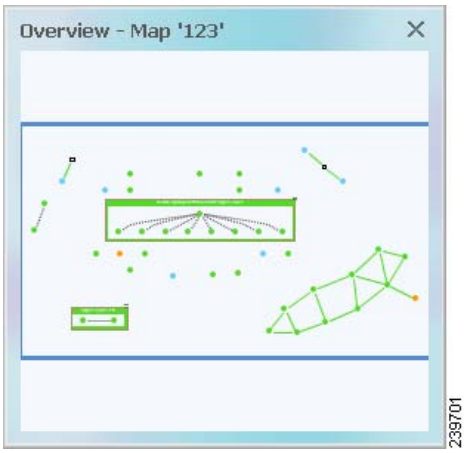
The Prime Network Vision Overview window enables you to display the entire network map or any part of the map that you require in the map pane. The Overview window also enables you to see all the changes and alarms taking place in the network.

To open the network Overview window do either of the following:

- Click **Overview** in the main toolbar.
- Choose **View > Overview** from the main menu.

Figure 4-4 shows an example of the Overview window.

Figure 4-4 Overview Window



The Overview window can contain the following components:

- Dot—Indicates an element. The dot color indicates the severity of an associated alarm.
- Line—Indicates a link. The line color indicates the severity of an associated alarm.
- Blue rectangle—Indicates the selection area. The area within the rectangle is displayed in the map pane. Handles on the corners enable you to resize the selection area.
- Pan mode cursor—Displayed within the selection area. Use this cursor to move the selection area, and thereby view different elements in the map pane.
- Zoom mode cursor—Displayed outside the selection area. Use this cursor to define a new selection area or to zoom in on an existing selection area.

Click the upper right corner to close the Overview window.

Renaming a Map

Prime Network Vision enables you to rename a map that is displayed in the Prime Network Vision window. The name change affects all users of the map and the new name is displayed in the Prime Network Vision window of all users.

To rename a map:

Step 1 Do one of the following:

- Click **Open Map** in the main toolbar.
- Choose **File > Open** from the main menu.

Step 2 In the Open Map dialog box, select the map that you want to rename.

Step 3 Click **Rename Map** in the toolbar.

Step 4 Enter the new map name.

Step 5 Click **OK**. The selected map is renamed in the Open Map dialog box, in the Prime Network Vision window, and in the database.

Step 6 Click **Cancel** to close the Open Map dialog box.

Saving Maps

Prime Network Vision provides three options for saving maps:

- To save more map information than Prime Network Vision saves by default, see Saving a Map with Information, page 4-20.
- To save a copy of a map so that you can use it as a template for another map, see Saving a Map as a New Map, page 4-21.
- To save a map as an image, see Saving a Map as an Image, page 4-21.

Saving a Map with Information

By default, Prime Network Vision saves basic map information whether or not you manually save the map. This default information includes element additions and removals, link additions and removals, aggregations, and disaggregations. However, you must use the Save Map option if you want to retain the following information in the database:

- Device location on the map
- Thumbnails
- Icon size

To save these changes, do one of the following:

- Click **Save Map Appearance** in the main toolbar.
- Choose **File > Save Map**.

Saving a Map as a New Map

You can save a copy of an entire map or parts of a map (such as specific elements and aggregations) while leaving the original map intact.

To save a map or part of a map as a new map:

Step 1 Make sure that the map that you want to save is displayed in the Prime Network Vision content pane.

Step 2 Select the required map, elements, or aggregations in the navigation tree or the map.

Step 3 Right-click in the navigation pane or one of the selected items in the map pane, and choose **Save as New Map**.

Step 4 In the Create Map dialog box, enter a new name for the map.

Step 5 Click **OK**. The new map is created.

For information about opening the new map, see Opening a Map from the Open Map Dialog Box, page 4-6.

Saving a Map as an Image

To save a map as an image:

Step 1 Display the required map in Prime Network Vision.

Step 2 Choose **File > Save As Image** from the main menu.

Step 3 In the Save as Image dialog box, define the image characteristics as described in Table 4-7.

Figure 4-5 Save as Image Dialog Box

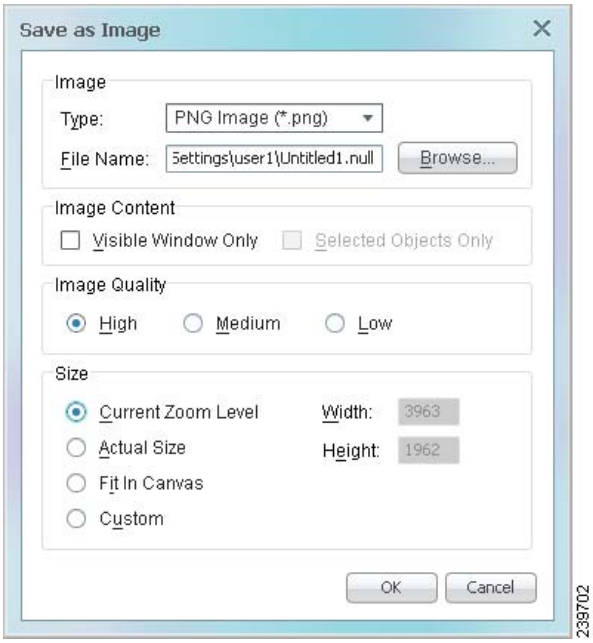


Table 4-7 Save as Image Dialog Box Options

Attribute	Description
Image	Specify the image type and filename: • Type—In the drop-down list, select one of the following file types: – GIF Image (*.gif) – JPEG Image (*.jpg) – PDF Document (*.pdf) – Portable Network Graphics (*.png) – Scalable Vector Graphics (*.svg) • File Name—Browse to the required location and enter a filename for the image.
Image Content	Check the appropriate check box for the content to be included in the image: • Visible Window Only—Saves the currently selected map as an image, even if the content area displays the list view or the links view. The option is enabled only if Current Zoom Level is selected for the Size attribute. • Selected Objects Only—Saves the selected network objects as an image. This option is enabled only if network objects are selected in the content pane.
Image Quality	Select the required image quality level: • High • Medium • Low
Size	Specify the required zoom level for the image: • Current Zoom Level—Saves the image at the currently selected zoom level. Selecting this option enables the Visible Window Only check box. • Actual Size—Saves the image at the actual size. • Fit in Canvas—Saves the image so that it fits in the canvas. • Custom—Saves the image at an enlarged or reduced size. Selecting this option enables the Width and Height options, so that you can enter the required size in pixels.

Step 4 Click **OK**. The map is saved as an image in the directory you specified.

Previewing and Printing a Map

To print a map, choose **File > Print**. If you would like to preview a map before printing it, or define the print setup for a map, see the following topics:

- Previewing a Map Before Printing It, page 4-23
- Defining the Print Setup for a Map, page 4-23

Previewing a Map Before Printing It

Using Prime Network Vision, you can preview a map before printing it.

To preview a map:

Step 1 In Prime Network Vision, display the map that you want to print.

Step 2 From the main menu, choose **File > Print Preview**. The Print Preview window is displayed with the active map.

The following buttons are displayed in the Print Preview window:

Button	Name	Description
	Print Setup	Opens the Printer Setup dialog box so you can specify your print settings.
	Print	Opens the Print dialog box so you can print the displayed network or map to the required printer.
	Zoom In	Zooms in on the network or map.
	Zoom Out	Zooms out of the network or map.
	Fit	Displays the entire network or map in the Print Preview window.

Step 3 Click **Print**. The required map is printed to the selected printer.

Defining the Print Setup for a Map

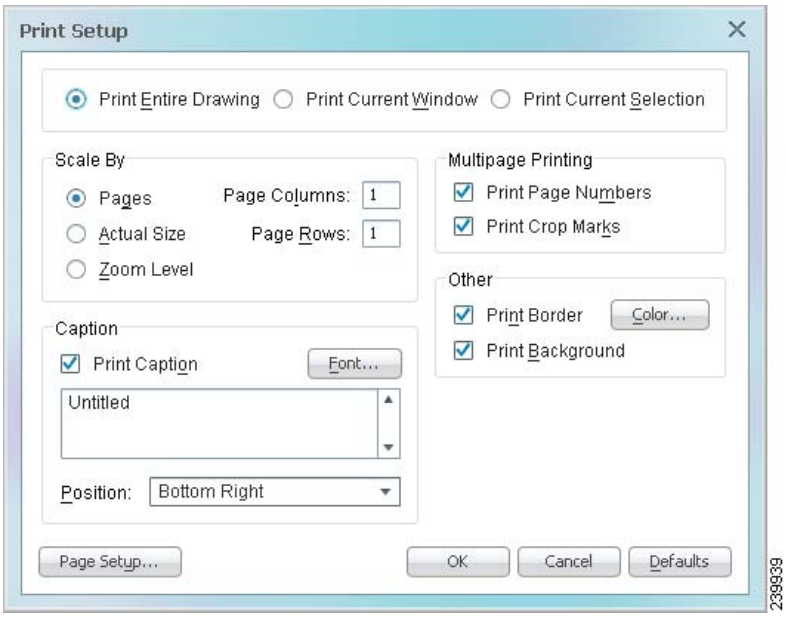
Prime Network Vision enables you to define the print setup of a map before it is printed.

To define the print setup:

Step 1 From the main menu, choose **File > Print Preview** to open the Print Preview dialog box.

Step 2 Click **Print Setup**. The Print Setup dialog box is displayed.

Figure 4-6 Print Setup Dialog Box



Step 3 Define the print setup, using the information in Table 4-8.

Table 4-8 Print Setup Dialog Box Options

Option	Description
Print Selection	
Print Entire Drawing	Prints the currently displayed map, including aggregations.
Print Current Window	Prints the currently displayed map, excluding aggregations.
Print Current Selection	Prints the area selected in the currently displayed map.
Scale By	
Pages	Prints the currently displayed map according to the numbers specified in the Page Columns and Page Rows fields.
Actual Size	Prints the currently displayed map at the actual size.
Zoom Level	Prints the currently displayed map according to the selected zoom level.
Caption	
Print Caption	Adds the specified caption to the printed map.
Font	Specifies the font to use for the caption.
Caption	Prints the text entered in this field as the caption.
Position	Defines the position of the caption in the printed map.

Table 4-8 Print Setup Dialog Box Options (continued)

Option	Description
Multipage Printing	
Print Page Numbers	Prints the map with page numbers.
Print Crop Marks	Prints the map with crop marks.
Other	
Print Border	Prints a border around the printed map.
Color	Displays the Choose Color dialog box so you can select the border color.
Print Background	Prints the background of the currently displayed map.
Page Setup	
Page Setup	Offers standard printer options, such as printing in portrait or landscape mode and setting margin widths.

Step 4 Click **OK** to save your settings, or **Default** to restore the default settings.

The Print Preview dialog box is refreshed with the current settings.

Step 5 If you are satisfied with your settings, click **Print**. Otherwise, click **Print Setup** and revise your settings.

Deleting a Map from the Prime Network Vision Database

Prime Network Vision enables you to delete a map from all the views in the Prime Network Vision window.

If another client is using a map that you are deleting, Prime Network Vision displays a message to those clients advising them that the map is being closed and deleted from the database.

To delete a map from Prime Network Vision and the Prime Network Vision database:

Step 1 Open the Open Map dialog box in one of the following ways:

- Click **Open Map** in the main toolbar.
- Choose **File > Open** from the File menu.

Step 2 In the Open Map dialog box, complete the following steps:

a. Select the map you want to delete.

b. In the toolbar, click **Delete Map**. A confirmation message is displayed.

c. Click **Yes**. The selected map is deleted from the Open Map dialog box, the Prime Network Vision window, and the database. If the map is open when you click **Yes**, a message is displayed, stating that the map will be closed.

d. Click **OK** to acknowledge that the map can be closed.

e. Click **Cancel** to close the Open Map dialog box.

Finding Items in a Map

The following topics describe how to find network elements, services, links, or elements affected by a ticket in Prime Network Vision maps:

- Finding a Network Element or Service, page 4-26
- Finding and Selecting Links in Maps, page 4-27
- Finding Elements Affected by a Ticket, page 4-27

Finding a Network Element or Service

Prime Network Vision enables you to find an element or service (such as a VPN or VLAN) in the map by entering the element or service name, the device IP address, or any part of the name or IP address.

To find an element or service in a map:

Step 1 Do one of the following:

- Click **Find** in the main toolbar.
- Choose **Edit > Find in Map** from the main menu.

Step 2 In the Find in Map dialog box, enter the device name or the IP address.

Note You can enter a partial name (case insensitive) or IP address. For example, entering **`xy`** finds elements or services with names containing the string xy, such as Axy, Xy, xY, or xyZ.

The Search all map levels check box enables you to search for an element, name, or IP address at all levels of the map. When disabled, this option searches for the element or service, but excludes aggregations from the search. This option is disabled by default.

Step 3 Check or uncheck the Search all map levels check box, as required.

Step 4 Click **OK.** An element or service matching the search criteria is selected in the map.

Step 5 Continue searching using the following methods:

- To view the next element or service that matches the search criteria, click **Find Next** in the or press **F3**.
- To view the previous element or service that matches the search criteria, click **Find Previous** in the or press **Shift + F3**.

Finding and Selecting Links in Maps

Prime Network Vision enables you to find a specific link and select it in a map. If more than one edge device contains the same link in the same map or context, all related edge devices are selected in the map.

To find and select a link:

Step 1 In the Links view, right-click the required link and choose **Select Link in Map**.

The link is highlighted in the map pane.

Step 2 If two or more lines represent the same link (such as a VRF link), the Select Link Context dialog box is displayed. Select the required link context from the drop-down list and click **OK**. The link is highlighted in the map pane.

Step 3 Click in the map background to remove the highlight from the selected link.

For more information about links in Prime Network Vision, see Chapter 5, "Working with Links."

Finding Elements Affected by a Ticket

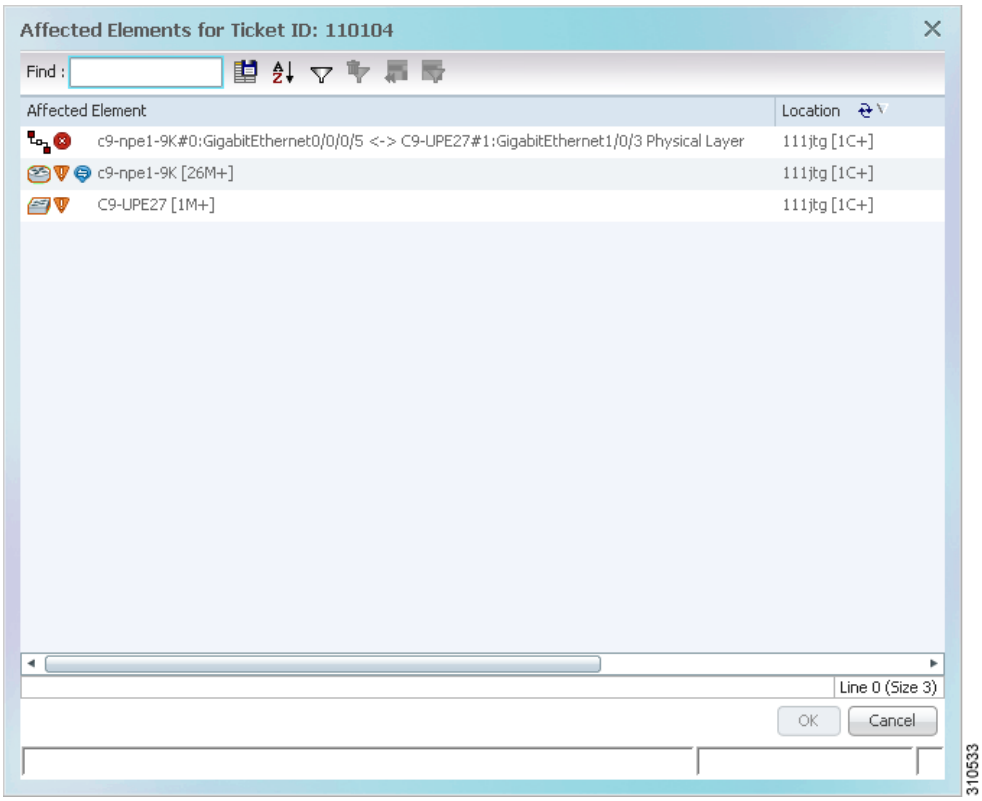
Prime Network Vision enables you to find the elements that might be affected by a ticket displayed in the ticket pane.

To find elements affected by a ticket:

Step 1 In the ticket pane, right-click the required ticket and choose **Find Affected Elements**. Depending on the number of affected elements, the information is displayed in one of the following ways:

- If only one element is affected, the affected element is selected in the navigation pane and the content area.
- If a link is affected, the affected link is selected in the links view.
- If two or more elements are affected, the affected elements are displayed in the Affected Elements window as shown in Figure 4-7.

Figure 4-7 Affected Elements Window



Step 2 In the Affected Elements window, select the required element, then click **OK**. The selected element is selected in the Prime Network Vision map or links view.

Step 3 Click in the navigation pane or the map pane to remove the highlight from the selected device or link.

Working with Aggregations

Prime Network Vision enables you to group network elements and display them as an aggregation. Aggregations can contain network elements, services, other aggregations, and so forth.

Note You cannot aggregate service entities that exist within a service. For example, you cannot aggregate VRFs that exist within a VLAN.

For more information on working with aggregations, see the following topics:

- Grouping Network Elements into Aggregations, page 4-29
- Adding Elements to an Existing Aggregation, page 4-30
- Viewing an Aggregation Thumbnail, page 4-30
- Ungrouping Aggregations, page 4-33
- Renaming Aggregations, page 4-32

Grouping Network Elements into Aggregations

To aggregate network elements:

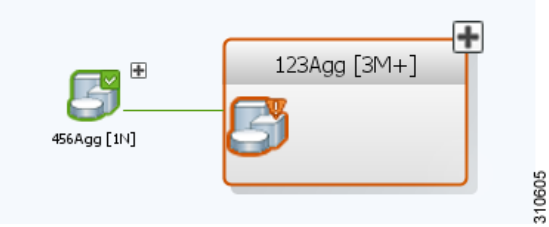
Step 1 Select the network elements using one of the following methods:

- Select a single item in the map pane or navigation tree.
- Select multiple items in the map pane or navigation tree while pressing **Ctrl**.

Step 2 Aggregate the network elements using one of the following methods:

- In the menu bar, choose **Node > Aggregate**.
- Right-click the navigation pane and choose **Aggregate**.
- In the map pane, right-click one of the selected items and choose **Aggregate**.

Step 3 In the Aggregation dialog box, enter a unique name for the aggregation and click **OK**. The aggregation is displayed in the navigation pane and the map pane. Aggregations are displayed as a single entity with the Aggregation icon and a plus sign, as in the following examples:



The aggregation icon changes color according to the alarm severity. For more information about severity colors, see Alarm Indicators, page 2-17.

Adding Elements to an Existing Aggregation

You can add elements to an existing aggregation at any time. When adding elements to an aggregation, keep in mind that certain restrictions exist. For example, you cannot add an EVC to a VLAN.

To add elements to an existing aggregation:

Step 1 Select the existing aggregation in the map pane.

Step 2 Navigate to the required aggregation thumbnail in either of the following ways:

- Click the plus sign in the upper right corner of the aggregation icon.
- Right-click the aggregation, and choose **Show Thumbnail**.

Step 3 When the required aggregation thumbnail is open, double-click the thumbnail frame to view the aggregation at the map level.

Step 4 Click **Add to Map** to add the required element to the aggregation.

Step 5 To return to the map, do one of the following:

- Double-click the map background.
- Right-click the cursor in the map background, and choose **Go to Root**.
- Click **Go to Parent** in the toolbar. Depending on the number of nested aggregations, you might need to do this more than once.

Viewing an Aggregation Thumbnail

You can view a thumbnail of a selected aggregation in the map pane, including all aggregated elements and any nested aggregations.

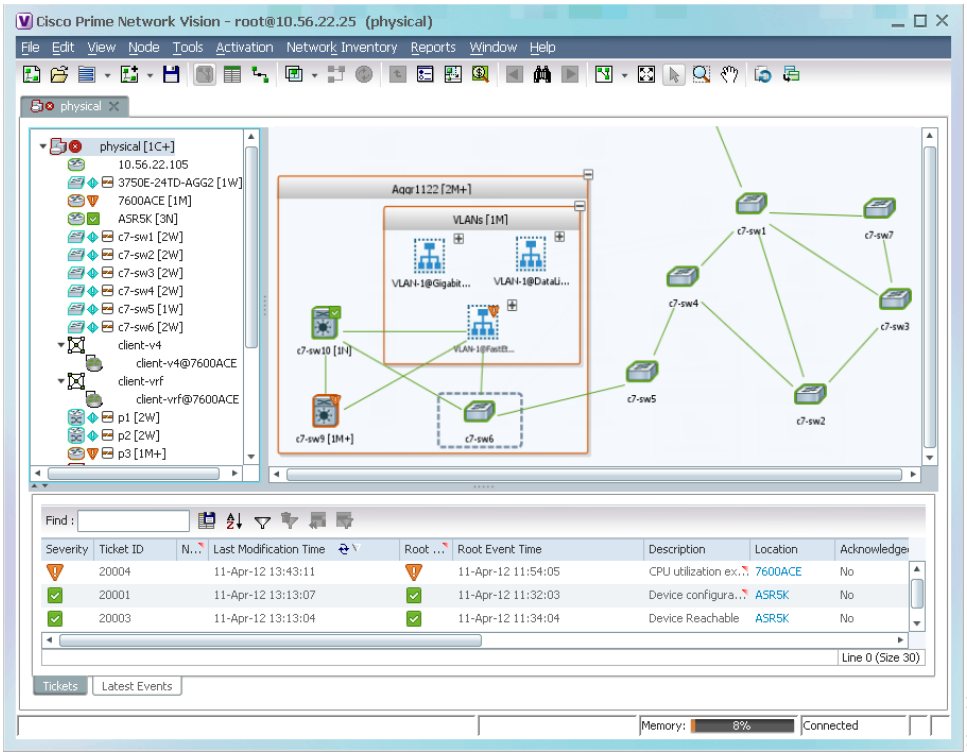
To display an aggregation thumbnail:

Step 1 Open the thumbnail in either of the following ways:

- Click the plus sign in the upper right corner of the aggregation icon.
- Right-click an aggregation, and choose **Show Thumbnail**.

The thumbnail is displayed in the map pane as shown in Figure 4-8.

Figure 4-8 Aggregation Thumbnail



When a thumbnail is opened, neighboring nodes are moved aside by default to allow room for the thumbnail to expand. Similarly, when a thumbnail is closed, the neighboring nodes usually return to their original locations. This behavior of the neighboring nodes when a thumbnail is opened and closed is configured in the registry, and can be disabled, if required.

Note Changes to the registry should only be carried out with the support of Cisco. For details, contact your Cisco account representative.

A dashed gray border around an icon indicates that the element resides within a thumbnail and not at the current map level.

Table 4-9 describes the options available when working with aggregation thumbnails.

Table 4-9 Aggregation Thumbnail Options

If you want to...	Do this...
Rearrange the icons in the thumbnail	Click and drag the required icons to arrange them as needed.
Resize an icon	Select the icon to be resized, and then either click and drag the gray border or right-click a selected icon and choose **Resize**. The right-click Resize option allows you to resize multiple selected icons at the same time.
Resize the thumbnail frame	Click and drag one or more icons. If you drag an icon beyond the thumbnail frame, Prime Network Vision adjusts the thumbnail size automatically.
View a nested aggregation	Click the nested aggregation plus sign.
View only the aggregation in the map pane	Double-click the thumbnail frame.
View the next higher level in the map pane	Double-click the current map background.
Zoom in or out in the thumbnail	Position your mouse cursor in the map and use the mouse scroll wheel to zoom in or out.

Step 2 To close the aggregation thumbnail, do either of the following:

- Click the minus sign in the upper right corner of the thumbnail frame.
- Right-click the thumbnail frame and choose **Show As Aggregation**.

Renaming Aggregations

You can rename aggregations that are displayed in Prime Network Vision. The name change affects all users of the map, and the new name is displayed in the Prime Network Vision window of all users.

To rename an aggregation:

Step 1 Select the aggregation that you want to rename in the navigation tree or the map.

Step 2 Right-click the aggregation icon and choose **Rename**.

Step 3 In the Rename Node dialog box, enter a new name for the aggregation and click **OK**. The selected aggregation is renamed in the navigation tree, map pane, and database.

Ungrouping Aggregations

Aggregations can be ungrouped. If the aggregation that you ungroup contains nested aggregations, the nested aggregations move up one level, and the original aggregation is removed.

If an element in the aggregation that you ungroup also exists at the parent level, the element is represented only once after the aggregation is ungrouped. As a result, no elements are represented twice at the same level.

To ungroup an aggregation:

Step 1 Select the required aggregation in Prime Network Vision.

Step 2 Ungroup the node in one of the following ways:

- Select the aggregation in the map pane, and choose **Node > Disaggregate**.
- Right-click the aggregation in the navigation tree or map pane, and choose **Disaggregate**.
- If the aggregation is shown in the thumbnail view, right-click the thumbnail frame and choose **Disaggregate**.

If the aggregation contains elements that already exist at the parent level, a confirmation message is displayed, stating that any duplicate elements will be removed.

Step 3 Confirm the disaggregation.

The node is disaggregated. Any aggregations in the selected node move up one level, and the original aggregation is removed.

For more information about resizing aggregation icons, see Resizing Map Elements, page 4-14.

Working with Overlays

Prime Network Vision enables you to apply overlays to a map and thus isolate the parts of a network that are being used by a specific service.

The following topics discuss the overlay options in more detail:

- Applying an Overlay, page 4-34
- Hiding or Viewing an Overlay, page 4-37
- Removing an Overlay, page 4-37

Applying an Overlay

To apply an overlay:

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

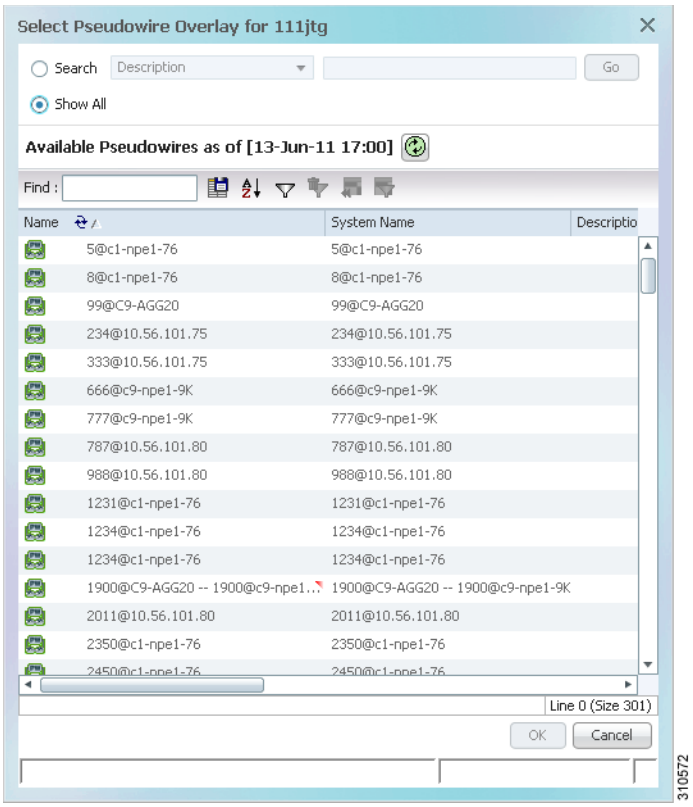
Step 2 From the toolbar, choose **Choose Overlay Type >** *overlay-type* where *overlay-type* is one of the following options:

Overlay Option	Description
Ethernet Service	Applies an Ethernet service overlay to the map.
MPLS-TP Tunnel	Applies and MPLS-TP tunnel overlay to the map.
Network Clock	Applies a network clock overlay to the map.
None	Removes any existing overlays on the map.
Pseudowire	Applies a pseudowire overlay to the map.
VLAN	Applies a VLAN overlay to the map.
VPLS	Applies a VPLS instance overlay to the map.
VPN	Applies a VPN overlay to the map.

With the exception of the None option, a dialog box is displayed that allows you to select the specific overlay to apply.

Figure 4-9 shows an example of the Select Pseudowire Overlay dialog box.

Figure 4-9 Select Overlay Dialog Box



Each overlay type allows you to search for specific overlays. Table 4-10 identifies the search fields available for each overlay type.

Table 4-10 Overlay Type Search Fields

Overlay Type	Search Fields
Ethernet Service	• EVC Terminating EFPs • Name • System Name
MPLS-TP Tunnel	• Description • Name • System Name
Network Clock	• Name
Pseudowire	• Description • Is Multisegment Pseudowire • Name • Pseudowire Role • Pseudowire Type • System Name

Table 4-10 Overlay Type Search Fields (continued)

Overlay Type	Search Fields
VLAN	• EFD Name • EFD System Name • ID • Name • System Name
VPLS	• Name • System Defined Name • VPN ID
VPN	• Description • Name

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

- To search for specific overlays:

  a. Choose **Search**.

  b. In the Search field, choose a search category.

  c. Enter a search string to narrow the display to a range of overlays or to a specific overlay. Table 4-10 identifies the search categories available for each type of overlay.

  d. Click **Go**.

  Search strings are case-insensitive. If you choose Name and enter **`NET`**, the overlays that contain "net" in their names are displayed. If you choose System Name and enter **`System123`**, only the overlay with the system named System123 is displayed.

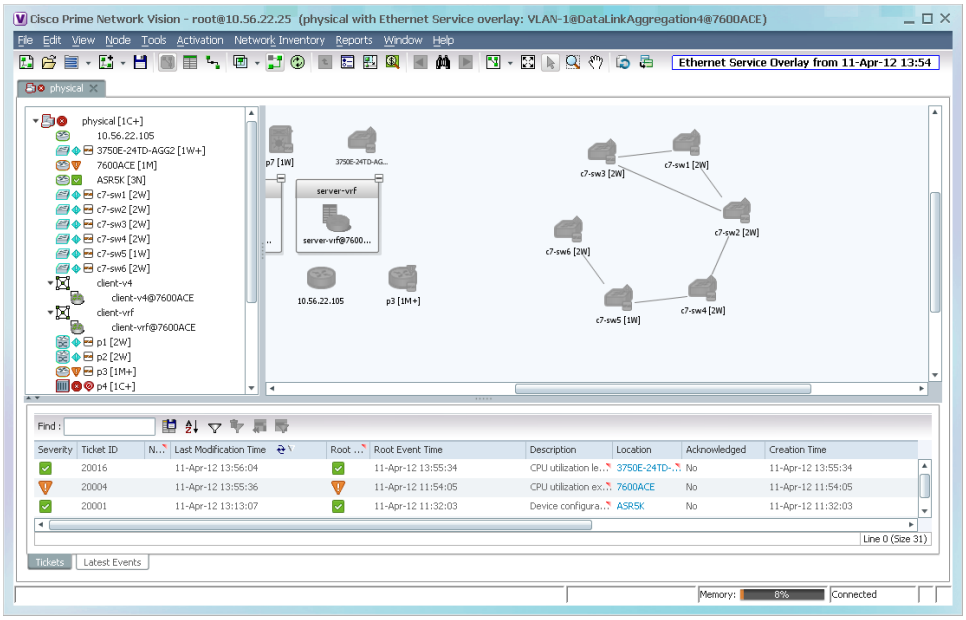
- To view all available overlays, choose **Show All**.

The available overlays that meet the specified search criteria are displayed in the Select Overlay 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**.

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

The elements and links that are used by the overlay are displayed in the map, and the overlay name and date are displayed in the toolbar, as shown in Figure 4-10.

Figure 4-10 Overlay Example



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

Hiding or Viewing an Overlay

When an overlay is applied to a map, the Show Overlay/Hide Overlay button becomes active in the toolbar.

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.

Removing an Overlay

To remove an overlay, choose **Choose Overlay Type > None**. The overlay is removed from the map.

Filtering Links in a Map

The links filter enables you to filter the links displayed in the map view and the links view.

You can quickly select the types of links to be filtered by selecting from a predefined set of link types in the list, or by manually configuring a customized set of link types.

To filter links, do either of the following:

- Create a new map, select a filter, and then add the devices to the map. This filter is applied to the new map and only the required link types are visible in the map view and the links view. For more information, see Filtering Links During Map Creation, page 4-38.
- Create a map and add the devices with all links enabled and visible in the map view and links view. You can then filter (display or hide) the different types of links as required. For more information, see Filtering Links in an Existing Map, page 4-40.

The links filter applies to all aspects of Prime Network Vision: the map view, links view, ticket pane, severity calculation, and other items, such as memory consumption and thresholds. Prime Network Vision holds only the links that are relevant to the filter and synchronizes the links with the gateway according to that filter.

For more information about links in Prime Network Vision, see Chapter 5, "Working with Links."

Filtering Links During Map Creation

To filter links while creating a map:

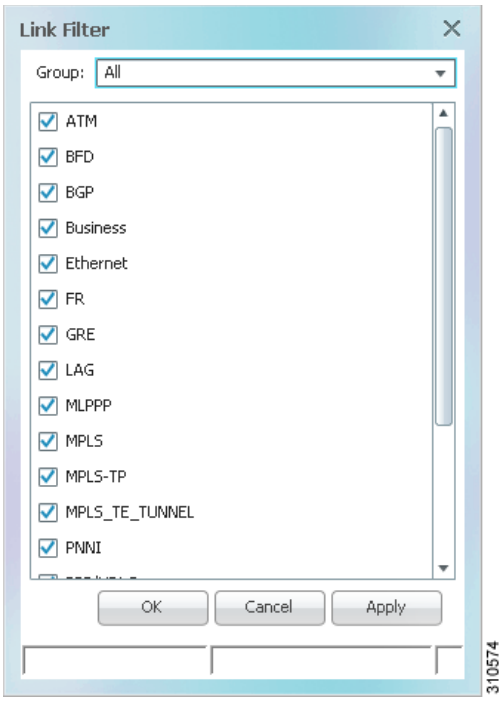
Step 1 Open the Create Map dialog box using one of the following methods:

- Click **New Map** in the main toolbar.
- Choose **File > New Map** from the main menu.

The Create Map dialog box is displayed. For more information, see Creating a New Map, page 4-8.

Step 2 Click **Advanced**. The Link Filter dialog box is displayed.

Figure 4-11 Link Filter Dialog Box



The Link Filter dialog box displays a list of all the types of links that you can filter in the map view and links view.

Note By default all link types are selected in the Link Filter dialog box. That is, all links are displayed in the map view and links view.

Step 3 Select the required option from the Group drop-down list:

- All—All the links are displayed in the map view and links view.
- Custom—Only the links defined for the customized filter are displayed in the map view and links view.
- Data Link—The data link layer class of links (ATM and Frame Relay) is displayed in the map view and links view.
- None—None of the links are displayed in the map view and links view.
- Physical—Only the physical links are displayed in the map view and links view.
- VPN—Only VPN-related links (GRE, Pseudowire, VPN, and VPN IPv6) are displayed in the map view and links view.

Note You can customize the Group drop-down list options by selecting an option and adding or removing the required link types. The next time the Link Filter dialog box is opened, the Custom option is displayed with the specified link types.

Step 4 Check the check boxes for the links that you want to display in the map view and links view. Uncheck the check boxes for the links you do not want to display in the map view and links view.

Step 5 Click **Apply** to apply the defined link filter settings and continue with more selections.

Step 6 Click **OK** when you have completed your selections.

Step 7 In the Create Map dialog box, enter a name for the new map and click **OK**. An empty new map is displayed in the navigation pane and content area, and the Link Filter Applied button is displayed in the to indicate that the links have been filtered.

Step 8 Add the required elements to the map. For more information, see Creating a New Map, page 4-8.

The links are displayed in the map view and links view according to your selections.

Filtering Links in an Existing Map

You can also create a map, add elements with all links enabled and visible in the map view and links view, and then filter (display or hide) the different types of links as required.

To filter links in an existing map:

Step 1 Click **Link Filter** in the main toolbar.

Step 2 In the Link Filter dialog box, uncheck the check boxes for the links that you do not want to display in the map view and links view.

Step 3 Click **Apply** to apply the defined link filter settings and continue with more selections.

Step 4 Click **OK** when you have completed your selections.

The links are displayed in the map view and links view according to the defined filter, and the Link Filter Applied button is displayed in the to indicate that the links are filtered.

Opening the CPU Usage Graph

Prime Network Vision enables you to display memory and CPU usage information for a device or network element, including its history.

To open the CPU usage graph:

Step 1 Right-click a network element in the navigation tree and choose **Tools > CPU Usage**.

The CPU Usage dialog box displays the following information:

- CPU Usage—The CPU usage rate as a percentage.
- CPU Usage History—The CPU usage rate history is graphically displayed.
- Memory Usage—The memory usage rate as a percentage.
- Memory Usage History—The memory usage rate history is graphically displayed.

Step 2 If desired, click **Save to CSV File** to export the displayed data. For more information, see Exporting Tables to a File, page 2-55.

Step 3 Click the upper right corner to close the CPU Usage dialog box.

Communicating with Devices Using Ping and Telnet

Prime Network Vision enables you to communicate with devices in the following ways:

- Pinging a Device, page 4-41
- Telneting a Device, page 4-41

Pinging a Device

Prime Network Vision enables you to ping a device to verify that the device is responding.

The ping is performed from the client to the device, and not from the Prime Network Vision unit hosting the VNE to the device.

To ping a device, right-click a device in the navigation tree or map, and choose **Tools > Ping**.

The results are displayed in a new window.

Telneting a Device

Prime Network Vision enables you to communicate with a device using the Telnet window.

The Telnet session is performed from the client to the device, and not from the Prime Network Vision unit hosting the VNE to the device.

Note If you are using a Windows 7 system, you must enable the Windows Telnet Client before you can use the Prime Network Telnet option.

- For Windows 7 32-bit systems, enable the Windows Telnet Client to use the Prime Network Telnet option.

- For Windows 7 64-bit systems, a solution is available on the Cisco Developer Network at http://developer.cisco.com/web/ana/forums/-/message_boards/message/2780108.

To telnet a device:

Step 1 Right-click a device in the navigation tree or map, and choose **Tools > Telnet**. A terminal window opens.

Step 2 Log in and use the Telnet window as needed.



CHAPTER 5

Working with Links

The following topics describe how to view information about static and dynamic links using the Cisco Prime Network Vision (Prime Network Vision) user interface:

- User Roles Required to Work with Links, page 5-1
- Understanding Dynamic and Static Links, page 5-3
- Link Discovery and Flickering Ethernet Topology Links, page 5-3
- Viewing Link Properties, page 5-4
- Viewing Link Impact Analysis, page 5-13
- Adding Static Links, page 5-15
- Filtering Links Using the Collection Method, page 5-18
- Selecting a Link, page 5-18

User Roles Required to Work with Links

This topic identifies the GUI default permission or element scope security level that is required to work with links in Prime Network Vision. Prime Network determines whether you are authorized to perform a task as follows:

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

For more information on user authorization, see the *Cisco Prime Network 3.9 Administrator Guide*.

The following tables identify the tasks that you can perform:

- Table 5-1 identifies the tasks that you can perform if a selected element **is not in** one of your assigned scopes.
- Table 5-2 identifies the tasks that you can perform if a selected element **is in** one of your assigned scopes.

By default, users with the Administrator role have access to all managed elements. To change the Administrator user scope, see the topic on device scopes in the *Cisco Prime Network 3.9 Administrator Guide*.

Table 5-1 Default Permission/Security Level Required for Working with Links - Element Not in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View link properties in Map view	X[1]	X[1]	X[1]	X[1]	X
View link properties in Links view	X[2]	X[2]	X[2]	X[2]	X
View link properties in the Link Properties window	—	—	—	—	X
View link impact analysis	—	—	—	—	X
Add static links	—	—	—	—	X
Filter links using collection method	X	X	X	X	X
Find and select a link in a map	X	X	X	X	X

1. Link properties are limited in the Map view; not all link information is available.
2. Link properties are limited in the Links view; not all link information is available.

Table 5-2 Default Permission/Security Level Required for Working with Links - Element in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View link properties in Map view	X	X	X	X	X
View link properties in Links view	X[1]	X[1]	X[1]	X[1]	X
View link properties in the Link Properties window	X	X	X	X	X
View link impact analysis	—	—	—	—	X
Add static links	—	—	—	X	X
Filter links using collection method	X	X	X	X	X
Find and select a link in a map	X	X	X	X	X

1. Link properties are limited in the Links view; not all information is available.

Understanding Dynamic and Static Links

Prime Network Vision provides a topological model of the physical and logical links that exist between elements in the network. Prime Network Vision automatically discovers these links using various protocols (such as STP, CDP, and LLDP), and the ongoing process of autodiscovery maintains this topological information. Prime Network Vision discovers any new links that are added and continues to verify that the discovered links still exist; for this reason, they are called *dynamic* links.

Property information is provided for links that are:

- Between two devices.
- Between a device and an aggregation that connects this device to another device inside the aggregation.
- Between two aggregations that contain devices that cross the aggregations.

If a link is unidirectional, Prime Network Vision displays an arrowhead on the link. If it is bidirectional, an arrowhead is not displayed.

Prime Network Vision also provides functionality that allows you to create links on the VNE level. These links do not perform any configuration or provisioning on a device or in the network. Because the links do not really exist in the network, the links are not updated. For this reason they are called *static link*s. Static links are useful for map visualization and network correlation; for example, if Prime Network Vision does not discover a link that you know exists in the network, you can create a static link that is displayed in the map. For correlation purposes, Prime Network Vision treats the static link as if it were a physical or logical link and allows correlation flows to go through the static link. For information on creating static links, see Adding Static Links, page 5-15.

Link Discovery and Flickering Ethernet Topology Links

As mentioned in Understanding Dynamic and Static Links, page 5-3, Prime Network discovers topology links using various protocols, such as STP, CDP, and LLDP. In some situations, the link configurations themselves can prevent Prime Network from discovering the correct information. For example, if Layer 2 protocol tunneling is configured and the discovery protocols are tunneled, Prime Network can create an incorrect link. This scenario results in a flickering link that is first created incorrectly due to tunneled discovery information, and then disconnected when the Prime Network counters test discovers that the counters on the edges of the link do not match. During the next topology cycle, Prime Network recreates the link, which is disconnected again during the counters test.

A link is considered flickering when it is connected, disconnected, and reconnected when using the same connection technique because the topology information is conflicting. When this situation occurs, Prime Network generates a system event with the message “Physical Link discovery inconsistent.”

To prevent an ongoing cycle of link creation and disconnecting, Prime Network detects such case of flickering links, creates a system event with the message “Inconsistent Physical Link Discovery between *system:interface1* and *system:interface2*,” and stops the link from flickering by disconnecting it.

To remedy the situation, we recommend that you wait until the link disappears from the map and then create a static link.

Note This feature applies only to Ethernet links.

Viewing Link Properties

By default, you can view links in maps only if both ends of the link are in your scope. However, Prime Network Vision 3.9 provides an option that allows you to view links and any associated tickets if only one end of the link is in your scope. For more information about this option, see the *Cisco Prime Network 3.9 Administrator Guide.*

Note Changes to the registry should only be carried out with the support of Cisco. For details, contact your Cisco account representative.

Prime Network Vision provides information about links in the following ways:

- Through the physical characteristics of the link in a map, tooltips, and link quick views—See Viewing Link Properties in Prime Network Vision Maps, page 5-4.
- In the Links view—See Viewing Link Properties in the Links View, page 5-8.
- In the link properties window—See Viewing Link Properties in the Link Properties Window, page 5-10.

Viewing Link Properties in Prime Network Vision Maps

The representation of a link in a map provides information about that link. The characteristics that provide information about a link are:

- Whether the link is solid or dashed.
- Whether or not the link displays an arrow at one end.
- Link color.

Table 5-3 describes the link variations that can be displayed in a map and provides examples of each.

Table 5-3 Link Properties in Prime Network Vision Maps

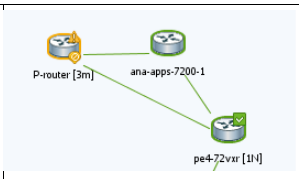
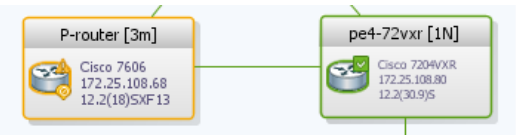
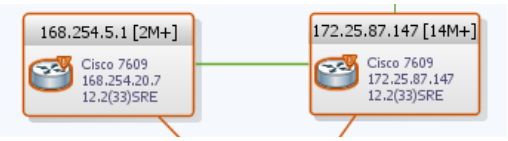
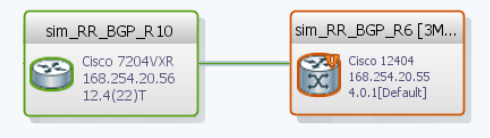
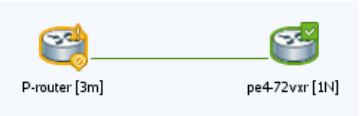
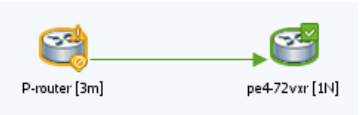
Link Characteristic	Description	Example
Solid Line vs. Dashed Line		
Solid line	Physical, topological, or service link, such as a link between two devices.	
Dashed line	Association or *business link* between such elements as EVCs, VPLS service instances, or VPN components.	

Table 5-3 Link Properties in Prime Network Vision Maps (continued)

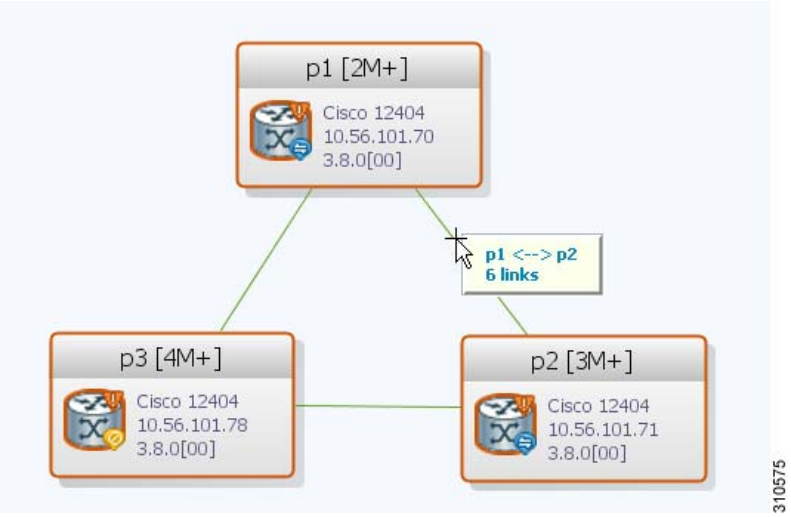
Link Characteristic	Description	Example
Link Widths		
Normal	Contains links of the same group. Available groups are: • Business • GRE • MPLS-TP • Pseudowire • VLAN • All others	
Wide	*Aggregated links* that contain links of different groups. When viewing a map at a low zoom level, aggregated links cannot be distinguished in the GUI.	
Tunnel	A tunnel, with the center color representing the severity of any alarms on the link.	
Arrowhead vs. No Arrowhead		
No arrowhead	Bidirectional link.	
Arrowhead	Unidirectional link, with the flow in the direction of the arrowhead.	
Link Color		
Red	Critical alarm is on the link.	
Orange	Major alarm is on the link.	
Yellow	Minor alarm is on the link.	
Green	Link is operating normally.	
Blue	Link is selected.	

Note The color of a selected link is customizable. The default color is blue. For more information on link colors, see Map View, page 2-10.

To view link properties:

Step 1 Hover your mouse cursor over the required link in a map. A link tooltip is displayed as shown in Figure 5-1.

Figure 5-1 Link Tooltip in Prime Network Vision



The tooltip contains the following information about the link:

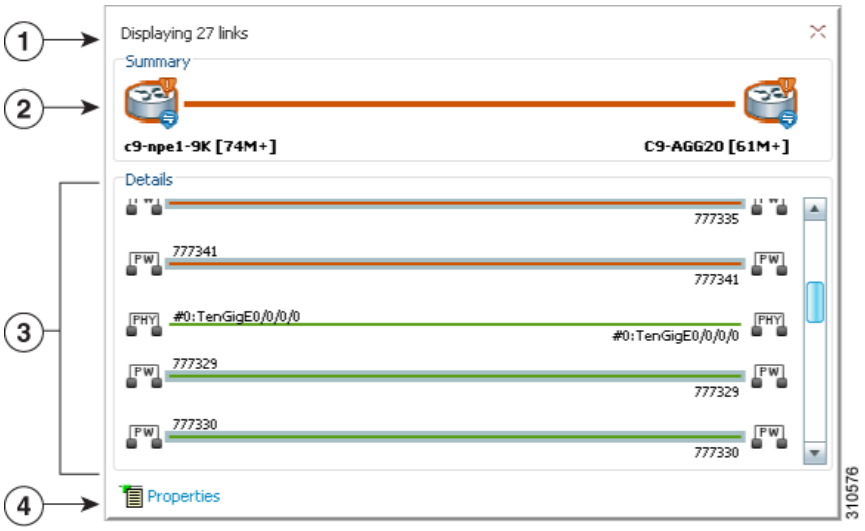
- Link endpoints, identified by the element or service name.
- The number of links represented by the line on the map.

Examples of tooltips are:

- `169.254.12.34 <--> 169.254.56.78 6 links`
- `22@169.254.12.34 <--> CEM1/2:1@169.254.56.78 1 link`

Step 2 To view additional link information, click the tooltip. The link quick view window is displayed as shown in Figure 5-2.

Figure 5-2 Link Quick View Example



1	Number of links represented by the single link in the map. In this example, 29 links.
2	Link endpoints.
3	List of all links represented by the link in the map with the following information, as appropriate: • Type of link, such as Physical, MPLS, or Tunnel. For a complete list of the types of links and their abbreviations, see Link Icons, page A-9. • Link detail, such as the interface used on each endpoint, service name, or type of service. • Link alarm status, indicated by the link color.
4	Hyperlink to the link properties window. The Properties button is available for physical, topographical, and service links, but is not available for business links (dashed links). For more information, see Viewing Link Properties in the Link Properties Window, page 5-10.

Step 3 To view more link properties, click **Properties** in the link quick view.

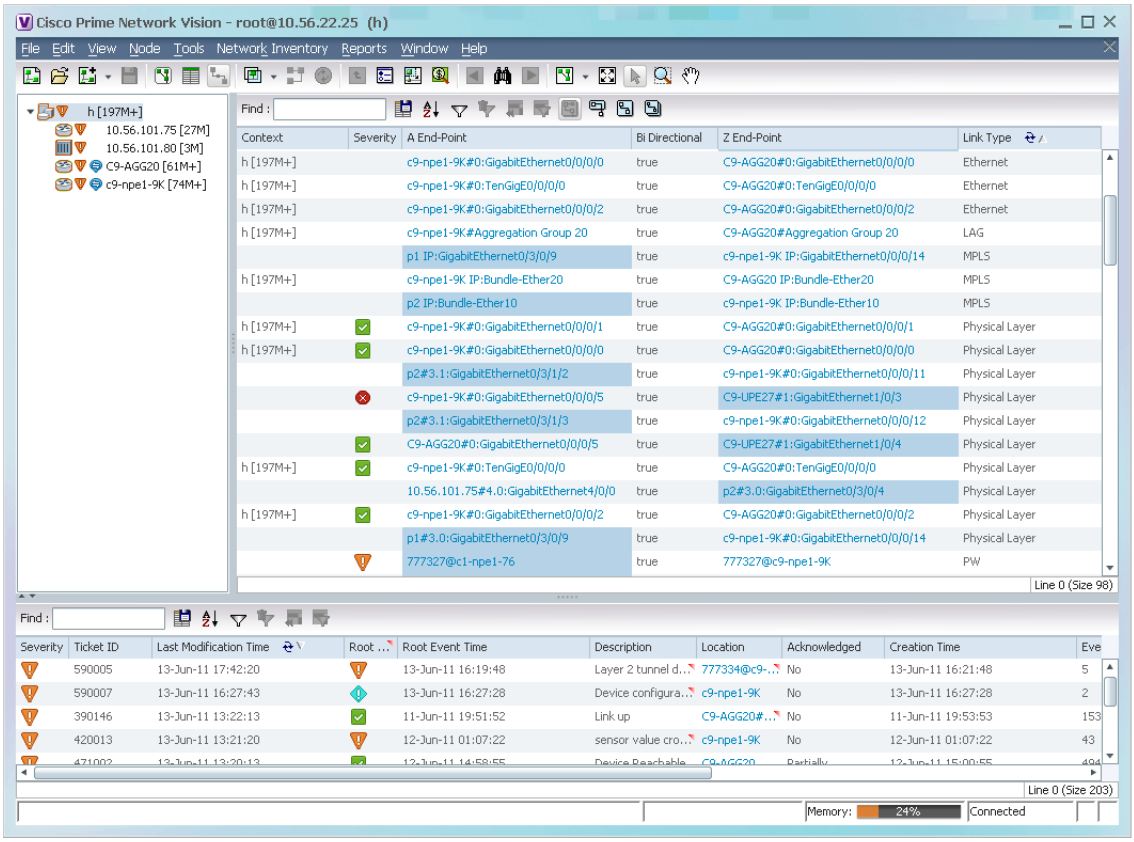
For more information about the link properties window, see Viewing Link Properties in the Link Properties Window, page 5-10.

Viewing Link Properties in the Links View

The links shown in a map represent many other links as described in Viewing Link Properties in Prime Network Vision Maps, page 5-4. By using the links view, you can view a list of all links represented in a map and their status.

To display the links view in the Prime Network Vision window, click **Show Links View** in the main toolbar. Figure 5-3 shows an example of the links view.

Figure 5-3 Links View



Note A link external to the network has a blue cell background in the table.

Any links that are added or removed from the map are automatically added or removed from the links view, provided they have not been filtered out.

Table 5-4 describes the information that is displayed in the links view.

Table 5-4 Links View Content

Field	Description
Context	Name of the map or aggregation containing the link. The links view can include multiple contexts. This field can be empty for either of the following reasons: • One side of the link is not included in the map. • The link is filtered out of all contexts.
Severity	Severity bell icon, colored according to the severity of the alarm on the link and indicating the impact of the alarm on the network. For more information, see Prime Network Vision Status Indicators, page 2-24.
A End Point	Device or site that is the source of the link, as a hyperlink to the inventory of the device or site.
Bidirectional	Whether the link is bidirectional or unidirectional: True (bidirectional) or False (unidirectional).
Z End Point	Device or site that is the destination of the link, hyperlinked to the relevant entry in inventory.
Link Type	Type of link, such as Physical Layer, VPN, MLPPP, or MPLS.

By default, the links displayed in the links view are sorted according to link type and the deep collection method.

The buttons in Table 5-5 are displayed at the top of the links view and enable you to filter the links according to the collection method.

Note If you load a map with many links (for example, thousands of links), it can take a while for the complete list of links to load. The filtering options in the table are unavailable until the table has completely loaded.

Table 5-5 Links View Tools

Icon	Name	Description
	All Links	Complete list of links for the selected map or aggregation.
	External Links	Links with one side of the link in the selected map or aggregation and the other side of the link outside the currently selected map or aggregation.
	Flat Links	Links currently visible in the map pane for the selected map or aggregation, excluding any thumbnails.
	Deep Links	Links for the selected aggregation and any nested aggregations, with both endpoints within the currently selected map or aggregation.

For more information about filtering links using the collection method, see Filtering Links Using the Collection Method, page 5-18.

Viewing Link Properties in the Link Properties Window

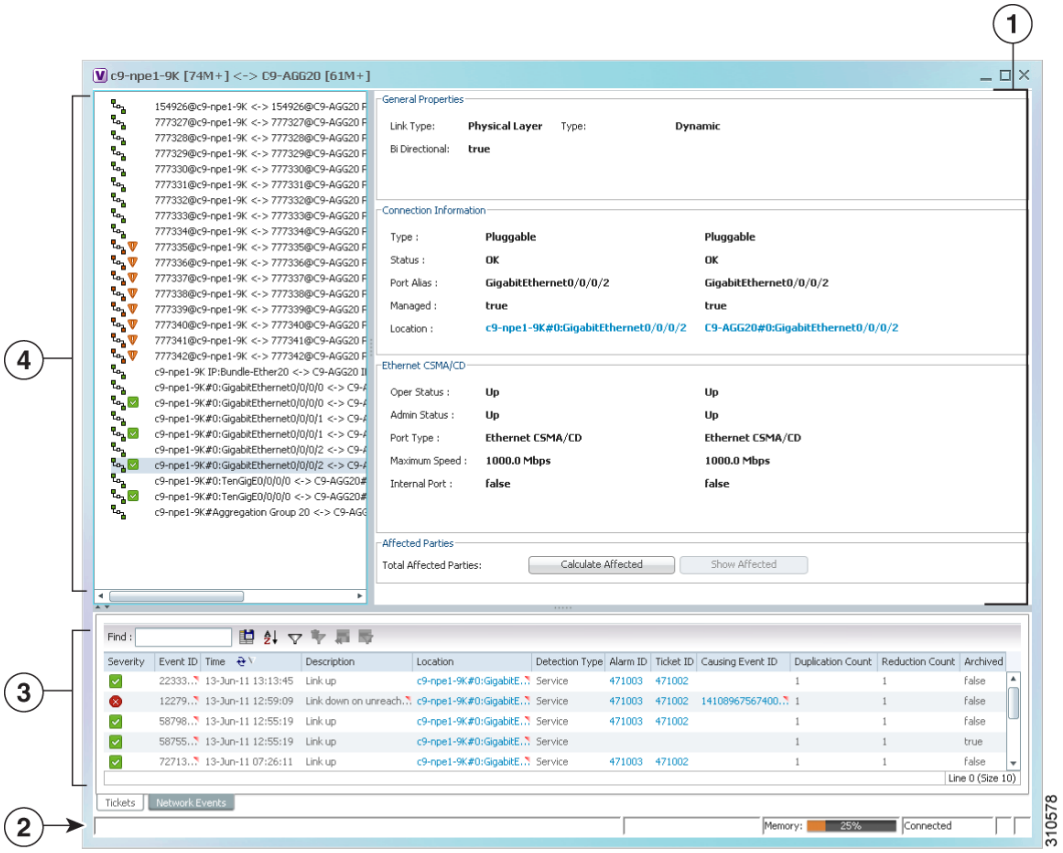
The link properties window contains general information about the selected link, details of the link connection, and technology-specific information appropriate for the link.

In a Prime Network Vision map, open the link properties window in one of the following ways:

- Double-click a link between two elements.
- Right-click a link and choose **Properties**.
- In the links quick view window, click **Properties**.

The link properties window is displayed as shown in Figure 5-4.

Figure 5-4 Link Properties Window



1	Properties pane	**3**	Ticket and events pane
2	Status bar	**4**	Link list pane

Note If multiple links exist between the elements or aggregations, the link properties window displays information for all the links.

See the following topics for more information about each of the panes in the link properties window:

- Link List Pane, page 5-11
- Properties Pane, page 5-11
- Ticket and Events Pane, page 3-18

The information displayed in the link properties window changes according to the ports or subports selected in the link list pane.

Link List Pane

In the link properties window, the link list pane displays a list of the links that are represented by a single link on the map. Each link has a single entry in the link list pane.

When an entry is selected in the link list pane, the information displayed in the properties pane is updated. The color of the icon in the link list pane reflects its severity. For more information about severity, see Prime Network Vision Status Indicators, page 2-24.

The heading and the link list pane display the left and right link identifiers between the two nodes, the device alias, and Connection Termination Point (CTP).

Properties Pane

The properties pane enables you to view the following, depending on your selection in the link list pane:

- Properties of a selected link, including port properties information.
- Hyperlinks to relevant entries in logical or physical inventory.
- Status.

The properties pane displays the link type, port alias, and port location, all of which uniquely identify the port. The port location information is also displayed as a hyperlink to the inventory window.

The properties pane also displays the parameters for each end of the link, aligned under the relevant link identifier. Any discrepancies between the link's ports are displayed in red.

The following fields are displayed in the Connection Information area for physical links:

- Type—Type of connector, such as fiber optic.
- Status—Status of the link, such as OK.
- Port Alias—Name used in the device CLI or EMS for the selected port.
- Managed—Whether or not the link is managed: True or False.

- Pluggable Port State—Whether or not a pluggable module is inserted.
- Location—Location of the entity, slot number, and port on the slot, as a hyperlink that opens the properties of the relevant location.

Depending on the link and its configuration, the following areas containing status and configuration information are displayed in the properties pane:

- Ethernet CSMA/CD
- Gigabit Ethernet
- LAG
- MLPPP
- MP-BGP
- MPLS Link Information
- PPP
- Pseudowire
- T1
- VRF

IP addresses are displayed in IPv4 or IPv6 format, as appropriate.

Depending on the type of link, the following areas might be displayed:

- Affected Parties—Enables you to view all elements potentially affected by the link. For more information, see Viewing Link Impact Analysis, page 5-13.
- Labels—Enables you to view all LSPs on an Ethernet link. For more information, see Viewing LSPs Configured on an Ethernet Link, page 17-11.
- VCs—Enables you to view configured and misconfigured VCs on an ATM link. For more information, see Viewing ATM VPI and VCI Properties, page 18-10.

Ticket and Events Pane

The ticket and events pane is displayed at the bottom of the link properties window and contains the following tabs:

- Tickets—Displays the tickets that are collected on the selected element, service, or component in the navigation pane.

  Table 9-3 on page 9-5 describes the information that is available in the Tickets tab.

- Network Events—Displays all active network events associated with tickets and alarms, and all archived events with a timestamp that falls within the specified events history size (see Selecting Prime Network Vision Options, page 2-47).

  Table 3-7 on page 3-18 describes the information that is available in the Network Events tab.

When displaying network events, Prime Network Vision monitors the history size value defined in the Events tab of the Options dialog box (**Tools > Options > Events**). The default value is six hours and can be changed in Prime Network Administration. In addition, Prime Network Vision limits the maximum number of network and provisioning events that are sent from the server to client to 15,000 each. If the number of network or provisioning events exceeds the limit specified in the Options Events tab or the 15,000 maximum limit, Prime Network Vision purges the oldest events from table. The purging mechanism runs once per minute.

Tip You can display or hide the ticket and events pane by clicking the arrows displayed below the device view panel.

Viewing Link Impact Analysis

Prime Network Vision enables you to select a network link and calculate the elements that might be affected if the link were to go down. This enables you to perform proactive impact analysis when a fault has not actually occurred.

Note Impact analysis applies only to physical links.

To calculate impact analysis:

Step 1 Select a map or aggregation in the navigation pane, and click **Show Links View** in the main toolbar. The links view is displayed in the content pane.

Step 2 In the table toolbar, click **Link Filter**. The Link Filter dialog box is displayed. For information about the Link Filter dialog box, see Filtering Links in a Map, page 4-38.

Step 3 In the Filter dialog box:

a. In the Match drop-down list, choose **All**.

b. In the field drop-down list, choose **Link Type**.

c. In the operand drop-down list, choose **Equals**.

d. In the matching criteria drop-down list, choose **Physical Layer**.

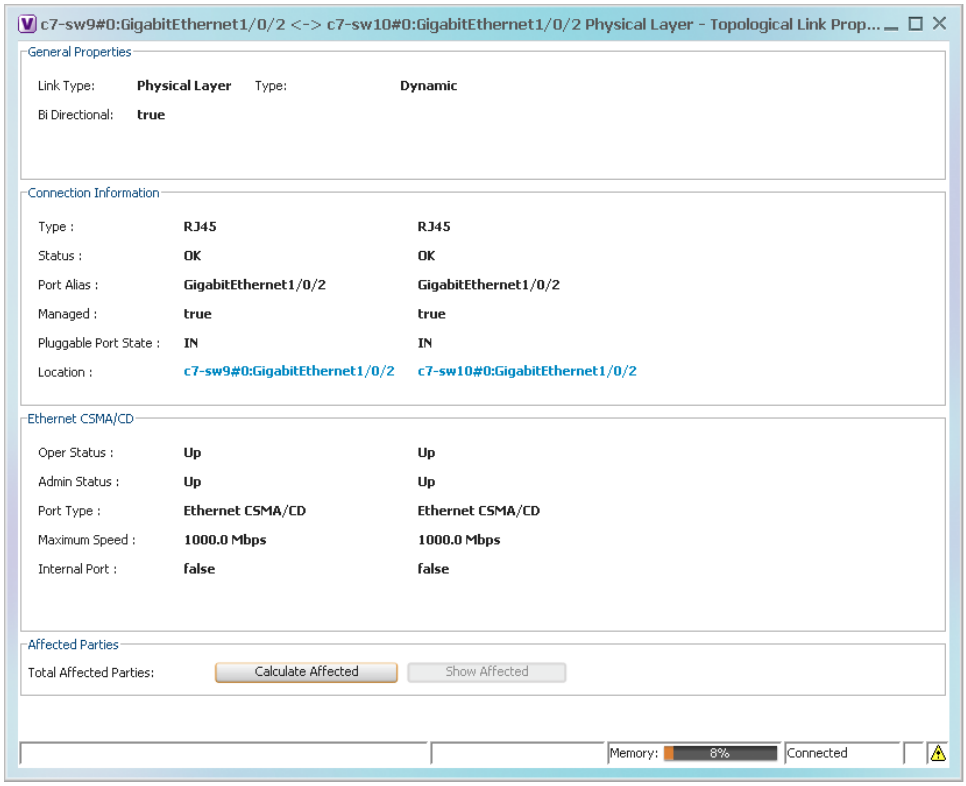
e. Click **OK**.

Only physical links are displayed in the links view.

Step 4 In the links view, right-click the required link and choose **Properties**. The Topological Link Properties window is displayed.

Note Resize the window as needed to view all the information.

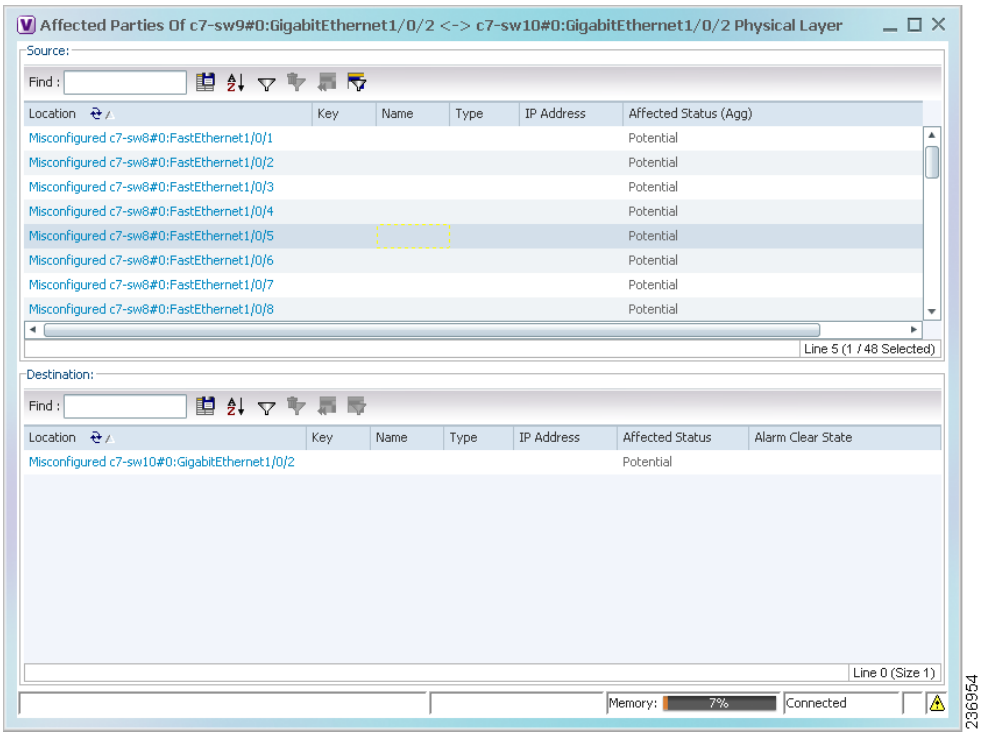
Figure 5-5 Topological Link Properties Window



Step 5 Click **Calculate Affected**. The total number of potentially affected parties is displayed in the Affected Parties area.

Step 6 Click **Show Affected**. The Affected Parties window is displayed as shown in Figure 5-6.

Figure 5-6 Affected Parties Window



Step 7 To view the potentially affected destinations if a link were go to down, click an entry in the Source table. The potentially affected destinations are displayed in the Destination table.

Step 8 To view source or destination properties in inventory, click the required hyperlinked entry.

Note The Affected Parties window occasionally displays entries that start with the word *Misconfigured*. Entries that start with Misconfigured indicate that the flow has stopped unexpectedly between the source and destination points. An unexpected termination point can be a routing entity, bridge, or VC switching entity. The significant aspects of Misconfigured entries are:
- Because the link does not terminate as expected, the link is not actually impacted.
- An error might exist in the configuration or status of the termination points.
We recommend that you check the configuration and status of the affected termination points.

Adding Static Links

Prime Network Vision enables you to create static links that exist only on the VNE level. Static links are useful for visualization and network correlation because Prime Network Vision allows correlation flows to go through the links, as if they were real physical or logical links. Static link properties are not updated because the links do not really exist in the network.

To create a static link, select a device or port and define it as the A side. Then define a second device or port as the Z side. Prime Network Vision validates the new link after the two ports are selected. Validation checks the consistency of the port types (for example, RJ45 on both sides), and Layer 2 technology type (for example, ATM OC-3 on both sides).

You can also create static links between Ethernet Link Aggregation Groups (LAGs) by choosing a LAG and the desired port channel for the A or Z side as described in the following procedure.

When you add a new link, the color of the link reflects its current state. For example, if the operation status of a port is down, the link is colored red. You can add links from either the Prime Network Vision window's navigation and a map (method 1), or from the inventory window navigation pane (method 2).

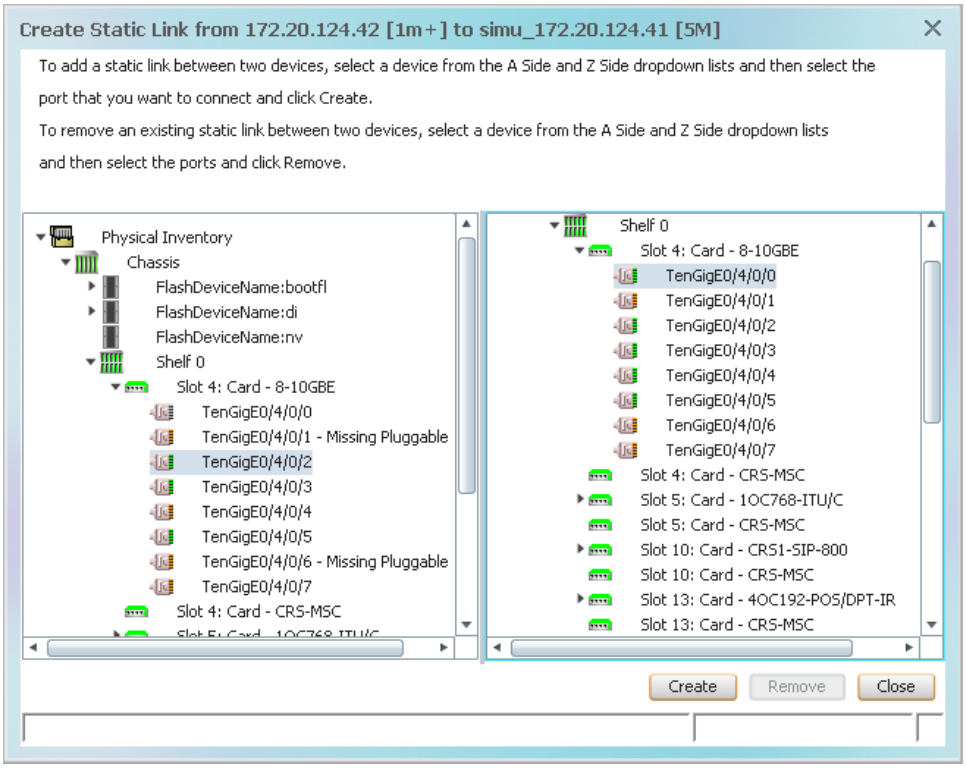
In addition, you can add a new link using Cisco Prime Network Administration. For more information, see the *Cisco Prime Network 3.9 Administrator Guide*.

Adding a Link (Method 1)

Step 1 Right-click the required A Side device in the navigation pane or in a map, and choose **Topology > Mark as A Side**.

Step 2 Right-click the required Z Side device or LAG in the navigation pane or properties pane to display the right-click menu and choose **Topology > Mark as Z Side**. The Create Static Link window is displayed as shown in Figure 5-7, so that you can select the ports to connect.

Figure 5-7 Create Static Link Window



Step 3 Select the required port on both the A Side device and the Z Side device.

Step 4 Click **Create** to validate the connection and create the new link.

A success message is displayed.

A warning message is displayed if any of the following apply:

- A validation check fails.
- The operation status of one port is Up and the other port is Down.
- The selected ports are not of the same type.
- The Layer 2 technology type is not the same.
- One of the ports is part of another link.

Adding a Link (Method 2)

Step 1 Open the inventory window for the required A Side device.

Step 2 In the navigation pane, navigate to the required port or LAG.

Step 3 Right-click the required port or LAG and choose **Topology > Mark as A Side**.

Step 4 Repeat Step 1 and Step 2 for the Z Side port or LAG.

Step 5 Right-click the required port or LAG and choose **Topology > Mark as Z Side**. A confirmation message is displayed.

Step 6 Click **Yes.**

The ports are connected, and a link is created between the selected ports.

A warning message is displayed if any of the following conditions exist:

- One of the validation checks fails.
- The operation status of one port is Up and the other port is Down.
- The ports selected are not of the same type.
- The Layer 2 technology type is not the same.
- One of the ports is part of another link.

For information about removing a static link, see the *Cisco Prime Network 3.9 Administrator Guide*.

Filtering Links Using the Collection Method

The links view table enables you to view links that are not displayed graphically in the Prime Network Vision window map pane. The links view table is dynamic and automatically refreshes itself so that you can view up-to-date network links in real time.

The collection method enables you to filter the links displayed in the links view by selecting the collection method from the toolbar.

Note

- The deep collection method is applied by default in the links view.
- The filter applies only to the links view; it has no effect elsewhere in Prime Network Vision.

To filter links according to the collection method:

Step 1 Click **Show Links View** in the Prime Network Vision main toolbar.

Step 2 Select a map or aggregation in the navigation pane or links view.

Step 3 In the links view toolbar, click one of the following buttons in the toolbar:

- **All Links**
- **External Links**
- **Flat Links**
- **Deep Links**

The links are displayed in the links view according to the selected collection method.

Selecting a Link

Prime Network Vision enables you to select a link listed in the links view and highlight the link in the map in the content pane.

To select and highlight a link in a map:

Step 1 In the Links view, right-click the required link and choose **Select Link in Map**. The link is displayed in blue in the map.

Step 2 If two or more links are the same (for example, two VRF links), but they are in different contexts or aggregations, the Select Link Context dialog box is displayed. Select the required context from the drop-down list, then click **OK**. The link is displayed in blue in the map.

Step 3 To remove the blue highlight from the selected link, click the map background.



CHAPTER 6

Working with Business Tags and Business Elements

A business tag is a string that is meaningful to the business, and which can be used to label a component of a network element for use in Prime Network screens and reports.

A business element is a construction or organization of certain network elements and their properties into a logical entity, to provide the ability to track them in a way that makes sense from a business perspective. Examples of business elements include Layer 2 VPNs, Layer 3 VPNs, and virtual routers.

The following topics describe how to manage and view Cisco Prime Network Vision business tags and business elements:

- User Roles Required to Work with Business Tags and Business Elements, page 6-1
- Using Chinese Characters, page 6-3
- Attaching and Detaching Business Tags, page 6-3
- Searching for Business Tags and Viewing Their Properties, page 6-5
- Renaming a Business Element, page 6-8
- Deleting a Business Element, page 6-8

User Roles Required to Work with Business Tags and Business Elements

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

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

For more information on user authorization, see the *Cisco Prime Network 3.9 Administrator Guide*.

The following tables identify the tasks that you can perform:

- Table 6-1 identifies the tasks that you can perform if a selected element **is not in** one of your assigned scopes.
- Table 6-2 identifies the tasks that you can perform if a selected element **is in** one of your assigned scopes.

By default, users with the Administrator role have access to all managed elements. To change the Administrator user scope, see the topic on device scopes in the *Cisco Prime Network 3.9 Administrator Guide*.

Table 6-1 Default Permission/Security Level Required for Working with Business Tags and Business Elements - Element Not in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Attach a business tag	—	—	—	Partial[1]	X
Detach a business tag	—	—	—	Partial[1]	X
Search for a business tag	—	—	—	Partial[1]	X
View business tag properties	—	—	—	Partial[1]	X
Rename a business element	X	X	X	X	X
Delete a business element	X	X	X	X	X

1. Configurator user role default permission supports the action for business elements, which do not have scopes. The Configurator user role default permission supports the action for elements only if the elements are in the user's scope.

Table 6-2 Default Permission/Security Level Required for Working with Business Tags and Business Elements - Element in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Attach a business tag	—	—	—	Partial[1]	X
Detach a business tag	—	—	—	Partial[1]	X
Search for a business tag	—	—	—	Partial[1]	X
View business tag properties	—	—	—	Partial[1]	X
Rename a business element	X	X	X	X	X
Delete a business element	X	X	X	X	X

1. Configurator user role default permission supports the action for business elements, which do not have scopes. The Configurator user role default permission supports the action for elements only if the elements are in the user's scope.

Using Chinese Characters

Cisco Prime Network Vision supports Chinese characters in business tags, enabling you to perform the following activities using Chinese characters:

- Create a business tag—Attaching and Detaching Business Tags, page 6-3.
- Search for business tags and view business tag properties—Searching for Business Tags and Viewing Their Properties, page 6-5.
- Generate a list of business tags.
- Edit the details of a business tag.
- Write business tag notes.
- Remove business tags.
- Create aggregations.
- Export a business tag through a northbound interface.

See the following documents for more information about these features:

- Configuring your system to use Chinese characters— *Cisco Prime Network 3.9 Installation Guide*.
- Integration over northbound interfaces—*Cisco Prime Network 3.9 Integration Developer Guide*.

Attaching and Detaching Business Tags

Cisco Prime Network Vision enables you to attach one business tag for each entity, such as a port or interface. A business tag might identify a new subscriber to a port, or other information that is relevant in your environment. You can also detach existing business tags from entities.

Attaching a Business Tag

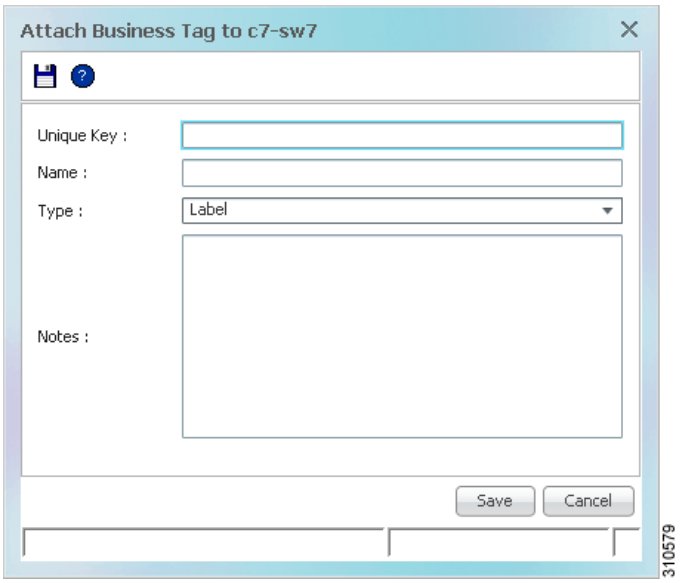
To attach a business tag:

Step 1 Do either of the following:

- If the element icon is at the largest size, click the **Attach Business Tag** button.
- Right-click the required network object and choose **Attach Business Tag**.

The Attach Business Tag dialog box is displayed, as shown in Figure 6-1.

Figure 6-1 Attach Business Tag Dialog Box



Step 2 Enter the information for the business tag:

- Unique Key—Enter a unique identifier for the business tag.
- Name—Enter a name for the business tag.

Note Business tag names are case-sensitive.

- Type—Choose the type of business tag: Subscriber, Provider Connection, or Label.

Note If you select Label, the name of the network object changes to display the business tag name if the Replace name with Business Tag option is selected in the Options dialog box (**Tools > Options**). For more information about display options, see Selecting Prime Network Vision Options, page 2-47.

- Notes—(Optional) Enter a free-text message.

Step 3 Click **Save**. The business tag is attached to the network object and displayed in the Business Tag tab of the inventory window for the selected network object. The business tag name is also displayed throughout Cisco Prime Network Vision, such as in the navigation pane, maps, and Cisco PathTracer.

In addition:

- The Edit Business Tag and Detach Business Tag options are displayed in the right-click menu when a business tag is attached to a network element.
- The Attach Business Tag button is not displayed in the element icon if a business tag is attached to the element.

You can search and edit business tag information attached to a network object using tools available from the appropriate Business Tag dialog box.

Detaching a Business Tag

A business tag that has been attached to a network object can also be detached. You can detach one more more business tags at a time.

To detach a business tag:

Step 1 In the Cisco Prime Network Vision window, navigate to the network object that contains the business tag you want to remove. You can also search for the business tag as described in Searching for Business Tags and Viewing Their Properties, page 6-5.

Step 2 Right-click the network object and choose **Detach Business Tag**.

The business tag is detached from the network object and is no longer displayed.

Searching for Business Tags and Viewing Their Properties

Cisco Prime Network Vision enables you to find a business tag by entering the full or partial business tag key, the full or partial business tag, or by specifying a specific type of business tag. In response, the business tags that meet the search criteria are listed.

If you know the location of the business tag, you can view its properties by opening the Business Tag tab in the element's inventory window.

To search for a business tag:

Step 1 Open the Find Business Tag dialog box in one of the following ways:

- Click **Find Business Tag** in the main toolbar.
- Choose **Edit > Find Business Tag** from the main menu.

Figure 6-2 shows an example of the Find Business Tag dialog box.

Figure 6-2 Find Business Tag Dialog Box

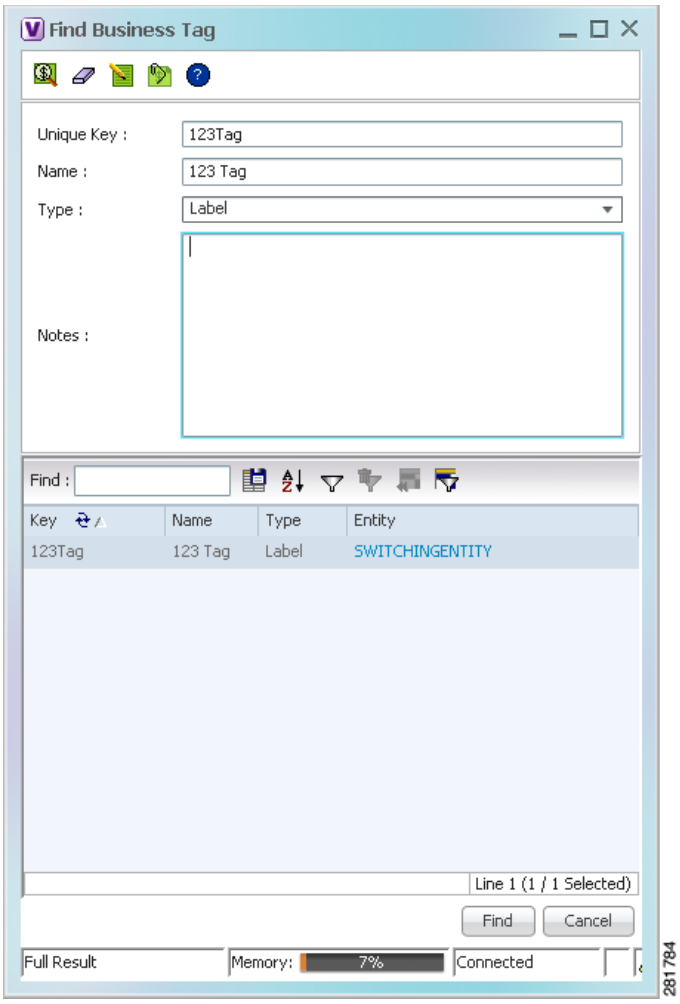


Table 6-3 describes the fields in the Find Business Tag dialog box.

Table 6-3 Find Business Tag Dialog Box Fields

Icon	Name	Description
	Find Business Tag	Finds the business tag according to a name, key, or type entered in the Find Business Tag dialog box.
	Clear Search	Clears the search information entered in fields in the Find Business Tag dialog box.
	Edit Business Tag	Opens the Edit Business Tag dialog box so you can edit the selected business tag.
	Detach Business Tag	Removes the selected business tag from the element.
	Help	Displays online help for Cisco Prime Network Vision and Cisco Prime Network Events.
Input Fields		
Unique Key		Enter the key you are searching for.
Name		Enter a full or partial entry of the name you are searching for. The search function is case-insensitive, so entering the string `biz tag` in the Name field results in business tags with names containing Biz Tag, Biz tag, and biz tag.
Type		From the drop-down list, select the type of business tag you are searching for: Label, Subscriber, Provider Connection, or All Types.
Note		Enter a full or partial entry of the note for the business tag you are searching for.
Results Table		
Key		Business tag key matching the search criteria.
Name		Business tag names matching the search criteria.
Type		Business tag type matching the search criteria.
Entity		Entity to which the business tag is attached, hyperlinked to entity properties.

Step 2 Enter the search criteria using the information for the Input Fields in Table 6-3, keeping in mind that the search function is case-sensitive.

Step 3 Click **Find**. The search results are displayed in the Results Table at the bottom of the Find Business Tag dialog box, as shown in Figure 6-2.

Step 4 View additional details as required:

- To view the business tag's properties, double-click the business tag in the search results table.
- To go to the business tag's location, click the hyperlink provided in the search results table.

Renaming a Business Element

The following caveats apply when renaming a business element:

- Except for network VLANs, the original name of the business element is not saved, so you cannot revert to the original name.
- Renaming a business element affects all users who have the business element loaded in their service view maps.

To rename business elements in service view maps:

Step 1 In the Cisco Prime Network Vision navigation pane or a map, right-click the business element and choose **Rename**.

Step 2 In the Rename Node dialog box, enter a new name.

Step 3 Click **OK**.

The changed business element name appears in the Cisco Prime Network Vision navigation pane and map.

Deleting a Business Element

You can delete business elements from the database. However, if you delete a business element from the database, it can no longer be viewed in Prime Network. We recommend that you delete a business element only when the physical element no longer exists.

Caution Deleting business elements affects all users who have the business elements loaded in their service view map.

Table 6-4 lists the requirements that must be met before you can delete a business element.

Table 6-4 Business Element Deletion Requirements

Business Element	Requirements
Layer 2 VPN	The Layer 2 VPN has no Logical Circuit Peers (LCPs), or, if it does, the LCPs display the reconciliation icon.
Layer 3 VPN	The VPN has no virtual routers, or, if it does, the virtual routers and sites display the reconciliation icon.
Site	No sites or interfaces are connected or bound to the VRF, or, if they are connected, they display the reconciliation icon.
Virtual router	The virtual router contains no VRFs, sites, or interfaces, or, if it does, the VRFs, sites, and interfaces display the reconciliation icon.

To delete a business element:

Step 1 Verify that the business element meets all requirements specified in Table 6-4. You cannot delete the element if all requirements are not met.

Step 2 In the Cisco Prime Network Vision navigation pane or a map, right-click the business element, and choose **Delete**.

Step 3 In the confirmation message, click **Yes** to delete the currently selected element, or click **Yes to All** to delete multiple selected elements.

The selected business element is deleted from the business configuration of all users.



CHAPTER 7

Working with the Prime Network Events Client

These topics describe the Cisco Prime Network Events (Prime Network Events) application and the options you can use to view system events and tickets that are generated within the Prime Network system:

- User Roles Required to Work with Prime Network Events, page 7-1
- Launching Prime Network Events, page 7-2
- Prime Network Events Window, page 7-3
- Prime Network Events Right-Click Options, page 7-9
- Selecting Prime Network Events Viewing Options, page 7-10

User Roles Required to Work with Prime Network Events

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

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

For more information on user authorization, see the topic on device scopes in the *Cisco Prime Network 3.9 Administrator Guide*.

Only users with the Administrator role can log into Prime Network Events (see Table 7-1).

Table 7-1 Default Permission/Security Level Required for Prime Network Events

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Opening Prime Network Events	—	—	—	—	X
Selecting Prime Network Events viewing options	—	—	—	—	X

Launching Prime Network Events

Prime Network provides two methods for launching Prime Network Events:

- From the Cisco Prime Central portal
- As a standalone application

Prime Network Events is password protected to ensure security. Before you start working with Prime Network Events, make sure you know your username and password. If you use the standalone application, you also need to know the Prime Network Events gateway IP address or hostname.

Note If you do not log into Prime Network Administration, Prime Network Vision, or Prime Network Events during a specified period of time (the default is one month) from the standalone application, your account is automatically locked. The default period can be changed per user in Prime Network Administration. The period of time is measured from the time you last logged out of any of the Prime Network client applications. For more information about changing the default period and unlocking an account, see the *Cisco Prime Network 3.9 Administrator Guide*.

The following conditions apply when working with Prime Network Events:

- Prime Network Events shows events only from the fault database and not from the event archive. Use Report Manager to view events from the event archive. For more information, see Chapter 10, "Working with Reports."
- Only users with the Administrator role can log into Prime Network Events.

The following topics describe how to launch Prime Network Events:

- Launching Prime Network Events from Prime Central, page 7-3
- Launching Prime Network Events as a Standalone Application, page 7-3

Launching Prime Network Events from Prime Central

If Prime Central is available in your environment, you can launch Prime Network applications from the main Prime Central page.

To launch Prime Network Events from Prime Central, choose **Assure > Prime Network > Events** in the menu bar.

The Prime Network Events application is opened in a separate window.

For more information about using Prime Network Events with the Prime Central suite of products, see:

- Cisco Prime Central *1.0 User Guide*
- Prime Network Events Right-Click Options, page 7-9

Launching Prime Network Events as a Standalone Application

To launch Prime Network Events as a standalone application:

Step 1 Choose **Start > Programs > Cisco Prime Network > gateway hostname/IP address >**Cisco Prime Network Events.

Note The hostname/IP address corresponds to the gateway on which Prime Network was configured.

The Cisco Prime Network Events login dialog box is displayed.

Step 2 Enter your username and password.

The Server field should already be populated with the hostname/IP address of the Prime Network gateway.

Step 3 Click **OK**.

When you launch Prime Network Events, messages are displayed if the server and client have different versions of the application that launches the client. For more information about these messages, see the *Cisco Prime Network 3.9 Installation Guide*.

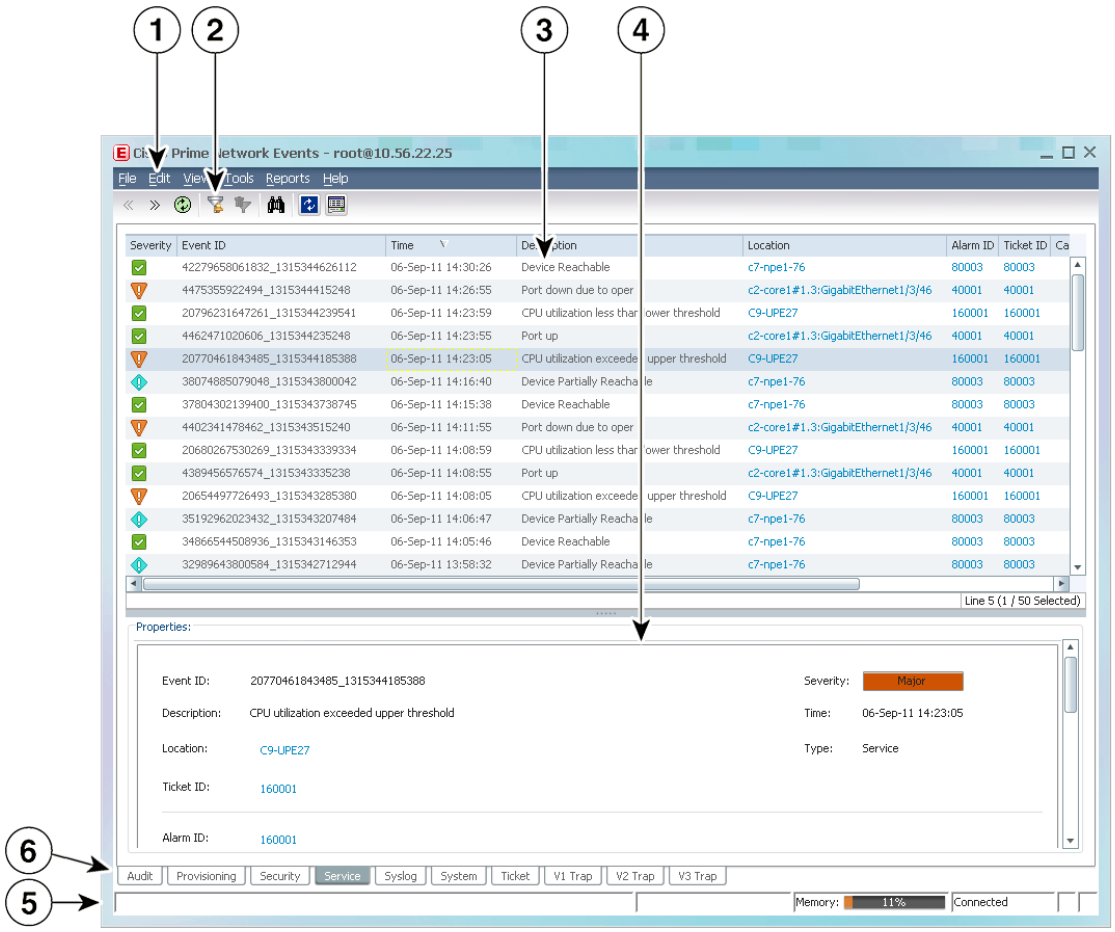
The first time you log in, the Ticket tab is displayed in the Cisco Prime Network Events window.

When you log in again, the tab and filter that were visible when you last logged out of the application are displayed.

Prime Network Events Window

The Prime Network Events window displays the events generated in the system. Figure 7-1 shows an example of the Prime Network Events window.

Figure 7-1 Prime Network Events Window



1	Menu bar	**4**	Details or properties pane
2	Toolbar	**5**	Status bar
3	Table pane	**6**	Prime Network Events tabs

Prime Network Events displays events for the last two hours by default. To modify the default number of hours for which events are displayed, see Selecting Prime Network Events Viewing Options, page 7-10. Increasing the number of hours can affect how long it takes for the events to be displayed. Also, if you want to find specific events and you are not interested in browsing all the available events, you can set Prime Network Events to operate in Find mode. To enable and use Find mode, see Selecting Prime Network Events Viewing Options, page 7-10.

You can display the events table with or without the properties pane, and select the specific type of information to display, such as provisioning events or SNMPv3 traps. For details on the information that is displayed in each tab, see Viewing Events and Tickets in Cisco Prime Network Events, page 8-2.

You can also use the Prime Network Events window and menu options to:

- Filter results so that events meeting your criteria are displayed. See Filtering Events, page 8-22.
- View selected event properties in a separate window. See Viewing Event Properties, page 8-14.

Event Status Indicators

The Severity column contains color-coded icons that reflect the severity of the event. An icon appears for each ticket or event in the Prime Network Events tabs (based on its severity) as shown in Table 7-2.

Table 7-2 Severity Indicators

Icon	Color	Severity
	Red	Critical
	Orange	Major
	Yellow	Minor
	Light Blue	Warning
	Green	Cleared, Normal, or OK
	Medium Blue	Information
	Dark blue	Indeterminate

Event Types and Categories

Every event that occurs in the Prime Network system and the Prime Network gateway is logged. This includes events that are performed as part of the normal operation of the Prime Network system, as well as events that might need further attention. Events are categorized, and any of the log entries can be viewed in the Prime Network Events tabs as described in Table 7-3.

Table 7-3 Event Categories in Prime Network Events

Tab	Description
Audit	Events related to commands running in the Prime Network gateway.
Provisioning	Events related to configuration and provisioning activities, including activations from Prime Network Activation.
Security	Events related to client login and user activity when managing the system and the environment.
Service	Events related to the alarms that are generated by the Prime Network system.
Syslog	Events related to the predefined set of syslogs received from the devices by the VNEs, which are used to generate the syslog events.
System	Events related to the everyday working of the internal system and its components. These events may be related to Prime Network and Prime Network gateway resources, representing the system log.
Ticket	Tickets that were opened in Prime Network.
V1 Trap	SNMPv1 traps that are generated by a network element and received by Prime Network; Prime Network uses these traps to generate the trap events.
V2 Trap	SNMPv2 traps that are generated by a network element and received by Prime Network; Prime Network uses these traps to generate the trap events.
V3 Trap	SNMPv3 traps that are generated by a network element and received by Prime Network; Prime Network uses these traps to generate the trap events.
All	A flat list of all events and tickets, sorted by time. Displayed when you choose **File > Open All Tab**.
3.6.x *Type*	Five tabs where *Type* represents one of the following: • Ticket • Service • Syslog • V1 Trap • V2-V3 Trap These tabs are: • Available only if Prime Network was upgraded from Cisco ANA 3.6.x to the current Prime Network version. • Displayed when you choose **File > Open 3.6.x Tabs**.

Prime Network Events Toolbar

Table 7-4 describes the tools that are displayed in the Prime Network Events toolbar.

Table 7-4 Prime Network Events Toolbar Tools

Button	Function
	Displays the previous page of events in the Prime Network Events window.
	Displays the next page of events in the Prime Network Events window.
	Refreshes the events displayed in the log by querying the database. If a filter is active, the refresh is done according to the filter. The log returns to the beginning of the list, displaying the events in ascending or descending order depending on the order of the current list. Descending order means that the last event is displayed first. For more information, see Refreshing Cisco Prime Network Events Information, page 8-21.
	Displays the Filter Events dialog box, which enables you to define a filter for the events displayed in the Prime Network Events log. For more information, see Filtering Events, page 8-22.
	Clears the existing filter.
	Displays the Find Events dialog box so that you can view events matching specific criteria. When finished selecting your criteria, click **OK**. The Prime Network Events window updates and displays the matching events. Note the following: • You can select multiple criteria here, as needed. • The Find Events dialog box returns every matching event in the database unless you specify a specific timeframe. This differs from the Filter Events dialog box, which returns events from the past 2 days (by default). For a description of the items in the Find Events dialog box, see Table 8-23 on page 8-24.
	Toggles automatic refresh of event data on and off. You define the refresh-time period (in seconds) in the Prime Network Events Options dialog box. The default is 60 seconds. If a filter is active, the refresh is done according to the filter. For more information, see Selecting Prime Network Events Viewing Options, page 7-10.
	Displays the properties of the selected event or ticket in the Properties pane.

Prime Network Events Menu Bar

Table 7-5 describes the options available in the Prime Network Events main menus. In addition to these options, Prime Network Events displays a Properties option when you right-click an event or ticket (see Viewing Event Properties, page 8-14).

Table 7-5 Prime Network Events Menu Options

Menu Option	Description
File Menu	
Export	Exports the log event information displayed in the Prime Network Events window according to the criteria defined in the Prime Network Events Options dialog box.
Open 3.6.x Tabs	Displays the following tabs: • 3.6.x Ticket • 3.6.x Service • 3.6.x Syslog • 3.6.x V1 Trap • 3.6.x V2-V3 Trap This option is available only if Prime Network was upgraded from Cisco ANA 3.6.x to the current version of Prime Network.
Open All Tab	Displays the All tab so you can view a flat list of all events and tickets sorted only by time.
Exit	Exits Prime Network Events.
Edit Menu	
Filter	Defines a filter for the events displayed in the Prime Network Events window according to the tab selected. See Filtering Events, page 8-22.
Purge	This option is unavailable.
View Menu	
Refresh	Refreshes the information displayed in the Prime Network Events window.
Go To	Navigates through the pages of the Prime Network Events window.
Properties	Displays the properties of the selected event, such as the root cause and source, in a separate window. For more information, see Viewing Event Properties, page 8-14.
Details Pane	Displays or hides the Details pane. If an event is selected, the properties of the selected event are displayed in the Details pane.

Table 7-5 Prime Network Events Menu Options (continued)

Menu Option	Description
Tools Menu	
Change User Password	Allows you to change the password used when logging into the Prime Network Events client application suite. The change takes effect the next time you log into the application.
Options	Defines the display options for the Prime Network Events window. For more information, see Selecting Prime Network Events Viewing Options, page 7-10
Reports Menu	
Report Manager	Opens the Reports Manager dialog box so you can create, run, and manage reports.
Run Report	Enables you to run standard event, inventory, and network service reports on demand.
Help Menu	
Cisco Prime Network Events Help	Opens the online help for Prime Network Events and Prime Network Vision.
Cisco.com	This option is unavailable.
About Cisco Prime Network Events	Displays application information, such as the version number.

Prime Network Events Right-Click Options

Prime Network Events offers the following right-click options in its tabs. Not all options are available in all tabs.

- Show Only Selected Rows—Displays only the rows that you choose.
- Show All Rows—Displays all rows that meet the current filter criteria.
- Launch external applications or tools—Enables you to launch any external application or tool for any event in Prime Network Events. For more information, see the *Cisco Prime Network 3.9 Customization User Guide*.
- Properties—Displays the properties window for the selected event or ticket.

Selecting Prime Network Events Viewing Options

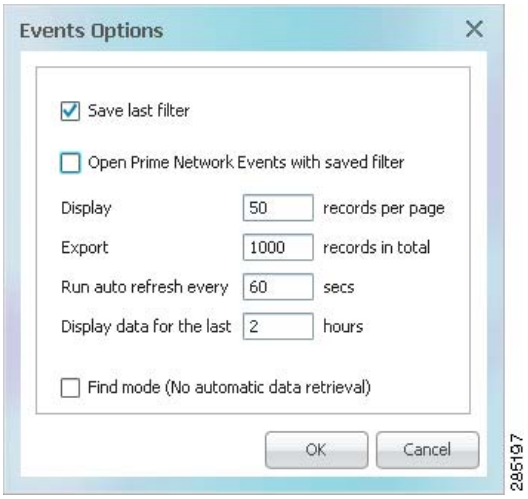
The Prime Network Events Options dialog box enables you to define the options for displaying events in the Prime Network Events window.

To define Prime Network Events options:

Step 1 From the main menu, choose **Tools > Options**.

The Prime Network Events Options dialog box is displayed, as shown in Figure 7-2.

Figure 7-2 Prime Network Events Options Dialog Box



Step 2 Set the options, using the information in Table 7-6.

Table 7-6 Prime Network Events Options Dialog Box

Option	Description
Save last filter	Saves the filter criteria defined per event type in the Filter Events dialog box. The filter criteria are available the next time you log into Prime Network Events. **Note** Events are not filtered automatically when you next log into Prime Network Events unless the *Open Events with saved filter* option is also selected.
Open Prime Network Events with saved filter	When enabled, applies the previously defined filter to the events as soon as you log into Prime Network Events. The events are continuously filtered according to the defined settings, even after you close the application.
Display *n* records per page	Specifies the number of events to be displayed per page.
Export *n* records in total	Sets the maximum number of events to be exported to a file.

Table 7-6 Prime Network Events Options Dialog Box (continued)

Option	Description
Run auto refresh every *n* secs	Automatically refreshes the Prime Network Events display after the specified number of seconds. **Note** This option uses rapid refresh from the database, which can affect the performance of other vital database options.
Display data for the last *n* hours	Displays past events from the specified number of hours. Values range from 1 to 336 hours (14 days), with a default of 2 hours. If you increase the number of hours, it can take longer for the events to be displayed.
Find mode (No automatic data retrieval)	Operates the Prime Network Events window in Find mode. In this mode, no events will be retrieved from the database when you open the application or switch between tabs. You can click the Find button in the toolbar to search for the events you need. When in Find mode, the status bar in the Prime Network Events window shows "Find Mode (no automatic data retrieval)."

Step 3 Click **OK**.



CHAPTER 8

Tracking Faults Using Prime Network Events

The following topics describe how to use Cisco Prime Network Events (Prime Network Events) to track faults:

- User Roles Required to Work with Prime Network Events, page 8-1
- Viewing Events and Tickets in Cisco Prime Network Events, page 8-2
- Viewing 3.6.x Tabs, page 8-12
- Working with Cisco Prime Network Events, page 8-14

User Roles Required to Work with Prime Network Events

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

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

For more information on user authorization, see the topic on device scopes in the *Cisco Prime Network 3.9 Administrator Guide*.

Only users with the Administrator role can log into Cisco Prime Network Events, as shown in Table 8-1.

Table 8-1 Default Permission/Security Level Required for Cisco Prime Network Events

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Viewing events and tickets	—	—	—	—	X
Viewing events and ticket properties	—	—	—	—	X
Refreshing information displayed in tables	—	—	—	—	X
Filtering events and tickets	—	—	—	—	X
Exporting displayed data	—	—	—	—	X

Viewing Events and Tickets in Cisco Prime Network Events

Events are displayed according to event categories, which are represented by tabs in the Cisco Prime Network Events window. Each tab displays an events list log that provides event information for the specific event category. Events can be of system type or network type.

Note Cisco Prime Network Events shows events only from the fault database and not from the event archive. Use Report Manager to view events from the event archive. For more information, see Chapter 10, "Working with Reports."

The Ticket tab displays the tickets that have been generated for correlated events.

Events and tickets are sorted by date, with the latest item displayed first and the oldest item displayed last.

Note Prime Network stores events in the database in Greenwich Mean Time (GMT) format. The Prime Network client converts events to the time zone that is configured on the client workstation. The times displayed in the Cisco Prime Network Events GUI reflect the time according to the client workstation.

By using the Cisco Prime Network Events Options dialog box, you can define a filter to be used or the number of items to be displayed in the list. Each tab displays the specified number of entries per page as defined in the Cisco Prime Network Events Options dialog box.

For more information, see Selecting Prime Network Events Viewing Options, page 7-10.

Because the lists of events and tickets can be lengthy, you can use the left and right arrows on the navigation to move through the records. You can also use the submenus that are available from **View > Go To** in the main menu.

All Tab

The All tab displays information about all events. Additional information specific to the event category can be viewed in the Event Properties window or individual category tabs.

When you launch Cisco Prime Network Events, the All tab is not displayed. You can view this tab by choosing **File > Open All Tab**.

Note When you open the All tab, it might take some time to retrieve information from the Prime Network database for all category events.

You can disable the All tab by following the instructions provided in the *Cisco Prime Network 3.9 Installation Guide*.

Table 8-2 describes the information that is displayed in the All tab.

Table 8-2 All Tab

Column	Description
Severity	Icon indicating the severity of the alarm on the event (the color and type of alarm are displayed in the Properties window Severity field). See Event Status Indicators, page 7-5.
Event ID	Event identifier, assigned sequentially.
Time	Date and time when the event occurred and was logged and recorded.
Description	Description of the event.
Location	Entity that triggered the event.
Event Type	Type of event: Audit, Provisioning, Security, Service, Syslog, System, V1 Trap, V2 Trap, or V3 Trap.

System Event Tabs

The following tabs in the Cisco Prime Network Events window display the system events:

- Audit Tab, page 8-3
- Provisioning Tab, page 8-5
- Security Tab, page 8-5
- System Tab, page 8-6

Audit Tab

The Audit tab displays all events generated for each command or request in Prime Network; for example, opening Cisco Prime Network Events displays the **Get** command as shown in Figure 8-1.

Figure 8-1 Audit Tab

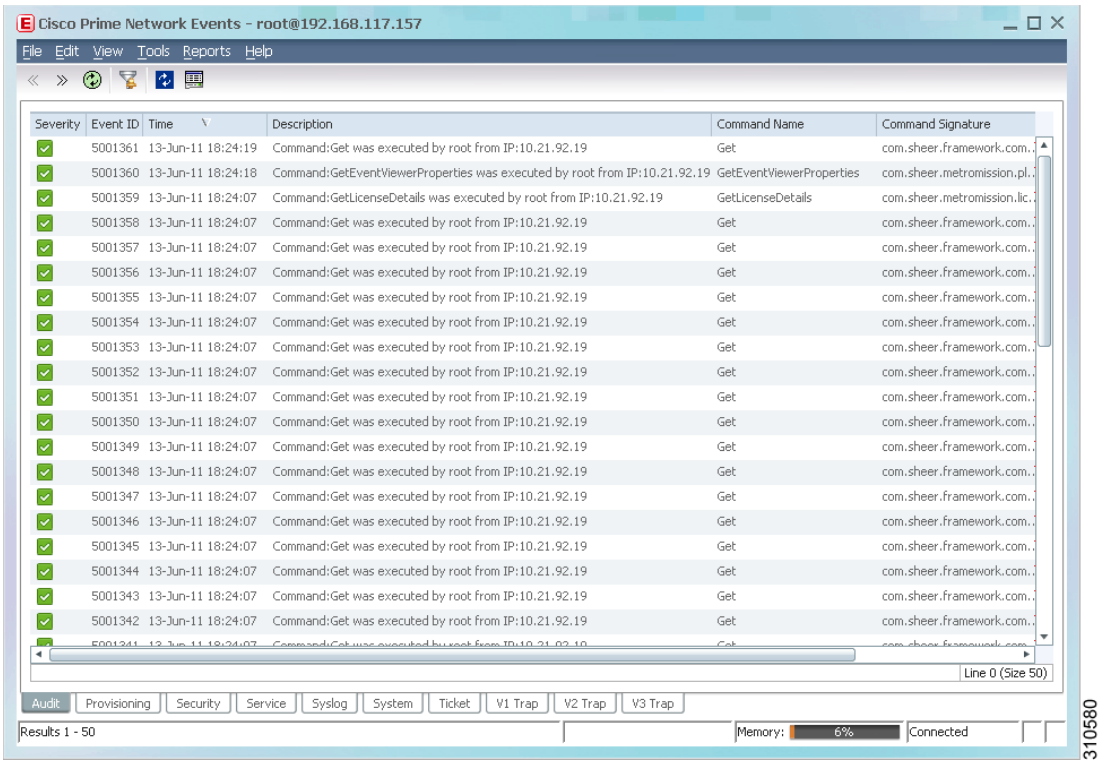


Table 8-3 describes the information that is displayed in the Audit tab.

Table 8-3 Audit Tab

Column	Description
Severity	Icon indicating the severity of the alarm on the event (the color and type of alarm are displayed in the Properties window Severity field). See Event Status Indicators, page 7-5.
Event ID	Identifier of the event, assign sequentially.
Time	Date and time when the event happened and was logged and recorded.
Description	Aggregation of portions of the same fields in the Audit Command fields.
Command Name	Audit-specific command name, prefaced by, for example, Get, Update, or Find.
Command Signature	Actual command run by Prime Network, such as **GetEventViewerProperties**.
Command Parameters	Command parameters issued with the command identified in the Command Name column.
Originating IP	IP address of the client that issued the command
User Name	Name of the user who initiated the command.

The audit service enables you to audit all the commands executed in the system; for example, the **Get** command can be audited. The Audit tab then displays this information.

Provisioning Tab

Events displayed in the Provisioning tab are events triggered during the configuration of a device. Prime Network sends an event explaining the configuration operation, such as configuring the cross-connect table in a device. The Provisioning tab displays detailed information specific to this event category. It contains events from Prime Network Command Builder, Prime Network Activation, and Prime Network Workflow Editor[1].

Additional information specific to this event category can be viewed in the Event Properties window.

If a provisioning event is the result of an activation script, the provisioning event can include an extremely long description. This description is displayed in the Event Properties window in the Details field. If the description exceeds the size of the Details field, Prime Network truncates the description in the database and Details field, and displays the following line to indicate that the description has been truncated:

=====CONTENT TRUNCATED BY CISCO PRIME NETWORK=====

Table 8-4 describes the information that is displayed in the Provisioning tab.

Table 8-4 Provisioning Tab

Column	Description
Severity	Icon indicating the severity of the alarm on the event (the color and type of alarm are displayed in the Properties window Severity field). See Event Status Indicators, page 7-5.
Event ID	Identifier of the event, assigned sequentially.
Time	Date and time when the event happened and was logged and recorded.
Description	Description of the event, such as “Script Show has failed.”
Location	Entity that triggered the event.
Username	Name of the user who performed the provisioning operations.
Status	Status, such as Success or Fail.

Security Tab

The Security tab displays detailed information specific to this event category. Security events are related to client login and user activity when managing the system and the environment. Additional information specific to this event category can be viewed in the Event Properties window.

Table 8-5 describes the information that is displayed in the Security tab.

Table 8-5 Security Tab

Column	Description
Severity	Icon indicating the severity of the alarm on the event (the color and type of alarm are displayed in the Properties window Severity field). See Event Status Indicators, page 7-5.
Event ID	Identifier of the event, assigned sequentially.
Time	Date and time when the event happened and was logged and recorded.

1. The Workflow Editor is based on LiquidBPM by Autonomy, Inc.

Table 8-5 Security Tab (continued)

Column	Description
Description	Description of the event, such as “Invalid password. Couldn’t authenticate user root.”
Location	Entity that triggered the event.
Username	Name of the user who triggered the event.
Originating IP	IP address of the client where the event was triggered.

For more information about the system security events displayed in this tab, see the *Cisco Prime Network 3.9 Reference Guide*.

System Tab

The System tab displays all the system events related to the everyday working of the internal system and its components. These events can be related to Prime Network and Prime Network gateway resources, representing the system log. Additional information specific to this event category can be viewed in the Event Properties window.

Table 8-6 describes the information that is displayed in the System tab.

Table 8-6 System Tab

Column	Description
Severity	Icon indicating the severity of the alarm on the event (the color and type of alarm are displayed in the Properties window Severity field). See Event Status Indicators, page 7-5.
Event ID	Identifier of the event, assigned sequentially.
Time	Date and time when the event happened and was logged and recorded.
Description	Description of the event, such as “AVM 77 is shutting down. Unit = 11.22.33.444.”
Location	Entity that triggered the event.

For more information about the system error and event messages displayed in this tab, see the *Cisco Prime Network 3.9 Reference Guide*.

Network Event Tabs

The following topics describe the information displayed in Prime Network Events for network events:

- Service Tab, page 8-7
- Syslog Tab, page 8-7
- Ticket Tab, page 8-8
- V1 Trap Tab, page 8-10
- V2 Trap Tab, page 8-10
- V3 Trap Tab, page 8-11

Service Tab

The Service tab displays all the events generated by Prime Network, such as Link Down. Service events are related to the alarms that are generated by the Prime Network system. Additional information specific to this event category can be viewed in the Event Properties window.

Table 8-7 describes the information that is displayed in the Service tab.

Table 8-7 Service Tab

Column	Description
Severity	Icon indicating the severity of the alarm on the event (the color and type of alarm are displayed in the Properties window Severity field). See Event Status Indicators, page 7-5.
Event ID	Calculated correlation identifier.
Time	Date and time when the event happened and was logged and recorded.
Description	Description of the event, such as “Port down due to oper.”
Location	Hyperlink to the entity that triggered the event.
Alarm ID	Hyperlinked identifier of the alarm associated with the event. Click the link to view the Ticket Properties window.
Ticket ID	Hyperlinked identifier of the ticket associated with the event. Click the link to view the Ticket Properties window.
Causing Event ID	Identifier of the causing event.
Duplication Count	For network events, the duplication count is calculated by the VNE and pertains only to flapping events. The duplication count represents the number of noncleared events aggregated by the flapping event.
Reduction Count	For network events, the reduction count is calculated by the VNE and pertains only to flapping events. The reduction count represents the number of events that are aggregated by the flapping event.

For more information about the service alarms that are displayed in this tab, see the *Cisco Prime Network 3.9 Reference Guide*.

Syslog Tab

The Syslog tab displays all the syslog events. These events are related to the predefined set of syslogs received from the devices by the VNEs, which are used to generate the syslog events. Additional information specific to this event category can be viewed in the Event Properties window.

Table 8-8 describes the information that is displayed in the Syslog tab.

Table 8-8 Syslog Tab

Column	Description
Severity	Icon indicating the severity of the alarm on the event (the color and type of alarm are displayed in the Properties window Severity field). See Event Status Indicators, page 7-5.
Event ID	Calculated correlation identifier.
Time	Date and time when the event happened and was logged and recorded.
Description	Description of the event, such as “Device configuration changed.”
Location	Hyperlink to the entity that triggered the event.
Alarm ID	Identifier of the alarm associated with the event.
Ticket ID	Identifier of the ticket associated with the event.
Causing Event ID	Identifier of the causing event.
Duplication Count	For network events, the duplication count is calculated by the VNE and pertains only to flapping events. The duplication count represents the number of noncleared events aggregated by the flapping event.
Reduction Count	For network events, the reduction count is calculated by the VNE and pertains only to flapping events. The reduction count represents the number of events that are aggregated by the flapping event.

Ticket Tab

The Ticket tab displays detailed information specific to tickets. A ticket contains a single root alarm (the root cause alarm can be of any alarm type, such as syslog or service), and all its subsequent correlated alarms. Additional information specific to tickets can be viewed in the Ticket Properties window.

A *Tickets capacity overflow, red threshold reached* system alarm is generated when the maximum number of tickets is exceeded. The alarm severity is defined as critical.

Table 8-9 describes the information that is displayed in the Ticket tab.

Table 8-9 Ticket Tab

Column	Description
Severity	Icon indicating the severity of the alarm on the ticket (the color and type of alarm are displayed in the Ticket Properties window Severity field). See Event Status Indicators, page 7-5.
Ticket ID	Sequentially assigned identifier of the ticket, hyperlinked to the Ticket Properties window.
Notes	An icon in this column indicates that a note has been added for the ticket. Click on the icon to read the note and add your own note, if necessary.
Last Modification Time	Date and time (per the database) that the ticket was last updated. Updates can result from either manual or automatic operations.
Root Event Time	Date and time that the event that created the root cause alarm of the ticket was detected.
Description	Description of the event, such as “Layer 2 tunnel down.”
Location	Hyperlink to the entity that triggered the event.
Acknowledged	Whether the ticket is acknowledged or has been modified: Yes, No, or Modified.
Creation Time	Date and time that the ticket was created.
Event Count	Number of events associated with the ticket.
Affected Devices Count	Number of devices affected by the ticket (the sources of the alarm and their subsequent alarms).
Duplication Count	For tickets, the duplication count is the sum of the duplication counts of all events that are associated with the root alarm.
Reduction Count	Ticket reduction count is the sum of reduction counts of all the events that are associated to the ticket. The History tab in the Ticket Properties window displays one reduction count for each event listed. For more information, see Chapter 9, “Working with Tickets in Cisco Prime Network Vision.”
Alarm Count	Total number of alarms associated with the ticket, including the root alarm.

For information about viewing ticket properties, see Viewing Ticket Properties, page 8-19.

V1 Trap Tab

This event is triggered when the network element sends a trap message to Prime Network because of a network event, such as Link Down. The V1 Trap tab displays detailed information specific to this category. Additional information specific to each event category can be viewed in the Event Properties window.

Table 8-10 describes the information that is displayed in the V1 Trap tab.

Table 8-10 V1 Trap Tab

Column	Description
Severity	Icon indicating the severity of the alarm on the event (the color and type of alarm are displayed in the Properties window Severity field). See Event Status Indicators, page 7-5.
Event ID	Calculated correlation identifier.
Time	Date and time when the event happened and was logged and recorded.
Description	Description of the event, such as “Enterprise generic trap.”
Location	Hyperlink to the entity that triggered the trap.
Alarm ID	Identifier of the alarm associated with the event, hyperlinked to the Alarm Properties window.
Ticket ID	Hyperlinked sequential identifier of the ticket. Click the link to view the Ticket Properties window.
Causing Event ID	Identifier of the causing event, hyperlinked to the Network Event Properties window.
Duplication Count	For network events, the duplication count is calculated by the VNE and pertains only to flapping events. The duplication count represents the number of noncleared events aggregated by the flapping event.
Reduction Count	For network events, the reduction count is calculated by the VNE and pertains only to flapping events. The reduction count represents the number of events that are aggregated by the flapping event.

For more information about the Cisco IOS and Cisco IOX traps displayed in one of these tabs, see the *Cisco Prime Network 3.9 Reference Guide*.

V2 Trap Tab

This event is triggered when the network element sends a trap message to Prime Network because of a network event. The V2 Trap tab displays detailed information specific to this category. Additional information specific to each event category can be viewed in the Event Properties window.

Table 8-11 describes the information that is displayed in the V2 Trap tab.

Table 8-11 V2 Trap Tab

Column	Description
Severity	Icon indicating the severity of the alarm on the event (the color and type of alarm are displayed in the Properties window Severity field). See Event Status Indicators, page 7-5.
Event ID	Calculated correlation identifier.
Time	Date and time when the event happened and was logged and recorded.
Description	Description of the event, such as "SNMP authentication failure."
Location	Hyperlink to the entity that triggered the trap.
Alarm ID	Identifier of the alarm associated with the event, hyperlinked to the Alarm Properties window.
Ticket ID	Sequential identifier of the ticket, hyperlinked to the Ticket Properties window.
Causing Event ID	Identifier of the causing event, hyperlinked to the Network Event Properties window.
Duplication Count	For network events, the duplication count is calculated by the VNE and pertains only to flapping events. The duplication count represents the number of noncleared events aggregated by the flapping event.
Reduction Count	For network events, the reduction count is calculated by the VNE and pertains only to flapping events. The reduction count represents the number of events that are aggregated by the flapping event.
Trap Type OID	Trap object identifier.
Translated Enterprise	Translation of the OID using the MIB. For example, an enterprise OID of .1.3.6.1.2.1.88.2 is displayed in this column as .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIB NotificationPrefix.
Enterprise	Enterprise OID for the trap, representing the company or organization that is associated with the trap.

For more information about the Cisco IOS and Cisco IOX traps displayed in this tab, see the *Cisco Prime Network 3.9 Reference Guide*.

V3 Trap Tab

This event is triggered when the network element sends a trap message to Prime Network because of a network event. The V3 Trap tab displays detailed information specific to this category. Additional information specific to each event category can be viewed in the Event Properties window.

Table 8-12 describes the information that is displayed in the V3 Trap tab.

Table 8-12 V3 Trap Tab

Column	Description
Severity	Icon indicating the severity of the alarm on the event (the color and type of alarm are displayed in the Properties window Severity field). See Event Status Indicators, page 7-5.
Event ID	Calculated correlation identifier.
Time	Date and time when the event happened and was logged and recorded.
Description	Description of the event, such as “Enterprise generic trap.”
Location	Hyperlink to the entity that triggered the trap.
Alarm ID	Identifier of the alarm associated with the event, hyperlinked to the Alarm Properties window.
Ticket ID	Sequential identifier of the ticket, hyperlinked to the Ticket Properties window.
Causing Event ID	Identifier of the causing event, hyperlinked to the Network Event Properties window.
Duplication Count	For network events, the duplication count is calculated by the VNE and pertains only to flapping events. The duplication count represents the number of noncleared events aggregated by the flapping event.
Reduction Count	For network events, the reduction count is calculated by the VNE and pertains only to flapping events. The reduction count represents the number of events that are aggregated by the flapping event.
Trap Type OID	Trap object identifier.
Translated Enterprise	Translation of the OID using the MIB. For example, an enterprise OID of .1.3.6.1.2.1.88.2 is displayed in this column as .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIB NotificationPrefix.
Enterprise	Enterprise OID for the trap, representing the company or organization that is associated with the trap.

For more information about the Cisco IOS and Cisco IOX traps displayed in this tab, see the *Cisco Prime Network 3.9 Reference Guide*.

Viewing 3.6.x Tabs

If you upgrade to Prime Network 3.9 from Cisco ANA 3.6.x, you can view the following tabs by choosing **File > Open 3.6.x Tabs**:

- 3.6.x Ticket
- 3.6.x Service
- 3.6.x Syslog
- 3.6.x V1 Trap
- 3.6.x V2-V3 Trap

Table 8-13 describes the information that is displayed in each of the 3.6.x tabs.

Table 8-13 3.6.x Tab Contents in Events

Field	Description
3.6.x Ticket Tab	
Severity	Icon of a bell, colored according to the severity of the alarm on the ticket. For more information, see Event Status Indicators, page 7-5.
Ticket ID	Sequentially assigned identifier of the ticket.
Short Description	Description of the event.
Location	Hyperlink to the entity that triggered the event.
Last Modification Time	Date and time (per the database) that the ticket was last updated. Updates can result from either manual or automatic operations.
Time	Date and time recorded when the first event happened.
Acknowledged	Status of the ticket: Acknowledged, Not Acknowledged, or Modified.
Affected Devices Count	Number of devices affected by the ticket (the sources of the alarm and their subsequent alarms).
Correlation Count	Number of correlated alarms included in the ticket.
Reduction Count	Ticket reduction count is the sum of reduction counts of all the events that are associated to the ticket. The History tab in the Ticket Properties window displays one reduction count for each event listed. For more information, see Chapter 9, "Working with Tickets in Cisco Prime Network Vision."
Duplication Count	For tickets, the duplication count is the sum of the duplication counts of all events that are associated with the root alarm.
3.6.x Service Tab	
Severity	Icon of a bell, colored according to the severity of the alarm. For more information, see Event Status Indicators, page 7-5.
Alarm ID	Sequentially assigned identifier of the alarm.
Short Description	Description of the event.
Location	Hyperlink to the entity that triggered the event.
Time	Date and time recorded when the first event happened.
3.6.x Syslog Tab	
Severity	Icon of a bell, colored according to the severity of the alarm. For more information, see Event Status Indicators, page 7-5.
Alarm ID	Sequentially assigned identifier of the alarm.
Short Description	Description of the event.
Location	Hyperlink to the entity that triggered the event.
Time	Date and time recorded when the first event happened.

Table 8-13 3.6.x Tab Contents in Events (continued)

Field	Description
3.6.x V1 Trap Tab	
Severity	Icon of a bell, colored according to the severity of the alarm. For more information, see Event Status Indicators, page 7-5.
Alarm ID	Sequentially assigned identifier of the alarm.
Short Description	Description of the event.
Location	Hyperlink to the entity that triggered the event.
Time	Date and time recorded when the first event happened.
Suppress Display	Whether or not the display of the alarm is suppressed.
3.6.x V2-V3 Trap Tab	
Severity	Icon of a bell, colored according to the severity of the alarm. For more information, see Event Status Indicators, page 7-5.
Alarm ID	Sequentially assigned identifier of the alarm.
Short Description	Description of the event.
Location	Hyperlink to the entity that triggered the event.
Time	Date and time recorded when the first event happened.
Suppress Display	Whether or not the display of the alarm is suppressed.

Working with Cisco Prime Network Events

The following topics describe how to view, filter, and display the properties of specific events and tickets, and how to refresh and export events:

- Viewing Event Properties, page 8-14
- Viewing Ticket Properties, page 8-19
- Refreshing Cisco Prime Network Events Information, page 8-21
- Filtering Events, page 8-22
- Exporting Displayed Data, page 8-25

Viewing Event Properties

Cisco Prime Network Events enables you to view the properties of a specific event type. The Event Properties window displays detailed information about the event; for example, the severity and the number of affected parties.

Tip Clicking **Detailed Pane** on the displays the properties of the selected ticket or event in the Properties pane.

To view event properties:

Step 1 Select the required tab for the specific event type and the event in the Cisco Prime Network Events window.

Step 2 Do one of the following:

- Double-click the event in the events list.
- Click **Detailed Pane** in the toolbar.
- Choose **View > Properties** from the main menu.
- Right-click the event and choose **Properties**.

The event properties are displayed for the selected event, either in the lower portion of the Cisco Prime Network Events window or in a separate window as shown in Figure 8-2. The Details tab is displayed by default.

Figure 8-2 Event Properties Window - Details Tab

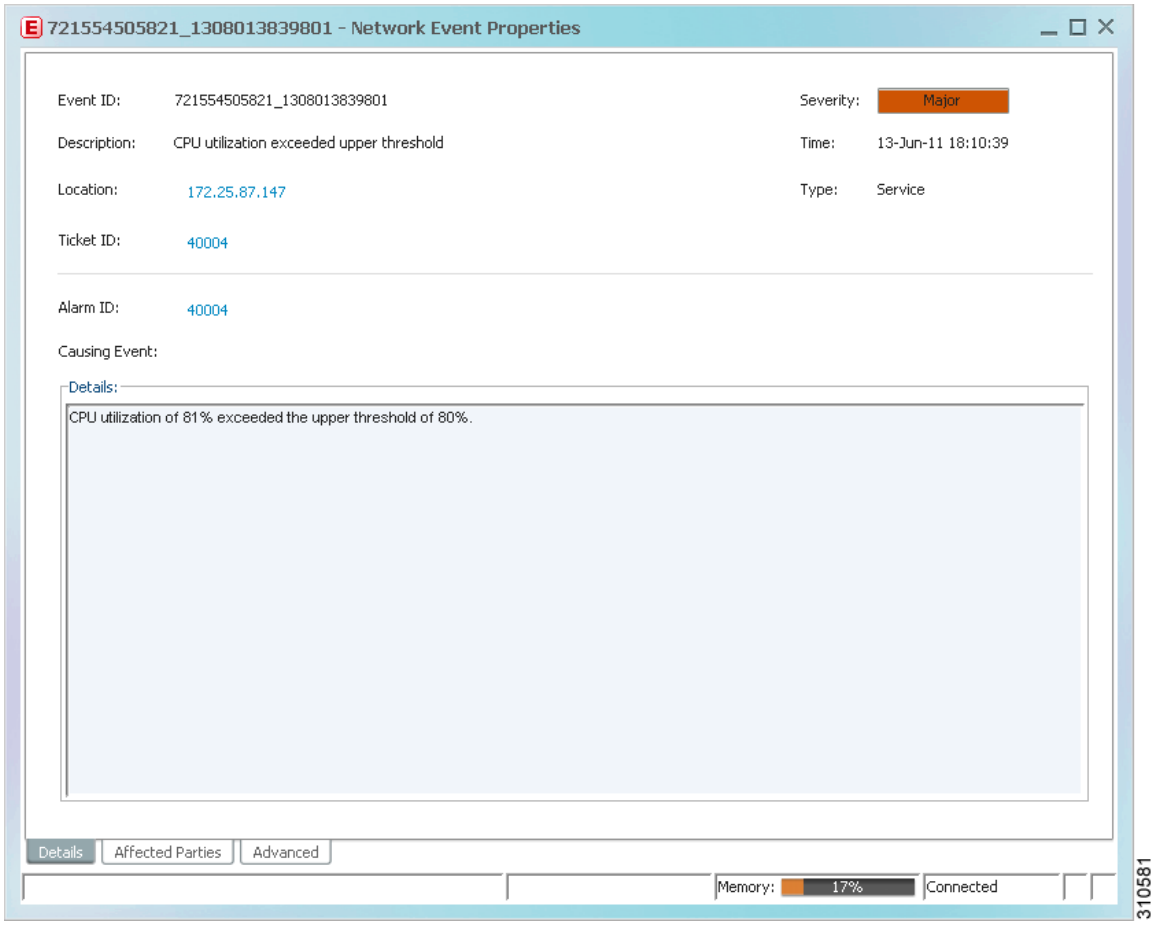


Table 8-14 describes the information that is displayed in the Details tab in the Event Properties window.

Table 8-14 Details Tab for Events

Field	Description
Event ID	Unique identifier for the selected event.
Severity	Severity of the event, indicated by color and text label.
Description	Description of the event.
Time	Date and time when the event happened and was logged and recorded.
Location	Entity that triggered the event, hyperlinked to its entry in inventory.
Type	Type of event, such as Security or Service.
Ticket ID	This field is displayed only for network events. Sequential identifier of the ticket, hyperlinked to the Ticket Properties window.
Alarm ID	This field is displayed only for network events. Alarm identifier, hyperlinked to the Ticket Properties window.
Causing Event	This field is displayed only for network events. The identifier of the causing event.
Details	Detailed description of the event.

Step 3 You can view additional properties in the following tabs:

- Advanced tab—See Table 8-15 on page 8-17.
- Affected Parties tab—See Table 9-12 on page 9-15.
- Audit tab—See Table 8-16 on page 8-17.
- Provisioning tab—See Table 8-17 on page 8-17.
- Security tab—See Table 8-18 on page 8-18.
- Trap tab—See Table 8-19 on page 8-18.

The tabs that are displayed depend on the type of event, such as a Service event or a Provisioning event.

Table 8-15 Advanced Tab

Field	Description
Duplication Count	For network events, the duplication count is calculated by the VNE and pertains only to flapping events. The duplication count represents the number of noncleared events aggregated by the flapping event.
Reduction Count	For network events, the reduction count is calculated by the VNE and pertains only to flapping events. The reduction count represents the number of events that are aggregated by the flapping event.
Affected Devices	The number of devices affected by the ticket.
Alarm Count	The total number of alarms associated with the ticket, including the root alarm.

Table 8-16 Audit Tab

Field	Description
User Name	Name of user who initiated the command.
Result	Command result, if available.
Originating IP	IP address of the client that issued the command.
Command Signature	Actual command run by Prime Network, such as **GetEventViewerProperties**.
Command Parameters	Parameters applied to the command.

Table 8-17 Provisioning Tab

Field	Description
User Name	Name of the user who performed the provisioning operation.
Status	Status of the operation: Success or Fail.

Table 8-18 Security Tab

Field	Description
User Name	Name of the user who triggered the event.
Client Type	Client that triggered the event: Cisco Prime Network Vision, Cisco Prime Network Administration, Cisco Prime Network Events, or Unknown.
Originating IP	IP address of the client where the event was triggered.

Table 8-19 Trap Tab

Field	Description
Version	SNMP version: version-1, version-2c, or version-3.
Community String	Community that the device sends in the Protocol Data Unit (PDU).
Error Status	Error status: No Error, Too Big, No Such Name, Bad Value, Read Only, and Gen Err.
Values Table	
Translated OID	String representation of the OID. For example, 1.3.6 is translated into iso.org.dod where: • 1 represents iso. • 3 represents org. • 6 represents dod.
Translated Value	String representation of the OID value. For example, 1.3 is translated to iso(1).org.10, or a specific value, such as “down” or “4 days, 20 hours, 32 minutes, 11 seconds.”
OID	OID that is not translated. It is a dot notation representation of the OID, such as 1.3.6.1.4.1.9.
Value	Value that is not translated.

The properties of a selected ticket can be viewed in the Ticket Properties window. For a detailed description of the Ticket tab properties, see Viewing Ticket Properties, page 8-19.

Viewing Ticket Properties

You can view the properties of a selected ticket in Cisco Prime Network Events by displaying the Ticket Properties window.

To view ticket properties in Cisco Prime Network Events:

Step 1 In the Ticket tab in the Cisco Prime Network Events window, select the required ticket.

Step 2 Do one of the following:

- Double-click the ticket.
- Click **Detailed Pane** in the toolbar.
- Choose **View > Properties** from the main menu.
- Right-click the ticket and choose **Properties**.

The properties are displayed for the selected ticket, either in the lower portion of the Cisco Prime Network Events window or in a separate window as shown in Figure 8-3.

Figure 8-3 Ticket Properties Window - Details Tab

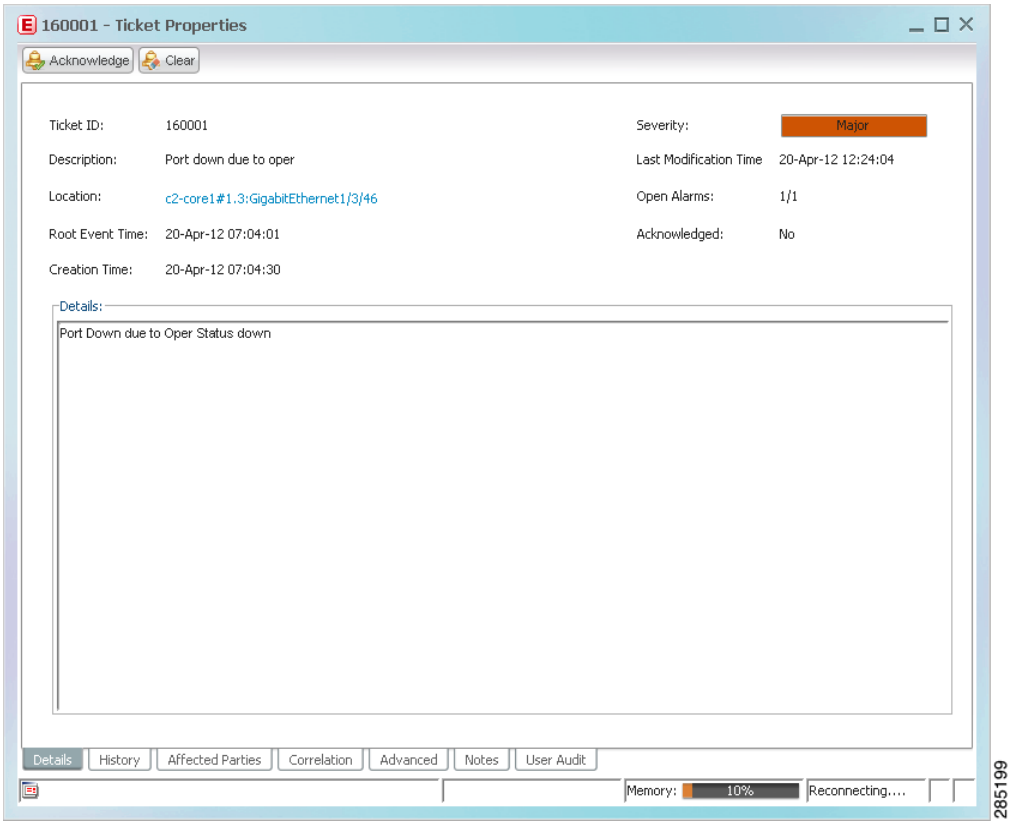


Table 8-20 describes the information that is displayed in the Details tab in the Ticket Properties window.

Table 8-20 Ticket Properties Window - Details Tab

Field	Description
Buttons	
Acknowledge	Acknowledges that the ticket is being handled. The status of the ticket is displayed as true in the ticket pane and in the Ticket Properties dialog box. For more information, see Acknowledged Ticket, page 9-7. If a ticket is acknowledged, and events are correlated to it after correlation, the ticket is considered to have not been acknowledged. This button is enabled only if the ticket is not acknowledged.
Clear	Requests the Prime Network system to remove the faulty network element from the Prime Network networking inventory. In addition, it sets the ticket to Cleared severity or status and automatically changes the acknowledged status of the ticket to Yes. For more information, see Cleared Ticket, page 9-7. This button is enabled only if the severity of the alarm is higher than Cleared or Normal.
Details Tab	
Ticket ID	Sequentially assigned identifier of the ticket.
Severity	Severity of the ticket, indicated by color and text label.
Description	Description of the ticket.
Last Modification Time	Date and time (per the database) that the ticket was last updated. Updates can result from either manual or automatic operations.
Location	Hyperlink to the entity that triggered the event. **Note** If the entity that triggered the event is outside your scope, a message is displayed that states you do not have permission to access the selected item.
Open Alarms	Number of open alarms out of all alarms, such as 3/4.
Root Event Time	Date and time that the event that created the root cause alarm of the ticket was detected.
Acknowledged	Whether or not the ticket has been acknowledged: Yes or No.
Creation Time	Date and time when the ticket was created.
Details	Detailed description of the ticket.

Step 3 As required, review additional properties for the ticket.

Table 8-21 identifies the additional tabs that are displayed in the Ticket Properties window and links to the relevant information.

Table 8-21 Ticket Properties Window - Additional Tabs

Tab	Description
History	Contains the history of the ticket, including all the events. For more information, see History Tab, page 9-13.
Affected Parties	The services (affected pairs) that are potentially affected (potential impact analysis) by the ticket. For more information, see Affected Parties Tab, page 9-14.
Correlation	Displays all alarms that are correlated to the selected ticket. For more information, see Correlation Tab, page 9-17.
Advanced	The number of affected devices, correlations, duplications, and reductions for the selected ticket. In addition, it provides any other additional information available about the ticket. For more information, see Advanced Tab, page 9-18.
Notes	Enables you to add and save notes for the selected ticket. The Notes tab is not available for tickets that have been archived. For more information, see Notes Tab, page 9-18.
User Audit	Enables you to see which ticket-related actions were carried out by which users, and when the action took place. For more information, see User Audit Tab, page 9-19.

Refreshing Cisco Prime Network Events Information

Cisco Prime Network Events displays current information in lists in each tab. While you view a list, the information is not updated unless you manually refresh the list or activate autorefresh. The default autorefresh setting is 60 seconds and can be adjusted (see Selecting Prime Network Events Viewing Options, page 7-10). Your filter settings remain intact.

Table 8-22 shows the refresh buttons.

Table 8-22 Cisco Prime Network Events Refresh Buttons

Button	Name	Function
	Refresh Now	Manually refreshes the events list.
	Auto Refresh	Automatically refreshes the events list. The Auto Refresh icon toggles to indicate whether auto refresh is on or off. This icon indicates auto refresh is on.

To manually refresh a list, do one of the following:

- Click **Refresh Now** in the main toolbar.
- Choose **View > Refresh** from the main menu.

To automatically refresh a list, click **Auto Refresh** in the toolbar.

Filtering Events

The Filter Events dialog box allows you to filter events according to a number of criteria including severity, identifier, time stamp, description, location, and category-specific information.

You may also use the filter to search for information in the database.

The Filter icon toggles to indicate that a filter has been applied.

The following settings in the Cisco Prime Network Events Options dialog box also affect your filters:

- If you check the Keep Last Filter check box, the currently defined filter settings are saved in the registry and are displayed the next time you log in, but are not applied.
- If you check the Open Using Filter check box, the events are continuously filtered according to the defined settings, even when you log out of and back into the application.

For more information, see Selecting Prime Network Events Viewing Options, page 7-10.

See the following topics for more information about filtering events:

- Defining Filters, page 8-23
- Removing Filters, page 8-24

For information about filtering tickets, see Filtering Tickets by Criteria, page 9-8.

Defining Filters

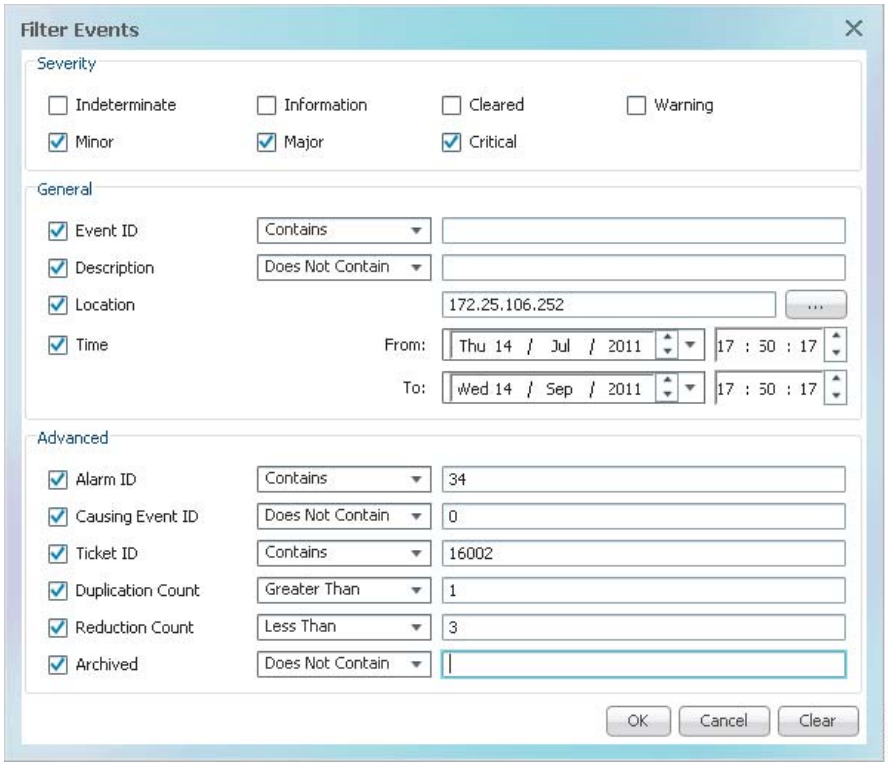
To define a filter:

Step 1 Do one of the following:

- Choose **Edit > Filter** from the main menu.
- Click **Filter** in the main toolbar.

The criteria that you can use for filtering differs for events and tickets. For example, Figure 8-4 shows the Filter Events dialog box for service events. For an example of the Ticket Filter dialog box, see Figure 9-2 on page 9-9.

Figure 8-4 Filter Events Dialog Box - Service Events



Step 2 Specify the filter criteria by using the following steps and the information in Table 8-23:

a. Check the check box for each criterion to use for filtering.

b. As needed, choose the operator for the filter, such as Contains or Does Not Contain.

c. Supply the specific information to apply to the filter, such as the time, a string, or one or more IP addresses.

Table 8-23 Cisco Prime Network Events Filter Events Options

Field	Description
Severity	Severities to be included in the filter.
General	
Event ID	Event identifier to apply to the filter.
Description	String to include or exclude.
Location	Network elements to include. This field is not displayed for Audit events.
Time	Beginning and ending dates and times to apply to the filter.
Network Events Advanced Options	
Alarm ID	Alarm identifier to apply to the filter.
Causing Event ID	Identifier of the causing event to apply to the filter.
Ticket ID	Ticket identifier to apply to the filter.
Duplication Count	Duplication count value to use for filtering.
Reduction Count	Reduction count value to use for filtering.
Archived	Archive status to use for filtering: True or False.
System Events Advanced Options	
Command Name	String in the command name to use for filtering.
Command Signature	String in the command signature to use for filtering.
Command Parameters	String in a command parameter to use for filtering.
Originating IP	Originating IP address to include or exclude from filtering.
Status	Status to use for filtering: Configuring, Fail, Success, or Unknown.
User Name	String in the username to use for filtering.

Step 3 Click **OK** to save your filter settings and apply the filter. The filtered entries are displayed in the list according to the defined criteria.

Removing Filters

To remove a filter:

Step 1 Click **Filter** in the main toolbar.

Step 2 In the Filter Events dialog box, click **Clear**. The selected options in the Filter Events dialog box are cleared.

Step 3 Click **OK**. All events are displayed in the list.

Exporting Displayed Data

Cisco Prime Network Events enables you to export the currently displayed data from the Cisco Prime Network Events table according to the criteria defined in the Cisco Prime Network Events Options dialog box. You can then import and view at a later time.

To export a table to a file:

Step 1 Choose **File > Export**.

Step 2 In the Export Table to File dialog box, browse to the directory where you want to save the list.

Step 3 In the File name field, enter a name for the list.

Step 4 Click **Save**. The displayed events list or rows are saved in the selected directory.



CHAPTER 9

Working with Tickets in Cisco Prime Network Vision

This chapter covers the following topics:

- Tickets - Overview, page 9-1
- User Roles Required to Work with Tickets in Prime Network Vision, page 9-1
- Viewing Tickets and Network Events for Elements in a Map, page 9-3
- Viewing Ticket Properties, page 9-10
- Managing Tickets, page 9-19
- Impact Analysis in Prime Network, page 9-22

Tickets - Overview

A ticket represents the complete hierarchy of correlated alarms representing a single specific fault scenario. A ticket points to the root cause alarm that is the top-most alarm in the correlation hierarchy. Examples of alarms are Link Down, Device Unreachable, or Module Out. Some event types are capable of creating tickets. When an event is generated, it is correlated to an existing event, which is correlated to a ticket. If there is no existing ticket, a new ticket is created.

Prime Network identifies the relationship between a root cause alarm and its consequent alarms. It automatically correlates the consequent alarms as children of the root alarm. The ticket pane displays the ticket (the root cause alarm), the aggregated severity of the ticket, and the severity of the root cause alarm. The root cause alarm severity is the top-most severity of its contained alarms. In addition, the ticket pane displays the time at which the original event was detected, the ticket creation time, and a description of the event that caused the ticket creation.

User Roles Required to Work with Tickets in Prime Network Vision

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

- For GUI-based tasks (tasks that do not affect elements), authorization is based on the default permission that is assigned to your user account.

- For element-based tasks (tasks that do affect elements), authorization is based on the default permission that is assigned to your account. That is, whether the element is in one of your assigned scopes and whether you meet the minimum security level for that scope.

For more information on user authorization, see the topic on device scopes in the *Cisco Prime Network 3.9 Administrator Guide*.

The following conditions apply when working with tickets in Prime Network Vision:

- If an element that is outside of your scope is the root cause of a ticket that affects an element in your scope, you can view the ticket in Prime Network Vision, but you will not be able to:
  - View inventory by clicking the Location hyperlink.
  - Acknowledge, clear, or remove the ticket.
- You can acknowledge, clear, remove, or add notes for a ticket only if you have OperatorPlus or higher permission for the element that holds the root alarm for that ticket.
- If the source or contained sources of the ticket are not in your scope, you cannot view the ticket in the ticket table, view ticket properties, or perform actions on the ticket.
- If the ticket contains a source that is in your scope, but the source is not the root cause, you can view the ticket in the ticket table and view ticket properties, but you cannot perform actions on the ticket.
- If the source of the ticket is in your scope, you can view the ticket in the ticket table, view ticket properties, filter tickets, and perform actions on the ticket.
- By default, users with the Administrator role have access to all managed elements and can perform any action on tickets. To change the Administrator user scope, see the topic on device scopes in the *Cisco Prime Network 3.9 Administrator Guide*.

Table 9-1identifies the roles required to perform the high level tasks:

Table 9-1 Default Roles/Permissions Required for Working with Tickets in Prime Network Vision

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Acknowledge tickets	—	—	X[1]	X	X
Add notes to a ticket	—	—	X[1]	X	X
Clear and remove tickets	—	—	X[1]	X	X
Clear tickets	—	—	X[1]	X	X
Filter tickets	X	X	X	X	X
Find affected elements	X	X	X	X	X
Remove tickets	—	—	X[1]	X	X
View ticket properties	X	X	X	X	X
View tickets	X	X	X	X	X

1. In addition, the security level for the device scope must be OperatorPlus or higher for the device that holds the root alarm for a ticket.

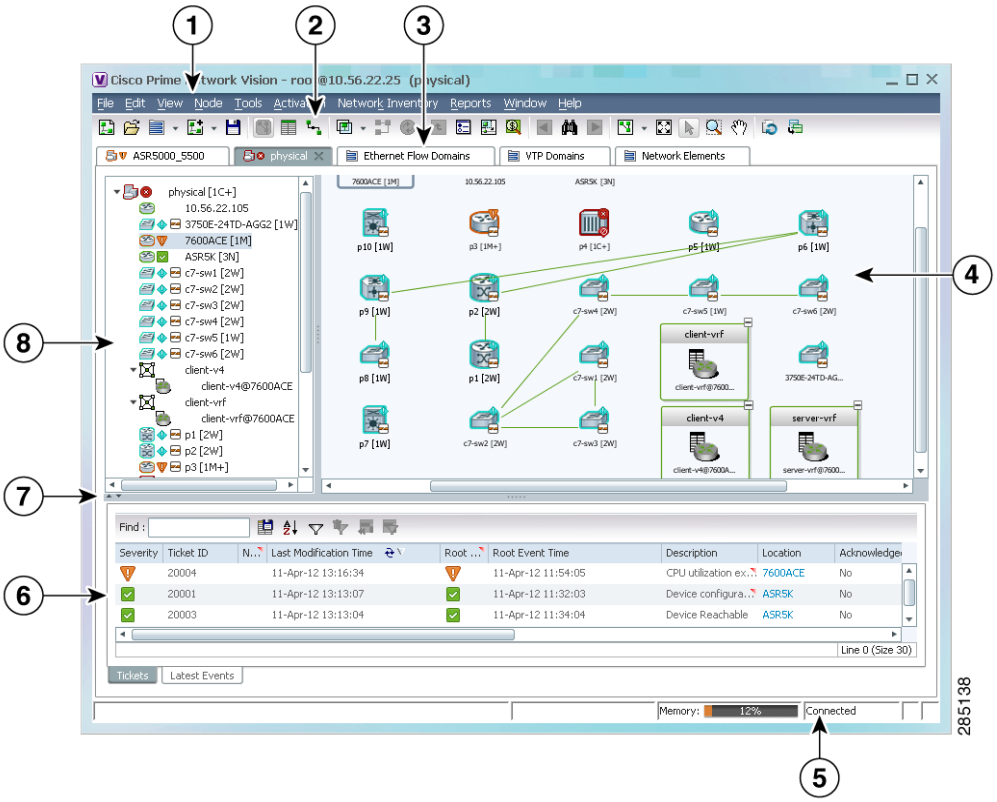
Viewing Tickets and Network Events for Elements in a Map

The ticket pane, located below the navigation and content panes in the Prime Network Vision window, displays tickets and network events specific to the elements in the currently displayed map (see Figure 9-1). You can view or hide the ticket pane by clicking the arrows displayed below the navigation pane.

The ticket pane contains two tabs:

- Tickets tab—Lists all the tickets relevant to the elements in the map and allows you to manage them. See Managing Tickets in the Tickets Tab, page 9-4 for details of the information displayed and the actions available from the Tickets tab.
- Latest Events tab:
  - Lists network events that were created for the elements in the map from the time the map was opened.
  - Shows network events that Prime Network recognizes and is able to process (actionable events). Some of these events might be correlated into tickets.
  - An hourglass in the Status column indicates that processing of the event is in progress. A check mark indicates that the event has been processed.
  - If an event has been correlated into a ticket, the ticket ID will appear in the table and you can click the link to access the ticket properties.
  - Events are removed from the Latest Events tab after 6 hours or when a maximum of 15000 events is reached, in which case the oldest events are removed first.

Figure 9-1 Prime Network Vision Window



1	Menu bar	**5**	Status bar
2	Toolbar	**6**	Ticket pane
3	Inventory and map tabs	**7**	Hide/Display ticket pane
4	Content pane	**8**	Navigation pane

Managing Tickets in the Tickets Tab

Table 9-2 describes the functions that are available from the Tickets tab in the ticket pane.

Table 9-2 Ticket Pane Available Functions

Function	Related Documentation
Acknowledge a ticket.	Acknowledging a Ticket, page 9-19
Clear a ticket.	Clearing a Ticket, page 9-20
Clear and remove a ticket.	Clearing and Removing Tickets, page 9-21
Filter and view all tickets that meet specific criteria.	Filtering Tickets by Criteria, page 9-8

Table 9-2 Ticket Pane Available Functions (continued)

Function	Related Documentation
Locate the elements or links affected by the ticket in the map or links view.	Finding Affected Elements, page 9-19
Remove a ticket.	Removing a Ticket, page 9-21
View all tickets or only the filtered tickets of a selected element.	Filtering Tickets by Network Element, page 9-8
View tickets.	Viewing Tickets and Network Events for Elements in a Map, page 9-3
View ticket properties, including the history, correlated alarms, severity of the root cause alarm, and affected parties.	Viewing Ticket Properties, page 9-10

Table 9-3 describes the information displayed in the ticket pane.

Table 9-3 Ticket Information Displayed in the Ticket Pane

Field Name	Description
Severity	Severity of alarm, represented by an icon. The icon and its color indicate the alarm severity and thereby the impact of the alarm on the network. For more information about severity, see Map View, page 2-10. • Red—Critical • Orange—Major • Yellow—Minor • Light Blue—Warning • Green—Cleared, Normal, or OK • Medium Blue—Informational • Dark Blue—Indeterminate
Ticket ID	Ticket identifier, assigned sequentially. Click the hyperlinked entry to view ticket properties, and to acknowledge, clear, or refresh the ticket. For more information, see Chapter 9, "Working with Tickets in Cisco Prime Network Vision."
Notes	An icon in this column indicates that a note has been added for the ticket. Click on the icon to read the note and add your own note, if necessary.
Last Modification Time	Date and time (per the database) that the ticket was last updated. Updates can result from either manual or automatic operations.
Root Cause	Severity of the root cause alarm, represented by a bell icon. The color indicates the severity of the root cause alarm, as described in the Severity field.
Root Event Time	Date and time that the event that created the root cause alarm of the ticket was detected.
Description	Description of the event that caused the ticket creation.
Location	Entity that triggered the ticket, as a hyperlink that displays the relevant location in the inventory.

Table 9-3 Ticket Information Displayed in the Ticket Pane (continued)

Field Name	Description
Acknowledged	Whether the ticket is acknowledged or has been modified: Yes, No, or Partially Acknowledged. If the ticket is acknowledged, this field also displays the user who acknowledged the ticket; for example, Yes(root).
Creation Time	Date and time (per the database) that the ticket was created.
Event Count	Number of events associated with the ticket.
Affected Devices Count	Number of devices affected by the ticket, including the sources of the alarm and their subsequent alarms.
Duplication Count	For network events, the duplication count is calculated by the VNE and pertains only to flapping events. The duplication count represents the number of noncleared events aggregated by the flapping event. For tickets, the duplication count is the sum of the duplication counts of all events that are associated with the root alarm.
Reduction Count	For network events, the reduction count is calculated by the VNE and pertains only to flapping events. The reduction count represents the number of events that are aggregated by the flapping event. Ticket reduction count is the sum of reduction counts of all the events that are associated to the ticket. The History tab in the Windows Properties window displays one reduction count for each event listed.
Alarm Count	Total number of alarms associated with the ticket, including the root alarm.

The ticket details in the ticket pane change automatically as new information arrives. For example, Port Down is updated to Port Up.

By default, the tickets in the ticket pane are sorted according to the last modification time.

The Find field enables you to search for information in the ticket pane table according to the selected column. For more information about the buttons displayed in Prime Network Vision tables and table functionality, see Working with Prime Network Tables, page 2-49.

Understanding Ticket Status

The appearance of a ticket displayed in the ticket pane depends on the severity of the ticket and the operations that have been performed on the ticket. Tickets detailed in the ticket pane change when:

- A ticket is generated.
- A ticket is cleared.
- A ticket is acknowledged.
- An Up ticket is generated.
- A ticket is cleared and removed.
- A ticket is removed.
- Other properties are updated, such as severity, description, or counters.

Generated Ticket

Table 9-4 shows an example of the appearance of the ticket pane when a ticket is generated.

Table 9-4 Generated Ticket

Icon	Severity	Ticket ID	Short Description	Acknowledged
	Major	27	Port down	Yes

Cleared Ticket

Table 9-5 shows an example of the appearance of the ticket pane when a ticket is cleared.

Table 9-5 Cleared Ticket

Icon	Severity	Ticket ID	Short Description	Acknowledged
	Normal	27	Cleared due to Force Clear	Yes

A ticket that has been cleared can be removed from the ticket pane.

When a ticket is cleared, its definition automatically changes to acknowledged in the ticket pane and its definition in the Acknowledged column is Acknowledged.

Acknowledged Ticket

Table 9-6 shows an example of the appearance of the ticket pane when a ticket is acknowledged. When a ticket is acknowledged it can then be cleared and the severity changes to Normal.

Table 9-6 Acknowledged Ticket

Icon	Severity	Ticket ID	Short Description	Acknowledged
	Major	27	Port up	Yes



Note When a ticket with an Information severity is acknowledged, the ticket is automatically removed from the Prime Network gateway and from the ticket pane.

Generated Up Ticket

The cause of the alarm is fixed; therefore an Up ticket is automatically generated with a Normal severity. Table 9-7 shows an example of the appearance of the ticket pane when an Up ticket is generated.

Table 9-7 Generated Up Ticket

Icon	Severity	Ticket ID	Short Description	Acknowledged
	Normal	27	Port up	Yes

Filtering Tickets by Network Element

Prime Network Vision enables you to filter the tickets that are shown in the ticket pane so that you see only the tickets that have the selected network element as the root cause.

If the selected network element is alarmed due to an operation that occurred on a different VNE, element, or link, no tickets are displayed.

To view tickets that have a specific network element as the root cause, do either of the following:

- If the network element icon is at the largest size, click the **Filter Tickets** button.
- Right-click the required network element in the navigation pane or a map and choose **Filter Tickets**.

In response:

- The ticket pane displays only the tickets that have the selected network element as the root cause.
- The Filter button in the ticket pane toggles to indicate that a filter has been applied.

Click **Clear Filter** in the ticket pane to view all tickets.

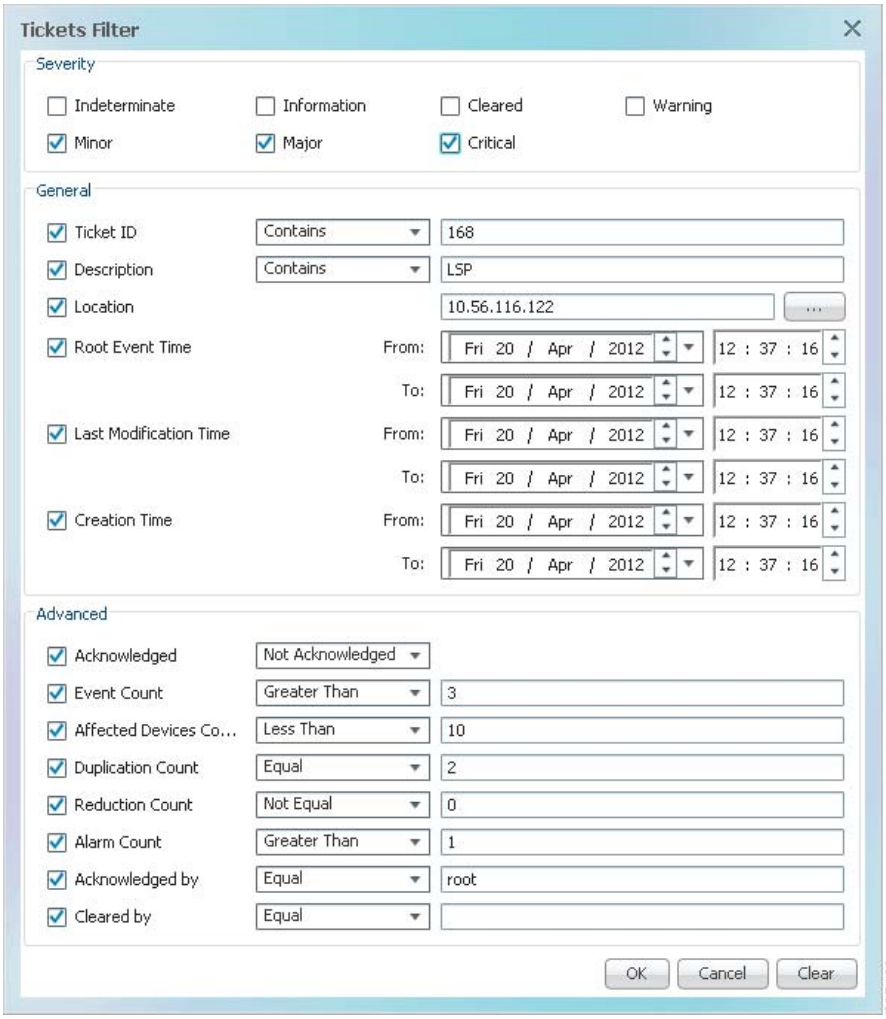
Filtering Tickets by Criteria

Prime Network Vision enables you to define a filter for the tickets displayed in the ticket pane according to various criteria. For example, tickets can be filtered according to the number of affected parties or acknowledged tickets.

To define a ticket filter:

Step 1 Click **Ticket Filter** in the ticket pane toolbar. The Ticket Filter dialog box is displayed (Figure 9-2).

Figure 9-2 Ticket Filter Dialog Box



Step 2 Specify the filter criteria by using the following steps and the information in Table 9-8:

a. Check the check box for each criterion to use for filtering.

b. As needed, choose the operator for the filter, such as Contains or Does Not Contain.

c. Supply the specific information to apply to the filter, such as the time, a string, or one or more IP addresses.

Table 9-8 Prime Network Ticket Filter Options

Field	Description
Severity	Severity to be included in the filter.
General	
Ticket ID	Ticket identifier to be included or excluded when filtering.
Description	String in the ticket description to include or exclude.
Location	Network elements to include.

Table 9-8 Prime Network Ticket Filter Options (continued)

Field	Description
Root Event Time	Beginning and ending dates and times of the range for the root event time to apply to the filter.
Last Modification Time	Beginning and ending dates and times of the range for the ticket last modification time to apply to the filter.
Creation Time	Beginning and ending dates and times of the range for the ticket creation time to apply to the filter.
Advanced	
Acknowledged	Ticket acknowledgement status to include in the filter: Acknowledged, Not Acknowledged, or Modified.
Event Count	Event count value to use for filtering.
Affected Devices Count	Number of affected devices to use for filtering.
Duplication Count	Duplication count value to use for filtering.
Reduction Count	Reduction count value to use for filtering.
Alarm Count	Alarm count value to use for filtering.
Archived	Archive status to use for filtering: True or False.
Acknowledged By	Username of the person who acknowledged the ticket.
Cleared By	Username of the person who cleared the ticket.

Step 3 Click **OK**. The tickets are displayed in the ticket pane according to the defined criteria.

Note The Ticket Filter button in the ticket pane toggles to indicate that a filter has been applied.

To remove a ticket filter:

Step 1 Click **Ticket Filter** in the ticket pane toolbar. The Ticket Filter dialog box is displayed.

Step 2 Click **Clear**. The selected options in the Ticket Filter dialog box are cleared.

Step 3 Click **OK**. All the tickets are displayed in the ticket pane.

Viewing Ticket Properties

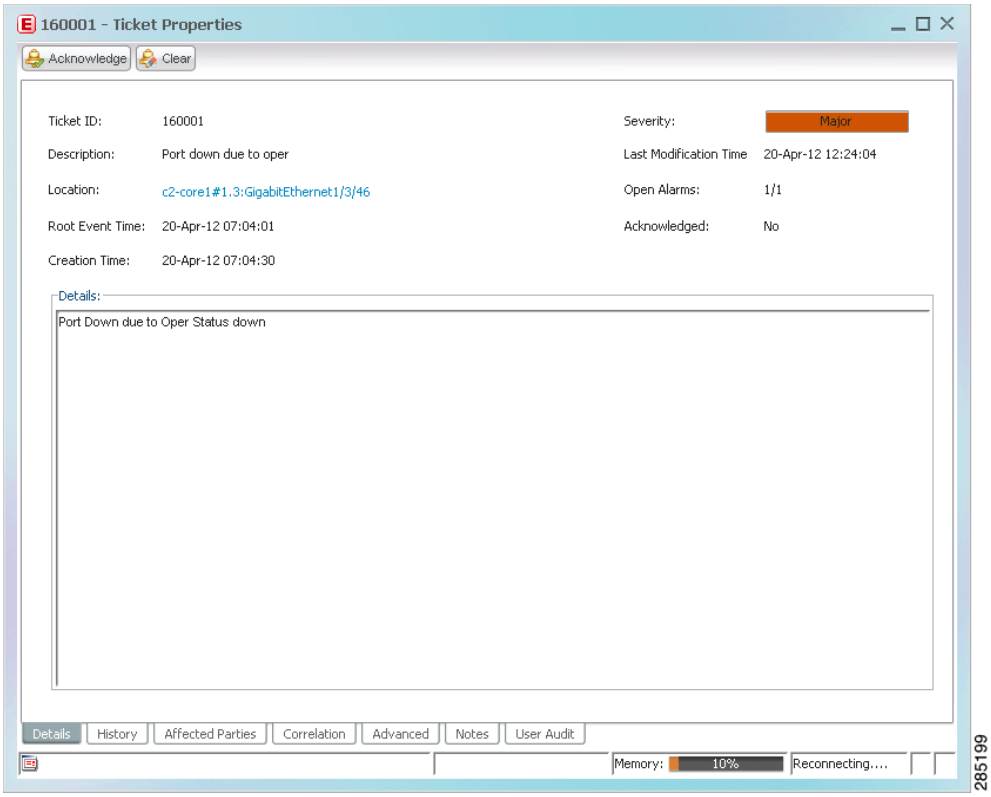
The properties of a selected ticket can be viewed by displaying the Ticket Properties window. For example, you can view alarm severity, correlated alarms, active alarms, alarm history, or the source of the alarm.

In Prime Network Vision, open the Ticket Properties window in one of the following ways:

- Open the required map and then double-click the required ticket identifier in the ticket pane.
- Open the required map, right-click a ticket in the ticket pane, and choose **Properties**.

Figure 9-3 shows the Ticket Properties window.

Figure 9-3 Ticket Properties Window



The information displayed in the Ticket Properties window corresponds with the information displayed in the Prime Network Vision ticket pane or the Prime Network Vision window. The ID number displayed in the header corresponds to the ID number of the ticket selected in the ticket pane.

The Ticket Properties window contains the following components:

- Ticket Properties Toolbar, page 9-12
- Details Tab, page 9-12
- History Tab, page 9-13
- Affected Parties Tab, page 9-14
- Correlation Tab, page 9-17
- Advanced Tab, page 9-18
- Notes Tab, page 9-18
- User Audit Tab, page 9-19

Ticket Properties Toolbar

The Ticket Properties window contains the tools described in Table 9-9.

Table 9-9 Ticket Properties Window Toolbar

Icon	Description
	Acknowledges that the ticket is being handled. The status of the ticket is displayed as true in the ticket pane and in the Ticket Properties dialog box. For more information, see Acknowledged Ticket, page 9-7. If a ticket was acknowledged, and some events were correlated to it afterward, then the ticket is considered to have not been acknowledged. This button is enabled only if the ticket is not acknowledged.
	Requests the relevant Prime Network system to remove the faulty network element from the Prime Network networking inventory. In addition, it sets the ticket to Cleared severity or status (the icon is displayed in green) and automatically changes the acknowledged status of the ticket to true. For more information, see Cleared Ticket, page 9-7. This button is enabled only if the severity of the alarm is higher than Cleared or Normal.
	Saves the notes for the selected ticket. This button is enabled only when text is entered in the Notes field of the Notes tab.

Details Tab

Table 9-10 describes the information that is displayed in the Details tab about the compiled alarm.

Table 9-10 Event Properties Window - Details Tab

Field	Description
Ticket ID	Ticket identifier.
Severity	Severity propagated from all the correlated alarms.
Description	Description of the ticket.
Last Modification Time	Date and time (per the database) that the ticket was last updated. Updates can result from either manual or automatic operations.
Location	Entity that triggered the root-cause alarm, as a hyperlink that opens the relevant location. **Note** If the entity that triggered the alarm is outside your scope, a message is displayed that states you do not have permission to access the selected item.
Open Alarms	Number of correlated alarms for the ticket that are open, such as 3/4. In this example, four indicates the total number of correlated alarms for the ticket, and three indicates the number of alarms that have not been cleared. Therefore, one alarm has been cleared.

Table 9-10 Event Properties Window - Details Tab (continued)

Field	Description
Root Event Time	Date and time that the event that created the root cause alarm of the ticket was detected.
Acknowledged	Whether the alarm has been acknowledged: Yes or No. If the alarm is acknowledged, this field also displays the user who acknowledged the alarm; for example, Yes(root).
Creation Time	Date and time the ticket was created.
Details	Detailed description of the alarm.

History Tab

The History tab enables you to display the history of the ticket, including all the events. Figure 9-4 shows the History tab.

Figure 9-4 History Tab

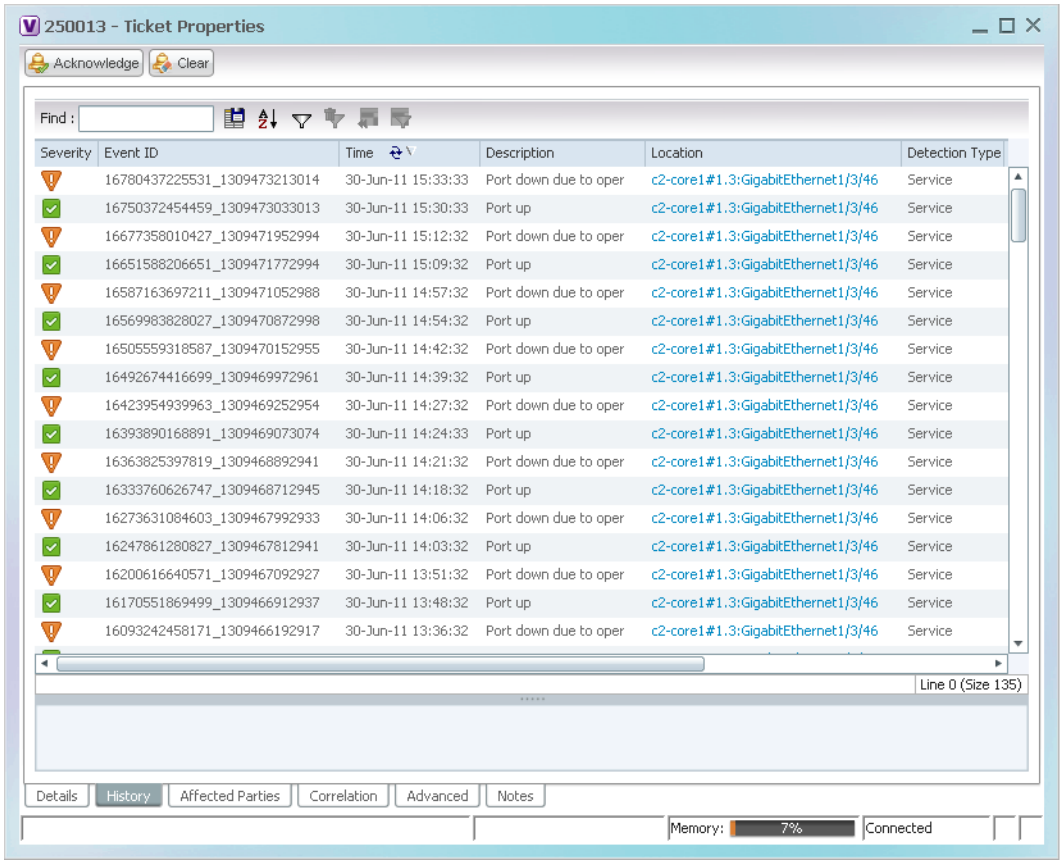


Table 9-11 describes the information that is displayed in the History tab.

Table 9-11 Ticket Properties Window - History Tab

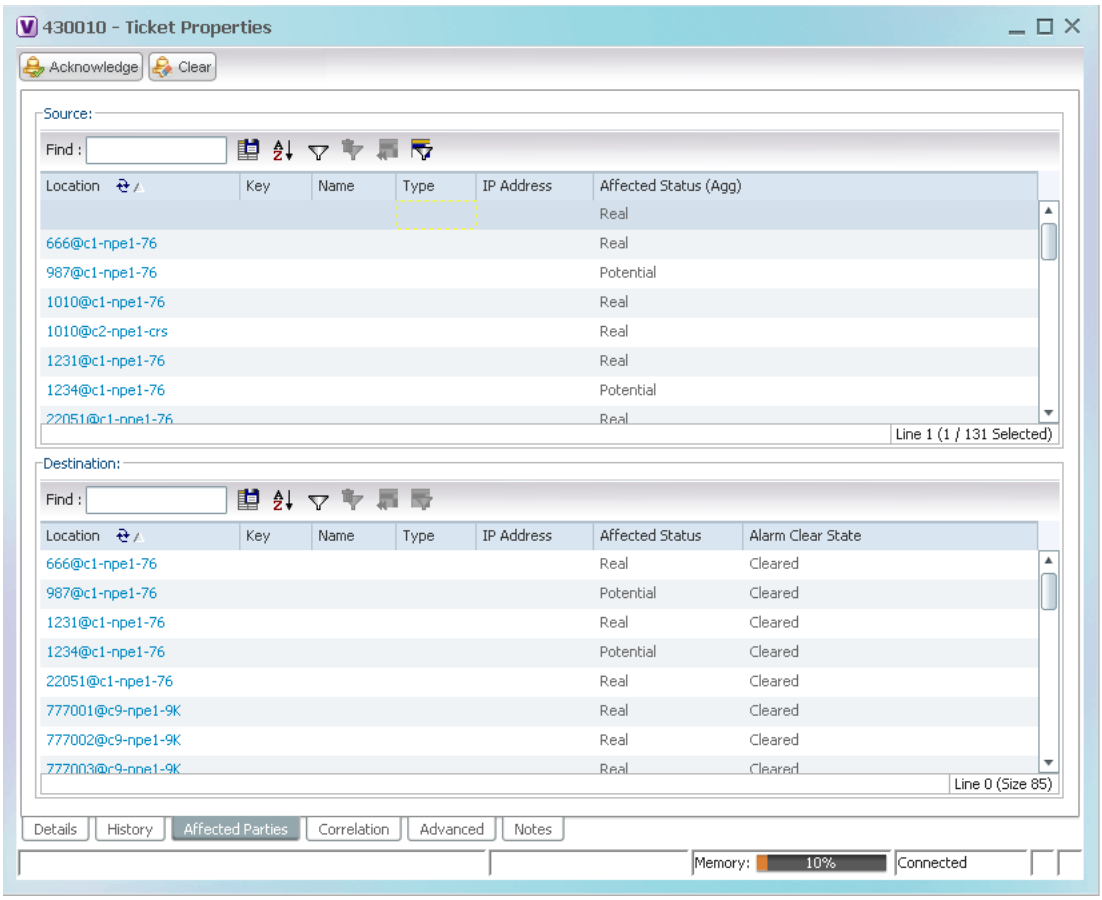
Field	Description
Severity	Severity bell icon, colored according to the severity of the alarm.
Event ID	Event identifier of the specific alarm.
Time	Date and time the event was received by the Event Collector.
Description	Description of the event.
Location	Entity that triggered the alarm, as a hyperlink that opens the relevant location. **Note** If the entity that triggered the alarm is outside your scope, a message is displayed that states you do not have permission to access the selected item.
Alarm ID	Alarm identifier.
Ticket ID	Ticket identifier. This field appears in the History tab only in Prime Network Events.
Causing Event ID	Identifier of the causing event for the ticket.
Duplication Count	For network events, the duplication count is calculated by the VNE and pertains only to flapping events. The duplication count represents the number of noncleared events aggregated by the flapping event.
Reduction Count	For network events, the reduction count is calculated by the VNE and pertains only to flapping events. The reduction count represents the number of events that are aggregated by the flapping event.
Detail panel	Long description of the selected event.

Affected Parties Tab

The Affected Parties tab displays the service resources (pairs) that are affected by an event, an alarm, or a ticket. When a fault occurs, Prime Network automatically calculates the affected parties and embeds this information in the ticket along with all the correlated faults. You can view a list of all the endpoints that are affected.

The Affected Parties tab displays the service resources (affected pairs) that are affected by the ticket.

Figure 9-5 Affected Parties Tab



The Affected Parties tab contains two tables: Source and Destination. Table 9-12 describes the information that is displayed in the Affected Properties tab.

Table 9-12 Ticket Properties Window - Affected Parties Tab

Field	Description
Source Table	
Location	Hyperlinked entry to the port with the affected parties.
Key	Unique value taken from the affected element's business tag key, if it exists.
Name	Subinterface (site) name or business tag name of the affected element, if it exists.
Type	Business tag type.
IP Address	If the affected element is an IP interface, the IP address of the subinterface site.

Table 9-12 Ticket Properties Window - Affected Parties Tab (continued)

Field	Description
Affected Status (Agg)	Status for the affected pair (destination). The same source can be part of multiple pairs, and therefore each pair can have a different affected status. The highest affected status reflects the highest among these. The affected status can be one of the following: • Potential • Real • Recovered • N/A—From the links view, this indicates *Not Applicable*.
Destination Table	
Location	Hyperlinked entry to the port with the affected parties.
Key	Unique value taken from the affected element's business tag key, if it exists.
Name	Subinterface name or business tag name of the affected element, if it exists.
Type	Business tag type.
IP Address	If the affected element is an IP interface, the IP address of the subinterface site.
Affected Status	Status of the affected pair as calculated by the client according to the rules defined in Status Values for Affected Parties, page 9-22.
Alarm Clear State	For each pair, an indication of the clear state of the alarm: • Cleared—All related alarms for this pair have been cleared. • Not Cleared—One or more alarms for this pair have not been cleared.

When an affected side is selected in the Source table, the Destination table lists all endpoints with services that have been affected between them and the entry selected in the Source table.

Note The Affected Parties dialog box occasionally displays entries that start with the word *Misconfigured*. Entries that start with Misconfigured indicate that the flow has stopped unexpectedly between the source and destination points. An unexpected termination point can be a routing entity, bridge, or VC switching entity. The significant aspects of Misconfigured entries are:
- Because the link does not terminate as expected, the link is not actually impacted.
- An error might exist in the configuration or status of the termination points. We recommend that you check the configuration and status of the affected termination points.

Correlation Tab

The Correlation tab displays all the alarms that are correlated to the selected ticket.

Figure 9-6 Correlation Tab

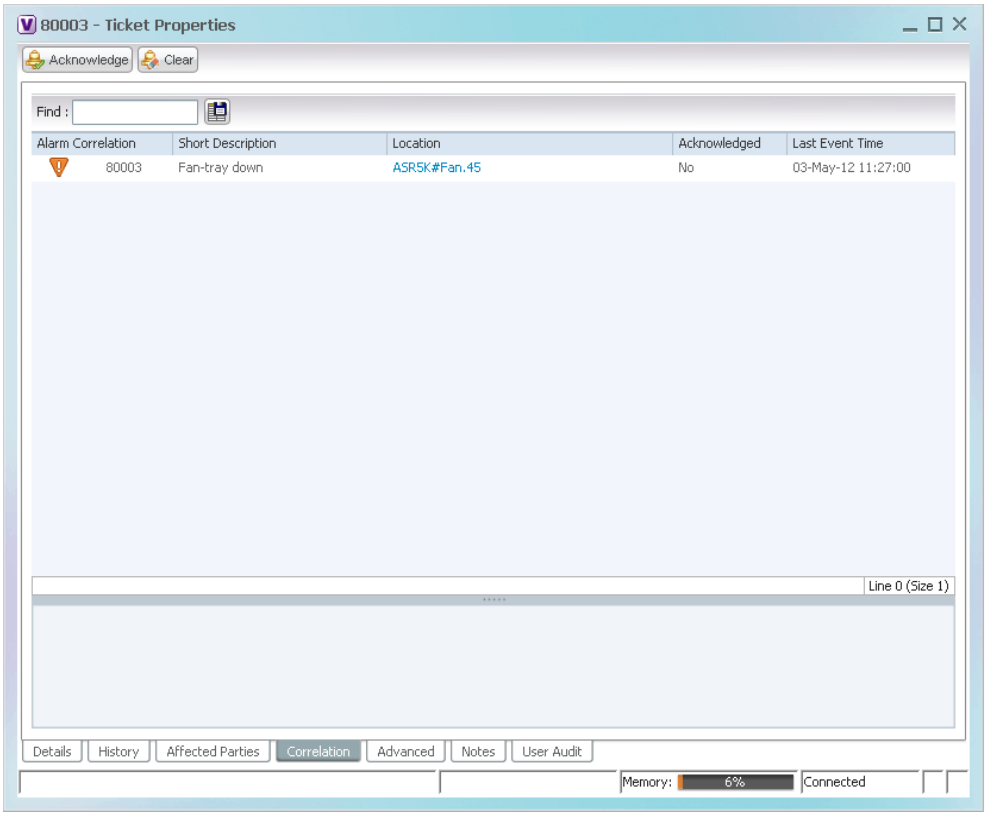


Table 9-13 describes the information that is displayed in the Correlation tab.

Table 9-13 Ticket Properties Window - Correlation Tab

Field	Description
Alarm Correlation	Alarms correlated with the ticket. Expand or collapse the branch to display or hide information as needed. The severity displayed is the severity of the root alarm.
Short Description	Description of the alarm.
Location	Hyperlinked entry that opens an window displaying the selected node along with the affected parties. **Note** If the entity that triggered the alarm is outside your scope, a message is displayed that states you do not have permission to access the selected item.

Table 9-13 Ticket Properties Window - Correlation Tab (continued)

Field	Description
Acknowledged	Whether or not the root alarm has been acknowledged: Yes or No.
Last Event Time	Date and time the alarm was last modified.
Detail panel	Long description of the selected entry.

Advanced Tab

The Advanced tab displays the following values for the selected ticket:

- Duplication Count:
  - For network events, the duplication count is calculated by the VNE and pertains only to flapping events. The duplication count represents the number of noncleared events aggregated by the flapping event.
  - For tickets, the duplication count is the sum of the duplication counts of all events that are associated with the root alarm.
- Reduction Count:
  - For network events, the reduction count is calculated by the VNE and pertains only to flapping events. The reduction count represents the number of events that are aggregated by the flapping event.
  - For tickets, reduction count is the sum of reduction counts of all the events that are associated to the ticket. The History tab in the Ticket Properties window displays one reduction count for each event listed.
- Affected Devices—The number of devices affected by the ticket.
- Alarm Count—The total number of alarms associated with the ticket, including the root alarm.

Notes Tab

The Notes tab enables you to add and save notes for the selected ticket. To add text, enter text in the Notes field and click **Save Notes**. The new text is added to any previously existing text.

After you save a note, it appears in the Previous Notes section of the Notes tab, with the name of the user who added the note and the time it was added. If the user is an external user (for example, a Netcool user), the username will be displayed in the following format:
“Added by prime-networkUserName (as externalUserName)”

The following restrictions apply to the Notes tab:

- You can add notes for a ticket only if both of the following conditions are true:
  - The default permission for your account is OperatorPlus or higher.
  - The security level for the device scope is OperatorPlus or higher for the device that holds the root alarm for that ticket.
- The Notes tab is not available for archived tickets.
- The Save Notes button is enabled only when text is entered in the Notes field.
- The text cannot be edited or removed once you have saved the notes.

User Audit Tab

The User Audit tab enables you to see which ticket-related actions were carried out by which users, and when the action took place.

If the user is an external user (for example, a Netcool user), the username will be displayed in the following format in the User Name column:
"Added by prime-networkUserName (as externalUserName)"

The following actions are reported in the User Audit tab:

- Acknowledge ticket
- Remove ticket (archive)
- Clear ticket

Managing Tickets

The following topics describe how to manage tickets:

- Finding Affected Elements, page 9-19
- Acknowledging a Ticket, page 9-19
- Clearing a Ticket, page 9-20
- Removing a Ticket, page 9-21
- Clearing and Removing Tickets, page 9-21

You can acknowledge, clear, remove, or clear and remove a ticket only if both of the following conditions are true:

- The default permission for your account is OperatorPlus or higher.
- The security level for the device scope is OperatorPlus or higher for the device that holds the root alarm for that ticket.

Prime Network automatically clears and removes (archives) tickets with more than 150 associated events, and generates a system notification event regarding the actions taken. For more information about this feature, see the *Cisco Prime Network 3.9 Administrator Guide*.

Finding Affected Elements

To locate elements affected by a ticket in Prime Network Vision, right-click the desired ticket in the ticket pane and then choose **Find Affected Elements**.

Depending on the number of affected elements, the results are displayed in one of the following ways:

- If only one element is affected, it is highlighted in the navigation pane and the content area.
- If multiple elements are affected, they are displayed in the Affected Events window.

Acknowledging a Ticket

When an alarm occurs, a warning or ticket is displayed in the ticket pane. Prime Network Vision enables you to handle the status of a ticket by acknowledging it. This acknowledges the fault.

The change is reported to the Prime Network gateway and all open Prime Network applications. You can acknowledge multiple tickets at the same time.

An acknowledged ticket returns to a status of Not Acknowledged when a new event is correlated to it.

Note You cannot undo this operation.

To acknowledge one or more tickets, do one of the following:

- Select one or more tickets in the ticket pane, and then right-click and choose **Acknowledge**.
- Double-click a ticket in the ticket pane and click **Acknowledge** in the Ticket Properties window.

For more information, see Understanding Ticket Status, page 9-6.

Clearing a Ticket

When an alarm occurs, a warning or ticket is displayed in the ticket pane. Prime Network Vision enables you to handle the reported ticket by verifying the report of what is faulty and clearing the faulty network element. The change is reported to the Prime Network gateway and all open Prime Network applications. This operation cannot be reversed.

You can clear multiple tickets at the same time.

Note Before using **Clear and Remove** (which might also be available when you right-click a ticket), be sure you understand the results of *removing* a ticket. Like clearing a ticket, removing a ticket cannot be reversed. See Removing a Ticket, page 9-21.

Clearing an open ticket performs the following operations:

- For certain network elements, such as cards and links, sends a request to the Prime Network system to remove the faulty network element from the Prime Network networking inventory.
- Sets the alarm to Cleared or Normal severity or status by issuing a corresponding Clear alarm.
- Automatically sets the alarm severity or status to acknowledged (true).

To clear one or more tickets, do one of the following:

- Select one or more tickets in the ticket pane, and then right-click and choose **Clear**.
- Double-click a ticket in the ticket pane and click **Clear** in the Ticket Properties window.

For more information, see Understanding Ticket Status, page 9-6.

Removing a Ticket

When an alarm occurs, a warning or ticket is displayed in the ticket pane. Prime Network Vision enables you to completely remove the ticket and all of its active alarms and business tags. The change is reported to the Prime Network gateway and all instances of Prime Network that are open. In addition, several tickets can be removed at the same time. After a ticket is cleared or an Up alarm occurs, the ticket can be removed.

You can remove multiple tickets at the same time.

Note This operation cannot be reversed. A ticket that has been removed can be viewed only by using Prime Network Events.

Removing a ticket performs the following operations:

- For certain network elements, such as cards or links, sends a request to the Prime Network system to remove the faulty network element from the Prime Network networking inventory.
- Archives the ticket and active alarms.
- Notifies all open instances of Prime Network clients (Prime Network Vision or BQL) that are registered on the ticket that the ticket has been removed and deletes the ticket from the ticket pane.

Removing a ticket within seven minutes of its creation results in the following behavior:

- New alarms that might be related to the ticket, and should therefore be correlated to it, are not correlated to the original ticket because the ticket has been removed from Prime Network Vision.
- Flagging events that are ticketable open new tickets. These new tickets might be delayed and might not be visible in Prime Network Vision for up to seven minutes after the event was created.
- Flagging events that are not ticketable are archived.
- Clearing events are archived.

Note Only tickets with a severity of Cleared, Normal, or Information can be removed.

To remove one or more tickets, select the required tickets in the ticket pane, and then right-click and choose **Remove**.

For more information, see Understanding Ticket Status, page 9-6.

In addition, an uncleared ticket (which has a severity higher than Cleared or Normal) can be cleared and removed by right-clicking in the ticket pane and choosing **Clear and Remove**. For more information about the Ticket right-click menu, see Ticket Right-Click Menu, page 2-46.

Clearing and Removing Tickets

Clearing and removing a ticket:

- Approves the reported faulty ticket.
- Clears the faulty networking entity from Prime Network Vision.
- Archives the ticket.

You can clear and remove multiple tickets at the same time. This operation will attempt to modify any ticket which is not being used by other processes, such as a ticket that is being updated with new network events. In order to clear and remove a highly active ticket, you should select only that ticket. That way, the system will wait until it becomes available for an update before removing it.

To clear and remove one or more tickets, select the required tickets in the ticket pane, and then right-click and choose **Clear and Remove**.

Impact Analysis in Prime Network

Impact analysis enables you to identify the network elements and services that are impacted by a network fault or outage.

Prime Network offers two modes of impact analysis:

- Automatic impact analysis—When a fault occurs that has been identified as potentially service affecting, Prime Network automatically generates the list of potential and actual service resources that were affected by the fault, and embeds this information in the ticket along with all the correlated faults.

  Note This applies only to specific alarms. Not every alarm initiates automatic impact analysis.

- Proactive impact analysis—Prime Network provides what-if scenarios for determining the possible effect of network failures. This enables on-demand calculation of affected service resources for every link in the network, thus enabling an immediate service availability check and analysis for potential impact and identification of critical network links. Upon execution of the what-if scenario, Prime Network initiates an end-to-end flow that determines all the potentially affected edges.

Note Each fault that has been identified as potentially service affecting triggers an impact analysis calculation, even if the fault recurs in the network.

Status Values for Affected Parties

In automatic mode, the affected parties can be marked with one of the following status values:

- Potential—The service might be affected but its actual state is not yet known.
- Real—The service is affected.
- Recovered—The service has recovered. This state applies only to entries that were marked previously as potentially affected. It indicates only the fact that there is an alternate route to the service, regardless of the service quality level.

Initially, Prime Network might identify the services as either potentially or real affected. As time progresses and more information is accumulated from the network, Prime Network updates the information to indicate which of the potentially affected parties are real or recovered.

The indications for these states are available through both the API and in the GUI.

Note There is no clear state for the affected services when the alarm is cleared.

Accumulating Affected Parties

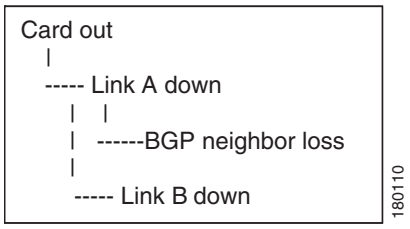
During automatic impact analysis, Prime Network automatically calculates the accumulation of affected parties. This information is embedded in the ticket along with all of the correlated faults.

In the following example, these alarm types exist in the correlation tree:

- Ticket root-cause alarm (Card Out).
- An alarm which is correlated to the root cause and has other alarms correlated to it (Link A Down).
- An alarm with no other alarms correlated to it (Link B Down and BGP Neighbor Loss).

An event sequence is correlated to each of these alarms.

Figure 9-7 Correlation Tree Example



Prime Network identifies the affected parties for each type of alarm and accumulates the following information:

- The affected parties reported on all the events in the alarm event sequence, including flapping alarms.
- The affected parties reported on the alarms that are correlated to it.

The gathered information includes the accumulation of the affected report of all the events in its own correlation tree.

For example, in Figure 9-7:

- BGP neighbor loss includes the affected parties of all events in its own event sequence.
- Link A Down includes the affected parties of its own event sequence and the accumulated information of the BGP Neighbor Loss event.

Accumulating the Affected Parties in an Alarm

If two events form part of the same event sequence in a specific alarm, the recurring affected pairs are displayed only once in the Affected Parties tab. If different affected severities are reported for the same pair, the pair is marked with the severity that was reported by the latest event, according to the time stamp.

Accumulating the Affected Parties in the Correlation Tree

If two or more alarms that are part of the same correlation tree report on the same affected pair of edgepoints and have different affected severities, the recurring affected pairs are displayed only once in the Affected Parties tab. If different affected severities are reported for the same pair, the pair is marked with the highest severity.

For example, assume that X and Y are the OIDs of edgepoints in the network, and a service is running between them. Both alarms, Link B Down and BGP Neighbor Loss, report on the pair X < > Y as affected:

- Link B Down reports on X < > Y as potentially affected.
- BGP Neighbor Loss reports on X < > Y as real affected.

The affected severity priorities are:

- Real—Priority 1
- Recovered—Priority 2
- Potential—Priority 3

Card Out reports on X < > Y as real, affected only once.

Updating Affected Severity over Time

In some cases, Prime Network updates the affected severity of the same alarm over time because the effect of the fault on the network cannot be determined until the network has converged.

For example, a Link Down alarm creates a series of affected severity updates over time. These updates are added to the previous updates in the system database. In this case, the system provides the following reports:

- The first report of a link down reports on X < > Y as potentially affected.
- Over time, the VNE identifies that this service is real affected or recovered, and generates an updated report.
- The Affected Parties tab of the Ticket Properties dialog box displays the latest severity as real affected.
- The Affected Parties Destination Properties dialog box displays both reported severities.

This functionality is available only in the link-down scenario in MPLS networks.



CHAPTER 10

Working with Reports

Cisco Prime Network (Prime Network) provides a Report Manager that enables you to schedule, generate, view, and export reports of the information managed by Prime Network. You can save the generated reports in any of the following formats: PDF, CSV, HTML, XLS, and XML.

In addition to a variety of standard reports for events and inventory, you can define reports as required for your environment. The following topics discuss the Report Manager and reports in more detail:

- User Roles Required to Manage Reports, page 10-1
- Using the Report Manager, page 10-4
- Report Categories, page 10-11
- Generating Reports, page 10-22
- Scheduling Reports, page 10-38
- Managing Reports, page 10-39
- Defining Report Types, page 10-46
- Working with Report Folders, page 10-46

User Roles Required to Manage Reports

This topic identifies the roles that are required to manage reports. Prime Network determines whether you are authorized to perform a task as follows:

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

For more information on user authorization, see the *Cisco Prime Network 3.9 Administrator Guide*.

The following tables identify the tasks that you can perform:

- Table 10-1 identifies whether you can generate a report if a selected element **is not in** one of your assigned scopes.
- Table 10-2 identifies whether you can generate a report if a selected element **is in** one of your assigned scopes.
- Table 10-3 identifies the tasks you can perform on the reports that you generate.
- Table 10-4 identifies the tasks you can perform on the reports that someone else generates.
- Table 10-5 identifies the tasks you can perform on report folders.

By default, users with the Administrator role have access to all managed elements. To change the Administrator user scope, see the topic on device scopes in the *Cisco Prime Network 3.9 Administrator Guide*.

Table 10-1 Default Permission/Security Level Required for Generating Reports - Element Not in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Generate Events Reports					
• Detailed Network Events Reports	—	—	—	—	X
• Detailed Non-Network Events Reports	—	—	—	Partial[1]	X
• All other events reports	—	—	—	—	X
Generate Inventory Reports	—	—	—	—	X
Generate Network Service Reports	—	—	—	—	X

1. A user with the Configurator role can generate Detailed Provisioning Events reports for elements that are in and outside their scope.

Table 10-2 Default Permission/Security Level Required for Generating Reports - Element in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Generate Events Reports					
• Detailed Network Events Reports[1]	X	X	X	X	X
• Detailed Non-Network Events Reports	—	—	—	Partial[2]	X
• All other events reports	X	X	X	X	X
Generate Inventory Reports	X	X	X	X	X
Generate Network Service Reports	X	X	X	X	X

1. Detailed Ticket reports include only those tickets that have a root cause alarm associated with an element in the user's scope.
2. A user with the Configurator role can generate Detailed Provisioning Events reports for elements that are in and outside their scope.

Table 10-3 Default Permission/Security Level Required for Working with Reports You Generate

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Report Tasks					
Schedule reports	X	X	X	X	X
Cancel reports	X	X	X	X	X
Delete reports	X	X	X	X	X
Export reports	X	X	X	X	X
Rename reports	X	X	X	X	X
Save reports	X	X	X	X	X
Set report preferences for purging and sharing	—	—	—	—	X
Share/unshare reports	X[1]	X[1]	X[1]	X[1]	X
View report properties	X	X	X	X	X
View reports	X	X	X	X	X

1. You can share or unshare reports only if sharing is enabled in Prime Network Administration.

Table 10-4 Default Permission/Security Level Required for Working with Reports Another User Generates

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Report Tasks					
Schedule reports	—	—	—	—	X
Cancel reports	—	—	—	—	X
Delete reports	—	—	—	—	X
Export reports	—	—	—	—	X
Rename reports	—	—	—	—	X
Save reports	—	—	—	—	X
Set report preferences for purging and sharing	—	—	—	—	X
Share/unshare reports	—	—	—	—	X
View report properties	—	—	—	—	X
View reports	—	—	—	—	X

Table 10-5 Default Permission/Security Level Required for Working with Report Folders

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Report Folder Tasks					
Create folders	X	X	X	X	X
Delete folders[1]	X	X	X	X	X
Move folders[1]	X	X	X	X	X
Rename folders[1]	X	X	X	X	X

Table 10-5 Default Permission/Security Level Required for Working with Report Folders (continued)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View report folder properties	X	X	X	X	X
View report type properties	X	X	X	X	X

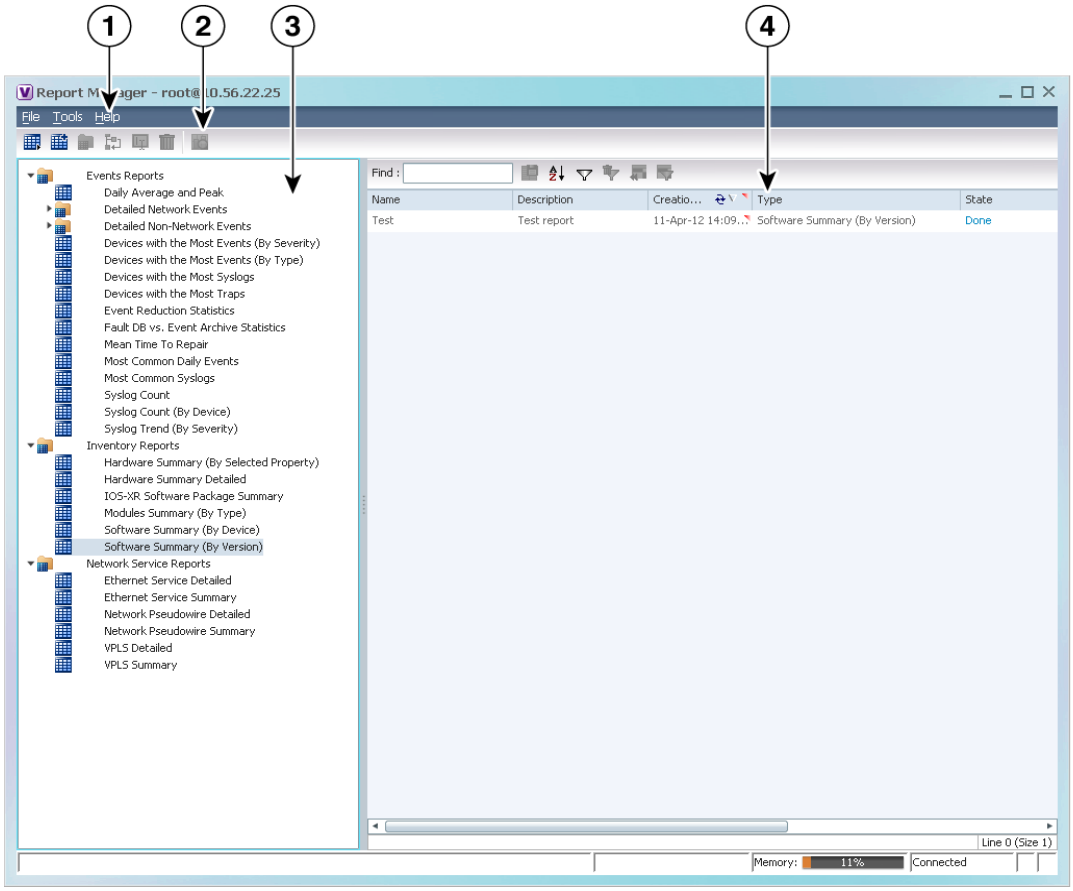
1. You cannot perform this action on system-generated folders, such as the Events Reports folder.

Using the Report Manager

The Report Manager is available from Prime Network Vision, Prime Network Events, and Prime Network Administration by choosing **Reports > Report Manager**. The Report Manager (shown in Figure 10-1) enables you to run standard reports, such as the number of syslogs by device.

The Report Manager also enables you to create reports and folders, view previously generated reports, define report types for your use, and organize reports in a manner suited to your environment and needs.

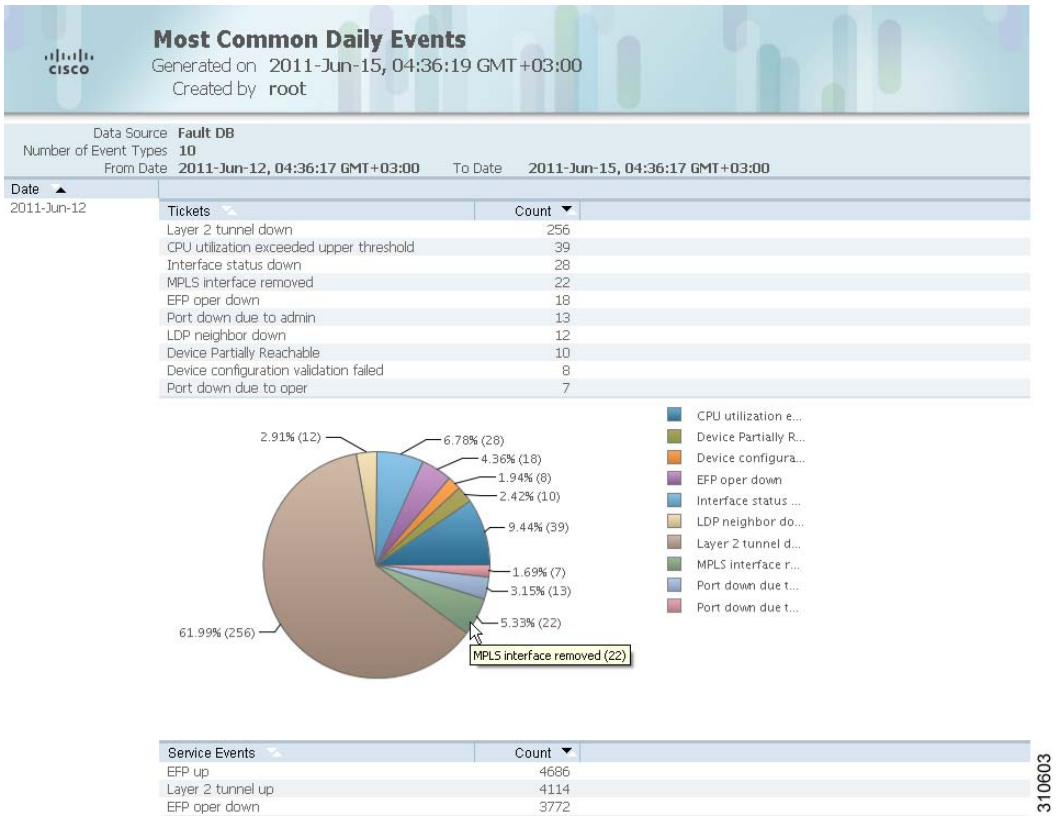
Figure 10-1 Report Manager Window



1	Menu bar	**3**	Navigation tree with report types and folders
2	Toolbar	**4**	Content pane

Figure 10-2 shows an example of a generated report with a pie chart.

Figure 10-2 Sample Report



Generated reports contain the following information in the report heading:

- Report name
- Date, time, and timezone in which the report was generated
- Name of user who generated the report

Depending on the type of report, the following additional information can appear in the report heading:

- Source of the data, such as the fault or alarm database
- Time period covered by the report
- Number of items included in the report
- Any filters or maps applied to the report

A report might also include a pie chart. If you hover your mouse cursor over a section in the pie chart, a tooltip displays the information associated with that section, such as IP address, number of events, type of event, or percentage of total events.

Note Not all reports include pie charts. In addition, reports that normally include a pie chart do not display a pie chart if the chart exceeds 25 slices.

Menu Options

Table 10-6 describes the menu options available in the Report Manager window.

Table 10-6 Report Manager Menu Options

Option	Description
File Menu	
Exit	Exits the Report Manager window.
Tools Menu	
Change User Password	Enables you to change the password used when logging into the Prime Network client application suite. The change takes effect the next time you log into the application. **Note** The administrator can also change a user password in Prime Network Administration.
Help Menu	
Cisco Prime Network Report Manager Help	Opens the online help for Prime Network Vision and Prime Network Events.
Cisco.com	Unavailable.
About Cisco Report Manager	Displays application information about Prime Network Vision and Prime Network Events.

Report Manager Toolbar

Table 10-7 identifies the buttons that appear in the Report Manager toolbar.

Table 10-7 Report Manager Toolbar Buttons

Icon	Name	Description
	Run	Generates the selected report.
	Define Report of This Type	Enables you to define a report of this type that is suited specifically to your environment.
	New Folder	Creates a new folder.
	Move	Moves one or more folders or reports that you created.

Table 10-7 Report Manager Toolbar Buttons (continued)

Icon	Name	Description
	Rename	Renames a folder that you created.
	Delete	Deletes one or more folders that you created.
	Delete Report	Deletes one or more selected reports.
	View	Displays the selected report in HTML format.

Navigation Tree

The navigation pane displays a tree-and-branch representation of report folders and types of reports. The highest level in the tree displays report folders. The following standard report folders are provided in Report Manager:

- Events Reports
- Inventory Reports
- Network Service Reports

Each folder contains the types of reports that are provided with Prime Network and any user-defined reports. For more information on the standard report types, see Table 10-12.

When you select an item in the tree, the content pane displays the generated reports as follows:

- If you select a folder, the content pane lists all reports that have been generated using any of the report types in that folder.
- If you select a report type, the content pane lists all reports that have been generated of that report type.

Content Pane

The content pane lists all reports generated for the folder or report type selected in the navigation tree. You can double-click a report to view the report in HTML format.

Figure 10-3 shows an example of the content pane.

Figure 10-3 Reports Manager Content Pane

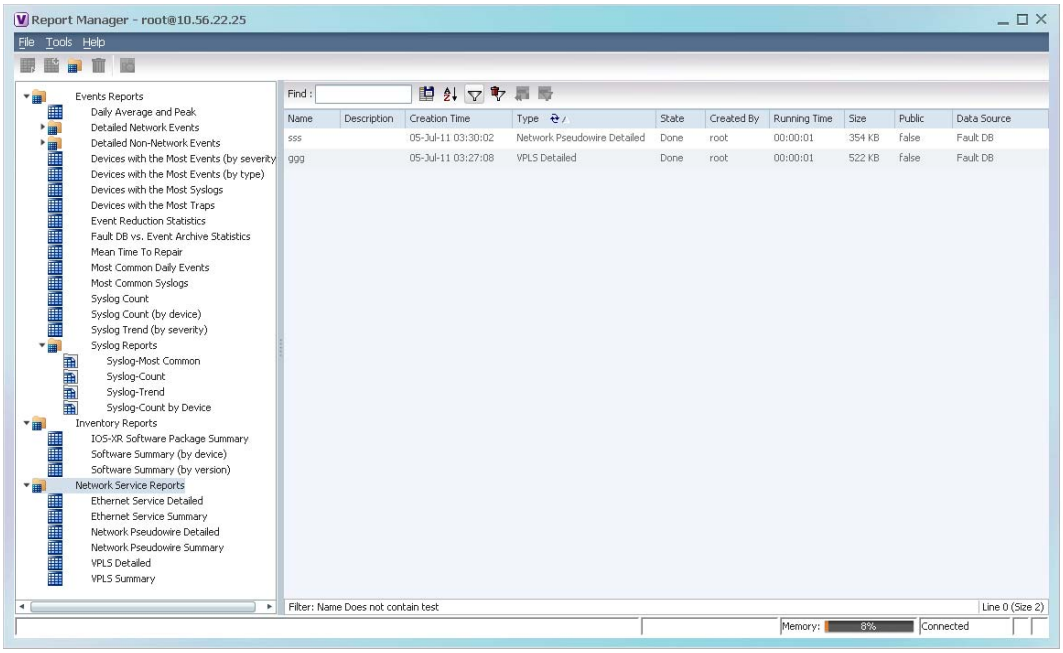


Table 10-8 describes the information displayed in the content pane for each report.

Table 10-8 Reports Manager Content Pane Information

Attribute	Description
Name	Name of the report. Double-click the report to view the report in HTML format.
Description	Brief description of the report.
Creation Time	Date and time when the report was generated.
Type	Report type.
State	State of the report: Running, Done, Canceled, or Failed. For more information about the Failed state, see Generating Reports, page 10-22.
Created By	User who created the report.
Running Time	Amount of time it takes for the report to be complete.
Size	Report size.

Table 10-8 Reports Manager Content Pane Information (continued)

Attribute	Description
Public	Availability of the report to other users: • True—The report is available to all users. • False—The report is available to only the user who generated the report and the administrator.
Data Source	Source of the information for the report: Fault Database, Event Archive, or Network Elements.

Note Reports are purged from Prime Network after 90 days by default. This setting can be modified by changing the setting in Prime Network Administration. For more information, see the *Cisco Prime Network 3.9 Administrator Guide.*

Right-Click Options

Right-click options are available for:

- Navigation Pane Folders, page 10-9
- Navigation Pane Reports, page 10-10
- Content Pane Reports, page 10-10

Navigation Pane Folders

Table 10-9 describes the options available when you right-click a folder in the navigation pane.

Table 10-9 Report Manager Navigation Pane Folder Right-Click Options

Option	Description
New Folder	Creates a new folder.
Delete	Deletes a user-defined folder.
Rename	Renames a user-defined folder.
Move	Moves a user-defined folder.
Properties	Displays the Folder Properties window which lists the folder contents. For more information on the Reports Category Properties window, see Viewing Folder and Report Type Properties, page 10-48.

Navigation Pane Reports

Table 10-10 describes the options available when you right-click a report in the navigation pane.

Table 10-10 Report Manager Navigation Pane Report Right-Click Options

Option	Description
Run	Displays the Run Report dialog box so you can run a report of this type specifically for your environment and adds the generated report to the table in the content pane.
Define Report of This Type	This option is available only for Cisco-supplied report types. Displays the Define Report dialog box so you can create a report of this type specifically for your environment, and adds the newly defined report to the navigation tree.
Delete	Deletes a user-defined report.
Move	Moves a user-defined report.
Properties	For a standard report type, displays the Reports Type Properties window which includes a brief description of the report and enables you to generate the report. For more information on the Reports Type Properties window, see Viewing Report Properties, page 10-44. For a user-defined report, displays the Edit report dialog box so that you can modify the currently defined settings and generate the report.

Content Pane Reports

Table 10-11 describes the options available when you right-click a report in the content pane.

Table 10-11 Report Manager Content Pane Report Right-Click Options

Option	Description
View As	Displays the report in the selected format: • HTML • PDF • CSV • XLS • XML The default option, HTML, is displayed in bold font. For more information on viewing reports, see Viewing and Saving Reports, page 10-40.
Rename	Renames the selected report.

Table 10-11 Report Manager Content Pane Report Right-Click Options (continued)

Option	Description
Share or Unshare	Shares the selected reports or limits them to your viewing only. The option toggles between Share and Unshare, as appropriate for the selected reports. By default, the Share and Unshare options are available only to users with administrator access. These options are available to other users only if an administrator has enabled sharing in Prime Network Administration. For more information, see the *Cisco Prime Network 3.9 Administrator Guide*.
Delete Report	Deletes the selected reports.
Cancel	This option is displayed only while the selected report is being generated or queued. Cancels the report that is being generated or is queued.
Show Only Selected Rows	Displays only the rows that you select.
Show All Rows	Displays all table rows that meet the current filtering criteria.
Properties	Displays the Reports Type Properties window, which includes a brief description of the report and enables you to edit its name and description.

Report Categories

Prime Network Vision provides reports related to:

- Events—See Events Reports, page 10-11.
- Inventory—See Inventory Reports, page 10-18.
- Network services—See Network Service Reports, page 10-20.

Events Reports

Prime Network Vision provides the following standard event report types:

- General report types, as described in Table 10-12.
- Detailed network event reports, as described in Table 10-13.
- Detailed non-network event reports, as described in Table 10-14.

Table 10-12 Standard Events Report Types

Report Name	Description	Data Source
Daily Average and Peak	For each day of the specified time period, the peak number and average rate of syslogs and traps for each of the following time periods: • Second • Ten seconds • Minute • Hour • Day	Fault database
Devices with the Most Events (By Severity)	For the specified number of devices with the most events, the following information for each device for the specified time period: • Severity of the events associated with the device, sorted by severity • Number of events for each severity A pie chart presents the information by device and percentage in a graphical format.	Fault database
Devices with the Most Events (By Type)	For the specified number of devices with the most events, the following information for each device for the specified time period: • Type of events associated with the device • Number of events received for each event type A pie chart presents the information by device and percentage in a graphical format.	Fault database
Devices with the Most Syslogs	For the specified number of devices with the most syslogs, the number of syslog messages for each device for the specified time period. You can run this report on the Prime Network fault database or the event archive. A pie chart presents the information by device and percentage in a graphical format.	User choice: • Fault database • Event archive
Devices with the Most Traps	For the specified number of devices with the most traps, the number of traps associated with each device for the specified time period. You can run this report on the fault database or the event archive. A pie chart presents the information by device and percentage in a graphical format.	User choice: • Fault database • Event archive

Table 10-12 Standard Events Report Types (continued)

Report Name	Description	Data Source
Event Reduction Statistics	For the specified devices and time period: • Names of those tickets with: – The root cause in the device list – The ticket creation time within the specified period • For each ticket type identified: – Number of tickets of that type – Fewest number of correlated events – Highest number of correlated events – Average number of correlated events	Fault database
Fault DB vs. Event Archive Statistics	For each day in the specified time period, the number of each of the following items in the fault database and the event archive: • Syslogs • Traps • Tickets • Correlated events • Uncorrelated events • Nonnetwork events • Network-originated events • Network-originated and service events	Fault database and event archive
Mean Time to Repair	For the specified devices and time period: • Names of those tickets with: – The root cause in the device list – The ticket creation time within the specified period • For each ticket type identified: – Whether the tickets were cleared by the user or network – Number of tickets – Minimum time (in seconds) to repair – Maximum time (in seconds) to repair – Average time (in seconds) to repair **Note** The time to repair is based on the ticket creation time and the time the ticket was last modified. For example, if you acknowledge a ticket after it has been cleared. the acknowledgement time affects the time to repair for that ticket.	Fault database

Table 10-12 Standard Events Report Types (continued)

Report Name	Description	Data Source
Most Common Daily Events	For each day in the specified time period: • Specified number of most common tickets, service events, syslogs, and traps • Number of each type of ticket, service event, syslog, and trap • If selected, a pie chart presenting the events by percentage in a graphical format	Fault database
Most Common Syslogs	Most common syslog messages and the number of each for the specified time period and devices. A pie chart presents the information by syslog message and percentage in a graphical format.	Fault database
Syslog Count	Number of syslog messages by type for the specified time period with the times of the first and last occurrences. A pie chart presents the information by syslog message and percentage in a graphical format.	Fault database
Syslog Count (By Device)	For each device, the type and number of each syslog message and the times of the first and last occurrences for each type. A pie chart presents the information by device and percentage in a graphical format.	Fault database
Syslog Trend (By Severity)	For the specified devices, the trend of specified syslog messages in graph format: • By priority • For the specified time period • At the specified intervals	Fault database

Table 10-13 Detailed Network Events Report Types

Report Name	Description	Data Source
Detailed Event Count (By Device)	For each device, the following information for the specified time period: • For syslogs: – Syslog severities – Number of syslogs per severity – Syslog type – Number of each syslog type • For traps: – Trap severities – Number of traps per severity – Trap type – Number of each trap type • For tickets: – Ticket severities – Number of tickets per severity – Ticket type – Number of each ticket type You can select a maximum of 1000 devices for this report.	Fault database
Detailed Service Events	For each service event of the specified severities, time period, and devices: • Event severity • Event identifier • Timestamp • Brief and detailed descriptions • Device on which the event occurred • Alarm identifier • Ticket identifier • Causing event identifier • Duplication count • Reduction count	Fault database

Table 10-13 Detailed Network Events Report Types (continued)

Report Name	Description	Data Source
Detailed Syslogs	For each device that is selected, the following information from the event archive for the specified time period: • IP address • Date and time of each syslog, in ascending order • Syslog raw data or description, depending on the data source The maximum number of syslogs retrieved for this report is 250,000.	User selection: Event archive or fault database
Detailed Tickets	For each ticket of the specified severities, time period, and device: • Ticket severity • Ticket identifier • Last modification time • Root event time • Description • Entity that caused the alarm • Whether or not the ticket is acknowledged • Ticket creation time • Event count • Affected devices count • Duplication count • Reduction count • Alarm count	Fault database
Detailed Traps	For each managed device that is selected, the following information for the specified time period: • IP address • Time of trap • SNMP version • Trap description • Generic or device-specific trap OID, if the source is the event archive • Long description, if the data source is the fault database The maximum number of traps retrieved for this report depends on whether the Long Description check box is selected. When selected, a maximum of 30,000 traps are retrieved. When this check box is not selected, a maximum of 100,000 traps are retrieved for this report.	User Selection: Event archive or fault database

Table 10-14 Detailed Non-Network Events Report Types

Report Name	Description	Data Source
Detailed Audit Events	For each audit event included in the report for the specified time period, severities, and search criteria: • Event severity • Event identifier • Timestamp • Description • Command name • Command signature • Command parameters • Originating IP address • Username	Fault database
Detailed Provisioning Events	For each provisioning event included in the report for the specified time period, severities, and search criteria: • Event severity • Event identifier • Timestamp • Description • Location • Username • Status	Fault database
Detailed Security Events	For each security event included in the report for the specified time period, severities, and search criteria: • Event severity • Event identifier • Timestamp • Description • Location • Username • Originating IP address	Fault database
Detailed System Events	For each system event included in the report for the specified time period, severities, and search criteria: • Event severity • Event identifier • Timestamp • Description • Location	Fault database

Inventory Reports

Table 10-15 describes the standard inventory report types provided by Prime Network Vision and the data source.

Table 10-15 Standard Inventory Report Types

Report Name	Description	Data Source
Hardware Summary Detailed	For each device included in the report: • IP address • Device series • Element type You can view other hardware information for each device by selecting the required items from the available list as given below: • Chassis—chassis description, chassis serial number, shelf description, shelf serial number, and shelf status • Module—module name, sub module name, module status, hardware type, and hardware version • Port—port location, port type, porting sending alarm, port alias, port status, port managed, PID, and pluggable type serial number.	Network elements
Hardware Summary (By Selected Property)	For each device included in the report: • IP address • System name • Serial number • Element type • Device series • Vendor • Product • Chassis You can group the report contents by vendor, product, device series, element type, system name, or chassis and specify part or whole of the selected entity, if required.	Network elements

Table 10-15 Standard Inventory Report Types (continued)

Report Name	Description	Data Source
IOS-XR Software Package Summary	For each device included in the report: • Device name • Element type • IP address • Serial number • Cisco IOS XR software version • For each software package installed on the device: – Storage location – Software package name – Module name – Software package state: Active or Inactive	Network elements
Modules Summary (By Type)	For each device filtered by module type: • IP address • Module serial number • Module hardware version • Module software version You can filter the report contents by specifying part or whole of the module type.	Network elements
Software Summary (By Device)	For each device included in the report: • Device name • Element type • IP address • Serial number • Software version on the device • Name of image file	Network elements
Software Summary (By Version)	For each software version included in the report: • Number of devices running the version • Device names • Element types • Device IP address • Device serial number • Name of image file	Network elements

Network Service Reports

Table 10-16 describes the standard network service report types provided by Prime Network Vision and the data source.

Table 10-16 Standard Network Service Report Types

Report Name	Description	Data Source
Ethernet Service Detailed	For each Ethernet service in the report: • Ethernet service or Layer 2 VPN name • Business tag assigned to the Ethernet service or Layer 2 VPN instance • EVC name • Business tag assigned to the EVC • Maps containing the Ethernet service or Layer 2 VPN • Edge EFPs associated with the EVC or Layer 2 VPN • EFD fragment names • EFD fragment type You can filter report content by specifying part or all of the: • Ethernet service name • EVC name • Ethernet service business tag • EVC business tag • Map name	Fault database
Ethernet Service Summary	For each Ethernet service in the report: • Ethernet service or Layer 2 VPN name • Business tag assigned to the Ethernet service or Layer 2 VPN instance • EVC name • Business tag assigned to the EVC • Maps containing the Ethernet service or Layer 2 VPN You can filter report content by specifying part or all of the: • Ethernet service name • EVC name • Ethernet service business tag • EVC business tag • Map name	Fault database

Table 10-16 Standard Network Service Report Types (continued)

Report Name	Description	Data Source
Network Pseudowire Detailed	For each network pseudowire in the report: • Pseudowire name • Pseudowire type • Business tag assigned to the pseudowire • Maps containing the pseudowire • Pseudowire details • Type of pseudowire, such as pseudowire edge, Ethernet flow point, or switching entity You can filter report content by specifying part or all of the: • Pseudowire name • Pseudowire type • Business tag • Map name	Fault database
Network Pseudowire Summary	For each network pseudowire in the report: • Pseudowire name • Pseudowire type • Business tag assigned to the pseudowire • Maps containing the pseudowire You can filter the report content by specifying part or all of the: • Pseudowire name • Pseudowire type • Business tag • Map name	Fault database

Table 10-16 Standard Network Service Report Types (continued)

Report Name	Description	Data Source
VPLS Detailed	For each VPLS or H-VPLS instance in the report: • VPLS or H-VPLS name • Business tag associated with the VPLS or H-VPLS instance • Maps containing the VPLS or H-VPLS instance • VPLS details • Type of VPLS service, such as VPLS forward, access EFP, or core pseudowire You can filter report content by specifying part or all of the: • VPLS or H-VPLS name • Business tag • Map name	Fault database
VPLS Summary	For each VPLS or H-VPLS instance in the report: • VPLS or H-VPLS name • Business tag assigned to the VPLS or H-VPLS instance • Maps containing the VPLS or H-VPLS instance You can filter report content by specifying part or all of the: • VPLS or H-VPLS name • Business tag • Map name	Fault database

Generating Reports

You can generate reports in any of the following ways:

- Generating Reports from Report Manager, page 10-23
- Generating Reports from the Reports Menu, page 10-37
- Generating Reports from Prime Network Vision, page 10-38

You can generate reports only for devices that are within your scope.

Note Report Manager generates reports up to 150 MB in size. If you generate a report that exceeds this limit:

- Report Manager window displays Failed in the State column.
- An error message is entered in the log stating that the report failed because the resulting output is too large.

To run the report successfully, enter more specific report criteria or limit the time period covered by the report.

Database Load and Report Generation

If you generate reports while Prime Network Vision is working under a database load, the reports move to a *Load* mode which is indicated by a system event. While Prime Network Vision is in Load mode, the reports currently running are cancelled and new reports are queued.

After Prime Network Vision returns to normal operation and is no longer operating under a load, a new system event is generated and the queued reports start running.

Report Generation Failure

If a report fails to generate successfully, the State column contains the word *Failed*. Click **Failed** to view the reason for the failure. A window is displayed with the cause of the failure, such as *The disk space allocated for report storage is full* or *AVM 84 was restarted while the report was running*.

Report Generation Canceled

If a report is canceled before it completes, the State column contains the word *Canceled*. Click **Canceled** to view the reason for the cancellation. A window is displayed with the cause of the cancellation, such as *The report was canceled by user <user-name>* or *The report was canceled by the system to prevent system overload*.

Generating Reports from Report Manager

Prime Network Vision provides three report categories as described in Report Categories, page 10-11. The information that you need to provide when generating a report depends on the report type. The following topics describe the information required to generate each report type:

- Generating Events Reports, page 10-23
- Generating Inventory Reports, page 10-31
- Generating Network Service Reports, page 10-34

Note You can generate reports only for devices that are within your scope.

Generating Events Reports

To generate an events report using Report Manager:

Step 1 In Prime Network Vision, Prime Network Events, or Prime Network Administration, choose **Reports > Report Manager**.

Step 2 In the Report Manager window, choose **Events Reports >** *report-type*.

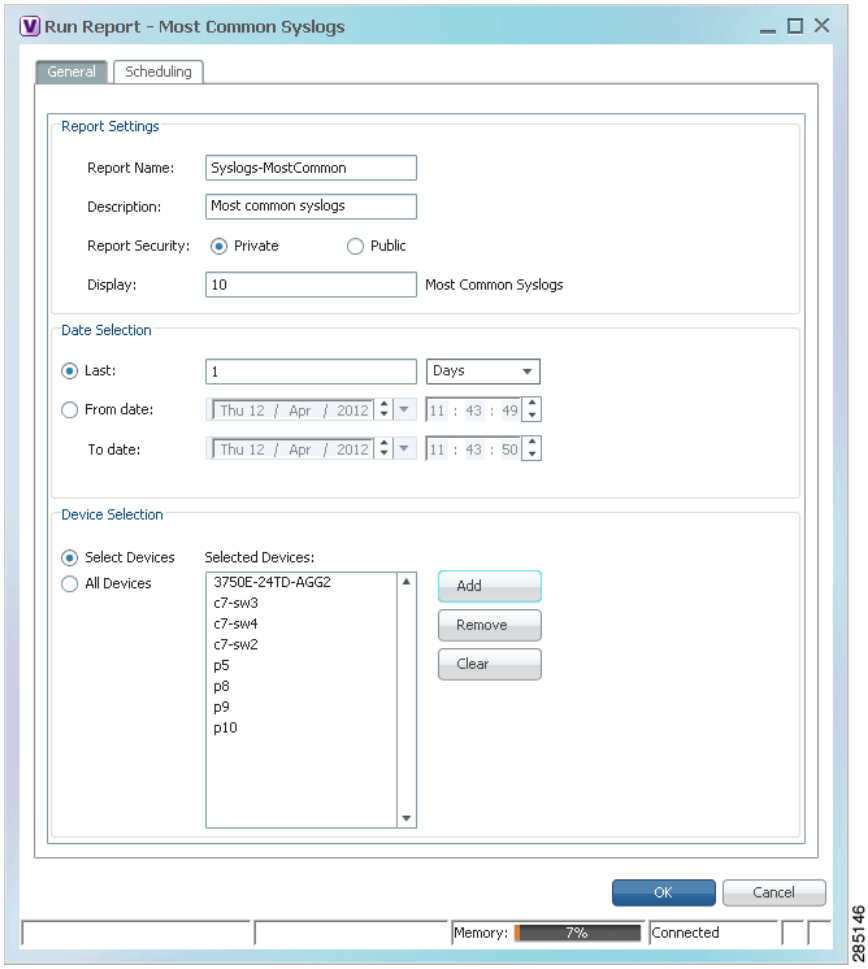
For information on the reports available for events, see Table 10-12.

Step 3 Generate the report in either of the following ways:

- Click **Run** in the toolbar.
- Right-click the report type, then choose **Run**.

The Run Report dialog box is displayed. An example is shown in Figure 10-4. The fields displayed in the Run Report dialog box vary depending on the type of report.

Figure 10-4 Events Report - Run Report Dialog Box



Step 4 In the Run Report dialog box, specify the report settings as follows:

- For standard events reports, use the information in Table 10-17.
- For detailed network reports, use the information in Table 10-18.
- For detailed non-network reports, use the information in Table 10-19.

Table 10-17 Events Report - Run Report Dialog Box Fields

Option	Description
Report Settings	
Report Name	Enter a unique name for the report, from 1 to 150 characters in length. Report names cannot include the following characters: ;?<>/:\"#*|.
Description	Enter a brief description of the report.
Report Security	This field is displayed only if report sharing is enabled in Prime Network Administration. Indicate the level of security for the report by clicking the appropriate option: • Private—The report can be viewed and used only by the report creator and the administrator. • Public—The report can be viewed and used by all other users, regardless of whether the devices are listed in the report are in the user's scope. **Note** You can share reports with others only if sharing is enabled in Prime Network Administration. For more information, see the *Cisco Prime Network 3.9 Administrator Guide*.
Display *n*	This field does not appear for all reports. Enter the number of items to be displayed in the generated report.
Data Source	This field does not appear for all reports. Select the source of information to use for the report: Fault Database or Event Archive.
Include pie charts in report output	This field does not appear for all reports. Check the check box to view pie charts in the report with the standard numerical output.
Date Selection	
Last	Specify the length of time before the current date and time, and the unit of measure: seconds, minutes, hours, days, weeks, or months.
From Date To Date	Specify the date range for the report: 1. Click **From Date**. 2. In the From date field, enter the start date for the time period, or click the drop-down arrow to select the start date from a calendar. 3. Enter a time for the start date, using the format HH MM SS. 4. In the To Date field, enter the end date for the time period, or click the drop-down arrow to select the end date from a calendar. 5. Enter a time for the end date, using the format HH MM SS.

Table 10-17 Events Report - Run Report Dialog Box Fields (continued)

Option	Description
Device Selection	
Select Devices	**Note** • You can add only those devices that are within your scope. • A user with the Administrator role can select unmanaged devices (by IP address) for reports that run on the Event Archive. Select devices to include in the report: 1. Click **Select Devices**. 2. Click **Add**. 3. In the Add Network Element dialog box, select devices using either of the following methods: – To select devices that meet specific criteria, click **Search** and enter the required criteria. – To select from all network elements, click **Show All**. 4. In the list of displayed elements, select the network elements that you want to include in the report. You can select multiple network elements at a time. 5. Click **OK**.
All Devices	This field does not appear for all reports. Click **All Devices** to include all devices in your scope in the report.
Syslog Trend (by Severity) Report—Additional Report Specifications	
Intervals	In the Grouped by drop-down list, choose the unit of time to use for tracking the trend: Seconds, Minutes, Hours, or Days.
Severity	Check the check boxes of the syslog message severities to be included in the report: All, Critical, Major, Minor, Warning, Cleared, Information, and Indeterminate.
Syslog Messages	Specify the syslog messages to be included in the report: • To include selected syslog messages in the report, in the list of syslog messages on the left, select the required syslog messages, and then click **Add Selected** to move them to the list of syslog messages on the right. • To include all syslog messages in the report, click **Add All**. To find syslog messages that match a string, enter the string in the Find field. The list of syslog messages is automatically updated to include only those messages that contain the string you enter. Click the **Sort Order** button to sort the syslog messages in alphabetic or reverse alphabetic order.

Table 10-18 Detailed Network Events Reports - Run Report Dialog Box Fields

Option	Description
Report Settings	
Report Name	Enter a unique name for the report, from 1 to 150 characters in length. Report names cannot include the following characters: ;?<>/:\"#*|.
Description	Enter a brief description of the report.
Report Security	This field is displayed only if report sharing is enabled in Prime Network Administration. Indicate the level of security for the report by clicking the appropriate option: • Private—The report can be viewed and used only by the report creator and the administrator. • Public—The report can be viewed and used by all other users, regardless of whether the devices are listed in the report are in the user's scope. **Note** You can share reports with others only if sharing is enabled in Prime Network Administration. For more information, see the *Cisco Prime Network 3.9 Administrator Guide*.
Data Source	This field does not appear for all reports. Select the source of information to use for the report: Fault Database or Event Archive.
Date Selection	
Last	Specify the length of time before the current date and time, and the unit of measure: seconds, minutes, hours, days, weeks, or months.
From Date To Date	Specify the date range for the report: 1. Click **From Date**. 2. In the From date field, enter the start date for the time period, or click the drop-down arrow to select the start date from a calendar. 3. Enter a time for the start date, using the format HH MM SS. 4. In the To Date field, enter the end date for the time period, or click the drop-down arrow to select the end date from a calendar. 5. Enter a time for the end date, using the format HH MM SS.

Table 10-18 Detailed Network Events Reports - Run Report Dialog Box Fields (continued)

Option	Description
Device Selection	
Select Devices	**Note** • You can add only those devices that are within your scope. • A user with the Administrator role can select unmanaged devices (by IP address) for reports that run on the Event Archive. • The Detailed Event Count (by device) report accepts a maximum of 1000 devices. Select devices to include in the report: 1. Click **Select Devices**. 2. Click **Add**. 3. In the Add Network Element dialog box, select devices using either of the following methods: – To select devices that meet specific criteria, click **Search** and enter the required criteria. – To select from all network elements, click **Show All**. 4. In the list of displayed elements, select the network elements that you want to include in the report. You can select multiple network elements at a time. 5. Click **OK**.
All Devices	This field does not appear for all reports. Click **All Devices** to include all devices in your scope in the report.
Severity	
Severity	This field does not appear for all reports. Check the check boxes of the syslog message severities to be included in the report: All, Critical, Major, Minor, Warning, Cleared, Information, and Indeterminate.
Detailed Service Events Report—Additional Report Specifications	
Description Contains	Enter the string that the service event must contain to be included in the report.
Detailed Syslogs Report—Additional Report Specifications	
Syslogs Description	This field is displayed if you choose Fault DB for the data source. In the Description Contains field, enter the string that the syslog must contain to be included in the report.
Syslogs Raw Data	This field is displayed if you choose Event Archive for the data source. In the Raw Data Contains field, enter the string that the syslog raw data must contain to be included in the report.

Table 10-18 Detailed Network Events Reports - Run Report Dialog Box Fields (continued)

Option	Description
Detailed Traps Report—Additional Report Specifications	
Traps Detailed Description	In the Description Contains field, enter the string that the trap must contain to be included in the report.
Long Description	This option is enabled if you choose Fault DB for the data source. 1. Check the Show Long Description check box to include the long description in the report. 2. In the Long Description Contains field, enter the string that the long description must contain to be included in the report.
SNMP Version	Specify the SNMP versions to include in the report: All, 1, 2, or 3.
Generic	This option is enabled if you choose Event Archive for the data source. Specify the generic traps to include in the report: 1. Select the generic traps to include in the report: – All—Include all generic traps – 0—coldStart – 1—warmStart – 2—linkDown – 3—linkUp – 4—authenticationFailure – 5—egpNeighborLoss – 6—enterpriseSpecific 2. If you select generic type 6, enter the OIDs (comma separated) in the Vendor Specific field. The Vendor Specific field accepts a maximum of 125 digits.

Table 10-19 Detailed Non-Network Events Reports - Run Report Dialog Box Fields

Option	Description
Report Settings	
Report Name	Enter a unique name for the report, from 1 to 150 characters in length. Report names cannot include the following characters: ;?<>/:\"#*|.
Description	Enter a brief description of the report.
Report Security	This field is displayed only if report sharing is enabled in Prime Network Administration. Indicate the level of security for the report by clicking the appropriate option: • Private—The report can be viewed and used only by the report creator and the administrator. • Public—The report can be viewed and used by all other users, regardless of whether the devices are listed in the report are in the user's scope. **Note** You can share reports with others only if sharing is enabled in Prime Network Administration. For more information, see the *Cisco Prime Network 3.9 Administrator Guide*.
Date Selection	
Last	Specify the length of time before the current date and time, and the unit of measure: seconds, minutes, hours, days, weeks, or months.
From Date To Date	Specify the date range for the report: 1. Click **From Date**. 2. In the From date field, enter the start date for the time period, or click the drop-down arrow to select the start date from a calendar. 3. Enter a time for the start date, using the format HH MM SS. 4. In the To Date field, enter the end date for the time period, or click the drop-down arrow to select the end date from a calendar. 5. Enter a time for the end date, using the format HH MM SS.
Severity	
Severity	Check the check boxes of the syslog message severities to be included in the report: All, Critical, Major, Minor, Warning, Cleared, Information, and Indeterminate.
Detailed Audit Events Report—Additional Report Specifications	
Description Contains	Enter the string that the event must contain to be included in the report.
Command Name Contains	Enter the string that the command name must contain to be included in the report.
Originator IP Contains	Enter the string that the originating IP address must contain to be included in the report.
User Name Contains	Enter the string that the username must contain to be included in the report.

Table 10-19 Detailed Non-Network Events Reports - Run Report Dialog Box Fields (continued)

Option	Description
Detailed Provisioning Events Report—Additional Report Specifications	
Description Contains	Enter the string that the trap must contain to be included in the report.
User Name Contains	Enter the string that the username must contain to be included in the report.
Status	Choose the statuses to be included in the report: All, Unknown, Configuring, Success, and Fail.
Detailed Security Events Report—Additional Report Specifications	
Description Contains	Enter the string that the event must contain to be included in the report.
Originator IP Contains	Enter the string that the originating IP address must contain to be included in the report.
User Name Contains	Enter the string that the username must contain to be included in the report.
Detailed System Events Report—Additional Report Specifications	
Description Contains	Enter the string that the event must contain to be included in the report.

Step 5 To schedule a report to run immediately or at a later point in time, click the **Scheduling** tab. For more information, see Scheduling Reports, page 10-38.

Step 6 Click **OK**.

The report appears in the table in the content pane with a state of Running, if the report is scheduled to run immediately, or Scheduled, if the report is scheduled to run at a later point in time. When the report is complete, the state changes to Done.

You can view the reports when the state is Done. Occasionally, some report formats require additional time for generation. If so, a progress bar is displayed, indicating that the report is being created and will be available soon.

If the report exceeds 150 MB, the state changes to Failed and an error message is written to the log. We recommend running the report with more specific criteria or a shorter time period to avoid this situation.

If no data is found for the report, the report states that no results were found.

Generating Inventory Reports

To generate an inventory report using Report Manager:

Step 1 In Prime Network Vision, Prime Network Events, or Prime Network Administration, choose **Reports > Report Manager**.

Step 2 In the Report Manager window, choose **Inventory Reports >** *report-type*.

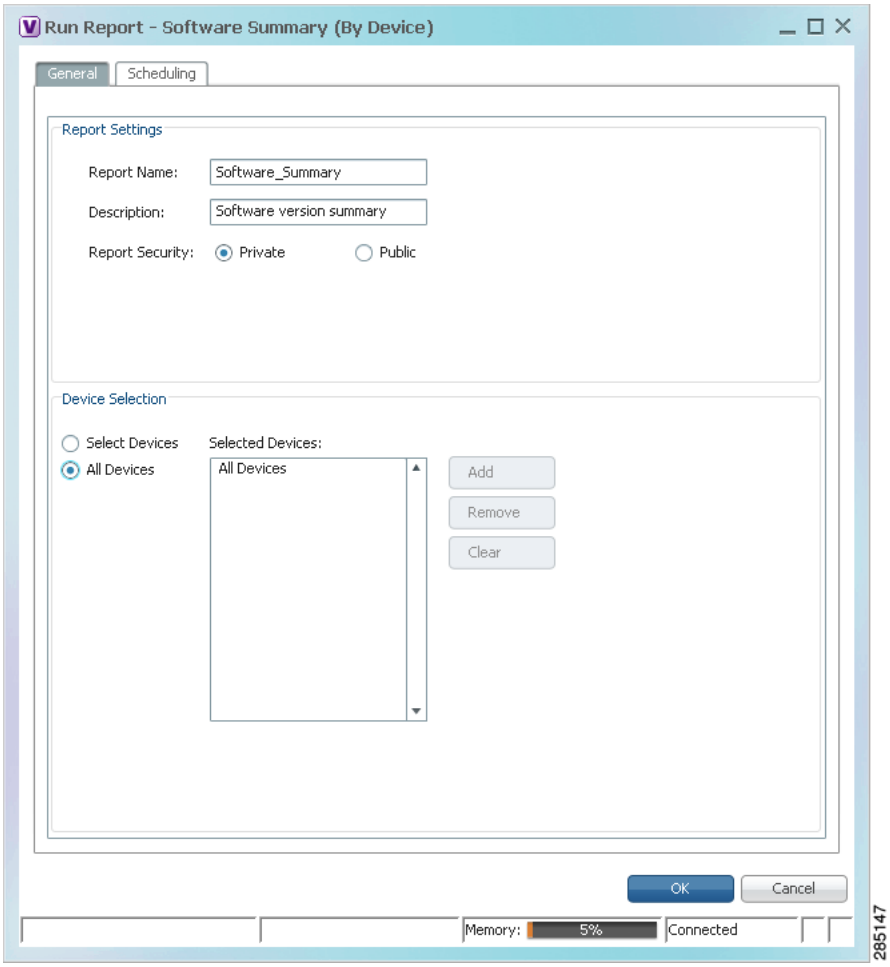
For information on the standard reports available for inventory, see Table 10-15.

Step 3 Generate the report in either of the following ways:

- Click **Run** in the toolbar.
- Right-click the report type, then choose **Run**.

The Run Report dialog box is displayed as shown in Figure 10-5.

Figure 10-5 Inventory Report - Run Report Dialog Box



Step 4 Enter the required information in the Run Report dialog box as described in Table 10-20.

Table 10-20 Inventory Report - Run Report Dialog Box Fields

Field	Description
Report Settings	
Report Name	Enter a unique name for the report, from 1 to 150 characters in length. Report names cannot include the following characters: ;?<>/:\"#*|.
Description	Enter a brief description of the report.

Table 10-20 Inventory Report - Run Report Dialog Box Fields (continued)

Field	Description
Report Security	This field is displayed only if report sharing is enabled in Prime Network Administration. Indicate the level of security for the report by clicking the appropriate option: • Private—The report can be viewed and used only by the report creator and the administrator. • Public—The report can be viewed and used by all other users, regardless of whether the devices are listed in the report are in the user's scope. **Note** You can share reports with others only if sharing is enabled in Prime Network Administration. For more information, see the *Cisco Prime Network 3.9 Administrator Guide*.
Device Selection	
Select Devices	**Note** You can add only those devices that are within your scope. Select devices to include in the report: 1. Click **Select Devices**. 2. Click **Add**. 3. In the Add Network Element dialog box, select devices using either of the following methods: – To select devices that meet specific criteria, click **Search** and enter the required criteria. – To select from all network elements, click **Show All**. 4. In the list of displayed elements, select the network elements that you want to include in the report. You can select multiple network elements at a time. 5. Click **OK**.
All devices	Click **All Devices** to include all devices in your scope in the report.

Step 5 To schedule a report to run immediately or at a later point in time, click the **Scheduling** tab. For more information, see Scheduling Reports, page 10-38.

Step 6 Click **OK**.

The report appears in the table in the content pane with a state of Running, if the report is scheduled to run immediately, or Scheduled, if the report is scheduled to run at a later point in time. When the report is complete, the state changes to Done.

You can view the reports when the state is Done. Occasionally, some report formats require additional time for generation. If so, a progress bar is displayed, indicating that the report is being created and will be available soon.

If the report exceeds 150 MB, the state changes to Failed and an error message is written to the log. We recommend running the report with more specific criteria or a shorter time period to avoid this situation.

If no data is found for the report, the report states that no results were found.

Generating Network Service Reports

If you generate a detailed network service report on a large-scale setup, a message is displayed in the Run Report dialog box recommending that you apply a filter to limit the size of the report.

To generate a network service report using Report Manager:

Step 1 In Prime Network Vision, Prime Network Events, or Prime Network Administration, choose **Reports > Report Manager**.

Step 2 In the Report Manager window, choose **Network Service Reports >** *report-type*.

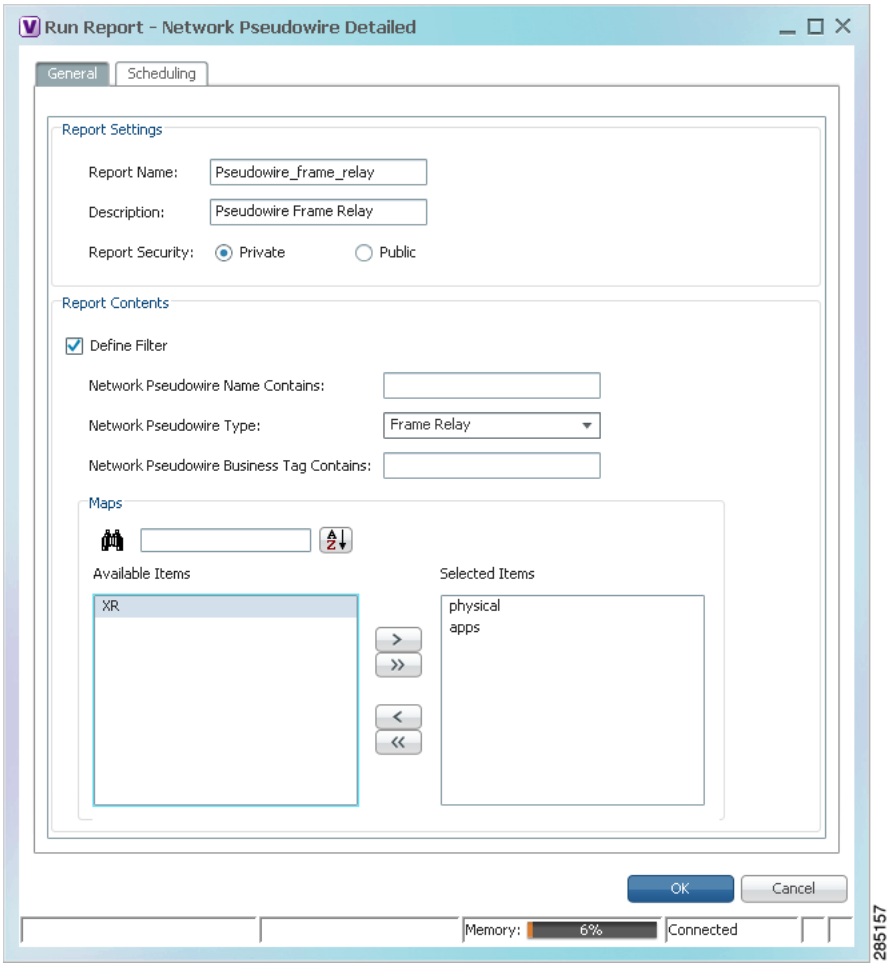
For information on the standard reports available for network services, see Table 10-16.

Step 3 Generate the report in either of the following ways:

- Click **Run** in the toolbar.
- Right-click the report type, then choose **Run**.

The Run Report dialog box is displayed as shown in Figure 10-6.

Figure 10-6 Network Service Report - Run Report Dialog Box



Step 4 Enter the required information the Run Report dialog box as described in Table 10-21.

Table 10-21 Network Service Report - Run Report Dialog Box Fields

Field	Description
Report Settings	
Report Name	Enter a unique name for the report, from 1 to 150 characters in length. Report names cannot include the following characters: ;?<>/:\"#*|.
Description	Enter a brief description of the report.
Report Security	This field is displayed only if report sharing is enabled in Prime Network Administration. Indicate the level of security for the report by clicking the appropriate option: • Private—The report can be viewed and used only by the report creator and the administrator. • Public—The report can be viewed and used by all other users, regardless of whether the devices are listed in the report are in the user's scope. **Note** You can share reports with others only if sharing is enabled in Prime Network Administration. For more information, see the *Cisco Prime Network 3.9 Administrator Guide*.
Ethernet Service Reports—Report Contents	
Define Filter	Check the **Define Filter** check box to enter criteria that must be matched for inclusion in the report. You can specify match criteria in any or all of the following fields.
Ethernet Service Name Contains	Enter a string that must appear in the Ethernet service name for the Ethernet service to be included in the report.
EVC Name Contains	Enter a string that must appear in the EVC name for the EVC to be included in the report.
Ethernet Service Business Tag Contains	Enter a string that must appear in the Ethernet service business tag for the Ethernet service to be included in the report.
EVC Business Tag Contains	Enter a string that must appear in the EVC business tag for the EVC to be included in the report.
Maps	Specify the maps to include in the report: • To include specific maps in the report, in the list of maps on the left, select the required maps, and then click **Add Selected** to move them to the list of maps on the right. • To include all maps in the report, click **Add All**. To find maps that match a string, enter the string in the Find field. The list of maps is automatically updated to include only those maps that contain the string you enter. Click the **Sort Order** button to sort the maps alphabetically or in reverse alphabetic order.

Table 10-21 Network Service Report - Run Report Dialog Box Fields (continued)

Field	Description
Network Pseudowire Reports—Report Contents	
Define Filter	Check the **Define Filter** check box to enter criteria that must be matched for inclusion in the report. You can specify match criteria in any or all of the following fields.
Network Pseudowire Name Contains	Enter a string that must appear in the network pseudowire name for the pseudowire to be included in the report.
Network Pseudowire Type	In the drop-down list, choose the type of network pseudowire to be included in the report.
Network Pseudowire Business Tag Contains	Enter a string that must appear in the network pseudowire business tag for the pseudowire to be included in the report.
Maps	Specify the maps to include in the report: • To include specific maps in the report, in the list of maps on the left, select the required maps, and then click **Add Selected** to move them to the list of maps on the right. • To include all maps in the report, click **Add All**. To find maps that match a string, enter the string in the Find field. The list of maps is automatically updated to include only those maps that contain the string you enter. Click the **Sort Order** button to sort the maps alphabetically or in reverse alphabetic order.
VPLS Reports—Report Contents	
Define Filter	Check the **Define Filter** check box to enter criteria that must be matched for inclusion in the report. You can specify match criteria in any or all of the following fields.
VPLS Name Contains	Enter a string that must appear in the VPLS name for the VPLS or H-VPLS to be included in the report.
VPLS Business Tag Contains	Enter a string that must appear in the VPLS business tag for the VPLS or H-VPLS to be included in the report.
Maps	Specify the maps to be included in the report: • To include specific maps in the report, in the list of maps on the left, select the required maps, and then click **Add Selected** to move them to the list of maps on the right. • To include all maps in the report, click **Add All**. To find maps that match a string, enter the string in the Find field. The list of maps is automatically updated to include only those maps that contain the string you enter. Click the **Sort Order** button to sort the maps alphabetically or in reverse alphabetic order.

Step 5 To schedule a report to run immediately or at a later point in time, click the **Scheduling** tab. For more information, see Scheduling Reports, page 10-38.

Step 6 Click **OK**.

The report appears in the table in the content pane with a state of Running, if the report is scheduled to run immediately, or Scheduled, if the report is scheduled to run at a later point in time. When the report is complete, the state changes to Done.

You can view the reports when the state is Done. Occasionally, some report formats require additional time for generation. If so, a progress bar is displayed, indicating that the report is being created and will be available soon.

If the report exceeds 150 MB, the state changes to Failed and an error message is written to the log. We recommend running the report with more specific criteria or a shorter time period to avoid this situation.

If no data is found for the report, the report states that no results were found.

Generating Reports from the Reports Menu

To generate reports quickly and without opening the Reports Manager window, choose **Reports > Run Report >** *folder* **>** *report-type*. The menus include all standard folders and reports, and any folders or reports that you have created. After entering the required information, you can view the report as soon as it is generated or at a later time.

Note You can generate reports only for devices that are within your scope.

To generate a report from the Reports menu:

Step 1 Choose **Reports > Run Report >** *folder* **>** *report-type* where:

- *folder* is the required folder.
- *report-type* is the required type of report.

Step 2 In the Run Report dialog box, enter the required information. For more information on the options in the Run Report dialog box, see Generating Reports, page 10-22.

Step 3 To schedule a report to run immediately or at a later point in time, click the **Scheduling** tab. For more information, see Scheduling Reports, page 10-38.

Step 4 Click **OK**.

Step 5 In the Running Report dialog box, select the required viewing options:

a. Check the **Open Report Manager to monitor status** check box to open the Report Manager window so that you can view the report generation process. Uncheck the check box to proceed without opening the Report Manager window.

b. Check the **View report immediately upon completion** check box to view the report as soon as it is generated. If you enable this option, the report is displayed in HTML format as soon as it is complete. Uncheck the check box to view the report at a later time by using Report Manager.

Step 6 Click **OK**.

Depending on your selections in Step 5, the Report Manager window is displayed, the report is displayed, or the report is available for viewing at a later time.

Generating Reports from Prime Network Vision

Prime Network Vision enables you to run reports on selected devices from the map and list views.

Note You can generate reports only for devices that are within your scope.

To generate a report from Prime Network Vision:

Step 1 In Prime Network Vision, select the required devices in the map or list view.

Step 2 In the navigation tree or content pane, right-click the selected devices, then choose **Run Report >** *folder* **>** *report-type*.

Step 3 In the Run Report dialog box, enter the required information as described in Generating Reports, page 10-22.

The devices that you select in the navigation pane or content pane are automatically included in the report.

Step 4 To schedule a report to run immediately or at a later point in time, click the **Scheduling** tab. For more information, see Scheduling Reports, page 10-38.

Step 5 Click **OK**.

Step 6 In the Running Report dialog box, specify the desired viewing options:

a. Check the **Open Report Manager to monitor status** check box to open the Report Manager window so that you can view the report generation process. Uncheck the check box to proceed without opening the Report Manager window.

b. Check the **View report immediately upon completion** check box to view the report as soon as it is generated. If you enable this option, the report is displayed in HTML format as soon as it is complete. Uncheck the check box to view the report at a later time by using Report Manager.

Depending on your selections in Step 6, the Report Manager window is displayed, the report is displayed, or the report is available for viewing at a later time.

Scheduling Reports

Prime Network allows you to schedule a report to run immediately or at a later point in time.

To schedule a report:

Step 1 In Prime Network Vision, Prime Network Events, or Prime Network Administration, choose **Reports > Report Manager**.

Step 2 In the Report Manager window, choose *report-category* **>** *report-type*.

For information on the various report categories and report types, see Report Categories, page 10-11.

Step 3 Generate the report in either of the following ways:

- Click **Run** in the toolbar.
- Right-click the report type, then choose **Run**.

The Run Report dialog box is displayed.

Step 4 In the Settings tab, specify the required report criteria. For more information on the options in the Run Report dialog box, see Generating Reports, page 10-22.

Step 5 Click the **Scheduling** tab. By default, the Run Now option is selected and the report is scheduled to run immediately.

Step 6 To schedule the report for a later date/time:

a. Select the **Schedule Job** radio button. The scheduling options Once and Recurring are enabled.

b. To generate the report once, select the **Once** radio button and specify the date and time when you want the report to be generated.

c. To generate the report on a recurring basis, select the **Recurring** radio button and specify the following:

- The date and time range for the recurrence.
- How often you want to generate the report within that time range - every X minutes, daily, weekly, or monthly.

Step 7 Specify comments, if required and click **Schedule**. Prime Network creates a report job and executes it according to your scheduling specifications. Go to the **Scheduled Jobs** page (**Tools > Scheduled Jobs**), to check that your report job has been created. You can use the Scheduled Jobs page to monitor the job status and to reschedule a job if necessary.

Managing Reports

Prime Network provides the following options for working with reports:

- Managing the Maximum Number of Concurrent Reports, page 10-39
- Viewing and Saving Reports, page 10-40
- Renaming Reports, page 10-41
- Sharing Reports, page 10-42
- Moving Reports Between Folders, page 10-43
- Deleting Reports, page 10-43
- Viewing Report Properties, page 10-44

Managing the Maximum Number of Concurrent Reports

Prime Network enables you to run multiple reports at the same time. When the maximum number of concurrent reports is running, new report requests are queued for generation and have the status Queued (*n*) where *n* is the number in the report queue. When a running report moves to a Completed, Failed, or Cancelled state, the first report in the queue starts running.

The maximum number of concurrent reports is set at 5 by default. As the event rate approaches the maximum committed event rate, we recommend that you decrease the maximum number of concurrent reports. The maximum number of concurrent reports is defined in the registry, in reports.xml, under site/reports/reports-setting/reports-running-settings/maxRunningReports.

Note Changes to the registry should only be carried out with the support of Cisco. For details, contact your Cisco account representative.

To change the maximum number of concurrent reports, use the **runRegTool** command (located in *ANAHOME*/Main) as follows:

```
./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
site/reports/reports-setting/reports-running-settings/maxRunningReports value
```

where *value* is the new maximum number of concurrent reports.

You do not need to restart any AVMs after entering this command.

For more information on the **runRegTool** command, see the *Cisco Prime Network 3.9 Administrator Guide*.

Viewing and Saving Reports

You can view any reports that appear in the Report Manager content pane with the state Done. After viewing a report, you can save it in any of the available formats.

Note Reports are purged from Prime Network after 90 days by default. This setting can be modified by changing the setting in Prime Network Administration. For more information, see the *Cisco Prime Network 3.9 Administrator Guide*.

To view and save a report:

Step 1 Choose **Reports > Report Manager**.

Step 2 In the navigation pane, locate the required report in either of the following ways:

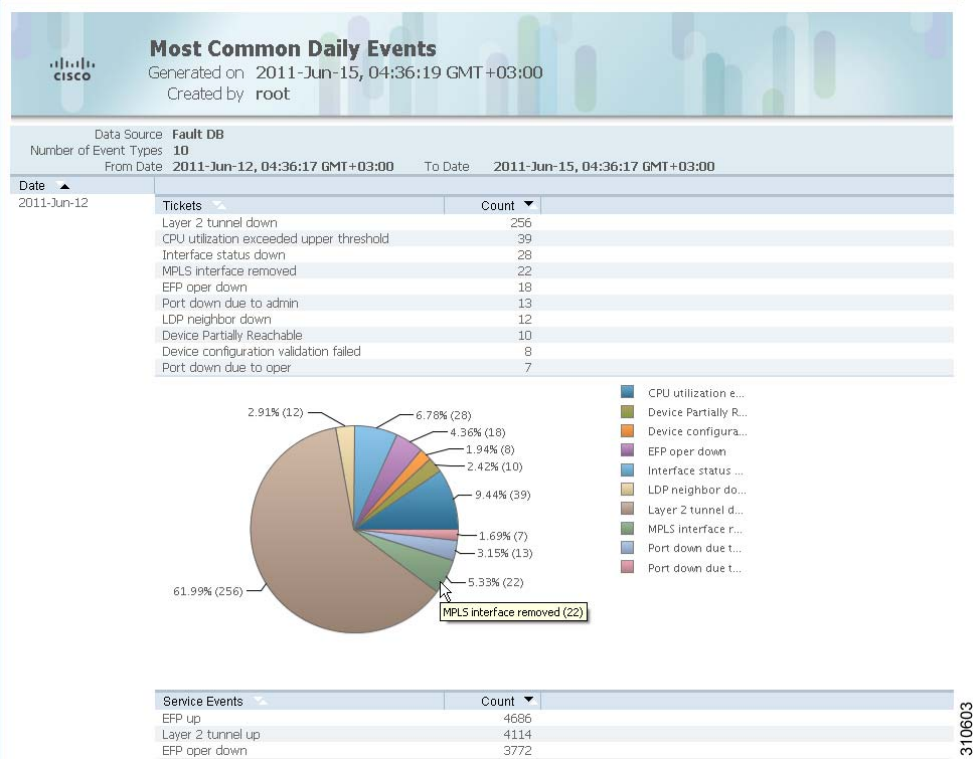
- Select the folder containing the report.
- Select the report type.

Step 3 In the content pane, right-click the report, then choose **View As >** *format* where *format* is one of the following:

- HTML—Displays the report in a browser window. Clicking a column heading in the report sorts the report by that value; clicking the column heading again sorts the data in the reverse order. HTML is the default format.
- PDF—Displays a PDF version of the report.
- CSV—Creates a CSV version of the report that you can either save to a specific location or view using another application. The CSV version contains only the report data; it does not contain the header information, layout, or formatting information that is available in other formats.
- XLS—Creates an XLS version of the report that you can either save to a specific location or view using another application, such as Microsoft Excel.
- XML—Creates an XML version of the report that you can either save to a specific location or view using an XML editor or viewer.

Figure 10-7 is an example of the Most Common Daily Events report in HTML format. The data is sorted by the Count column, in descending order.

Figure 10-7 Most Common Daily Events Report Example



Step 4 Save the report as required.

Renaming Reports

You can rename:

- Any report type that you defined.
- Any generated report that you have access to.

You cannot rename any of the Prime Network standard report types.

Renaming a User-Defined Report Type

Note When you rename a report type, the new name applies to only those reports that you run after changing the name; it does not change the names of reports that were run prior to changing the name.

To rename a user-defined report type:

Step 1 In the navigation tree, select the user-defined report type.

Step 2 Right-click the report type, then choose **Properties**.

Step 3 In the Edit dialog box, enter a new name for the report type in the Report Name field, using the following conventions:

- The name can contain 1 to 150 characters.
- The name cannot include the following characters: ;?<>/:\"#*|.

Step 4 Click **OK**.

The navigation pane is refreshed and the report type is displayed with the new name.

Renaming a Generated Report

To rename a report:

Step 1 Choose **Reports > Report Manager**.

Step 2 In the content pane, right-click the report that you want to rename, then choose **Rename** or **Properties**.

Step 3 In the Name field, enter the new name for the report, using the following conventions:

- The name can contain 1 to 150 characters.
- The name cannot include the following characters: ;?<>/:\"#*|.

Step 4 Click **OK**.

The content pane is refreshed and the report is displayed with the new name.

Sharing Reports

Prime Network enables you to share reports that you generate with other users, or limit access to a report to only you and the administrator.

Note You can share reports with others only if sharing is enabled in Prime Network Administration. For more information, see the *Cisco Prime Network 3.9 Administrator Guide*.

Sharing a Report

To share access to a report that you generated:

Step 1 Choose **Reports > Report Manager**.

Step 2 In the navigation pane, locate the required report in either of the following ways:

- Select the folder containing the report.
- Select the report type.

Step 3 In the content pane, right-click the report that you want to share, then choose **Share**.

The report is available to all system users for viewing and using.

Limiting Access to a Report

To limit access to a report that you generated and subsequently shared:

Step 1 Choose **Reports > Report Manager**.

Step 2 In the navigation pane, locate the required report in either of the following ways:

- Select the folder containing the report.
- Select the report type.

Step 3 In the content pane, right-click the report that you want to limit access to, then choose **Unshare**.

The report can be viewed and used by only you and the administrator.

Moving Reports Between Folders

You can move a report type that you have defined from the current folder to another folder in the navigation tree.

Note You cannot move a standard report type from one folder to another.

To move a report type to a new folder:

Step 1 Choose **Reports > Report Manager**.

Step 2 In the navigation tree, select the required report that you have defined.

Step 3 Do either of the following:

- Click **Move** in the toolbar.
- Right-click the report, then choose **Move**.

Step 4 In the Move To dialog box, select the folder to which you want to move the report.

Step 5 Click **OK**.

The Report Manager window is refreshed and the report appears in the specified folder.

Deleting Reports

You can delete reports to which you have access.

To delete a report:

Step 1 Choose **Reports > Report Manager**.

Step 2 In the navigation pane, locate the required report in either of the following ways:

- Select the folder containing the report.
- Select the report type.

Step 3 In the content pane, select the required report.

Step 4 Delete the report in either of the following ways:

- Right-click the report, then choose **Delete Report**.
- Click **Delete Report** in the toolbar.

Step 5 In the Delete Report confirmation window, click **Yes** to confirm deletion.

The Report Manager window is refreshed and the deleted report no longer appears.

Viewing Report Properties

The Report Properties dialog box enables you to view the report settings and to modify some of them.

To view report properties, and optionally change the name, description, or access:

Step 1 Choose **Reports > Report Manager**.

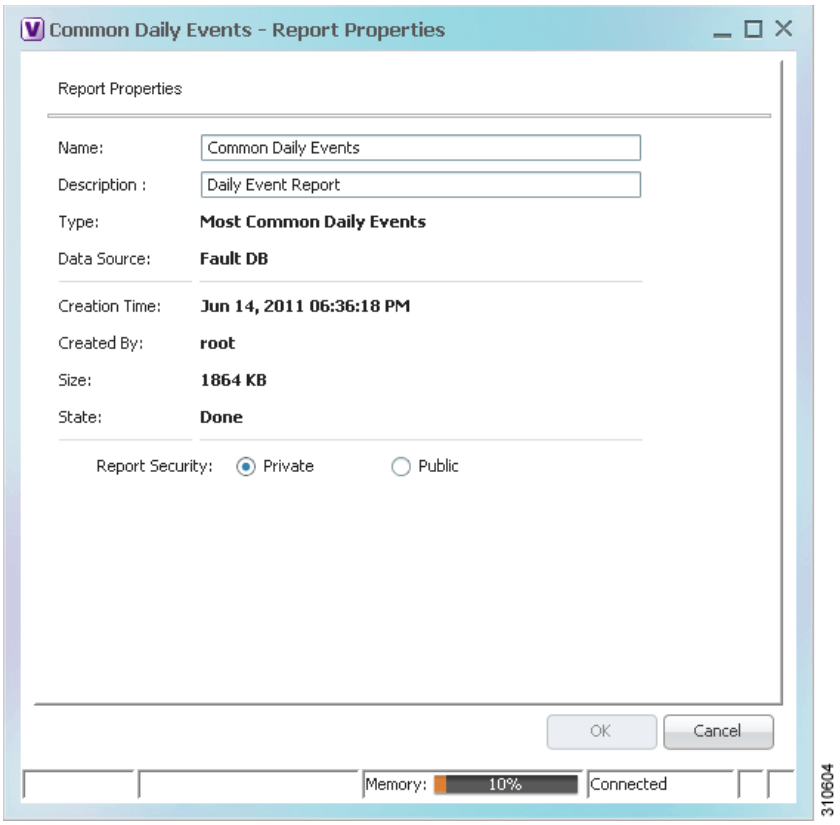
Step 2 In the navigation pane, locate the required report in either of the following ways:

- Select the folder containing the report.
- Select the report type.

Step 3 In the content pane, right-click the selected report, then choose **Properties**.

The Report Properties dialog box is displayed, as shown in Figure 10-8.

Figure 10-8 Report Properties Dialog Box



The Report Properties dialog box contains the following information about the report:

- Name
- Description
- Type
- Source of the information
- Date and time it was created
- User who created it
- Size
- State
- Access

Step 4 Change the information in the following fields as required:

- Name
- Description
- Report Security

Step 5 Click **OK**.

Defining Report Types

You can modify any of the report types provided by Prime Network so that it better suits your needs and environment. This is extremely beneficial if you generate a particular type of report for specific devices or events on a regular basis.

To define a report type:

Step 1 Choose **Reports > Report Manager**.

Step 2 In the navigation pane, select the existing report type on which you want to base your report type and then do either of the following:

- Right-click the existing report type, then choose **Define Report of This Type**.
- Click **Define Report of This Type** in the toolbar.

Step 3 In the Define report of type dialog box, specify the options using the information in Generating Reports, page 10-22.

Step 4 In the Location field, use the specified reports folder or click **Browse** to select a different folder.

Step 5 Click **OK**.

The newly defined report type appears in the navigation tree in the specified folder.

Working with Report Folders

Prime Network provides the following options for working with report folders:

- Creating Folders, page 10-46
- Moving Folders, page 10-47
- Renaming Folders, page 10-47
- Deleting Folders, page 10-48
- Viewing Folder and Report Type Properties, page 10-48

Creating Folders

Prime Network enables you to create additional report folders in Report Manager.

To create a report folder:

Step 1 Choose **Reports > Report Manager**.

Step 2 Select a folder in which to place the new folder.

Step 3 Do one of the following:

- Click **New Folder** in the toolbar.
- Right-click the folder, then choose **New Folder**.

Step 4 In the New Folder dialog box, enter a name for the folder.

Step 5 Click **OK**.

The navigation pane is refreshed and the new folder is displayed.

Step 6 To move the new folder to another folder, or to the top level in the folder hierarchy:

a. In the navigation pane, select the newly created folder, and then do one of the following:
   - Click **Move** in the toolbar.
   - Right-click the folder, then choose **Move**.

b. In the Move To dialog box, select the location where you want the folder to reside.

c. Click **OK**.

   The folder is displayed in the new location.

Moving Folders

Prime Network enables you to move folders that you have created in Report Manager. You cannot move the Events Reports, Inventory Reports, or Network Service Reports folder.

To move a report folder:

Step 1 Choose **Reports > Report Manager**.

Step 2 In the navigation pane, select the folder you want to move, and then do one of the following:
- Click **Move** in the toolbar.
- Right-click the folder, then choose **Move**.

Step 3 In the Move To dialog box, select the location where you want the folder to reside.

Step 4 Click **OK**.

The navigation pane is refreshed and the folder is displayed in the new location.

Renaming Folders

Prime Network enables you to rename folders that you have created in Report Manager. You cannot:
- Rename a folder that resides at the highest level in the hierarchy, such as the Events Reports, Inventory Reports, or Network Service Reports folder.
- Use the same name for different folders that reside at the same level in the hierarchy.

To rename a report folder:

Step 1 Choose **Reports > Report Manager**.

Step 2 In the navigation pane, select the folder you want to rename, and then do one of the following:
- Click **Rename** in the toolbar.
- Right-click the folder, then choose **Rename**.

Step 3 In the Rename Folder dialog box, enter the new name for the folder.

Step 4 Click **OK**.

The navigation pane is refreshed and the folder is displayed with the new name.

Deleting Folders

You can delete folders that you have created in Report Manager if they are empty. You cannot delete the following folders:

- Events Reports
- Detailed Network Events
- Detailed Non-Network Events
- Inventory Reports
- Network Service Reports
- User-created folders that contain other folders or report types

To delete a report folder:

Step 1 Choose **Reports > Report Manager**.

Step 2 In the navigation pane, select the folder you want to delete, and then do one of the following:

- Click **Delete** in the toolbar.
- Right-click the folder, then choose **Delete**.

Step 3 In the Confirm Folder Delete dialog box, click **Yes** to confirm the deletion.

The navigation pane is refreshed and the folder no longer appears.

Viewing Folder and Report Type Properties

The following topics describe how to view properties for folders and report types:

- Viewing Report Folder Properties, page 10-48
- Viewing Report Type Properties, page 10-50

Viewing Report Folder Properties

The Report Properties window enables you to view report properties and to add folders.

To view report properties:

Step 1 Choose **Reports > Report Manager**.

Step 2 In the navigation pane, right-click the required folder, then choose **Properties**.

The Folder Properties window is displayed, as shown in Figure 10-9.

Figure 10-9 Folder Properties

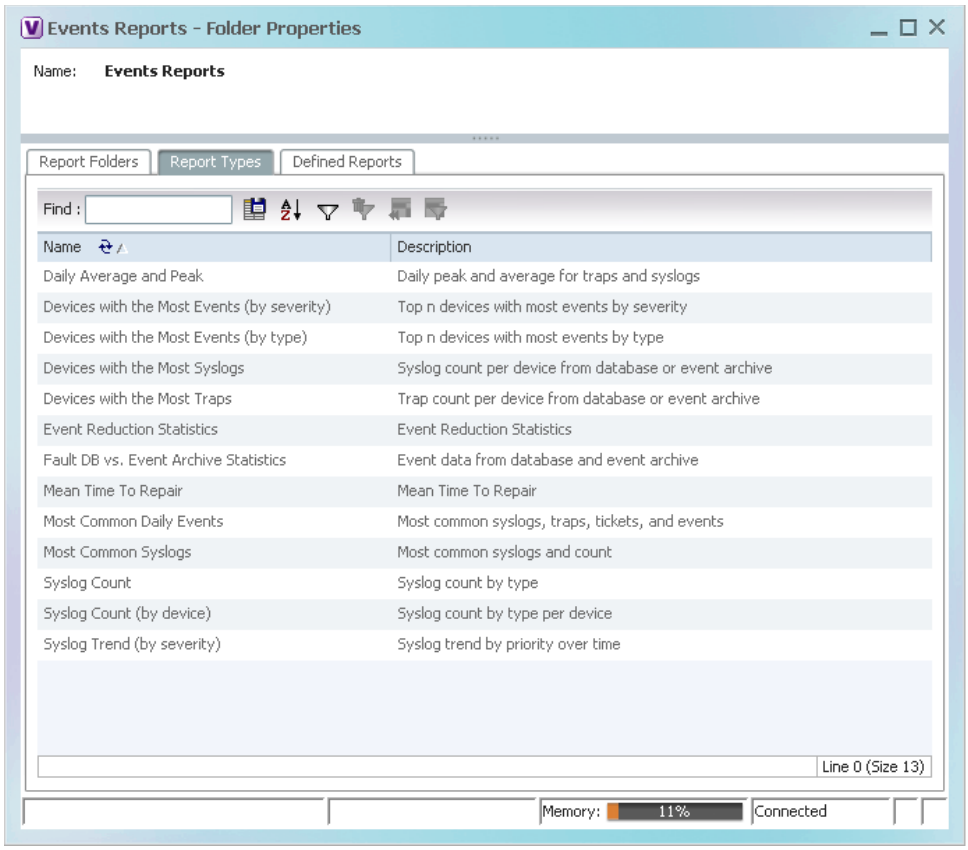


Table 10-22 describes the information that is displayed in each tab, depending on the folder's contents.

Table 10-22 Folder Properties Window

Field	Description
Report Folders Tab	
Name	Name of the folder included in the selected folder.
Report Types Tab	
Name	Name of the report type included in the selected folder.
Description	Description of the report type included in the selected folder.
Defined Reports Tab	
Name	Name of the user-defined report in the selected folder.
Description	Description of the user-defined report in the selected folder.
Type	Report type on which the user-defined report is based.
Public	Status of public access to the report: True or False.

Viewing Report Type Properties

To view report type properties:

Step 1 In the navigation pane, right-click the required report type, then choose **Properties**.

The information that is displayed depends on whether the report type is one that you defined or one provided by Prime Network:

- Prime Network-provided report type—The Report Type Properties window is displayed with the report name and description. Click **Run** to generate the report.
- User-defined report type—The Edit dialog box is displayed with all settings specified for the report type. You can modify the settings or leave them as they are.

Step 2 Click **Close** or the upper right corner to close the window.



CHAPTER 11

Using Cisco PathTracer to Diagnose Problems

Cisco PathTracer enables you to view a network path between two network objects. The following topics describe Cisco PathTracer and how to use it:

- User Roles Required to Work with Cisco PathTracer, page 11-1
- Cisco PathTracer Overview, page 11-2
- Launching Path Traces, page 11-3
- Viewing Path Traces in Cisco PathTracer, page 11-14
- Viewing Path Trace Details, page 11-21
- Saving and Opening Cisco PathTracer Map Files, page 11-26
- Saving Cisco PathTracer Counter Values, page 11-27
- Rerunning a Path and Comparing Results, page 11-27
- Viewing Q-in-Q Path Information, page 11-28
- Viewing L2TP Path Information, page 11-29
- Using Cisco PathTracer in MPLS Networks, page 11-29

User Roles Required to Work with Cisco PathTracer

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

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

For more information on user authorization, see the *Cisco Prime Network 3.9 Administrator Guide*.

The following tables identify the tasks that you can perform:

- Table 11-1 identifies the tasks that you can perform if a selected element **is not in** one of your assigned scopes.
- Table 11-2 identifies the tasks that you can perform if a selected element **is in** one of your assigned scopes.

By default, users with the Administrator role have access to all managed elements. To change the Administrator user scope, see the topic on device scopes in the *Cisco Prime Network 3.9 Administrator Guide*.

Table 11-1 Default Permission/Security Level Required for Working with Cisco PathTracer - Element Not in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Launch a path trace	—	—	—	—	X
View path information	—	—	—	—	X
Save Cisco PathTracer map files	—	—	—	—	X
Save Cisco PathTracer counter values	—	—	—	—	X
Rerun a path and compare results	—	—	—	—	X

Table 11-2 Default Permission/Security Level Required for Working with Cisco PathTracer - Element in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Launch a path trace	—	X	X	X	X
View path information	—	X	X	X	X
Save Cisco PathTracer map files	—	X	X	X	X
Save Cisco PathTracer counter values	—	X	X	X	X
Rerun a path and compare results	—	X	X	X	X

Cisco PathTracer Overview

Cisco PathTracer enables you to launch end-to-end route traces and view related performance information for Layer 1, Layer 2, and Layer 3 traffic. Upon receiving a path's start and endpoint, Cisco PathTracer visually traces the route through the network. For example, in an ATM network environment, Cisco PathTracer identifies all information regarding the connection of a subscriber to a provider, including all ATM PVCs, ATM switching tables, ATM class of service (CoS) definitions, IP-related information, and so on.

You can also use Cisco PathTracer to:

- Trace paths using IPv4, IPv6, or both IPv4 and IPv6 addresses for the source and destination.
- Trace a hypothetical Ethernet frame from a VLAN interface to a specified MAC address.
- Trace a hypothetical Ethernet frame from an Ethernet interface to a specified MAC address within a specific VLAN identifier.

In MPLS and Carrier Ethernet environments, Cisco PathTracer can trace paths across:

- Carrier Supporting Carrier (CSC) configurations—A path trace along a CSC flow follows the path from the customer CE through the customer carrier VPN, across the customer backbone carrier VPN, back to the customer carrier VPN, and to the destination CE.
- VLANs—A path trace across VLANs follows the path based on the forwarding table, which means that the trace follows ports in the Forwarding STP state.
- Q-in-Q—A path trace across Q-in-Q creates a single path trace (if the MAC address is learned) or a multiple-path (multipath) trace if the MAC address is not in the forwarding table. If the VLAN bridge has not learned a given MAC address, the bridge floods the Ethernet frame to the confines of a given VLAN or switching entity and across those ports that allow the given VLAN identifier. A MAC/VLAN path trace can be conducted from a customer edge (CE) VLAN interface across a service provider (SP) VLAN; that is, across Q-in-Q configurations with the CE-VLAN identifier as the inner VLAN identifier and Cisco PathTracer detecting the outer SP-VLAN identifier that encapsulates the CE-VLAN.
- Pseudowires (also known as EoMPLS)—A MAC/VLAN path trace can be conducted from a VLAN interface across a VLAN attachment to a pseudowire.
- VLAN-VPLS-VLAN configurations—A multiple-point MAC/VLAN path trace can be conducted on CE-VLANs across a service provider VPLS transport from a VLAN interface that attaches to the VPLS.

In addition, Cisco PathTracer can trace a path:

- If the destination MAC address is not reachable—If Cisco PathTracer cannot complete a MAC/VLAN path trace to a specified destination MAC address across an MPLS core, VPLS, or H-VPLS, then Cisco PathTracer displays the portion of the path that Cisco PathTracer can trace toward the destination MAC address.
- That contains a simulated Ethernet frame—Cisco PathTracer can trace a simulated Ethernet frame from a VLAN port, across a VLAN (VLAN-based flow domain fragment), VPLS (VPLS-based flow domain fragment), and VLAN, for an end-to-end MAC address trace.

Prime Network derives the various paths on the network from its up-to-date knowledge of the network. After a user selects a source and destination, Cisco PathTracer finds and retrieves the path of a specified service, and displays the path in the Cisco PathTracer window. The retrieved information contains network elements in the path, including all properties at Layer 1, Layer 2, and Layer 3, plus alarm information, counters, and more, all of which is available via Cisco PathTracer.

Launching Path Traces

Cisco PathTracer can be launched from a bridge, switching entity, Ethernet interface, Ethernet flow point, VLAN interface, ATM VC, DLCI, or IP interface entry point. Ethernet flow points can be starting points whether they are associated with an interface, bridge, or LAG.

The virtual route is found according to the cross connect table of each ATM switch or Frame Relay device. The IP routing and path-finding process is enabled according to the VRF tables of each router, and the Ethernet-simulated path is found according to the various Layer 2 forwarding tables, such as bridges or VSIs.

To view a specific path, you must specify an initial point and a destination, such as an IP or MAC address. If you specify VC or DLCI information, which ends in a router, Cisco PathTracer finds the next hop according to the destination IP address. If you do not specify a destination IP or MAC address, Cisco PathTracer uses the default gateway in the router. Any business tags that are associated with the physical or logical entities are also displayed.

Note A path can also be launched if a business tag attached to an endpoint that can be used as the starting point.

Path Traces and Blocked Ports

The following conditions apply for blocked ports:

- You can launch a path trace from a blocked port. This action is equivalent to launching a path trace from a bridge.
- You can specify a blocked port as a destination.
- If Cisco PathTracer encounters a blocked port in its path to the destination, the path trace stops. Path traces do not traverse blocked ports.

Table 11-3 identifies the available path trace launching points and their locations within Cisco Prime Network Vision. Cisco PathTracer is available in each location as a right-click menu option.

Cisco PathTracer Right-Click Menu Options

Cisco PathTracer is launched by using right-click menu options. Table 11-3 identifies the launching points for the different types of elements.

Table 11-3 Cisco PathTracer Right-Click Menu Options

Element	Location
Affected Parties	• Inventory window • Ticket Properties window (Affected Parties tab)
Bridge	Inventory window
Business tag	The path can be found using a business tag, which is attached to the VPI/VCI, or using an IP interface by entering its key. The path can then be opened from the Find Business Tag dialog box.
Ethernet flow point	• Map view or navigation pane • Inventory window
IP interface	• Inventory window • Affected entry
Layer 2 MPLS tunnel	Inventory window
MPLS-TE tunnel	Inventory window
MPLS-TP tunnel endpoint	• Map view or navigation pane • Inventory window
Port	Inventory window

Table 11-3 Cisco PathTracer Right-Click Menu Options (continued)

Element	Location
Pseudowire endpoint	• Map view or navigation pane • Inventory window
Site	Map view
Switching entity	Map view
Virtual connection	Inventory window: • Cross Connect window • VC Table window
VLAN	• Navigation pane • Map view

Starting a Path Trace

You can start a path trace in the following ways:

- From the Map View, page 11-5
- From Logical or Physical Inventory, page 11-7

From the Map View

To start a path trace from the map view:

Step 1 In a Cisco Prime Network Vision map, start the path trace in one of the following ways:

- For a VLAN:

  a. In the navigation pane or map pane, select the required network VLAN.

  b. Double-click the VLAN to view the VLAN entities.

  c. Right-click the required item and choose **PathTracer > From Here to Destination** or **PathTracer > Start Here**.

- For a VPN:

  a. In the navigation pane or map pane, select the required network VPN.

  b. Double-click the VPN to view the VPN entities.

  c. Right-click the site and choose **PathTracer > From Here to Destination** or **PathTracer > Start Here**.

- For an Ethernet flow point:

  a. Choose **Network Inventory > Ethernet Flow Domains**.

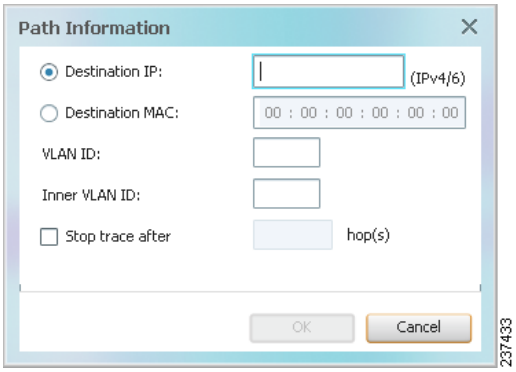
  b. In the Ethernet Flow Domain List Properties window, double-click the required domain.

  c. In the Ethernet Flow Domain Properties window, right-click the required element and choose **PathTracer > From Here to Destination** or **PathTracer > Start Here**.

The next step depends on your choice in Step 1:

- If you choose **PathTracer > From Here to Destination**, the Path Information dialog box is displayed (Figure 11-1). Continue with Step 2.
- If you choose **PathTracer > Start Here**, continue with Step 3.

Figure 11-1 Path Information Dialog Box



Step 2 To specify a destination:

a. In the Path Information dialog box, enter the required information, as described in Table 11-4.

Depending on the launch point, the Path Information dialog box might not contain all of the fields in Table 11-4.

Table 11-4 Cisco PathTracer Path Information Dialog Box

Field	Description
Destination IP	Select this option to specify an IP address as the destination. Enter either an IPv4 or IPv6 address.
Destination MAC	Select this option to specify a MAC address as the destination. Enter the MAC address.
VLAN ID	Enter the required VLAN identifier. You must enter an IP address or a MAC address to use this option.
Inner VLAN ID	Enter the required inner VLAN identifier.
Stop trace after	Check this check box to limit the number of hops that Cisco PathTracer makes in its attempt to reach the destination. Enter the maximum number of hops that you want to allow in the hops field.

b. Click **OK**.

Step 3 If you choose **Start Here**, navigate to the destination interface, port, or bridge, right-click it, and choose **End Here**.

The Cisco PathTracer window is displayed showing the path or paths that were found.

Step 4 To view additional details regarding the path traces, select one or more paths in the paths pane.

Step 5 In the toolbar, click **Cisco PathTracer**.

- If you select one or more paths in the paths pane, each selected path is displayed in its own window with the Layer 1, Layer 2, Layer 3, and Business Tag tabs.
- If you select nothing in the Paths pane, each path found is displayed in its own window with the Layer 1, Layer 2, Layer 3, and Business Tag tabs.

For more information about the end-to-end path and networking layer details, see Viewing Path Trace Details, page 11-21.

From Logical or Physical Inventory

To start a path trace from logical or physical inventory:

Step 1 Open the inventory window for the required device.

Step 2 Select one of the following launch points in logical or physical inventory:

- IP interface
- MPLS-TP tunnel endpoint
- Port
- Pseudowire endpoint
- VLAN bridge

Step 3 Right-click the selected item and choose one of the following:

- **PathTracer > From Here to Destination**—If you choose this option, continue with Step 2 in From the Map View, page 11-5.

  Note If you select an IP interface as the launch point, the right-click menu displays IPv4 and IPv6 options. These options are enabled or dimmed, depending on whether the IP interface has an IPv4 IP address, an IPv6 address, or both IPv4 and IPv6 addresses. For an example, see Figure 11-3.

- **PathTracer > Start Here**—If you choose this option, continue with Step 3 in From the Map View, page 11-5.

Examples of Launching Cisco PathTracer

The following topics provide examples for launching Cisco PathTracer from different locations in Cisco Prime Network Vision:

- Using an Ethernet Flow Point, page 11-8
- Using an IP Interface, page 11-9
- Using a VLAN Bridge, page 11-10
- Using an Ethernet Port, page 11-12
- Using a Pseudowire, page 11-12

- Using an MPLS-TP Tunnel Endpoint, page 11-13

Using an Ethernet Flow Point

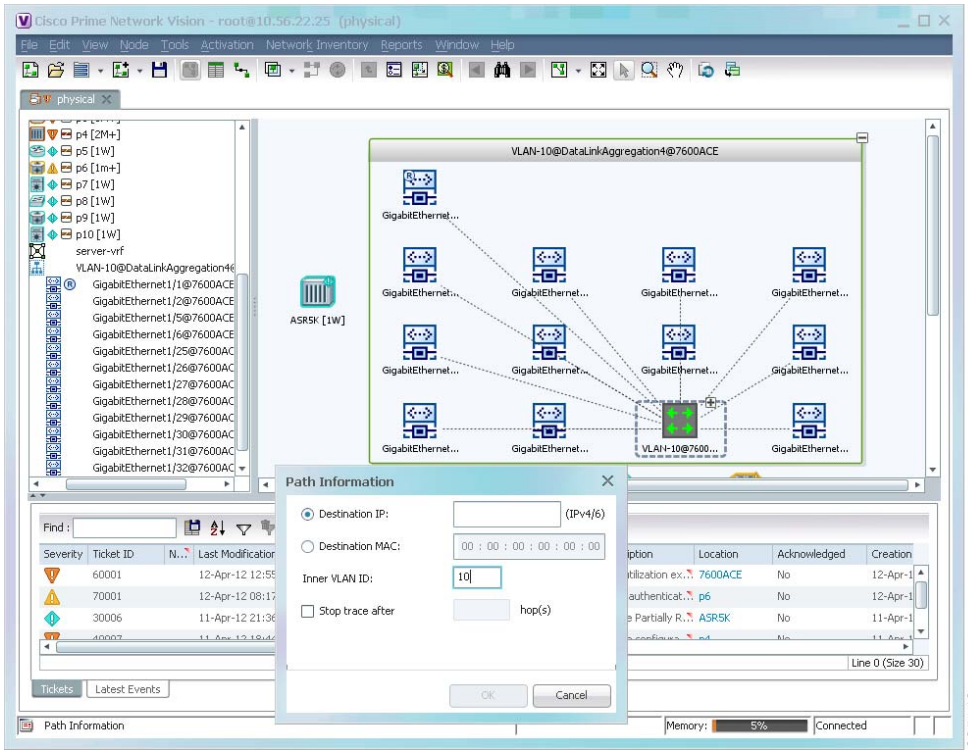
A network VLAN is required for you to start a path trace using an Ethernet flow point.

To launch a path trace from an Ethernet flow point:

Step 1 In the Cisco Prime Network Vision navigation pane or map pane, expand the required network VLAN.

Step 2 In the VLAN, right-click the required Ethernet flow point and choose **PathTracer > From Here to Destination**. The Path Information dialog box is displayed as shown in Figure 11-2.

Figure 11-2 Ethernet Flow Point Path Trace Launch Point



Step 3 Specify the destination using the information in Table 11-4.

Step 4 To limit the number of hops for the path trace, check the *Stop trace after* check box, and enter the maximum number of hops for the path trace.

Step 5 Click **OK**. The Cisco PathTracer window is displayed with the resulting path trace.

Using an IP Interface

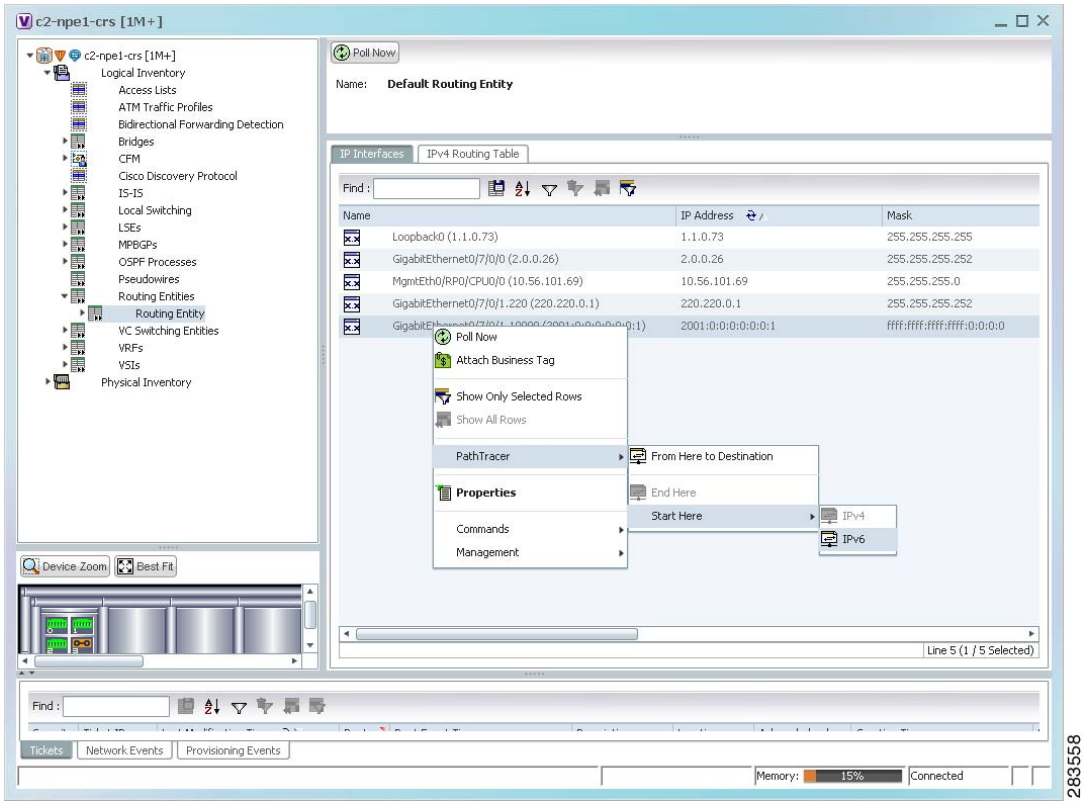
Both IPv4 and IPv6 addresses are supported as valid path trace sources and destinations as illustrated in the following procedure.

To launch a path trace from an IP interface:

Step 1 In logical inventory, right-click the required IP interface (**Logical Inventory > Routing Entities > Routing Entity >** *ip-interface*).

The right-click menu displays IPv4 and IPv6 options. These options are enabled or dimmed, depending on whether the IP interface has an IPv4 address, an IPv6 address, or both IPv4 and IPv6 addresses. See Figure 11-3.

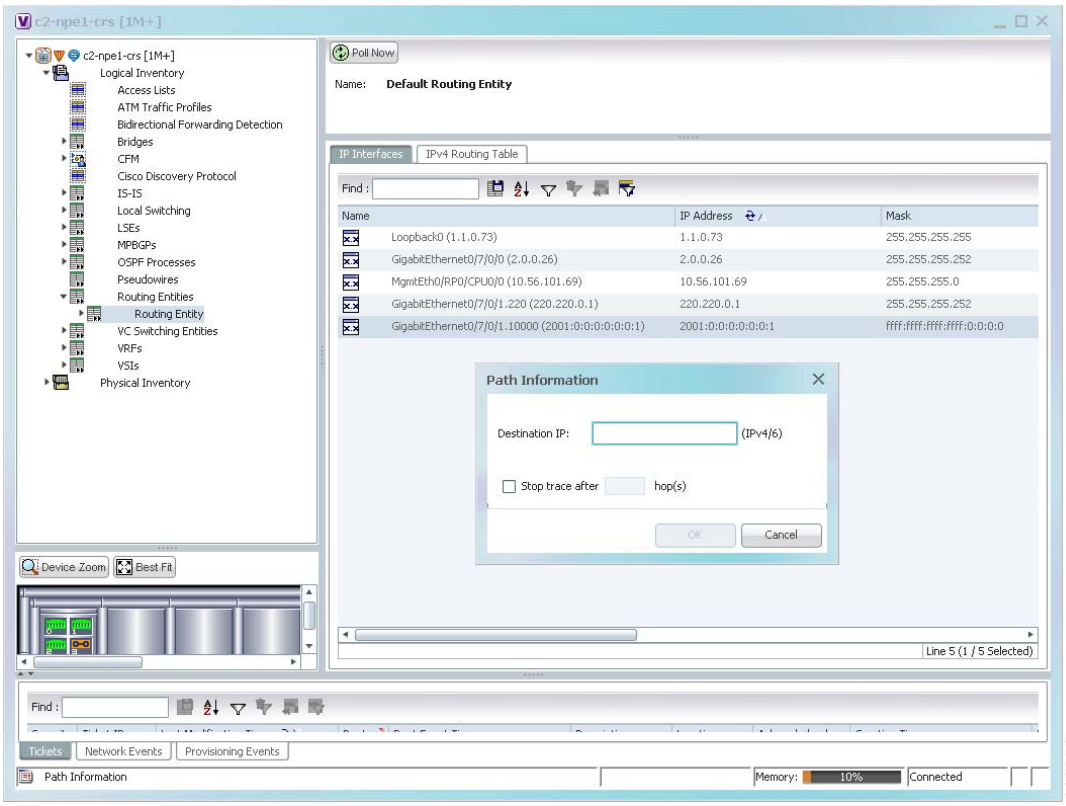
Figure 11-3 IP Interface Path Trace Launch Point - Right-Click Menu



Step 2 Choose **PathTracer > From Here to Destination**.

The Path Information dialog box is displayed as shown in Figure 11-4.

Figure 11-4 IP Interface Path Trace Launch Point - Path Information Dialog Box



Step 3 In the Destination IP field, enter the IPv4 or IPv6 address.

Step 4 To limit the number of hops for the path trace, check the *Stop trace after* check box, and enter the maximum number of hops for the path trace.

Step 5 Click **OK**. The Cisco PathTracer window appears, displaying the resulting path trace.

Using a VLAN Bridge

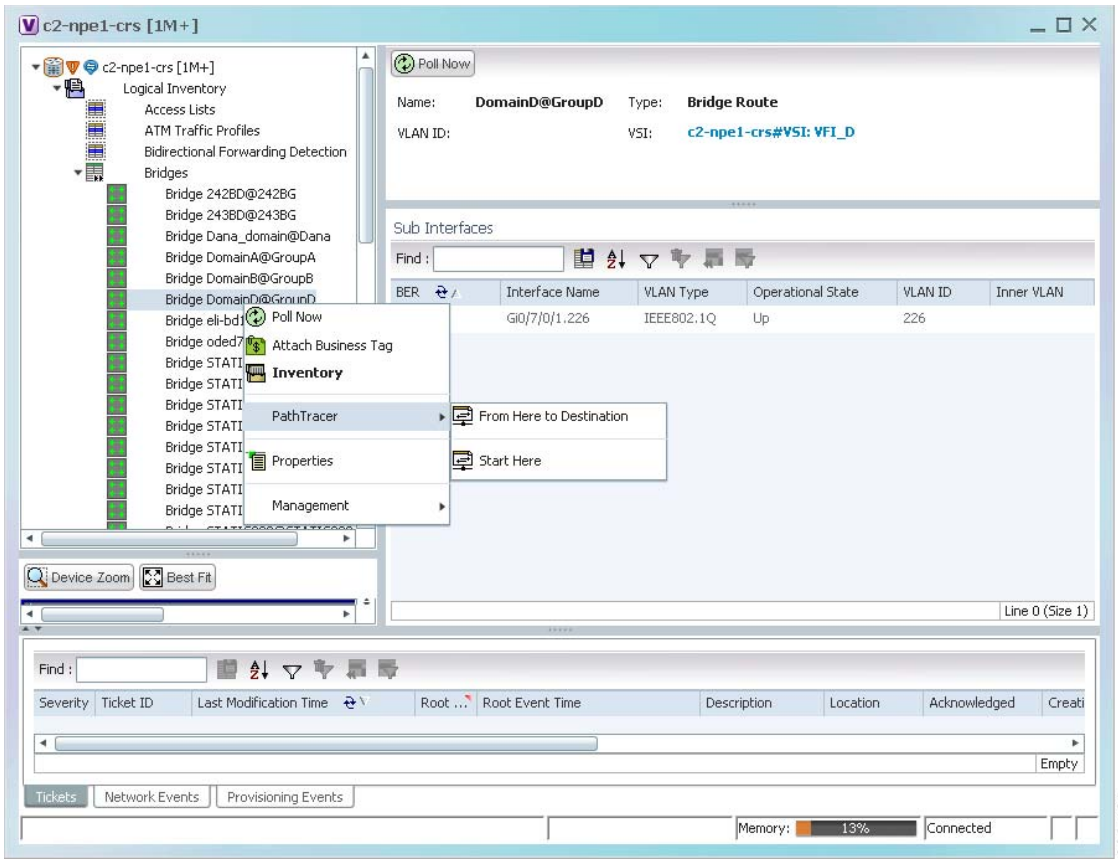
You can launch path traces from VLAN bridges. Additionally, MAC addresses in the VLAN bridge forwarding table can be path trace destinations.

To launch a path trace from a VLAN bridge:

Step 1 In logical inventory, right-click the required bridge (**Logical Inventory > Bridges >** *bridge*) and choose one of the following options as shown in Figure 11-5:

- **PathTracer > From Here to Destination**
- **PathTracer > Start Here**

Figure 11-5 VLAN Bridge Path Trace Launch Point



Step 2 If you choose **From Here to Destination** in Step 1, the Path Information dialog box is displayed. Specify the required destination using the information in Table 11-4.

Step 3 If you choose **Start Here**, navigate to the destination, right-click it, and choose **End Here**. Destination options include:

- IP interface—**Logical Inventory > Routing Entities > Routing Entity >** *IP-interface*
- Bridge—**Logical Inventory > Bridges >** *bridge*
- MAC address—**Logical Inventory > Bridges >** *bridge* **> Bridge Table >** *MAC-address*
- Ethernet port—**Physical Inventory >** *chassis* **>** *slot* **>** *port*

When a destination is selected, the system extracts the relevant IP address from this point and uses it as the destination.

The Cisco PathTracer window is displayed with the resulting path trace.

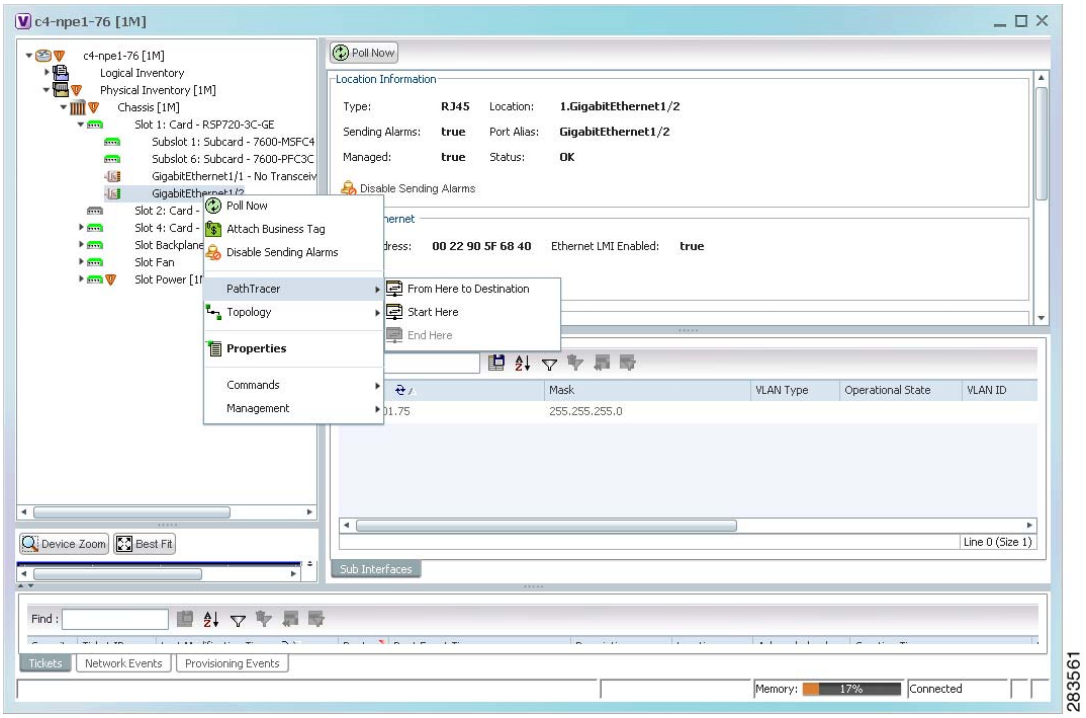
Using an Ethernet Port

To launch a path trace from an Ethernet port:

Step 1 In physical inventory, right-click the required port (**Physical Inventory > Chassis >** *slot* **>** *subslot* **>** *port*) and choose one of the following options as shown in Figure 11-6:

- **PathTracer > From Here to Destination**
- **PathTracer > Start Here**

Figure 11-6 Ethernet Port Path Trace Launch Point



Step 2 Depending on your choice in Step 1, specify the required destination information or select the path trace endpoint.

The Cisco PathTracer window appears, displaying the resulting path trace.

Using a Pseudowire

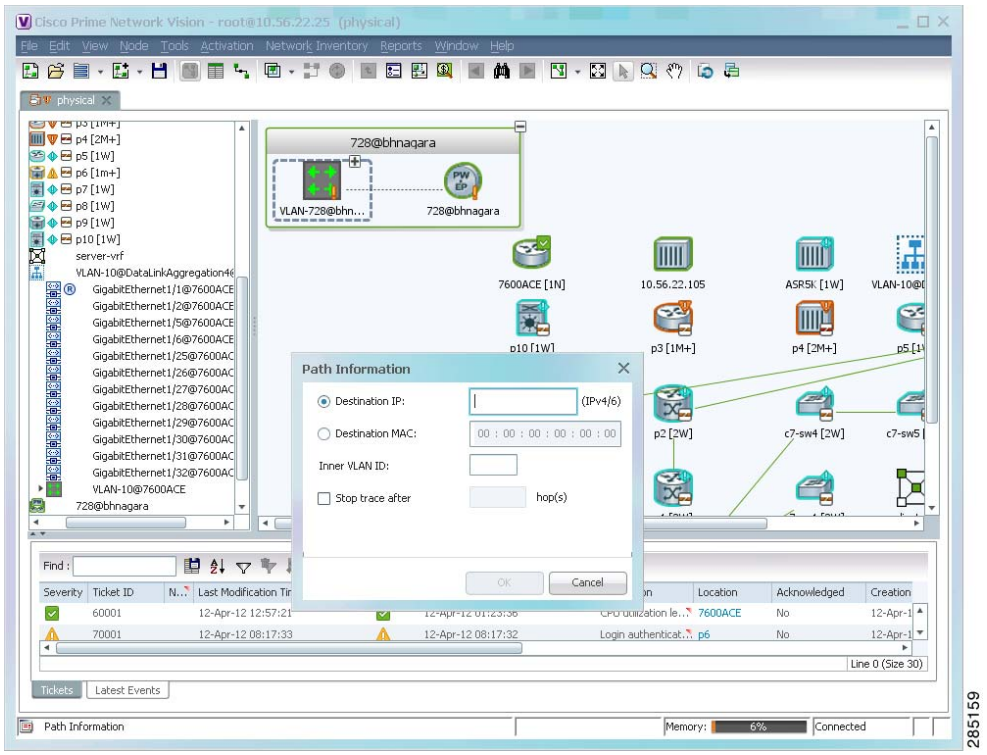
To launch a path trace from a network pseudowire endpoint:

Step 1 In the navigation pane or map pane, expand the required network pseudowire.

Step 2 Right-click the required pseudowire endpoint and choose **PathTracer > From Here to Destination**.

The Path Information dialog box is displayed as shown in Figure 11-7.

Figure 11-7 Path Information Dialog Box for a Network Pseudowire



Step 3 Specify the destination using the information in Table 11-4.

Step 4 To limit the number of hops for the path trace, check the *Stop trace after* check box, and enter the maximum number of hops for the path trace.

The Cisco PathTracer window appears, displaying the resulting path trace.

Using an MPLS-TP Tunnel Endpoint

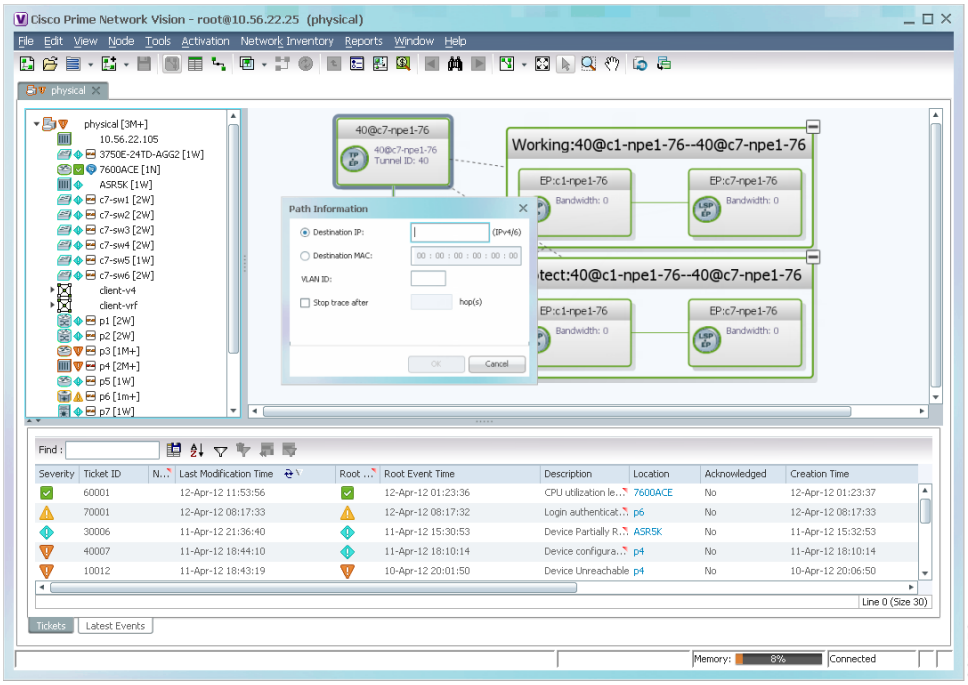
To launch a path trace from an MPLS-TP tunnel endpoint:

Step 1 In the navigation pane or map pane, expand the required MPLS-TP tunnel.

Step 2 Right-click the required MPLS-TP tunnel endpoint and choose **PathTracer > From Here to Destination**.

The Path Information dialog box is displayed as shown in Figure 11-8.

Figure 11-8 MPLS-TP Tunnel Endpoint Path Trace Launch



Step 3 Specify the destination using the information in Table 11-4.

Step 4 To limit the number of hops for the path trace, check the *Stop trace after* check box, and enter the maximum number of hops for the path trace.

The Cisco PathTracer window appears, displaying the resulting path trace.

Viewing Path Traces in Cisco PathTracer

The Cisco PathTracer window displays all discovered paths for the specified source and destination of the path trace, including the devices and physical links.

In addition, the Cisco PathTracer window enables you to:

- Zoom in and out on path traces by using your mouse scroll wheel.
- Apply one of four icon sizes to icons.
- View more or less information about the element by resizing the icon.
- Access common functions from the icons, such as attaching business tags or viewing properties.

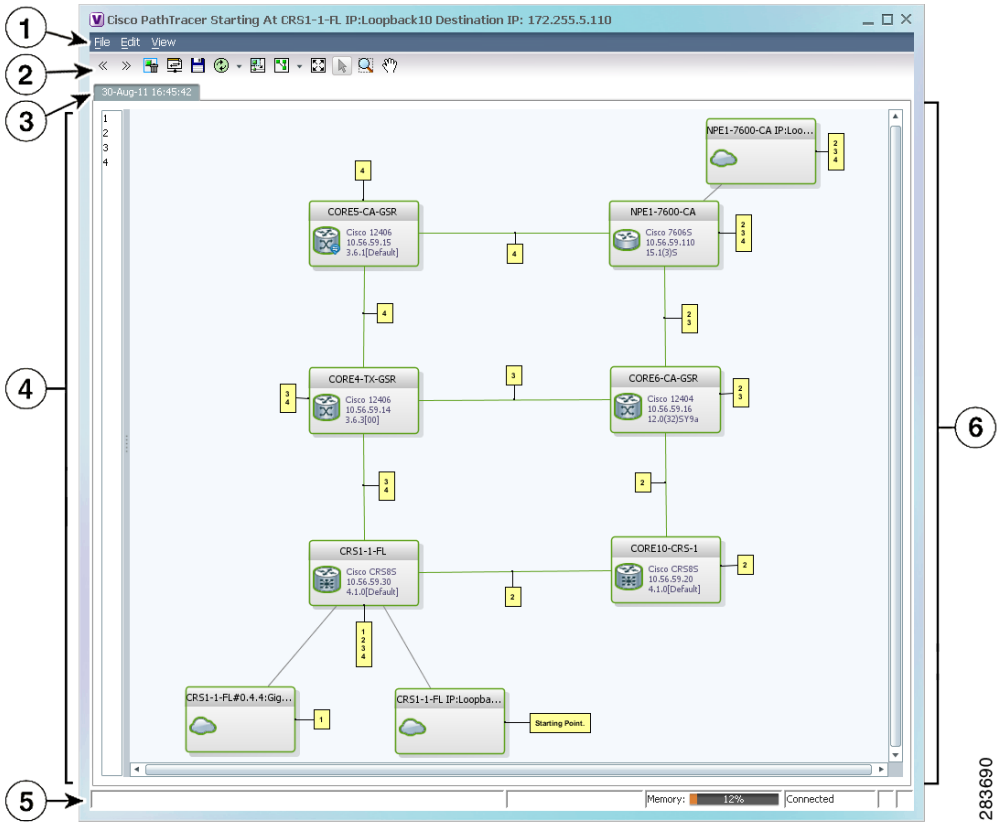
You can also right-click elements in the Cisco PathTracer window and choose options from a right-click menu. The right-click menu is context sensitive depending on the view and the item selected. For more information about the right-click menu and the available options, see Right-Click Menu Options, page 11-19.

The Cisco PathTracer window enables you to:

- View multiple paths for a selected source and destination either sequentially or simultaneously.
- View individual paths with networking layer details.
- Save a map with multiple paths to a file.
- Run Cisco PathTracer again, using the same trace or with a different limit number of hops.

Figure 11-9 shows an example of the Cisco PathTracer window with a multiple-path trace.

Figure 11-9 Cisco PathTracer Window - Multiple-Path Trace



1	Menu bar	**4**	Paths pane
2	Toolbar	**5**	Status bar
3	Trace tabs	**6**	Path trace pane

The Cisco PathTracer window contains the following components and options:

- Menus, page 11-16
- Toolbar, page 11-17
- Trace Tabs, page 11-18
- Paths Pane, page 11-18

- Path Trace Pane, page 11-18
- Right-Click Menu Options, page 11-19

Menus

Table 11-5 describes the options available in the Cisco PathTracer menus.

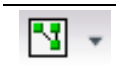
Table 11-5 Cisco PathTracer Window Menu Options

Option	Description
File Menu	
Run Again	Offers the following options for running Cisco PathTracer again for the same source and destination: • Change Hop Count—Enables you to enter a new hop count. • Repeat Last Trace—Runs the previous trace with the same settings. • Run Full Path Trace—Runs the previous trace without a hop count limit.
Save	Opens the Save dialog box so that you can save the current path trace to your local system in XML format.
Close	Closes the Cisco PathTracer window.
Edit Menu	
Select All	Selects all paths in the selected path trace pane.
View Menu	
Layout	Specifies how the elements are arranged in the path trace pane: circular, hierarchical, orthogonal, or symmetric.
Overview	Opens a window displaying an overview of the path trace.
Zoom In	Zooms in on the current path trace.
Zoom Out	Zooms out on the current path trace.
Fit in Window	Fits the entire path trace in the path trace pane.
Normal Select	Activates the normal selection mode.
Pan	Activates the pan mode, which enables you to move around in the path trace by clicking and dragging.
Zoom Selection	Enables you to zoom in on a specific area in the path trace.

Toolbar

Table 11-6 describes the options available in the Cisco PathTracer toolbar.

Table 11-6 Cisco PathTracer Toolbar Options

Button	Function
	Displays the previous path in the path trace pane.
	Displays the next path in the path trace pane.
	Clears the path selection made in the path trace pane.
	Opens the Cisco PathTracer details window. A map is displayed for the selected path, including network element details, links, and property information. For more information, see Viewing Path Trace Details, page 11-21.
	Saves the current multiple-path trace to an XML file on your local system. For more information, see Saving and Opening Cisco PathTracer Map Files, page 11-26.
	Offers the following options for running Cisco PathTracer again for the same source and destination: • Change Hop Count—Enables you to enter a new hop count. • Repeat Last Trace—Runs the previous trace with the same settings. • Run Full Path Trace—Runs the previous trace without a hop count limit. The new path trace map is displayed in the path trace pane. A new tab with the up-to-date (or refreshed) path map is created for each run, with each tab representing a run and the tab label indicating the snapshot time.
	Opens a window displaying a high level view of the path trace currently displayed in the path trace pane.
	Specifies how the elements are arranged in the path trace pane: circular, hierarchical, orthogonal, or symmetric.
	Fits the entire path trace in the path trace pane.
	Activates the normal selection mode. The button toggles when selected or deselected.
	Activates the zoom selection mode, which enables you to select a specific area in the path to zoom in on by clicking and dragging. The button toggles when selected or deselected.
	Activates the pan mode, which enables you to move around in the path trace by clicking and dragging. The button toggles when selected or deselected.

Trace Tabs

The discovered path trace is initially displayed in the path trace pane with a tab that displays the date and time when Prime Network started the path tracing process (snapshot time).

If you load a saved path from a file or run the displayed path trace again, the opened or refreshed path is displayed in a new tab with a refreshed path map for each run or file. When using a saved path from a file, the source and destination must be the same as the current display for it to appear in the same path trace window. Each tab represents a run or file, and its header displays the snapshot time.

Paths Pane

The paths pane lists all the paths discovered in the current path trace. A new path is created for each source and destination pair. The paths are identified by number, such as 1, 2, and 3.

If you launch a path trace with a specific hop count, the paths pane displays First *n* Hops where *n* is the number of hops specified.

Selecting a path in the paths pane highlights the selected path in the path trace pane. The paths that are not selected are dimmed in the map.

To view a different path, do either of the following:

- Choose a different path in the paths pane.
- Click **Select Previous Path** or **Select Next Path** in the toolbar.

To remove a path selection, click **Clear Path Selection** in the toolbar.

Path Trace Pane

The path trace pane displays the devices, links, and topological paths that are part of the path trace. All links and nodes in the path trace pane are labeled with their relevant path numbers, corresponding to the numbers in the paths pane. The starting point is labeled with a Starting Point callout. All other edge points are displayed as clouds.

The same coloring conventions that are used for links in the Prime Network content pane are used to display links in the Cisco PathTracer path trace pane.

Cisco PathTracer uses icons to display the network objects and their status. The status of a network object can be indicated on the topological map in the following ways:

- Severity
- Management state
- New alarms

For more information, see:

- Prime Network Vision Status Indicators, page 2-24
- Chapter 2, “Working with the Cisco Prime Network Vision Client”
- Map View, page 2-10

Right-Click Menu Options

You can right-click network elements in the path trace window and choose items from a right-click menu. The right-click menu is context sensitive depending on the view and the element selected.

Table 11-7 describes the right-click menu options that are available for elements selected in the Cisco PathTracer window.

Table 11-7 Cisco PathTracer Element Right-Click Menu Options

Option	Description
Inventory	Opens the inventory window for the selected element.
Aggregate	Groups the selected devices into an aggregation.
Disaggregate	Ungroups the devices in the selected aggregation. **Note** This option is available only when an aggregation is selected.
Poll Now	Polls the selected element.
Attach Business Tag	Attaches a business tag to the selected network element
Config Mgmnt	This option is available only if Prime Network Change and Configuration Management is installed. Displays the Configuration Management page for the selected device in Prime Network Change and Configuration Management.
Image Mgmnt	This option is available only if Prime Network Change and Configuration Management is installed. Displays the Configuration Management page for the selected device in Prime Network Change and Configuration Management.
Resize	Enables you to resize an object on the map by percentage or size.
Open Relevant Maps	Displays the Open Map dialog box so that you can view and open maps that contain the selected element.
Run Report	Enables you to run standard or user-defined events, inventory, and network service reports on demand.
Show Callouts/ Hide Callouts	Displays or hides callouts associated with the selected element.

Table 11-7 Cisco PathTracer Element Right-Click Menu Options (continued)

Option	Description
Tools	Contains the following choices: • CPU Usage—Displays memory and CPU usage information for a device or network element. • Ping—Pings the device from the client station. • Telnet—Communicates with the device using the Telnet window from the client station. **Note** If you use a Windows 7 system, you must enable the Windows Telnet Client before you can use the Prime Network Vision Telnet option. - For Windows 7 32-bit systems, enable the Windows Telnet Client to use the Prime Network Vision Telnet option. - For Windows 7 64-bit systems, a solution is available on the Cisco Developer Network at http://developer.cisco.com/web/ana/forums/-/message_boards/message/2780108.
Topology	Enables you to add: • A static link between two devices. • A static topology between a device and an unmanaged network. • A tunnel to a VPN.
Launch external applications	Starts an external application or tool that has been configured for access via the right-click menu. For more information, see the *Cisco Prime Network 3.9 Customization User Guide*.
Properties	Displays the properties of the selected item, such as the IP address and system name.
Commands	Launches available activation and configuration scripts. This can include the commands documented in Commands part of the *Cisco Prime Network 3.9 Reference Guide*, and those you create using Command Builder. For more information, see the *Cisco Prime Network 3.9 Customization User Guide*.
Management	Contains the following submenu options: • Command Builder—Defines commands and scripts using the Prime Network Command Builder tool (Configurator security level required). • Soft Properties Management—Extends VNEs by adding SNMP MIB or Telnet/SHH/TL-1 properties to the device's collected information model using the Prime Network Soft Properties Manager (Administrator security level required).
VNE Tools	Contains the following submenu options: • Poll Now—Updates the VNE information. • Stop VNE—Stops the VNE. • Start VNE—Starts the VNE.

Viewing Path Trace Details

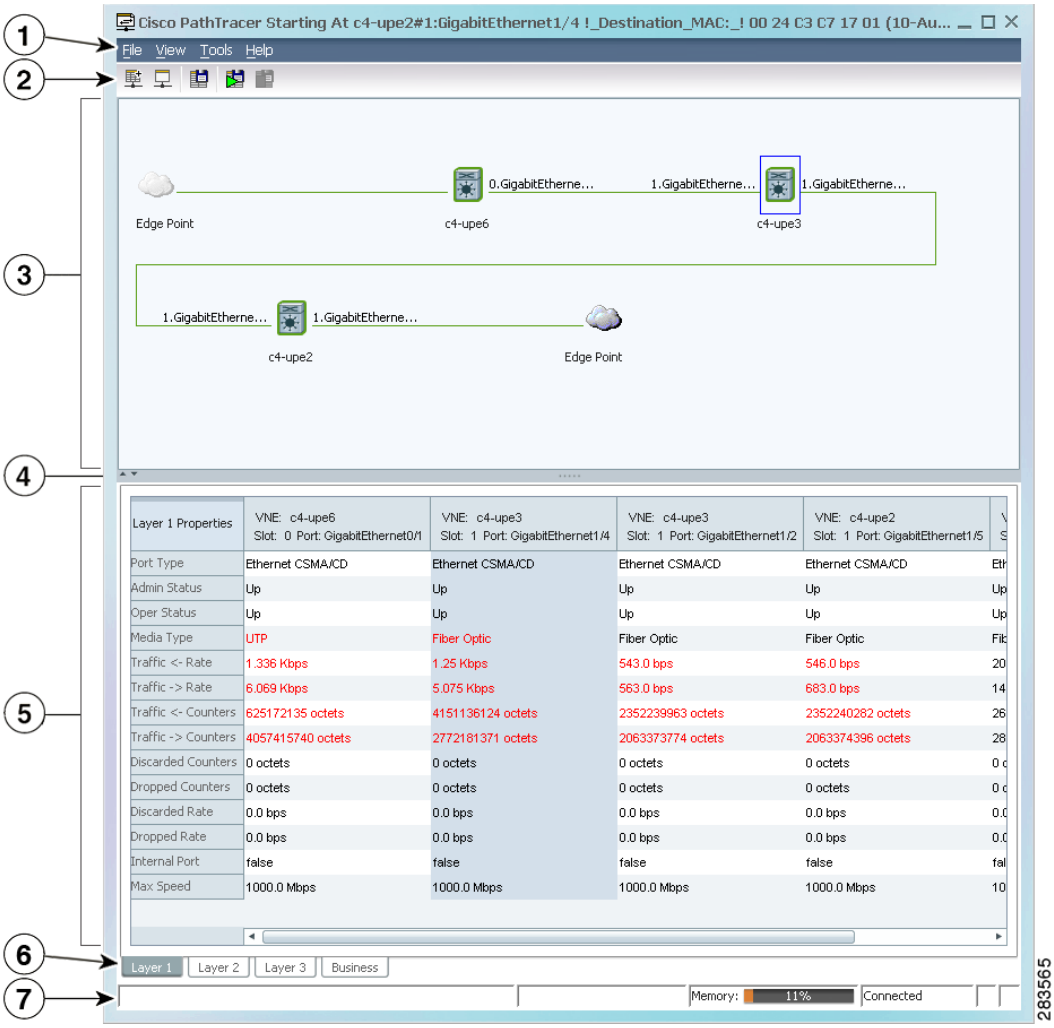
In addition to the information displayed in the Cisco PathTracer window, you can:

- View the following information for each network element:
  - The relevant parameters for each interface on all layers along the path.
  - For each layer, an indication of a mismatch between the parameters of the interfaces on both sides of a link.
  - Traffic statistics along the path.
- Monitor the status and traffic of all links along the path.
- View In and Out port properties.

To view this information, select the required path in the Cisco PathTracer window, and then click **PathTracer** in the toolbar. If you select multiple paths, a separate window is opened for each path.

Figure 11-10 shows an example of the Cisco PathTracer details window.

Figure 11-10 Cisco PathTracer Details Window



1	Menu bar	**5**	Details pane
2	Toolbar	**6**	Layer and Business tabs
3	Path trace pane	**7**	Status bar
4	Hide/display path trace pane		

The Cisco PathTracer details window contains the following components:

- Menus, page 11-22
- Cisco PathTracer Details Window Toolbar, page 11-23
- Path Trace Pane, page 11-23
- Details Pane, page 11-25

Menus

Table 11-8 describes the Cisco PathTracer details window menu options.

Table 11-8 Cisco PathTracer Details Window Menus

Option	Description
File Menu	
Close	Closes the Cisco PathTracer window.
View Menu	
Show All	Displays all the information in the tabs.
Hide All	Hides all the information in the tabs.
Tools Menu	
Export to File	Exports the currently displayed data to a CSV file.
Start Saving to File	Starts exporting the counter values of the path displayed in the Cisco PathTracer window to a CSV file.
Stop Saving to File	Stops exporting the counter values of the path displayed in the Cisco PathTracer window to a CSV file.
Help Menu	
Help Contents	Opens the online help for Cisco Prime Network Vision and Cisco Prime Network Events.
Help About	Displays the Cisco Prime Network Vision version and any additionally installed applications.

Cisco PathTracer Details Window Toolbar

Table 11-9 describes the tools that are available in the Cisco PathTracer details window toolbar.

Table 11-9 Cisco PathTracer Details Window Toolbar Options

Button	Name	Function
	Show All	Displays all the information in the tabs.
	Hide All	Hides all the information in the tabs.
	Export to File	Exports the currently displayed data to a CSV file.
	Start Saving to File	Starts exporting the counter values of the path displayed in the Cisco PathTracer window to a CSV file.
	Stop Saving to File	Stops exporting the counter values of the path displayed in the Cisco PathTracer window to a CSV file.

Path Trace Pane

The path trace pane in the Cisco PathTracer details window displays information related to the tab selected in the details pane. For example, if you choose the Layer 2 tab in the details pane, Layer 2 information is displayed in the path trace pane. Similarly, if you choose an element or link in the path trace pane, the related parameters are highlighted in the details pane.

By default, the path trace pane includes:

- Edge points
- Elements included in the path trace, including badges
- Links included in the path trace

Hovering your mouse over an element displays a tooltip that contains the element name, device type, and IP address. Hovering your mouse over the link to the right or left of the element displays the associated incoming or outgoing interface for that element and link.

Table 11-10 describes the right-click menu options that are available for elements in the path trace pane.

Table 11-10 Cisco PathTracer Element Right-Click Menu Options

Option	Description
Inventory	Opens the inventory window for the selected element.
Attach Business Tag	Attaches a business tag to the selected network element
Poll Now	Polls the selected element.
Config Mgmnt	This option is available only if Prime Network Change and Configuration Management is installed. Displays the Configuration Management page for the selected device in Prime Network Change and Configuration Management.
Image Mgmnt	This option is available only if Prime Network Change and Configuration Management is installed. Displays the Configuration Management page for the selected device in Prime Network Change and Configuration Management.
Run Report	Enables you to run standard or user-defined events, inventory, and network service reports on demand.
Tools	Contains the following choices: • CPU Usage—Displays memory and CPU usage information for a device or network element. • Ping—Pings the device from the client station. • Telnet—Communicates with the device using the Telnet window from the client station. **Note** If you use a Windows 7 system, you must enable the Windows Telnet Client before you can use the Prime Network Vision Telnet option. - For Windows 7 32-bit systems, enable the Windows Telnet Client to use the Prime Network Vision Telnet option. - For Windows 7 64-bit systems, a solution is available on the Cisco Developer Network at http://developer.cisco.com/web/ana/forums/-/message_boards/message/2780108.
Topology	Enables you to add: • A static link between two devices. • A static topology between a device and an unmanaged network. • A tunnel to a VPN.

Table 11-10 Cisco PathTracer Element Right-Click Menu Options (continued)

Option	Description
Launch external applications	Starts an external application or tool that has been configured for access via the right-click menu. For more information, see the *Cisco Prime Network 3.9 Customization User Guide*.
Properties	Displays the properties of the selected item, such as the IP address and system name.
Commands	Launches available activation and configuration scripts. This can include the commands documented in Commands part of the *Cisco Prime Network 3.9 Reference Guide*, and those you create using using Command Builder. For more information, see the *Cisco Prime Network 3.9 Customization User Guide*.
Management	Contains the following submenu options: • Command Builder—Defines commands and scripts using the Prime Network Command Builder tool (Configurator security level required). • Soft Properties Management—Extends VNEs by adding SNMP MIB or Telnet/SHH/TL-1 properties to the device's collected information model using the Prime Network Soft Properties Manager (Administrator security level required).
VNE Tools	Contains the following submenu options: • Poll Now—Updates the VNE information. • Stop VNE—Stops the VNE. • Start VNE—Starts the VNE.

Details Pane

Selecting a device or link in the path trace pane automatically highlights the related parameters in the details pane.

The details pane, with its Layer and Business tabs, displays the supported parameters of the selected element in a table, with the ingress and egress ports along the top and the parameters on the left.

Any inconsistencies between the two connected ports are colored to emphasize a discrepancy, such as different admin statuses.

The information parameters are arranged as follows:

- Layer *n* tabs—These tabs provide information about each network element, including ingress and egress port information. The information is either plain data that is extracted from the element or calculated data, such as rates or statistics. This information is displayed in the Layer 1, Layer 2, and Layer 3 tabs, as follows:
  - Layer 1—Displays the Layer 1 information in the selected path and enables you to view the link parameters. The name of each device is displayed, as well as the subslot, slot, and port details.
  - Layer 2—Displays the Layer 2 information in the selected path and enables you to view the link and connection parameters. For each device, the name and MAC address are displayed, as well as the VPI/VCI in an ATM link or the DLCI in a Frame Relay link. By default, the Cisco PathTracer details window is displayed with the Layer 2 tab active.
  - Layer 3—Displays the Layer 3 information in the selected path and enables you to view the link parameters. The name of each device is displayed.

  If a field has no value on any of the interfaces, the field is not displayed in the table. For example, if none of the interfaces is configured for MTU, the MTU row is not displayed in the table. If at least one of the interfaces is configured for MTU, the MTU row is displayed.
- Business tab—This tab provides the name and key of business tags that are attached to the network entities displayed, including ports, devices (physical entities), VCIs, VPIs, DLCIs, contexts (logical entities), or MPLS. This information is displayed in the Business Tag area.

Saving and Opening Cisco PathTracer Map Files

Prime Network enables you to export multiple-path trace maps that are displayed in the Cisco PathTracer window to an XML file. You can view the data later to assess whether anything has changed.

Saving Cisco PathTracer Map Files

To save Cisco PathTracer map files:

Step 1 Open the Cisco PathTracer window as described in Launching Path Traces, page 11-3.

Step 2 Click **Save MultiPath** in the toolbar.

Step 3 In the Save dialog box, navigate to the directory where you want to save the file and enter a name for the map file.

Step 4 Click **Save**. The map file is saved in the selected directory.

Opening Cisco PathTracer Map Files

Prime Network enables you to open saved XML-formatted path-tracing maps.

The following conditions apply when working with multiple-path trace files:

- When you load a multiple-path trace file, Prime Network queries the file (not the network), and loads the persisted information.
- If you load a multiple-path trace file that does not contain the same start and end points, the map is automatically opened in a new Cisco PathTracer window.

To open Cisco PathTracer map files:

Step 1 In Cisco Prime Network Vision, choose **File > Load MultiPath** from the main menu. The Open dialog box is displayed.

Step 2 Navigate to the directory of the saved file and select the file.

Step 3 Click **Open**. The previously saved map is displayed in the Cisco PathTracer window.

Saving Cisco PathTracer Counter Values

Prime Network enables you to export, over a period of time, the counter values of the path displayed in the Cisco PathTracer window to a CSV file. The data can then be viewed later, as required.

Note This topic applies to the Cisco PathTracer details window only.

To save Cisco PathTracer counter values that are generated over a period of time:

Step 1 Open the Cisco PathTracer details window as described in Viewing Path Trace Details, page 11-21.

Step 2 Click **Start Saving to File** in the toolbar.

Step 3 In the Export Table to File dialog box, navigate to the directory where you want to save the Cisco PathTracer counter values.

Step 4 In the File name field, enter a name for the file in which to save the counter values.

Step 5 Click **Save**. Cisco PathTracer starts saving the counter values to the specified file.

Step 6 To stop exporting counter values to the file, click **Stop Saving to File** in the toolbar.

Cisco PathTracer stops exporting the counter values to the file.

Rerunning a Path and Comparing Results

If you save a path to a file (see Saving and Opening Cisco PathTracer Map Files, page 11-26), you can use the file to rerun the same path automatically with the same source and destination. You can also compare the saved path to a newly run path to determine if the path has changed or to assess a problem.

To rerun a saved path:

Step 1 Load the required map file as described in Saving and Opening Cisco PathTracer Map Files, page 11-26. The Cisco PathTracer window is displayed with the previously saved map file.

Step 2 Click **Run Again** in the toolbar.

The path trace runs automatically using the same source and destination as the loaded map file, and a new tab is displayed in the Cisco PathTracer window with the updated map. The tab displays the date and time when the path was rerun.

Step 3 Compare the previous map to the updated one by switching between the tabs in the Cisco PathTracer window.

Note

- If you load a Cisco PathTracer map file that does not contain the same source and destination information as the map that is currently displayed in the window, the map is automatically opened in a new Cisco PathTracer window.
- If you load a Cisco PathTracer map file that contains the same source and destination information as a map that is currently displayed in the window, the map is loaded in a new tab in the same window.

Viewing Q-in-Q Path Information

The Q-in-Q (IEEE 802.1) tagging technology (also known as Dot1q tunneling) allows the nesting of another VLAN tag in a packet, in addition to an existing one. Either VLAN tag is considered an 802.1Q header.

Cisco PathTracer uses the VLAN tags of the Ethernet header and the port configuration to trace the path from one interface to another over the network. Among other things, you can:

- View a Layer 2 path across a LAN domain with all the VLAN tag information.
- For each network element, view the relevant parameters for each interface on all layers along the path.

Q-in-Q and Dot1q information is displayed in the Cisco PathTracer window when a path is traced over Ethernet ports with Dot1q and a Q-in-Q configuration.

As described in Launching Path Traces, page 11-3, to view a specific path, you must specify an initial start point, such as an IP interface, and then an endpoint, such as a destination IP address.

To trace a Q-in-Q path, you start the path from any:

- Router or switch that is part of the Ethernet domain with Dot1q and Q-in-Q configurations.
- IP destination that can be reached from that point of the network.

After you select the endpoint, the Cisco PathTracer window is displayed. From this window, you can open the Cisco PathTracer details window, with the appropriate Q-in-Q information displayed in the Layer 2 tab.

The Layer 2 tab can display the following information specific to Q-in-Q and VLAN port configurations:

- VLAN Mode—The work mode for the interface: Unknown, Access, Trunk, or Dot1Q Tunnel. Trunk mode also refers to multiple tagging.
- Native VLAN ID—The VLAN identifier that is used to tag untagged traffic received on a trunked interface:
  - If VLAN tagging is enabled, the default native VLAN identifier is 1.
  - If VLAN tagging is disabled, the native VLAN identifier is 0 (zero) or “no VLAN ID.”
- CE VLAN ID—The customer edge device VLAN identifier.
- SP VLAN ID—The service provider VLAN identifier.

Viewing L2TP Path Information

Cisco PathTracer uses VC ID encapsulation information to trace the path from one tunnel interface to another over the network. The Cisco PathTracer tool enables you to:

- View a path for the defined Layer 2 Tunneling Protocol (L2TP) session across the network.
- For each network element, view the relevant parameters for each interface on all layers along the path.

The Layer 3 tab displays the peer name for L2TP tunnels.

Table 11-11 describes the information that is displayed in the Layer 2 tab for L2TP tunnels.

Table 11-11 Layer 2 Tab Information for L2TP Tunnels

Field	Description
Encapsulation Type	Encapsulation type, such as Point-to-Point Protocol over ATM (PPPoA).
Binding Information	Name of the subscriber.
Binding Status	Binding status: bound or unbound.
Tunnel Session Count	Number of current sessions.
Tunnel Remote ID	Remote tunnel identifier.
Tunnel ID	Local tunnel identifier.
Tunnel Name	Name of the subscriber and the tunnel identifier.
Session ID	Session identifier.
Traffic > L2TPSessionCounters	Number of traffic packets passing through the L2TP tunnel.
Traffic < L2TPSessionCounters	Number of traffic packets passing through the L2TP tunnel.
Tunnel Ctl Errors	Number of control errors.
Tunnel State	Tunnel state: unknown, idle, connecting, established, or disconnecting.
Session Type	Session type: unknown, LAC, or LNS.
Peer Name	Peer name.
Tunnel Remote IP	Remote IP address of the tunnel.
Last Error Code	Value of the last error code that caused the tunnel disconnection.
Session State	Session state: unknown, idle, connecting, established, or disconnecting.
Remote Session ID	Remote session identifier.

Using Cisco PathTracer in MPLS Networks

You can open and view Cisco PathTracer information between service endpoints, such as an IP interface that is attached to the VRF over an MPLS network. The LSP in the MPLS network is found according to the cross-connect table of each router.

Note An LSP can be traced and displayed by Cisco PathTracer as part of an end-to-end tracing of a service; for example, when viewing a path between one CE device and another. Cisco PathTracer traces the path that goes over circuits or VLANs in the access networks. It also traces the LSPs between the VRFs going through all intermediate devices such as CE devices, aggregation switches, PE routers, and core routers.

To view a specific path, you must specify an initial starting point, such as an IP interface; specifying a destination IP address is optional. If the traced path (for example, a VC or VLAN) ends in a router, Cisco PathTracer finds the next hop according to the destination IP address. If you select an endpoint, Cisco PathTracer extracts the relevant IP address from this point and uses it as the destination.

The following topics provide more information on using Cisco PathTracer in MPLS networks:

- Cisco PathTracer MPLS Start and Endpoints, page 11-30
- Using Cisco PathTracer for CSC Configurations, page 11-31
- Using Cisco PathTracer for Layer 3 VPNs, page 11-32
- Using Cisco PathTracer for Layer 2 VPNs, page 11-33
- Using Cisco PathTracer for MPLS TE Tunnels, page 11-34

Cisco PathTracer MPLS Start and Endpoints

You can open Cisco PathTracer by right-clicking a starting point and entering the required destination IP address. Table 11-12 lists the Cisco PathTracer starting points.

Table 11-12 Cisco PathTracer MPLS Starting Points

Element	Location	Start Options
IP interface	• Inventory window • Affected entity (enabled only if the affected entity has an IP interface)	• From Here to Destination • Start Here
MPLS-TP tunnel endpoint	• Navigation or map pane • Inventory window	• From Here to Destination • Start Here
Site	Service view map	• From Here to Destination • To Subnet Destination • Start Here
Business tag attached to the VPI/VCI or IP interface	The path can be found using a business tag, which is attached to the VPI/VCI or IP interface by entering its key. It can then be opened from the Find Business Tag window.	From Here to Destination
Layer 2 MPLS Tunnel	Inventory window	From Here to Destination

If you choose the Start Here option, Table 11-13 lists the endpoints that can be selected as path destinations.

Table 11-13 Cisco PathTracer MPLS Endpoints

Element	Location	End Options
IP interface	• Inventory window • Affected entity (enabled only if the affected entity has an IP interface)	End Here
MPLS-TP tunnel endpoint	Inventory window	End Here
Site	Service view map	End Here

The Cisco PathTracer window is displayed. From this window you can open the Cisco PathTracer details window with the VPN information displayed in the Layer 2 and Layer 3 tabs.

Note If multiple paths are selected in the paths pane, or if nothing is selected in the paths pane, all available paths are opened automatically, and each is displayed in a separate Cisco PathTracer window.

Using Cisco PathTracer for CSC Configurations

Cisco PathTracer traces a CSC flow from the customer CE through the customer carrier VPN, across the customer backbone carrier VPN, back to the customer carrier VPN, and to the destination CE.

To launch a path trace for a CSC configuration:

Step 1 In a map, double-click the required CE device.

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

Step 3 In the IP Interfaces table, right-click the required interface and choose **PathTracer > Start Here >** *IPvn* where *IPvn* represents IPv4 or IPv6.

Step 4 Navigate to the destination CE device and double-click it.

Step 5 In the inventory window, choose **Logical Inventory > Routing Entities > Routing Entity**.

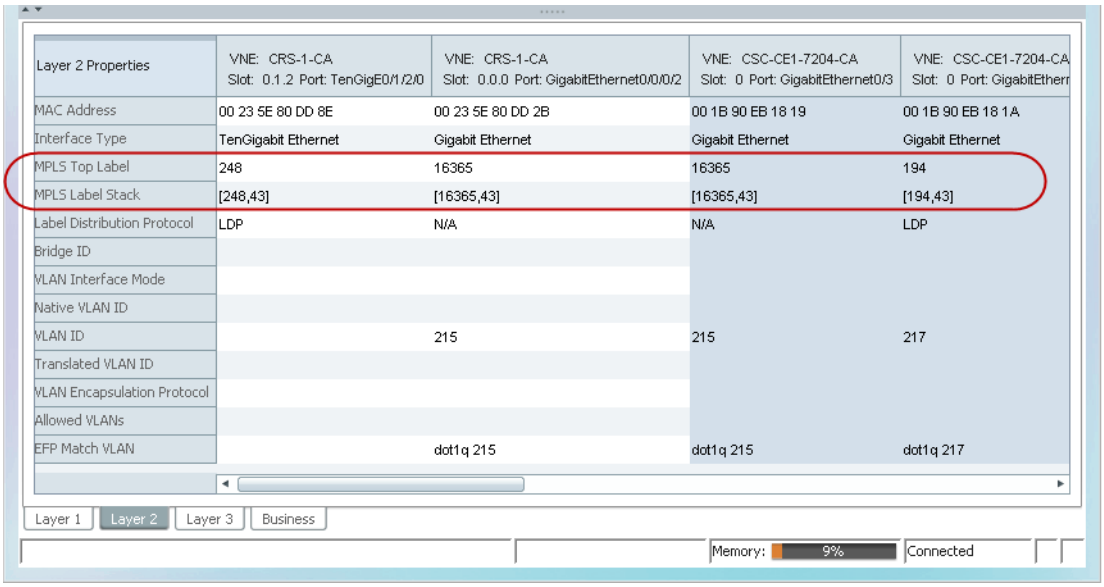
Step 6 In the IP Interfaces table, right-click the required interface and choose **PathTracer > End Here**.

The path trace is displayed in the Cisco PathTracer window.

Step 7 To view the detailed pane, click Cisco PathTracer in the toolbar.

The Layer 2 tab displays a single outer label and two inner labels for each interface, reflecting the CSC configuration. (See Figure 11-11.)

Figure 11-11 CSC Configuration Path Trace



Using Cisco PathTracer for Layer 3 VPNs

Cisco PathTracer uses VRF routing and label switching information to trace the path from one VRF interface to another. If you choose a launch point and destination from the right-click menu, you can open the Cisco PathTracer for Layer 3 VPNs. The Cisco PathTracer window shows the VPN topology map. From this window, you can open the Cisco PathTracer details window with the appropriate VPN information displayed in the Layer 2 and Layer 3 tabs.

For Layer 3 path information, Prime Network uses VRF routing and label switching information to trace the path from one VRF interface to another. Layer 3 path trace information is displayed in the Cisco PathTracer window when the path goes over connections and ends in VRFs.

If a VRF table includes more than one path toward a destination, Cisco PathTracer shows all paths.

To view Layer 3 path information, choose the **Layer 3** tab and choose **Show All** from the View menu. The path information is displayed in the active tab.

The table displays the Layer 3 VPN information on the device that has a VRF. The following Layer 3 properties displayed in the Layer 3 tab relate specifically to VPNs:

- Name—The name of the site. For example, ATM4/0.100(10.0.0.1) is a combination of the interface name and IP address used to reach the site. Each site belongs to a particular VPN, so the address must be unique within the VPN.
- IP Address—The IP address of the interface.
- Mask—The mask of the specific network.
- State—The state of the interface (up or down).
- VRF Name—The name of the VRF.

Cisco PathTracer does not display or trace EXP bits for Layer 3 VPNs that use policy-based tunnel selection (PBTS).

Using Cisco PathTracer for Layer 2 VPNs

Cisco PathTracer uses VC ID and label switching information to trace the path from one tunnel interface to another over the MPLS network.

Cisco PathTracer also covers end-to-end Layer 2 VPN service paths from one CE router to another. The path goes over circuits (such as a VC) or VLANs in access networks and over LSP between the Layer 2 tunnel edge.

The Cisco PathTracer window shows the VPN topology map for the relevant devices and links. From this window, you can open the Cisco PathTracer details window with the appropriate VPN information displayed in the Layer 2 and Layer 3 tabs.

For Layer 2 path information, Cisco PathTracer uses VC ID and label switching information to trace the path from one tunnel interface to another. Layer 2 path trace information is displayed in the Cisco PathTracer window when the path goes over pseudowire tunnels.

To view Layer 2 path information, choose the **Layer 2** tab and then **View > Show All**. The path information is displayed in the active tab.

Table 11-14 describes the Layer 2 properties that can be displayed in the Layer 2 tab specifically for VPNs.

Table 11-14 Cisco PathTracer Layer 2 Properties for VPNs

Field	Description
Top Label	Details of the outer MPLS label.
Label Stack	Details of the inner MPLS label.
MAC Address	MAC address.
Tunnel ID	Tunnel identifier. The identifier and the router IP address of the two tunnel edges identify the pseudowire tunnel.
Tunnel Type	Tunnel type: • 0—Unknown • 1—PWE3 • 2—TE
Tunnel Status	Operational state of the tunnel: Up or Down.
Tunnel Local VC Label	MPLS label that is used by the router to identify or access the tunnel. It is inserted in the MPLS label stack by the local router.
Tunnel Peer VC Label	MPLS label that is used by the router to identify or access the tunnel. It is inserted in the MPLS label stack by the peer router.
Tunnel Local Router IP	IP address of the tunnel edge, which is used as the MPLS router identifier.
Tunnel Peer Router IP	IP address of the peer tunnel edge, which is used as the MPLS router identifier.
Distribution Protocol Type	Protocol used by MPLS to build the tunnel, such as LDP or TDP.
Peer OID	Tunnel identifier and device name.

Using Cisco PathTracer for MPLS TE Tunnels

Cisco PathTracer uses label switching information to trace the end-to-end path of a TE tunnel path from one PE router to another.

Using MPLS TE technology, Cisco PathTracer enables you to:

- View a path or list of devices.
- View the following information for each network element:
  - The relevant parameters for each interface on all layers along the path.
  - The path for the defined MPLS TE-LSP across the network.

The Cisco PathTracer window is displayed showing the MPLS TE tunnel topology map. From this window, you can open the Cisco PathTracer details window with the appropriate MPLS TE tunnel information displayed in the Layer 2 tab.

Note Cisco PathTracer does not display or trace EXP bits for Layer 3 VPNs that use PBTS.

Layer 2 and Layer 3 path trace information is displayed in the Cisco PathTracer details window when a path is traced over MPLS TE tunnels. To view Layer 2 path information, choose the **Layer 2** tab and then **View > Show All**. The path information is displayed in the active tab.

Table 11-15 describes the Layer 2 properties that can be displayed in the Layer 2 tab specifically for MPLS TE tunnels.

Table 11-15 Cisco PathTracer Layer 2 Properties for MPLS TE Tunnels

Field	Description
MPLS TE Properties	MPLS TE data set in an MPLS interface, primarily bandwidth allocation levels and signaling protocol.
Tunnel Oper Status	Operational status of the tunnel: Up or Down. If this value is Up, the Tunnel Admin Status must also be Up. See Tunnel Admin Status properties for additional information.
Tunnel Bandwidth Kbps	Configured bandwidth (in Kb/s) for the tunnel.
Tunnel Description	Description of the tunnel.
Tunnel Name	Interface name.
Tunnel Admin Status	Administrative status of the tunnel (Up or Down) with the following caveats: • If the Tunnel Oper Status value is Up, the Tunnel Admin Status value must also be Up. • If the Tunnel Admin Status value is Down, the Tunnel Oper Status value must also be Down.
Tunnel Lockdown	Whether or not the tunnel can be rerouted: • Enabled—The tunnel cannot be rerouted. • Disabled—The tunnel can be rerouted.
Tunnel LSP ID	LSP identifier.

Table 11-15 Cisco PathTracer Layer 2 Properties for MPLS TE Tunnels (continued)

Field	Description
Tunnel Auto Route	Whether or not destinations behind the tunnel are routed through the tunnel: Enabled or disabled.
Tunnel Hold Priority	Tunnel priority after path setup.
Tunnel Setup Priority	Tunnel priority upon path setup.
Tunnel Path Option	Tunnel path option: • Dynamic—The tunnel is routed along the ordinary routing decisions after taking into account the tunnel constraints such as attributes, priority, and bandwidth. • Explicit—The route is explicitly mapped with the included and excluded links.
Tunnel Out Label	TE tunnel MPLS label distinguishing the LSP selection in the adjacent device.
Tunnel Affinity	Tunnel's preferential bits for specific links.
Tunnel Destination Address	IP address of the device in which the tunnel ends.
Tunnel Peak Rate Kbps	Peak flow specification (in Kb/s) for this tunnel.
Tunnel Out Interface	Interface through which the tunnel exits the device.
Tunnel Burst Kbps	Burst flow specification (in Kb/s) for this tunnel.
Tunnel Average Rate Kbps	Tunnel average rate in Kb/s.
Tunnel Affinity Mask	Tunnel affinity bits that should be compared to the link attribute bits.



CHAPTER 12

Monitoring Carrier Ethernet Services

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

- User Roles Required to Work with Carrier Ethernet Services, page 12-2
- Viewing CDP Properties, page 12-6
- Viewing Link Layer Discovery Protocol Properties, page 12-8
- Viewing Spanning Tree Properties, page 12-10
- Viewing Resilient Ethernet Protocol Properties, page 12-14
- Viewing Access Gateway Properties, page 12-18
- Working with Ethernet Link Aggregation Groups, page 12-21
- Viewing mLACP Properties, page 12-27
- Viewing Provider Backbone Bridge Properties, page 12-30
- Viewing EFP Properties, page 12-31
- Understanding EFP Severity and Ticket Badges, page 12-36
- Viewing EVC Service Properties, page 12-37
- Viewing and Renaming Ethernet Flow Domains, page 12-39
- Working with VLANs and VLAN Overlays, page 12-42
- Understanding Unassociated Bridges, page 12-70
- Working with Ethernet Flow Point Cross-Connects, page 12-72
- Working with VPLS and H-VPLS Instances, page 12-75
- Working with Pseudowires, page 12-88
- Working with Ethernet Services, page 12-101
- Viewing IP SLA Responder Service Properties, page 12-108
- Viewing IS-IS Properties, page 12-110
- Viewing OSPF Properties, page 12-113

User Roles Required to Work with Carrier Ethernet Services

This topic identifies the roles that are required to work with to Carrier Ethernet services in Prime Network Vision. Prime Network determines whether you are authorized to perform a task as follows:

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

For more information on user authorization, see the *Cisco Prime Network 3.9 Administrator Guide*.

The following tables identify the tasks that you can perform:

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

By default, users with the Administrator role have access to all managed elements. To change the Administrator user scope, see the topic on device scopes in the *Cisco Prime Network 3.9 Administrator Guide*.

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

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

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

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View EVC service properties	—	—	—	—	X
View IP SLA responder service properties	—	—	—	—	X
View IS-IS properties	—	—	—	—	X
View Link Layer Discovery Protocol (LLDP) properties	—	—	—	—	X
View mLACP properties	—	—	—	—	X
View OSPF properties	—	—	—	—	X
View Provider Backbone Bridge (PBB) properties	—	—	—	—	X
View pseudowire properties	Partial[1]	Partial[1]	Partial[1]	Partial[1]	X
View pseudowire redundancy service properties	Partial[2]	Partial[2]	Partial[2]	Partial[2]	
View REP properties	—	—	—	—	X
View REP properties for VLAN service links	—	—	—	—	X
View STP properties	—	—	—	—	X
View STP properties for VLAN service links	—	—	—	—	X
View virtual service instance properties	—	—	—	—	X
View VLAN bridge properties	—	—	—	—	X
View VLAN links between VLAN elements and devices	Partial[3]	Partial[3]	Partial[3]	Partial[3]	X
View VLAN mappings	—	—	—	—	X
View VLAN service link properties	—	—	—	—	X
View VLAN trunk group properties	—	—	—	—	X
View VPLS access EFP properties	—	—	—	—	X
View VPLS core or access pseudowire endpoint properties	—	—	—	—	X
View VPLS instance properties	X	X	X	X	X
Working with Overlays					
Apply overlays	X	X	X	X	X
Display or hide overlays	X	X	X	X	X
Remove overlays	X	X	X	X	X
View pseudowire tunnel links in VPLS overlays	—	—	—	—	X

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

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View REP information in VLAN domain views and VLAN overlays	—	—	—	—	X
View STP information in VLAN domain views and VLAN overlays	—	—	—	—	X
Other Tasks					
Display pseudowire information	—	—	—	—	X
Ping a pseudowire	—	—	—	—	X
Remove VLANs from a map	—	—	X	X	X
Rename Ethernet flow domains	X	X	X	X	X

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

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

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

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

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View EVC service properties	X	X	X	X	X
View IP SLA responder service properties	X	X	X	X	X
View IS-IS properties	X	X	X	X	X
View Link Layer Discovery Protocol (LLDP) properties	X	X	X	X	X
View mLACP properties	X	X	X	X	X
View OSPF properties	X	X	X	X	X
View Provider Backbone Bridge (PBB) properties	X	X	X	X	X
View pseudowire properties	X	X	X	X	X
View pseudowire redundancy service properties	X	X	X	X	X
View REP properties	X	X	X	X	X
View REP properties for VLAN service links	X	X	X	X	X
View STP properties	X	X	X	X	X
View STP properties for VLAN service links	X	X	X	X	X
View VLAN bridge properties	X	X	X	X	X
View VLAN links between VLAN elements and devices	X	X	X	X	X
View VLAN mappings	X	X	X	X	X
View VLAN service link properties	X	X	X	X	X
View VLAN trunk group properties	X	X	X	X	X
View VPLS access EFP properties	X	X	X	X	X
View VPLS core or access pseudowire endpoint properties	X	X	X	X	X
View VPLS instance properties	X	X	X	X	X
View VSI properties	X	X	X	X	X

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

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

Viewing CDP Properties

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

In Logical Inventory

To view CDP properties:

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

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

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

Figure 12-1 CDP in Logical Inventory

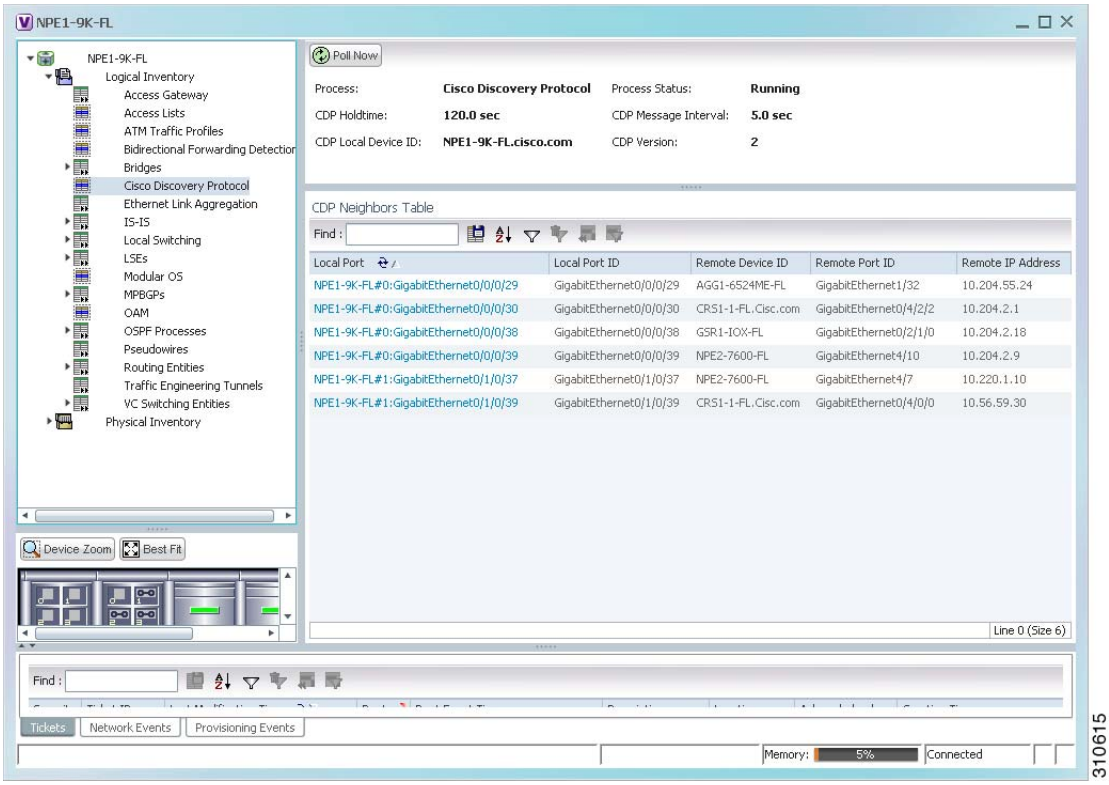


Table 12-3 describes the CDP instance properties that are displayed.

Table 12-3 CDP Properties in Logical Inventory

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

In Physical Inventory

To view CDP on a Layer 2 port:

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

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

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

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

Viewing Link Layer Discovery Protocol Properties

LLDP stores and maintains the local device information, including a list of devices directly connected to the device.

In Logical Inventory

To view LLDP properties:

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

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

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

Figure 12-2 LLDP in Logical Inventory

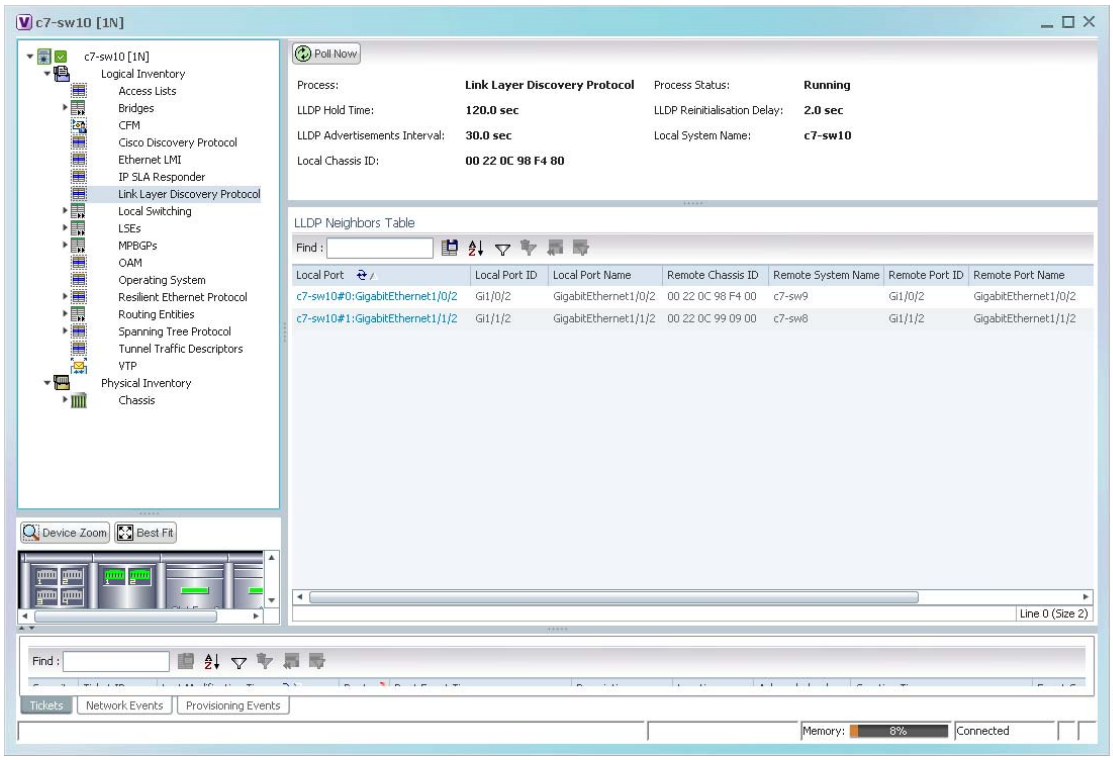


Table 12-4 describes the properties that are displayed for LLDP.

Table 12-4 Link Layer Discovery Protocol Properties

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

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

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

In Physical Inventory

To view LLDP on a Layer 2 port:

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

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

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

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

Viewing Spanning Tree Properties

STP is a link management protocol that provides path redundancy while preventing undesirable loops in the network.

To view Spanning Tree properties:

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

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

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

Figure 12-3 STP in Logical Inventory

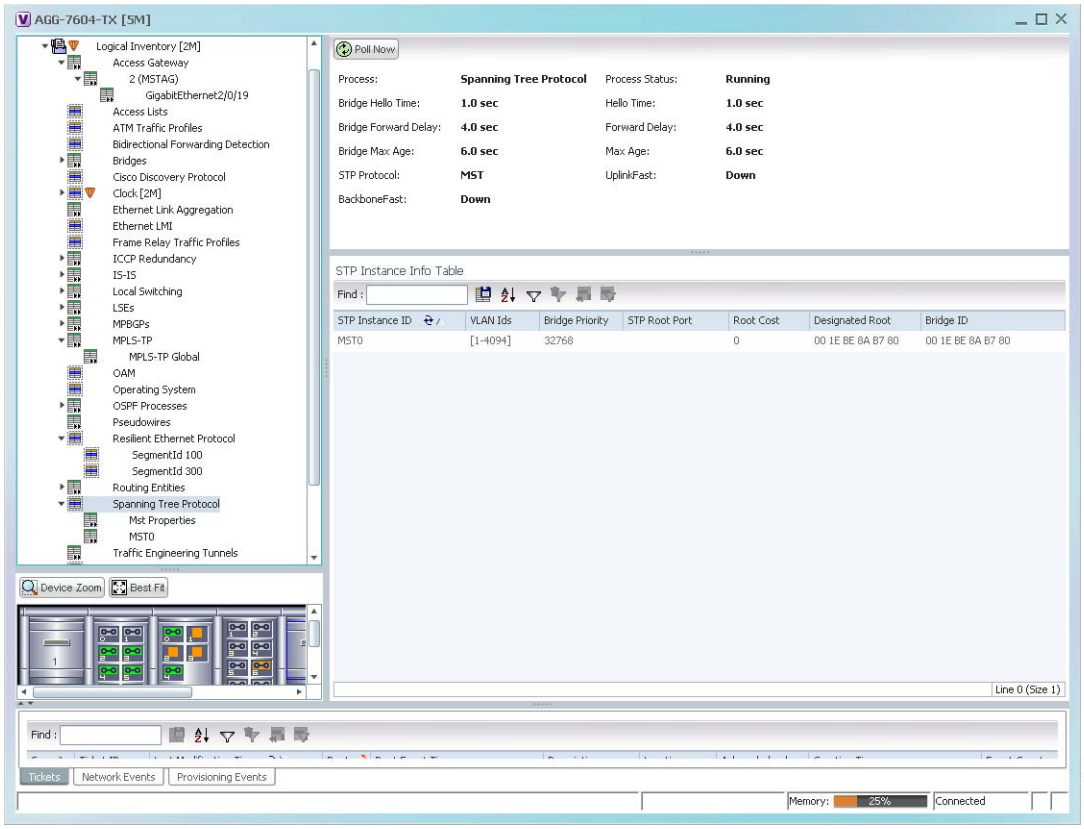


Table 12-5 describes the properties that are displayed for STP.

Table 12-5 STP Properties

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

Table 12-5 STP Properties (continued)

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

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

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

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

Table 12-6 STP Instance Information Properties

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

Table 12-6 STP Instance Information Properties (continued)

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

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

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

Table 12-7 MSTP Properties in Logical Inventory

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

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

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

Viewing Resilient Ethernet Protocol Properties

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.

To view REP properties in logical inventory:

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

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

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

Figure 12-4 REP in Logical Inventory

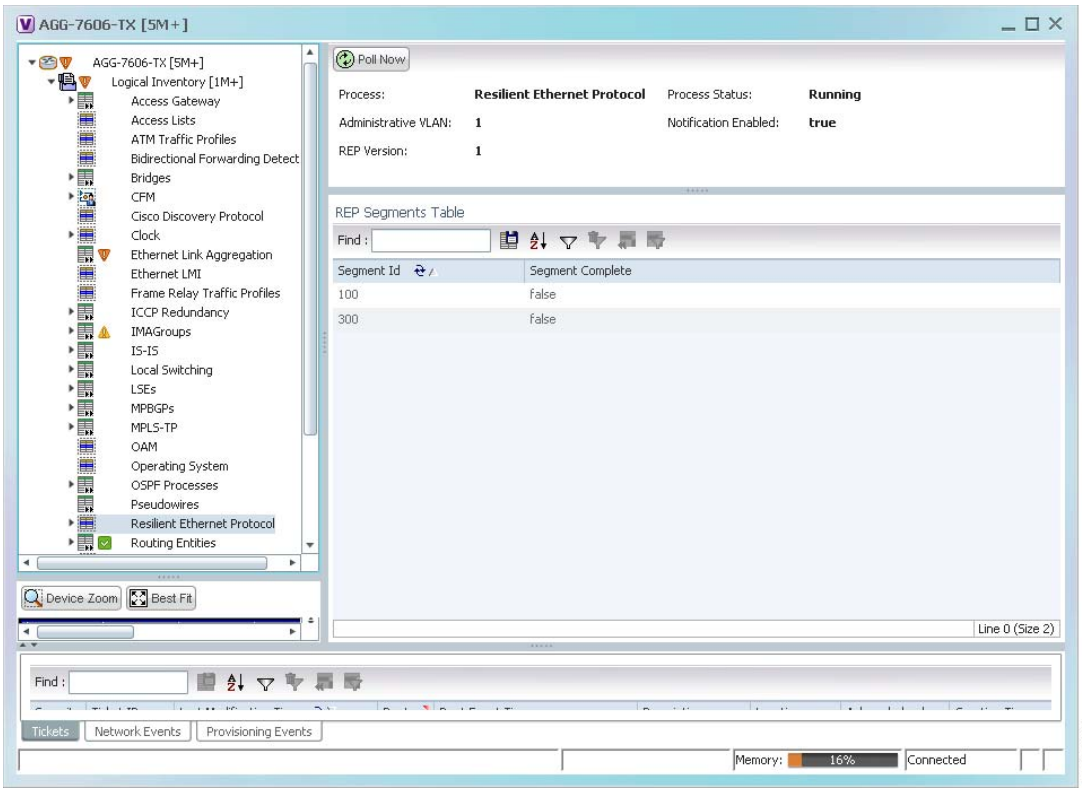


Table 12-8 describes the information that is displayed for REP.

Table 12-8 REP Properties

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

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

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

Figure 12-5 REP Segment Properties

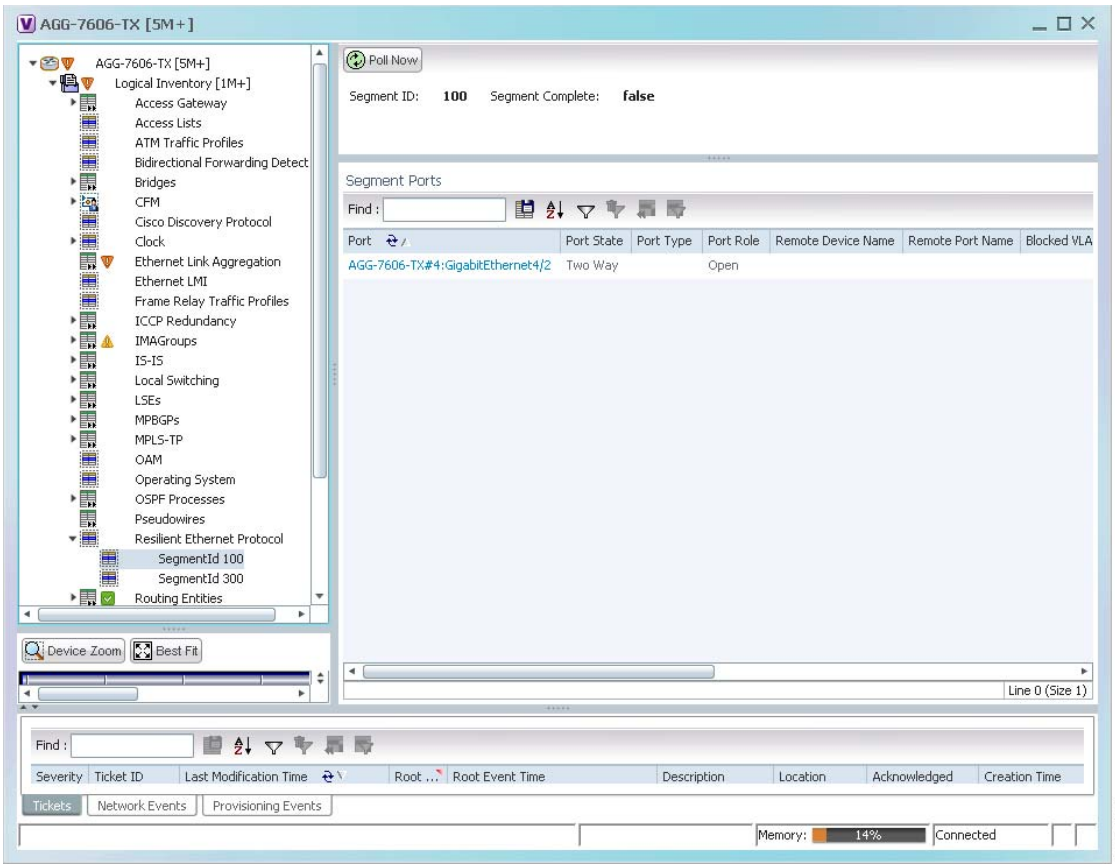


Table 12-9 describes the information that is displayed for REP segments.

Table 12-9 REP Segment Properties

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

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

- VLAN domain views and overlays—See Viewing REP Information in VLAN Domain Views and VLAN Overlays, page 12-60.
- VLAN service link properties—See Viewing REP Properties for VLAN Service Links, page 12-61.

Viewing Access Gateway Properties

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

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

To view access gateway properties:

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

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

Figure 12-6 shows an example of an access gateway entry in logical inventory.

Figure 12-6 Access Gateway in Logical Inventory

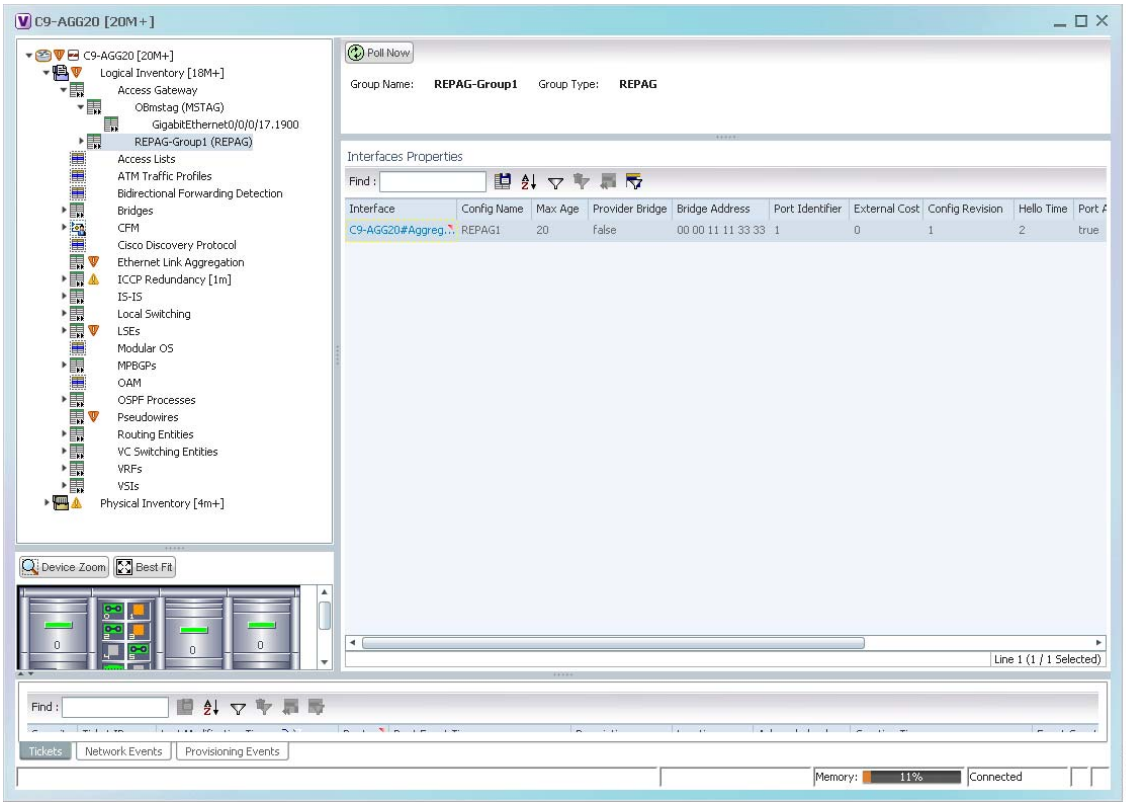


Table 12-10 describes the information that is displayed for an access gateway.

Table 12-10 Access Gateway Properties in Logical Inventory

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

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

Figure 12-7 shows an example of the information displayed for an access gateway instance.

Figure 12-7 Access Gateway Instance in Logical Inventory

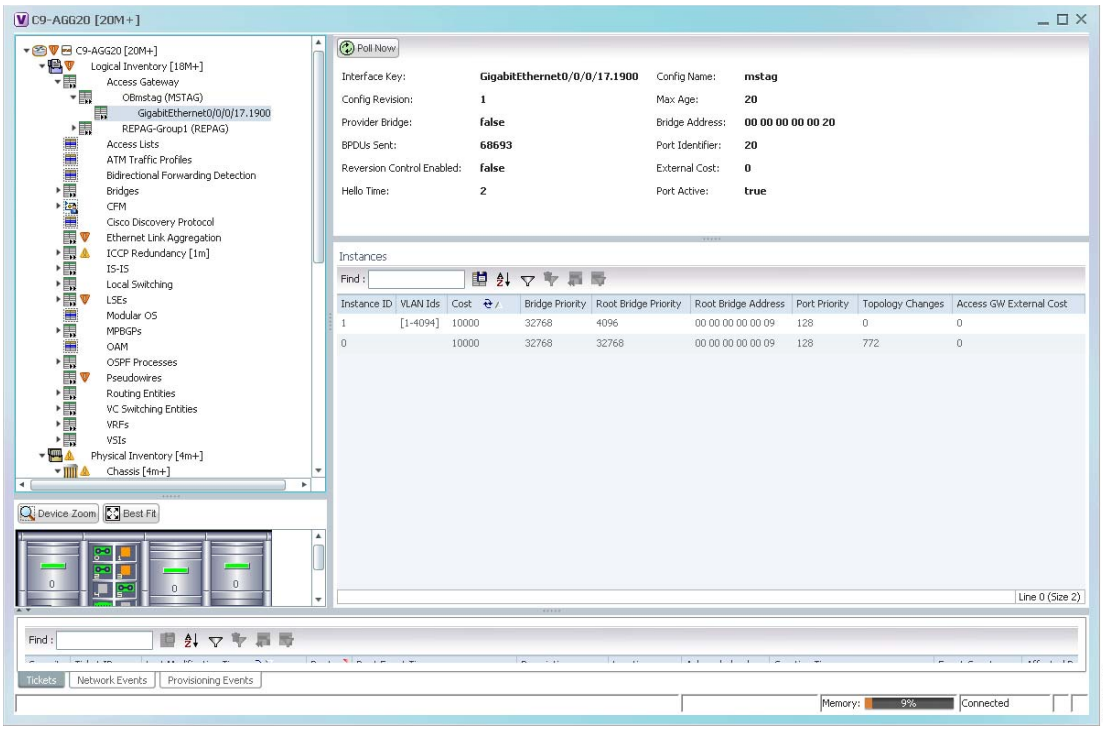


Table 12-11 describes the information that is displayed for an access gateway instance.

Table 12-11 Access Gateway Instance Properties

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

Table 12-11 Access Gateway Instance Properties (continued)

Field	Description
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 IDs	VLAN identifiers.
Cost	Path cost for this instance.
Bridge Priority	Priority associated with current bridge.
Root Bridge Priority	Priority associated with the root bridge.
Root Bridge Address	Address of the root bridge.
Port Priority	Priority of the interface for this instance.
Topology Changes	Number of times the topology has changed for this instance.
Access GW External Cost	External root cost of this instance.

Working with Ethernet Link Aggregation Groups

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

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

You can create static links between Ethernet LAGs by choosing a LAG and the desired port channel for the A or Z side as described in Adding Static Links, page 5-15.

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

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

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

- An aggregation service alarm is generated.

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

Viewing Ethernet LAG Properties

Note Cisco CRS devices must be configured to receive SNMP traps in order to view Ethernet LAG properties. For more information on required SNMP settings, see the *Cisco Prime Network 3.9 Administrator Guide*.

To view properties for Ethernet link aggregation groups:

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

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

The link aggregation properties are displayed as shown in Figure 12-8.

Figure 12-8 Ethernet Link Aggregation in Logical Inventory

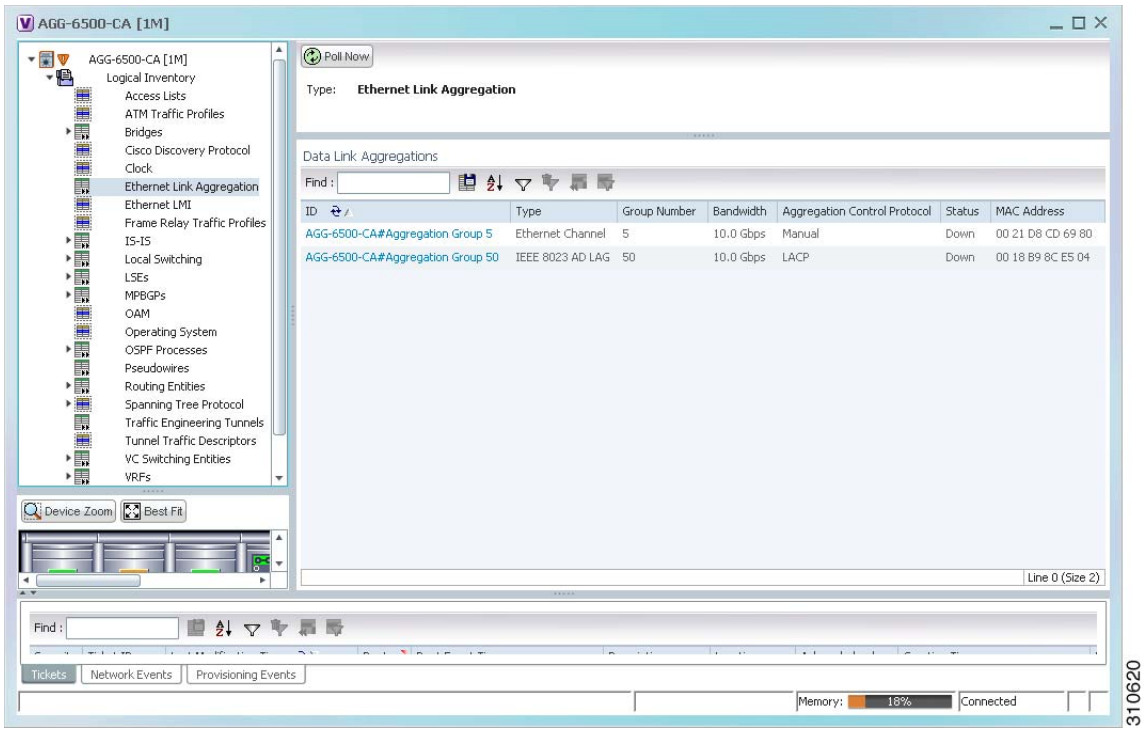


Table 12-12 describes the aggregation group properties that are displayed in the Data Link Aggregations table.

Table 12-12 Data Link Aggregations Table

Field	Description
ID	Aggregation identifier. Double-click the entry to view the properties for that aggregation.
Type	Aggregation group type: Ethernet Channel or IEEE 8023 AD LAG.
Group Number	Aggregation group number.

Table 12-12 Data Link Aggregations Table (continued)

Field	Description
Bandwidth	Aggregation bandwidth.
Aggregation Control Protocol	Aggregation control protocol: Manual, Link Aggregation Control Protocol (LACP), or Port Aggregation Protocol (PagP).
Status	Aggregation status: Up or Down.
MAC Address	Aggregation MAC address.

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

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

- For Ethernet Channel aggregations, see Table 12-13.
- For IEEE 802.3 AD aggregations, see Table 12-14.

Table 12-13 LAG Ethernet Channel Properties

Field	Description
Group Number	Aggregation group number.
Bandwidth	Aggregation bandwidth in b/s.
Control Protocol	Aggregation control protocol: Manual, Link Aggregation Control Protocol (LACP), or Port Aggregation Protocol (PagP).
MAC Address	Aggregation MAC address.
Administrative State	Aggregation administrative status: Up or Down.
Operational State	Aggregation operational status: Up or Down.
Adjacent	Adjacent group, hyperlinked to the group in logical inventory.
mLACP Properties	mLACP properties are displayed if the aggregation group is associated with an ICCP redundancy group.
ICCP Redundancy Group	ICCP redundancy group associated with this aggregation group, hyperlinked to the relevant entry in logical inventory.
mLACP Role	Role of the LAG in the redundancy group: Active or Standby.
mLACP Operational System MAC	MAC address used in a dual-homed environment that is selected by ICCP from one of the configured system MAC addresses for one of the points of attachment (PoAs).
mLACP Operational System Priority	Priority used in a dual-homed environment that is selected by ICCP from the configured system priority on one of the PoAs.
mLACP Failover Option	Configured mLACP failover mode: Revertive or Nonrevertive.
mLACP Max Bundle	Maximum number of links allowed per bundle.

Table 12-13 LAG Ethernet Channel Properties (continued)

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

Table 12-14 LAG IEEE 802.3 AD Properties

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

Table 12-14 LAG IEEE 802.3 AD Properties (continued)

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

Table 12-14 LAG IEEE 802.3 AD Properties (continued)

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

Viewing mLACP Properties

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

To view mLACP properties:

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

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

In response, Prime Network Vision lists the Inter-Chassis Communication Protocol (ICCP) redundancy groups configured on the device as shown in Figure 12-9.

Figure 12-9 ICCP Redundancy in Logical Inventory

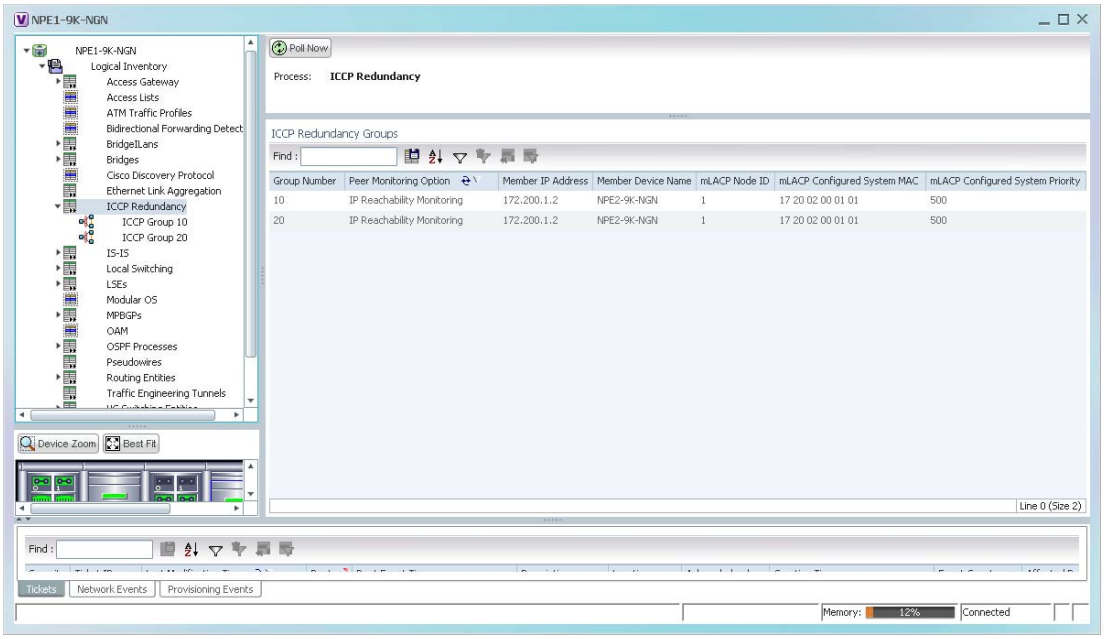


Table 12-15 describes the information displayed in the ICCP Redundancy Groups table.

Table 12-15 ICCP Redundancy Groups in Logical Inventory

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

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

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

The ICCP Redundancy Group Properties window is displayed with the Backbone Interfaces and Data Link Aggregations tabs as shown in Figure 12-10.

Figure 12-10 ICCP Redundancy Group Properties Window

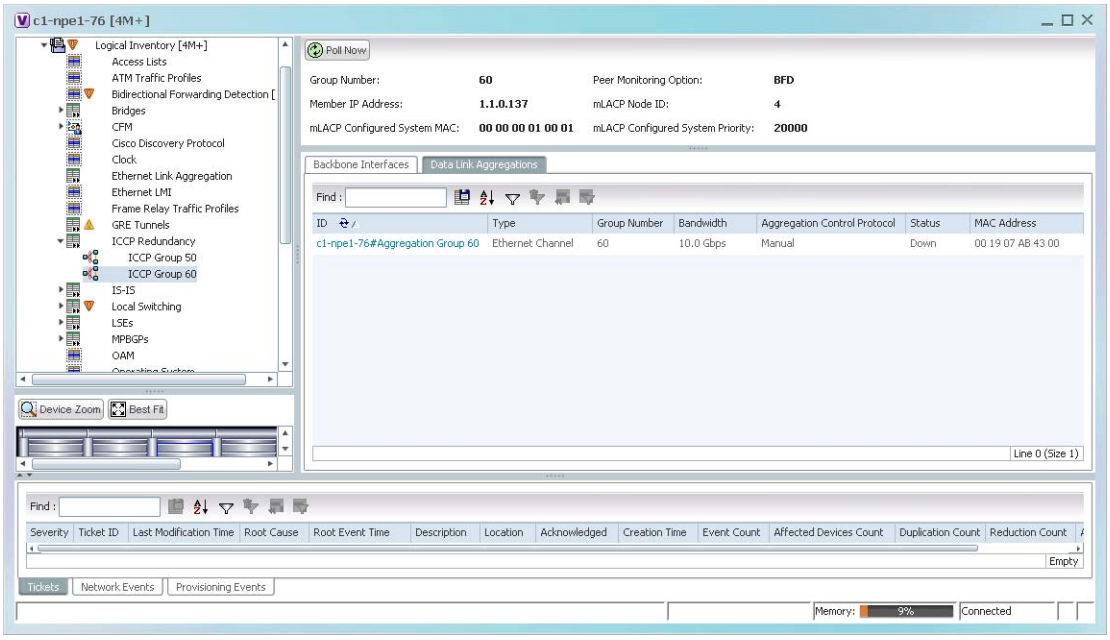


Table 12-16 describes the information available in the ICCP Redundancy Group Properties window.

Table 12-16 ICCP Redundancy Group Properties Window

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

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

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

- Table 12-13—LAG Ethernet Channel Properties
- Table 12-14—LAG IEEE 802.3 AD Properties

Viewing Provider Backbone Bridge Properties

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

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

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

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

To view PBB properties:

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

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

Figure 12-11 shows an example of PBB properties in logical inventory.

Figure 12-11 PBB Properties in Logical Inventory

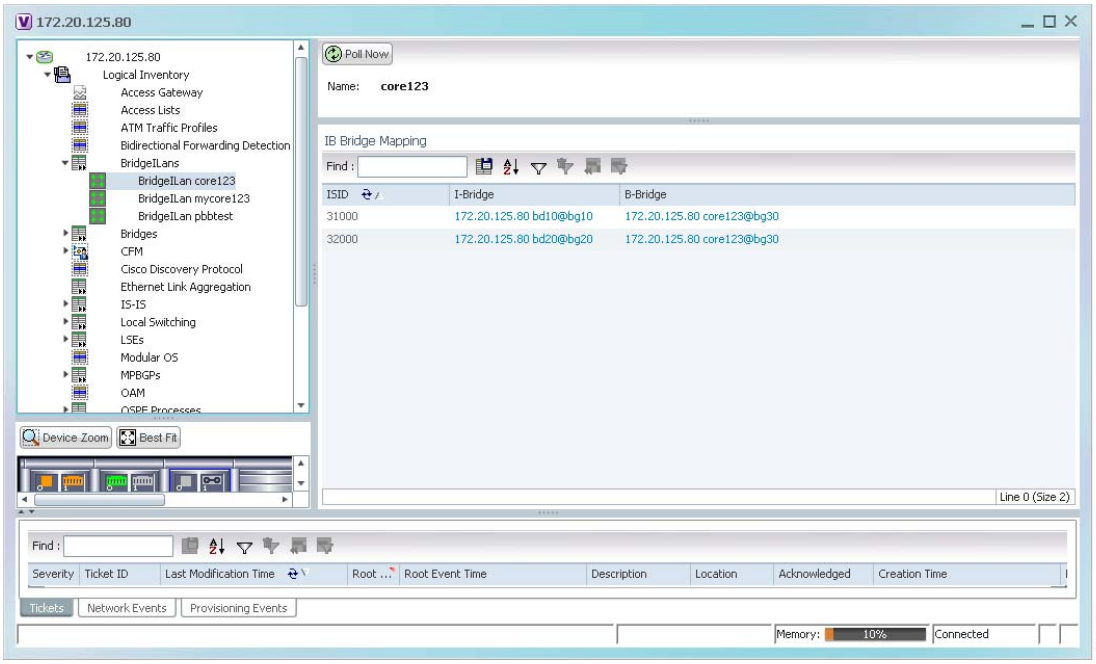


Table 12-17 describes the information displayed for PBB.

Table 12-17 PBB Properties in Logical Inventory

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

Viewing EFP Properties

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

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

To view additional EFP properties:

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

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

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

Figure 12-12 EFP Properties Window

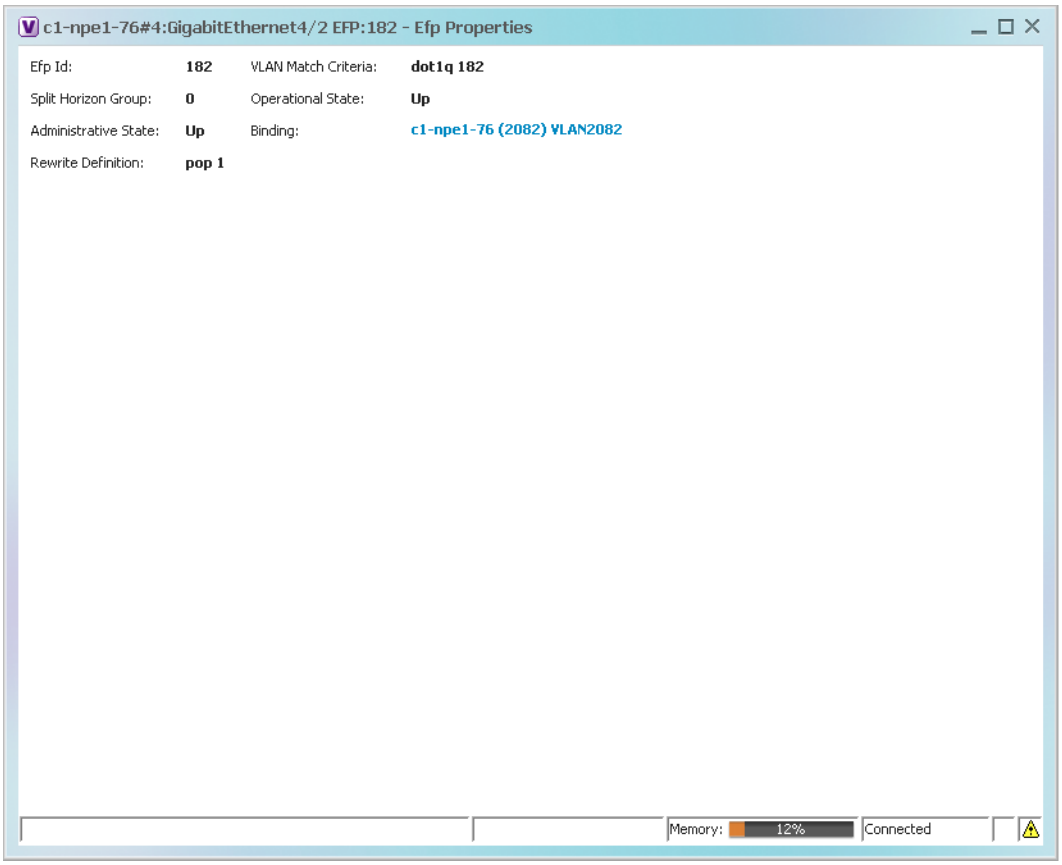


Table 12-18 describes the information displayed in the EFP Properties window.

Table 12-18 EFP Properties Window

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

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

In this example, clicking the hyperlink displays the relevant bridge in logical inventory, as shown in Figure 12-13.

Figure 12-13 Bridge Associated with EFP in Logical Inventory

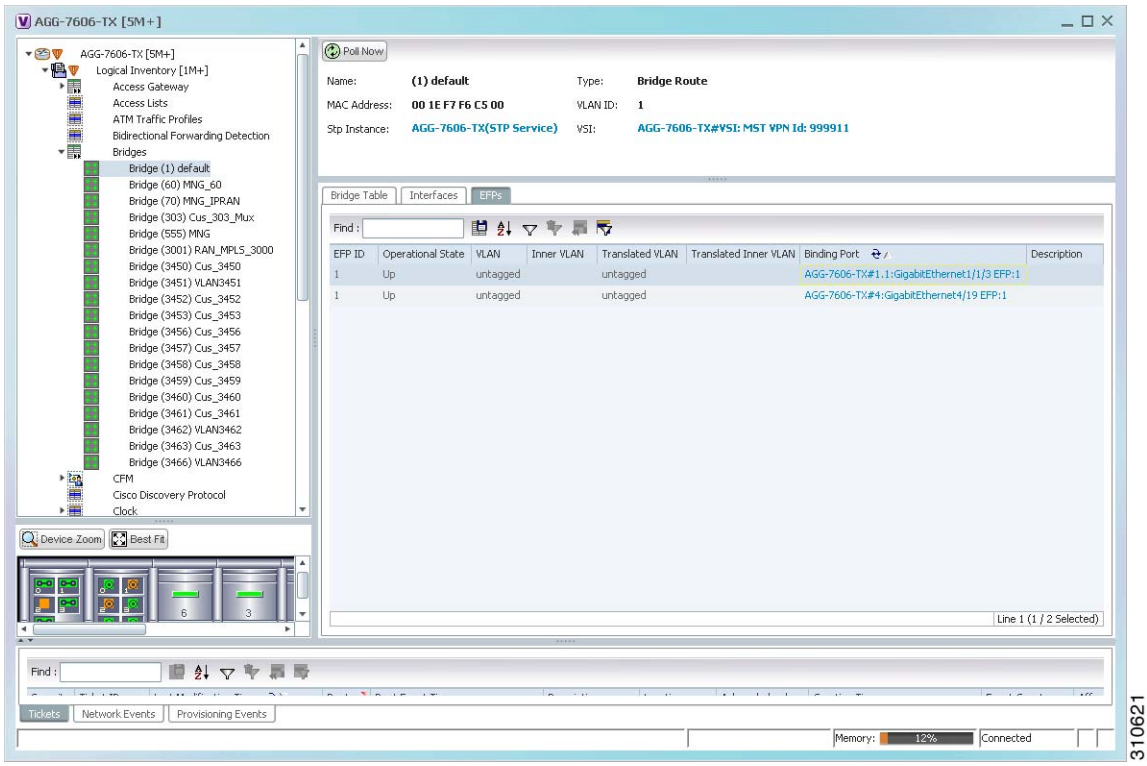


Table 12-19 describes the information displayed for an EFP associated with a bridge.

Table 12-19 EFP Associated with a Bridge in Logical Inventory

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

Table 12-19 EFP Associated with a Bridge in Logical Inventory (continued)

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

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

- In the bridge entry in logical inventory, click the hyperlinked entry in the Binding field.
- Use the procedure described in Viewing and Renaming Ethernet Flow Domains, page 12-39 to navigate to the individual interface.
- In physical inventory, navigate to and then select the required interface.

The EFPs tab is displayed in the content pane next to the Subinterfaces tab as shown in Figure 12-14.

Figure 12-14 EFPs Tab in Physical Inventory

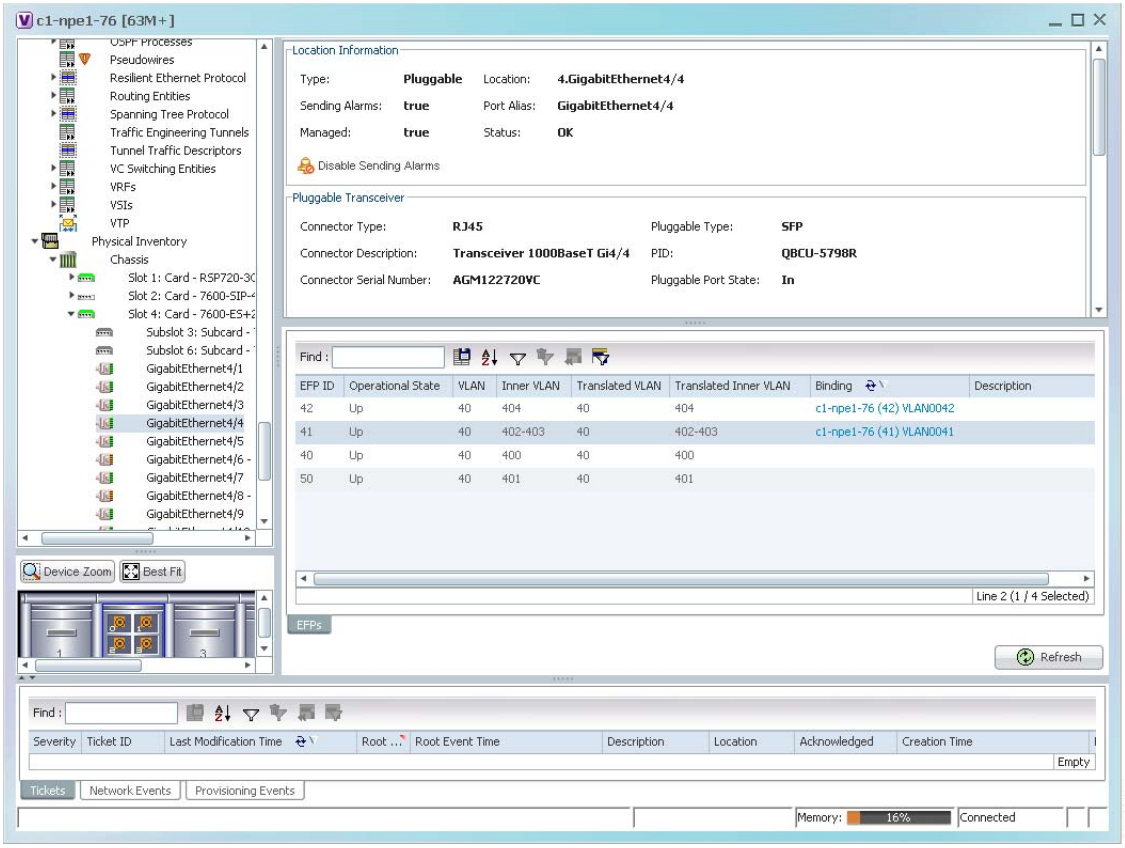


Table 12-20 describes the information displayed in the EFPs tab.

Table 12-20 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.

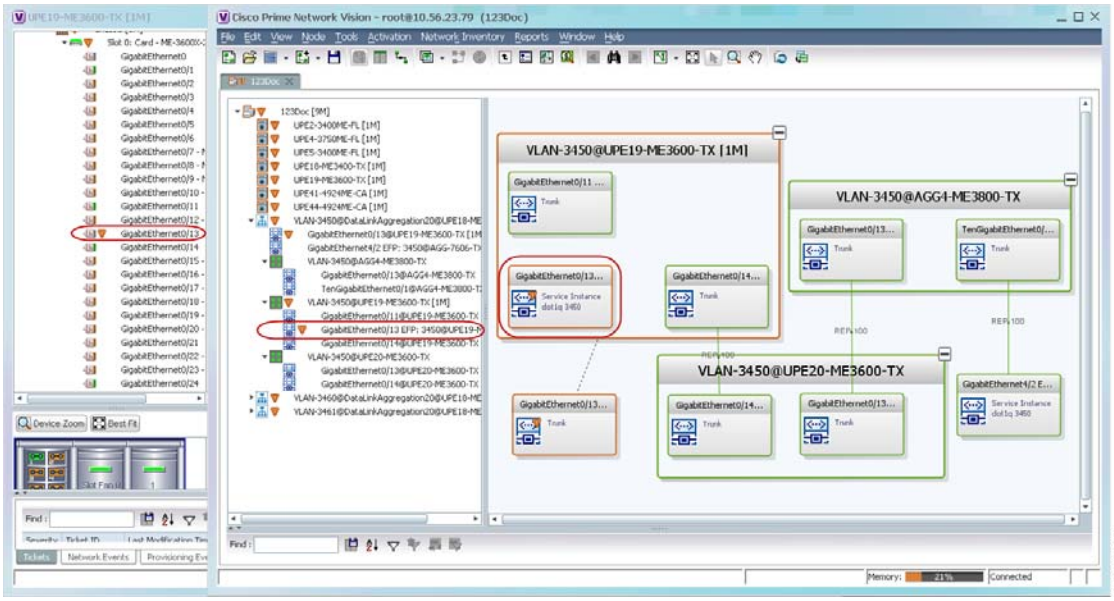
Understanding EFP Severity and Ticket Badges

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

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

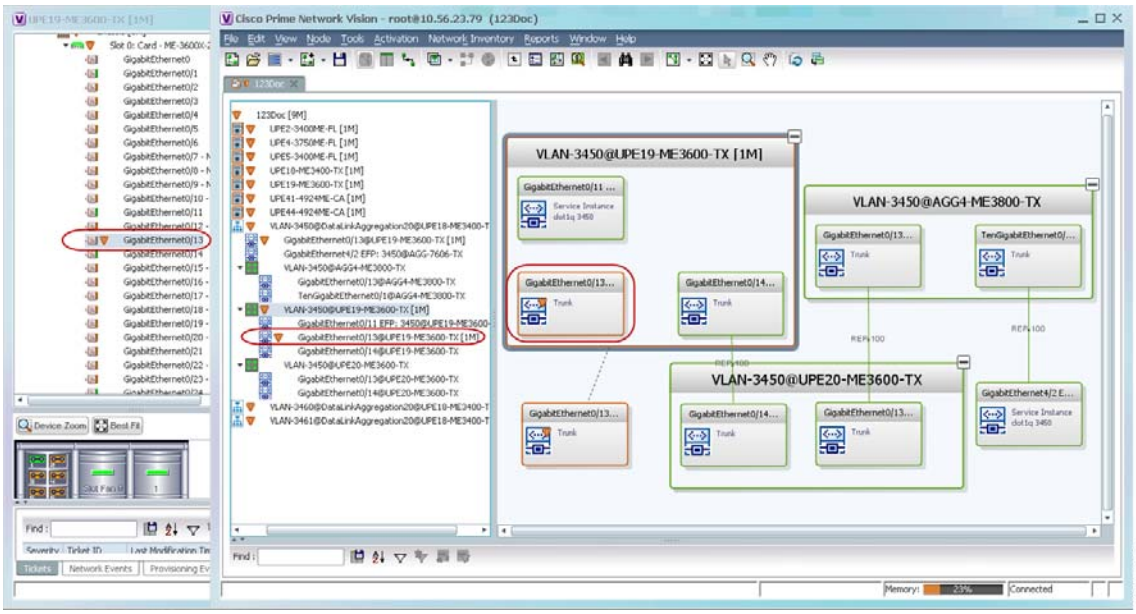
  Figure 12-15 shows an example of a ticket badge based on a service instance.

Figure 12-15 EFP Severity and Ticket Badges Based on Underlying Service Instance



- If the Ethernet flow point element represents a VLAN interface for a regular switch port, the severity and ticket badges are based on the corresponding port, as shown in Figure 12-16.

Figure 12-16 EFP Severity and Ticket Badges Based on Corresponding Port



Viewing EVC Service Properties

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

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

Shared Switching Entities and EVC Service View

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

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

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

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

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

Figure 12-17 shows an example of a port in physical inventory configured with these EVC properties.

Figure 12-17 EVC Port Properties in Physical Inventory

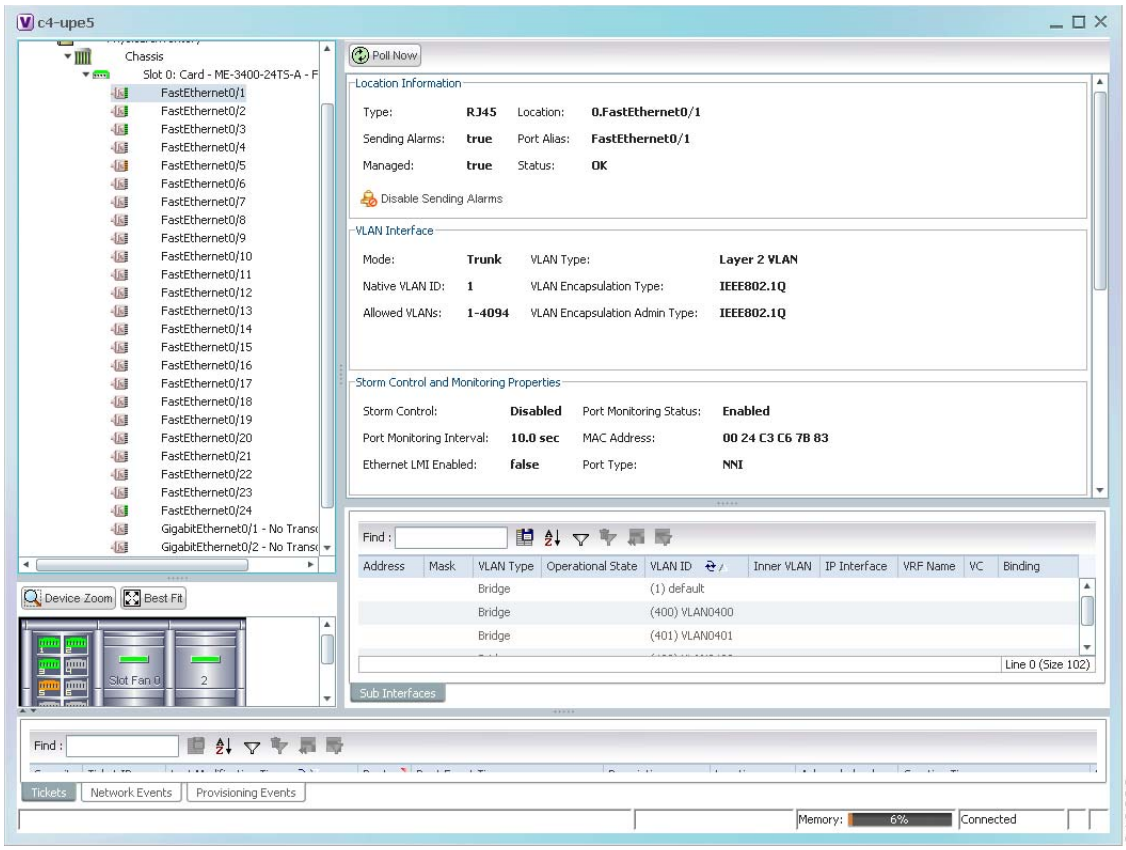


Table 12-21 describes the information displayed for these properties.

Table 12-21 EVC Port Properties in Physical Inventory

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

Table 12-21 EVC Port Properties in Physical Inventory (continued)

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

Viewing and Renaming Ethernet Flow Domains

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

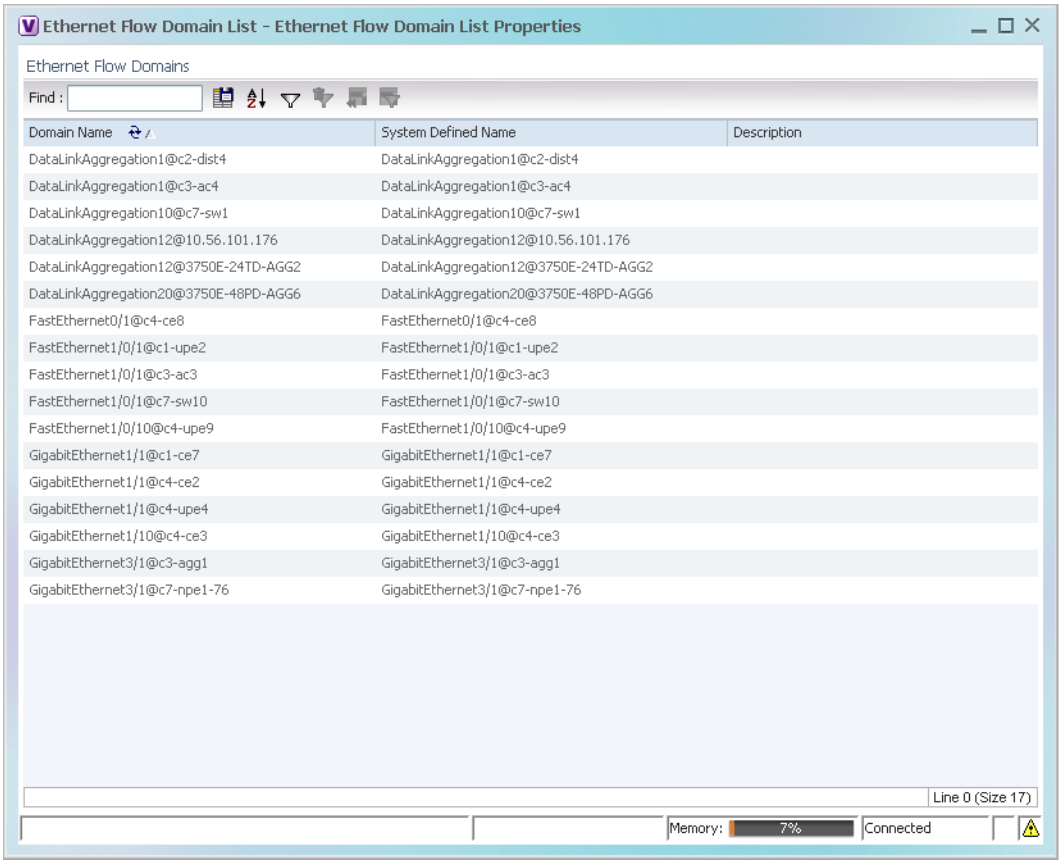
An Ethernet flow domain can have no N-PEs (flat VLAN) or one or more N-PEs (N-PE redundancy configuration). The Ethernet flow domain is defined using physical connectivity at the port level, and not at the network element level. STP is used to mark the root bridge, root or blocked ports, and blocked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

To view Ethernet flow domains:

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

The Ethernet Flow Domain List window is displayed with the domain name, the system-defined domain name, and a brief description for each Ethernet flow domain as shown in Figure 12-18.

Figure 12-18 Ethernet Flow Domain List Properties Window



Step 2 To rename an Ethernet flow domain:

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

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

c. Click **OK**.

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

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

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

The Ethernet Flow Domain Properties window is displayed as shown in Figure 12-19.

Figure 12-19 Ethernet Flow Domain Properties Window

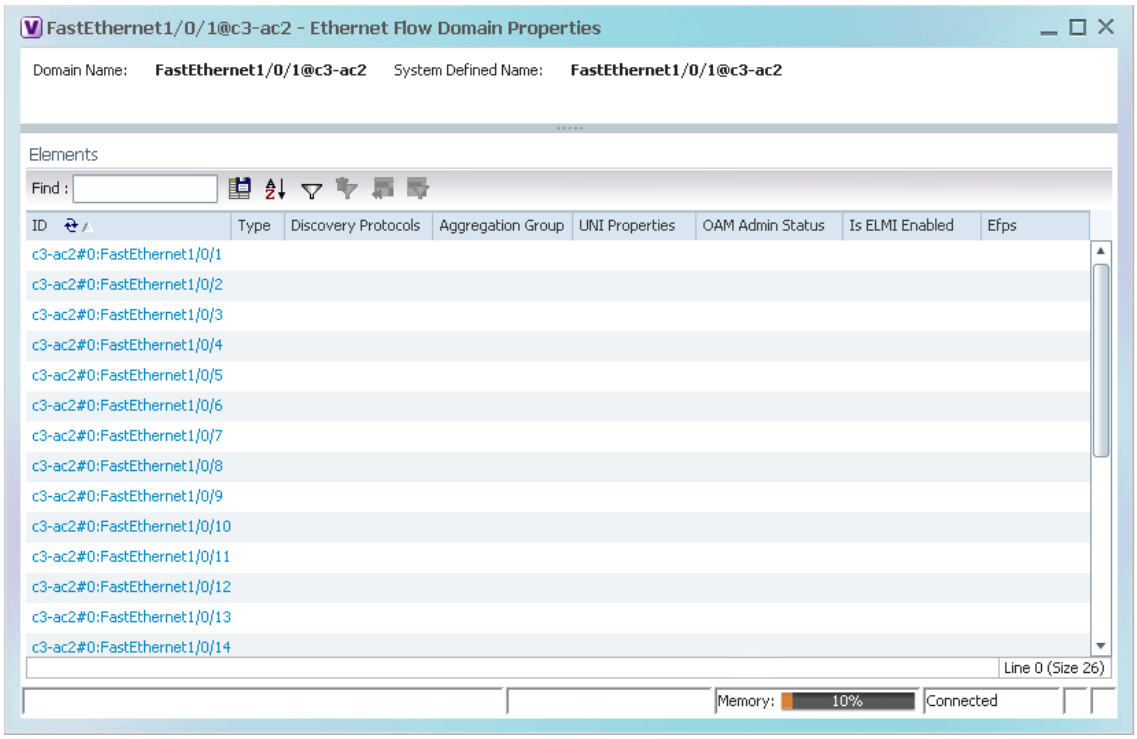


Table 12-22 describes the information displayed in the Ethernet Flow Domain Properties window.

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

Table 12-22 Ethernet Flow Domain Properties Window

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

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

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

Working with VLANs and VLAN Overlays

The following topics provide information and procedures for working with VLANs and VLAN overlays:

- Understanding VLAN and EFD Discovery, page 12-42
- Understanding VLAN Elements, page 12-43
- Switching Entities Containing Termination Points, page 12-48
- Adding VLANs to a Map, page 12-48
- Removing VLANs from a Map, page 12-50
- Viewing VLAN Mappings, page 12-50
- Working with Associated VLANs, page 12-52
- Viewing VLAN Links Between VLAN Elements and Devices, page 12-55
- Applying VLAN Overlays, page 12-58
- Displaying or Hiding VLAN Overlays, page 12-59
- Removing a VLAN Overlay, page 12-59
- Viewing VLAN Service Link Properties, page 12-60
- Viewing REP Information in VLAN Domain Views and VLAN Overlays, page 12-60
- Viewing REP Properties for VLAN Service Links, page 12-61
- Viewing STP Information in VLAN Domain Views and VLAN Overlays, page 12-63
- Viewing STP Properties for VLAN Service Links, page 12-64
- Viewing VLAN Trunk Group Properties, page 12-65
- Viewing VLAN Bridge Properties, page 12-67

Understanding VLAN and EFD Discovery

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

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

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

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

Understanding VLAN Elements

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

- VLAN Elements in Prime Network Vision, page 12-43
- VLANs, page 12-43
- Switching Entities, page 12-43
- Ethernet Flow Points, page 12-44

VLAN Elements in Prime Network Vision

Table 12-23 describes the icons that Prime Network Vision uses to represent VLAN elements.

Table 12-23 VLAN Elements and Icons in Prime Network Vision

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

VLANs

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

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

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

Switching Entities

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

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

A switching entity typically contains EFP elements.

Ethernet Flow Points

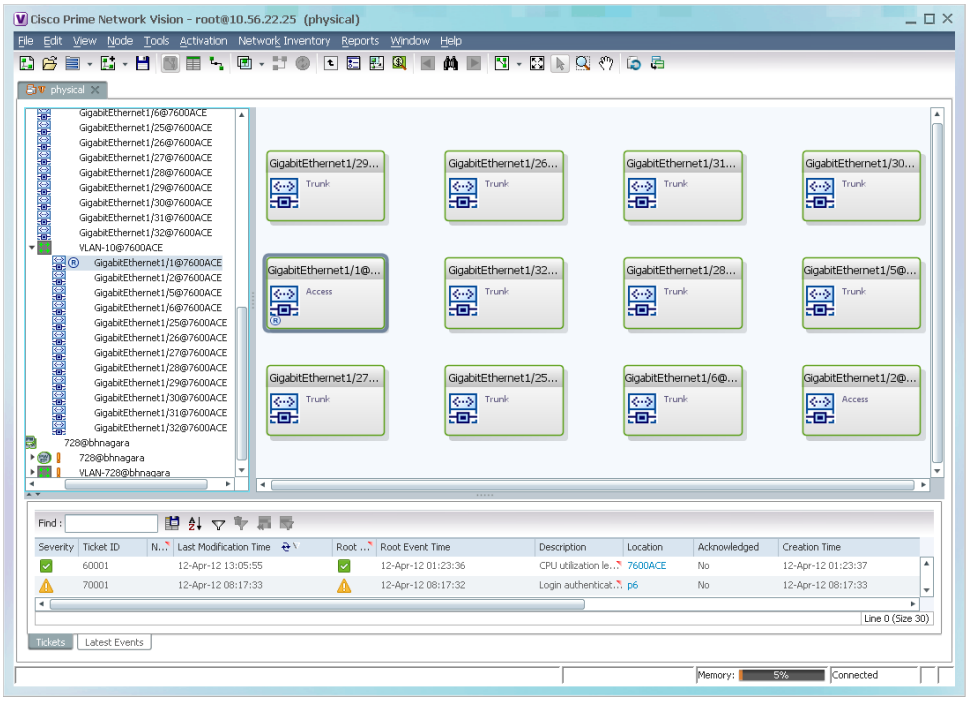
An Ethernet flow point (EFP) can represent a port that is configured for participation in a specific VLAN.

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

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

Figure 12-20 shows an example of EFPs configured as switch ports in Prime Network Vision.

Figure 12-20 EFPs Configured as Switch Ports

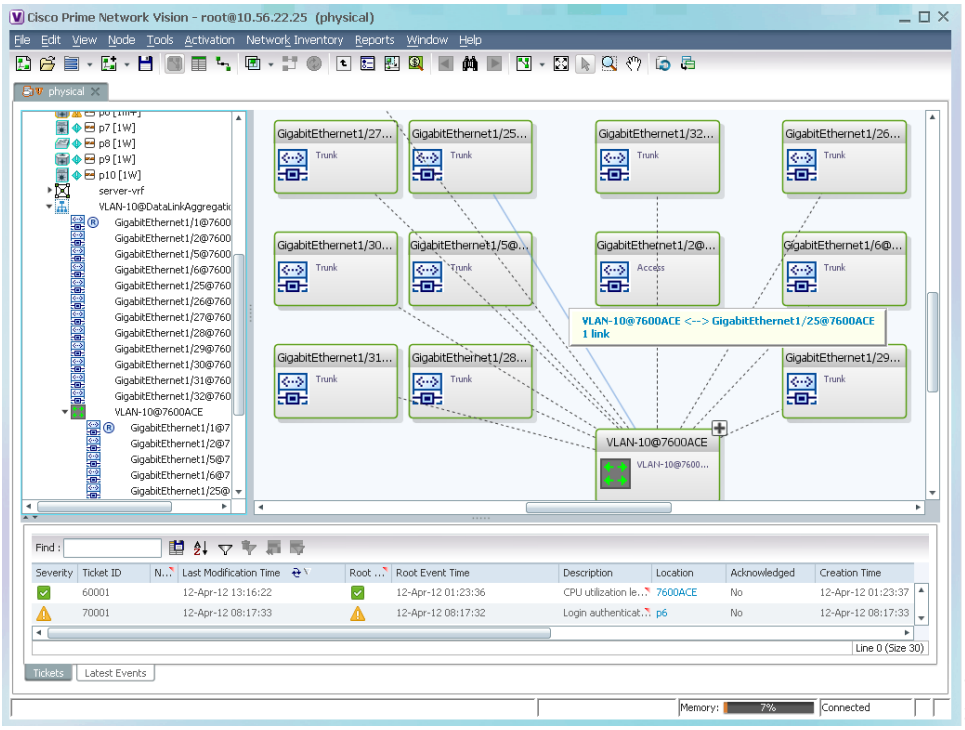


EFPs that are located directly inside a VLAN represent one of the following:

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

  These EFPs are typically connected to a switching entity inside the VLAN by a VLAN link, as shown in Figure 12-21.

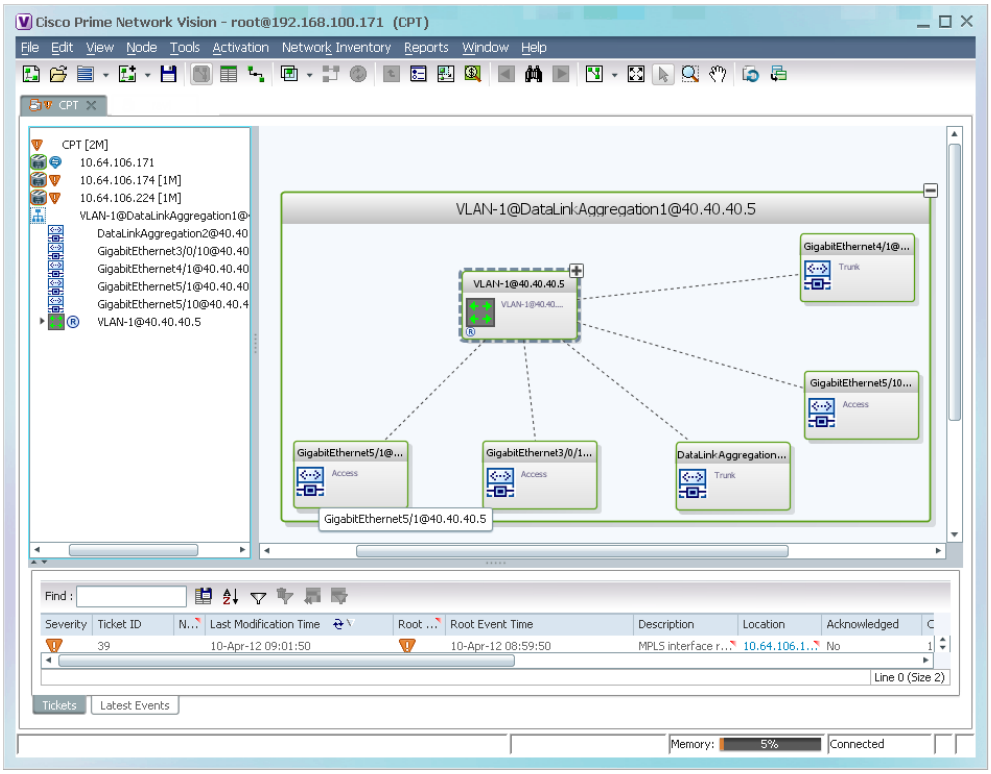
Figure 12-21 Termination Point EFP Inside a VLAN



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

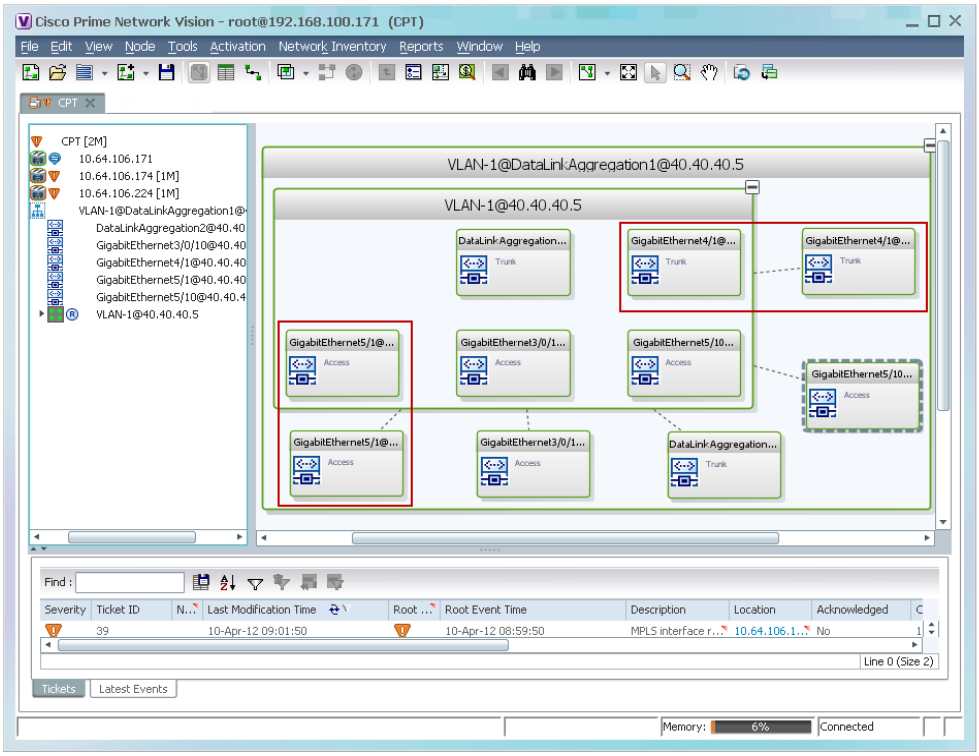
  In Prime Network Vision, edge EFPs are displayed directly under the VLAN at the same level as their switching entities and are connected to their corresponding switching entities by a dotted link, as shown in Figure 12-22.

Figure 12-22 Edge EFP Inside a VLAN



An edge EFP can be displayed both inside and outside of its switching entity, as shown (highlighted with a red outline) in Figure 12-23:

Figure 12-23 Edge EFPs Displayed Inside and Outside of Switching Entities



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

Switching Entities Containing Termination Points

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

Adding VLANs to a Map

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

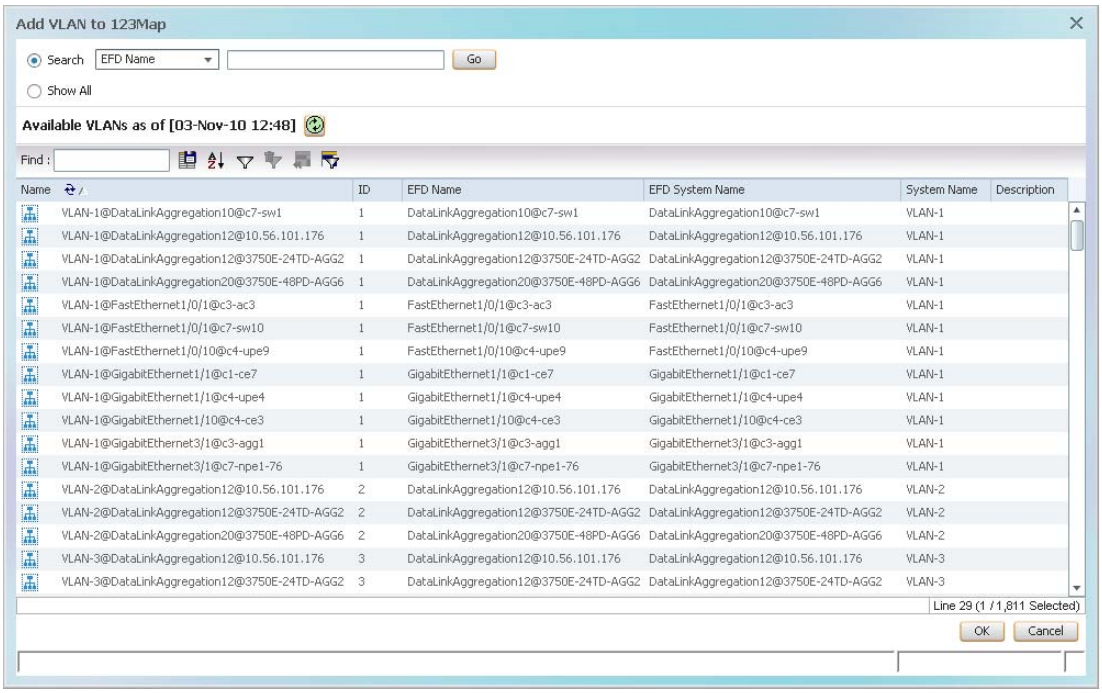
Note Adding VLANs affects other users if they are working with the same map.

To add VLANs to a map:

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

Step 2 Choose **File > Add to Map > VLAN**. The Add VLAN to *map* dialog box is displayed as shown in Figure 12-24.

Figure 12-24 Add VLAN Dialog Box



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

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

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

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

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

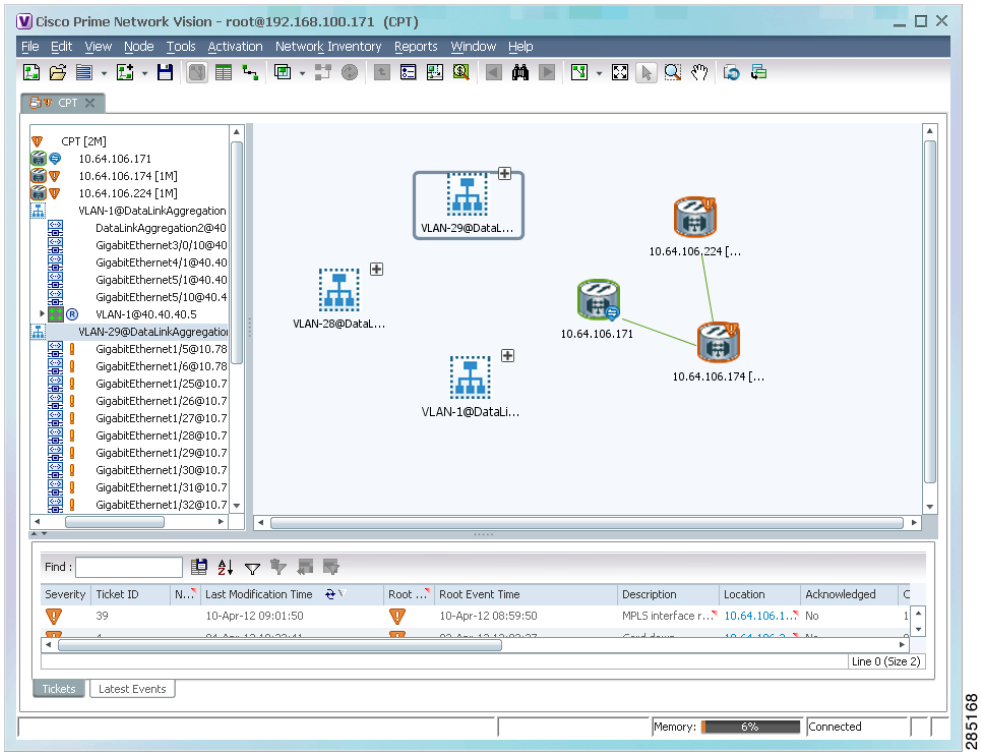
Tip Press **Shift** or **Ctrl** to choose multiple adjoining or nonconsecutive VLANs.

Step 5 Click **OK**.

The VLANs are displayed in the Prime Network Vision content pane as shown in Figure 12-25.

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

Figure 12-25 VLANs in Map View



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

- Viewing and Renaming Ethernet Flow Domains, page 12-39
- Viewing EFP Properties, page 12-31

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, page 12-14
- Viewing REP Information in VLAN Domain Views and VLAN Overlays, page 12-60
- Viewing REP Properties for VLAN Service Links, page 12-61

For STP, see:

- Viewing Spanning Tree Properties, page 12-10
- Viewing STP Information in VLAN Domain Views and VLAN Overlays, page 12-63
- Viewing STP Properties for VLAN Service Links, page 12-64

Removing VLANs from a Map

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

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

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

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

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

Viewing VLAN Mappings

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

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

To view VLAN mappings:

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

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

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

The VLAN Mappings tab is displayed as shown in Figure 12-26.

Figure 12-26 VLAN Mappings Tab in Physical Inventory

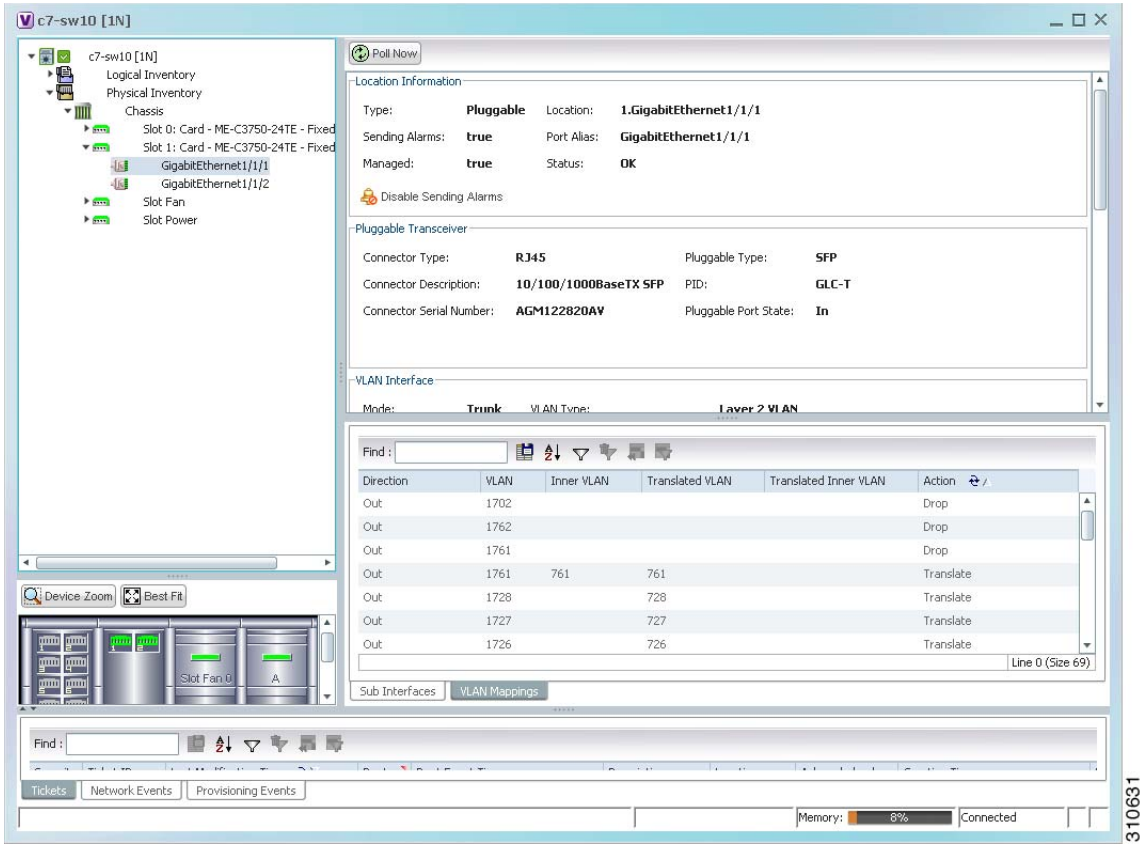


Table 12-24 describes the information that is displayed in the VLAN Mappings table.

Table 12-24 VLAN Mappings Table

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

Working with Associated VLANs

Prime Network Vision discovers associations between network VLANs and displays the information in Prime Network Vision. Network VLAN associations are represented by VLAN service links, and can be any of the tag manipulation types described in Table 12-25.

Table 12-25 Types of Tag Manipulations in VLAN Associations

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

When working with VLANs, you can:

- Add an associated VLAN—See Adding an Associated VLAN, page 12-52.
- View properties for associated VLANs—See Viewing Associated Network VLAN Service Links and VLAN Mapping Properties, page 12-54.

Adding an Associated VLAN

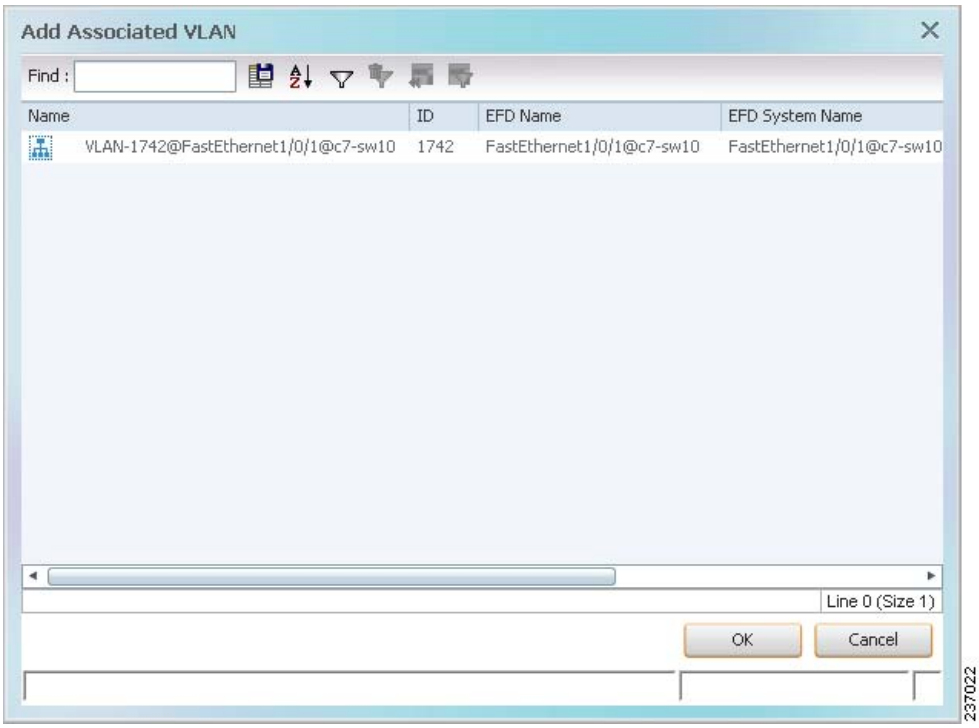
To add an associated VLAN to an existing VLAN in a map:

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

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

The Add Associated VLAN table is displayed as shown in Figure 12-27.

Figure 12-27 Add Associated VLAN Window



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

Table 12-26 describes the information displayed in the Add Associated VLAN table.

Table 12-26 Add Associated VLAN Table

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

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

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

Viewing Associated Network VLAN Service Links and VLAN Mapping Properties

After you add an associated network VLAN, you can:

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

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

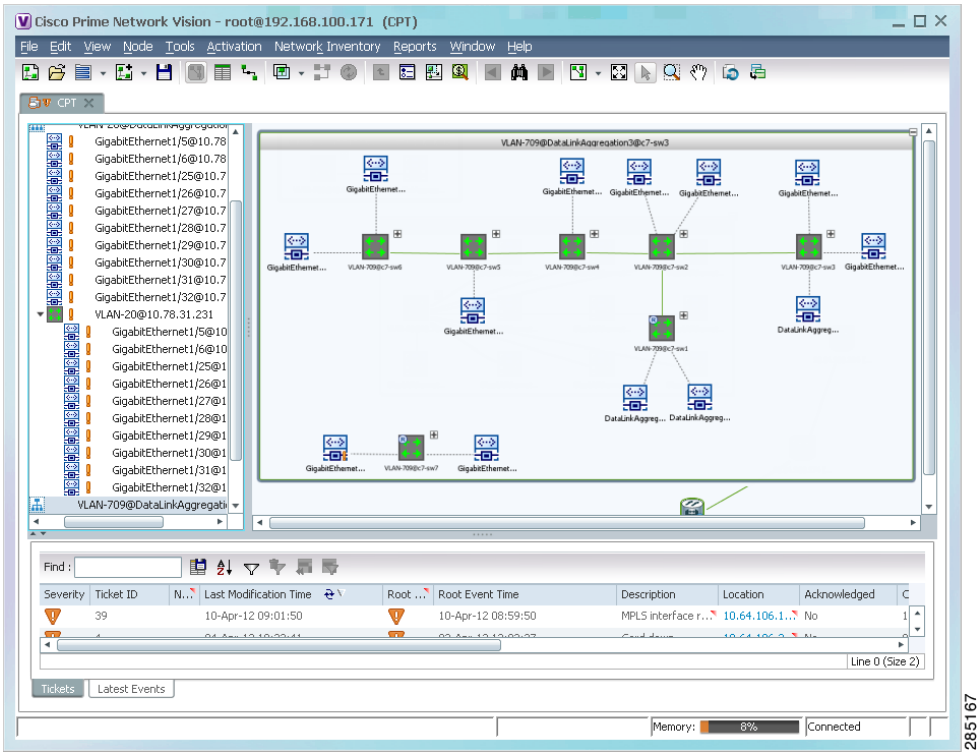
Step 1 Select the required network VLAN in the map view.

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

Figure 12-28 shows an example of a network VLAN in a thumbnail.

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

Figure 12-28 VLAN Service Links Between Associated Network VLANs

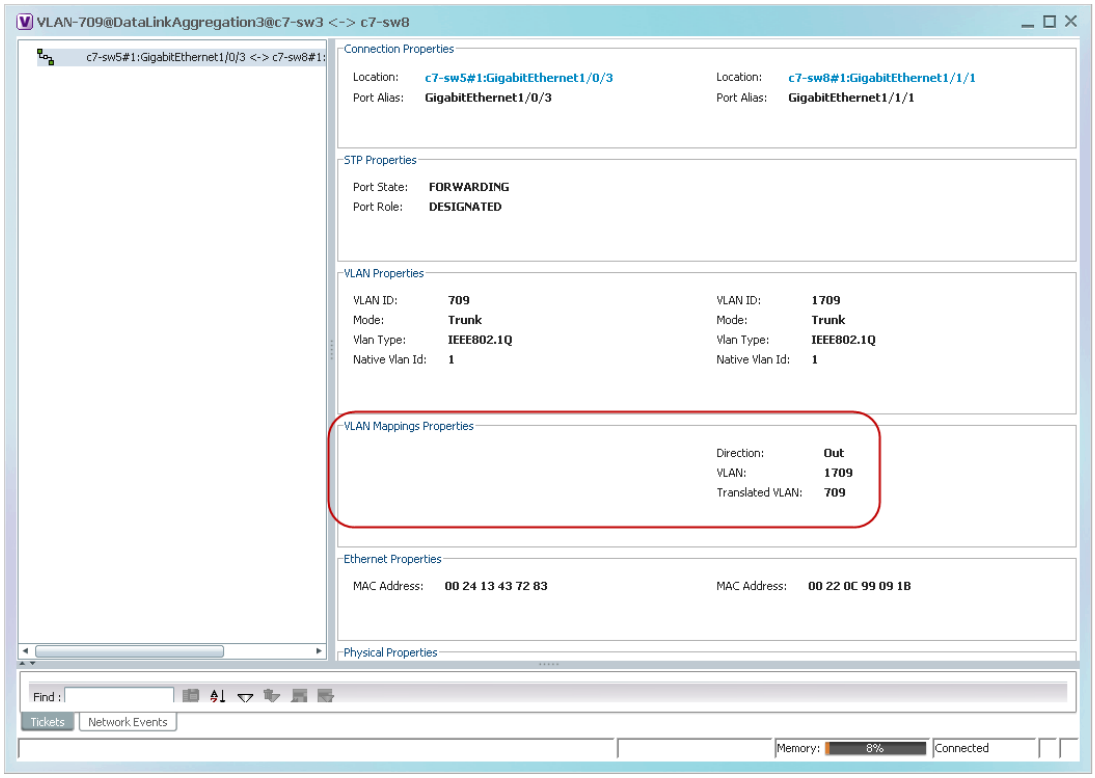


Step 3 To view additional information, right-click a link, and choose **Properties**.

The Link Properties window is displayed as shown in Figure 12-29.

If VLAN tag manipulation is configured on the link, the VLAN Mapping Properties area in the Link Properties window displays the relevant information. For example, in Figure 12-29, the VLAN Mapping Properties area shows that a one-to-one VLAN mapping for VLAN tag 1709 to VLAN tag 709 is configured on GigabitEthernet1/1/1 on c7-sw8 on the egress direction.

Figure 12-29 VLAN Mapping Properties in Link Properties Window



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

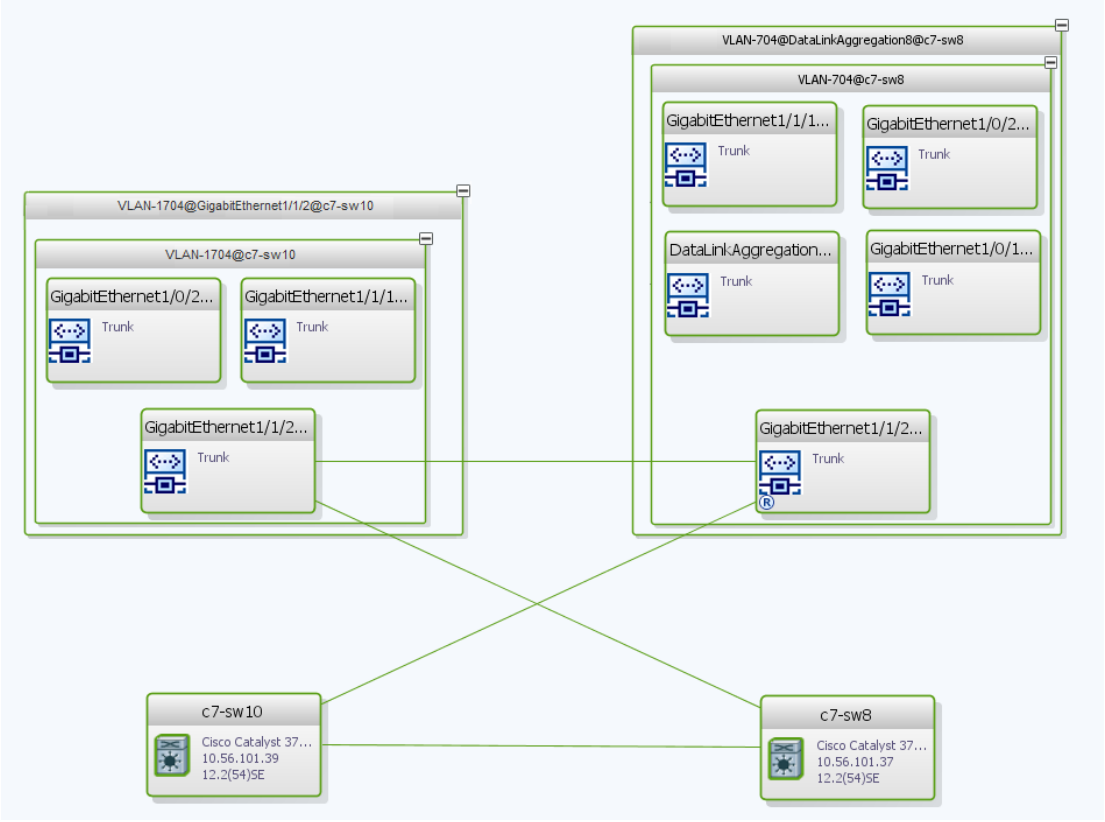
- Viewing REP Properties for VLAN Service Links, page 12-61
- Viewing STP Properties for VLAN Service Links, page 12-64

Viewing VLAN Links Between VLAN Elements and Devices

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

For example, assume that you have the following situation, as shown in Figure 12-30 and described in the following paragraphs.

Figure 12-30 VLAN Elements and Devices in Prime Network Vision



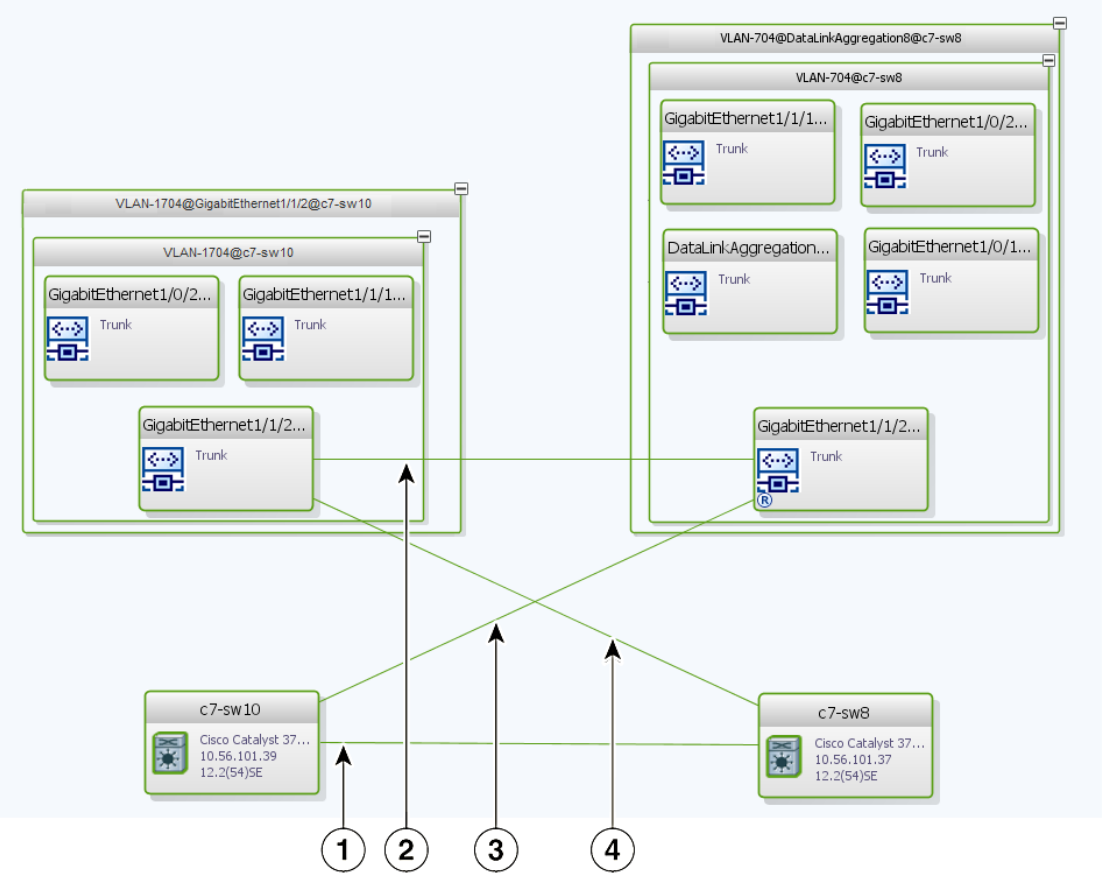
The elements are configured as follows:

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

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

The four links in the map are identified in Figure 12-31 and described in the following table.

Figure 12-31 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.

Applying VLAN Overlays

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.

To add a VLAN overlay:

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

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

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

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

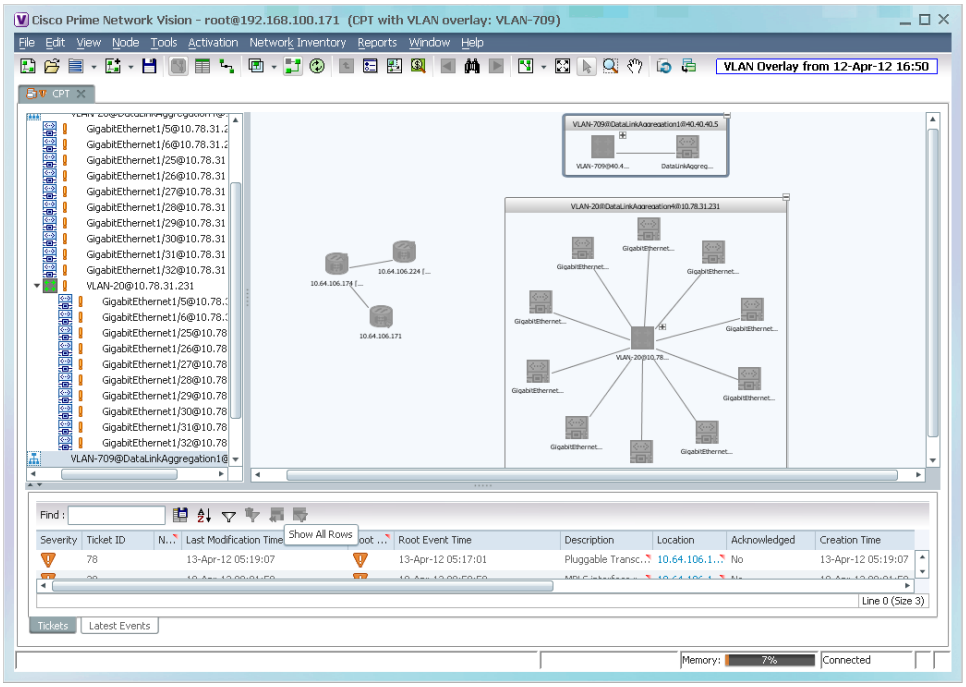
  The search condition is “contains.” Search strings are case-insensitive. For example, if you choose the Name category and enter “net,” Prime Network Vision displays overlays that have “net” in their names. The string “net” can be at the beginning, middle, or end of the name, such as Ethernet.

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

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

The network elements and physical links used by the selected VLAN overlay are highlighted in the network map. All other network elements and links are dimmed. The VLAN name is displayed in the title of the window. See Figure 12-32.

Figure 12-32 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.

Displaying or Hiding VLAN Overlays

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

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

Removing a VLAN Overlay

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

Viewing VLAN Service Link Properties

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

- Viewing REP Properties for VLAN Service Links, page 12-61
- Viewing STP Properties for VLAN Service Links, page 12-64
- Viewing Associated Network VLAN Service Links and VLAN Mapping Properties, page 12-54

Viewing REP Information in VLAN Domain Views and VLAN Overlays

You can view REP segment and port information in Prime Network Vision in the map view. The icons displayed depend on whether you view the REP information in the VLAN domain view or in a VLAN overlay. Table 12-27 describes the icons and badges used to represent REP segment and port information.

Table 12-27 REP Icons and Badges in VLAN Domain Views and Overlays

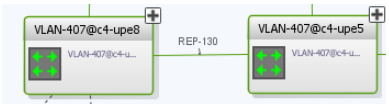
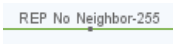
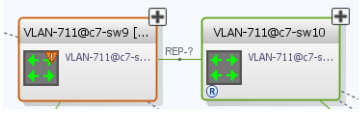
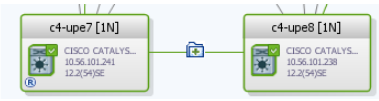
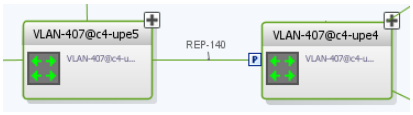
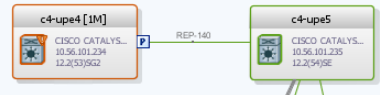
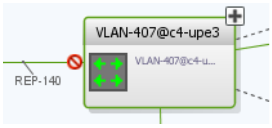
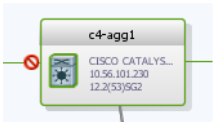
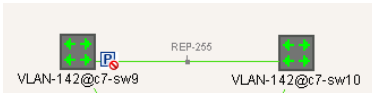
Item	Description	VLAN Domain View	VLAN Overlay
	REP identifier—Uses the format REP-*id* where *id* represents the REP segment identifier.	 The REP identifier is displayed in the domain view if the visual link represents only one link. f the visual link represents more than one link, no REP identifier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

Table 12-27 REP Icons and Badges in VLAN Domain Views and Overlays (continued)

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

Viewing REP Properties for VLAN Service Links

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

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

Figure 12-33 shows an example of the Link Properties window with REP information.

Figure 12-33 VLAN Service Link Properties Window with REP Information

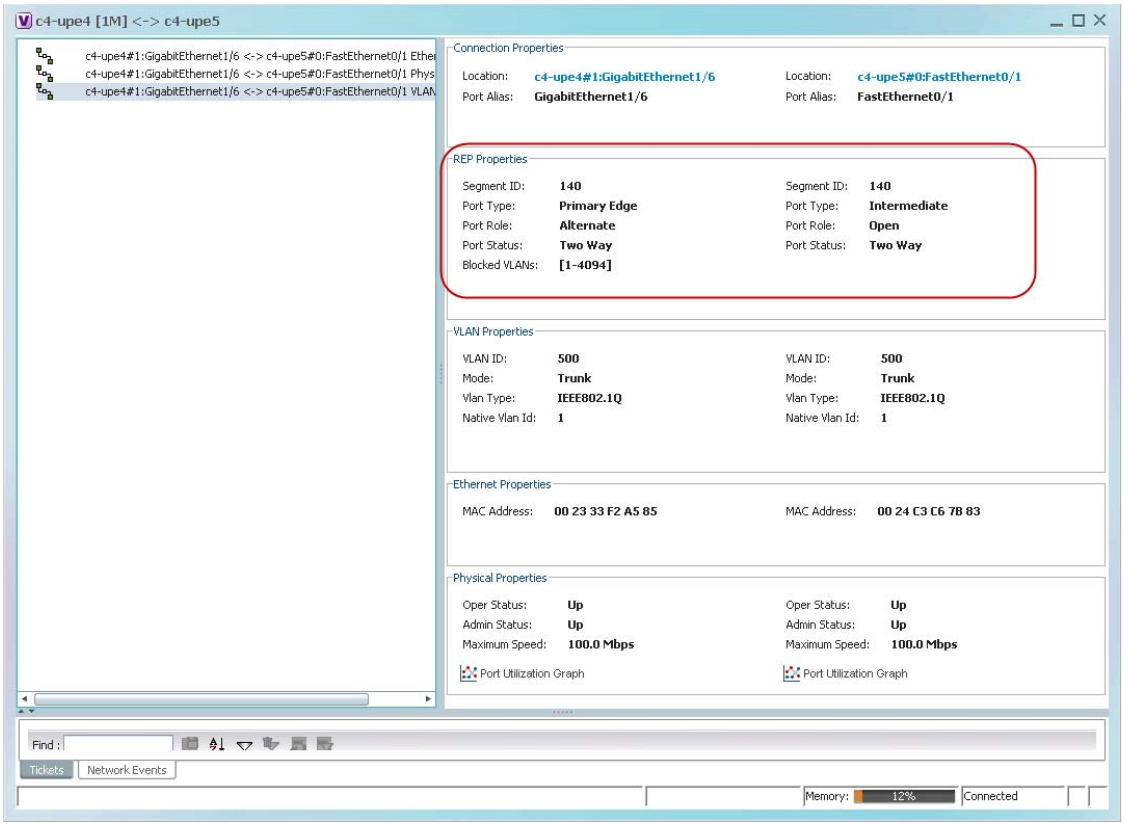


Table 12-28 describes the information that is displayed for REP for each end of the link.

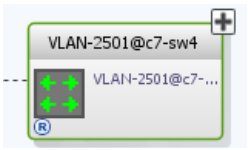
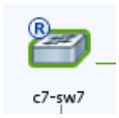
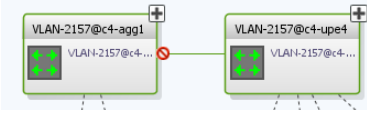
Table 12-28 REP Properties in VLAN Service Link Properties Window

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

Viewing STP Information in VLAN Domain Views and VLAN Overlays

You can view STP segment and port information in Prime Network Vision in the map view. The icons displayed depend on whether you view the STP information in the VLAN domain view or in a VLAN overlay. Table 12-29 describes the icons and badges used to represent STP link and port information.

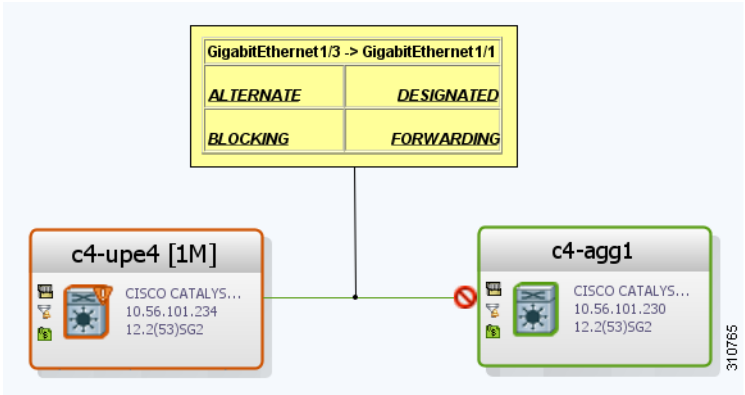
Table 12-29 STP Information in VLAN Domain Views and Overlays

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

To view additional STP information in a VLAN overlay, right-click an STP link and choose **Show Callouts**. The following STP port information is displayed as shown in Figure 12-34:

- Port name
- Port role
- Port state

Figure 12-34 STP Link Information in a VLAN Overlay



Viewing STP Properties for VLAN Service Links

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

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

Figure 12-35 shows an example of the Link Properties window with STP information.

Figure 12-35 STP Properties in VLAN Service Link Properties Window

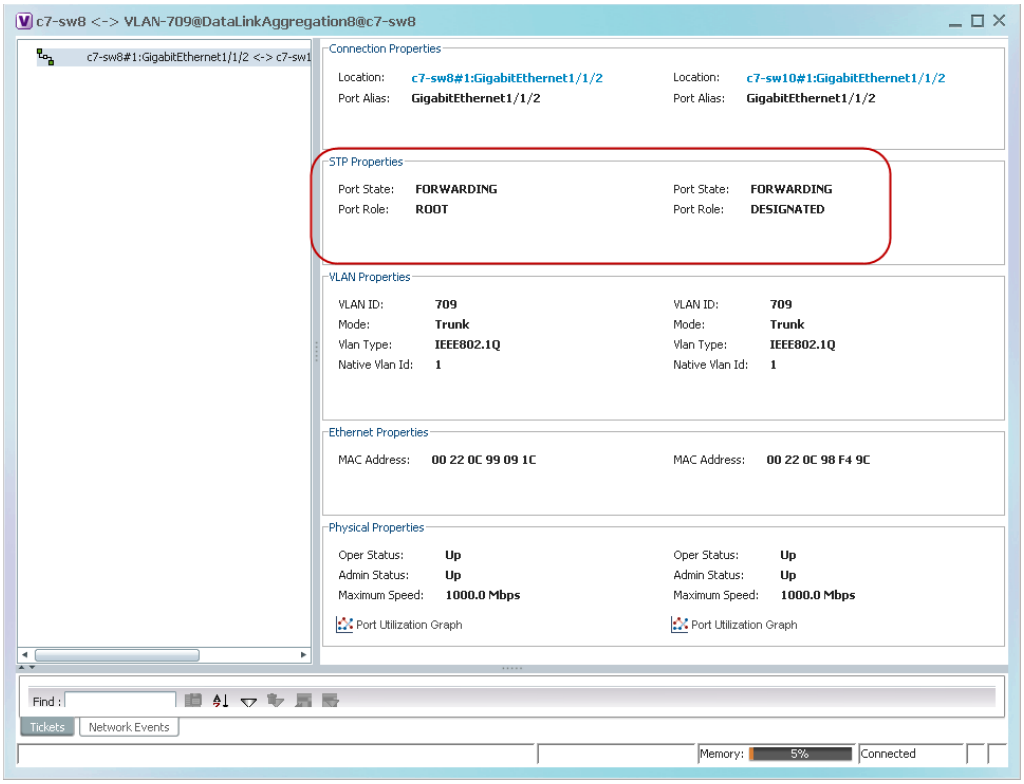


Table 12-30 describes the information that is displayed for STP for the VLAN service link.

Table 12-30 STP Properties in VLAN Service Link Properties Window

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

Viewing VLAN Trunk Group Properties

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

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

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

To view VTP properties:

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

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

The VTP Domain Properties window is displayed as shown in Figure 12-36.

Figure 12-36 VTP Domain Properties Window in Logical Inventory

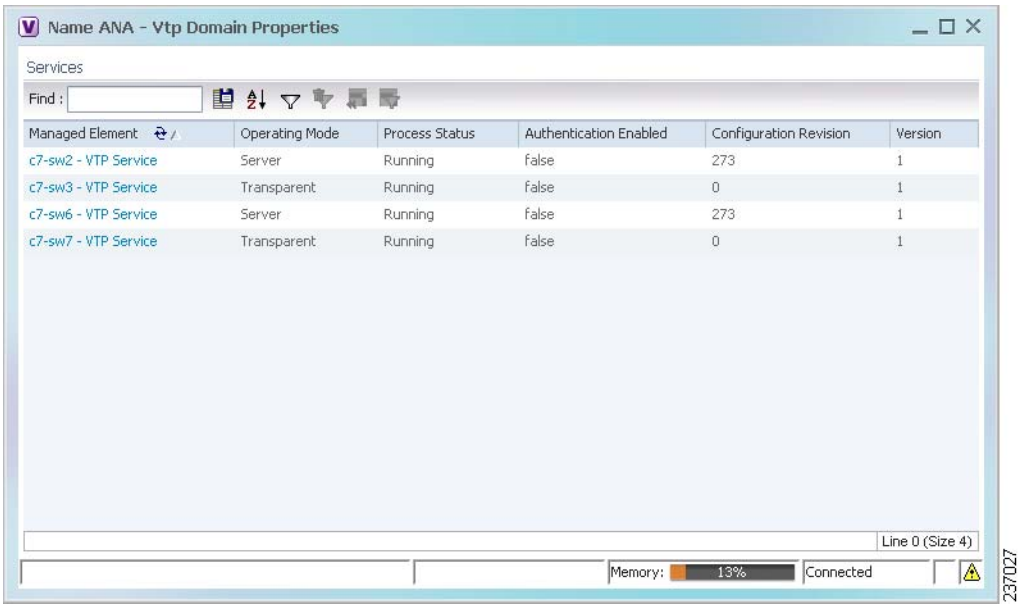


Table 12-31 describes the information that is displayed in the VTP Domain Properties window.

Table 12-31 VTP Domain Properties Window

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

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

Table 12-32 describes the VTP information that is displayed in the inventory window content pane.

Table 12-32 VTP Properties in Inventory

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

Table 12-32 VTP Properties in Inventory (continued)

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

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

Viewing VLAN Bridge Properties

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

To view VLAN bridge properties:

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

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

VLAN bridge properties are displayed as shown in Figure 12-37.

Figure 12-37 VLAN Bridge Properties in Logical Inventory

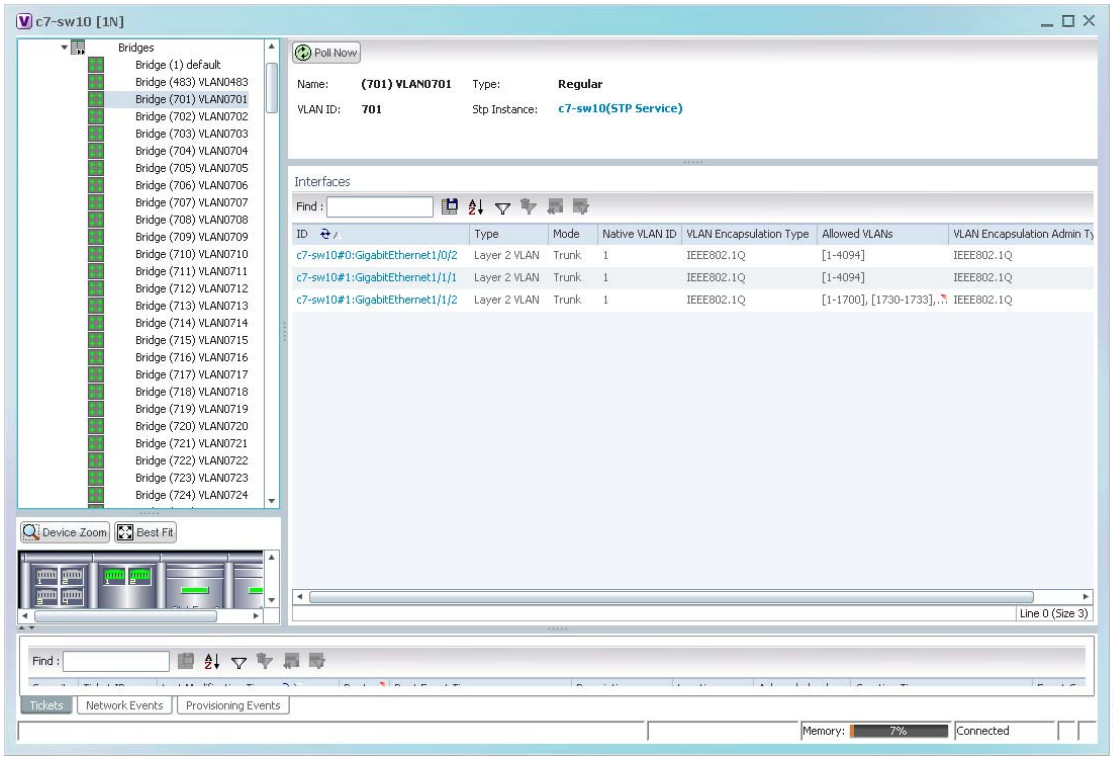


Table 12-33 describes the information that is displayed. Depending on the bridge configuration, any of the tabs might be displayed for the selected bridge.

Table 12-33 VLAN Bridge Properties

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

Table 12-33 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.

Understanding Unassociated Bridges

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

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

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

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

Adding Unassociated Bridges

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

To add an unassociated bridge to a map:

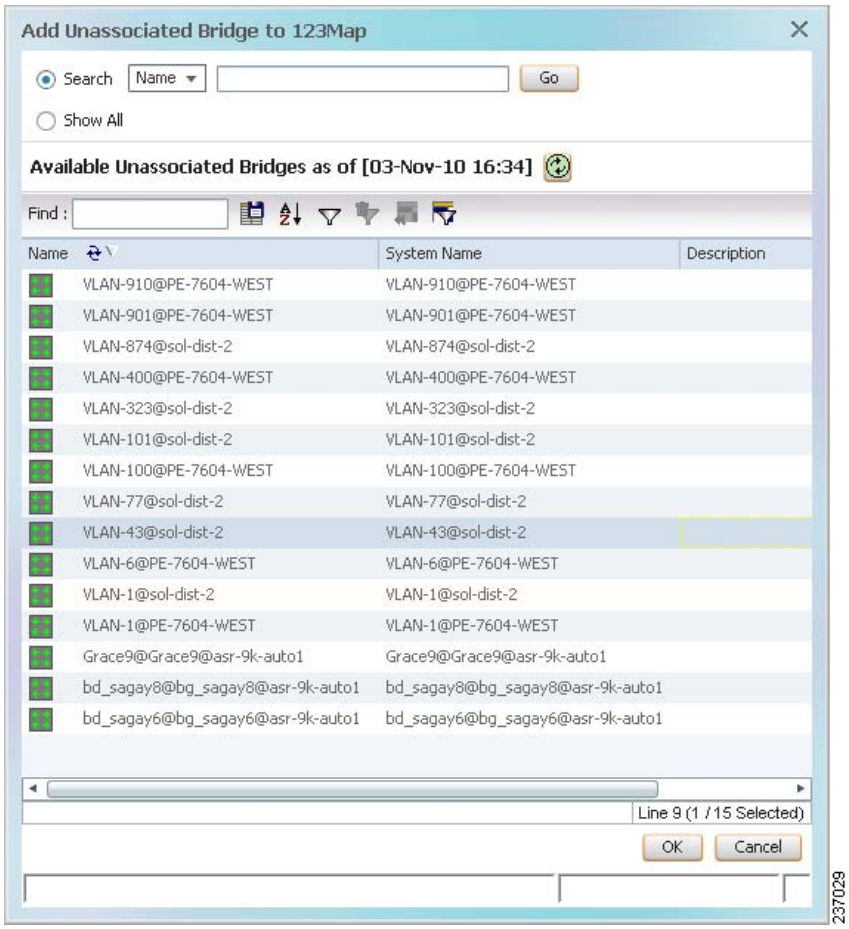
Step 1 In Prime Network Vision, select the required map or domain.

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

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

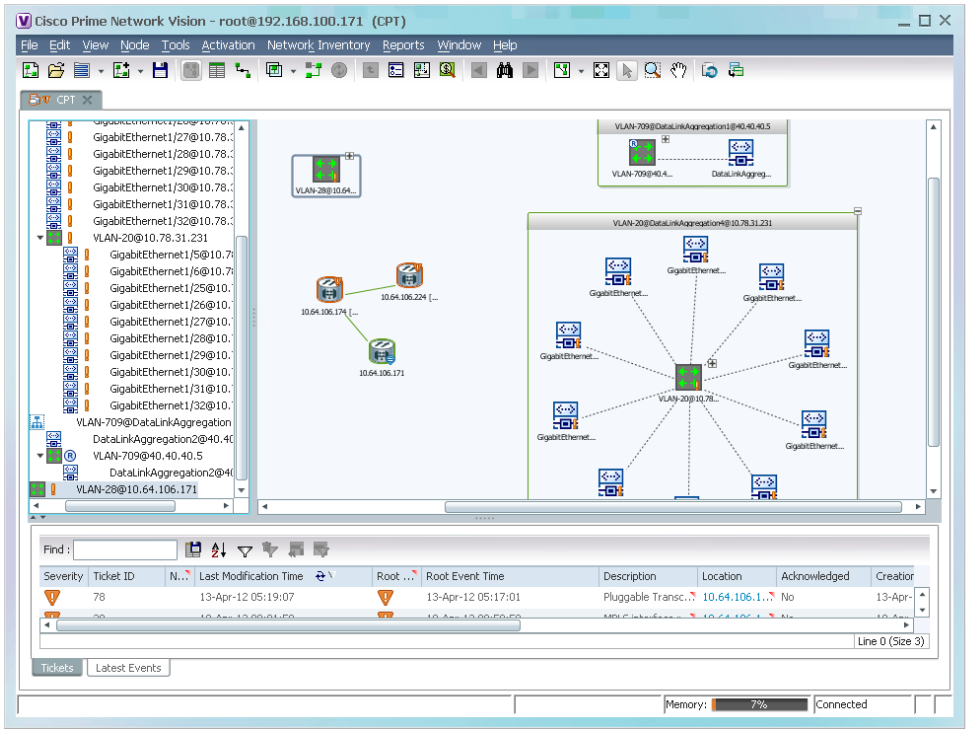
Figure 12-38 shows an example of the Add Unassociated Bridge dialog box.

Figure 12-38 Add Unassociated Bridge Dialog Box



Step 3 In the Add Unassigned Bridge to *domain* dialog box, select the required bridge and click **OK**. The map is refreshed and displays the newly added bridge as shown in Figure 12-39.

Figure 12-39 Unassociated Bridge in Prime Network Vision



Working with Ethernet Flow Point Cross-Connects

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

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

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

- Adding EFP Cross-Connects, page 12-73
- Viewing EFP Cross-Connect Properties, page 12-73

Adding EFP Cross-Connects

To add an EFP cross-connect to a map:

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

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

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

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

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

Viewing EFP Cross-Connect Properties

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

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

The information that is displayed for EFP cross-connects is the same in both the Local Switching Entry Properties window and in the Local Switching Table in logical inventory (as shown in Figure 12-40).

Figure 12-40 Local Switching Table in Logical Inventory

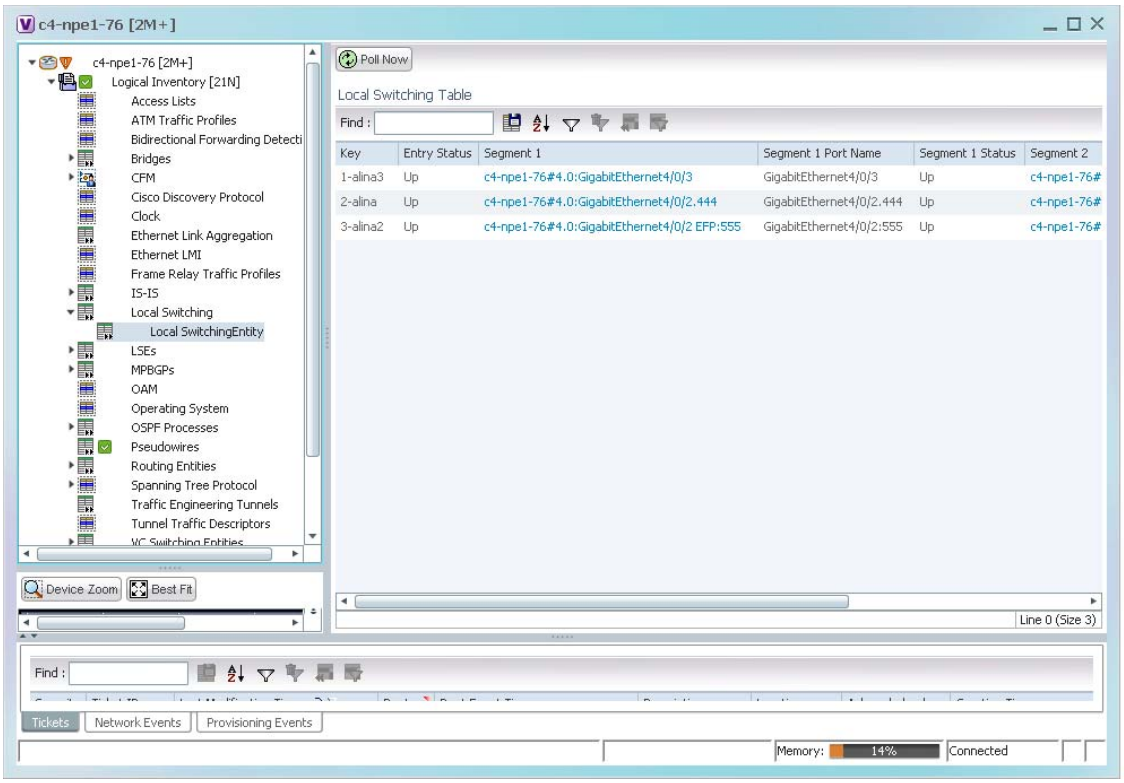


Table 12-34 describes the information displayed for the EFP cross-connects in the Local Switching Table.

Table 12-34 EFP Cross-Connect Properties in Local Switching Table

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

Working with VPLS and H-VPLS Instances

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

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

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

- VSIs
- Pseudowires
- EFPs
- Switching entities

Working with VPLS and H-VPLS in Prime Network Vision

Prime Network Vision enables you to:

- Add VPLS instances to a map—See Adding VPLS Instances to a Map, page 12-76.
- Apply VPLS overlays—See Applying VPLS Instance Overlays, page 12-77.
- View link details in VPLS overlays—See Viewing Pseudowire Tunnel Links in VPLS Overlays, page 12-79.
- View VPLS-related properties—See the following topics:
  - Viewing VPLS Instance Properties, page 12-81
  - Viewing Virtual Switching Instance Properties, page 12-83
  - Viewing VPLS Core or Access Pseudowire Endpoint Properties, page 12-85
  - Viewing VPLS Access Ethernet Flow Point Properties, page 12-87

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

Adding VPLS Instances to a Map

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

To add a VPLS instance to a map:

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

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

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

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

- To search for specific elements:

  a. Choose **Search**.

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

  c. Click **Go**.

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

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

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

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

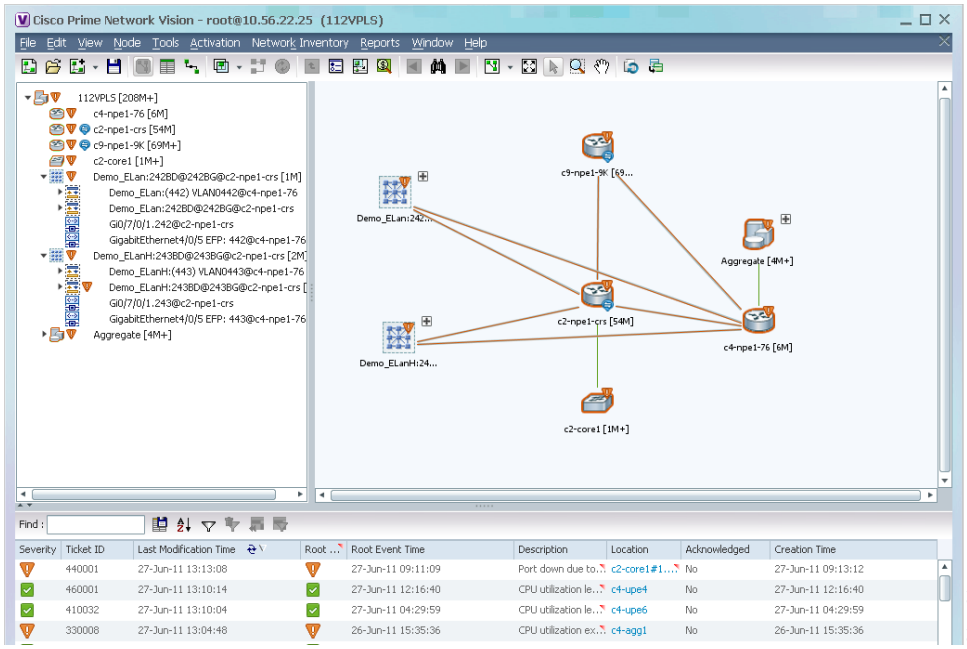
For information about sorting and filtering the table contents, see Working with Prime Network Tables, page 2-49.

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

Step 5 Click **OK**.

The VPLS instance is displayed in the navigation pane and in the content area. In addition, any associated tickets are displayed in the ticket pane. See Figure 12-41.

Figure 12-41 VPLS Instance in Prime Network Vision Map



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

Applying VPLS Instance Overlays

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

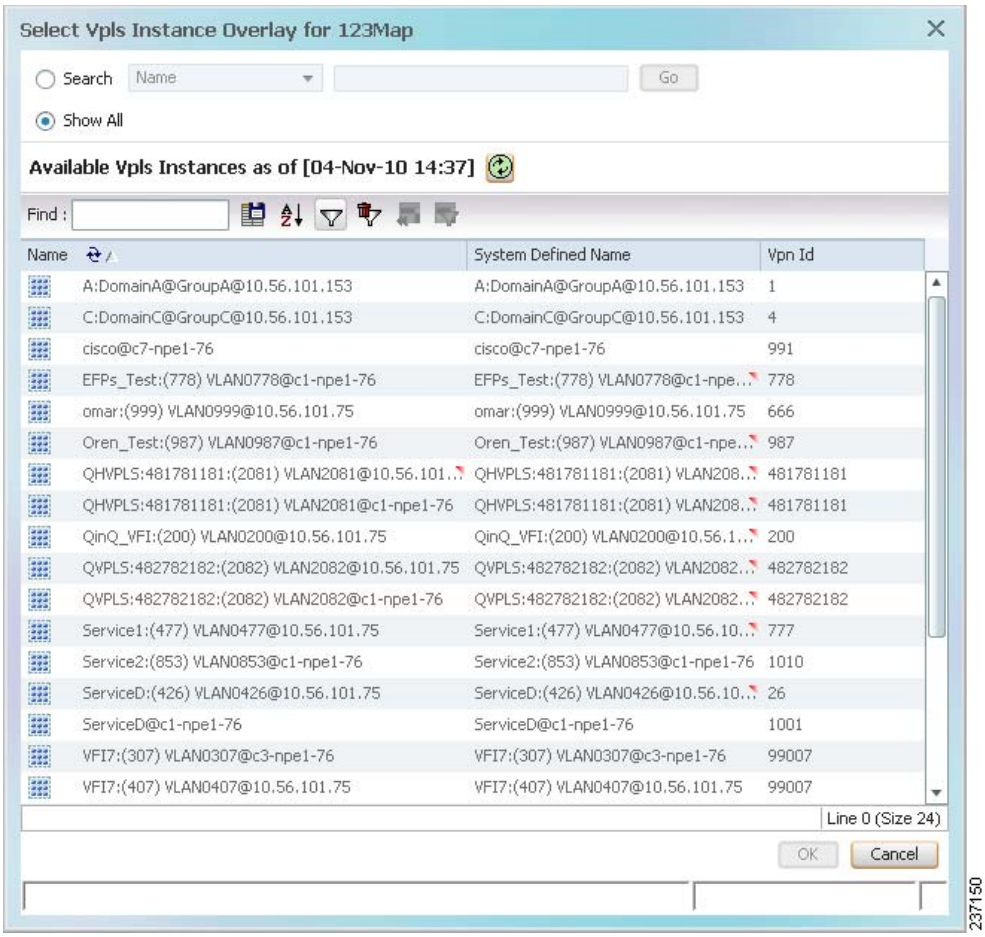
To apply a VPLS instance overlay:

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

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

Figure 12-42 shows an example of the Select VPLS Instance Overlay for *map* dialog box.

Figure 12-42 Select VPLS Instance Overlay Dialog Box

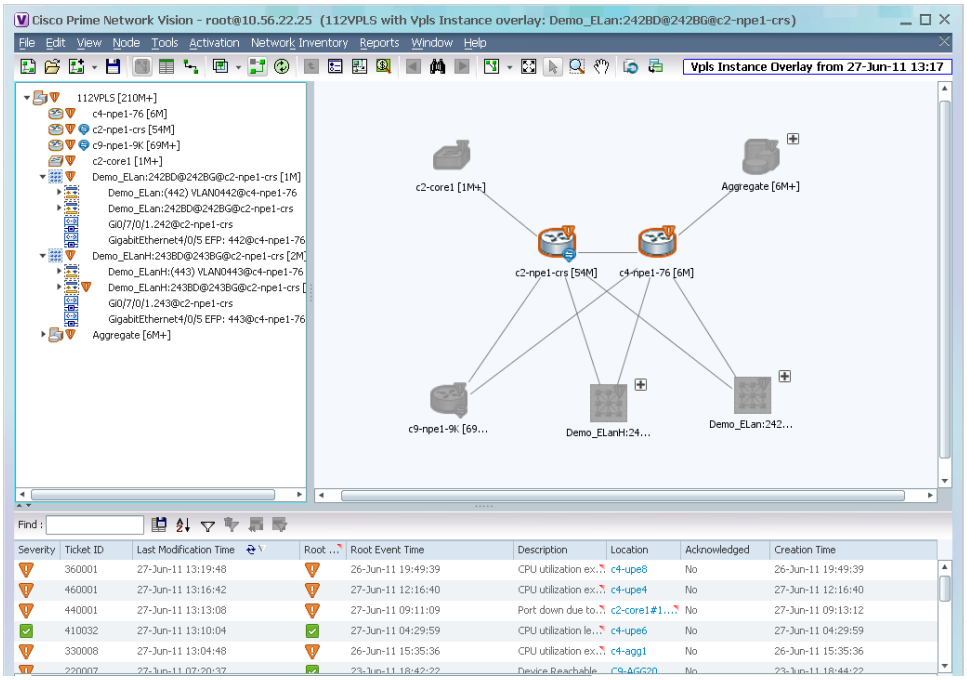


Step 3 Select the required VPLS instance for the overlay.

Step 4 Click **OK**.

The elements being used by the selected VPLS instance are highlighted in the map while the other elements are dimmed, as shown in Figure 12-43.

Figure 12-43 VPLS Instance Overlay in Prime Network Vision



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

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

Viewing Pseudowire Tunnel Links in VPLS Overlays

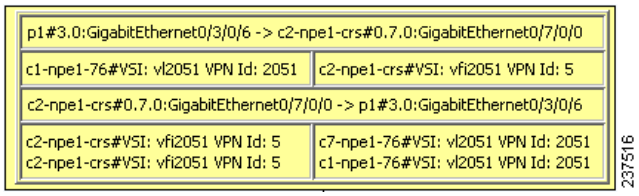
When a VPLS overlay is applied to a map in Prime Network Vision, you can view the details of the pseudowires that are interconnected through selected links.

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

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

Link information is displayed as shown in Figure 12-44.

Figure 12-44 Link Callout Window for a VPLS Overlay



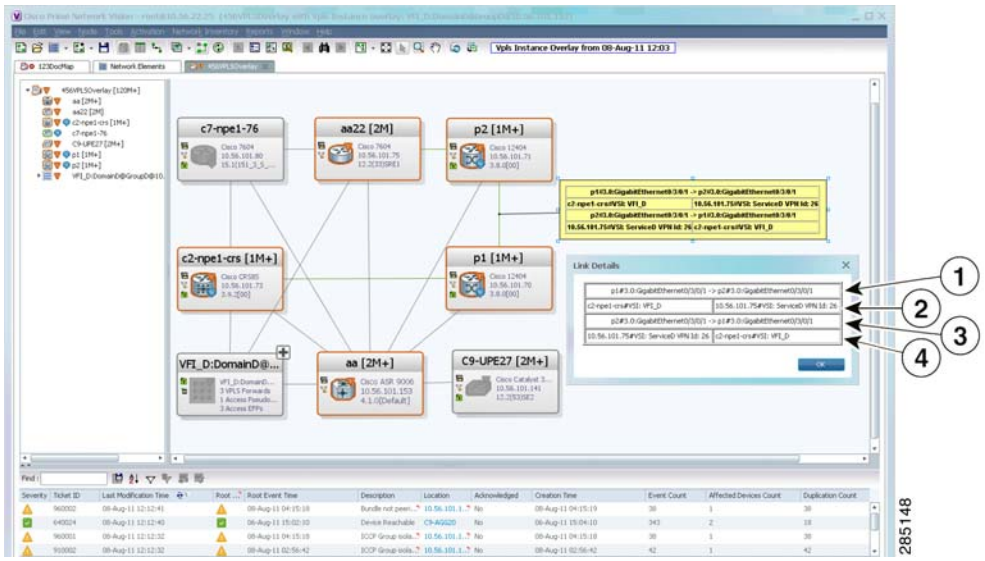
The callout window displays the following information for each link represented by the selected link:

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

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

The details about the link are displayed in the Link Details window as shown in Figure 12-45.

Figure 12-45 Link Details Window for a VPLS Overlay



The Link Details window provides the following information:

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

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

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

Viewing VPLS-Related Properties

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

- VPLS instances—See Viewing VPLS Instance Properties, page 12-81.
- Virtual Switching Instances—Viewing Virtual Switching Instance Properties, page 12-83
- Tunnels—See Viewing VPLS Core or Access Pseudowire Endpoint Properties, page 12-85.
- Port connectors—See Viewing VPLS Access Ethernet Flow Point Properties, page 12-87.

Viewing VPLS Instance Properties

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

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

Figure 12-46 shows an example of the VPLS Instance Properties window.

Figure 12-46 VPLS Instance Properties Window

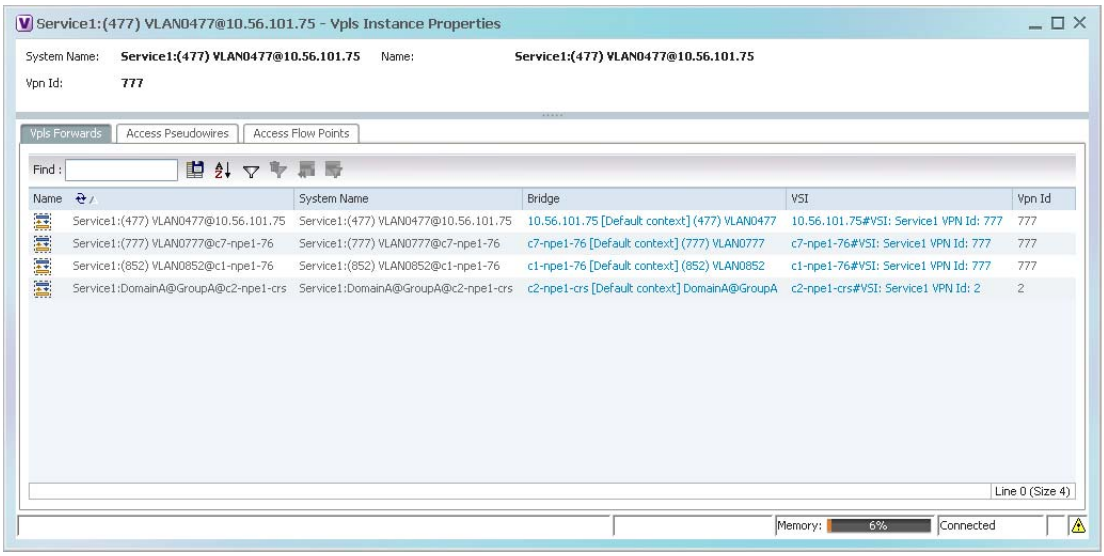


Table 12-35 describes the information that is displayed for VPLS instance properties.

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

Table 12-35 VPLS Instance Properties

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

Table 12-35 VPLS Instance Properties (continued)

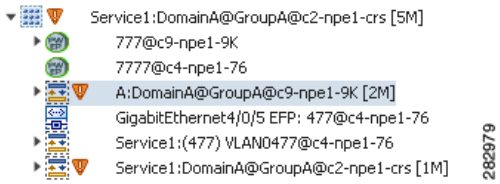
Field	Description
Access Pseudowires Tab	
Name	Pseudowire name.
Port	VSI on which the pseudowire is configured, hyperlinked to the entry in logical inventory.
Local Router IP	Local router IP address on which the pseudowire is configured.
Tunnel ID	Virtual circuit identifier of the pseudowire.
PTP Tunnel	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: • 0—Unknown • 1—Connection termination point • 2—Ethernet flow point • 3—Switching entity • 4—Pseudowire switching entity • 5—VPLS forward
Access Flow Points Tab	
Name	Access flow point name. Double-click to view port connector properties.
Port	Interface configured as a flow point, hyperlinked to the interface in physical inventory.

Viewing Virtual Switching Instance Properties

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

- Double-click the required device and, in the inventory window, choose **Logical Inventory > VSIs >** *vsi*.
- In the navigation pane, expand the VPLS instance, right-click the required VPLS forward, and choose **Inventory** or **Properties**. (See Figure 12-47.)

Figure 12-47 VPLS Forward in Prime Network Vision Navigation Pane



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

VSI properties are displayed as shown in Figure 12-48.

Figure 12-48 VSI Properties in Logical Inventory

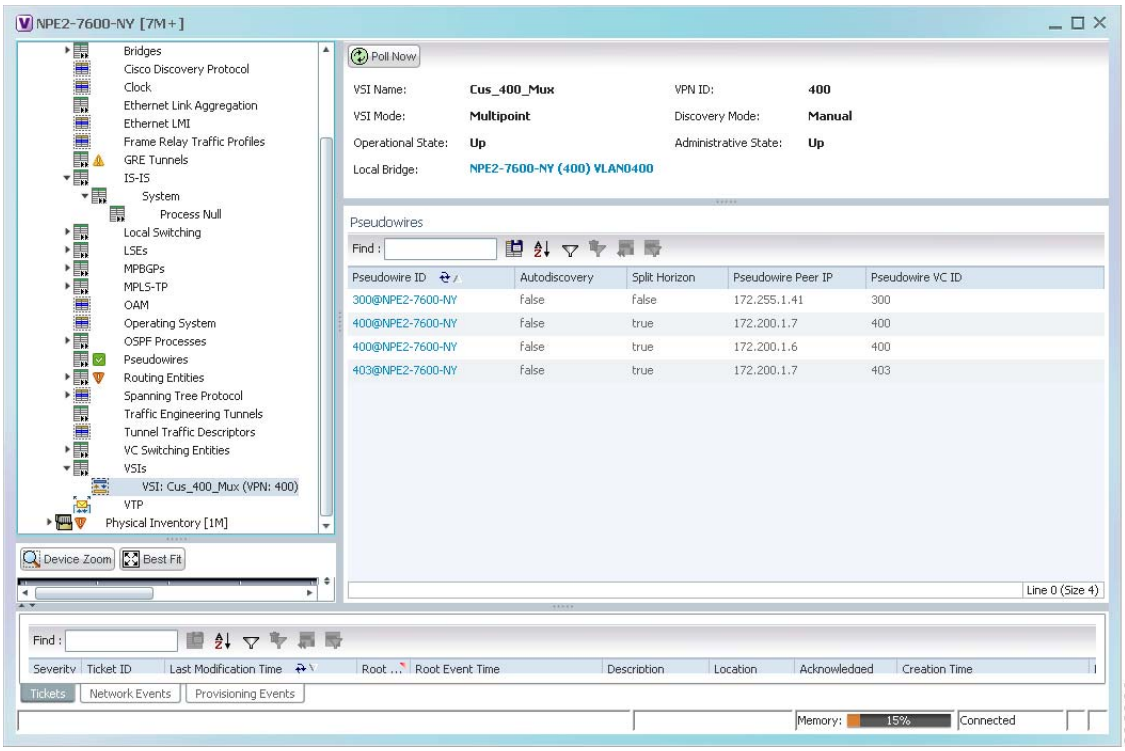


Table 12-36 describes the information that is displayed for the selected VSI.

Table 12-36 VSI Properties in Logical Inventory

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

Viewing VPLS Core or Access Pseudowire Endpoint Properties

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

To view pseudowire endpoint properties for a VPLS instance, right-click the required pseudowire endpoint in the navigation pane, and choose **Properties**. (See Figure 12-49.)

Figure 12-49 VPLS Pseudowire in Prime Network Vision Navigation Pane

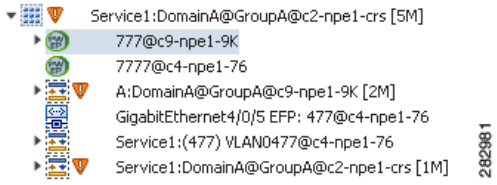


Figure 12-50 shows an example of the Tunnel Properties window that is displayed.

Figure 12-50 VPLS Tunnel Properties Window

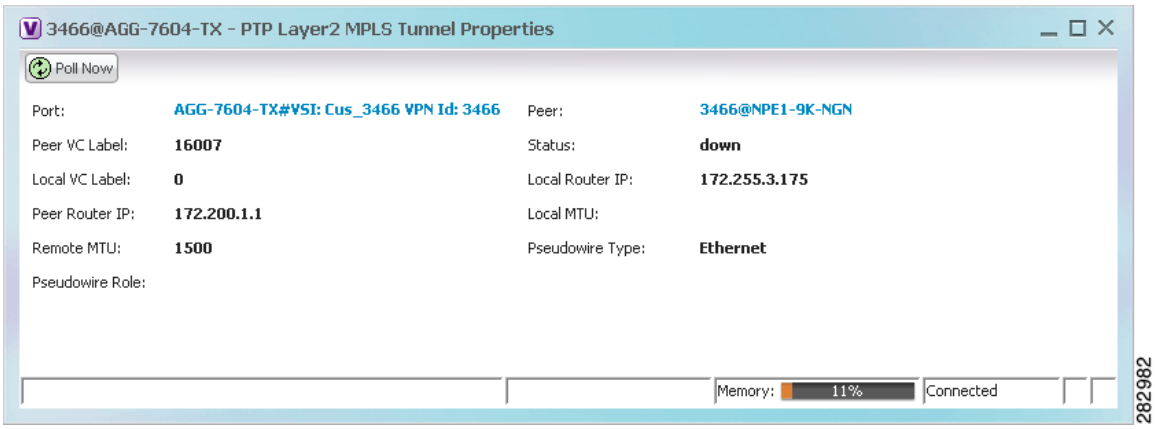


Table 12-37 describes the information that is displayed for pseudowire endpoint properties.

Table 12-37 Tunnel Properties Window

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

Viewing VPLS Access Ethernet Flow Point Properties

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

To view the properties for the Access Ethernet Flow Points configured for a VPLS instance, right-click the required interface in the navigation pane, and choose **Inventory**. (See Figure 12-51.)

Figure 12-51 VPLS Interface in Prime Network Vision Navigation Pane

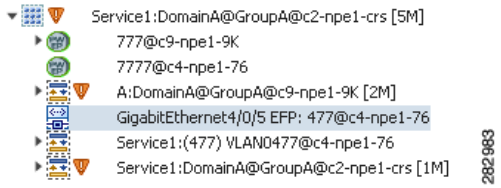
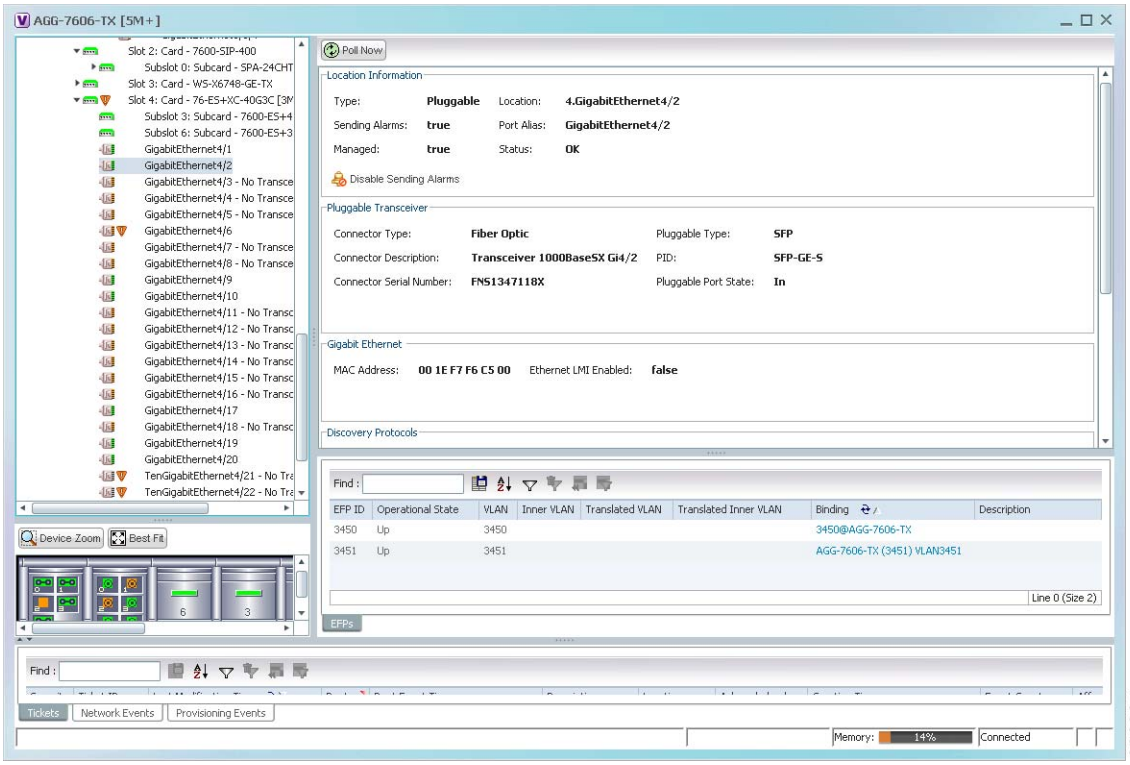


Figure 12-52 shows an example of the information displayed for the interface in physical inventory.

Figure 12-52 EFP Properties in Physical Inventory



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

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

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

- List of the configured subinterfaces on the port. For more information on the Subinterfaces table, see Viewing a Port Configuration, page 3-24.
- List of the configured EFPs on the port. For more information on the EFPs table, see Viewing EFP Properties, page 12-31.
- List of VLAN mappings configured on the port. For more information about the VLAN Mappings table, see Viewing VLAN Mappings, page 12-50.

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.

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

- Adding Pseudowires to a Map, page 12-88
- Viewing Pseudowire Properties, page 12-91
- Pinging a Pseudowire, page 12-94
- Displaying Pseudowire Information, page 12-96
- Viewing Pseudowire Redundancy Service Properties, page 12-98
- Applying Pseudowire Overlays, page 12-100

Adding Pseudowires to a Map

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

To add a pseudowire to a map:

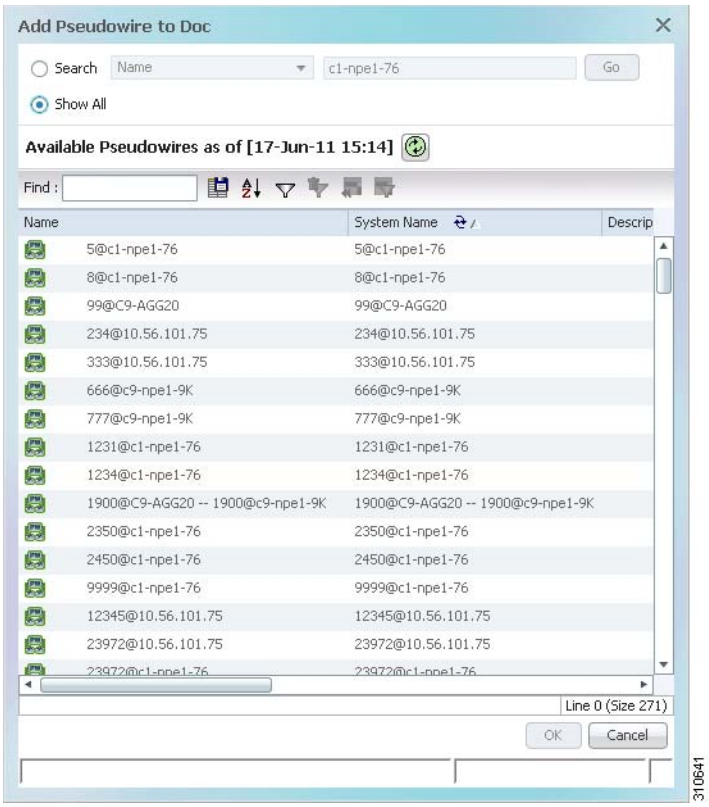
Step 1 In Prime Network Vision, select the required map or domain.

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

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

Figure 12-53 shows an example of the Add Pseudowire dialog box.

Figure 12-53 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.

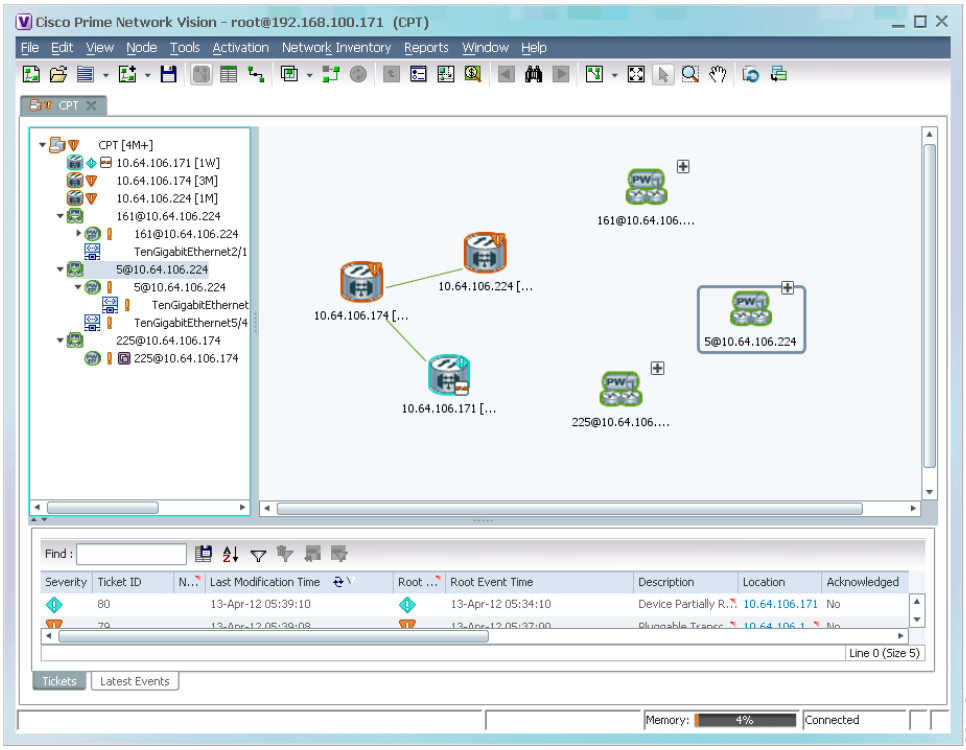
For information about sorting and filtering the table contents, see Working with Prime Network Tables, page 2-49.

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

Step 5 Click **OK**.

The pseudowire is displayed in the navigation pane and in the content area. In addition, any associated tickets are displayed in the ticket pane. See Figure 12-54.

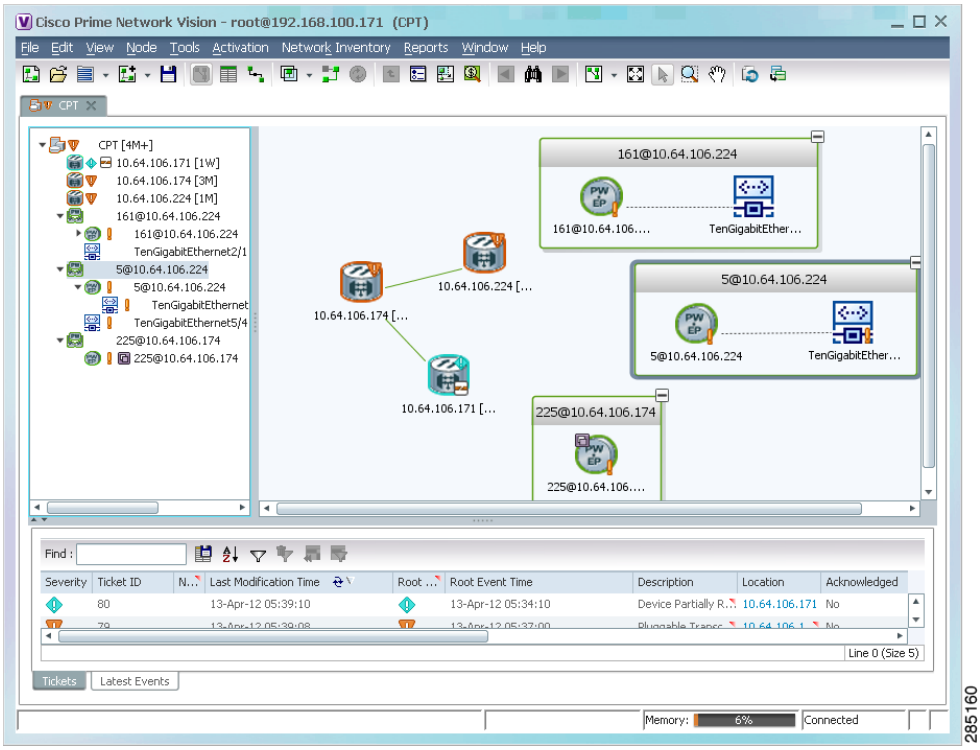
Figure 12-54 Pseudowire in Prime Network Vision Map



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

Figure 12-55 shows an example of an expanded pseudowire in Prime Network Vision.

Figure 12-55 Pseudowire Components in Prime Network Vision Maps



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

Viewing Pseudowire Properties

To view pseudowire properties:

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

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

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

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

The Tunnel Edges table is displayed, listing the pseudowire endpoints configured on the selected element. For a description of the information contained in the Pseudowires Tunnel Edges table, see Table 17-24 on page 17-48.

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

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

The Pseudowire Properties window is displayed as shown in Figure 12-56.

Figure 12-56 Pseudowire Properties Window

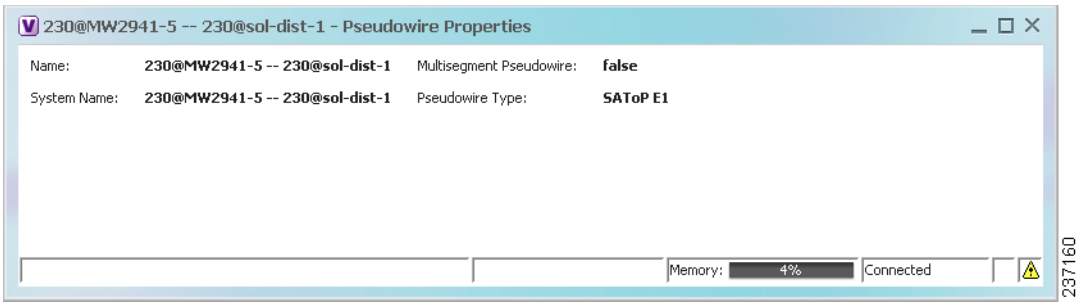


Table 12-38 describes the information presented in the Pseudowire Properties window.

Table 12-38 Pseudowire Properties Window

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

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

The Tunnel Properties window containing the pseudowire endpoint properties is displayed as shown in Figure 12-50 and described in Table 12-37.

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

The Local Switching table is displayed as shown in Figure 12-40.

Table 12-34 describes the information displayed in the Local Switching table.

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

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

Table 12-39 describes the information displayed in the Contained Current CTPs table.

Table 12-39 Contained Current CTPs Table

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

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

See Viewing EFP Properties, page 12-31 for the information that is displayed for EFPs.

Pinging a Pseudowire

Prime Network Vision enables you to ping a peer router to ensure that the pseudowire tunnel is available.

To ping a pseudowire peer router:

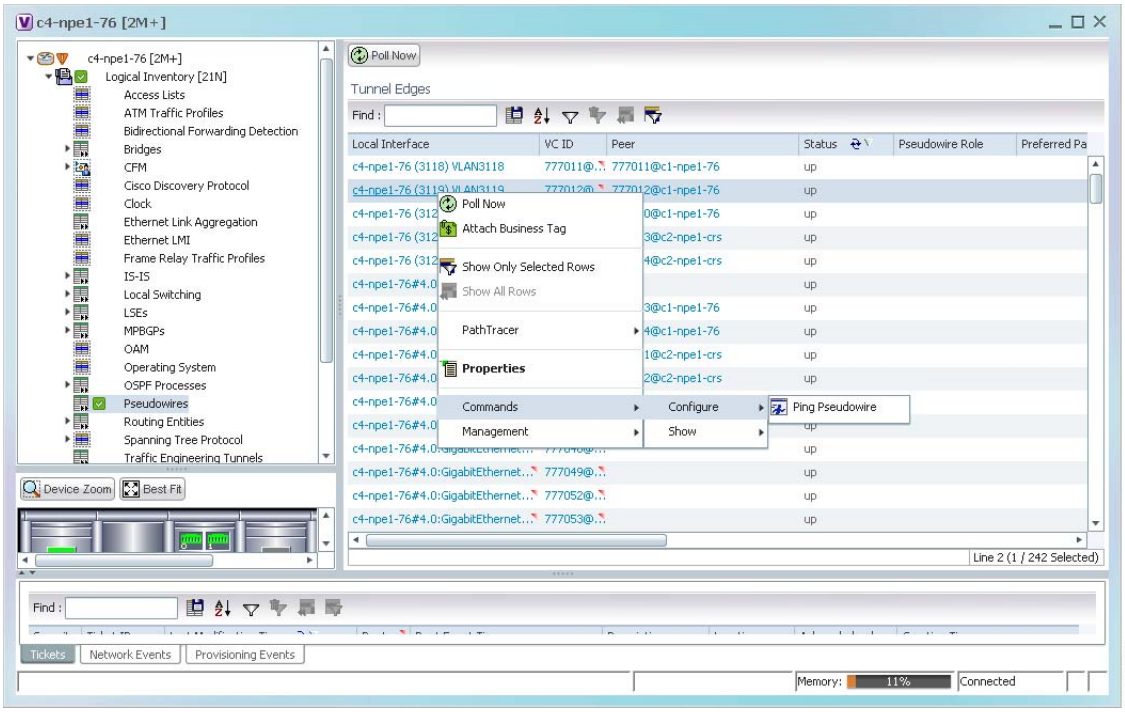
Step 1 In the require map, double-click the required device configured for pseudowire.

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

Step 3 In the Tunnel Edges table, select the interface with the peer edge that you want to ping, and make sure that the tunnel status is up.

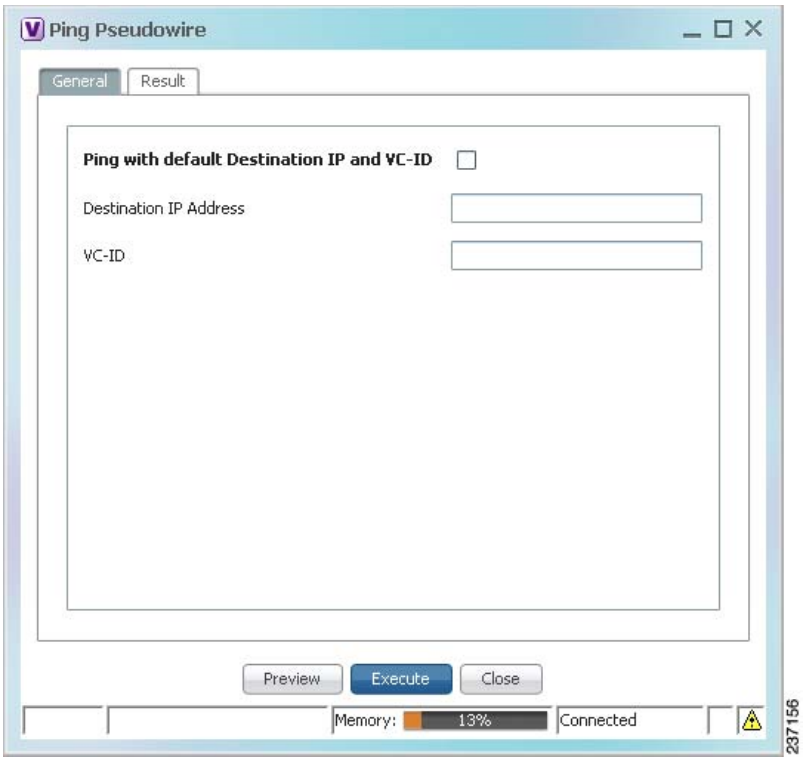
Step 4 Right-click the interface and choose **Commands > Configure > Ping Pseudowire** as shown in Figure 12-57.

Figure 12-57 Ping Pseudowire Command



The Ping Pseudowire dialog box is displayed with the General tab as shown in Figure 12-58.

Figure 12-58 Ping Pseudowire Dialog Box - General Tab



Step 5 In the General tab, specify the destination as follows:

- Ping with default Destination IP and VC-ID—Check the check box to ping the selected peer pseudowire endpoint using the default destination IP address and VC identifier. You do not need to enter a destination IP address or tunnel identifier if you choose this option.
- Destination IP Address—Enter the required destination IP address if you do not want to use the default destination IP address. If you enter a destination IP address, you must enter the tunnel identifier in the VC-ID field.
- VC-ID—Enter the required tunnel identifier if you do not want to use the default VC identifier. If you enter a tunnel identifier, you must enter the destination IP address in the Destination IP Address field.

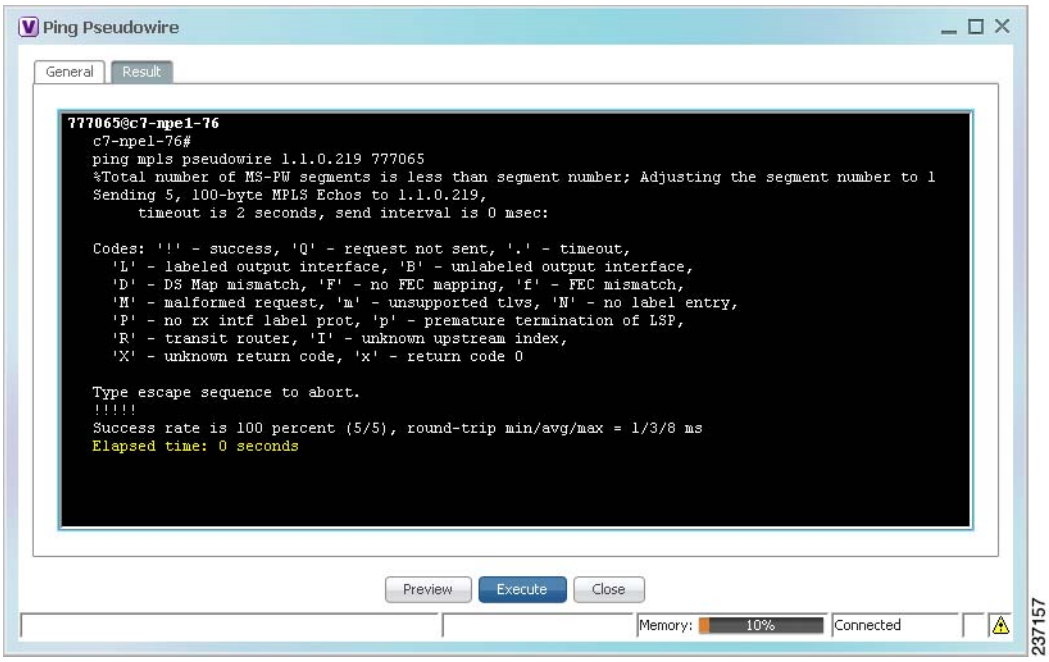
Step 6 To preview the command to ensure it is right, click **Preview**.

The command is displayed in the Result tab for your review.

Step 7 To execute the command, click **Execute**.

The result of the command is displayed in the Result tab, as shown in Figure 12-59.

Figure 12-59 Ping Pseudowire Dialog Box - Result Tab



Step 8 Click **Close** to close the Ping Pseudowire dialog box.

Displaying Pseudowire Information

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

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

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

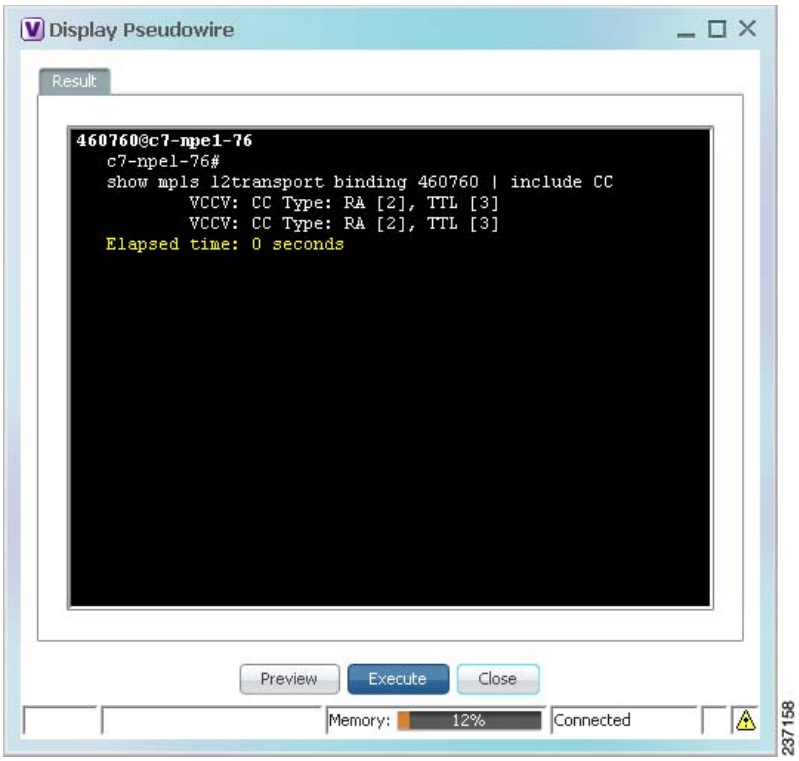
Step 3 In the Tunnel Edges table, right-click the required interface and choose **Commands > Show > Display Pseudowire**.

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

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

When you click **Execute**, the results are displayed in the dialog box as shown in Figure 12-60.

Figure 12-60 Display Pseudowire Dialog Box



Step 5 The following information is displayed:

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

    - CW [1]—Control Word

    - RA [2]—Router Alert

    - TTL [3]—Time to Live

    - Unkn [x]—Unknown

  - Elapsed time—The elapsed time, in seconds.

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

Viewing Pseudowire Redundancy Service Properties

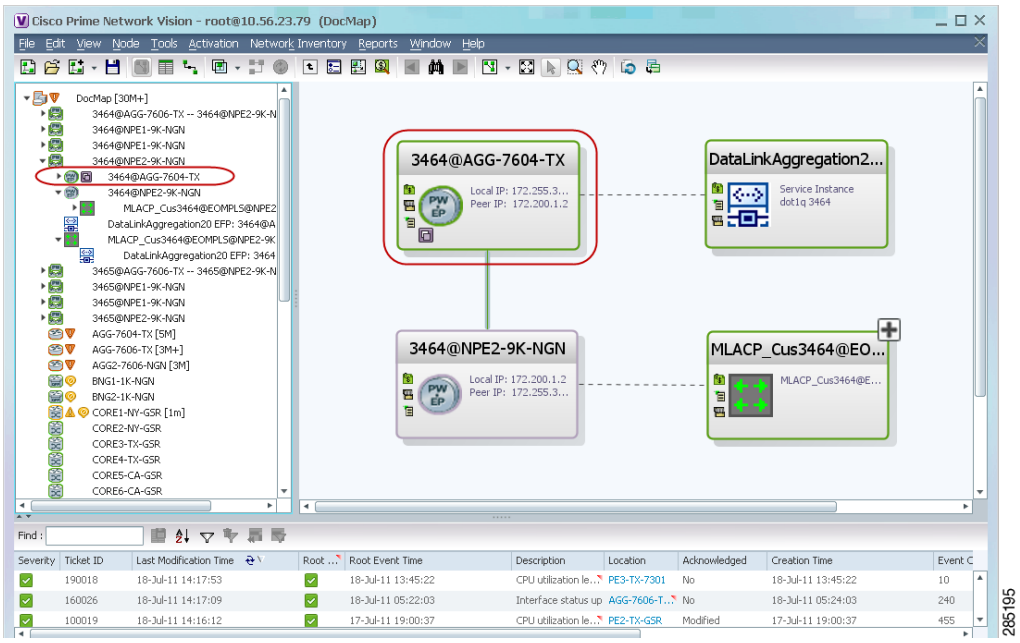
If a pseudowire is configured for redundancy service, a redundancy service badge is applied to the secondary (backup) pseudowire in the navigation and map panes in the Prime Network Vision window. Additional redundancy service details are provided in the inventory window for the device on which the pseudowire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

To view redundancy service properties for pseudowires:

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

If the pseudowire is configured for redundancy service, the redundancy service badge appears in the navigation and map panes as shown in Figure 12-61.

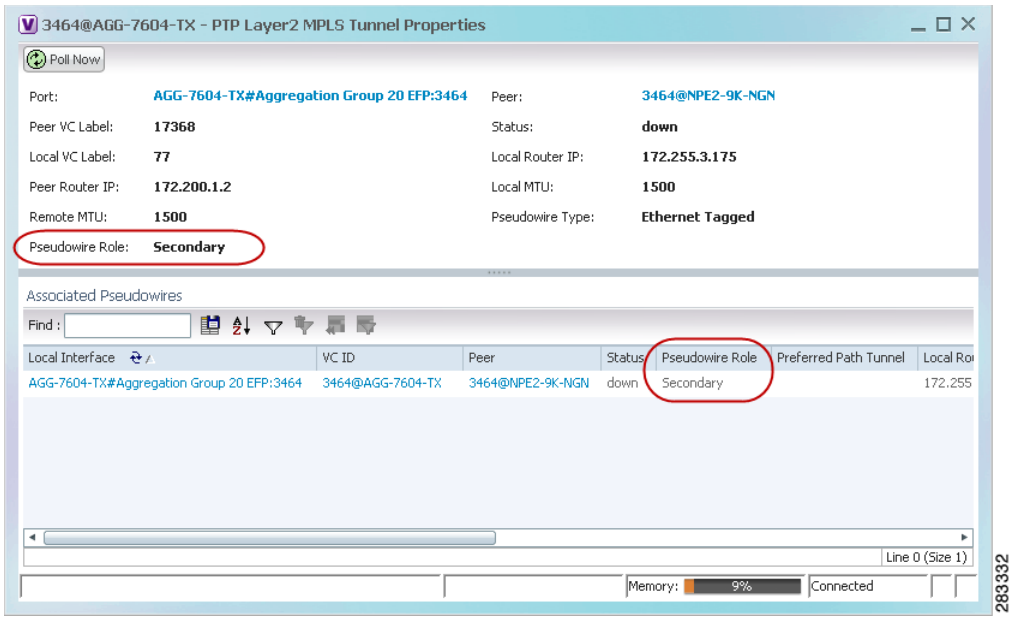
Figure 12-61 Pseudowire Redundancy Service Badge in a Map



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

The PTP Layer 2 MPLS Tunnel Properties window is displayed as shown in Figure 12-62 and shows that the selected pseudowire has a Secondary role in a redundancy service.

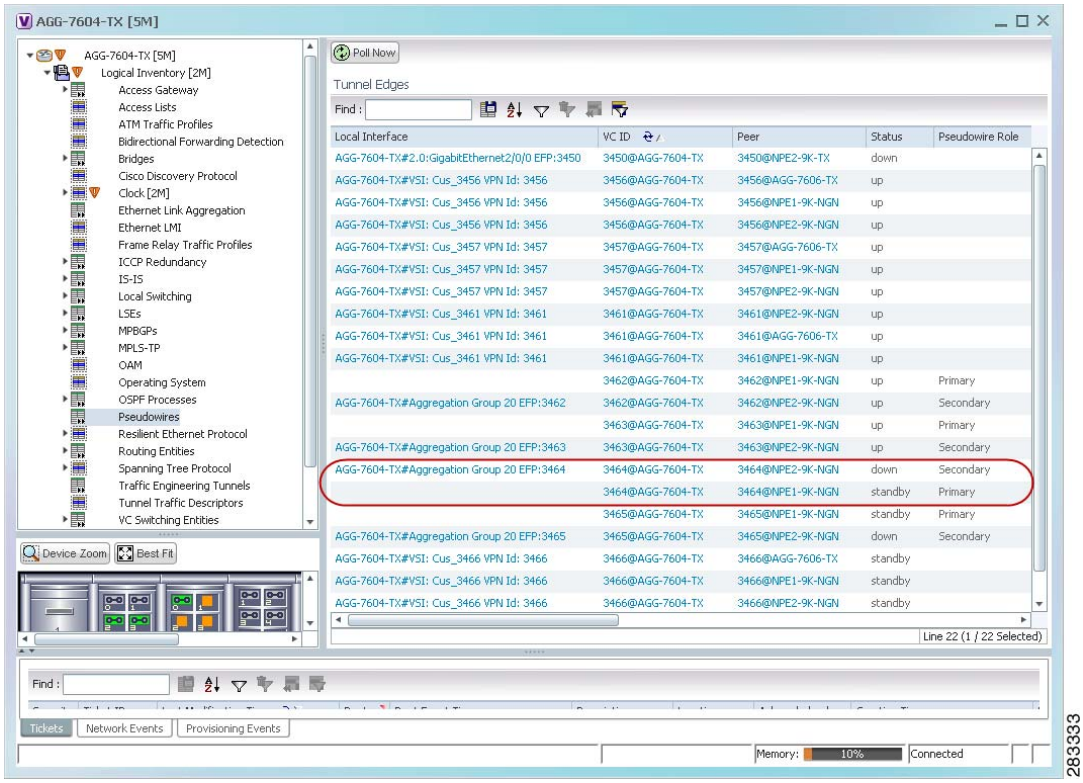
Figure 12-62 Layer 2 MPLS Tunnel Properties for Pseudowire Redundancy Service



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

The Tunnel Edges table in logical inventory is displayed, with the local interface selected in the table. (See Figure 12-63.)

Figure 12-63 Pseudowire Redundancy Service in Logical Inventory



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

For more information about the Pseudowires Tunnel Edges table, see Table 17-24 on page 17-48.

Applying Pseudowire Overlays

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

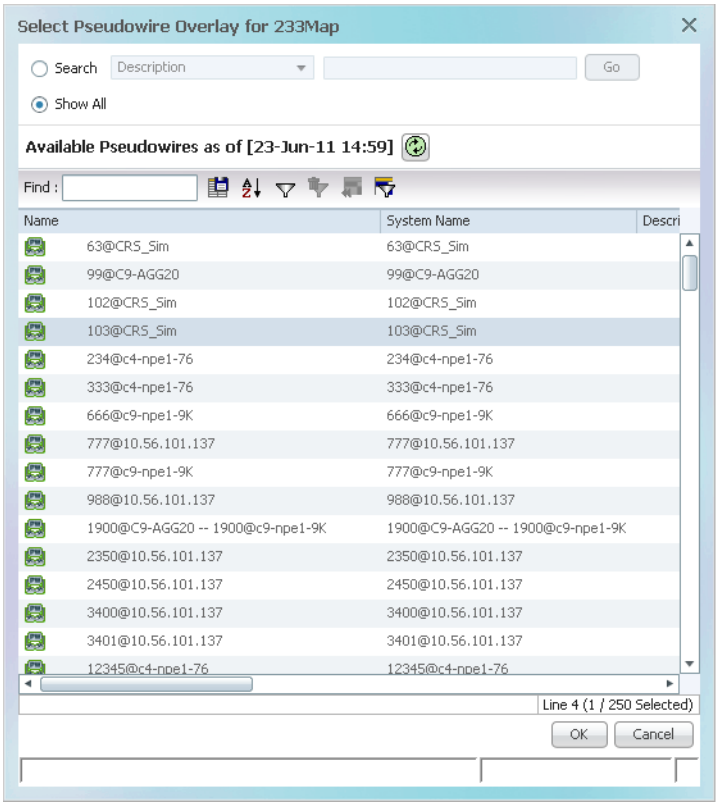
To apply a pseudowire overlay:

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

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

Figure 12-64 shows an example of the Select Pseudowire Overlay for *map* dialog box.

Figure 12-64 Select Pseudowire Overlay Dialog Box

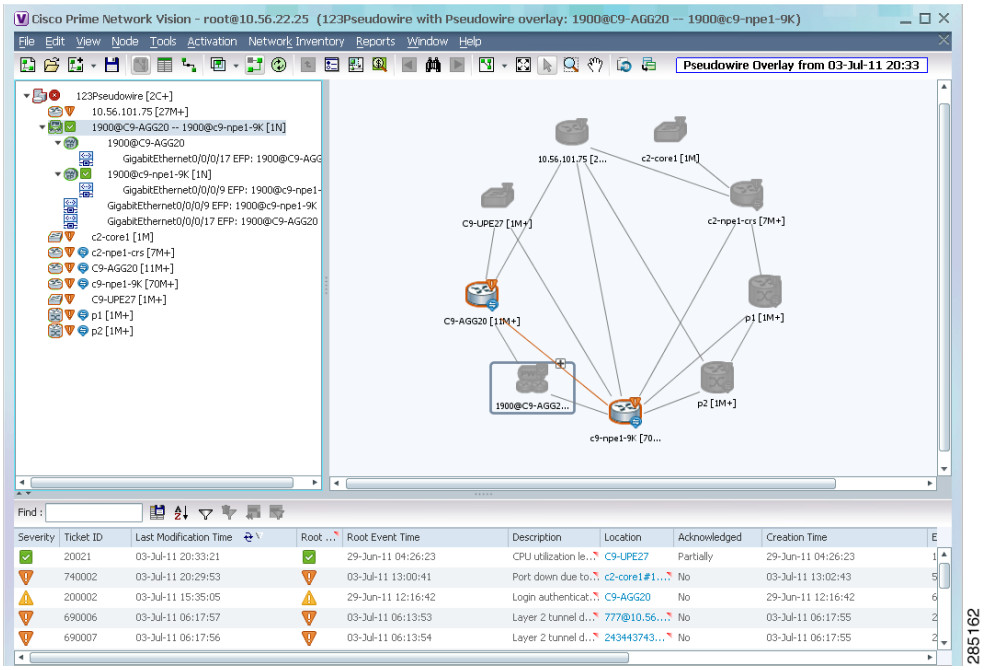


Step 3 Select the required pseudowire for the overlay.

Step 4 Click **OK**.

The elements being used by the selected pseudowire are highlighted in the map while the other elements are dimmed, as shown in Figure 12-65.

Figure 12-65 Pseudowire Overlay in Prime Network Vision



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

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

Working with Ethernet Services

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

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

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

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

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

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

- Adding Ethernet Services to a Map, page 12-102
- Applying Ethernet Service Overlays, page 12-104
- Viewing Ethernet Service Properties, page 12-105

Adding Ethernet Services to a Map

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

To add an Ethernet service to a map:

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

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

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

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

- To search for specific elements:

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

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

  c. Click **Go**.

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

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

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

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

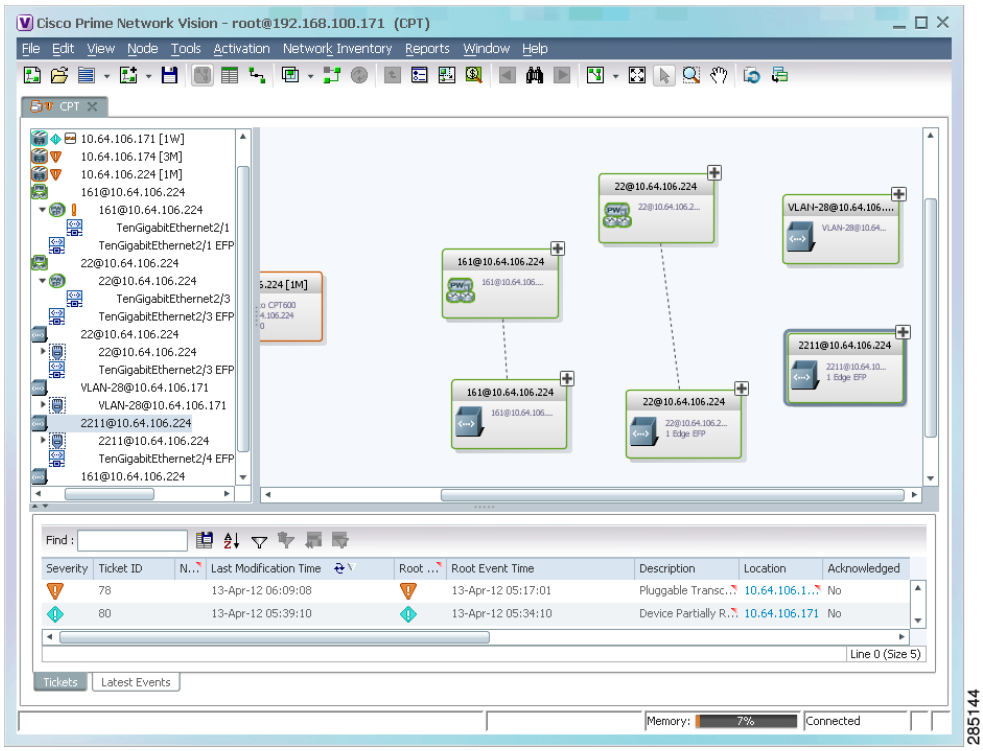
For information about sorting and filtering the table contents, see Working with Prime Network Tables, page 2-49.

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

Step 5 Click **OK**.

The Ethernet service is displayed in the navigation pane and in the content area. In addition, any associated tickets are displayed in the ticket pane. See Figure 12-66.

Figure 12-66 Ethernet Service in Prime Network Vision



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

Applying Ethernet Service Overlays

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

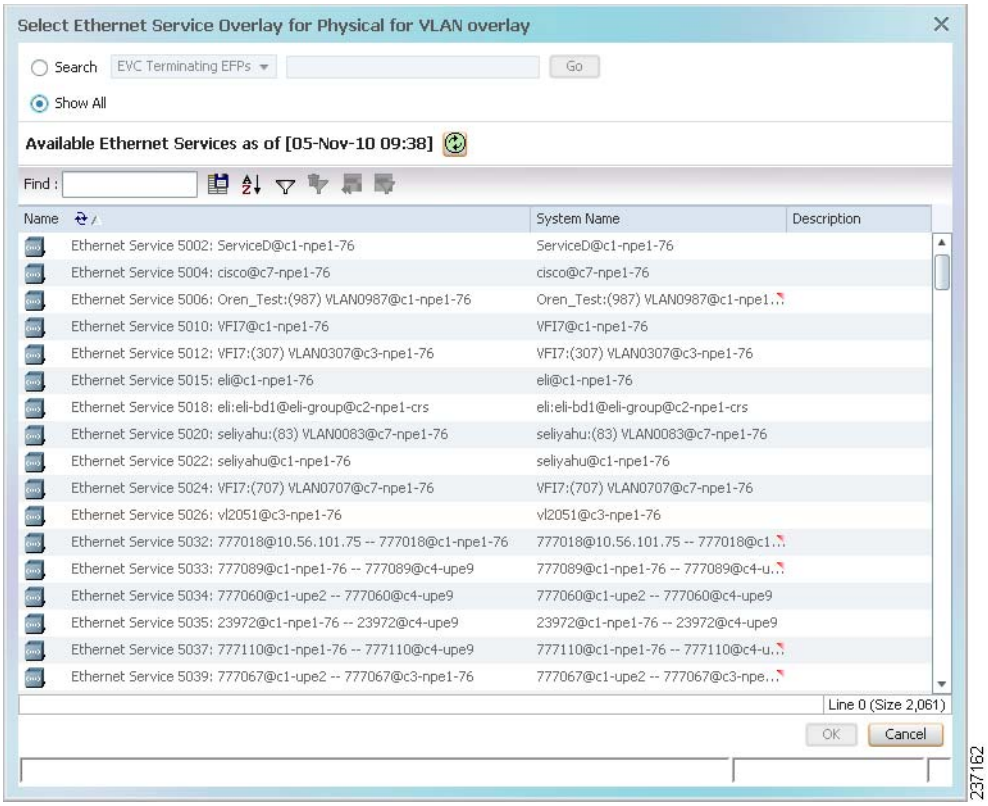
To apply an Ethernet service overlay:

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

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

Figure 12-67 shows an example of the Select Ethernet Service Overlay for *map* dialog box.

Figure 12-67 Select Ethernet Service Overlay Dialog Box

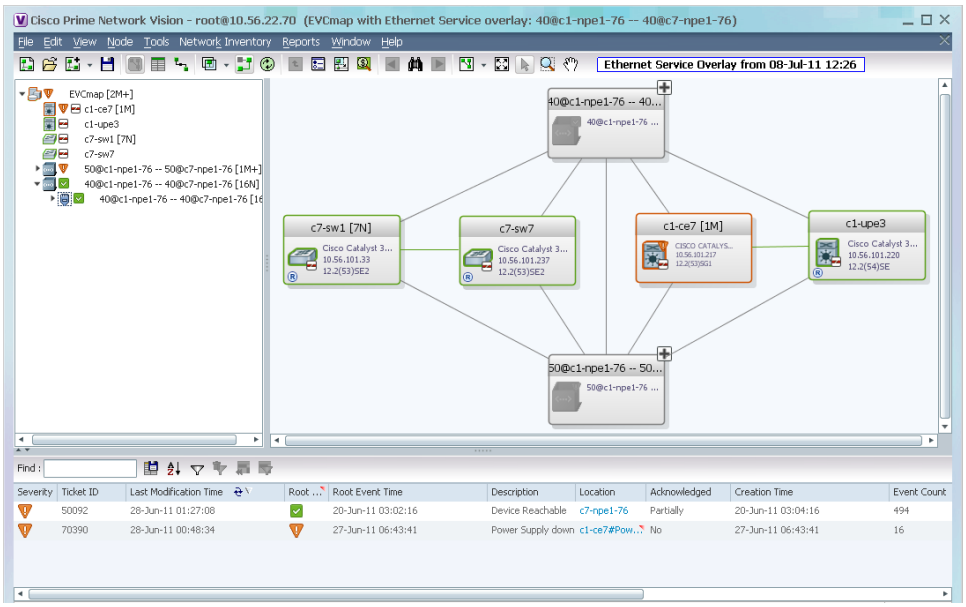


Step 3 Select the required Ethernet Service for the overlay.

Step 4 Click **OK**.

The elements being used by the selected Ethernet service are highlighted in the map while the other elements are dimmed, as shown in Figure 12-68.

Figure 12-68 Ethernet Service Overlay in Prime Network Vision



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

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

Viewing Ethernet Service Properties

To view Ethernet service properties:

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

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

Figure 12-69 shows an example of an Ethernet Service Properties window with the EVC Terminating table. Depending on the types of service in the EVC, tabs might be displayed. For example, if the EVC contains two network VLANs and a VPLS, tabs are displayed for the following:

- EVC Terminating table
- Network VLANs
- VPLS

Figure 12-69 Ethernet Service Properties Window

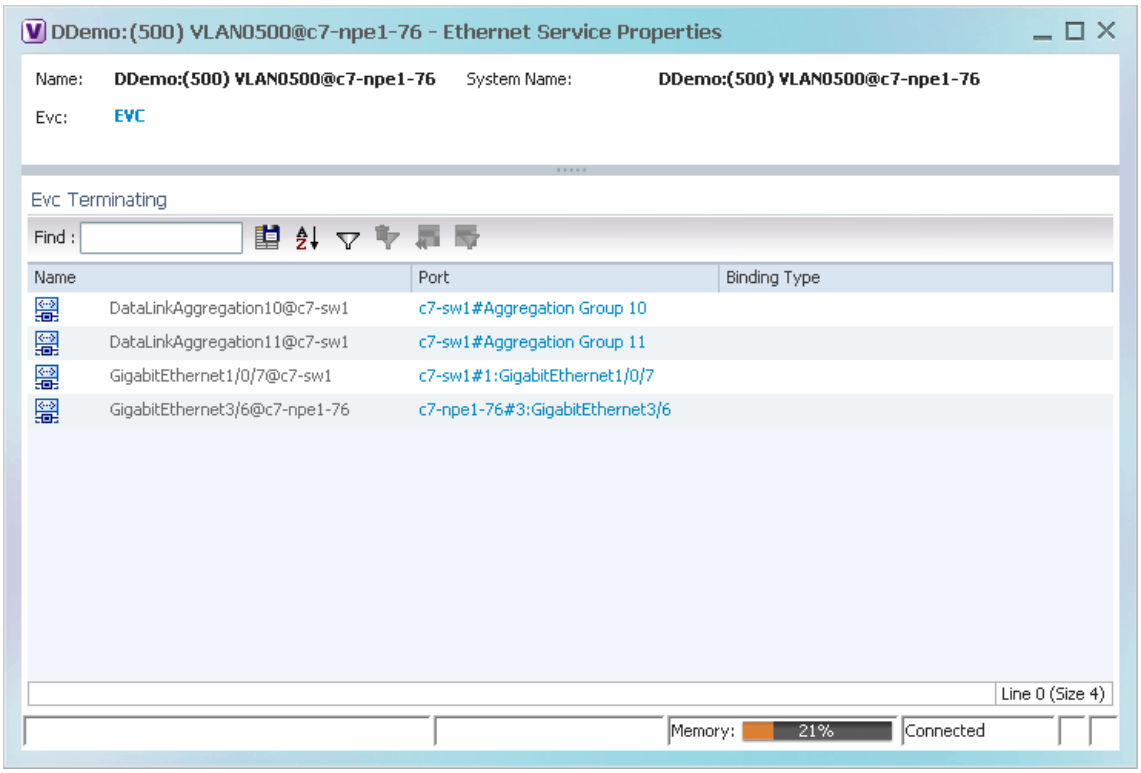


Table 12-40 describes the information that is displayed for an Ethernet service.

Table 12-40 Ethernet Service Properties Window

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

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

Figure 12-70 shows an example of the EVC Properties window.

Figure 12-70 EVC Properties Window

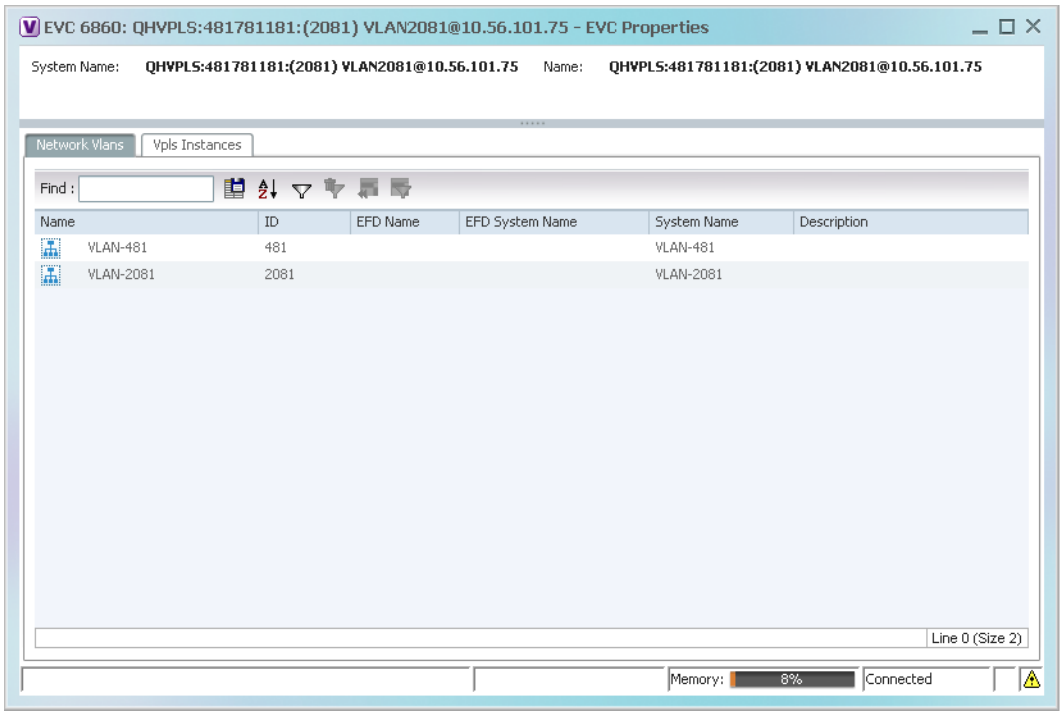


Table 12-41 describes the information that is displayed in the EVC Properties window. The tabs that are displayed depend on the services included in the EVC. For example, if the EVC contains two network VLANs and a VPLS, tabs are displayed for the following:

- EVC Terminating table
- Network VLANs
- VPLS

Table 12-41 EVC Properties Window

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

Table 12-41 EVC Properties Window (continued)

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

Viewing IP SLA Responder Service Properties

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

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

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

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

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

To view IP SLA Responder service properties:

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

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

IP SLA Responder properties are displayed as shown in Figure 12-71.

Figure 12-71 IP SLA Responder in Logical Inventory

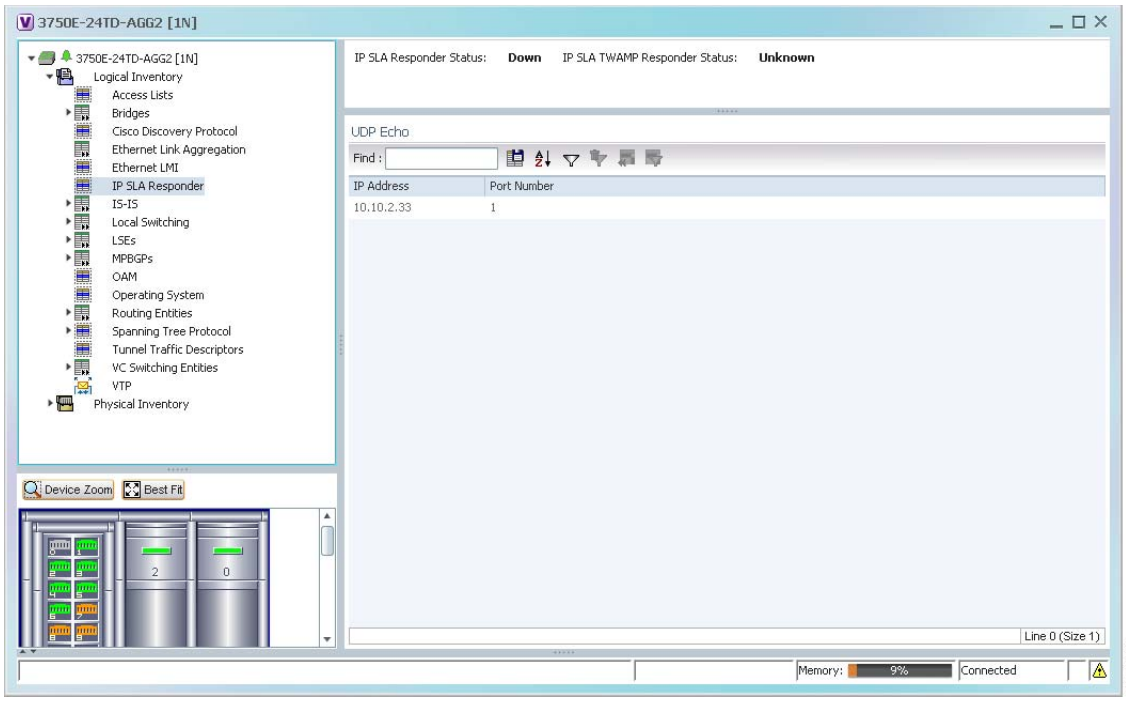


Table 12-42 describes the properties displayed for IP SLA Responder service.

Table 12-42 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.

To view IS-IS properties:

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

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

Figure 12-72 shows an example of the IS-IS window with the Process table in logical inventory.

Figure 12-72 IS-IS Window in Logical Inventory

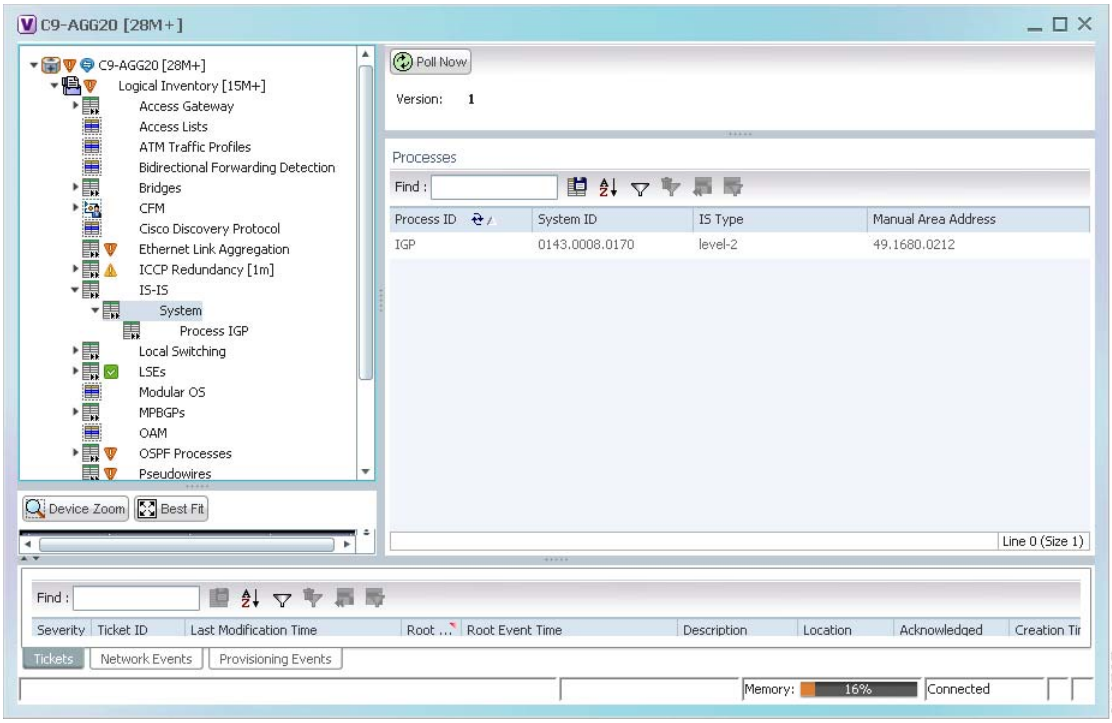


Table 12-43 describes the information that is displayed in this window and the Processes table.

Table 12-43 IS-IS Properties in Logical Inventory - Processes Table

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

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

Figure 12-73 shows an example of the information that is displayed for the IS-IS process.

Figure 12-73 IS-IS Process Properties in Logical Inventory

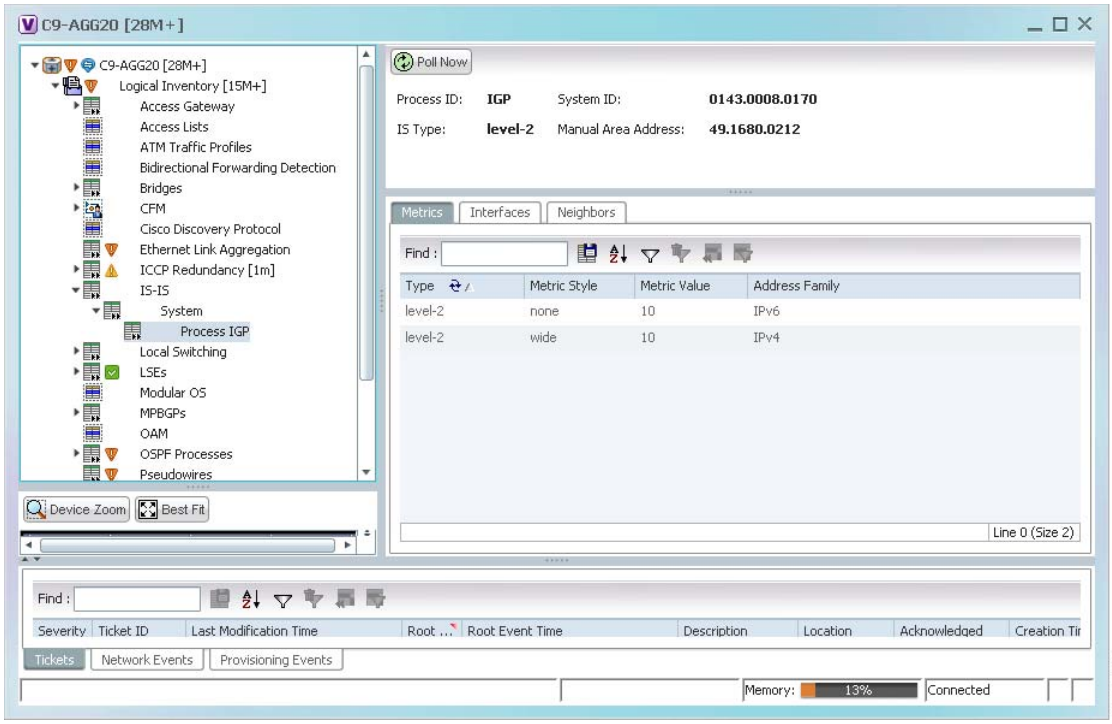


Table 12-44 describes the information that is displayed for the selected IS-IS process.

Table 12-44 IS-IS Process Properties in Logical Inventory

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

Viewing OSPF Properties

Prime Network Vision supports the following versions of OSPF:

- OSPFv1
- OSPFv2
- OSPFv3

Using Prime Network Vision you can view OSPF properties for:

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

To view OSPF properties:

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

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

For example, in Figure 12-74, the entry in the navigation tree is OSPF Process (v2) 10.

Figure 12-74 OSPF Processes in Logical Inventory

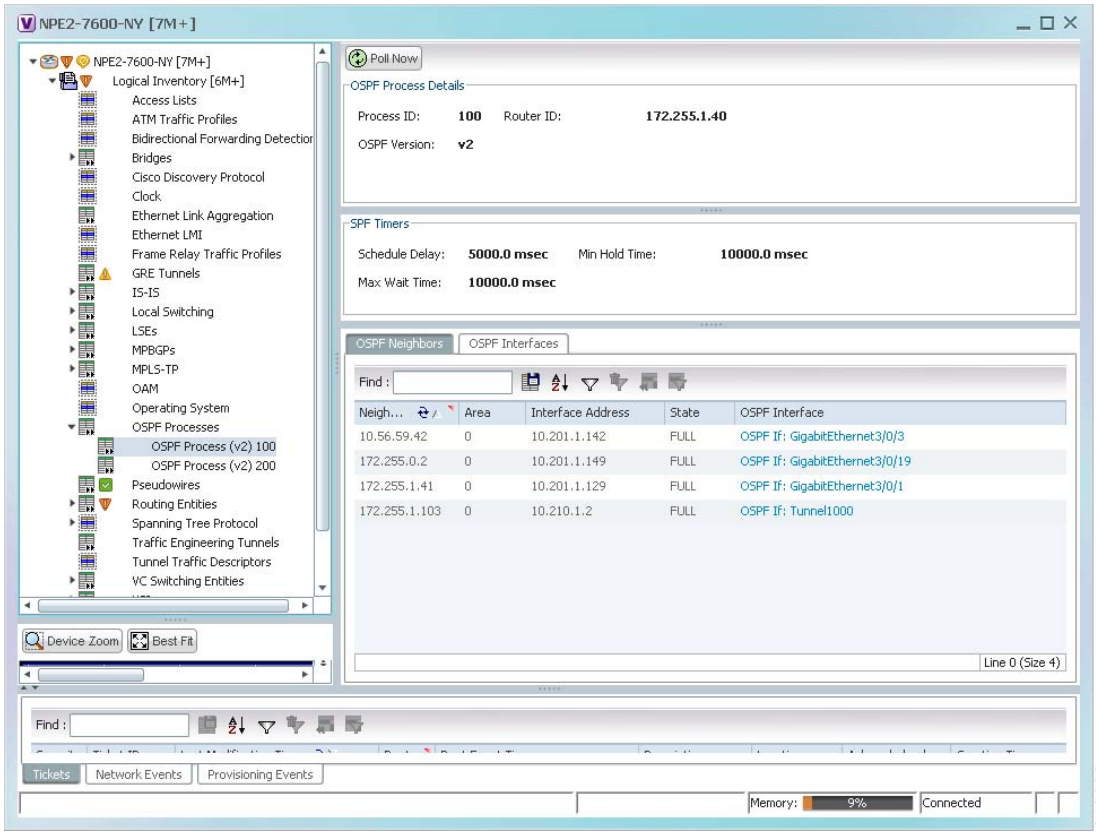


Table 12-45 describes the information that is displayed for OSPF processes.

Table 12-45 OSPF Processes in Logical Inventory

Field	Description
OSPF Process Details	
Process ID	Unique process identifier.
Router ID	Router IP address.
OSPF Version	OSPF version: v1, v2, or v3.
SPF Timers	
Schedule Delay	Number of milliseconds to wait after a change before calculating the shortest path first (SPF).
Min Hold Time	Minimum number of milliseconds to wait between two consecutive SPF calculations.
Max Wait Time	Maximum number of milliseconds to wait between two consecutive SPF calculations.
OSPF Neighbors Table	
Neighbor ID	OSPF neighbor IP address.
Area	OSPF area identifier.
Interface Address	IP address of the interface on the neighbor configured for OSPF.
State	State of the communication with the neighbor: Down, Attempt, Init, 2-Way, Exstart, Exchange, Loading, and Full.
OSPF Interface	Hyperlinked entry to the OSPF Interface Properties window. The OSPF Interfaces window displays the same information as the OSPF Interfaces Table below.
OSPF Interfaces Table	
IP Interface	OSPF interface, hyperlinked to the relevant entry in the routing entity IP Interfaces table in logical inventory. For more information about the IP Interfaces table, see Table 17-11.
Internet Address	OSPF interface IP address.
Area ID	OSPF area identifier.
Priority	Eight-bit unsigned integer that specifies the priority of the interface. Values range from 0 to 255. Of two routers, the one with the higher priority takes precedence.
Cost	Specified cost of sending a packet on the interface, expressed as a metric. Values range from 1 to 65535.
Status	State of the interface: Up or Down.
State	OSPF state: BDR, DR, DR-Other, Waiting, Point-to-Point, or Point-to-Multipoint.
Network Type	Type of OSPF network: Broadcast, Nonbroadcast Multiple Access (NBMA), Point-to-Multipoint, Point-to-Point, or Loopback.
DR Address	Designated router IP address.
BDR Address	Backup designated router IP address.



CHAPTER 13

Monitoring Carrier Grade NAT Properties

Carrier Grade NAT is a large-scale NAT, capable of providing private-IPv4-to-public-IPv4 translation in the order of millions of translations. Carrier Grade NAT can support several hundred thousand subscribers with the bandwidth throughput of at least 10Gb/s full-duplex. With IPv4 addresses reaching depletion, Carrier Grade NAT is vital in providing private IPv4 connectivity to the public IPv4 internet. In addition, Carrier Grade NAT is not limited to IPv4 NAT; it can also translate between IPv4 and IPv6 addresses.

Cisco Prime Network Vision (Prime Network Vision) supports Carrier Grade NAT on Cisco CRS routers containing a Cisco CRS-CGSE-PLIM card.

Note IPv4 Network Address Translation (NAT44) is not supported for devices running Cisco IOS XR software version 4.0.

The following topics describe using Prime Network Vision to view Carrier Grade NAT properties:

- User Roles Required to View Carrier Grade NAT Properties, page 13-1
- Viewing Carrier Grade NAT Properties in Logical Inventory, page 13-2
- Viewing Carrier Grade NAT Properties in Physical Inventory, page 13-5

User Roles Required to View Carrier Grade NAT Properties

This topic identifies the roles that are required to view Carrier Grade NAT properties in Prime Network Vision. Prime Network determines whether you are authorized to perform a task as follows:

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

For more information on user authorization, see the *Cisco Prime Network 3.9 Administrator Guide*.

The following tables identify the tasks that you can perform:

- Table 13-1 identifies the tasks that you can perform if a selected element **is not in** one of your assigned scopes.
- Table 13-2 identifies the tasks that you can perform if a selected element **is in** one of your assigned scopes.

By default, users with the Administrator role have access to all managed elements. To change the Administrator user scope, see the topic on device scopes in the *Cisco Prime Network 3.9 Administrator Guide*.

Table 13-1 Default Permission/Security Level Required for Viewing Carrier Grade NAT Properties - Element Not in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View Carrier Grade NAT properties	—	—	—	—	X

Table 13-2 Default Permission/Security Level Required for Viewing Carrier Grade NAT Properties - Element in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View Carrier Grade NAT properties	X	X	X	X	X

Viewing Carrier Grade NAT Properties in Logical Inventory

To view Carrier Grade NAT properties in logical inventory:

Step 1 In Prime Network Vision, double-click the Cisco CRS device configured for Carrier Grade NAT.

Step 2 In the inventory window, click **Logical Inventory > Carrier Grade NAT**.

The Carrier Grade NAT properties are displayed in logical inventory as shown in Figure 13-1.

Figure 13-1 Carrier Grade NAT in Logical Inventory

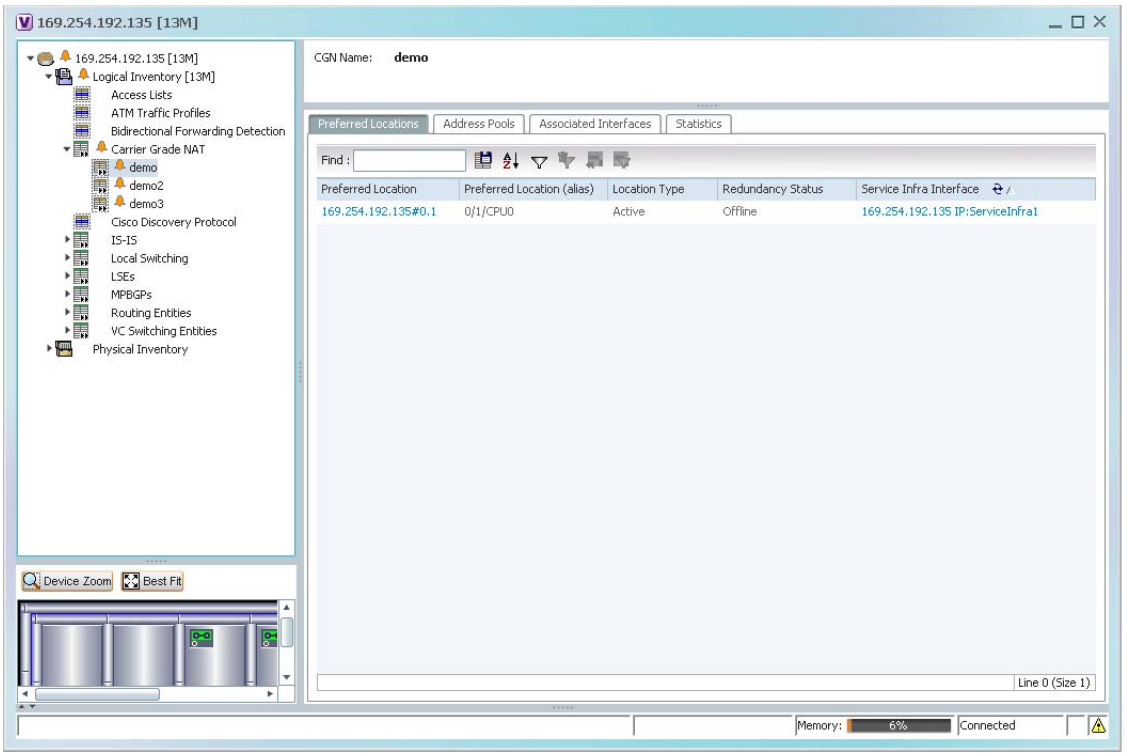


Table 13-3 describes the Carrier Grade NAT properties that are displayed.

Table 13-3 Carrier Grade NAT Properties in Logical Inventory

Field	Description
CGN Name	Name of the Carrier Grade NAT service.
Preferred Location Tab	
Preferred Location	Hyperlinked entry to the card in physical inventory.
Preferred Location (alias)	Location of module in clear text.
Location Type	Configured type of location: Active or Standby.
Redundancy Status	Redundancy state: Online or Offline. If the field is empty, it means the data was not collected from the device.
Service Infra Interface	Hyperlinked entry to the routing entity in logical inventory. For more information about routing entities in logical inventory, see Viewing Routing Entities, page 17-31.

Table 13-3 Carrier Grade NAT Properties in Logical Inventory (continued)

Field	Description
Address Pools Tab	
Inside VRF	Hyperlinked entry to the inside VRF in logical inventory. For more information about VRF properties in logical inventory, see Viewing VRF Properties, page 17-27.
Address Family	Type of IP address in this pool: IPv4 or IPv6.
Outside VRF	Hyperlinked entry to the outside VRF in logical inventory. For more information about VRF properties in logical inventory, see Viewing VRF Properties, page 17-27.
Address Pool	Range of IP addresses that can be used for the service instance. If an end address is not specified, the entire range of 255 addresses is used for the address pool.
Associated Interfaces Tab	
Interface	Hyperlinked entry to the associated entry in logical inventory: • For SVI service interfaces, hyperlinked entry to the routing entity in logical inventory. • For SVI service applications, hyperlinked entry to the VRF entity in logical inventory.
Service Types Tab	
Service Type Name	Name of the Carrier Grade NAT service.
Service Type	Type of Carrier Grade NAT service: 6RD, XLAT, or NAT44.
Statistics Tab	
Statistics Name	Name of the statistic. For statistic names and descriptions, see Table 13-4.
Statistics Value	Value of the statistic.

Table 13-4 Carrier Grade NAT Statistics in Logical Inventory

Statistic Name	Description
Inside to outside drops port limit exceeded	Number of packets dropped because the port limit has been exceeded. The value is calculated from the time Carrier Grade NAT was configured and running on the card.
Inside to outside drops resource depletion	Number of packets that are dropped because no ports are available. The value is calculated from the time Carrier Grade NAT was configured and running on the card.
Inside to outside drops limit system reached	Number of packets that are dropped because the system limit has been exceeded. The value is calculated from the time Carrier Grade NAT was configured and running on the card.
Inside to outside forward rate	Number of packets forwarded from the inside to the outside in the last one second.
Outside to inside forward rate	Number of packets forwarded from the outside to the inside in the last one second.
Translations create rate	Number of translation entries created in the last one second.
Translations delete rate	Number of translation entries deleted in the last one second.

Viewing Carrier Grade NAT Properties in Physical Inventory

To view Carrier Grade NAT properties in physical inventory:

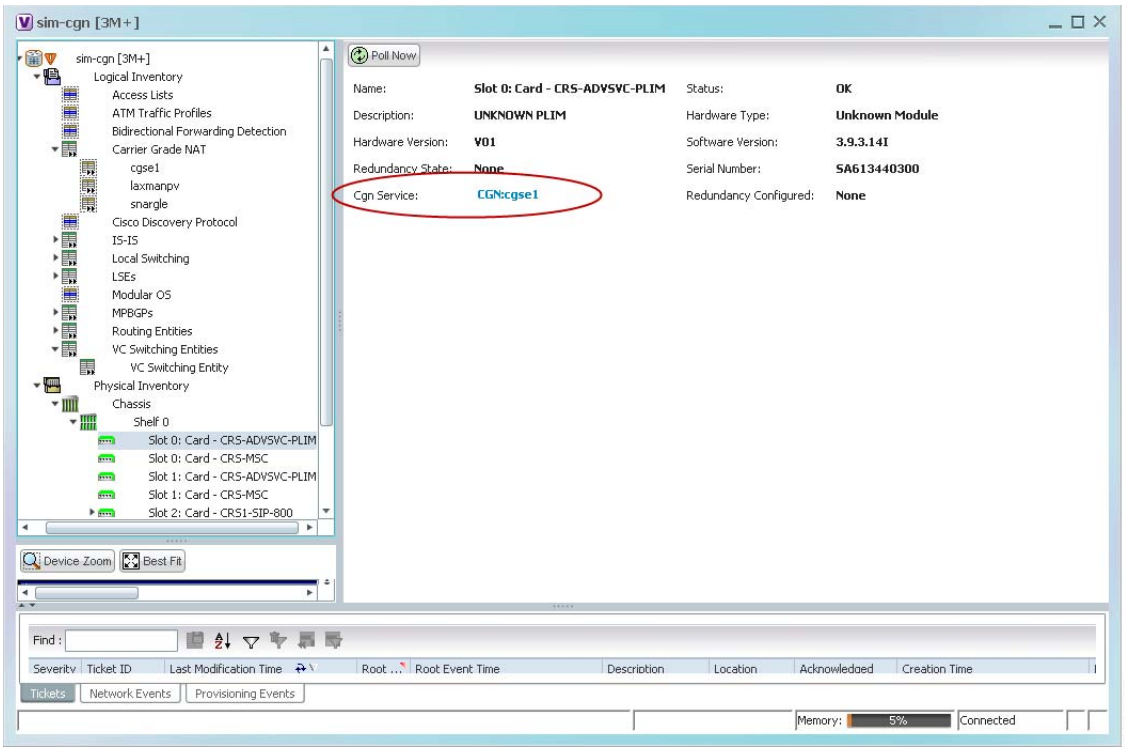
Step 1 In Prime Network Vision, double-click the Cisco CRS device configured for Carrier Grade NAT.

Step 2 To view Carrier Grade NAT properties configured on a specific interface, click **Physical Inventory** > ***chassis*** > *shelf* > *slot* > *card* > *interface*. See Table 3-10 for a description of the information displayed in the Subinterfaces table.

Step 3 To view Carrier Grade NAT properties configured on a Cisco CRS-CGSE-PLIM card, click **Physical Inventory** > *chassis* > *shelf* > *slot* > *PLIM-card*.

Figure 13-2 shows an example of Carrier Grade NAT properties in physical inventory.

Figure 13-2 Carrier Grade NAT Properties in Physical Inventory



The field CGN Service is displayed, and the entry is hyperlinked to the associated Carrier Grade NAT service in logical inventory.



CHAPTER 14

Monitoring DWDM Properties

The following topics describe how you can view and monitor IP over dense wavelength division multiplexing (DWDM) properties configured on network elements by using Cisco Prime Network Vision (Prime Network Vision):

- User Roles Required to View DWDM Properties, page 14-1
- Viewing DWDM in Physical Inventory, page 14-2
- Viewing G.709 Properties, page 14-4
- Viewing Performance Monitoring Configuration, page 14-10

User Roles Required to View DWDM Properties

This topic identifies the roles that are required to view DWDM properties using Prime Network Vision. Prime Network determines whether you are authorized to perform a task as follows:

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

For more information on user authorization, see the *Cisco Prime Network 3.9 Administrator Guide*.

The following tables identify the tasks that you can perform:

- Table 14-1 identifies the tasks that you can perform if a selected element **is not in** one of your assigned scopes.
- Table 14-2 identifies the tasks that you can perform if a selected element **is in** one of your assigned scopes.

By default, users with the Administrator role have access to all managed elements. To change the Administrator user scope, see the topic on device scopes in the *Cisco Prime Network 3.9 Administrator Guide*.

Table 14-1 Default Permission/Security Level Required for Viewing DWDM Properties - Element Not in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View DWDM properties	—	—	—	—	X
View G.709 properties	—	—	—	—	X
View performance monitoring configuration information	—	—	—	—	X

Table 14-2 Default Permission/Security Level Required for Viewing DWDM Properties - Element in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View DWDM properties	X	X	X	X	X
View G.709 properties	X	X	X	X	X
View performance monitoring configuration information	X	X	X	X	X

Viewing DWDM in Physical Inventory

Prime Network Vision enables you to monitor a variety of DWDM properties in physical inventory, including forward error correction (FEC), G.709 status, and performance monitoring parameters.

To view DWDM properties in physical inventory:

Step 1 In a Prime Network Vision map, double-click the device on which DWDM is configured.

Step 2 In the inventory window, choose **Physical Inventory > Chassis** and navigate to the interface configured for DWDM. DWDM details are displayed in the DWDM area in the content pane as shown in Figure 14-1.

Figure 14-1 DWDM Properties in Physical Inventory

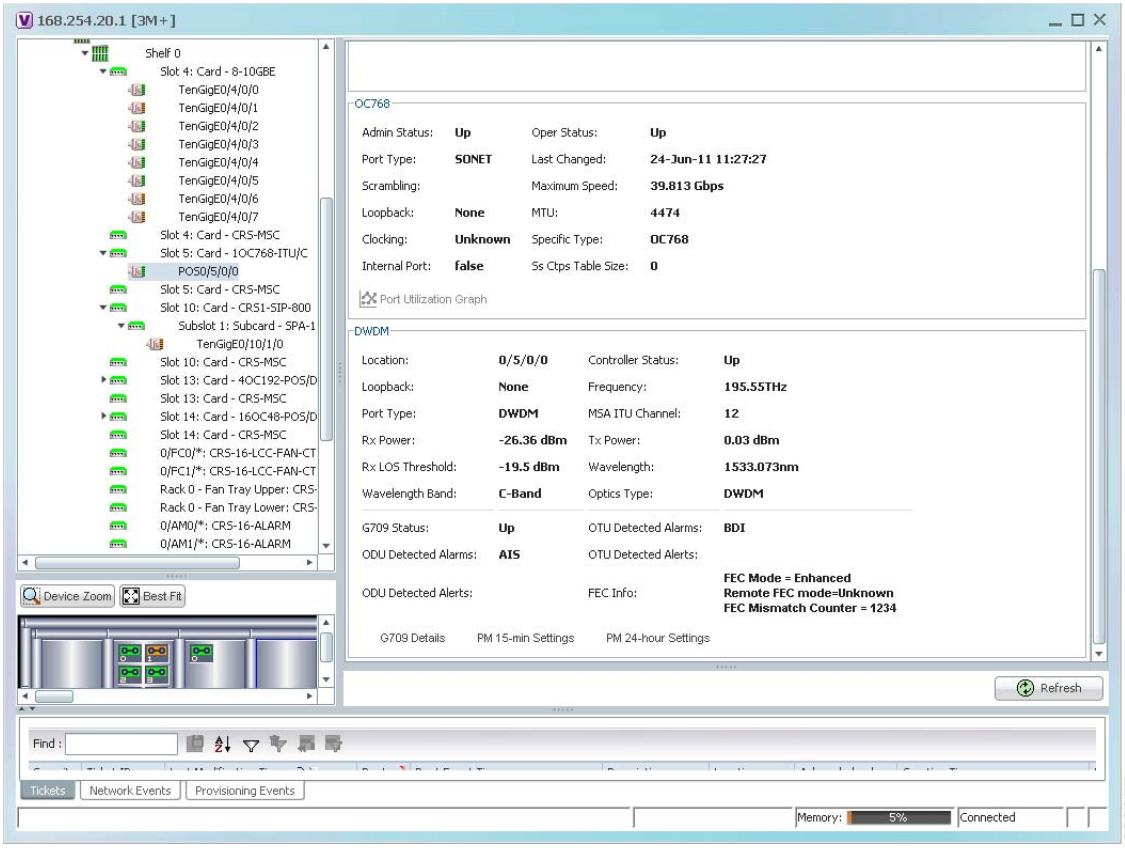


Table 14-3 describes the information displayed for DWDM.

Table 14-3 DWDM Properties in Physical Inventory

Field	Description
Location	Physical interface using the format *rack*/*slot*/*module*/*port* where: • *rack* is the chassis number of the rack. • *slot* is the physical slot number of the line card. • *module* is the module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number. • *port* is the physical port number of the interface.
Controller Status	Status of the controller: Up or Down.
Loopback	Whether or not the DWDM controller is configured for loopback mode.
Frequency	Frequency of the channel in terahertz.
Port Type	The port type. In this case, DWDM.
MSA ITU Channel	Multi Source Agreement (MSA) ITU channel number.
Rx Power	Actual optical power at the receiving port.
Tx Power	Value of the transmit power level.

Table 14-3 DWDM Properties in Physical Inventory (continued)

Field	Description
Rx LOS Threshold	Number of optical channel transport unit (OTU) loss of signal (LOS) alarms. If the receive optical power is less than or equal to this defined threshold, the optical LOS alarm is raised.
Wavelength	Wavelength corresponding to the channel number in nanometers.
Wavelength Band	Indicates the wavelength band: C-band or L-band.
Optics Type	Indicates the optics type: GE or DWDM.
G709 Properties	
G709 Status	Whether the G.709 wrapper is enabled or disabled: Up or Down.
OTU Detected Alarms	OTU overhead alarms.
ODU Detected Alarms	Optical channel data unit (ODU) alarms.
OTU Detected Alerts	OTU alerts.
ODU Detected Alerts	ODU alerts.
FEC Info	Indicates the: • FEC mode of the controller: Disabled, Enhanced, Standard, or Unknown. • FEC mode on the remote device: Disabled, Enhanced, Standard, or Unknown. • Number of sync word mismatches found during the tracking phase.
G709 Details	Click to view G709 properties. For more information, see Viewing G.709 Properties, page 14-4.
PM 15-min Settings	Click to view 15-minute performance monitoring properties. For more information, see Viewing Performance Monitoring Configuration, page 14-10.
PM 24-hour Settings	Click to view 24-hour performance monitoring properties. For more information, see Viewing Performance Monitoring Configuration, page 14-10.

Viewing G.709 Properties

The Telecommunication Standardization Sector (ITU-T) Recommendation G.709 provides a standardized method for transparently transporting services over optical wavelengths end to end. A significant component of G.709 is the FEC code that improves performance and extends the distance that optical signals can span.

To view G.709 properties:

Step 1 In Prime Network Vision, double-click the device on which DWDM is configured.

Step 2 In the inventory window, choose **Physical Inventory > Chassis** and navigate to the interface configured for DWDM.

Step 3 In the content pane, click **G709 Details**.

The G709 Info Properties window is displayed as shown in Figure 14-2 for all Cisco devices except the Cisco 7600 series devices.

Figure 14-2 DWDM G709 Properties Window

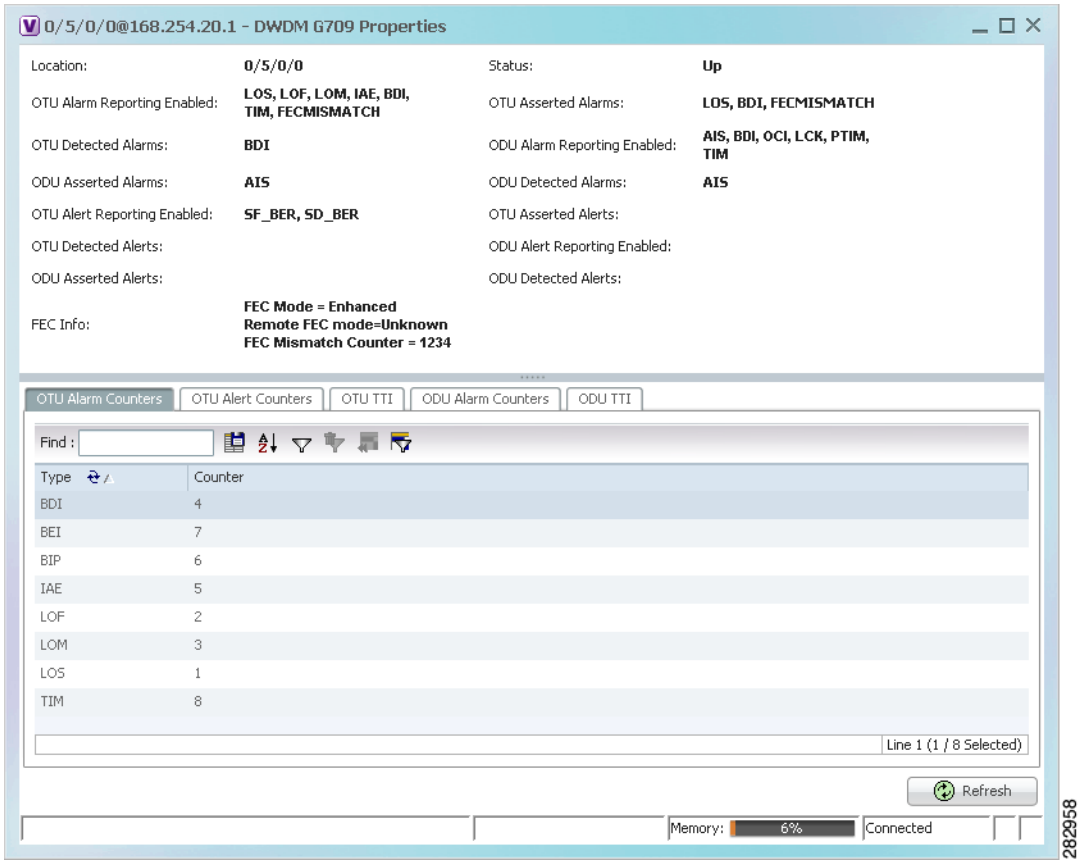


Figure 14-3 shows the tabs that are displayed in the G709 Info Properties window for Cisco 7600 series devices. For Cisco 7600 series devices:

- The ODU Alert Counters tab is displayed.
- The ODU TTI and OTU TTI tabs are not displayed.

Figure 14-3 DWDM G709 Properties Window for Cisco 7600 Series Devices

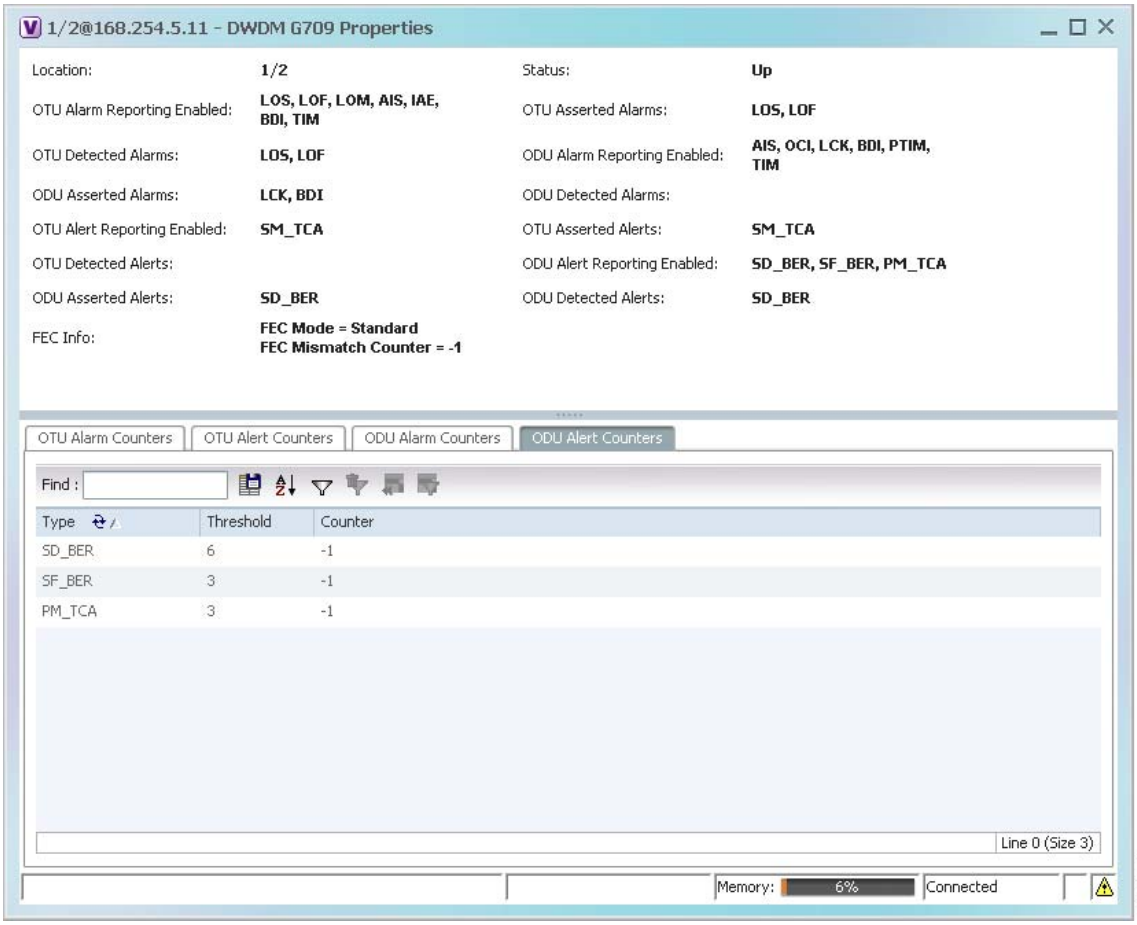


Table 14-4 describes the fields that are displayed above the tabs in the G709 Info Properties window.

Table 14-4 DWDM G709 Properties Window

Field	Description
Location	Physical interface using the format *rack*/*slot*/*module*/*port* where: • *rack* is the chassis number of the rack. • *slot* is the physical slot number of the line card. • *module* is the module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number. • *port* is the physical port number of the interface.
OTU Alarms	
OTU Alarm Reporting Enabled for	The types of alarms enabled for reporting: • AIS—Alarm indication signal (AIS) alarms. • BDI—Backward defect indication (BDI) alarms. • BEI—Backward error indication (BEI) alarms. • BIP—Bit interleaved parity (BIP) alarms. • FECMISMATCH—FEC mismatch alarms. • IAE—Incoming alignment error (IAE) alarms. • LOF—Loss of frame (LOF) alarms. • LOM—Loss of multiple frames (LOM) alarms. • LOS—Loss of signal (LOS) alarms. • TIM—Type identifier mismatch (TIM) alarms.
OTU Asserted Alarms	OTU alarms indicated to be reported by the user.
OTU Detected Alarms	OTU alarms detected by the hardware.
ODU Alarms	
ODU Alarm Reporting Enabled for	The types of ODU alarms enabled for reporting: • AIS—Incoming SONET AIS error status. • BDI—Path termination BDI error status. • BEI—Backward error indication (BEI) error status. • BIP—Bit interleaved parity (BIP) error status. • LCK—Upstream connection locked (LCK) error status. • OCI—Open connection indication (OCI) error status. • PTIM—Payload TIM error status. • TIM—Data stream TIM error status.
ODU Asserted Alarms	ODU alarms indicated to be reported by the user.
ODU Detected Alarms	ODU alarms detected by the hardware.

Table 14-4 DWDM G709 Properties Window (continued)

Field	Description
OTU Alerts	
OTU Alert Reporting Enabled for	The types of alerts enabled for reporting: • SD-BER—Section Monitoring (SM) bit error rate (BER) is in excess of the signal degradation (SD) BER threshold. • SF-BER—SM BER is in excess of the signal failure (SF) BER threshold. • PM-TCA—Performance monitoring (PM) threshold crossing alert (TCA). • SM-TCA—SM threshold crossing alert.
OTU Asserted Alerts	OTU alerts indicated to be reported by the user.
OTU Detected Alerts	OTU alerts detected by the hardware.
ODU Alerts	
ODU Alert Reporting Enabled for	The types of ODU alerts enabled for reporting: • SD-BER—SM BER is in excess of the SD BER threshold. • SF-BER—SM BER is in excess of the SF BER threshold. • PM-TCA—PM threshold crossing alert. • SM-TCA—SM threshold crossing alert.
ODU Asserted Alerts	ODU alerts indicated to be reported by the user.
ODU Detected Alerts	ODU alerts detected by the hardware.
Other	
FEC Info	FEC properties: • FEC mode for the controller—Disable, Enhanced, Standard, or Unknown. • Remote FEC mode—FEC mode on the remote device: Disabled, Enhanced, Standard, or Unknown. • FEC mismatch counter—Number of sync word mismatches found during the tracking phase.
Status	G.709 wrapper administrative status: Up or Down.

The G709 Info Properties window contains the following tabs, depending on the selected network element:

- OTU Alarm Counters Tab, page 14-9
- OTU Alert Counters Tab, page 14-9
- ODU Alarm Counters Tab, page 14-9
- OTU TTI Tab, page 14-9
- ODU TTI Tab, page 14-9
- ODU Alert Counters Tab, page 14-10

Step 4 To view additional G.709 properties, click the required tab. Table 14-5 describes the information displayed in each tab.

Table 14-5 G709 Properties Window Tabs

Field	Description
OTU Alarm Counters Tab	
Type	Type of OTU alarm, such as BDI or BEI.
Counter	Number of alarms reported for each alarm type.
OTU Alert Counters Tab	
Type	Type of OTU alert, such as SD-BER or SF-BER.
Threshold	Threshold set for the type of alert.
Counter	Number of alerts reported for each alert type. A value of -1 indicates that no value has been set up.
ODU Alarm Counters Tab	
Type	Type of ODU alarm, such as AIS or BDI.
Counter	Number of alarms reported for each alarm type.
OTU TTI Tab This tab is not displayed for Cisco 7600 series devices.	
Type	Type of OTU Trail Trace Identifier (TTI) configured: • Expected • Received • Sent
String Type	For each TTI type, the type of string: • ASCII • Hexadecimal
TTI String	For each TTI type, the specific TTI string configured.
ODU TTI Tab This tab is not displayed for Cisco 7600 series devices.	
Type	Type of ODU TTI configured: • Expected • Received • Sent
String Type	For each TTI type, the type of string: • ASCII • Hexadecimal
TTI String	For each TTI type, the specific TTI string configured.

Table 14-5 G709 Properties Window Tabs (continued)

Field	Description
ODU Alert Counters Tab	
This tab is displayed only for Cisco 7600 series devices.	
Type	Type of OTU alert, such as SD-BER or SF-BER.
Threshold	Threshold set for the type of alert.
Counter	Number of alerts reported for each alert type. A value of -1 indicates that no value has been set up.

Step 5 To close the G709 Info Properties window, click the upper right corner.

Viewing Performance Monitoring Configuration

Performance monitoring parameters are used to gather, store, set thresholds for, and report performance data for early detection of problems. Thresholds are used to set error levels for each performance monitoring parameter. During the accumulation cycle, if the current value of a performance monitoring parameter reaches or exceeds its corresponding threshold value, a threshold crossing alert (TCA) can be generated. The TCAs provide early detection of performance degradation.

Prime Network Vision enables you to view the configuration settings for performance monitoring. Performance monitoring statistics are accumulated on a 15-minute basis, synchronized to the start of each quarter-hour. They are also accumulated on a daily basis starting at midnight. Historical counts are maintained for thirty-three 15-minute intervals and two daily intervals.

To view performance monitoring configuration settings:

Step 1 In Prime Network Vision, double-click the device on which DWDM is configured.

Step 2 In the inventory window, choose **Physical Inventory > Chassis** and navigate to the interface configured for DWDM.

Step 3 In the content pane, select the performance monitoring configuration settings you want to view:

- To view the performance monitoring 15-minute configuration settings, click **PM 15-min Settings**.
- To view the performance monitoring 24-hour configuration settings, click **PM 24-hour Settings**.

The Client DWDM PM Settings Properties window is displayed as shown in Figure 14-4.

Figure 14-4 Client DWDM PM Settings Properties Window

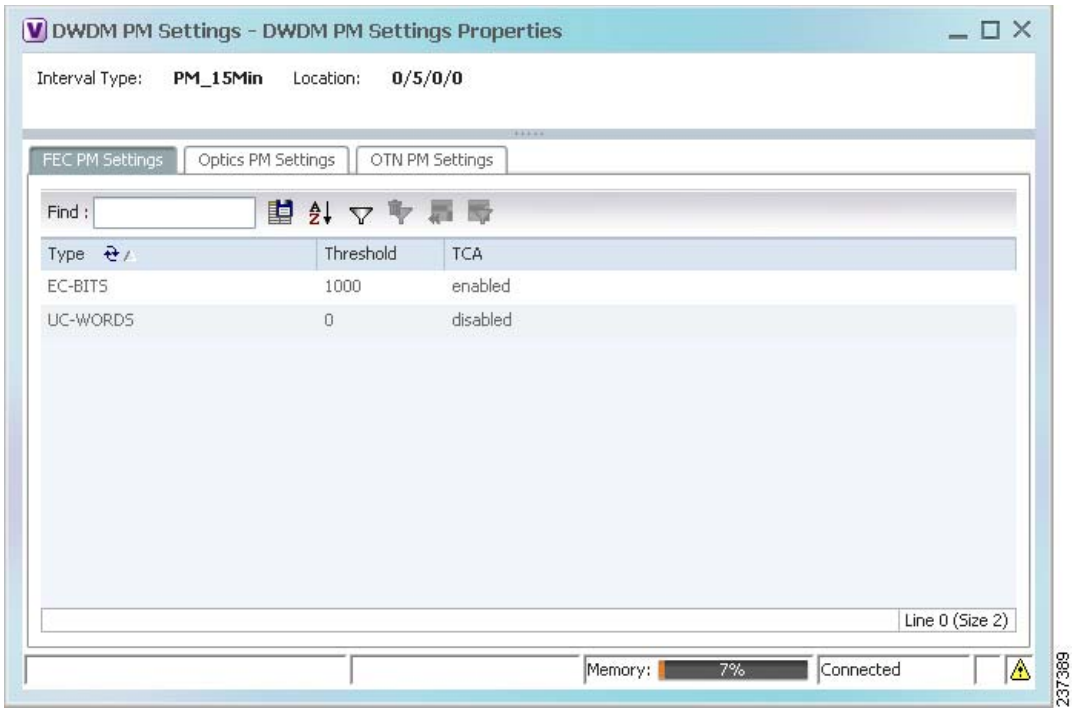


Table 14-6 describes the information displayed above the tabs in the Client DWDM PM Settings Properties window and in each of the tabs.

Table 14-6 Client DWDM PM Settings Properties Window and Tabs

Field	Description
Interval Type	The performance monitoring interval, either 15 minutes or 24 hours.
Location	Physical interface using the format *rack*/*slot*/*module*/*port* where: • *rack* is the chassis number of the rack. • *slot* is the physical slot number of the line card. • *module* is the module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number. • *port* is the physical port number of the interface.
FEC PM Settings Tab	
Type	FEC performance monitoring parameter being tracked: • EC-BITS—The number of bit errors corrected (EC-BITS) in the DWDM trunk line during the performance monitoring time interval. • UC-WORDS—The number of uncorrectable words (UC-WORDS) detected in the DWDM trunk line during the performance monitoring time interval.
Threshold	Threshold for the performance monitoring parameter.
TCA	Whether TCA generation for the specified parameter on the DWDM controller is enabled or disabled.
Optics PM Settings Tab	
Type	Optics performance monitoring parameter being tracked: • LBC—Laser bias current. • OPR—Optical power on the unidirectional port. • OPT—Transmit optical power in dBm.
Max Threshold	Maximum threshold configured for the parameter.
Max TCA	If enabled, indicates a TCA is generated if the value of the parameter exceeds the maximum threshold during the performance monitoring period. If disabled, TCAs are not generated if the maximum threshold is exceeded.
Min Threshold	Minimum threshold configured for the parameter.
Min TCA	If enabled, indicates a TCA is generated if the value of the parameter drops below the minimum threshold during the performance monitoring period. If disabled, TCAs are not generated if the value drops below the minimum threshold.

Table 14-6 Client DWDM PM Settings Properties Window and Tabs (continued)

Field	Description
OTN PM Settings Tab	
Type	OTN performance monitoring parameter being tracked: • bbe-pm-fe—Far-end path monitoring background block errors (BBE-PM). Indicates the number of background block errors recorded in the optical transport network (OTN) path during the performance monitoring time interval. • bbe-pm-ne—Near-end path monitoring background block errors (BBE-PM). • bbe-sm-fe—Far-end section monitoring background block errors (BBE-SM). Indicates the number of background block errors recorded in the OTN section during the performance monitoring time interval. • bbe-sm-ne—Near-end section monitoring background block errors (BBE-SM). • bber-pm-fe—Far-end path monitoring background block errors ratio (BBER-PM). Indicates the background block errors ratio recorded in the OTN path during the performance monitoring time interval. • bber-pm-ne—Near-end path monitoring background block errors ratio (BBER-PM). • bber-sm-fe—Far-end section monitoring background block errors ratio (BBER-SM). Indicates the background block errors ratio recorded in the OTN section during the performance monitoring time interval. • bber-sm-ne—Near-end section monitoring background block errors ratio (BBER-SM) • es-pm-fe—Far-end path monitoring errored seconds (ES-PM). Indicates the errored seconds recorded in the OTN path during the performance monitoring time interval. • es-pm-ne—Near-end path monitoring errored seconds (ES-PM). • es-sm-fe—Far-end section monitoring errored seconds (ES-SM). Indicates the errored seconds recorded in the OTN section during the performance monitoring time interval. • es-sm-ne—Near-end section monitoring errored seconds (ES-SM). • esr-pm-fe—Far-end path monitoring errored seconds ratio (ESR-PM). Indicates the errored seconds ratio recorded in the OTN path during the performance monitoring time interval. • esr-pm-ne—Near-end path monitoring errored seconds ratio (ESR-PM). • esr-sm-fe—Far-end section monitoring errored seconds ratio (ESR-SM). Indicates the errored seconds ratio recorded in the OTN section during the performance monitoring time interval. • esr-sm-ne—Near-end section monitoring errored seconds ratio (ESR-SM). • fc-pm-fe—Far-end path monitoring failure counts (FC-PM). Indicates the failure counts recorded in the OTN path during the performance monitoring time interval. • fc-pm-ne—Near-end path monitoring failure counts (FC-PM). • fc-sm-fe—Far-end section monitoring failure counts (FC-SM). Indicates the failure counts recorded in the OTN section during the performance monitoring time interval. • fc-sm-ne—Near-end section monitoring failure counts (FC-SM).

Table 14-6 Client DWDM PM Settings Properties Window and Tabs (continued)

Field	Description
Type (cont.)	• ses-pm-fe—Far-end path monitoring severely errored seconds (SES-PM). Indicates the severely errored seconds recorded in the OTN path during the performance monitoring time interval. • ses-pm-ne—Far-end path monitoring severely errored seconds (SES-PM). • ses-sm-fe—Far-end section monitoring severely errored seconds (SES-SM). Indicates the severely errored seconds recorded in the OTN section during the performance monitoring time interval. • ses-sm-ne—Near-end section monitoring severely errored seconds (SES-SM). • sesr-pm-fe—Far-end path monitoring severely errored seconds ratio (SESR-PM). Indicates the severely errored seconds ratio recorded in the OTN path during the performance monitoring time interval. • sesr-pm-ne—Near-end path monitoring severely errored seconds ratio (SESR-PM). • sesr-sm-fe—Far-end section monitoring severely errored seconds ratio (SESR-SM). Indicates the severely errored seconds ratio recorded in the OTN section during the performance monitoring time interval. • sesr-sm-ne—Near-end section monitoring severely errored seconds ratio (SESR-SM). • uas-pm-fe—Far-end path monitoring unavailable seconds (UAS-PM). Indicates the unavailable seconds recorded in the OTN path during the performance monitoring time interval. • uas-pm-ne—Near-end path monitoring unavailable seconds (UAS-PM). • uas-sm-fe—Far-end section monitoring unavailable seconds (UAS-SM). Indicates the unavailable seconds recorded in the OTN section during the performance monitoring time interval. • uas-sm-ne—Near-end section monitoring unavailable seconds (UAS-SM).
Threshold	Threshold configured for the parameter.
TCA	If enabled, indicates a TCA is generated if the value of the parameter crosses the threshold during the performance monitoring period. If disabled, TCAs are not generated if the value crosses the threshold.



CHAPTER 15

Viewing Ethernet Operations, Administration, and Maintenance Tool Properties

The following topics describe how you can use Cisco Prime Network Vision (Prime Network Vision) to monitor Ethernet operations, administration, and maintenance (OAM) tools:

- User Roles Required to View Ethernet OAM Tool Properties, page 15-1
- Ethernet OAM Overview, page 15-2
- Viewing Connectivity Fault Management Properties, page 15-3
- Viewing Ethernet LMI Properties, page 15-9
- Viewing Link OAM Properties, page 15-13

User Roles Required to View Ethernet OAM Tool Properties

This topic identifies the roles that are required to view Ethernet OAM tool properties. Prime Network determines whether you are authorized to perform a task as follows:

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

For more information on user authorization, see the *Cisco Prime Network 3.9 Administrator Guide*.

The following tables identify the tasks that you can perform:

- Table 15-1 identifies the tasks that you can perform if a selected element **is not in** one of your assigned scopes.
- Table 15-2 identifies the tasks that you can perform if a selected element **is in** one of your assigned scopes.

By default, users with the Administrator role have access to all managed elements. To change the Administrator user scope, see the topic on device scopes in the *Cisco Prime Network 3.9 Administrator Guide*.

Table 15-1 Default Permission/Security Level Required for Viewing Ethernet OAM Tool Properties - Element Not in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View CFM properties	—	—	—	—	X
View Ethernet LMI properties	—	—	—	—	X
View Link OAM properties	—	—	—	—	X

Table 15-2 Default Permission/Security Level Required for Viewing Ethernet OAM Tool Properties - Element in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View CFM properties	X	X	X	X	X
View Ethernet LMI properties	X	X	X	X	X
View Link OAM properties	X	X	X	X	X

Ethernet OAM Overview

Prime Network Vision supports three, interrelated OAM components, including:

- Connectivity Fault Management—Connectivity Fault Management (CFM) is an end-to-end per-service-instance (per VLAN) Ethernet layer OAM protocol that includes connectivity monitoring, fault verification, and fault isolation. CFM allows you to manage individual customer service instances. Ethernet Virtual Connections (EVCs) are the services that are sold to customers and are designated by service VLAN tags. CFM operates on a per-service-VLAN (or per-EVC) basis. It lets you know when an EVC fails and provides tools to isolate the failure.
- Ethernet Local Management Interface—Ethernet Local Management Interface (Ethernet LMI) operates between the customer edge (CE) and the user-facing provider edge (U-PE) devices. Ethernet LMI allows you to automatically provision CEs based on EVCs and bandwidth profiles.
- Link OAM—Link OAM allows you to monitor and troubleshoot a single Ethernet link. It is an optional sublayer implemented in the Data Link Layer between the Logical Link Control (LLC) and MAC sublayers of the Open Systems Interconnect (OSI) model. You can monitor a link for critical events and, if needed, put a remote device into loopback mode for link testing. Link OAM also discovers unidirectional links, which are created when one transmission direction fails.

Viewing Connectivity Fault Management Properties

CFM provides capabilities for detecting, verifying, and isolating connectivity failures in networks with bridges operated by multiple independent organizations, each with restricted management access to each other's equipment. CFM allows you to discover and verify end-to-end, Carrier Ethernet PE-to-PE or CE-to-CE paths through bridges and LANs.

CFM consists of maintenance domains. Maintenance domains are administrative regions used to manage and administer specific network segments. Maintenance domains are organized in a hierarchy. The administrator assigns a maintenance level to the domain from 0 (lowest level) to 7 (highest level); the maintenance level determines the domain's position within the CFM hierarchy.

CFM maintenance domain boundaries are indicated by maintenance points. A maintenance point is an interface point that participates within a CFM maintenance domain. Maintenance point types include:

- Maintenance Endpoints—Maintenance endpoints (MEPs) are active CFM elements residing at the edge of a domain. MEPs can be inward or outward facing. They periodically transmit continuity check messages and expect to periodically receive similar messages from other MEPs within a domain. If requested, MEPs can also transmit traceroute and loopback messages. MEPs are responsible for keeping CFM messages within the boundaries of a maintenance domain.
- Maintenance Intermediate Points—Maintenance intermediate points (MIPs) are passive elements that catalog information received from MEPs and other MIPs. MIPs only respond to specific CFM messages such as traceroute and loopback, and they forward those messages within the maintenance domain.

Note Prime Network Vision does not display information for CFM maintenance endpoints or maintenance intermediate points for Cisco Viking devices if errors exist in their configurations. An error in the configuration is indicated by an exclamation point (!) in the CLI output.

For example, if you enter the command **show ethernet cfm local maintenance-points**, a configuration error is indicated as follows:

```
cfm_d100/2        cfm_s100        Te0/2/0/3.100        Up MEP 2100 eb:7a:53!
```

To view CFM properties:

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

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

Figure 15-1 shows an example of CFM in logical inventory.

Figure 15-1 CFM in Logical Inventory

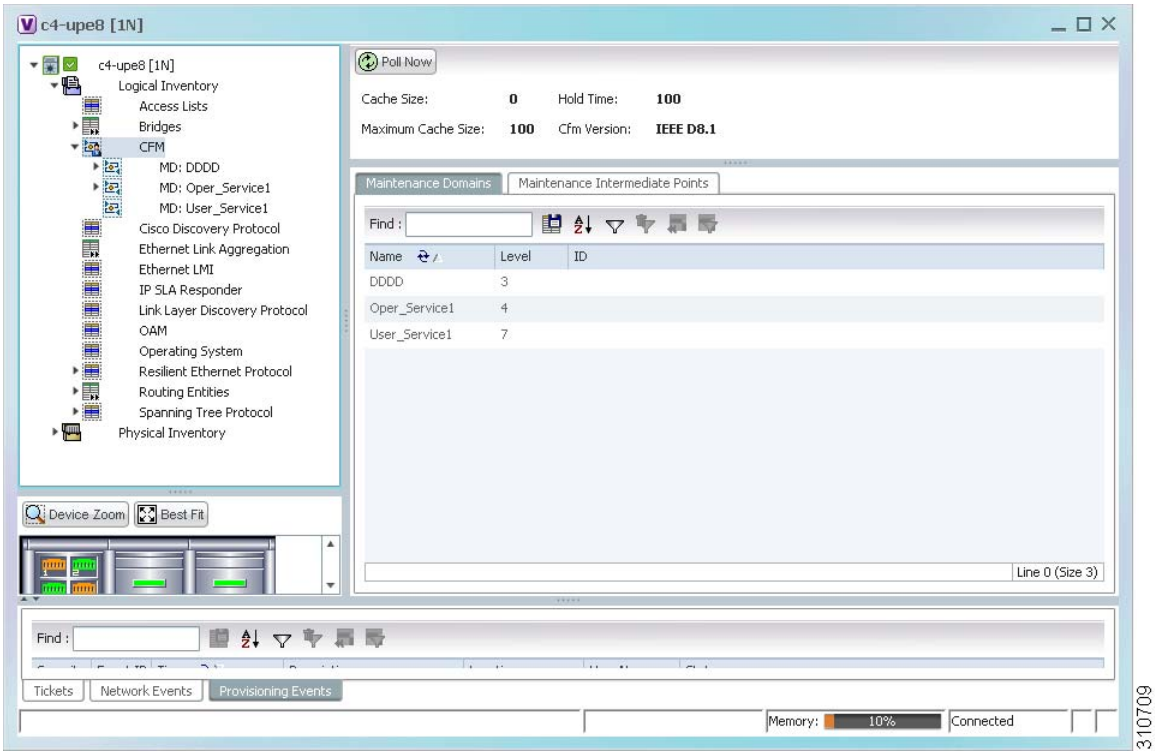


Table 15-3 describes the information displayed for CFM.

Table 15-3 CFM Properties

Field	Description
Cache Size	CFM traceroute cache size in number of lines.
Hold Time	Configured hold time (in minutes) that is used to indicate to the receiver the validity of traceroute and loopback messages transmitted by the device. The default value is 2.5 times the transmit interval.
Maximum Cache Size	Maximum CFM traceroute cache size in number of lines.
CFM Version	CFM version, such as IEEE D8.1.
Maintenance Domains Table	
Name	Domain name.
Level	Unique level the domain is managed on. Values range from 0 to 7.
ID	Optional domain identifier.

Step 3 Click the Maintenance Intermediate Points tab to view MIP information. See Figure 15-2.

Figure 15-2 CFM Maintenance Intermediate Points Tab

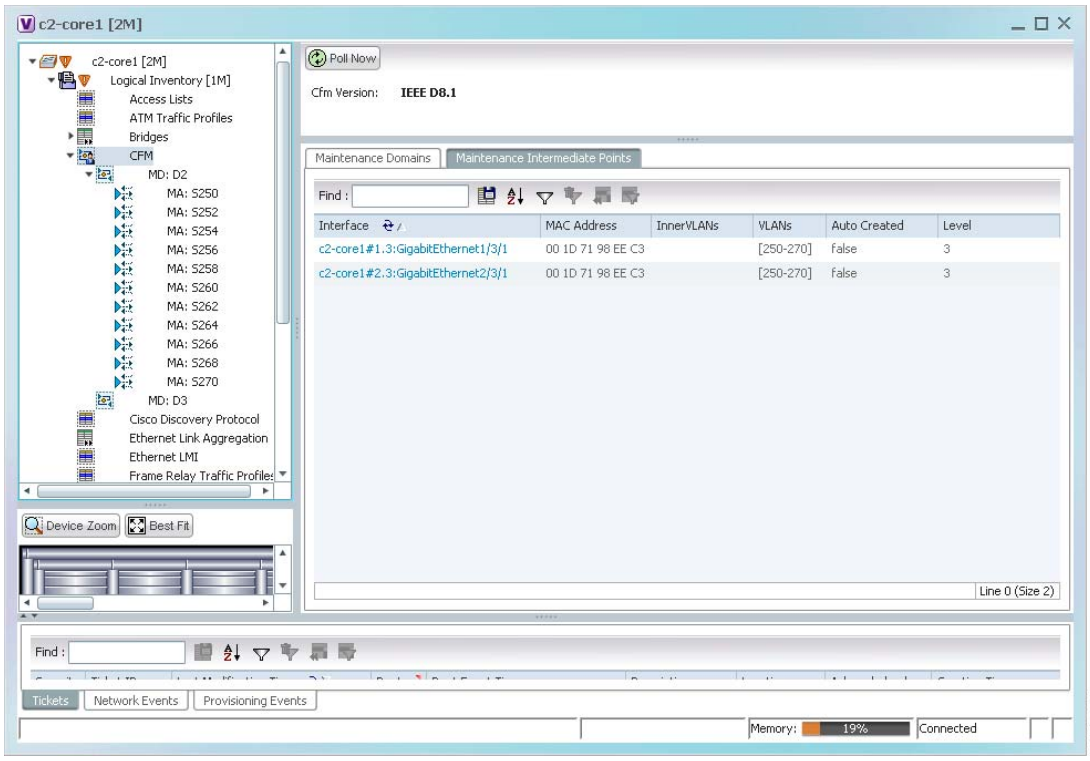


Table 15-4 describes the information that is displayed in the Maintenance Intermediate Points table.

Table 15-4 CFM Maintenance Intermediate Point Properties

Field	Description
Interface	Interface configured as a MIP, hyperlinked to its entry in physical inventory.
MAC Address	MAC address of the interface.
Inner VLANs	Inner VLAN identifiers.
VLANs	VLANs associated with the interface.
Auto Created	Whether or not the MIP was automatically created: True or False.
Level	Unique level the domain is managed on. Values range from 0 to 7.

Step 4 To view the details of a specific maintenance domain, do one of the following:

- Choose **Logical Inventory > CFM >** *domain*.
- Double-click the required entry in the Maintenance Domains table.

Figure 15-3 shows an example of the information displayed for the maintenance domain.

Figure 15-3 CFM Maintenance Domain Properties

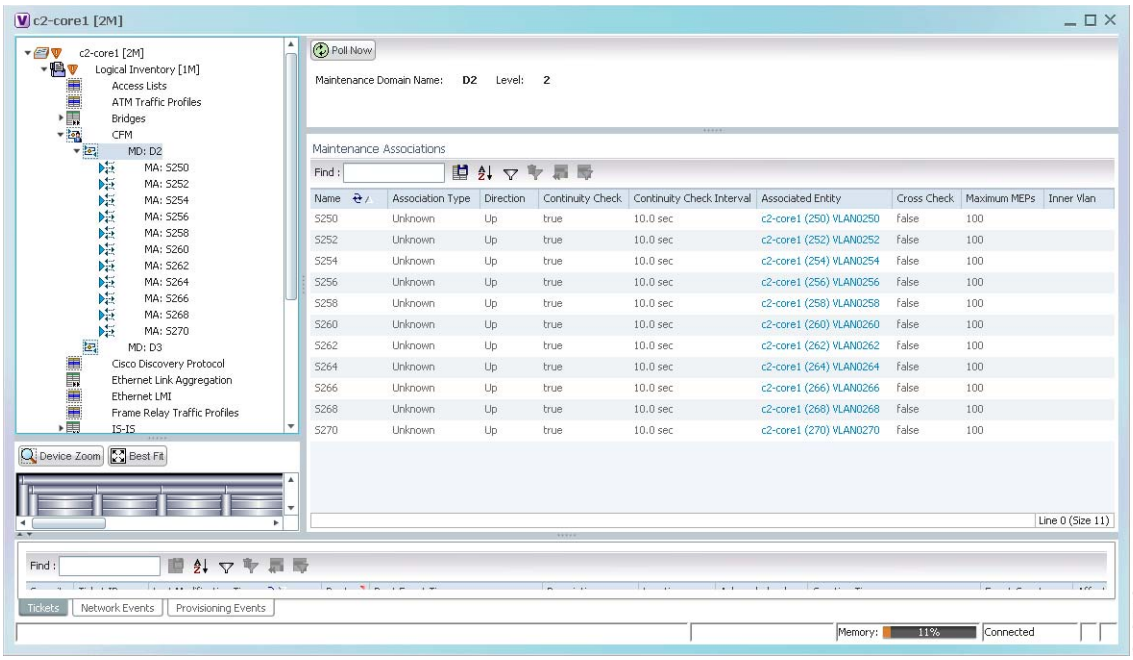


Table 15-5 describes the information that is displayed for CFM maintenance domains.

Table 15-5 CFM Maintenance Domain Properties

Field	Description
Maintenance Domain Name	Name of the domain.
Level	Level at which the domain is managed: 0-7.
ID	Optional maintenance domain identifier.
Maintenance Associations Table	
Name	Name of the maintenance association.
Association Type	Maintenance association type.
Direction	Direction of the maintenance association: Up or Down.
Continuity Check	Whether or not the continuity check is enabled: True or False.
Continuity Check Interval	Interval (in seconds) for checking continuity.
Associated Entity	Bridge, port, or pseudowire that the maintenance association uses for CFM. Click the hyperlinked entry to view the item in inventory.
Cross Check	Whether or not cross checking is enabled: True or False.
Maximum MEPs	Maximum number of maintenance endpoints (MEPs) that can be configured on the maintenance association.
Inner VLAN	Inner VLAN identifier.

Step 5 To view the properties for a maintenance association's endpoints, do one of the following:

- Choose **Logical Inventory > CFM >** *domain* **>** *association*.
- In the Maintenance Associations table, double-click the required association.

Figure 15-4 shows the information displayed for the maintenance association endpoints.

Figure 15-4 CFM Maintenance Association - Endpoint Properties

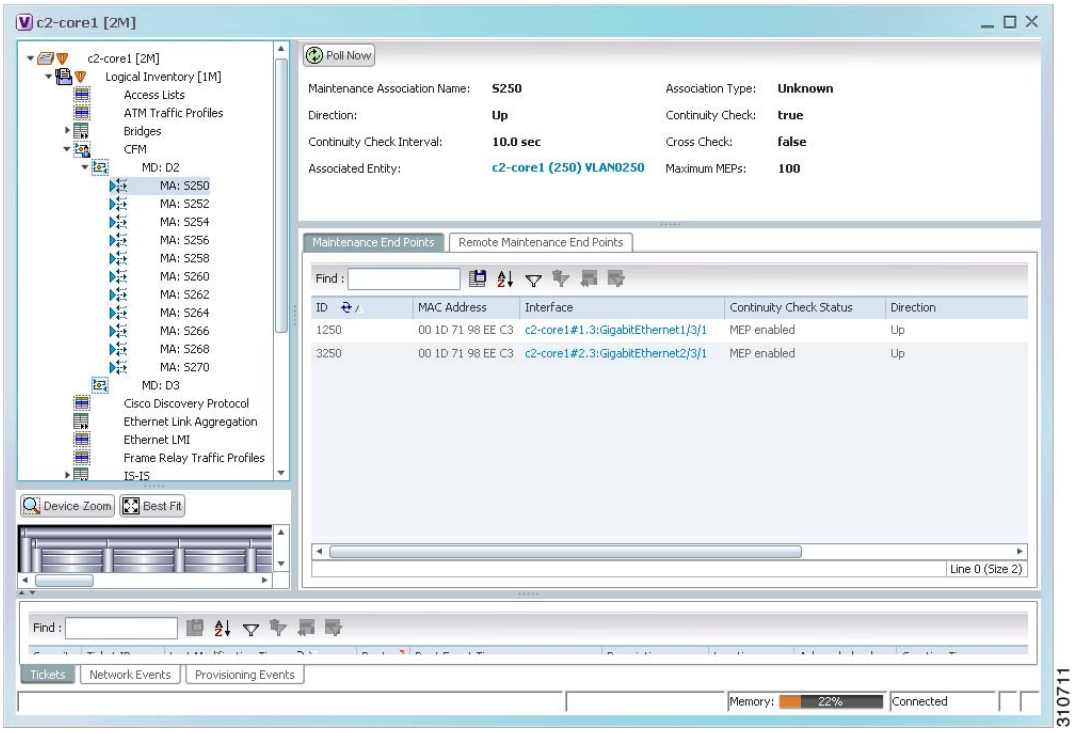


Table 15-6 describes the information that is displayed for CFM maintenance associations and MIPs.

Table 15-6 CFM Maintenance Association Properties

Field	Description
Maintenance Association Name	Name of the maintenance association.
Association Type	Maintenance association type, such as Bridge Domain.
Direction	Direction of the maintenance association: Up or Down.
Continuity Check	Whether or not the continuity check is enabled: True or False.
Continuity Check Interval	Interval (in seconds) for checking continuity.
Cross Check	Whether or not cross checking is enabled: True or False.
Associated Entity	Bridge that the maintenance association uses for CFM. Click the hyperlinked entry to view the bridge in logical inventory.
Maximum MEPs	Maximum number of MEPs that can be configured on the maintenance association.
Inner VLANs	Inner VLAN identifiers.

Table 15-6 CFM Maintenance Association Properties (continued)

Field	Description
Maintenance End Points Table	
ID	Local identifier for the MEP.
MAC Address	MAC address that identifies the MEP.
Interface	Interface on which the MEP is configured, hyperlinked to the respective EFP, VSI or interface in inventory.
Continuity Check Status	CFM continuity check status: MEP Active, MEP Inactive, MEP Enabled, MEP Disabled, or Unknown.
Direction	Direction of traffic on which the MEP is defined: Up, Down, or Unknown.

Step 6 Click the **Remote Maintenance End Points** tab to view the information displayed for remote MEPs. See Figure 15-5.

Figure 15-5 Remote Maintenance End Points Table

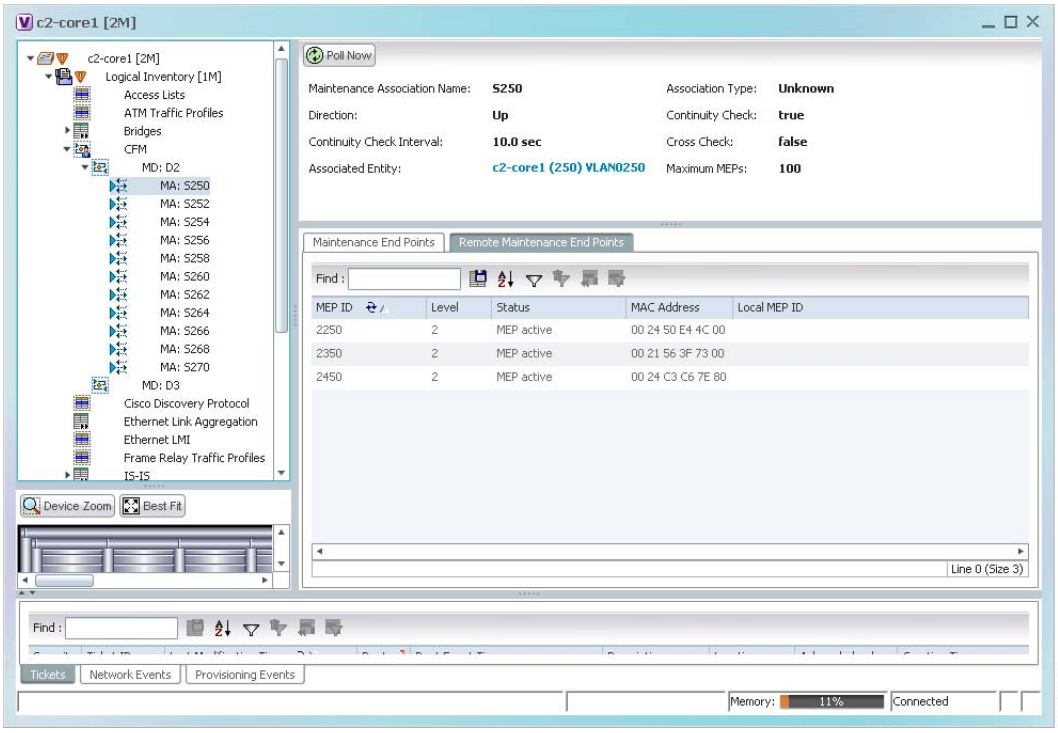


Table 15-7 describes the information presented for remote MEPs.

Table 15-7 CFM Remote Maintenance End Points Table

Field	Description
MEP ID	Remote MEP identifier.
Level	Level at which the remote MEP is managed: 0-7.
Status	Status of the remote MEP, such as MEP Active.
MAC Address	MAC address of the remote MEP.
Local MEP ID	Numeric identifier assigned to the local MEP. Values range from 1 to 8191. **Note** If the remote MEP is in Up mode, the remote MEP is not associated to the local MEP. As a result, the Local MEP ID column is empty.

Viewing Ethernet LMI Properties

Ethernet Local Management Interface (LMI) is a protocol that operates between the customer edge (CE) network element and the provider edge (PE) network element.

Ethernet LMI:

- Runs only on the PE-CE User Network Interface (UNI) link.
- Notifies the CE of connectivity status and configuration parameters of Ethernet services available on the CE port.

Ethernet LMI interoperates with CFM, another OAM protocol that runs within the provider network, to collect OAM status. CFM runs at the provider maintenance level with inward-facing MEPs at the UNI. Using the OAM Ethernet infrastructure, Ethernet LMI works with CFM to provide end-to-end status of Ethernet virtual connections (EVCs) across CFM domains.

To view Ethernet LMI properties:

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

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

Figure 15-6 shows an example of Ethernet LMI properties in logical inventory.

Figure 15-6 Ethernet LMI in Logical Inventory

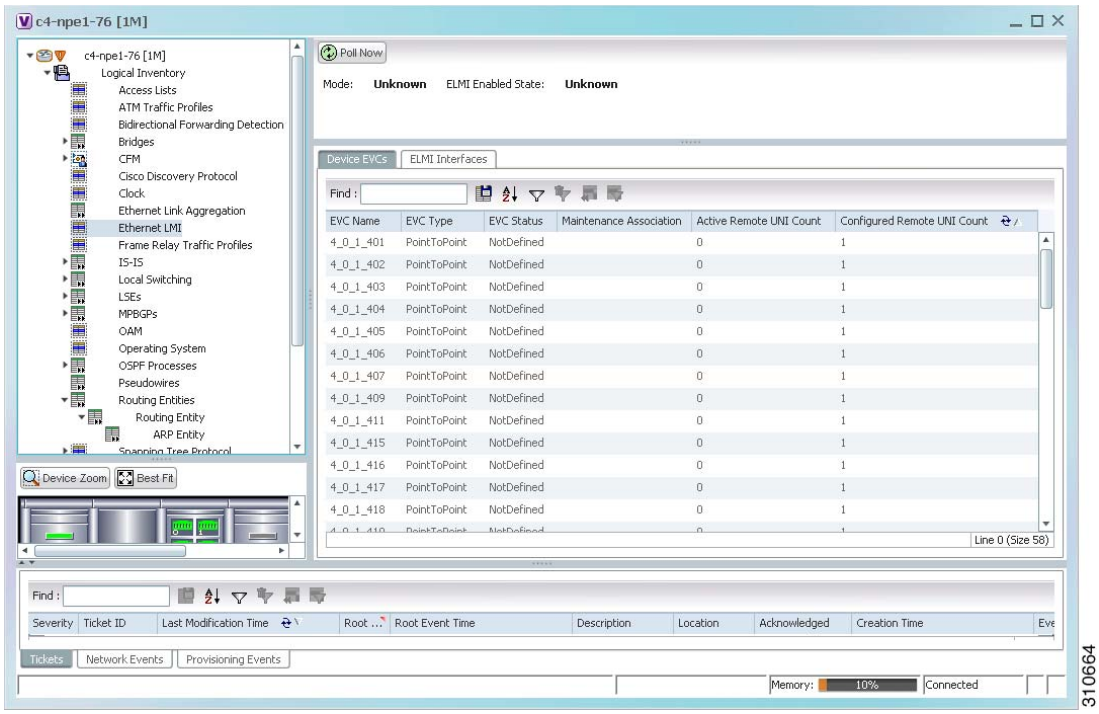


Table 15-8 describes the information displayed for Ethernet LMI.

Table 15-8 Ethernet LMI Properties in Logical Inventory

Field	Description
Globally Enabled	Whether or not Ethernet LMI is enabled globally: True or False.
Mode	Ethernet LMI mode: CE or PE.
Device EVCs Tab	
EVC Name	Name of the EVC.
EVC Type	Type of EVC: Point-to-point or Multipoint.
EVC Status	EVC status: Active, Inactive, Not Defined, or Partially Active.
Maintenance Association	Hyperlinked entry to the maintenance association in CFM in logical inventory. For more information about maintenance associations, see Table 15-6.
Active Remote UNI Count	Number of active remote UNIs.
Configured Remote UNI Count	Number of configured remote UNIs.

Table 15-8 Ethernet LMI Properties in Logical Inventory (continued)

Field	Description
ELMI Interfaces Tab	
Interface Name	Hyperlinked entry to the interface in physical inventory. For more information, see Step 4 in this procedure.
T391	Frequency at which the customer equipment sends status inquiries. The range is 5-30 seconds, with a default of 10 seconds.
T392	Frequency at which the metro Ethernet network verifies that status enquiries have been received. The range is 5-30 seconds, with a default of 15 seconds. A value of 0 (zero) indicates the timer is disabled.
N391	Frequency at which the customer equipment polls the status of the UNI and all EVCs. The range is 1-65000 seconds, with a default of 360 seconds.
N393	Error count for the metro Ethernet network. The range is 1-10, with a default of 4.

Step 3 To view device EVC properties, double-click an EVC name in the Device EVCs tab.

The Device EVC Properties window is displayed as shown in Figure 15-7.

Figure 15-7 Device EVC Properties Window

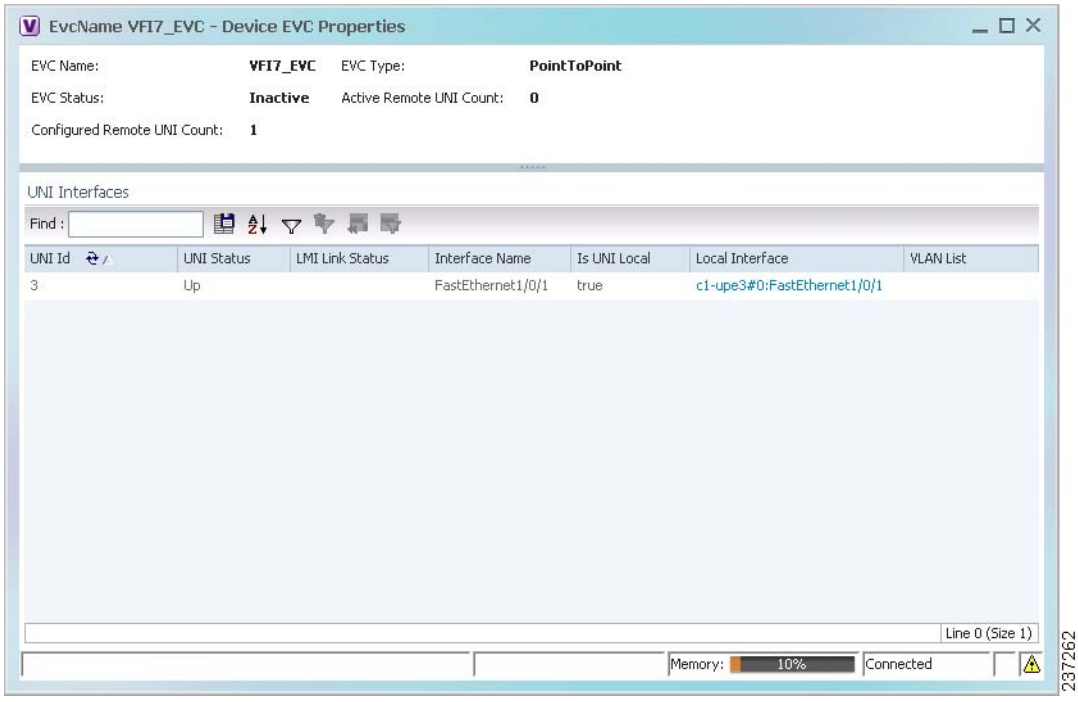


Table 15-9 describes the information displayed in the Device EVC Properties window.

Table 15-9 Device EVC Properties in Logical Inventory

Field	Description
EVC Name	Name of the EVC.
EVC Type	Type of EVC: Point-to-point or Multipoint.
EVC Status	EVC status: Active, Inactive, Not Defined, or Partially Active.
Maintenance Association	Hyperlinked entry to the maintenance association in CFM in logical inventory. For more information about maintenance associations, see Table 15-6.
Active Remote UNI Count	Number of active remote UNIs.
Configured Remote UNI Count	Number of configured remote UNIs.
UNI Interfaces Table	
UNI Id	UNI identifier.
UNI Status	Status of the UNI: Up or Down.
LMI Link Status	Status of the LMI link: Up or Down.
Interface Name	Interface on which UNI is configured.
Is UNI Local	Whether or not UNI is local: True or False.
Local Interface	Hyperlinked entry to the interface in physical inventory.
VLAN List	Name of the VLAN associated with the UNI interface.

Step 4 To view properties for an Ethernet LMI interface in physical interface, click the required interface name in the ELMI Interfaces table.

Table 15-10 describes the information displayed in the UNI Properties area in physical inventory.

Table 15-10 Ethernet LMI UNI Properties in Physical Inventory

Field	Description
Service Multiplexing Enabled	Whether or not the interface is configured for UNI multiplexing: True or False.
Bundling Enabled	Whether or not the interface is configured for UNI bundling: True or False.
UNI Id	UNI identifier.
Bundling Type	Type of bundling applied: All-to-One or None. This field appears only when a bundling type is set.

Viewing Link OAM Properties

Link OAM is an optional sublayer implemented in the OSI Data Link Layer between the Logical Link Control and MAC sublayers.

The Link OAM frames, OAM Protocol Data Units (OAMPDUs), cannot propagate beyond a single hop within an Ethernet network. Link OAM processes include:

- Discovery—Discovery is the first Link OAM process. During discovery, Link OAM identifies the devices at each end of the link and learns their OAM capabilities.
- Link monitoring—Link OAM link monitoring includes:
  - Monitoring links and issuing notifications when error thresholds are exceeded or faults occur.
  - Collecting statistics on the number of frame errors (or percent of frames that have errors) and the number of coding symbol errors.
- Remote MIB Variable Retrieval—Provides 802.3ah MIB polling and response (but not writing).
- Remote Failure indication—Informs peers when a received path goes down. Because link connectivity faults caused by slowly deteriorating quality are difficult to detect, Link OAM communicates such failure conditions to its peer using OAMPDU flags. The failure conditions that can be communicated are a loss of signal in one direction on the link, an unrecoverable error (such as a power failure), or some other critical event.
- Remote Loopback—Puts the peer device in (near-end) intrusive loopback mode using the OAMPDU loopback control. Statistics can be collected during the link testing. In loopback mode, every frame received is transmitted back unchanged on the same port (except for OAMPDUs, which are needed to maintain the OAM session). Loopback mode helps ensure the quality of links during installation or troubleshooting. Loopback mode can be configured so that the service provider device can put the customer device into loopback mode, but the customer device cannot put the service provider device in loopback mode.

Prime Network Vision supports topology discovery based on Link OAM information and enables you to view Link OAM properties.

To view Link OAM properties:

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

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

Figure 15-8 shows an example of Link OAM properties in logical inventory.

Figure 15-8 Link OAM Properties in Logical Inventory

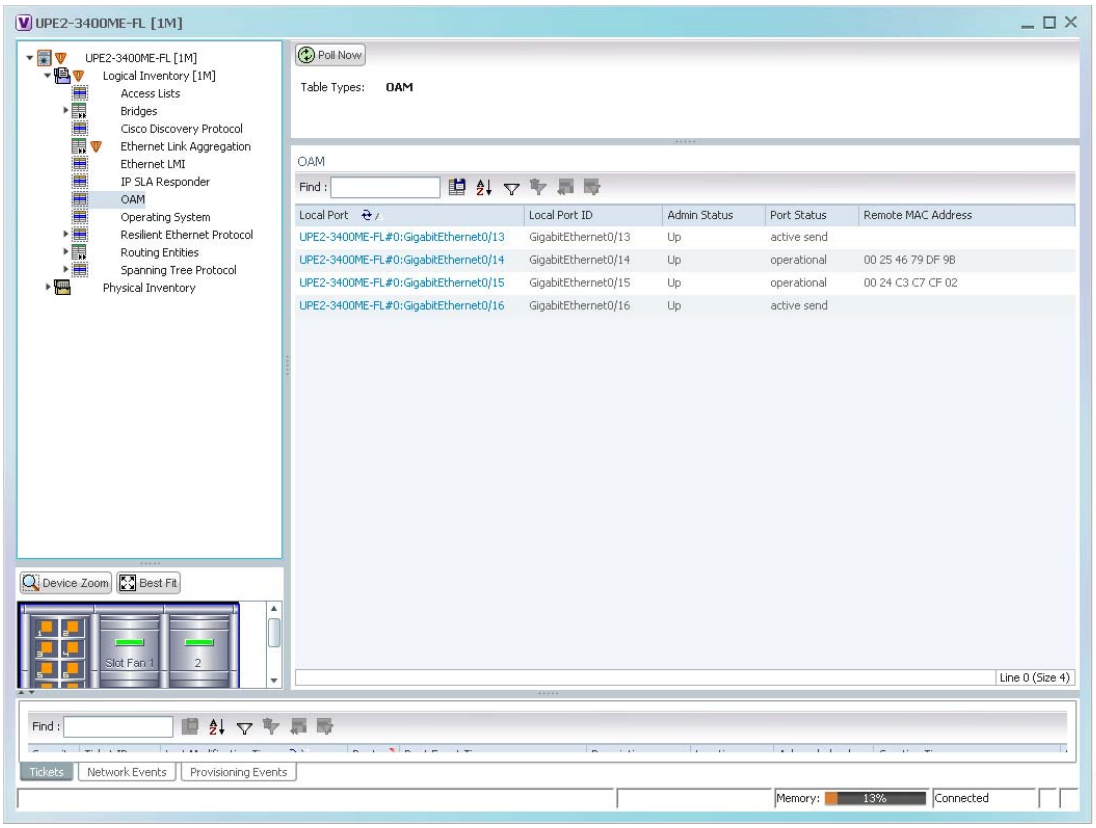


Table 15-11 describes the information displayed for Link OAM.

Table 15-11 Link OAM Properties in Logical Inventory

Field	Description
Table Types	Type of table. In this case, it is OAM.
OAM Table	
Local Port	Name of the OAM-supported interface, hyperlinked to the location in physical inventory.
Local Port ID	Local port identifier, such as FastEthernet1/0/9.
Admin Status	Administrative status of the interface.
Port Status	Status of the port.
Remote MAC Address	Remote client MAC address.

Step 3 To view detailed information about an entry in the table, double-click the required entry.

The Link OAM Data Properties window is displayed as shown in Figure 15-9.

Figure 15-9 Link OAM Data Properties Window

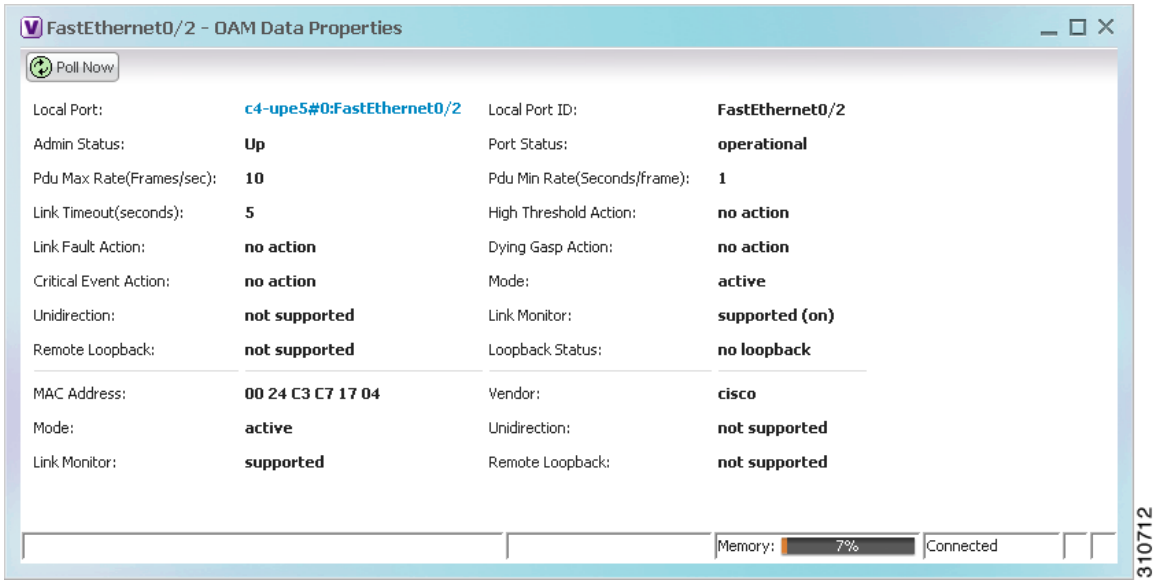


Table 15-12 describes the information that is displayed in the Link OAM Data Properties window.

Table 15-12 Link OAM Data Properties Window

Field	Description
Local Interface	
Local Port	Name of the OAM-supported interface, hyperlinked to the location in physical inventory.
Local Port ID	Local port identifier.
Admin Status	Administrative status of the interface: Up or Down.
Port Status	Status of the port, such as Operational.
PDU Max Rate (Frames/sec)	Maximum transmission rate measured by the number of OAM PDUs per second; for example, 10 packets per second.
PDU Min Rate (Seconds/frame)	Minimum transmission rated measured by the number of seconds required for one OAM PDU; for example, 1 packet per 2 seconds.
Link Timeout	Number of seconds of inactivity on a link before the link is dropped.
High Threshold Action	Action that occurs when the high threshold for an error is exceeded.
Link Fault Action	Action that occurs when the signal is lost.

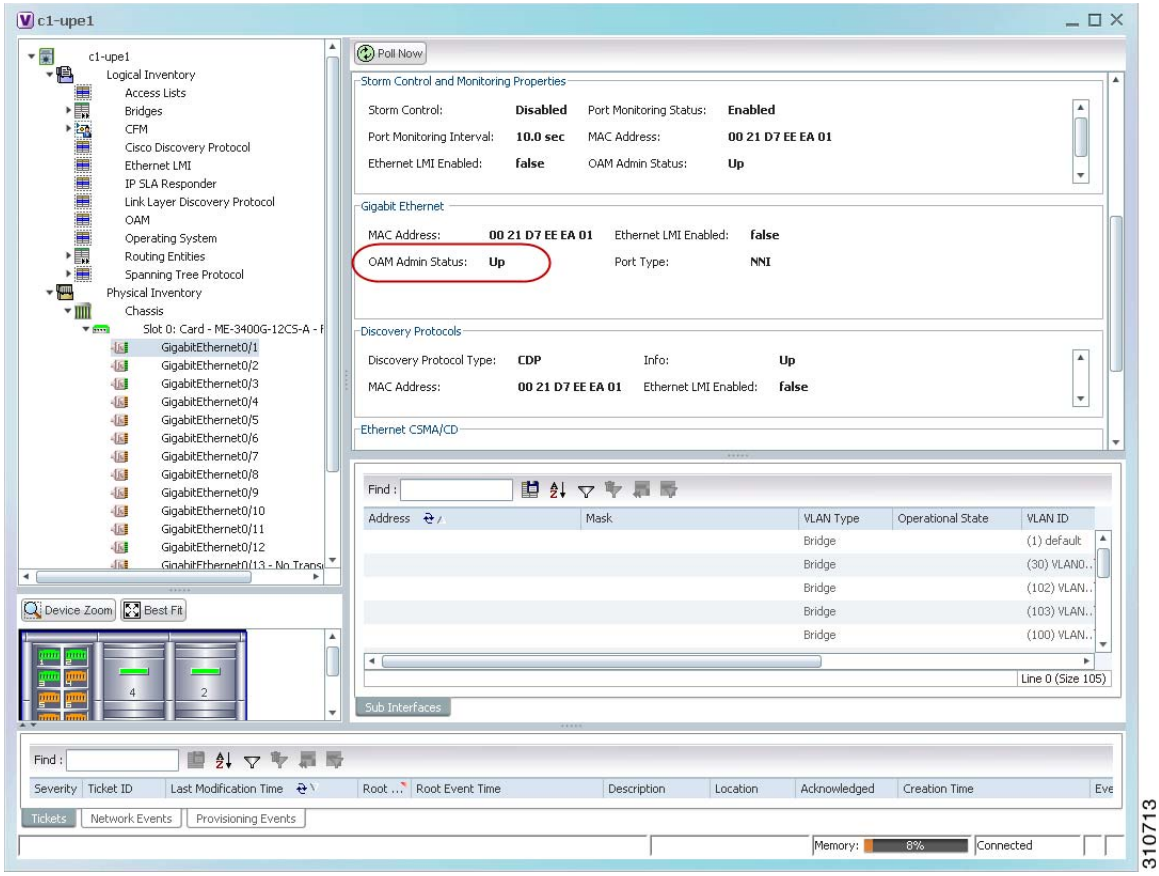
Table 15-12 Link OAM Data Properties Window (continued)

Field	Description
Dying Gasp Action	Action that occurs when an unrecoverable condition is encountered.
Critical Event Action	Action that occurs when an unspecified vendor-specific critical event occurs.
Mode	Mode of the interface: Active or Passive.
Unidirection	Status of unidirectional Ethernet on the local interface: Supported or Not supported.
Link Monitor	Status of link monitoring on the local interface: Supported or Not supported.
Remote Loopback	Status of remote loopback on the local interface: Supported or Not supported.
Loopback Status	Status of loopback on the local interface: Supported or No loopback.
Remote Client	
MAC Address	MAC address for the remote client.
Vendor	Vendor of the remote client.
Mode	Mode of the remote client: Active or Passive.
Unidirection	Status of unidirectional Ethernet on the remote client interface: Supported or Not supported.
Link Monitor	Status of link monitoring on the remote client interface: Supported or Not supported.
Remote Loopback	Status of loopback on the remote client interface: Supported or Not supported.

Step 4 To view Link OAM status in physical inventory, choose **Physical Inventory** > *chassis* > *slot* > *interface*.

The Link OAM administrative status is displayed as shown in Figure 15-10.

Figure 15-10 Link OAM Administrative Status in Physical Inventory





CHAPTER 16

IPv6 and IPv6 VPN over MPLS

Cisco Prime Network (Prime Network) supports IPv6 for:

- Gateways, clients, and units using IPv6.
- Communications between VNEs and devices in IPv6 environments, whether the device management IP address is IPv4 or IPv6.
- Polling and notification using the following protocols over IPv6:
  - SNMP v1, SNMPv2c, and SNMPv3
  - Telnet
  - SSHv2
  - ICMP
  - XML (for Cisco IOS XR devices)
  - HTTP (for Cisco UCS devices)
- All reports with devices that use IPv6 addresses.
- Fault management, including event processing and service alarm generation.

Prime Network supports correlation and path tracing for:

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

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

In 6VPE environments, Prime Network supports:

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

User Roles Required to Work with IPv6 and 6VPE

This topic identifies the roles that are required to work with IPv6 and 6VPE in Prime Network Vision. Prime Network determines whether you are authorized to perform a task as follows:

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

For more information on user authorization, see the *Cisco Prime Network 3.9 Administrator Guide*.

The following tables identify the tasks that you can perform:

- Table 16-1 identifies the tasks that you can perform if a selected element **is not in** one of your assigned scopes.
- Table 16-2 identifies the tasks that you can perform if a selected element **is in** one of your assigned scopes.

By default, users with the Administrator role have access to all managed elements. To change the Administrator user scope, see the topic on device scopes in the *Cisco Prime Network 3.9 Administrator Guide*.

Table 16-1 Default Permission/Security Level Required for Viewing IPv6 Properties - Element Not in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View IPv6 properties	—	—	—	—	X

Table 16-2 Default Permission/Security Level Required for Viewing IPv6 Properties - Element in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View IPv6 properties	X	X	X	X	X

Viewing IPv6 Information

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

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

Table 16-3 describes where IPv6 information appears in logical and physical inventory.

Table 16-3 IPv6 Information in Inventory

Inventory Location	Description
Logical Inventory	
6rd Tunnels	The Tunnel Edges table displays IPv6 addresses and the IPv6 prefixes that are used to translate IPv4 addresses to IPv6 addresses. For more information, see Viewing 6rd Tunnel Properties, page 17-43.
Access Lists	• The Type field displays IPv6 for IPv6 access lists. • If an IPv6 access list is configured, the Access List Properties window displays IPv6 addresses in the Source, Destination, Source Wildcard, and Destination Wildcard fields.
Carrier Grade NAT	Carrier Grade NAT service types include 6rd and XLAT. For more information, see Viewing Carrier Grade NAT Properties in Logical Inventory, page 13-2.
GRE Tunnels	The IP Address field supports IPv6 addresses. For more information, see Viewing MPLS Pseudowire over GRE Properties, page 18-31.
IS-IS	IS-IS properties support: • IPv6 address families in the Metrics tab. • IPv6 addresses in the Neighbors tab and the IS-IS Neighbor Properties window. For more information, see Viewing IS-IS Properties, page 12-110.
MPBGPs	• IP address family identifiers indicate the BGP peer address family: IPv4, IPv6, Layer 2 VPN, VPNv4, or VPNv6. • MP-BGP BGP neighbor entries display IPv6 addresses. For information, see Viewing MP-BGP Information, page 17-42.
OSPFv3	IPv6 addresses are displayed for OSPF neighbor interface addresses, OSPF interface internet addresses, OSPF neighbor properties window, and OSPF interface properties window. For more information, see Viewing OSPF Properties, page 12-113.

Table 16-3 IPv6 Information in Inventory (continued)

Inventory Location	Description
Routing Entities	• IPv6 addresses appear in the IP Interfaces tab, the IPv6 Routing tab, and the interface properties window. • IPv6 addresses are displayed in the NDP Table tab and the ARP Entry Properties window. • VRRP groups using IPv6 display IPv6 addresses in the IP Interfaces Properties window in the VRRP group tab. For more information, see Viewing Routing Entities, page 17-31.
VRFs	IPv6 addresses appear in the IPv6 tab, Sites tab, VRF Properties window, and IP Interface Properties window. For more information, see Viewing VRF Properties, page 17-27.
Physical Inventory	
Port	IPv6 addresses appear in the Subinterfaces tab and interface properties popup window.

The IP addresses that appear depend on whether the interface has only IPv4 addresses, only IPv6 addresses, or both IPv4 and IPv6 addresses, as shown in Table 16-4.

Table 16-4 IP Addresses Displayed in the Interface Table and Properties Window

Addresses	Interface Table	Properties Window
IPv4 only	Primary IPv4 address	The primary IPv4 address and any secondary IPv4 addresses.
IPv6 only	Lowest IPv6 address	All IPv6 addresses.
IPv6 and IPv4	Primary IPv4 address	All IPv4 and IPv6 addresses.

Note the following when working with IPv6 addresses:

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

```
12AB::CD30:123:4567:89AB:CDEF, 12AB:0:0:CD30::/60
```

Note Interfaces or subinterfaces that do not have IP addresses are not discovered and therefore are not shown in Prime Network Vision.

Figure 16-1 shows a port inventory view of a port with IPv4 and IPv6 addresses. In this example, one IPv4 address and multiple IPv6 addresses are provisioned on the interface.

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

Figure 16-1 Port with IPv4 and IPv6 Addresses

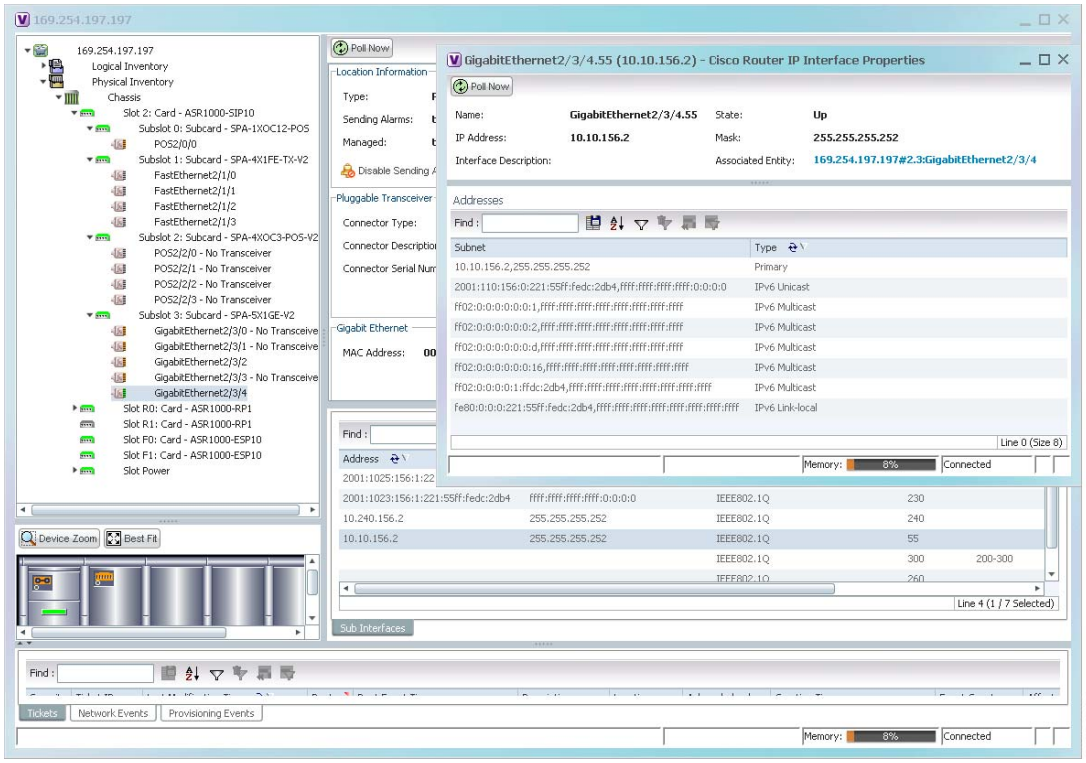
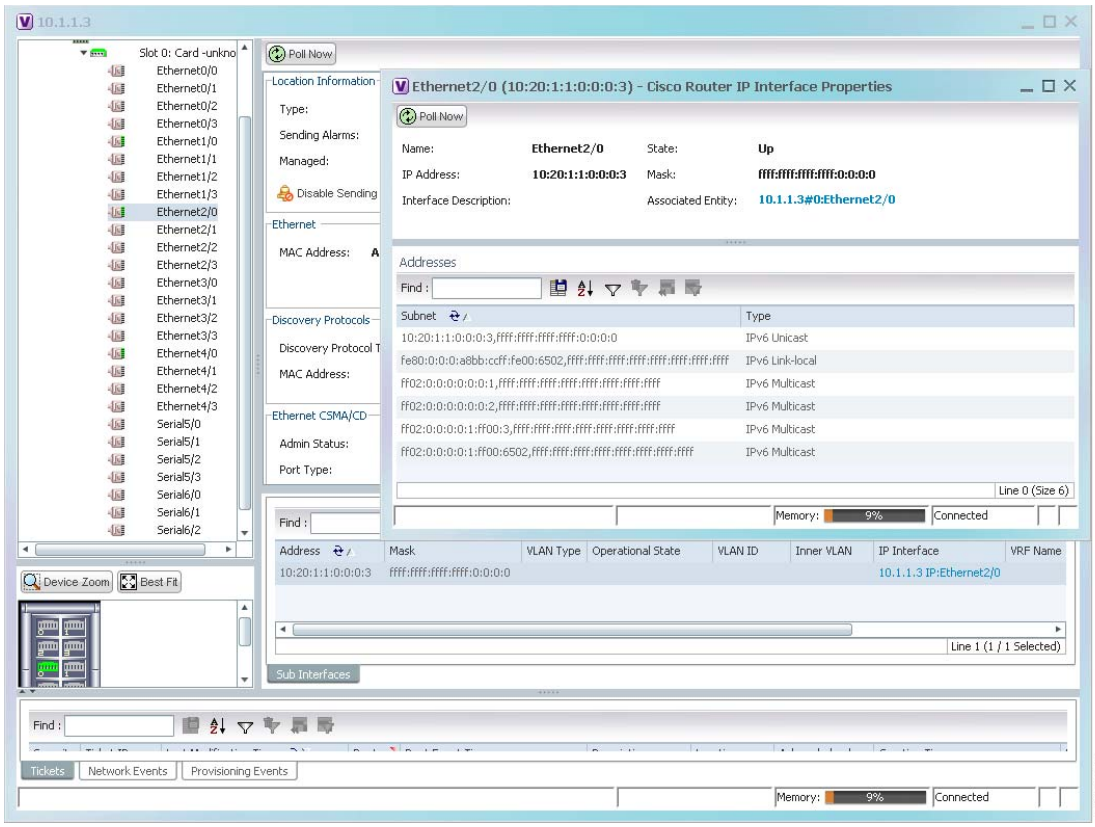


Figure 16-2 shows a port with only IPv6 addresses provisioned. In this example, the lowest IPv6 address is shown in the subinterface table, and all IPv6 addresses are shown in the interface properties window.

Figure 16-2 Port with IPv6 Addresses





CHAPTER 17

Monitoring MPLS Services

The following topics describe how to view and manage aspects of Multiprotocol Label Switching (MPLS) services using Cisco Prime Network Vision (Prime Network Vision), including the MPLS service view, business configuration, and maps. The topics also describe the device inventory specific to MPLS VPNs, including routing entities, label switched entities (LSEs), BGP neighbors, Multiprotocol BGP (MP-BGP), VRF instances, pseudowires, and TE tunnels. Topics include:

- User Roles Required to Work with MPLS Networks, page 17-1
- Working with MPLS-TP Tunnels, page 17-4
- Viewing VPNs, page 17-18
- Managing VPNs, page 17-21
- Working with VPN Overlays, page 17-24
- Monitoring MPLS Services, page 17-26

User Roles Required to Work with MPLS Networks

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

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

For more information on user authorization, see the *Cisco Prime Network 3.9 Administrator Guide*.

The following tables identify the tasks that you can perform:

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

By default, users with the Administrator role have access to all managed elements. To change the Administrator user scope, see the topic on device scopes in the *Cisco Prime Network 3.9 Administrator Guide*.

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

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

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

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

Working with MPLS-TP Tunnels

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

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

MPLS-TP features include:

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

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

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

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

The following options are available for working with MPLS-TP tunnels in Prime Network Vision:

- Adding an MPLS-TP Tunnel, page 17-5
- Viewing MPLS-TP Tunnel Properties, page 17-7
- Viewing LSPs Configured on an Ethernet Link, page 17-11
- Viewing LSP Endpoint Redundancy Service Properties, page 17-13
- Applying an MPLS-TP Tunnel Overlay, page 17-16
- Viewing MPLS-TP BFD session properties—See Viewing BFD Session Properties, page 17-44.

Adding an MPLS-TP Tunnel

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

To add an MPLS-TP tunnel to a map:

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

Step 2 Do either of the following:

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

The Add MPLS-TP Tunnel dialog box is displayed.

Step 3 Do either of the following:

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

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

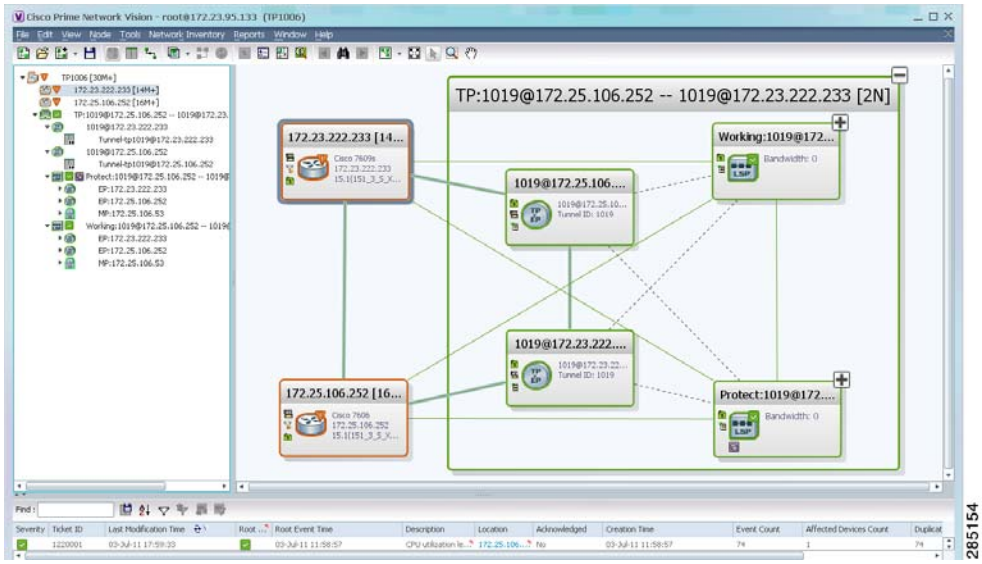
Step 5 Click **OK**.

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

In Figure 17-1:

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

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

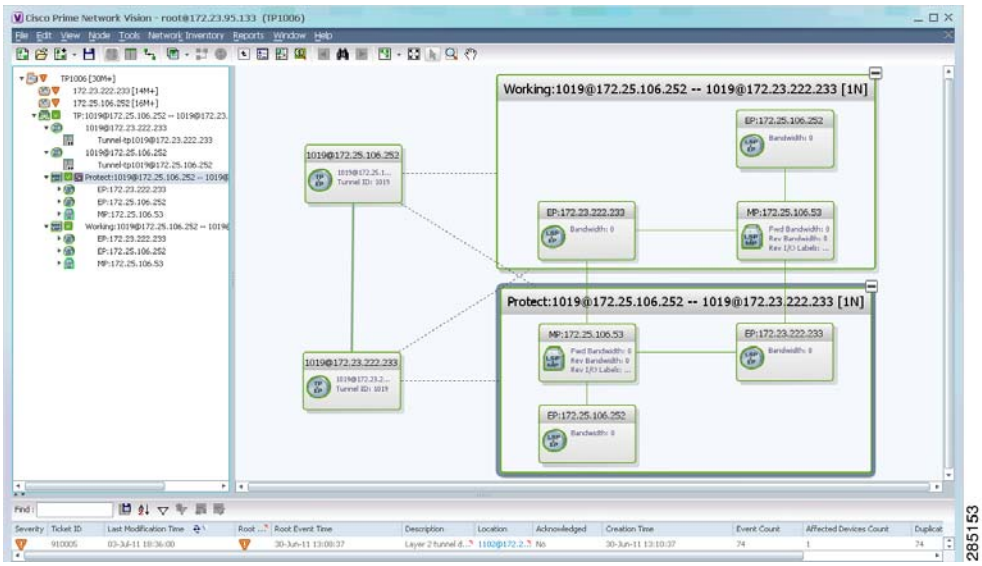


If an LSP is in lockout state, it is displayed with the lock badge ( ).

By expanding all aggregations in the MPLS-TP tunnel (see Figure 17-2), you can see components and links in the MPLS-TP tunnel, including:

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

Figure 17-2 MPLS-TP Tunnel Expanded



If an LSP is configured for redundancy service, a redundancy service badge is applied to the secondary (backup) LSP in the navigation and map panes in the navigation and map panes.

For more information about LSP redundancy service, see Viewing LSP Endpoint Redundancy Service Properties, page 17-13.

Viewing MPLS-TP Tunnel Properties

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

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

- Routing Entities—See Viewing Routing Entities, page 17-31.
- LSEs—See Viewing Label Switched Entity Properties, page 17-38.
- Pseudowires— See Viewing Pseudowire End-to-End Emulation Tunnels, page 17-47.

To view MPLS-TP tunnel properties:

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

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

The routing information is displayed as shown in Figure 17-3.

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

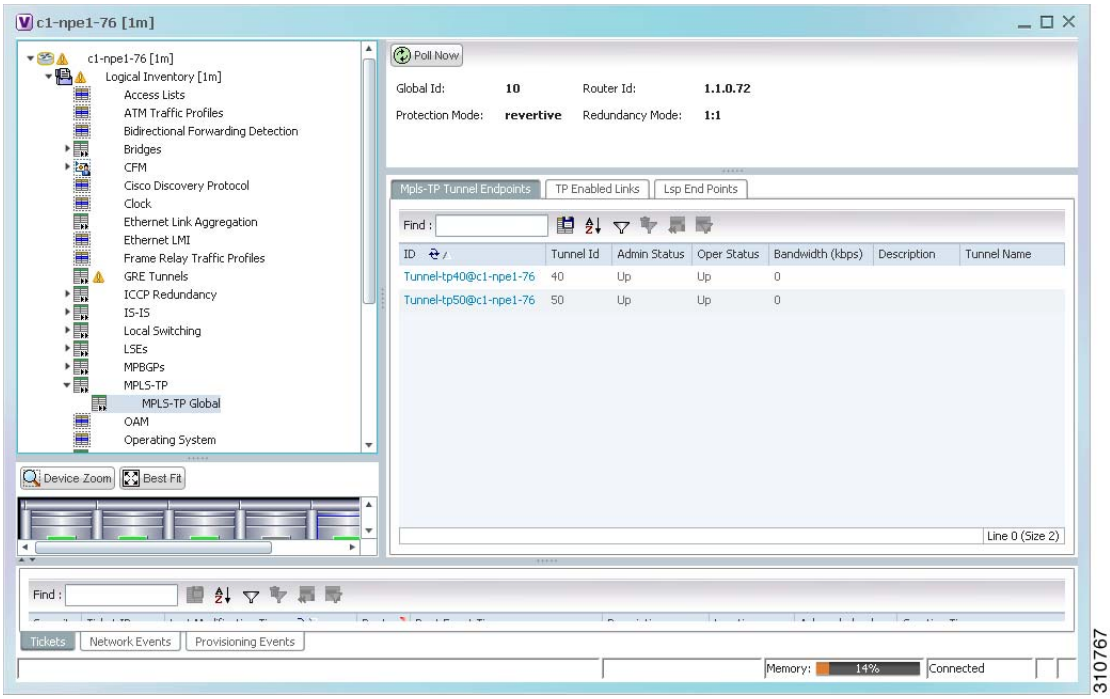


Table 17-3 describes the information that is available for MPLS-TP tunnels. The information that is displayed depends on the configuration.

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

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

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

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

Step 3 To view additional MPLS-TP tunnel endpoint properties, double-click the required entry in the MPLS-TP Tunnel Endpoints table.

The MPLS-TP Tunnel Properties window is displayed as shown in Figure 17-4.

Figure 17-4 MPLS-TP Tunnel Properties Window

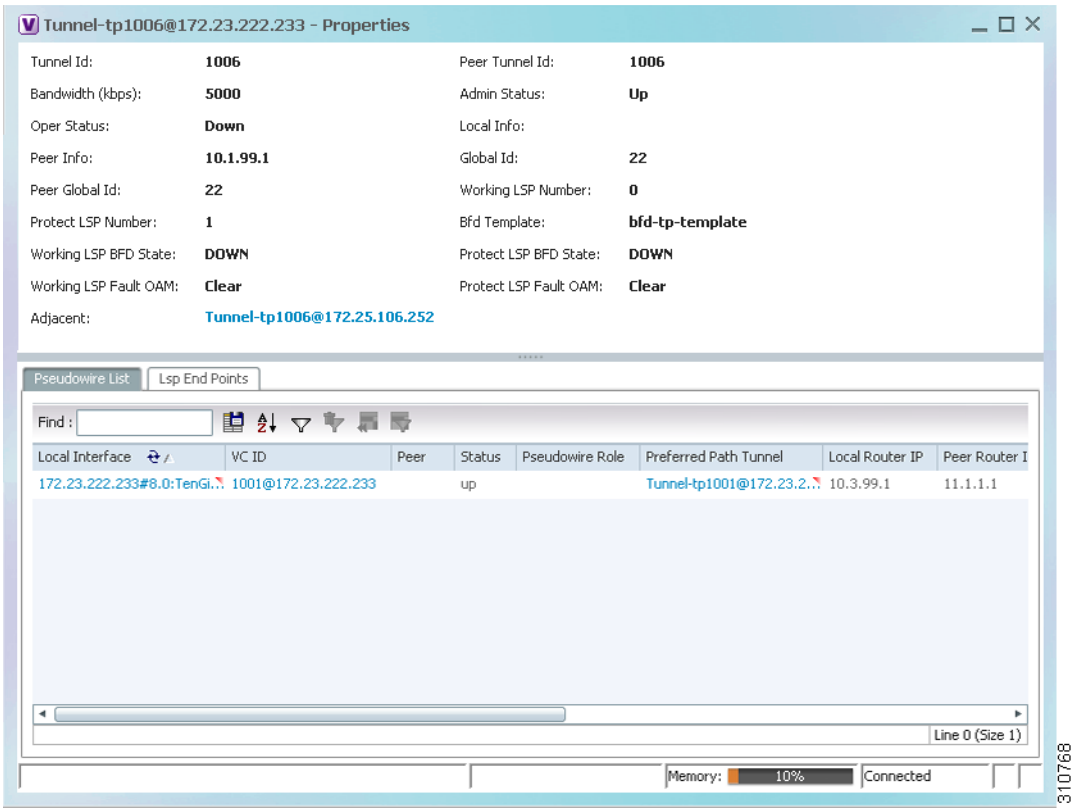


Table 17-4 describes the information available in the top portion of the MPLS-TP Tunnel Properties window. For information about the tabs that are displayed, see Table 17-3.

Table 17-4 MPLS-TP Tunnel Properties Window

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

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

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

Viewing LSPs Configured on an Ethernet Link

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

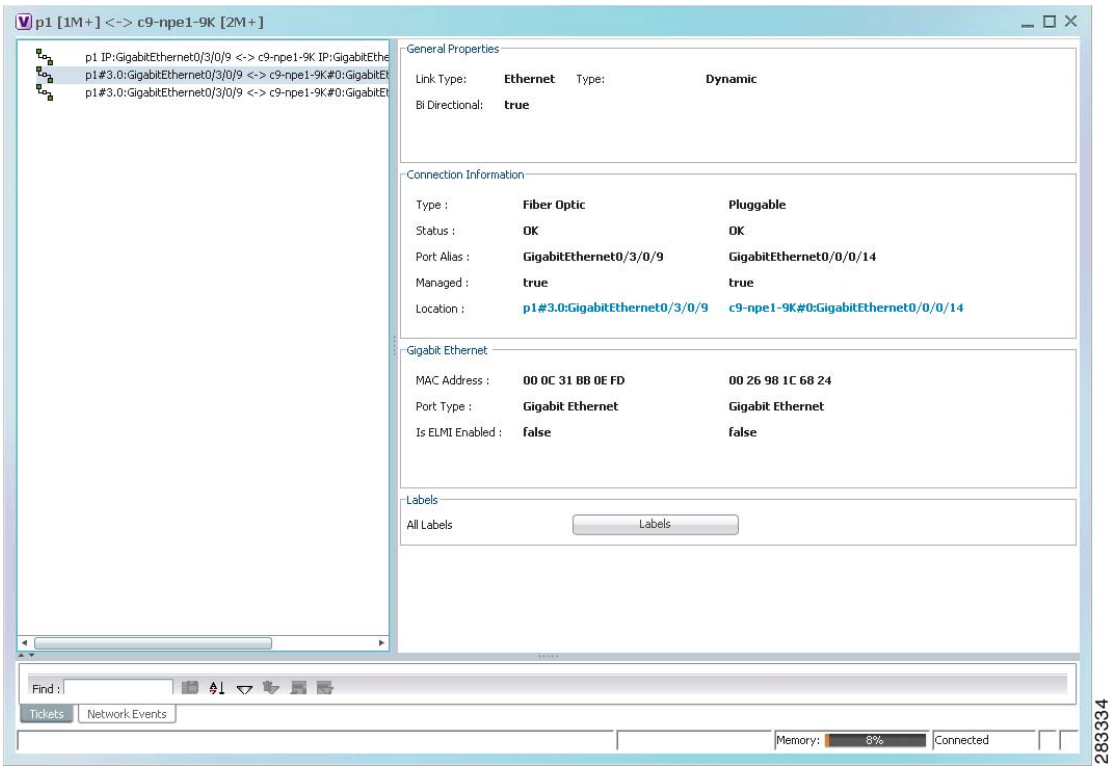
To view LSPs configured on an Ethernet link:

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

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

The link properties window refreshes and displays the Labels button as shown in Figure 17-5.

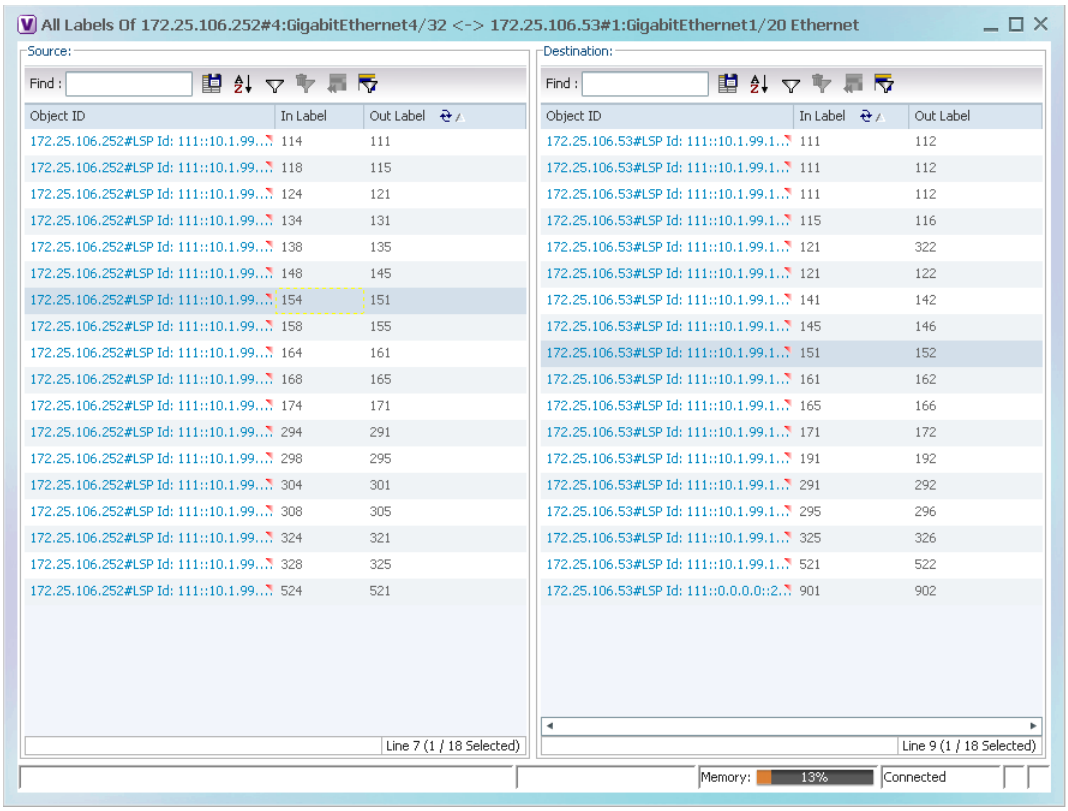
Figure 17-5 Link Properties Window with All Labels Button



Step 3 Click **Labels**.

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

Figure 17-6 All Labels Table



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

Viewing LSP Endpoint Redundancy Service Properties

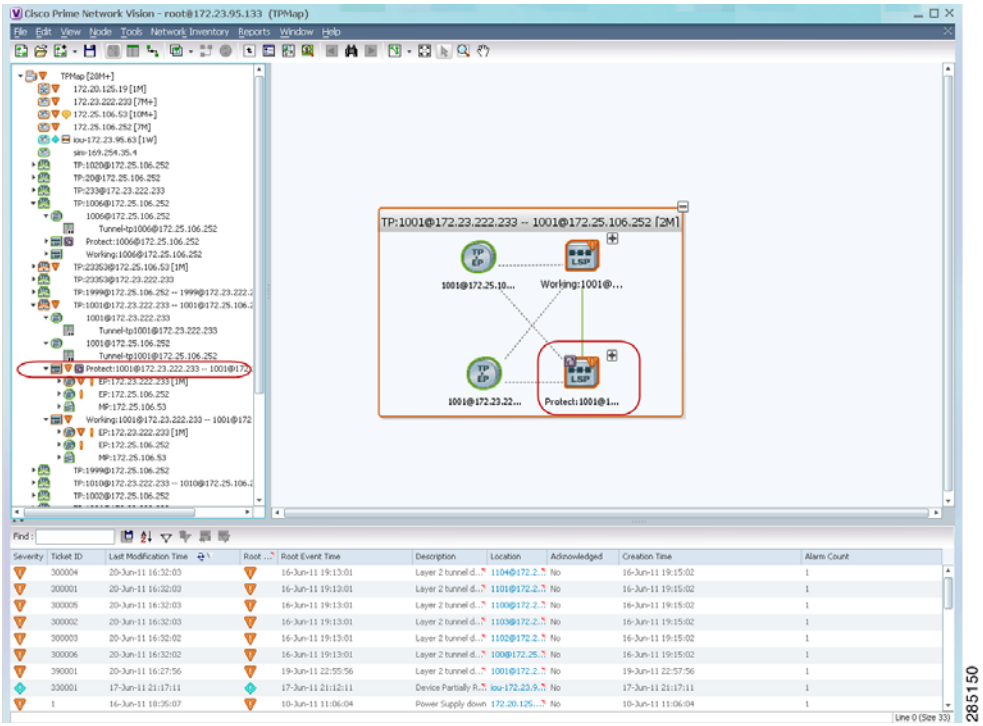
If an LSP endpoint in an MPLS-TP tunnel is configured for redundancy service, a redundancy service badge is applied to the secondary (backup) LSP endpoint in the navigation and map panes in Prime Network Vision. Additional redundancy service details are provided in the LSP endpoint properties window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

To view LSP endpoint redundancy service properties:

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

If the LSP endpoint is configured for redundancy service, the redundancy service badge is displayed in the navigation and map panes as shown in Figure 17-7.

Figure 17-7 LSP Endpoint with Redundancy Service Badge



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

The LSP endpoint properties window is displayed as shown in Figure 17-8.

Figure 17-8 LSP Endpoint Properties Window

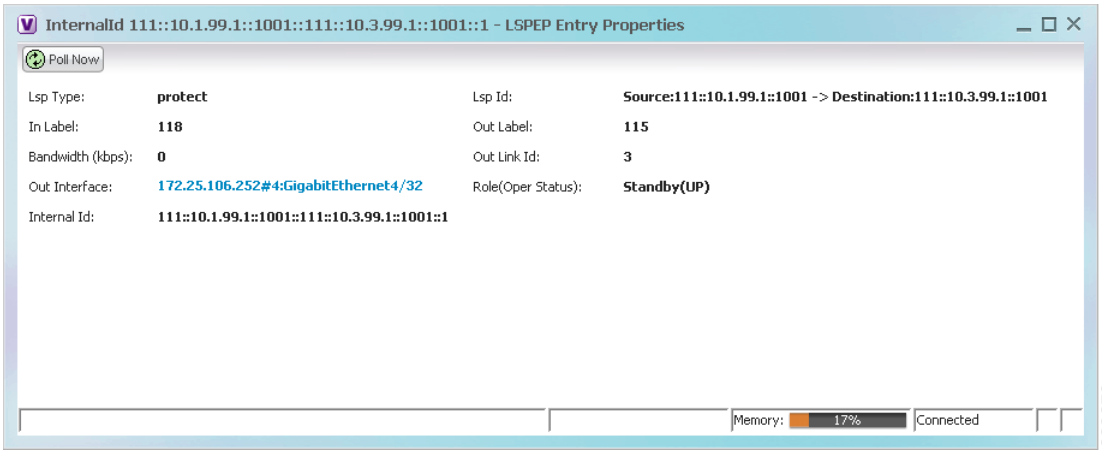


Table 17-5 describes the information displayed in the LSP Endpoint Properties window.

Table 17-5 LSP Endpoint Properties Window

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

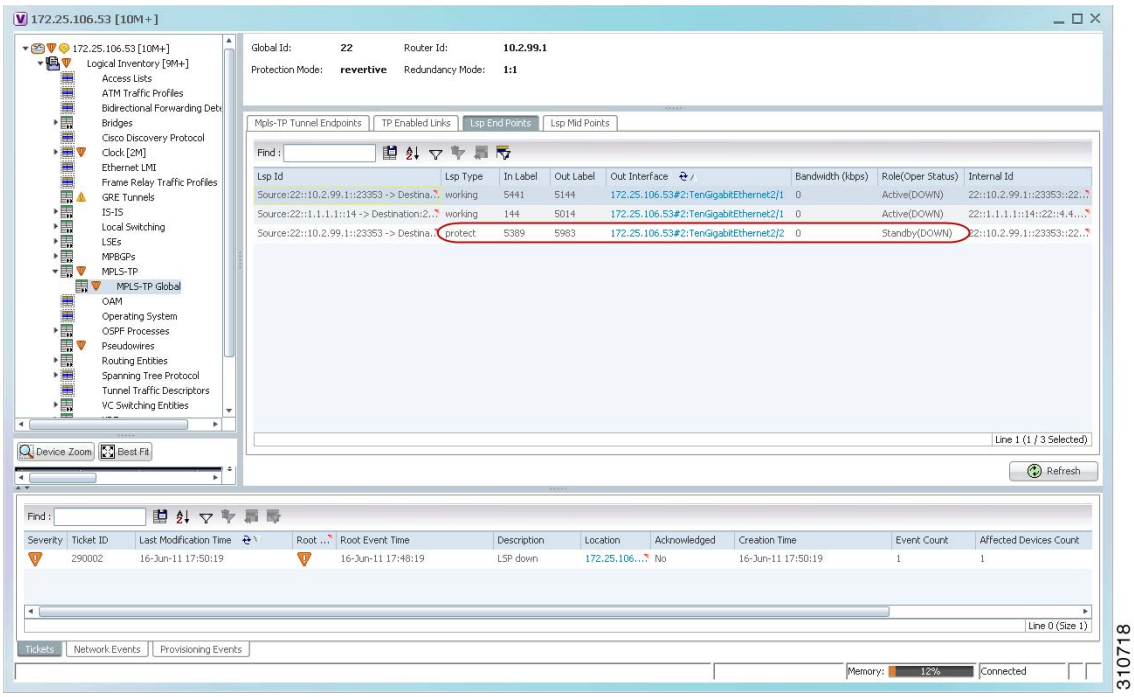
Step 3 To view LSP endpoint redundancy status in inventory, double-click the element on which the MPLS-TP tunnel is configured.

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

Step 5 The LSP End Points tab contains the following information related to LSP redundancy service (see Figure 17-9):

- Whether the LSP endpoint is Working or Protected.
- The LSP endpoint role, either Active or Standby.
- The operational status of the LSP endpoint, either Up or Down.

Figure 17-9 LSP End Points Tab in Logical Inventory



Applying an MPLS-TP Tunnel Overlay

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

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

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

To apply an MPLS-TP tunnel overlay:

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

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

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

Step 3 Do one of the following:

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

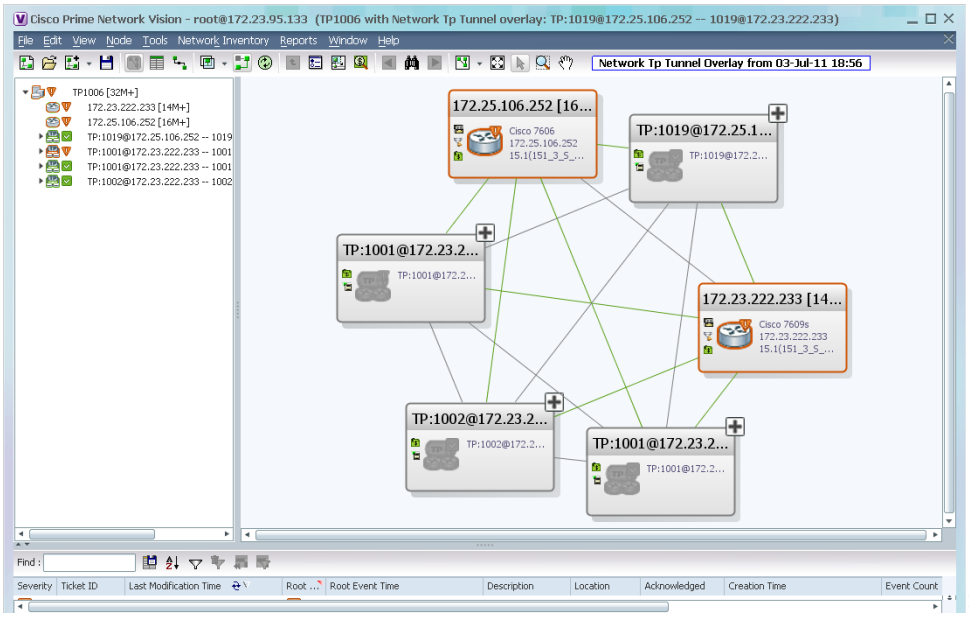
The search condition is “contains.” Search strings are case-insensitive. For example, if you choose the Name category and enter “net,” Prime Network Vision displays MPLS-TP tunnels that have “net” in their names whether net appears at the beginning of the name, the middle, or at the end: for example,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

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

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

The elements and links used by the selected MPLS-TP tunnel are highlighted in the network map, and the MPLS-TP tunnel name is displayed in the window title bar as shown in Figure 17-10.

Figure 17-10 MPLS-TP Tunnel Overlay

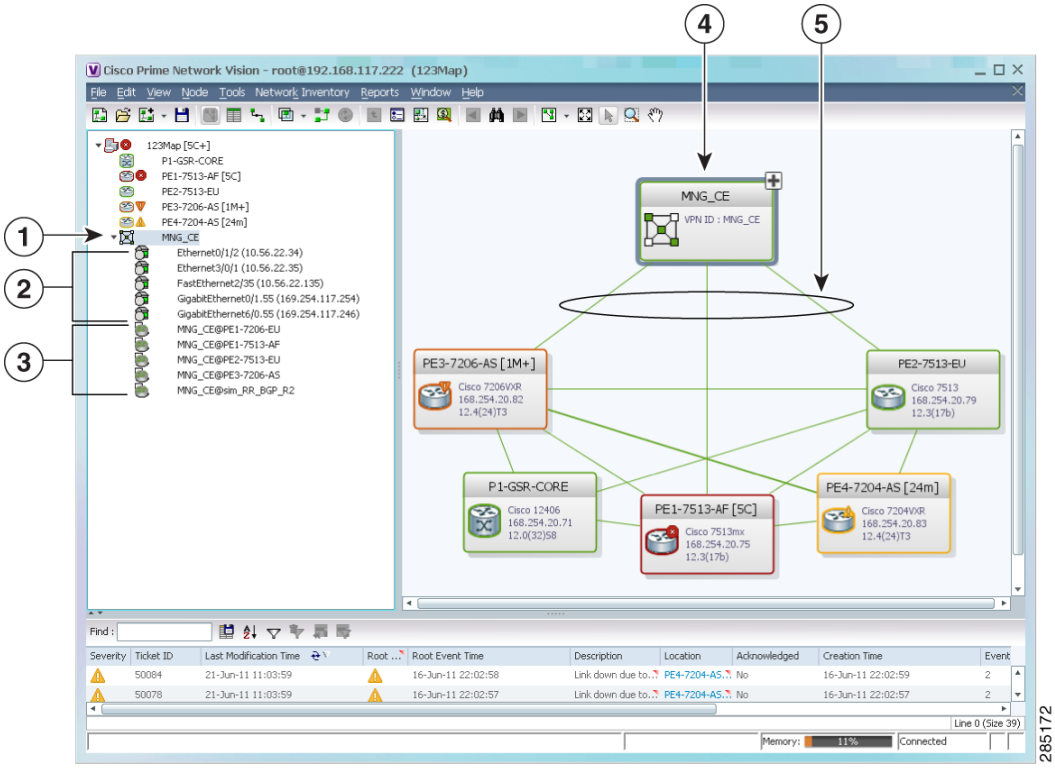


Note An overlay is a snapshot taken at a specific point in time and does not reflect changes that occur in the service. As a result, the information in an overlay can become stale. To update the overlay, click **Refresh Overlay** in the main toolbar.

Viewing VPNs

Figure 17-11 shows a VPN displayed in the Prime Network Vision map view. In this example, the VPN is selected in the navigation pane, so the VPN details, such as virtual routers and IP interfaces, are not shown in the map view.

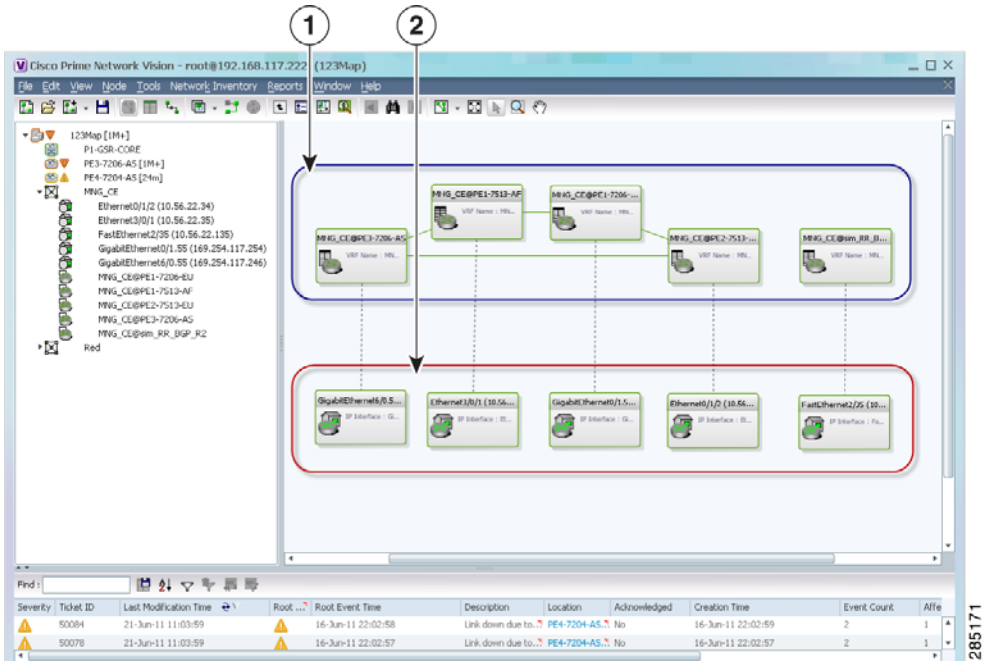
Figure 17-11 VPN in Prime Network Vision Map View



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

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

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



1	Virtual routers
2	Sites

The Prime Network Vision navigation pane displays the VPN business elements in a tree-and-branch representation. Each business element is represented by an icon in a color that reflects the highest alarm severity. The icon might also have a management state badge or alarm. For more information about icon severity colors and badges, see Prime Network Vision Status Indicators, page 2-24.

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

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

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

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

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

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

Viewing Additional VPN Properties

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

Table 17-7 Displaying Additional VPN Properties

Object	Option	For Additional Information
VPN	• Double-click a VPN to view the participating VRFs, sites, and network elements in the navigation pane and map view. • Right-click a VPN and choose **Properties** to view the VPN Properties window.	Viewing VPN Properties, page 17-26
VRF	Double-click a VRF to view the VRF properties window.	Viewing VRF Properties, page 17-27

Table 17-7 Displaying Additional VPN Properties (continued)

Object	Option	For Additional Information
Site	Double-click a site to view the IP Interface Properties window	Viewing Site Properties, page 17-27
Link	Double-click a link to view the link properties window. The properties that are depend on the link type.	Chapter 5, "Working with Links"

Managing VPNs

The following topics describe:

- Creating a VPN, page 17-21
- Adding a VPN to a Map, page 17-22
- Removing a VPN from a Map, page 17-23
- Moving a Virtual Router Between VPNs, page 17-23

Creating a VPN

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

To create a VPN:

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

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

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

- Name—A unique name for the new VPN.

  Note VPN business element names are case sensitive.

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

  Note If a path is not specified to an icon, the default VPN icon is used (for more information about icons, see Table 17-6 on page 17-20).

- Description—(Optional) An additional VPN description.

Step 4 Click **OK**.

The new VPN is added to the VPN list in the Add VPN dialog box.

For more information about loading the newly created VPN in the service view map, see Adding a VPN to a Map, page 17-22.

Adding a VPN to a Map

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

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

To add an existing VPN to a map:

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

Step 2 Do either of the following:

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

The Add VPN dialog box is displayed.

Step 3 Do either of the following:

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

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

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

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

Step 5 Click **OK**.

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

Removing a VPN from a Map

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

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

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

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

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

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

Moving a Virtual Router Between VPNs

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

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

To move a virtual router:

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

Step 2 Right-click the required VPN in the navigation pane or map to where you want to move the virtual router and choose **Edit > Move here**.

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

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

Working with VPN Overlays

The following topics describe:

- Applying VPN Overlays, page 17-24
- Managing a VPN Overlay Display in the Map View, page 17-25
- Displaying VPN Callouts in a VPN Overlay, page 17-25

Applying VPN Overlays

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

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

To apply a VPN overlay:

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

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

The Select VPN Overlay dialog box is displayed.

Step 3 Do one of the following:

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

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

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

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

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

Managing a VPN Overlay Display in the Map View

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

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

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

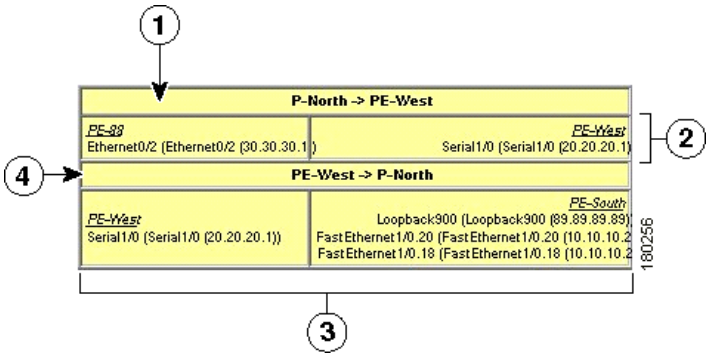
- To remove the VPN overlay, choose **Show Overlay Type > None**.

Displaying VPN Callouts in a VPN Overlay

You can display or hide the callouts for VPN links displayed in a VPN overlay to show the details of the sites that are interlinked through the selected links. The callouts (see Figure 17-13) enable you to view the VPN traffic links for a specific link (either bidirectional or unidirectional).

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

Figure 17-13 Callouts Window



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

To display or hide the callouts:

Step 1 In the Prime Network Vision window, display the map view with the VPN overlay.

Step 2 Right-click the required link in the map view and choose **Show Callouts**.

Step 3 To hide the callouts, right-click the link in the map view that is displaying the callouts and choose **Hide Callouts**.

Monitoring MPLS Services

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

- Viewing VPN Properties, page 17-26
- Viewing Site Properties, page 17-27
- Viewing VRF Properties, page 17-27
- Viewing VRF Egress and Ingress Adjacents, page 17-30
- Viewing Routing Entities, page 17-31
- Viewing Label Switched Entity Properties, page 17-38
- Viewing MP-BGP Information, page 17-42
- Viewing BFD Session Properties, page 17-44
- Viewing Cross-VRF Routing Entries, page 17-47
- Viewing Pseudowire End-to-End Emulation Tunnels, page 17-47
- Viewing MPLS TE Tunnel Information, page 17-49

Viewing VPN Properties

To view the properties of a VPN:

Step 1 In the Prime Network Vision navigation pane or map view, do either of the following:

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

The VPN Properties window displays the following information:

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

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

Viewing Site Properties

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

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

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

Table 17-8 Router IP Interface Properties Window for Sites

Field	Description
Name	Name of the site, such as FastEthernet4/1.252.
State	Interface state, either Up or Down.
IP Address	IP address of the interface.
Mask	Network mask.
Interface Description	Description applied to the interface.
Associated Entity	Element and interface associated with the site, hyperlinked to its entry in physical inventory.
Addresses Table	
Subnet	IP address and subnet mask. **Note** If the site is an IPv6 VPN over MPLS with IPv6 addresses provisioned, the IPv6 addresses are displayed. For more information, see Viewing IPv6 Information, page 16-3.
Type	Address type, such as Primary, Secondary, or IPv6 Unicast.

Viewing VRF Properties

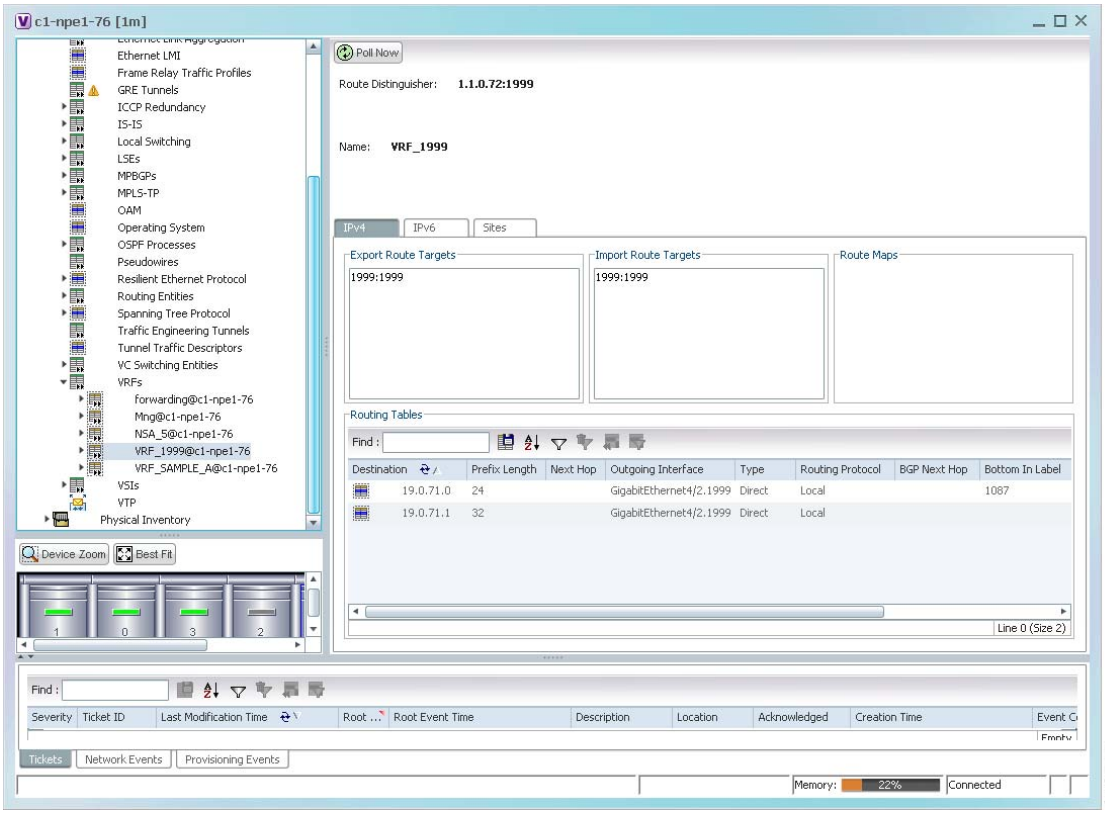
Prime Network Vision enables you to view VRF properties, including the VRF route distinguisher, import and export route targets, and any provisioned sites and VRF routes.

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

- Double-click the element configured for VRFs.
- Expand the required VPN and double-click the virtual router.

The VRF properties window is displayed as shown in Figure 17-14.

Figure 17-14 VRF Properties



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

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

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

Table 17-9 VRF Properties

Field	Description
Route Distinguisher	Route distinguisher configured in the VRF.
Name	VRF name.
Description	Description of the VRF.
IPv4 Tab	
Export Route Targets	IPv4 export route targets contained by the VRF.
Import Route Targets	IPv4 import route targets contained by the VRF.
Route Maps	Route maps for the VRF.
IPv6 Tab	
Export Route Targets	IPv6 export route targets contained by the VRF.
Import Route Targets	IPv6 import route targets contained by the VRF.
Route Maps	Route maps for the VRF.
Routing Tables	
Destination	Destination of the specific network.
Prefix Length	Length of the network prefix in bits.
Next Hop	Next routing hop.
Outgoing Interface	Name of the outgoing interface; displayed if the Routing Protocol type is local.
Type	Route type: Direct (local), Indirect, or Static.
Routing Protocol	Routing protocol used to communicate with the other sites and VRFs: BGP or local.
BGP Next Hop	Border Gateway Protocol (BGP) next hop. This is the PE address from which to continue to get to a specific address. This field is empty when the routing entry goes to the CE.
Bottom In Label	Innermost label that is expected when MPLS traffic is received.
Bottom Out Label	Innermost label sent with MPLS traffic.
Outer Label	Outermost or top label in the stack used for MPLS traffic.

Table 17-9 VRF Properties (continued)

Field	Description
Sites Tab	
Name	Site name.
IP Address	IP address of the interface.
Mask	Subnet mask.
State	State of the subinterface: Up or Down.
Associated Entity	Element and interface associated with the site, hyperlinked to its entry in physical inventory.
Description	Interface description.
Input Access List	Access list applied to the inbound traffic.
Output Access List	Access list applied to the outbound traffic.
Rate Limits	If a rate limit is configured on an IP interface, the limit is shown as an IP interface property. This option is checked when a rate limit is defined on the IP interface, meaning the access list is a rate limit access list. IP interface traffic is measured and includes the average rate, normal burst size, excess burst size, conform action, and exceed action. **Note** Double-clicking a row displays the properties of the IP interface. When a rate limit is configured on the IP interface, the Rate Limits tab is displayed. For more information about rate limits, see Viewing Rate Limit Information, page 17-35. **Note** The Input Access, Output Access, and Rate Limits parameters apply only to Cisco IOS devices.
IP Sec Map Name	IP Security (IPsec) map name.
Site Name	Name of the business element to which the interface is attached.

Viewing VRF Egress and Ingress Adjacents

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

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

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

Table 17-10 describes the information displayed in the Adjacents window.

Table 17-10 VRF Adjacents Properties Window

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

Viewing Routing Entities

To view routing entities:

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

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

The routing information is displayed as shown in Figure 17-15.

Figure 17-15 Routing Entity Table

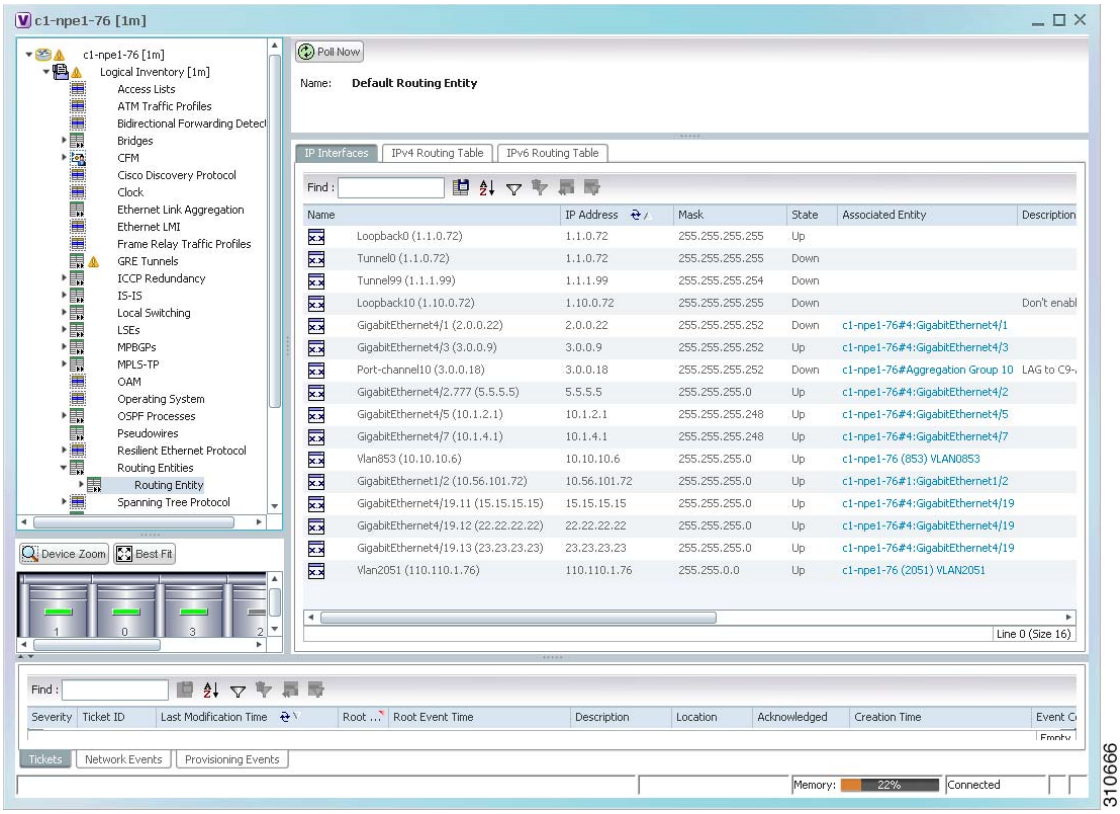


Table 17-11 describes the information that is displayed in the Routing Entity table.

Table 17-11 Routing Entity Table

Field	Description
Name	Name of the routing entity.
IP Interfaces Tab	
Name	Site name.
IP Address	IP address of the interface.
Mask	Network mask.
State	State of the subinterface: Up or Down.
Associated Entity	Interface associated with the routing entity, hyperlinked to its location in physical inventory.
Description	Description of the interface.
Input Access List	If an input access list is assigned to an IP interface, the list is shown as an IP interface property, and a hyperlink highlights the related access list in the Access List table. When an access list is assigned to the inbound traffic on an IP interface, the actions assigned to the packet are performed.
VRRP Group	If a VRRP group is configured on an IP interface, the information is shown as an IP interface property. This option is checked when a rate limit is defined on the IP interface. **Note** Double-clicking a row displays the properties of the IP interface. When a VRRP group is configured on an IP interface, the VRRP Groups tab is displayed in the IP Interface Properties window. For more information, see Viewing VRRP Information, page 17-36.
Output Access List	If an output access list is assigned to an IP interface, the list is shown as an IP interface property, and a hyperlink highlights the related access list in the Access List table. When an access list is assigned to the outbound traffic on an IP interface, the actions assigned to the packet are performed.
Rate Limits	If a rate limit is configured on an IP interface, the limit is shown as an IP interface property. This option is checked when a rate limit is defined on the IP interface, meaning the access list is a rate limit access list. IP interface traffic is measured and includes the average rate, normal burst size, excess burst size, conform action, and exceed action. **Note** Double-clicking a row displays the properties of the IP interface. When a rate limit is configured on the IP interface, the Rate Limits tab is displayed. For more information, see Viewing Rate Limit Information, page 17-35. **Note** The Input Access, Output Access, and Rate Limits parameters apply only to Cisco IOS devices.
IP Sec Map Name	IP Security (IPsec) crypto map name.
Site Name	Name of the business element to which the interface is attached.

Table 17-11 Routing Entity Table (continued)

Field	Description
IPv4 and IPv6 Routing Table Tabs	
Destination	Destination of the specific network.
Outgoing If Name	Name of the outgoing interface; displayed if the Routing Protocol type is local.
Type	Routing type: Direct, Indirect, Static, Other, Invalid, or Unknown.
Next Hop	IP address from which to continue to get to a specific address. This field is empty when the routing entry goes to a PE router.
Prefix Length	Length of the network prefix in bits.
Route Protocol Type	Routing protocol used to communicate with other routers.

Viewing the ARP Table

To view the ARP table:

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

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

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

Table 17-12 ARP Table

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

Viewing the NDP Table

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

NDP functionality includes:

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

To view the NDP table:

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

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

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

Figure 17-16 shows an example of the NDP Table tab.

Figure 17-16 NDP Table in Logical Inventory

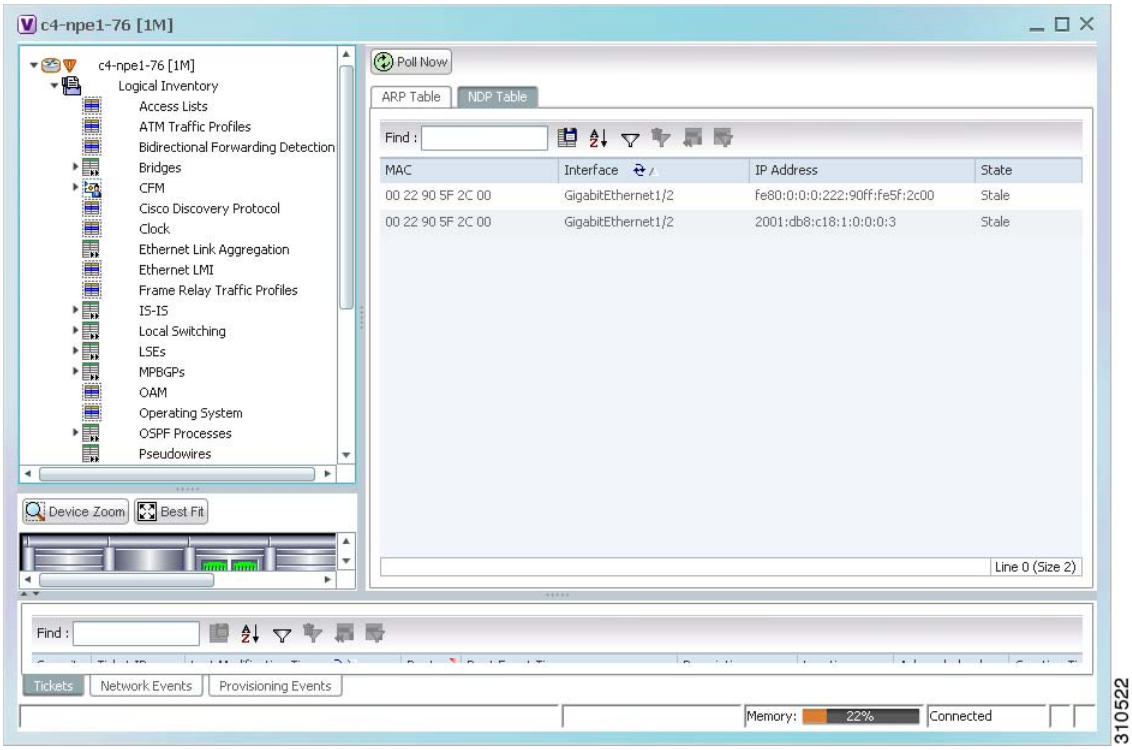


Table 17-13 describes the information displayed for NDP.

Table 17-13 NDP Table

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

Viewing Rate Limit Information

To view rate limit information:

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

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

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

Note Rate limit information is relevant only for Cisco IOS devices.

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

Table 17-14 Rate Limits Information

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

Viewing VRRP Information

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

To view VRRP information:

Step 1 Double-click the required element in Prime Network Vision.

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

Step 3 In the IP Interfaces tab, double-click the required interface to view the IP interface properties. If VRRP is configured on the IP interface, the VRRP Groups tab is displayed.

Figure 17-17 VRRP Properties in IP Interface Properties Window

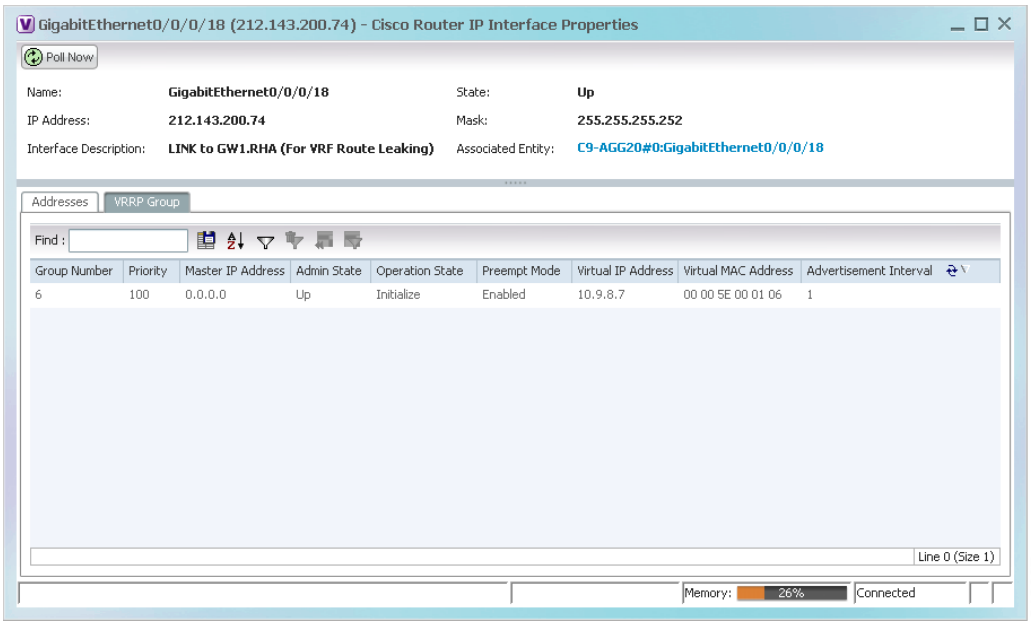


Table 17-15 describes the information in the VRRP Groups tab.

Table 17-15 VRRP Group Properties

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

Viewing Label Switched Entity Properties

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

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

  Two LDP peer discovery types are supported:

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

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

To view information for label switched entities:

Step 1 Double-click the required device in Prime Network Vision.

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

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

Table 17-16 Label Switching Properties in Logical Inventory

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

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

Field	Description
Traffic Engineering LSPs	
LSP Name	Label switched path (LSP) name.
LSP Type	Segment type: Head, Midpoint, or Tail.
Source Address	Source IP address.
Destination Address	Destination IP address.
In Label	Incoming label, if not a head segment.
In Interface	Incoming interface, if not a head segment.
Out Interface	Outgoing interface, if not a tail segment.
Out Label	Outgoing label, if not a tail segment.
Average Bandwidth (Kbps)	Current bandwidth (in Kb/s) used to automatically allocate the tunnel's bandwidth.
LSP ID	LSP identifier.
Burst (Kbps)	Tunnel bandwidth burst rate, in Kb/s.
Peak (Kbps)	Tunnel bandwidth peak rate, in Kb/s.
FRR TE Tunnel	Fast Reroute (FRR) TE tunnel name, hyperlinked to the routing entity in logical inventory.
FRR TE Tunnel State	State of the FRR TE tunnel: • Active—A failure exists in the primary tunnel and the backup is in use. • Not Configured—The primary tunnel has no designated backup tunnel. • Ready—The primary tunnel is in working condition.
MPLS Label Range	
MPLS Label Type	Type of MPLS label: Dynamic or Static.
Minimum Label Value	Lowest acceptable MPLS label in the range.
Maximum Label Value	Highest acceptable MPLS label in the range.

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

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

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

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

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

Viewing MP-BGP Information

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

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

To view MP-BGP information:

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

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

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

Table 17-18 MP-BGP Information in Logical Inventory

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

Viewing 6rd Tunnel Properties

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

- Cisco 7600 series devices
- Cisco ASR 1000 series devices

To view 6rd tunnel properties:

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

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

The 6rd tunnel properties are displayed as shown in Figure 17-18.

Figure 17-18 6rd Tunnel Properties in Logical Inventory

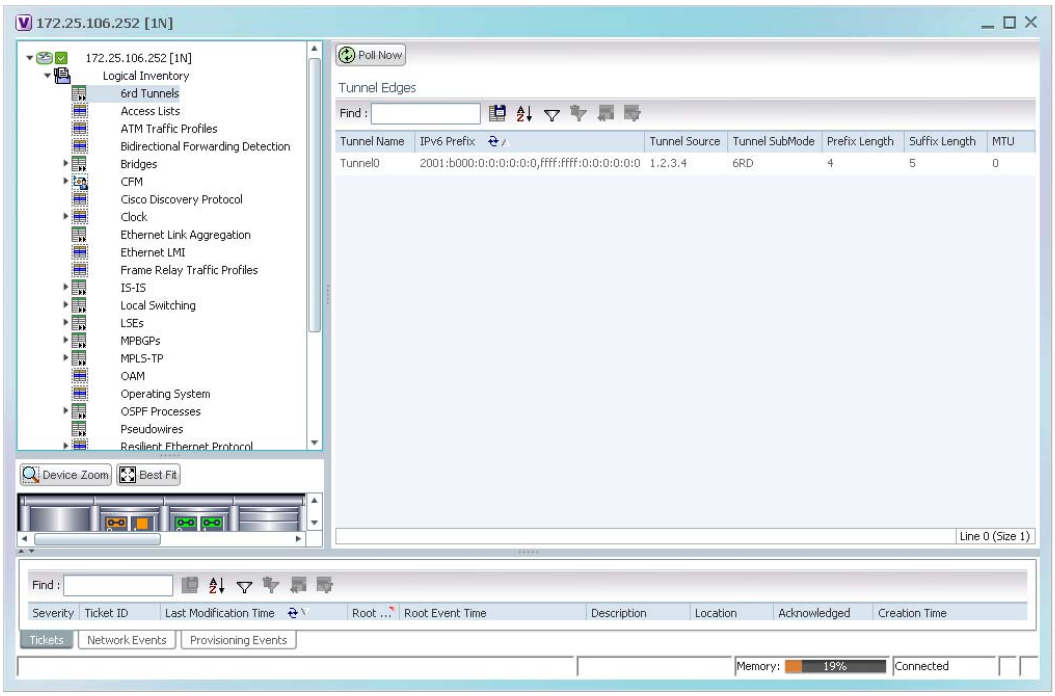


Table 17-19 describes the information displayed for 6rd tunnels.

Table 17-19 6rd Tunnel Properties in Logical Inventory

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

Viewing BFD Session Properties

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

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

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

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

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

The properties for BFD sessions are displayed as shown in Figure 17-19.

Figure 17-19 BFD Session Properties

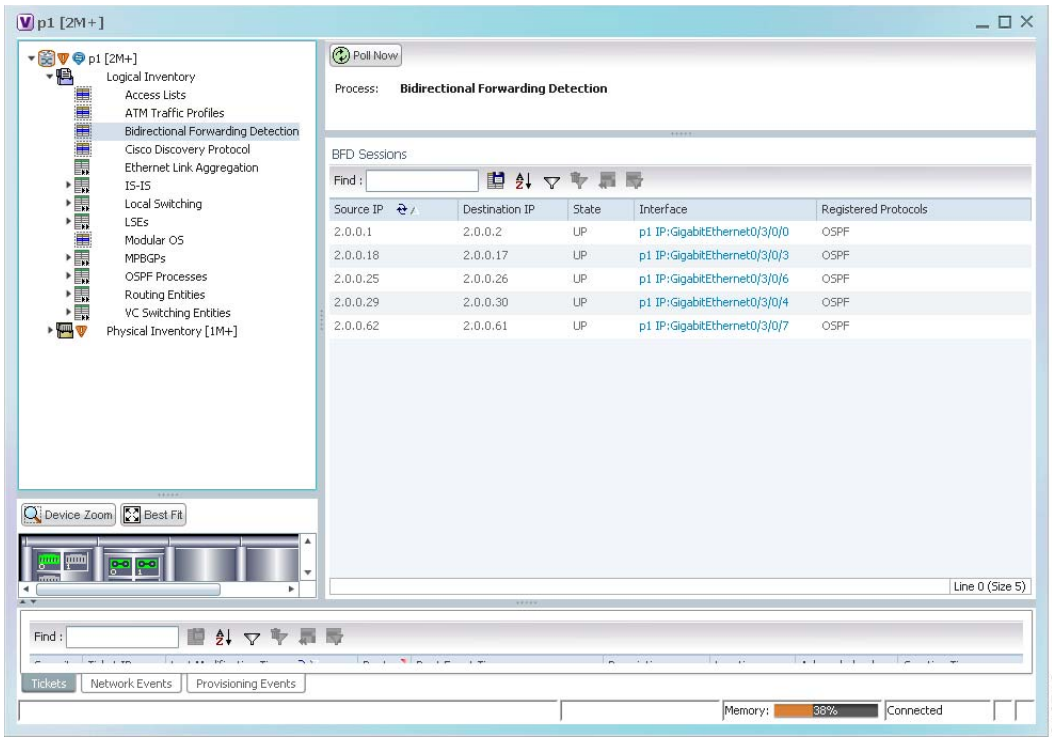


Table 17-20 describes the information displayed for BFD sessions.

Table 17-20 BFD Session Properties

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

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

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

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

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

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

Table 17-22 Session Properties Window

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

Viewing Cross-VRF Routing Entries

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

To view properties for cross-VRF routing entries:

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

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

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

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

The Cross VRF Properties window is displayed, containing the information described in Table 17-23.

Table 17-23 Cross-VRF Properties Window

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

Viewing Pseudowire End-to-End Emulation Tunnels

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

To view pseudowire properties:

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

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

The Tunnel Edges table is displayed and contains the information described in Table 17-24.

Table 17-24 Pseudowires Branch Tunnel Edges Table

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

Viewing MPLS TE Tunnel Information

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

To view MPLS TE tunnel information:

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

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

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

Table 17-25 Tunnel Edges Table

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

Table 17-25 Tunnel Edges Table (continued)

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

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

For details about the information displayed for TE tunnel LSPs, see Traffic Engineering LSPs, page 17-40.



CHAPTER 18

Monitoring MToP Services

The following topics describe Mobile Transport over Packet (MToP) services and the properties available in Cisco Prime Network Vision (Prime Network Vision):

- User Roles Required to Work with MToP, page 18-1
- Viewing SAToP Pseudowire Type in Logical Inventory, page 18-2
- Viewing CESoPSN Pseudowire Type in Logical Inventory, page 18-3
- Viewing Virtual Connection Properties, page 18-5
- Viewing IMA Group Properties, page 18-13
- Viewing TDM Properties, page 18-16
- Viewing Channelization Properties, page 18-17
- Viewing MLPPP Properties, page 18-26
- Viewing MLPPP Link Properties, page 18-29
- Viewing MPLS Pseudowire over GRE Properties, page 18-31
- Network Clock Service Overview, page 18-34
- Viewing CEM and Virtual CEM Properties, page 18-50

User Roles Required to Work with MToP

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

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

For more information on user authorization, see the *Cisco Prime Network 3.9 Administrator Guide*.

The following tables identify the tasks that you can perform:

- Table 18-1 identifies the tasks that you can perform if a selected element **is not in** one of your assigned scopes.
- Table 18-2 identifies the tasks that you can perform if a selected element **is in** one of your assigned scopes.

By default, users with the Administrator role have access to all managed elements. To change the Administrator user scope, see the topic on device scopes in the *Cisco Prime Network 3.9 Administrator Guide*.

Table 18-1 Default Permission/Security Level Required for Viewing MToP Properties - Element Not in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View MToP properties	—	—	—	—	X

Table 18-2 Default Permission/Security Level Required for Viewing MToP Properties - Element in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View MToP properties	X	X	X	X	X

Viewing SAToP Pseudowire Type in Logical Inventory

Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP) enables the encapsulation of TDM bit-streams (T1, E1, T3, or E3) as pseudowires over PSNs. As a structure-agnostic protocol, SAToP disregards any structure that might be imposed on the signals and TDM framing is not allowed.

To view the SAToP pseudowire type in logical inventory:

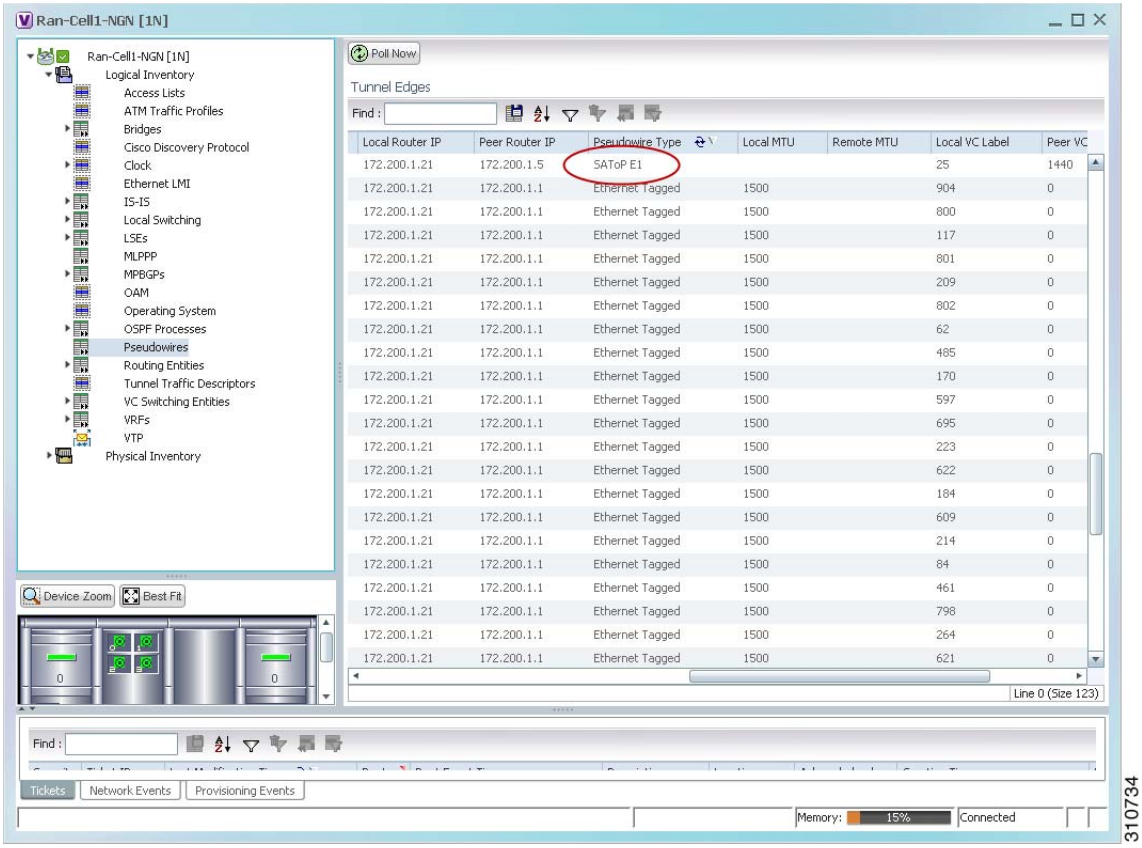
Step 1 In Prime Network Vision, right-click the device on which SAToP is configured, then choose **Inventory**.

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

Step 3 In the Tunnel Edges table, select the required entry and scroll horizontally until you see the Pseudowire Type column. See Figure 18-1.

Note You can also view this information by right-clicking the entry in the table and choosing **Properties**.

Figure 18-1 SAToP Pseudowire Type in Logical Inventory



Step 4 To view the physical inventory for the port, click the hypertext port link.

Viewing CESoPSN Pseudowire Type in Logical Inventory

Circuit Emulation Services over PSN (CESoPSN) is a method for encapsulating structured (NxDS0) TDM signals as pseudowires over packet-switching networks, complementary to SAToP. By emulating NxDS0 circuits, CESoPSN:

- Saves PSN bandwidth.
- Supports DS0-level grooming and distributed cross-connect applications.

To view TDM properties for Circuit Emulation (CEM) groups in Prime Network Vision:

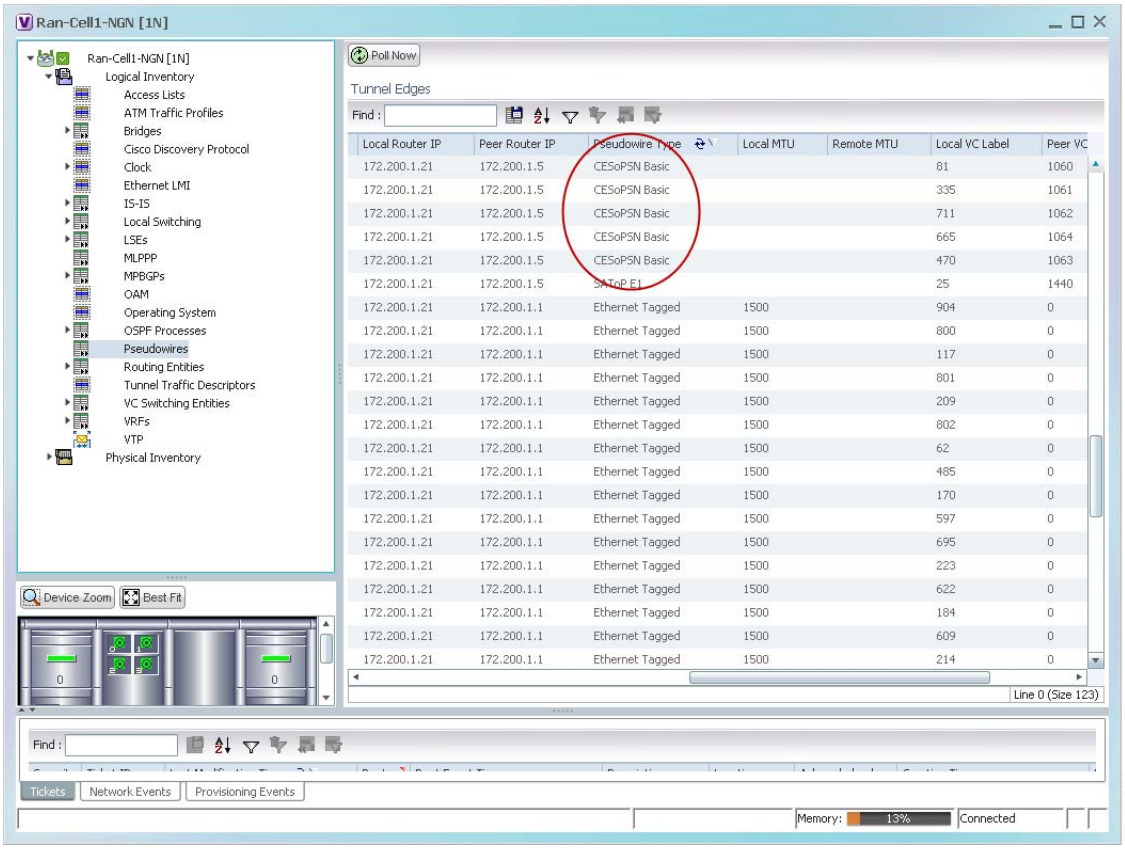
Step 1 In Prime Network Vision, right-click the device on which CESoPSN is configured, then choose **Inventory**.

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

Step 3 In the Tunnel Edges table, select the required entry and scroll horizontally until you see the Pseudowire Type column. See Figure 18-2.

Note You can also view this information by right-clicking the entry in the table and choosing **Properties**.

Figure 18-2 CESoPSN Pseudowire Type in Logical Inventory



Step 4 To view the physical inventory for the port, click the hypertext port link.

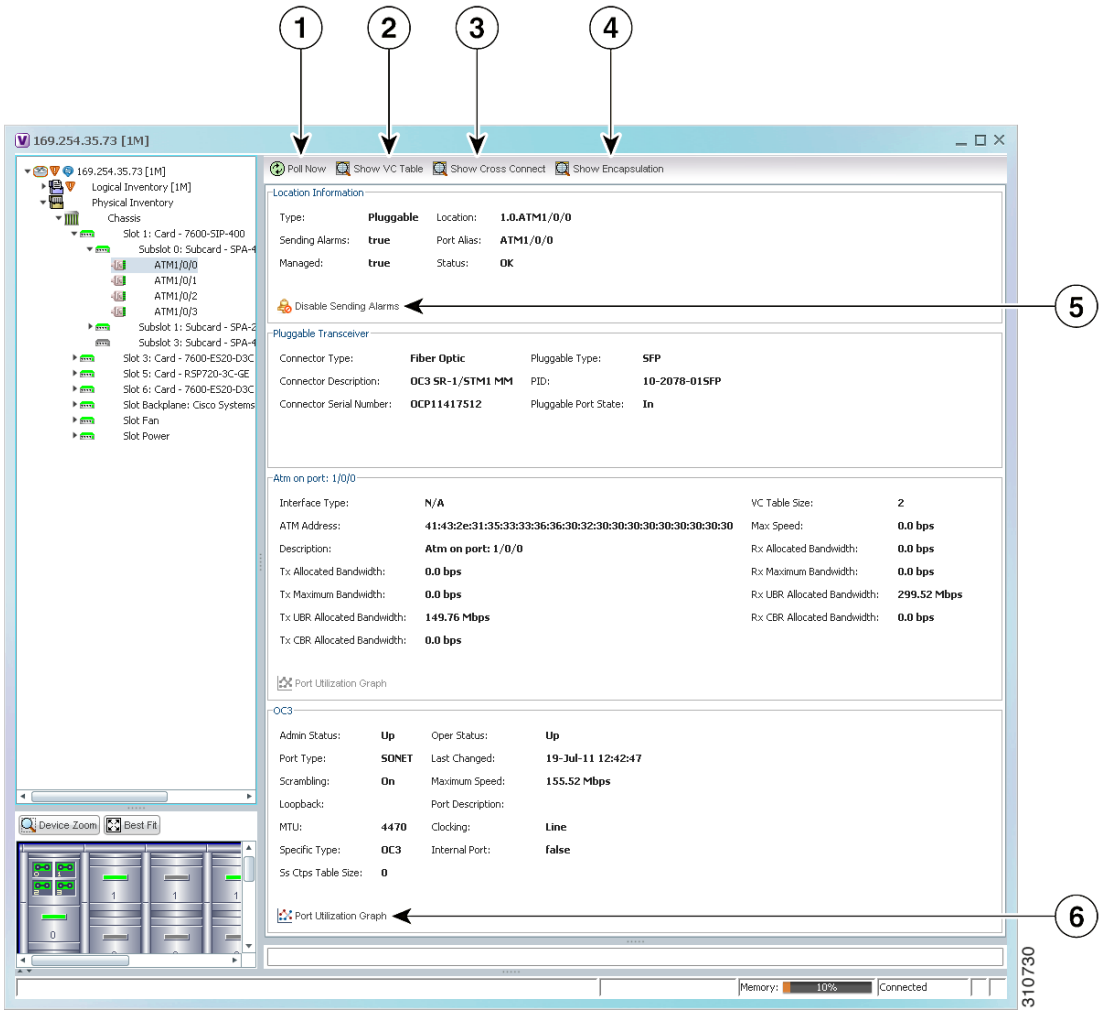
Viewing Virtual Connection Properties

The following topics describe how to view properties related to virtual connections:

- Viewing ATM Virtual Connection Cross-Connects, page 18-6
- Viewing ATM VPI and VCI Properties, page 18-10
- Viewing Encapsulation Information, page 18-11

Buttons for viewing these properties are available at the top of the physical inventory window for the selected interface, as shown in Figure 18-3.

Figure 18-3 ATM-Related Properties Available in Physical Inventory



1	Poll Now button	Polls the VNE for updated status.
2	Show VC Table button	Displays virtual circuit (VC) information for the selected port. For more information, see Viewing ATM VPI and VCI Properties, page 18-10.
3	Show Cross Connect button	Displays cross-connect information for incoming and outgoing ports. For more information, see Viewing ATM Virtual Connection Cross-Connects, page 18-6.
4	Show Encapsulation button	Displays encapsulation information for incoming and outgoing traffic for the selected item. For more information, see Viewing Encapsulation Information, page 18-11.
5	Disable/Enable Sending Alarms button	Enables you to manage the alarms on a port. For more information, see Working with Ports, page 3-22.
6	Port Utilization Graph button	Displays the selected port traffic statistics: Rx/Tx Rate and Rx/Tx Rate History. For more information, see Generating the Port Utilization Graph, page 3-27.
—	Show DLCI Table button (not displayed)	Displays data-link connection identifier (DCLI) information for the selected port.

Viewing ATM Virtual Connection Cross-Connects

ATM networks are based on virtual connections over a high-bandwidth medium. By using cross-connects to interconnect virtual path or virtual channel links, it is possible to build an end-to-end virtual connection.

An ATM cross-connect can be mapped at either of the following levels:

- Virtual path—Cross-connecting two virtual paths maps one Virtual Path Identifier (VPI) on one port to another VPI on the same port or a different port.
- Virtual channel—Cross-connecting at the virtual channel level maps a Virtual Channel Identifier (VCI) of one virtual channel to another VCI on the same virtual path or a different virtual path.

Cross-connect tables translate the VPI and VCI connection identifiers in incoming ATM cells to the VPI and VCI combinations in outgoing ATM cells. For information about viewing VPI and VCI properties, see Viewing ATM VPI and VCI Properties, page 18-10.

To view ATM virtual connection cross-connects:

Step 1 In Prime Network Vision, right-click the required device, then choose **Inventory**.

Step 2 Open the VC Cross Connect table in either of the following ways:

- In the inventory window, choose **Logical Inventory > VC Switching Entities > VC Switching Entity**. The Cross-Connect Table is displayed in the content pane as shown in Figure 18-4.
- In the inventory window:

  a. Choose **Physical Inventory > Chassis >** *Slot* **>** *Subslot* **>** *Port*.

  b. Click the **Show Cross Connect** button.

  The VC Cross Connections window is displayed and contains the same information as the Cross-Connect Table in logical inventory.

Step 3 Select an entry and scroll horizontally until you see the required information.

Figure 18-4 ATM Virtual Connection Cross-Connect Properties

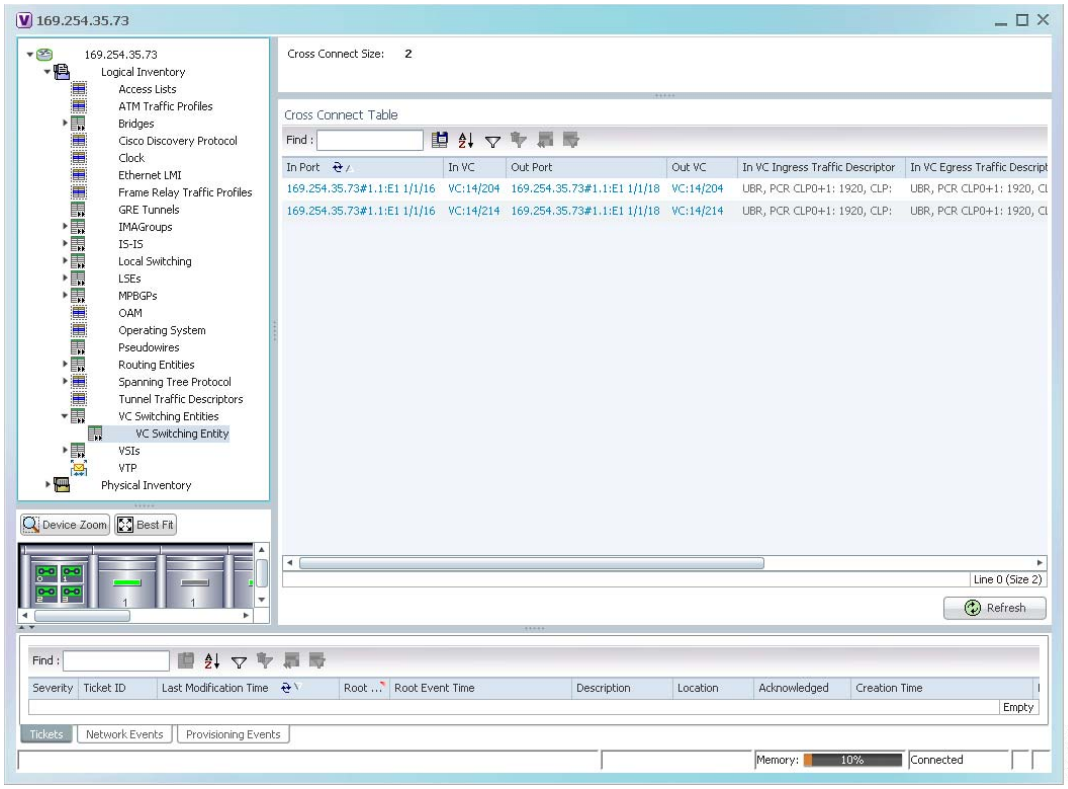


Table 18-3 identifies the properties that are displayed for ATM VC cross-connects.

Table 18-3 ATM Virtual Connection Cross-Connect Properties

Field	Description
In Port	Incoming port for the cross-connect.
In VC	Incoming virtual connection for the cross-connect. You can view additional details about the virtual connection in the following ways: • Click the hyperlinked entry to view the VC table. • Right-click the entry, then choose **Properties** to view information about the incoming and outgoing VCIs, VPI, service category, and traffic descriptors.
Out Port	Outgoing port for the cross-connect.
Out VC	Outgoing virtual connection for the cross-connect. You can view additional details about the virtual connection in the following ways: • Click the hyperlinked entry to view the VC table. • Right-click the entry, then choose **Properties** to view information about the incoming and outgoing VCIs, VPI, service category, and traffic descriptors.
In VC Ingress Traffic Descriptor	ATM traffic parameters and service categories for the incoming traffic on the incoming VC cross-connect. For information on VC traffic descriptors, see Table 18-4.
In VC Egress Traffic Descriptor	ATM traffic parameters and service categories for the outgoing traffic on the incoming VC cross-connect. For information on VC traffic descriptors, see Table 18-4.
Out VC Egress Traffic Descriptor	ATM traffic parameters and service categories for the outgoing traffic on the outgoing VC cross-connect. For information on VC traffic descriptors, see Table 18-4.
Out VC Ingress Traffic Descriptor	ATM traffic parameters and service categories for the incoming traffic on the outgoing VC cross-connect. For information on VC traffic descriptors, see Table 18-4.

Table 18-4 Virtual Connection Traffic Descriptors

Value	Description
ABR	Available bit rate (ABR) supports nonreal-time applications that tolerate high cell delay, and can adapt cell rates according to changing network resource availability to prevent cell loss.
CBR	Constant bit rate (CBR) supports real-time applications that request a static amount of bandwidth that is continuously available for the duration of the connection.
CDVT	Cell Delay Variation Tolerance (CDVT) specifies an acceptable deviation in cell times for a PVC that is transmitting above the PCR. For a given cell interarrival time expected by the ATM switch, CDVT allows for some variance in the transmission rate.
CLP	Cell loss priority (CLP) indicates the likelihood of a cell being dropped to ease network congestion.
MBS	Maximum Burst Size (MBS) specifies the number of cells that the edge device can transmit up to the PCR for a limited period of time without penalty for violation of the traffic contract.
MCR	Minimum Cell Rate (MCR) specifies the cell rate (cells per second) at which the edge device is always allowed to transmit.
PCR	Peak Cell Rate (PCR) specifies the cell rate (cells per second) that the edge device cannot exceed.
PDR CLP0+1: 1536	Packet delivery ratio (PDR) for all cells (both CLP1 and CLP0 cells) on the circuit.
SCR	Sustainable Cell Rate (SCR) specifies the upper boundary for the average rate at which the edge device can transmit cells without loss.
UBR	Unspecified Bit Rate (UBR) supports nonreal-time applications that tolerate both high cell delay and cell loss on the network.
UBR+	Unspecified bit rate plus (UBR+) supports nonreal-time applications that tolerate both high cell delay and cell loss on the network, but request a minimum guaranteed cell rate.
nrt-VBR	Nonreal-time variable bit rate (nrt-VBR) supports nonreal-time applications with bursty transmission characteristics that tolerate high cell delay, but require low cell loss.
rt-VBR	rt-VBR—Real-time variable bit rate (rt-VBR) supports real-time applications that have bursty transmission characteristics.

Viewing ATM VPI and VCI Properties

If you know the interface or link configured for virtual connection cross-connects, you can view ATM VPI and VCI properties from the physical inventory window or from the link properties window.

To view ATM VPI and VCI properties, open the VC Table window in either of the following ways:

- To open the VC Table window from physical inventory:
  a. In the map view, double-click the element configured for virtual connection cross-connects.
  b. In the inventory window, choose **Physical Inventory > Chassis >** *Slot* **>** *Subslot* **>** *Port*.
  c. Click **Show VC Table**.
- To view the VC Table window from the link properties window:
  a. In the map or links view, right-click the required ATM link and choose **Properties**.
  b. In the link properties window, click **Calculate VCs**.
  c. After the screen refreshes, click either **Show Configured** or **Show Misconfigured** to view the virtual connection cross-connects.

The VC Table window is displayed, as shown in Figure 18-5.

Figure 18-5 VC Table

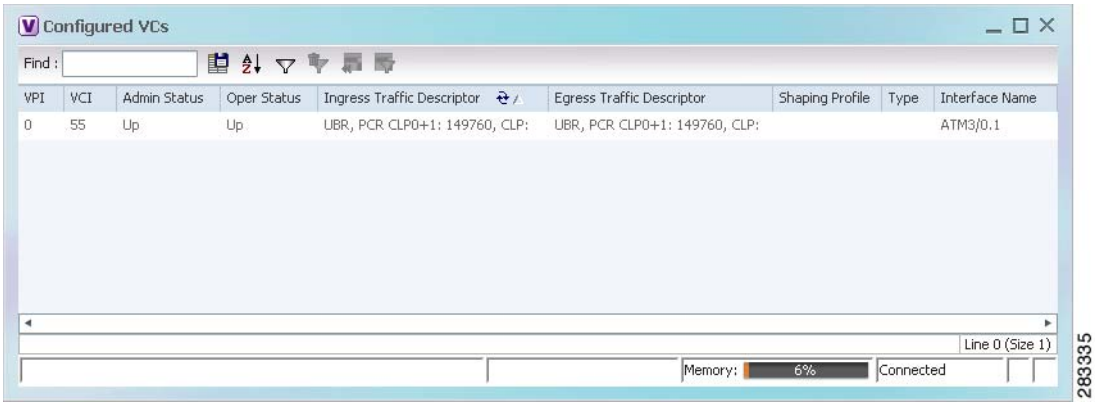


Table 18-5 describes the information displayed in the VC Table window.

Table 18-5 VC Table Properties

Field	Description
VPI	Virtual Path Identifier for the selected port.
VCI	Virtual Channel Identifier for the selected port.
Admin Status	Administrative state of the connection: Up, Down, or Unknown.
Oper Status	Operational state of the connection: Up, Down, or Unknown.
Ingress Traffic Descriptor	Traffic parameters and service categories for the incoming traffic. For information on VC traffic descriptors, see Table 18-4.
Egress Traffic Descriptor	Traffic parameters and service categories for the outgoing traffic. For information on VC traffic descriptors, see Table 18-4.
Shaping Profile	Traffic shape profile used for the virtual connection.
Type	ATM traffic descriptor type for the virtual connection.
Interface Name	Interface name, such as ATM1/1/16.

Viewing Encapsulation Information

To view virtual connection encapsulation information:

Step 1 In Prime Network Vision, double-click the element configured for virtual connection encapsulation.

Step 2 In the inventory window, choose **Physical Inventory > Chassis >** *Slot* **>** *Subslot* **>** *Port*.

Step 3 Click the **Show Encapsulation** button.

The VC Encapsulation window is displayed as shown in Figure 18-6.

Figure 18-6 VC Encapsulation Properties

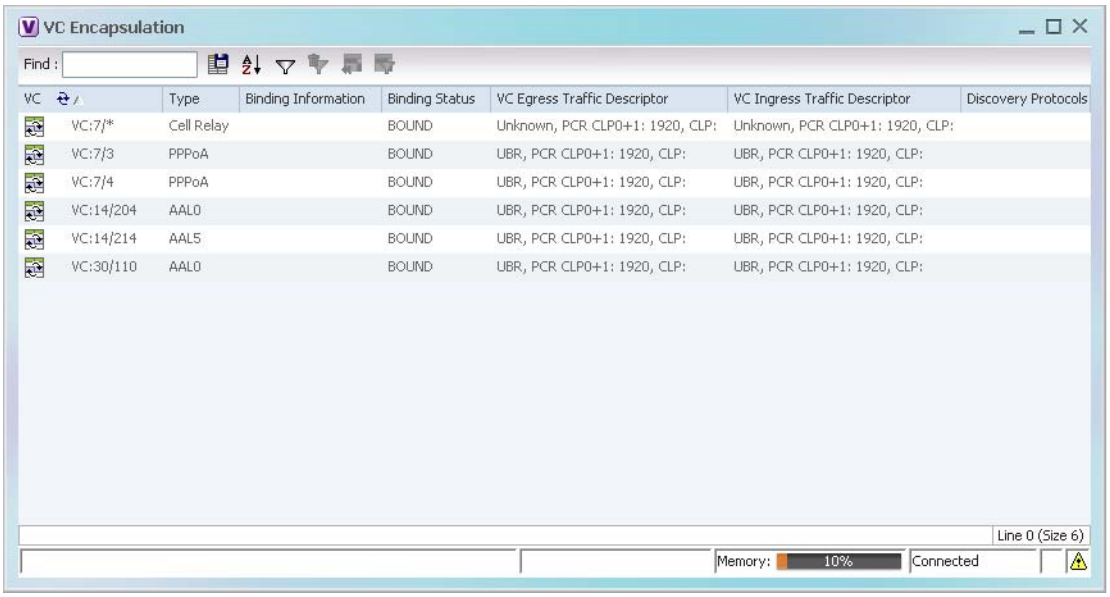


Table 18-6 describes the information displayed in the VC Encapsulation window.

Table 18-6 VC Encapsulation Properties

Field	Description
VC	Virtual connection identifier, such as VC:7/4.
Type	Type of encapsulation, such as Point-to-Point Protocol (PPP) over ATM (PPPoA) or ATM adaption layer Type 5 (AAL5).
Binding Information	Information tied to the virtual connection, such as a username.
Binding Status	Binding state: Bound or Unbound.
VC Egress Traffic Descriptor	Traffic parameters and service categories for the outgoing traffic. For information on VC traffic descriptors, see Table 18-4.
VC Ingress Traffic Descriptor	Traffic parameters and service categories for the incoming traffic. For information on VC traffic descriptors, see Table 18-4.
Discovery Protocols	Discovery protocol used for the VC.

Viewing IMA Group Properties

To view IMA group properties:

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

Step 2 In the inventory window, choose **Logical Inventory > IMA Groups >** *group*. IMA group properties and the IMA Members table are displayed in the content pane as shown in Figure 18-7.

Figure 18-7 IMA Group Properties

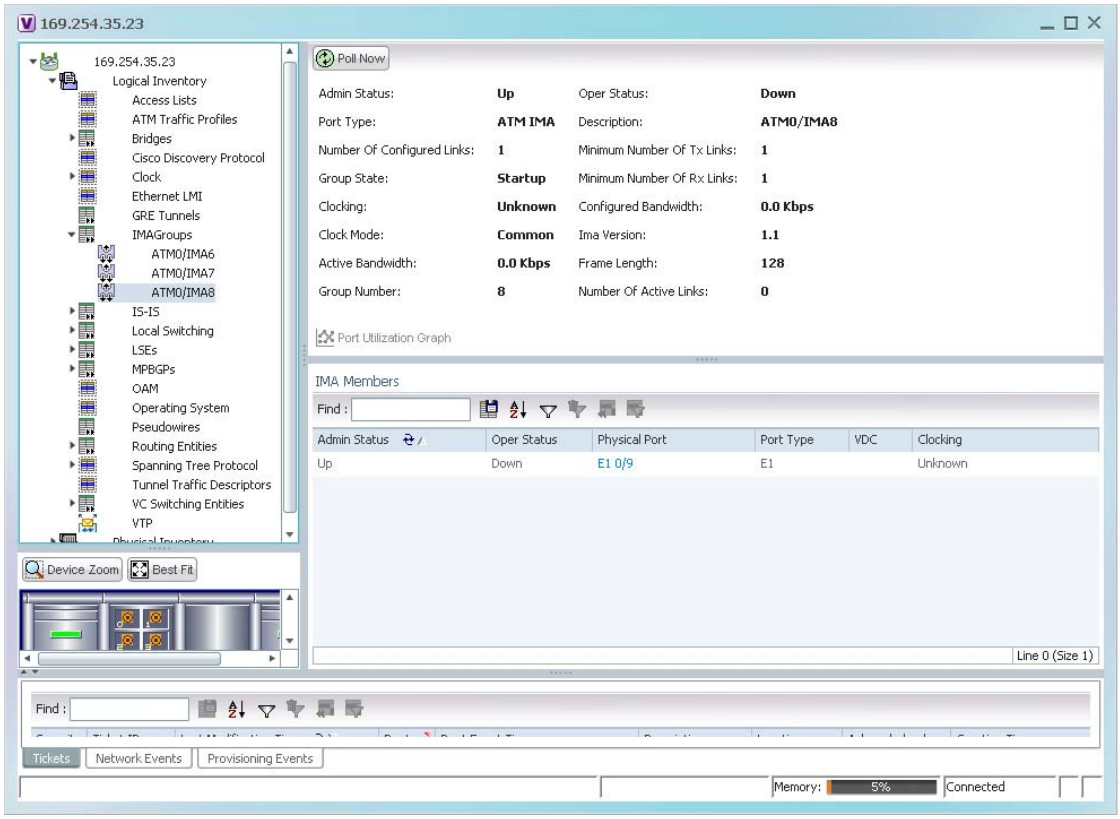


Table 18-7 describes the information displayed for the IMA group.

Table 18-7 IMA Group Properties

Field	Description
Active Bandwidth	Active bandwidth of the IMA group.
Admin Status	Administrative status of the IMA group.
Clock Mode	Clock mode the IMA group is using: • Common—Common transmit clocking (CTC). • Independent—Independent transmit clocking (ITC).
Configured Bandwidth	Total bandwidth of the IMA group, which is the sum of all individual links in the group.

Table 18-7 IMA Group Properties (continued)

Field	Description
Description	IMA group interface name.
Frame Length	Length of the IMA group transmit frames, in the number of cells: 32, 64, 128, or 256. A small frame length causes more overhead but loses less data if a problem occurs. We recommend a frame length of 128 cells.
Group Number	IMA group number.
Group State	IMA group status, in the order of usual appearance: • Startup—The near end is waiting to receive indication that the far end is in Startup. The IMA group moves to the Startup-Ack state when it can communicate with the far end and has recorded IMA identifier, group symmetry, and other IMA group parameters. • Startup ACK—Both sides of the link are enabled. • Config Aborted—The far end has unacceptable configuration parameters, such as an unsupported IMA frame size, an incompatible group symmetry, or an unsupported IMA version. • Insufficient Links—The near end has accepted the far end group parameters, but the far end does not have sufficient links to move into the Operational state. • Operational—The group is not inhibited and has sufficient links in both directions. The IMA interface can receive ATM layer cells and pass them from the IMA sublayer to the ATM layer. • Blocked—The group is blocked, even though sufficient links are active in both directions.
IMA Version	IMA version configured, either 1.0 or 1.1.
Minimum Number of Rx Links	Minimum number of Rx links needed for the IMA group to be operational.
Minimum Number of Tx Links	Minimum number of Tx links needed for the IMA group to be operational.
Number of Active Links	Number of DS1 (E1 or T1) links that are active in the group.
Number of Configured Links	Number of DS1 (E1 or T1) links that are configured in the IMA group.
Oper Status	Operational state of the IMA group interface: • Dormant—The interface is dormant. • Down—The interface is down. • Not Present—An interface component is missing. • Testing—The interface is in test mode. • Unknown—The interface has an unknown operational status. • Up—The interface is up.
Port Type	Type of port, such as ATM IMA.

Table 18-8 describes the information displayed in the IMA Members table.

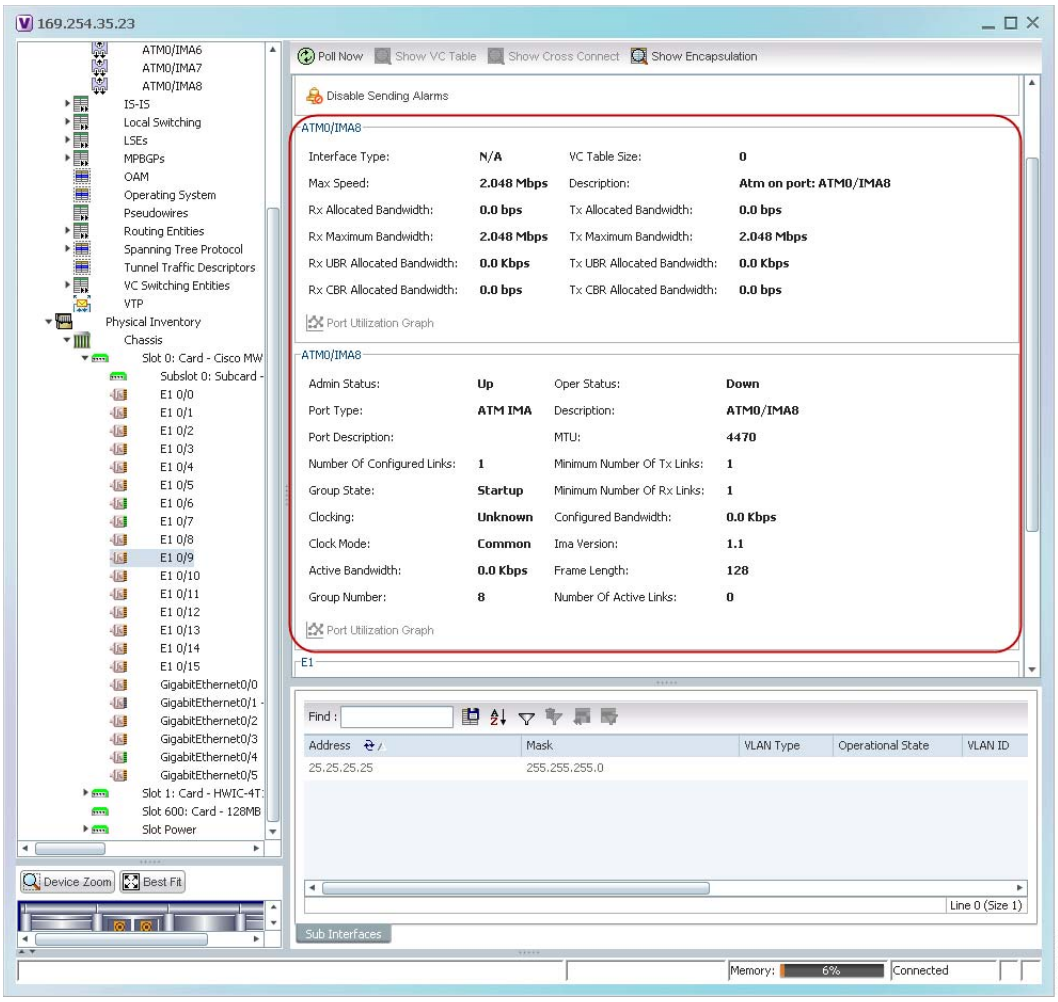
Table 18-8 IMA Members Table

Column	Description
Admin Status	Administrative status of the IMA member.
Channelization	Channelization that occurs through the path, such as STS1-> VTG-> VT15. Information is displayed in this field only if the T1 or E1 path was channelized. If the line was not channelized, this field is not displayed. For example, if the IMA group is configured on a T1 or E1 card, this field is not displayed.
Clocking	Source of the clocking mechanism: Internal or Line.
Description	Type of channelization, such as Synchronous Transport Signal 1 (STS-1) or Synchronous Transport Module level 1 (STM-1).
Oper Status	Operational state of the IMA member:
Physical Port	Hyperlinked entry to the port in physical inventory.
Port Type	Type of port, such as E1 or T1.

Step 3 In the IMA Members table, click a hyperlinked port entry to view the port properties in physical inventory. See Figure 18-8.

The information that is displayed for the port in physical inventory depends on the type of connection, such as SONET or ATM.

Figure 18-8 ATM IMA Port in Physical Inventory



Viewing TDM Properties

TDM is a mechanism for combining two or more slower-speed data streams into a single high-speed communication channel. In this model, data from multiple sources is divided into segments that are transmitted in a defined sequence. Each incoming data stream is allocated a timeslot of a fixed length, and the data from each stream is transmitted in turn. For example, data from data stream 1 is transmitted during timeslot 1, data from data stream 2 is transmitted during timeslot 2, and so on. After each incoming stream has transmitted data, the cycle begins again with data stream 1. The transmission order is maintained so that the input streams can be reassembled at the destination.

MToP encapsulates TDM streams for delivery over packet-switching networks (PSNs) using the following methods:

- SAToP—A method for encapsulating TDM bit-streams (T1, E1, T3, or E3) as pseudowires over PSNs.
- CESoPSN—A method for encapsulating structured (NxDS0) TDM signals as pseudowires over PSNs.

For T1 or E1 entries, the TDM properties presented in Table 18-9 are displayed in physical inventory in addition to the existing T1 or E1 properties.

Table 18-9 TDM-Specific Properties for DS1 (T1 or E1) in Physical Interfaces

Field	Description
International Bit	Whether or not the international bit is used by the controller: • 0—The international bit is not used. • 1—The international bit is used. This property applies only to E1.
National Bits	Whether or not the national reserve bits (sa4, sa5, sa6, sa7, and sa8) are used by the controller: • 0—The national reserve bits are not used. • 1—The national reserve bits are used. This property applies only to E1.
Line Code	Line encoding method for the DS1 link: • For E1, the options are Alternate Mark Inversion (AMI) and high-density bipolar of order 3 (HDB3). • For T1, the options are AMI and bipolar with 8 zero substitution (B8ZS).
Cable Length	For T1 ports in short-haul mode, the length of the cable in feet.

Viewing Channelization Properties

Prime Network Vision supports the channelization of SONET/SDH and T3 lines. When a line is channelized, it is logically divided into smaller bandwidth channels called paths. These paths (referred to as high order paths or HOPs) can, in turn, contain low order paths, or LOPs. The sum of the bandwidth on all paths cannot exceed the line bandwidth.

The following topics describe how to view channelization properties for SONET/SDH and T3 lines:

- Viewing SONET/SDH Channelization Properties, page 18-18
- Viewing T3 DS1 and DS3 Channelization Properties, page 18-21

Viewing SONET/SDH Channelization Properties

SONET and SDH use the same concepts for channelization, but the terminology differs. Table 18-10 describes the equivalent terms for SONET and SDH channelization. The information displayed in Prime Network Vision reflects whether SONET or SDH is configured on the interface.

Table 18-10 SONET and SDH Channelization Terminology

Concept	SONET Term	SDH Term
Frame	Synchronous Transport Signal level N (STS-N)	Synchronous Transport Module level N (STM-N)
HOP channel	STS-1	Administrative Unit (AU-*n*)
Lower-order channels	Virtual Tributary (VT)	Tributary Unit Group (TUG)
LOP payloads	DS1, DS3, or E1	

To view SONET/SDH channelization properties:

Step 1 In Prime Network Vision, right-click the required device, then choose **Inventory**.

Step 2 Choose **Physical Inventory > Chassis >** *slot* **>** *subslot* **>** *SONET/SDH-interface*. The properties for SONET/SDH and OC-3 are displayed in the content pane. See Figure 18-9.

Figure 18-9 SONET/SDH Interface in Physical Inventory

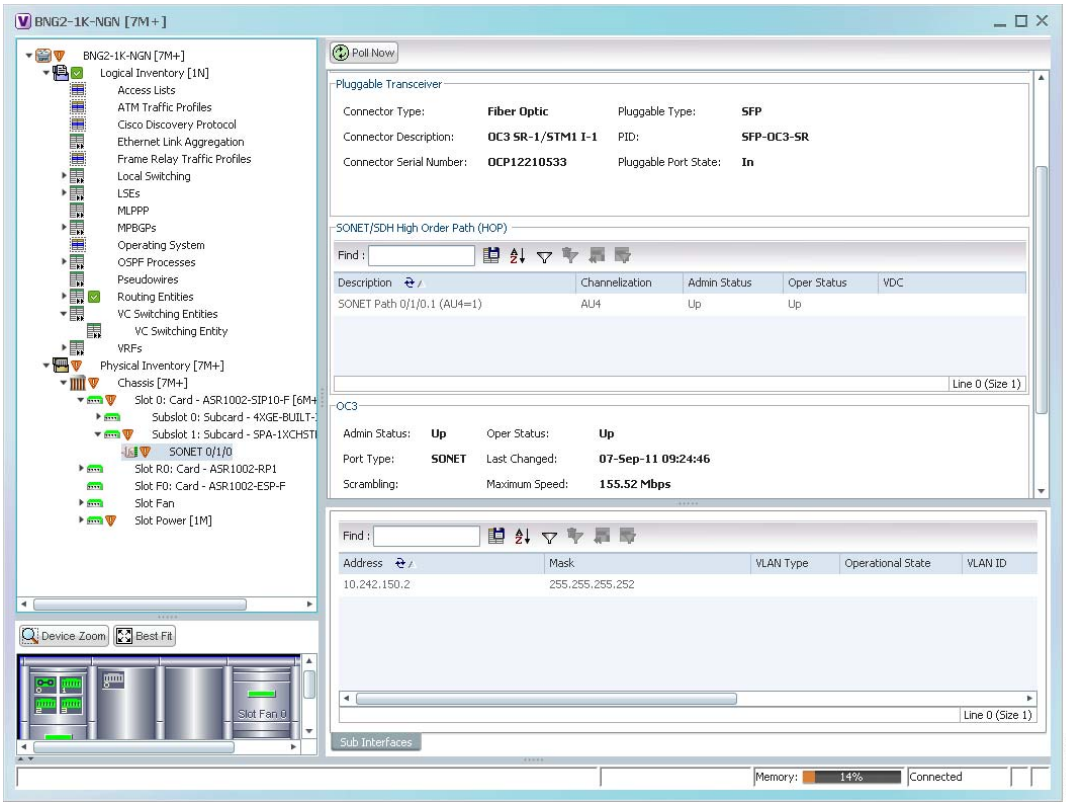


Table 18-11 describes the information that is displayed for SONET/SDH and OC3 in the content pane.

Table 18-11 SONET/SDH and OC3 Properties

Field	Description
SONET/SDH High Order Path (HOP) Area	
Description	SONET/SDH path description including the interface and high order path. Double-click an entry to view additional details about the path.
Channelization	Type of channelization, such as STS-1 or STM-1.
Admin Status	Administrative status of the HOP.
Oper Status	Operational status of the HOP.
OC3 Area	
Admin Status	Administrative status of the OC-3 line.
Oper Status	Operational status of the OC-3 line.
Port Type	Type of port.
Last Changed	Date and time of the last status change of the line.
Scrambling	Any scrambling that has been applied to the SONET payload.
Maximum Speed	Maximum bandwidth for the line.
Loopback	Loopback setting configured on the line.
Port Description	Description of the port defined by the user.
Clocking	Clocking configured on the line.
Specific Type	Specific type of line; in this case, OC3.
Internal Port	Whether or not the line includes an internal port: True or False.
Ss Ctps Table Size	Size of the SONET/SDH Connection Termination Point (CTP) table.

Step 3 To view additional information about a channelized path, double-click the required entry in the Description column. The SONET/SDH High Order Path Properties window is displayed as shown in Figure 18-10.

Figure 18-10 SONET/SDH High Order Path Properties Window

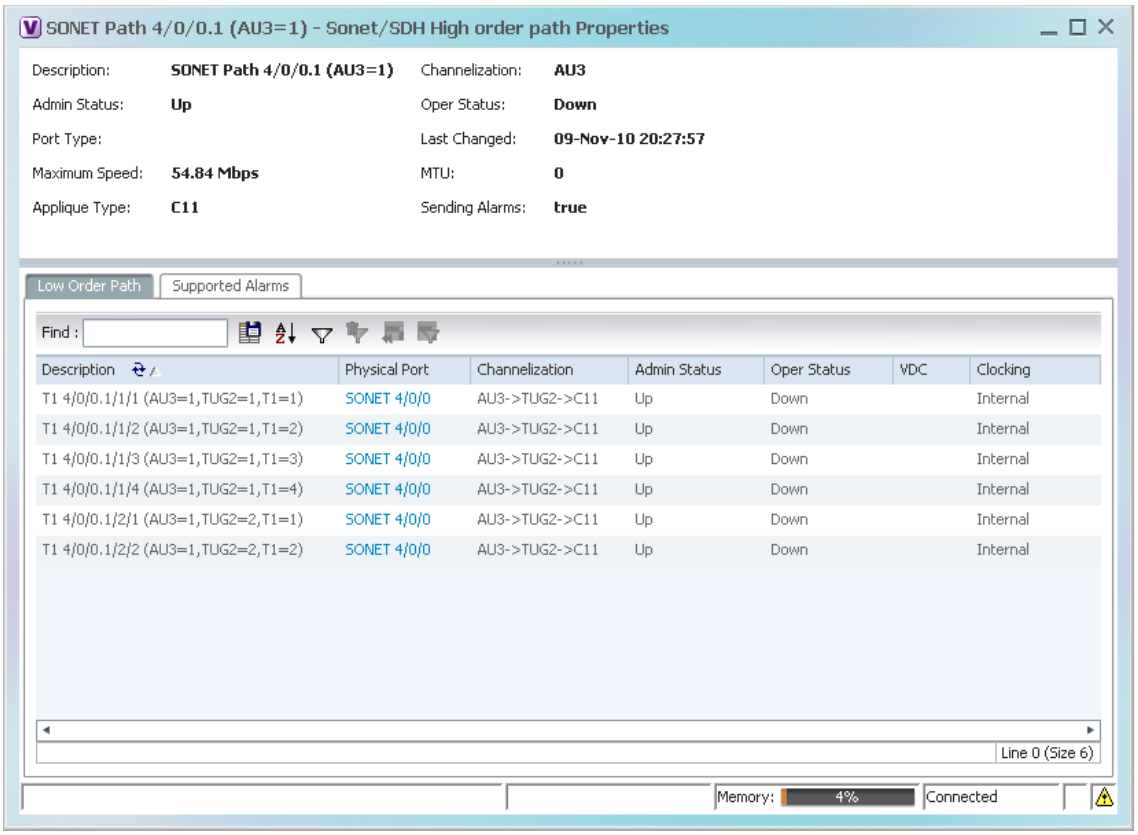


Table 18-12 describes the information displayed in SONET/SDH High Order Path Properties window.

Table 18-12 SONET/SDH High Order Path Properties

Field	Description
Description	SONET/SDH path description including the interface and high order path. Double-click an entry to view additional details about the path.
Channelization	Type of channelization, such as Synchronous Transport Signal 1 (STS-1) or Synchronous Transport Module level 1 (STM-1).
Admin Status	Administrative status of the HOP.
Oper Status	Operational status of the HOP.
Port Type	Type of port.
Last Changed	Date and time of the last status change of the path.
Maximum Speed	Maximum bandwidth for the line.
MTU	MTU for the path.
Applique Type	Sub-STS-1 facility applied to this path. In this example, the facility applied is Virtual Tributary 1.5 (VT1.5).
Sending Alarms	Whether or not the path is sending alarms: True or False.

Table 18-12 SONET/SDH High Order Path Properties (continued)

Field	Description
Low Order Path Tab	
Description	Description of the low order path down to the T1 level, including the channel types (such as STS-1, VTG, or VT) and channel allocated.
Physical Port	Hyperlinked entry to the port in physical inventory.
Channelization	Channelization that occurs through the path, such as STS1-> VTG-> VT15.
Admin Status	Administrative status of the path.
Oper Status	Operational status of the path.
Clocking	Source of the clocking mechanism: Internal or Line.
Supported Alarms Tab	
Name	Supported alarm.
Enable	Whether the alarm is enabled or disabled.

Viewing T3 DS1 and DS3 Channelization Properties

To view T3 DS1 and DS3 channelization properties:

Step 1 In Prime Network Vision, right-click the required device, then choose **Inventory**.

Step 2 Choose **Physical Inventory > Chassis >** *slot* **>** *subslot* **>** *T3-interface*.

Figure 18-11 shows DS1 channelization properties for T3 in physical inventory.

Figure 18-11 T3 DS1 Channelization Properties in Physical Inventory

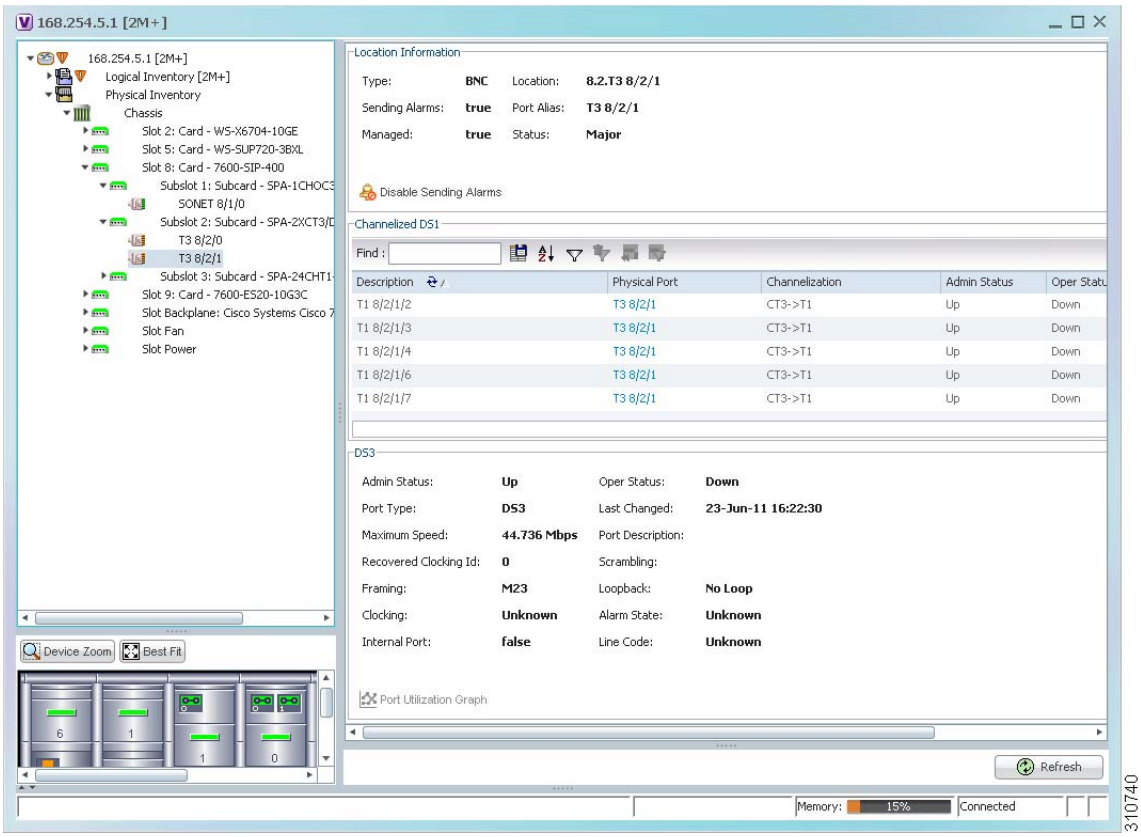


Table 18-13 describes the information that is displayed for Channelized DS1 and DS3 in the content pane.

Table 18-13 Channelized DS1 and DS3 Properties

Field	Description
Channelized DS1 Table	
Description	Path description including the physical interface and the channel number. Double-click an entry to view additional details about the path.
Physical Port	Physical port for the channelized line.
Channelization	Type of channelization, such as channelized T3 (CT3) to T1.
Admin Status	Administrative status of the channelized line.
Oper Status	Operational status of the channelized line.
VDC	For devices with multiple virtual contexts, the context associated with the channelized line.
Clocking	Clocking configured on the line: Internal or Line.

Table 18-13 Channelized DS1 and DS3 Properties (continued)

Field	Description
DS3 Area	
Admin Status	Administrative status of the DS3 line.
Oper Status	Operational status of the DS3 line.
Port Type	Type of port.
Last Changed	Date and time of the last status change of the line.
Maximum Speed	Maximum bandwidth for the line.
Port Description	Description of the port configured on the interface.
Recovered Clocking ID	Recovered clock identifier, if known.
Scrambling	Any scrambling that has been applied to the SONET payload.
Framing	Type of framing applied to the line.
Loopback	Loopback setting configured on the line.
Clocking	Clocking configured on the line: Internal or Line.
Alarm State	Alarm state of the DS3 line: • Clear—The alarm state is clear. • AIS—Alarm Indication Signal (AIS). • LOS—Loss of signal (LOS) alarm. • AIS_LOS—AIS loss of signal alarm. • LOF—Loss of frame (LOF) alarm. • AIS_LOF—AIS loss of frame alarm. • LOS_LOF—Loss of signal and loss of frame alarm. • AIS_LOS_LOF—AIS loss of signal and loss of frame alarm. • Unknown—Unknown alarm.
Internal Port	Whether or not the line includes an internal port: True or False.
Line Code	Line coding applied to the line.

Step 3 To view additional information about a DS1channelized path, double-click the required entry in the Channelized DS1 table. Figure 18-12 shows the information that is displayed in the Channelized DS1 PDH Properties window.

Figure 18-12 Channelized DS1 PDH Properties Window

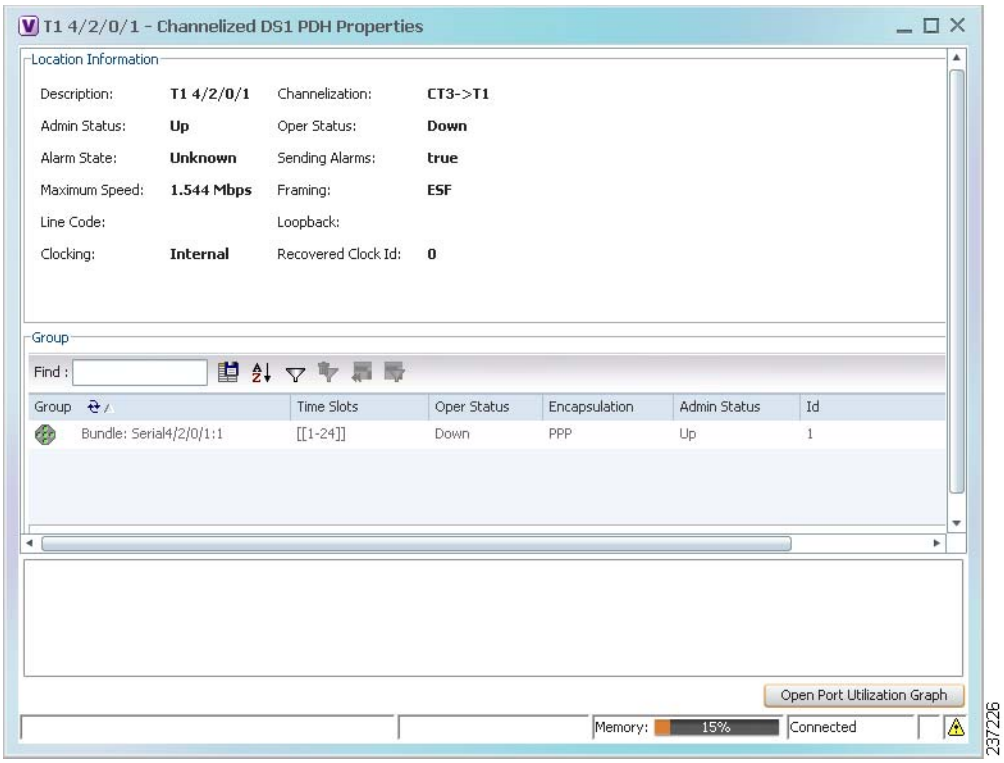


Table 18-14 describes the information that is displayed in the Channelized DS1 PDH Properties window.

Table 18-14 Channelized DS1 PDH Properties Window

Field	Description
Location Area	
Description	Path description including the physical interface and the channel number.
Channelization	Type of channelization used on the line, such as CT3-> T1.
Admin Status	Administrative status of the channelized line.
Oper Status	Operational status of the channelized line.

Table 18-14 Channelized DS1 PDH Properties Window (continued)

Field	Description
Alarm State	Alarm state of the DS1 line: • Clear—The alarm state is clear. • AIS—Alarm Indication Signal (AIS). • LOS—Loss of signal (LOS) alarm. • AIS_LOS—AIS loss of signal alarm. • LOF—Loss of frame (LOF) alarm. • AIS_LOF—AIS loss of frame alarm. • LOS_LOF—Loss of signal and loss of frame alarm. • AIS_LOS_LOF—AIS loss of signal and loss of frame alarm. • Unknown—Unknown alarm.
Sending Alarms	Whether or not the line is sending alarms: True or False.
Maximum Speed	Maximum bandwidth for the line.
Framing	Type of framing applied to the line.
Line Code	Line coding applied to the line.
Loopback	Loopback setting configured on the line.
Clocking	Clocking configured on the line: Internal or Line.
Recovered Clock ID	Recovered clock identifier, if known.
Group Table	
This table appears only if a DS0 bundle is configured on a channelized DS1 line. The properties that are displayed pertain to the DS0 bundle.	
Group	Name of the DS0 bundle.
Time Slots	Range of timeslots (DS0 channels) allotted to the group.
Oper Status	Operational status of the group.
Encapsulation	Type of encapsulation used, such as High-Level Data Link Control (HDLC).
Admin Status	Administrative status of the group.
ID	DS0 bundle identifier.

Viewing MLPPP Properties

Multilink PPP (MLPPP) is a protocol that connects multiple links between two systems as needed to provide bandwidth when needed. MLPPP packets are fragmented, and the fragments are sent at the same time over multiple point-to-point links to the same remote address. MLPPP provides bandwidth on demand and reduces transmission latency across WAN links.

To view MLPPP properties:

Step 1 In Prime Network Vision, right-click the required device, then choose **Inventory**.

Step 2 In the inventory window, choose **Logical Inventory > MLPPP**. See Figure 18-13.

Figure 18-13 MLPPP Properties in Logical Inventory

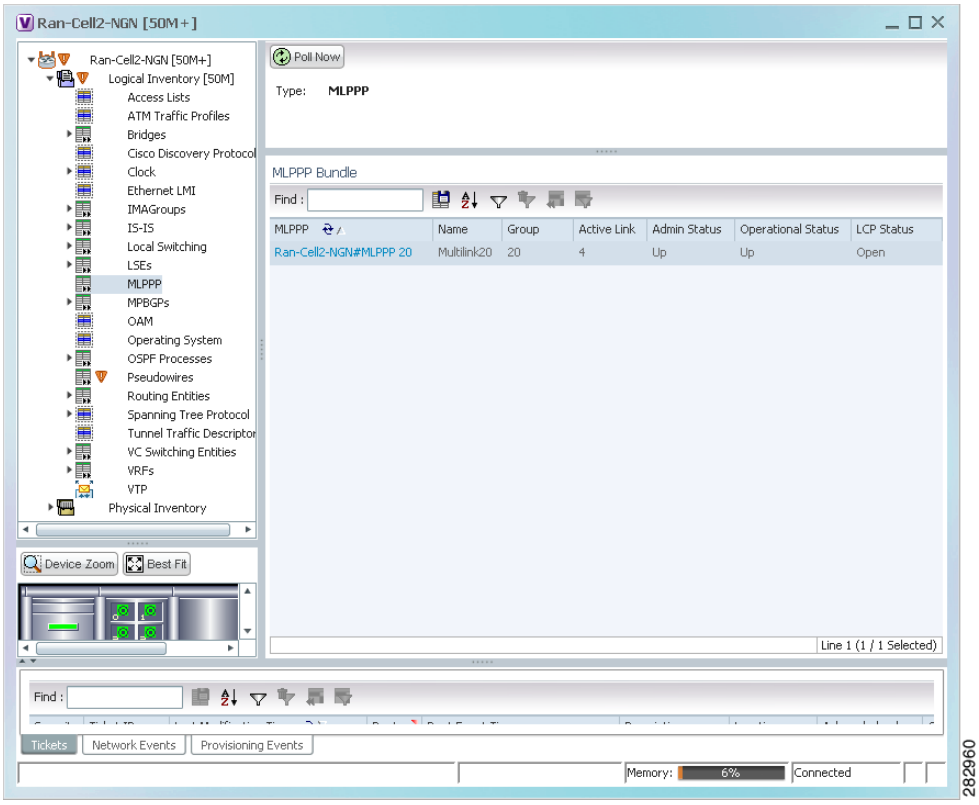


Table 18-15 describes the information that is displayed for MLPPP.

Table 18-15 MLPPP Properties

Field	Description
Type	Type of properties; in this case, MLPPP.
MLPPP Bundle Table	
MLPPP	MLPPP bundle name, hyperlinked to the MLPPP Properties window.
Name	MLPPP interface name.
Group	MLPPP group to which the bundle belongs.
Active Link	Number of active interfaces participating in MLPPP.
Admin Status	Administrative status of the MLPPP bundle: Up or Down.
Operational Status	Administrative status of the MLPPP bundle: Up or Down.
LCP Status	Link Control Protocol (LCP) status of the MLPPP bundle: Closed, Open, Started, or Unknown.

Step 3 To view properties for individual MLPPP bundles, double-click the hyperlinked entry in the MLPPP Bundle table.

The MLPPP Properties window is displayed as shown in Figure 18-14.

Figure 18-14 MLPPP Bundle Properties Window

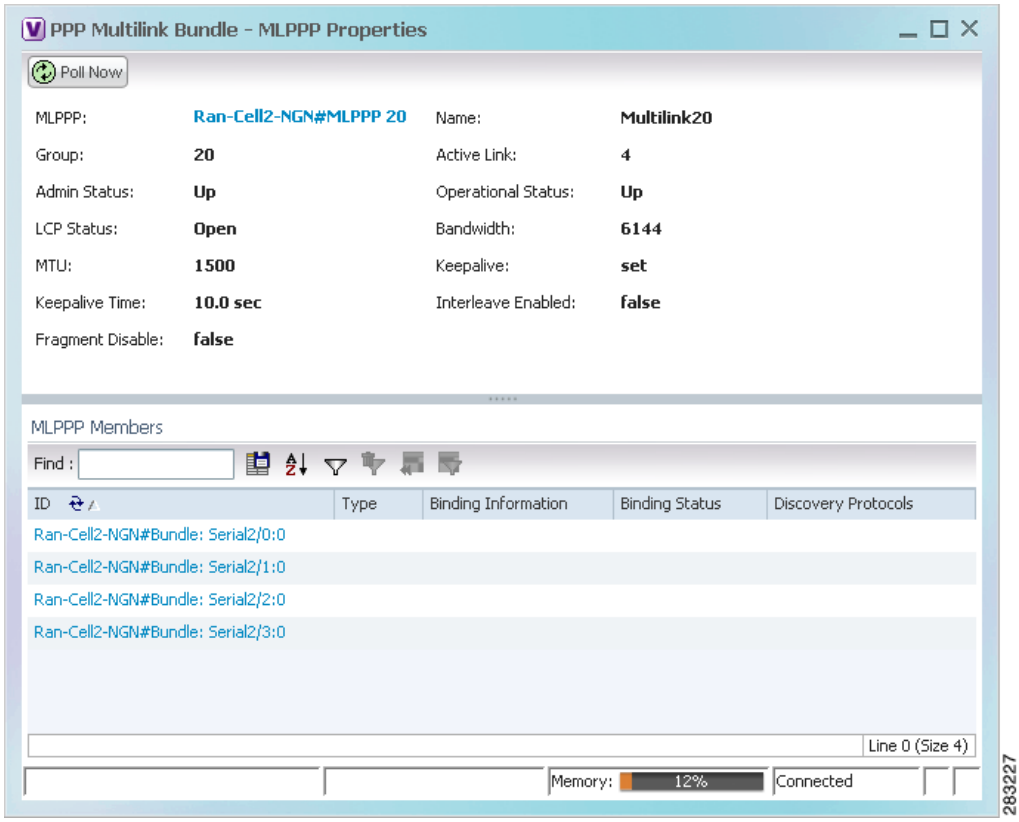


Table 18-16 describes the information that is displayed in the MLPPP Properties window.

Table 18-16 MLPPP Bundle and Member Properties

Field	Description
MLPPP	MLPPP bundle name, hyperlinked to MLPPP in logical inventory.
Name	MLPPP interface name.
Group	Group to which the MLPPP bundle belongs.
Active Link	Number of active interfaces participating in MLPPP.
Admin Status	Administrative status of the MLPPP bundle: Up or Down.
Operational Status	Operational status of the MLPPP bundle: Up or Down.
LCP Status	Link Control Protocol (LCP) status of the MLPPP bundle: Closed, Open, Started, or Unknown.
Minimum Configured Link	Minimum number of configured links for an MLPPP bundle.
Maximum Configured Link	Maximum number of configured links for an MLPPP bundle.
Bandwidth	Bandwidth allocated to the MLPPP bundle.
MTU	Size of the Maximum Transmission Unit (MTU), from 1 to 2147483647 bytes.
Keepalive	Status of the keepalive function: Set, Not Set, or Unknown.
Keepalive Time	If keepalive is enabled, the amount of time, in seconds, to wait before sending a keepalive message.
Interleave Enabled	Whether or not interleaving of small fragments is enabled.
Fragment Disable	Whether fragmentation is enabled or disabled: True or False.
Fragment Delay	Maximum size, in units of time, for packet fragments on an MLPPP bundle. Values range from 1 to 999.
Fragment Maximum	Maximum number of MLPPP bundle fragments.
Keepalive Retry	Number of times that the device sends keepalive packets without response before closing the MLPPP bundle protocol. Values range from 2 to 254.
Load Threshold	Minimum load threshold for the MLPPP bundle. If the traffic load falls below the threshold, the link is removed.

Table 18-16 MLPPP Bundle and Member Properties (continued)

Field	Description
MLPPP Members Table	
ID	MLPPP bundle member identifier, hyperlinked to the interface in physical inventory.
Type	No value is displayed in this field.
Binding Information	Binding information to which the interface is associated. The value is null.
Binding Status	No value is displayed in this field.
Discovery Protocols	Discovery protocol used on the interface.

Step 4 To view the interface properties in physical inventory, double-click the required entry in the ID column.

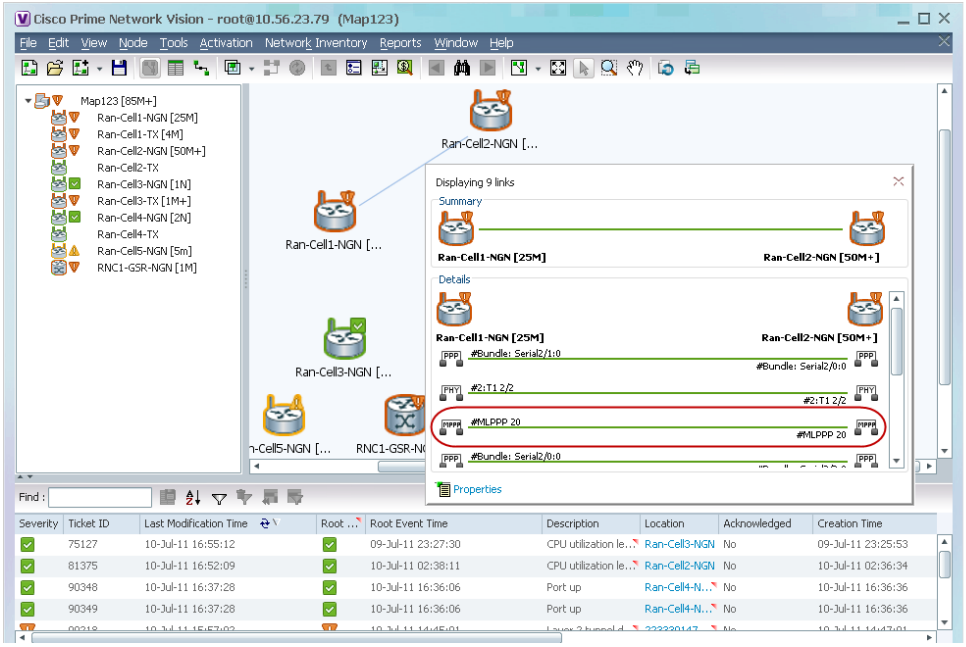
Viewing MLPPP Link Properties

An MLPPP link is a link that connects two MLPPP devices.

To view MLPPP link properties:

Step 1 In the Prime Network Vision map view, select a link connected to two MLPPP devices and open the link quick view window as shown in Figure 18-15.

Figure 18-15 MLPPP Link in Link Quick View



Step 2 In the link quick view window, click **Properties**.

Step 3 In the link properties window, select the MLPPP link. The link properties are displayed as shown in Figure 18-16.

Figure 18-16 MLPPP Link Properties

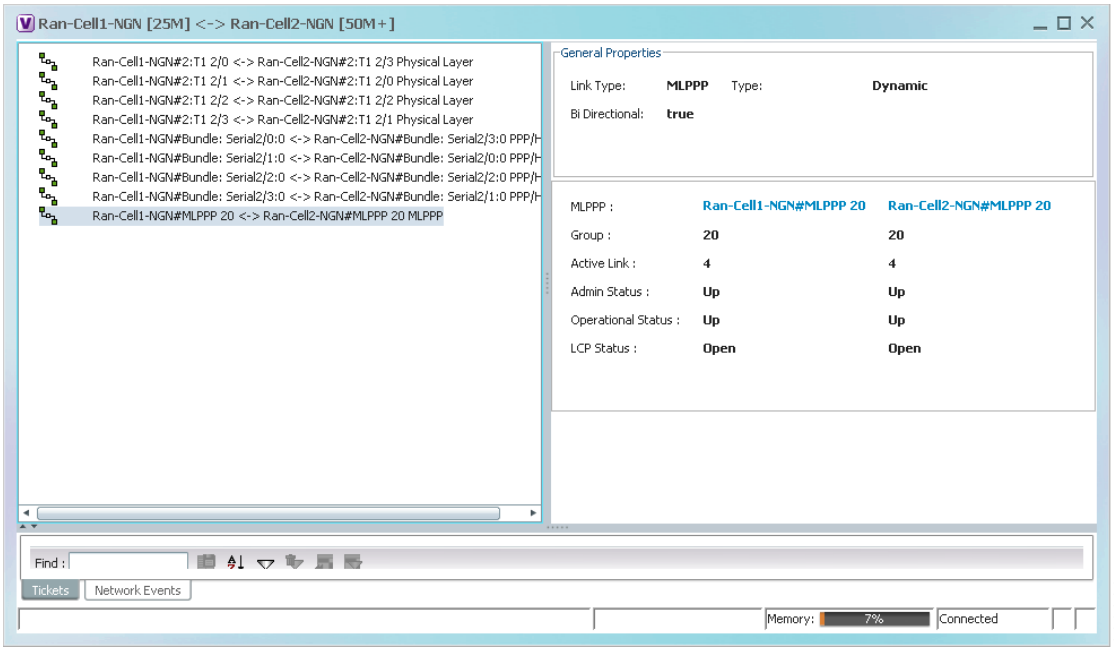


Table 18-17 describes the information that is displayed for the MLPPP link.

Table 18-17 MLPPP Link Properties

Field	Description
General Properties	
Link Type	Link protocol. In this case, MLPPP.
Type	Type of link: Dynamic or Static.
Bi Directional	Whether the link is bidirectional: True or False.
MLPPP Properties	Properties are displayed for both ends of the MLPPP link.
MLPPP	Interface configured for MLPPP, hyperlinked to the entry in physical inventory.
Group	MLPPP group to which the interface belongs.
Active Link	Number of active interfaces participating in the MLPPP link for each device.
Admin Status	Administrative status of the interface: Up or Down.
Operational Status	Operational status of the interface: Up or Down.
LCP Status	LCP status of the MLPPP interface: Closed, Open, Started, or Unknown.

Viewing MPLS Pseudowire over GRE Properties

Generic routing encapsulation (GRE) is a tunneling protocol, originated by Cisco Systems and standardized in RFC 2784. GRE encapsulates a variety of network layer packets inside IP tunneling packets, creating a virtual point-to-point link to devices at remote points over an IP network. GRE encapsulates the entire original packet with a standard IP header and GRE header before the IPsec process. GRE can carry multicast and broadcast traffic, making it possible to configure a routing protocol for virtual GRE tunnels.

In RAN backhaul networks, GRE is used to transport cell site traffic across IP networks (nonMPLS). In addition, GRE tunnels can be used to transport TDM traffic (TDMoMPLSoGRE) as part of the connectivity among cell site-facing Cisco 7600 routers and base station controller (BSC) site-facing Cisco 7600 routers, or between a Cisco Mobile Wireless Router (MWR) device and a BSC site-facing Cisco 7600 router.

Using GRE tunnels to transport Any Traffic over MPLS (AToM) enables mobile service providers to deploy AToM pseudowires in a network where MPLS availability is discontinuous; for example, in networks where the pseudowire endpoints are located in MPLS edge routers with a plain IP core network, or where two separate MPLS networks are connected by a transit network with plain IP forwarding.

To view the properties for MPLS pseudowire over GRE:

Step 1 In Prime Network Vision, right-click the required device, then choose **Inventory**.

Step 2 In the inventory window, choose **Logical Inventory > Pseudowires**. The Tunnel Edges table is displayed in the content pane as shown in Figure 18-17.

Step 3 Select the required entry and scroll horizontally until you see the required information.

Figure 18-17 MPLS Pseudowire Tunnels over GRE Properties

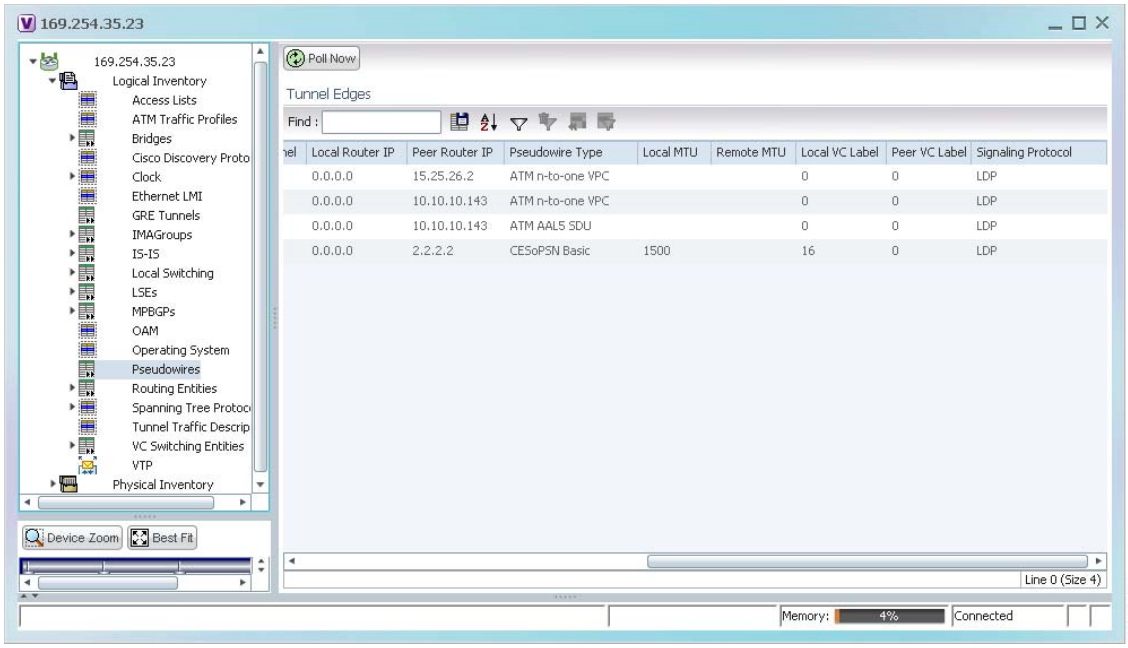


Table 18-18 describes the information included in the Tunnel Edges table specifically for MPLS pseudowire tunnels over GRE.

Table 18-18 MPLS Pseudowire over GRE Properties

Field	Description
Pseudowire Type	Type of pseudowire relevant to MToP: • ATM AAL5 SDU—ATM with ATM Adaptation Layer 5 (AAL5) service data units. • ATM n-to-one VCC—ATM with n-to-one virtual channel connection (VCC). • ATM n-to-one VPC—ATM with n-to-one virtual path connection (VPC). • CESoPSN Basic—CESoPSN basic services with CAS. • SAToP E1—SAToP on an E1 interface.
Local MTU	Size, in bytes, of the MTU on the local interface.
Remote MTU	Size, in bytes, of the MTU on the remote interface.
Preferred Path Tunnel	Path to be used for MPLS pseudowire traffic. Click the hyperlinked entry to view the tunnel details in logical inventory.

Step 4 To view GRE Tunnel properties, choose **Logical Inventory > GRE Tunnels**.

Figure 18-18 shows the Tunnel Edges table that is displayed for GRE tunnels.

Figure 18-18 GRE Tunnel Properties in Logical Inventory

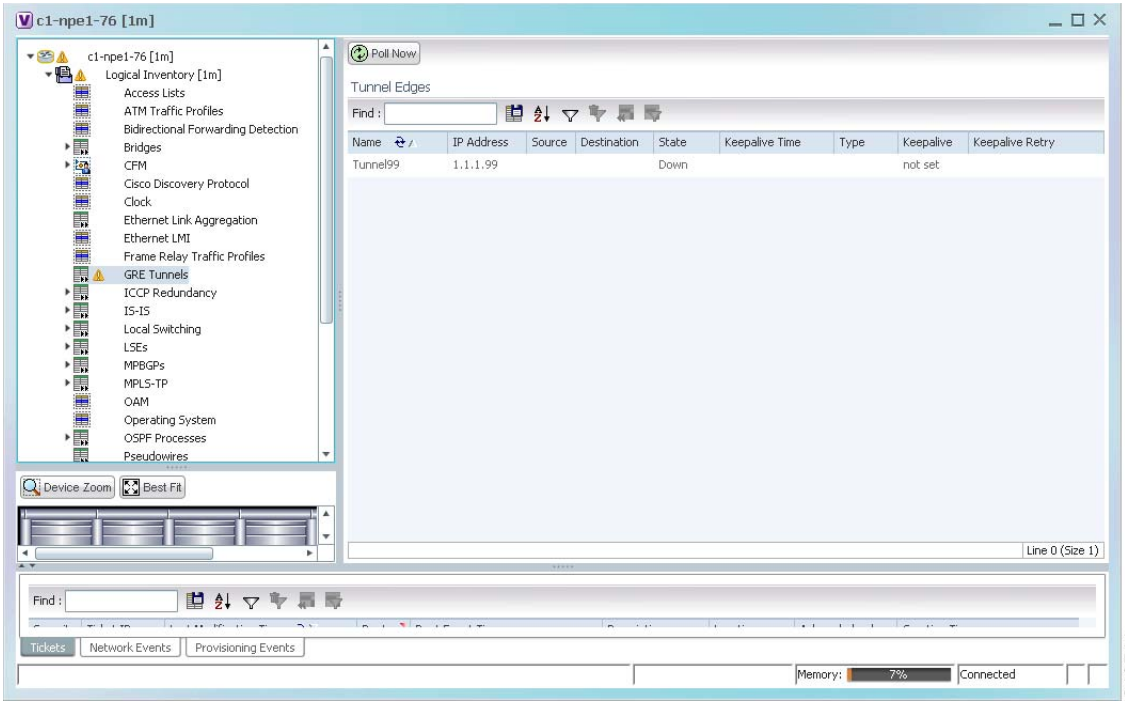


Table 18-19 describes the information that is displayed for GRE tunnels in logical inventory.

Table 18-19 GRE Tunnel Properties in Logical Inventory

Field	Description
Name	Tunnel name.
IP Address	Tunnel IP address.
Source	IP address local to the device.
Destination	IP address of the remote router.
State	State of the tunnel: Up or Down.
Keepalive Time	If keepalive is enabled, the amount of time, in seconds, to wait before sending a keepalive message.
Type	Tunnel type.
Keepalive	Status of the keepalive function: Set, Not Set, or Unknown.
Keepalive Retry	Number times that the device continues to send keepalive packets without response before bringing the tunnel interface protocol down. Values range from 2 to 254, with a default of 3.

Network Clock Service Overview

Network clock service refers to the means by which a clock signal is generated or derived and distributed through a network and its individual nodes for the purpose of ensuring synchronized network operation. Network clocking is particularly important for mobile service providers to ensure proper transport of cellular traffic from cell sites to Base Station Control (BSC) sites.

Note In Prime Network Vision, *clock service* refers to *network clock service*.

The following topics describe how to use Prime Network Vision to monitor clock service:

- Monitoring Clock Service, page 18-34
- Monitoring PTP Service, page 18-36
- Viewing Pseudowire Clock Recovery Properties, page 18-41
- Viewing SyncE Properties, page 18-45
- Applying a Network Clock Service Overlay, page 18-48

Monitoring Clock Service

To monitor clock service:

Step 1 In Prime Network Vision, right-click the required device, then choose **Inventory**.

Step 2 In the inventory window, choose **Logical Inventory > Clock**. Clock service information is displayed in the content pane as shown in Figure 18-19.

Figure 18-19 Clock Service Properties

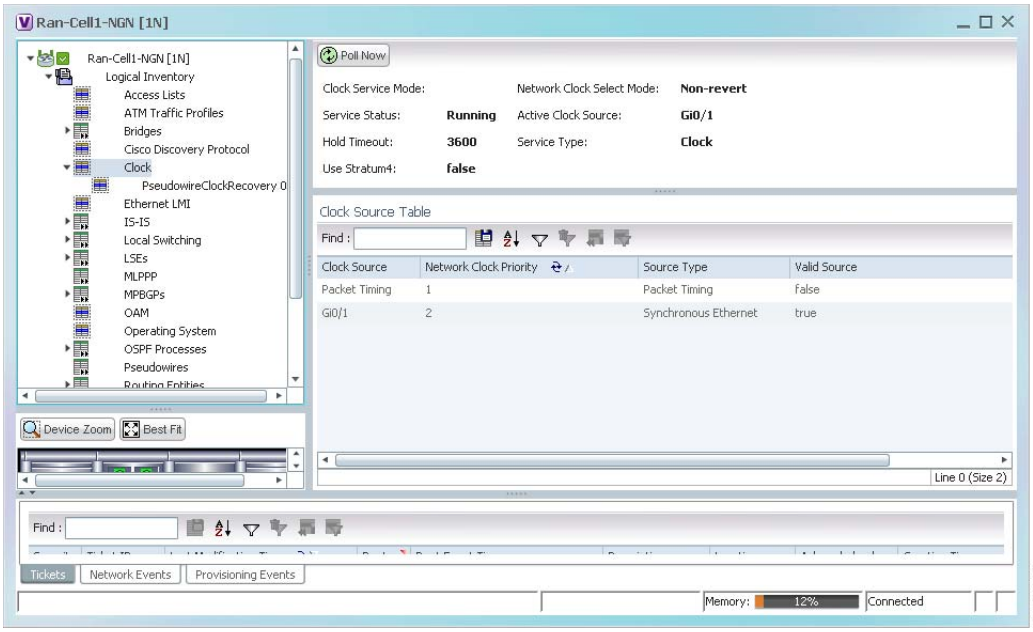


Table 18-20 describes the information displayed for clocking service.

Table 18-20 Clock Service Properties

Field	Description
Clock Service Mode	This field is not populated.
Network Clock Select Mode	Action to take if the master device fails: • Non-revert—Do not use the master device again after it recovers from the failure. • Revert—Use the master device again after it recovers and functions correctly for a specified amount of time. • Unknown—The network clock selection mode is unknown.
Service Status	Status of the system service: • Initializing—The service is starting up. • Down—The service is down. • Reset—The service has been reset. • Running—The service is running. • Other—A status other than those listed.
Active Clock Source	Current active clock source used by the device.
Hold Timeout	How long the device waits before reevaluating the network clock entry. Values can be from 0-86400 seconds, Not Set, or infinite.
Service Type	Type of system service, such as Clock or Cisco Discovery Protocol.
Use Stratum4	Quality of the clock source: • True—Use Stratum 4, the lowest level of clocking quality. • False—(Default) Use Stratum 3, a higher level of clocking quality than Stratum 4.

Table 18-20 Clock Service Properties (continued)

Field	Description
Clock Source Table	This table is displayed only if there are active clock sources.
Clock Source	Current active clock source used by the device.
Network Clock Priority	Priority of the clock source with 1 being the highest priority.
Source Type	Method by which clocking information is provided: • BITS—Timing is supplied by a Building Integrated Timing Supply (BITS) port clock. • E1/T1—Clocking is provided via an E1 or T1 interface. • Packet-Timing—Clocking is provided over a packet-based network. • Synchronous Ethernet—Clocking is provided by Synchronous Ethernet. • Others—Clocking is provided by a source other than the above.
Valid Source	Validity of the clock source: • True—The clock source is valid and operational. • False—The clock source is not valid or is not operational.

Monitoring PTP Service

In networks that employ TDM, periodic synchronization of device clocks is required to ensure that the receiving device knows which channel is which for accurate reassembly of the data stream. The Precision Time Protocol (PTP) standard:

- Specifies a clock synchronization protocol that enables this synchronization.
- Applies to distributed systems that consist of one or more nodes communicating over a network.

Defined by IEEE 1588-2008, PTP Version 2 (PTPv2) allows device synchronization at the nanosecond level.

PTP uses the concept of master and slave devices to achieve precise clock synchronization. Using PTP, the master device periodically starts a message exchange with the slave devices. After noting the times at which the messages are sent and received, each slave device calculates the difference between its system time and the system time of the master device. The slave device then adjusts its clock so that it is synchronized with the master device. When the master device initiates the next message exchange, the slave device again calculates the difference and adjusts its clock. This repetitive synchronization ensures that device clocks are coordinated and that data stream reassembly is accurate.

To monitor PTP service:

Step 1 In Prime Network Vision, right-click the required device, then choose **Inventory**.

Step 2 In the inventory window, choose **Logical Inventory > Clock > PTP Service**. The PTP service properties are displayed in the content pane as shown in Figure 18-20.

Figure 18-20 PTP Service Properties

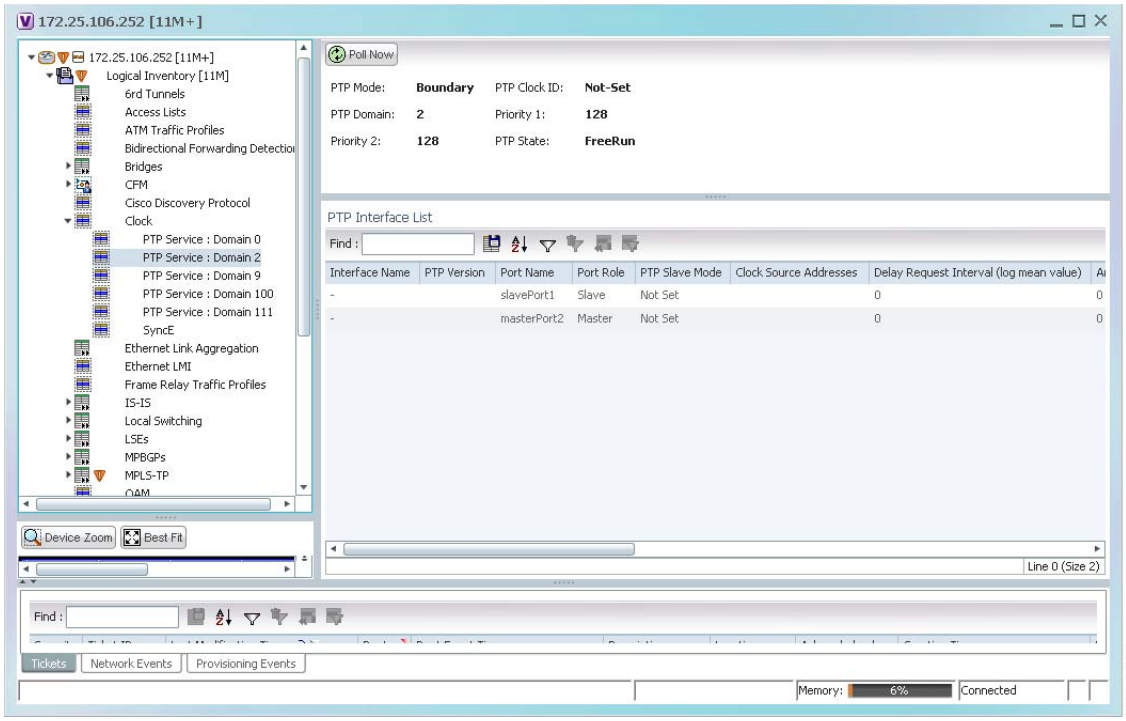


Table 18-21 describes the properties that are displayed for PTP service.

Table 18-21 PTP Service Properties

Field	Description
PTP Mode	Mode of PTP operation: • Boundary—Boundary clock mode. • E2E Transparent—End-to-end transparent clock mode. • Ordinary—Ordinary clock mode. • P2P Transparent—Peer-to-peer transparent clock mode. • Unknown—The clock mode is unknown. **Note** Cisco MWR-2941 routers support Ordinary mode only.
PTP Clock ID	Clock identifier derived from the device interface.
PTP Domain	Number of the domain used for PTP traffic. A single network can contain multiple separate domains.
Priority 1	First value checked for clock selection. The clock with the lowest priority takes precedence.
Priority 2	If two or more clocks have the same value in the Priority 1 field, the value in this field is used for clock selection.
Port State	Clock state according to the PTP engine: • Freerun—The slave clock is not locked to a master clock. • Holdover—The slave device is locked to a master device, but communication with the master is lost or the timestamps in the PTP packet are incorrect. • Acquiring—The slave device is receiving packets from a master and is trying to acquire a clock. • Freq locked—The slave device is locked to the master device with respect to frequency, but is not aligned with respect to phase. • Phase aligned—The slave device is locked to the master device with respect to both frequency and phase.
PTP Interface List Table	
Interface Name	Interface identifier.
PTP Version	Version of PTP used. The default value is 2, indicating PTPv2.
Port Name	Name of the PTP port clock.
Port Role	PTP role of the clock: Master or Slave.

Table 18-21 PTP Service Properties (continued)

Field	Description
PTP Slave Mode	For an interface defined as a slave device, the mode used for PTP clocking: • Not Set—The slave mode is not used. • Multicast—The interface uses multicast mode for PTP clocking. • Unicast—The interface uses unicast mode for PTP clocking. • Unicast with Negotiation—The interface uses unicast mode with negotiation for PTP clocking.
Clock Source Addresses	IP addresses of the clock source.
Delay Request Interval (log mean value)	When the interface is in PTP master mode, the interval specified to member devices for delay request messages. The intervals use base 2 values, as follows: • 4—1 packet every 16 seconds. • 3—1 packet every 8 seconds. • 2—1 packet every 4 seconds. • 1—1 packet every 2 seconds. • 0—1 packet every second. • -1—1 packet every 1/2 second, or 2 packets per second. • -2—1 packet every 1/4 second, or 4 packets per second. • -3—1 packet every 1/8 second, or 8 packets per second. • -4—1 packet every 1/16 seconds, or 16 packets per second. • -5—1 packet every 1/32 seconds, or 32 packets per second. • -6—1 packet every 1/64 seconds, or 64 packets per second.
Announce Interval (log mean value)	Interval value for PTP announcement packets: • 4—1 packet every 16 seconds. • 3—1 packet every 8 seconds. • 2—1 packet every 4 seconds. • 1—1 packet every 2 seconds. • 0—1 packet every second. • -1—1 packet every 1/2 second, or 2 packets per second. • -2—1 packet every 1/4 second, or 4 packets per second. • -3—1 packet every 1/8 second, or 8 packets per second. • -4—1 packet every 1/16 seconds, or 16 packets per second. • -5—1 packet every 1/32 seconds, or 32 packets per second. • -6—1 packet every 1/64 seconds, or 64 packets per second.

Table 18-21 PTP Service Properties (continued)

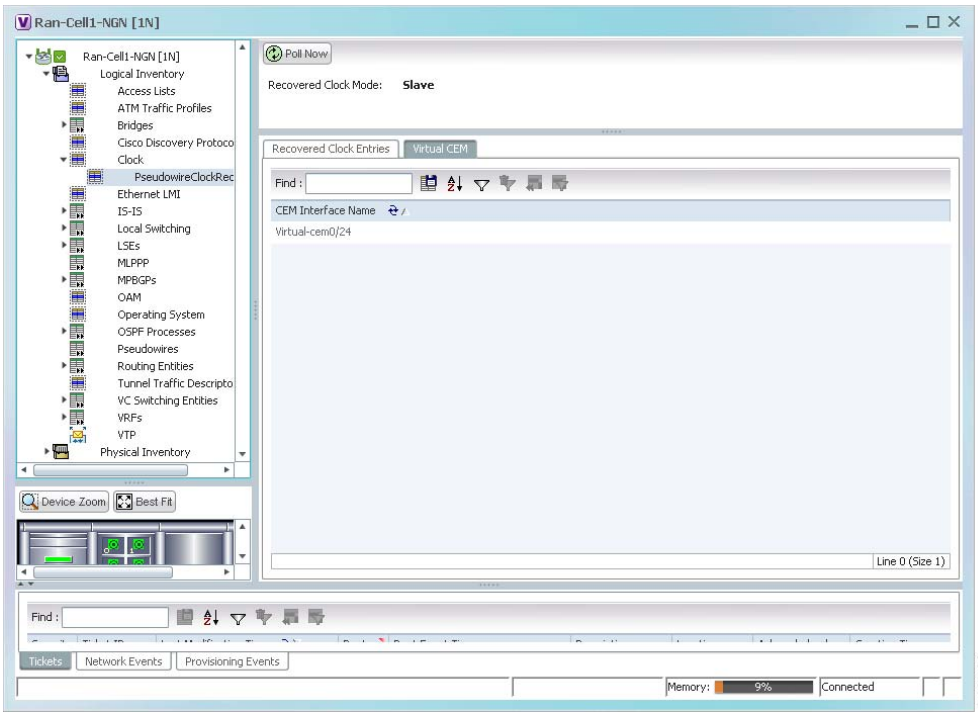
Field	Description
Announce Timeout	Number of PTP announcement intervals before the session times out. Values are 2-10.
Sync Interval (log mean value)	Interval for sending PTP synchronization messages: • 4—1 packet every 16 seconds. • 3—1 packet every 8 seconds. • 2—1 packet every 4 seconds. • 1—1 packet every 2 seconds. • 0—1 packet every second. • -1—1 packet every 1/2 second, or 2 packets per second. • -2—1 packet every 1/4 second, or 4 packets per second. • -3—1 packet every 1/8 second, or 8 packets per second. • -4—1 packet every 1/16 seconds, or 16 packets per second. • -5—1 packet every 1/32 seconds, or 32 packets per second. • -6—1 packet every 1/64 seconds, or 64 packets per second.
Sync Limit (nanoseconds)	Maximum clock offset value, in nanoseconds, before PTP attempts to resynchronize.
Interface	Physical interface identifier, hyperlinked to the routing information for the interface.
PTP Master Mode	For an interface defined as a master device, the mode used for PTP clocking: • Not Set—The master mode is not used. • Multicast—The interface uses multicast mode for PTP clocking. • Unicast—The interface uses unicast mode for PTP clocking. This mode allows a single destination. • Unicast with Negotiation—The interface uses unicast mode with negotiation for PTP clocking. This mode allows up to 128 destinations.
Clock Destination Addresses	IP addresses of the clock destinations. This field contains IP addresses only when Master mode is enabled.
Domain	Clocking domain.

Viewing Pseudowire Clock Recovery Properties

To view pseudowire clock recovery properties:

Step 1 Choose **Logical Inventory > Clock > Pseudowire Clock Recovery**. Prime Network Vision displays the Virtual CEM information by default. See Figure 18-21.

Figure 18-21 Pseudowire Clock Recovery - Virtual CEM Tab



Step 2 To view more information about a virtual CEM, right-click the virtual CEM, then choose **Properties**. The Virtual CEM Properties window is displayed.

The information that is displayed in the Virtual CEM Properties window depends on whether or not the virtual CEM belongs to a group:

- If a CEM group is not configured on the virtual CEM, the Virtual CEM Properties window contains only the CEM interface name.
- If a CEM group is configured on the virtual CEM, the Virtual CEM Properties window contains the information described in Table 18-22.

Table 18-22 Virtual CEM Group Properties

Field	Description
CEM Interface Name	CEM interface name.
CEM Group Table	
CEM Group	Name of the virtual CEM group.
Framing	Framing mode used for the CEM channel: • Framed—Specifies the channels used for the controller, such as Channels: (1-8), (10-14). The channels that are available depend on the type of controller: T1, E1, T3, or E3. • Unframed—Indicates that a single CEM channel is used for all T1/E1 timeslots. SAToP uses the unframed mode.
Pseudowire	Name of the pseudowire configured on the CEM interface, hyperlinked to the pseudowire properties in logical inventory.
Oper Status	Operational status of the CEM interface: • Dormant—The interface is dormant. • Down—The interface is down. • Not Present—An interface component is missing. • Testing—The interface is in test mode. • Unknown—The interface has an unknown operational status. • Up—The interface is up.
Admin Status	Administrative status of the CEM interface: • Down—The CEM interface is administratively down. • Testing—The administrator is testing the CEM interface. • Unknown—The administrative status is unknown. • Up—The CEM interface is administratively up.

Step 3 To view additional CEM group properties, double-click the required CEM group.

Table 18-23 describes the information displayed in the CEM Group Properties window.

Table 18-23 CEM Group Properties

Field	Description
Oper Status	Operational status of the CEM interface: • Dormant—The interface is dormant. • Down—The interface is down. • Not Present—An interface component is missing. • Testing—The interface is in test mode. • Unknown—The interface has an unknown operational status. • Up—The interface is up.
Idle Pattern	Eight-bit hexadecimal number that is transmitted on a T1 or E1 line when missing packets are detected on the pseudowire (PW) circuit.
Type	Type of CEM group. This is always DS0 Bundle.
Idle CAS Pattern	When CAS is used, the 8-bit hexadecimal signal that is sent when the CEM interface is identified as idle.
Bundle Location	Associated card and slot for the virtual CEM, using the virtual CEM port 24; for example virtual-cem/8/3/24:0.
Dejitter	Size of the dejitter buffer in milliseconds (ms). The range is 4 to 500 ms with a default of 4 ms.
RTP Hdr Compression	Whether RTP header compression is enabled or disabled.
RTP Enabled	Whether RTP compression is enabled or disabled.
Admin Status	Administrative status of the CEM interface: • Down—The CEM interface is administratively down. • Testing—The administrator is testing the CEM interface. • Unknown—The administrative status is unknown. • Up—The CEM interface is administratively up.
ID	DS0 bundle CEM group identifier.
Payload Size	Size of the payload for packets on the CEM interface. The range is 32 to 1312 bytes.

Step 4 To view recovered clock entries, click the Recovered Clock Entries tab. See Figure 18-22.

If no recovered clock entries exist, this tab is not displayed.

Figure 18-22 Pseudowire Clock Recovery - Recovered Clock Entries Tab

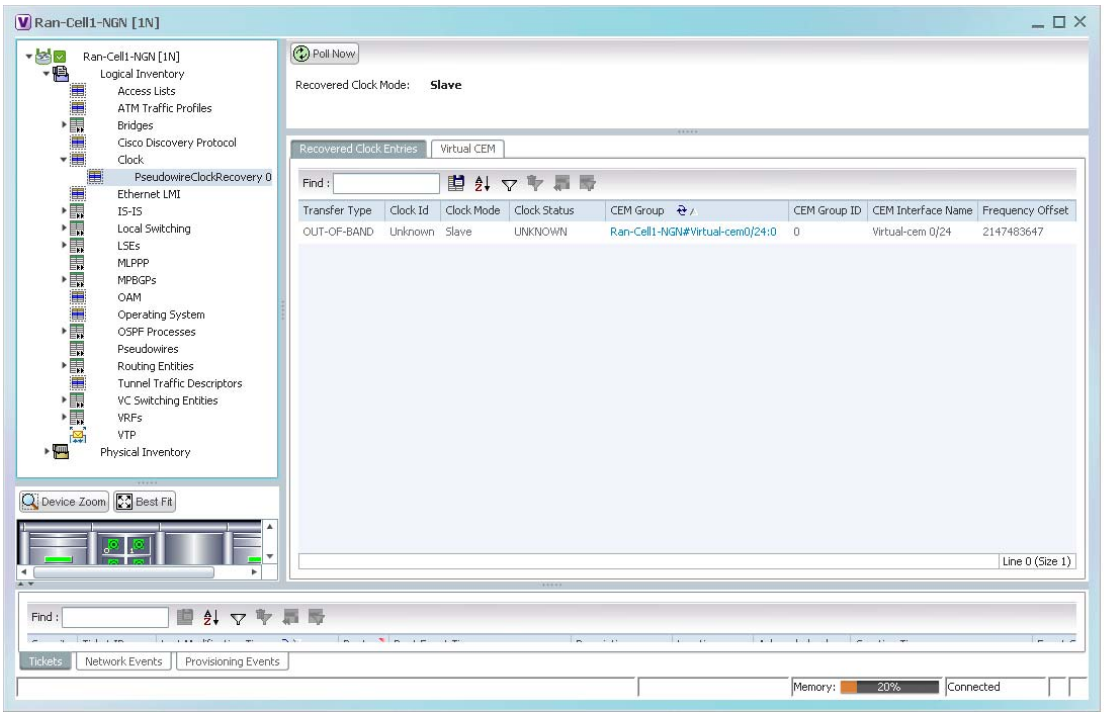


Table 18-24 describes the information displayed for pseudowire clock recovery.

Table 18-24 Pseudowire Clock Recovery Properties

Field	Description
Recovered Clock Source	Interface (slot/subslot) in which clock recovery occurred. Click the hyperlinked entry to view its properties in physical inventory.
Recovered Clock Mode	Recovered clock mode: • Adaptive—The devices do not have a common clock source. The recovered clock is derived from packet arrival. • Differential—The edge devices have a common clock source, and the recovered clock is derived from timing information in packets and the related difference from the common clock. • Synchronous—A GPS or BITS clock source externally synchronizes both end devices. This method is extremely accurate, but is rarely available for all network devices.

Table 18-24 Pseudowire Clock Recovery Properties (continued)

Field	Description
Virtual CEM Tab	
CEM Interface Name	Virtual CEM interface associated with the clock.
Recovered Clock Entries Tab	This tab appears if recovered entries exist.
Transfer Type	• In-band—The clocking information is sent over the same pseudowire as the bearer traffic. • Out-of-band—The clocking information is sent over a dedicated pseudowire between the sending and receiving SPAs.
Clock ID	Clock identifier, if known.
Clock Mode	Clock mode of the recovered clock: • Adaptive—The recovered clock was obtained using ACR. • Primary—The recovered clock was obtained from a clock with the highest priority. • Secondary—The recovered clock was obtained from a clock with a lower priority than the primary clock.
Clock Status	Status of the clock: • Acquiring—The clock is obtaining clocking information. • Acquired—The clock has obtained the required clocking information. • Holdover—The current primary clock is invalid and a holdover timer has started to check whether or not the clock becomes valid within the specified holdover time.
CEM Group	CEM group associated with the clock.
CEM Group ID	Identifier of the CEM group associated with the clock.
CEM Interface Name	Virtual CEM interface associated with the clock.
Frequency Offset	Offset to the clock frequency, in Hz.

Viewing SyncE Properties

With Ethernet equipment gradually replacing SONET and SDH equipment in service-provider networks, frequency synchronization is required to provide high-quality clock synchronization over Ethernet ports. Synchronous Ethernet (SyncE), a recently adopted standard, provides the required synchronization at the physical level.

In SyncE, Ethernet links are synchronized by timing their bit clocks from high-quality, stratum-1-traceable clock signals in the same manner as SONET/SDH. Operations messages maintain SyncE links, and ensure a node always derives timing from the most reliable source.

To view SyncE properties, choose **Logical Inventory > Clock > SyncE**. (See Figure 18-23.)

Figure 18-23 SyncE Properties in Logical Inventory

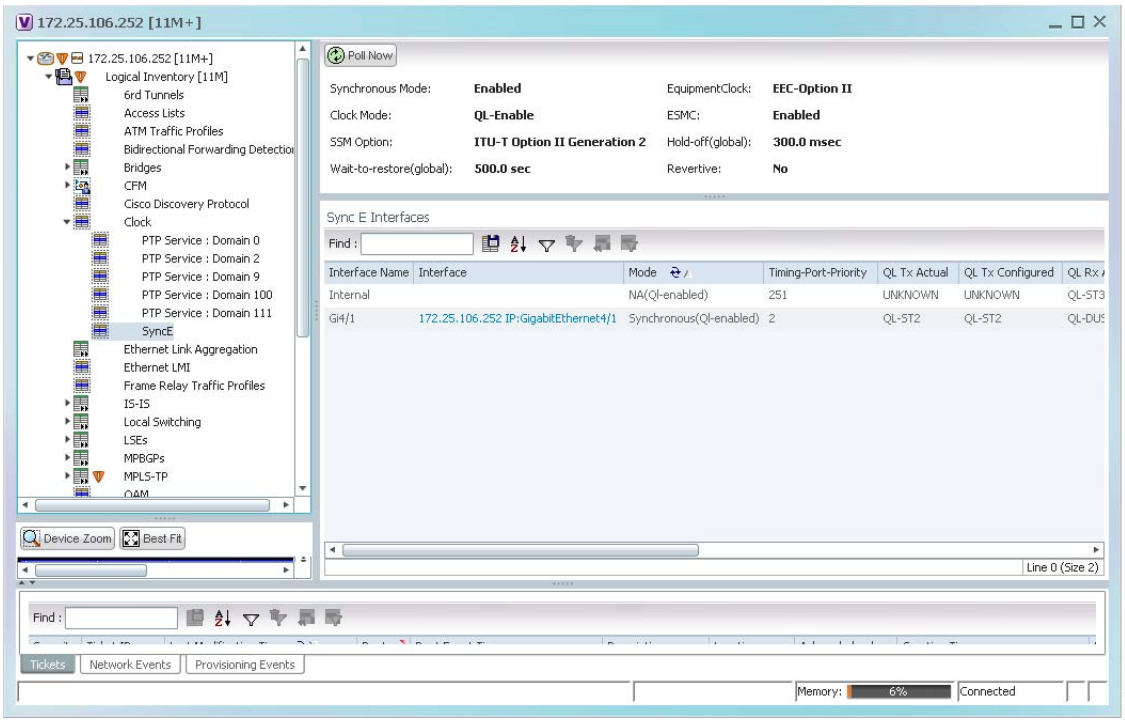


Table 18-25 describes the information that is displayed for SyncE.

Table 18-25 SyncE Properties

Field	Description
Synchronous Mode	Status of the automatic synchronization selection process: Enabled or Disable.
Equipment Clock	Ethernet Equipment Clock (EEC) options: EEC-Option I or EEC-Option II.
Clock Mode	Whether the clock is enabled or disabled for the Quality Level (QL) function: QL-Enabled or QL-Disabled.
ESMC	Ethernet Synchronization Message Channel (ESMC) status: Enabled or Disabled.
SSM Option	Synchronization Status Message (SSM) option being used: • ITU-T Option I • ITU-T Option II Generation 1 • ITU-T Option II Generation 2
Hold-off (global)	Length of time (in milliseconds) to wait before issuing a protection response to a failure event.
Wait-to-restore (global)	Length of time (in seconds) to wait after a failure is fixed before the span returns to its original state.
Revertive	Whether the network clock is to use revertive mode: Yes or No.

Table 18-25 SyncE Properties (continued)

Field	Description
SyncE Interfaces Table	
Interface Name	Name of the Gigabit or 10 Gigabit interface associated with SyncE. If SyncE is not associated with a Gigabit or 10 Gigabit interface, this field contains *Internal*.
Interface	Hyperlinked entry to the interface routing information in the Routing Entity Controller window. For more information, see Viewing Routing Entities, page 17-31. This field does not apply for Internal interfaces.
Mode	Whether the interface is enabled or disabled for the QL function: QL-Enabled or QL-Disabled.
Timing Port Priority	Value used for selecting a SyncE interface for clocking if more than one interface is configured. Values are from 1 to 250, with 1 being the highest priority.
QL Tx Actual	Actual type of outgoing quality level information, depending on the globally configured SSM option: • ITU-T Option I—Available values are QL-PRC, QL-SSU-A, QL-SSU-B, QL-SEC, and QL-DNU. • ITU-T Option II Generation 1—Available values are QL-PRS, QL-STU, QL-ST2, QL-SMC, QL-ST4, and QL-DUS. • ITU-T Option II Generation 2—Available values are QL-PRS, QL-STU, QL-ST2, QL-TNC, QL-ST3, QL-SMC, QL-ST4, and QL-DUS.
QL Tx Configured	Configured type of outgoing quality level information, depending on the globally configured SSM option. See QL Tx Actual for the available values.
QL Rx Actual	Actual type of incoming quality level information, depending on the globally configured SSM option. See QL Tx Actual for the available values.
QL Rx Configured	Configured type of incoming quality level information, depending on the globally configured SSM option. See QL Tx Actual for the available values.
Hold-Off Timer (msecs)	Length of time (in milliseconds) to wait after a clock source goes down before removing the source.
Wait-to-Restore (secs)	Length of time (in seconds) to wait after a failure is fixed before the interface returns to its original state.

Table 18-25 SyncE Properties (continued)

Field	Description
ESMC Tx	Whether ESMC is enabled for outgoing QL information on the interface: Enabled, Disabled, or NA (Not Available).
ESMC Rx	Whether ESMC is enabled for incoming QL information on the interface: Enabled, Disabled, or NA (Not Available).
SSM Tx	Whether SSM is enabled for outgoing QL information on the interface: Enabled, Disabled, or NA (Not Available).
SSM Rx	Whether SSM is enabled for incoming QL information on the interface: Enabled, Disabled, or NA (Not Available).

Applying a Network Clock Service Overlay

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

To apply a network clock overlay:

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

Step 2 From the main toolbar, click **Choose Overlay Type** and choose **Network Clock**.

The Select Network Clock Service Overlay dialog box is displayed.

Step 3 Do one of the following:

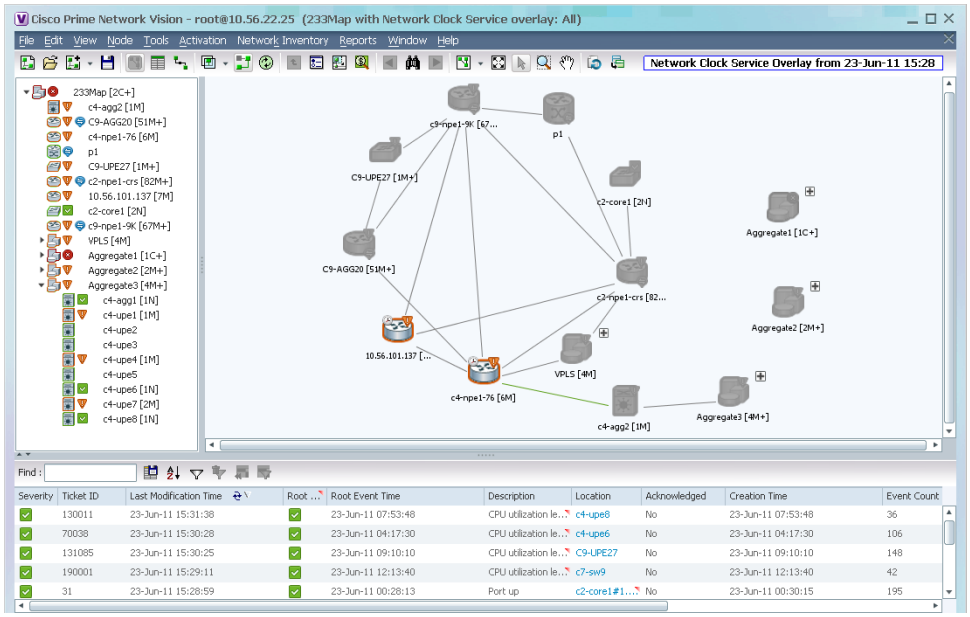
- Choose a search category, enter a search string, then click **Go** to narrow the search results to a range of network clock services or a specific network clock service. Search categories include:
  - Description
  - Name

  The search condition is “contains.” Search strings are case-insensitive. For example, if you choose the Name category and enter “net,” Prime Network Vision displays network clock services that have “net” in their names whether net appears at the beginning of the name, the middle, or at the end: for example, Ethernet.
- Choose **Show All** to display all network clock services.

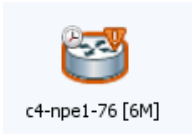
Step 4 Select the network clock service overlay that you want to apply to the map.

The elements and links used by the selected network clock are highlighted in the map, and the overlay name is displayed in the title of the window. (See Figure 18-24.)

Figure 18-24 Network Clock Service Overlay Example



In addition, the elements configured for clocking service display a clock service icon as in the following example:



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

Viewing CEM and Virtual CEM Properties

The following topics describe how to view CEM and virtual CEM properties and interfaces:

- Viewing CEM Interfaces, page 18-50
- Viewing Virtual CEMs, page 18-51
- Viewing CEM Groups, page 18-51

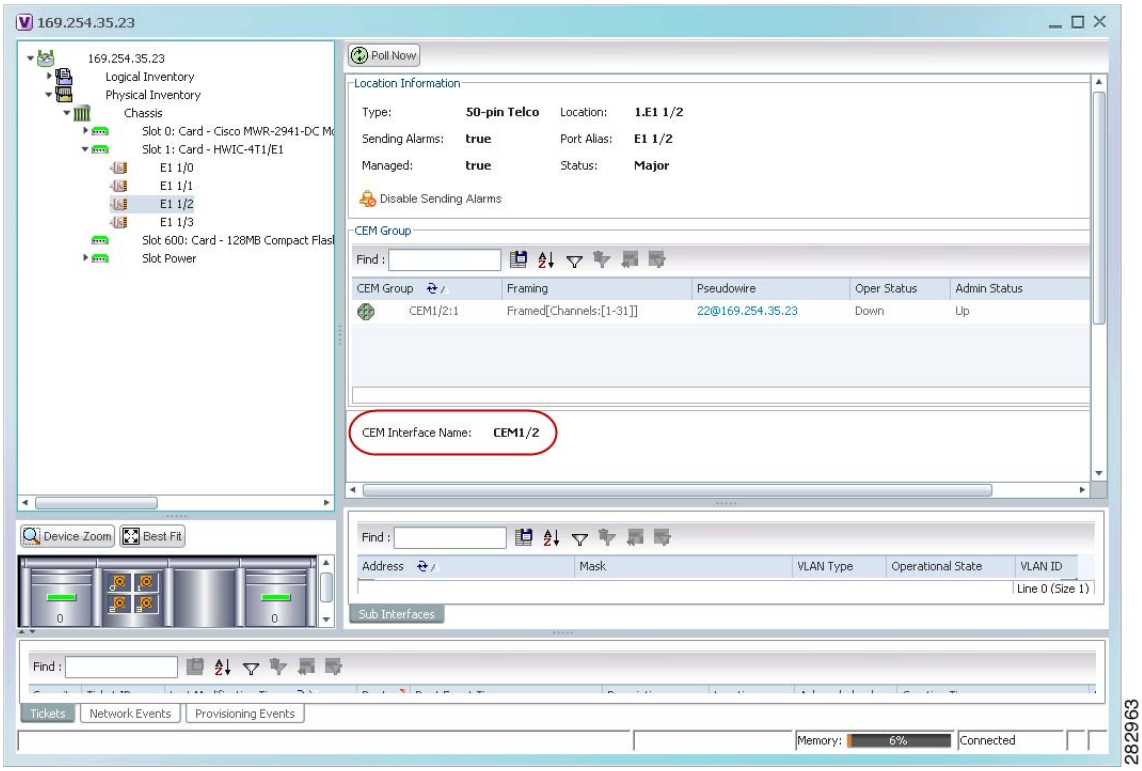
Viewing CEM Interfaces

To view CEM interfaces:

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

Step 2 In the inventory window, choose **Physical Inventory > Chassis >** *slot* **>** *subslot* **>** *interface*. The CEM interface name is displayed in the content pane as shown in Figure 18-25.

Figure 18-25 CEM Interface



Viewing Virtual CEMs

To view virtual CEMs, choose **Logical Inventory > Clock > Pseudowire Clock Recovery**.

The virtual CEM interfaces are listed in the Virtual CEM tab.

Viewing CEM Groups

CEM groups can be configured on physical or virtual CEM interfaces. The underlying interface determines where you view CEM group properties in Prime Network Vision:

- Viewing CEM Groups on Physical Interfaces, page 18-51
- Viewing CEM Groups on Virtual CEM Interfaces, page 18-53

Viewing CEM Groups on Physical Interfaces

When you configure a CEM group on a physical interface, the CEM group properties are displayed in physical inventory for that interface.

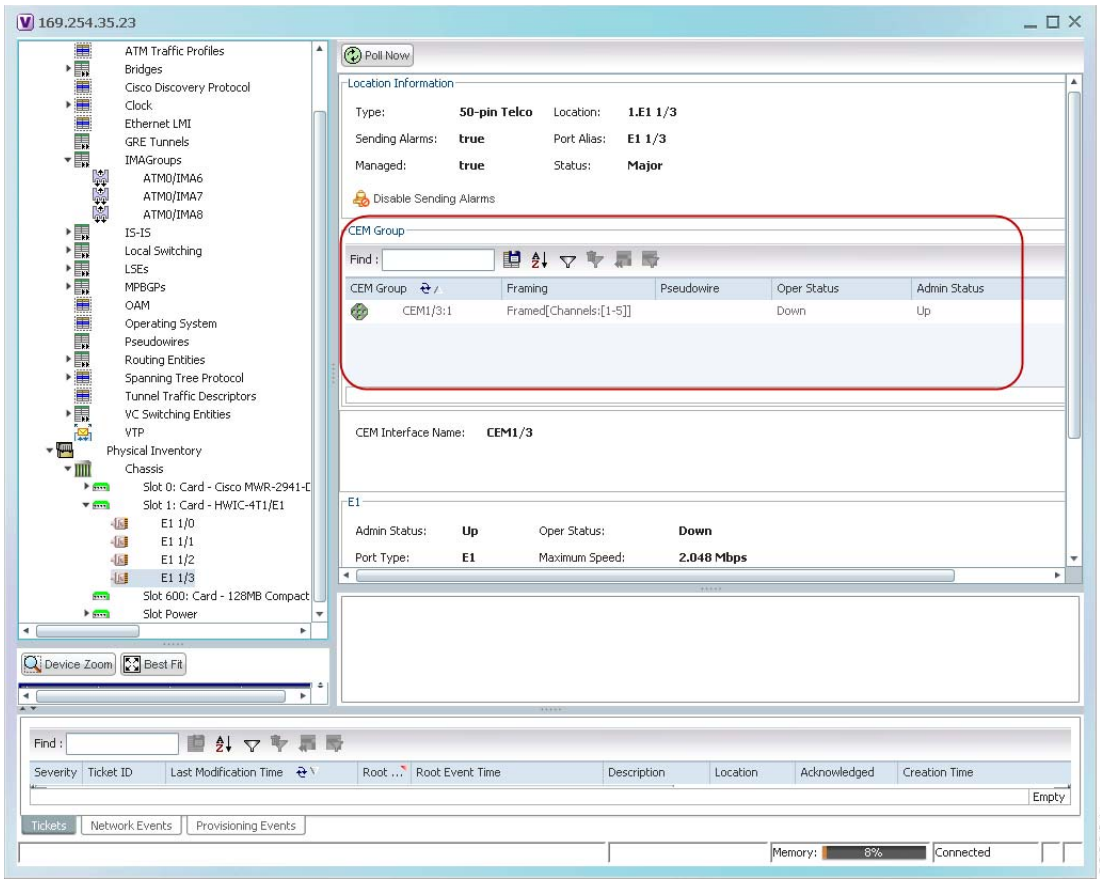
To view CEM groups configured on physical interfaces:

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

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

The CEM group information is displayed in the content pane with other interface properties (Figure 18-26).

Figure 18-26 CEM Group Information

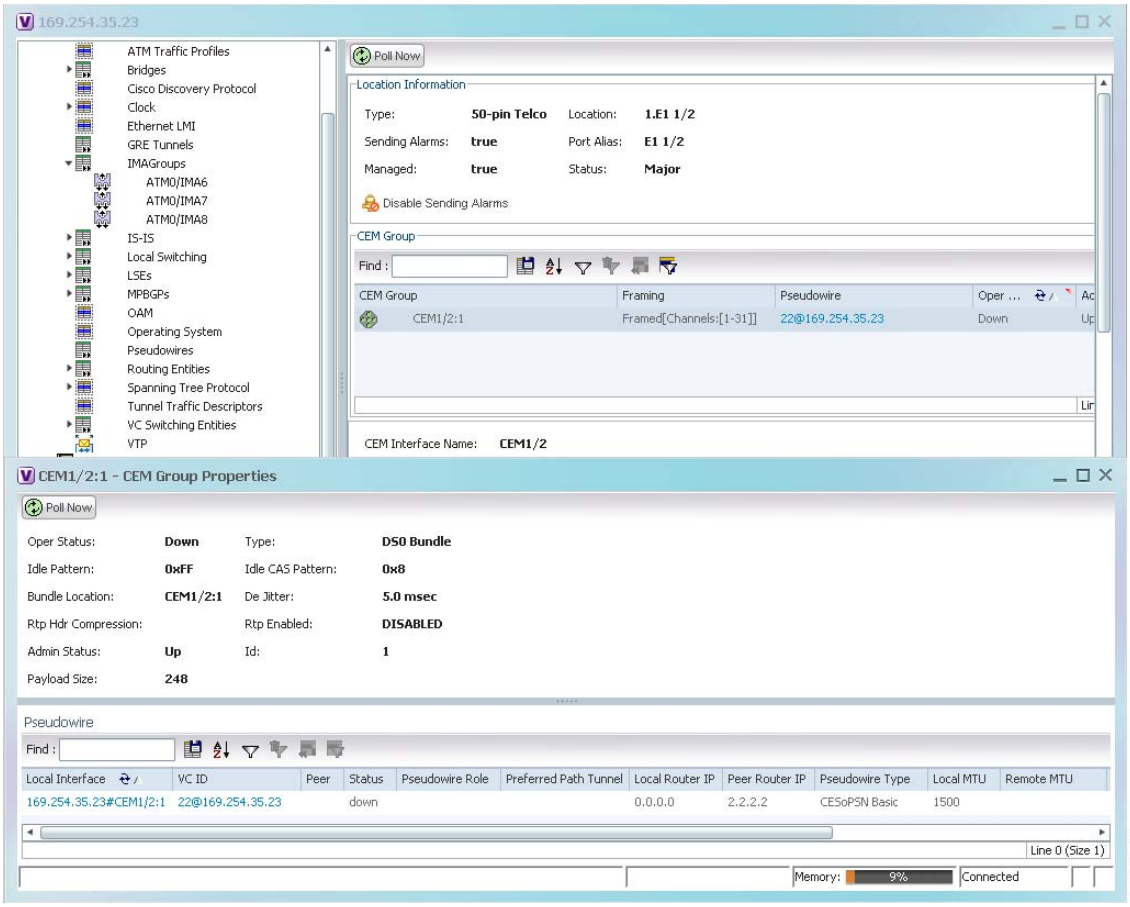


See Table 18-22 for a description of the properties displayed for CEM groups in the content pane.

Step 3 To view additional information, double-click the required group.

The CEM Group Properties window is displayed as shown in Figure 18-27.

Figure 18-27 CEM Group Properties Window



See Table 17-24 on page 17-48 for the properties displayed in the Pseudowire table in the CEM Group Properties window.

Viewing CEM Groups on Virtual CEM Interfaces

When you configure a CEM group on a virtual CEM, the CEM group information is displayed below the virtual CEM in logical inventory.

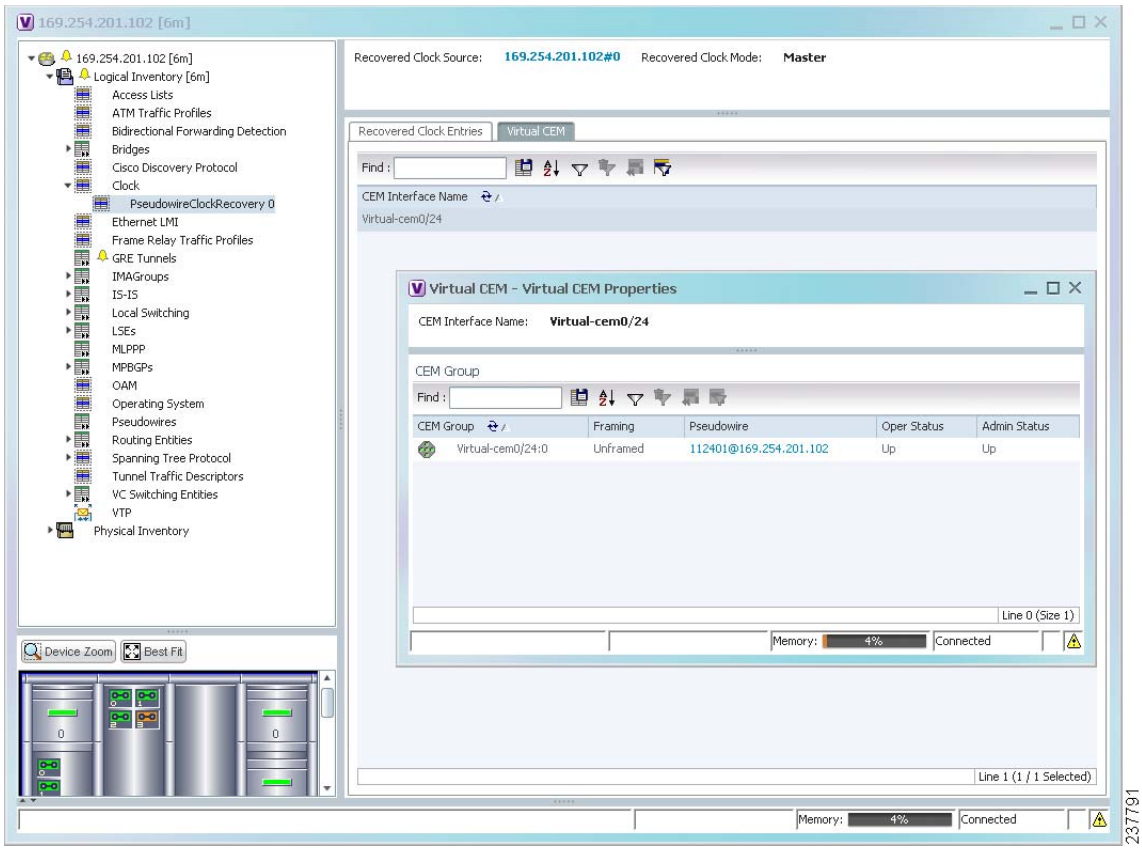
To view CEM groups on virtual CEM interfaces:

Step 1 In Prime Network Vision, right-click the required device, then choose **Inventory**.

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

Step 3 In the Virtual CEM tab, right-click the CEM interface name and choose **Properties**. The CEM group properties are displayed in a separate window (Figure 18-28). If a pseudowire is configured on the CEM group for out-of-band clocking, the pseudowire VCID is also shown.

Figure 18-28 CEM Group Properties



Step 4 To view additional CEM group properties, double-click the required CEM group.

Table 18-23 describes the information displayed in the CEM Group Properties window.



CHAPTER 19

Viewing SBC Properties

This topic identifies and describes the properties for Session Border Controllers (SBCs) that appear in Cisco Prime Network Vision (Prime Network Vision)logical inventory.

An SBC can provide the following types of services:

- Protocol and media interworking
- Session routing
- Hosted Network Address Translation (NAT) and firewall traversal
- Security and AAA
- Intra- and inter-VPN interconnections and optimization
- Media transcoding with an external media server

SBC services are divided into the following components:

- Data Border Element (DBE)—Responsible for media-related functions.
- Signaling Border Element (SBE)—Responsible for call signaling-related functions.

Note The existing Cisco SBC platforms support only DBE.

An SBC itself consists of the combined DBE and SBE functionality.

In addition, the SBC can operate in the following deployment models:

- Distributed Model (DM)—Contains only the SBE or DBE, resulting in a distributed SBC.
- Unified Model (UM)—Contains both the SBE and DBE, thereby implementing the SBE and DBE as a single device.

The following topics describe the SBC properties that are displayed in Prime Network Vision logical inventory:

- User Roles Required to View SBC Properties, page 19-2
- Viewing SBC Properties in Logical Inventory, page 19-3
- Viewing SBC DBE Properties, page 19-4
- Viewing SBC SBE Properties, page 19-6

User Roles Required to View SBC Properties

This topic identifies the GUI default permission or scope security level that is required to view SBC properties in Prime Network Vision. Prime Network determines whether you are authorized to perform a task as follows:

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

For more information on user authorization, see the *Cisco Prime Network 3.9 Administrator Guide*.

The following tables identify the tasks that you can perform:

- Table 19-1 identifies the tasks that you can perform if a selected element **is not in** one of your assigned scopes.
- Table 19-2 identifies the tasks that you can perform if a selected element **is in** one of your assigned scopes.

By default, users with the Administrator role have access to all managed elements. To change the Administrator user scope, see the topic on device scopes in the *Cisco Prime Network 3.9 Administrator Guide*.

Table 19-1 Default Permission/Security Level Required for Viewing SBC Properties - Element Not in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Viewing SBC properties	—	—	—	—	X

Table 19-2 Default Permission/Security Level Required for Viewing SBC Properties - Element in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Viewing SBC properties	X	X	X	X	X

Viewing SBC Properties in Logical Inventory

To view SBC properties in Prime Network Vision logical inventory, right-click the element configured for SBC, then choose **Inventory > Logical Inventory > Session Border Controller**.

The SBC properties are displayed as shown in Figure 19-1.

Figure 19-1 SBC Properties in Logical Inventory

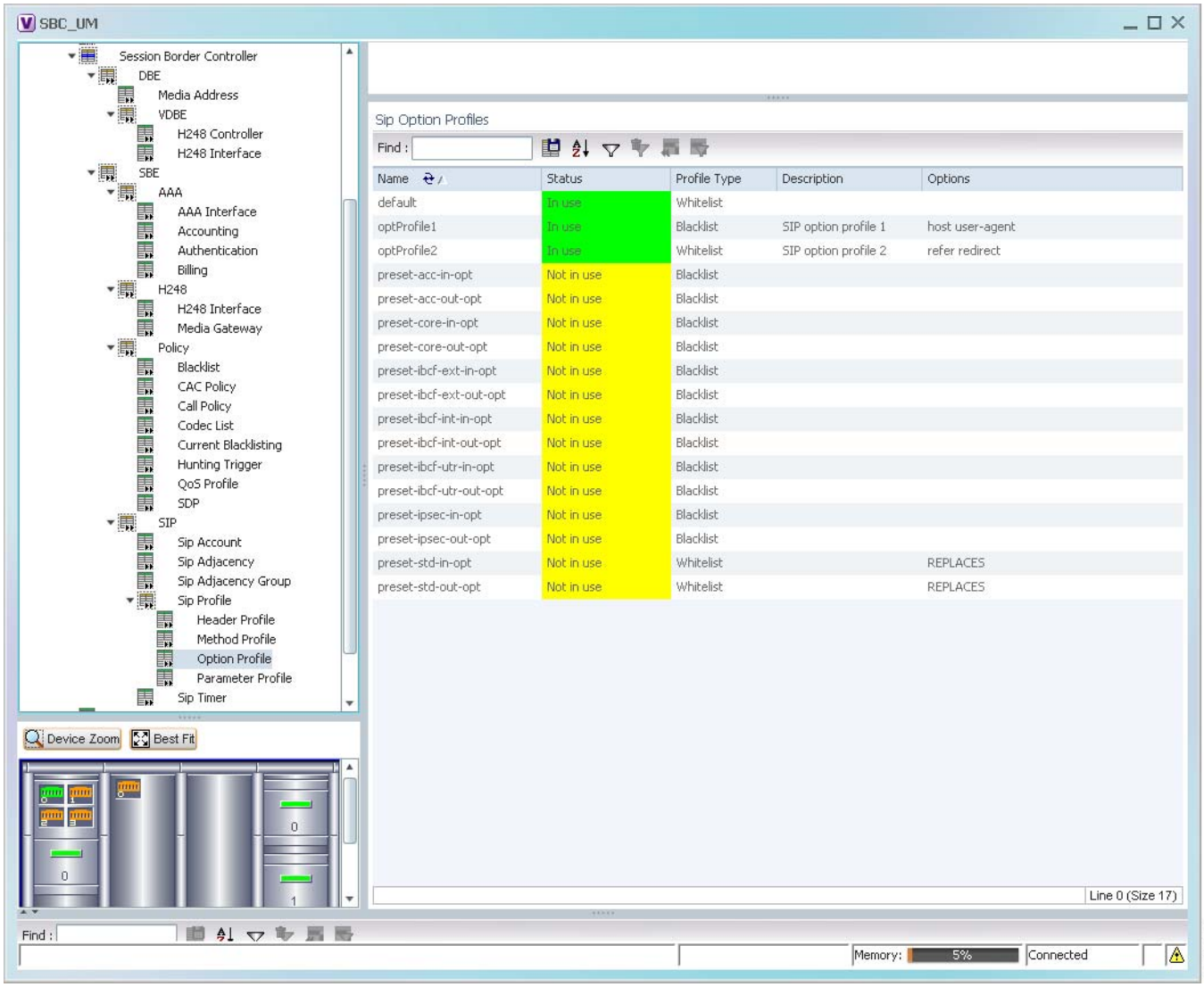


Table 19-3 describes the general SBC properties displayed in logical inventory.

Table 19-3 SBC Properties

Field	Description
Process	Process name, such as Session Border Controller.
Process Status	Status of the process, such as Running.
Application Version	SBC version number.
Mode	Mode in which the SBC is operating: • Unified • Distributed DBE
SBC Service Name	Name of the service.

Viewing SBC DBE Properties

The DBE controls media packet access to the network, provides differentiated services and QoS for different media streams, and prevents service theft.

To view SBC DBE properties, choose **Logical Inventory > Session Border Controller > DBE**.

Table 19-4 describes the DBE properties that appear in logical inventory.

Table 19-4 SBC DBE Properties

Field	Description
Process	Process name, such as DBE.
Process Status	Status of the process, such as Running.
Name	Name assigned to the DBE.
Type	Type of DBE, either DBE or virtual DBE (vDBE).
DBE Location Id	Unique identifier configured on each vDBE within a UM DBE.

Viewing Media Address Properties

A DBE uses a pool of sequential IPv4 media addresses as local media addresses.

To view SBC media address properties, choose **Logical Inventory > Session Border Controller > DBE > Media Address**.

Table 19-5 describes the SBC media address properties that are displayed in logical inventory.

Table 19-5 Media Address Properties

Field	Description
Address Range	IP addresses defined for the pool.
Port Range Lower	Lower end of the port range for the interface. If no range is specified, all possible Voice over IP (VoIP) port numbers are valid.
Port Range Upper	Upper end of the port range for the interface.
VRF Name	VRF that the interface is assigned to.
Service Class	Class of service (CoS) for each port range, such as fax, signaling, voice, or any.

Viewing VDBE H.248 Properties

To view VDBE H.248 properties, choose **Logical Inventory > Session Border Controller > DBE > VDBE**.

Table 19-6 describes the VDBE H.248 properties that are displayed in logical inventory.

Table 19-6 VDBE H.248 Properties

Branch	Description
H248 Controller	H.248 controller used by the DBE. The Media Gateway Configuration (MGC) table displays the following information: • Index—The number of the H.248 controller. The profile is used to interoperate with the SBE. • Remote IP—The remote IP address for the H.248 controller. • Remote Port—The remote port for the H.248 controller. • Transport—The transport for communications with the remote device.
H248 Interface	The SBC H248 Control Interface table displays the following information: • IP Address: – In DM mode, the local IP address of the DBE used to connect to the SBE. – In UM mode, the local IP address used to connect to the media gateway. • Port—The port for the H.248 controller interface. • Transport—The transport the H.248 controller interface uses. • Association—The relationship between the SBE and the media gateway.

Viewing SBC SBE Properties

The SBE controls the access of VoIP signaling messages to the network core and manipulates the contents of these messages. It does this by acting as a SIP B2BUA or H.323 gateway.

To view SBC SBE properties, choose **Logical Inventory > Session Border Controller > SBE**.

Table 19-7 describes the information displayed in logical inventory for an SBE.

Table 19-7 SBC SBE Properties

Field	Description
Process	Name of the process, such as SBE.
Process Status	Status of the process, such as Running or Idle.
Name	Name assigned to this SBE.
Call Redirect Limit	Maximum number of times a call is redirected before the call is declared failed. The range is 0 to 100 with a default of 2.
On Hold Timeout	Amount of time, in milliseconds, that the SBE waits after receiving a media timeout notification from the DBE for an on-hold call before tearing down the call.

Viewing AAA Properties

For devices that support local and remote billing, the SBC can send billing records to a AAA server using the RADIUS protocol.

To view AAA properties, choose **Logical Inventory > Session Border Controller > SBE > AAA**.

Table 19-8 describes the AAA properties that appear in logical inventory for the SBC SBE.

Table 19-8 AAA Properties

Branch	Description
AAA Interface	The SBE AAA Interface table displays the following information: • AAA Address—The local AAA interface address. • Network ID—A unique identifier for the SBE.
Accounting	The Accounting Radius Client table displays the following information: • Name—The name of the accounting client. • Client Type—The type of client, either Accounting or Authentication.

Table 19-8 AAA Properties (continued)

Branch	Description
Authentication	The Authentication Radius Client table displays the following information: • Name—The name of the authentication client. • Client Type—The type of client, either Accounting or Authentication.
Billing	The SBE Billing table displays the following information related to billing: • LDR Check Time—The time of day (local time) to run the long duration record check. • Local Billing Address—The local IP address for SBE billing. This IP address can be different from the local AAA IP address and is the IP address written in the bill records. • Admin Status—The configuration status, available with the **running-config** command. • Operational Status—The running status, available from the CLI. This entry indicates whether or not the billing interface is up. The status is derived from the interworking of the SBC and the AAA server.

Viewing H.248 Properties

The H.248 interface is used for signaling between an SBE and a DBE in distributed mode and between an SBE and a transcoding media gateway. The SBE or SBC acts as an H.248 MGC, and the transcoding device acts as an H.248 media gateway. The connection between the MGC and the media gateway is an H.248 link.

To view H.248 properties, choose **Logical Inventory > Session Border Controller > H248**.

Table 19-9 describes the H.248 properties that appear in logical inventory for the SBC SBE.

Table 19-9 H.248 Properties

Branch	Description
H248 Interface	The SBC H248 Control Interface table displays the following information: • IP Address: – In DM mode, the IP address used to connect the DBE and the MGC. – In UM mode, the IP address used to connect the SBC and the media gateway. • Port—The port for the H.248 controller interface. • Transport—The transport the H.248 controller interface uses. • Association—The relationship between the SBE and the media gateway.
Media Gateway	The Media Gateway table displays the following information: • IP Address—The IP address of the media gateway. • Codec List—A comma-separated list of the codecs supported.

Viewing Policy Properties

An SBC policy is a set of rules that define how the SBC treats different kinds of VoIP events. An SBC policy allows control of the VoIP signaling and media that pass through the SBC at an application level.

A *policy set* is a group of policies that can be active on the SBC at any one time. If a policy set is active, the SBC uses the rules defined within it to apply policy to events. Multiple policies can be set on a single SBC.

To view policy properties, choose **Logical Inventory > Session Border Controller > Policy**.

Table 19-10 describes the policy properties that appear in logical inventory for the SBC SBE.

Table 19-10 Policy Properties

Branch	Description
Blacklist	The Blacklists table contains the following information: • Name—The blacklist name. • Type—The type of source that this blacklist applies to, such as critical or normal.
CAC Policy	A Call Admission Control (CAC) policy is used to define admission control. The SBE CAC Policy Set table contains the following information: • Policy Set Number—An identifying number the SBE has assigned to the policy set. • First Table—A CAC policy table. • Status—Whether the policy is active or inactive. If the policy is active, the SBC applies the defined rules to events. • First CAC Scope—The scale that the CAC applies for, such as source adjacency or destination adjacency. This is the first CAC table used for CAC policy match. • Description—A brief description of the policy set.
Call Policy	A call policy set is used for number analysis and routing. The SBE Call Policy Set table contains the following information: • Policy Set Number—An identifying number the SBE has assigned to the policy set. • Status—Whether the policy is active or inactive. If the policy is active, the SBC applies the defined rules to events. • First Call Table—The first call table used for call policy match. • Description—A brief description of the policy set.
Codec List	The SBE Codec List table contains the following information: • Name—The name of the codec list. • Codecs—The codecs contained in each list.

Table 19-10 Policy Properties (continued)

Branch	Description
Current Blacklisting	The Current Blacklistings table contains the following information: • Type—The type of source this blacklist applies to. Blacklists are used to block certain VoIP services that meet specified conditions. • Event Type—The type of event this blacklist applies to, such as CORRUPT_MESSAGE. • Is All Source Addresses—Whether the blacklist applies to all source IP addresses: – True—Ignore any IP address in the Source Address field. – False—Use the IP address in the Source Address field. • Source Address—The IP address that this blacklist applies to. • Source Port Number—The port number that this blacklist applies to. • Source Port Type—The type of port this blacklist applies to. *All* is a valid entry. • Time Remaining—The amount of time, in hours, minutes, or seconds, before the blacklist is removed.
Hunting Trigger	The hunting trigger enables the SBC to search for other routes or destination adjacencies if an existing route fails. The Global Hunting Trigger List table contains the following information: • Hunting Mode—Indicates the protocol to use to search for routes, such as Session Initiation Protocol (SIP). • Hunting Triggers—The SIP responses, such as 468 or 503, that indicate the SBC is to search for an alternate route or destination adjacency. SIP responses are defined in RFC3261.

Table 19-10 Policy Properties (continued)

Branch	Description
QoS Profile	QoS profiles can be used by CAC policies and are used exclusively for marking IP packets. The QoS Profile table contains the following information: • Name—The name of the QoS profile. • Class of Service—The type of call this profile applies to, such as voice, video, signaling, or fax. • Marking Type—The type of marking to be applied to the IP packet. Options include Passthrough, Differentiated Service Code Point (DSCP), and IP Precedence/ToS. • IP Precedence—If the marking type is IP Precedence, the specified precedence, either 0 or 1. • ToS—If the marking type is ToS, the ToS value. • DSCP—If the marking type is DSCP, the DSCP value.
SDP	The Session Description Protocol (SDP) content pane contains the following tabs, each with their respective table: • SBE SDP Policy Table: – Instance Name—The name of the policy table. – SBE SDP Match Table—The name of the SDP match table. • SBE SDP Match Table: – Instance Name—The name of the SDP match table. – Match Strings—The match criteria. – Table Type—The type of table, either Blacklist or Whitelist.

Viewing SIP Properties

To view SIP properties, choose **Logical Inventory > Session Border Controller > SIP**.

Table 19-11 describes the SIP entries that appear in logical inventory for the SBC SBE.

Table 19-11 SIP Properties

Branch	Description
SIP Account	The SBE Account table contains the following information: • Name—The name of the account associated with the adjacencies. • Adjacencies—The identified adjacencies.
SIP Adjacency	An adjacency represents a signaling relationship with a remote call agent. One adjacency is defined per external call agent. Each adjacency belongs within an account. Each incoming call is matched to an adjacency, and each outgoing call is routed out over a second adjacency. The SBC SIP Adjacencies table contains the following information: • Name—The adjacency name. • Status—The status of the adjacency, either Attached or Detached. • Signaling Address—The local IP address and port (optional) for communications. • Signaling Peer—The remote IP address and port (optional) for communications. • Description—A brief description of the adjacency.
SIP Adjacency Group	The Adjacencies Groups table contains the following information: • Name—The name of the SIP adjacency group. • Adjacencies—The adjacencies that belong to the group.
SIP Profile	The SBC can be configured with whitelist and blacklists profiles on SIP messages. The following types of SIP profiles are available: • Header profile—A profile based on SIP header information. • Method profile—A profile based on SIP method strings. • Option profile—A profile based on SIP option strings. • Parameter profile—A profile based on SIP parameters.
SIP Profile > Header Profile	The SIP Header Profiles table contains the following information: • Name—The name of the SIP header profile. • Status—Whether or not the profile is in use. • Profile Type—The type of profile: – Whitelist—Accepts SIP requests that match the profile. – Blacklist—Rejects SIP requests that match the profile. • Description—A brief description of the profile.

Table 19-11 SIP Properties (continued)

Branch	Description
SIP Profile > Method Profile	The SIP Method Profiles table contains the following information: • Name—The name of the SIP method profile. • Status—Whether or not the profile is in use. • Profile Type—The type of profile: – Whitelist—Accepts SIP requests that match the profile. – Blacklist—Rejects SIP requests that match the profile. • Description—A brief description of the profile. • Is Passthrough—Whether or not passthrough is enabled: – True—Permits message bodies to be passed through for nonvital methods that match this profile. – False—Strips the message body out of any nonvital SIP messages that match this profile.
SIP Profile > Option Profile	The SIP Option Profiles table contains the following information: • Name—The name of the SIP option profile. • Status—Whether or not the profile is in use. • Profile Type—The type of profile: – Whitelist—Accepts SIP requests that match the profile. – Blacklist—Rejects SIP requests that match the profile. • Description—A brief description of the profile. • Options—The SIP option strings that define this profile, such as host user-agent, refer redirect, or replaces.

Table 19-11 SIP Properties (continued)

Branch	Description
SIP Profile > Parameter Profile	The SIP Parameter Profiles table contains the following information: • Name—The name of the SIP parameter profile. • Status—Whether or not the profile is in use. • Description—A brief description of the profile.
SIP Timer	The SBE SIP Timer table contains the following information: • TCP Connect Timeout—The time, in milliseconds, that the SBC waits for a SIP TCP connection to a remote peer to complete before failing that connection. The default is 1000 milliseconds. • TCP Idle Timeout—The minimum time, in milliseconds, that a TCP socket does not process any traffic before it closes the connection. The default is 120000 milliseconds (2 minutes). • TLS Idle Timeout—The minimum time, in milliseconds, that a Transport Layer Security (TLS) socket does not process traffic before it closes the connection. • Invite Timeout—The time, in seconds, that the SBC waits for a final response to an outbound SIP invite request. The default is 180 seconds. If no response is received during that time, an internal request timeout response is generated and returned to the caller. • UDP First Retransmit Interval—The time, in milliseconds, that the SBC waits for a UDP response or ACK before sending the first retransmission of a signal. The default value is 500 milliseconds. • UDP Max Retransmit Interval—The maximum time interval, in milliseconds, for an SBC to retransmit a signal. The maximum retransmission interval is 4000 milliseconds (4 seconds). • UDP Response Linger Period—The time, in milliseconds, for which the SBC retains negative UDP responses to invite requests. The default value is 32000 milliseconds (32 seconds).



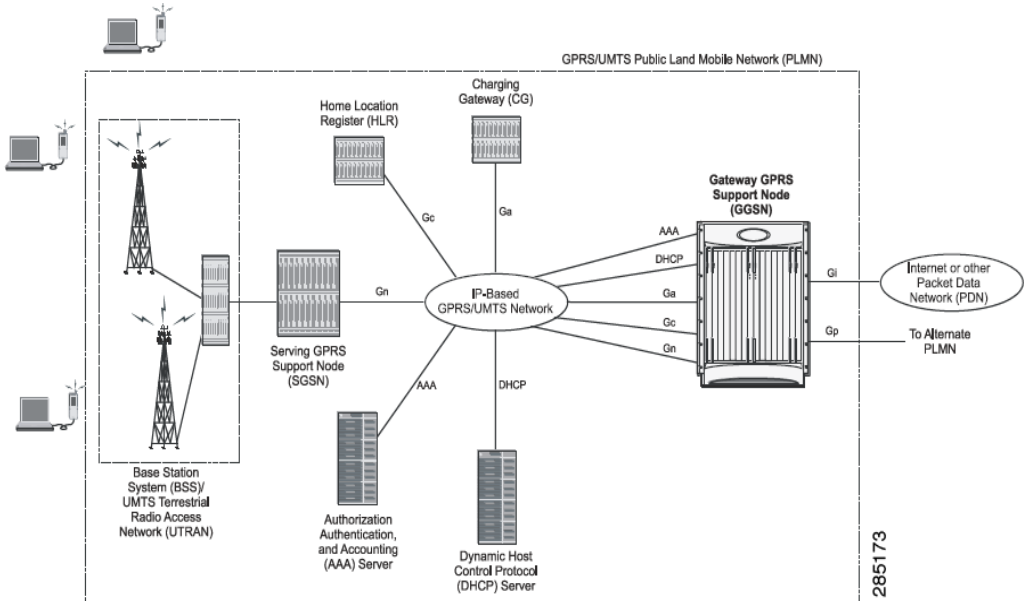
CHAPTER 20

Viewing Mobile Technologies in Prime Network

General Packet Radio Service (GPRS) and Universal Mobile Telecommunication System (UMTS) are evolutions of Global System for Mobile Communication (GSM) networks.

GPRS is a 2.5G mobile communications technology that enables mobile wireless service providers to offer their mobile subscribers packet-based data services over GSM networks. UMTS is a 3G mobile communications technology that provides wideband code division multiple access (CDMA) radio technology. Figure 20-1 shows a basic GPRS/UMTS network topology.

Figure 20-1 Basic GPRS/UMTS Network Topology



The GPRS/UMTS packet core comprises two major network elements:

- Gateway GPRS support node (GGSN)—A gateway that provides mobile cell phone users access to a Packet Data Network (PDN) or specified private Internet Protocol (IP) networks.
- Serving GPRS support node (SGSN)—Connects the radio access network (RAN) to the GPRS/UMTS core and tunnels user sessions to the GGSN. The SGSN sends data to and receives data from mobile stations, and maintains information about the location of a mobile station (MS). The SGSN communicates directly with the MS and the GGSN.

PDNs are associated with Access Point Names (APNs) configured on the system. Each APN consists of a set of parameters that dictate how subscriber authentication and IP address assignement is to be handled for that APN.

You can configure GGSN, associated GPRS Tunneling Protocol User Plane (GTPU), and APN with the required parameters using command-line interface (CLI). Prime Network Vision allows you to view the properties of GGSN, GTPU, and APN configured on the system.

From Prime Network 3.9, the mobile technologies are supported on Cisco Aggregation Service Router (ASR) 5000 series mobile gateways.

This chapter contains the following sections:

- User Roles Required to View GGSN, GTPU, and APN Parameters, page 20-2
- GGSN Overview, page 20-3
- Viewing GGSN Properties, page 20-4
- GTPU Overview, page 20-6
- Viewing GTPU Properties, page 20-6
- APN Overview, page 20-8
- Viewing APN Properties, page 20-9

User Roles Required to View GGSN, GTPU, and APN Parameters

This topic identifies the GUI default permission or scope security level that is required to view the GGSN and APN properties in Prime Network Vision. Prime Network determines whether you are authorized to perform a task as follows:

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

For more information on user authorization, see the *Cisco Prime Network 3.9 Administrator Guide*.

The following tables identify the tasks that you can perform:

- Table 20-1 identifies the tasks that you can perform if a selected element **is not in** one of your assigned scopes.
- Table 20-2 identifies the tasks that you can perform if a selected element **is in** one of your assigned scopes.

By default, users with the Administrator role have access to all managed elements. To change the Administrator user scope, see the topic on device scopes in the *Cisco Prime Network 3.9 Administrator Guide*.

Table 20-1 Default Permission/Security Level Required for Viewing GGSN, GTPU, and APN Properties - Element Not in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
GGSN					
Viewing GGSN properties	—	—	—	—	X

Table 20-1 Default Permission/Security Level Required for Viewing GGSN, GTPU, and APN Properties - Element Not in User's Scope (continued)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
GTPU					
Viewing GTPU properties	—	—	—	—	X
APN					
Viewing APN properties	—	—	—	—	X
Viewing additional APN characterisitcs	—	—	—	—	X

Table 20-2 Default Permission/Security Level Required for Viewing GGSN, GTPU, and APN Properties - Element in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
GGSN					
Viewing GGSN properties	X	X	X	X	X
GTPU					
Viewing GTPU properties	X	X	X	X	X
APN					
Viewing APN properties	X	X	X	X	X
Viewing additional APN characterisitcs	X	X	X	X	X

GGSN Overview

The GGSN works in conjunction with SGSNs within the network to perform the following functions:

- Establish and maintain subscriber Internet Protocol (IP) or Point-to-Point Protocol (PPP) type Packet Data Protocol (PDP) contexts originated by either the mobile or the network.
- Provide charging detail records (CDRs) to the charging gateway (CG, also known as the Charging Gateway Function (CGF)).
- Route data traffic between the subscriber's Mobile Station (MS) and a PDN such as the Internet or an intranet.

In addition, to providing basic GGSN functionality as described above, the system can be configured to support Mobile IP and/or Proxy Mobile IP data applications in order to provide mobility for subscriber IP PDP contexts. When supporting these services, the system can be configured to function as a GGSN and Foreign Agent (FA), a stand-alone Home Agent (HA), or a GGSN, FA, and HA simultaneously within the carrier's network.

Viewing GGSN Properties

Prime Network Vision displays the GGSNs in a GGSN container under the Mobile node in the logical inventory. The icon used for representing GGSNs in the logical inventory is explained in Logical Inventory Icons, page A-6.

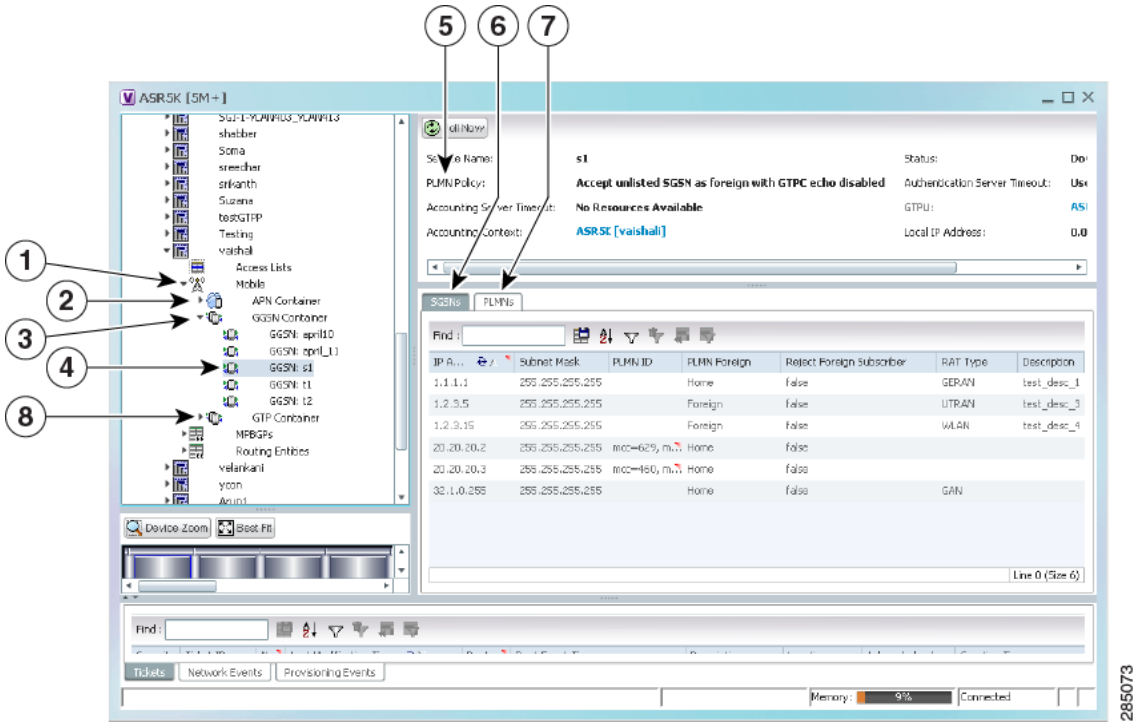
To view GGSN properties:

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

Step 2 In the logical inventory window, choose **Logical Inventory >** *Context* **> Mobile > GGSN Container**.

Prime Network Vision displays the list of GGSNs configured under the container as shown in Figure 20-2. You can view the individual GGSN details from the table on the right pane or by choosing **Logical Inventory >** *Context* **> Mobile > GGSN Container >** *GGSN*.

Figure 20-2 GGSN Properties in Logical Inventory



1	Mobile node	**5**	GGSN properties
2	APN container	**6**	Associated SGSNs
3	GGSN container	**7**	Associated PLMNs
4	GGSN	**8**	GTP container

Table 20-3 describes the details available for each GGSN.

Table 20-3 GGSN Properties in Logical Inventory

Field	Description
Service Name	The name of the GGSN service.
Status	The status of the GGSN service. Value could be Unknown, Running, or Down.
PLMN Policy	The PLMN policy for handling communications from SGSNs that are not configured to communicate with.
Newcall Policy	Specifies whether to accept or reject a new incoming call.
Authentication Server Timeout	The code used by the GGSN as a response message if communication with an authentication server times out. Value could be System Failure or User Authentication Failed.
Accounting Server Timeout	The code used by the GGSN as a response message if communication with an accounting server times out. Value could be System Failure or No Resouces.
GTPU	The GTPU that is associated with the GGSN and manages the GTP messages between GGSN and a radio access network equipment (RNC).
Accounting Context	The context that processes accounting for PDP contexts handled by the GGSN service.
Local IP Address	The local IP address bounded with the GGSN service.
GTPU	
Service Name	The name of the GTPU service.
State	The status of the GTPU service. Status could be Unknown, Running, or Down.
Max Retransmissions	The maximum limit for GTPU echo retransmissions. Default value is 4.
Retransmission Timeout	The timeout in seconds for GTPU echo retransmissions. Default value is 5 Secs.
Echo Interval	The rate at which the GTPU echo packets are sent.
IPSEC Tunnel Idle Timeout	The IPSec tunnel idle timeout after which IPSec tunnel deletion is triggered. Default value is 60 Secs.
Allow Error Indication	Specifies whether error indication is dropped or sent without IPSec tunnel. Default value is Disabled.
Include UDP Port Ext Hdr	Specifies whether to include an extension header in the GTPU packet for error indication messages. Default value is False.
IP Address	The list of IP addresses configured on the GTPU. The IP addresses are available only when configured for the GTPU.

If the GGSN is associated with SGSNs and Public Land Mobile Networks (PLMNs), you can view the details from the respective tabs for that GGSN as shown in Figure 20-2.

Table 20-4 describes the SGSN and PLMN information associated with the GGSN.

Table 20-4 SGSN and PLMN information for a GGSN

Field	Description
SGSNs	
IP Address	The IP address of the SGSN.
Subnet Mask	The subnet mask of the SGSN.
PLMN ID	The PLMN ID associated with the SGSN.
MCC	The mobile country code (MCC) portion of the PLMN.
MNC	The mobile network code (MNC) portion of the PLMN.
PLMN Foreign	Indicates whether the SGSN belongs to a home or foreign PLMN. This field is available only if MCC and MNC are not available.
Reject Foreign Subscriber	Specifies whether to accept or reject foreign subscriber. Value could be True or False.
RAT Type	The type of radio access technology (RAT) that is used for communication.
Description	The description of the SGSN entry in the GGSN service.
PLMNs	
PLMN ID	The ID of the PLMN associated with the GGSN.
Primary	Indicates whether the PLMN ID is the primary PLMN ID for the GGSN. Value could be True or False. When multiple PLMN IDs are configured, the one configured as primary is used for the Authentication, Authorization, and Accounting (AAA) attribute.

GTPU Overview

The GGSN communicates with SGSNs on a Public Land Mobile Network (PLMN) using the GPRS Tunneling Protocol (GTP). The signaling or control aspect of this protocol is referred to as the GTP Control Plane (GTPC) while the encapsulated user data traffic is referred to as the GTP User Plane (GTPU). GTPU is used for transferring user data in separated tunnels for each PDP context.

You can configure various parameters for a GTPU using the command-line interface. You can view the configured parameters for a GTPU in the logical inventory.

Viewing GTPU Properties

Prime Network Vision displays the GTPUs in a GTP container under the Mobile node in the logical inventory. The icon used for representing GTPUs in the logical inventory is explained in Logical Inventory Icons, page A-6.

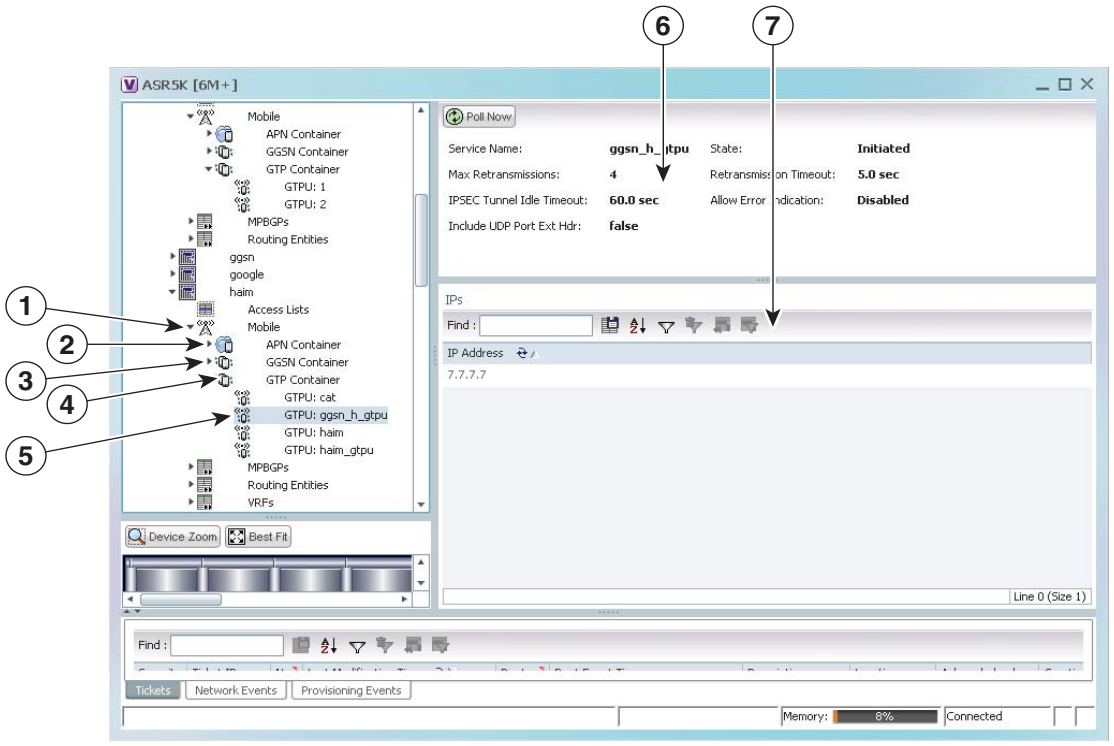
To view GTPU properties:

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

Step 2 In the logical inventory window, choose **Logical Inventory >** *Context* **> Mobile > GTP Container**.

Prime Network Vision displays the list of GTPUs configured under the container as shown in Figure 20-3. You can view the individual GTPU details from the table on the right pane or by choosing **Logical Inventory >***Context* **> Mobile > GTP Container >** *GTPU*.

Figure 20-3 GTPU Properties in Logical Inventory



1	Mobile node	**5**	GTPU
2	APN container	**6**	GTPU properties
3	GGSN container	**7**	IP addresses configured
4	GTP container		

Table 20-5 describes the details available for each GTPU.

Table 20-5 GTPU Properties in Logical Inventory

Field	Description
Service Name	The name of the GTPU service.
State	The status of the GTPU service. Status could be Unknown, Running, or Down.
Max Retransmissions	The maximum limit for GTPU echo retransmissions. Default value is 4.
Retransmission Timeout	The timeout in seconds for GTPU echo retransmissions. Default value is 5 Secs.
Echo Interval	The rate at which the GTPU echo packets are sent.
IPSEC Tunnel Idle Timeout	The IPSec tunnel idle timeout after which IPSec tunnel deletion is triggered. Default value is 60 Secs.
Allow Error Indication	Specifies whether error indication is dropped or sent without IPSec tunnel. Default value is Disabled.
Include UDP Port Ext Hdr	Specifies whether to include an extension header in the GTPU packet for error indication messages. Default value is False.
IP Address	The list of IP addresses configured on the GTPU. The IP addresses are available only when configured for the GTPU.

APN Overview

APN is the access point name that is configured in the GGSN configurations. The GGSN's APN support offers the following benefits:

- Extensive parameter configuration flexibility for the APN.
- Extensive QoS support.
- Virtual APNs to allow differentiated services within a single APN. The APN that is supplied by the SGSN is evaluated by the GGSN in conjunction with multiple configurable parameters. Then the GGSN selects an APN configuration based on the supplied APN and those configurable parameters.

Up to 1024 APNs can be configured in the GGSN. An APN may be configured for any type of PDP context, i.e., PPP, IPv4, IPv6 or both IPv4 and IPv6.

Many parameters can be configured independently for each APN by using the CLI. They are categorized as given below:

- Accounting—RADIUS, GTPP, or none. Server group to use. Charging characteristics. Interface with mediation servers.
- Authentication—Protocol, such as, Challenge Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), or none. Default username/password. Server group to use. Limit for number of PDP contexts.
- Enhanced Charging—Name of rulebase to use, which holds the enhanced charging configuration (e.g., eG-CDR variations, charging rules, prepaid/postpaid options, etc.).

- IP: Method for IP address allocation (e.g., local allocation by GGSN, Mobile IP, Dynamic Host Control Protocol (DHCP), DHCP relay, etc.). IP address ranges, with or without overlapping ranges across APNs.
- Tunneling: PPP may be tunneled with L2TP. IPv4 may be tunneled with GRE, IP-in-IP or L2TP. Load-balancing across multiple tunnels. IPv6 is tunneled in IPv4. Additional tunneling techniques, such as, IPsec and VLAN tagging may be selected by the APN, but are configured in the GGSN independently from the APN.
- QoS: IPv4 header ToS handling. Traffic rate limits for different 3GPP traffic classes. Mapping of R98 QoS attributes to work around particular handset defections. Dynamic QoS renegotiation (described elsewhere).

You can view the configured parameters for an APN in the logical inventory. After an APN is determined by the GGSN, the subscriber may be authenticated/authorized with an AAA server. The GGSN allows the AAA server to return VSAs (Vendor Specific Attributes) that override any or all of the APN configuration. This allows different subscriber tier profiles to be configured in the AAA server, and passed to the GGSN during subscriber authentication/authorization.

Viewing APN Properties

Prime Network Vision displays the APNs in an APN container under the Mobile node in the logical inventory. You can also view additional characteristics configured on the APN as explained in Viewing Additional Characteristics of an APN, page 20-12. The icon used for representing APNs in the logical inventory is explained in Logical Inventory Icons, page A-6.

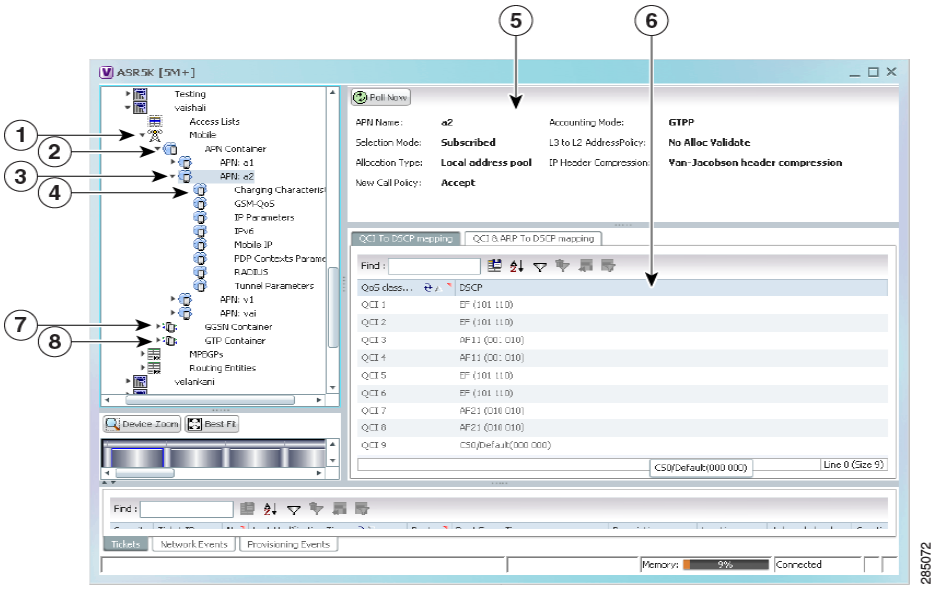
To view APN properties:

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

Step 2 In the logical inventory window, choose **Logical Inventory >***Context* **> Mobile > APN Container >***APN*.

The APN details are displayed as shown in Figure 20-4.

Figure 20-4 APN Properties in Logical Inventory



1	Mobile node	**5**	APN properties
2	APN container	**6**	APN additional properties
3	APN	**7**	GGSN container
4	Configured APN characteristics	**8**	GTP container

Table 20-6 describes the information that is available for the APN. The information that is displayed depends on the configuration of the APN.

Table 20-6 APN Properties in Logical Inventory

Field	Description
APN Name	The APN name.
Accounting Mode	The accounting protocol in use in the APN. Values are GTPP (GPRS Tunneling Protocol Prime), RADIUS (Remote Authentication Dial In User Service), or None.
Selection Mode	The selection mode in use in the APN. Selection mode indicates the origin of the requested APN and whether or not the Home Location Register (HLR) has verified the user subscription.
L3 to L2 Address Policy	The layer 2 to layer 3 IP address allocation or validation policy.
Allocation Type	The method by which the APN obtains IP addresses for PDP contexts.
IP Header Compression	IP packet header compression parameters for the APN.
New Call Policy	Specifies whether to accept or reject a new incoming call in case of duplicate session calls with a request for same IP address.

Step 3 To view additional details configured for the APN, use the following tabs:

- Virtual APNs—A virtual APN is a non-physical entity that represents an access point that does not itself provide direct access to a real target network. A virtual APN can be used to consolidate access to multiple, physical target networks through a single access point.
- QCI to DSCP Mapping—Shows the mapping between QoS Class Indices (QCI) to Differentiated Services Code Point (DSCP).
- QCI & ARP DSCP Mapping—Shows the mapping between QCI and Allocation/Retention Priority (ARP) to DSCP.

Field	Description
Virtual APNs	
Preference	Specifies the order in which the referenced APNs are compared by the system. Can be configured to any integer value from 1 (highest priority) to 1000 (lowest priority).
APN	Specifies the name of an alternative APN configured on the system that is to be used for PDP contexts with matching properties. Value can be from 1 to 62, alpha and/or numeric characters, and is not case-sensitive. It may also contain dots (.) and/or dashes (-).
Rule Definition	The virtual APN rule definition can be one of the following: • access-gw-address—Specifies the access gateway (SGSN/SGW/Others) address for the virtual APN. The IP address can be an IPv4 or IPv6 address in decimal notation. IPv6 also supports :: notation for the IP address. • bearer-access-service—Specifies the bearer access service name for the virtual APN. • service name—Specifies the service name. Service name is unique across all the contexts. Value is a string of size 1 to 63. • cc-profile—Specifies the APN for charging characteristics (CC) profile index. Value is an integer from 1 to 15. • Domain name—Specifies the subscriber's domain name (realm). Domain name can be from 1 to 79 alpha and/or numeric characters. • MCC—Specifies the MCC portion of the PLMN identifier. Value is an integer between 100 to 999. • MCN—Specifies the MNC portion of the PLMN identifier. Value is an integer between 00 to 999. • msisdn-range—Specifies the APN for this MSISDN range. The starting and ending values of the range is a string of size 2 to 15 with values between 00 and 999999999999999. • Rat-Typ—Specifies the rat-type option, which could be gan, geran, hspa, utran, or wlan. • Roaming mode—Specifies the roaming mode, which could be Home, Visiting, or Roaming.

Field	Description
QCI to DSCP Mapping	
QoS class index	Denotes a set of transport characteristics used to differentiate various packet flows.
DSCP	Denotes a mechanism for classifying and managing network traffic and providing QoS.
QCI & ARP DSCP Mapping	
QoS class index	Denotes a set of transport characteristics used to differentiate various packet flows.
Allocation retention priority	Indicates the priority of allocation and retention of the service data flow. This parameter allows prioritizing allocation of resources during bearer establishment and modification. During network traffic congestions, a lower ARP flow is dropped to free up the capacity.
DSCP	Denotes a mechanism for classifying and managing network traffic and providing QoS.

Viewing Additional Characteristics of an APN

To view additional characteristics of an APN:

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

Step 2 In the logical inventory window, choose **Logical Inventory > Mobile > APN Container >***APN*.

Step 3 Expand the *APN* node. The following list of characteristics configured for the APN are displayed:

- Charging Characteristics—Charging characteristics configured on the APN for different subscribers.
- GSM-QoS—Represents the negotiated QoS attribute reliability class based on the configuration provided for service data unit (SDU) error ratio and residual bit error rate (BER) attributes in the APN.
- IP Parameters—Represents the APN parameters related to IP.
- IPv6—Represents IPv6 configurations and related services for the APN.
- Mobile IP—Represents mobile IP configuration of the APN.
- PDP Contexts Parameters—Represents the PDP contexts supported by the APN.
- RADIUS—Represents the APN parameters related to communication with the RADIUS server.
- Tunnel Parameters—Represents the parameters configured for tunneling between the GGSN and an external gateway for the APN.
- DNS Configuration—Represents the Domain Name System (DNS) settings configured on the APN.

Step 4 Click each of one of these characteristics to view its properties on the right pane. See Table 20-7 for more details on the properties of each characteristics configured for the APN.

Table 20-7 APN Characteristics

Field	Description
Charging Characteristics	
Home Bit Behavior	The behavior bit for charging a home subscriber.
Home Profile	The profile index for a home subscriber.
Roaming Bit Behavior	The behavior bit for charging a roaming subscriber.
Roaming Profile	The profile index for a roaming subscriber.
Visiting Bit Behavior	The behavior bit for charging a visiting subscriber.
Visting Profile	The profile index for a visiting subscriber.
All Bit Behavior	The behavior bit for charging all subscribers. This value is used only if all subscribers are configured to use the same charging characteristics. This value is overridden by the behavior bit set for a subscriber type.
All Profile	The profile index for all subscribers.
Use GGSN	The type of the subscriber using the charging characteristics configured on the APN. Value could be Home, Roaming, Visitor, or None. None indicates that the subscriber is using the charging characteristics from the SGSN.
Use RADIUS Returned	Specifies whether the GGSN accepts charging characteristics returned from the RADIUS server for all subscribers for the APN. Value could be True or False.
GSM-QoS	
SDU Error Ratio Code	The SDU error ratio code based on which the negotiation of QoS attribute reliability class needs to be configured on the APN. Value is an integer between the range 1 and 7. Each code has an assigned value.
Residual BER Code	The residual bit error rate (BER) based on which the negotiation of QoS attribute reliability class needs to be configured on the APN. This value is specified if the SDU error ratio code is 1, 2, 3, or 7. Residual BER code is an integer in the range 1 and 9. Each code has an assigned value.
IP Parameters	
In Access Group	The name of the IPv4/IPv6 access group for the APN when configured for inbound traffic.
Out Access Group	The name of the IPv4/IPv6 access group for the APN when configured for outbound traffic.
Local Address	The static local IP address assigned to the APN.
Next Hop Gateway Address	The IP address of the next hop gateway for the APN. This parameter is available only if it is configured on the APN.
Is Discard Enabled	Specifies whether multicast discard is enabled or disabled. Value could be True or False.

Table 20-7 APN Characteristics (continued)

Field	Description
IPv6	
Inbound Access Group Name	The name of the IPv6 access group for the APN when configured for inbound traffic.
Outbund Access Group Name	The name of the IPv6 access group for the APN when configured for outbound traffic.
Router Advertisement Interval	The time interval (in milliseconds) the intial IPv6 router advertisement is sent to the mobile node. Value is an integer in the range 100 and 16,000. Smaller the advertisement interval greater is the chance of the router being discovered quickly.
Router Advertisement Number	The number of initial IPv6 router advertisements sent to the mobile node. Value is an integer in the range of 1 and 16.
Prefix Pool Name	The name of the IPv6 address prefix pool configured for the subscriber. You can configure upto a maximum of four pools per subscriber.
Egress Address Filtering	Specifies whether filtering of packets not meant for the mobile interface, is enabled or disabled.
Mobile IP	
Home Agent	The IP address of the home agent (HA) used by the current APN to facilitate subscriber mobile IP sessions.
Mobile Node Home Agent SPI	The mobile node Security Parameter Index (SPI) configured for the APN. Value is an integer between 256 and 4294967295.
Mobile Node Home Agent Hash Algorithm	The encryption algorithm used (if any) by the APN for security.
Mobile Node AAA Removal Indication	Specifies whether the system is configured to remove various information elements when relaying registration request (RRQ) messages to HA. Value could be Enabled or Disabled.
PDP Contexts Parameters	
Total Contexts	The total number of primary and secondary PDP contexts that can be supported by the APN. Value is an integer between 1 and 4,000,000.
PDP Type	The type of the PDP contexts supported by the APN.
Primary Contexts	The status of the primary contexts of the APN.
RADIUS	
RADIUS Group	The Authentication, Authorization, and Accounting (AAA) group name for the subscriber. If no group is set, the value is displayed as Default.
RADIUS Secondary Group	The secondary AAA group for the APN. If no group is set, the value is displayed as None.
Returned Framed IP Address Policy	The policy which indicates whether to accept or reject a call when the RADIUS server supplies 255.255.255.255 as the framed IP address and when the MS does not supply an IP address.
Tunnel Parameters	
Address Policy	The address allocation / validation policy for all tunneled calls except Layer 2 Tunneling Protocol (L2TP) calls.

Table 20-7 APN Characteristics (continued)

Field	Description
Peer Load Balancing	The algorithm that defines how the tunnel peers are selected by the APN when multiple peers are configured in the APN.
DNS Configuration	
Primary DNS Address	The primary DNS server for the APN.
Secondary DNS Address	The secondary DNS server for the APN.



APPENDIX A

Icon and Button Reference

The following topics identify the buttons, icons, and badges used in Cisco Prime Network Vision (Prime Network Vision) and Cisco Prime Network Events (Prime Network Events):

- Icons, page A-1
- Links, page A-8
- Severity Icons, page A-11
- Buttons, page A-12
- Badges, page A-17

Icons

The following topics describe the icons used in Prime Network Vision:

- Network Element Icons, page A-2
- Business Element Icons, page A-4
- Logical Inventory Icons, page A-6
- Physical Inventory Icons, page A-8

Network Element Icons

Table A-1 Prime Network Vision Network Element Icons

Icon	Network Element
	Access pseudowire Router
	ATM switch
	Basic rate access (BRA)
	Cisco 7600 series router
	Cisco ASR 1000 series router
	Cisco ASR 5000 series router
	Cisco ASR 9000 series router
	Cisco CRS series router
	Cisco IOS XR 12000 series router
	Cisco MWR 3941
	Cisco Nexus 1000 series
	Cisco Unified Computing System (UCS) 6100 series
	Cloud
	Digital subscriber line access multiplexer (DSLAM)

Table A-1 Prime Network Vision Network Element Icons (continued)

Icon	Network Element
	Ethernet switch
	Generic SNMP device
	Ghost, or unknown device
	ICMP device
	Lock, or security violation; viewable by a user with a higher permission level
	Missing icon, displayed in either of the following situations: • A device has been deleted via Prime Network Administration, but remains in the map. • A unique icon for an element (physical or logical) does not exist.
	Sun Netra server
	PC
	Printer
	Service control switch
	WiFi element

Business Element Icons

Table A-2 Prime Network Vision Business Element Icons

Icon	Business Element
	Aggregation or root node
	Backup pseudowire edge
	Business IP interface
	Connection termination point (TP) Ethernet flow point (EFP) MToP service
	Customer
	EFP cross-connect
	Ethernet service
	Ethernet virtual connection (EVC)
	Label-Switched Path (LSP) end point
	LSP mid point
	Network LSP
	Network pseudowire
	Network TP tunnel

Table A-2 Prime Network Vision Business Element Icons (continued)

Icon	Business Element
	Network VLAN
	Protected LSP
	Pseudowire edge
	Pseudowire switching entity
	Site
	Subnet
	Switching entity
	TP tunnel end point
	Virtual router
	VPLS forward
	VPLS instance
	VPN
	Working LSP

Logical Inventory Icons

Table A-3 describes the icons used in logical inventory.

Table A-3 Logical Inventory Icons

Icon	Logical Inventory Item	
	Access Lists	Link Layer Discovery Protocol (LLDP)
	ATM Traffic Profiles	Modular OS
	Bidirectional Forwarding Detection (BFD)	Operating System
	Cisco Discovery Protocol (CDP)	Operations, Administration, and Maintenance (OAM)
	Clock	Resilient Ethernet Protocol (REP)
	Ethernet LMI	Session Border Controller
	Frame Relay Traffic Profiles	Spanning Tree Protocol
	IP SLA	Tunnel Traffic Descriptors
	Access Gateway	MPBGPs
	ARP Entity	Multiple Spanning Tree protocol (MST) instance
	Bridges	OSPF Processes
	Ethernet Link Aggregation	Pseudowires
	GRE Tunnels	Routing Entities
	ICCP Redundancy container	Traffic Engineering Tunnels
	IMA Groups	VC Switching Entities
	Local Switching	VRFs
	LSEs	VSIs
	MLPPP	
	Bridge	
	Connectivity Fault Management (CFM) Maintenance Association	
	CFM Maintenance Domain	

Table A-3 Logical Inventory Icons (continued)

Icon	Logical Inventory Item
	Connectivity Fault Management
	Context, for devices that support multiple virtual contexts
	Cross-VRF
	Encapsulation
	ICCP Redundancy group
	Inverse Multiplexing over ATM (IMA) group
	Label switching
	Layer 2 Tunnel Protocol (TP) peer
	Logical inventory
	Virtual Switch Interface (VSI)
	VLAN Trunk Protocol (VTP)
	Mobile node
	Gateway GPRS Support Node (GGSN) container
	GGSN
	GPRS Tunneling Protocol user plane (GTPU)

Table A-3 Logical Inventory Icons (continued)

Icon	Logical Inventory Item
	Access Point Name (APN) container
	APN

Physical Inventory Icons

Table A-4 describes the icons used in physical inventory.

Table A-4 Physical Inventory Icons

Icon	Device
	Chassis
	Shelf
	Slot/Subslot
	Port/Logical Port
	Unmanaged Port

Links

The following sections describe link icons and characteristics:

- Link Icons, page A-9
- Link Colors, page A-10
- Link Characteristics, page A-10

Link Icons

Table A-5 identifies the available link types and their representation in Prime Network Vision.

Table A-5 Prime Network Vision Link Icons

Icon	Description	Icon	Description
	Asynchronous Transfer Mode		Unknown
	Bidirectional Forwarding Detection		Physical layer
	Border Gateway Protocol		Private Network-to-Network Interface
	Business link		Point-to-Point Protocol
	Ethernet		Pseudowire
	Frame Relay		Serial
	Generic Routing Encapsulation		MPLS TE Tunnel
	Internal		MPLS TP Tunnel
	IP		VLAN
	Link aggregation group		IPv6 VPN over IPv4-MPLS
	Multilink Point-to-Point Protocol		VPN
	MPLS		

Link Colors

Table A-6 Link Colors and Severity

Color	Severity	Description
	Critical	Critical alarm is on the link.
	Major	Major alarm is on the link.
	Minor	Minor alarm is on the link.
	Normal	Link is operating normally.
	Selected	Link is selected.

Link Characteristics

Table A-7 Link Characteristics

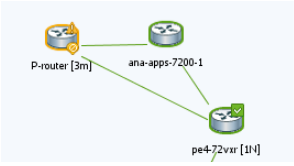
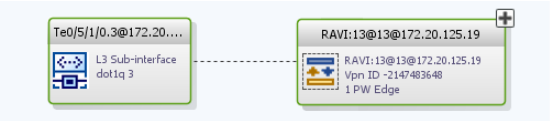
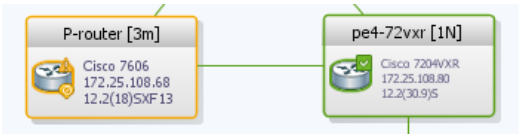
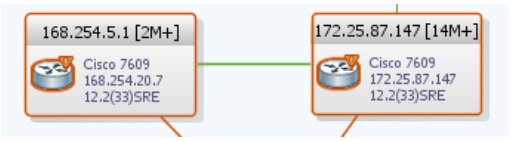
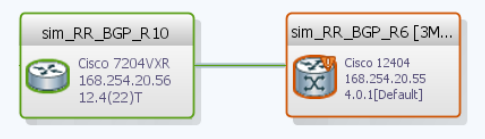
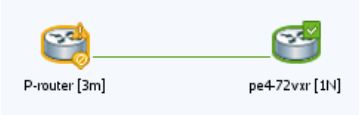
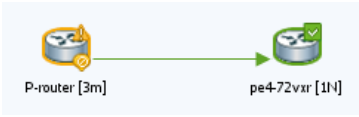
Example	Description
Solid Line vs. Dashed Line	
	Solid line—Physical, topological, or service link, such as a link between two devices.
	Dashed line—Association or *business link* between such elements as EVCs, VPLS service instances, or VPN components.
Link Widths	
	Normal—Contains links of the same group. Available groups are: • Business • GRE • MPLS-TP • Pseudowire • VLAN • All others
	Wide—Aggregated links that contain links of different groups. When viewing a map at a low zoom level, aggregated links cannot be distinguished in the GUI.

Table A-7 Link Characteristics (continued)

Example	Description
	Tunnel—The center color represents the severity of any alarms on the link.
Arrowhead vs. No Arrowhead	
	No arrowhead—Bidirectional link.
	Arrowhead Unidirectional link, with the flow in the direction of the arrowhead.

Severity Icons

Table A-8 identifies the severity icons used in Prime Network Events and Prime Network Vision.

The icons and colors are used as follows:

- The icons are used to indicate the severity of alarms in Prime Network Events and tickets in the Prime Network Vision ticket pane.
- The icons are used as badges in Prime Network Vision maps to indicate the highest severity alarm that is not acknowledged for the associated network element.
- The colors are used with network elements in Prime Network Vision to indicate the severity of the highest uncleared ticket on the element.
- The colors are used with links in Prime Network Vision to indicate the severity of the alarm on the link. For more information, see Link Colors, page A-10.

Table A-8 Severity Indicators

Icon	Color	Severity
	Red	Critical
	Orange	Major
	Yellow	Minor
	Light Blue	Warning

Table A-8 Severity Indicators (continued)

Icon	Color	Severity
	Green	Cleared, Normal, or OK
	Medium Blue	Information
	Dark Blue	Indeterminate

Buttons

The following topics describe the buttons used in Prime Network Vision:

- Prime Network Vision Buttons, page A-12
- Table Buttons, page A-15
- Link Filtering Buttons, page A-15
- Prime Network Events Buttons, page A-16
- Ticket Properties Buttons, page A-16
- Report Manager Buttons, page A-17

Prime Network Vision Buttons

Table A-9 Prime Network Vision Buttons

Button	Function
Map Options	
	Creates a new map in the database.
	Opens a map saved in the database using the Open dialog box.
	Adds a network element to the map or to the subnetwork selected in the navigation pane and displayed in the content pane.
	Saves the current map (the background and the location of devices) to the database.
Viewing Options	

Table A-9 Prime Network Vision Buttons (continued)

Button	Function
	Displays the map view in the Prime Network Vision content pane (the button toggles when selected or deselected).
	Displays the list view in the Prime Network Vision content pane (the button toggles when selected or deselected).
	Displays the links view in the Prime Network Vision content pane (the button toggles when selected or deselected).
Overlay Tools	
	Chooses and displays an overlay of a specific type on top of the elements displayed in the content pane in the map view. When an overlay is selected, all the elements and links that are part of the overlay are colored, and those that are not part of the overlay are dimmed.
	Displays or hides a previously defined overlay of a specific type on top of the elements displayed in the content pane in map view.
	Refreshes the overlay.
Navigation Tools	
	Moves up a level in the navigation pane and map pane to enable you to view different information.
	Opens the Link Filter dialog box, enabling you to display or hide different types of links in the map and links views. If a link filter is applied to the map, the Link Filter Applied button is displayed instead.
	Indicates a link filter is currently applied to the map and opens the Link Filter dialog box so you can remove or modify the existing link filter. If no link filter is applied to the map, the Link Filter button is displayed instead.
	Opens a window displaying an overview of the network.
Search Tools	
	Finds the previous instance of the search string entered in the Find in Map dialog box.
	Opens the Find in Map dialog box, enabling you to find a device or aggregation in the map by its name or IP address.
	Finds the next instance of the search string entered in the Find in Map dialog box.

Table A-9 Prime Network Vision Buttons (continued)

Button	Function
	Opens the Find Business Tag dialog box, enabling you to find and detach a business tag according to a name, key, or type.
Map Zoom and Layout Tools	
	Defines the way in which the NES are arranged in the Prime Network Vision map view: circular, hierarchical, orthogonal, or symmetric.
	Fits the entire subnetwork or map in the map pane.
	Activates the normal selection mode.
	Activates the zoom selection mode, which enables you to select an area in the map pane to zoom in on by clicking and dragging.
	Activates the pan mode, which enables you to move around in the map pane by clicking and dragging.
	Opens the Activation dialog box.
	Opens the Activation List dialog box.
Print Preview Options	
	Opens the Printer Setup dialog box so you can specify your print settings.
	Opens the Print dialog box so you can print the displayed network or map to the required printer.
	Zooms in on the network or map.
	Zooms out of the network or map.
	Displays the entire network or map in the Print Preview window.

Table Buttons

Table A-10 Table Buttons

Icon	Name	Description
	Find	Searches the current table for the string you enter.
	Export to CSV	Exports the information displayed in the list view. Either the selected rows are exported, or, when nothing is selected, the entire table is exported.
	Sort Table Values	Sorts the information displayed in the list view (for example, according to *element category*).
	Filter	Filters the information displayed in the table by the criteria you specify.
	Clear Filter	Clears the existing filter.
	Show All Rows	Displays all table rows that meet the current filtering criteria.
	Show Only Selected Rows	Displays only the rows that you select.

Link Filtering Buttons

Table A-11 Link Filtering Buttons

Button	Name	Description
	All Links	Displays the complete list of links for the selected context (map or aggregation). In other words, the list is not filtered and all the links are displayed, including external links.
	External Links	Displays links with only one side of the link in this context (map or aggregation) and the other side either not in the map or outside the selected context.
	Flat Links	Displays the links currently visible on the map for the selected context (map or aggregation), excluding any thumbnails.
	Deep Links	Displays the links for the current aggregation where both endpoints are within the currently selected context.

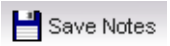
Prime Network Events Buttons

Table A-12 Prime Network Events Buttons

Button	Function
	Displays the previous page of events in the Prime Network Events window.
	Displays the next page of events in the Prime Network Events window.
	Refreshes the events displayed in the log by querying the database. If a filter is active, the refresh is done according to the filter. The log returns to the beginning of the list, displaying the events in ascending or descending order depending on the order of the current list. Descending order means that the last event is displayed first.
	Displays the Prime Network Events Filter dialog box, which enables you to define a filter for the events displayed in the Prime Network Events log.
	Toggles automatic refresh of event data on and off. You define the refresh-time period (in seconds) in the Prime Network Events Options dialog box. The default is 60 seconds. If a filter is active, the refresh is done according to the filter.
	Displays the properties of the selected event or ticket in the Properties pane.

Ticket Properties Buttons

Table A-13 Ticket Properties Window Buttons

Icon	Description
	Refreshes the information displayed in the Ticket Properties dialog box.
	Acknowledges that the ticket is being handled. The status of the ticket is displayed as true in the ticket pane and in the Ticket Properties dialog box. If a ticket was acknowledged, and some events were correlated to it afterward, then the ticket is considered to have not been acknowledged. This button is enabled only if the ticket is not acknowledged.
	Requests the relevant Prime Network system to remove the faulty network element from the Prime Network Vision networking inventory. In addition, it sets the ticket to Cleared severity or status (the icon is displayed in green) and automatically changes the acknowledged status of the ticket to true. This button is enabled only if the severity of the alarm is higher than Cleared or Normal.
	Saves the notes for the selected ticket. This button is enabled only when text is entered in the Notes field of the Notes tab.

Report Manager Buttons

Table A-14 Report Manager Buttons

Icon	Name	Description
	Define Report of This Type	Enables you to define a report of this type that is suited specifically to your environment.
	Delete	Deletes one or more folders that you created.
	Delete Report	Deletes the selected report.
	Move	Moves one or more folders or reports that you created.
	New Folder	Creates a new folder
	Rename	Renames a folder that you created.
	Run	Generates the selected report
	View	Displays the selected report in HTML format.

Badges

Badges are small icons that appear with other network elements, such as element icons or links.

The following topics describe the badges used by Prime Network Vision and Prime Network Events:

- VNE Communication State Badges, page A-18
- VNE Investigation State Badges, page A-18
- Network Element Technology-Related Badges, page A-20

VNE Communication State Badges

Table A-15 VNE Communication State Badges

Badge	State Name	Description
None	Agent Not Loaded	The VNE is not responding to the gateway because it was stopped, or it was just created. This communication state is the equivalent of the Defined Not Started investigation state.
	VNE/Agent Unreachable	The VNE is not responding to the gateway. This can happen if the unit or AVM is overutilized, the connection between the gateway and unit or AVM was lost, or the VNE is not responding in a timely fashion. (A VNE in this state does not mean the device is down; it might still be processing network traffic.)
None	Connecting	The VNE is starting and the initial connection has not yet been made to the device. This is a momentary state. Because the investigation state decorator (the hourglass) will already be displayed, a special GUI decorator is not required.
	Device Partially Reachable	The element is not fully reachable because at least one protocol is not operational.
	Device Unreachable	The connection between the VNE and the device id down because all of the protocols are down (though the device might be sending traps or syslogs).
None	Tracking Disabled	The reachability detection process is not enabled for any of the protocols used by the VNE. The VNE will not perform reachability tests nor will Prime Network generate reachability-related events. In some cases this is desirable; for example, tracking for Cloud VNEs should be disabled because Cloud VNEs represent unmanaged network segments.

VNE Investigation State Badges

Table A-16 VNE Investigation State Badges

Badge	State Name	Description
None	Defined Not Started	A new VNE was created (and is starting); or an existing VNE was stopped. In this state, the VNE is managed and is validating support for the device type. (This investigation state is the equivalent of the Agent Not Loaded communication state.) A VNE remains in this state until it is started (or restarted) by a user.
	Unsupported	The device type is either not supported by Prime Network or is misconfigured (it is using the wrong scheme, or is using reduced polling but the device does not support it). To extend Prime Network functionality so that it recognizes unsupported devices, use the VNE Customization Builder. See the *Cisco Prime Network 3.9 Customization User Guide*.
	Discovering	The VNE is building the model of the device (the device type was found and is supported by Prime Network). A VNE remains in this state until all device commands are successfully executed at least once, or until there is a discovery timeout.

Table A-16 VNE Investigation State Badges (continued)

Badge	State Name	Description
None	Operational	The VNE has a stable model of the device. Modeling may not be fully complete, but there is enough information to monitor the device and make its data available to other applications, such as activation scripts. A VNE remains in this state unless it is stopped or moved to the maintenance state, or there are device errors.
	Currently Unsynchronized	The VNE model is inconsistent with the device. This can be due to a variety of reasons; for a list of these reasons along with troubleshooting tips, see the topic on troubleshooting VNE investigation state issues in the *Cisco Prime Network 3.9 Administrator Guide*.
	Maintenance	VNE polling was suspended because it was manually moved to this state (by right-clicking the VNE and choosing **Actions > Maintenance**). The VNE remains in this state until it is manually restarted. A VNE in the maintenance state has the following characteristics: • Does not poll the device, but handles syslogs and traps. • Maintains the status of any existing links. • Does not fail on VNE reachability requests. • Handles events for correlation flow issues. It does not initiate new service alarms, but does receive events from adjacent VNEs, such as in the case of a Link Down alarm. The VNE is moved to the Stopped state if: it is VNE is moved, the parent AVM is moved or restarted, the parent unit switches to a standby unit, or the gateway is restarted.
	Partially Discovered	The VNE model is inconsistent with the device because a required device command failed, even after repeated retries. A common cause of this state is that the device contains an unsupported module. To extend Prime Network functionality so that it recognizes unsupported modules, use the VNE Customization Builder. See the *Cisco Prime Network 3.9 Customization User Guide*.
	Shutting Down	The VNE has been stopped or deleted by the user, and the VNE is terminating its connection to the device.
None	Stopped	The VNE process has terminated; it will immediately move to Defined Not Started.

Network Element Technology-Related Badges

Table A-17 Network Element Technology-Related Badges

Icon	Description
	Access gateway
	Blocking
	Clock service
	Associated LSP is in lockout state
	Multiple links
	Reconciliation
	REP blocking primary
	REP primary
	Redundancy service
	STP root

Alarm and Ticket Badges

See Severity Icons, page A-11 for information about the icons used for alarm and ticket badges.



INDEX

Numerics

3.6.x tabs, in Prime Network Events 8-12
6rd tunnels, viewing properties 17-43
6VPE
  and IPv6 16-1
  IPv6 VPN over MPLS 16-1

A

access gateway
  badge 3-8, A-20
  viewing properties 12-18
accumulating affected parties
  in an alarm 9-23
  in the correlation tree 9-23
acknowledged tickets 9-7
acknowledging tickets 9-19
activation script, launching 2-40, 2-44, 4-1
adding
  associated VLANs 12-52
  EFP cross-connects 12-73
  Ethernet services 12-102
  MPLS-TP tunnels 17-5
  network elements 4-9
  pseudowires 12-88
  unassociated bridges 12-70
  VLANs 12-48
  VPLS instances 12-76
  VPNs
    existing 17-22
    new 17-21
Advanced tab
  events 8-17
  tickets 9-18
affected elements, finding 9-19
Affected Elements window 4-28
affected parties 9-22
  accumulating 9-23
  Affected Parties tab (tickets) 9-14
  calculating 9-23
  finding 9-19
affected severity, updating over time 9-24
Agent Not Loaded, VNE communication state 2-27
Agent Unreachable, VNE communication state 2-27
aggregation, definition 1-1
aggregations
  adding elements to 4-30
  aggregating network elements 4-28
  disaggregating 4-33
  renaming 4-32
  using Chinese characters 4-5
  viewing thumbnails 4-30
  working with thumbnail views 4-32
alarm count, definition 9-6
alarms
  badges A-20
  customizing 2-47
  definition 1-1
  disabling on a port 3-26
  enabling on a port 3-26
  severities 9-22
All tab, in Prime Network Events 8-3
APN
  additional characteristics 20-12
  overview 20-8

roles required for viewing properties 20-2
view properties 20-9
application, launching external 2-40, 2-44, 4-1
applying overlays
Ethernet service 12-104
MPLS-TP tunnels 17-16
network clock 18-48
pseudowire 12-100
VLAN 12-58
VPLS instance 12-77
VPN 17-24
ARP table 17-33
associated VLANs
adding 12-52
tag manipulations 12-52
viewing
mapping properties 12-54
service links 12-54
working with 12-52
association, definition 1-2
ATM cross-connects
in logical and physical inventory 18-6
overview 18-6
properties 18-7
viewing 18-6
audience, intended xvii
audio options, customizing 2-47
Audit tab
events 8-17
in Prime Network Events 8-3
auto refresh, in Prime Network Events 8-21

B

background images for maps 4-17
badges
access gateway 3-8, A-20
alarms 2-25, A-20
blocking 3-8, A-20
clock service 3-8, A-20
for elements and links 3-8
icons A-17
lock 3-8, 17-6, A-20
management states A-17
multiple links 3-8, A-20
reconciliation 3-9, 6-8, 12-47, A-20
redundancy service 3-9, A-20
REP primary 3-9, A-20
REP primary blocking 3-9, A-20
STP root 3-9, A-20
technology related A-20
tickets A-20
VNE communication states A-18
VNE investigation states A-18
VNE management states 2-25
BFD
viewing BFD session properties 17-44
viewing MPLS-TP BFD session properties 17-46
BGP, viewing inventory details 17-42
Bidirectional Forwarding Detection. See BFD
blocked ports, using with Cisco PathTracer 11-4
blocking badge 3-8, A-20
borders for selected icons 4-14
bridges
understanding unassociated 12-70
viewing properties for VLANs 12-67
business configurations 6-8
business elements
definition 1-2
icons 2-14, A-4
roles required 6-1
business tag
definition 1-2
detaching 6-5
roles required 6-1
searching for 6-5
using Chinese characters 6-3
working with 6-3

buttons A-15
for filtering links A-15
in table toolbars A-15
Prime Network Events
Auto Refresh 8-21
Refresh Now 8-21
Ticket Properties dialog box A-16
toolbar A-16
Prime Network Vision A-12
link filtering A-15
table toolbar A-15
toolbar A-12
Report Manager toolbar A-17

C

callouts, VPN service overlay 17-25
Carrier Ethernet services, monitoring 12-1, 13-1
Carrier Grade NAT
roles required for viewing properties 13-1
viewing properties
logical inventory 13-2
physical inventory 13-5
Carrier Supporting Carrier (CSC) path traces 11-31
CEM groups
configured on
physical interfaces 18-51
virtual CEM interfaces 18-53
viewing in
logical inventory 18-53
physical inventory 18-51
viewing properties 18-51
CEM interfaces
properties 18-52
viewing in physical inventory 18-50
CESoPSN, viewing properties 18-3
CFM
description
maintenance domains 15-3
maintenance endpoints (MEPs) 15-3
maintenance intermediate points (MIPS) 15-3
overview 15-3
viewing properties for
maintenance associations 15-7
maintenance domains 15-4, 15-6
MEPs 15-8
MIPs 15-5
remote MEPs 15-9
Chinese characters
support for business tags 6-3
using in map and aggregation names 4-5
Circuit Emulation Services over PSN. See CESoPSN
Cisco Discovery Protocol (CDP) properties
in logical inventory 12-6
in physical inventory 12-8
viewing 12-6
Cisco PathTracer
across CSC configurations 11-31
comparing paths 11-27
counter values, saving 11-27
destinations 11-11
details pane 11-25
details window
menu options 11-22
toolbar 11-23
in MPLS networks 11-29
launching from
Ethernet Flow Point (EFP) 11-8
Ethernet port 11-12
examples 11-7
IP interface 11-9
MPLS-TP tunnel endpoint 11-13
pseudowire endpoint 11-12
VLAN bridge 11-10
Layer 2 VPNs 11-33
Layer 3 VPNs 11-32
menus 11-16
opening 11-3

overview 1-6, 11-1, 11-2
path pane 11-18
path trace
from inventory 11-7
from map view 11-5
options for starting 11-5
path trace pane 11-18, 11-23
rerunning paths 11-27
right-click
options in path trace window 11-19
trace launch options 11-4
roles required 11-1
single-path window 11-16
starting points 11-30
tabs 11-18
toolbar 11-17
viewing
Layer 2 Tunnel Protocol path information 11-29
path trace details 11-21
path traces 11-14
QinQ path information 11-28
clearing and removing tickets 9-21
clearing tickets 9-7, 9-20
clock recovery, pseudowire properties 18-44
clock service
badge 3-8, A-20
properties 18-35
color coding, severity icons 7-5
Command Builder. See Prime Network Command Builder
communication status, for VNEs 3-11
configuration scripts, launching 2-40, 2-44, 4-1
Connecting, VNE communication state 2-27
Connectivity Fault Management. See CFM
content pane
in Prime Network Vision 2-10
in the Prime Network Vision inventory window 3-16
tabs in logical inventory 3-32
Control Channel (CC), viewing information for pseudowire endpoint 12-96
conventions, used in this document xx
Correlation tab (tickets) 9-17
CPU usage graph, opening 4-40
creating
maps 4-8
report folders 10-46
VPNs 17-21
cross-connects
ATM
overview 18-6
properties 18-7
viewing 18-6
EFP
adding 12-73
overview 12-72
properties 12-73
cross-VRF routing entries 17-47
Currently Unsynchronized, VNE investigation state 2-28
customizing
audio options 2-47
event history size 2-47

D

Daily Average and Peak report 10-12
Daily Event Count by device report 10-15
Defined Not Started, VNE investigation state 2-27
defining report types 10-46
deleting
business elements 6-8
maps 4-25
report folders 10-48
reports 10-43
Dense Wavelength Division Multiplexing. See DWDM
destination, for Cisco PathTracer 11-11
Detailed Audit Events report 10-17
Detailed Provisioning Events report 10-17
Detailed Security Events report 10-17
Detailed Service Events report 10-15

Detailed Syslogs report 10-16
Detailed System Events report 10-17
Detailed Tickets report 10-16
Detailed Traps report 10-16
details pane, Cisco PathTracer 11-25
Details tab
events 8-16
tickets 8-20, 9-12
Device Partially Reachable, VNE communication state 2-27
devices
adding to maps 4-9
aggregations 4-28
CPU usage, checking 4-40
finding in maps 4-26
icons 2-10, A-2
in maps 4-28
pinging 4-41
removing from map 4-15
renaming aggregations 4-32
resizing in maps 4-14
severity indicator 2-24
status indicators 2-24
Telnet to a device 4-41
viewing
operating system information 3-33
properties 3-5
Devices with the Most Events report
by severity 10-12
by type 10-12
Devices with the Most Syslogs report 10-12
Devices with the Most Traps report 10-12
Device Unreachable, VNE communication state 2-27
device view pane
in the Prime Network Vision inventory window 3-16
toolbar 3-17
disaggregating aggregations 4-33
Discovering, VNE investigation state 2-28
discovery
based on Link OAM 15-13
EFD 12-42
EVC multiplex services 12-102
MPLS-TP tunnels 17-5
VLAN 12-42
document
audience xvii
conventions xx
organization xviii
related documentation xxi
terminology 1-1
duplication count, definition 9-6
DWDM
roles required for viewing properties 14-1
viewing
alert and alarm counters 14-9
G.709 properties 14-4
ODU alarm properties 14-7
ODU alert properties 14-8
OTU alarm properties 14-7
OTU alert properties 14-8
performance monitoring configuration 14-10
properties 14-2

E

EFD discovery 12-42
EFP
launching a path trace 11-8
overview 12-44
understanding severity and ticket badges 12-36
EFP cross-connects
adding 12-73
viewing properties 12-73
working with 12-72
egress adjacents, VRF 17-30
element icons, and information displayed 3-3
elements, business
deleting 6-8

renaming 6-8
elements, viewing operating system information 3-33
Ethernet flow domains
renaming 12-39
viewing 12-39
Ethernet Flow Domains inventory tab 2-6
Ethernet flow point (EFP), viewing properties 12-31
Ethernet LAGs
viewing 12-21
viewing properties 12-22
Ethernet links, and configured LSPs 17-11
Ethernet LMI
Device EVC Properties window 15-11
overview 15-9
viewing properties
for device EVCs 15-10
for physical interfaces 15-11
for UNI interfaces 15-12
in logical inventory 15-10
Ethernet Local Management Interface. See Ethernet LMI
Ethernet OAM
overview 15-2
roles required for viewing properties 15-1
Ethernet Operations, Administration, and Maintenance. See Ethernet OAM
Ethernet port, launching a path trace 11-12
Ethernet Service report
detailed 10-20
options 10-35
summary 10-20
Ethernet services
adding overlays 12-104
adding to maps 12-102
viewing properties 12-105
working with 12-101
EVC multiplex services, discovery 12-102
EVCs
shared switching entities 12-37
viewing service properties 12-37
event history size, customizing 2-47
Event Reduction Statistics report 10-13
events
Advanced tab 8-17
Audit tab 8-17
categories 7-5
definition 1-2
Details tab 8-16
filtering 8-22, 8-23
Provisioning tab 8-17
refreshing list in Prime Network Events 8-21
removing filters 8-24
Security tab 8-18
Trap tab 8-18
viewing
in Prime Network Events 8-2
properties 8-14
events reports 10-11
detailed network events, report options 10-27
detailed non-network events, report options 10-30
generating from
Prime Network Vision 10-38
Report Manager 10-23
Reports menu 10-37
report options 10-25
Run Report dialog box 10-24
exporting data from
Prime Network Events 8-25
Prime Network Vision 2-55
external application, launching 2-40, 2-44, 4-1

F

Fault Database vs. Event Archive Statistics report 10-13
filtering
events 8-22, 8-23
links
by type 4-38, 4-40
during map creation 4-38

in an existing map 4-40
using collection method 5-18
removing for events and tickets 8-24
tables 2-53, 2-54
tickets
by criteria 9-8
flickering links 5-3

G

General tab, in inventory window 3-16
generated ticket 9-7
GGSN
overview 20-3
roles required for viewing properties 20-2
view properties 20-4
graphical links, reducing number of in maps 2-17
GTPU
overview 20-6
roles required for viewing properties 20-2
view properties 20-6

H

Hardware Summary By Selected Property 10-18
Hardware Summary Detailed report 10-18
History tab (tickets) 9-13
H-VPLS
working with 12-75
working with in Prime Network Vision 12-75

I

icons
See also buttons *and* badges
alarm and ticket A-20
badges A-17
business elements 2-14, A-4
information displayed for elements 3-3
links A-8, A-9
logical inventory 3-30, A-6
management states 2-25, A-17
maps 17-20
map view 2-11
network elements 2-10, 2-13, A-2
physical inventory 3-19, A-8
Prime Network Events A-11
Prime Network Vision 2-11, A-1
reconciliation 3-9
reference A-1
REP 12-60
selecting 4-14
severities A-11
severity, color coding 2-24, 7-5
sizes 2-11, 3-3
tickets 2-29
VLAN domains 12-60
VLAN overlays 12-60
IMA group
properties 18-13
viewing properties 18-13
impact analysis
accumulating affected parties 9-23
affected severities 9-22
automatic mode 9-22
links and 5-13
proactive mode 9-22
Initializing management state 2-25
Inter-Chassis Communication Protocol (ICCP), viewing properties 12-27
inventory reports 10-18
generating from
Prime Network Vision 10-38
Report Manager 10-31
Reports menu 10-37
report options 10-32
Run Report dialog box 10-32

inventory tabs
Ethernet Flow Domains 2-6
in Prime Network Vision 2-5
Network Elements 2-5
opening 2-6
types of 2-5
VTP Domains 2-6
working with 2-7
inventory window
content pane 3-16
device view pane 3-16
device view pane toolbar 3-17
General tab 3-16
logical inventory 3-27
navigation pane 3-15
Network Events tab 3-18
opening 3-12
options
Disable Sending Alarms button 3-22, 18-6
Open Port Utilization Graph button 3-22, 18-6
Show Cross-Connect Table button 3-21, 18-6
Show DLCI Table button 3-22, 18-6
Show Encapsulation button 3-21, 18-6
Show VC Table button 3-21, 18-6
overview 3-12, 3-14
physical inventory 3-19, 3-21, 3-22, 18-6
Ports tab 3-16, 3-22
Provisioning Events tab 3-18
ticket and events pane 3-18
Tickets tab 3-18
IOS-XR Software Package Summary report 10-19
IP interface, launching a path trace 11-9
IP SLA, viewing responder service properties 12-108
IPv6
addresses
in logical inventory 16-3
in physical inventory 16-4
in inventory 16-3
in Prime Network 16-3
notes, for viewing IPv6 addresses 16-4
support in Prime Network 16-1
viewing IPv6 information 16-3
IPv6 VPN over MPLS (6VPE) 16-1
IS-IS, viewing properties 12-110

J

jobs scheduler 10-39

K

keyboard shortcuts, for tables 2-51

L

launching Prime Network Events
as a standalone application 7-3
from Prime Central 7-3
in Find mode 7-4
launching Prime Network Vision
as a standalone application 2-3
from Prime Central 2-2
Layer 2 Cisco PathTracer (VPN) 11-33
Layer 3 Cisco PathTracer (VPN) 11-32
link aggregation group. See Ethernet LAGs
Link Layer Discovery Protocol (LLDP), viewing properties 12-8
Link OAM
and topology discovery 15-13
overview 15-13
viewing properties in
logical inventory 15-14
physical inventory 15-17
link properties window
link list pane 5-11
overview 5-10
properties pane 5-11
ticket and events pane 5-12

links
- adding 5-15
- arrowheads 5-5, A-11
- bidirectional vs. unidirectional 5-5, A-11
- colors 5-5
- dashed line 5-4, A-10
- definition 1-2
- dynamic 5-3
- exceeding number that can be displayed 2-16
- filtering A-15
  - by type 4-38, 4-40
  - in maps 4-38
  - using collection method 5-18
- finding in maps 4-27
- flickering 5-3
- graphical representation 2-16
- icons A-8, A-9
- impact analysis 5-13
- in maps 2-16
- links view 5-8
- normal vs. wide vs. tunnel 5-5
- overview 5-1
- properties 5-4
- quick view 5-7
- reducing number of in maps 2-17
- selecting in maps 4-27, 5-18
- significance of
  - arrowheads A-11
  - characteristics A-10
  - color A-10
  - solid vs. dashed lines A-10
  - width A-10
- solid line 5-4, A-10
- static 5-3
- tooltips 2-17, 5-6
- tunnels 5-5
- types A-9
- use of arrowheads 5-5
- user roles required for working with 5-1
- viewing
  - between VLAN elements and devices 12-55
  - in links view 5-8
  - options 5-18
  - properties 5-4, 5-10
- width 5-5

links view
- filtering 2-23, A-15
- information displayed 2-23
- in Prime Network Vision 2-22

list view
- in Prime Network Vision 2-18
- overview 2-18
- right-click options 2-21
- toolbar 2-20, 2-50, A-15

LLDP, viewing properties 12-8

lock badge 3-8, A-20

logical inventory
- branches 3-29
- content pane 3-32
- content pane tabs 3-32
- icons 3-30, A-6
- navigation pane 3-29
- tabs 3-32
- viewing in Prime Network Vision 3-27
- window 3-28

logical link, definition 1-2

LSEs
- inventory details 17-38
- viewing 17-38

LSP endpoints 17-13
- properties 17-13

LSPs
- lockout state 17-6
- on Ethernet links 17-11
- properties 17-13
- redundancy service properties 17-13
- Working and Protected 17-5

M

Maintenance, VNE investigation state 2-28
maintenance domains, in CFM 15-3
managed element, definition 1-2
management states
  badges A-17
  icons A-17
  overview 2-25
managing maps, roles required 4-2
managing report folders
  creating 10-46
  deleting 10-48
  moving 10-47
  renaming 10-47
  viewing properties 10-48
managing reports
  deleting 10-43
  moving reports 10-43
  renaming 10-41
  roles required 10-1
  saving 10-40
  sharing 10-42
  viewing
    report properties 10-44
    reports 10-40
managing tickets 9-19
managing VPNs 17-21
  adding to maps 17-22
  creating 17-21
  moving virtual routers between 17-23
  overlays
    adding 17-24
    displaying 17-25
    hiding 17-25
  removing from maps 17-23
maps
  adding network elements 4-9
  adding VLANs 12-48
  aggregations 4-28
  applying background images 4-17
  Cisco PathTracer files 11-26
  closing 4-5, 4-8
  creating 4-8
  customizing 2-47
  deleting 4-25
  devices in 4-26
  filtering links 4-38
  finding
    affected elements 4-27
    links in maps 4-27
  in Prime Network Vision 2-10
  layouts 4-17
  link icons A-8
  network elements in 4-26, 4-28
  opening 2-8, 4-5
    any map 4-6
    options 4-7
    previously viewed 4-6
  overlays
    callouts 17-25
    VPN 17-24
  overview 17-18, 17-19
  previewing before printing 4-23
  printing 4-23
  print setup 4-23
  red border and graphical links 2-16
  removing
    devices 4-15
    network elements 4-15
    VLANs 12-50
    VPNs 17-23
  renaming 4-20
  renaming aggregations 4-32
  roles required 4-2
  saving 4-20
    as an image 4-21
    as new map 4-21

with information 4-20
selecting views 4-16
using Chinese characters 4-5
using overview windows 4-19
viewing
aggregation thumbnails 4-30
thumbnails 4-30
VPNs
adding 17-22
overlays 17-24
viewing 17-18
working with 4-1
zooming in 4-15
map view
adding VLAN overlays 12-58
in Prime Network Vision 2-10
Mean Time to Repair report 10-13
menus
Cisco PathTracer 11-16
Cisco PathTracer details window 11-22
Prime Network Events 7-8
Prime Network Vision 2-31
Report Manager 10-6
MEPs, in CFM 15-3
MIPS, in CFM 15-3
MLPPP
viewing link properties 18-29
viewing properties 18-26
Mobile technologies 20-1
APN 20-8
GGSN 20-3
GTPU 20-6
user roles 20-2
Mobile Transport over Packet. See MToP
modifying VNE properties 3-9
Modules Summary By Type 10-19
monitoring
Carrier Ethernet services 12-1
Carrier Grade NAT properties 13-1
network clocking service 18-34
PTP service 18-36
Most Common Daily Events report 10-14
Most Common Syslogs report 10-14
moving
report folders 10-47
reports between folders 10-43
MP-BGP properties in logical inventory 17-42
MPLS
ARP table 17-33
BGPs, viewing 17-42
Cisco PathTracer and 11-29
LSEs, viewing 17-38
monitoring services 17-26
NDP table 17-34
pseudowire end-to-end emulation tunnels, viewing 17-47
rate limit information 17-35
roles required for viewing properties 17-1
routing entities 17-31
TE tunnels, viewing 17-49
MPLS pseudowire over GRE, properties 18-32
MPLS TE tunnel, inventory details 17-49
MPLS-TP tunnel endpoint, launching a path trace 11-13
MPLS-TP tunnels
adding to maps 17-5
applying overlays 17-16
BFD sessions, viewing properties 17-46
discovery 17-5
LSP lockout state 17-6
overview 17-4
properties 17-7
working with 17-4
MToP
channelized lines 18-17
IMA group properties 18-13
monitoring
network clocking service 18-34
PTP service 18-36

network clocking service 18-34
PTP service overview 18-36
roles required for working with 18-1
TDM
overview 18-16
viewing properties in physical inventory 18-17
viewing
ATM cross-connects 18-6
ATM VCI properties 18-10
ATM VPI properties 18-10
CEM groups 18-51, 18-53
CEM interfaces 18-50
CEM properties 18-50
CESoPSN pseudowire properties 18-3
encapsulation information 18-11
IMA group properties 18-13
MLPPP link properties 18-29
MLPPP properties 18-26
network clocking service 18-34
pseudowire clock recovery properties 18-41
PTP service properties 18-36
SAToP pseudowire properties 18-2
SONET/SDH channelization properties 18-18
SyncE properties 18-45
T3 DS1 and DS3 channelization properties 18-21
TDM properties 18-17
virtual CEMs, list of 18-51
virtual CEMs properties 18-50
Multichassis LACP (mLACP), viewing properties 12-27
multiple links badge 3-8, A-20
multiplex services, discovery of 12-102

N

navigation pane
logical inventory 3-29
physical inventory 3-19
Prime Network Vision 2-9
NDP table 17-34
network clocking service
applying an overlay 18-48
clock service properties 18-35
monitoring 18-34
monitoring PTP service 18-36
overview 18-34
PTP interface properties 18-37
PTP service 18-36
network elements
adding to existing aggregations 4-30
adding to maps 4-9
aggregating 4-29
aggregations 4-28
CPU usage, checking 4-40
definition 1-2
finding in maps 4-26
icons 2-10, 2-13, A-2
information displayed in icons 3-3
in maps 4-28
management state 2-25
pinging 4-41
removing from maps 4-15
renaming aggregations 4-32
resizing in maps 4-14
severity indicators and network elements 2-24
status indicators 2-24
Telnet to 4-41
viewing
operating system information 3-33
properties 3-5
zooming in 4-15
Network Elements inventory tab 2-5
Network Events tab
inventory window 3-18
link properties window 5-12
network event tabs, in Prime Network Events 8-6
Network Pseudowire report
detailed 10-21
options 10-36

summary 10-21
network service reports 10-20
generating from
Prime Network Vision 10-38
Report Manager 10-34
Reports menu 10-37
report options 10-35
Run Report dialog box 10-34
Notes tab (tickets) 9-18, 9-19

O

opening
inventory tabs 2-6
maps 2-8
Open Map dialog box options 4-7
operating system information, viewing for devices 3-33
Operational, VNE investigation state 2-28
options
Open Map dialog box 4-7
working with aggregation thumbnails 4-32
OSPF
supported versions 12-113
viewing properties 12-113
overlays
applying to
Ethernet services 12-104
maps 4-34
MPLS-TP tunnels 17-16
network clocks 18-48
pseudowire 12-100
VLANs 12-58
VPLS instances 12-77
VPNs 17-24
displaying and hiding
for VLANs 12-59
for VPNs 17-25
in maps 4-37
Ethernet service 12-104
pseudowire 12-88, 12-100
removing 4-37, 12-59
viewing 4-37
pseudowire tunnel links in VPLS 12-79
REP information 12-60
STP information 12-63
VLAN
adding 12-58
removing 12-59
viewing STP link information 12-63
working with 12-42
VPLS
callouts 12-80
instance 12-77
viewing pseudowire tunnel links 12-79
VPN 17-24
adding 17-24
callouts 17-25
working with 4-26, 4-33
overview
ATM cross-connects 18-6
CFM 15-3
Cisco PathTracer 1-6, 11-1
EFP cross-connects 12-72
EFPs 12-44
Ethernet LMI 15-9
Ethernet OAM 15-2
Link OAM 15-13
MPLS-TP tunnels 17-4
network clocking service 18-34
Prime Network Command Builder 1-6
Prime Network Events 1-7
Prime Network Soft Properties Manager 1-6
Prime Network Vision 1-4
Prime Network Vision inventory window 3-12
Prime Network Vision maps 2-7
PTP service 18-36
Report Manager 1-6
reports 10-1

SAToP 18-2
SBC 19-1
switching entities 12-43
TDM 18-16
unassociated bridges 12-70
VLANs 12-43
overview window 4-19

P

Partially Discovered, VNE investigation state 2-28
password, changing 2-47
path pane, in Cisco PathTracer 11-18
path trace
and blocked ports 11-4
examples 11-7
launching from
EFP 11-8
Ethernet port 11-12
IP interface 11-9
MPLS-TP tunnel endpoint 11-13
pseudowire endpoint 11-12
VLAN bridge 11-10
starting 11-5
from inventory 11-7
from map view 11-5
viewing
in Cisco PathTracer 11-14
Layer 2 Tunnel Protocol path information 11-29
path trace details 11-21
QinQ path information 11-28
path trace details window 11-21
path trace pane, Cisco PathTracer 11-18, 11-23
PathTracer. See Cisco PathTracer
permissions, security 1-3
physical inventory
branches 3-19
buttons
Disable Sending Alarms 3-22, 18-6
Open Port Utilization Graph 3-22, 18-6
Show Encapsulation 3-21, 18-6
content pane 3-20
icons 3-19, A-8
navigation pane 3-19
viewing device properties 3-19
viewing in Prime Network Vision 3-19
window 3-17
physical link, definition 1-2
pinging
devices 4-41
network elements 4-41
pseudowires 12-94
polling, initiating 3-12
Poll Now button 3-12
ports
alarms
disabling 3-26
enabling 3-26
viewing
configuration 3-24
status 3-22
with IPv4 and IPv6 addresses 16-5
Ports tab, in inventory window 3-16, 3-22
Port Utilization graph, generating 3-27
Prime Central
launching Prime Network Events 7-3
launching Prime Network Vision 2-2
Prime Network 3.6.x tabs, in Prime Network Events 8-12
Prime Network Command Builder
launching scripts 2-40, 2-44, 4-1
overview 1-6
Prime Network Events
All tab 8-3
Audit tab 8-3
buttons
Ticket Properties dialog box A-16
toolbar A-16
customizing 7-10

displaying all events 7-5
event categories 7-5
exporting data 8-25
icon severities A-11
launching
as a standalone application 7-3
from Prime Central 7-3
in Find mode 7-4
options 7-2
menus 7-8
network event tabs 8-6
overview 1-7
Prime Network 3.6.x tabs 8-12
Provisioning tab 8-5
right-click options 7-9
roles required 7-1, 8-1
Security tab 8-5
Service tab 8-7
Syslog tab 8-7
system event tabs 8-3
System tab 8-6
Ticket tab 8-8
toolbar 7-7
toolbar buttons A-16
V1 Trap tab 8-10
V2 Trap tab 8-10
V3 Trap tab 8-11
viewing
all events 7-5
events and tickets 8-2
window 7-3
working with 8-14
Prime Network Soft Properties Manager overview 1-6
Prime Network Vision
adding network elements 4-9
buttons A-12
filtering links A-15
table toolbar A-15
toolbar A-12
creating maps 4-8
customizing 2-47
deleting maps 4-25
exporting data 2-55
generating reports 10-38
GUI overview 17-18, 17-19
icons 17-20, A-1
links A-9
logical inventory A-6
map A-2, A-4
physical inventory A-8
selecting 4-14
sizes 2-11
interface components 2-4
inventory tabs 2-5
launching
as a standalone application 2-3
from Prime Central 2-2
options 2-2
links
characteristics A-10
colors A-10
icons A-9
list view toolbar A-15
maps 2-10, 2-47
adding network elements 4-9
choosing layout 4-17
closing 4-5, 4-8
creating 4-8
deleting 4-25
opening 4-5
overview 2-7
renaming 4-20
resizing elements 4-14
saving 4-20
saving as an image 4-21
saving as new map 4-21
saving with information 4-20
using Chinese characters 4-5

viewing options 4-16
menus 2-31
Activation 2-35
Edit 2-33
File 2-32
Help 2-37
Network Inventory 2-36
Node 2-34
Reports 2-36
right-click 2-37
Tools 2-35
View 2-33
Window 2-36
navigation 2-4
opening
inventory tabs 2-6
the inventory window 3-12
overlays 17-25
overview 1-4
port information 3-24
properties window 3-6
removing network elements 4-15
renaming maps 4-20
resizing map elements 4-14
right-click menus 2-37
roles required 2-1, 3-2
tables
defining filters 2-53
finding text in 2-51
managing 2-49
setting selection filters 2-54
sorting 2-51
toolbar options 2-50
toolbar buttons A-12
viewing tickets 9-3
VLAN elements and icons 12-43
windows 2-4
working with
H-VPLS 12-75
inventory tabs 2-7
multiple tabs 2-9
tickets 9-1
VPLS 12-75
Prime Network Vision window
content pane 2-10
inventory tabs 2-5
links view 2-22
list view
overview 2-18
toolbar 2-20, 2-50
map view 2-10
icons 2-11
right-click options 2-18
severity indicators 2-17
navigation pane 2-9
right-click menus
aggregation 2-42
device 2-38
link 2-42
links view 2-45
list view 2-43
maps 2-38
ticket 2-46
ticket pane 2-24
toolbar 2-29
layout tools 2-31
map options 2-29
map zoom tools 2-31
navigation tools 2-30
overlay tools 2-30
viewing options 2-30
printing maps 4-23
properties
6rd tunnels 17-43
CEM interface 18-52
clock service 18-35
ICCP 12-27
mLACP 12-27

MPLS pseudowire over GRE 18-32
MPLS-TP tunnels 17-7
MToP
ATM VCI 18-10
ATM VPI 18-10
pseudowire clock recovery 18-44
PTP interface 18-37
REP 12-14
report folders 10-48
report types 10-50
SBC 19-4
AAA 19-6
DBE 19-4
H.248 19-5, 19-7
media address 19-4
policy 19-8
SBE 19-6
SIP 19-11
virtual connections 18-5
properties window in Prime Network Vision 3-6
provider, definition 1-2
Provider Backbone Bridge (PBB), viewing properties 12-30
Provisioning Events tab, in the inventory window 3-18
Provisioning tab
events 8-17
in Prime Network Events 8-5
pseudowire clock recovery
properties 18-44
viewing properties 18-41
pseudowire endpoint, launching a path trace 11-12
pseudowires
adding 12-88
applying overlay 12-100
overlays 12-88
pinging 12-94
redundancy service properties 12-98
viewing
endpoint properties 12-85
properties 12-91
redundancy service properties 12-98
tunnel links in VPLS overlays 12-79
VCCV and CC information 12-96
working with 12-88
PTP
interface properties 18-37
monitoring service 18-36
service overview 18-36
PWE3
inventory details 17-47
viewing 17-47

Q

quick view, for links 5-7

R

rate limits, for routing entities 17-35
reconciliation badge A-20
aggregations 2-42
business elements 6-8
description 3-9
EFPs 12-47
switching entities 12-47
VPLS forwards 12-75
red border in maps, and graphical links 2-16
reduced polling 3-12
reduction count, definition 9-6
redundancy service 17-13
badge 3-9, A-20
on LSP endpoints 17-13
pseudowires 12-98
related documentation xxi
removing
overlays 4-37
tickets 9-21

VLAN overlays 12-59
VLANs from maps 12-50
VPNs 17-23
renaming
Ethernet flow domains 12-39
maps 4-20
report folders 10-47
reports 10-41
REP
icons and badges 12-60
viewing
for VLAN service link properties 12-61
in VLAN domain views 12-60
in VLAN overlays 12-60
report categories 10-11
report folders
creating 10-46
deleting 10-48
moving 10-47
renaming 10-47
viewing properties 10-48
working with 10-46
Report Manager
content pane 10-7
events reports 10-11
generating reports 10-23
inventory reports 10-18
menu options 10-6
navigation tree 10-7
network service reports 10-20
overview 1-6
report categories 10-11
right-click options 10-9
roles required 10-1
toolbar buttons 10-6, A-17
using 10-4
report properties, viewing 10-44
reports
and database load 10-23
canceled 10-23
creating folders 10-46
defining types 10-46
deleting
folders 10-48
reports 10-43
events
Daily Average and Peak 10-12
Devices with the Most Events by severity 10-12
Devices with the Most Events by type 10-12
Devices with the Most Syslogs 10-12
Devices with the Most Traps 10-12
Event Reduction Statistics 10-13
Fault Database vs. Event Archive Statistics 10-13
Mean Time to Repair 10-13
Most Common Daily Events 10-14
Most Common Syslogs 10-14
Syslog Count by device 10-14
Syslog Count by type 10-14
Syslog Trend by severity 10-14
fail to generate 10-23
formats 10-40
generating 10-22
events reports 10-23
inventory reports 10-31
network service reports 10-34
generating from
Prime Network Vision 10-38
Report Manager 10-23
Reports menu 10-37
inventory
Hardware Summary By Selected Property 10-18
Hardware Summary Detailed 10-18
IOS-XR Software Package Summary 10-19
Modules Summary By Type 10-19
Software Version Summary by device 10-19
Software Version Summary by version 10-19
limiting access to 10-43
managing

maximum concurrent reports 10-39
options 10-39
maximum number of concurrent reports 10-39
moving
folders 10-47
reports between folders 10-43
network events
Detailed Event Count (by device) 10-15
Detailed Service Events 10-15
Detailed Syslogs 10-16
Detailed Tickets 10-16
Detailed Traps 10-16
network service
Ethernet Service Detailed 10-20
Ethernet Service Summary 10-20
Network Pseudowire Detailed 10-21
Network Pseudowire Summary 10-21
VPLS Detailed 10-22
VPLS Summary 10-22
non-network events
Detailed Audit Events 10-17
Detailed Provisioning Events 10-17
Detailed Security Events 10-17
Detailed System Events 10-17
options for
detailed network events reports 10-27
detailed non-network events reports 10-30
events reports 10-25
inventory reports 10-32
network service reports 10-35
overview 10-1
queued 10-39
renaming
folders 10-47
reports 10-41
Report Properties dialog box 10-45
roles required 10-1
saving 10-40
scheduling 10-38
sharing 10-42
using Report Manager 10-4
viewing 10-40
report folder properties 10-48
report properties 10-44
report type properties 10-50
working with folders 10-46
Reports menu, and generating reports 10-37
report types, viewing properties 10-50
REP primary badge 3-9, A-20
REP primary blocking badge 3-9, A-20
Resilient Ethernet Protocol (REP), viewing properties 12-14
resizing icons
using the Resize option 4-14
using your mouse 4-14
right-click options
aggregations 2-42
Cisco PathTracer 11-4, 11-19
devices 2-38
links 2-42
links view 2-45
list view 2-21, 2-43
maps 2-38
Prime Network Events 7-9
Prime Network Vision 2-18, 2-37
Report Manager 10-9
tickets 2-46
roles
managing reports 10-1
security 1-3
viewing
Carrier Ethernet properties 12-2
Carrier Grade NAT properties 13-1
DWDM properties 14-1
Ethernet OAM tool properties 15-1
IPv6 information 16-2
SBC properties 19-2
working with

business tags 6-1
Cisco PathTracer 11-1
links 5-1
maps 4-2
MPLS networks 17-1
MToP 18-1
Prime Network Events 7-1, 8-1
Prime Network Vision 2-1, 3-2
reports 10-1
tickets 9-1
routing entities 17-31
ARP table 17-33
NDP table 17-34
rate limit information 17-35
viewing properties 17-31

S

SAToP, overview 18-2
saving
maps 4-20
reports 10-40
SBC
AAA properties 19-6
DBE properties 19-4
H.248 properties 19-5, 19-7
logical inventory properties 19-1
media address properties 19-4
overview 19-1
policy properties 19-8
properties 19-4
SBE properties 19-6
SIP properties 19-11
user roles required for viewing properties 19-2
viewing in logical inventory 19-3, 19-4
scheduled jobs
monitoring 10-39
scopes, and security 1-3
scripts
launching 2-40, 2-44
launching for activation and configuration 4-1
security
permissions 1-3
roles 1-3
scopes 1-3
Security tab
events 8-18
in Prime Network Events 8-5
selecting
icons 4-14
links in maps 4-27
Service tab, in Prime Network Events 8-7
service view
overlays 17-25
removing VLANs 12-50
removing VPNs 17-23
virtual routers 17-23
VPNs 17-21, 17-26
Session Border Controller. See SBC
severity
color of device icon 2-25
icons A-11
indicators
in Prime Network Vision map view 2-17
overview 2-24
propagation 2-24
shared switching entities 12-37
sharing reports 10-42
Shutting Down, VNE investigation state 2-28
sites, viewing properties 17-27
Soft Properties Manager. See Prime Network Soft Properties Manager
Software Version Summary report
by device 10-19
by version 10-19
SONET/SDH, viewing properties 18-18
Spanning Tree Protocol. See STP
static link, adding 5-15

status indicators, for network elements 2-24
Stopped, VNE investigation state 2-28
STP
viewing
link information in VLAN overlay 12-63
properties 12-10
VLAN service link properties 12-64
viewing in
VLAN domain views 12-63
VLAN overlays 12-63
STP root badge 3-9, A-20
Structure-Agnostic TDM over Packet. See SAToP
subscriber, definition 1-2
switching entities
containing termination points 12-48
overview 12-43
Synchronous Ethernet (SyncE), viewing properties 18-45
Syslog Count report
by device 10-14
by type 10-14
Syslog tab, in Prime Network Events 8-7
Syslog Trend report by severity 10-14
system event tabs, in Prime Network Events 8-3
System tab, in Prime Network Events 8-6

T

T3 DS1 and DS3, viewing properties 18-21
tables
filtering 2-53
finding text in 2-51
keyboard shortcuts 2-51
keyboard shortcuts for 2-51
managing in Prime Network Vision 2-49
sorting 2-51
toolbar buttons A-15
tabs
in Cisco PathTracer window 11-18
working with multiple tabs 2-9
tag manipulations, for associated VLANs 12-52
TDM
overview 18-16
viewing properties in physical inventory 18-17
Telnet to devices 4-41
termination points, in switching entities 12-48
terminology in this document 1-1
TE tunnels and Cisco PathTracer 11-34
thumbnail views, options 4-32
ticket and events pane, Prime Network Vision inventory window 3-18
ticket pane
information displayed 9-5
Prime Network Vision 2-24
ticket properties, Details tab 8-20
Ticket Properties dialog box
Advanced tab 9-18
Affected Parties tab 9-14
Correlation tab 9-17
Details tab 9-12
History tab 9-13
Notes tab 9-18, 9-19
toolbar 9-12
tickets
acknowledged 9-7
acknowledging 9-19
and EFP severities 12-36
badges A-20
clearing 9-7, 9-20
clearing and removing 9-21
definition 1-3
filtering
by criteria 9-8
finding
affected elements in map 4-27
affected elements using the ticket pane 9-19
generated 9-7
icons 2-29
managing 9-19

propagating new 2-25
properties 9-10
removing 9-21
removing filters 8-24
right-click menu 2-46
roles required 9-1
status 9-6
viewing
in Prime Network Events 8-2
in Prime Network Vision 9-3
properties 9-12
working with in Prime Network Vision 9-1
Tickets tab
inventory window 3-18
link properties window 5-12
Prime Network Events 8-8
Time Division Multiplexing. See TDM or MToP TDM
toolbar buttons
Cisco PathTracer single-path window 11-17
for filtering links A-15
for tables 2-50, A-15
Prime Network Vision list view A-15
Report Manager 10-6, A-17
Ticket Properties window 9-12
toolbars
Cisco PathTracer 11-17
Cisco PathTracer details window 11-23
device view pane 3-17
Prime Network Events 7-7
Prime Network Vision 2-29, 2-50
Prime Network Vision list view 2-20, 2-50
Report Manager 10-6
Ticket Properties window 9-12
tooltips for links 5-6
Tracking Disabled, VNE communication state 2-27
Trap tab (events) 8-18

U

unassociated bridges
adding 12-70
overview 12-70
understanding
EFP severity and ticket badges 12-36
static and dynamic links 5-3
unassociated bridges 12-70
VLAN and EFD discovery 12-42
ungrouping aggregations 4-33
unmanaged network, definition 1-3
Unsupported, VNE investigation state 2-27
updating
affected severity 9-24
VNE information 3-12
Up ticket 9-8
user roles
viewing
APN 20-2
Carrier Grade NAT properties 13-1
DWDM properties 14-1
Ethernet OAM properties 15-1
GGSN 20-2
GTPU 20-2
MToP properties 18-1
SBC properties 19-2
working with
business elements 6-1
business tags 6-1
Carrier Ethernet services 12-2
Cisco PathTracer 11-1
IPv6 and 6VPE 16-2
links 5-1
maps 4-2
MPLS networks 17-1
Prime Network Events 7-1, 8-1
Prime Network Vision 2-1, 3-2
reports 10-1

tickets 9-1

V

V1 Trap tab, in Prime Network Events 8-10
V2 Trap tab, in Prime Network Events 8-10
V3 Trap tab, in Prime Network Events 8-11
viewing
6rd tunnel properties 17-43
access gateway properties 12-18
additional APN characteristics 20-12
APN properties 20-9
ATM cross-connects 18-6
ATM VCI properties 18-10
ATM VPI properties 18-10
BFD session properties 17-44
Carrier Ethernet properties, roles required 12-2
Carrier Grade NAT properties 13-2, 13-5
CDP properties 12-6
CEM groups 18-51, 18-53
CEM interfaces 18-50
CEM properties 18-50
CESoPSN pseudowire properties 18-3
CFM properties 15-3
cross-VRF routing entries 17-47
device operating system information 3-33
device properties 3-5
DWDM properties 14-2
EFP cross-connect properties 12-73
EFP properties 12-31
encapsulation information 18-11
Ethernet flow domains 12-39
Ethernet LAG properties 12-22
Ethernet LAGs 12-21
Ethernet Link Aggregation Groups 12-21
Ethernet services properties 12-105
EVC service properties 12-37
GGSN properties 20-4
GTPU properties 20-6
ICCP properties 12-27
IMA group properties 18-13
IP SLA responder service properties 12-108
IPv6 information 16-2
IS-IS properties 12-110
Layer 2 Tunnel Protocol path trace 11-29
Link Layer Discovery Protocol (LLDP) properties 12-8
Link Layer Discovery Protocol properties 12-8
Link OAM properties 15-13
link properties 5-10
links between VLAN elements and devices 12-55
LLDP properties 12-8
LSE properties 17-38
LSP endpoint properties 17-13
LSPs on Ethernet links 17-11
mLACP properties 12-27
MLPPP link properties 18-29
MLPPP properties 18-26
MPLS TE tunnel information 17-49
MPLS-TP BFD sessions 17-46
MPLS-TP tunnel properties 17-7
network element properties 3-5
operating system information for devices 3-33
OSPF properties 12-113
path trace details in Cisco PathTracer 11-21
path traces in Cisco PathTracer 11-14
PBB properties 12-30
port configuration information 3-24
pseudowire
clock recovery properties 18-41
endpoint properties 12-85
properties 12-91
redundancy service properties 12-98
VCCV and CC information 12-96
PWE3 tunnel information 17-47
QinQ path trace 11-28
REP information in
VLAN domain views 12-60

VLAN overlays 12-60
report folder properties 10-48
report properties 10-44
reports 10-40
report type properties 10-50
REP properties
for VLAN service links 12-61
in logical inventory 12-14
routing entities 17-31
SAToP pseudowire properties 18-2
SBC properties 19-3, 19-4
SONET/SDH channelization properties 18-18
STP
information in VLAN domain views 12-63
information in VLAN overlays 12-63
properties 12-10
properties for VLAN service links 12-64
SyncE properties 18-45
T3 DS1 and DS3 channelization properties 18-21
TDM properties 18-17
ticket properties 8-19
tickets in Prime Network Vision 9-3
virtual CEMs
list of 18-51
properties 18-50
virtual connection properties 18-5
Virtual Switching Instance properties 12-83
VLAN
bridge properties 12-67
mapping properties 12-54
mappings 12-50
service link properties 12-60
trunk group properties 12-65
VNE properties 3-9
VPLS
access Ethernet EFP properties 12-87
instance properties 12-81
properties 12-81
VPN
properties 17-26
site properties 17-27
VRF properties 17-27
VRRP information 17-36
VSI properties 12-83
virtual CEMs
listing 18-51
viewing properties 18-50
Virtual Circuit Connectivity Verification (VCCV), viewing information for pseudowire endpoint 12-96
virtual cloud, definition 1-3
virtual connections
viewing encapsulation information 18-11
viewing properties 18-5
Virtual Router Redundancy Protocol (VRRP), viewing information 17-36
virtual routers
moving 17-23
properties, viewing 17-27
VRF tables 17-30
Virtual Switching Instance. See VSI
VLAN bridge, launching a path trace 11-10
VLAN overlays
adding to maps 12-58
working with 12-42
VLANs
adding associated VLANs 12-52
adding to map view 12-48
associations 12-52
definition 1-3
discovery 12-42
elements
EFPs 12-44
icons in Prime Network Vision 12-43
network VLAN 12-43
overview 12-43
switching entities 12-43
overlays
STP link information 12-63

viewing REP information 12-60
viewing STP information 12-63
overview 12-43
removing
from maps 12-50
overlays 12-59
tag manipulations for associations 12-52
viewing
associated VLAN mapping properties 12-54
associated VLAN service links 12-54
bridge properties 12-67
links between elements and devices 12-55
mappings 12-50
REP properties 12-61
service link properties 12-60
STP properties 12-64
working with 12-42
VLAN trunk group, viewing properties 12-65
VNE/Agent Unreachable, VNE communication state 2-27
VNE communication states
Agent Not Loaded 2-27
Connecting 2-27
Device Partially Reachable 2-27
Device Unreachable 2-27
Tracking Disabled 2-27
VNE/Agent Unreachable 2-27
VNE investigation states
Currently Unsynchronized 2-28
Defined Not Started 2-27
Discovering 2-28
Maintenance 2-28
Operational 2-28
Partially Discovered 2-28
Shutting Down 2-28
Stopped 2-28
Unsupported 2-27
VNEs
communication state badges A-18
investigation state badges A-18
management state 2-25
modifying properties 3-9
updating information 3-12
viewing communication status 3-11
viewing properties 3-9
VPLS
adding instances to maps 12-76
instance overlays 12-77
overlays
link callout 12-80
viewing pseudowire tunnel links 12-79
viewing
access Ethernet EFP properties 12-87
instance properties 12-81
properties 12-81
pseudowire endpoint properties 12-85
working with 12-75
VPLS report
detailed 10-22
options 10-36
summary 10-22
VPNs
adding to maps 17-22
and virtual routers 17-23
creating 17-21
definition 1-3
managing 17-21
moving virtual routers between 17-23
overlays 17-24
callouts 17-25
creating 17-24
displaying 17-25
hiding 17-25
properties, viewing 17-26
removing from maps 17-23
sites 17-27
viewing in maps 17-18
virtual routers 17-27
VRFs

cross-VRF routing entries 17-47
tables
egress 17-30
ingress 17-30
viewing properties 17-27
with IPv4 and IPv6 addresses 16-6
VSI, viewing properties 12-83
VTP Domains inventory tab 2-6

W

Working and Protected LSPs 17-5
working with
associated VLANs 12-52
business elements 6-1
business tags 6-1
EFP cross-connects 12-72
Ethernet services 12-101
H-VPLS 12-75
inventory tabs 2-7
links, user roles required 5-1
MPLS-TP tunnels 17-4
overlays 4-33
Prime Network Events 8-14
pseudowire overlays 12-88
pseudowires 12-88
tickets in Prime Network Vision 9-1
VLAN overlays 12-42
VLANs 12-42
VPLS 12-75

Z

zooming in and out of maps 4-15