# Cisco Prime Network 3.11 User Guide

May 2013

**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-29355-01

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 3.11 User Guide*
© 1999-2013 Cisco Systems, Inc. All rights reserved.

# CONTENTS


**Preface** xxiii

Audience xxiii

Document Organization xxiv

Conventions xxvi

Related Documentation xxvii

Obtaining Documentation and Submitting a Service Request xxvii

xxvii

CHAPTER 1 **Setting Up Devices and Using the GUI Clients** 1-1

Overview of the GUI Clients 1-1

Setting Up Devices and Validating Device Information 1-2

Configure Basic Device Settings: Name, DNS, NTP, RADIUS, TACACs, ACLs 1-4

Configure SNMP and SNMP Traps on Device 1-5

Configure Device Ports and Interfaces 1-6

View Device and VRF Routing Tables and Device Interface Briefs 1-7

Ping Destinations and VRFs, and View Trace Route from Device 1-7

Change Device Syslog Logging Level 1-8

View, Copy, and Overwrite Device Configuration Files 1-8

View Users (Telnet Sessions) on Device 1-8

Using Prime Network with Prime Central 1-8

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

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

Launching Prime Network Vision 2-2

Changing Your GUI Client Password 2-3

The Prime Network Vision Window 2-3

Prime Network Vision Inventory Tabs 2-4

Prime Network Vision Maps 2-5

Opening Maps 2-6

Navigation Pane 2-6

Content Pane: Map, List, and Links Views 2-7

Ticket Pane 2-16

Prime Network Vision Status Indicators 2-16

Severity 2-17
VNE Management State 2-18
Tickets 2-22
Prime Network Vision Toolbar 2-22
Prime Network Vision Menu Bar 2-24
File Menu 2-25
Edit Menu 2-26
View Menu 2-26
Node Menu 2-27
Tools Menu 2-27
Activation Menu 2-28
Network Inventory Menu 2-28
Reports Menu 2-29
Window Menu 2-29
Help Menu 2-29
Prime Network Vision Right-Click Menus 2-29
Map Right-Click Menu 2-30
Element Right-Click Menu 2-31
Aggregation Right-Click Menu 2-34
Link Right-Click Menu 2-35
List View Right-Click Menu 2-35
Links View Right-Click Menu 2-37
Ticket Right-Click Menu 2-38
Adjusting the Prime Network Vision GUI Client Settings 2-39
Filtering and Sorting Tabular Content 2-40

CHAPTER 3 **Viewing and Managing NE Properties 3-1**
User Roles Required to Work with Prime Network Vision 3-1
Information Available in Element Icons 3-3
Viewing the Properties of a Network Element 3-6
Network Element Badges 3-8
The Inventory Window 3-9
Navigation Pane 3-12
Content Pane 3-13
Device View Pane 3-13
Device View Pane Toolbar 3-14
Ticket and Events Pane 3-15
Checking VNE Connectivity and Communication Status 3-16

Viewing the Physical Properties of a Device 3-19
Redundancy Support 3-21
Viewing Satellite Properties 3-22
Working with Ports 3-23
Viewing Port Status and Properties 3-23
Viewing a Port Configuration 3-25
Disabling and 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 3-30
Viewing Device Operating System Information 3-31
Running an Activation from the Activation Menu 3-33
Network Activation Window 3-34
Running Activations 3-34
Searching for Activations (Activation History) 3-35
Rolling Back an Activation 3-35
Cloning an Existing Activation 3-36
Deleting Activations 3-36

CHAPTER 4 **Device Configurations and Software Images** 4-1
What is Change and Configuration Management? 4-1
Set Up Change and Configuration Management 4-2
Prime Network Setup Tasks 4-3
Device Setup Tasks 4-4
Configuration Management Setup Tasks 4-5
NEIM Setup Tasks 4-6
Device Groups Setup Tasks 4-8
Use the CCM Dashboard 4-10
Device Configurations 4-11
What is In the Archive? 4-11
Protect Configurations in the Archive 4-12
Find Out What is Different Between Configurations 4-13
Copy a Configuration File to a Central Server 4-15
Are Running and Startup Configs Mismatched? (Cisco IOS and Cisco Nexus) 4-16
Copy the Device Files to the Archive (Backups) 4-17
Fix a Live Device Configuration (Restore) 4-20

Clean Up the Archive 4-22
Find Out What Changed on Live Devices 4-23
Software Images 4-24
Add New Images to the Repository 4-24
New Devices: Create an Image Baseline 4-25
Distribute Images and Make Sure They Will Work 4-27
What is Upgrade Analysis? 4-28
Distribute Images to Devices 4-28
Activate Cisco IOS Software Images 4-32
Perform Cisco IOS XR Software Package Operations 4-34
Clean Up the Repository 4-41
Configuration Audit 4-42
Manage Configuration Policies 4-43
Schedule Configuration Audit 4-44
View Configuration Audit Jobs and Audit Results 4-45
Global Settings and Administration 4-47
Change Configuration Archive Global Settings 4-48
Change Image Management Global Settings 4-53
Check the Processes 4-54
Manage Jobs 4-55
User Authentication and Authorization 4-55

CHAPTER 5 **Working with Prime Network Vision Maps** 5-1
User Roles Required for Working with Prime Network Vision Maps 5-2
Opening and Closing Maps 5-5
Creating and Deleting Maps 5-6
Creating New Maps 5-6
Deleting Maps from the Database 5-8
Adding and Removing NEs from Maps 5-9
Managing Maps 5-11
Selecting Map Viewing Options 5-12
Applying a Background Image 5-12
Using the Overview Window 5-14
Saving Maps 5-15
Finding NEs, Services, and Links, and Elements Affected by Tickets 5-15
Working with Aggregations 5-16
Grouping Network Elements into Aggregations 5-16
Viewing an Aggregation Thumbnail 5-16

Adding Elements to an Existing Aggregation 5-18
Ungrouping Aggregations 5-19
Viewing Multi Chassis Devices 5-19
Viewing Inter Rack Links 5-20
Viewing Inter Chassis Links 5-20
Working with Overlays 5-21
Applying an Overlay 5-22
Hiding and Viewing Overlays, and Removing Overlays from a Map 5-25
Filtering Links in a Map 5-25
Filtering Links During Map Creation 5-26
Filtering Links in an Existing Map 5-27
Opening the CPU Usage Graph 5-27
Communicating with Devices Using Ping and Telnet 5-28

CHAPTER 6 **Working with Links** 6-1
User Roles Required to Work with Links 6-1
What Are Dynamic and Static Links? 6-3
Link Discovery and Flickering Ethernet Topology Links 6-3
Viewing Link Properties 6-4
Viewing Link Properties in Prime Network Vision Maps 6-4
Viewing Link Properties in the Links View 6-8
Viewing Link Properties in the Link Properties Window 6-10
Link List Pane 6-11
Properties Pane 6-11
Ticket and Events Pane 6-12
Viewing Link Impact Analysis 6-12
Adding Static Links 6-15
Filtering Links Using the Collection Method 6-17
Selecting a Link 6-18

CHAPTER 7 **Labeling NEs Using Business Tags** 7-1
User Roles Required to Work with Business Tags and Business Elements 7-1
Using Chinese Characters 7-2
Attaching and Detaching Business Tags 7-3
Searching for Business Tags and Viewing Their Properties 7-4
Renaming a Business Element 7-7
Deleting a Business Element 7-7

CHAPTER 8 **Working with the Prime Network Events Client** 8-1

User Roles Required to Work with Prime Network Events 8-1
Launching Prime Network Events 8-2
Prime Network Events Window 8-2
Prime Network Events Toolbar 8-5
Prime Network Events Menu Bar 8-6
Prime Network Events Right-Click Options 8-7
Adjusting the Prime Network Events GUI Client Settings 8-8

CHAPTER 9 **Tracking Faults Using Prime Network Events** 9-1

User Roles Required to Work with Prime Network Events 9-1
Viewing Events and Tickets in Cisco Prime Network Events 9-2
All Tab 9-3
System Event Tabs 9-3
Audit Tab 9-3
Provisioning Tab 9-5
Security Tab 9-6
System Tab 9-6
Network Event Tabs 9-7
Service Tab 9-7
Syslog Tab 9-8
Ticket Tab 9-8
V1 Trap Tab 9-10
V2 Trap Tab 9-10
V3 Trap Tab 9-11
Viewing 3.6.x Tabs 9-12
Working with Cisco Prime Network Events 9-14
Viewing Event Properties 9-14
Viewing Ticket Properties 9-18
Refreshing Cisco Prime Network Events Information 9-21
Filtering Events 9-22
Defining Filters 9-23
Removing Filters 9-24
Exporting Displayed Data 9-25

CHAPTER 10 **Working with Tickets in Cisco Prime Network Vision** 10-1

What are Tickets? 10-1
User Roles Required to Work with Tickets in Prime Network Vision 10-1

Viewing Tickets and Network Events for Elements in a Map 10-3
Managing Tickets in the Tickets Tab 10-4
Understanding Ticket Status 10-6
Filtering Tickets by Network Element 10-8
Filtering Tickets by Criteria 10-8
Viewing Ticket Properties 10-10
Ticket Properties Toolbar 10-12
Details Tab 10-12
History Tab 10-13
Affected Parties Tab 10-14
Correlation Tab 10-17
Advanced Tab 10-18
Notes Tab 10-18
User Audit Tab 10-19
Managing Tickets 10-19
Finding Affected Elements 10-19
Acknowledging a Ticket 10-19
Clearing a Ticket 10-20
Removing a Ticket 10-20
Clearing and Removing Tickets 10-21
Impact Analysis in Prime Network 10-22
Status Values for Affected Parties 10-22
Accumulating Affected Parties 10-22
Accumulating the Affected Parties in an Alarm 10-23
Accumulating the Affected Parties in the Correlation Tree 10-23
Updating Affected Severity over Time 10-24

CHAPTER 11 **Working with Reports** 11-1
User Roles Required to Manage Reports 11-1
Using the Report Manager 11-4
Menu Options 11-6
Report Manager Toolbar 11-6
Navigation Tree 11-7
Content Pane 11-7
Right-Click Options 11-9
Report Categories 11-11
Events Reports 11-11
Inventory Reports 11-19
Network Service Reports 11-21

Generating Reports 11-23
Database Load and Report Generation 11-24
Report Generation Failure 11-24
Report Generation Canceled 11-24
Generating Reports from Report Manager 11-24
Generating Events Reports 11-24
Generating Inventory Reports 11-32
Generating Network Service Reports 11-35
Generating Reports from the Reports Menu 11-38
Generating Reports from Prime Network Vision 11-39
Scheduling Reports 11-39
Managing Reports 11-40
Managing the Maximum Number of Concurrent Reports 11-40
Viewing and Saving Reports 11-41
Renaming Reports 11-42
Sharing Reports 11-43
Moving Reports Between Folders 11-44
Deleting Reports 11-44
Viewing Report Properties 11-45
Defining Report Types 11-46
Managing Report Folders 11-46
Creating Folders 11-46
Moving Folders 11-47
Renaming Folders 11-47
Deleting Folders 11-48
Viewing Folder and Report Type Properties 11-48

CHAPTER 12 **Using Cisco PathTracer to Diagnose Problems** 12-1
User Roles Required to Work with Cisco PathTracer 12-1
Cisco PathTracer Overview 12-2
Launching Path Tracer 12-3
Cisco PathTracer Right-Click Menu Options 12-4
Starting a Path Trace 12-5
From the Map View 12-5
From Logical or Physical Inventory 12-7
Examples of Launching Cisco PathTracer 12-7
Viewing Path Traces in Cisco PathTracer 12-14
Menus 12-16
Toolbar 12-17

Trace Tabs 12-18
Paths Pane 12-18
Path Trace Pane 12-18
Right-Click Menu Options 12-19
Viewing Path Trace Details 12-20
Menus 12-22
Cisco PathTracer Details Window Toolbar 12-22
Path Trace Pane 12-23
Details Pane 12-25
Saving and Opening Cisco PathTracer Map Files 12-26
Saving Cisco PathTracer Counter Values 12-26
Rerunning a Path and Comparing Results 12-27
Viewing Q-in-Q Path Information 12-27
Viewing L2TP Path Information 12-28
Using Cisco PathTracer in MPLS Networks 12-29
Cisco PathTracer MPLS Start and Endpoints 12-30
Using Cisco PathTracer for CSC Configurations 12-31
Using Cisco PathTracer for Layer 3 VPNs 12-32
Using Cisco PathTracer for Layer 2 VPNs 12-32
Using Cisco PathTracer for MPLS TE Tunnels 12-33

CHAPTER 13 **Monitoring Carrier Ethernet Services** 13-1
User Roles Required to Work with Carrier Ethernet Services 13-2
Viewing CDP Properties 13-6
Viewing Link Layer Discovery Protocol Properties 13-8
Viewing Spanning Tree Protocol Properties 13-10
Viewing Resilient Ethernet Protocol Properties 13-14
Viewing HSRP Properties 13-17
Viewing Access Gateway Properties 13-19
Working with Ethernet Link Aggregation Groups 13-22
Viewing Ethernet LAG Properties 13-23
Viewing mLACP Properties 13-28
Viewing Provider Backbone Bridge Properties 13-31
Viewing EFP Properties 13-32
Connecting a Network Element to an EFP 13-37
Understanding EFP Severity and Ticket Badges 13-37
Viewing EVC Service Properties 13-39

Viewing and Renaming Ethernet Flow Domains 13-41
Working with VLANs and VLAN Overlays 13-44
Understanding VLAN and EFD Discovery 13-44
Understanding VLAN Elements 13-45
Switching Entities Containing Termination Points 13-49
Adding VLANs to a Map 13-49
Removing VLANs from a Map 13-52
Viewing VLAN Mappings 13-52
Working with Associated VLANs 13-54
Adding an Associated VLAN 13-54
Viewing Associated Network VLAN Service Links and VLAN Mapping Properties 13-56
Viewing VLAN Links Between VLAN Elements and Devices 13-57
Applying VLAN Overlays 13-60
Displaying or Hiding VLAN Overlays 13-61
Removing a VLAN Overlay 13-61
Viewing VLAN Service Link Properties 13-62
Viewing REP Information in VLAN Domain Views and VLAN Overlays 13-62
Viewing REP Properties for VLAN Service Links 13-63
Viewing STP Information in VLAN Domain Views and VLAN Overlays 13-65
Viewing STP Properties for VLAN Service Links 13-66
Viewing VLAN Trunk Group Properties 13-67
Viewing VLAN Bridge Properties 13-69
Using Commands to Work With VLANs 13-71
Understanding Unassociated Bridges 13-72
Adding Unassociated Bridges 13-72
Working with Ethernet Flow Point Cross-Connects 13-74
Adding EFP Cross-Connects 13-75
Viewing EFP Cross-Connect Properties 13-75
Working with VPLS and H-VPLS Instances 13-77
Working with VPLS and H-VPLS in Prime Network Vision 13-77
Adding VPLS Instances to a Map 13-78
Applying VPLS Instance Overlays 13-79
Viewing Pseudowire Tunnel Links in VPLS Overlays 13-81
Viewing VPLS-Related Properties 13-82
Viewing VPLS Instance Properties 13-83
Viewing Virtual Switching Instance Properties 13-84
Viewing VPLS Core or Access Pseudowire Endpoint Properties 13-86
Viewing VPLS Access Ethernet Flow Point Properties 13-88
Working with Pseudowires 13-89

Adding Pseudowires to a Map 13-89
Viewing Pseudowire Properties 13-92
Displaying Pseudowire Information 13-94
Viewing Pseudowire Redundancy Service Properties 13-95
Applying Pseudowire Overlays 13-97
Monitoring the Pseudowire Headend 13-99
Viewing the PW-HE configuration 13-101
Viewing PW-HE Configured as a Local Interface under Pseudowire 13-103
Viewing PW-HE Generic Interface List 13-103
Viewing PW-HE as an Associated Entity for a Routing Entity 13-104
Viewing PW-HE as an Associated Entity for a VRF 13-104
Working with Ethernet Services 13-104
Adding Ethernet Services to a Map 13-105
Applying Ethernet Service Overlays 13-106
Viewing Ethernet Service Properties 13-108
Viewing IP SLA Responder Service Properties 13-111
Viewing IS-IS Properties 13-113
Viewing OSPF Properties 13-116
Configuring REP and mLACP 13-118
Using Pseudowire Ping and Show Commands 13-119
Configuring IS-IS 13-120

CHAPTER 14 **Monitoring Carrier Grade NAT Properties** 14-1
User Roles Required to View Carrier Grade NAT Properties 14-2
Viewing Carrier Grade NAT Properties in Logical Inventory 14-2
Viewing Carrier Grade NAT Properties in Physical Inventory 14-5
Configuring CG NAT Service 14-6

CHAPTER 15 **Monitoring DWDM Properties** 15-1
User Roles Required to View DWDM Properties 15-1
Viewing DWDM in Physical Inventory 15-3
Viewing G.709 Properties 15-5
Viewing Performance Monitoring Configuration 15-11
Configuring and Viewing DWDM 15-15

CHAPTER 16 **Monitoring Ethernet Operations, Administration, and Maintenance Tool Properties** 16-1
User Roles Required to View Ethernet OAM Tool Properties 16-1

Ethernet OAM Overview 16-2
Viewing Connectivity Fault Management Properties 16-3
Viewing Ethernet LMI Properties 16-10
Viewing Link OAM Properties 16-14
Configuring CFM 16-18
Configuring E-LMI 16-21
Configuring L-OAM 16-22

CHAPTER 17 **Monitoring Y.1731 IPSLA Configuration** 17-1
Y.1731 Technology - An Overview 17-1
Y.1731 Performance Management Mechanisms 17-1
User Roles Required to Work with Y.1731 Probes 17-2
Working with Y.1731 IPSLA Configurations 17-2
Viewing the Y.1731 Probe Properties 17-2
Configuring Y.1731 Probes 17-4

CHAPTER 18 **IPv6 and IPv6 VPN over MPLS** 18-1
User Roles Required to Work with IPv6 and 6VPE 18-2
Viewing IPv6 Information 18-2

CHAPTER 19 **Monitoring MPLS Services** 19-1
User Roles Required to Work with MPLS Networks 19-1
Working with MPLS-TP Tunnels 19-4
Adding an MPLS-TP Tunnel 19-5
Viewing MPLS-TP Tunnel Properties 19-7
Viewing LSPs Configured on an Ethernet Link 19-11
Viewing LSP Endpoint Redundancy Service Properties 19-13
Applying an MPLS-TP Tunnel Overlay 19-16
Viewing VPNs 19-18
Viewing Additional VPN Properties 19-20
Managing VPNs 19-21
Creating a VPN 19-21
Adding a VPN to a Map 19-22
Removing a VPN from a Map 19-23
Moving a Virtual Router Between VPNs 19-23
Working with VPN Overlays 19-24
Applying VPN Overlays 19-24

Managing a VPN Overlay Display in the Map View 19-25
Displaying VPN Callouts in a VPN Overlay 19-25
Monitoring MPLS Services 19-26
Viewing VPN Properties 19-26
Viewing Site Properties 19-27
Viewing VRF Properties 19-27
Viewing VRF Multicast Configuration details 19-30
Viewing VRF Egress and Ingress Adjacents 19-31
Viewing Routing Entities 19-31
Viewing the ARP Table 19-34
Viewing the NDP Table 19-34
Viewing Rate Limit Information 19-36
Viewing VRRP Information 19-37
Viewing Label Switched Entity Properties 19-39
Multicast Label Switching 19-42
Viewing MP-BGP Information 19-45
Viewing 6rd Tunnel Properties 19-46
Viewing BFD Session Properties 19-47
Viewing Cross-VRF Routing Entries 19-49
Viewing Pseudowire End-to-End Emulation Tunnels 19-50
Viewing MPLS TE Tunnel Information 19-52
Configuring VRF 19-53
Configuring IP Interface 19-54
Configuring MPLS-TP 19-54
Locking/Unlocking MPLS-TP Tunnels in Bulk 19-55
Configuring MPLS-TE 19-57
Configuring MPLS 19-57
Configuring RSVP 19-58
Configuring BGP 19-59
Configuring VRRP 19-60
Configuring Bundle Ethernet 19-61

CHAPTER 20 **Viewing IP and MPLS Multicast Configurations** 20-1
IP and MPLS Multicast Configuration - An Overview 20-1
User Roles Required to View IP and Multicast Configurations 20-2
Viewing the Multicast Configurations 20-2
Viewing Multicast Node 20-2
Viewing Multicast Protocols 20-4

Viewing the Address Family (IPv4) Profile 20-4
Viewing the Address Family (IPv6) Profile 20-5
Viewing the IGMP profile 20-5
Viewing the PIM Profile 20-7
Multicast Label Switching 20-9
Multicast Routing Entities 20-10

CHAPTER 21 **Monitoring MToP Services** 21-1
User Roles Required to Work with MToP 21-1
Viewing SAToP Pseudowire Type in Logical Inventory 21-2
Viewing CESoPSN Pseudowire Type in Logical Inventory 21-3
Viewing Virtual Connection Properties 21-5
Viewing ATM Virtual Connection Cross-Connects 21-6
Viewing ATM VPI and VCI Properties 21-10
Viewing Encapsulation Information 21-11
Viewing IMA Group Properties 21-13
Viewing TDM Properties 21-16
Viewing Channelization Properties 21-17
Viewing SONET/SDH Channelization Properties 21-18
Viewing T3 DS1 and DS3 Channelization Properties 21-21
Viewing MLPPP Properties 21-26
Viewing MLPPP Link Properties 21-29
Viewing MPLS Pseudowire over GRE Properties 21-31
Network Clock Service Overview 21-34
Monitoring Clock Service 21-34
Monitoring PTP Service 21-37
Viewing Pseudowire Clock Recovery Properties 21-42
Viewing SyncE Properties 21-46
Applying a Network Clock Service Overlay 21-49
Viewing CEM and Virtual CEM Properties 21-50
Viewing CEM Interfaces 21-51
Viewing Virtual CEMs 21-51
Viewing CEM Groups 21-51
Viewing CEM Groups on Physical Interfaces 21-52
Viewing CEM Groups on Virtual CEM Interfaces 21-53
Configuring SONET 21-54
Configuring Clock 21-56
Configuring TDM and Channelization 21-59

Configuring Automatic Protection Switching (APS ) 21-61

CHAPTER 22 **Viewing and Managing SBCs** 22-1

User Roles Required to View SBC Properties 22-2

Viewing SBC Properties in Logical Inventory 22-3

Viewing SBC DBE Properties 22-4

Viewing Media Address Properties 22-4

Viewing VDBE H.248 Properties 22-5

Viewing SBC SBE Properties 22-5

Viewing AAA Properties 22-6

Viewing H.248 Properties 22-7

Viewing Policy Properties 22-7

Viewing SIP Properties 22-10

Viewing SBC Statistics 22-14

Configuring SBC Components 22-14

CHAPTER 23 **Monitoring AAA Configurations** 23-1

Supported Network Protocols 23-1

Viewing AAA Configurations in Prime Network Vision 23-2

Viewing AAA Group Profile 23-2

Viewing Dynamic Authorization Profile 23-3

Viewing Radius Global Configuration Details 23-4

Viewing AAA Configuration Details for an AAA group 23-5

Viewing Diameter Configuration Details for an AAA group 23-6

Viewing Radius Configuration Details for an AAA Group 23-7

Viewing Radius Accounting Configuration Details for an AAA group 23-7

Viewing the Radius Keepalive and Detect Dead Server Configuration Details for an AAA group 23-8

Viewing the Radius Authentication Configuration Details for an AAA group 23-9

Viewing the Charging Configuration Details for an AAA group 23-10

Viewing the Charging Trigger Configuration Details for an AAA group 23-11

Configuring AAA Group 23-12

CHAPTER 24 **Monitoring IP Pools** 24-1

Viewing the IP Pool Properties 24-1

Configuring IP Pool 24-3

CHAPTER 25 **Monitoring BNG Configurations** 25-1

Broadband Network Gateway (BNG) - An Overview 25-1

User Roles Required to Work With BNG 25-2

Working with BNG Configurations 25-3

View Broadband Access (BBA) Groups 25-3

View Subscriber Access Points 25-5

Diagnose Subscriber Access Points 25-6

View Dynamic Host Configuration Protocol (DHCP) Service Profile 25-7

View Dynamic Config Templates 25-9

Viewing the Settings for a PPP Template 25-11

Viewing Policy Container 25-12

Viewing QoS Profile 25-15

CHAPTER 26 **Monitoring Mobile Technologies** 26-1

User Roles Required to Work with Mobile Technologies 26-1

GPRS/UMTS Networks - An Overview 26-4

Working With GPRS/UMTS Network Technologies 26-6

Working with GGSN 26-6

Viewing GGSN Properties 26-7

Viewing Additional Characteristics of a GGSN 26-8

GGSN Commands 26-10

Working with GTPU 26-11

Viewing GTPU Properties 26-11

GTPU Commands 26-12

Working with APN 26-13

Viewing APN Properties 26-14

Viewing Additional Characteristics of an APN 26-18

APN Commands 26-23

Working with GTPP 26-23

Viewing GTPP Properties 26-24

Viewing Additional Characteristics of a GTPP 26-25

GTPP Commands 26-28

Working with EGTP 26-29

Viewing EGTP Properties 26-30

EGTP Commands 26-31

LTE Networks - An Overview 26-31

Working with LTE Network Technologies 26-32

Monitoring SAE-GW 26-33

Viewing SAE-GW Properties 26-33
Working with PDN-Gateway 26-34
Viewing P-GW Properties 26-35
P-GW Commands 26-35
Working with Serving Gateway 26-36
Viewing S-GW Properties 26-36
S-GW Commands 26-37
Viewing QCI-QoS Mapping 26-38
Viewing the Layer 2 Tunnel Access Concentrator Configurations 26-39
Monitoring the HRPD Serving Gateway 26-44
Basic Features of HSGW 26-45
Viewing the HSGW Configuration 26-46
Configuration Commands for HSGW 26-52
Viewing the MAG Configuration for HSGW 26-55
Viewing the Profile-QCI Mapping Details 26-56
Configuration Commands for MAG 26-57
Monitoring Home Agent (HA) 26-59
Viewing the Home Agent Configuration 26-59
Monitoring the Foreign Agent 26-65
Viewing the Foreign Agent Configuration Details 26-65
Configuration Commands for Foreign Agent 26-74
Monitoring Evolved Packet Data Gateway (ePDG) 26-77
IP Security (IPSec) 26-78
ePDG Security 26-78
Viewing the ePDG Configuration Details 26-84
Configuration Commands for ePDG 26-86
Monitoring Packet Data Serving Node 26-87
PDSN Configurations 26-87
Viewing the PDSN Configuration Details 26-88
Configuration Commands for PDSN 26-100
Viewing the Local Mobility Anchor Configuration 26-103
Viewing Operator Policies, APN Remaps, and APN Profiles 26-105
Viewing Operator Policies 26-106
Viewing APN Remaps 26-108
Viewing APN Profiles 26-110
Viewing Additional Characteristics of an APN Profile 26-114
Working with Active Charging Service 26-116
Viewing Active Charging Services 26-118
Viewing Content Filtering Categories 26-120
Viewing Credit Control Properties 26-120

Viewing Charging Action Properties 26-123
Viewing Rule Definitions 26-126
Viewing Rule Definition Groups 26-127
Viewing Rule Base for the Charging Action 26-128
Viewing Bandwidth Policies 26-130
Viewing Fair Usage Properties 26-131
ACS Commands 26-131
Configuring and Viewing Mobile Technologies 26-133

CHAPTER 27 **Monitoring Data Center Configurations** 27-1
User Roles Required to Work with Data Center Configurations 27-1
Virtual Port Channel (vPC) 27-2
Viewing Virtual Port Channel Configuration 27-4
Viewing vPC Configuration 27-5
Cisco FabricPath 27-6
Viewing Cisco FabricPath Configuration 27-7
Monitoring Cisco FabricPath Configuration 27-9
Virtualization 27-9
Viewing Virtual Data Centers 27-10
Viewing the Data Stores of a Data Center 27-11
Viewing the Host Servers of a Data Center 27-11
Viewing the Virtual Machines of a Data Center 27-14

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-9
Links A-9
Link Icons A-9
Link Colors A-10
Link Characteristics A-11
Severity Icons A-12
Buttons A-12
Prime Network Vision Buttons A-13
Table Buttons A-15
Link Filtering Buttons A-16

Prime Network Events Buttons **A-16**
Ticket Properties Buttons **A-17**
Report Manager Buttons **A-17**
Badges **A-18**
VNE Communication State Badges **A-18**
VNE Investigation State Badges **A-19**
Network Element Technology-Related Badges **A-20**
Alarm and Ticket Badges **A-21**

GLOSSARY

INDEX

# Preface

This guide describes Cisco Prime Network (Prime Network) 3.11. 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 xxiii
- Document Organization, page xxiv
- Conventions, page xxvi
- Related Documentation, page xxvii
- Obtaining Documentation and Submitting a Service Request, page xxvii


## Audience

The intended audience for this guide 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:

| Chapter and Title | Description |
|---|---|
| Chapter 1, “Setting Up Devices and Using the GUI Clients” | 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 and Managing NE 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, “Device Configurations and Software Images” | Describes the features that Change and Configuration Management provides, some initial setup tasks you must perform, and how to work with the GUI. |
| Chapter 5, “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 6, “Working with Links” | Describes how to view information about static and dynamic links using the Prime Network Vision user interface. |
| Chapter 7, “Labeling NEs Using Business Tags” | Describes how to manage and view Prime Network Vision business tags and business elements. |
| Chapter 8, “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 9, “Tracking Faults Using Prime Network Events” | Describes how to use Prime Network Events to track faults. |
| Chapter 10, “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 11, “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 and Title | Description |
|---|---|
| Chapter 12, “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. |
| Chapter 13, “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 14, “Monitoring Carrier Grade NAT Properties” | Describes the Carrier Grade Name Address Translation (NAT) properties available in Prime Network Vision. |
| Chapter 15, “Monitoring DWDM Properties” | Describes how to view and monitor IP over dense wavelength division multiplexing (DWDM) properties in Prime Network Vision. |
| Chapter 16, “Monitoring Ethernet Operations, Administration, and Maintenance Tool Properties” | Describes how to use Prime Network Vision to monitor Ethernet operations, administration, and maintenance (OAM) tools. |
| Chapter 17, “Monitoring Y.1731 IPSLA Configuration” | Describes how to view Y.1731 IP Service Level Agreement (SLA) configurations for the OAM functionality in Ethernet networks. |
| Chapter 18, “IPv6 and IPv6 VPN over MPLS” | Describes how to use Prime Network Vision to view IPv6 and 6PVE properties. |
| Chapter 19, “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 chapter 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 20, “Viewing IP and MPLS Multicast Configurations” | Describes how to view multicast configurations and how Prime Network Vision supports multicast on MPLS and routing entities. |
| Chapter 21, “Monitoring MToP Services” | Describes Mobile Transport over Packet (MToP) services and how to view their properties in Prime Network Vision. |
| Chapter 22, “Viewing and Managing SBCs” | Describes the Session Border Controller (SBC) properties available in Prime Network Vision. |
| Chapter 23, “Monitoring AAA Configurations” | Describes how to view Authentication, Authorization, and Accounting (AAA) configuration, which is a security architecture for distributed systems that determines the access given to users for specific services and the amount of resources they have used. |

| Chapter and Title | Description |
|---|---|
| Chapter 24, “Monitoring IP Pools” | Describes how to view IP pool properties in Prime Network Vision. An IP pool is a sequential range of IP addresses within a certain network. Prime Network provides the flexibility of assigning IP addresses dynamically for services running on a network element. |
| Chapter 25, “Monitoring BNG Configurations” | Describes how to view Broadband Network Gateway (BNG) configuration in Prime Network Vision. |
| Chapter 26, “Monitoring Mobile Technologies” | Describes how to configure and view the mobile technologies in Prime Network Vision. |
| Chapter 27, “Monitoring Data Center Configurations” | Describes the Data Center components and how to view their configurations 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 guide 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. |

*Table 1 Conventions (continued)*

| Convention | Description |
|---|---|
| `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.

*Cisco Prime Network 3.11 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 *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

CHAPTER 1

# Setting Up Devices and Using the GUI Clients

These topics introduce you to the Cisco Prime Network GUI clients:


- Overview of the GUI Clients, page 1-1
- Setting Up Devices and Validating Device Information, page 1-2
- Using Prime Network with Prime Central, page 1-8


## Overview of the GUI Clients

Cisco Prime Network (Prime Network) provides the following GUI clients that offer an intuitive interface for managing your network and services, and for performing required system administration activities:


- Prime Network Vision, page 1-1
- Prime Network Events, page 1-2
- Prime Network Administration, page 1-2


### Prime Network Vision

Prime Network Vision is the main GUI client for Prime Network. Maps of devices create a visualization of the network, from the intricacies of a single device physical and logical inventory, to multi-layer topological information on connections, traffic, and routes. Faults and alarms are graphically displayed with built-in troubleshooting tools. Network elements and links using color cues and graphic symbols to indicate status and alarms.

All user actions are controlled by *user roles* and *device scopes*. Each user is assigned a role which controls the GUI actions the user can perform. When a user does not have the required permission level to perform a function, the appropriate menu option or button is disabled. Similarly, device scopes, which are named collections of managed network elements, control which devices a user can access. User roles and device scopes are controlled from the Prime Network Administration GUI client.

Prime Network Vision is also the launching point for these features.

| Feature | Provides this function: | Described in: |
|---|---|---|
| Path Tracer | Route tracing and performance | Chapter 12, "Using Cisco PathTracer to Diagnose Problems." |
| Change and Configuration Management | Manage software images and device configuration files | Chapter 4, "Device Configurations and Software Images" |

| Feature | Provides this function: | Described in: |
|---|---|---|
| Report Manager | Set up regular reports | Chapter 11, "Working with Reports." |
| Soft Properties Manager | Extend what is displayed in the GUI clients and monitored by Prime Network, and create new TCAs | *Cisco Prime Network 3.10 Customization Guide* |
| Command Builder | Create new device commands and add them to the GUI client | *Cisco Prime Network 3.10 Customization Guide* |
| Workflow | Create a series of sequential device tasks and add them to the GUI client | *Cisco Prime Network 3.10 Customization Guide* |
| Activation | Create wizards and add them to the GUI client | *Cisco Prime Network 3.10 Customization Guide* |

For more information on the Prime Network Vision GUI client, see Working with the Cisco Prime Network Vision Client, page 2-1.

### Prime Network Events

Prime Network Events is the interface used by system managers and administrators for viewing system events that occur in the network. You can use the GUI to retrieve detailed information about the different types of system events and tickets that are generated; it also helps predict and identify the sources of system problems. The GUI client also provides information about events within the Prime Network system. For more information, see Working with the Prime Network Events Client, page 8-1.

### Prime Network Administration

Prime Network Administration is the GUI client used to manage the Prime Network system, which is comprised of gateway servers, units, AVMs, and VNEs. These components work together to create the information model, which is constantly updated. Administrators use this GUI client to create user accounts, device scopes, polling groups, redundancy settings, and so forth. For information on this GUI client, see the *Cisco Prime Network 3.10 Administrator Guide*.

# Setting Up Devices and Validating Device Information

Prime Network provides a variety of management and configuration commands that you can launch from the Vision GUI client by right-clicking an NE and selecting **Commands**. These commands are executed on the actual physical device versus being performed on the network model that is stored in memory (and subsequently on the real device). This is useful to validate information displayed in a Prime Network GUI client against a device, using the device command line interface (CLI). Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands, if you have user permissions to do so.

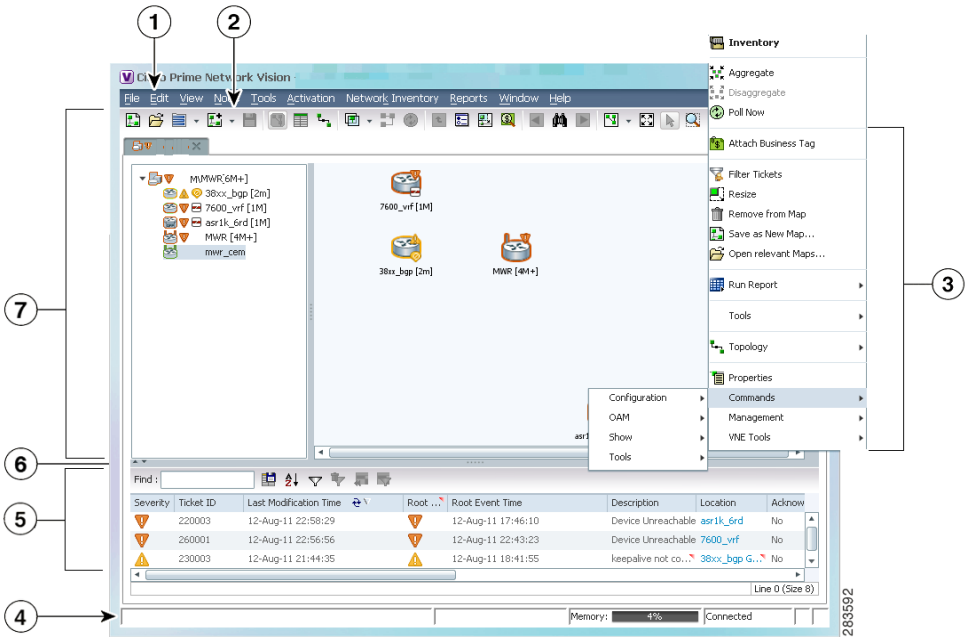
Prime Network also provides a variety of technology-specific commands—such as configuring the clock source for signals on SONET ports, enabling global ELM-I, enabling OAM on an interface. Whether you can use these commands depends on whether the technology is enabled on the device.

**Note** The basic operation commands in this chapter can be executed by all network elements that run on Cisco IOS software, Cisco IOS XR software, and Cisco NX OS software. You will not be able to execute these commands on network elements that have Cisco Catalyst OS software.

**Note** To view the basic operation commands in the Cisco Carrier Packet Transport (CPT) System, you must right-click the Cisco Carrier Packet Transport (CPT) System in the Prime Network Vision List or Map View and click **Logical Inventory > CPT Context Container**.

Figure 1-1 illustrates how to launch these commands.

***Figure 1-1 Launching NE Management and Configuration Commands***




| | | | |
|---|---|---|---|
| **1** | Menu Bar | **5** | Ticket Pane |
| **2** | Tool bar | **6** | Hide/display Ticket Pane |
| **3** | Device Right-click Menu | **7** | Navigation Pane |
| **4** | Status Bar | | |

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

These topics describe the available commands:

- Configure Basic Device Settings: Name, DNS, NTP, RADIUS, TACACs, ACLs, page 1-4
- Configure SNMP and SNMP Traps on Device, page 1-5
- Configure Device Ports and Interfaces, page 1-6
- View Device and VRF Routing Tables and Device Interface Briefs, page 1-7

- Ping Destinations and VRFs, and View Trace Route from Device, page 1-7
- Change Device Syslog Logging Level, page 1-8
- View, Copy, and Overwrite Device Configuration Files, page 1-8
- View Users (Telnet Sessions) on Device, page 1-8


# Configure Basic Device Settings: Name, DNS, NTP, RADIUS, TACACs, ACLs

Use the following commands to configure system-level settings on the real device. Unless otherwise noted, all of the following commands are launched by right-clicking the device and choosing **Commands > Configuration > System**.

### Configure the Device Host Name and DNS

| Command | Description |
|---|---|
| **Add Host Name**<br>**Remove Host Name** | Configures the device hostname.<br>**Note** Be sure to also apply any hostname changes to the device in Prime Network so that the name is also updated in the Prime Network model. |
| **DNS > Add DNS Server**<br>**DNS > Remove DNS Server** | Assigns the device to a Domain Name System (DNS) server to manage translating the hostname to and from the device IP address. |

### Configure a Device NTP Server

| Command | Description |
|---|---|
| **NTP > Add NTP Server**<br>**NTP > Remove NTP Server** | Assigns the device to a Network Time Protocol (NTP) server to manage clock synchronization. |

### Configure RADIUS or TACACS Server on Device

| Command | Description |
|---|---|
| **TACACS > Add Tacacs Server**<br>**TACACS > Remove Tacacs Server** | Assigns the device to a Terminal Access Controller Access-Control System (TACACS) server to manage authentication (uses TCP or UDP). |
| **TACACS+ > Add Tacacs+ Server**<br>**TACACS+ > Remove Tacacs+ Server** | Assigns the device to a TACACS+ server to manage authentication (uses TCP). |
| **RADIUS > Add Radius Server**<br>**RADIUS > Remove Radius Server** | Assigns the device to a Remote Authentication Dial In User Service (RADIUS) server to manage centralized authentication, authorization, and accounting (uses UDP). |

### Configure IP Access Control Lists (ACL) on Device

| Command | Navigation | Description | Supported On |
|---|---|---|---|
| Create Access List | *Right-click on a context* > **Commands** > **Configuration** | Use this command to create a new access list. | These commands are applicable only for ASR5000 and ASR5500 Modify Access devices. |
| Modify Access List<br>Delete Access List | Expand **Access List** node > *right-click an access list* > **Commands** > **Configuration** | Use these commands to modify/delete an access list. | |
| Show Access List | Expand **Access List** node > *right-click an access list* > **Commands** > **Show** | Use this command to view and confirm configuration details of an access list. | |

# Configure SNMP and SNMP Traps on Device

Use the following commands to configure SNMP settings and SNMP traps on the real device. All of the following commands are launched by right-clicking the device and choosing **Commands > Configuration > System**.

| Command | Description |
|---|---|
| **SNMP > Add SNMP Configuration**<br>**SNMP > Update SNMP Configuration**<br>**SNMP > Remove SNMP Configuration** | Configures SNMP on the device, including community settings, read-write access control, view-based access control, group settings, and so forth.<br>**Note** Be sure to also apply any SNMP configuration changes to the device in Prime Network so that the settings are also updated in the Prime Network model. |
| **SNMP > Add Traps**<br>**SNMP > Enable Traps**<br>**SNMP > Remove Traps** | Configures traps on the device (for example, improper user authentication, restarts, the closing of a connection, loss of connection to a neighbor router, and so forth). You can choose traps from a drop-down list. |

# Configure Device Ports and Interfaces

## Configure Device Ports

**Note** To apply description or status changes to an interface and port at the same time, use the interface commands listed in Configure Device Interfaces, page 1-6.

| Command | Navigation | Description |
|---|---|---|
| **Add / Remove / Update port description** | **Physical Inventory** > *navigate to port* > **Commands** > **Configuration** | Configures the descriptive information that is displayed in GUI clients when the port is selected. Examples are customer information or business case details.<br>**Note** Not supported on the Cisco Carrier Packet Transport (CPT) System. |
| **Change Port Status** | | Disables (Shutdown) or enables (No Shutdown) the port. An example is disabling (No Shutdown) a port in response to a fault so that the port will not generate further errors.<br>**Note** Not supported on the Cisco Carrier Packet Transport (CPT) System. |
| **Modify Port** | **Physical Inventory** > *Ethernet Slot* > *navigate to port* > **Commands** > **Configuration** | (Cisco ASR 5000 series only) Controls a variety of ASR 5000 port characteristics (bindings, contexts, link aggregations, and so forth). For more information, see the appropriate Cisco ASR 5000 documentation. |
| **Assign Port to Vlan**<br>**DeAssign Port To Vlan** | **Logical Inventory** > **Routing Entities** > **Routing Entity** > *interface* > **Commands** > **Configuration** | Controls a port's VLAN assignment. Enter a VLAN between 1-4094. When assigned, the port can communicate only with or through other devices in that VLAN. When deassigned, you can move a port to a new VLAN. |

## Configure Device Interfaces

| Command | Navigation | Description |
|---|---|---|
| **Add Interface Configuration** | **Physical Inventory** > *interface* > **Commands** > **Configuration** | Configures descriptive information that is displayed in GUI clients when the interface (or port) is selected. Examples are customer information or business case details. |

| Command | Navigation | Description |
|---|---|---|
| **Enable Interface**<br>**Disable Interface** | **Logical Inventory** > **Routing Entities** > **Routing Entity** > *interface* > **Commands** > **Configuration** | Disables or enables an interface (and port). An example is disabling an interface in response to a fault so that the interface will not generate further errors. |
| **Update Interface Configuration**<br>**Remove Interface Configuration** | | Changes or removes descriptive information that is displayed in GUI clients when the interface (or port) is selected. Examples are customer information or business case details. |
| **Add Loopback Interface** | **Logical Inventory** > **Routing Entities** > **Routing Entity** > **Commands** > **Configuration** | Configures a software-only interface that emulates an interface. If the virtual interface receives traffic, it immediately reroutes it back to the device. |

# View Device and VRF Routing Tables and Device Interface Briefs

### View Interface Briefs and IP Routes

| Command | Navigation | Description |
|---|---|---|
| **Show** > **IP Route** | **Logical Inventory** > **Routing Entities** > **Routing Entity** > **Commands** | Displays the device routing table. |
| **Show** > **VRF IP route** | **Logical Inventory** > **VRFs** > *VRF* > **Commands** | Displays the routing table of a selected VRF. |
| **Show** > **IP** > **Interface Brief** | *NE* > **Commands** | Lists all IP interfaces on the device. |

# Ping Destinations and VRFs, and View Trace Route from Device

| Command | Navigation | Description |
|---|---|---|
| **OAM** > **Trace Route from Device** | *NE* > **Commands** | Performs a traceroute to a destination address, showing how many hops were required and how long each hop takes. |
| **OAM** > **Ping** > **Destination From Device** | | Pings a specified IP address to see if the IP address is accessible. |
| **OAM** > **Traceroute VRF** | **Logical Inventory** > **VRFs** > *VRF* > **Commands** | Performs a traceroute from selected VRF to a destination address, showing how many hops were required and how long each hop takes. |
| **OAM** > **Ping VRF** | | Pings a specified VRF to see if the VRF is accessible. |

## Change Device Syslog Logging Level

| Command | Navigation | Description |
|---|---|---|
| **Syslog Host Logging** | *NE* > **Commands** > **Configuration** > **System** | Changes the syslog logging level to one of the following: alerts, critical, debugging, emergencies, errors, informational, notifications, warnings |

## View, Copy, and Overwrite Device Configuration Files

| Command | Navigation | Description |
|---|---|---|
| **Write memory** | *NE* > **Commands** > **Configuration** | Overwrites the startup-config file with the current running-config.<br>**Note** Not supported on Cisco IOS XR devices. |
| **Show > Running Config** | *NE* > **Commands** | Displays the contents of the device's current running-config (which can be different from the running-config on file). |
| **Show > Running Config from file** | | Displays the contents of the device's running-config file. |
| **Show > Startup Config** | | Displays the contents of the device's current startup-config. |
| **From FTP**<br>**From TFTP** | *NE* > **Commands** > **Tools** > **File copy**<br>**Note** Not supported on Cisco Carrier Packet Transport (CPT) System. | Copies the starting-config or running-config file from a remote source to a local location. The remote source is identified by its IP address. FTP requires the FTP username and password. |
| **To FTP**<br>**To TFTP** | | Copies a local configuration file to a remote destination's starting-config or running-config file. The remote destination is identified by an IP address. FTP requires the FTP username and password. |

## View Users (Telnet Sessions) on Device

| Command | Navigation | Description |
|---|---|---|
| **Users (Telnet Sessions)** | *NE* > **Commands** > **Show** | Provides details about the device's current Telnet sessions. |

# Using Prime Network with Prime Central

Prime Network can be installed as a standalone product or with Cisco Prime Central. When installed with Cisco Prime Central, you can launch Prime Network GUI clients from the Cisco Prime Portal. Cross-launch to and from other suite applications is also supported. The applications share a common inventory.

The Cisco Prime Portal uses a single sign-on (SSO) mechanism so that users need not reauthenticate with each GUI client. All session management features are controlled by the portal (such as client timeouts). If a user tries to log into a standalone GUI client, the user will be redirected to the portal login. The only exception is the emergency user, who will still be allowed to log into a standalone GUI client.

If the Cisco Prime Performance Manager application is also installed, the Prime Network Event Collector will receive threshold crossing alarm (TCA) events from Prime Performance Manager components and generate a ticket that you can view in Prime Network Events.

Prime Network also receives EPM-MIB traps from the network. By default Prime Network receives EPM-MIB traps from any source in the network. If desired, you can configure Prime Network to only process EPM-MIB traps arriving from a specific Prime Performance Manager server. The instructions for doing this are provided on the Cisco Developer Network at http://developer.cisco.com/web/prime-network/home.

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 Basic Operations in Prime Network Vision, page 2-1
- Launching Prime Network Vision, page 2-2
- Changing Your GUI Client Password, page 2-3
- The Prime Network Vision Window, page 2-3
- Prime Network Vision Status Indicators, page 2-16
- Prime Network Vision Toolbar, page 2-22
- Prime Network Vision Menu Bar, page 2-24
- Prime Network Vision Right-Click Menus, page 2-29
- Adjusting the Prime Network Vision GUI Client Settings, page 2-39
- Filtering and Sorting Tabular Content, page 2-40


## User Roles Required to Work with Basic Operations in 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 3.10 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 3.10 Administrator Guide*.

*Table 2-1 Default Permission/Security Level Required for the Basic 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 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.

- 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 information on Prime Central, see the Cisco Prime Central *User Guide*.
- Launch Prime Network Vision as a Standalone Application—Choose **Start > Programs > Cisco Prime Network >** ***gateway IP address*** **>** Cisco Prime Network Vision, and enter your username and password. If any client updates are available, Prime Network automatically installs them.

  If you see messages that say the server and client have different versions of the application, you need to update your client as described in the *Cisco Prime Network 3.10 Installation Guide*.

Once the GUI client is displayed, open an existing map or create a new one; see Working with Prime Network Vision Maps, page 5-1.

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 Adjusting the Prime Network Vision GUI Client Settings, page 2-39.

# Changing Your GUI Client Password

The method used to change your password depends on whether authentication is provided by Prime Network or an LDAP server. If you can see the **Tools > Change User Password** choice in the Prime Network Vision menu, the system is using authentication provided by Prime Network. You can change your password by entering the old and new passwords.

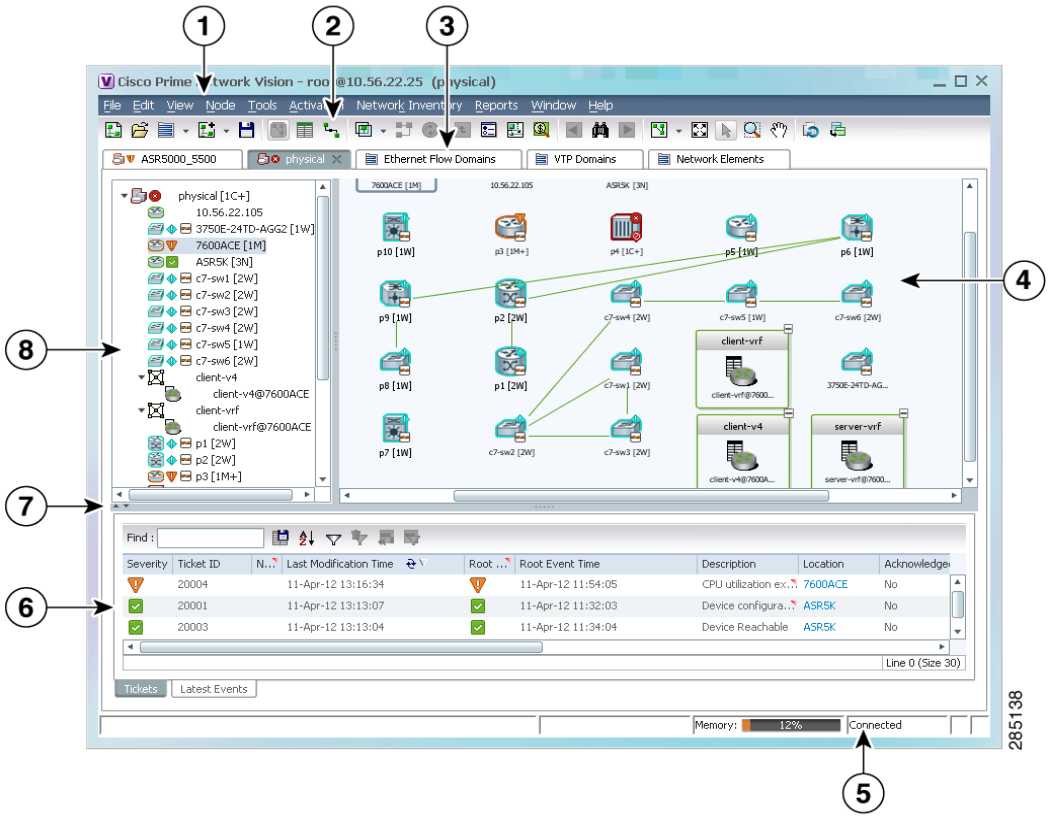
If the menu choice is disabled, the system is using an external authentication method. To change your password, contact your administrator. For more information about user authentication, see the *Cisco Prime Network 3.10 Administrator Guide*.

# The Prime Network Vision Window

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

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

*Figure 2-1 Prime Network Vision Window*




| | | | |
|---|---|---|---|
| **1** | GUI client menu bar | **5** | GUI client status bar (amount of memory used by client and gateway connection status) |
| **2** | GUI client toolbar | **6** | List of tickets on selected item |
| **3** | Active map and inventory tabs | **7** | Toggle to hide/display ticket pane |
| **4** | Map view (content pane) | **8** | Inventory window (navigation pane) |

# Prime Network Vision Inventory Tabs

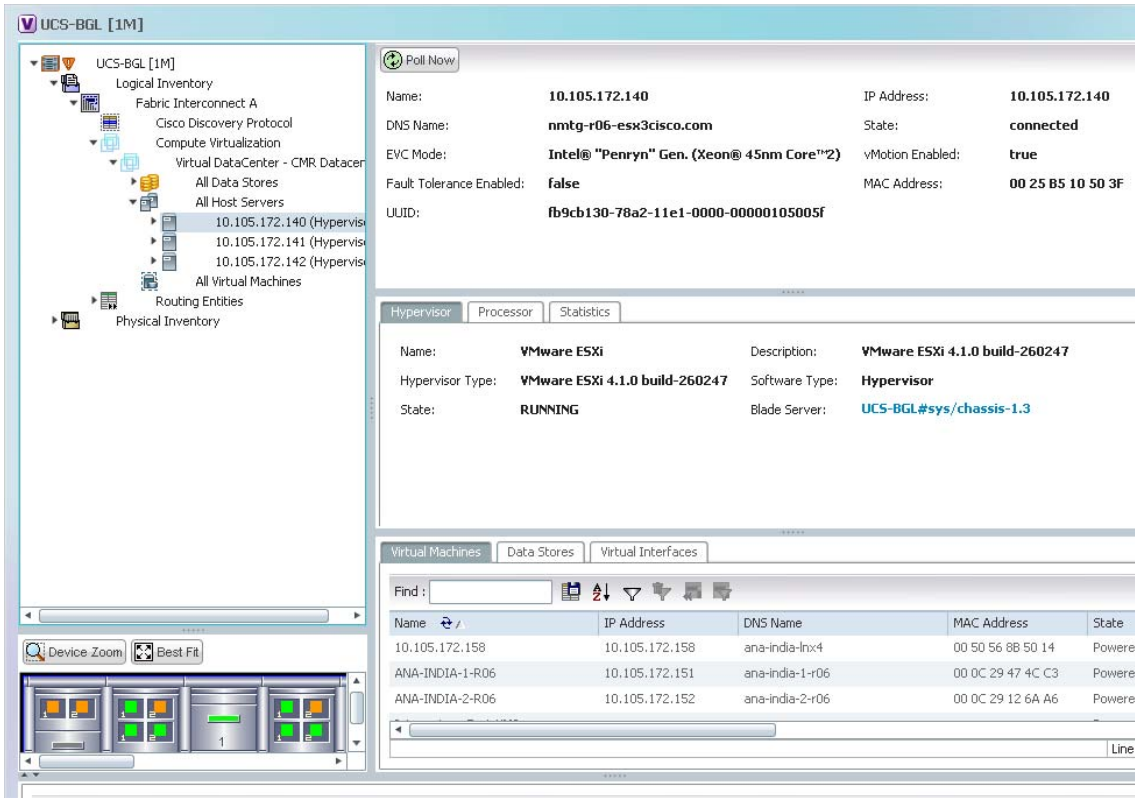
Prime Network Vision includes the following inventory tabs:

- Network Elements—Lists all network elements with the information described in Table 2-7, Network Element Information Displayed in List View. If there are tickets associated with the element, an icon is displayed. The color of the icon indicates the ticket severity.
- 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 13-41.
- VTP Domains—Lists all VTP domains. For more information about VTP domains, see Viewing VLAN Trunk Group Properties, page 13-67.

- Virtual Machines—Lists all the virtual machines. For more information about virtual machines, see Viewing the Virtual Machines of a Data Center, page 27-14. If there are tickets associated with the virtual machine, an icon is displayed. The color of the icon indicates the ticket severity.

To open an inventory tab, choose **Network Inventory** 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***




# Prime Network Vision Maps

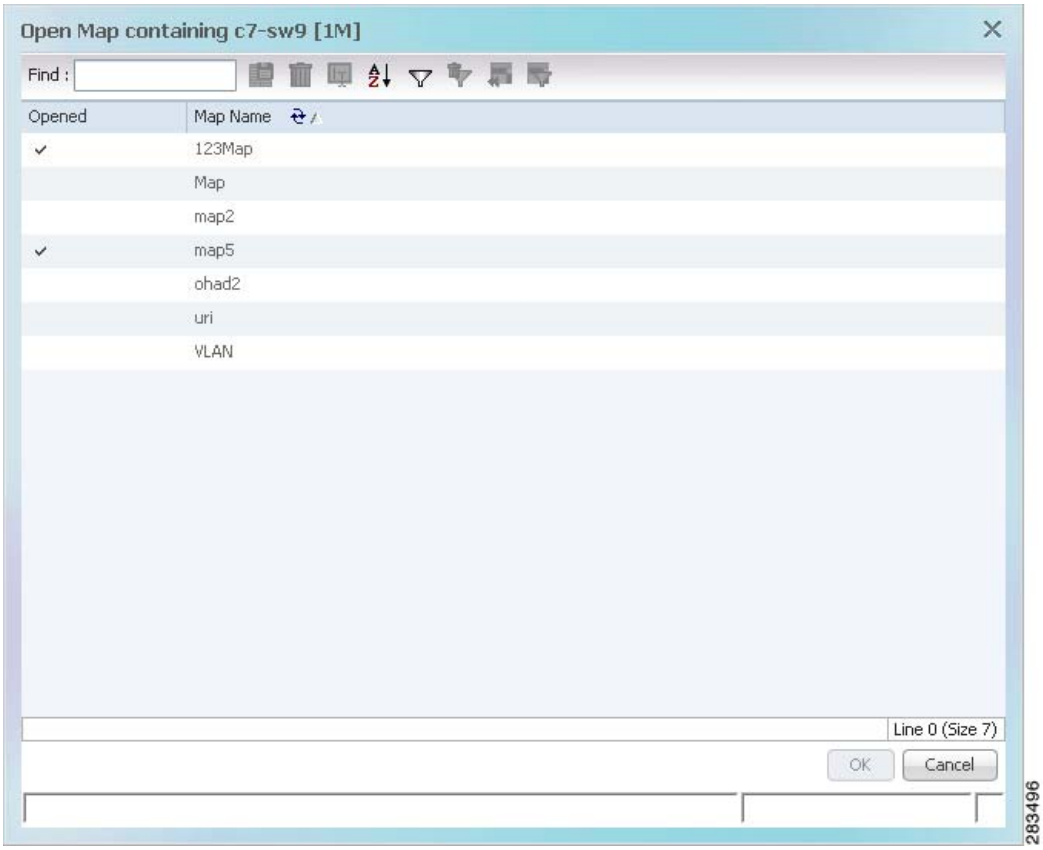
You can create as many maps as required to represent the network views you need. For example, maps can include specific network segments, customer networks, or the particular network elements and services that you require. Each map has three major areas:

- A tee-and-branch representation of the network elements and aggregations in the current map. For more information, see Navigation Pane, page 2-6.
- A large area showing the 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 2-7.
- A table of tickets associated with elements displayed in the map. For more information, see Ticket Pane, page 2-16.

## Opening Maps

You can open up to five maps at one time. To open a map, choose **File > Open Map**. The Open Map dialog box is displayed (see Figure 2-3).

***Figure 2-3 Open Map Dialog Box***




A check mark in the Opened column indicates that the map is already open. 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. For more information about maps, see Working with Prime Network Vision Maps, page 5-1.

You can open up to eight tabs at one time.

## Navigation Pane

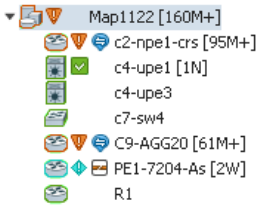
The navigation pane displays a tree-and-branch representation of the network elements and aggregations defined for the loaded map.

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 2-16.

## 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 2-7.
- 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 2-11.
- Links view—Displays a complete list of the links in the map view and their status. For more information, see Links View, page 2-14.

### 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 2-11.
  - 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

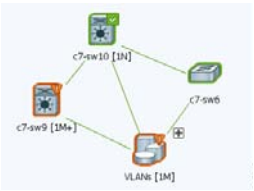
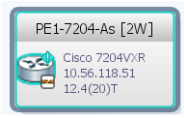
- Links
  - Service and business links are represented as well as physical and topological links.
  - Unidirectional links include arrowheads that indicate the direction of the flow, while bidirectional links do not have arrowheads.
- Relationships between network elements, aggregations, and networks

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 5, "Working with Prime Network Vision Maps."

## Element Icons

To view icons more easily, zoom in with your mouse. Four sizes are supported. Table 2-2 provides examples of each. For more details about data this is displayed, see Information Available in Element Icons, page 3-3.

***Table 2-2 Prime Network Vision Element Icon Sizes***

| Example Icon | Name and Description |
|---|---|
| | Tiny—Elements are displayed as dots. Alarm severity is indicated by colors. |
|   | Normal—Elements are displayed with icons and names. Alarms include badges. Alarm severity is represented by colors. |
|   | Large—Same as Normal, with additional NE properties. You can also perform cut-and-paste operations by pressing and dragging the mouse scroll wheel over the text. |
| | Huge—Same as Normal, with additional action buttons. |

Prime Network Vision also provides additional features for working with aggregations. For more information, see Working with Aggregations, page 5-16.

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 2-3, Network Element Icons
- Table 2-4, Business Element Icons

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

*Table 2-3 Network Element Icons*

| Icon | Network Element | Icon | Network Element |
|---|---|---|---|
| | Access pseudowire<br>Router | | Cloud |
| | ATM switch | | Digital subscriber line access multiplexer (DSLAM) |
| | Basic rate access (BRA) | | Ethernet switch |
| | Cisco 7600 series router | | Generic SNMP device |
| | Cisco ASR 1000 series router | | Ghost, or unknown device |
| | Cisco ASR 5000 series router | | ICMP device |
| | Cisco ASR 9000 series router | | Lock, or security violation; viewable by a user with a higher permission level |
| | Cisco CRS series router | | Missing icon or ghost NE (the NE was deleted and is no longer managed, or there is no icon for this NE) |
| | Cisco MWR 3941 | | Sun Netra server |
| | Cisco Nexus 1000 series devices | | Service control switch |
| | Cisco IOS XR 12000 series router | | WiFi element |
| | Cisco Unified Computing System (UCS) | | |

*Table 2-4 Business Element Icons*

| Icon | Business Element | Icon | Business Element |
|---|---|---|---|
| | Aggregation or root node | | Network Traffic Profile (TP) tunnel |
| | Backup pseudowire edge | | Network VLAN |
| | Connection termination point (TP)<br>Ethernet flow point (EFP)<br>MToP service | | Pseudowire edge |
| | EFP cross-connect | | Pseudowire switching entity |
| | Ethernet service | | Subnet |
| | Ethernet virtual connection (EVC) | | Switching entity |
| | Label-Switched Path (LSP) endpoint | | TP tunnel endpoint |
| | LSP midpoint | | VPLS forward |
| | Missing icon or ghost NE (the NE was deleted and is no longer managed, or there is no icon for this NE) | | VPLS instance |
| | Network LSP<br>Protected LSP<br>Working LSP | | VPN |
| | Network pseudowire | | |

## 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.

To reduce the number of graphical links in a map, click **Link Filter** in the toolbar, and uncheck the check boxes for the links you do not need to view.

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 6-4.

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

## Alarm Indicators

Table 2-5 shows the colors that are used to display the severity (or propagated severity) of a network element. The same coloring conventions apply to the link severities.

***Table 2-5 Severity Indicators***

| Icon | Color | Severity | Icon | Color | Severity |
|---|---|---|---|---|---|
| | Red | Critical | | Light Blue | Warning |
| | Orange | Major | | Medium Blue | Information |
| | Yellow | Minor | | Dark blue | Indeterminate |
| | Green | Cleared, Normal, or OK | | | |

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

## 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 2-29.

## 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 2-6, depending on the items included in the current map and the item selected in the navigation tree.

*Table 2-6 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. |
| 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 2-7 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 2-7 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. |

*Table 2-7 Network Element Information Displayed in List View (continued)*

| Field Name | Description |
|---|---|
| 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 3.10 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 3.10 Administrator Guide.* |
| Vendor | Vendor name. |
| Product | Network element category, such as Router or Eth-Switch (Ethernet switch). |
| 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.

See Filtering and Sorting Tabular Content, page 2-40 for more information about filtering, finding details about a network element in Prime Network Vision tables.

Table 2-8 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 2-8 List View Right-Click Options*

| Right-Click Option | Function | Related Documentation |
|---|---|---|
| Inventory | View network element inventory | The Inventory Window, page 3-9 |
| Poll Now | Poll the selected element | |
| Attach / Detach / Edit Business Tag | Configure and view business tag information | Chapter 7, "Labeling NEs Using Business Tags" |
| Config Mgmnt | View the Configuration Management page in Prime Network Change and Configuration Management | Chapter 4, "Device Configurations and Software Images" |
| Image Mgmnt | View the Image Management page in Prime Network Change and Configuration Management | Chapter 4, "Device Configurations and Software Images" |
| Run Report | Generate reports | Chapter 11, "Working with Reports" |
| Tools | Ping or telnet a VNE, or check VNE CPU usage | List View Right-Click Menu, page 2-35 |
| Topology | Configure the topology | Adding Static Links, page 6-15 |

*Table 2-8 List View Right-Click Options (continued)*

| Right-Click Option | Function | Related Documentation |
|---|---|---|
| Properties | View network element properties | Viewing the Properties of a Network Element, page 3-6 |
| Commands | Launch any of the commands that are included with Prime Network Vision | |
| Management | Access Command Builder and Soft Properties Management | *Cisco Prime Network 3.10 Customization Guide* |
| VNE Tools | Poll a VNE, or start or stop a VNE | Performing a Manual Device Poll, page 3-18 |

**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.

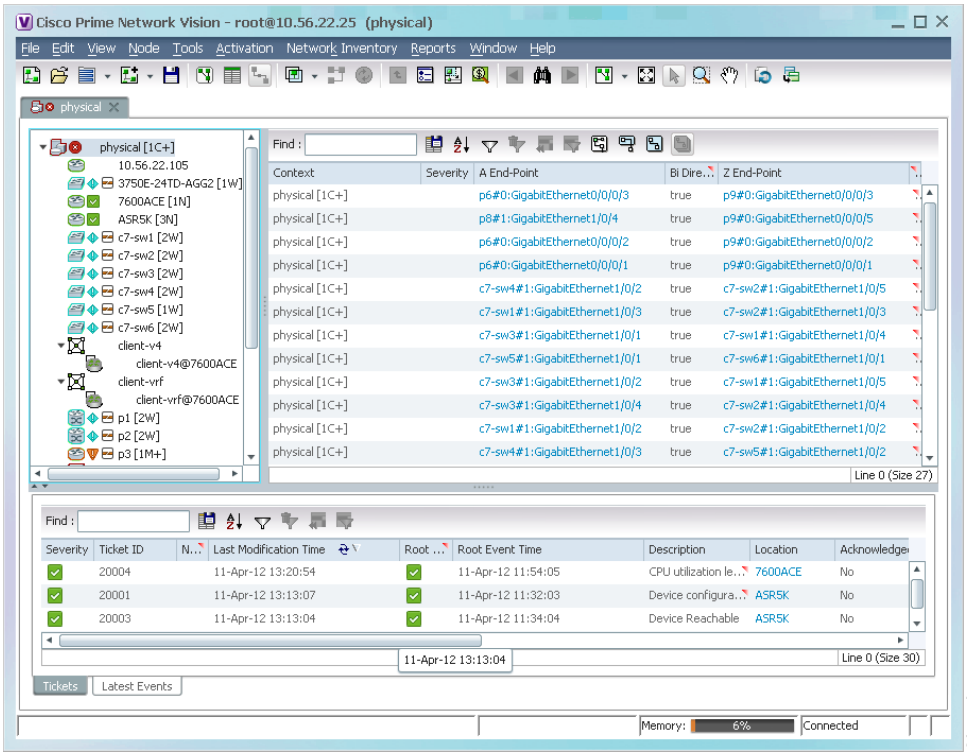
**Note** You can view and filter the links according to type by using the Link Filter dialog box. For more information, see Filtering Links in a Map, page 5-25.

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 6-8.

Table 2-9 describes the information that is displayed in the links view.

***Table 2-9 Information Displayed in the Links View***

| Field Name | Description |
|---|---|
| Context | Name of the map or aggregation containing the link.<br>This field can be empty for either of the following reasons:<br>• One side of the link is not included in the map.<br>• 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 2-7. |
| 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. |

*Table 2-9 Information Displayed in the Links View (continued)*

| Field Name | Description |
|---|---|
| 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. |

The links view toolbar includes the tools described in Table 2-10 and the link filtering buttons described in Table 2-10.

*Table 2-10 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 6-8.

For information about the right-click options available in the links view, see Links View Right-Click Menu, page 2-37.

## 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 10, “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 2-17
- VNE Management State, page 2-18
- Tickets, page 2-22

# 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 2-11.

### 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***

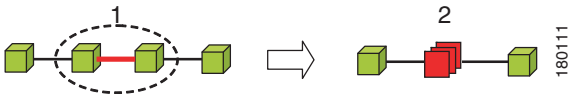



Figure 2-6 shows critical link 1 between two network elements in an aggregation. This critical link affects the severity of aggregation 2. That is, the aggregation is critical because it contains a link with a critical severity. Link severity affects the context.

***Figure 2-7 Link Severity Example 2***

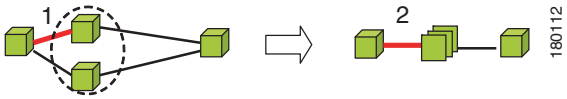



Figure 2-7 shows critical link 1 that forms part of a link aggregation. This affects the severity of link 2 because it contains a link with a critical severity.

### New Ticket Propagation

A new ticket indicates a new local fault or accumulates and propagates the number of new faults in its children.

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 alarms with the highest severity that have the source as the network element and are part of the network element ticket(s). |
| *s* | The highest severity level in the new tickets:<br>• C = Critical<br>• M = Major<br>• m = Minor<br>• W = Warning<br>• N = Normal (cleared alarm)<br>• 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 2-11.

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 2-8. For more information about severity colors, see Alarm Indicators, page 2-11.

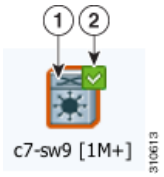
- An alarm badge is displayed on top of a managed element icon, and the color of the alarm badge indicates the severity of the highest severity ticket that is *not acknowledged* for the element. If all tickets are acknowledged, no alarm icon appears.

  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.

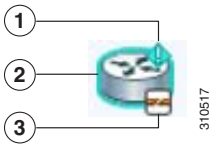
***Figure 2-8 Element with Ticket and Alarm Severity Indicators***




| | |
|---|---|
| **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 2-11 and Table 2-12 describe network element communication and investigation states and shows the related badge for each state.

***Table 2-11 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.<br>**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 3.10 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).<br>**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 3.10 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.<br>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 3.10 Administrator Guide*. | None |

***Table 2-12 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).<br>To extend Cisco Prime Network functionality so that it recognizes unsupported devices, use the VNE Customization Builder. See the *Cisco Prime Network 3.10 Customization Guide*. | |

*Table 2-12 VNE Investigation States (continued)*

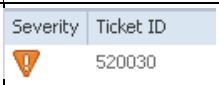
| State Name | Description | Badge |
|---|---|---|
| Discovering | The VNE is building the model of the device (the device type was found and is supported by Cisco Prime Network). A VNE remains in this state until all device commands are successfully executed at least once, or until there is a discovery 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 3.10 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:<br>• Does not poll the device, but handles syslogs and traps.<br>• Maintains the status of any existing links.<br>• Does not fail on VNE reachability requests.<br>• 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.<br>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.<br>To extend Cisco Prime Network functionality so that it recognizes unsupported modules, use the VNE Customization Builder. See the *Cisco Prime Network 3.10 Customization 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 3.10 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 2-5) 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 5-2.

Table 2-13 identifies the toolbar buttons and describes the functions that are available in the Prime Network Vision toolbar.

***Table 2-13 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. |
| **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). |

*Table 2-13 Prime Network Vision Toolbar (continued)*

| Button | Name | Function |
|---|---|---|
| | 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.<br>Available overlay options are:<br>• Ethernet Service<br>• MPLS-TP Tunnel<br>• Network Clock<br>• Pseudowire<br>• VLAN<br>• VPLS<br>• VPN<br>• 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.<br>**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.<br>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.<br>If no link filter is applied to the map, the Link Filter button is displayed instead. |
| | 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. |

*Table 2-13 Prime Network Vision Toolbar (continued)*

| Button | Name | Function |
|---|---|---|
| **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.<br>For more information, see the *Cisco Prime Network 3.10 Customization Guide.* |
| | Activation History | Opens the Activation History dialog box.<br>For more information, see the *Cisco Prime Network 3.10 Customization Guide.* |

# Prime Network Vision Menu Bar

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


- File Menu, page 2-25
- Edit Menu, page 2-26
- View Menu, page 2-26
- Node Menu, page 2-27
- Tools Menu, page 2-27
- Activation Menu, page 2-28
- Network Inventory Menu, page 2-28

- Reports Menu, page 2-29
- Window Menu, page 2-29
- Help Menu, page 2-29

**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 5-2. Also, the menus are context-sensitive and the options vary depending on your selection in the application.

# File Menu

Table 2-14 describes the options that are available in the Prime Network Vision File menu. For more information, see Chapter 5, "Working with Prime Network Vision Maps."

***Table 2-14 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:<br>• Cross Connect<br>• Ethernet Service<br>• MPLS-TP Tunnel<br>• Network Element<br>• Pseudowire<br>• Unassociated Bridge<br>• VLAN<br>• VPLS<br>• 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. |
| 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. |

*Table 2-14 File Menu Options (continued)*

| File Menu Option | Description |
|---|---|
| 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 2-15 identifies the options available in the Prime Network Vision Edit menu. For more information, see Chapter 5, "Working with Prime Network Vision Maps."

*Table 2-15 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.<br>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 2-16 identifies the options available in the Prime Network Vision View menu. For more information, see Using the Overview Window, page 5-14.

*Table 2-16 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. |
| 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 2-17 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 2-17 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 and Managing NE 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.<br>**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 and Managing NE Properties." |

# Tools Menu

Table 2-18 describes the Tools menu options.

*Table 2-18 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.<br>**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 Adjusting the Prime Network Vision GUI Client Settings, page 2-39. |

*Table 2-18 Tools Menu Options (continued)*

| Tools Menu Option | Description |
|---|---|
| Change and Config Mgmnt | Displays the Prime Network Change and Configuration Management dashboard.<br>For more information, see Chapter 4, "Device Configurations and Software Images." |
| Command Jobs | Displays all Command Builder jobs that have been scheduled and their details.<br>For more information, see the *Cisco Prime Network 3.10 Customization Guide.* |

# Activation Menu

See the *Cisco Prime Network 3.10 Customization Guide* for more information about any of the options in this menu.

Table 2-19 describes the Activation menu options.

*Table 2-19 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 2-20 describes the Network Inventory menu options.

*Table 2-20 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 2-4. |
| 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 13-41 |
| 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 13-67. |
| Virtual Machines | Displays a list of the available virtual machines in the Virtual Machines tab. For more information about virtual machines, see Viewing the Virtual Machines of a Data Center, page 27-14. |

## Reports Menu

Table 2-21 describes the Reports menu options.

*Table 2-21 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 11, "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 2-22 describes the Help menu options.

*Table 2-22 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 Setting Up Devices and Validating Device Information, page 1-2.

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 5-2.

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

- Map Right-Click Menu, page 2-30
- Element Right-Click Menu, page 2-31
- Aggregation Right-Click Menu, page 2-34
- Link Right-Click Menu, page 2-35
- List View Right-Click Menu, page 2-35
- Links View Right-Click Menu, page 2-37
- Ticket Right-Click Menu, page 2-38

# 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 2-23 describes the map right-click menu options.

***Table 2-23 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 5-12. |

# 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 2-24 describes the options available in the element right-click menu.

***Table 2-24 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 13-54. |
| 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 5, "Working with Prime Network Vision Maps."<br>**Note** You cannot aggregate service entities that exist within services. For example, you cannot aggregate VRFs that exist in a VLAN. |
| Attach / Detach / Edit Business Tag | Allows you to perform the following actions:<br>• Attach a business tag to the selected network element.<br>• Detach a business tag from a network element.<br>• Edit a business tag for a network element.<br>**Note** The Detach and Edit options are displayed only when a business tag is attached to a network element.<br>For more information, see Chapter 7, "Labeling NEs Using Business Tags." |
| Commands | Enables you to launch any of the commands that are included with Prime Network Vision.<br>For more information on the available commands and how to implement them, see Setting Up Devices and Validating Device Information, page 1-2. |
| Config Mgmnt | This option is available only if Prime Network Change and Configuration Management is installed.<br>Displays the Configuration Management page for the selected device in Prime Network Change and Configuration Management.<br>For more information, see Chapter 4, "Device Configurations and Software Images." |
| Delete | Deletes the selected item from the map. |

*Table 2-24 Element Right-Click Menu Options (continued)*

| Option | Description |
|---|---|
| Disaggregate | Ungroups the devices in the selected aggregation in the navigation and map panes. For more information, see Chapter 5, "Working with Prime Network Vision Maps."<br>**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.<br>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.<br>Displays the Image Management page for the selected device in Prime Network Change and Configuration Management.<br>For more information, see Chapter 4, "Device Configurations and Software Images." |
| 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 and Managing NE 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 3.10 Customization Guide.* |
| Management | Contains the following submenu options:<br>• Command Builder—Defines commands and scripts using the Prime Network Command Builder tool (Configurator security level required).<br>• 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).<br>For more information about Command Builder and Soft Properties Manager, see the *Cisco Prime Network 3.10 Customization 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. |

*Table 2-24 Element Right-Click Menu Options (continued)*

| Option | Description |
|---|---|
| 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 and Managing NE 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 Setting Up Devices and Validating Device Information, page 1-2. |
| Show as Aggregation / Thumbnail | Displays the selected aggregation as a single entity or as a collection of items.<br>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:<br>• CPU Usage—Displays memory and CPU usage information for a device or network element.<br>• Ping—Pings the device from the client station.<br>• Telnet—Communicates with the device using the Telnet window from the client station.<br>**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:<br>- For Windows 7 32-bit systems, enable the Windows Telnet Client to use the Prime Network Telnet option.<br>- For Windows 7 64-bit systems, a solution is available on the Cisco Developer Network at http://developer.cisco.com/web/prime-network/forums/-/message_boards/message/2780108. |

*Table 2-24 Element Right-Click Menu Options (continued)*

| Option | Description |
|---|---|
| Topology | The Topology option enables you to add:<br>• A static link between two devices.<br>• A static topology between a device and an unmanaged network.<br>• A tunnel to a VPN.<br>When working with static links, the following submenu options enable you to define the A Side and Z Side of the link:<br>• Mark as A Side<br>• Mark as Z Side<br>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:<br>• Poll Now—Updates the VNE information.<br>• Stop VNE—Stops the VNE.<br>• Start VNE—Starts the VNE.<br>For more information, see Chapter 3, "Viewing and Managing NE Properties." |

# Aggregation Right-Click Menu

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

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

*Table 2-25 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 5, "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 5, "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. |

*Table 2-25 Aggregation Right-Click Menu Options (continued)*

| Option | Description |
|---|---|
| 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.<br>The options toggle, depending on whether the aggregation is in a thumbnail or aggregated view. |
| Delete | Deletes the selected item.<br>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 6, "Working with Links."

Table 2-26 describes the link right-click menu options.

*Table 2-26 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 2-11.

Table 2-27 describes the list view right-click menu options.

*Table 2-27 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 and Managing NE Properties." |
| Attach / Detach / Edit Business Tag | Allows you to perform the following actions:<br>• Attach a business tag to the selected element.<br>• Remove a business tag from the selected element.<br>• Edit an existing business tag for the selected element.<br>**Note** The Detach and Edit options are available only when a business tag is attached to a link.<br>For more information, see Chapter 7, "Labeling NEs Using Business Tags." |

*Table 2-27 List View Right-Click Menu Options - Network Elements Tab (continued)*

| Option | Description |
|---|---|
| Config Mgmnt | Displays the Configuration Management page for the selected device in Prime Network Change and Configuration Management.<br>For more information, see Chapter 4, "Device Configurations and Software Images." |
| Image Mgmnt | Displays the Image Management page for the selected device in Prime Network Change and Configuration Management.<br>For more information, see Chapter 4, "Device Configurations and Software Images." |
| 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. |
| Show All Rows | Displays all table rows that meet the current filtering criteria. |
| Tools | Contains the following submenu options:<br>• CPU Usage—Displays memory and CPU usage information for a device or network element.<br>• Ping—Pings the device from the client station.<br>• Telnet—Communicates with the device using the Telnet window from the client station.<br>**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:<br>- For Windows 7 32-bit systems, enable the Windows Telnet Client to use the Prime Network Telnet option.<br>- For Windows 7 64-bit systems, a solution is available on the Cisco Developer Network at http://developer.cisco.com/web/prime-network/forums/-/message_boards/message/2780108. |
| Topology | Enables you to add:<br>• A static link between two devices.<br>• A static topology between a device and an unmanaged network.<br>• A tunnel to a VPN.<br>When working with static links, the following submenu options enable you to define the A Side and Z Side of the link:<br>• Mark as A Side<br>• Mark as Z Side<br>When working with VPNs in VPN Service View, the Add Tunnel submenu option allows you define and configure tunnels. |

*Table 2-27 List View Right-Click Menu Options - Network Elements Tab (continued)*

| Option | Description |
|---|---|
| *Launch external applications* | Launches external applications or tools, such as an SSH client. See the *Cisco Prime Network 3.10 Customization 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 and Managing NE 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 Setting Up Devices and Validating Device Information, page 1-2. |
| *Script names* | Launches available activation and configuration scripts. This can include the commands documented in , page 3-36, and those you create using Command Builder (can be launched against multiple network elements). For more information, see the *Cisco Prime Network 3.10 Customization Guide.* |
| Management | Contains the following submenu options:<br>• Command Builder—Defines commands and scripts using the Prime Network Command Builder tool (Configurator security level required).<br>• 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).<br>For more information about Command Builder and Soft Properties Manager, see the *Cisco Prime Network 3.10 Customization Guide.* |
| VNE Tools | Contains the following submenu options:<br>• Poll Now—Updates the VNE information.<br>• Stop VNE—Stops the VNE.<br>• Start VNE—Starts the VNE.<br>For more information, see Chapter 3, "Viewing and Managing NE 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 6, "Working with Links."

Table 2-28 describes the links view right-click menu options.

*Table 2-28 Links View Right-Click Menu Options*

| Option | Description |
|---|---|
| Attach Business Tag | Attaches a business tag to the selected link. For more information, see Chapter 7, "Labeling NEs Using Business Tags." |
| Detach/Edit Business Tag | Detaches or edits a business tag from the selected link. For more information, see Chapter 7, "Labeling NEs Using Business Tags."<br>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. |
| 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 10, "Working with Tickets in Cisco Prime Network Vision."

Table 2-29 describes the ticket right-click menu options.

*Table 2-29 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.<br>**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.<br>**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. |

*Table 2-29 Ticket Right-Click Menu Options (continued)*

| Option | Description |
|---|---|
| Find Affected Elements | Finds any elements affected by the selected ticket:<br>• If only one element is affected, it is selected in the Prime Network navigation pane and content area.<br>• If multiple elements are affected, they are displayed in the Affected Elements window. |
| 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 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 10-10. |

# Adjusting the Prime Network Vision GUI Client Settings

Table 2-30 lists the options for changing the GUI client display and audio settings, and for controlling the startup view and event history. You can adjust these settings by selecting **Tools > Options** from the main menu.

*Table 2-30 Options for Changing Prime Network Vision GUI Client*

| Field | | Description |
|---|---|---|
| **Startup** | | |
| Load Workspace on Startup | Open to content pane on login. Check the box if you do *not* want to view the content pane when you log in. | |
| **Display Tab** | | |
| Preferences | Map Labels Font Size | Font size for map labels (26, 28, 30, 32, and 34; 30 is the default). |
| Severity | Show Severity Text (e.g. [3M+] | List severity levels in the navigation pane and maps, using the formula described in New Ticket Propagation, page 2-17. Check the box if you *do* want to see severity text. |
| | Show Acknowledged | View both acknowledged and unacknowledged alarms in the network element display name. Check the box if you do want to see both unacknowledged and acknowledged alarms. |
| | Show Propagated | View propagated alarms on the specific entity. Propagated alarms are those that occur on other NEs. Check the box if you *do* want to see propagated alarms. |
| Display Name | How NE name is displayed:<br>• Do not use Business Tag—Display NE name only<br>• Add Business Tag to name—Display NE name *and* business tag.<br>• Replace name with Business Tag—Display business tag only (when a subscriber is attached to a port, the subscriber name is also added) | |

*Table 2-30 Options for Changing Prime Network Vision GUI Client (continued)*

| Field | Description |
|---|---|
| **Audio Tab** | |
| Enable Audio Response for Alarm | Audio notification settings. Check the box if you *do* want a sound to be issued when an alarm is triggered. |
| Critical | The .wav file to use for critical alarms. |
| Major | The .wav file to use for major alarms. |
| Minor | The .wav file to use for minor alarms. |
| Loop Sound on Critical Alarm | If critical alarm sound should sound continuously when a critical alarm is triggered. Check the box if you *do* want a sound to play continuously. |
| **Events Tab** | |
| Events History Size in Hours | Maximum age of events to display in the Network Events and Provisioning Events tab in the inventory window (see Ticket and Events Pane, page 3-15). If you only want to see active events, enter 0 (zero). The default (6 hours) is controlled from the Prime Network Administration GUI client. |

# Filtering and Sorting Tabular Content

For tables with extensive data, you can view all of the information in a table cell by hovering your mouse cursor over the cell. These topics explain how to sort and filter tabular information.

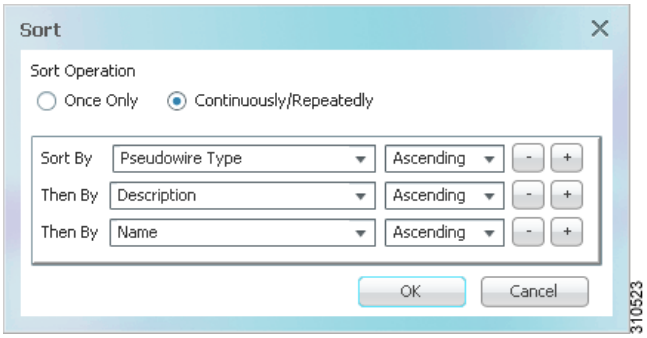
### Sorting Tables

Sorting a table lets you arrange existing data in various ways, while filtering a table only displays the information that matches the filter.

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 Tables

Filtering 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.

You can tell a table is being filtered if any filter details are displayed in the status line below the table or when you hover the mouse cursor over the filter button.

*Table 2-31 Table Toolbar Options*

| Option | Name | Description |
|---|---|---|
| | Filter | Filters the information displayed in the table by the criteria you specify.<br>For more information, see Filtering Tables, page 2-41. |
| | Clear Filter | Clears the existing filter. |

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.

**c.** The third field either lists the available values or allows you to enter text using a drop-down list or free text.

**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.

CHAPTER 3

# Viewing and Managing NE 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 3-1
- Information Available in Element Icons, page 3-3
- Viewing the Properties of a Network Element, page 3-6
- The Inventory Window, page 3-9
- Checking VNE Connectivity and Communication Status, page 3-16
- Viewing the Physical Properties of a Device, page 3-19
- Working with Ports, page 3-23
- Viewing the Logical Properties of a Network Element, page 3-27
- Viewing Device Operating System Information, page 3-31
- Running an Activation from the Activation Menu, 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 3.10 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 3.10 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 |
| Create activation wizards | — | — | — | — | — |
| Preview and perform activations and deactivations | — | — | — | — | — |
| View activation details and output | — | — | — | — | X |
| Search for activations | — | — | — | — | 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 |
| Create activation wizards | — | X | X | X | X |
| Preview and perform activations and deactivations | — | — | — | X | X |
| View activation details and output | X | X | X | X | X |
| Search for activations | — | 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 2-2. 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<br>• Number of Ethernet flow points | • Name in card title and body<br>• Number of Ethernet flow points |
| EFP cross-connect | Color representing the associated alarm severity | Name | Name in card title | Name in card title |

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

| Element Type | Icon Size | | | |
|---|---|---|---|---|
| | Tiny (Dot) | Normal | Large | Huge |
| Ethernet flow point | Color representing the associated alarm severity | Name | • Name in card title<br>• Type, such as Trunk, Access, Dot1Q Tunnel, and so on<br>• Match criteria | • Name in card title<br>• Type, such as Trunk, Access, Dot1Q Tunnel, and so on<br>• Match criteria |
| Ethernet service | Color representing the associated alarm severity | Name | • Name in card title<br>• Number of edge EFPs | • Name in card title<br>• Number of edge EFPs |
| EVC | Color representing the associated alarm severity | Name | • Name in card title<br>• Number of instances of domains (VPLS, EoMPLS, bridge, or cross-connect) with a maximum of three lines | • Name in card title<br>• 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<br>• Bandwidth | • Name in card title<br>• Bandwidth<br>• Attach Business Tag button<br>• Properties button |
| LSP Midpoint | Color | Name | • Name in card title<br>• Forward bandwidth<br>• Reverse bandwidth<br>• Reverse in and out labels | • Name in card title<br>• Forward bandwidth<br>• Reverse bandwidth<br>• Reverse in and out labels<br>• Attach Business Tag button<br>• Inventory button<br>• Properties button |
| MPLS-TP Tunnel | Color representing the associated alarm severity | Name | Name in card title and body | • Name in card title and body<br>• Attach Business Tag button<br>• Properties button |
| MPLS-TP Tunnel Endpoint | Color representing the associated alarm severity | Name | • Name in card title and body<br>• Tunnel identifier | • Name in card title and body<br>• Tunnel identifier<br>• Attach Business Tag button<br>• Inventory button<br>• Properties button |

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

| Element Type | Icon Size | | | |
|---|---|---|---|---|
| | Tiny (Dot) | Normal | Large | Huge |
| Network element | Color representing the associated alarm severity | Name | • Name in card title<br>• Element model<br>• IP address<br>• Software version | • Name in card title<br>• Element model<br>• IP address<br>• Software version<br>• Inventory button<br>• Filter Tickets button<br>• Attach Business Tag button |
| Pseudowire | Color representing the associated alarm severity | Name | Name in card title and body | • Name in card title and body<br>• Attach Business Tag button<br>• Properties button |
| Pseudowire edge | Color representing the associated alarm severity | Name | • Name in card title<br>• Local IP address<br>• Peer IP address | • Name in card title<br>• Local IP address<br>• Peer IP address<br>• Attach Business Tag button<br>• Inventory button<br>• Properties button |
| VLAN | Color representing the associated alarm severity | Name | Name in card title and body | • Name in card title<br>• Name in card body<br>• Number of switching entities<br>• Number of edge EFPs |
| VPLS | Color representing the associated alarm severity | Name | • Name in card title<br>• Number of access EFPs<br>• Number of access pseudowires<br>• Number of VPLS forwards | • Name in card title<br>• Number of access EFPs<br>• Number of access pseudowires<br>• Number of VPLS forwards |
| VPLS Forward | Color representing the associated alarm severity | Name | • Name in card title<br>• VPN identifier<br>• Number of core pseudowires | • Name in card title<br>• VPN identifier<br>• Number of core pseudowires |
| VPN | Color representing the associated alarm severity | Name | Name in card title and body | • Name in card title and body<br>• Attach Business Tag button<br>• 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.

**Step 1** To view general information about a network element, hover your mouse cursor over the NE icon, and use the mouse scroll to zoom in and out.

**Step 2** For more detail, open the Properties (inventory) window, double-click the icon.

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***

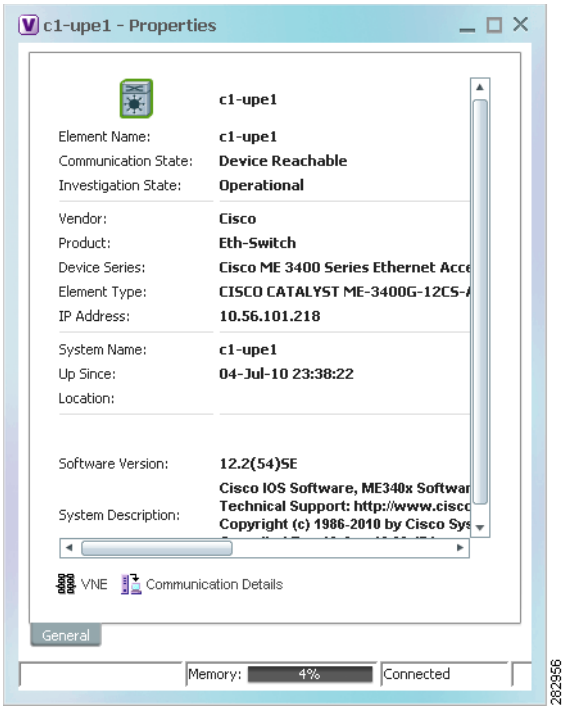



Table 3-4 describes the information displayed in both the Properties and inventory windows.

*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 2-16.<br>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 3.10 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 3.10 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 | Displays the VNE's general properties, from 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:<br>• VNE Properties Window (VNE Status Button in the content pane of the Inventory Window), page 3-16<br>• *Cisco Prime Network 3.10 Administrator Guide* |
| VNE Status | Displays details about the VNE's communication and connectivity, such as the status of device protocols and whether the device is sending traps and syslogs. For more information, see VNE Communication Status (VNE Details Button in the content pane of the Inventory Window), page 3-17. |

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 13-19 |
| | Blocking | The element associated with this badge has a REP alternate port. | Viewing REP Information in VLAN Domain Views and VLAN Overlays, page 13-62 |
| | Clock service | A clocking service is running on the associated element. | Applying a Network Clock Service Overlay, page 21-49 |
| | Lock | The associated network LSP is in lockout state. | Viewing MPLS-TP Tunnel Properties, page 19-7 |
| | 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 13-62 |

*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.<br>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 7-7 |
| | 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 13-62 |
| | REP primary | The element associated with this badge has a REP primary port. | Viewing REP Information in VLAN Domain Views and VLAN Overlays, page 13-62 |
| | Redundancy service | The element associated with this badge is a backup pseudowire or a protected LSP. | • Adding an MPLS-TP Tunnel, page 19-5<br>• Viewing Pseudowire Redundancy Service Properties, page 13-95 |
| | 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 13-65 |

# 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 6-15 |
| 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 3-23 |
| Open Cisco PathTracer and launch a path trace. | Using Cisco PathTracer to Diagnose Problems, page 12-1 |
| Open the Prime Network Command Builder to create customized commands. | *Cisco Prime Network 3.10 Customization Guide* |

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

| Task | Related Topic |
|---|---|
| Open the Prime Network Soft Properties Manager to extend the amount of information displayed. | *Cisco Prime Network 3.10 Customization Guide* |
| Check VNE properties and communication status when inventory is incomplete or missing | Checking VNE Connectivity and Communication Status, page 3-16 |
| View physical and logical inventory information. | • Viewing the Physical Properties of a Device, page 3-19<br>• 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 3-15 |

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:

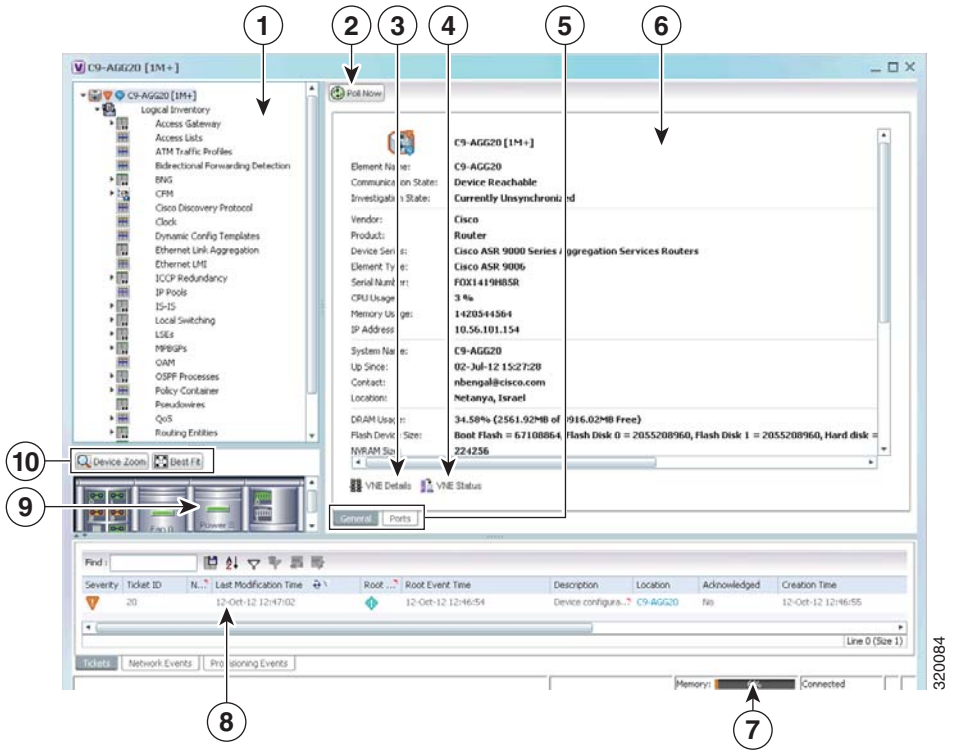
- Chapter 13, “Monitoring Carrier Ethernet Services”
- Chapter 14, “Monitoring Carrier Grade NAT Properties”
- Chapter 15, “Monitoring DWDM Properties”
- Chapter 16, “Monitoring Ethernet Operations, Administration, and Maintenance Tool Properties”
- Chapter 17, “Monitoring Y.1731 IPSLA Configuration”
- Chapter 18, “IPv6 and IPv6 VPN over MPLS”
- Chapter 19, “Monitoring MPLS Services”
- Chapter 20, “Viewing IP and MPLS Multicast Configurations”
- Chapter 21, “Monitoring MToP Services”
- Chapter 22, “Viewing and Managing SBCs”
- Chapter 23, “Monitoring AAA Configurations”
- Chapter 24, “Monitoring IP Pools”
- Chapter 25, “Monitoring BNG Configurations”
- Chapter 26, “Monitoring Mobile Technologies”
- Chapter 27, “Monitoring Data Center Configurations”

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 3-2 shows an example of an inventory window.

*Figure 3-2 Inventory Window*




| | | | |
|---|---|---|---|
| **1** | Navigation pane | **6** | Content pane |
| **2** | Poll Now button (see Performing a Manual Device Poll, page 3-18) | **7** | Status bar |
| **3** | VNE Details button (see VNE Properties Window (VNE Status Button in the content pane of the Inventory Window), page 3-16) | **8** | Ticket and events pane |
| **4** | VNE Status button (see VNE Communication Status (VNE Details Button in the content pane of the Inventory Window), page 3-17) | **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 3-12
- Device View Pane, page 3-13
- Device View Pane Toolbar, page 3-14
- Ticket and Events Pane, page 3-15
- Content Pane, page 3-13
- Checking VNE Connectivity and Communication Status, page 3-16

- Working with Ports, page 3-23

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, satellite, 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 2-16
- VNE Management State, page 2-18

## 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 2-18.

## 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 3-23.

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**.

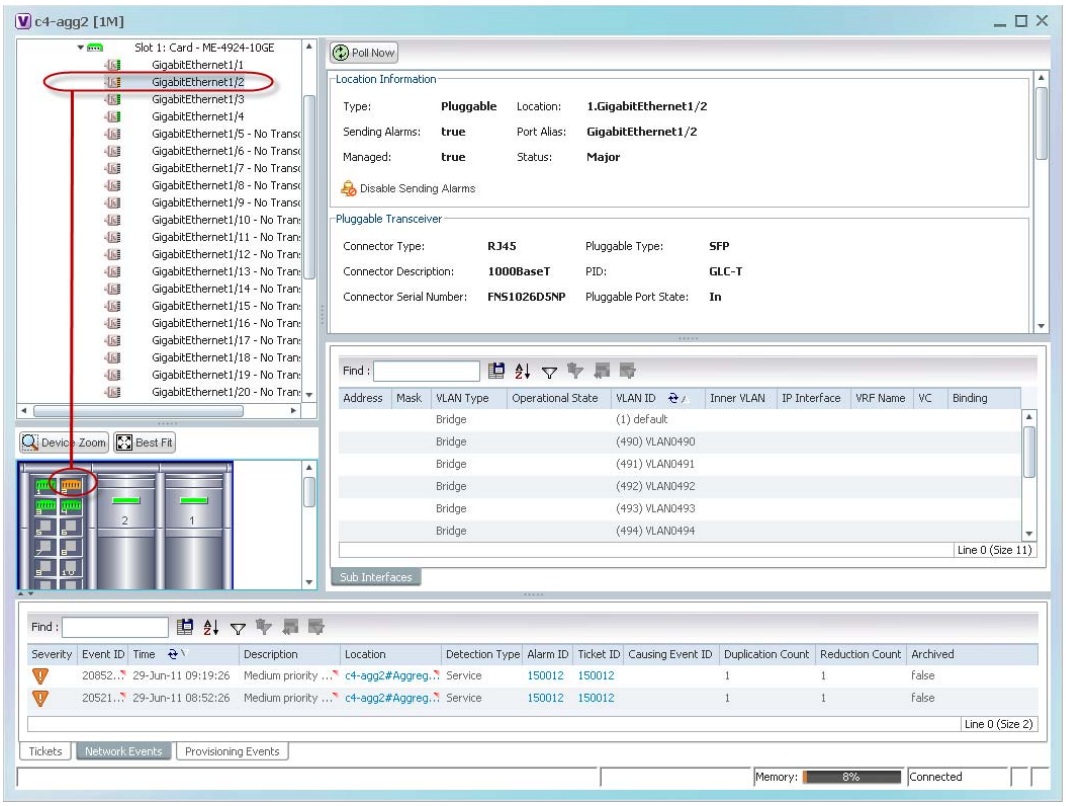
For information about tables that appear in the content pane, see Filtering and Sorting Tabular Content, page 2-40.

## 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 3-3 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 3-3 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 10-3 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 Adjusting the Prime Network Vision GUI Client Settings, page 2-39).

  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 Adjusting the Prime Network Vision GUI Client Settings, page 2-39).

  All activations that occur are also included in this tab.

  Table 9-4 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.

# Checking VNE Connectivity and Communication Status

Virtual Network Elements (VNEs) are the Prime Network entities that simulate managed devices. Each VNE is assigned to manage a single network element instance and is designated by the NE name and IP address.

VNEs are created using the Prime Network Administration GUI client. After a VNE is created and started, Prime Network investigates the network element and automatically builds a live model of it including its physical and logical inventory, configuration, and status. As different VNEs build their model, a complete model of the network is created.

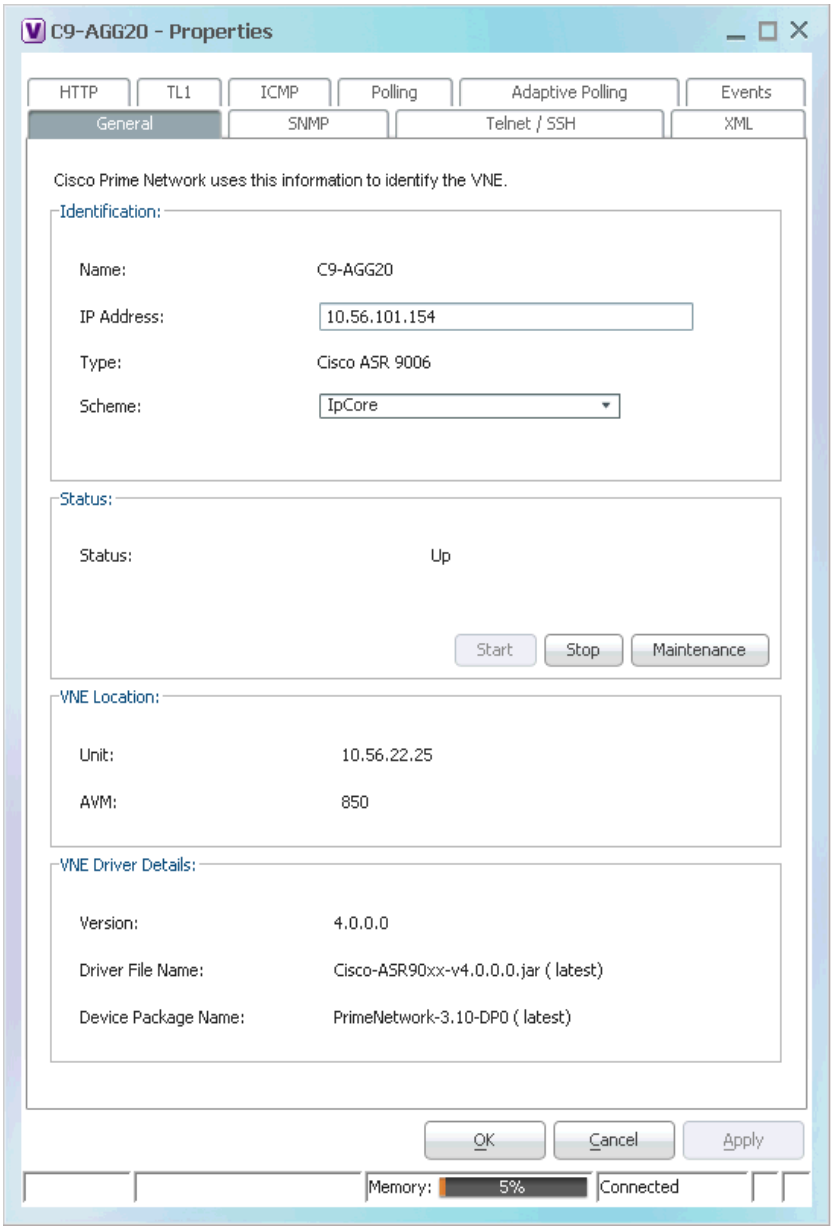
For the most part, VNE operations are hidden from Prime Network Vision GUI client users because those users are interested in devices, not these back-end processes. But VNEs must have connectivity to a device in order to maintain the NE model. To provide connectivity and polling information, you can view VNE properties from the device inventory:

- **VNE Status** to view the VNE Properties window. This window provides details such as the VNE's protocol and polling settings and other configuration information. See VNE Properties Window (VNE Status Button in the content pane of the Inventory Window), page 3-16.
- **VNE Details** to view more details about device and VNE connectivity. See VNE Communication Status (VNE Details Button in the content pane of the Inventory Window), page 3-17.

### VNE Properties Window (VNE Status Button in the content pane of the Inventory Window)

Figure 3-4 provides an example of a VNE properties window. This VNE is modeling a Cisco 3620 router.

*Figure 3-4 VNE Properties Window*



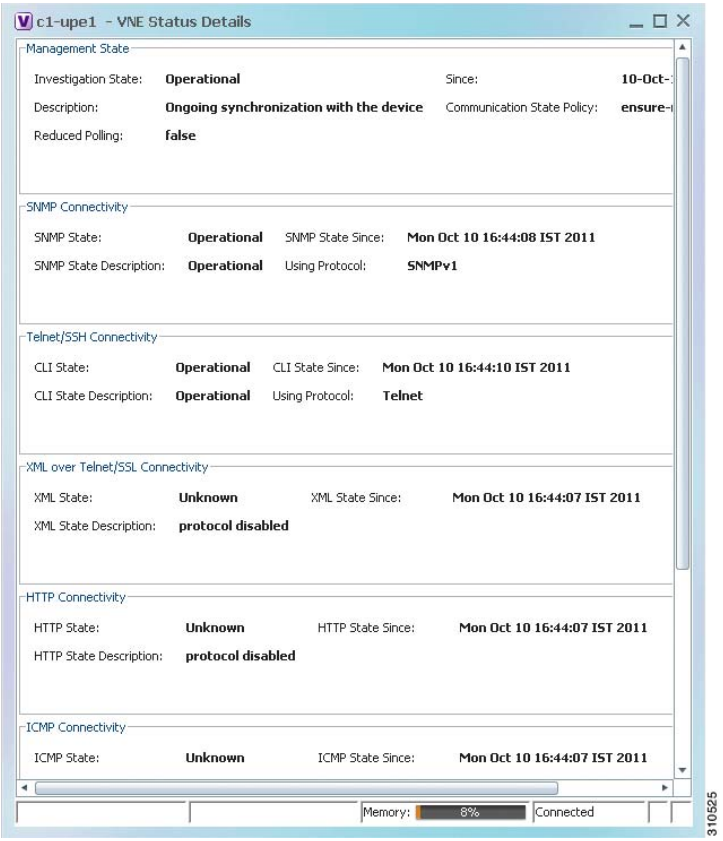

**Note** VNE status is not the same as device status. A device may be fully reachable and operating even though the VNE status is Down, Unreachable, or Disconnected.

The *Cisco Prime Network 3.10 Administrator Guide* describes these properties in detail, but for a Prime Network Vision GUI Client user, probably the most important information is the VNE status.

### VNE Communication Status (VNE Details Button in the content pane of the Inventory Window)

Figure 3-5 provides an example of a VNE Status Details window for a different VNE. This window provides information about the VNE and device connectivity.

*Figure 3-5 VNE Status Details Window*




The VNE Status Details window provides this information about the VNE:

- Its management connectivity state, which has to do with how the VNE was configured
- The protocols the VNE is using to communicate with the device and the status of each
- Whether the device is generating syslogs or traps

In the Management State area, if the Reduced Polling field is true and the Investigation State is Currently Unsychronized, refer to the information in the topic Performing a Manual Device Poll, page 3-18.

This information can be useful to users who are troubleshooting device problems. For more information about the VNE Status Details window, see the *Cisco Prime Network 3.10 Administrator Guide*.

### Performing a Manual Device Poll

The VNE settings determine how often a VNE polls a device to update its model. Some VNEs use the *reduced polling* (also called *event-based polling*) mechanism. A reduced polling VNE polls the device when a configuration change syslog is received and immediately updates the VNE information accordingly. In other words, updates are driven by incoming events.

The risk with reduced polling is dropped events. But if an event is dropped, the network element shows a Currently Unsynchronized investigation state. If you notice this VNE state, initiate polling by right-clicking the element and choosing **VNE Tools > Poll Now**.

For more information about reduced polling, see the *Cisco Prime Network 3.10 Administrator Guide*.

# 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, as shown in Table 3-8.

*Table 3-8 Physical Inventory Icons*

| Icon | Device |
|---|---|
| | Chassis |
| | Satellite |
| | Shelf |
| | Card/Subcard |
| | Port/Logical Port<br>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.

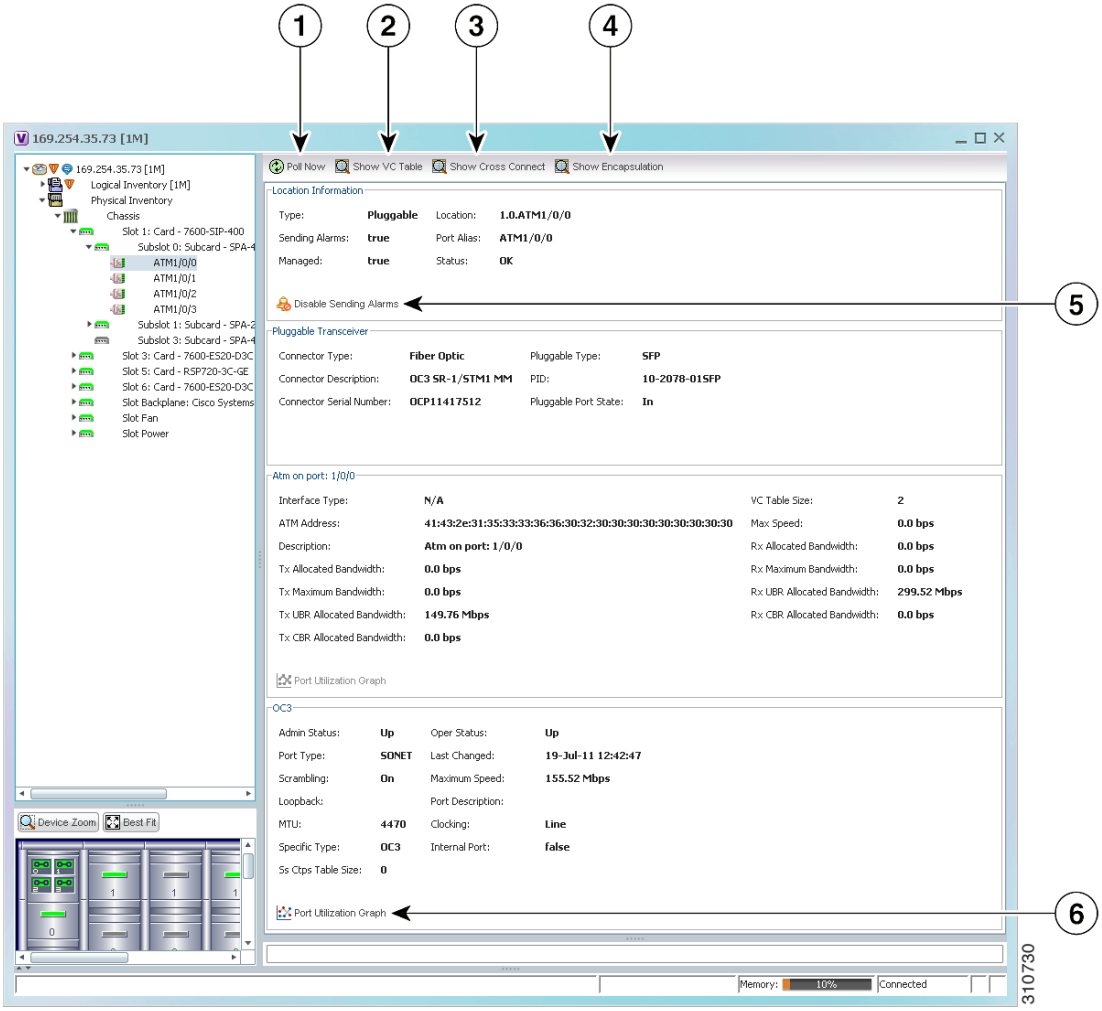
Fans and power supplies are displayed in physical inventory if they are field replacable units (FRUs). The manner in which the fans are displayed depends on whether the fans can be separated or not:

- 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.<br>For more information, see Performing a Manual Device Poll, page 3-18. |
| **2** | Show VC Table button | Displays virtual circuit (VC) information for the selected port.<br>For more information, see Viewing ATM VPI and VCI Properties, page 21-10. |
| **3** | Show Cross Connect button | Displays cross-connect information for incoming and outgoing ports.<br>For more information, see Viewing ATM Virtual Connection Cross-Connects, page 21-6. |
| **4** | Show Encapsulation button | Displays encapsulation information for incoming and outgoing traffic for the selected item.<br>For more information, see Viewing Encapsulation Information, page 21-11. |
| **5** | Disable Sending Alarms button | Enables you to manage the alarms on a port.<br>For more information, see Working with Ports, page 3-23. |
| **6** | Port Utilization Graph button | Displays the selected port traffic statistics: Rx/Tx Rate and Rx/Tx Rate History.<br>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 6-15.

For a detailed description of device properties, see Viewing the Properties of a Network Element, page 3-6.

# Redundancy Support

In Prime Network, redundancy is modeled as part of the physical inventory. You can view the redundancy parameters including the following:

- Redundancy Configured—Indicates whether redundancy is configured for the Route Switch Processor (RSP) or Route Processor (RP) card. This parameter displays “Working” if redundancy is configured and “None” if it is not configured.
- Redundancy Status—Indicates the redundancy status of the RSP or RP card, which can be Active or Standby Mode.
- Redundancy Type—The type of redundancy, which can be Stateful or Stateless. This parameter is available only for Cisco ASR9000 and Cisco ASR903 series routers.

- Redundancy Info—Provides information about the redundancy technology that is configured. For example, Nonstop Routing (NSR), Stateful Switchover (SSO), or Route Processor Redundancy (RPR). This parameter is available only for Cisco ASR9000 and Cisco ASR903 series routers.

**Note** If SSO is configured, then the Redundancy type will be Stateful. If RPR is configured, then the Redundancy Type will be Stateless.

# Viewing Satellite Properties

Prime Network provides satellite support for Cisco Aggregation Service Router (ASR) 9000 series network elements. Satellites are used to enhance performance bandwidth of Cisco ASR 9000 network elements. Each satellite is modeled as a chassis in the physical inventory.

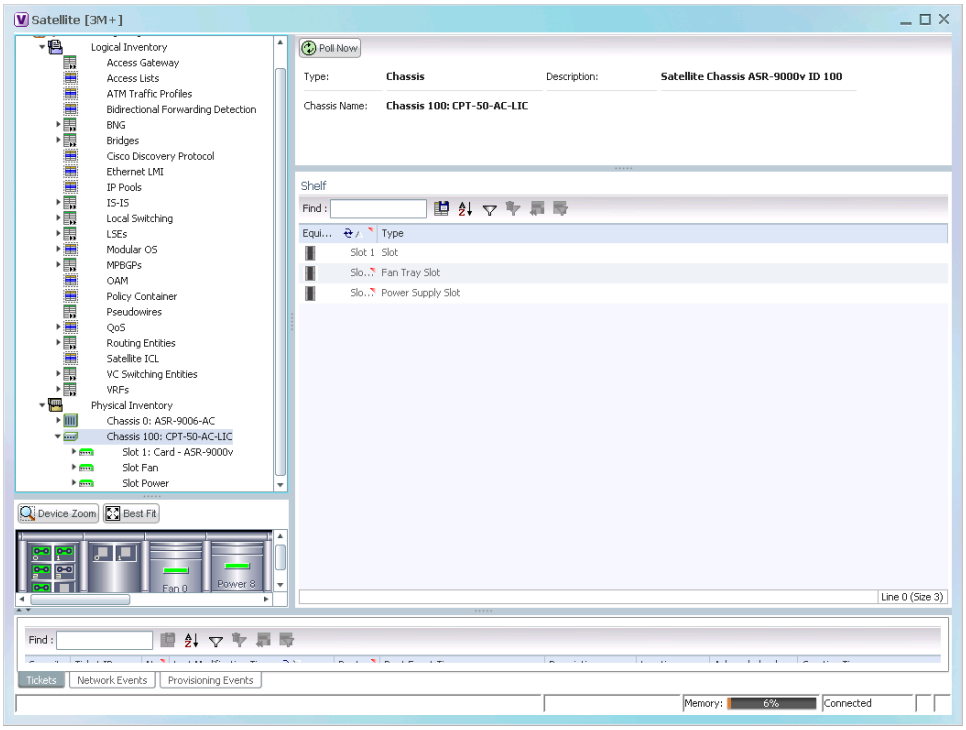
To view the satellite properties:

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

**Step 2** In the Inventory window, choose **Physical Inventory >** *Satellite*. Satellite is modeled as a type of chassis in the physical inventory.

Figure 3-7 shows an example of the information (including the slots) displayed when a satellite is selected in the physical inventory branch of the inventory window.

***Figure 3-7 Satellite Properties***



One or more satellites are connected to the host Cisco ASR 9000 series network element by using the physical ethernet links, which also act as inter-chassis links (ICLs) for connecting the satellites with the other chassis or satellites within the host.

To view the satellite ICLs, choose the **Satellite ICL** container in the logical inventory of the device. The content pane displays a list of satellite ICLs with the following details.

*Table 3-9 Satellite ICL Properties*

| Field | Description |
|---|---|
| Host Interface | Interface by which satellite is configured on the host network element. Click the hyperlink to view the interface properties in the physical inventory. |
| Satellite IC Interface | Inter-chassis interface used by the satellite. Click the hyperlink to view the satellite interface properties in the physical inventory. |
| Satellite ID | Satellite ID. Click the hyperlink to view the satellite properties in the physical inventory. |
| Satellite Port Range | Port associated with the satellite. |
| Satellite Status | Connection status of the satellite: Connected or Disconnected. |
| Fabric Link Status | Status of the fabric link connected to the satellite. |

# Working with Ports

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

- Viewing Port Status and Properties, page 3-23
- Viewing a Port Configuration, page 3-25
- Disabling and 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 and Enabling Alarms, page 3-26
- Generating the Port Utilization Graph, page 3-27

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

Figure 3-8 shows an example of the Ports tab in the inventory window.

*Figure 3-8 Ports Tab in the Inventory Window*

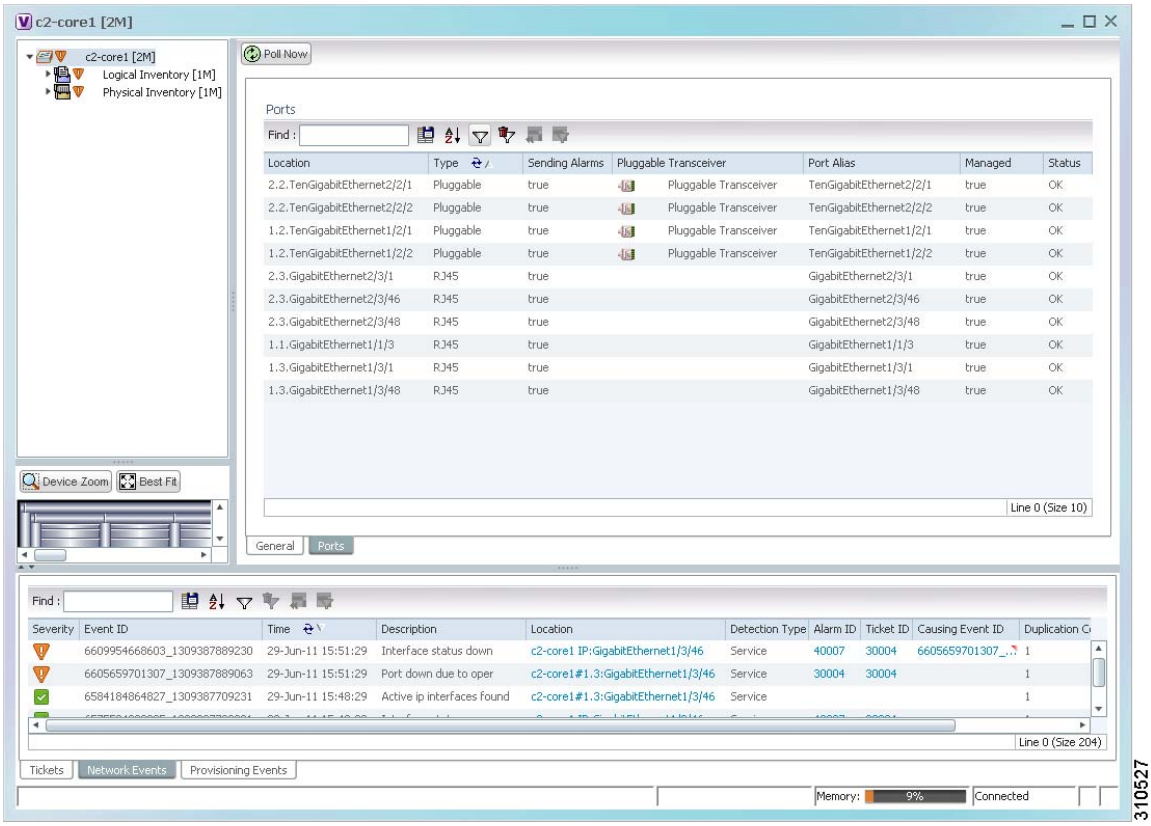



Table 3-10 describes the information that is displayed in the Ports tab.

*Table 3-10 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.

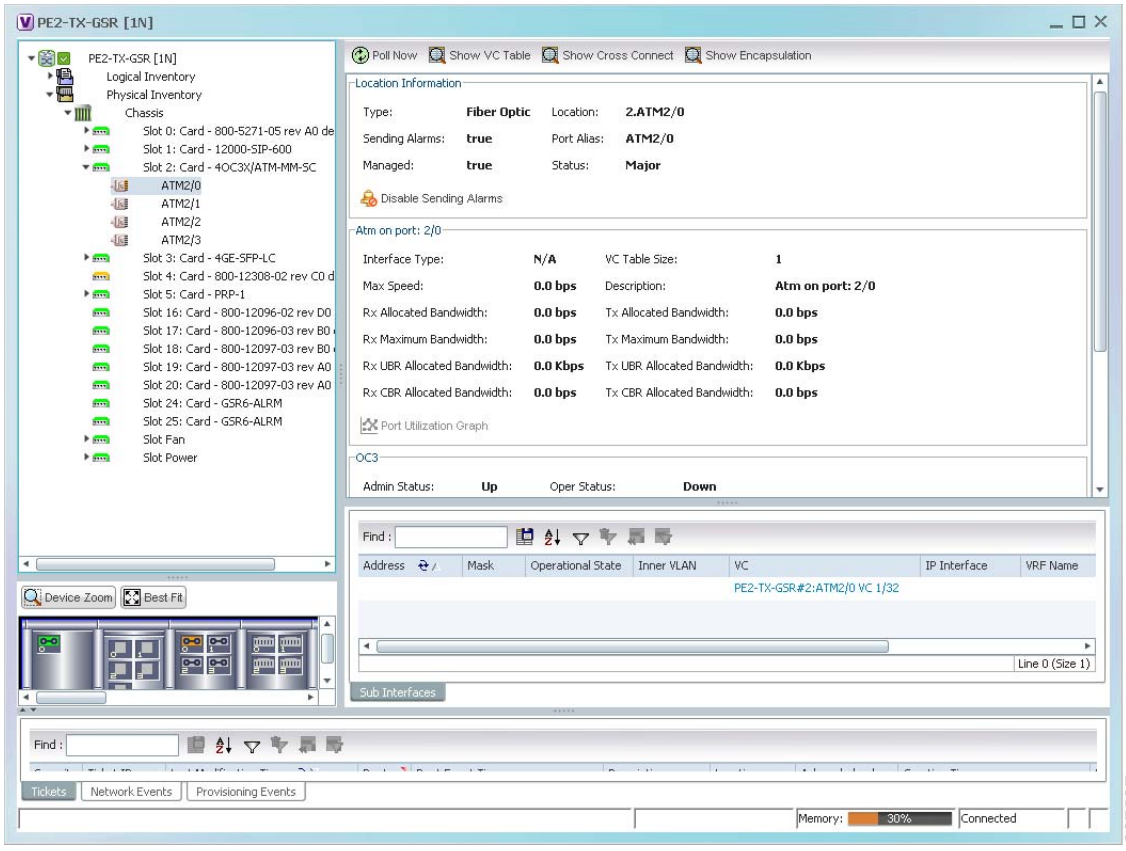
To view a port's configuration:

**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 3-9 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 3-9 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 3-11 describes the information that can be displayed in the Subinterfaces table. Not all fields appear in all Subinterfaces tables.

*Table 3-11 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.<br>Double-click the entry to view the Port IP VLAN Properties window containing:<br>• VLAN type<br>• VLAN identifier<br>• Operational status<br>• 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.<br>For more information about VC properties, see Viewing ATM Virtual Connection Cross-Connects, page 21-6. |
| 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 and Enabling 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, right-click the port and choose **Disable Sending Alarms**.

The Sending Alarms field displays the value *false*, indicating that the alarm for the required port has been disabled, and 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.

To enable alarms, use the previous procedure but choose **Enable Sending Alarms**.

## 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

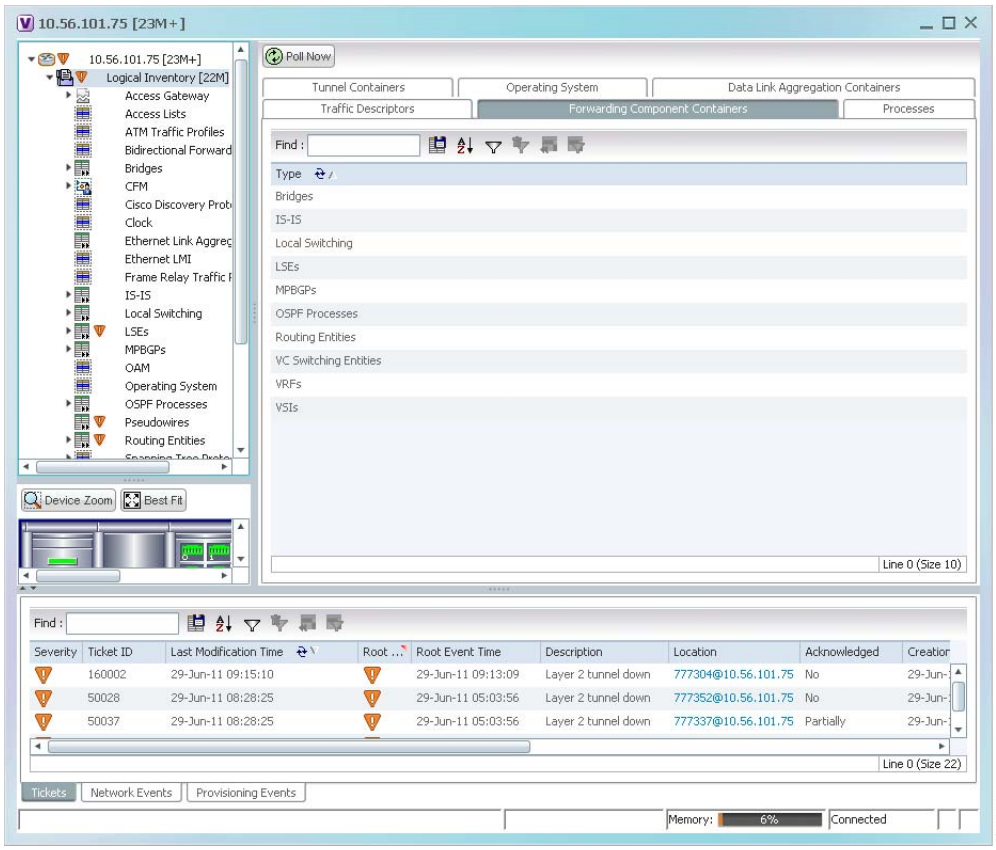
Prime Network Vision enables you to view logical inventory information. Prime Network Vision maintains logical inventory for each network element. The logical inventory reflects dynamic data such as configuration data, forwarding, and service-related components that affect traffic handling in the element.

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 3-10.

***Figure 3-10 Logical Inventory Information Displayed in the Inventory Window***




**Note** For more information about opening the inventory window, see The Inventory Window, page 3-9.

# Logical Inventory Navigation Pane Branches

Table 3-12 describes the branches that appear in the logical inventory navigation pane.

*Table 3-12 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 3-12 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 the status.

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

# 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. |
| 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 by clicking **Logical Inventory** and choose the **Operating System** tab. Table 3-14 describes the information that is displayed in the Operating System tab.

*Table 3-14 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.<br>This field applies to Cisco IOS XR devices only. |
| Software Version | Cisco IOS software version, such as 12.2(33)SRC3, Release Software (fc2). |

*Table 3-14 Operating System Information in Logical Inventory (continued)*

| Field | Description |
|---|---|
| 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 by opening the inventory window and choosing **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*

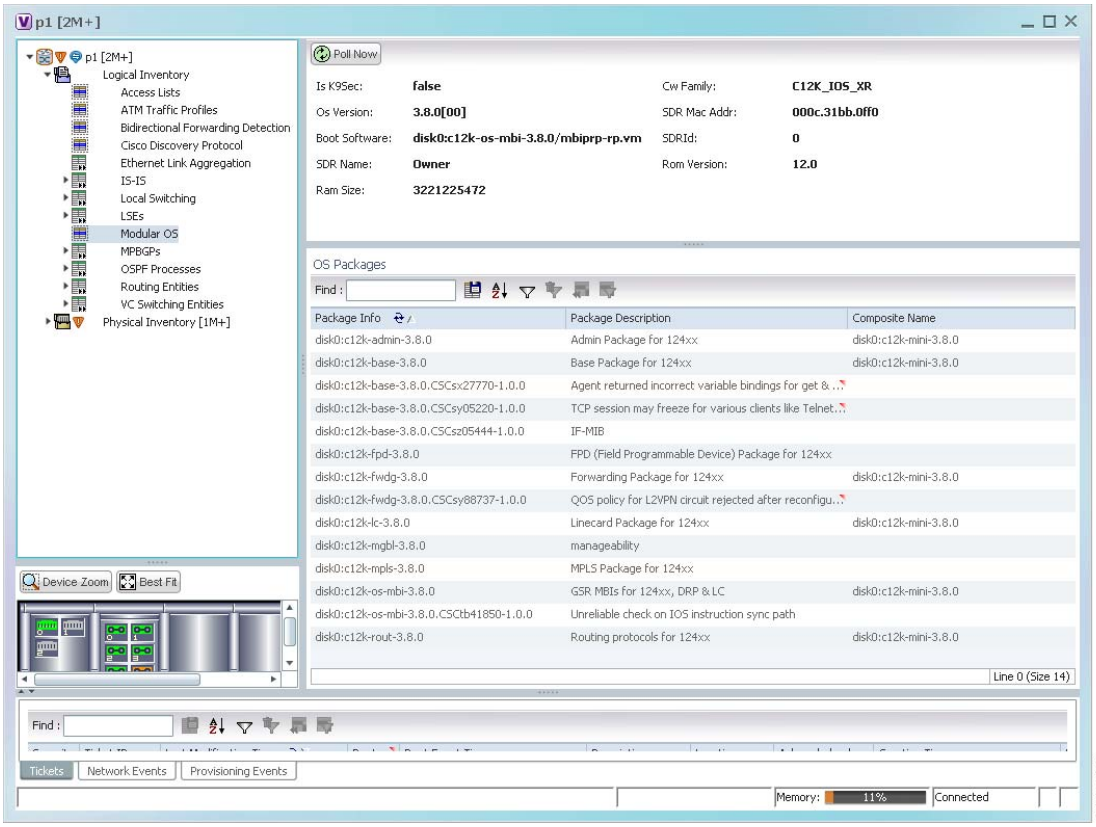



Table 3-15 describes the information that is displayed for Cisco IOS XR system.

*Table 3-15 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]. |

*Table 3-15 Modular OS Information in Logical Inventory (continued)*

| Field | Description |
|---|---|
| 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. |
| **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:<br>`Tues Feb 8 20:37:07.966 UTC`<br>`disk0:comp-hfr-mini-3.9.3.14` |

Table 3-16 describes the information that is displayed for modular operating systems in the Operating System tab.

*Table 3-16 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. |

# Running an Activation from the Activation Menu

You can run activation wizards from the GUI client using the Activations main menu. These are wizards that have been created using the Activation Wizard Builder (AWB), which is described in the *Cisco Prime Network 3.10 Customization Guide*. You can only run activations on devices that are within your device scope.

These topics describe how to run activations:


- Network Activation Window, page 3-34
- Running Activations, page 3-34
- Searching for Activations (Activation History), page 3-35
- Rolling Back an Activation, page 3-35
- Cloning an Existing Activation, page 3-36
- Deleting Activations, page 3-36


# Network Activation Window

Operators can access Activation wizards by launching them from the Activation menu in Prime Network Vision. The window is divided into the following parts.

| Activation Menu Choices | Description |
|---|---|
| Activation | Displays available activation wizards. From here operators can launch the wizards, enter the necessary information, and run the activation. |
| Activation History | Displays all the activations that have been executed. |
| Activation Modification Utility | Used by activation planners to download and upload wizard files.<br>**Tip** A best practice is to use the AWB to upload and download wizard files. |

# Running Activations

Activations can be launched from the Prime Network Vision GUI client.

**Note** The Cisco Developer Network (CDN) has some scripts that you can use as examples for using the framework. Other activation scripts are only available through Cisco Advanced Services.

**Step 1** From the Vision main menu, choose **Activation > Activation**. This opens a menu that lists the activations that the user can launch, depending on their user access role.

**Step 2** Expand the tree and highlight the activation wizard you want to launch, and click **Next**.

**Step 3** Enter all of the required data. You can only run activations on devices that are within your device scope.

**Step 4** Check your entries and preview your changes:

a. Click the User Input tab and check all of the values you entered.

b. Click the Preview Configuration tab, which displays and validates the CLI commands that will be run on the device. It also highlights any errors so that you can make corrections to your input.

**Step 5** Run the activation.

**Note** You might be prompted to enter your device access credentials. Once you have entered them, these credentials will be used for every subsequent activation in the same GUI client session. If you want to change the credentials, click **Edit Credentials**.

**Step 6** View the output:

a. Select the activation in the Activation History window, right-click and choose **Show Output**. The information presented in similar to the data displayed in Step 4 except it reflects the real runtime results.
   - Workflow Output—The sequence of commands that were run on the devices.
   - CLI Output—The actual CLI commands that were executed for the selected activation (for activations with an **Add** operation and a **Done** state).

b. If you want to view the output at a later time, export the activation to a local drive by clicking **Export to File**. We recommend that you do not change the file type in case you seek help from a support team.

# Searching for Activations (Activation History)

The Activation History window displays information about executed activations, even if the activations failed. The window displays a user-friendly search tools that allow you to locate specific activations and filter the results. A counter displays the total number of activations in the system.

Keep the following in mind when using the Activation History window:

- Searches are case-insensitive and wild card characters are not supported.
- Results are returned only if the utility can match attributes with data in the database.

If the search results display any empty fields, this is most likely because the search criteria was not entered correctly. If you confirm that the attributes were entered correctly and the fields are still empty, the attributes were probably not used by the activation so they were not saved in the database.

# Rolling Back an Activation

Completed activations can be deactivated—that is, rolled back—to return a device to its original configuration. The rollback is a best effort; in some cases complete rollbacks may not be possible.

Before you roll back and activation, you can preview the CLI configuration sequence that will be executed before the rollback is performed.

**Step 1** From the Activation menu, choose **Activation History**. The Activation History window displays a list of recent activation attempts.

**Step 2** If necessary, search for the desired activation (see Searching for Activations (Activation History), page 3-35).

**Step 3** Select the activation and view its details. Activations can be rolled back if the Operation column displays **Add** and the State column displays **Done**.

**Note** You can attempt a deactivation on an aborted activation to clean up partial rollbacks, but the cleanup is a best effort.

**Step 4** Right-click the selected activation and choose **Deactivate Preview**. You should verify the information in the User Input tab and the Preview configuration tab (errors will be highlighted).

If you want to test the deactivation on a single device before performing it on all selected devices, export the *preview* deactivation sequence to you local drive using **Export to File**. Then you can copy and paste the commands to a specific device.

**Step 5** Right-click the selected activation and choose **Deactivate**.

**Step 6** On the confirmation dialog box, click **Yes** and **Close**.

# Cloning an Existing Activation

Cloning is useful when you know you will have to repeat an activation in the future. The cloning process saves all of the values that you entered in the original activation. This is useful when you have to perform a deactivation, but you know it will be followed be a re-activation with the same settings.

**Step 1** From the Activation menu, choose **Activation**.

**Step 2** Select the activation that you want to clone and click **Clone Activation**. The Activation History window is displayed.

**Step 3** Search for the specific activation deployment that contains the settings you want to clone.

**Note** The search results return the search based on the activation you have selected.

**Step 4** Click **OK**. The activation clone is created.

# Deleting Activations

Users with Administrator privileges can delete activations and activation templates from the Prime Network Administrator GUI client. Executed activations are automatically purged from the Prime Network database according to the purging settings set by the administrator. For more information on the Administrator GUI client, see the *Cisco Prime Network 3.10 Administrator Guide.*

CHAPTER 4

# Device Configurations and Software Images

Cisco Prime Network Change and Configuration Management (CCM) provides tools for managing the software images and device configuration files used by the devices in your network. These topics provide an overview of the features that CCM provides, some initial setup tasks you must perform, and how to work with the GUI:


- What is Change and Configuration Management?, page 4-1
- Set Up Change and Configuration Management, page 4-2
- Use the CCM Dashboard, page 4-10
- Device Configurations, page 4-11
- Software Images, page 4-24
- Configuration Audit, page 4-42
- Global Settings and Administration, page 4-47


For information on the devices supported by CCM, see *Addendum: Additional VNE Driver Support for Cisco Prime Network*.

# What is Change and Configuration Management?

Cisco 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 Image Management function. Operations can be performed on user-created groups of devices. For more information on user-defined device groups, see Device Groups Setup Tasks, page 4-8.

### Configuration Management

Configuration Management enables you to control and track changes that are made to a device configuration. It uses a change management feature to detect ongoing changes to devices in two ways:

- When doing periodic archiving of device configurations. If CM detects a change in a configuration file, it will get the new version of the file from the device and copy it to the archive.
- When a configuration change notification is received from a device. This is called event-triggered archiving. You can configure CM to copy a new version of a configuration file to the archive whenever a change is detected, or to queue the changes and then copy the files to the archive according to a schedule.

By default, neither of these methods are enabled. You can configure them from the Configuration Management Settings page (see Configuration Management Setup Tasks, page 4-5).

Change Logs provide information on the changes made to devices in the network, sorted by their time stamp. The Configuration Management Settings page controls how long these logs are saved. CM saves messages that can be used for debugging in PRIME_NETWORK_HOME/XMP_Platform/logs/ConfigArchive.log.

**Note** All configuration management operations are performed only on devices with Communication State as Reachable and Investigation State as Operational, Partially Discovered, or Currently Unsynchronized. For a Cisco IOS device with SNMPv3 configuration, configuration management operations can be performed only if the device is configured with write permission for CISCO-CONFIG-COPY-MIB MIB group.

### Image Management

Image Management provides tools for performing rapid, reliable software upgrades and automate the steps associated with upgrade planning and monitoring. This topic provides an overview of both features and an introduction to the Change and Configuration Management dashboard. Cisco IOS and Cisco IOS XR software images are stored in the Prime Network image repository, to which you can add new images by importing them from Cisco.com, from existing devices, from a local file system, or from an external image repository. Software images in the repository are stored in binary format. Before an image is distributed, NEIM performs an upgrade analysis to ensure that the network element is compatible with the image. For Cisco IOS XR devices, you can add individual packages, deactivate packages, test changes before committing them, commit changes, and roll packages back to stored rollback points. The image repository is located in the Cisco Prime database. NEIM saves messages that can be used for debugging in PRIME_NETWORK_HOME/XMP_Platform/logs/NEIM.log.

**Note** All image management operations are performed only on completely managed devices. (This means the Communication State of the device must be Reachable and Investigation State of the device must be Operational.)

**Note** We recommend that you verify that an image operation is correct on a single device, preferably in a lab, prior to distributing and activating a change in image on multiple devices in a production network.

# Set Up Change and Configuration Management

The following topics explain the setup tasks required for Change and Configuration Management:

- Prime Network Setup Tasks, page 4-3
- Device Setup Tasks, page 4-4
- Configuration Management Setup Tasks, page 4-5
- NEIM Setup Tasks, page 4-6
- Device Groups Setup Tasks, page 4-8

# Prime Network Setup Tasks

Verify the following:

- Verify that CCM is installed. The installation process is described in the *Cisco Prime Network 3.10 Installation Guide*. CCM can be installed using the network-conf command. The guide includes information about supported browsers, ports that must be available, and so forth.

  To check if CCM is installed, log into the Prime Network gateway and enter the following command:

  ```
  # cd $PRIME_NETWORK_HOME/Main
  # dmctl status
  ```

  If you see the following in the output, CCM is installed and running.

  ```
  - Checking Prime Network Web Server Status                          [UP]
  ```

- Verify the port to be used. 8043 is the secure HTTP port enabled by default for Change and Configuration Management web client. However, you can still use port 8080 to launch the Change and Configuration Management GUI. To do so, you must manually enable it using this command:

  ```
  # cd $NCCM_HOME/scripts/
  # ./nccmHTTP.csh enable
  # dmctl stop
  # dmctl start
  ```

  To disable port 8080, perform the same operation but use the disable argument.

- If a gateway is behind a firewall, you must open special ports. You do not have to open special ports if units are located behind firewalls (and with NAT). This approach prevents issues when the unit is behind NAT, as the unit does not require a publicly available IP address for the gateway to contact it.
- SNMP read-write community in Cisco Prime Network Administration must match that on the devices. Make sure that pop-up windows are enabled on the Firefox and Internet Explorer browsers.
- For IPv6, CM and NEIM functions run smoothly on a combination of network and devices with IPv6 addresses. Either the device or the unit must be configured with an IPv6 address to work. For Cisco IOS devices with IPv6 address, the CM and NEIM operations will work only in FTP mode.
- For NEIM, verify that the gateway has sufficient space for the storing and staging directories (see Change Image Management Global Settings, page 4-53).
- For config and image transfers using TFTP, verify that the TFTP directory is set up and available in the Prime Network gateway and/or unit. To modify and verify the TFTP directory, run the following commands:
  - To change the TFTP directory, go to the Prime Network directory and run the following commands in the Prime Network gateway:

    ```
    ./runRegTool.sh -gs 127.0.0.1 set <GW/Unit IP> avm83/services/tftp/read-dir tftp dir name

    ./runRegTool.sh -gs 127.0.0.1 set <GW/Unit IP> avm83/services/tftp/write-dir tftp dir name
    ```

  - To check the TFTP directory, run the following commands:

    ```
    ./runRegTool.sh -gs 127.0.0.1 get <GW/Unit IP> avm83/services/tftp/read-dir

    ./runRegTool.sh -gs 127.0.0.1 get <GW/Unit IP> avm83/services/tftp/write-dir
    ```

  - Restart AVM 83 in the gateway or the unit, by using the following command:

    ```
    anactl -avm 83 restart
    ```

# Device Setup Tasks

- Verify that the device is supported. See *Addendum: Additional VNE Driver Support for Cisco Prime Network*.
- For CM, verify that devices are configured to forward configuration change notifications to Prime Network. This is documented as a prerequisite to adding VNEs, in the *Cisco Prime Network 3.10 Administrator Guide*. (Specifically, if you will be using event-triggered archiving, make sure the logging gateway-IP command is configured on all devices. This command should have been configured as a prerequisite to adding VNEs to Prime Network.)
- Simple Network Management Protocol (SNMP) read-write community must be configured on devices. For more information on configuring SNMP community strings for devices, see the *Cisco Prime Network 3.10 Administrator Guide*. SNMP read-write community in Cisco Prime Network Administration must match that on the devices.
- Ensure reachability from Prime Network units to devices and vice versa.
- Make sure you have performed all of the device configuration prerequisites for adding VNEs. These commands are described in the *Cisco Prime Network 3.10 Administrator Guide*.
- Change and Configuration Management supports FTP for all config and image transfers. Although you can configure a username and password using the **ip ftp** command, adding the unit's FTP credentials to the device may not be safe if the network is not secure. Before using FTP for Change and Configuration Management, we recommend that you:
  - Configure the network device to add the *Prime Network Unit User* credentials of the unit that manages the device. You need not add the super user credentials of the *Prime Network Unit Server* to the device configuration.
  - For Cisco Carrier Packet Transport (CPT) devices, add the *Prime Network Unit User* credentials to the registry. This is required because Prime Network initiates the FTP operation using a TL1 interface, and the TL1 commands require the username and password as input parameters. After you add this information to the registry, the credentials are automatically read when needed.

    ```
    # $ANAHOME/Mail/runRegTool.sh -gs 127.0.0.1 setEncrypted 127.0.0.1
    nccm-settings/ftpsettings/username ftp-username

    # $ANAHOME/Mail/runRegTool.sh -gs 127.0.0.1 setEncrypted 127.0.0.1
    nccm-settings/ftpsettings/password ftp-passwd
    ```

  - Restrict the FTP configuration such that the *Prime Network Unit User* has read-write access only to the $PRIME_NETWORK_HOME/tftp directory and hence does not have access to unwanted files outside the home directory.

**Note** FTP support is not available for Cisco IOS XR devices and Cisco Nexus 5000 and Cisco Nexus 7000 series devices.

- For IPv6, CM and NEIM functions run smoothly on a combination of network and devices with IPv6 addresses. Either the device or the unit must be configured with an IPv6 address to work. For Cisco IOS devices with IPv6 address, the CM and NEIM operations will work only in FTP mode.

# Configuration Management Setup Tasks

**Note** In the Configuration Management and Image Management Settings pages, Change and Configuration Management does not support the following special characters:

- For Password fields—>, <, ', /, \, !, :, ;, and "
- For all other fields—`, ~, @, #, $, %, ^, &, *, (, ), +, =, |, {, }, [, ], ', ?, >, <, /, \, !, :, ;, and "

The CM features are disabled by default so that you do not encounter unexpected processing loads on your server. The following steps explain what you must do to set up CM. All of these items are configured from the Configuration Management Settings page (**Configurations > Settings**). Many of these settings can be overridden when you create specific jobs.

1. Configure the transport protocol that Prime Network will use between the device and the gateway. these are controlled from the **Transport Protocol** area. The options are TFTP, SFTP/SCP, and FTP. The default is TFTP. Note the following:

**Caution** FTP is not a secure mode of transfer. Use SCP/SFTP instead, for secure config and image transfers.

   - The TFTP source interface on the devices must be able to reach the unit. Otherwise, the configuration management jobs that require TFTP may fail.
   - To use SFTP/SCP for config transfers from a device to a unit, you need to ensure that an SSH server is configured and running on the device, such that the device acts as a server and the unit as a client during the transfer. For Cisco IOS XR devices, you need to configure the device with K9 security (k9sec) enabled images such that the SSH server is up and running on the device.

2. Enable CM to perform an initial synchronization of the CM archive files with the configurations that are running on the network devices. Whenever the Prime Network gateway is restarted, CM will perform this synchronization. By default, synchronization is disabled. To enable it, activate **Enable Initial Config Syncup**.
3. Configure the policies that control how often CM retrieves information from devices and copies configuration files to the archive. By default, all of these settings are disabled. You must answer the following basic questions:
   a. How much disk space is available? Smaller space may require more frequent purging.
   b. Should new configuration files be copied (backed up) to the archive on a periodic basis or on an event-driven basis?

      If configurations are changing frequently and the changes are not important to you, you should use periodic backups by selecting **Enable Period Config Backup**. This will minimize server workload.

      **Note** The periodic setting is recommended.

      If every change is considered significant, use event-driven backups (**Enable Event-Triggered Config Archive**).
   c. For event-driven archiving, should information be copied to the archive immediately upon receiving a change (**Sync archive on each configuration change**)? Or should changes be queued and then copied at a certain interval (**Sync archives with changed configurations**

**every ___ hours and ___ minutes**)? If information needs to be copied to the archive immediately, you must sync the archive on each configuration change. Otherwise, you can sync the archive with changed configurations at a certain interval (every 1-24 hours).

4. Enable CM to perform periodic synchronization of out-of-sync devices by selecting **Enable Periodic Sync for Out of Sync Devices (24Hours)**.
5. Enable CM to export archived configuration to an export server on a periodic basis by selecting **Enable Periodic Config Export** and **Export Settings.** This allows you to free up disk space while keeping a permanent record of historical archives.
6. Configure when configuration files should be purged from the archive using the **Archive Purge Settings**. You should consider:
   - How big are the configuration files?
   - How often are changes made to devices?
7. Specify the default mode of restoring configuration files to the devices using **Restore Mode**.
8. Configure the SMTP server and e-mail IDs to send notifications on the status of configuration management jobs to users. (You can also specify e-mail settings when you create a job.)
9. Specify the commands that you want CM to exclude when comparing files (for example, clock rates). A set of common exclude commands is provided by default (for example, ntp-clock-period). these are controlled in the **Exclude Commands** area (see Notes on Exclude Commands, page 4-51).

**Note** Configuring exclude commands is especially important if you are using event-driven archiving. Doing so avoids unnecessary file backups to the archive.

# NEIM Setup Tasks

**Note** In the Configuration Management and Image Management Settings pages, Change and Configuration Management does not support the following special characters:

- For Password fields—>, <, ', /, \, !, :, ;, and "
- For all other fields—`, ~, @, #, $, %, ^, &, *, (, ), +, =, |, {, }, [, ], ', ?, >, <, /, \, !, :, ;, and "

**Caution** FTP is not a secure mode of transfer. Use SCP/SFTP instead, for secure config and image transfers.

The following are the NEIM prerequisites, all of which are controlled by the Image Management Settings page (**Images > Settings**). Many of these settings can be overridden when you create specific jobs.

1. Configure the transport protocol that Prime Network will use between the device and the gateway; these are controlled from the **Transport Protocol** area. The options are TFTP, SFTP/SCP, and FTP. The default is TFTP. Note the following:
   - The TFTP source interface on the devices must be able to reach the unit. Otherwise, the image management jobs that require TFTP may fail.

  - To use SFTP/SCP for image transfers from a device to a unit, you need to ensure that an SSH server is configured and running on the device, such that the device acts as a server and the unit as a client during the transfer. For Cisco IOS XR devices, you need to configure the device with K9 security (k9sec) enabled images such that the SSH server is up and running on the device.

2. Configure the gateway staging directory to use when transferring images from Prime Network out to devices in the **File Locations** area. The default is *PRIME_NETWORK_HOME/NCCMComponents/NEIM/staging/*. PRIME_NETWORK_HOME is the Cisco Prime Network installation directory (by default, /export/home/*network-user*; where *network-user* is the operating system user for the Prime Network application and an example of *network-user* is network39).
3. Use the **Clear Flash** option (under **Flash Properties**) to recover the disk space occupied by files that were marked for deletion in the device, before distributing the image or package, if there is insufficient memory.
4. Enable the warm upgrade facility to reduce the downtime of a device during planned Cisco IOS software upgrades or downgrades (in the **Warm Upgrade** area).
5. Configure the gateway storing directory to use when transferring images from an outside source into the image repository (from Cisco.com or from another file system). This is controlled from the **File Locations** area. The default is *PRIME_NETWORK_HOME/NCCMComponents/NEIM/images/*. *PRIME_NETWORK_HOME* is the Prime Network installation directory (by default, /export/home/*network-user*; where *network-user* is the operating system user for the Prime Network application and an example of *network-user* is network39).
6. Configure the SMTP server and e-mail IDs to send notifications on the status of image management jobs to users. (You can also specify e-mail settings when you create a job.) This is controlled in the **E-mail Settings** area.
7. If you plan to download files from Cisco.com, configure the necessary vendor credentials to connect to Cisco.com. These are set in the **Vendor Credentials** area. If you do not have login privileges, follow the procedure in Obtaining Cisco.com Login Privileges for Image Management, page 4-7.
8. Configure the proxy server details to use while importing images to the archive from Cisco.com (in the **Proxy Settings** field).
9. If you plan to download images from an external repository, set up the details of the external server to import images to the Prime Network image repository (in the **External Server Details** area).

### Obtaining Cisco.com Login Privileges for Image Management

Login privileges are required for all Images operations that access Cisco.com. To get access, you must have a Cisco.com account. If you do not have a user account and password on Cisco.com, contact your channel partner or enter a request on the main Cisco website.

You can register by going to the following URL:

http://tools.cisco.com/RPF/register/register.do

To download cryptographic images from Cisco.com, you must have a Cisco.com account with cryptographic access.

To obtain the eligibility for downloading strong encryption software images:

**Step 1** Go to the following URL:

http://tools.cisco.com/legal/k9/controller/do/k9Check.x?eind=Y&return_url=http://www.cisco.com

**Step 2** Enter your Cisco.com username and password, and click **Log In**.

**Step 3** Follow the instructions provided on the page and update the user details.

**Step 4** Click **Accept** to submit the form.

**Step 5** To verify whether you have obtained the eligibility to download encrypted software:

**a.** Go to the following URL:

http://tools.cisco.com/legal/k9/controller/do/k9Check.x?eind=Y&return_url=http://www.cisco.com

**b.** Enter your username and password, and click **Log In**.

The following confirmation message is displayed:

```
You have been registered for download of Encrypted Software.
```

# Device Groups Setup Tasks

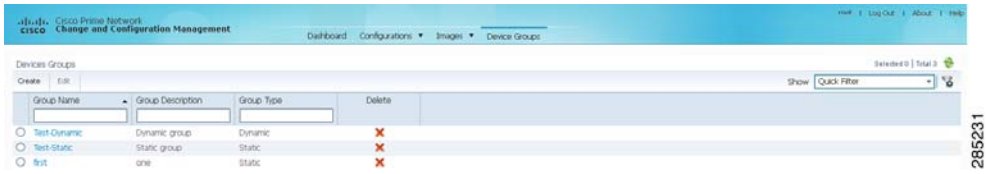
You can create user-defined device groups for ease of performing operations. A static group contains a specific set of devices; new devices must be added manually. A dynamic group is populated according to membership rules; if newly-added devices match the rules, they are automatically added to the group.

If you are backing up the configuration archive or importing software images from devices into the repository, and a device group changes during the operation, Prime Network updates the job accordingly such that all the devices available in the group at the time of execution of the job are considered for the backup or import operation. All other job types are not updated; you must delete and recreate the job.

To view the existing and create new user-defined device groups:

**Step 1** Click the **Device Groups** tab. The Device Groups page appears as shown in Figure 4-1.

***Figure 4-1 Device Groups Page***




The Device Groups page displays the name, description, and whether the membership is static or dynamic. To delete a group, click the red X next to the group name.

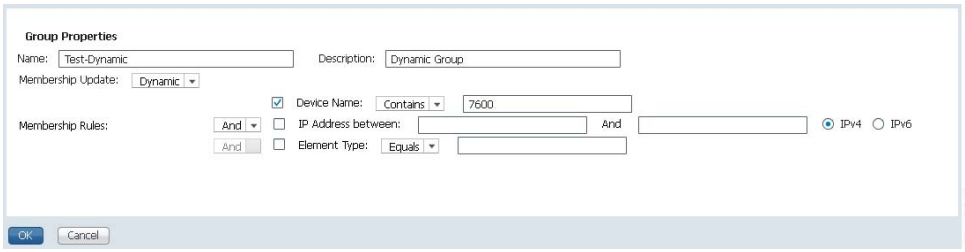
To view the devices in a group, click the hyperlinked group name to view the devices mapped to the group in the Group Members page. The device status, IP address and element type is listed. To display more properties, click the Device Name hyperlink. The status icons are illustrated in the following.

| Symbol | Description |
|---|---|
| | Device is in operational state. |
| | Device is not in operational state. Most likely the device is in the Maintenance investigation state or the Unreachable communication state. Click the device hyperlink and open the device properties popup to see details about the device. |

**Step 2** To create a new group, click **Create** and enter the required information. Names must be unique; do not use the reserved names **adminGroup** and **ROOT-DOMAIN.**

**Step 3** In the Membership Update drop-down list box, choose Static or Dynamic.

- For dynamic groups, set up a membership rule to indicate which devices must be added to the group. The following figure provides an example of the Create Device Group page for a dynamic group.

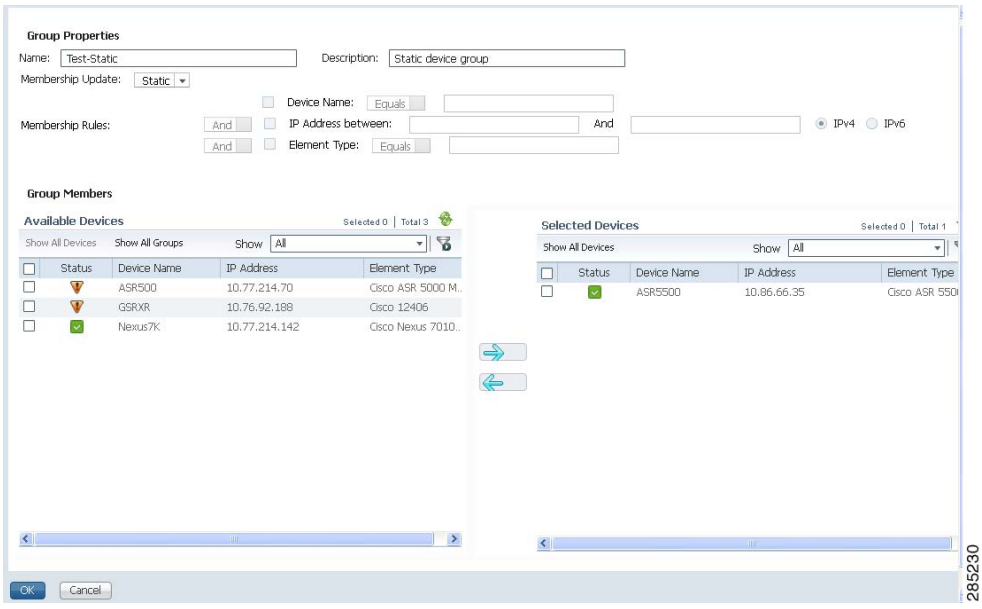



You can set up membership rules with parameters such as device name, range of device IP addresses, and the device element type. For example:

```
Device Name    equals    1800
IP Address between    10.77.214.107    And    10.77.214.171    IPv4
Element Type    equals    Cisco 1801
```

**Note** You can choose to include any one or a combination of these parameters in the rule by using the And/Or operator. Also, you can provide multiple values for the Device Name and Element Type parameters as a comma-separated list, if required.

- For static device groups, in the Group Members section, under the Available Devices list, Prime Network lists all the devices that are available in the database. The following figure provides an example of the Create Device Group page for a static group.




**Step 4** Click **OK** to save the group.

# Use the CCM Dashboard

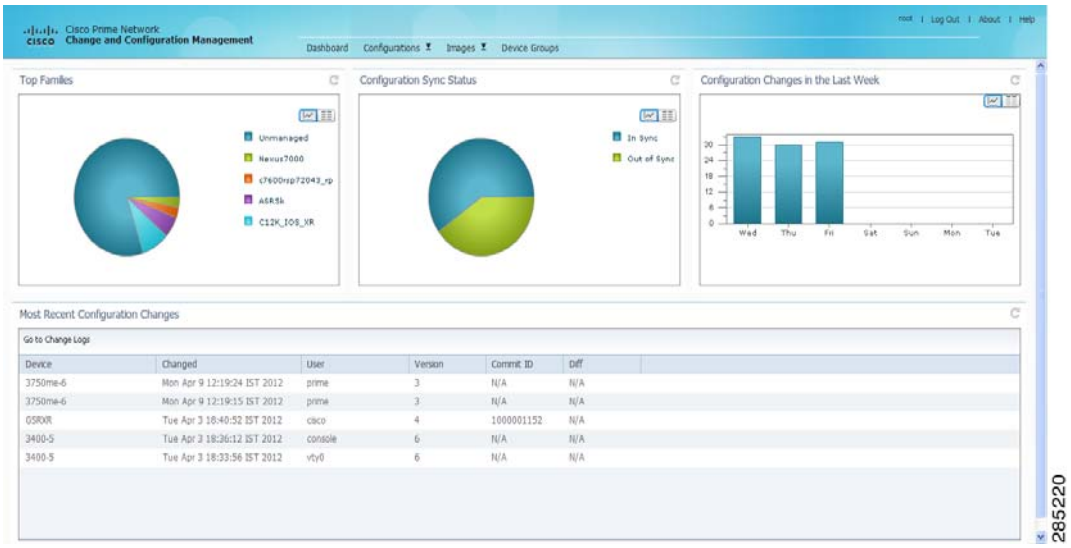
To launch the GUI from a web browser, enter the following URL in the address bar:

**https://***gateway-IP***:8043/ccmweb/ccm/login.htm**

**Note** Change and Configuration Management does not support special characters for any of the editable fields in the GUI, including filters.

Figure 4-2 shows the CCM Dashboard, which contains four dashlets or subdivisions to display real-time information about the most frequently used software images, devices with startup and running configurations that are not in sync, and recent configuration changes.

***Figure 4-2 CCM Dashboard***




| Dashlet | Provides information about: |
|---|---|
| Top Families | Four device families with the highest number of devices in the network. Smaller groups can be viewed by toggling to the tabular form. From here, you can distribute and activate software images to a selected family.<br>**Note** You may face resizing issues when you hover the cursor over this dashlet, if you have enabled the Right to Left (Hebrew) settings in your browser. |
| Configuration Sync Status | (Cisco IOS) Devices for which the startup and running device configurations are in sync or not in sync. Whenever a Cisco IOS configuration file is retrieved from a device and copied to the archive, Prime Network compares the latest version of the startup configuration with the latest version of the running configuration file. If there is a mismatch, Prime Network adds the device to the list of out-of-sync devices. The information is refreshed whenever you click the Dashboard.<br>A "100% Unavailable" message is displayed when there are no Cisco IOS device images or if the initial configuration sync up setting is not enabled (controlled by the "Enable/Disable Initial config sync up on restart" setting on the Configuration Management Settings page). |

| Dashlet | Provides information about: |
|---|---|
| Configuration Changes in the Last Week | Number of device configuration changes detected for each day of the previous week. This dashlet is empty when configuration change notification is not enabled (controlled by the "Enable/Disable Event-Triggered Config Archive" setting on the Configuration Management Settings page). |
| Most Recent Configuration Changes | Last five device configuration changes that were made to devices in the network. This dashlet is empty if configuration change notification is not enabled. It is controlled by the "Enable/Disable Event Triggered Config Archive" setting on the Configuration Management Settings page (see Change Configuration Archive Global Settings, page 4-48).<br><br>The Commit ID and Diff columns apply only to Cisco IOS XR devices. Other device types will display N/A in those columns. |

Use the following icons to toggle between different views in the Top Families, Configuration Sync Status, and Configuration Changes in the Last Week dashlets.

| Icon | Description |
|---|---|
| | Displays the details in the form of a pie or bar chart. If you hover your mouse cursor over a section in the pie chart, a tooltip displays the information associated with that section. |
| | Displays the details in a tabular form. |

# Device Configurations

The following topics explain how to work with device configurations:

- What is In the Archive?, page 4-11
- Protect Configurations in the Archive, page 4-12
- Find Out What is Different Between Configurations, page 4-13
- Copy a Configuration File to a Central Server, page 4-15
- Are Running and Startup Configs Mismatched? (Cisco IOS and Cisco Nexus), page 4-16
- Copy the Device Files to the Archive (Backups), page 4-17
- Fix a Live Device Configuration (Restore), page 4-20
- Clean Up the Archive, page 4-22
- Find Out What Changed on Live Devices, page 4-23

## What is In the Archive?

Choose **Tools > Change and Config Mgmnt** to open Change and Configuration Management.

Choose **Configurations > Archives** to view the contents of the archive. The CM archive maintains copies of device configuration files, storing them in the Prime Network database. Configuration files are stored in readable format, as received from the device. Users can only see devices that are in their device

scope. The total number of archives available in the Prime Network database is also displayed in the header. The Archived Configurations page displays the following information about each configuration file.

# Protect Configurations in the Archive

*Table 4-1 Configuration Information Displayed on Archived Configurations Page*

| Field | Description |
|---|---|
| Device Name | Name of device. Click the icon next to the device name to open a popup that displays device properties. Additional information is listed depending on the device type:<br>• Current active packages on the device—For Cisco IOS XR devices<br>• Active kickstart images—For Cisco Nexus series devices<br>• Priority list—For Cisco ASR 5000 series devices. The priority list displays various combinations of a configuration file and an image file in priority order for the device. |
| Version | An internally-used number. A version will not have an associated configuration file under the following circumstances:<br>• The associated configuration file was deleted from the archive.<br>• The associated configuration file has not yet been copied to the archive. (Prime Network supports queuing change notifications and copying the configuration files to the archive at a later time. See Change Image Management Global Settings, page 4-53.)<br>Click a version number hyperlink to launch the Device Configuration Viewer, from which you can view the contents of a configuration file. |
| Type | Type of configuration:<br>• Cisco IOS and Cisco Nexus series devices—Running or Startup<br>• Cisco IOS XR devices—Running or Admin<br>• Cisco ASR 5000 series devices—Running or Boot. For boot configuration, the version is always displayed as 1.<br>• Cisco CPTdevices—Startup |
| Commit Id | (Cisco IOS XR only) ID that identifies the last configuration change on the device (maximum number saved is 100). |
| Date Changed | Date and time of last change, displayed accordingly to the local time zone settings of the client.<br>For Cisco CPT and Cisco ASR 5000 series devices, this field displays N/A. |
| Label | User-assigned archive labels. |
| Running Image | The software image currently running on the device. |

*Table 4-1 Configuration Information Displayed on Archived Configurations Page (continued)*

| Field | Description |
|---|---|
| Comments | User-assigned free text. |
| Context / Module / Priority | For Cisco Nexus series devices, this field displays the virtual device context (VDC) name.<br>For Cisco 7600 series devices, this field displays the module name.<br>For Cisco ASR 5000 series devices, this field displays the boot configuration files with their priorities.<br>For other devices, this field displays N/A. |

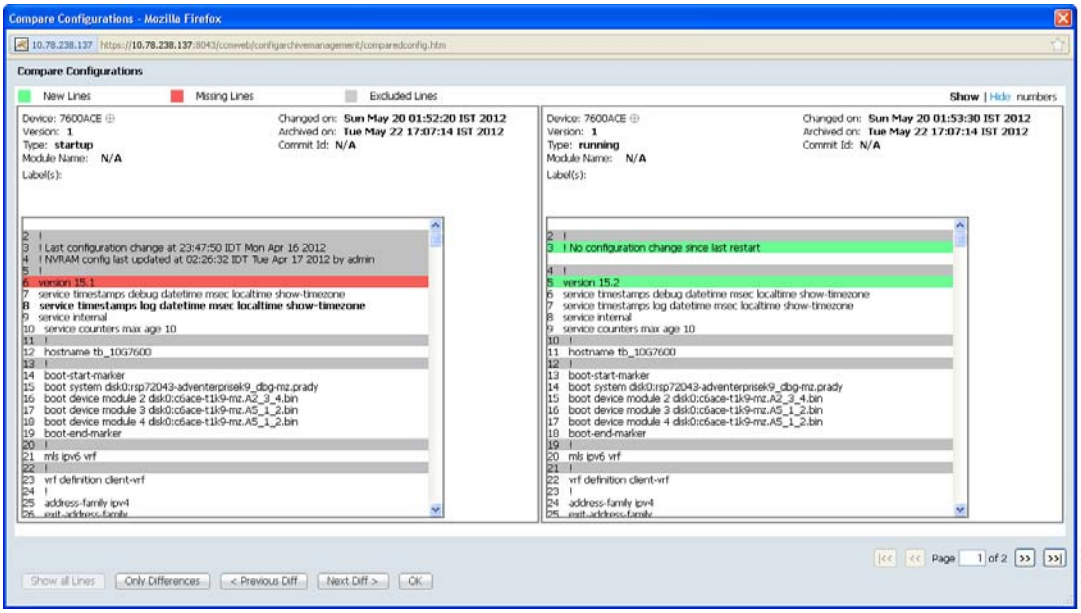
Assigning labels to configuration files is a clear, simple way to identify important configurations and convey critical information. You can manage labels by choosing **Labels > Manage**.

- Adding a label adds it to the catalog where it is made available to all users. Add labels by clicking **Add Row**.
- Deleting a label unassigns the label from configurations that are using it. Likewise, if you edit a label, the change is applied to all configurations using the label.
- Unassigning a label does not delete the label from the catalog.
- Labels with the "do not purge" property will not be purged from the archive (the delete action is disabled). When calculating the total number of archives to see if the maximum has been reached and archives should be purged, CM does not include configurations with this label in the total (see Change Configuration Archive Global Settings, page 4-48).

# Find Out What is Different Between Configurations

Prime Network allows you to compare two configuration files that are saved in the archive and display them side by side, highlighting configuration differences and allowing you to move between them. Prime Network excludes a small set of commands by default, such as the NTP clock rate (which constantly changes on a managed network element but is not considered a configuration change). You can change the excluded commands list as described in Change Configuration Archive Global Settings, page 4-48. Additions, deletions, and excluded values are color-coded as shown in the following example.

*Figure 4-3 Compare Configurations Dialog Box*




You can compare any types of configurations as long as they run on the same operating system. However, you cannot compare a Cisco IOS configuration with Cisco IOS XR configuration.

The following are typical scenarios for using the compare function:

- Compare the latest and next-to-latest configuration to see the most recent change.
- Compare Cisco IOS running and startup configurations to see how they are out of sync.
- Compare the configurations on two different devices to find out how they are different.

**Note** When you are trying to compare an archive with an active startup, running, or admin configuration, if there is a change in the device configuration, Prime Network initiates a backup job and creates a latest version of the device configuration file. You can view the latest version of the configuration file in the Archived Configurations page.

To compare configurations:

**Step 1** Choose **Configurations > Archives**.

**Step 2** Locate the archives you want to compare. You can click the Version hyperlink next to a device to open the Device Configuration Viewer and quickly view the contents of the configuration file.

**Step 3** You can choose to do the following:

| Device Type or OS | Supported Function |
|---|---|
| For Cisco IOS XR devices | **Compare > To Active Running** or **Compare > To Active Admin** |
| Cisco IOS device | **Compare > To Active Startup** or **Compare > To Active Running** |
| Cisco ASR 5000 series device | **Compare > To Active Boot** or **Compare > To Active Running** |
| All | **Compare > Selected Archives** |

# Copy a Configuration File to a Central Server

You can export configurations to an FTP or SFTP server that is specified on the Configuration Management Settings page. They are exported as a .cfg (configuration) file.

Configuration files are saved using the following format:

*deviceName*-*configurationType*-*version*-*configChangeTimestamp*.**cfg**

For example, the following file would contain the 18th version of a running configuration for the device named 7200-5, saved on March 27, 2010 at 2:40:30 P.M:

7200-5-RUNNING_CONFIG-18-2010327144030.cfg

### Before You Begin

Make sure of the following:

- Export location and required credentials, and (for emails) SMTP host and port are configured on the Configuration Management Settings page.
- Specified FTP or SFTP server must have sufficient free space to accommodate the exported configurations. Also, the destination subdirectory on the FTP or SFTP server must have the required permissions.

To export configuration files:

**Step 1** Choose **Configurations > Archives** and locate the archives you want to export. You can click the Version hyperlink next to a device to open the Device Configuration Viewer and quickly view the contents of the configuration file.

**Step 2** Click **Export** and set the desired schedule and enter the e-mail ID(s) to which to send a notification after the scheduled export job is complete. For two or more users, enter a comma-separated list of e-mail IDs. A notification e-mail is sent based on the e-mail option specified in the Configuration Management Settings page.

**Note** The time you specify here to schedule the export job is the server time.

**Step 3** Click **Export**. The export job is created and you are redirected to the Job Manager page, where you can monitor the status of the job.

# Are Running and Startup Configs Mismatched? (Cisco IOS and Cisco Nexus)

Cisco IOS and Cisco Nexus series devices contain a startup and running configuration file. The startup configuration is loaded when a device is restarted. Ongoing changes to the device are applied to the running configuration. As a result, unless the running configuration is saved as the startup configuration, upon a device restart, any changes would be lost. It is therefore important to ensure that the device startup and running configurations are in sync. When Prime Network synchronizes a file, it overwrites the startup configuration on the device with the configuration that is currently running on the device.

Whenever a configuration file is retrieved from a device and copied to the archive (that is, backed up), Prime Network compares the latest version of the startup configuration with the latest version of the running configuration file. If there is a mismatch, Prime Network adds the device to the list of out-of-sync devices.

For Cisco Nexus series devices, CM backs up the startup and running configurations for all VDCs configured in the device. If there is a mismatch between the startup and running configurations of a VDC, CM creates an out-of-sync entry for that VDC.

**Note** The synchronize operation affects only the configurations running on the device. It does not affect any configuration files that are saved in the archive. Configuration sync is not applicable for Cisco CPT and Cisco ASR 5000 series devices.

The Dashboard maintains a Configuration Sync Status pie chart that shows how many devices have out-of-sync startup and running configuration files. When you click the pie chart (or choose **Configurations > Synchronize**), you are directed to the Out of Sync Devices page, where Prime Network lists all of the out-of-sync devices in tabular format. The information is refreshed whenever you choose **Configurations > Synchronize**.

### Before You Begin

Make sure the specified FTP or SFTP server must have sufficient free space to accommodate the exported configurations. Also, the destination subdirectory on the FTP or SFTP server must have the required permissions.

To view differences and synchronize configurations:

**Step 1** Choose **Configurations > Synchronize**. Prime Network lists all out-of-sync devices, the date and time when the device configurations were last changed, and when the files were last archived. Figure 4-4 provides an example. The date and time are displayed according to the local time zone settings of the client.

***Figure 4-4 Configuration Synchronization - Out of Sync Devices Page***

**Step 2** Click the Compare icon to launch the Compare Configuration window, which provides a side-by-side view of the two configurations and highlights the differences.

**Step 3** Choose the network elements you want to synchronize. This directs Prime Network to overwrite the startup configuration on the device with the configuration that is currently running.

**Step 4** Click **Synchronize**. The Schedule Synchronization page opens.

**Step 5** Set the desired schedule and enter the e-mail ID(s) to which to send a notification after the scheduled synchronization job is complete. For two or more users, enter a comma-separated list of e-mail IDs.

**Note** The time you specify here to schedule the synchronization job is the server time.

**Step 6** Click **Synchronize**. Prime Network schedules the job and redirects you to the Jobs page, where you can monitor the status of the job.

# Copy the Device Files to the Archive (Backups)

These topics describe how to automatically and manually back up configuration files to the archive:

- Automatic Backups and Manual Backups
- Manually Backing Up Configuration Files

Backing up a device configuration entails getting a copy of the configuration file from the device, and copying that file to the configuration archive. As part of the backup procedures, it is compared with the latest archived version of the same type (e.g. running with running, startup with startup). A new version of the file is archived only if the two files are different. If the number of archived versions exceeds the maximum, the oldest archive is purged (according to the values on the Configuration Management Settings page). Configurations marked with a “do not purge” label are not removed from the archive by the auto-purging procedures.

The backup procedure is also when Prime Network identifies out-of-sync devices.

The backup operation includes:

- Cisco IOS XR devices: Includes active packages. CCM does not back up running configurations for Cisco IOS XR devices that are managed with non-system user credentials; because copy command is not available in the command-line interface (CLI) for non-system users.
- Cisco Nexus series devices: Startup and running configurations for all VDCs configured in the device.
- Cisco 7600 series devices with an ACE card: Startup and running configurations of the ACE card.
- Cisco ASR 5000 series devices: Boot configuration file (Prime Network always overwrites the existing boot configuration in the archive)

## Automatic Backups and Manual Backups

Table 4-2 describes the methods you can use to back up configuration files to the archive. None of these methods are enabled by default. Choose the method that is appropriate to your network and how often changes are made to it. For more information, see Configuration Management Setup Tasks, page 4-5.

*Table 4-2 Methods for Archiving Configuration Files*

| Method | Description |
|---|---|
| Initial Sync | Activates CM to perform an initial synchronization of the CM archive files with the configurations that are running on the network devices. If this setting is enabled, whenever the Prime Network gateway is restarted, CM performs this synchronization. This behavior is controlled by the Enable Initial Config sync up setting on the Configuration Management Settings page. See Change Image Management Global Settings, page 4-53. |
| Manual | A user-driven backup that is controlled from the **Configurations > Backup** page. Performing a backup from the Backup page overrides all other archive settings. You can schedule the file backup to occur immediately or according to a schedule.<br>**Note** Any backups scheduled using this method are completely independent of any schedules for ongoing archiving. However, users can only back up devices that are within their scope, and if they have a sufficient device scope-based role.<br>See Manually Backing Up Configuration Files, page 4-19. |
| Ongoing | • Event-Driven—Backs up device files when Prime Network receives a configuration change notification. Use this method if you consider every configuration file change to be significant. This is controlled by the Enable Event-triggered Config Archive setting on the Configuration Management Settings page.<br>For this form of backup, you can choose one of the following methods for performing the archiving:<br>– Back up the files to the archive immediately when a change is detected.<br>– Queue the changes and back up the files to the archive according to a schedule.<br>Both of these settings are controlled from the Configuration Management Settings page.<br>If you are using event-driven archiving, you should also make sure that exclude commands are properly configured. Exclude commands are commands that Prime Network ignores when comparing configurations, and they are controlled from the Settings page. Using this mechanism eliminates unnecessary file backups to the archive.<br>• Periodic—Archives device files every 24 hours (system-defined). A new archive is created only if the newly-collected device configuration is different from the last version in the archive. Use this method if configurations change frequently and the changes are not important to you. This setting is controlled by the Enable Periodic Config Backup setting on the Configuration Management Settings page.<br>**Note** This CM collection is independent of the Prime Network inventory collection.<br>See Change Configuration Archive Global Settings, page 4-48. |

## Manually Backing Up Configuration Files

Files are automatically backed up to the archive according to the values on the Configuration Management Settings page. To perform an on-demand backup of configuration files to the archive:

**Step 1** Choose **Configurations > Backup**. Prime Network lists all devices with the following status symbols as shown in Figure 4-5.

| Symbol | Description |
|---|---|
| | Device is available for backup. |
| | Device is not available for backup. The device is most likely in the Maintenance investigation state or the Unreachable communication state. Click the device hyperlink and open the device properties popup to see details about the device. |

**Step 2** Choose the devices with files you want to back up.

***Figure 4-5 Configuration Backup Page***

**Step 3** To choose devices from a specific device group, click **Select Groups**. Click the hyperlinked device group name to view the list of devices that belong to the group.

**Step 4** Select the required device group in the Device Groups page and click **OK**. The devices that belong to the selected device group are highlighted in the Configuration Backup page. You can also schedule a backup simultaneously for all the devices existing in a group:

- Select a device group and click **Backup Groups**.
- Enter the scheduling information as explained after Step 5 and click **Backup Groups**.

**Step 5** In the Configuration Backup page, click **Backup** to configure the backup schedule. By default, the backup is performed as soon as possible. Other schedule choices (once, periodically, weekly, and so forth) are activated when you deselect Start as Soon as Possible.

**Note** The time you specify here to schedule the backup job is the server time.

**Step 6** Enter the e-mail ID(s) to which to send a notification after the schedule backup job is complete. For two or more users, enter a comma-separated list of e-mail IDs. A notification e-mail is sent based on the e-mail option specified in the Configuration Management Settings page.

**Step 7** Click **Backup**. Prime Network schedules the job and redirects you to the Jobs page, where you can monitor the status of the job.

**Note** If a backup is scheduled for an entire device group and if there is a change in the group by addition or deletion of devices after job creation, Prime Network updates the job accordingly such that all the devices available in the group at the time of execution of the job are considered for backup.

# Fix a Live Device Configuration (Restore)

CCM performs the configuration restore operation in either *overwrite* or *merge* mode, as described in the following.

- Overwrite mode—CCM overwrites the existing configuration on the device with a configuration file from the archive. After the restore operation is performed, the device configuration is identical to the configuration that was chosen from the archive.

  The following devices support overwrite mode:

  Cisco Catalyst 3550 Series Switches
  Cisco Catalyst 3560 Series Switches
  Cisco Catalyst 3750 Series Switches
  Cisco Catalyst 6500 Series Switches (IOS)
  Cisco 800 Series Routers
  Cisco 1800 Series Routers
  Cisco 1700 Series Routers
  Cisco 2600 Series Multiservice Platform Routers
  Cisco 2800 Series Integrated Services Routers
  Cisco 3700 Series Multiservice Access Routers
  Cisco 3800 Series Integrated Services Routers
  Cisco 7200 Series Routers
  Cisco 7600 Series Routers
  Cisco 10000 Series Routers
  Cisco 12000 Series Routers (IOS)

  Cisco ASR 901 Series Routers

  Cisco ASR 903 Series Routers

  Cisco MWR 2941 Router

  For Cisco IOS XR devices, the restore operation rolls back the configuration file to a commit ID associated with the selected archived configuration. If no commit ID is associated with the selected archived version, the restore will fail.

  For all other devices supported by CCM, restore operations in overwrite mode is *not* supported.

- Merge mode—CCM merges the selected configuration file from the archive with the configuration on the device. New commands in the archived version—that is, commands that are *not* in the device's current configuration—are pushed to the device. After the restore operation, the device configuration file retains its original commands, but it also contains new commands from the archived version.

**Note** The restore operation is not applicable to boot configuration files on Cisco ASR 5000 series devices.

By default, Prime Network uses the restore mode setting (overwrite or merge) that is specified in the Configuration Management Settings page (see Change Configuration Archive Global Settings, page 4-48. However, you can modify the default mode while scheduling the restore operation. If you have selected the overwrite mode, you can use the **Use Merge on Failure** option to restore the files in merge mode, if overwrite mode fails.

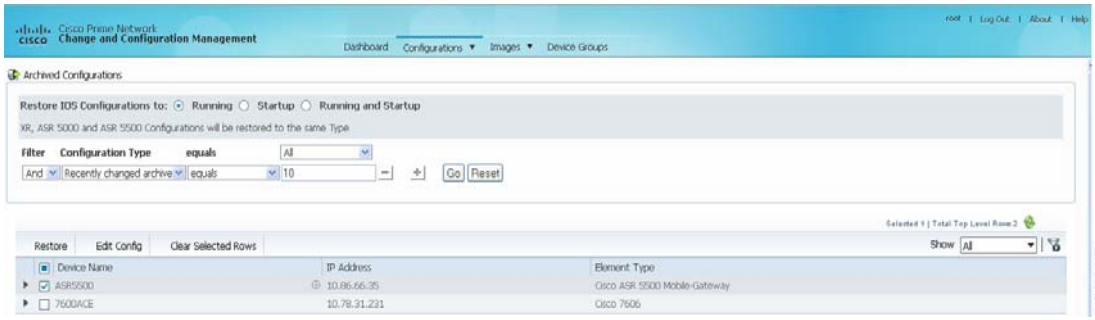
### Before You Begin

- Make sure you have installed Flash Player version 10 or higher to view the Configuration Restore page.
- Make sure you have the permissions to perform the restore operation. You will not be allowed to schedule a restore job, if you do not have permissions.

To restore a configuration:

**Step 1** Choose **Configurations > Restore**. Prime Network lists all configuration files in the archive. Figure 4-6 shows an example of a filtered page.

*Figure 4-6 Configuration Restore Page*



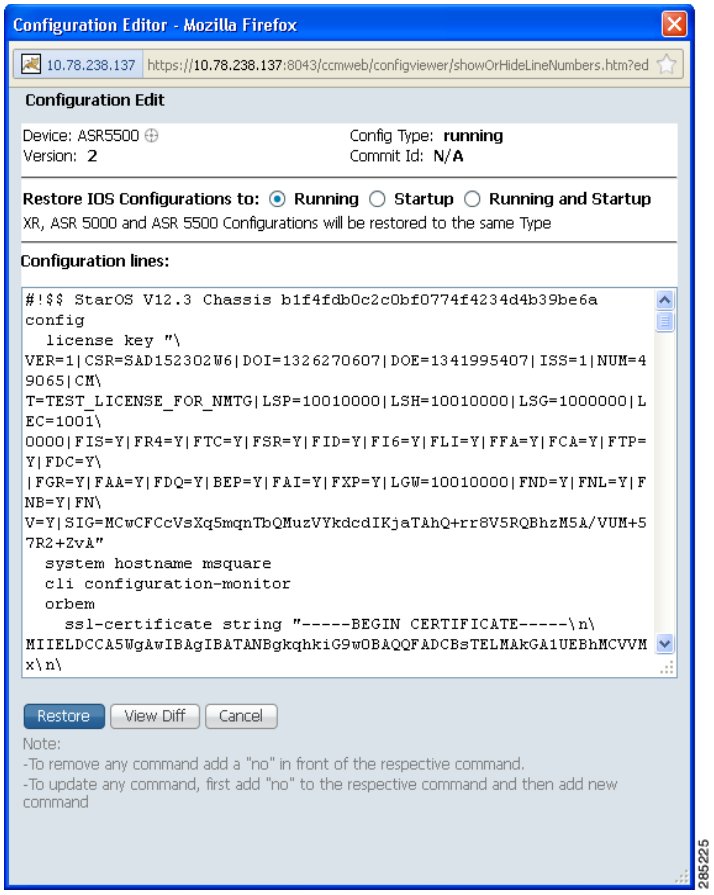

**Step 2** (Cisco IOS only) Specify the type of configuration files you want to restore: Running, Startup, or both. If you choose to restore to startup configuration, Prime Network will first copy the file to running configuration and then to startup configuration.

**Note** Cisco IOS XR and Cisco ASR 5000 series device configuration files are always restored to the same type. For Cisco CPT devices, the Running option restores the selected configuration to startup config and then to running config on the device.

**Step 3** Choose the configuration files you want to restore. You can click the arrow mark next to the device name to view the different versions of the configuration file of the device. You can also click the Version hyperlink to view the contents of a file.

**Step 4** If you want to edit a file before restoring it, click **Edit Config** (edited files are restored only in merge mode). You can view the details of the selected configuration file in the Configuration Editor page as shown in Figure 4-7.

*Figure 4-7 Configuration Edit*




Edit the configuration lines, as required. Note the following:

- To remove a command, add **no** in front of the command.
- To update a command, add **no** in front of the command and then add the new command.

**Step 5** Click **Restore**. The Config Restore Schedule dialog box opens.

**Step 6** (Optional) Override the default transport protocol and default restore mode.

**Step 7** Enter a comma-separated list of e-mail ID(s) to which to send a notification after the scheduled restore job is complete.

**Step 8** Click **Restore**. Prime Network schedules the job and redirects you to the Jobs page, where you can monitor the status of the job.

# Clean Up the Archive

Deleting a file removes it from the archive. You cannot delete an archived file if:

- It is marked “do not purge.”
- Deleting it would bring the number of versions below the minimum number of versions that must be retained (as specified on the Configuration Management Settings page).

When a device is removed from Prime Network, its configuration files are also removed from the archive.

To delete a configuration file from the archive:

**Step 1** Choose **Configurations > Archives**.

**Step 2** Choose the configuration file you want to delete. You can click the Version hyperlink to verify the contents of the configuration file.

**Step 3** To delete a single configuration file, click the delete icon (red **X**) at the end of the row. If the delete icon is disabled, this means the archive is assigned a label that is marked "do not purge." To delete this type of configuration, you must first unassign the label from the configuration.

**Step 4** To delete multiple configuration files, select the required files and then click the **Delete** button in the table header.

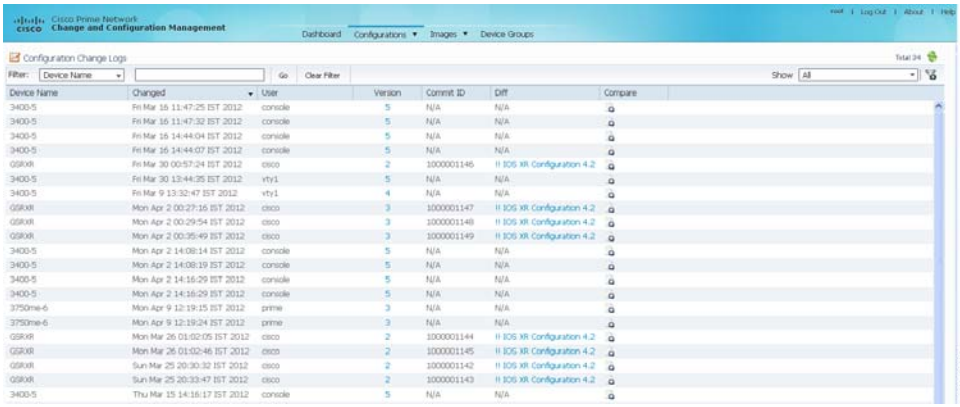
**Step 5** Confirm your choice. Prime Network schedules the job and redirects you to the Jobs page, where you can monitor the status of the job.

# Find Out What Changed on Live Devices

The Change Logs page displays a list of the latest device configuration changes detected by Prime Network. How Prime Network responds to these changes depends on the values on the Configuration Management Settings page. By default, Prime Network does not get new information from the device and copy it to the archive when a change occurs, but you can set it to do so. See Change Configuration Archive Global Settings, page 4-48.

All users can view the change logs, regardless of the user access role or assigned device scopes. To view the latest changes, choose **Configurations > Change Logs**. Figure 4-8 provides an example.

***Figure 4-8 Configuration Change Logs***




The Configuration Change Logs page displays change information, sorted according to the latest time stamp. (For a description of common fields, see Device Configurations, page 4-11.) The date and time stamps are displayed according to the local time zone settings of the client. These fields are specific to the Configuration Change Logs page:

| Field | Description |
|---|---|
| Diff | (Cisco IOS XR only) Displays only the commands that were changed. For long text, hover the cursor over the hyperlink to display the entire contents. |
| Compare | Launches the Compare Configuration window, which displays the entire original and changed files side by side. This data is generated only if file versions are available.<br>Additions and deletions are color-coded. From here, you can:<br>• Click **Show All Lines** or **Only Differences** to display the entire file contents or just the differences between the two files.<br>• Click **Previous Diff** or **Next Diff** to jump forward or backward to the previous or next difference between the two files.<br>• Click the arrow buttons or enter the page number to jump forward or backward to view the file contents that are running across pages. |

# Software Images

The following topics explain how to work with software images and packages:

- Add New Images to the Repository, page 4-24
- New Devices: Create an Image Baseline, page 4-25
- Distribute Images and Make Sure They Will Work, page 4-27
- Activate Cisco IOS Software Images, page 4-32
- Perform Cisco IOS XR Software Package Operations, page 4-34
- Clean Up the Repository, page 4-41

## Add New Images to the Repository

Images are copied to the storing directory specified on the Image Management Settings page. Prime Network verifies whether the file contents are different from the previous version in the repository. If there are no differences, the image is not added to the repository. By default, the storing directory is PRIME_NETWORK_HOME/NCCMComponents/NEIM/images/, where PRIME_NETWORK_HOME is the Prime Network installation directory (by default, /export/home/*network-user*; where *network-user* is the operating system user for the Prime Network application and an example of *network-user* is network310). From there, they are imported into the repository.

**Note** Before importing images, make sure internet connectivity is available to the server; otherwise, the imported images will not be populated with RAM, boot ROM, and feature set.

When you download an image from Cisco.com, Prime Network creates a job for the download. The job information is saved, along with other job information, in the database.

To import images into the Prime Network image repository:

**Step 1** Choose **Images > Repository**.

**Step 2** Choose the appropriate method:

| To import from: | Choose: | Notes |
|---|---|---|
| Cisco.com web site | **From Cisco.com** | Make sure the Cisco.com credentials are set on the Image Management Settings page. You must enter a device type, software version, and feature set. |
| Another IPv4 or IPv6 gateway server | **From External Repository** | The GUI will display available images, their size, and whether they already exist in the repository. |
| A file system on the local gateway server | **From File System** | Change and Configuration Management displays all images or packages (bin, pie, smu, and so on) from the directory specified in the Image Management Settings page, and also from its sub directory in order to support tar files. |

**Step 3** Select the images and import them. Change and Configuration Management redirects you to the Jobs page, where you can monitor the status of the import job.

**Step 4** Choose **Images > Repository** again to refresh the list of images.

**Step 5** If a field displays NA, the image attributes were not available from the image header. (If pre-existing filters are still in use, you may need to click **Clear Filter**.) We recommend that you manually enter the information to ensure the accuracy of the upgrade analysis.

**Step 6** Delete files from the storing directory (if applicable) to free space for future imports.

After the import, you can also add informational text to the Comments field. Normally at this point you will distribute the images; see Distribute Images and Make Sure They Will Work, page 4-27.

# New Devices: Create an Image Baseline

Use this method to create an image baseline—that is, import software images directly from existing devices to the Prime Network image repository. This is useful when you add devices from a new device series or family. This information is imported:

- Cisco IOS devices: Currently-running images. For Cisco 7600 series devices with ACE cards: ACE card images in the Cisco 7600 supervisor module filesystem (FTP, TFTP, and SCP are all supported).
- Cisco IOS XR devices: pie and .vm files corresponding to active packages.

**Note** Image baseline is not applicable for Cisco CPT devices.

To import images from devices into the Prime Network image repository:

**Step 1** Choose **Images > Repository**.

**Step 2** From the Import drop-down list, choose **From Devices**. The Devices dialog box displays information about the device. For long texts in the **Element Type**, **Software Version**, and **Running Image** fields, hover the cursor over the hyperlink to display the entire contents.

**Step 3** To import images from devices of a specific group, click **Select Groups**. Click the hyperlinked device group name to view the list of devices that belong to the group. See Device Groups Setup Tasks, page 4-8 for more information on user-defined device grouping.

**Step 4** Select the required device group in the Device Groups page and click **OK**.

The devices that belong to the selected device group are highlighted in the Devices page. You can also import all the devices existing in a group. To do so:

- Select a device group and click **Import from Group**.
- Enter the scheduling information as explained after Step 5 and click **Import from Group**.

**Step 5** In the Devices page, click **Import**. A scheduler popup window appears.

**Step 6** Enter the scheduling information. By default, jobs are scheduled to run as soon as possible.

**Note** The time you specify here to schedule the import job is the server time.

**Step 7** If you do not want to use the default transfer protocol, select a different protocol:

- TFTP (unsecured; Cisco ASR 5000 series devices use this protocol for importing images)
- SFTP/SCP (secured; Cisco IOS XR devices and Cisco Nexus 5000 and 7000 series devices use SFTP, and Cisco IOS devices use SCP)
- FTP (unsecured)

**Step 8** If you have selected two or more devices, click one of the following to specify the operation mode:

- Parallel Order—Imports images from all devices at the same time.
- Sequential Order—Allows you to specify the order of the devices to import the images from. You can do so by moving the devices up and down in the Device Order box.

**Note** The Device Order box will not be available, if the number of devices is more than 300. Prime Network sequences the devices based on the default order (that you used while selecting the devices.)

**Step 9** Enter the e-mail ID(s) to which to send a notification after the import job is complete. For two or more users, enter a comma-separated list of e-mail IDs. A notification e-mail is sent based on the e-mail option specified in the Image Management Settings page.

**Note** Before you enter the e-mail ID(s), ensure that you have set up the SMTP host and SMTP port in the Image Management Settings page (see Change Image Management Global Settings, page 4-53). The e-mail ID(s) configured in the Image Management Settings page, if any, will be displayed by default. You can modify the e-mail ID(s) if required.

**Step 10** Click **Import**. Prime Network redirects you to the Jobs page, where you can monitor the status of the import job.

**Note** If you chose to import all devices from a group and if there is a change in the group by addition or deletion of devices after job creation, Prime Network updates the job accordingly such that all the devices available in the group at the time of execution of the job are considered.

**Step 11** Choose **Images > Repository** again to refresh the list of images. If any of the image information could not be retrieved, the field will display NA. (If pre-existing filters are still in use, you may need to click **Clear Filter**.)

**Step 12** If a field displays NA, the image attributes were not available from the image header. (If pre-existing filters are still in use, you may need to click **Clear Filter**.) We recommend that you manually enter the information to ensure the accuracy of the upgrade analysis.

**Step 13** Delete files from the storing directory (if applicable) to free space for future imports.

After the import, you can also add informational text to the Comments field. Normally at this point you will distribute the images; see Distribute Images and Make Sure They Will Work, page 4-27.

# Distribute Images and Make Sure They Will Work

Prime Network copies an image to a network element without activating it. This lets you perform these tasks before activating the image:

- Find out if there is insufficient memory, clear the disk space for distributing the image or package
- Do an upgrade analysis to check the suitability of the device for the chosen image

If appropriate, the images can be activated as part of the distribution job, and these tasks can also be performed:

- Commit Cisco IOS XR (so that changes are saved across device reloads).
- Perform a warm upgrade, where one Cisco IOS image can read in and decompress another Cisco IOS image and transfer control to this new image (thus reducing the downtime of a device during planned software upgrades and downgrades).
- Perform an in-service software upgrade (ISSU) for Cisco ASR 903 devices to update the router software with minimal service interruption. CCM performs a s*ingle command upgrade* that installs a complete set of sub-packages using one command. Before using CCM to perform a single command upgrade, the ASR 903 device must *already* be booted in sub-package mode.

**Note** Cisco ASR 903 devices must be booted in sub-package mode *before* using CCM to perform an ISSU. For more information, see the *Cisco ASR 903 Series Router Chassis Configuration Guide.*

- Activate Cisco ASR 5000 boot configuration files

Prime Network uses the image staging location and transport protocol (TFTP, by default) specified on the Image Management Settings page. Prime Network displays the available upgradable modules and the storage partitions (if any) on the network element for the image distribution, from which you can choose the storage location you want to use.

The final step is to schedule the distribution job to occur either as soon as possible or at a future date (the default is as soon as possible).

## What is Upgrade Analysis?

An upgrade analysis checks the attributes of the selected image, checks certain device features, and generates a separate report for each device. It is required before any image can be distributed. However, even if the upgrade analysis reports errors, Prime Network will allow you to proceed with the distribution (because an error can be a simple matter of an unpopulated field). Prime Network gathers this information from two sources:

- The Prime Network image repository, which contains information about minimum RAM, minimum Flash, and so on, in the image header.
- The Prime Network inventory, which contains information about the active images on the device, as well as Flash memory, modules, and processor details.

**Note** For Cisco Nexus 5000 or Cisco Nexus 7000 series devices, Prime Network displays the upgrade analysis results for both the system and kickstart images selected for the device.

An upgrade analysis verifies that the device contains sufficient RAM or storage, the image is compatible with the device family, and the software version is compatible with the image version running on the device.

Table 4-3 denotes the symbols used on the Distribution page.

***Table 4-3 Status Icons***

| Symbol | Description | |
|---|---|---|
| | **In Device Status Column** | **In Distribution Upgrade Analysis Column or Activation Analysis Results** |
| | Device is available for upgrade analysis and distribution. | Device passed without warnings. |
| | Device is not available for upgrade analysis or distribution. Most likely the device is in the Maintenance investigation state or the Unreachable communication state. Click the device hyperlink and open the device properties popup to see details about the device. | Device passed with warnings. Click the icon to get more information. |
| | n/a | Device did not pass analysis. Click the icon to get more information. |

## Distribute Images to Devices

The following procedure explains how to perform an image distribution. You can also use this procedure to perform an upgrade analysis and then exit the procedure before performing the distribution.

### Before You Begin

- If you are doing a Cisco IOS XR version upgrade (which upgrades the core package), see Software Images, page 4-24 for information about other packages that you should upgrade at the same time.
- The device VNE (the device model in Prime Network) must be in a managed state when you run the command. (This means the VNE Communication State must be Reachable, and the Investigation State must be Normal or Incomplete. For more information on VNE states, see the *Cisco Prime Network 3.10 Administrator Guide*.)
- Make sure you have the permissions to perform the distribute operation. You will not be allowed to schedule a distribution job, if you do not have permissions.

To distribute images and use upgrade analysis:

**Step 1** Choose **Images > Distribute** and then choose the device type (**IOS** or **IOS XR**) and selection method (by image or package, or by device). It is often easier to start with devices due to the sometimes cryptic nature of software image names. In this example we start with devices.

a. To choose devices of a specific device group, click **Select Groups** in the table header. Click the hyperlinked device group name to view the list of devices that belong to the group.

b. Select the required device group in the Device Groups page and click **OK**.

c. Choose one or more devices and click **Next**.

**Step 2** Prime Network displays all images or packages which are valid for the selected devices from the internal image repository (for example, kickstart images for Cisco Nexus 5000 or Cisco Nexus 7000, and boot configs for Cisco ASR 5000). You can also choose **From External Repository** from the drop-down list (in the table header) to display the images or packages from the external image repository. Choose an image and click **Next**.

**Note** CCM allows image distribution from external repository only through FTP. Make sure you have configured the required credentials for accessing the external image repository in the Image Management Settings page.

**Step 3** In the Select Storage page, choose a storage location by device or for all devices. This specifies where on the network element the image or package will be copied when it is distributed. This operation is not applicable for Cisco CPT devices.

**Step 4** Perform an upgrade analysis to check whether the network element has sufficient space for the image or package by clicking **Upgrade Analysis**. After a few moments, Prime Network displays the results of the analysis in the Upgrade Analysis column. Click the symbol next to the icon to see the Upgrade Analysis report.

| Symbol | Description | |
|---|---|---|
| | In Device Status Column | In Distribution Upgrade Analysis Column or Activation Analysis Results |
| | Device is available for upgrade analysis and distribution. | Device passed without warnings. |
| | Device is not available for upgrade analysis or distribution. Most likely the device is in the Maintenance investigation state or the Unreachable communication state. Click the device hyperlink and open the device properties popup to see details about the device. | Device passed with warnings. Click the icon to get more information. |
| | n/a | Device did not pass analysis. Click the icon to get more information. |

If an error is reported, you will see a prompt asking you to confirm whether or not to proceed with the operation.

**Note** Check the report to verify whether the storage location has sufficient space for the image or package. If the space is insufficient, the distribution will fail. If there is insufficient memory, you can choose to clear the disk space while scheduling the distribution in the Schedule Distribution page.

**Step 5** If you do not want to distribute any images or packages (for example, if you only wanted to perform a manual upgrade analysis), click **Cancel**. Otherwise, proceed to Step 6.

**Step 6** Click **Next** to open the Schedule Distribution page in the wizard, and complete the schedule information.

**Note** You can proceed with scheduling the distribution only if upgrade analysis is completed for all the devices (spanning across multiple pages) in the Select Storage page.

| Field | Description |
|---|---|
| Schedule Distribution | When the distribution job should run.<br>**Note** The time you specify here to schedule the distribution job is the server time. |
| File Transport Protocol | Overrides the default transfer protocol (as configured on the Image Management Settings page). |
| Clear Flash | (Optional) If the job encounters insufficient space, recovers the disk space occupied by files that were marked for deletion in the device. |

| Field | Description |
|---|---|
| E-mail Id(s) | E-mail ID(s) to which to send a notification after the scheduled distribution job is complete. For two or more users, enter a comma-separated list of e-mail IDs. A notification e-mail is sent based on the e-mail option specified in the Image Management Settings page. |
| Install Add Package(s) | (Optional) Adds packages during distribution for Cisco IOS XR devices |
| Schedule Activation | (Optional) Starts an activation job once the images or packages are distributed (immediately or at future time). For multiple devices, we recommend that you perform the activation separately from the distribution. |
| Process | For multi-device jobs, controls the job processes for both distribution and activation. If you chose Sequentially, you can also do the following:<br>• Specify the order in which the operations should be processed, by moving the items up and down in the Reorderable Rows box.<br>• Stop the job if an error is encountered by checking the **Stop if an error occurs** check box.<br>**Note** If the job includes a reload, choose **Sequentially**. Otherwise, routers in the connectivity path of other routers may reload and cause problems. |
| Commit | Commits the packages after distribution for Cisco IOS XR devices. |
| Warm Upgrade | (For Cisco IOS only) Activates the Warm Upgrade feature to reduce the device downtime during the distribution process. |
| ISSU | (For Cisco ASR 903 devices only) Activates in-service software upgrade (ISSU) to update the router software with minimal service interruption. CCM performs the ISSU in sub-package mode (see Distribute Images and Make Sure They Will Work, page 4-27).<br>**Note** For Cisco ASR 903 devices, you can perform either warm upgrade or ISSU only. |

**Step 7** Click **Finished**. You are redirected to the Jobs page, where you can check the status of the distribution job.

**Note** Distribution fails if a timeout occurs after 30 minutes. You can view the job results for information on why the distribution failed. Remember to delete older images and packages from the staging directory.

# Activate Cisco IOS Software Images

These topics describe the tasks you can perform from the Activate page:

- Activate Cisco IOS Software Images
- Activate After Performing Boot Priority Modification for Cisco ASR 5000 Series Devices

When a new Cisco IOS image is activated on a device, it becomes the running image on the disk. Deactivated images remain on the disk to be removed by a user. Older images are automatically deactivated.

#### Before You Begin

- The device VNE (the device model in Prime Network) must be in a managed state when you run the command. (This means the VNE Communication State must be Reachable, and the Investigation State must be Normal or Incomplete. For more information on VNE states, see the *Cisco Prime Network 3.10 Administrator Guide*.)
- Make sure you have the permissions to perform the activate operation. You will not be allowed to schedule an activation job, if you do not have permissions.

## Activate Cisco IOS Software Images

To activate a Cisco IOS image on a network element:

**Step 1** Choose **Images > Activate > IOS** and the activation method (by **Images** or **Devices**). It is often easier to start with devices due to the sometimes cryptic nature of software image names. In this example we start with devices.

**Step 2** Prime Network displays all managed devices. It also displays the images that are currently running on the devices. You can filter by device name, IP address, element type, running image, or software version.

a. To choose devices of a specific device group, click **Select Groups** in the table header. Click the hyperlinked device group name to view the list of devices that belong to the group.

b. Select the required device group in the Device Groups page and click **OK**.

c. Choose one or more devices and click **Next**. Prime Network displays all images or packages which are valid for the selected devices from the internal image repository (for example, kickstart images for Cisco Nexus 5000 or Cisco Nexus 7000, and boot configs for Cisco ASR 5000). You can also choose **From External Repository** from the drop-down list (in the table header) to display the images or packages from the external image repository.

**Step 3** Prime Network displays all images or packages which are valid for the selected devices from the internal image repository.

Prime Network displays only root level bin files for selection. For a Cisco Nexus 5000 or Cisco Nexus 7000 series device, Prime Network displays the kickstart images available on the device in the Kickstart Images field. The field displays N/A if there are no kickstart images for the device.

**Step 4** Choose the image that you want to activate on the devices, and click **Next**.

**Step 5** For Cisco ASR 5000 series device, the Enter Boot Config page appears. You can activate a boot configuration file on the device in addition to an image. Select a boot configuration file from the available list and click **Save** and then **Next**.

**Step 6** Prime Network performs an image analysis. Check the Image Analysis page to see if analysis was successful. Click the icon in the Analysis column to get information about why the operation can or cannot proceed.

| Symbol | Description | |
|---|---|---|
| | In Device Status Column | In Distribution Upgrade Analysis Column or Activation Analysis Results |
| | Device is available for upgrade analysis and distribution. | Device passed without warnings. |
| | Device is not available for upgrade analysis or distribution. Most likely the device is in the Maintenance investigation state or the Unreachable communication state. Click the device hyperlink and open the device properties popup to see details about the device. | Device passed with warnings. Click the icon to get more information. |
| | n/a | Device did not pass analysis. Click the icon to get more information. |

If it cannot proceed, you will not be permitted to continue. Otherwise, click **Next**.

**Step 7** Enter the scheduling information in the **Schedule Activation** page. By default, jobs are scheduled to run as soon as possible.

**Note** The time you specify here to schedule the activation job is the server time.

**Step 8** Enter the e-mail ID(s) to which to send a notification after the scheduled activation job is complete. For two or more users, enter a comma-separated list of e-mail IDs. A notification e-mail is sent based on the e-mail option specified in the Image Management Settings page.

**Step 9** (For Cisco IOS only) Activate the **Warm Upgrade** option, which allows a Cisco IOS image to read in and decompress another Cisco IOS image and transfer control to this new image (thus reducing the downtime of a device during planned software upgrades and downgrades).

**Step 10** (For Cisco ASR 903 devices only) Activate the **ISSU** option, to update the router software with minimal service interruption. CCM performs the ISSU in sub-package mode (see Distribute Images and Make Sure They Will Work, page 4-27).

**Note** For Cisco ASR 903 devices, you can perform either warm upgrade or ISSU only.

**Step 11** Click one of the following to specify the operation mode, if you have selected two or more devices in the Select Devices page.

- **In Parallel**—Activates all packages for the devices at the same time.
- **Sequentially**—Allows you to define the order of the devices to activate the packages for.

**Step 12** Click **Finished** to schedule the activation.

### Activate After Performing Boot Priority Modification for Cisco ASR 5000 Series Devices

To modify boot priorities for Cisco ASR 5000 series devices and then perform activation:

**Step 1** Choose **Images > Activate > IOS** and the activation method (by **Devices**).

**Step 2** Choose the Cisco ASR 5000 device family from the table header.

Prime Network displays all managed Cisco ASR 5000 series devices. It also displays the images that are currently running on the devices. You can filter by device name, IP address, element type, running image, or software version.

**Step 3** Select a Cisco ASR5000 series device, choose the **Perform Edit Boot Priorities** option from the drop-down menu in the table header, and then click **Next**. The Select Boot Config page appears.

**Step 4** Click the **Edit Boot Priorities** hyperlink. The Current Boot Priorities table lists the existing boot configuration files with their priorities.

**Step 5** Provide the following inputs to set up and fetch the desired boot priorities:

- Number of boot priority entries to be maintained. Value should be in the range of 1-10.
- Boot priority number to start with. Value should be in the range of 1-100. Boot priority starting value should be greater than or equal to the number of boot priorities to be maintained.

**Step 6** Click **Go** to generate boot priorities based on the inputs provided. The modified boot priorities are listed in the table below.

**Step 7** You can choose to perform one of the following for each row in the table:

- **Edit**—Modify the boot priority value, the image name, and the configuration file, if required. The modified boot priority value should be unique.
- **Delete**—Delete the boot configuration priority.
- **Add Row**—Add boot priorities to the existing list. CCM generates boot priority values based on the inputs provided. Note that only the top ten boot priorities are considered for the device.

**Step 8** Click **Save**. A dialog box appears listing the existing and the modified boot priorities for your confirmation.

**Step 9** Click **Save** to confirm and apply the boot priority changes.

**Step 10** You can then schedule the activation as explained in steps 7 through 13 in the Activate Cisco IOS Software Images topic.

# Perform Cisco IOS XR Software Package Operations

**Note** We recommend that you do *not* commit the package change until the device runs with its configuration for a period of time, until you are sure the change is appropriate. In that way, the change is not yet persisted across device reloads.

These topics explain how to perform package operations:

- Notes on Cisco IOS XR Packages, page 4-35
- Add Cisco IOS XR Packages, page 4-35
- Activate, Deactivate, and Delete Cisco IOS XR Packages, page 4-36

- Synchronize and Upgrade Satellites for Cisco ASR 9000 Devices, page 4-38
- Commit Cisco IOS XR Packages Across Device Reloads, page 4-39
- Roll Back Cisco IOS XR Packages, page 4-40


## Notes on Cisco IOS XR Packages

Package management includes the add, activate, deactivate, commit, and rollback operations on Cisco IOS XR devices. Before you perform any of these operations, read the following:

- When doing a version upgrade (which upgrades the core package and involves a router reload) on a Cisco IOS XR device, all of the packages on the router should be upgraded at the same time, as part of the same job. For example, if the c12k-mini, c12k-mgbl, c12k-mpls, c12k-k9sec, and c12k-mcast packages are on the router at version 3.4.1, when upgrading to version 3.5.0, all of the packages must be upgraded at the same time to version 3.5.0.

**Note** An upgrade pie is required only when you upgrade Cisco IOS XR devices from version 3.x to 4.x. You must deactivate and remove the upgrade pie, if you wish to perform any install operations, including the install commit operation on the devices upgraded from 3.x to 4.x.

- When upgrading the core router package (such as c12k-mini or comp-hfr-mini), the manageability package (such as c12k-mgbl or hfr-mgbl-p) must be upgraded at the same time to ensure that the router remains manageable after the reload.
- Cisco IOS XR routers support the **clear install rollback oldest x** command, that allows you to manage the number of rollback points maintained on the router. Executing this CLI command periodically on the router allows you to limit the number of rollback points. When executing this command, you must ensure that at least one valid rollback point is always maintained to enable Prime Network to show the package status correctly. We recommend that you maintain about 20 rollback points on the router.
- NEIM does not support upgrading a router running Cisco IOS software to Cisco IOS XR software.

For more information, refer to the *System Management Configuration Guide* for the Cisco IOS XR release and device of interest.

## Add Cisco IOS XR Packages

Image Management supports package addition as a separate operation for Cisco IOS XR devices. To complete the package management life cycle, Image Management supports adding a package from a pie file, which is already present in the Cisco IOS XR device storage.

**Before you begin:**

Make sure you have the permissions to perform package addition. You will not be allowed to schedule a package addition job, if you do not have permissions.

To add packages for Cisco IOS XR devices:

**Step 1** Choose **Images > Package Add**. The Package Add wizard displays all the Cisco IOS XR devices in the Select Device(s) page.

**Step 2** Select a device and click **Next** to open the Select Package(s) page. Prime Network displays all the packages available for the selected device.

**Step 3** Choose the package(s) that you want to add for the selected device and click **Next** to open the Schedule Package Addition page in the wizard.

**Step 4** Enter the scheduling information. By default, jobs are scheduled to run as soon as possible.

**Note** The time you specify here to schedule the package addition job is the server time.

**Step 5** If you have selected two or more devices in the Select Devices page, click one of the following to specify the operation mode:

- In Parallel Order—Add packages for all devices at the same time.
- In Sequential Order—Allows you to specify the order of the devices to import the packages for.

**Step 6** Enter the e-mail ID(s) to which to send a notification after the scheduled package addition job is complete. For two or more users, enter a comma-separated list of e-mail IDs. A notification e-mail is sent based on the e-mail option specified in the Image Management Settings page.

**Step 7** Click **Finished**. Prime Network schedules the job and redirects you to the Jobs page, where you can monitor the status of the job.

## Activate, Deactivate, and Delete Cisco IOS XR Packages

**Note** For Cisco IOS XR devices, we recommend that you do not commit the package change until the device runs with its configuration for a period of time, until you are sure the change is appropriate. In that way, the change is not yet persisted across device reloads.

### Before You Begin

- If you are doing a Cisco IOS XR version upgrade (which upgrades the core package), see Software Images, page 4-24 for information about other packages that you should upgrade at the same time.
- The device VNE (the device model in Prime Network) must be in a managed state when you run the command. (This means the VNE Communication State must be Reachable, and the Investigation State must be Normal or Incomplete. For more information on VNE states, see the *Cisco Prime Network 3.10 Administrator Guide*.)

To activate or deactivate a Cisco IOS XR package, or delete a Cisco IOS XR package from a device:

**Step 1** Choose **Images > Activate > IOS-XR** and the activation method (by **Packages** or **Devices**.). It is often easier to start with devices due to the sometimes cryptic nature of software image names. In this example we start with devices.

**Step 2** Prime Network displays all managed devices. (It also displays the packages that are currently running on the devices.) From this page you can also view the running package of the Cisco IOS XR device.

**a.** To choose devices of a specific device group, click **Select Groups**. In the Device Groups page, you can view the user-defined device groups. Click the hyperlinked device group name to view the list of devices that belong to the group. See Device Groups Setup Tasks, page 4-8 for more information on user-defined device grouping.

**b.** Select the required device group in the Device Groups page and click **OK**.

**c.** Choose one or more devices and click **Next**. Prime Network displays all packages which are valid for the selected devices. You can filter your results by package name and version.

d. Choose the packages that you want to activate on the devices, and click **Next**.

**Step 3** Specify the operations you want to perform. You can perform different operations on different devices or the same operation on all devices (by selecting the desired operation from the **Use the following Operation for all Packages** drop-down list in the table header). When you select a device, Prime Network will display all of the packages that are installed on the device.

a. Choose a package operation for each package. Cisco IOS XR packages can be removed from a device only if they have been deactivated. If you want to apply the same operation to all packages, choose the operation from the **Use the following Operation for all Packages** drop-down list in the table header, and click **Apply**.

b. (Optional) Check **Test Only** to run a test of the activation (or deactivation) procedure on the device. This will not change the real device configuration. (This is similar to using the Compatibility Check option in the rollback process.)

c. Click **Next**. The Package Analysis page is displayed. Check the Package Analysis page to see if analysis was successful. Click the icon in the Analysis column to get information about why the operation can or cannot proceed (it will be one of the icons listed in Table 4-3 on page 4-28). If it cannot proceed, you will not be permitted to continue. Otherwise, click **Next**.

**Step 4** Enter the scheduling information. By default, jobs are scheduled to run as soon as possible.

**Note** The time you specify here to schedule the activation job is the server time.

**Step 5** Enter the e-mail ID(s) to which to send a notification after the scheduled activation job is complete. For two or more users, enter a comma-separated list of e-mail IDs. A notification e-mail is sent based on the e-mail option specified in the Image Management Settings page.

**Step 6** (For Cisco Carrier Routing System (CRS) devices only) Activate the **ISSU** option, to update the router software with minimal service interruption. CCM performs the ISSU in sub-package mode (see Distribute Images and Make Sure They Will Work, page 4-27).

**Step 7** Check the **Commit** check box to commit the packages after activation.

**Note** We recommend that you do *not* commit the package change until the device runs with its configuration for a period of time, until you are sure the change is appropriate. In that way, the change is not yet persisted across device reloads.

**Step 8** Click one of the following to specify the operation mode, if you have selected two or more devices in the Select Devices page.

- **In Parallel**—Activates packages for all devices at the same time.
- **Sequentially**—Allows you to define the order of the devices to activate the packages for.

**Step 9** Click **Finished** to schedule the activation.

**Step 10** After the job completes:

- For Test Only jobs, repeat this procedure to activate the packages.
- If you activated or deactivated a Cisco IOS XR package, remember to commit your changes. However, we recommend that you do not commit the package change until the device runs with its configuration for a period of time, until you are sure the change is appropriate. In that way, the change is not yet persisted across device reloads. See Commit Cisco IOS XR Packages Across Device Reloads, page 4-39.

## Synchronize and Upgrade Satellites for Cisco ASR 9000 Devices

CCM provides satellite support for Cisco ASR 9000 devices. Satellites are used to enhance performance bandwidth of Cisco ASR 9000 devices. Each satellite is a Cisco IOS device connected to the Cisco ASR 9000 device. Multiple satellites can be connected to a single Cisco ASR 9000 device and all communications to the satellites happen only through the Cisco ASR 9000 device. Each satellite has its own configuration and software image.

CCM provides the following support for Cisco ASR 9000 device with satellites:

- Synchronization of all satellites together.
- Activation of the satellite pie image on Cisco ASR 9000 device with and without synchronization of satellites. You must run a CLI/XML command to check for compatibility and then push the image to the remote satellite.

### Synchronize all satellites together without activation

To synchronize all satellites together without activation:

**Step 1** Choose **Images > Activate > IOS-XR** and the activation method (by **Devices**).

**Step 2** Choose the Cisco ASR 9000 device family and the **Sync Satellites** option from the **Select Operations** drop-down menu in the table header.

Prime Network displays all managed Cisco ASR 9000 series devices having satellites. (It also displays the packages that are currently running on the devices.)

**Step 3** Click **Next** to schedule the synchronization for all the satellites together. You cannot select a particular satellite for synchronization. The Select Operation function is not applicable for the Sync Satellites option.

**Step 4** In the Schedule Activation page, provide the scheduling information for synchronization of all satellites.

**Note** The time you specify here to schedule the synchronization job is the server time.

**Step 5** Check the **Sync Satellite(s)** check box and click **Finished**. The Sync Satellite(s) check box is available only for Cisco ASR 9000 devices having satellites.

### Activate satellite image on Cisco ASR 9000 device with/without synchronization

To activate a satellite image on the Cisco ASR 9000 device with/without satellite synchronization:

**Step 1** Choose **Images > Activate > IOS-XR** and the activation method (by **Devices**).

**Step 2** Choose the Cisco ASR 9000 device family and the **Activate and/or Sync Satellites** option from the **Select Operations** drop-down menu in the table header.

**Step 3** Perform steps 3 through 7 in the Activate, Deactivate, and Delete Cisco IOS XR Packages, page 4-36 topic.

**Step 4** Check the **Sync Satellite(s)** check box, if you wish to upgrade and synchronize the satellites. The Sync Satellite(s) check box is available only for Cisco ASR 9000 devices having satellites.

**Note** Synchronization of satellites is done, only if the operation selected is activation or deactivation. Otherwise, synchronization will not happen even if this check box is selected.

**Step 5** Click **Finished** to schedule the activation and/or synchronization.

## Commit Cisco IOS XR Packages Across Device Reloads

Committing a Cisco IOS XR package makes the device package configurations persist across device reloads. The commit operation also creates a rollback point on the device. See Roll Back Cisco IOS XR Packages, page 4-40, for more information on rollback points.

**Note** We recommend that you do not commit package changes until the device runs with its configuration for a period of time, until you are sure the change is appropriate. In that way, the change is not yet persisted across device reloads.

### Before You Begin

- Verify that the package to be committed is operating properly (for example, by doing a **show status** command).
- The device VNE (the device model in Prime Network) must be in a managed state when you run the command. (This means the VNE Communication State must be Reachable, and the Investigation State must be Normal or Incomplete. For more information on VNE states, see the *Cisco Prime Network 3.10 Administrator Guide*.)
- Make sure you have the permissions to perform the commit operation. You will not be allowed to schedule a commit job, if you do not have permissions.

To commit a package after it has been activated, deactivated, or rolled back:

**Step 1** Choose **Images > Commit**.

**Step 2** Choose the network elements with the packages you want to commit.

**Step 3** Click one of the following (in the table header) to specify the commit mode:

- **Commit in Parallel**—Commits all changes at the same time.
- **Commit Sequentially**—Allows you to define the order in which the changes are committed.

**Step 4** Enter the scheduling information.

**Note** The time you specify here to schedule the commit job is the server time.

**Step 5** Enter the e-mail ID(s) to which to send a notification e-mail after the scheduled commit job is complete. For two or more users, enter a comma-separated list of e-mail IDs. A notification e-mail is sent based on the e-mail option specified in the Image Management Settings page.

**Step 6** Click **Commit**. By default, jobs are scheduled to run as soon as possible.

## Roll Back Cisco IOS XR Packages

Rolling back a Cisco IOS XR package reverts the device packages to a previous installation state—specifically, to a package installation rollback point. If a package has been removed from a device, all rollback points associated with the package are also removed and it is no longer possible to roll back to that point.

### Before You Begin

- Read Software Images, page 4-24, for information about managing rollback points on Cisco IOS XR devices.
- The device VNE (the device model in Prime Network) must be in a managed state when you run the command. (This means the VNE Communication State must be Reachable, and the Investigation State must be Normal or Incomplete. For more information on VNE states, see the *Cisco Prime Network 3.10 Administrator Guide*.)
- Make sure you have the permissions to perform the rollback operation. You will not be allowed to schedule a rollback job, if you do not have permissions.

To roll back a Cisco IOS XR package:

**Step 1** Choose **Images > Rollback**. Prime Network displays all Cisco IOS XR devices. You can filter the results by using the **Quick Filter** option.

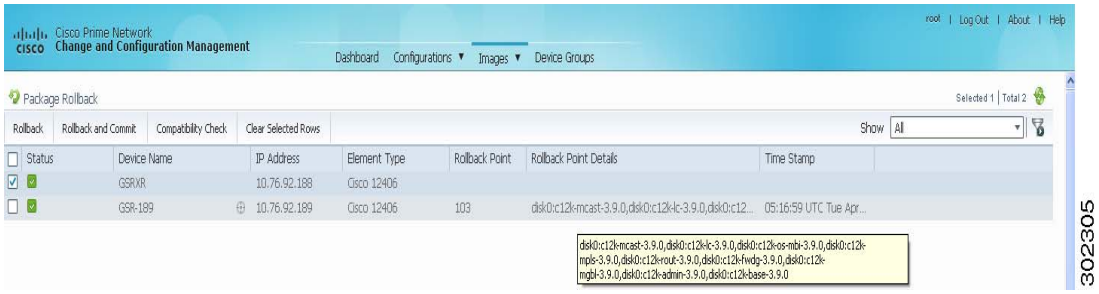
**Step 2** Choose the network elements. Prime Network populates the rollback points for the selected device package.

**Step 3** Choose a rollback ID from the Rollback ID drop-down list. The Rollback Point Details field lists the packages that were active when that ID was created.

**Step 4** To view all of the packages associated with the rollback point, place the mouse cursor on the Rollback Point Details field; see Figure 4-9 for an example. To view the time stamp associated with the selected rollback, see the value displayed in the Time Stamp field.

**Note** The date and time stamps are displayed according to the local time zone settings of the client.

*Figure 4-9 Packages Rollback Page with Rollback Point Details*



**Step 5** Click **OK** to close the popup window.

**Note** If a package has been deleted from the repository, the rollback points of the package are still displayed in the GUI. If you choose a rollback point for a deleted package, the rollback will fail. The job results popup provides information explaining why it failed.

**Step 6** (Optional) Click **Compatibility Check** in the table header to run a test of the rollback procedure on the device. This will not change the real device configuration. (This is similar to using the Test Only option in the activation process.)

**Step 7** Click **Rollback** or **Rollback and Commit**.

**Note** We recommend that you do not commit package changes until the device runs with its configuration for a period of time, until you are sure the change is appropriate. In that way, the change is not yet persisted across device reloads. See Commit Cisco IOS XR Packages Across Device Reloads, page 4-39.

**Step 8** Enter the scheduling information.

**Note** The time you specify here to schedule the rollback job is the server time.

**Step 9** Enter the e-mail ID(s) to which to send a notification after the scheduled rollback job is complete. For two or more users, enter a comma-separated list of e-mail IDs. A notification e-mail is sent based on the e-mail option specified in the Image Management Settings page.

**Note** Before you enter the e-mail ID(s), ensure that you have set up the SMTP host and SMTP port in the Image Management Settings page (see Change Image Management Global Settings, page 4-53). The e-mail ID(s) configured in the Image Management Settings page, if any, will be displayed by default. You can modify the e-mail ID(s) if required.

**Step 10** Click **Rollback**.

# Clean Up the Repository

The repository is purged according to the settings described in NEIM Setup Tasks, page 4-6. When files are removed from the repository, this does not affect files that are installed on the device. However, deleting a package could cause a rollback point to become unexecutable. If a package or version of a package that is associated with a specific rollback point is removed, it will no longer be possible to roll back to that point. See Roll Back Cisco IOS XR Packages, page 4-40.

To delete images from the Prime Network image repository:

**Step 1** Choose **Images > Repository**.

**Step 2** Select the image you want to delete and click the Delete button (with red **X**) in the table header.

**Step 3** To collectively delete all images in the repository, click the **Delete All** button in the table header. You will see a prompt asking you to confirm whether or not to proceed with the operation.

**Step 4** Click **OK** to confirm and image(s) available in the repository will be deleted.

These topics provide administrative information on CCM:

- Global Settings and Administration, page 4-47—How to use the Configuration Management Settings page to specify when configurations should be collected, when they should be purged, commands to exclude from comparisons, and other global settings.
- Change Image Management Global Settings, page 4-53—How to use the Image Management Settings page to specify the default transfer protocol, staging and storing locations, and credentials for accessing a vendor web site.
- Check the Processes, page 4-54—How CCM ensures communication security, authenticates and authorizes users, where log files for debugging purposes are located, and so forth.

You should also make sure you have properly set up CCM by reading Configuration Management Setup Tasks, page 4-5.

**Note** In the Configuration Management and Image Management Settings pages, CCM does not support the following special characters:

- For Password fields—>, <, ', /, \, !, :, ;, and "
- For all other fields—`, ~, @, #, $, %, ^, &, *, (, ), +, =, |, {, }, [, ], ', ?, >, <, /, \, !, :, ;, and "

# Configuration Audit

CCM facilitates a configuration compliance mechanism, which enables auditing configurations on a device against a specified configuration policy file (also called as a baseline or expected configuration). Prime Network facilitates administering multiple configuration policy files through a Configuration Audit Policy Manager. Each configuration policy is a set of CLI commands that define a desired baseline or expected configuration. Configuration policies can also be configured using valid, Java-based regular expressions. Table 4-4 provides examples of configuration policy CLIs.

*Table 4-4 Configuration Policy CLI Examples*

| Policy Name | Policy Description | Policy CLI |
|---|---|---|
| SamplePolicy1 | Sample policy for global configuration auditing | `spanning-tree mode rapid-pvst` |
| SamplePolicy2 | Sample policy for global regex and first sub level cli matching audit | `interface GigabitEthernet(.*)`<br>`  port-type nni` |
| SamplePolicy3 | Sample policy for global regex, first sub level cli matching, and second sub level regex matching | `router (.*)`<br>`  address-family ipv4 unicast`<br>`  network (.*)` |
| SamplePolicy4 | Sample policy for fixed cli matching | `interface GigabitEthernet3/4`<br>`  address-family ipv4 unicast` |

### Sample Configuration Policy

The following example shows a policy that performs audit for BGP configuration for a Cisco IOS router:

```
#BGP Configuration Audit
router bgp (.*)
   neighbor (.*) remote-as (.*)
   address-family ipv4
```

If user likes to have an audit check for specific BGP AS or neighbor ip address, the above CLI can be changed accordingly.

For example:

```
router bgp 65000
   neighbor (.*) remote-as 65001
    address-family ipv4
```

User can combine multiple different configurations into one policy.

For example:

```
#BGP Configuration Audit
router bgp (.*)
   neighbor (.*) remote-as (.*)
   address-family ipv4
# Interface MEP check
interface GigabitEthernet(.*)
   ethernet (.*)
      mep domain UP (.*)
```

Configuration audit can be scheduled against multiple configuration files to obtain an audit report that indicates the existence of configuration sequences stated in the baseline policy and any deviations from the baseline.

You can define a configuration policy, select the devices that need to be audited against the policy, and schedule the audit job to run immediately or at a later point in time. The audit job compares the CLI commands (as part of the configuration policy) against the actual running configuration on the device to identify the discrepancies.

You can view the status of all the scheduled configuration audit jobs in the Job Manager page. The configuration audit results are in the form of a report indicating the discrepancies (missing configuration commands on the device) in red and the matching commands in green.

# Manage Configuration Policies

CCM allows you to create, modify, view, and delete configuration policies. Choose **Configuration Audit > Configuration Policies**. The Configuration Policies page provides the list of existing policies. You can search the configuration policies by CLI strings.

## Create Configuration Policy

To create a configuration policy:

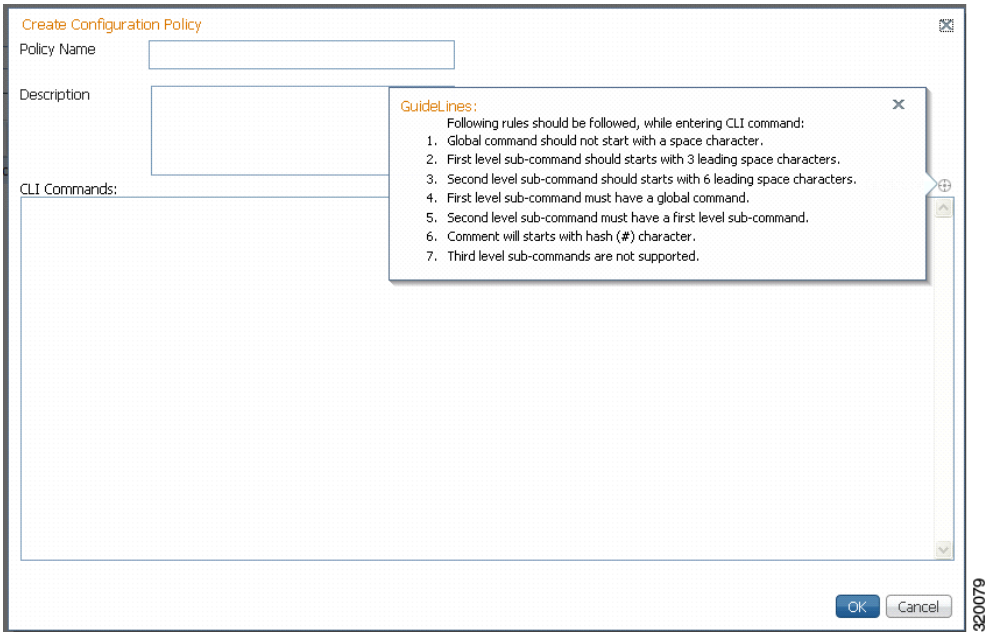
**Step 1** In the Configuration Policies page, click **Create**.

**Step 2** Provide the policy name and description.

**Step 3** Enter the CLI commands to set up a baseline configuration for that policy. This can also be a valid, Java-based regular expression. See Table 4-4 for sample configuration CLIs.

**Step 4** Make sure you follow the guidelines while entering the CLI commands. Click **Guidelines** to view these guidelines as shown in Figure 4-10.

***Figure 4-10 Create Configuration Policy-Showing Guidelines***




### Edit, View, or Delete Configuration Policy

In the Configuration Policies page, you can also do the following:

- Select a policy and click **Edit** to modify the policy description and CLI commands. You cannot modify the policy name. Keep in mind the policy guidelines while modifying the CLI commands.
- Select a policy and click **View** to view the policy name, description, and CLI commands.
- Select a policy or multiple policies and click **Delete** to delete the configuration policies. You cannot delete a policy if it is part of a scheduled audit job.

## Schedule Configuration Audit

You can schedule configuration audit jobs to run immediately or at a later point in time.

**Note** Only a maximum of 10 policies and 500 devices can be used for scheduling an audit job.

To schedule a configuration audit job:

**Step 1** Choose **Configuration Audit > Basic Audit**. The Select Configuration Policies page lists the available configuration policies. You can search the configuration policies by using CLI strings.

**Step 2** Select the desired configuration policy from the available list and click **Next**.

**Step 3** In the Select Devices page, select the devices that must be audited against the selected configuration policy, and then click **Next**.

**Step 4** In the Schedule Audit page, provide a job name and the scheduling information for the configuration audit job. You can choose to run the audit job immediately or at a later point in time. A popup with the server time is available to assist you in setting up the time for scheduling the audit job.

**Step 5** Click **Audit**. You will be redirected to the Configuration Audit Jobs page.

**Note** Once scheduled, you cannot edit the policies or devices that are part of the scheduled job.

# View Configuration Audit Jobs and Audit Results

The Configuration Audit Jobs page (**Configuration Audit > Configuration Audit Jobs**) provides the following details:

- Jobs—This table lists all configuration audit jobs submitted by the login user. The 'root' user can view jobs submitted by other users, by selecting the username from the table header.
- History—For a selected job in the Jobs table, this table lists all the instances. You can select only one job at a time to view the history details.

You can select a job and click **View** to view the associated devices and policies, and the schedule for the selected audit job.

You can also use this page to suspend, resume, cancel, delete, or reschedule a job.

To view the configuration audit job details and the audit result:

**Step 1** Click on the hyperlinked **LastRun Result** (Success/Partial Success/Failure) against a particular job in the Jobs table.

The Configuration Audit Job Details dialog box displays the job details and the audit results for a device and policy combination, as shown in Figure 4-11. The Job Results table includes the device audited, policy against which the device was audited, audit status, and the running configuration version used for the audit. A blue tick mark in the Status column indicates 'Audit Pass', and a red X indicates 'Audit Fail'. Click the hyperlinked policy name to view the configuration policy details, with updates if the policy has been modified.

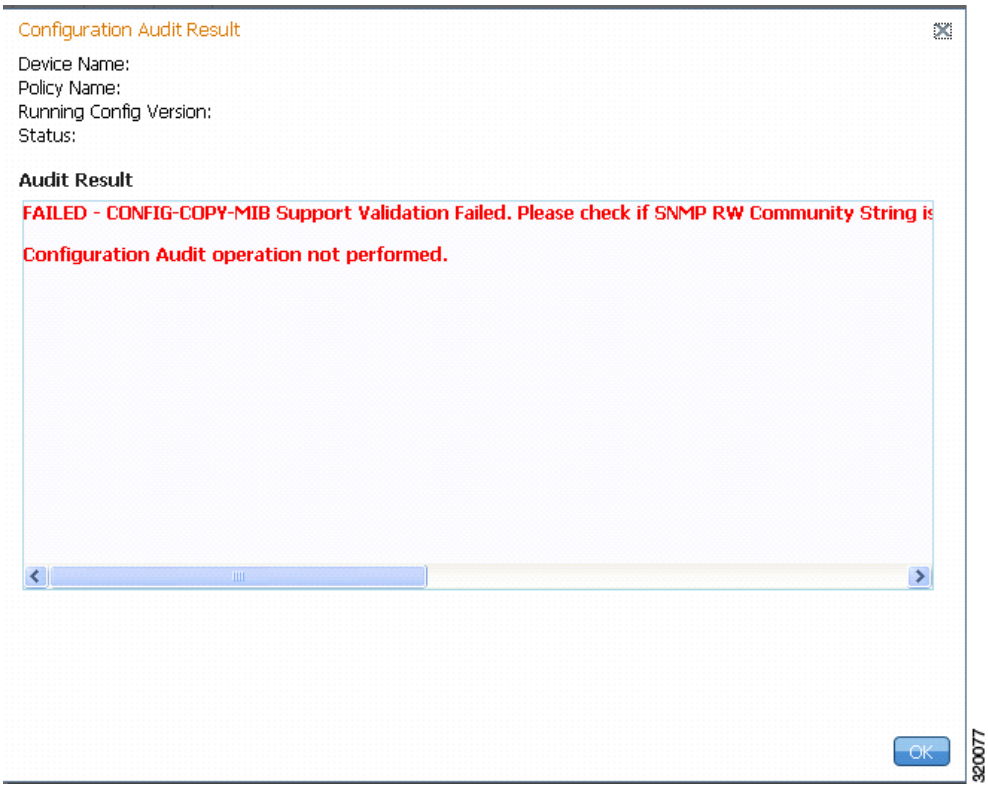
**Note** For Cisco Nexus devices, the VDC name is also displayed in the Device Name column.

*Figure 4-11 Configuration Audit Job Details*

**Step 2** Click on the hyperlinked **Status** (Pass/Fail icon) in the Job Results table. Or, click the hyperlinked Success or Failure hyperlink in the **Result** field of the History table.

The Configuration Audit Result dialog box displays the audit result with matching commands (for 'Audit Pass') and discrepancies or missing commands (for 'Audit Fail') between the policy and the running configuration on the device. See Figure 4-12 for an example of the Configuration Audit Result dialog box for an 'Audit Fail' scenario.

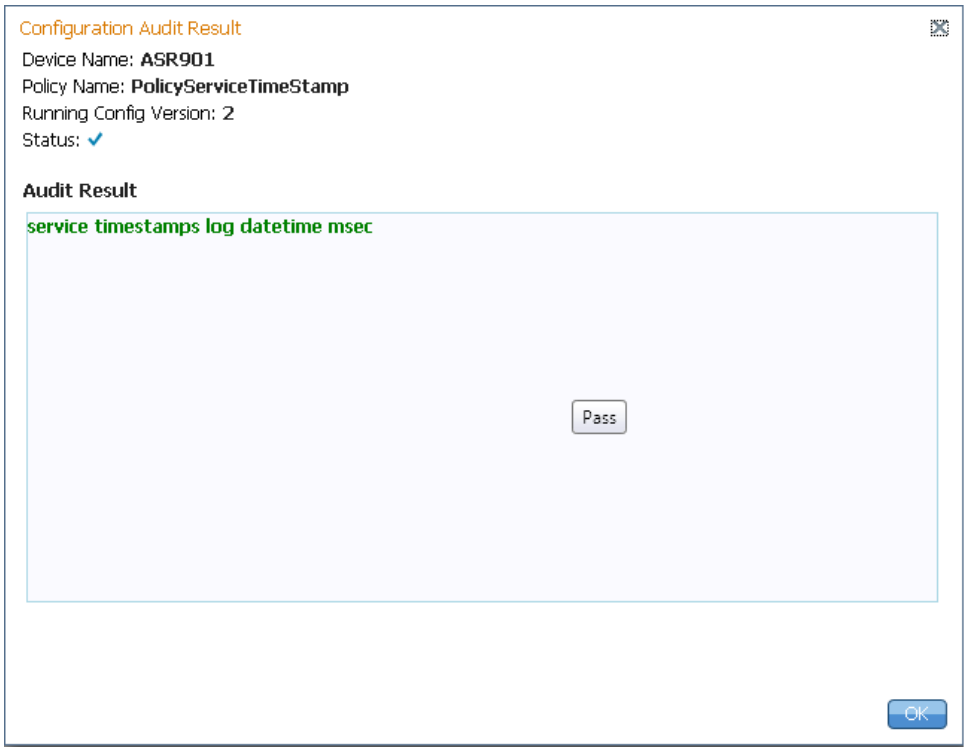
*Figure 4-12 Configuration Audit Result - Audit Fail*



The matching commands are displayed in green (see Figure 4-13), while the discrepancies are displayed in red (see Figure 4-12). For a failed job, the Audit Result section also displays the reason why the audit was not successful as shown in Figure 4-12. Some reasons for audit failure are:

- Failed to back up running configuration of the device
- Device not reachable
- Unable to download running configuration
- Device not under the scope of the user
- Policy is not available
- Invalid regular expression in the CLI

***Figure 4-13 Configuration Audit Result - Audit Pass***




**Step 3** Click **Export** in the Job Results table to export the audit job results to a .csv file. You can view the job details and audit results in the exported file.

# Global Settings and Administration

This topic contains the following sections:

- Change Configuration Archive Global Settings, page 4-48
- Change Image Management Global Settings, page 4-53
- Check the Processes, page 4-54

- Manage Jobs, page 4-55
- User Authentication and Authorization, page 4-55

# Change Configuration Archive Global Settings

To open the Configurations global settings page, choose **Configurations > Settings**. Table 4-5 lists all of the global settings you can configure for Configuration Management.

The backup settings you enter here do not affect the manual backups you can perform by choosing **Configurations > Backup**. The backups you perform from that page and the backups you configure on this Settings page are completely independent of each other.

**Note** Make sure that the configuration change detection schedule does not conflict with purging, since both processes are database-intensive.

*Table 4-5 Configuration Archive Global Settings*

| Field | Description |
|---|---|
| **Export Settings** | |
| Server Name | DNS-resolvable server name.<br>**Note** CCM supports export servers with IPv4 or IPv6 address. |
| Location | The full pathname of the directory to which Prime Network should copy the file on the server specified in the Server Name field. |
| Username | The login username that Prime Network should use when connecting to the server specified in the Server Name field. |
| Password | The login password that Prime Network should use when connecting to the server specified in the Server Name field. |
| Export Protocol | Default export protocol that Prime Network should use when exporting configuration files to another server. The choices are FTP and SFTP. The default is FTP.<br>You can override this protocol while scheduling an export job, if required. |
| **Archive Purge Settings** | |
| Minimum Versions to Retain | Minimum number of versions of each configuration that should be retained in the archive (default is 2). |
| Maximum Versions to Retain | Maximum number of versions of each configuration that Prime Network should retain (default is 5). The oldest configuration is purged when the maximum number is reached. Configurations marked “do not purge” are not included when calculating this number. |
| Minimum Age to Purge | Age (in days) at which configurations should be purged (between 5-360). |
| **Configuration Change Purge Settings** | |
| Purge Change Logs after | The age in days at which configuration change notifications (Change Logs) that are sent by devices should be purged. The default is 30 days and the range is 5-360. |

*Table 4-5 Configuration Archive Global Settings (continued)*

| Field | Description |
|---|---|
| **Global Settings** | |
| Transport Protocol | Default transport protocol that Prime Network should use when copying configuration files to and from a device. The options are TFTP, SFTP/SCP, and FTP. The default is TFTP. Note the following:<br>• The TFTP source interface on the devices must be able to reach the unit. Otherwise, the configuration management jobs that require TFTP may fail.<br>• To use SFTP/SCP for config transfers from a device to a unit, you need to ensure that an SSH server is configured and running on the device, such that the device acts as a server and the unit as a client during the transfer. For Cisco IOS XR devices, you need to configure the device with K9 security (k9sec) enabled images such that the SSH server is up and running on the device. |
| **Global Settings** | |
| Enable Periodic Config Backup | Detect ongoing configuration changes by performing a periodic collection of device information. Use this method if configurations change frequently and those changes are not important to you. CM compares the timestamp for the last configuration change on the archived version with the timestamp on the newer version. If they are different, CM backs the new file to the archive immediately. By default, this is not enabled.<br>You can set up an interval in the range of 1-100 hours. Default value is 72 hours.<br>**Note** This CM collection is independent of the Prime Network inventory collection. |
| Enable Periodic Sync for Out of Sync Devices (24Hours) | (For Cisco IOS only) Enables automatic synchronization of the out-of-sync devices on a periodic basis. Prime Network adds a device to the list of out-of-sync devices whenever the latest version of the startup configuration is not in sync with the latest version of the running configuration file on the device. |
| Enable Periodic Config Export | Allows CM to export archived configurations periodically to the export server. You can set up an interval in the range of 1-100 hours to export the archived configurations. The default value for export interval is 24 hours. You can also specify the start time for the periodic export operation.<br>If there are no configuration changes i.e. if the archived configuration is available in the export server, choose one of the following options to indicate how the export job should be performed:<br>• Export configuration file will all configuration—Overwrite the existing configuration on the export server.<br>• Do not export configuration file—Skip configuration export.<br>• Export configuration file with reference to previous configuration file—Create a configuration file with only a reference to the file having the actual configuration.<br>Refer to Configuration Export File Type for Devices, page 4-52, to know more about the type of configuration files exported for different devices. |

*Table 4-5 Configuration Archive Global Settings (continued)*

| Field | Description | |
|---|---|---|
| Enable Initial Config Syncup | Allows CM to fetch the configuration files from the network devices and archive it whenever a new device is added to Prime Network. If this setting is enabled:<br>• CM performs the configuration file fetch operation whenever the Prime Network gateway is restarted.<br>• The Disable Initial Config Syncup on Restart check box is enabled by default to prevent network device performance issues on subsequent Prime Network gateway restarts.<br>To preserve this setting such that CM fetches the configuration files from network devices on Prime Network gateway restarts, you must uncheck the Disable Initial Config Syncup on Restart check box after enabling the Enable Initial Config Syncup option.<br>**Note** The "sync up" described here pertains to making sure the archive correctly reflects the network device configurations. This is different from the CM Synchronize operation, where devices are checked to make sure their running and startup configurations are the same.<br>This "sync up" is required in order for Prime Network to populate the Configuration Sync Status dashlet (on the dashboard). | |
| | Disable Initial Config Syncup on Restart | Check the check box to set Enable Initial Config Syncup to its default setting (not enabled) if Prime Network restarts. |
| Enable Event-Triggered Config Archive | Detect ongoing configuration changes by monitoring device configuration change notifications. This setting also controls whether Prime Network populates the Configuration Changes in the Last Week and the Most Recent Configuration Changes dashlets (on the dashboard).<br>Use this method if you consider every configuration file change to be significant. When a notification is received, CM backs up the new running configuration file to the archive using one of the following methods.<br>**Note** If you are using event-triggered archiving, you should also make sure that exclude commands are properly configured. Exclude commands are commands that Prime Network ignores when comparing configurations, and they are controlled from the Settings page. Using this mechanism eliminates unnecessary file backups to the archive. | |
| | Sync archive on each configuration change | Upon receiving a change notification from a device, immediately backs up the device configuration file to the archive. |
| | Sync archives with changed configurations every ___ hours and ___ minutes | Upon receiving a change notification from a device, queue the changes and backs up the device configuration files according to the specified schedule. |
| **Restore Mode Settings** | | |
| Restore Mode | Mode for restoring configuration files to a device:<br>• Overwrite—Prime Network overwrites the existing configuration on the device with the file you selected from the archive. Check the **Use Merge on Failure** check box to restore configuration files in merge mode, if overwrite mode fails.<br>• Merge—Prime Network merges the existing running or startup configuration on the device with the configuration present in the version you selected from the archive. | |
| **E-mail Settings** | | |
| SMTP Host | SMTP server to use for sending e-mail notifications on the status of configuration management jobs to users. If an SMTP host is configured in the Image Management Settings page, the same value will be displayed here by default. You can modify it, if required. | |

*Table 4-5 Configuration Archive Global Settings (continued)*

| Field | Description |
|---|---|
| E-mail Id(s) | E-mail addresses of users to send a notification to after the scheduled job is complete. For two or more users, enter a comma-separated list of e-mail IDs. For example:<br>`xyz@cisco.com,abc@cisco.com`<br>The e-mail IDs configured here will appear by default while scheduling the configuration management jobs. However, you can add/modify the e-mail IDs then. |
| SMTP Port | SMTP port ID to connect to the host server. The default port is 25. |
| Email Option | Choose from the following options to specify when you want to send an e-mail notification for CM jobs:<br>• All—To send a notification e-mail irrespective of the job result.<br>• Failure—To send a notification e-mail only when the job has failed.<br>• No Mail—Do not send a notification e-mail on the job status.<br>The selected option will appear by default while scheduling CM jobs. However, you can modify the option then. |
| **Exclude Commands** | |
| (Device Selector) | Selected devices to which the exclude commands should be applied (that is, the commands will not be considered when comparing any type of device configuration files). The current selection is highlighted in green. All exclude commands applied to that selection will be listed below the device selector. See Notes on Exclude Commands, page 4-51. |
| Category Commands | Comma-separated list of commands to be excluded when comparing device configurations for any devices in this category (for example, all Cisco routers) |
| Series Commands | Comma-separated list of commands to be excluded when comparing device configurations for any devices in this series (for example, all Cisco 7200 series routers) |
| Device Commands | Comma-separated list of commands to be excluded when comparing device configurations for any devices of this same device type (for example, all Cisco 7201 routers) |

## Notes on Exclude Commands

Exclude commands are inherited; in other words, if three exclude commands are specified for Cisco routers, all devices is any of the Cisco router families will exclude those three commands when comparing configuration files.

**Caution** Exclude commands configured for a device family (such as Cisco 7200 Routers) will be applied to all device types in that family (Cisco 7201, Cisco 7204, Cisco 7204VXR, and so forth).

When you are working in the Exclude Commands GUI, your current selection will be highlighted in green. All exclude commands applied to that selection will be listed below the device selector. When Prime Network compares the router configuration files, it will exclude all of the commands listed in the Device Commands field. If a series is selected (example, Cisco 7200 Series), the commands listed in the Series Commands field will be excluded and so on.

The following procedure describes how to configure exclude commands.

**Step 1** Choose **Configurations > Settings**.

**Step 2** In the Exclude Commands area, navigate and choose one of the following (your selection is highlighted in green):

- A device category
- A device series
- A device type

**Step 3** Enter a comma-separated list of commands you want to exclude when comparing configuration files for that device category, series, or type. You can also edit an existing list of commands.

Your entries change to red until they are saved, and all affected device types, series, or categories are indicated in bold font.

**Step 4** If you want a device type to ignore the parent commands (that is, the series and category commands), check the **Ignore Above** check box.

**Step 5** Click **Save** to save your changes.

### Configuration Export File Type for Devices

The following table provides the types of configuration files exported for different types of devices.

| Device Type | Configuration File Exported | Condition(s) |
|---|---|---|
| Cisco IOS device | Only the latest running configuration | If there is no running version, the latest startup configuration is exported |
| Cisco IOS XR device | Latest running and startup configuration | None |
| Cisco ASR 5000 series devices | Latest running configuration | If there is no running version, boot configuration is NOT exported |
| Cisco 7600 device with ACE card | Latest running configuration | If there is no running version, the latest startup configuration is exported |
| Cisco Nexus device | Latest running configuration | If there is no running version, the latest startup configuration is exported |

# Change Image Management Global Settings

To open the Image Management global settings page, choose **Images > Settings**. Table 4-6 lists all of the global settings you can configure for Image Management.

***Table 4-6 Image Management Global Settings***

| Field | Description | |
|---|---|---|
| Transfer Protocol | Default transfer protocol to use when copying images to and from a device. This setting can be overridden when creating a distribution job (for example, if you know a device does not support the default protocol). FTP and TFTP are unsecured.<br>• The TFTP source interface on the devices must be able to reach the unit. Otherwise, the image management jobs that require TFTP may fail.<br>• To use SFTP/SCP for image transfers from a device to a unit, you need to ensure that an SSH server is configured and running on the device, such that the device acts as a server and the unit as a client during the transfer. For Cisco IOS XR devices, you need to configure the device with K9 security (k9sec) enabled images such that the SSH server is up and running on the device. (Cisco IOS XR devices use SFTP, and Cisco IOS devices use SCP). | |
| Flash Properties | If **Clear Flash** is checked, the flash memory is cleared on a device when performing a distribution if there is insufficient memory on the device. | |
| Warm Upgrade | If Warm Upgrade is checked, a Cisco IOS image can read in and decompress another Cisco IOS image and transfer control to this new image. This functionality reduces the downtime of a device during planned Cisco IOS software upgrades or downgrades. This can be overridden when creating the job. | |
| File Locations | Full pathname of directories where images are stored when they are being imported into the Prime Network image repository, or when they are being transferred out of the repository to devices. New directories must be empty and have the proper permissions (read, write, and execute permissions for users).<br>The entries must be full pathnames. In the following default locations, PRIME_NETWORK_HOME is the Prime Network installation directory, normally /export/home/*network-user*; where *network-user* is the operating system user for the Prime Network application and an example of *network-user* is network39. | |
| | Staging Directory | Location where images from the Prime Network image repository are placed before transferring them out to devices. The default is PRIME_NETWORK_HOME/NCCMComponents/NEIM/staging/. |
| | Storing Directory | Location where images from an outside source are placed before importing them into the Prime Network image repository (from Cisco.com, from existing devices, or from another file system). The default is PRIME_NETWORK_HOME/NCCMComponents/NEIM/images/. |
| External Server Details | Details about external server from which images can be imported into repository. | |
| | Server Name | IP address of the external server (IPv4 or IPv6 addresses supported). |
| | Image Location | Path where the image is located on the server. |
| | User Name | Username to access the external server. |
| | Password | Password to access the external server. |
| | SSH Port | SSH port ID to connect to the server. |

*Table 4-6 Image Management Global Settings (continued)*

| Field | Description | |
|---|---|---|
| E-mail Settings | Settings for automatic e-mail notifications about the status of jobs. | |
| | SMTP Host | SMTP server to use for sending e-mail notifications on the status of image management jobs to users. If an SMTP host is configured in the Configuration Management Settings page, the same value will be displayed here by default. You can modify it, if required. |
| | E-mail Id(s) | E-mail address of the user to send a notification to after the scheduled job is complete. For two or more users, enter a comma-separated list of e-mail addresses. For example:<br>**xyz@cisco.com,abc@cisco.com**<br>The e-mail IDs configured here will appear by default while scheduling the image management jobs. However, you can add/modify the e-mail IDs then. |
| | SMTP Port | SMTP port ID to connect to the host server. The default port is 25. |
| | Email Option | Controls when e-mail notifications for NEIM jobs are sent (can be overridden when creating the job):<br>• All—Send a notification irrespective of the job result.<br>• Failure—Send a notification e-mail only when the job has failed.<br>• No Mail—Do not send a notification e-mail on the job status. |
| Proxy Settings | Details about proxy server to use when importing images from Cisco.com | |
| | HTTP Proxy | HTTP proxy server to use for downloading images from Cisco.com. |
| | Port | Port address to use for downloading images from Cisco.com. |
| Vendor Credentials | Usernames and passwords that can be used to download images from Cisco.com. (See the procedure described in Check the Processes, page 4-54) | |

# Check the Processes

CCM runs on AVM 77. To check, start, stop, or restart the process, use the following commands:

```
dmctl status
dmctl start
dmctl stop
dmctl restart
```

# Manage Jobs

Prime Network redirects you to the Jobs page whenever a CM or image management job is scheduled to run immediately. When a job is created, Cisco Prime Network assigns it a job specification ID and attaches a time stamp, indicating when the job was created. Only the job creator and users with Administrator privileges can change the job settings. If a job involves more than 300 devices, the Jobs page only displays successful and unsuccessful jobs (not pending jobs).

Prime Network also facilitates automatic e-mail notification of the status of the CM and NEIM jobs upon completion based on the e-mail option you set up in the configuration and image management settings. The notification is sent to a list of e-mail IDs configured either in the settings page or while scheduling the job.

Keeps these items in mind when managing jobs:

- Job properties cannot be edited; you must delete the old job and create a new one.
- Jobs are persisted even if the gateway server is restarted.
- Only the job creators and users with Administrator privileges can perform the actions provided on the Jobs page (suspend, resume, reschedule, cancel, delete, refresh).
- Configuration and image management jobs fail under the following conditions:
  - If the device is not under the scope of the user to perform the config or image operation.
  - If the user is not authorized to perform the config or image operation.
  - For Cisco CPT devices, if the device is not in Cisco IOS mode.
- To view all instances of a job, in the Action area, click the hyperlinked **ShowAllRuns**.
- Running jobs cannot be suspended or cancelled; you must let them complete.
- Cancel stops all future instances of a job. To stop a job and resume it later, use Suspend and Resume.

Messages that can be used for debugging are saved in PRIME_NETWORK_HOME/XMP_Platform/logs/JobManager.log.

# User Authentication and Authorization

### User Authentication and Authorization

CCM uses the security methods employed by Prime Network. These are described in the *Cisco Prime Network 3.10 Administrator Guide*

**Note** If authentication fails, check the status of AVM 77 (XMP runtime DM) and Prime Network using Cisco Prime Network Administration. Cisco Prime Network Administration displays AVM 77 only when CCM is installed. For information on how to use Cisco Prime Network Administration, see the *Cisco Prime Network 3.10 Administrator Guide*.

The GUI-based functions and required roles are listed in Table 4-7. Note that these functions do not perform any actions on devices.

*Table 4-7 GUI-Based Access Roles Required to Use CCM*

| Function | Viewer | Operator | OperatorPlus | Configurator | Administrator |
|---|---|---|---|---|---|
| **Dashboard** | | | | | |
| Access top families | X | X | X | X | X |
| **Configuration Management** | | | | | |
| Delete files from archive [1] | | | | X | X |
| Add, change, delete archive file labels[1] | | | | X | X |
| Add change, delete archive file comments[1] | | | | X | X |
| Export files from archive[1] | | | | X | X |
| **Image Management** | | | | | |
| View images in repository | X | X | X | X | X |
| Add images to repository | | | | X | X |
| Delete images from repository | | | | X | X |
| **Global Tasks** | | | | | |
| View jobs | X | X | X | X | X |
| Administer jobs (suspend, delete, and so forth) | | | | X | X |
| Change settings | | | | X | X |
| **Configuration Audit** | | | | | |
| Define configuration policies | | | | X | X |
| Schedule configuration audit | | | | X | X |
| View configuration audit jobs and audit results | | | X | X | X |
| **Managing Device Groups** | | | | | |
| Create device groups | X | X | X | X | X |
| Edit device group details | | | | X | X |
| Delete device groups | | | | X | X |

1. Configuration files are filtered according to the device scope of a user.

Table 4-8 lists all of the CCM functions that are that filtered to only show devices in the device scope of a user, along with the role required to perform any functions on those devices.

*Table 4-8 Device Scope-Based Roles Required to Use CCM*

| Function | Viewer | Operator | Operator Plus | Configurator | Administrator |
|---|---|---|---|---|---|
| **Dashboard** | | | | | |
| Access configuration sync status[1] | X | X | X | X | X |
| Access configuration changes in the last week[1] | X | X | X | X | X |
| Access most recent configuration changes[1] | X | X | X | X | X |
| **Configuration Management** | | | | | |
| View files in archive[1] | X | X | X | X | X |
| Compare files in archive | X | X | X | X | X |
| Synchronize configurations | | | | X | X |
| Back up (copy) files from devices to archive | | | X | X | X |
| Restore files from archive to devices | | | | X | X |
| Edit configuration files before restoring them to devices | | | | X | X |
| View configuration change logs | X | X | X | X | X |
| **Image Management** | | | | | |
| Distribute images | | | | X | X |
| Activate and deactivate images | | | | X | X |
| Commit image changes | | | | X | X |
| Rollback images | | | | X | X |
| **Managing Device Groups** | | | | | |
| Create device groups | | | | X | X |
| Edit device group details | | | | X | X |
| Delete device groups | | | | X | X |
| **Configuration Audit** | | | | | |
| Define configuration policies | | | | X | X |
| Schedule configuration audit | | | | X | X |
| View configuration audit jobs and audit results | | | X | X | X |

1. Although users can view configuration files for devices in their scopes, the actions they can perform on those configuration files are controlled by the GUI-based access roles in Table 4-7.

For information on how Prime Network performs user authentication and authorization, including an explanation of user access roles and device scopes, see the *Cisco Prime Network 3.10 Administrator Guide*.

CHAPTER 5

# 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 5-2
- Opening and Closing Maps, page 5-5
- Creating and Deleting Maps, page 5-6
- Adding and Removing NEs from Maps, page 5-9
- Managing Maps, page 5-11
- Finding NEs, Services, and Links, and Elements Affected by Tickets, page 5-15
- Working with Aggregations, page 5-16
- Working with Overlays, page 5-21
- Filtering Links in a Map, page 5-25
- Opening the CPU Usage Graph, page 5-27
- Communicating with Devices Using Ping and Telnet, page 5-28


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 scripts and commands, depending on the NE device type, OS, supported technologies, and so forth. Those commands are documented throughout this guide (for example, , page 3-36). This also includes commands 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 3.10 Customization 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 3.10 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 3.10 Administrator Guide*.

***Table 5-1 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 5-1 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 5-2 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 5-2 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.

# Opening and Closing Maps

Whenever 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.

When you first log in, Prime Network Vision lists the maps you recently viewed but did not close when you exited the session. You can also open other maps by choosing **File > Open**, which displays the Open Map dialog.

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.

You can save maps as images or print them, if desired.

To close a map, choose **File > Close**. 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. If you made any changes that will not be saved, Prime Network Vision prompts you to save the map.

# Creating and Deleting Maps

You can create maps that cover specific network segments, customer networks, or any other mix of network elements required. Network maps provide a graphic display of active faults and alarms, and serve as access points for activating services. When you create a map, it is saved in the database and made available to other users if they have sufficient access and security privileges. When you delete a map, it is removed from the database. See these topics for more information:

- Creating New Maps, page 5-6
- Deleting Maps from the Database, page 5-8

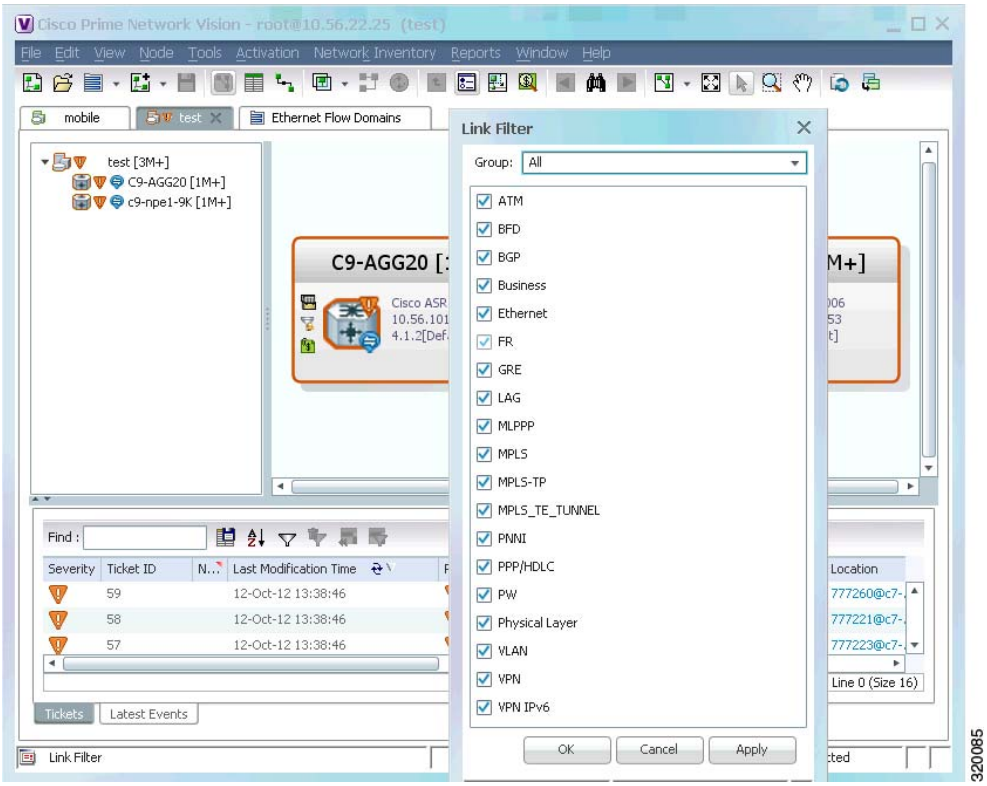
## Creating New Maps

To create a new map, choose **File > New Map** in the main menu. The following figures give examples of how you can create and manipulate maps. To add NEs to maps, see Adding and Removing NEs from Maps, page 5-9.

### Link Filters

Link filters let you choose the links in which you are interested, and then build a map that only displays NEs using those link types. Examples are physical links, data links, MPLS, VLANs, and so forth. When you open the New Map dialog, click the Advanced button and choose the types you want to display.

***Figure 5-1 Map with Link Filter***

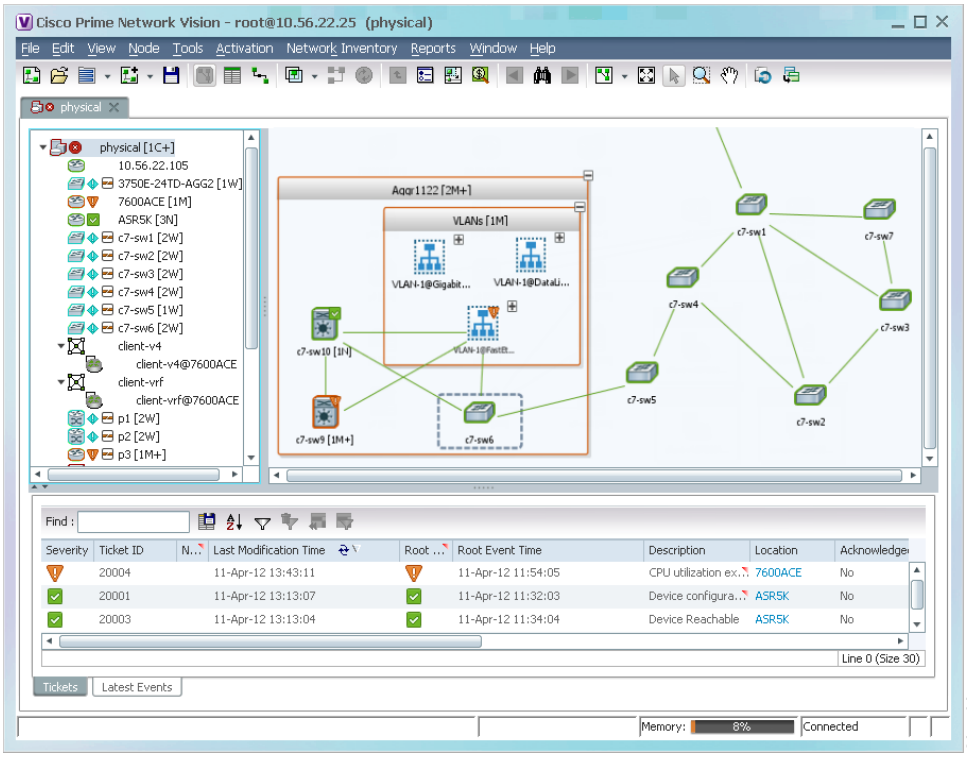



To create a map with link filters, see Figure 5-13.

### Aggregations

Aggregations are user-defined groups of elements. An aggregation can contain network elements, services, other aggregations, and so forth. Figure 5-2 shows an example of an aggregation.

*Figure 5-2 Map with Aggregation (Thumbnail View)*

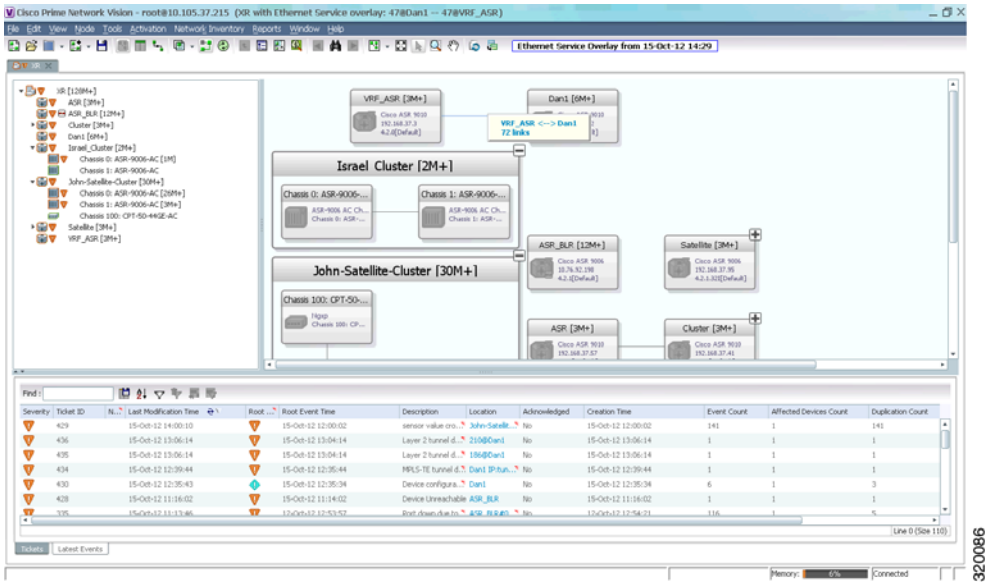



When you delete an aggregation, the member devices are not deleted from Prime Network; only the aggregation definition is deleted. To create an aggregation, see Working with Aggregations, page 5-16.

### Overlays

Overlays isolate the parts of a network that are being used by a specific service, such as an ethernet service or network clock. Figure 5-3 shows an example of an Ethernet Service overlay, where the ethernet link is using the service.

*Figure 5-3 Map with Overlay*




To create an overlay, see Working with Overlays, page 5-21.

# Deleting Maps from the Database

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 by choosing **File > Open**.

**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.

# Adding and Removing NEs from Maps

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

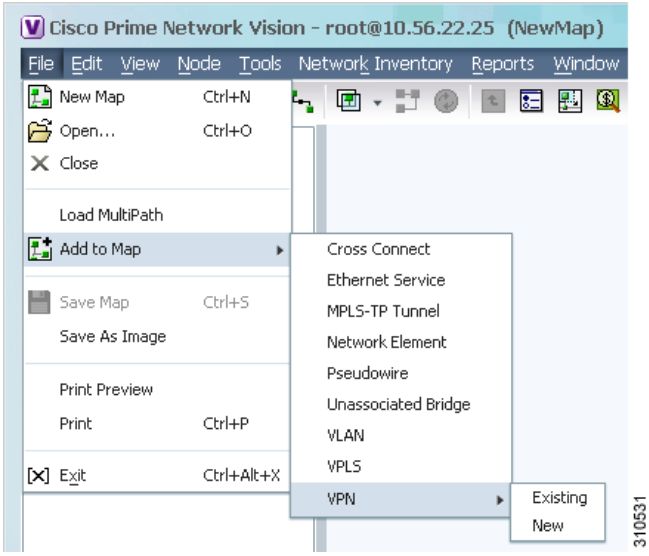
If the element you want to add is outside of your scope, it is not displayed if you enter a search string. You can display all NEs by selecting **Show All** in Step 2, but devices outside your scope will be displayed with a lock icon.

To add an element to a map:

**Step 1** Choose **File > Add to Map >** *element*.

Figure 5-4 shows the type of elements you can add to maps.

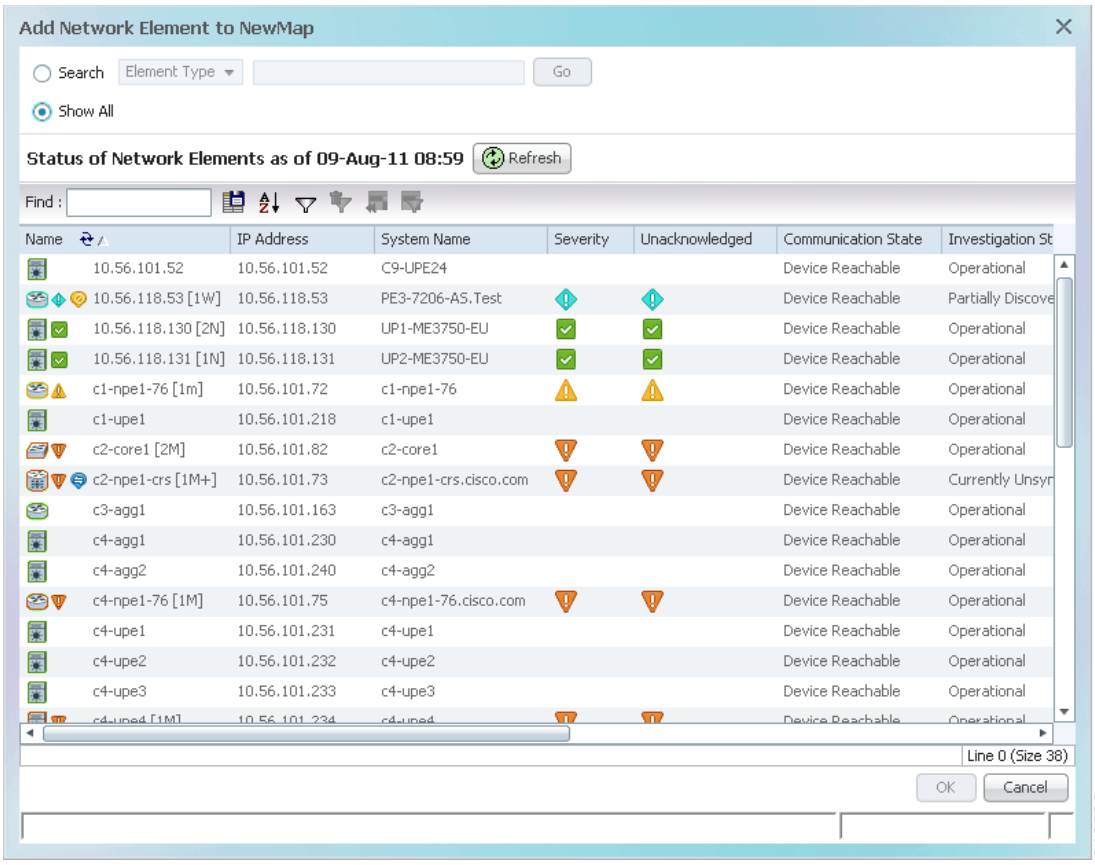
***Figure 5-4 Available Elements to Add to Maps***




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 19-21

In all other instances, the Add *element* to *map* dialog box is displayed, as shown in Figure 5-5.

*Figure 5-5 Add Element Dialog Box*




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

If you are working with a very large number of network elements, keep these items in mind:

- Search for the elements you want to add to the map. For example, you can search Ethernet Services by the system name, NEs element type, pseudowires by their role, and so forth.

**Note** If you are working with a large number of NEs, using the search filter Otherwise, it may take some time for all of the NEs to be listed.

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

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.

**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 selected a large number of elements (for example, more than 25 VLANs or VPLS instances), the action may take a while to complete.

The NEs are added to the map and are displayed in the navigation pane and content area. In addition, any associated tickets are displayed in the ticket 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 5-12
- Applying a Background Image, page 5-12
- Using the Overview Window, page 5-14
- Saving Maps, page 5-15

# Selecting Map Viewing Options

Table 5-3 describes the tools that you can use to view and manipulate maps in the Prime Network Vision map pane.

*Table 5-3 Prime Network Vision Map Viewing Options*

| Button | Name | Function |
|---|---|---|
| | Layout Map | Defines how a topology should be displayed: Circular, hierarchical, orthogonal, or symmetric. The default is circular. 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. |
| | Fit in Window | Fits an entire aggregation or map in the map pane. |
| | Normal Selection Mode | Activates 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. |

# 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.

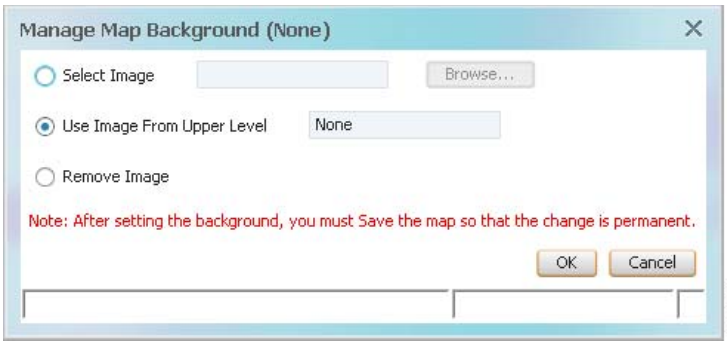
To apply a background image to a map:

**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 5-6.

*Figure 5-6 Manage Map Background Dialog Box*




**Step 3** Enter the required information as described in Table 5-4.

*Table 5-4 Manage Map Background Options*

| Field | Description |
|---|---|
| Select Image | Applies the selected image to the current map background:<br>1. Choose **Select Image**.<br>2. Click **Browse**.<br>3. In the Open dialog box, select the desired image and click **OK**.<br>The name of the selected image is displayed in the Manage Map Background dialog box.<br>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:<br>• 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.<br>• 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.<br>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

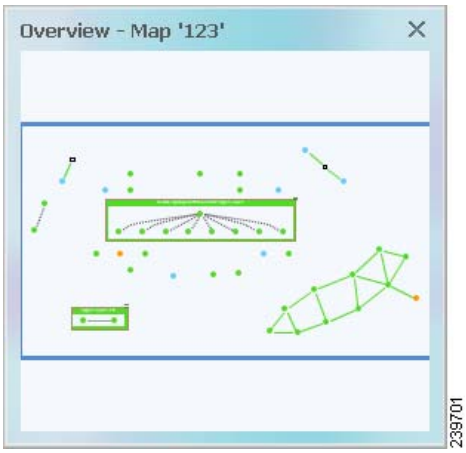
The Prime Network Vision Overview window enables you to display the entire network map or any part of the map that you require in the map pane. The Overview window also enables you to see all the changes and alarms taking place in the network.

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 5-7 shows an example of the Overview window.

***Figure 5-7 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.

## Saving Maps

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**.

**Step 6** Click **OK**. The map is saved as an image in the directory you specified.

# Finding NEs, Services, and Links, and Elements Affected by Tickets

The following topics describe how to find network elements, services, links, or elements affected by a ticket in Prime Network Vision maps.

*Table 5-5 Aggregation Thumbnail Options*

| If you want to find... | Do this... |
|---|---|
| An NE or service | From the Prime Network Vision main menu, choose **Edit > Find in Map.** Enter an element or service (such as a VPN or VLAN) by entering any part of its name or device IP address. If you want your search to include aggregations, check the Search all map levels check box. |
| A link | From the Links view, right-click the link and choose **Find Link in Map**. The link is highlighted in the map pane. If two or more lines represent the same link (such as a VRF link), you can choose the appropriate one.<br>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. |
| Which NEs are affected by a ticket | In the ticket pane, right-click the required ticket and choose **Find Affected Elements**. 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.<br>If two or more elements are affected, the affected elements are displayed in the Affected Elements window. |

# 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 5-16
- Adding Elements to an Existing Aggregation, page 5-18
- Viewing an Aggregation Thumbnail, page 5-16
- Ungrouping Aggregations, page 5-19
- Viewing Multi Chassis Devices, page 5-19

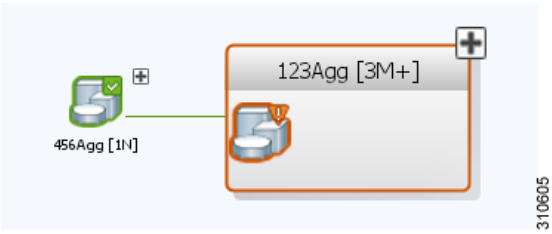
## Grouping Network Elements into Aggregations

To aggregate network elements:

**Step 1** Select the network elements. To select multiple items, press **Ctrl**.

**Step 2** Aggregate the network elements by choosing **Node > 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 2-11.

## 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.

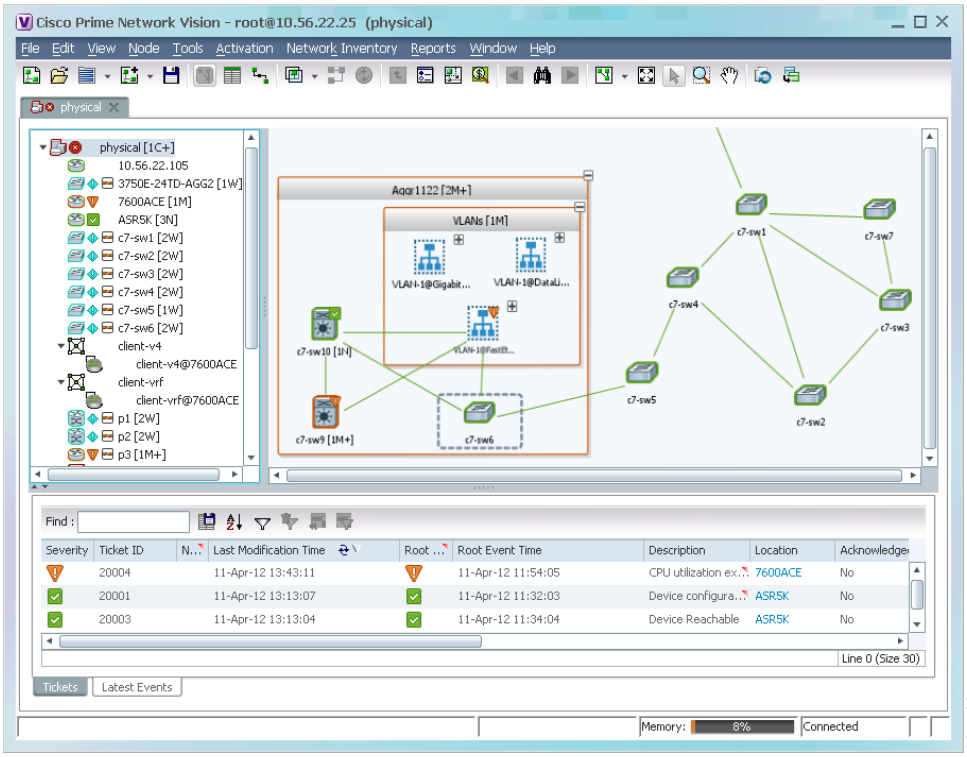
To display an aggregation thumbnail:

**Step 1** Select the existing aggregation in the map pane.

**Step 2** Open the thumbnail by right-clicking the aggregation, and choosing **Show Thumbnail**.

The thumbnail is displayed in the map pane as shown in Figure 5-8.

***Figure 5-8 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.

A dashed gray border around an icon indicates that the element resides within a thumbnail and not at the current map level.

Table 5-6 describes the options available when working with aggregation thumbnails.

*Table 5-6 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**.<br>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 3** To close the aggregation thumbnail, right-click the thumbnail frame and choose **Show As Aggregation**.

# 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** Open the thumbnail by right-clicking the aggregation, and choosing **Show Thumbnail**.

**Step 3** 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** Return to the map by double-clicking the map background.

# 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 by selecting the aggregation in the map pane and choosing **Node > 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.

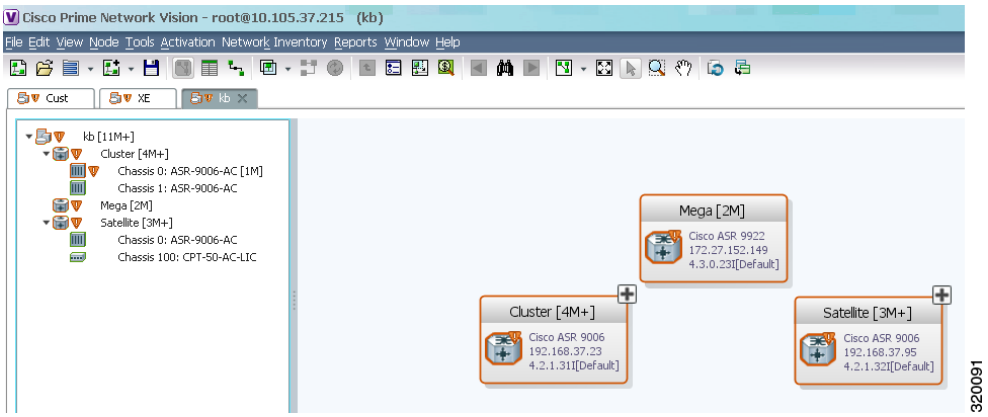
# Viewing Multi Chassis Devices

Using Prime Network Vision, you can view the physical layout and topology among the multi-chassis devices on the map. The multi chassis devices are grouped as an aggregation and are displayed as a single entity with a plus sign on the map as show in Figure 5-9. The plus sign can be expanded to display the devices under the group as shown in Figure 5-10.

You can see the multichassis grouping in the map view for network elements such as Cisco Aggregation Service Router (ASR) 9000 series network element and Cisco Unified Computing System (UCS). If satellites are configured for a Cisco ASR 9000 series network element, you can view the satellites grouped with the other chassis. For more information on how to view satellite properties, see Viewing Satellite Properties, page 3-22.

The physical ethernet links used for connecting the multi chassis devices are ICL (Inter Chassis Link) and IRL (Inter Rack Link). For more information on when each of these links are used, see Viewing Inter Rack Links, page 5-20 and Viewing Inter Chassis Links, page 5-20.

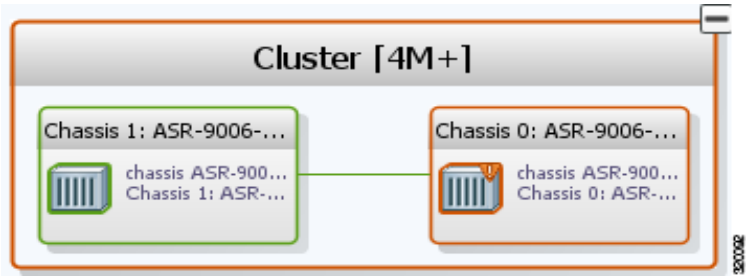
*Figure 5-9 Multichassis Devices in Map View*




## Viewing Inter Rack Links

Inter Rack Links (IRLs) are used to represent connectivity between the cluster hosts, Cisco ASR 9000 network elements.

*Figure 5-10 Multiple Chassis in a Cluster*




To view the cluster IRLs:

**Step 1** In Prime Network Vision, double-click the cluster device to open the Inventory Window for the device.

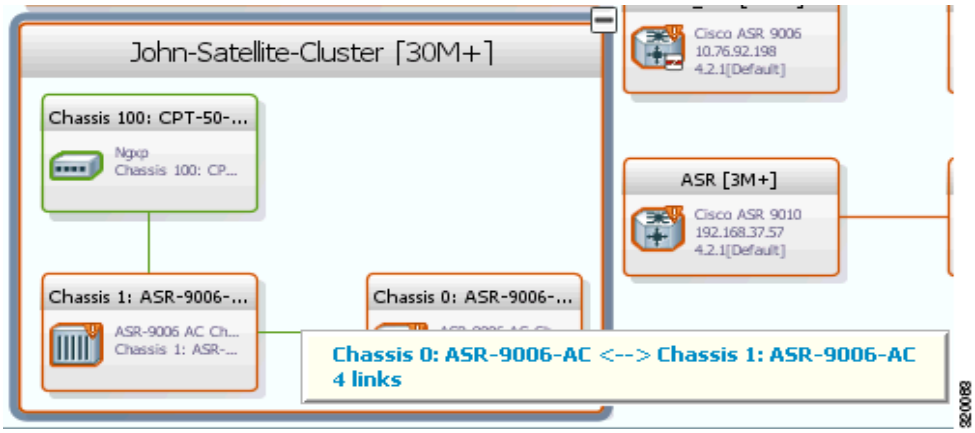
**Step 2** Choose the **Cluster IRL** container in the logical inventory of the cluster device. The content pane displays a list of cluster IRLs with the following details:

- A End Point—Device or site that is the source of the link, hyperlinked to the inventory of the device or site.
- Z End Point—Device or site that is the destination of the link, hyperlinked to the relevant entry in the inventory.

## Viewing Inter Chassis Links

Inter Chassis Links (ICLs) are used to represent the connectivity between the host Cisco ASR 9000 network element and the satellites. One or more satellites are connected to the host Cisco ASR 9000 series network element by using the ICLs. Figure 5-11 shows an ICL in the map view.

*Figure 5-11 ICL Connecting a Satellite with a Chassis*




To view the satellite ICLs:

**Step 1** In Prime Network Vision, double-click the satellite device to open the Inventory Window for the device.

**Step 2** Choose the **Satellite ICL** container in the logical inventory of the cluster device. The content pane displays a list of Satellite ICLs with the following details:

*Table 5-7 Satellite ICL Properties*

| Field | Description |
|---|---|
| Host Interface | Interface by which satellite is configured on the host network element. Click the hyperlink to view the interface properties in the physical inventory. |
| Satellite IC Interface | Inter-chassis interface used by the satellite. Click the hyperlink to view the satellite interface properties in the physical inventory. |
| Satellite ID | Satellite ID. Click the hyperlink to view the satellite properties in the physical inventory. |
| Satellite Port Range | Port associated with the satellite. |
| Satellite Status | Connection status of the satellite: Connected or Disconnected. |
| Fabric Link Status | Status of the fabric link connected to the satellite. |

# Working with Overlays

When you apply an overlay to a map, you can 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 5-22
- Hiding and Viewing Overlays, and Removing Overlays from a Map, page 5-25

# Applying an Overlay

To apply an overlay:

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

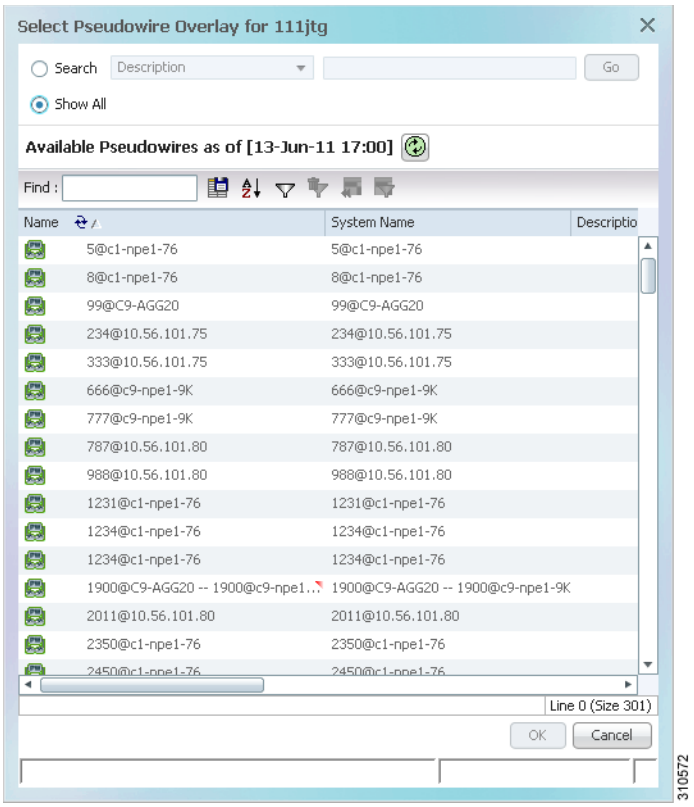
**Step 2** From the toolbar, choose **Choose Overlay Type >** *overlay-type* where *overlay-type* is one of the following options:

| 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 5-12 shows an example of the Select Pseudowire Overlay dialog box.

*Figure 5-12 Select Pseudowire Overlay Dialog Box*




Each overlay type allows you to search for specific overlays. Table 5-8 identifies the search fields available for each overlay type.

*Table 5-8 Overlay Type Search Fields*

| Overlay Type | Search Fields |
|---|---|
| Ethernet Service | • EVC Terminating EFPs<br>• Name<br>• System Name |
| MPLS-TP Tunnel | • Description<br>• Name<br>• System Name |
| Network Clock | • Name |
| Pseudowire | • Description<br>• Is Multisegment Pseudowire<br>• Name<br>• Pseudowire Role<br>• Pseudowire Type<br>• System Name |

*Table 5-8 Overlay Type Search Fields (continued)*

| Overlay Type | Search Fields |
|---|---|
| VLAN | • EFD Name<br>• EFD System Name<br>• ID<br>• Name<br>• System Name |
| VPLS | • Name<br>• System Defined Name<br>• VPN ID |
| VPN | • Description<br>• 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 5-8 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.

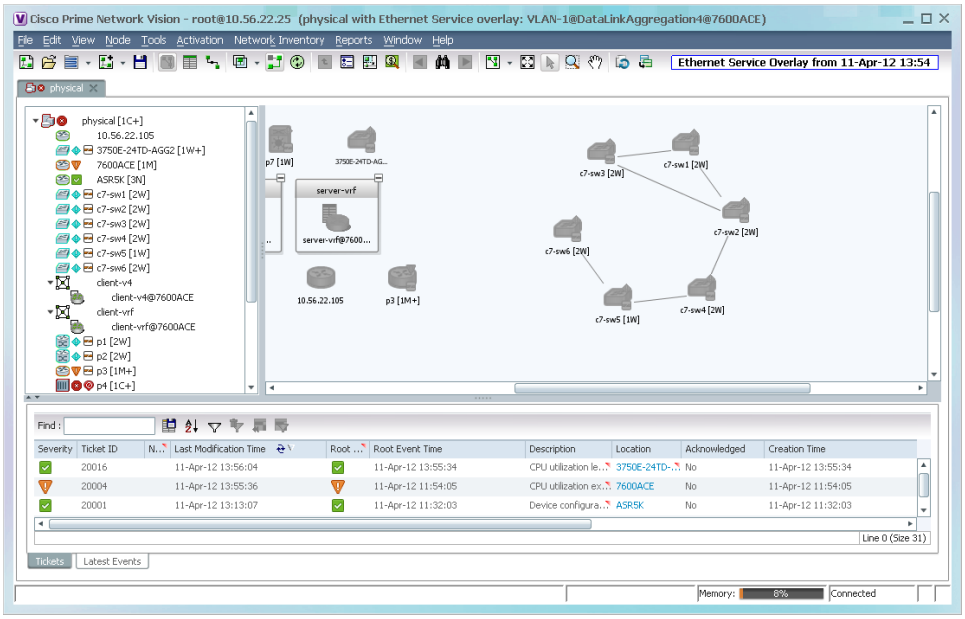
- To view all available overlays, choose **Show All**.

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 5-13.

*Figure 5-13 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 and Viewing Overlays, and Removing Overlays from a Map

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.

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 5-26.
- 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 5-27.

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 6, "Working with Links."

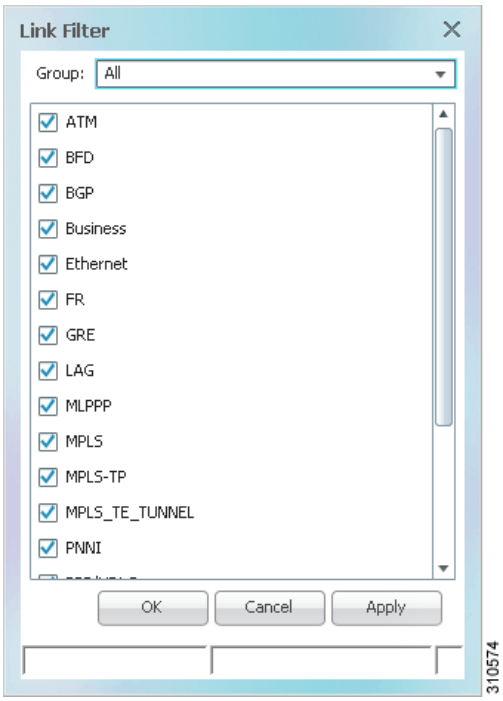
# Filtering Links During Map Creation

To filter links while creating a map:

**Step 1** Open the Create Map dialog box by choosing **File > New Map** from the main menu. The Create Map dialog box is displayed. For more information, see Creating and Deleting Maps, page 5-6.

**Step 2** Click **Advanced**. The Link Filter dialog box is displayed.

***Figure 5-14 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** Click **Apply** to apply the defined link filter settings and continue with more selections.

**Step 5** Click **OK** when you have completed your selections.

**Step 6** 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 7** Add the required elements to the map. For more information, see Creating and Deleting Maps, page 5-6.

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.

**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 5-28
- Telneting a Device, page 5-28

## 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/prime-network/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 6

# 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 6-1
- What Are Dynamic and Static Links?, page 6-3
- Link Discovery and Flickering Ethernet Topology Links, page 6-3
- Viewing Link Properties, page 6-4
- Viewing Link Impact Analysis, page 6-12
- Adding Static Links, page 6-15
- Filtering Links Using the Collection Method, page 6-17
- Selecting a Link, page 6-18


## 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 3.10 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 3.10 Administrator Guide*.

*Table 6-1 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 6-2 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.

# What Are Dynamic and Static Links?

*Dynamic links* are the physical and logical links that exist between elements in the network. These links are discovered by Prime Network using various protocols (such as STP, CDP, and LLDP). The ongoing process of autodiscovery maintains this topological information. 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.

*Static links* are links that are created at the VNE level but are not updated. These links do not perform any configuration or provisioning on a device or in the network. 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 6-15.

# Link Discovery and Flickering Ethernet Topology Links

As mentioned in What Are Dynamic and Static Links?, page 6-3, 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

In maps, you can view a link only if both ends of the link are in your scope. However, Prime Network Vision provides an option that allows users 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 3.10 Administrator Guide.*

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 6-4.
- In the Links view—See Viewing Link Properties in the Links View, page 6-8.
- In the link properties window—See Viewing Link Properties in the Link Properties Window, page 6-10.

## 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 6-3 describes the link variations that can be displayed in a map and provides examples of each.

***Table 6-3 Link Properties in Prime Network Vision Maps***

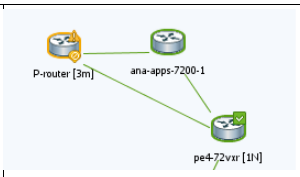
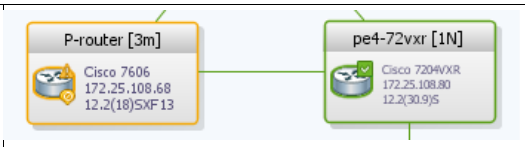
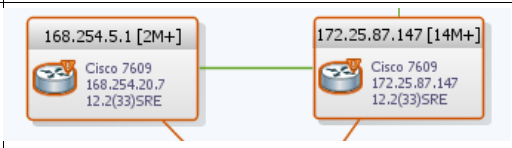
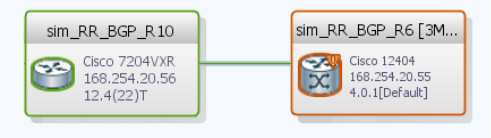
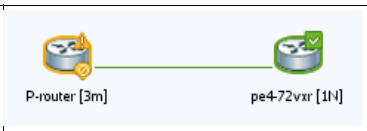
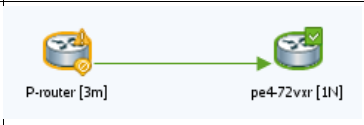
| Link Characteristic | Description | Example |
|---|---|---|
| **Solid Line vs. Dashed Line** | | |
| Solid line | Physical, topological, or service link, such as a link between two devices. |  |
| Dashed line | Association or *business link* between such elements as EVCs, VPLS service instances, or VPN components. | |

*Table 6-3 Link Properties in Prime Network Vision Maps (continued)*

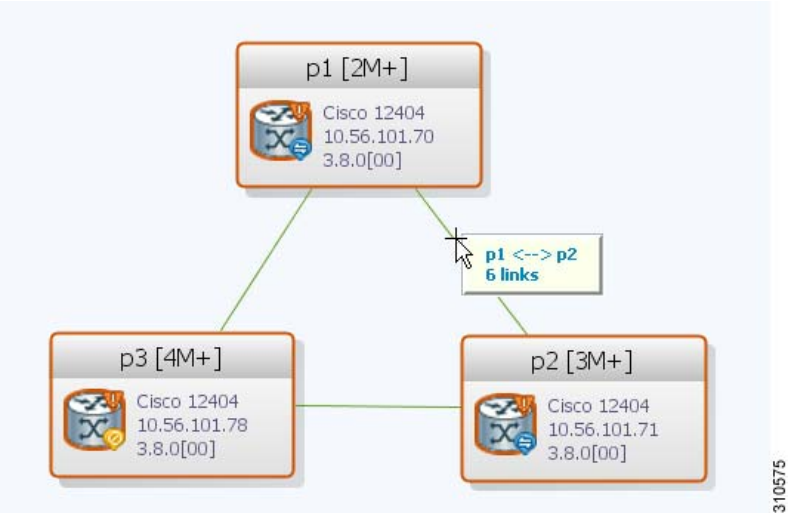
| Link Characteristic | Description | Example |
|---|---|---|
| **Link Widths** | | |
| Normal | Contains links of the same group. Available groups are:<br>• Business<br>• GRE<br>• MPLS-TP<br>• Pseudowire<br>• VLAN<br>• All others |  |
| Wide | *Aggregated links* that contain links of different groups.<br>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 2-7.

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 6-1.

***Figure 6-1 Link Tooltip in Prime Network Vision***




The tooltip contains the following information about the link:

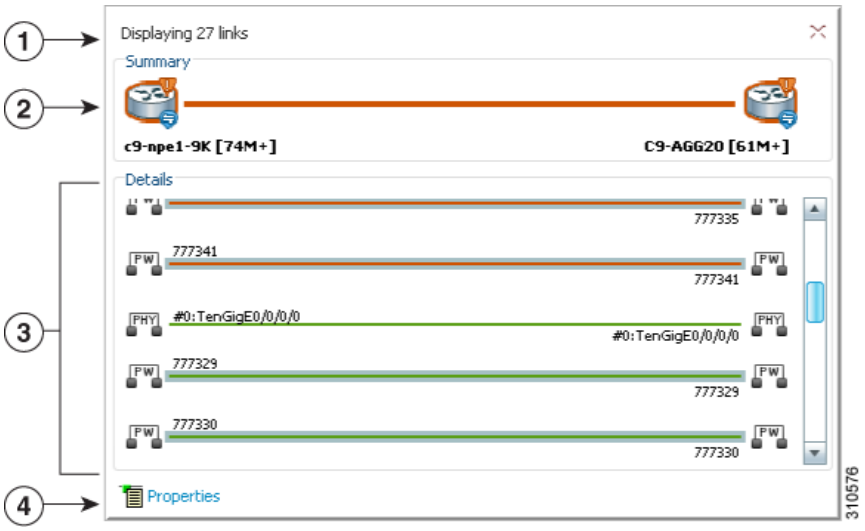
- Link endpoints, identified by the element or service name.
- The number of links represented by the line on the map.

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 6-2.

*Figure 6-2 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:<br>• 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.<br>• Link detail, such as the interface used on each endpoint, service name, or type of service.<br>• Link alarm status, indicated by the link color. |
| **4** | Hyperlink to the link properties window.<br>The Properties button is available for physical, topographical, and service links, but is not available for business links (dashed links).<br>For more information, see Viewing Link Properties in the Link Properties Window, page 6-10. |

**Step 3** To view more link properties, click **Properties** in the link quick view.

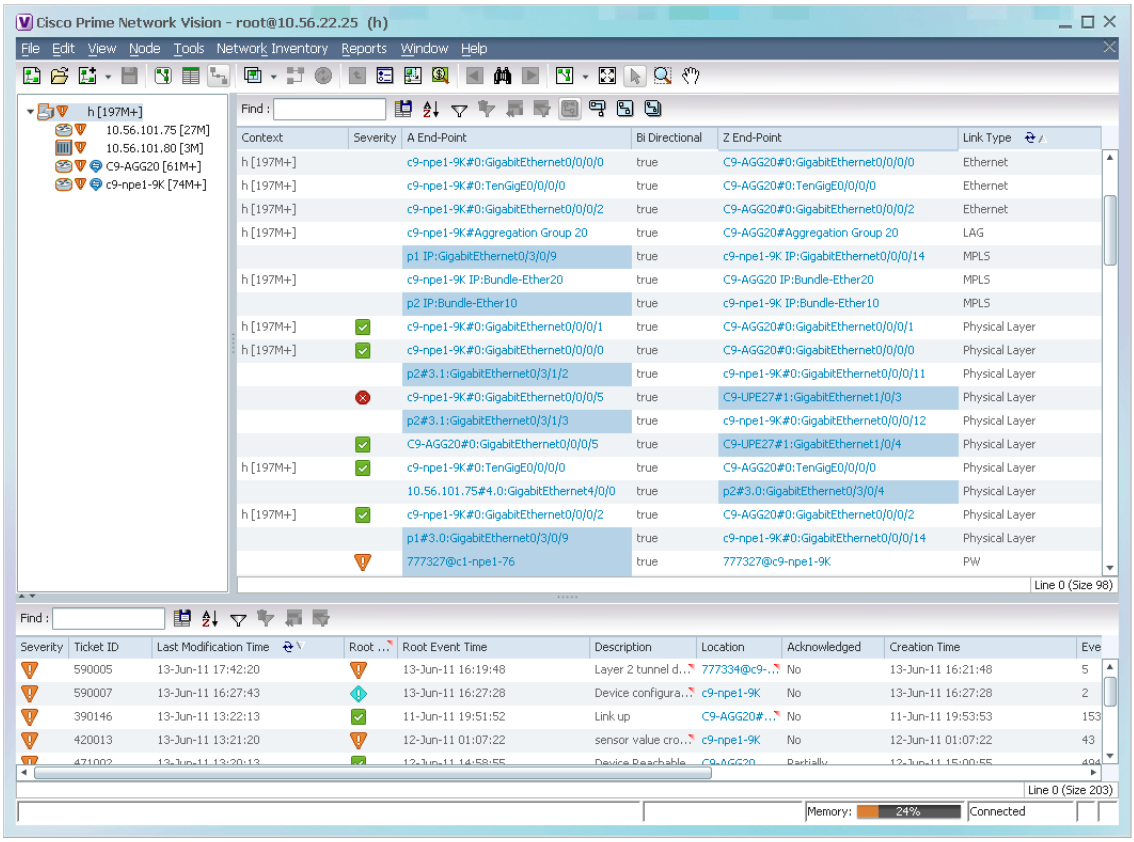
For more information about the link properties window, see Viewing Link Properties in the Link Properties Window, page 6-10.

# 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 6-4. 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 6-3 shows an example of the links view.

***Figure 6-3 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 6-4 describes the information that is displayed in the links view.

*Table 6-4 Links View Content*

| Field | Description |
|---|---|
| Context | Name of the map or aggregation containing the link. The links view can include multiple contexts.<br>This field can be empty for either of the following reasons:<br>• One side of the link is not included in the map.<br>• 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 2-16. |
| 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 6-5 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 6-5 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. |

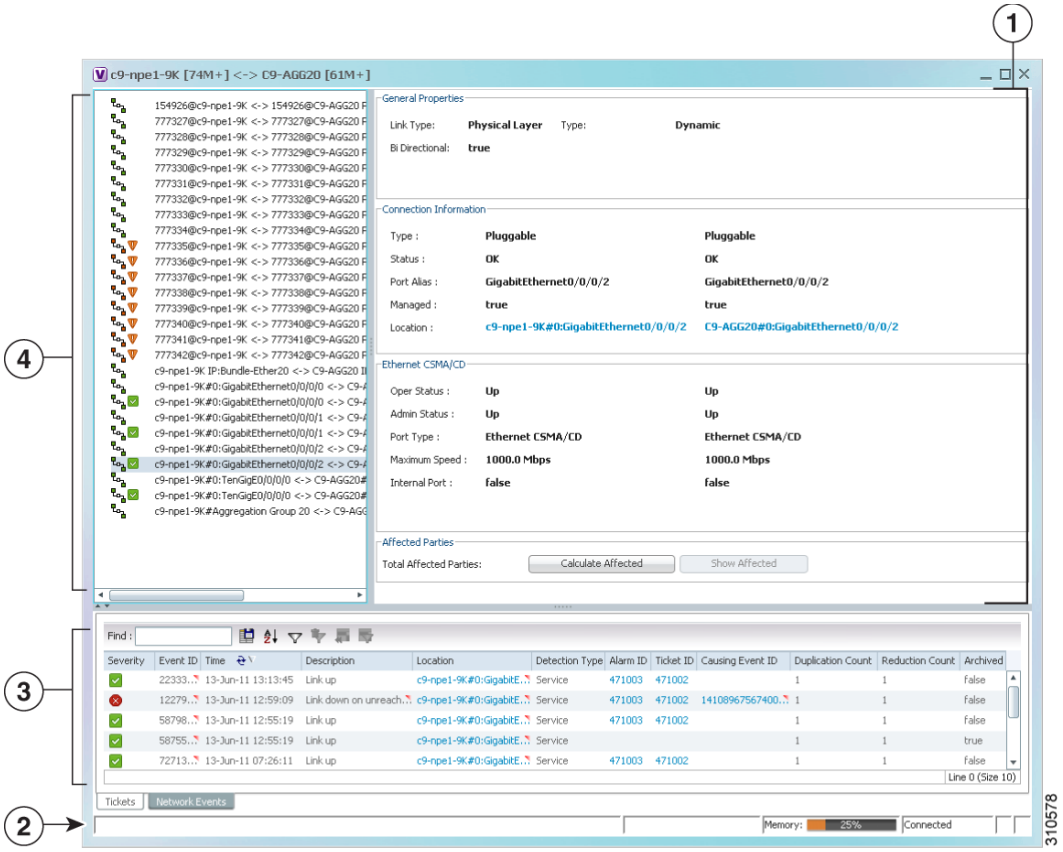
For more information about filtering links using the collection method, see Filtering Links Using the Collection Method, page 6-17.

# 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 by right-clicking a link and choosing **Properties**. The link properties window is displayed as shown in Figure 6-4.

***Figure 6-4 Link Properties Window***




| | | | |
|---|---|---|---|
| **1** | Properties pane (see Properties Pane, page 6-11) | 3 | Ticket and events pane (see Ticket and Events Pane, page 3-15) |
| **2** | Status bar | 4 | Link list pane (see Link List Pane, page 6-11) |

**Note** If multiple links exist between the elements or aggregations, the link properties window displays information for all the links.

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 2-16.

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 6-12.
- Labels—Enables you to view all LSPs on an Ethernet link. For more information, see Viewing LSPs Configured on an Ethernet Link, page 19-11.
- VCs—Enables you to view configured and misconfigured VCs on an ATM link. For more information, see Viewing ATM VPI and VCI Properties, page 21-10.

## 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 10-3 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 Adjusting the Prime Network Vision GUI Client Settings, page 2-39).

  Table 3-7 on page 3-15 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 5-25.

**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**.

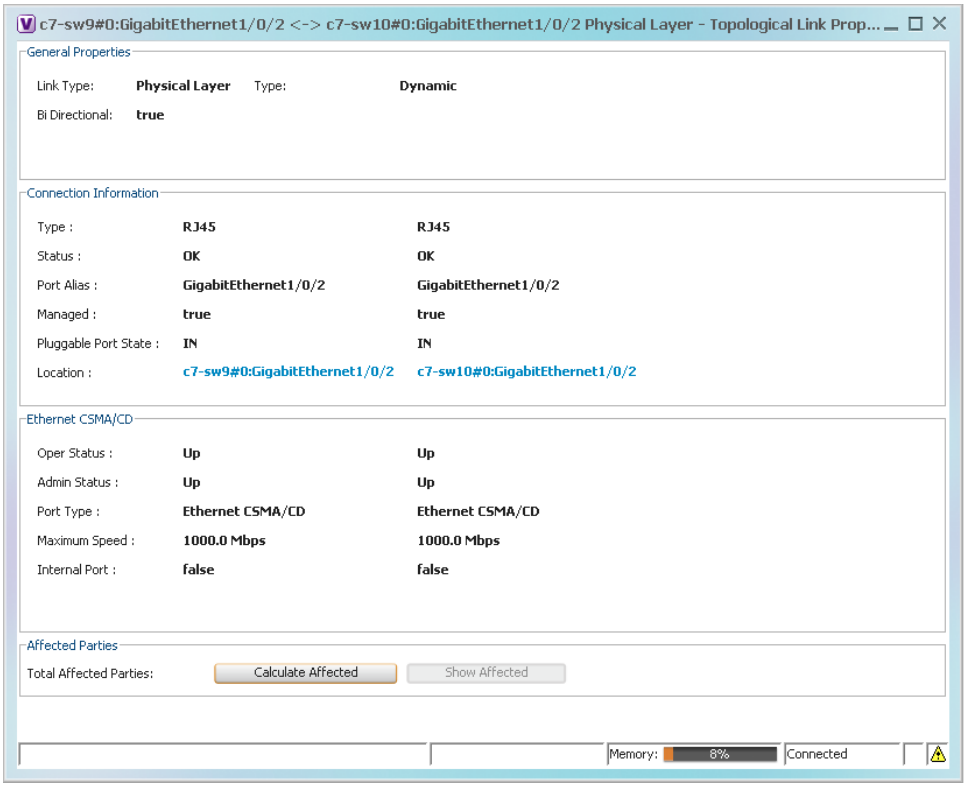
e. Click **OK**.

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.

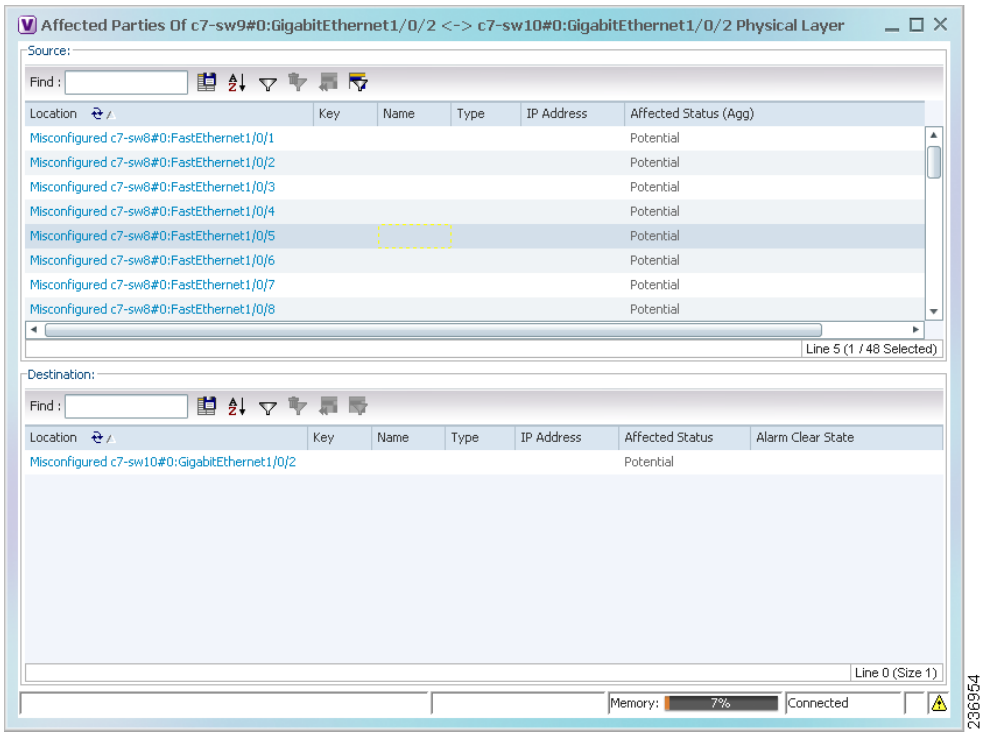
***Figure 6-5 Topological Link Properties Window***



**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 6-6.

***Figure 6-6 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, or from the inventory window navigation pane.

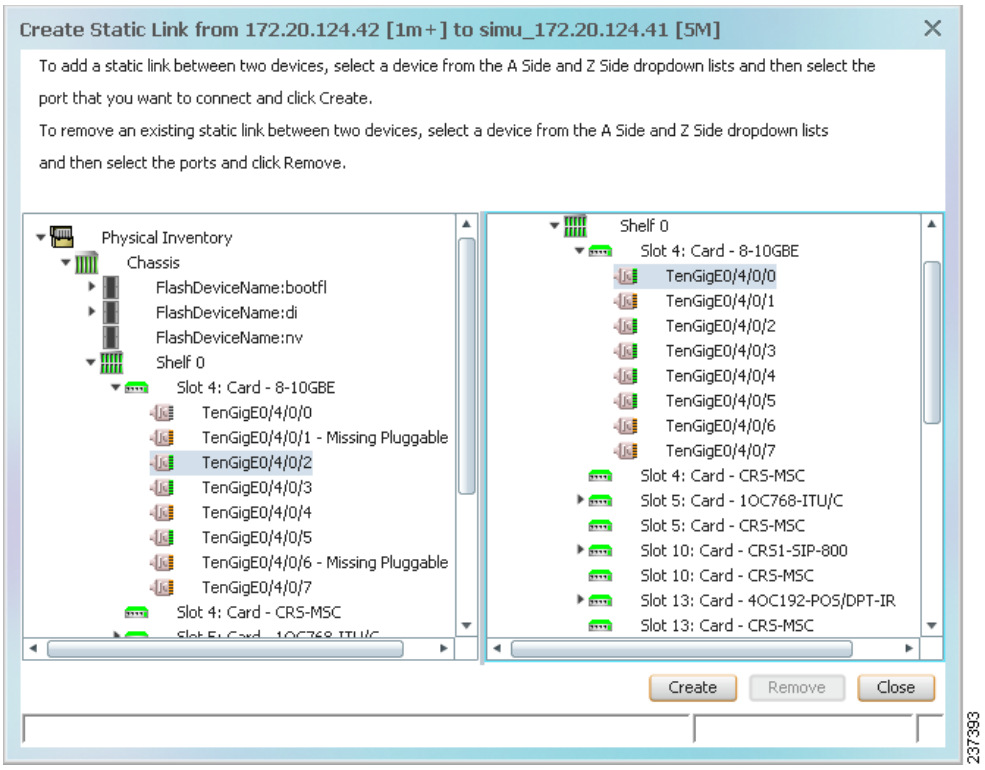
In addition, you can add a new link using Cisco Prime Network Administration. For more information, see the *Cisco Prime Network 3.10 Administrator Guide*.

### Adding a Link Using a Map and Its Navigation Pane

**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 6-7, so that you can select the ports to connect.

*Figure 6-7 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 Using the Inventory Window

**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 3.10 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 7

# Labeling NEs Using Business Tags

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.

Business tags are normally applied to a *business element*, which is a construction or organization of certain network elements and their properties into a logical entity. This provides users with 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 7-1
- Using Chinese Characters, page 7-2
- Attaching and Detaching Business Tags, page 7-3
- Searching for Business Tags and Viewing Their Properties, page 7-4
- Renaming a Business Element, page 7-7
- Deleting a Business Element, page 7-7


## 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 3.10 Administrator Guide*.

The following tables identify the tasks that you can perform:

- Table 7-1 identifies the tasks that you can perform if a selected element **is not in** one of your assigned scopes.
- Table 7-2 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 3.10 Administrator Guide*.

*Table 7-1 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 7-2 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 7-3.
- Search for business tags and view business tag properties—Searching for Business Tags and Viewing Their Properties, page 7-4.

- 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 3.10 Installation Guide*.
- Integration over northbound interfaces—*Cisco Prime Network 3.11 Integration Developer Guide*.

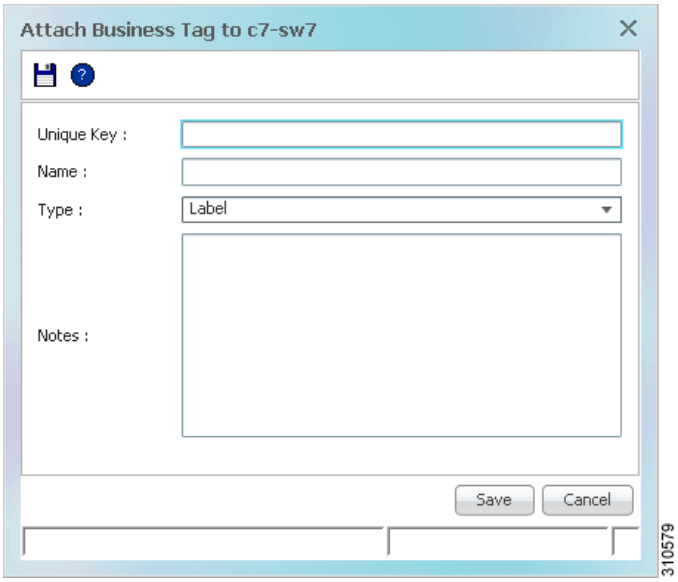
# Attaching and Detaching Business Tags

You can 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.

To attach a business tag:

**Step 1** Right-click the required network object and choose **Attach Business Tag**. The Attach Business Tag dialog box is displayed, as shown in Figure 7-1.

***Figure 7-1 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 Adjusting the Prime Network Vision GUI Client Settings, page 2-39.

- 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.

You can search and edit business tag information attached to a network object using tools available from the appropriate Business Tag dialog box.

To detach a business tag, right-click the network object and choose **Detach Business Tag**.

# 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** Choose **Edit > Find Business Tag** from the main menu. Figure 7-2 shows an example of the Find Business Tag dialog box.

*Figure 7-2 Find Business Tag Dialog Box*

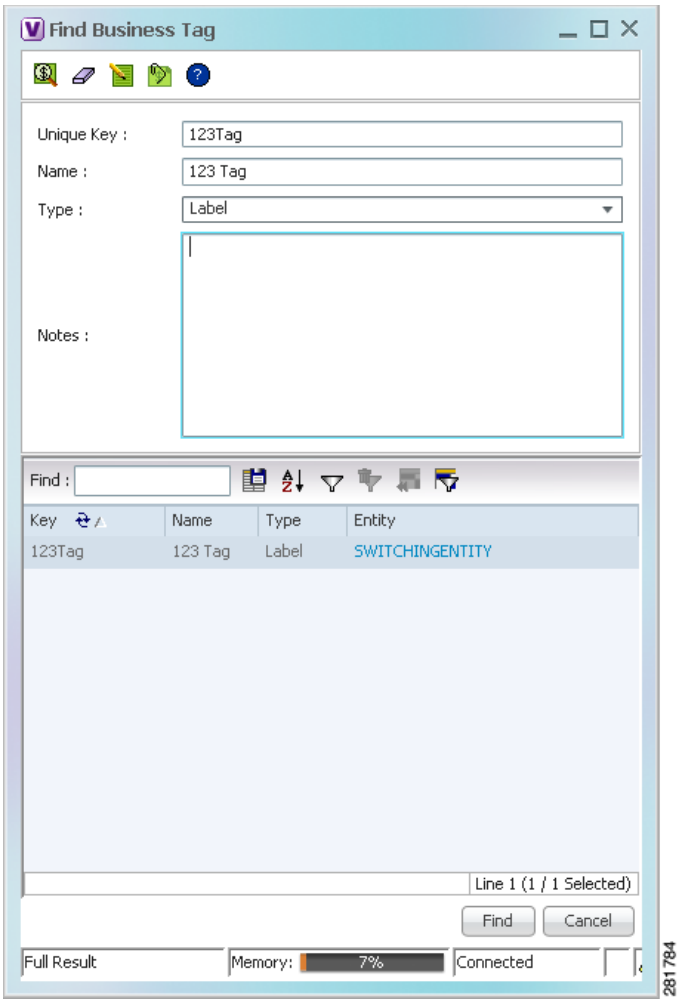



Table 7-3 describes the fields in the Find Business Tag dialog box.

*Table 7-3 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. |

*Table 7-3 Find Business Tag Dialog Box Fields (continued)*

| Icon | Name | Description |
|---|---|---|
| | 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.<br>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 7-3, 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 7-2.

**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, right-click the business element and choose **Rename**.

# 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 7-4 lists the requirements that must be met before you can delete a business element.

*Table 7-4 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 7-4. 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 8

# 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 8-1
- Launching Prime Network Events, page 8-2
- Prime Network Events Window, page 8-2
- Prime Network Events Right-Click Options, page 8-7
- Adjusting the Prime Network Events GUI Client Settings, page 8-8


## 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 3.10 Administrator Guide*.

Only users with the Administrator role can log into Prime Network Events (see Table 8-1).

*Table 8-1 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 Vision 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.

- 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 information on Prime Central, see the Cisco Prime Central *User Guide*.
- Launch Prime Network Events as a Standalone Application—Choose **Start > Programs > Cisco Prime Network >** ***gateway IP address*** **>** Cisco Prime Network Events, and enter your username and password. If any client updates are available, Prime Network automatically installs them.

  If you see messages that say the server and client have different versions of the application, you need to updated your client as described in the *Cisco Prime Network 3.10 Installation Guide*.

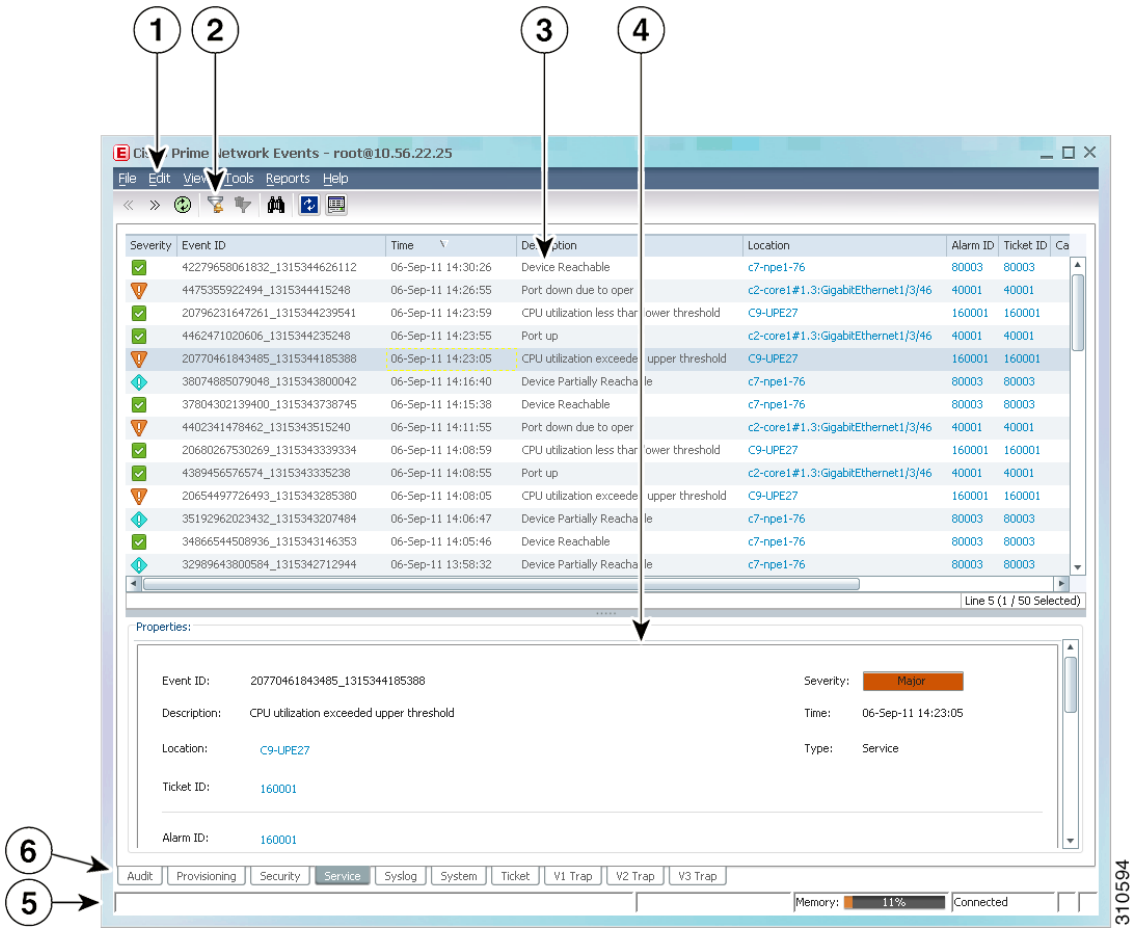
The following conditions apply when working with Prime Network Events:

- 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 11, "Working with Reports."
- Only users with the Administrator role can log into Prime Network Events.

# Prime Network Events Window

The Prime Network Events window displays the events generated in the system. Figure 8-1 shows an example of the Prime Network Events window.

*Figure 8-1 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 Adjusting the Prime Network Events GUI Client Settings, page 8-8. 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 Adjusting the Prime Network Events GUI Client Settings, page 8-8.

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 9-2.

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 9-22.
- View selected event properties in a separate window. See Viewing Event Properties, page 9-14.

### 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 8-2.

*Table 8-2 Severity Indicators*

| Icon | Color | Severity | Icon | Color | Severity |
|---|---|---|---|---|---|
| | Red | Critical | | Light Blue | Warning |
| | Orange | Major | | Medium Blue | Information |
| | Yellow | Minor | | Dark blue | Indeterminate |
| | Green | Cleared, Normal, or OK | | | |

### 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 8-3.

*Table 8-3 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. |

*Table 8-3 Event Categories in Prime Network Events (continued)*

| Tab | Description |
|---|---|
| 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.<br>Displayed when you choose **File > Open All Tab**. |
| 3.6.x *Type* | Five tabs where *Type* represents one of the following:<br>• Ticket<br>• Service<br>• Syslog<br>• V1 Trap<br>• V2-V3 Trap<br>These tabs are:<br>• Available only if Prime Network was upgraded from Cisco ANA 3.6.x to the current Prime Network version.<br>• Displayed when you choose **File > Open 3.6.x Tabs**. |

# Prime Network Events Toolbar

Table 8-4 describes the tools that are displayed in the Prime Network Events toolbar.

*Table 8-4 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 9-21. |
| | 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 9-22. |

*Table 8-4 Prime Network Events Toolbar Tools (continued)*

| Button | Function |
|---|---|
| | 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:<br>• You can select multiple criteria here, as needed.<br>• 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).<br>For a description of the items in the Find Events dialog box, see Table 9-23. |
| | 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 Adjusting the Prime Network Events GUI Client Settings, page 8-8. |
| | Displays the properties of the selected event or ticket in the Properties pane. |

# Prime Network Events Menu Bar

Table 8-5 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 9-14).

*Table 8-5 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:<br>• 3.6.x Ticket<br>• 3.6.x Service<br>• 3.6.x Syslog<br>• 3.6.x V1 Trap<br>• 3.6.x V2-V3 Trap<br>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. |

*Table 8-5 Prime Network Events Menu Options (continued)*

| Menu Option | Description |
|---|---|
| **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 9-22. |
| 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 9-14. |
| 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. |
| **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 Adjusting the Prime Network Events GUI Client Settings, page 8-8 |
| **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 3.10 Customization Guide*.
- Properties—Displays the properties window for the selected event or ticket.

# Adjusting the Prime Network Events GUI Client Settings

The Prime Network Events Options dialog box enables you to define the options for displaying events in the Prime Network Events window. To view these settings, choose **Tools > Options** from the main menu. The options are displayed in Table 8-6.

***Table 8-6 Options for Changing Prime Network Events GUI Client***

| 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.<br>**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. |
| Run auto refresh every *n* secs | Automatically refreshes the Prime Network Events display after the specified number of seconds.<br>**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.<br>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.<br>When in Find mode, the status bar in the Prime Network Events window shows "Find Mode (no automatic data retrieval)." |

CHAPTER 9

# 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 9-1
- Viewing Events and Tickets in Cisco Prime Network Events, page 9-2
- Viewing 3.6.x Tabs, page 9-12
- Working with Cisco Prime Network Events, page 9-14


## 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 3.10 Administrator Guide*.

Only users with the Administrator role can log into Cisco Prime Network Events, as shown in Table 9-1.

***Table 9-1 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 |

*Table 9-1 Default Permission/Security Level Required for Cisco Prime Network Events (continued)*

| Task | Viewer | Operator | OperatorPlus | Configurator | Administrator |
|---|---|---|---|---|---|
| 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 11, "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 Adjusting the Prime Network Events GUI Client Settings, page 8-8.

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 3.10 Installation Guide*.

Table 9-2 describes the information that is displayed in the All tab.

***Table 9-2 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 8-4. |
| 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 9-3
- Provisioning Tab, page 9-5
- Security Tab, page 9-6
- System Tab, page 9-6

## 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 9-1.

*Figure 9-1 Audit Tab*

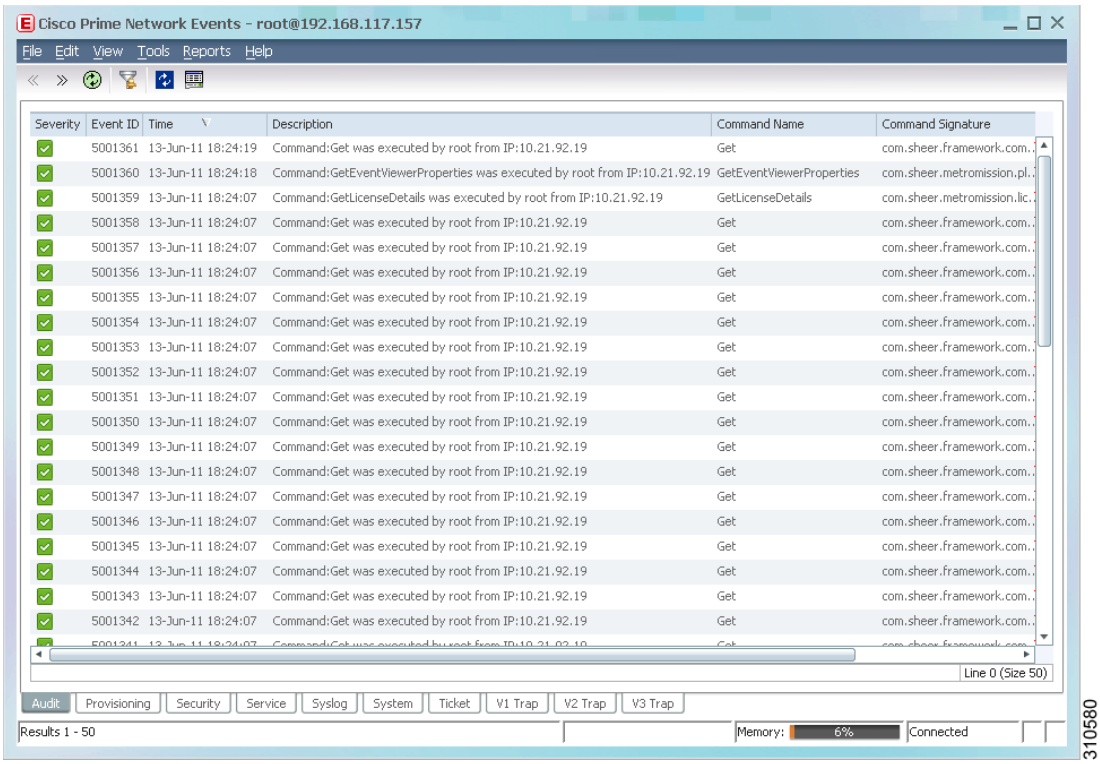



Table 9-3 describes the information that is displayed in the Audit tab.

*Table 9-3 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 8-4. |
| 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 9-4 describes the information that is displayed in the Provisioning tab.

***Table 9-4 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 8-4. |
| 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. |
| Prime Login Username | Username of the logged in user. |
| VNE Login Username | Username, which was used to access the device. This field is updated only for events generated by command scripts in Prime Network. For all other commands, this field shows ‘From VNE Login.’ |
| Status | Status, such as Success or Fail. |

1. The Workflow Editor is based on LiquidBPM by Autonomy, Inc.

## 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 9-5 describes the information that is displayed in the Security tab.

***Table 9-5 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 8-4. |
| 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 “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 *Cisco Prime Network Supported System and Security Events*.

## 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 9-6 describes the information that is displayed in the System tab.

***Table 9-6 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 8-4. |
| 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 *Cisco Prime Network 3.10 Supported System and Security Events*.

# Network Event Tabs

The following topics describe the information displayed in Prime Network Events for network events:


- Service Tab, page 9-7
- Syslog Tab, page 9-8
- Ticket Tab, page 9-8
- V1 Trap Tab, page 9-10
- V2 Trap Tab, page 9-10
- V3 Trap Tab, page 9-11


## 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 9-7 describes the information that is displayed in the Service tab.

***Table 9-7 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 8-4. |
| 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 *Cisco Prime Network 3.11 Supported Service Alarms*.

## 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 9-8 describes the information that is displayed in the Syslog tab.

***Table 9-8 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 8-4. |
| 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 9-9 describes the information that is displayed in the Ticket tab.

***Table 9-9 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 8-4. |
| 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 10, “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 9-18.

## 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 9-10 describes the information that is displayed in the V1 Trap tab.

***Table 9-10 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 8-4. |
| 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 *Cisco Prime Network Supported Traps*.

## 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 9-11 describes the information that is displayed in the V2 Trap tab.

*Table 9-11 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 8-4. |
| 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 *Cisco Prime Network Supported Traps*.

## 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 9-12 describes the information that is displayed in the V3 Trap tab.

*Table 9-12 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 8-4. |
| 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 *Cisco Prime Network 3.11 Supported Traps*.

# Viewing 3.6.x Tabs

If you upgrade to Prime Network 3.11 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 9-13 describes the information that is displayed in each of the 3.6.x tabs.

*Table 9-13 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 8-4. |
| 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 10, "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 8-4. |
| 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 8-4. |
| 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 9-13 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 8-4. |
| 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 8-4. |
| 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 9-14
- Viewing Ticket Properties, page 9-18
- Refreshing Cisco Prime Network Events Information, page 9-21
- Filtering Events, page 9-22
- Exporting Displayed Data, page 9-25

## 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 the **Details** tab on the Event Properties window 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.

**Step 2** Select an event and choose **View > Properties** from the main menu. 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 9-2. The Details tab is displayed by default.

***Figure 9-2 Network Event Properties Window - Details Tab***

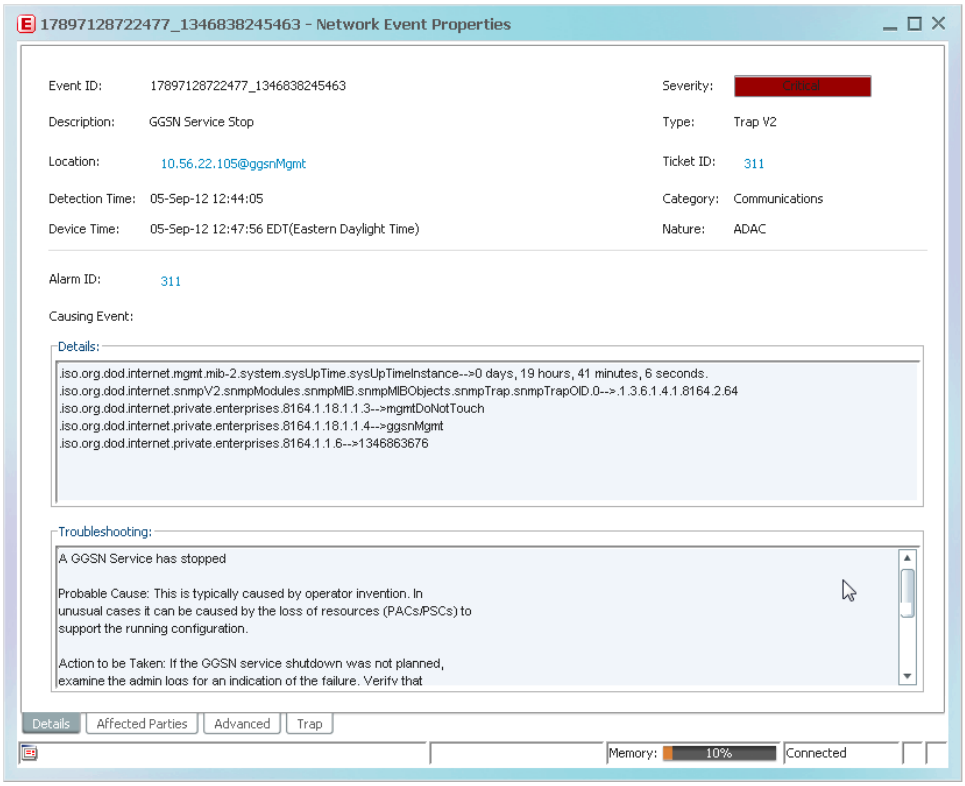



Table 9-14 describes the information that is displayed in the Details tab in the Event Properties window.

***Table 9-14 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. |
| Type | Type of event, such as Security or Service. |
| Location | Entity that triggered the event, hyperlinked to its entry in inventory. |
| Ticket ID | This field is displayed only for network events.<br>Sequential identifier of the ticket, hyperlinked to the Ticket Properties window. |
| Detection Time | Date and time when the event happened and was logged and recorded. |

*Table 9-14 Details Tab for Events (continued)*

| Field | Description |
|---|---|
| Device Time | The time zone of the device.<br>**Note** This information is available only for Cisco ASR5000 devices. |
| Category | The category of the fault, which can be any one of the following:<br>• Communications—Associated with procedures and/or processes required to convey information from one point to another.<br>• Quality of Service—Associated with a degradation in the quality of service.<br>• Processing error—Associated with a software or processing fault equipment.<br>• Environmental—Associated with a condition relating to an enclosure in which the equipment resides.<br>• Equipment—Associated with an equipment fault.<br>• Undetermined—Not categorized. |
| Nature | The nature of the fault, which can be one of the following:<br>• ADAC (Automatically Detected Automatically Cleared)—When the clearing is automatically detected and cleared by Element Management System (EMS). For example, Link Down.<br>• ADMC (Automatically Detected Manually Cleared)—When clearing requires manual intervention. For example, DWDM Fatal Error syslog. |
| Alarm ID | This field is displayed only for network events.<br>Alarm identifier, hyperlinked to the Ticket Properties window or the Alarm Properties window. |
| Causing Event | This field is displayed only for network events.<br>The identifier of the causing event. |
| Details | Detailed description of the event. |
| Troubleshooting | The probable cause of the event, action to be taken to rectify the problem, and the clearing condition.<br>**Note** This information is available only for Cisco ASR5000 traps. |

**Step 3** You can view additional properties in the following tabs:

- Advanced tab—See Table 9-15.
- Affected Parties tab—See Table 10-12.
- Audit tab—See Table 9-16.
- Provisioning tab—See Table 9-17.

- Security tab—See Table 9-18.
- Trap tab—See Table 9-19.

The tabs that are displayed depend on the type of event, such as a Service event or a Provisioning event.

*Table 9-15 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 9-16 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 9-17 Provisioning Tab*

| Field | Description |
|---|---|
| User Name | Name of the user who performed the provisioning operation. |
| Status | Status of the operation: Success or Fail. |

*Table 9-18 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 9-19 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:<br>• 1 represents iso.<br>• 3 represents org.<br>• 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 9-18.

# 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** Choose **View > Properties** from the main menu. 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 9-3.

*Figure 9-3 Ticket Properties Window - Details Tab*

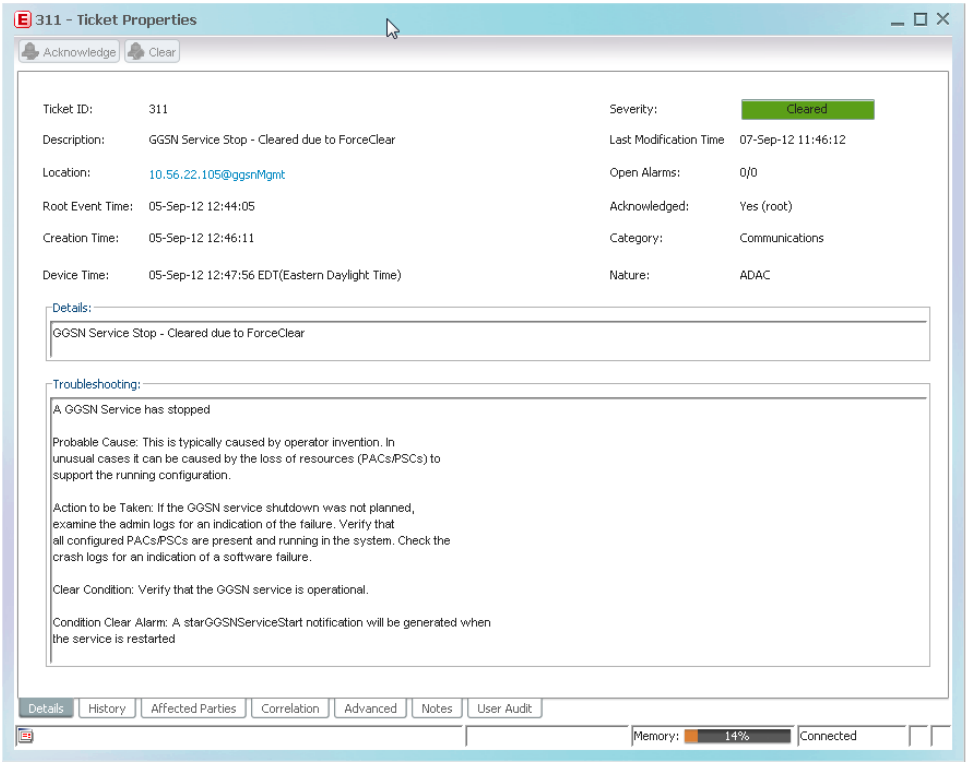



Table 9-20 describes the information that is displayed in the Details tab in the Ticket Properties window.

*Table 9-20 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 10-7.<br>If a ticket is acknowledged, and events are correlated to it after correlation, the ticket is considered to have not been acknowledged.<br>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 10-7.<br>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. |

*Table 9-20 Ticket Properties Window - Details Tab (continued)*

| Field | Description |
|---|---|
| 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.<br>**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. |
| Device Time | The time zone of the device.<br>**Note** This information is available only for Cisco ASR5000 devices. |
| Category | The category of the fault, which can be any one of the following:<br>• Communications—Associated with procedures and/or processes required to convey information from one point to another.<br>• Quality of Service—Associated with a degradation in the quality of service.<br>• Processing error—Associated with a software or processing fault equipment.<br>• Environmental—Associated with a condition relating to an enclosure in which the equipment resides.<br>• Equipment—Associated with an equipment fault.<br>• Undetermined—Not categorized. |
| Nature | The nature of the fault, which can be one of the following:<br>• ADAC (Automatically Detected Automatically Cleared)—When the clearing is automatically detected and cleared by Element Management System (EMS). For example, Link Down.<br>• ADMC (Automatically Detected Manually Cleared)—When clearing requires manual intervention. For example, DWDM Fatal Error syslog. |
| Details | Detailed description of the ticket. |
| Troubleshooting | The probable cause of the event, action to be taken to rectify the problem and the clearing condition.<br>**Note** This information is available only for Cisco ASR5000 traps. |

**Step 3** As required, review additional properties for the ticket.

Table 9-21 identifies the additional tabs that are displayed in the Ticket Properties window and links to the relevant information.

*Table 9-21 Ticket Properties Window - Additional Tabs*

| Tab | Description |
|---|---|
| History | Contains the history of the ticket, including all the events.<br>For more information, see History Tab, page 10-13. |
| Affected Parties | The services (affected pairs) that are potentially affected (potential impact analysis) by the ticket.<br>For more information, see Affected Parties Tab, page 10-14. |
| Correlation | Displays all alarms that are correlated to the selected ticket.<br>For more information, see Correlation Tab, page 10-17. |
| 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.<br>For more information, see Advanced Tab, page 10-18. |
| Notes | Enables you to add and save notes for the selected ticket.<br>The Notes tab is not available for tickets that have been archived.<br>For more information, see Notes Tab, page 10-18. |
| 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 10-19. |

# 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 Adjusting the Prime Network Events GUI Client Settings, page 8-8). Your filter settings remain intact.

Table 9-22 shows the refresh buttons.

*Table 9-22 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, 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 Adjusting the Prime Network Events GUI Client Settings, page 8-8.

See the following topics for more information about filtering events:

- Defining Filters, page 9-23
- Removing Filters, page 9-24

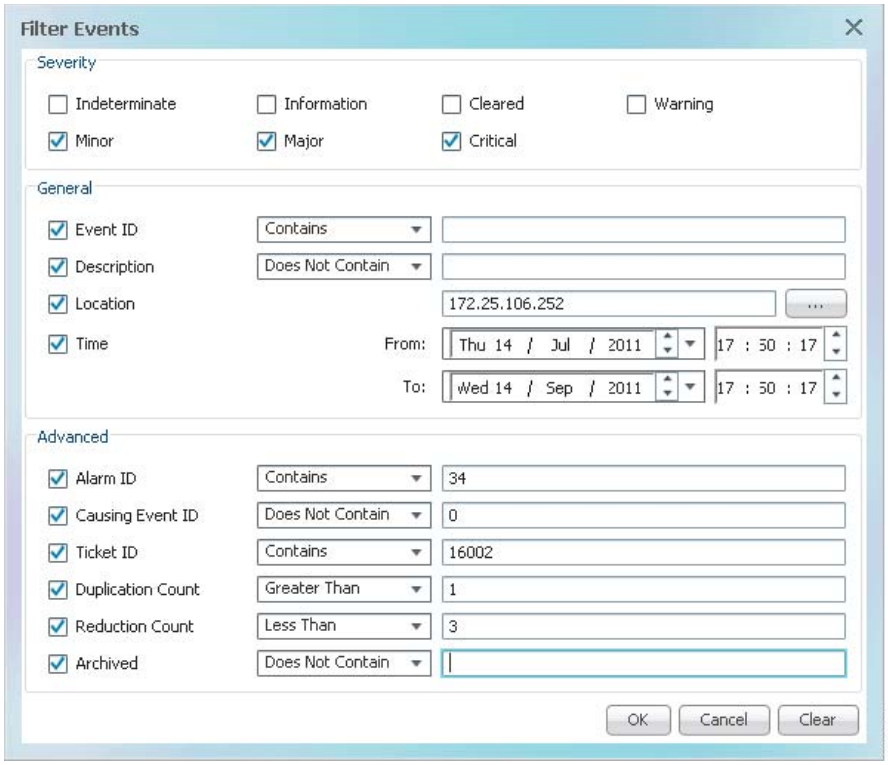
For information about filtering tickets, see Filtering Tickets by Criteria, page 10-8.

## Defining Filters

To define a filter:

**Step 1** Choose **Edit > Filter** from the main menu. The criteria that you can use for filtering differs for events and tickets. For example, Figure 9-4 shows the Filter Events dialog box for service events. For an example of the Ticket Filter dialog box, see Figure 10-2.

***Figure 9-4 Filter Events Dialog Box - Service Events***




**Step 2** Specify the filter criteria by using the following steps and the information in Table 9-23:

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 9-23 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. |

*Table 9-23 Cisco Prime Network Events Filter Events Options (continued)*

| Field | Description |
|---|---|
| Location | Network elements to include.<br>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 10

# Working with Tickets in Cisco Prime Network Vision

These topics describe how to work with tickets in Prime Network Vision:


- What are Tickets?, page 10-1
- User Roles Required to Work with Tickets in Prime Network Vision, page 10-1
- Viewing Tickets and Network Events for Elements in a Map, page 10-3
- Viewing Ticket Properties, page 10-10
- Managing Tickets, page 10-19
- Impact Analysis in Prime Network, page 10-22


## What are Tickets?

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 3.10 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 3.10 Administrator Guide*.

Table 10-1 identifies the roles required to perform the high level tasks:

***Table 10-1 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.

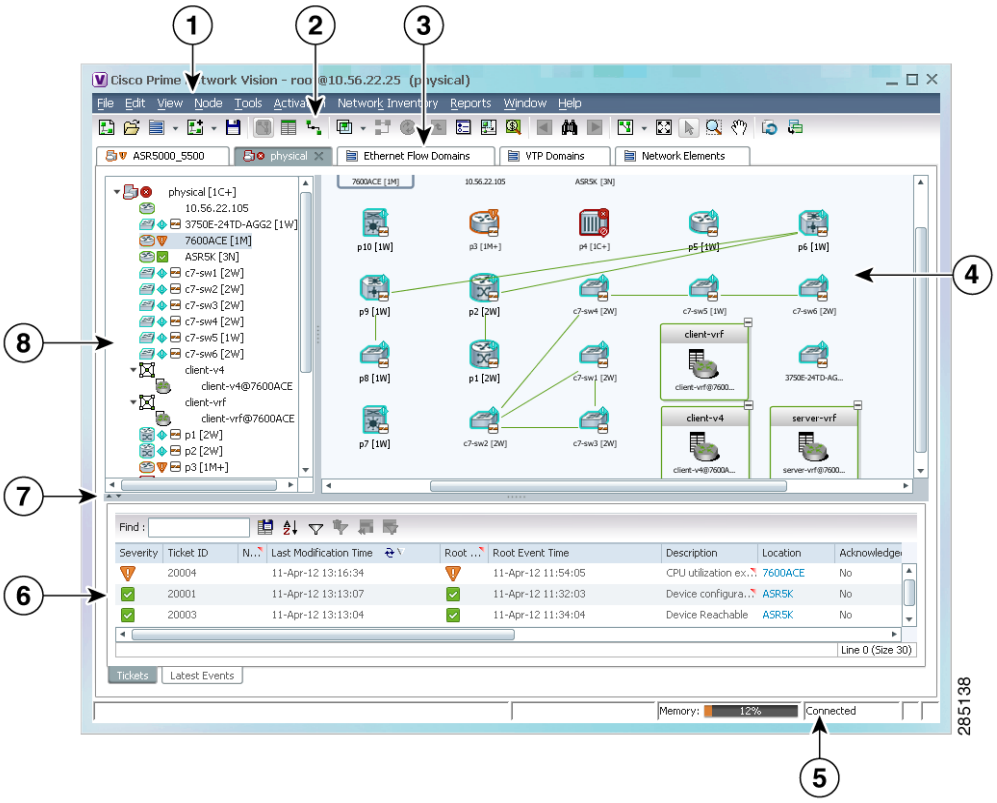
# Viewing Tickets and Network Events for Elements in a Map

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 10-1). 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 10-4 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 10-1 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 10-2 describes the functions that are available from the Tickets tab in the ticket pane.

*Table 10-2 Ticket Pane Available Functions*

| Function | Related Documentation |
|---|---|
| Acknowledge a ticket. | Acknowledging a Ticket, page 10-19 |
| Clear a ticket. | Clearing a Ticket, page 10-20 |
| Clear and remove a ticket. | Clearing and Removing Tickets, page 10-21 |
| Filter and view all tickets that meet specific criteria. | Filtering Tickets by Criteria, page 10-8 |

*Table 10-2 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 10-19 |
| Remove a ticket. | Removing a Ticket, page 10-20 |
| View all tickets or only the filtered tickets of a selected element. | Filtering Tickets by Network Element, page 10-8 |
| View tickets. | Viewing Tickets and Network Events for Elements in a Map, page 10-3 |
| View ticket properties, including the history, correlated alarms, severity of the root cause alarm, and affected parties. | Viewing Ticket Properties, page 10-10 |

Table 10-3 describes the information displayed in the ticket pane.

*Table 10-3 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 2-7.<br>• Red—Critical<br>• Orange—Major<br>• Yellow—Minor<br>• Light Blue—Warning<br>• Green—Cleared, Normal, or OK<br>• Medium Blue—Informational<br>• 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 10, "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 10-3 Ticket Information Displayed in the Ticket Pane (continued)*

| Field Name | Description |
|---|---|
| Acknowledged | Whether the ticket is acknowledged or has been modified: Yes, No, or Modified. 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.<br>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.<br>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 Filtering and Sorting Tabular Content, page 2-40.

## 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 10-4 shows an example of the appearance of the ticket pane when a ticket is generated.

*Table 10-4 Generated Ticket*

| Icon | Severity | Ticket ID | Short Description | Acknowledged |
|---|---|---|---|---|
| | Major | 27 | Port down | Yes |

### Cleared Ticket

Table 10-5 shows an example of the appearance of the ticket pane when a ticket is cleared.

*Table 10-5 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 10-6 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 10-6 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 10-7 shows an example of the appearance of the ticket pane when an Up ticket is generated.

*Table 10-7 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.

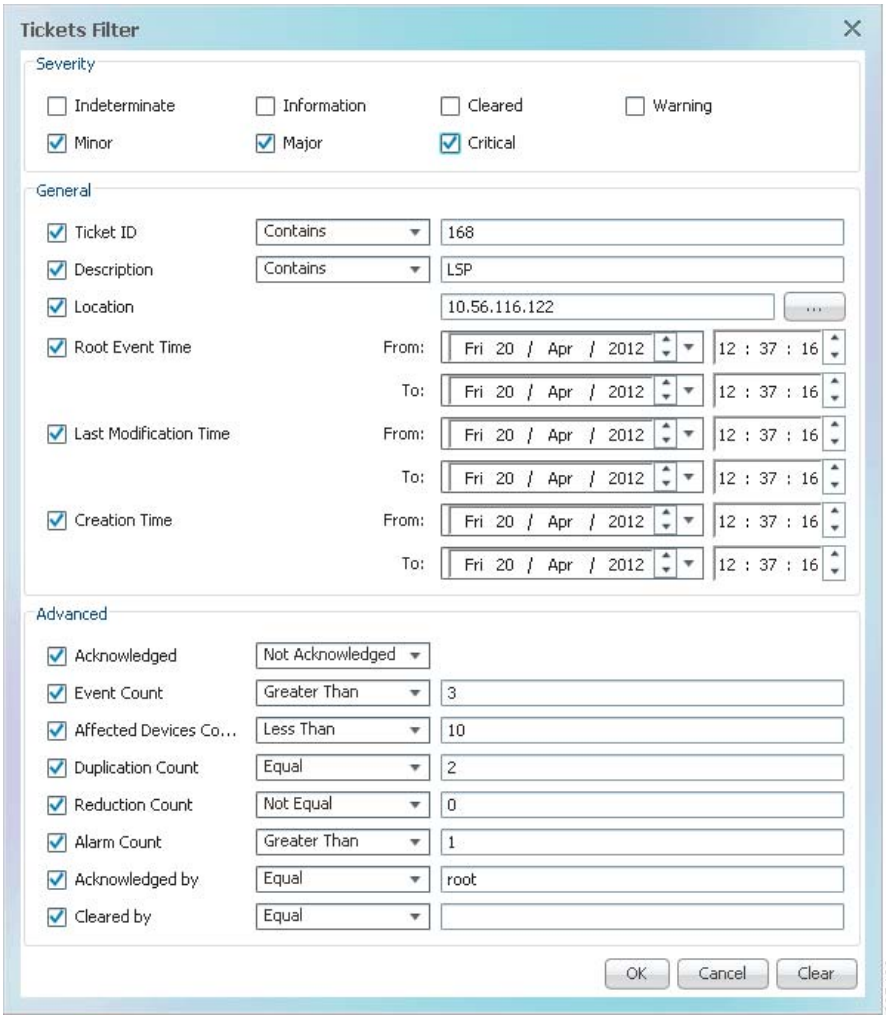
## Filtering Tickets by Criteria

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 10-2).

*Figure 10-2 Ticket Filter Dialog Box*




**Step 2** Specify the filter criteria by using the following steps and the information in Table 10-8:

**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 10-8 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 10-8 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

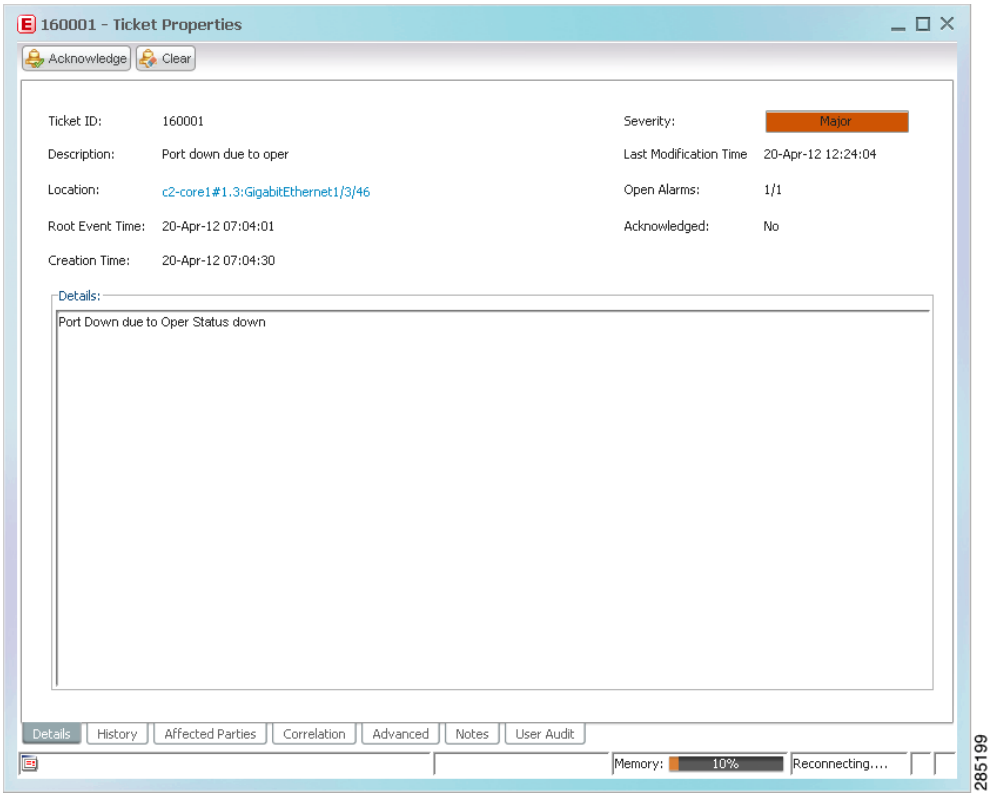
The properties of a selected ticket can be viewed by displaying the Ticket Properties window. For example, you can view alarm severity, correlated alarms, active alarms, alarm history, or the source of the alarm.

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 10-3 shows the Ticket Properties window.

***Figure 10-3 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 10-12
- Details Tab, page 10-12
- History Tab, page 10-13
- Affected Parties Tab, page 10-14
- Correlation Tab, page 10-17
- Advanced Tab, page 10-18
- Notes Tab, page 10-18
- User Audit Tab, page 10-19

# Ticket Properties Toolbar

The Ticket Properties window contains the tools described in Table 10-9.

*Table 10-9 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 10-7.<br>If a ticket was acknowledged, and some events were correlated to it afterward, then the ticket is considered to have not been acknowledged.<br>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 10-7.<br>This button is enabled only if the severity of the alarm is higher than Cleared or Normal. |
| | Saves the notes for the selected ticket.<br>This button is enabled only when text is entered in the Notes field of the Notes tab. |

# Details Tab

Table 10-10 describes the information that is displayed in the Details tab about the compiled alarm.

*Table 10-10 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.<br>**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 10-10 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 10-4 shows the History tab.

*Figure 10-4 History Tab*

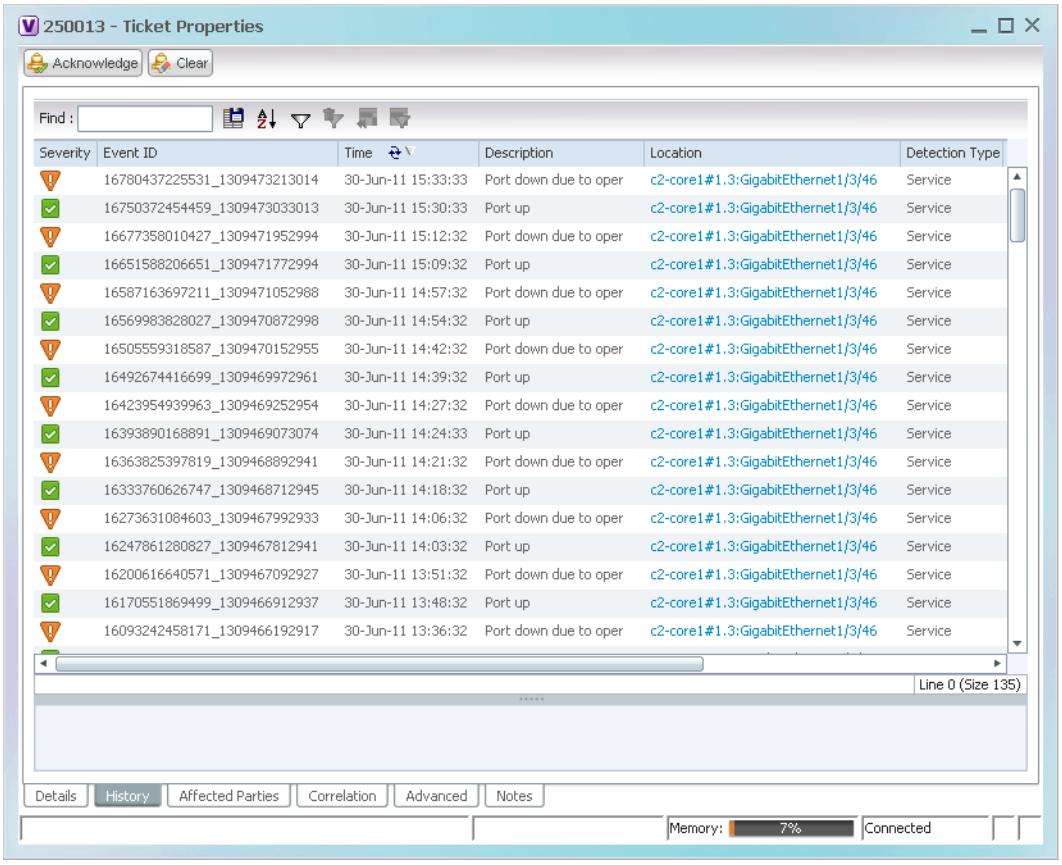


Table 10-11 describes the information that is displayed in the History tab.

*Table 10-11 Ticket Properties Window - History Tab*

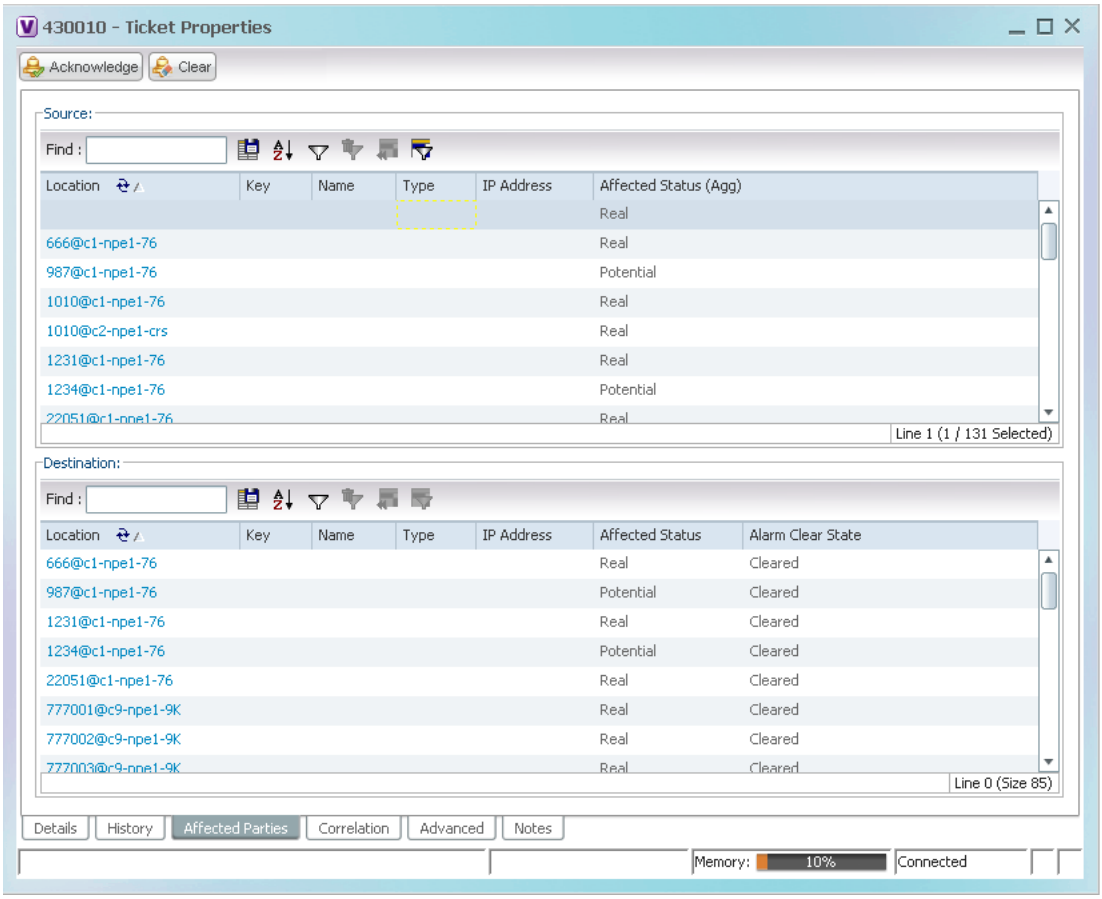
| Field | Description |
|---|---|
| Severity | Severity bell icon, colored according to the severity of the alarm. |
| Event ID | Event identifier of the specific alarm. |
| Time | Date and time the event was received by the Event Collector. |
| Description | Description of the event. |
| Location | Entity that triggered the alarm, as a hyperlink that opens the relevant location.<br>**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.<br>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 10-5 Affected Parties Tab*




The Affected Parties tab contains two tables: Source and Destination. Table 10-12 describes the information that is displayed in the Affected Properties tab.

*Table 10-12 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 10-12 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:<br>• Potential<br>• Real<br>• Recovered<br>• 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 10-22. |
| Alarm Clear State | For each pair, an indication of the clear state of the alarm:<br>• Cleared—All related alarms for this pair have been cleared.<br>• 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 10-6 Correlation Tab***

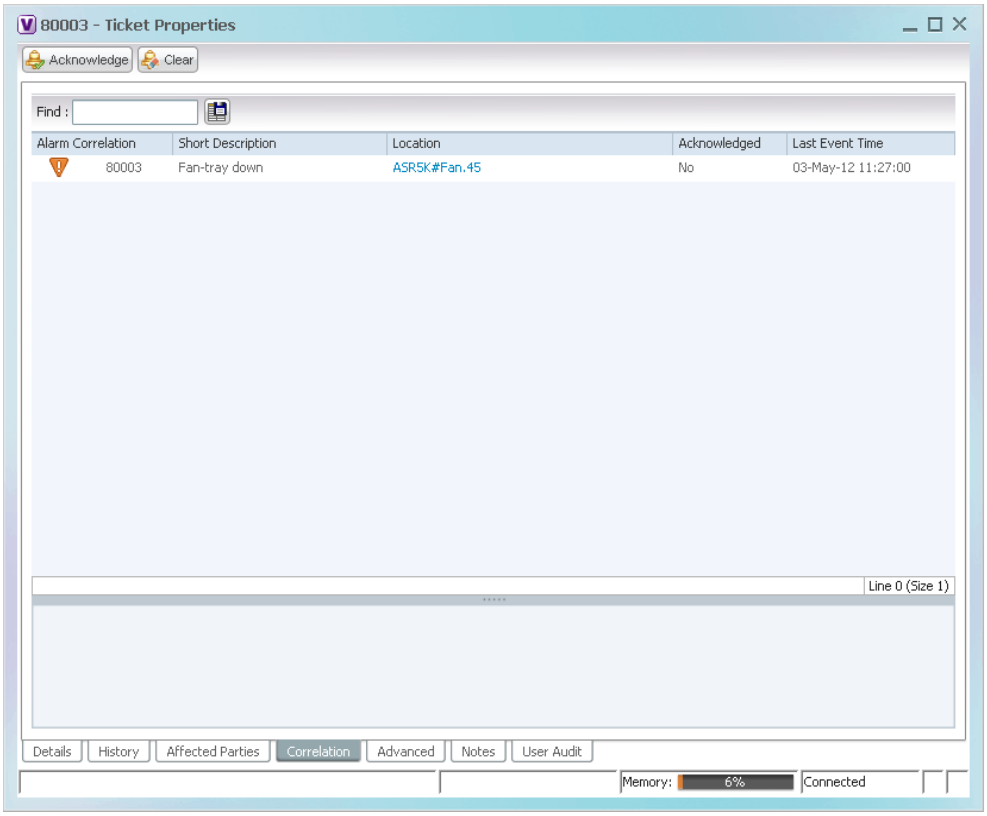



Table 10-13 describes the information that is displayed in the Correlation tab.

***Table 10-13 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.<br>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.<br>**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 10-13 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 10-19
- Acknowledging a Ticket, page 10-19
- Clearing a Ticket, page 10-20
- Removing a Ticket, page 10-20
- Clearing and Removing Tickets, page 10-21


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 3.10 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, select one or more tickets in the ticket pane, and then right-click and choose **Acknowledge**. For more information, see Understanding Ticket Status, page 10-6.

# 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 10-20.

Clearing an open ticket performs the following operations:

- For tickets relating to physical network elements (e.g., link down, card out), the faulty network element is removed from the Prime Network 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 10-6.

# 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 10-6.

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 2-38.

# 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.

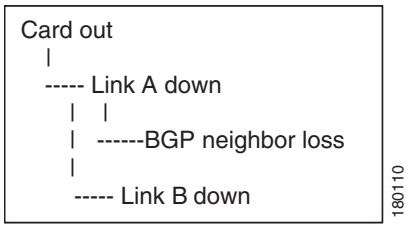
In the following example, these alarm types exist in the correlation tree:

- 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 10-7 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 10-7:

- 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 11

# 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 11-1
- Using the Report Manager, page 11-4
- Report Categories, page 11-11
- Generating Reports, page 11-23
- Scheduling Reports, page 11-39
- Managing Reports, page 11-40
- Defining Report Types, page 11-46
- Managing Report Folders, page 11-46


## 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 3.10 Administrator Guide*.

The following tables identify the tasks that you can perform:

- Table 11-1 identifies whether you can generate a report if a selected element **is not in** one of your assigned scopes.
- Table 11-2 identifies whether you can generate a report if a selected element **is in** one of your assigned scopes.
- Table 11-3 identifies the tasks you can perform on the reports that you generate.
- Table 11-4 identifies the tasks you can perform on the reports that someone else generates.
- Table 11-5 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 3.10 Administrator Guide*.

***Table 11-1 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 11-2 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 11-3 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 11-4 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 11-5 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 11-5 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 |

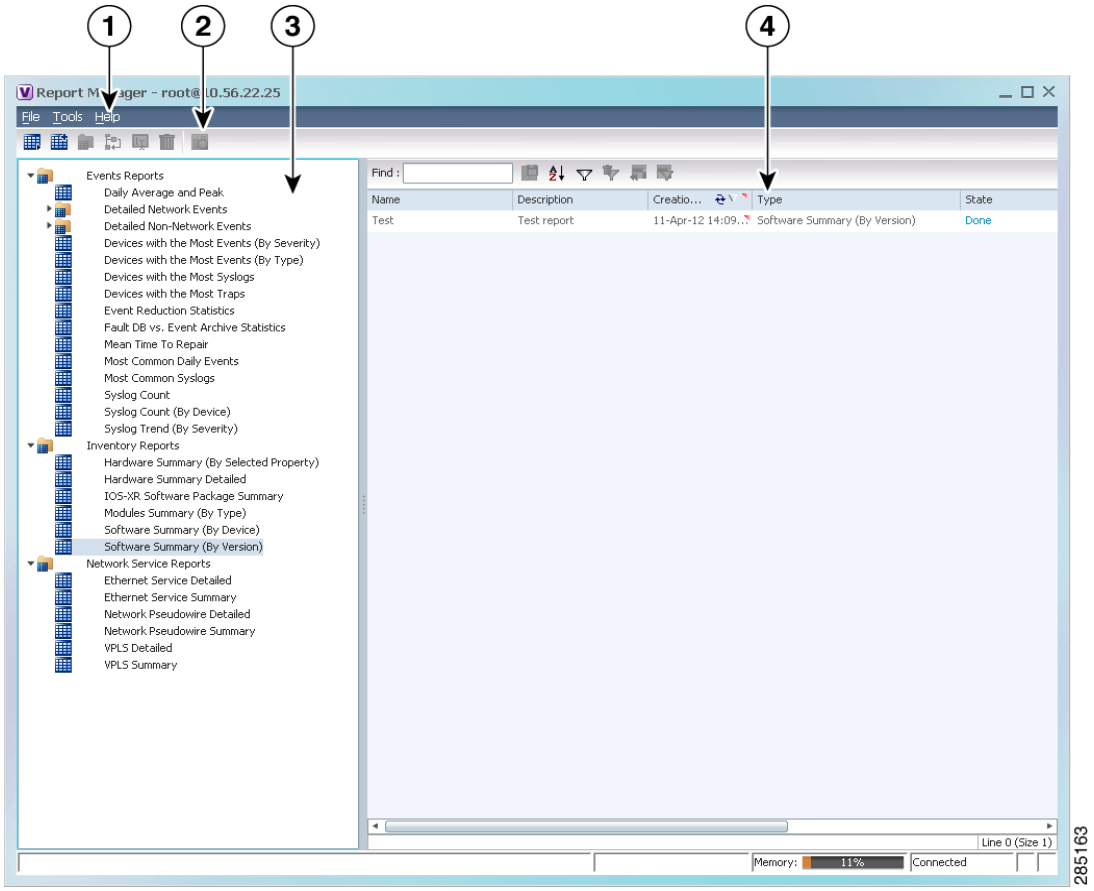
1. You cannot perform this action on system-generated folders, such as the Events Reports folder.

# 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 11-1) 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.

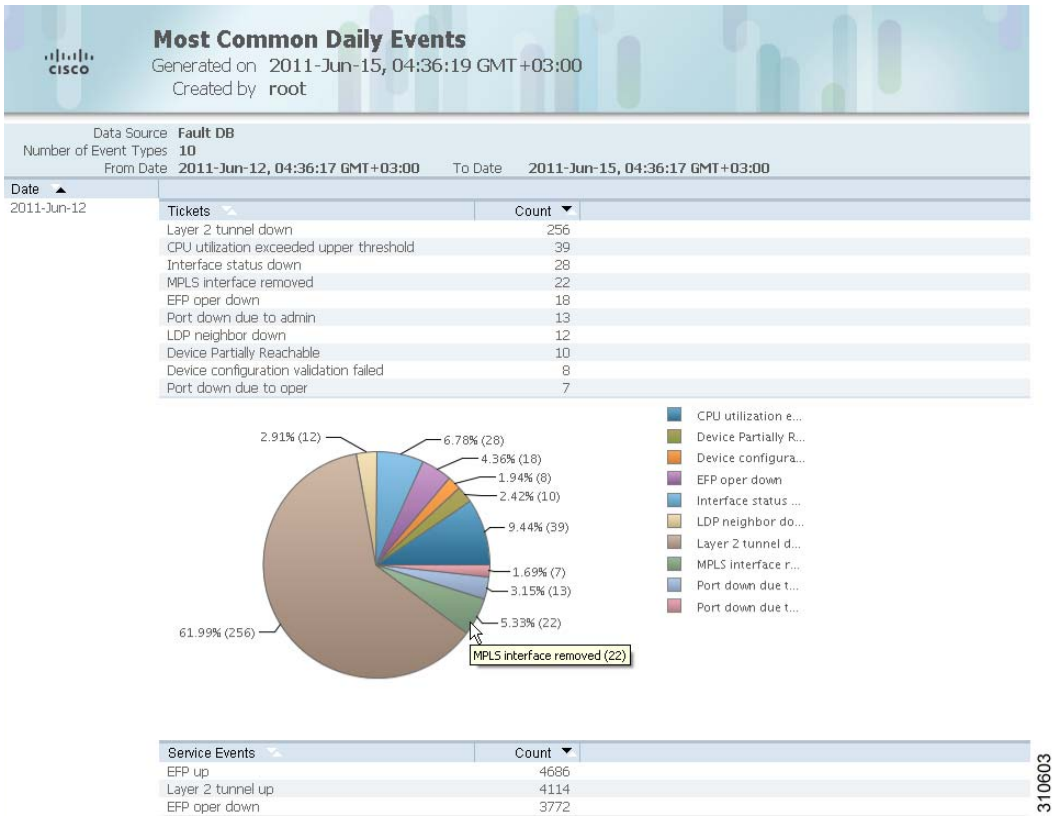
*Figure 11-1 Report Manager Window*




| | | | |
|---|---|---|---|
| **1** | Menu bar | **3** | Navigation tree with report types and folders |
| **2** | Toolbar | **4** | Content pane |

Figure 11-2 shows an example of a generated report with a pie chart.

***Figure 11-2 Sample Report***




Generated reports contain the following information in the report heading:

- Report name
- Date, time, and time zone 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 11-6 describes the menu options available in the Report Manager window.

*Table 11-6 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.<br>**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 11-7 identifies the buttons that appear in the Report Manager toolbar.

*Table 11-7 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 11-7 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 11-12.

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 11-3 shows an example of the content pane.

*Figure 11-3 Reports Manager Content Pane*

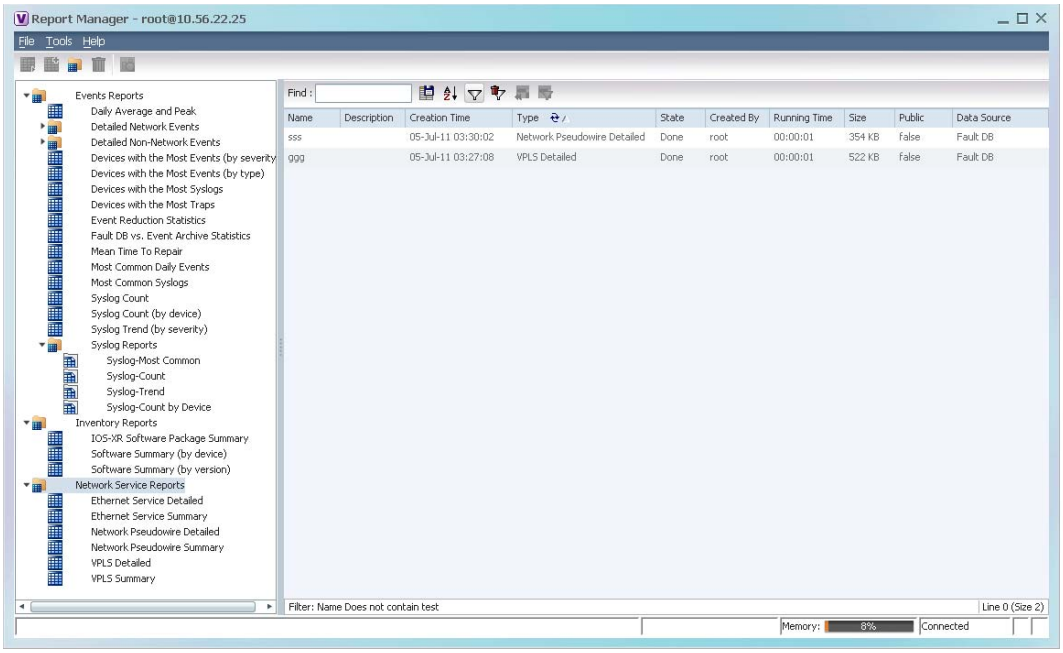



Table 11-8 describes the information displayed in the content pane for each report.

*Table 11-8 Reports Manager Content Pane Information*

| Attribute | Description |
|---|---|
| Name | Name of the report.<br>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.<br>For more information about the Failed state, see Generating Reports, page 11-23. |
| Created By | User who created the report. |
| Running Time | Amount of time it takes for the report to be complete. |
| Size | Report size. |

*Table 11-8 Reports Manager Content Pane Information (continued)*

| Attribute | Description |
|---|---|
| Public | Availability of the report to other users:<br>• True—The report is available to all users.<br>• 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 3.10 Administrator Guide.*

# Right-Click Options

Right-click options are available for:

- Navigation Pane Folders, page 11-9
- Navigation Pane Reports, page 11-10
- Content Pane Reports, page 11-10

## Navigation Pane Folders

Table 11-9 describes the options available when you right-click a folder in the navigation pane.

*Table 11-9 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 11-48. |

## Navigation Pane Reports

Table 11-10 describes the options available when you right-click a report in the navigation pane.

*Table 11-10 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.<br>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 11-45.<br>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 11-11 describes the options available when you right-click a report in the content pane.

*Table 11-11 Report Manager Content Pane Report Right-Click Options*

| Option | Description |
|---|---|
| View As | Displays the report in the selected format:<br>• HTML<br>• PDF<br>• CSV<br>• XLS<br>• XML<br>The default option, HTML, is displayed in bold font. For more information on viewing reports, see Viewing and Saving Reports, page 11-41. |
| Rename | Renames the selected report. |

*Table 11-11 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.<br><br>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 3.10 Administrator Guide*. |
| Delete Report | Deletes the selected reports. |
| Cancel | This option is displayed only while the selected report is being generated or queued.<br><br>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 11-11.
- Inventory—See Inventory Reports, page 11-19.
- Network services—See Network Service Reports, page 11-21.

# Events Reports

Prime Network Vision provides the following standard event report types:

- General report types, as described in Table 11-12.
- Detailed network event reports, as described in Table 11-13.
- Detailed non-network event reports, as described in Table 11-14.

*Table 11-12 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:<br>• Second<br>• Ten seconds<br>• Minute<br>• Hour<br>• Day | Fault database |
| Database Monitoring | For regular time intervals:<br>• Number of active tickets<br>• Number of active alarms<br>• Number of active events<br>• Number of unconnected events<br>• Number of auto-archive candidates<br>• Number of notifications<br>• Biggest Ticket ID<br>• Number of event count in the biggest ticket<br>• Actionable Event rate per second<br>• Number of dangling events handled by the integrity process<br>• Number of tickets created by the integrity process | 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:<br>• Severity of the events associated with the device, sorted by severity<br>• Number of events for each severity<br>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:<br>• Type of events associated with the device<br>• Number of events received for each event type<br>A pie chart presents the information by device and percentage in a graphical format. | Fault database |

*Table 11-12 Standard Events Report Types (continued)*

| Report Name | Description | Data Source |
|---|---|---|
| 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.<br>You can run this report on the Prime Network fault database or the event archive.<br>A pie chart presents the information by device and percentage in a graphical format. | User choice:<br>• Fault database<br>• 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.<br>You can run this report on the fault database or the event archive.<br>A pie chart presents the information by device and percentage in a graphical format. | User choice:<br>• Fault database<br>• Event archive |
| Event Reduction Statistics | For the specified devices and time period:<br>• Names of those tickets with:<br>– The root cause in the device list<br>– The ticket creation time within the specified period<br>• For each ticket type identified:<br>– Number of tickets of that type<br>– Fewest number of correlated events<br>– Highest number of correlated events<br>– Average number of correlated events | Fault database |
| Events Troubleshooting Info | Provides the following information:<br>• State—The event condition.<br>• Troubleshooting—The probable cause, action to be taken, and the clearing condition. | 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:<br>• Syslogs<br>• Traps<br>• Tickets<br>• Correlated events<br>• Uncorrelated events<br>• Nonnetwork events<br>• Network-originated events<br>• Network-originated and service events | Fault database and event archive |

*Table 11-12 Standard Events Report Types (continued)*

| Report Name | Description | Data Source |
|---|---|---|
| Mean Time to Repair | For the specified devices and time period:<br>• Names of those tickets with:<br>– The root cause in the device list<br>– The ticket creation time within the specified period<br>• For each ticket type identified:<br>– Whether the tickets were cleared by the user or network<br>– Number of tickets<br>– Minimum time (in seconds) to repair<br>– Maximum time (in seconds) to repair<br>– Average time (in seconds) to repair<br>**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 |
| Most Common Daily Events | For each day in the specified time period:<br>• Specified number of most common tickets, service events, syslogs, and traps<br>• Number of each type of ticket, service event, syslog, and trap<br>• 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.<br>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.<br>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.<br>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:<br>• By priority<br>• For the specified time period<br>• At the specified intervals | Fault database |

*Table 11-13 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:<br>• For syslogs:<br>– Syslog severities<br>– Number of syslogs per severity<br>– Syslog type<br>– Number of each syslog type<br>• For traps:<br>– Trap severities<br>– Number of traps per severity<br>– Trap type<br>– Number of each trap type<br>• For tickets:<br>– Ticket severities<br>– Number of tickets per severity<br>– Ticket type<br>– Number of each ticket type<br>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:<br>• Event severity<br>• Event identifier<br>• Timestamp<br>• Brief and detailed descriptions<br>• Device on which the event occurred<br>• Alarm identifier<br>• Ticket identifier<br>• Causing event identifier<br>• Duplication count<br>• Reduction count | Fault database |

*Table 11-13 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:<br>• IP address<br>• Date and time of each syslog, in ascending order<br>• Syslog raw data or description, depending on the data source<br>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:<br>• Ticket severity<br>• Ticket identifier<br>• Last modification time<br>• Root event time<br>• Description<br>• Entity that caused the alarm<br>• Whether or not the ticket is acknowledged<br>• Ticket creation time<br>• Event count<br>• Affected devices count<br>• Duplication count<br>• Reduction count<br>• Alarm count | Fault database |
| Detailed Traps | For each managed device that is selected, the following information for the specified time period:<br>• IP address<br>• Time of trap<br>• SNMP version<br>• Trap description<br>• Generic or device-specific trap OID, if the source is the event archive<br>• Long description, if the data source is the fault database<br>The maximum number of traps retrieved for this report depends on whether the Long Description check box is selected. When checked, a maximum of 30,000 traps are retrieved. When this check box is not checked, a maximum of 100,000 traps are retrieved for this report. | User Selection: Event archive or fault database |

*Table 11-14 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:<br>• Event severity<br>• Event identifier<br>• Timestamp<br>• Description<br>• Command name<br>• Command signature<br>• Command parameters<br>• Originating IP address<br>• Username | Fault database |
| Detailed Provisioning Events | For each provisioning event included in the report for the specified time period, severities, and search criteria:<br>• Event severity<br>• Event identifier<br>• Timestamp<br>• Description<br>• Location<br>• Username<br>• Device username<br>• Status | Fault database |

*Table 11-14 Detailed Non-Network Events Report Types (continued)*

| Report Name | Description | Data Source |
|---|---|---|
| Detailed Security Events | For each security event included in the report for the specified time period, severities, and search criteria:<br>• Event severity<br>• Event identifier<br>• Timestamp<br>• Description<br>• Location<br>• Username<br>• 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:<br>• Event severity<br>• Event identifier<br>• Timestamp<br>• Description<br>• Location | Fault database |

# Inventory Reports

Table 11-15 describes the standard inventory report types provided by Prime Network Vision and the data source.

*Table 11-15 Standard Inventory Report Types*

| Report Name | Description | Data Source |
|---|---|---|
| Hardware Detailed | For each device included in the report:<br>• IP address<br>• Device series<br>• Element type<br>You can view other hardware information for each device by selecting the required items from the available list as given below:<br>• Chassis—chassis description, chassis serial number, shelf description, shelf serial number, and shelf status<br>• Module—module name, sub module name, module status, hardware type, and hardware version<br>• Port—port location, port type, porting sending alarm, port alias, port status, port managed, PID, and pluggable type serial number. | Network elements |
| Hardware Summary | For each device included in the report:<br>• IP address<br>• System name<br>• Serial number<br>• Element type<br>• Device series<br>• Vendor<br>• Product<br>• Chassis<br>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 11-15 Standard Inventory Report Types (continued)*

| Report Name | Description | Data Source |
|---|---|---|
| IOS-XR Software Package Summary | For each device included in the report:<br>• Device name<br>• Element type<br>• IP address<br>• Serial number<br>• Cisco IOS XR software version<br>• For each software package installed on the device:<br>– Storage location<br>– Software package name<br>– Module name<br>– Software package state: Active or Inactive | Network elements |
| Modules Summary (By Type) | For each device filtered by module type:<br>• IP address<br>• Module serial number<br>• Module hardware version<br>• Module software version<br>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:<br>• Device name<br>• Element type<br>• IP address<br>• Serial number<br>• Software version on the device<br>• Name of image file | Network elements |
| Software Summary (By Version) | For each software version included in the report:<br>• Number of devices running the version<br>• Device names<br>• Element types<br>• Device IP address<br>• Device serial number<br>• Name of image file | Network elements |

# Network Service Reports

Table 11-16 describes the standard network service report types provided by Prime Network Vision and the data source.

*Table 11-16 Standard Network Service Report Types*

| Report Name | Description | Data Source |
|---|---|---|
| Ethernet Service Detailed | For each Ethernet service in the report:<br>• Ethernet service or Layer 2 VPN name<br>• Business tag assigned to the Ethernet service or Layer 2 VPN instance<br>• EVC name<br>• Business tag assigned to the EVC<br>• Maps containing the Ethernet service or Layer 2 VPN<br>• Edge EFPs associated with the EVC or Layer 2 VPN<br>• EFD fragment names<br>• EFD fragment type<br>You can filter report content by specifying part or all of the:<br>• Ethernet service name<br>• EVC name<br>• Ethernet service business tag<br>• EVC business tag<br>• Map name | Fault database |
| Ethernet Service Summary | For each Ethernet service in the report:<br>• Ethernet service or Layer 2 VPN name<br>• Business tag assigned to the Ethernet service or Layer 2 VPN instance<br>• EVC name<br>• Business tag assigned to the EVC<br>• Maps containing the Ethernet service or Layer 2 VPN<br>You can filter report content by specifying part or all of the:<br>• Ethernet service name<br>• EVC name<br>• Ethernet service business tag<br>• EVC business tag<br>• Map name | Fault database |

*Table 11-16 Standard Network Service Report Types (continued)*

| Report Name | Description | Data Source |
|---|---|---|
| Network Pseudowire Detailed | For each network pseudowire in the report:<br>• Pseudowire name<br>• Pseudowire type<br>• Business tag assigned to the pseudowire<br>• Maps containing the pseudowire<br>• Pseudowire details<br>• Type of pseudowire, such as pseudowire edge, Ethernet flow point, or switching entity<br>You can filter report content by specifying part or all of the:<br>• Pseudowire name<br>• Pseudowire type<br>• Business tag<br>• Map name | Fault database |
| Network Pseudowire Summary | For each network pseudowire in the report:<br>• Pseudowire name<br>• Pseudowire type<br>• Business tag assigned to the pseudowire<br>• Maps containing the pseudowire<br>You can filter the report content by specifying part or all of the:<br>• Pseudowire name<br>• Pseudowire type<br>• Business tag<br>• Map name | Fault database |

*Table 11-16 Standard Network Service Report Types (continued)*

| Report Name | Description | Data Source |
|---|---|---|
| VPLS Detailed | For each VPLS or H-VPLS instance in the report:<br>• VPLS or H-VPLS name<br>• Business tag associated with the VPLS or H-VPLS instance<br>• Maps containing the VPLS or H-VPLS instance<br>• VPLS details<br>• Type of VPLS service, such as VPLS forward, access EFP, or core pseudowire<br>You can filter report content by specifying part or all of the:<br>• VPLS or H-VPLS name<br>• Business tag<br>• Map name | Fault database |
| VPLS Summary | For each VPLS or H-VPLS instance in the report:<br>• VPLS or H-VPLS name<br>• Business tag assigned to the VPLS or H-VPLS instance<br>• Maps containing the VPLS or H-VPLS instance<br>You can filter report content by specifying part or all of the:<br>• VPLS or H-VPLS name<br>• Business tag<br>• Map name | Fault database |

# Generating Reports

You can generate reports in any of the following ways:

- Generating Reports from Report Manager, page 11-24
- Generating Reports from the Reports Menu, page 11-38
- Generating Reports from Prime Network Vision, page 11-39

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 11-11. 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 11-24
- Generating Inventory Reports, page 11-32
- Generating Network Service Reports, page 11-35

**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**.

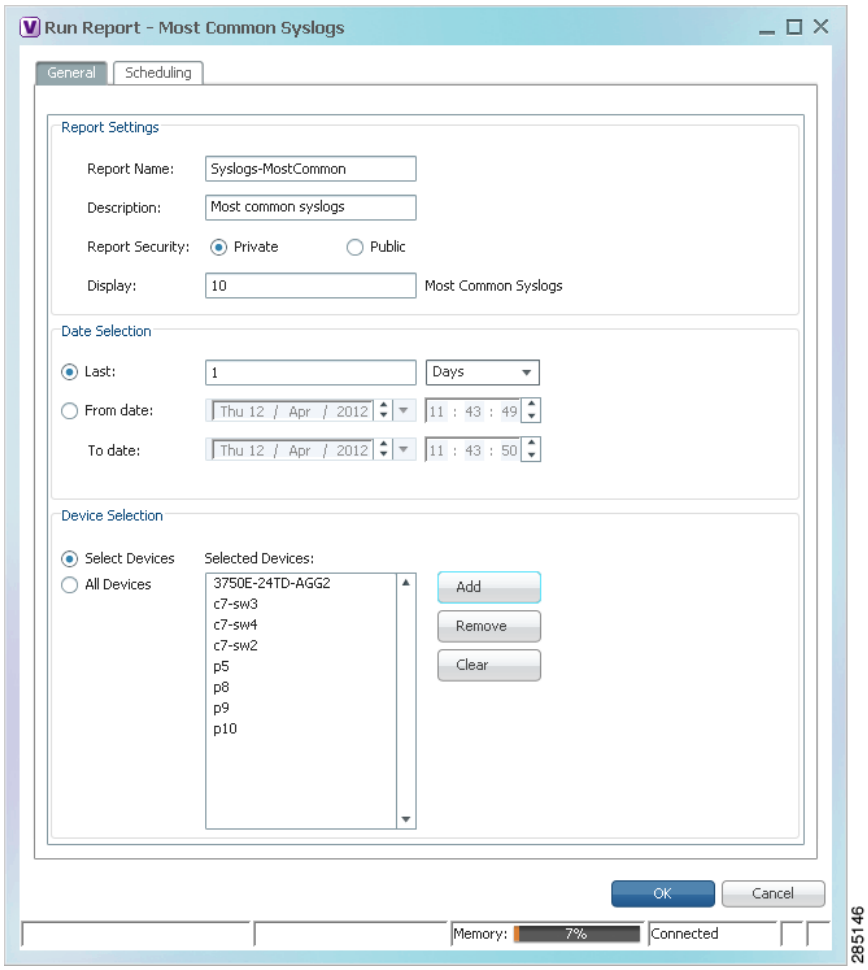
**Step 2** In the Report Manager window, choose **Events Reports >** *report-type*.

For information on the reports available for events, see Table 11-12.

**Step 3** Generate the report by right-clicking the report type, then choosing **Run**.

The Run Report dialog box is displayed. An example is shown in Figure 11-4. The fields displayed in the Run Report dialog box vary depending on the type of report.

*Figure 11-4 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 11-17.
- For detailed network reports, use the information in Table 11-18.
- For detailed non-network reports, use the information in Table 11-19.

*Table 11-17 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.<br>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.<br>Indicate the level of security for the report by clicking the appropriate option:<br>• Private—The report can be viewed and used only by the report creator and the administrator.<br>• 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.<br>**Note** You can share reports with others only if sharing is enabled in Prime Network Administration. For more information, see the *Cisco Prime Network 3.10 Administrator Guide*. |
| Display *n* | This field does not appear for all reports.<br>Enter the number of items to be displayed in the generated report. |
| Data Source | This field does not appear for all reports.<br>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.<br>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<br>To Date | Specify the date range for the report:<br>1. Click **From Date**.<br>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.<br>3. Enter a time for the start date, using the format HH MM SS.<br>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.<br>5. Enter a time for the end date, using the format HH MM SS. |

*Table 11-17 Events Report - Run Report Dialog Box Fields (continued)*

| Option | Description |
|---|---|
| **Device Selection** | |
| Select Devices | **Note**<br>• You can add only those devices that are within your scope.<br>• A user with the Administrator role can select unmanaged devices (by IP address) for reports that run on the Event Archive.<br>Select devices to include in the report:<br>1. Click **Select Devices**.<br>2. Click **Add**.<br>3. In the Add Network Element dialog box, select devices using either of the following methods:<br>– To select devices that meet specific criteria, click **Search** and enter the required criteria.<br>– To select from all network elements, click **Show All**.<br>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.<br>5. Click **OK**. |
| All Devices | This field does not appear for all reports.<br>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:<br>• 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.<br>• To include all syslog messages in the report, click **Add All**.<br>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.<br>Click the **Sort Order** button to sort the syslog messages in alphabetic or reverse alphabetic order. |

*Table 11-18 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.<br>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.<br>Indicate the level of security for the report by clicking the appropriate option:<br>• Private—The report can be viewed and used only by the report creator and the administrator.<br>• 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.<br>**Note** You can share reports with others only if sharing is enabled in Prime Network Administration. For more information, see the *Cisco Prime Network 3.10 Administrator Guide*. |
| Data Source | This field does not appear for all reports.<br>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<br>To Date | Specify the date range for the report:<br>1. Click **From Date**.<br>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.<br>3. Enter a time for the start date, using the format HH MM SS.<br>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.<br>5. Enter a time for the end date, using the format HH MM SS. |

*Table 11-18 Detailed Network Events Reports - Run Report Dialog Box Fields (continued)*

| Option | Description |
|---|---|
| **Device Selection** | |
| Select Devices | **Note**<br>• You can add only those devices that are within your scope.<br>• A user with the Administrator role can select unmanaged devices (by IP address) for reports that run on the Event Archive.<br>• The Detailed Event Count (by device) report accepts a maximum of 1000 devices.<br>Select devices to include in the report:<br>1. Click **Select Devices**.<br>2. Click **Add**.<br>3. In the Add Network Element dialog box, select devices using either of the following methods:<br>– To select devices that meet specific criteria, click **Search** and enter the required criteria.<br>– To select from all network elements, click **Show All**.<br>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.<br>5. Click **OK**. |
| All Devices | This field does not appear for all reports.<br>Click **All Devices** to include all devices in your scope in the report. |
| **Severity** | |
| Severity | This field does not appear for all reports.<br>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.<br>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.<br>In the Raw Data Contains field, enter the string that the syslog raw data must contain to be included in the report. |

*Table 11-18 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.<br>1. Check the Show Long Description check box to include the long description in the report.<br>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.<br>Specify the generic traps to include in the report:<br>1. Select the generic traps to include in the report:<br>– All—Include all generic traps<br>– 0—coldStart<br>– 1—warmStart<br>– 2—linkDown<br>– 3—linkUp<br>– 4—authenticationFailure<br>– 5—egpNeighborLoss<br>– 6—enterpriseSpecific<br>2. If you select generic type 6, enter the OIDs (comma separated) in the Vendor Specific field.<br>The Vendor Specific field accepts a maximum of 125 digits. |

*Table 11-19 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.<br>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.<br>Indicate the level of security for the report by clicking the appropriate option:<br>• Private—The report can be viewed and used only by the report creator and the administrator.<br>• 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.<br>**Note** You can share reports with others only if sharing is enabled in Prime Network Administration. For more information, see the *Cisco Prime Network 3.10 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<br>To Date | Specify the date range for the report:<br>1. Click **From Date**.<br>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.<br>3. Enter a time for the start date, using the format HH MM SS.<br>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.<br>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 11-19 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 11-39.

**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**.

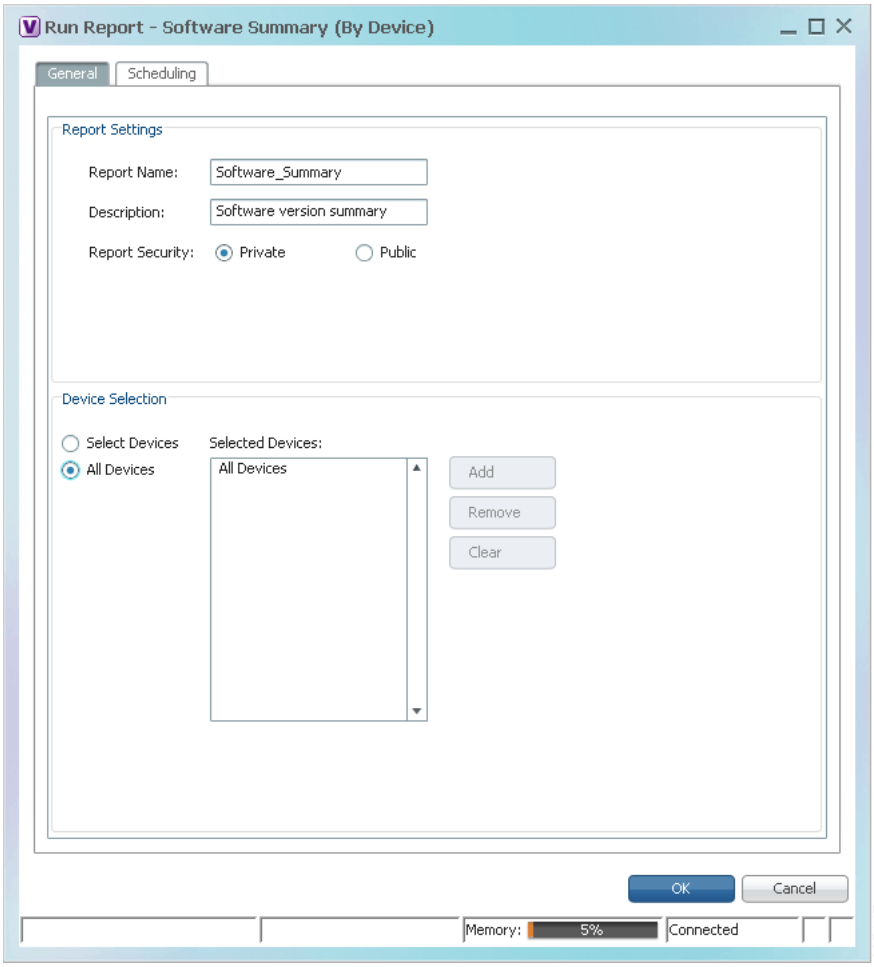
**Step 2** In the Report Manager window, choose **Inventory Reports >** *report-type*.

For information on the standard reports available for inventory, see Table 11-15.

**Step 3** Right-click the report type, then choose **Run**.

The Run Report dialog box is displayed as shown in Figure 11-5.

*Figure 11-5 Inventory Report - Run Report Dialog Box*




**Step 4** Enter the required information in the Run Report dialog box as described in Table 11-20.

*Table 11-20 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.<br>Report names cannot include the following characters: ;?<>/:\"#*\|. |
| Description | Enter a brief description of the report. |

*Table 11-20 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.<br>Indicate the level of security for the report by clicking the appropriate option:<br>• Private—The report can be viewed and used only by the report creator and the administrator.<br>• 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.<br>**Note** You can share reports with others only if sharing is enabled in Prime Network Administration. For more information, see the *Cisco Prime Network 3.10 Administrator Guide*. |
| **Device Selection** | |
| Select Devices | **Note** You can add only those devices that are within your scope.<br>Select devices to include in the report:<br>1. Click **Select Devices**.<br>2. Click **Add**.<br>3. In the Add Network Element dialog box, select devices using either of the following methods:<br>– To select devices that meet specific criteria, click **Search** and enter the required criteria.<br>– To select from all network elements, click **Show All**.<br>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.<br>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 11-39.

**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**.

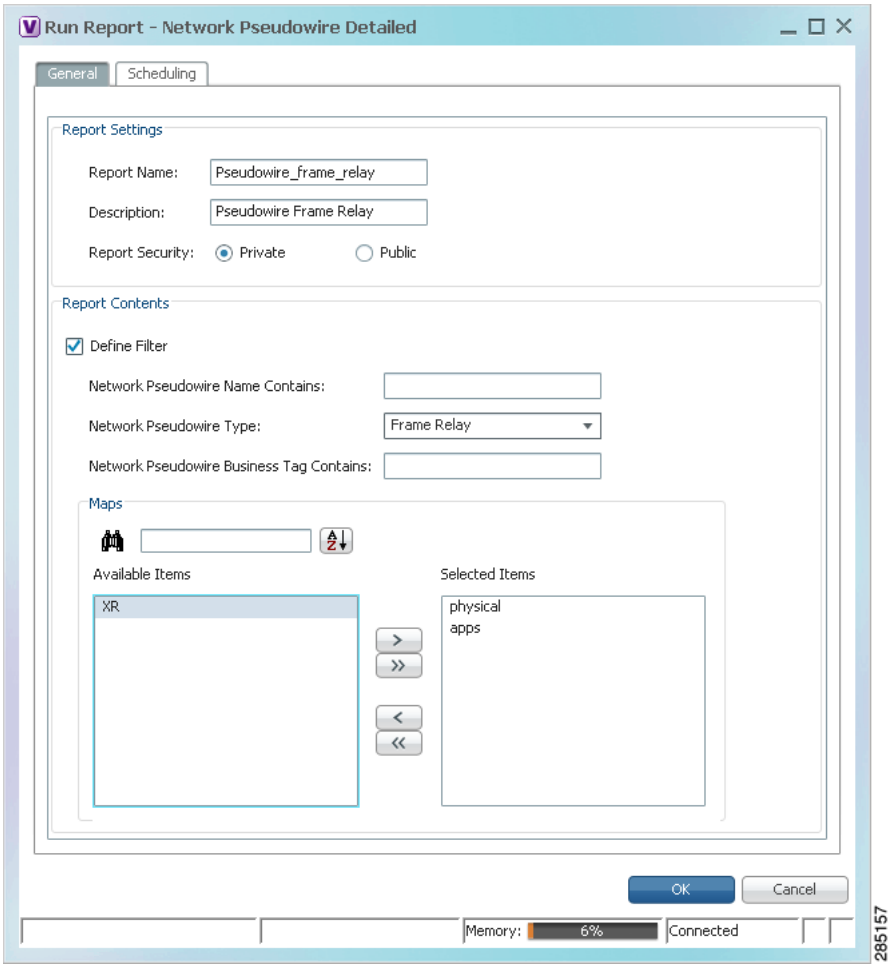
**Step 2** In the Report Manager window, choose **Network Service Reports >** *report-type*.

For information on the standard reports available for network services, see Table 11-16.

**Step 3** Right-click the report type, then choose **Run**.

The Run Report dialog box is displayed as shown in Figure 11-6.

***Figure 11-6 Network Service Report - Run Report Dialog Box***



**Step 4** Enter the required information the Run Report dialog box as described in Table 11-21.

*Table 11-21 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.<br>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.<br>Indicate the level of security for the report by clicking the appropriate option:<br>• Private—The report can be viewed and used only by the report creator and the administrator.<br>• 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.<br>**Note** You can share reports with others only if sharing is enabled in Prime Network Administration. For more information, see the *Cisco Prime Network 3.10 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.<br>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:<br>• 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.<br>• To include all maps in the report, click **Add All**.<br>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.<br>Click the **Sort Order** button to sort the maps alphabetically or in reverse alphabetic order. |

*Table 11-21 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.<br>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:<br>• 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.<br>• To include all maps in the report, click **Add All**.<br>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.<br>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.<br>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:<br>• 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.<br>• To include all maps in the report, click **Add All**.<br>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.<br>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 11-39.

**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 11-23.

**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 11-39.

**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 11-23.

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 11-39.

**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 11-11.

**Step 3** 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 11-23.

**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. You can also clone a scheduled job and edit the report criteria, if required.

# Managing Reports

Prime Network provides the following options for working with reports:


- Managing the Maximum Number of Concurrent Reports, page 11-40
- Viewing and Saving Reports, page 11-41
- Renaming Reports, page 11-42
- Sharing Reports, page 11-43
- Moving Reports Between Folders, page 11-44
- Deleting Reports, page 11-44
- Viewing Report Properties, page 11-45


## 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 3.10 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 3.10 Administrator Guide*.

To view and save a report:

**Step 1** Choose **Reports > Report Manager**.

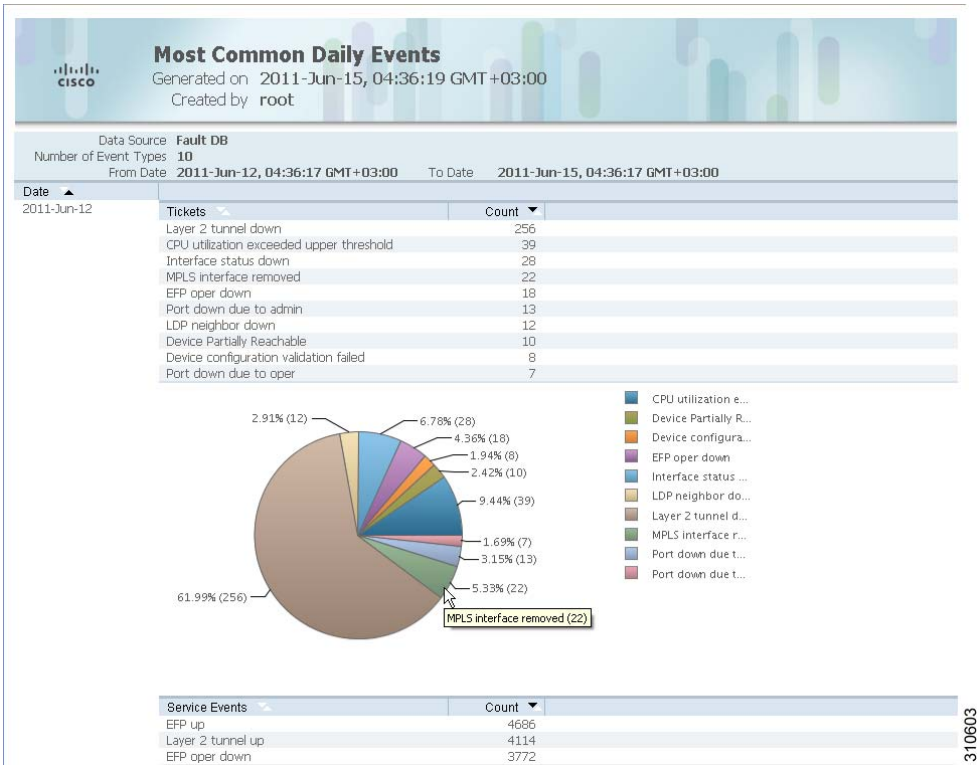
**Step 2** In the navigation pane, locate the required report.

**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 11-7 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 11-7 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 3.10 Administrator Guide*.

### Sharing a Report

To share access to a report that you generated:

**Step 1** Choose **Reports > Report Manager**.

**Step 2** Locate the required report.

**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** Locate the required report.

**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** 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** Locate the required report.

**Step 3** In the content pane, select the required report.

**Step 4** Right-click the report, then choose **Delete Report**.

**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:

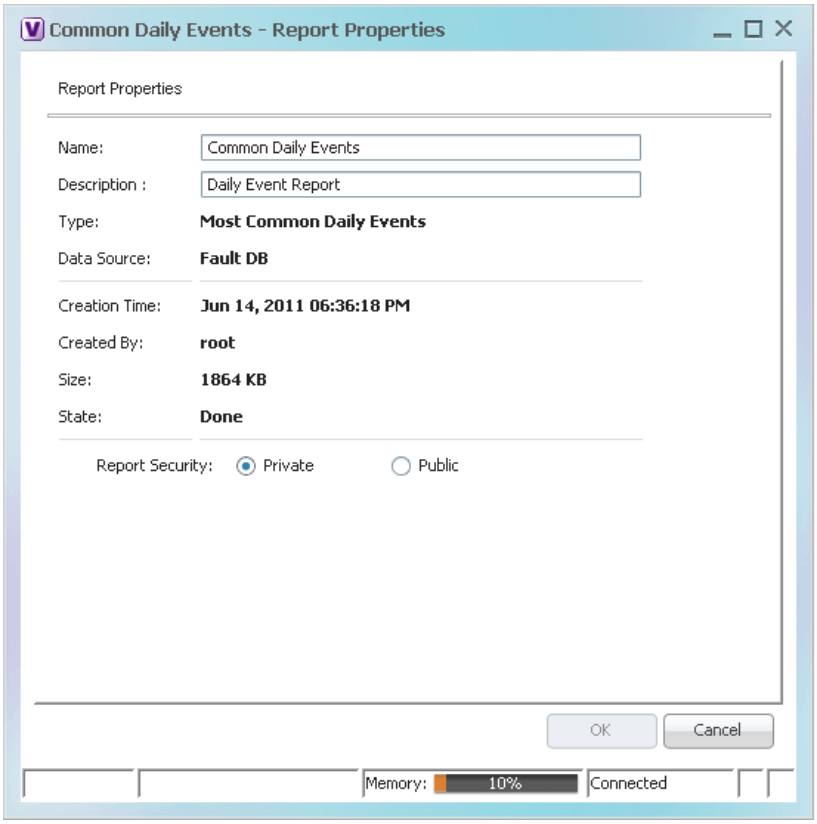
**Step 1** Choose **Reports > Report Manager**.

**Step 2** Locate the required report.

**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 11-8.

***Figure 11-8 Report Properties Dialog Box***




**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, right-click the existing report type, then choose **Define Report of This Type**.

**Step 3** In the Define report of type dialog box, specify the options using the information in Generating Reports, page 11-23.

**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.

# Managing Report Folders

Prime Network provides the following options for working with report folders:

- Creating Folders, page 11-46
- Moving Folders, page 11-47
- Renaming Folders, page 11-47
- Deleting Folders, page 11-48
- Viewing Folder and Report Type Properties, page 11-48

## 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** 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. 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** 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** 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** 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

### 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 11-9.

*Figure 11-9 Folder Properties*

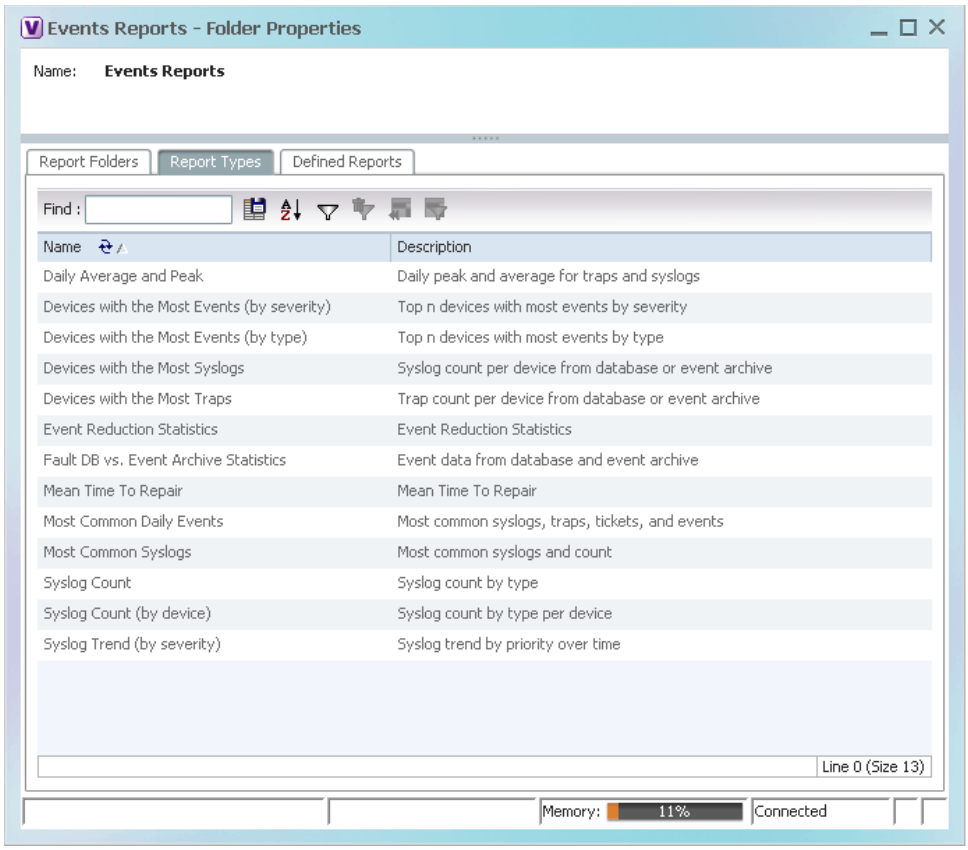



Table 11-22 describes the information that is displayed in each tab, depending on the folder's contents.

*Table 11-22 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 12

# 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 12-1
- Cisco PathTracer Overview, page 12-2
- Launching Path Tracer, page 12-3
- Viewing Path Traces in Cisco PathTracer, page 12-14
- Viewing Path Trace Details, page 12-20
- Saving and Opening Cisco PathTracer Map Files, page 12-26
- Saving Cisco PathTracer Counter Values, page 12-26
- Rerunning a Path and Comparing Results, page 12-27
- Viewing Q-in-Q Path Information, page 12-27
- Viewing L2TP Path Information, page 12-28
- Using Cisco PathTracer in MPLS Networks, page 12-29


## 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 3.10 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 3.10 Administrator Guide*.

***Table 12-1 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 12-2 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 Tracer

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 12-3 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 12-3 identifies the launching points for the different types of elements.

*Table 12-3 Cisco PathTracer Right-Click Menu Options*

| Element | Location |
|---|---|
| Affected Parties | • Inventory window<br>• 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<br>• Inventory window |
| IP interface | • Inventory window<br>• Affected entry |
| Layer 2 MPLS tunnel | Inventory window |
| MPLS-TE tunnel | Inventory window |
| MPLS-TP tunnel endpoint | • Map view or navigation pane<br>• Inventory window |
| Port | Inventory window |

*Table 12-3 Cisco PathTracer Right-Click Menu Options (continued)*

| Element | Location |
|---|---|
| Pseudowire endpoint | • Map view or navigation pane<br>• Inventory window |
| Site | Map view |
| Switching entity | Map view |
| Virtual connection | Inventory window:<br>• Cross Connect window<br>• VC Table window |
| VLAN | • Navigation pane<br>• Map view |

# Starting a Path Trace

You can start a path trace in the following ways:

- From the Map View, page 12-5
- From Logical or Physical Inventory, page 12-7

## 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**.

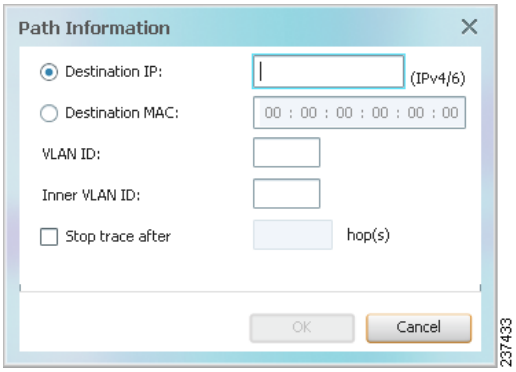
  **b.** In the Ethernet Flow Domain List Properties window, double-click the required domain.

  **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 12-1). Continue with Step 2.
- If you choose **PathTracer > Start Here**, continue with Step 3.

*Figure 12-1 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 12-4.

Depending on the launch point, the Path Information dialog box might not contain all of the fields in Table 12-4.

*Table 12-4 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 12-20.

## 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 12-5.

  **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 12-3.

- **PathTracer > Start Here**—If you choose this option, continue with Step 3 in From the Map View, page 12-5.

# 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 12-8
- Using an IP Interface, page 12-9
- Using a VLAN Bridge, page 12-10
- Using an Ethernet Port, page 12-12

- Using a Pseudowire, page 12-12
- Using an MPLS-TP Tunnel Endpoint, page 12-13

## Using an Ethernet Flow Point

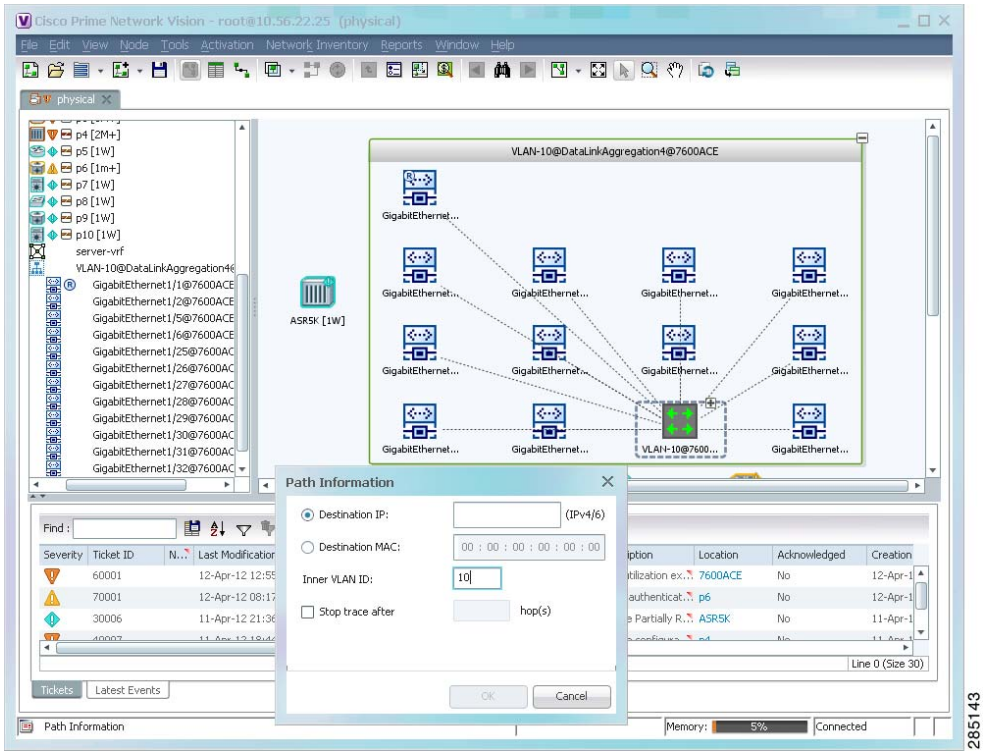
A network VLAN is required for you to start a path trace using an Ethernet flow point.

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 12-2.

***Figure 12-2 Ethernet Flow Point Path Trace Launch Point***




**Step 3** Specify the destination using the information in Table 12-4.

**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

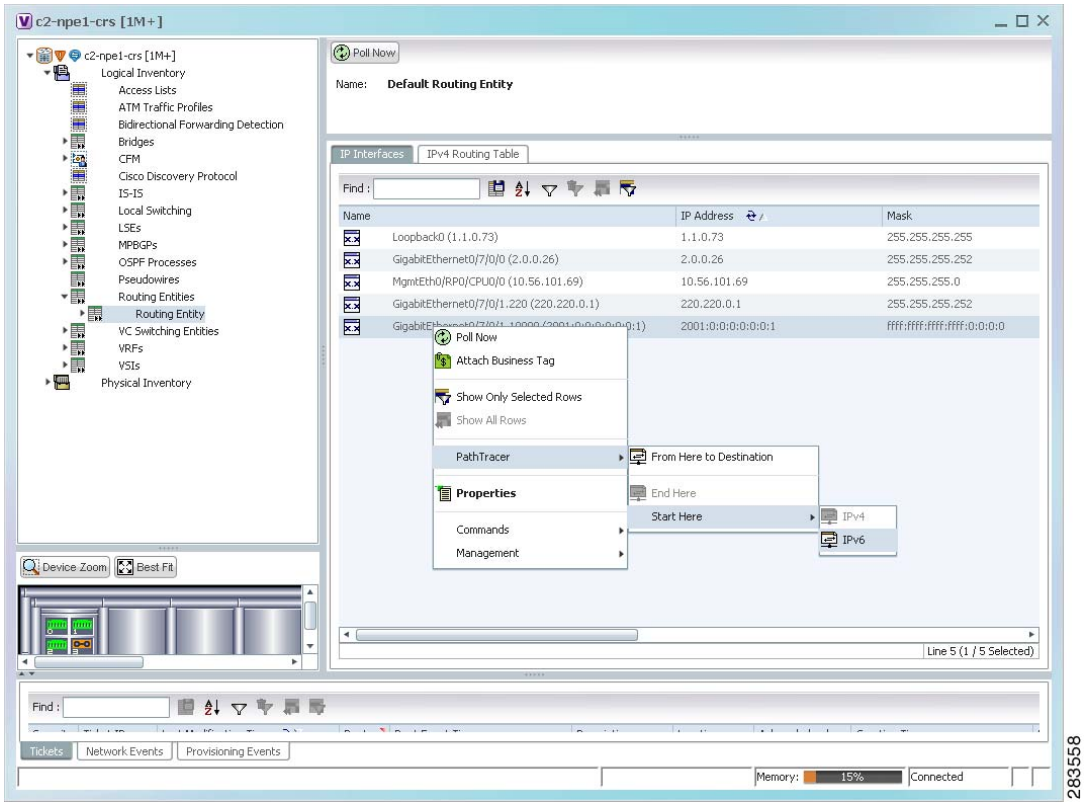
Both IPv4 and IPv6 addresses are supported as valid path trace sources and destinations as illustrated in the following procedure.

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 12-3.

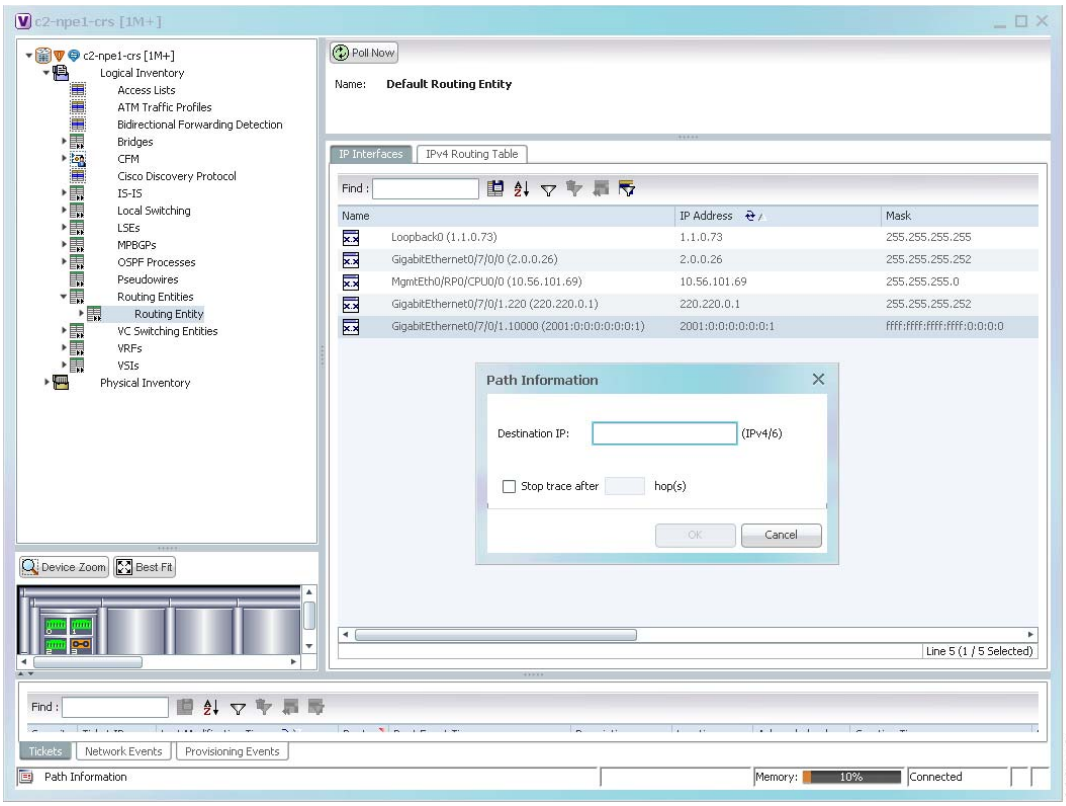
***Figure 12-3 IP Interface Path Trace Launch Point - Right-Click Menu***




**Step 2** Choose **PathTracer > From Here to Destination**.

The Path Information dialog box is displayed as shown in Figure 12-4.

*Figure 12-4 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

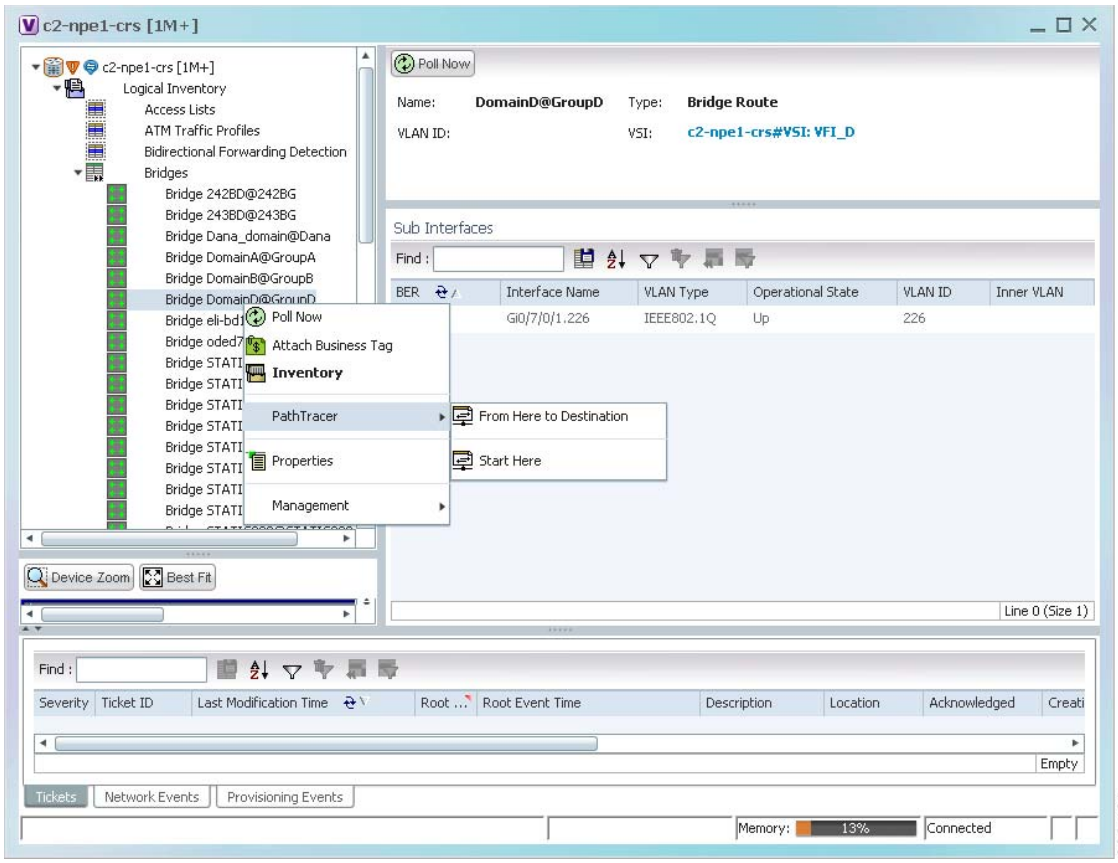
You can launch path traces from VLAN bridges. Additionally, MAC addresses in the VLAN bridge forwarding table can be path trace destinations.

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 12-5:

- **PathTracer > From Here to Destination**
- **PathTracer > Start Here**

*Figure 12-5 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 12-4.

**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.

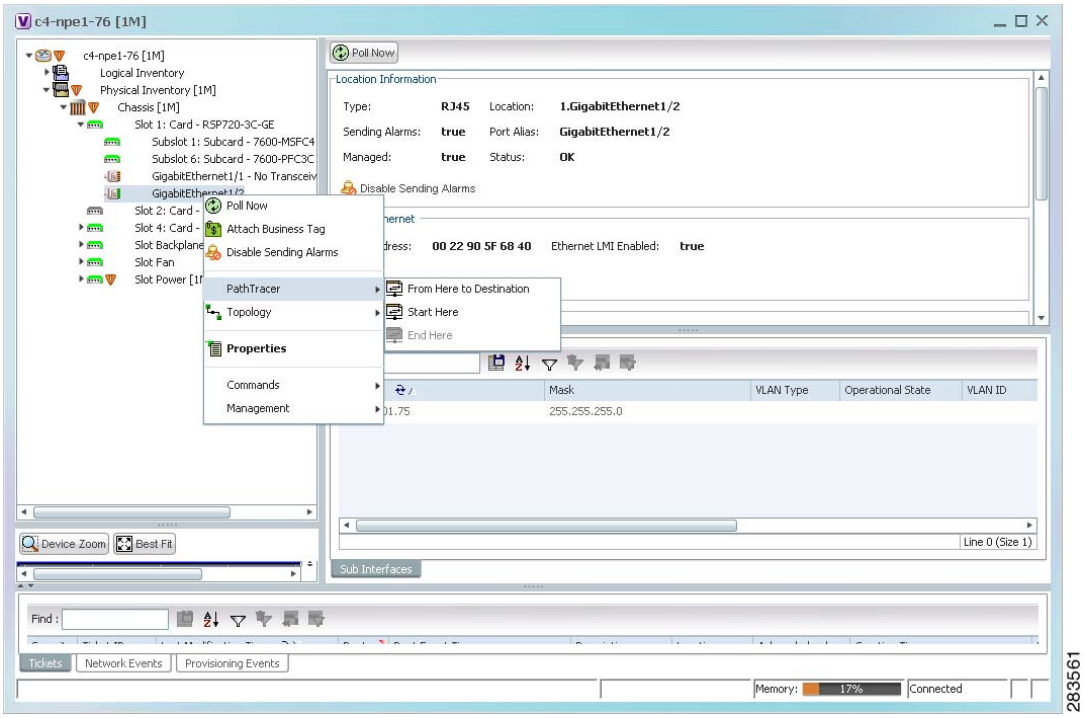
## Using an Ethernet Port

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 12-6:

- **PathTracer > From Here to Destination**
- **PathTracer > Start Here**

***Figure 12-6 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

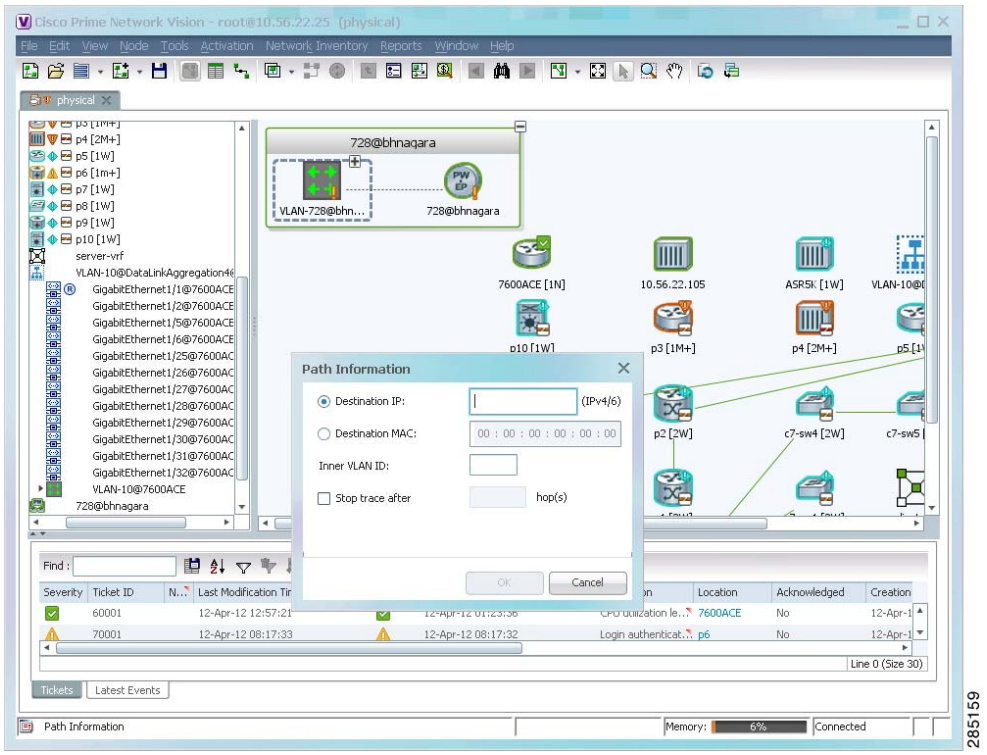
To launch a path trace from a network pseudowire endpoint:

**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 12-7.

*Figure 12-7 Path Information Dialog Box for a Network Pseudowire*




**Step 3** Specify the destination using the information in Table 12-4.

**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

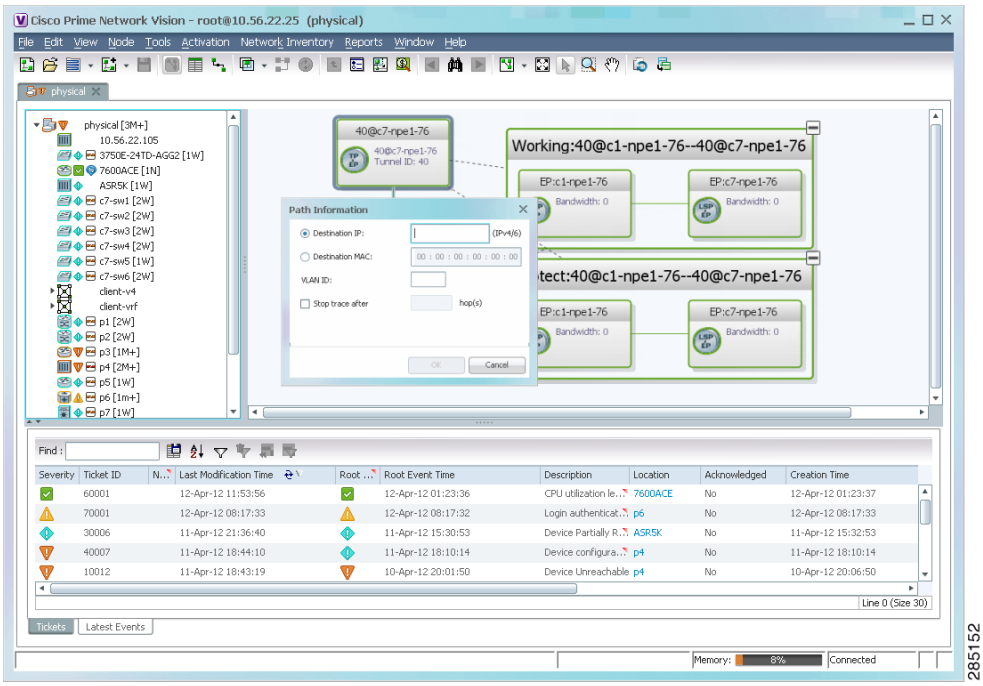
To launch a path trace from an MPLS-TP tunnel endpoint:

**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 12-8.

*Figure 12-8 MPLS-TP Tunnel Endpoint Path Trace Launch*




**Step 3** Specify the destination using the information in Table 12-4.

**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.

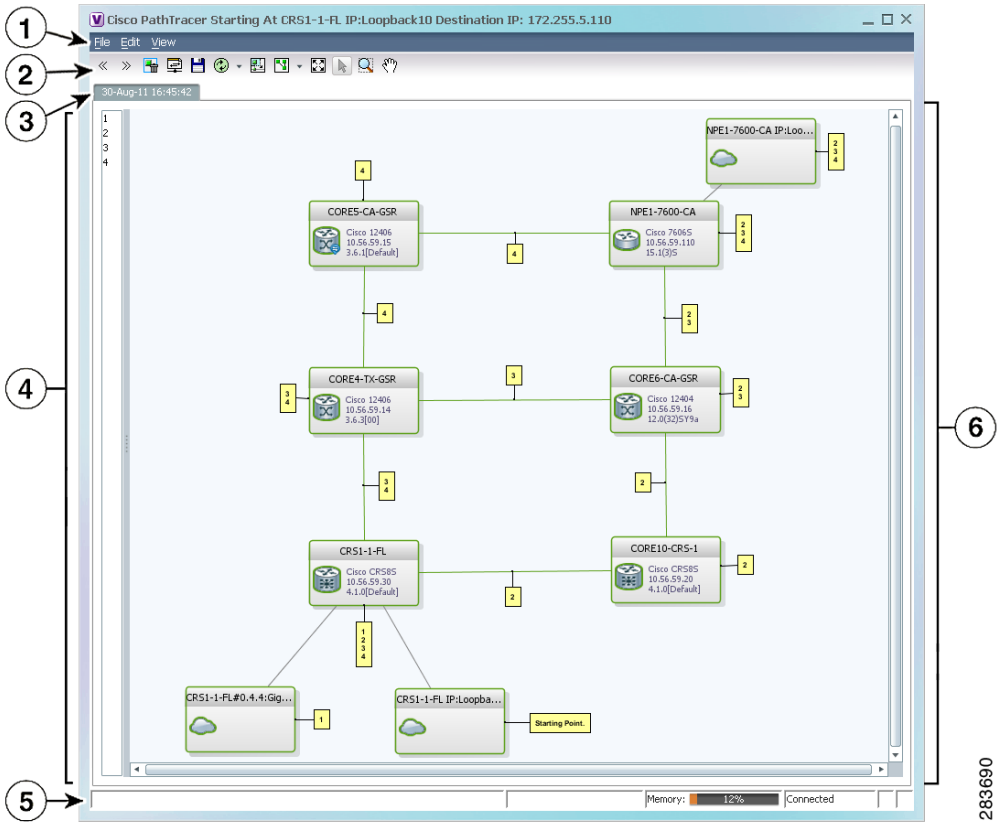
You can also right-click elements in the Cisco PathTracer window and choose options from a right-click menu. The right-click menu is context sensitive depending on the view and the item selected. For more information about the right-click menu and the available options, see Right-Click Menu Options, page 12-19.

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 12-9 shows an example of the Cisco PathTracer window with a multiple-path trace.

***Figure 12-9 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 12-16
- Toolbar, page 12-17
- Trace Tabs, page 12-18
- Paths Pane, page 12-18

- Path Trace Pane, page 12-18
- Right-Click Menu Options, page 12-19


# Menus

Table 12-5 describes the options available in the Cisco PathTracer menus.

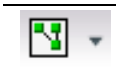
***Table 12-5 Cisco PathTracer Window Menu Options***

| Option | Description |
|---|---|
| **File Menu** | |
| Run Again | Offers the following options for running Cisco PathTracer again for the same source and destination:<br>• Change Hop Count—Enables you to enter a new hop count.<br>• Repeat Last Trace—Runs the previous trace with the same settings.<br>• 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 12-6 describes the options available in the Cisco PathTracer toolbar.

***Table 12-6 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 12-20. |
| | 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 12-26. |
| | Offers the following options for running Cisco PathTracer again for the same source and destination:<br>• Change Hop Count—Enables you to enter a new hop count.<br>• Repeat Last Trace—Runs the previous trace with the same settings.<br>• Run Full Path Trace—Runs the previous trace without a hop count limit.<br>The new path trace map is displayed in the path trace pane.<br>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 2-16
- Chapter 2, “Working with the Cisco Prime Network Vision Client”
- Map View, page 2-7

# 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 12-7 describes the right-click menu options that are available for elements selected in the Cisco PathTracer window.

*Table 12-7 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.<br>**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 | Displays the Configuration Management page for the selected device in Prime Network Change and Configuration Management. For more information, see Chapter 4, "Device Configurations and Software Images." |
| Image Mgmnt | Displays the Configuration Management page for the selected device in Prime Network Change and Configuration Management. For more information, see Chapter 4, "Device Configurations and Software Images." |
| 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. |
| Tools | Contains the following choices:<br>• CPU Usage—Displays memory and CPU usage information for a device or network element.<br>• Ping—Pings the device from the client station.<br>• Telnet—Communicates with the device using the Telnet window from the client station.<br>**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.<br>- For Windows 7 32-bit systems, enable the Windows Telnet Client to use the Prime Network Vision Telnet option.<br>- For Windows 7 64-bit systems, a solution is available on the Cisco Developer Network at http://developer.cisco.com/web/prime-network/forums/-/message_boards/message/2780108. |

*Table 12-7 Cisco PathTracer Element Right-Click Menu Options (continued)*

| Option | Description |
|---|---|
| Topology | Enables you to add:<br>• A static link between two devices.<br>• A static topology between a device and an unmanaged network.<br>• 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 3.10 Customization 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 , page 3-36, and those you create using Command Builder. For more information, see the *Cisco Prime Network 3.10 Customization Guide*. |
| Management | Contains the following submenu options:<br>• Command Builder—Defines commands and scripts using the Prime Network Command Builder tool (Configurator security level required).<br>• 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:<br>• Poll Now—Updates the VNE information.<br>• Stop VNE—Stops the VNE.<br>• Start VNE—Starts the VNE. |

# Viewing Path Trace Details

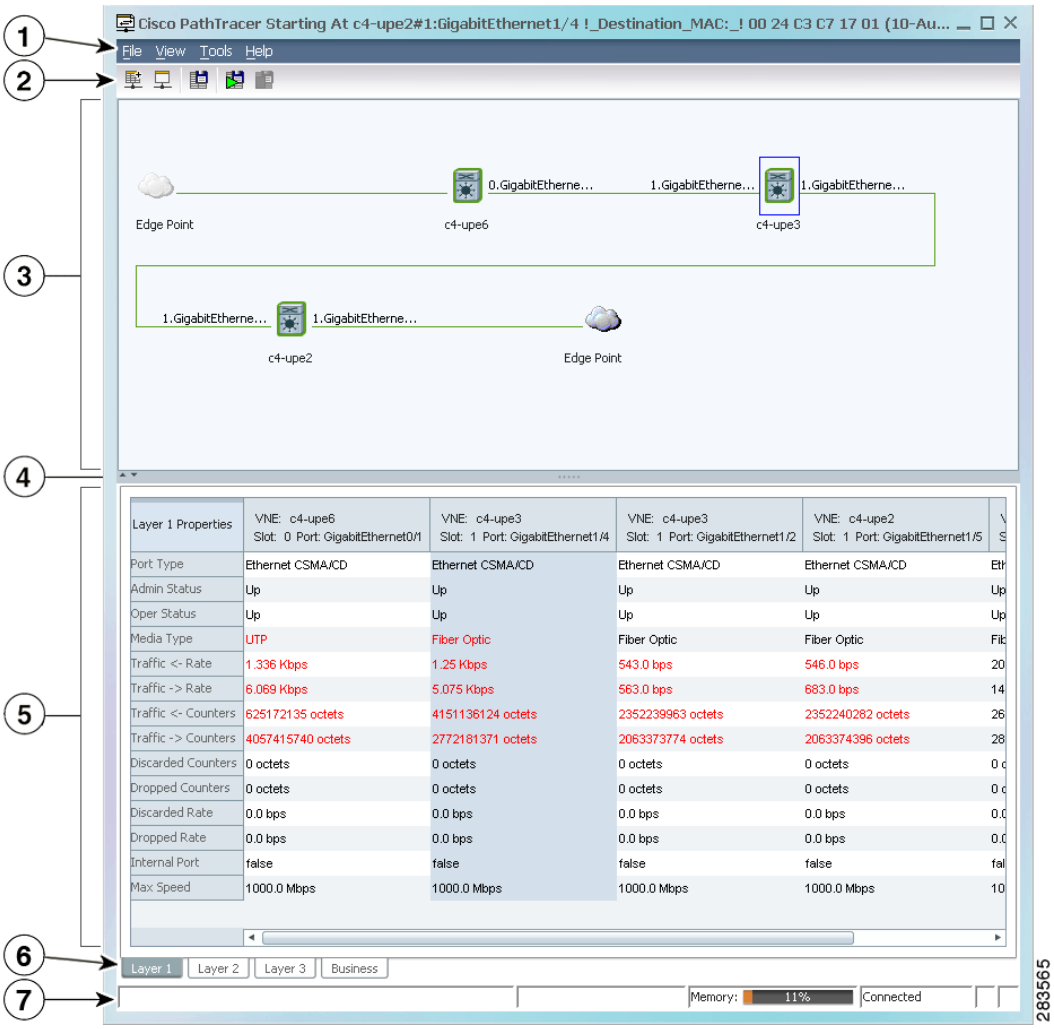
In addition to the information displayed in the Cisco PathTracer window, you can:

- 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 12-10 shows an example of the Cisco PathTracer details window.

*Figure 12-10 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 12-22
- Cisco PathTracer Details Window Toolbar, page 12-22
- Path Trace Pane, page 12-23
- Details Pane, page 12-25

# Menus

Table 12-8 describes the Cisco PathTracer details window menu options.

*Table 12-8 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 12-9 describes the tools that are available in the Cisco PathTracer details window toolbar.

*Table 12-9 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 12-10 describes the right-click menu options that are available for elements in the path trace pane.

***Table 12-10 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 | Displays the Configuration Management page for the selected device in Prime Network Change and Configuration Management. For more information, see Chapter 4, "Device Configurations and Software Images." |
| Image Mgmnt | Displays the Configuration Management page for the selected device in Prime Network Change and Configuration Management. For more information, see Chapter 4, "Device Configurations and Software Images." |
| Run Report | Enables you to run standard or user-defined events, inventory, and network service reports on demand. |

*Table 12-10 Cisco PathTracer Element Right-Click Menu Options (continued)*

| Option | Description |
|---|---|
| Tools | Contains the following choices:<br>• CPU Usage—Displays memory and CPU usage information for a device or network element.<br>• Ping—Pings the device from the client station.<br>• Telnet—Communicates with the device using the Telnet window from the client station.<br>**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.<br>- For Windows 7 32-bit systems, enable the Windows Telnet Client to use the Prime Network Vision Telnet option.<br>- For Windows 7 64-bit systems, a solution is available on the Cisco Developer Network at http://developer.cisco.com/web/prime-network/forums/-/message_boards/message/2780108. |
| Topology | Enables you to add:<br>• A static link between two devices.<br>• A static topology between a device and an unmanaged network.<br>• 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 3.10 Customization 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 Configure Basic Device Settings: Name, DNS, NTP, RADIUS, TACACs, ACLs, page 1-4, and those you create using Command Builder. For more information, see the *Cisco Prime Network 3.10 Customization Guide*. |

*Table 12-10 Cisco PathTracer Element Right-Click Menu Options (continued)*

| Option | Description |
|---|---|
| Management | Contains the following submenu options:<br>• Command Builder—Defines commands and scripts using the Prime Network Command Builder tool (Configurator security level required).<br>• 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:<br>• Poll Now—Updates the VNE information.<br>• Stop VNE—Stops the VNE.<br>• 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 Tracer, page 12-3.

**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 12-20.

**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 12-26), 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 12-26. 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 Tracer, page 12-3, 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 12-11 describes the information that is displayed in the Layer 2 tab for L2TP tunnels.

*Table 12-11 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. |

*Table 12-11 Layer 2 Tab Information for L2TP Tunnels (continued)*

| Field | Description |
|---|---|
| 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 > L2TPSession Counters | 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 12-30
- Using Cisco PathTracer for CSC Configurations, page 12-31
- Using Cisco PathTracer for Layer 3 VPNs, page 12-32
- Using Cisco PathTracer for Layer 2 VPNs, page 12-32
- Using Cisco PathTracer for MPLS TE Tunnels, page 12-33

# 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 12-12 lists the Cisco PathTracer starting points.

*Table 12-12 Cisco PathTracer MPLS Starting Points*

| Element | Location | Start Options |
|---|---|---|
| IP interface | • Inventory window<br>• Affected entity (enabled only if the affected entity has an IP interface) | • From Here to Destination<br>• Start Here |
| MPLS-TP tunnel endpoint | • Navigation or map pane<br>• Inventory window | • From Here to Destination<br>• Start Here |
| Site | Service view map | • From Here to Destination<br>• To Subnet Destination<br>• 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 12-13 lists the endpoints that can be selected as path destinations.

*Table 12-13 Cisco PathTracer MPLS Endpoints*

| Element | Location | End Options |
|---|---|---|
| IP interface | • Inventory window<br>• 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**.

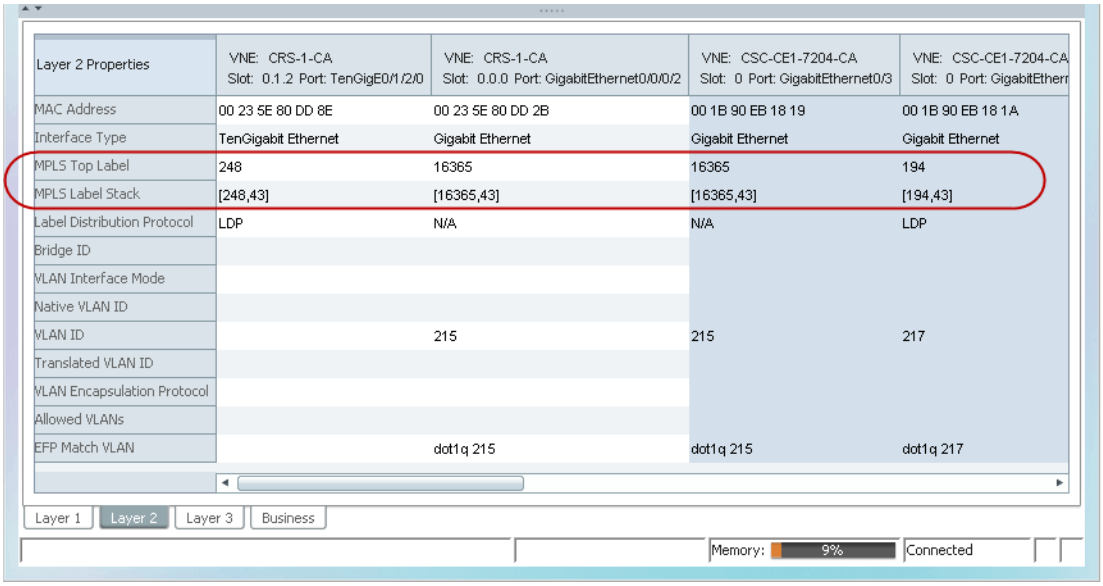
**Step 6** In the IP Interfaces table, right-click the required interface and choose **PathTracer > End Here**.

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 12-11.)

***Figure 12-11 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 12-14 describes the Layer 2 properties that can be displayed in the Layer 2 tab specifically for VPNs.

*Table 12-14 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:<br>• 0—Unknown<br>• 1—PWE3<br>• 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 12-15 describes the Layer 2 properties that can be displayed in the Layer 2 tab specifically for MPLS TE tunnels.

***Table 12-15 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.<br>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:<br>• If the Tunnel Oper Status value is Up, the Tunnel Admin Status value must also be Up.<br>• 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:<br>• Enabled—The tunnel cannot be rerouted.<br>• Disabled—The tunnel can be rerouted. |
| Tunnel LSP ID | LSP identifier. |
| 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:<br>• Dynamic—The tunnel is routed along the ordinary routing decisions after taking into account the tunnel constraints such as attributes, priority, and bandwidth.<br>• 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. |

*Table 12-15 Cisco PathTracer Layer 2 Properties for MPLS TE Tunnels (continued)*

| Field | Description |
|---|---|
| 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 13

# 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 13-2
- Viewing CDP Properties, page 13-6
- Viewing Link Layer Discovery Protocol Properties, page 13-8
- Viewing Spanning Tree Protocol Properties, page 13-10
- Viewing Resilient Ethernet Protocol Properties, page 13-14
- Viewing HSRP Properties, page 13-17
- Viewing Access Gateway Properties, page 13-19
- Working with Ethernet Link Aggregation Groups, page 13-22
- Viewing mLACP Properties, page 13-28
- Viewing Provider Backbone Bridge Properties, page 13-31
- Viewing EFP Properties, page 13-32
- Connecting a Network Element to an EFP, page 13-37
- Understanding EFP Severity and Ticket Badges, page 13-37
- Viewing EVC Service Properties, page 13-39
- Viewing and Renaming Ethernet Flow Domains, page 13-41
- Working with VLANs and VLAN Overlays, page 13-44
- Understanding Unassociated Bridges, page 13-72
- Working with Ethernet Flow Point Cross-Connects, page 13-74
- Working with VPLS and H-VPLS Instances, page 13-77
- Working with Pseudowires, page 13-89
- Working with Ethernet Services, page 13-104
- Viewing IP SLA Responder Service Properties, page 13-111
- Viewing IS-IS Properties, page 13-113
- Viewing OSPF Properties, page 13-116
- Configuring REP and mLACP, page 13-118
- Using Pseudowire Ping and Show Commands, page 13-119

- Configuring IS-IS, page 13-120

# 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 3.10 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 3.10 Administrator Guide*.

***Table 13-1 Default Permission/Security Level Required for Working with Carrier Ethernet Services - Element Not in User's Scope***

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

*Table 13-1 Default Permission/Security Level Required for Working with Carrier Ethernet Services - Element Not in User's Scope (continued)*

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

*Table 13-1 Default Permission/Security Level Required for Working with Carrier Ethernet Services - Element Not in User's Scope (continued)*

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

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

*Table 13-2 Default Permission/Security Level Required for Working with Carrier Ethernet Services - Element in User's Scope*

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

*Table 13-2 Default Permission/Security Level Required for Working with Carrier Ethernet Services - Element in User's Scope (continued)*

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

*Table 13-2 Default Permission/Security Level Required for Working with Carrier Ethernet Services - Element in User's Scope (continued)*

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

# Viewing CDP Properties

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

## In Logical Inventory

To view CDP properties:

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

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

The CDP properties are displayed in logical inventory as shown in Figure 13-1.

*Figure 13-1 CDP in Logical Inventory*

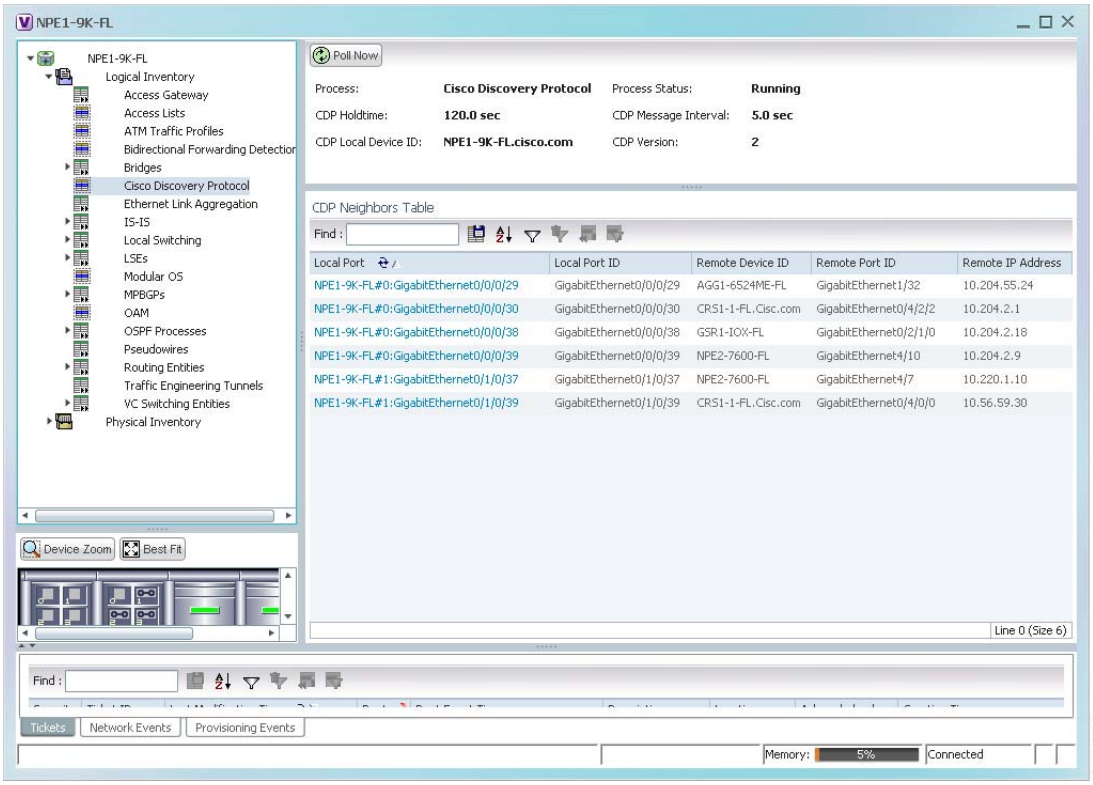



Table 13-3 describes the CDP instance properties that are displayed.

*Table 13-3 CDP Properties in Logical Inventory*

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

### In Physical Inventory

To view CDP on a Layer 2 port:

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

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

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

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

# Viewing Link Layer Discovery Protocol Properties

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

### In Logical Inventory

To view LLDP properties:

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

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

The LLDP properties are displayed in logical inventory as shown in Figure 13-2.

*Figure 13-2 LLDP in Logical Inventory*

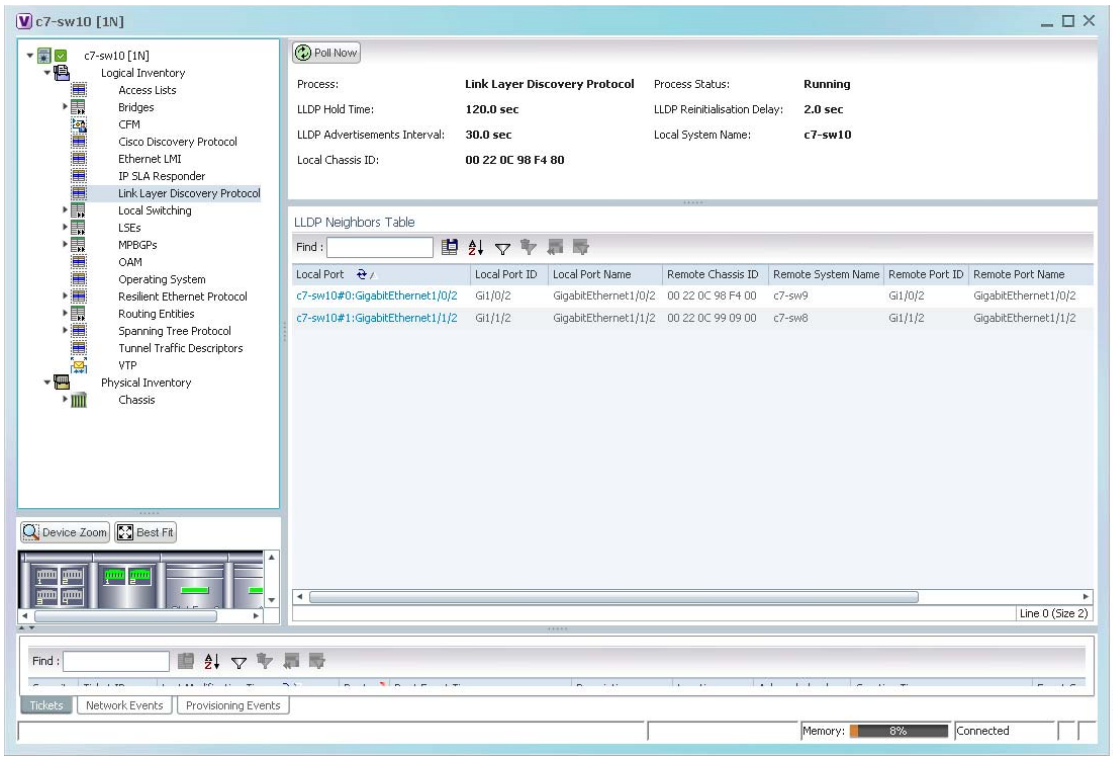



Table 13-4 describes the properties that are displayed for LLDP.

*Table 13-4 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 13-4 Link Layer Discovery Protocol Properties (continued)*

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

### In Physical Inventory

To view LLDP on a Layer 2 port:

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

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

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

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

# Viewing Spanning Tree Protocol Properties

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

To view Spanning Tree properties:

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

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

**Step 3** STP properties are displayed in logical inventory as shown in Figure 13-3.

*Figure 13-3 STP in Logical Inventory*

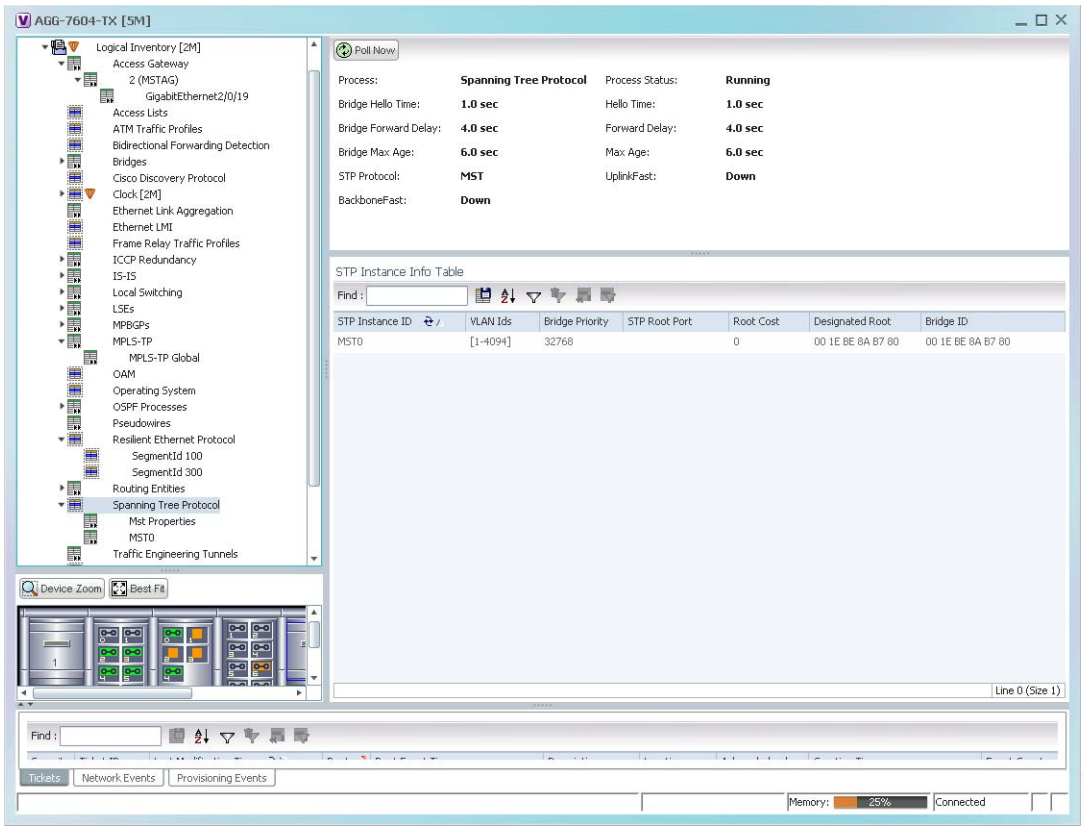



Table 13-5 describes the properties that are displayed for STP.

*Table 13-5 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 13-5 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 13-6 describes the information that is displayed in the STP Instance Information Properties window.

*Table 13-6 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 13-6 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.<br>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 13-7 describes the information that is displayed for MSTP.

*Table 13-7 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 13-65.
- VLAN service link properties—See Viewing STP Properties for VLAN Service Links, page 13-66.

# 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.

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

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

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

REP implementation supports the following faults:

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

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

You can view REP properties in logical inventory.

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

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

Figure 13-4 shows an example of REP in logical inventory.

***Figure 13-4 REP in Logical Inventory***

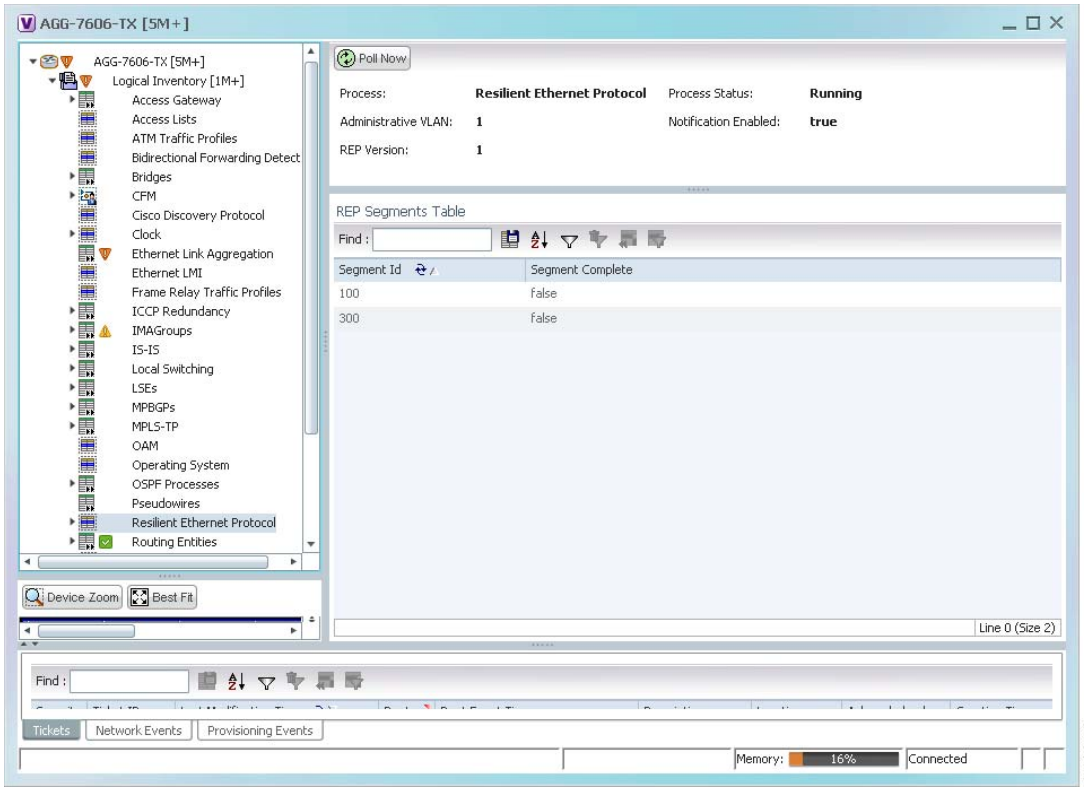



Table 13-8 describes the information that is displayed for REP.

***Table 13-8 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 13-5 shows an example of REP segment properties in logical inventory.

*Figure 13-5 REP Segment Properties*

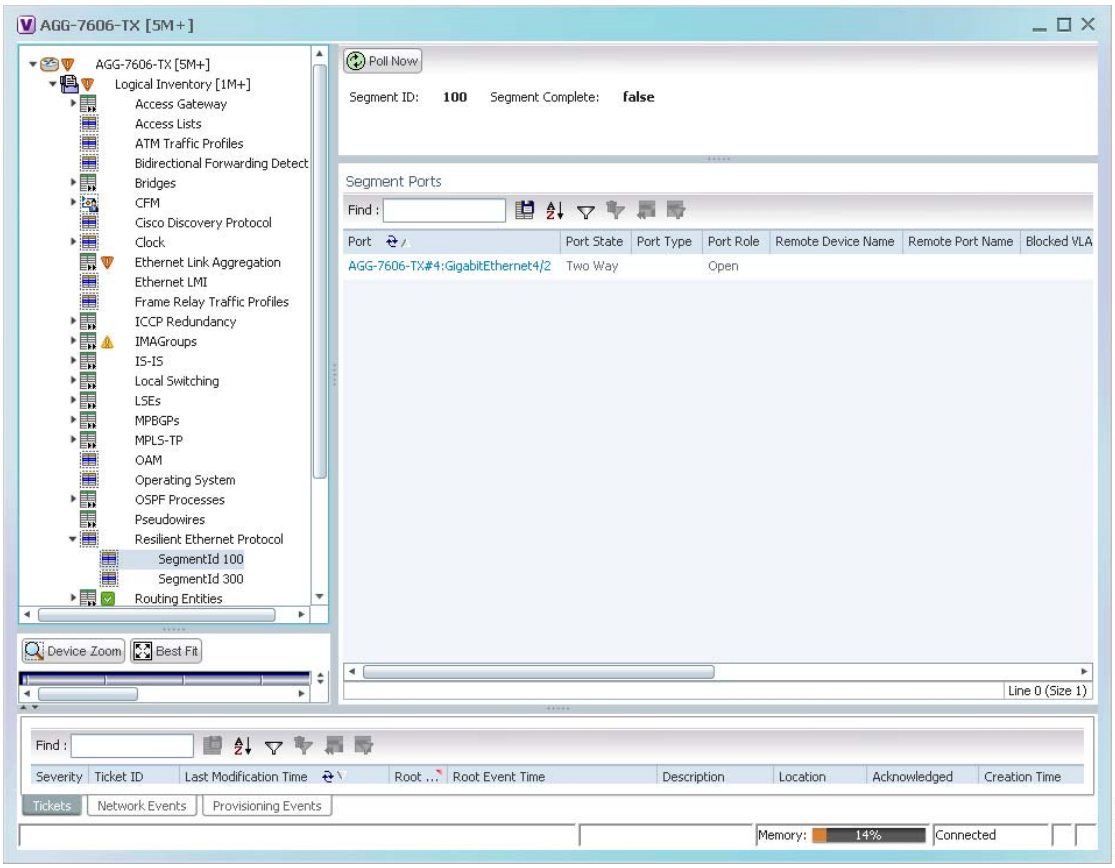



Table 13-9 describes the information that is displayed for REP segments.

*Table 13-9 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. |

*Table 13-9 REP Segment Properties (continued)*

| Field | Description |
|---|---|
| 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.<br>The value Disabled indicates that no time delay is configured, and that the preemption occurs manually.<br>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 13-62.
- VLAN service link properties—See Viewing REP Properties for VLAN Service Links, page 13-63.

# Viewing HSRP Properties

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

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

To view HSRP properties:

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

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

**Step 3** In the IP Interfaces tab, double-click the required interface to view the IP interface properties. If HSRP is configured on the IP interface, the HSRP Group tab is displayed as shown in Figure 13-6.

*Figure 13-6 HSRP Group Information*

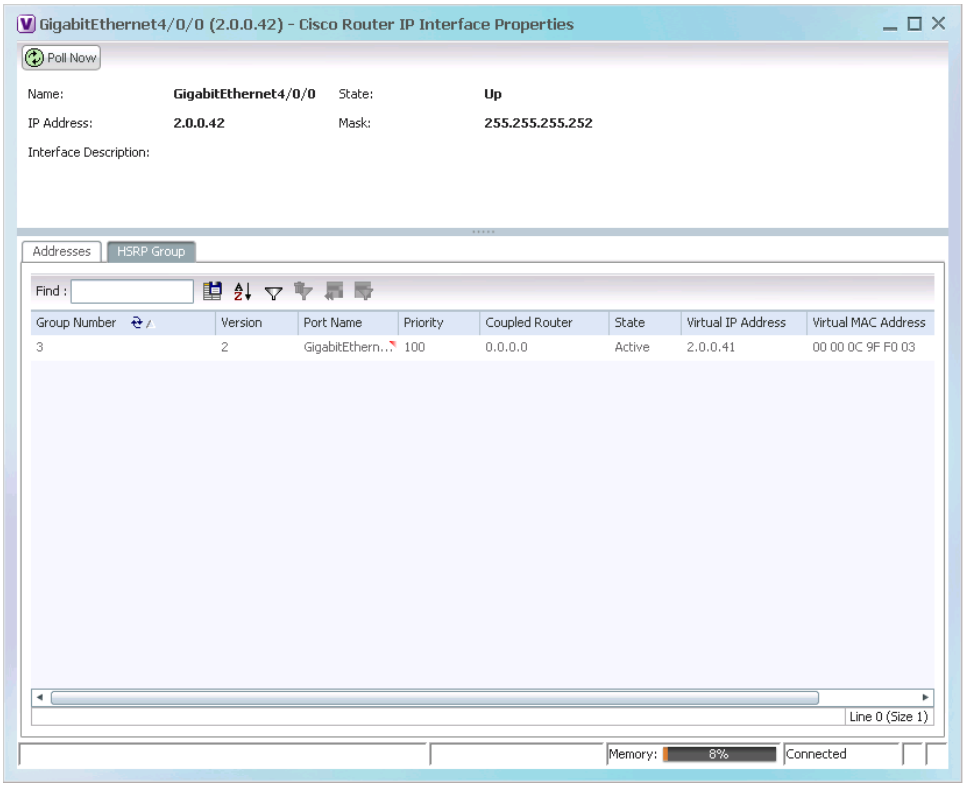



Table 13-10 describes the information in the HSRP Group tab.

*Table 13-10 HSRP Group Properties*

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

# Viewing Access Gateway Properties

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

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

To view access gateway properties:

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

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

Figure 13-7 shows an example of an access gateway entry in logical inventory.

***Figure 13-7 Access Gateway in Logical Inventory***

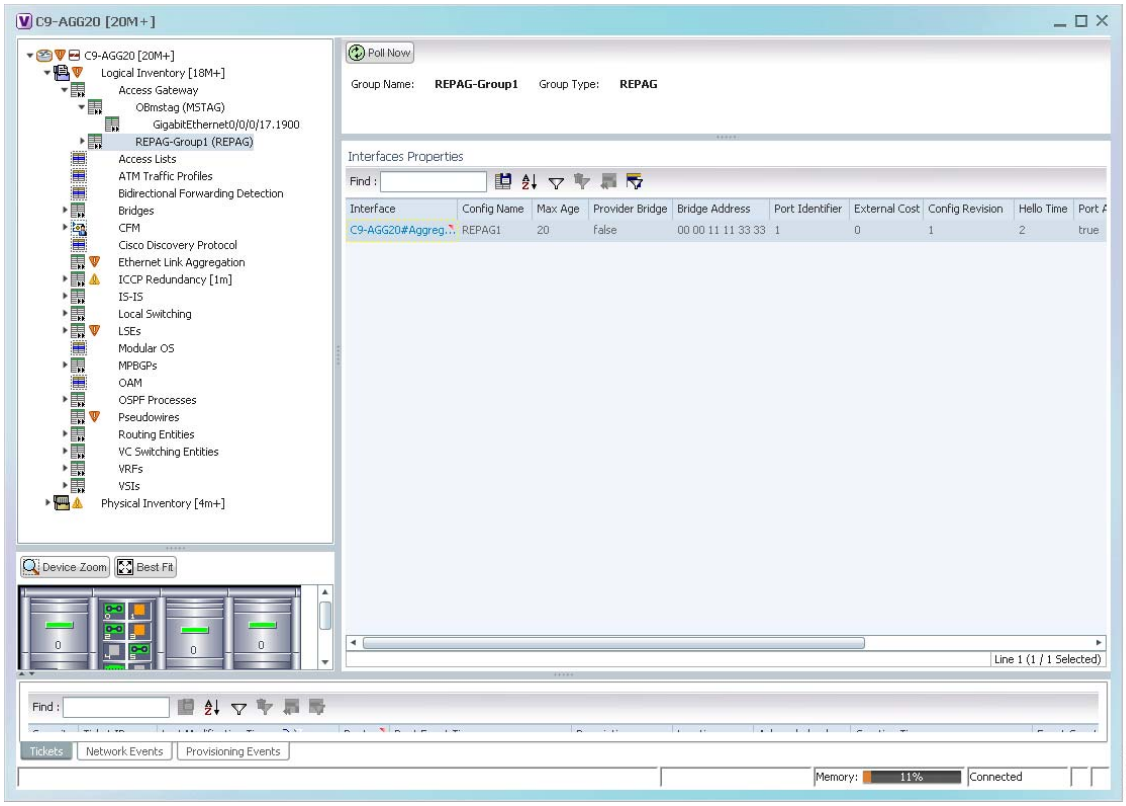


Table 13-11 describes the information that is displayed for an access gateway.

*Table 13-11 Access Gateway Properties in Logical Inventory*

| Field | Description |
|---|---|
| Group Name | Access gateway group name. |
| Group Type | Group type: MSTAG or REPAG. |
| **Interface Properties** | |
| Interface | Hyperlink to the interface in physical inventory on which access gateway is configured. |
| Config Name | Name of the MSTP region.<br>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.<br>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.<br>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 13-8 shows an example of the information displayed for an access gateway instance.

*Figure 13-8 Access Gateway Instance in Logical Inventory*

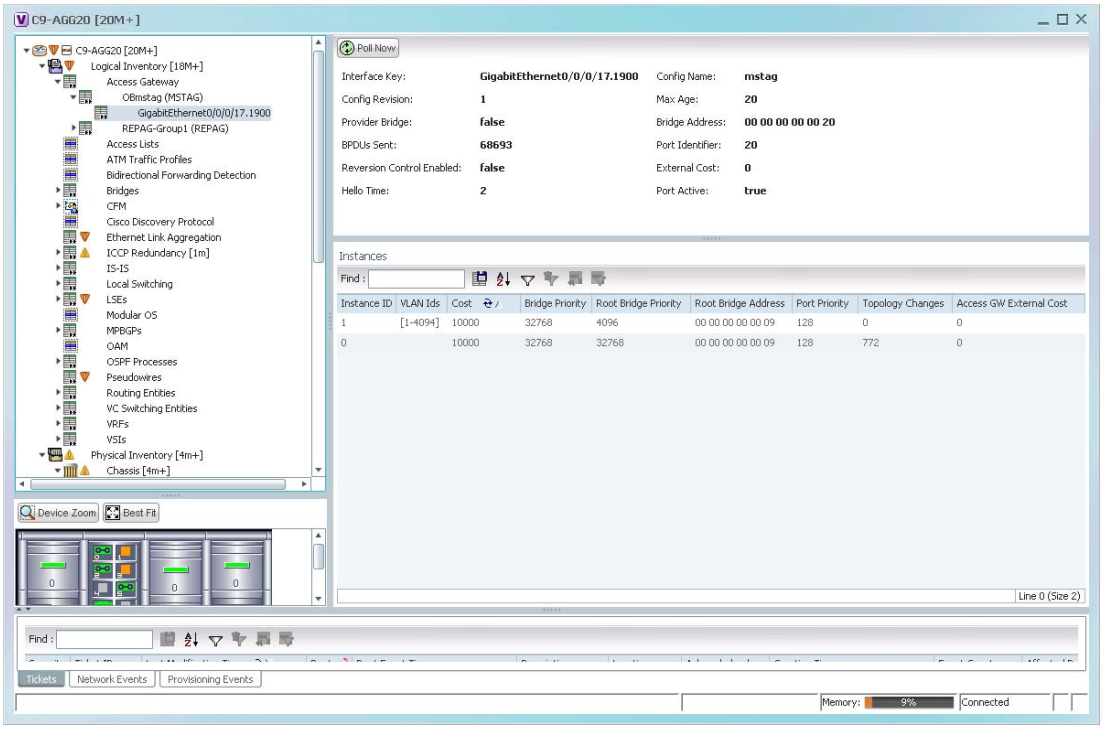



Table 13-12 describes the information that is displayed for an access gateway instance.

*Table 13-12 Access Gateway Instance Properties*

| Field | Description |
|---|---|
| Interface Key | Hyperlink to the interface in physical inventory on which access gateway is configured. |
| Config Name | Name of the MSTP region.<br>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.<br>Values range from 6 to 40 seconds. |
| Provider Bridge | Whether the current instance of the protocol is in 802.1ad mode: True or False. |
| Bridge Address | Bridge identifier for the current switch. |
| BPDUs Sent | Number of BPDUs sent. |
| Port Identifier | Port identifier for the interface. |
| Reversion Control Enabled | Whether reversion control is enabled: True or False. |
| External Cost | External path cost on the current port.<br>Values range from 1 to 200000000. |

*Table 13-12 Access Gateway Instance Properties (continued)*

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

# Working with Ethernet Link Aggregation Groups

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

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

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

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

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

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

- An aggregation service alarm is generated.

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

# Viewing Ethernet LAG Properties

**Note** Cisco CRS devices must be configured to receive SNMP traps in order to view Ethernet LAG properties. For more information on required SNMP settings, see the *Cisco Prime Network 3.10 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 13-9.

***Figure 13-9 Ethernet Link Aggregation in Logical Inventory***

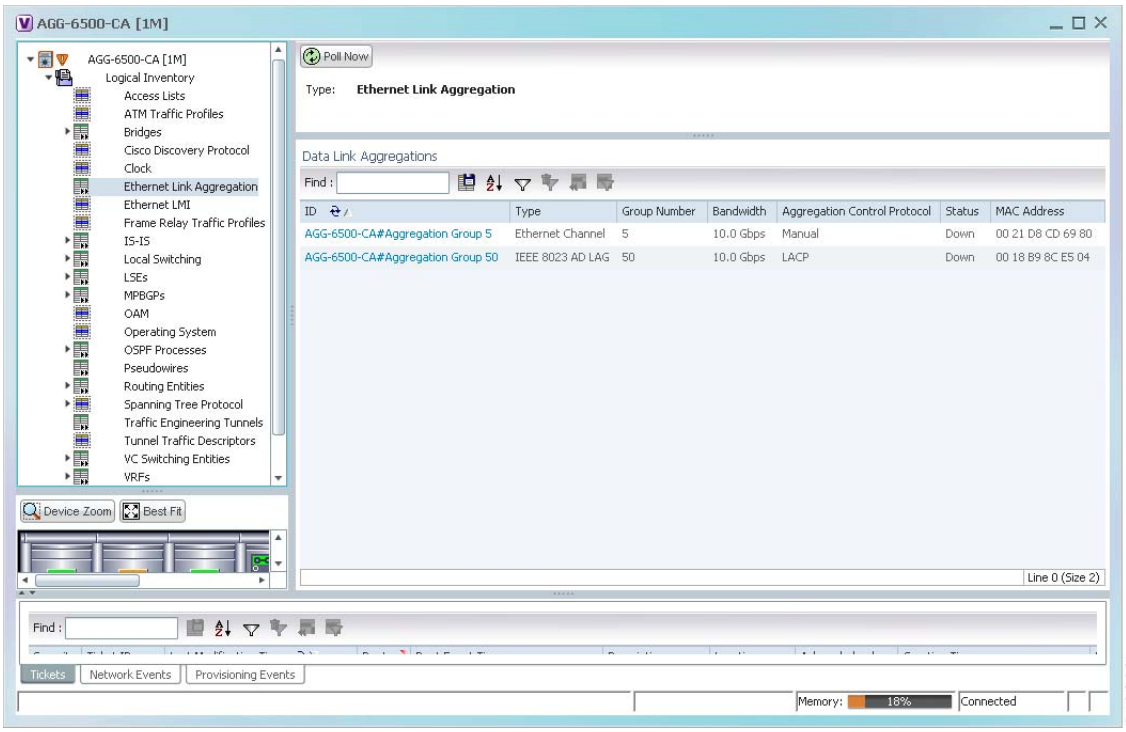



Table 13-13 describes the aggregation group properties that are displayed in the Data Link Aggregations table.

***Table 13-13 Data Link Aggregations Table***

| Field | Description |
|---|---|
| ID | Aggregation identifier. Double-click the entry to view the properties for that aggregation. |
| Type | Aggregation group type: Ethernet Channel or IEEE 8023 AD LAG. |
| Group Number | Aggregation group number. |

*Table 13-13 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 13-14.
- For IEEE 802.3 AD aggregations, see Table 13-15.

*Table 13-14 LAG Ethernet Channel Properties*

| Field | Description |
|---|---|
| Group Number | Aggregation group number. |
| Bandwidth | Aggregation bandwidth in b/s. |
| Control Protocol | Aggregation control protocol: Manual, Link Aggregation Control Protocol (LACP), or Port Aggregation Protocol (PagP). |
| MAC Address | Aggregation MAC address. |
| Administrative State | Aggregation administrative status: Up or Down. |
| Operational State | Aggregation operational status: Up or Down. |
| Adjacent | Adjacent group, hyperlinked to the group in logical inventory. |
| mLACP Properties | mLACP properties are displayed if the aggregation group is associated with an ICCP redundancy group. |
| ICCP Redundancy Group | ICCP redundancy group associated with this aggregation group, hyperlinked to the relevant entry in logical inventory. |
| mLACP Role | Role of the LAG in the redundancy group: Active or Standby. |
| mLACP Operational System MAC | MAC address used in a dual-homed environment that is selected by ICCP from one of the configured system MAC addresses for one of the points of attachment (PoAs). |
| mLACP Operational System Priority | Priority used in a dual-homed environment that is selected by ICCP from the configured system priority on one of the PoAs. |
| mLACP Failover Option | Configured mLACP failover mode: Revertive or Nonrevertive. |
| mLACP Max Bundle | Maximum number of links allowed per bundle. |

*Table 13-14 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.<br>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 13-15 LAG IEEE 802.3 AD Properties*

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

*Table 13-15 LAG IEEE 802.3 AD Properties (continued)*

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

*Table 13-15 LAG IEEE 802.3 AD Properties (continued)*

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

# Viewing mLACP Properties

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

To view mLACP properties:

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

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

In response, Prime Network Vision lists the Inter-Chassis Communication Protocol (ICCP) redundancy groups configured on the device as shown in Figure 13-10.

*Figure 13-10 ICCP Redundancy in Logical Inventory*

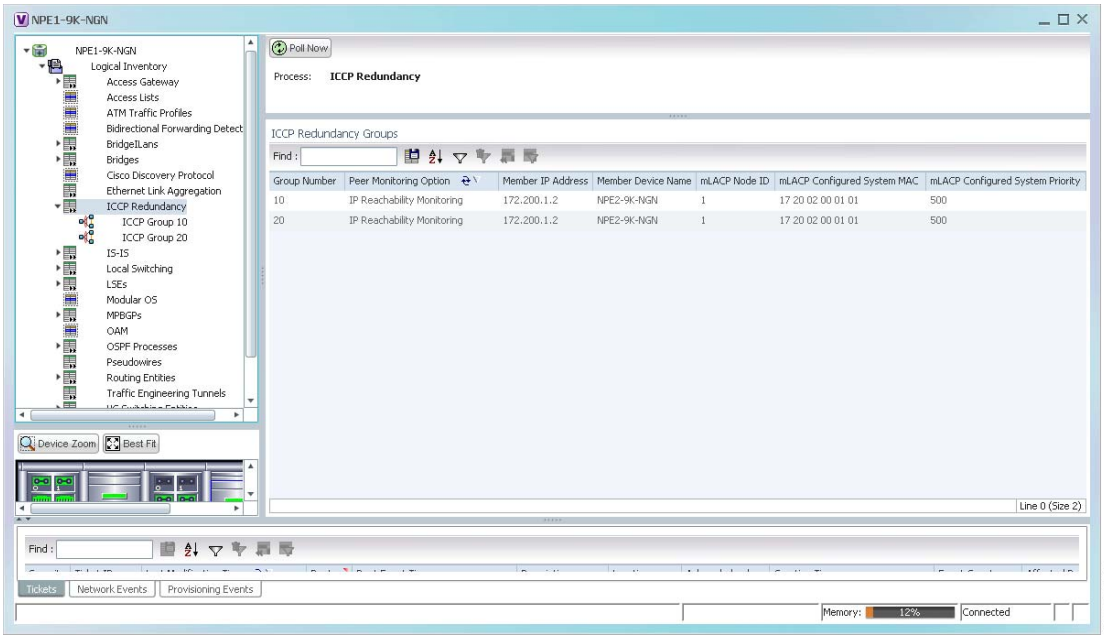


Table 13-16 describes the information displayed in the ICCP Redundancy Groups table.

*Table 13-16 ICCP Redundancy Groups in Logical Inventory*

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

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

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

The ICCP Redundancy Group Properties window is displayed with the Backbone Interfaces and Data Link Aggregations tabs as shown in Figure 13-11.

*Figure 13-11 ICCP Redundancy Group Properties Window*

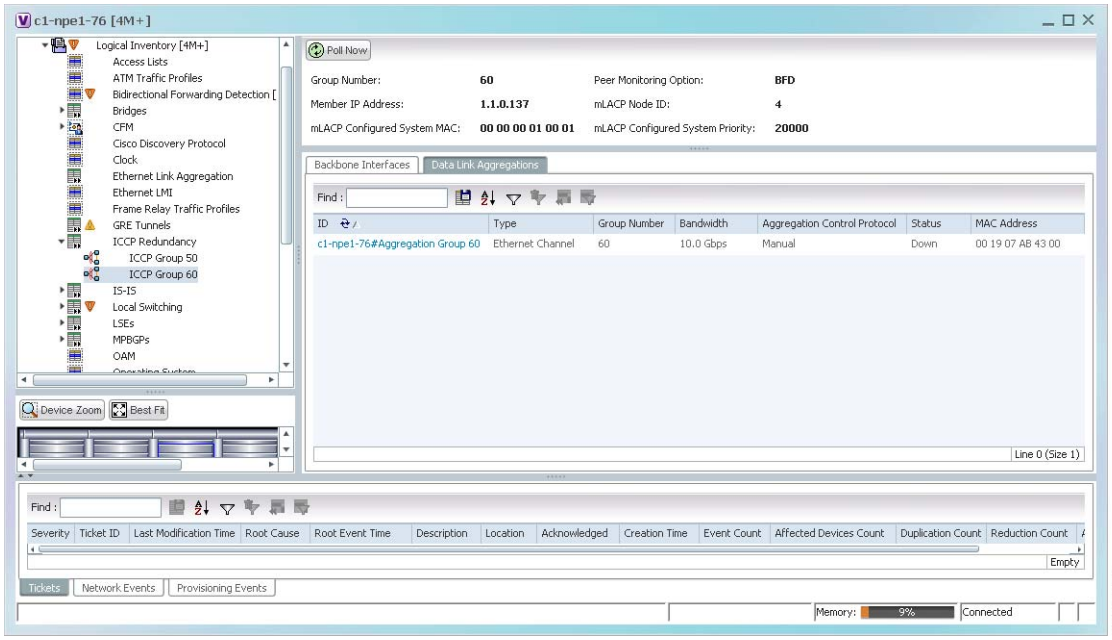


Table 13-17 describes the information available in the ICCP Redundancy Group Properties window.

*Table 13-17 ICCP Redundancy Group Properties Window*

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

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

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

- Table 13-14—LAG Ethernet Channel Properties
- Table 13-15—LAG IEEE 802.3 AD Properties

# Viewing Provider Backbone Bridge Properties

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

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

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

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

To view PBB properties:

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

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

Figure 13-12 shows an example of PBB properties in logical inventory.

***Figure 13-12 PBB Properties in Logical Inventory***

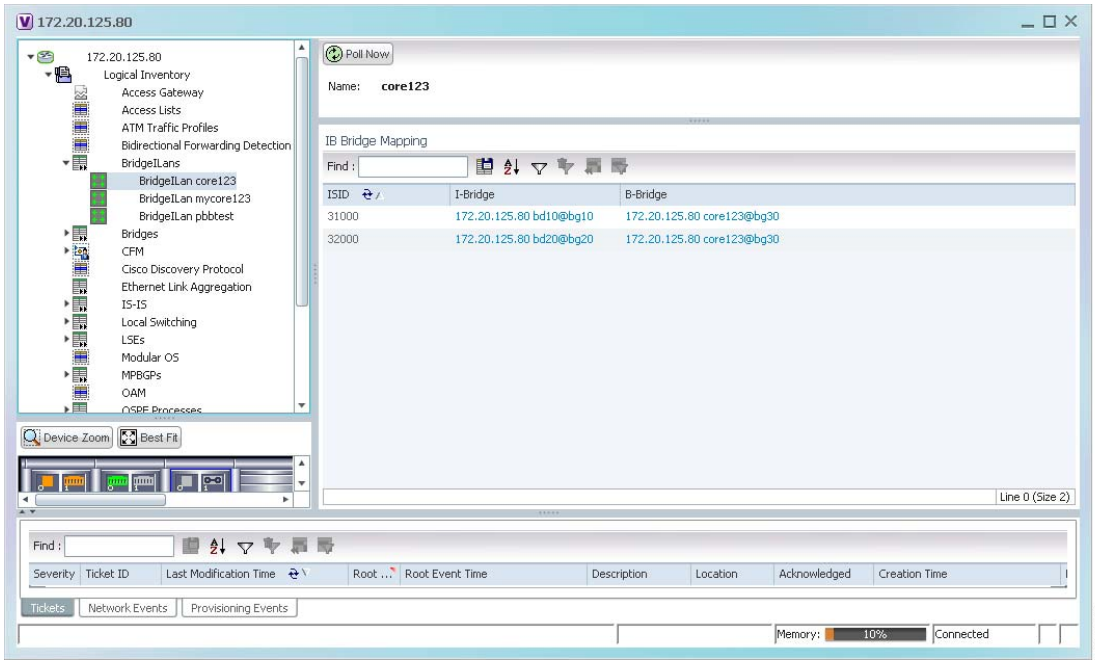


Table 13-18 describes the information displayed for PBB.

*Table 13-18 PBB Properties in Logical Inventory*

| Field | Description |
|---|---|
| Name | Identifier of the bridge as follows:<br>• For Cisco 7600 devices, the identifier of the MAC tunnel created.<br>• 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 13-13 shows an example of the EFP Properties window.

***Figure 13-13 EFP Properties Window***

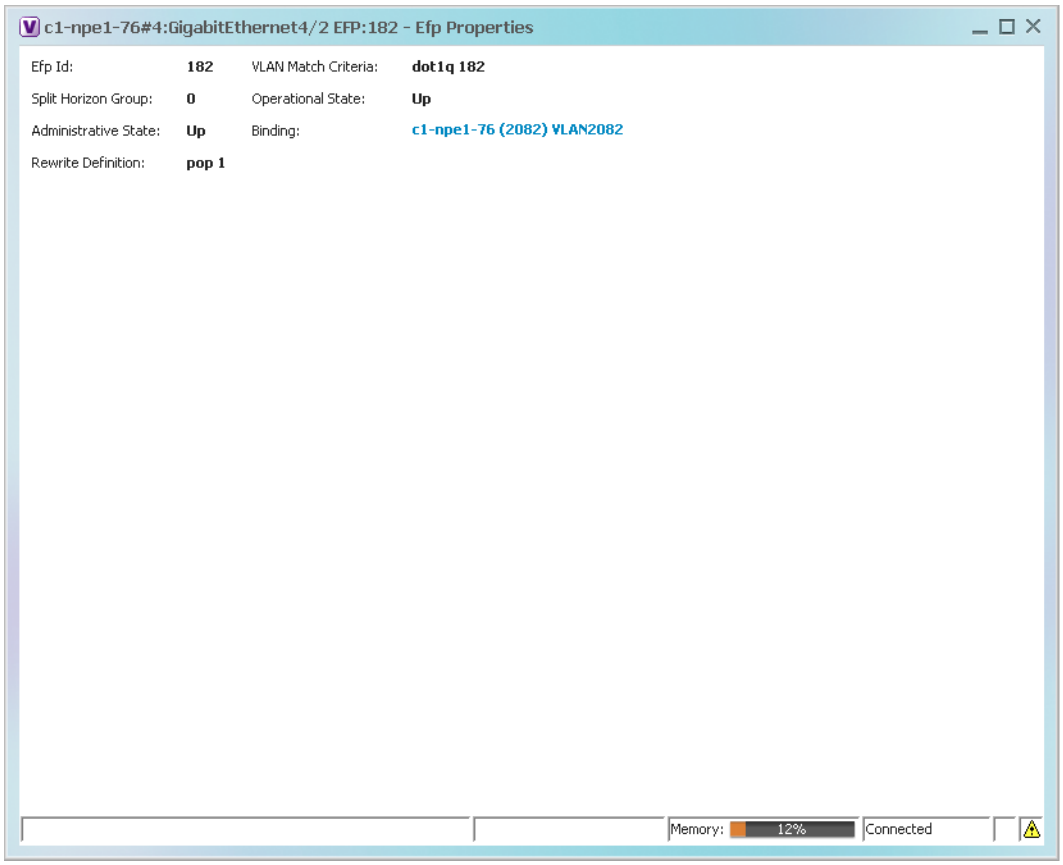



Table 13-19 describes the information displayed in the EFP Properties window.

***Table 13-19 EFP Properties Window***

| Field | Description |
|---|---|
| EFP ID | Identifier for the EFP. |
| VLAN Match Criteria | Match criteria configured on the EFP for forwarding decisions. |
| Split Horizon Group | Split horizon group to which the EFP is associated.<br>If no split horizon group is defined, the value is null.<br>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 13-14.

***Figure 13-14 Bridge Associated with EFP in Logical Inventory***

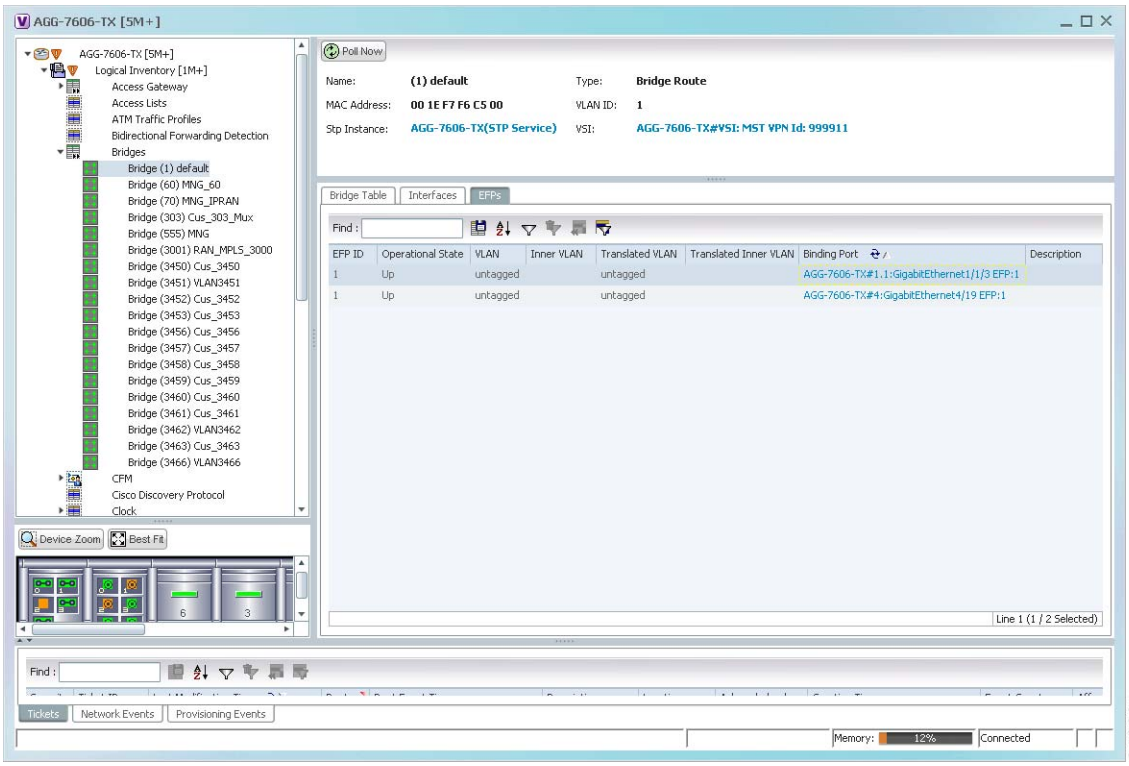



Table 13-20 describes the information displayed for an EFP associated with a bridge.

***Table 13-20 EFP Associated with a Bridge in Logical Inventory***

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

*Table 13-20 EFP Associated with a Bridge in Logical Inventory (continued)*

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

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

- In the bridge entry in logical inventory, click the hyperlinked entry in the Binding field.
- Use the procedure described in Viewing and Renaming Ethernet Flow Domains, page 13-41 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 13-15.

*Figure 13-15 EFPs Tab in Physical Inventory*

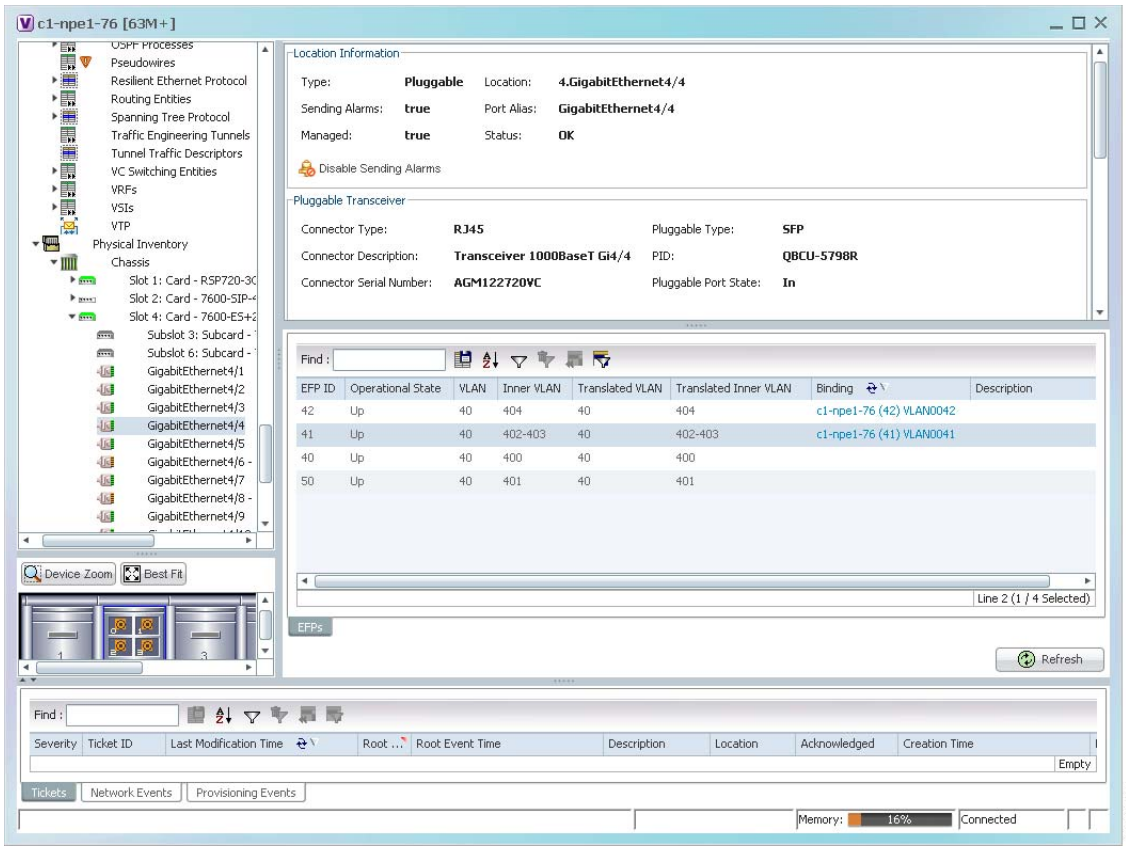



Table 13-21 describes the information displayed in the EFPs tab.

*Table 13-21 EFPs Tab*

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

# Connecting a Network Element to an EFP

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

To connect network elements to an EFP:

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

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

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

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

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

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

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

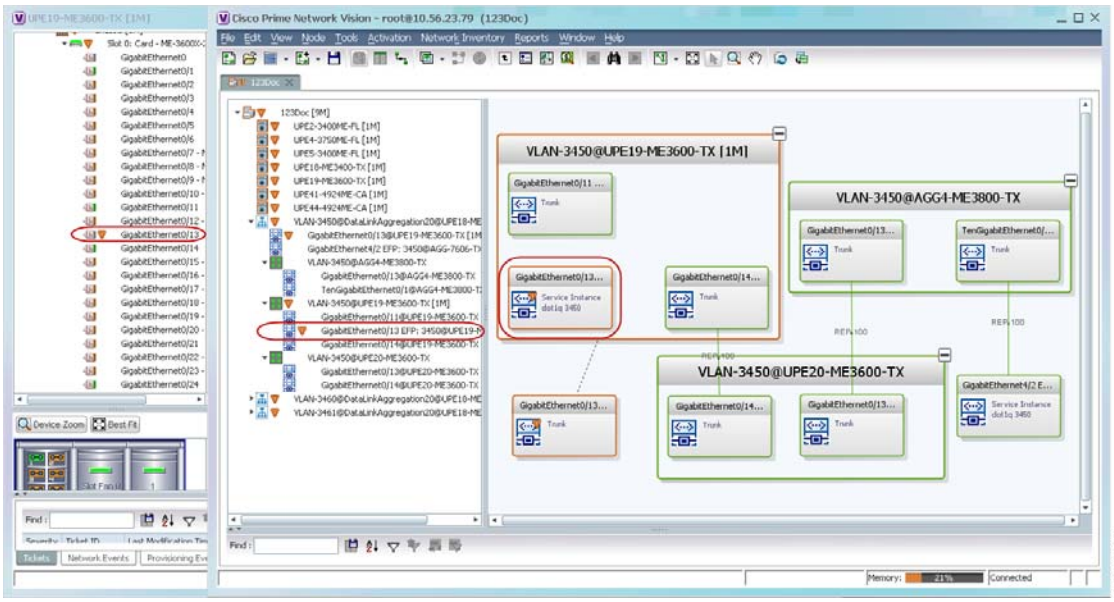
# Understanding EFP Severity and Ticket Badges

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

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

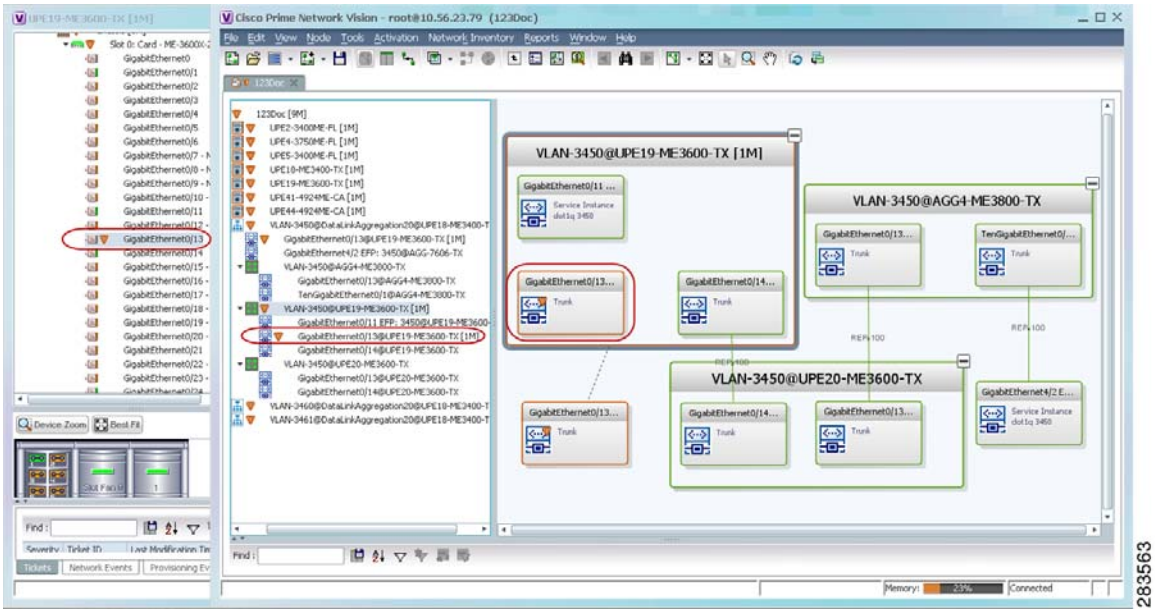
  Figure 13-16 shows an example of a ticket badge based on a service instance.

*Figure 13-16 EFP Severity and Ticket Badges Based on Underlying Service Instance*




- If the Ethernet flow point element represents a VLAN interface for a regular switch port, the severity and ticket badges are based on the corresponding port, as shown in Figure 13-17.

*Figure 13-17 EFP Severity and Ticket Badges Based on Corresponding Port*



# Viewing EVC Service Properties

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

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

### Shared Switching Entities and EVC Service View

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

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

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

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

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

Figure 13-18 shows an example of a port in physical inventory configured with these EVC properties.

*Figure 13-18 EVC Port Properties in Physical Inventory*

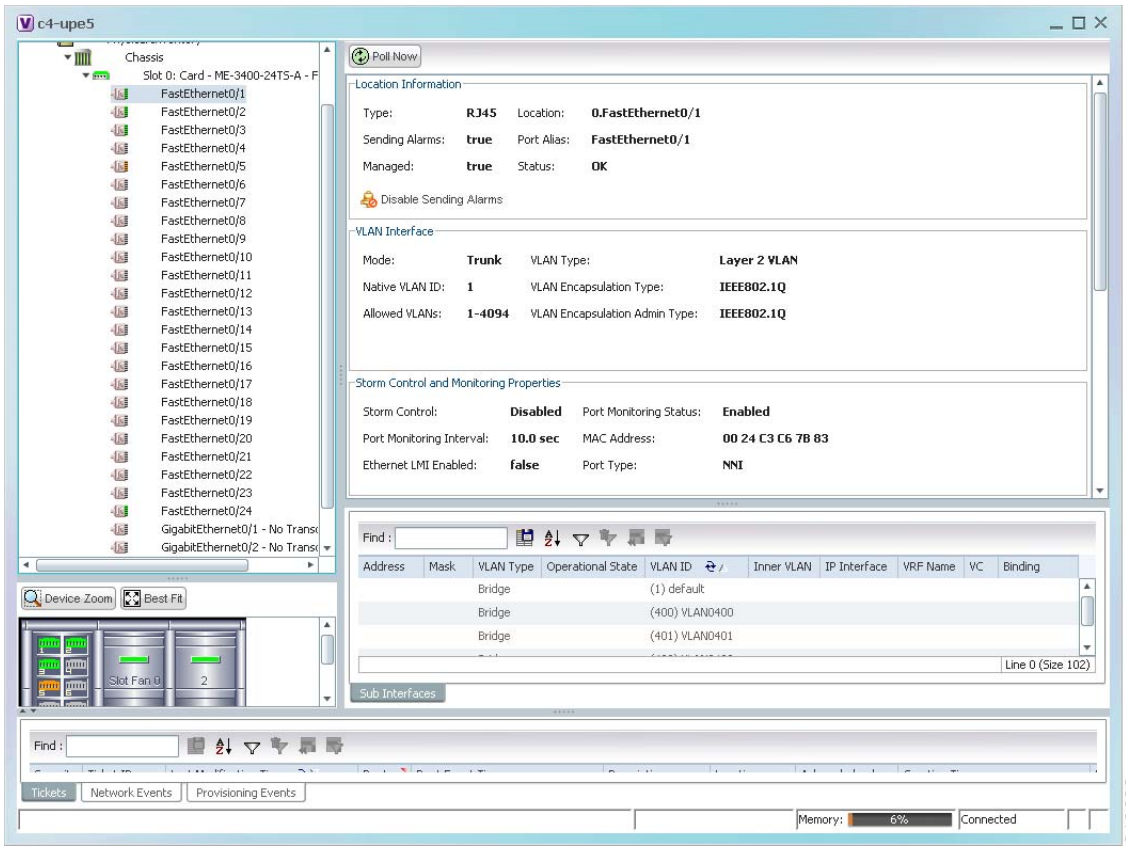



Table 13-22 describes the information displayed for these properties.

*Table 13-22 EVC Port Properties in Physical Inventory*

| Field | Description |
|---|---|
| **Storm Control and Monitoring Properties Area** | |
| Storm Control | Status of storm control on the port: Enabled or Disabled. |
| Port Monitoring Status | Status of port monitoring:<br>• 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).<br>• 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 13-22 EVC Port Properties in Physical Inventory (continued)*

| Field | Description |
|---|---|
| **Security Properties Areas** | |
| Port Security | Status of security on the port: Enabled or Disabled. |
| MAC Address Limit | Maximum number of MAC addresses allowed on the interface. |
| Aging Type | Type of aging used for automatically learned addresses on a secure port:<br>• 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.<br>• 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:<br>• Protect—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value<br>• 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.<br>• 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.

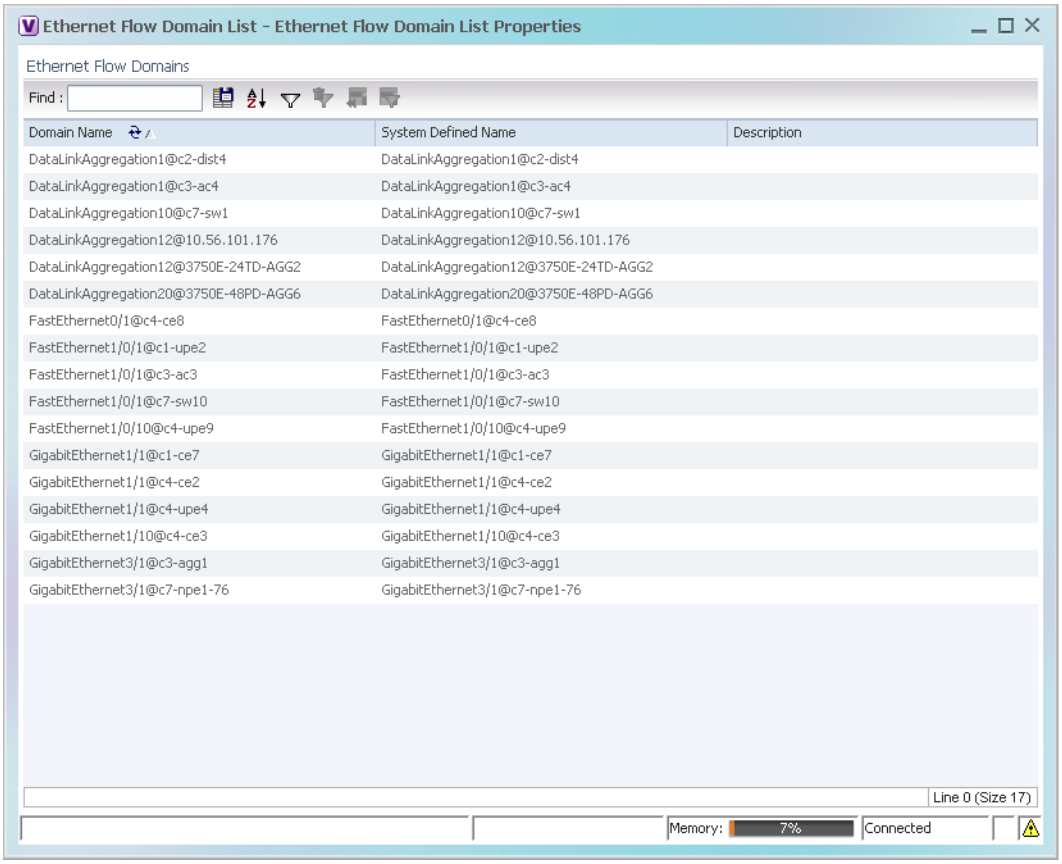
An Ethernet flow domain can have no N-PEs (flat VLAN) or one or more N-PEs (N-PE redundancy configuration). The Ethernet flow domain is defined using physical connectivity at the port level, and not at the network element level. STP is used to mark the root bridge, root or blocked ports, and blocked 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 13-19.

***Figure 13-19 Ethernet Flow Domain List Properties Window***




**Step 2** To rename an Ethernet flow domain:

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

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

c. Click **OK**.

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

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

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

The Ethernet Flow Domain Properties window is displayed as shown in Figure 13-20.

*Figure 13-20 Ethernet Flow Domain Properties Window*

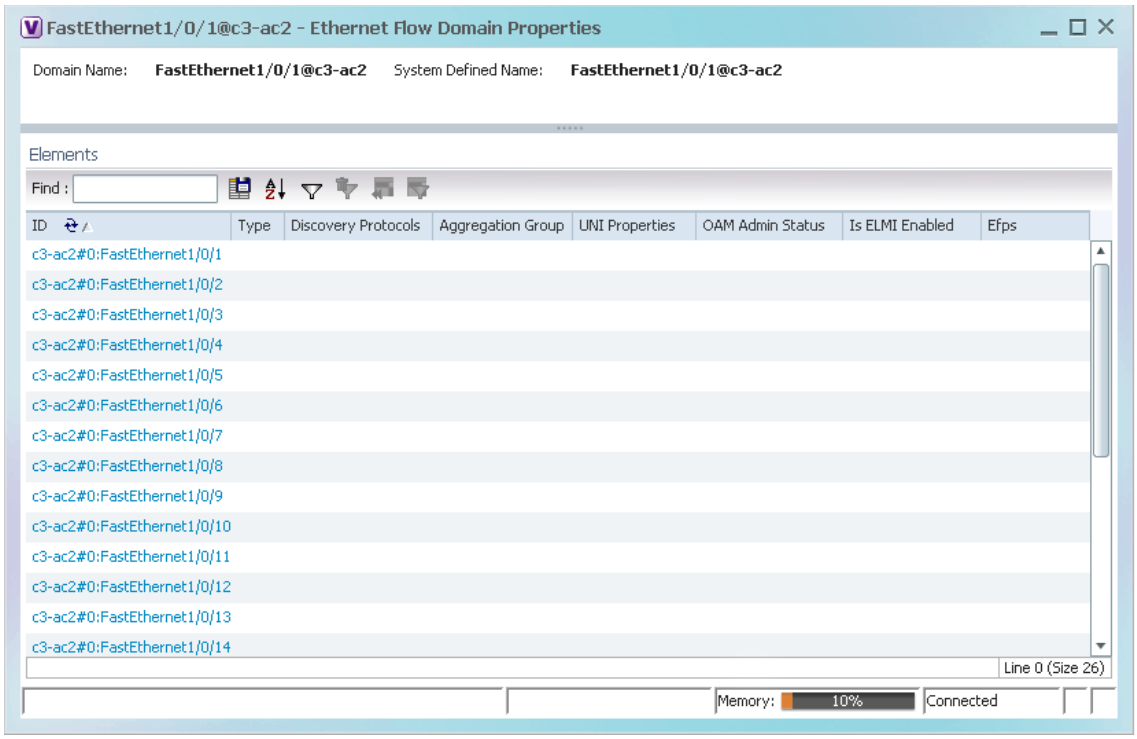



Table 13-23 describes the information displayed in the Ethernet Flow Domain Properties window.

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

*Table 13-23 Ethernet Flow Domain Properties Window*

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

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

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

# Working with VLANs and VLAN Overlays

The following topics provide information and procedures for working with VLANs and VLAN overlays:


- Understanding VLAN and EFD Discovery, page 13-44
- Understanding VLAN Elements, page 13-45
- Switching Entities Containing Termination Points, page 13-49
- Adding VLANs to a Map, page 13-49
- Removing VLANs from a Map, page 13-52
- Viewing VLAN Mappings, page 13-52
- Working with Associated VLANs, page 13-54
- Viewing VLAN Links Between VLAN Elements and Devices, page 13-57
- Applying VLAN Overlays, page 13-60
- Displaying or Hiding VLAN Overlays, page 13-61
- Removing a VLAN Overlay, page 13-61
- Viewing VLAN Service Link Properties, page 13-62
- Viewing REP Information in VLAN Domain Views and VLAN Overlays, page 13-62
- Viewing REP Properties for VLAN Service Links, page 13-63
- Viewing STP Information in VLAN Domain Views and VLAN Overlays, page 13-65
- Viewing STP Properties for VLAN Service Links, page 13-66
- Viewing VLAN Trunk Group Properties, page 13-67
- Viewing VLAN Bridge Properties, page 13-69


## 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 13-45
- VLANs, page 13-45
- Switching Entities, page 13-45
- Ethernet Flow Points, page 13-46


## VLAN Elements in Prime Network Vision

Table 13-24 describes the icons that Prime Network Vision uses to represent VLAN elements.

*Table 13-24 VLAN Elements and Icons in Prime Network Vision*

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

## VLANs

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

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

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

## Switching Entities

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

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

A switching entity typically contains EFP elements.

## Ethernet Flow Points

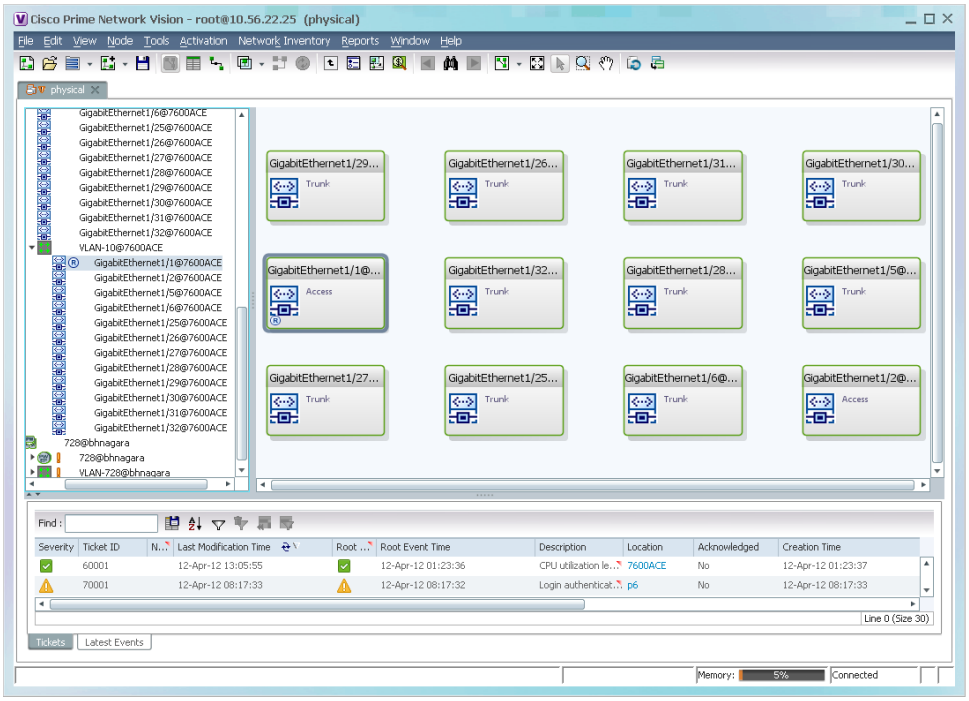
An Ethernet flow point (EFP) can represent a port that is configured for participation in a specific VLAN.

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

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

Figure 13-21 shows an example of EFPs configured as switch ports in Prime Network Vision.

***Figure 13-21 EFPs Configured as Switch Ports***

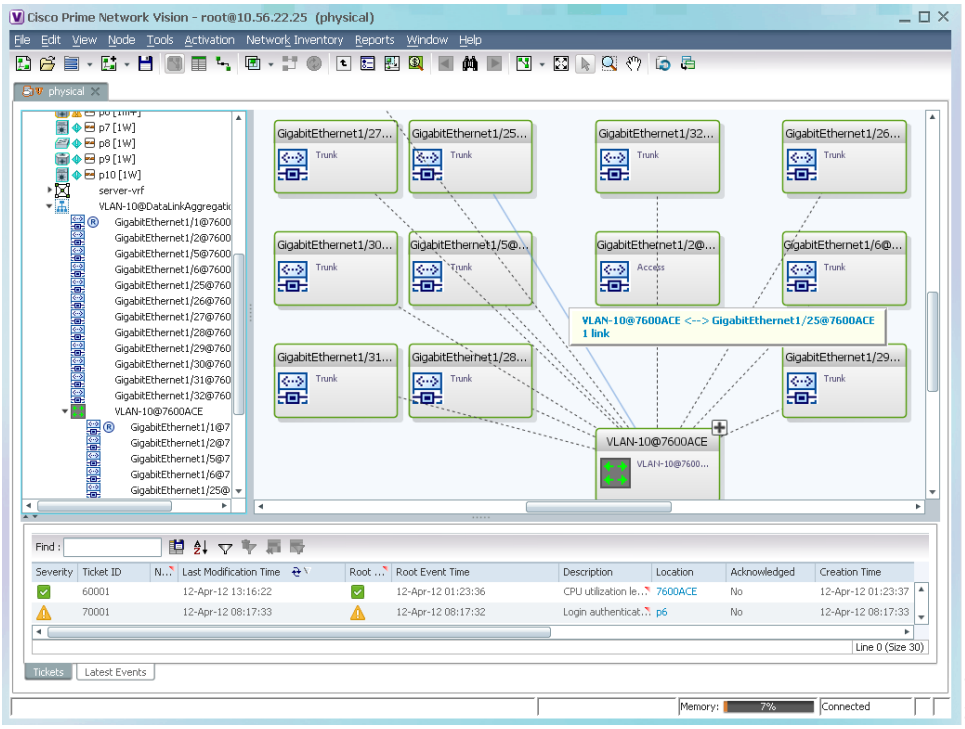



EFPs that are located directly inside a VLAN represent one of the following:

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

  These EFPs are typically connected to a switching entity inside the VLAN by a VLAN link, as shown in Figure 13-22.

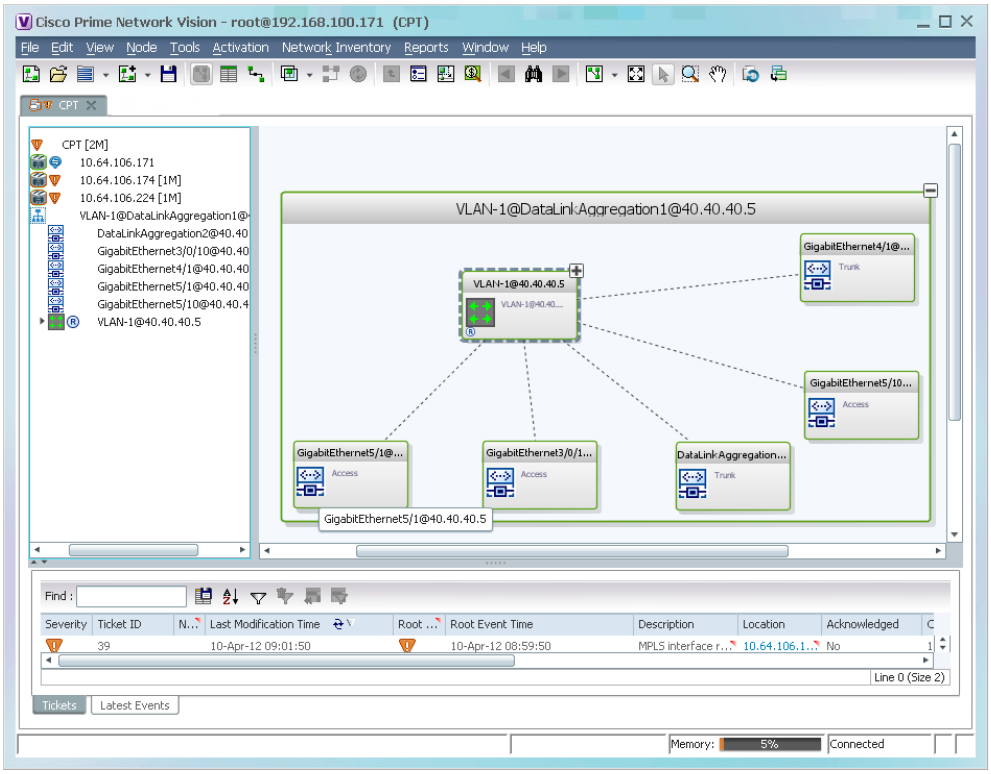
*Figure 13-22 Termination Point EFP Inside a VLAN*




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

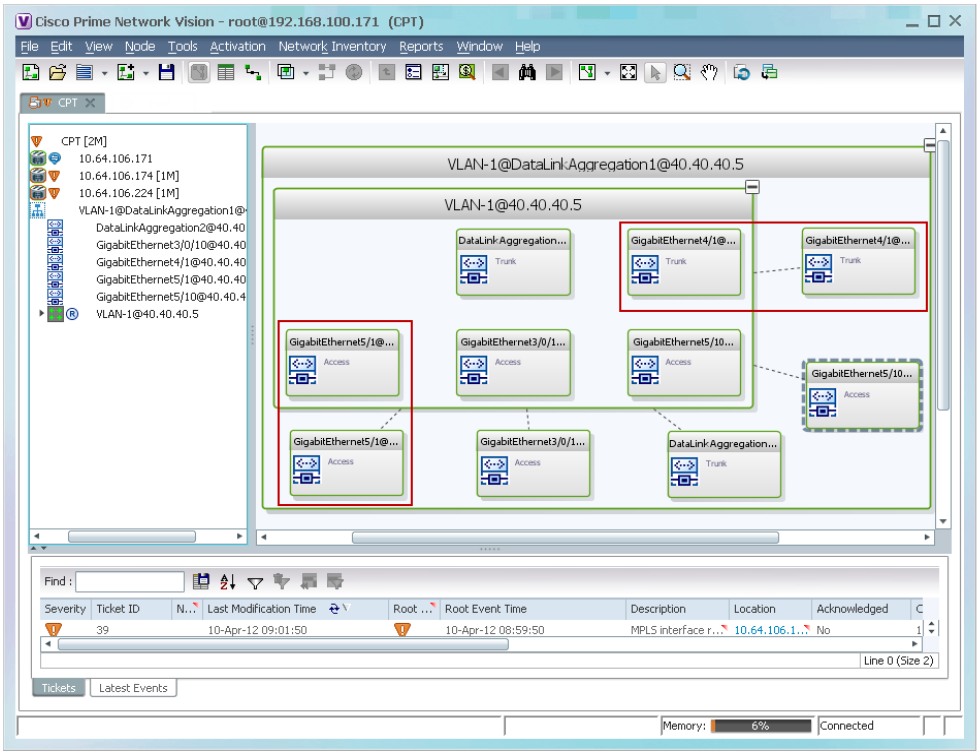
In Prime Network Vision, edge EFPs are displayed directly under the VLAN at the same level as their switching entities and are connected to their corresponding switching entities by a dotted link, as shown in Figure 13-23.

***Figure 13-23 Edge EFP Inside a VLAN***



An edge EFP can be displayed both inside and outside of its switching entity, as shown (highlighted with a red outline) in Figure 13-24:

***Figure 13-24 Edge EFPs Displayed Inside and Outside of Switching Entities***




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

# Switching Entities Containing Termination Points

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

# Adding 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.

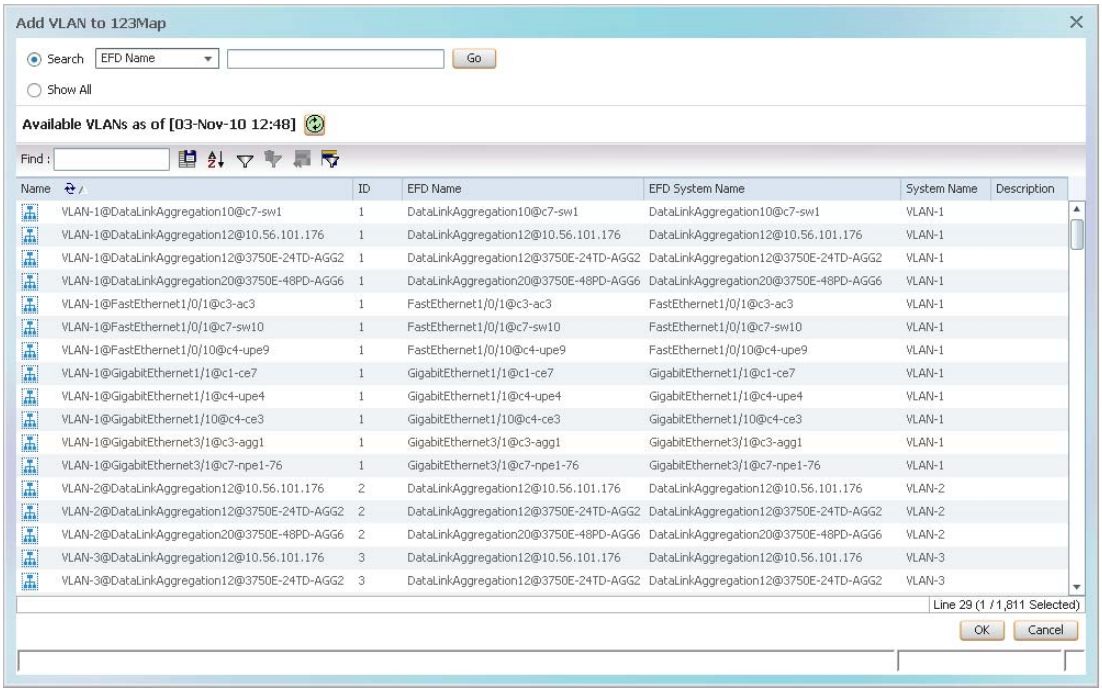
**Note** Adding VLANs affects other users if they are working with the same map.

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 13-25.

***Figure 13-25 Add VLAN Dialog Box***




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

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

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

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

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

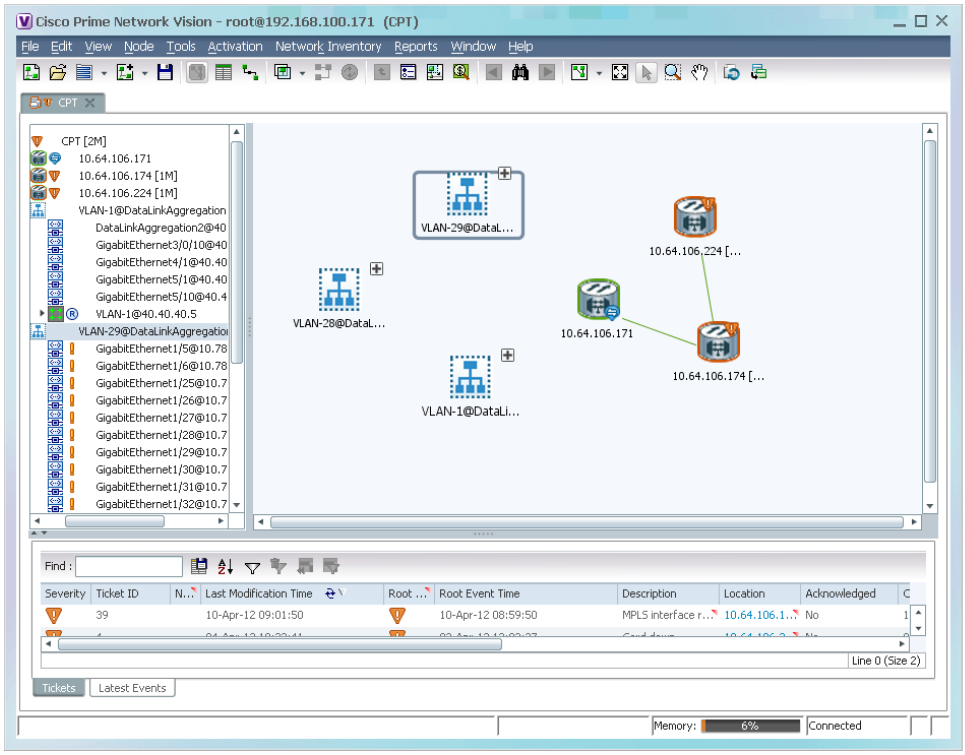
**Tip** Press **Shift** or **Ctrl** to choose multiple adjoining or nonconsecutive VLANs.

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

The VLANs are displayed in the Prime Network Vision content pane as shown in Figure 13-26.

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

*Figure 13-26 VLANs in Map View*




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

- Viewing and Renaming Ethernet Flow Domains, page 13-41
- Viewing EFP Properties, page 13-32

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 13-14
- Viewing REP Information in VLAN Domain Views and VLAN Overlays, page 13-62
- Viewing REP Properties for VLAN Service Links, page 13-63

For STP, see:

- Viewing Spanning Tree Protocol Properties, page 13-10
- Viewing STP Information in VLAN Domain Views and VLAN Overlays, page 13-65
- Viewing STP Properties for VLAN Service Links, page 13-66

# 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 13-27.

*Figure 13-27 VLAN Mappings Tab in Physical Inventory*

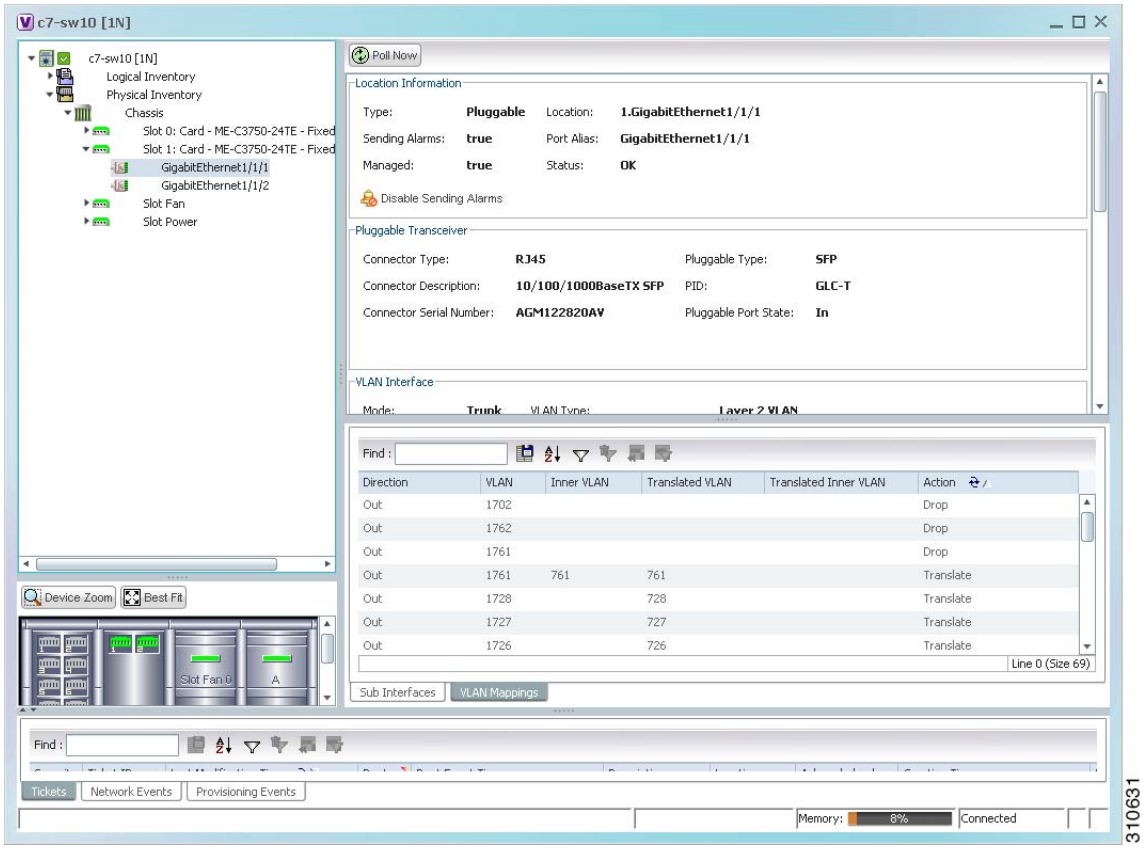



Table 13-25 describes the information that is displayed in the VLAN Mappings table.

*Table 13-25 VLAN Mappings Table*

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

# Working with Associated VLANs

Prime Network Vision discovers associations between network VLANs and displays the information in Prime Network Vision. Network VLAN associations are represented by VLAN service links, and can be any of the tag manipulation types described in Table 13-26.

*Table 13-26 Types of Tag Manipulations in VLAN Associations*

| VLAN Tag Manipulation | Description | Example |
|---|---|---|
| One-to-one | One VLAN tag is translated to another VLAN tag. | VLAN tag 100 > VLAN tag 200 |
| Two-to-two | • Two VLAN tags exist and both are translated to other tags.<br>• 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<br>• 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 13-54.
- View properties for associated VLANs—See Viewing Associated Network VLAN Service Links and VLAN Mapping Properties, page 13-56.

## Adding an Associated VLAN

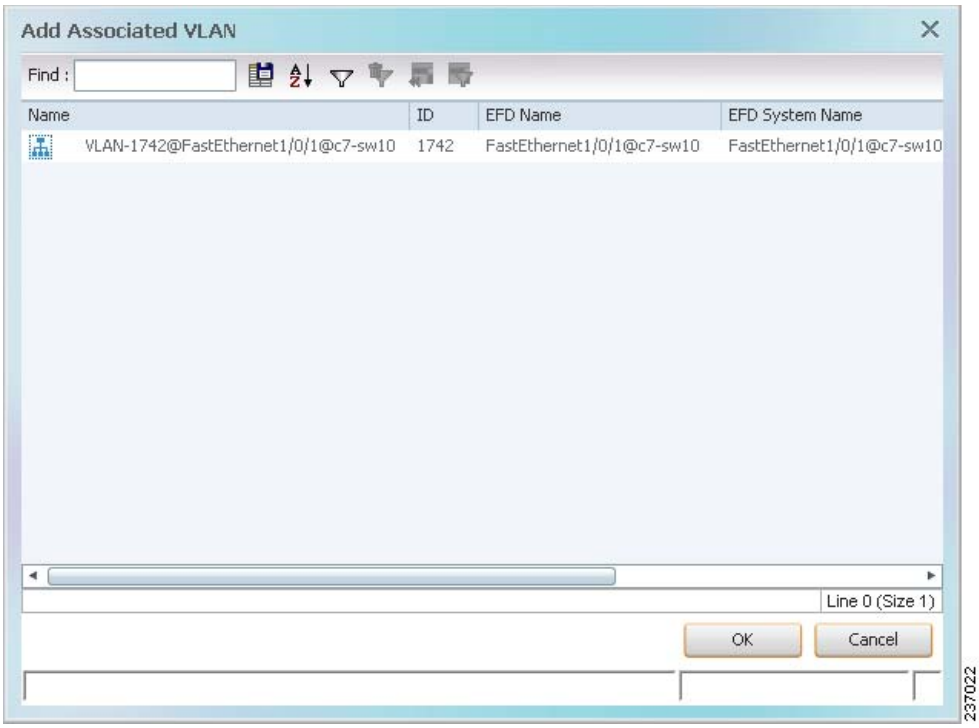
To add an associated VLAN to an existing VLAN in a map:

**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 13-28.

*Figure 13-28 Add Associated VLAN Window*




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

Table 13-27 describes the information displayed in the Add Associated VLAN table.

*Table 13-27 Add Associated VLAN Table*

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

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

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

# Viewing Associated Network VLAN Service Links and VLAN Mapping Properties

After you add an associated network VLAN, you can:

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

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

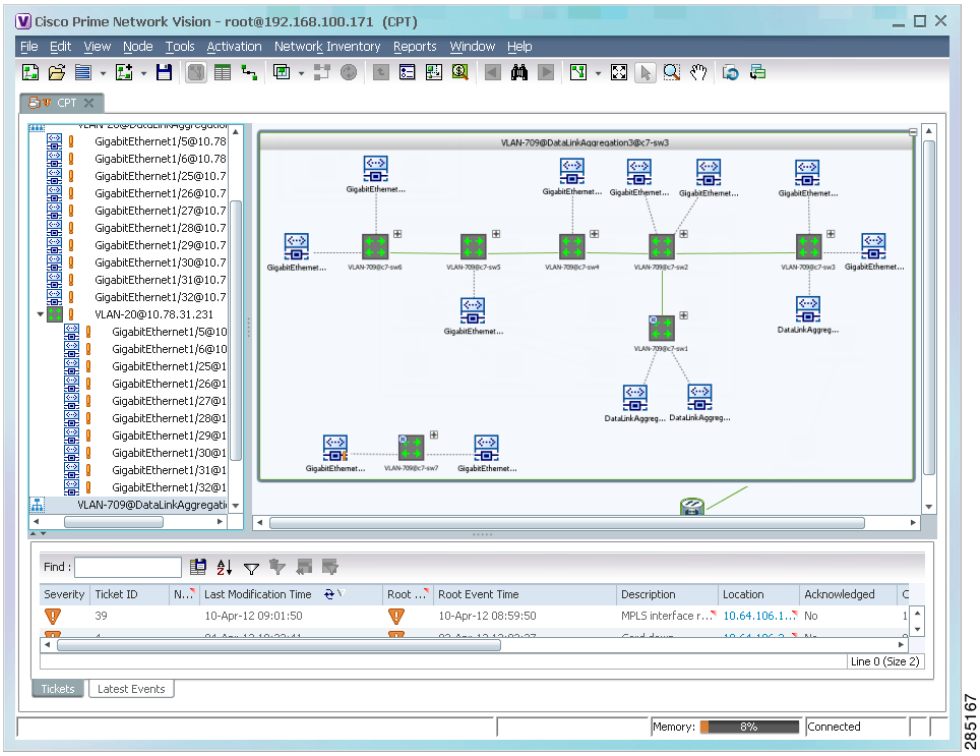
**Step 1** Select the required network VLAN in the map view.

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

Figure 13-29 shows an example of a network VLAN in a thumbnail.

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

***Figure 13-29 VLAN Service Links Between Associated Network VLANs***

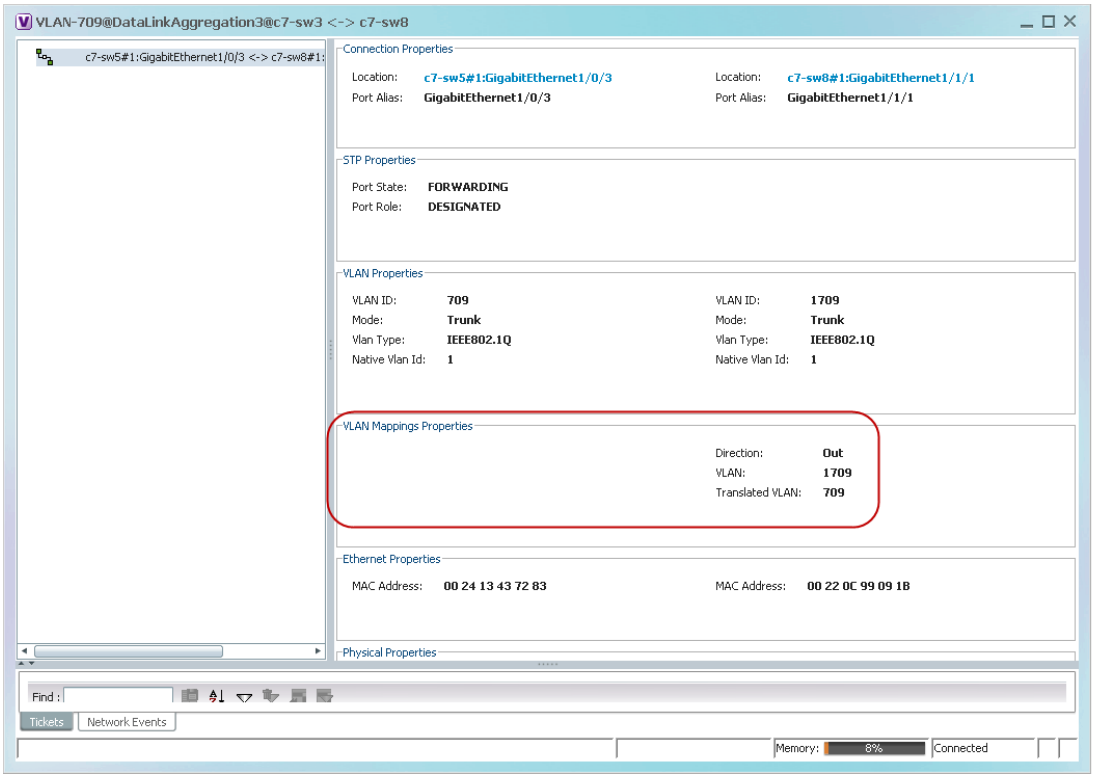



**Step 3** To view additional information, right-click a link, and choose **Properties**.

The Link Properties window is displayed as shown in Figure 13-30.

If VLAN tag manipulation is configured on the link, the VLAN Mapping Properties area in the Link Properties window displays the relevant information. For example, in Figure 13-30, the VLAN Mapping Properties area shows that a one-to-one VLAN mapping for VLAN tag 1709 to VLAN tag 709 is configured on GigabitEthernet1/1/1 on c7-sw8 on the egress direction.

***Figure 13-30 VLAN Mapping Properties in Link Properties Window***




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

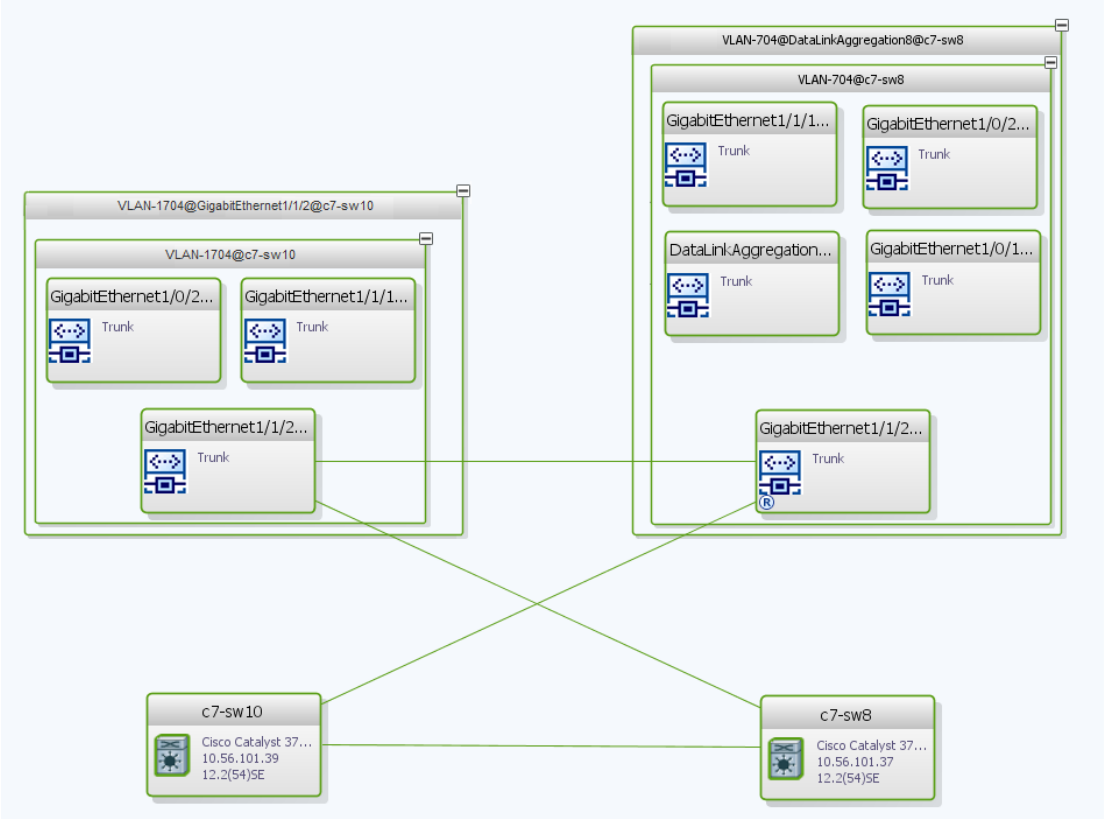
- Viewing REP Properties for VLAN Service Links, page 13-63
- Viewing STP Properties for VLAN Service Links, page 13-66

# 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 13-31 and described in the following paragraphs.

*Figure 13-31 VLAN Elements and Devices in Prime Network Vision*



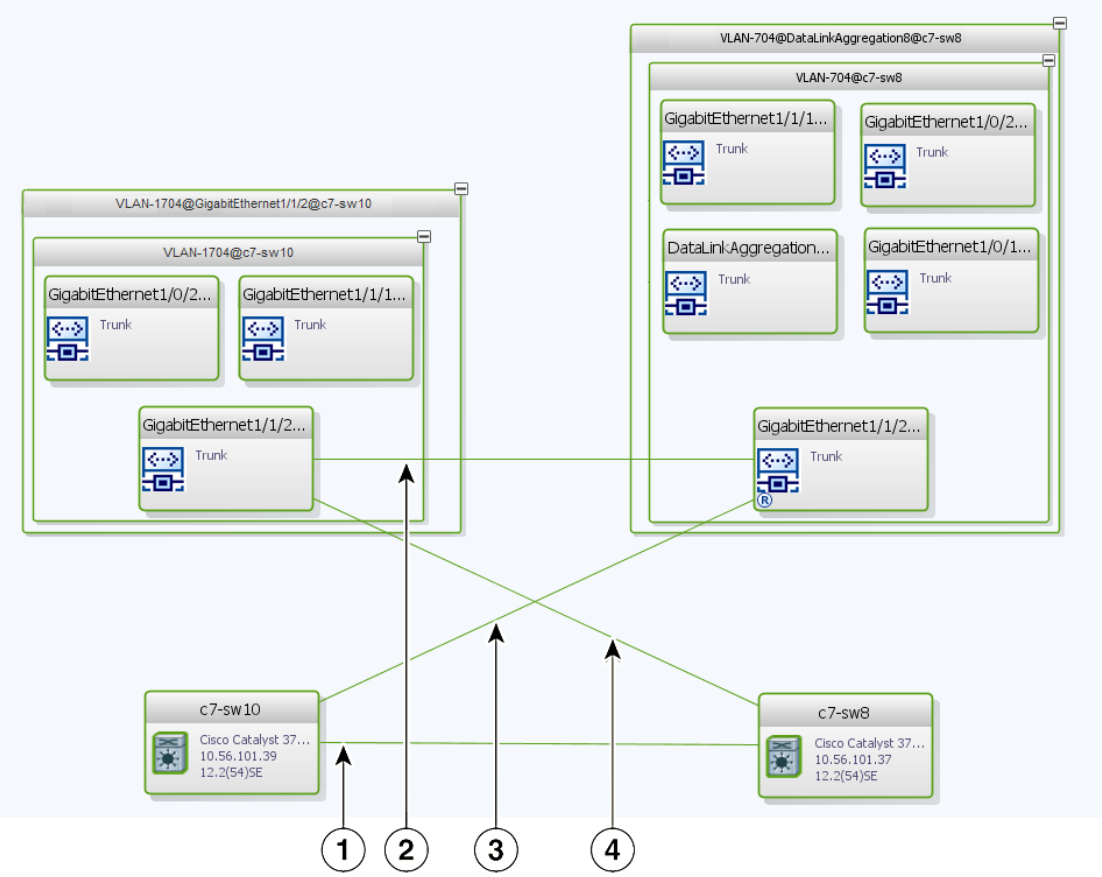

The elements are configured as follows:

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

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

The four links in the map are identified in Figure 13-32 and described in the following table.

*Figure 13-32 Links Between VLAN Elements and Devices*




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

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

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

# 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.

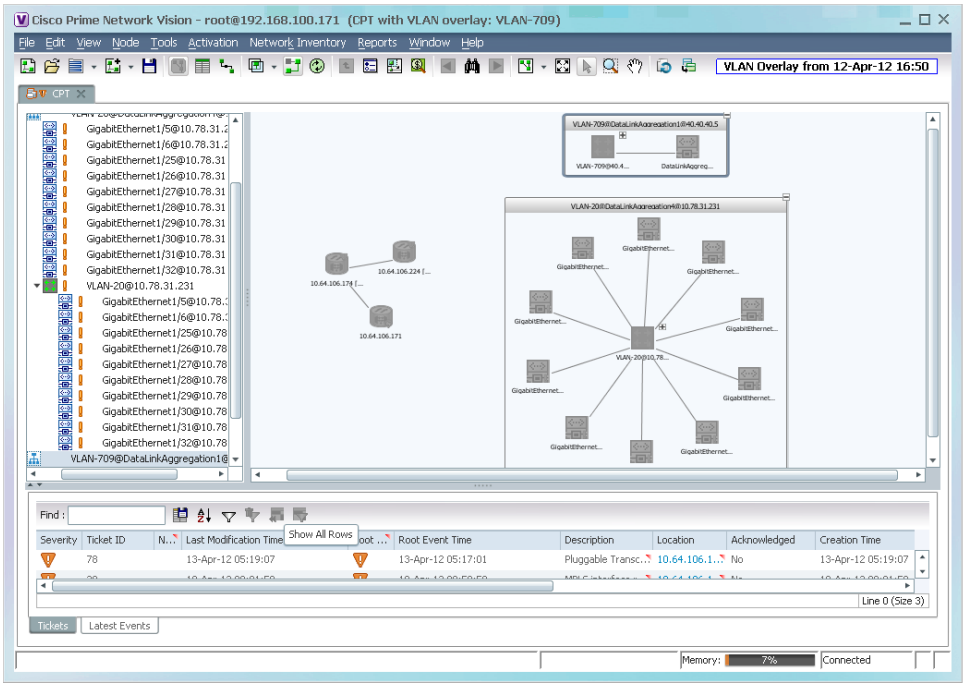
  The search condition is “contains.” Search strings are case-insensitive. For example, if you choose the Name category and enter “net,” Prime Network Vision displays overlays that have “net” in their names. The string “net” can be at the beginning, middle, or end of the name, such as Ethernet.

- 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 13-33.

*Figure 13-33 VLAN Overlay Example*




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

# 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 13-63
- Viewing STP Properties for VLAN Service Links, page 13-66
- Viewing Associated Network VLAN Service Links and VLAN Mapping Properties, page 13-56

# 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 13-28 describes the icons and badges used to represent REP segment and port information.

***Table 13-28 REP Icons and Badges in VLAN Domain Views and Overlays***

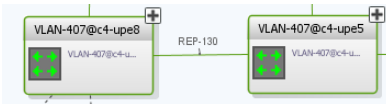
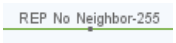
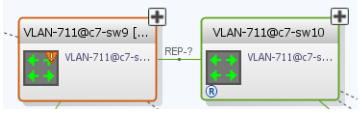
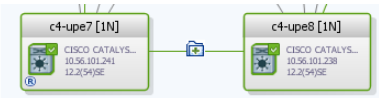
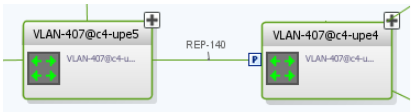
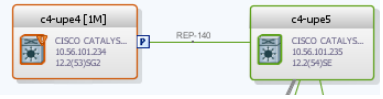
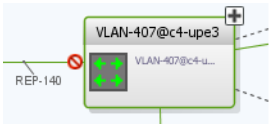
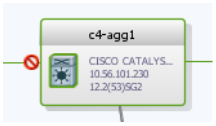
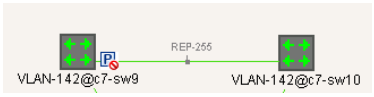
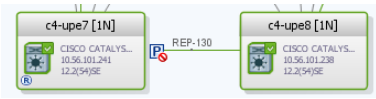
| Item | Description | VLAN Domain View | VLAN Overlay |
|---|---|---|---|
| | REP identifier—Uses the format REP-*id* where *id* represents the REP segment identifier. |  The REP identifier is displayed in the domain view if the visual link represents only one link.<br>f the visual link represents more 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 13-28 REP Icons and Badges in VLAN Domain Views and Overlays (continued)*

| Item | Description | VLAN Domain View | VLAN Overlay |
|---|---|---|---|
| | Multiple links with badges icon—Indicates that one or more link is represented by the visual link and at least one of the links contains a badge. | The multiple links icon is displayed in the domain view if more than one link is represented by the visual link and at least one of the links contains a badge. |  The multiple links icon is displayed in a VLAN overlay view if either of the following is true:<br>• More than one link is represented by the visual link and the links have different sources or destinations.<br>• 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 13-34 shows an example of the Link Properties window with REP information.

*Figure 13-34 VLAN Service Link Properties Window with REP Information*

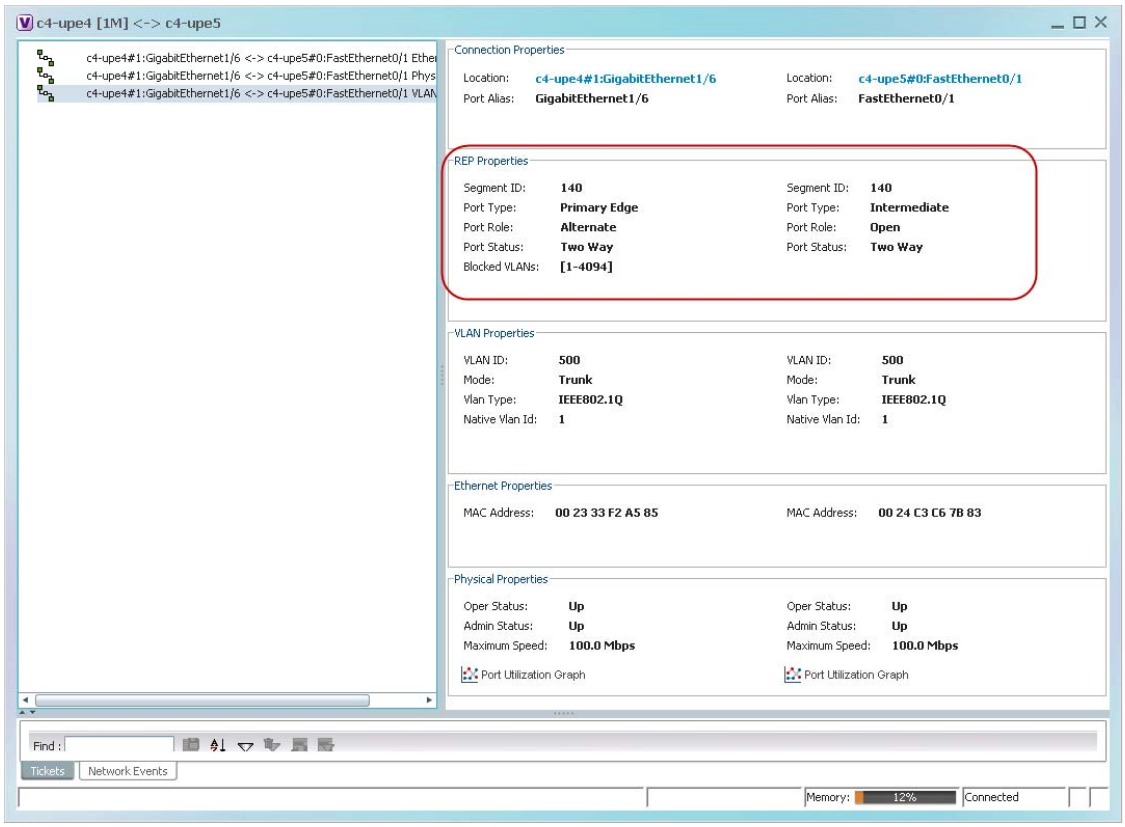



Table 13-29 describes the information that is displayed for REP for each end of the link.

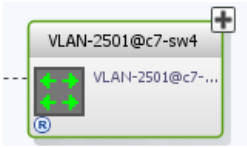
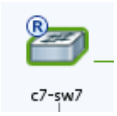
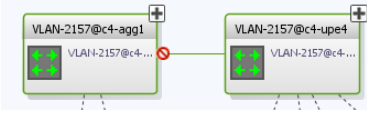
*Table 13-29 REP Properties in VLAN Service Link Properties Window*

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

# Viewing STP Information in VLAN Domain Views and VLAN Overlays

You can view STP segment and port information in Prime Network Vision in the map view. The icons displayed depend on whether you view the STP information in the VLAN domain view or in a VLAN overlay. Table 13-30 describes the icons and badges used to represent STP link and port information.

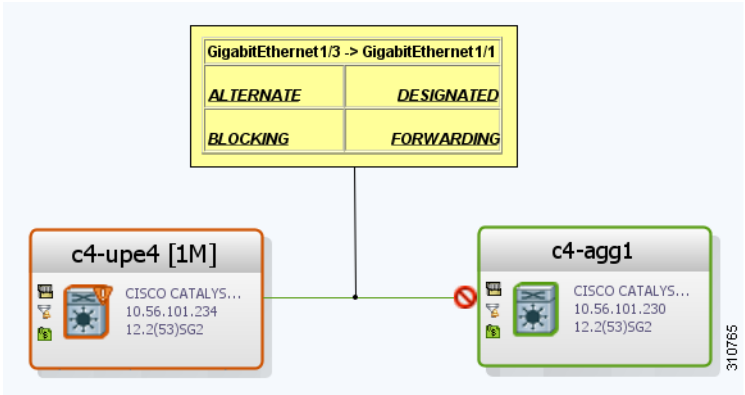
*Table 13-30 STP Information in VLAN Domain Views and Overlays*

| Item | Description | VLAN Domain View | VLAN Overlay |
|---|---|---|---|
| | The STP root bridge, or root of the STP tree, is indicated by an uppercase R. |  |  |
| | An STP root port is the port at the root of the STP tree. Each switching entity in the network VLAN should have a port designated as the root port.<br>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 13-35:

- Port name
- Port role
- Port state

*Figure 13-35 STP Link Information in a VLAN Overlay*



# Viewing STP Properties for VLAN Service Links

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

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

Figure 13-36 shows an example of the Link Properties window with STP information.

***Figure 13-36 STP Properties in VLAN Service Link Properties Window***

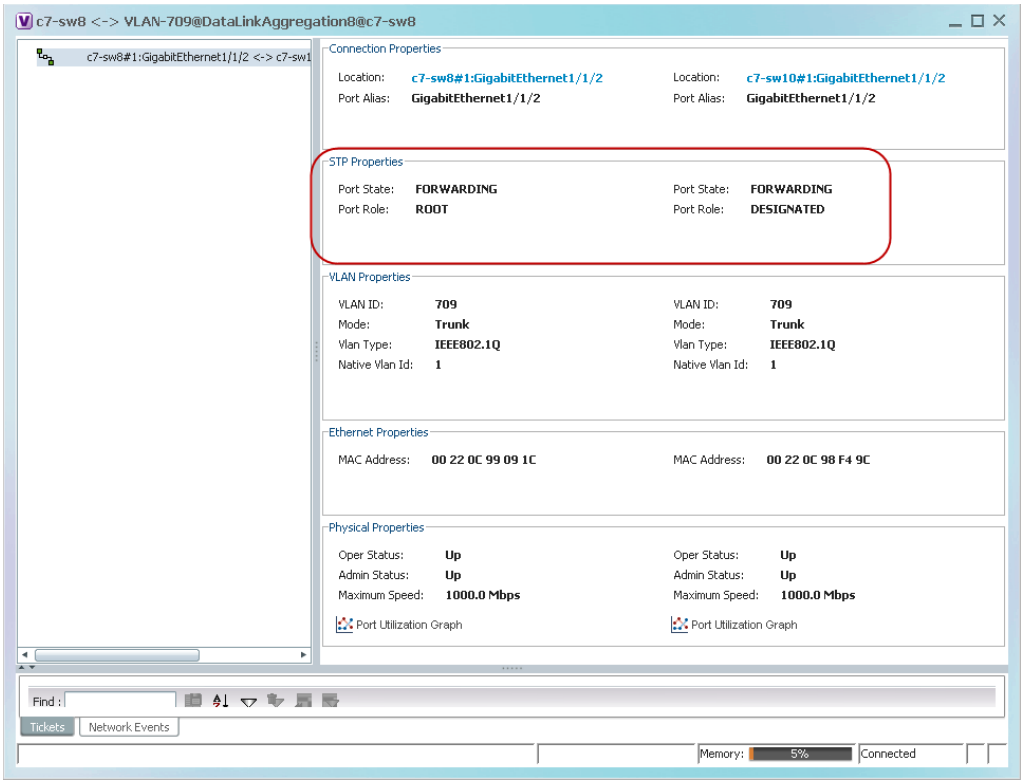



Table 13-31 describes the information that is displayed for STP for the VLAN service link.

***Table 13-31 STP Properties in VLAN Service Link Properties Window***

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

# Viewing VLAN Trunk Group Properties

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

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

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

To view VTP properties:

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

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

The VTP Domain Properties window is displayed as shown in Figure 13-37.

***Figure 13-37 VTP Domain Properties Window in Logical Inventory***

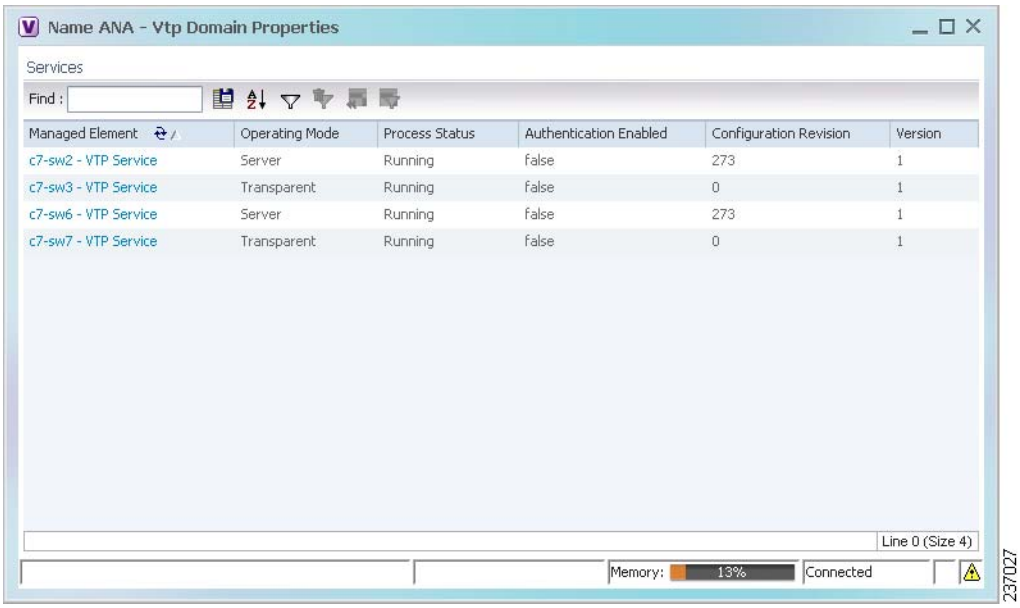


Table 13-32 describes the information that is displayed in the VTP Domain Properties window.

*Table 13-32 VTP Domain Properties Window*

| Field | Description |
|---|---|
| Managed Element | Managed element name, hyperlinked to VTP in logical inventory. |
| Operating Mode | VTP operating mode:<br>• Server—Allows VLAN creation, modification, and deletion, and specification of other configuration parameters for the entire VTP domain. Server is the default mode.<br>• Client—Same behavior as VTP server, except VLANs cannot be created, changed, or deleted.<br>• 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.<br>However, the device forwards received VTP advertisements out of their trunk ports in VTP Version 2.<br>• 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.<br>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.<br>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 13-33 describes the VTP information that is displayed in the inventory window content pane.

*Table 13-33 VTP Properties in Inventory*

| Field | Description |
|---|---|
| Operating Mode | VTP operating mode: Server, Client, Transparent, or Off. |
| Domain Name | VTP domain name. |
| Version | VTP version: 1, 2, or 3. |
| Pruning | Whether or not VTP pruning is enabled: True or False.<br>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 13-33 VTP Properties in Inventory (continued)*

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

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

# Viewing VLAN Bridge Properties

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

To view VLAN bridge properties:

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

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

VLAN bridge properties are displayed as shown in Figure 13-38.

*Figure 13-38 VLAN Bridge Properties in Logical Inventory*

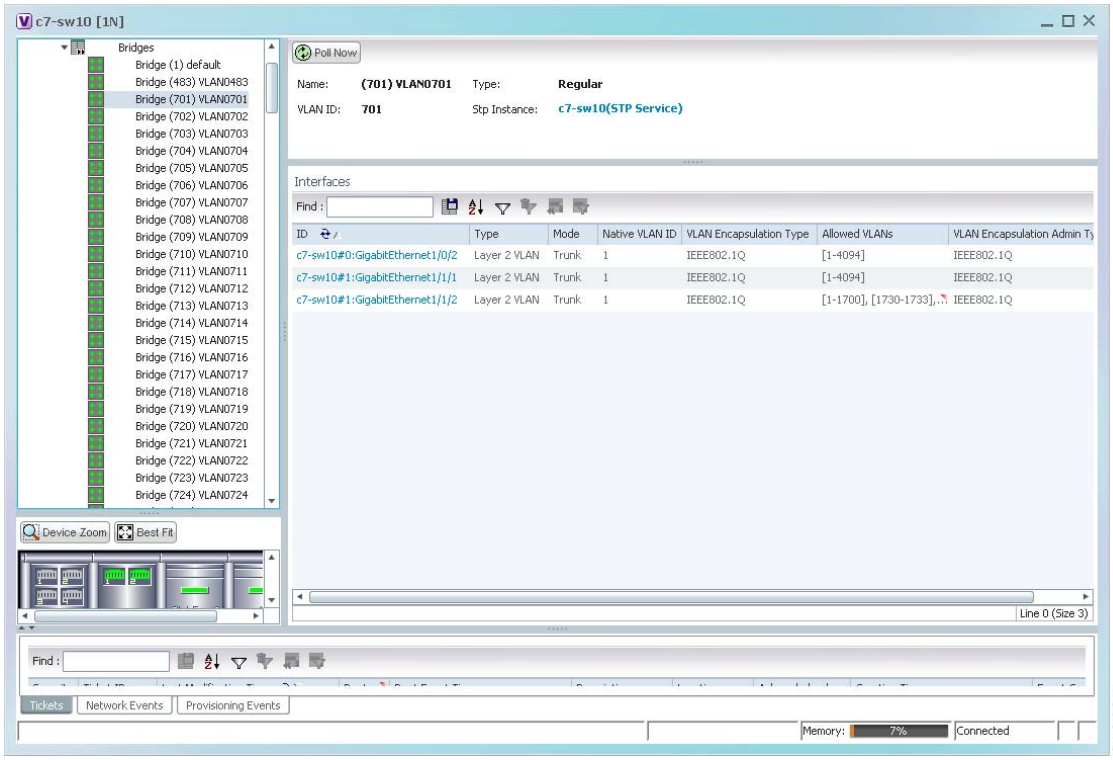


Table 13-34 describes the information that is displayed. Depending on the bridge configuration, any of the tabs might be displayed for the selected bridge.

***Table 13-34 VLAN Bridge Properties***

| Field | Description |
|---|---|
| Name | VLAN bridge name. |
| Type | VLAN bridge type. |
| MAC Address | VLAN bridge MAC address. |
| VLAN ID | VLAN bridge VLAN identifier. |
| STP Instance | STP instance information, hyperlinked to the STP entry in logical inventory. |
| **Bridge Table Tab** | |
| MAC Address | Bridge MAC address. |
| Port | Port associated with the bridge, hyperlinked to the interface in physical inventory. |
| **Interfaces Tab** | |
| ID | VLAN interface identifier, hyperlinked to the interface in physical inventory. |
| Type | VLAN interface type, such as Layer 2 VLAN. |
| Mode | VLAN interface configuration mode:<br>• Unknown—The interface is not VLAN aware.<br>• Access—Puts the interface into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The interface becomes nontrunking.<br>• 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.<br>• 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.<br>• 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.<br>• 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 13-34 VLAN Bridge Properties (continued)*

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

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

# Using Commands to Work With VLANs

The following commands can be launched from the physical inventory by right-clicking an Ethernet slot and choosing **Commands > Configuration**. Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

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

*Table 13-35 VLAN Commands*

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

# Understanding Unassociated Bridges

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

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

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

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

## Adding Unassociated Bridges

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

To add an unassociated bridge to a map:

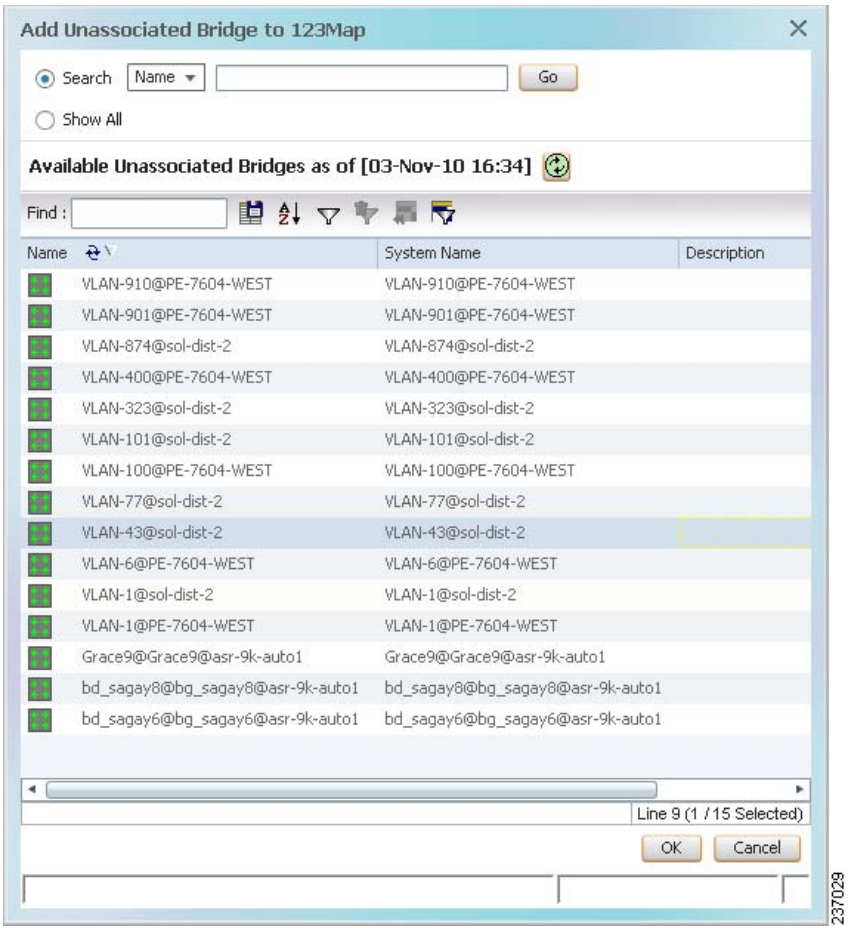
**Step 1** In Prime Network Vision, select the required map or domain.

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

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

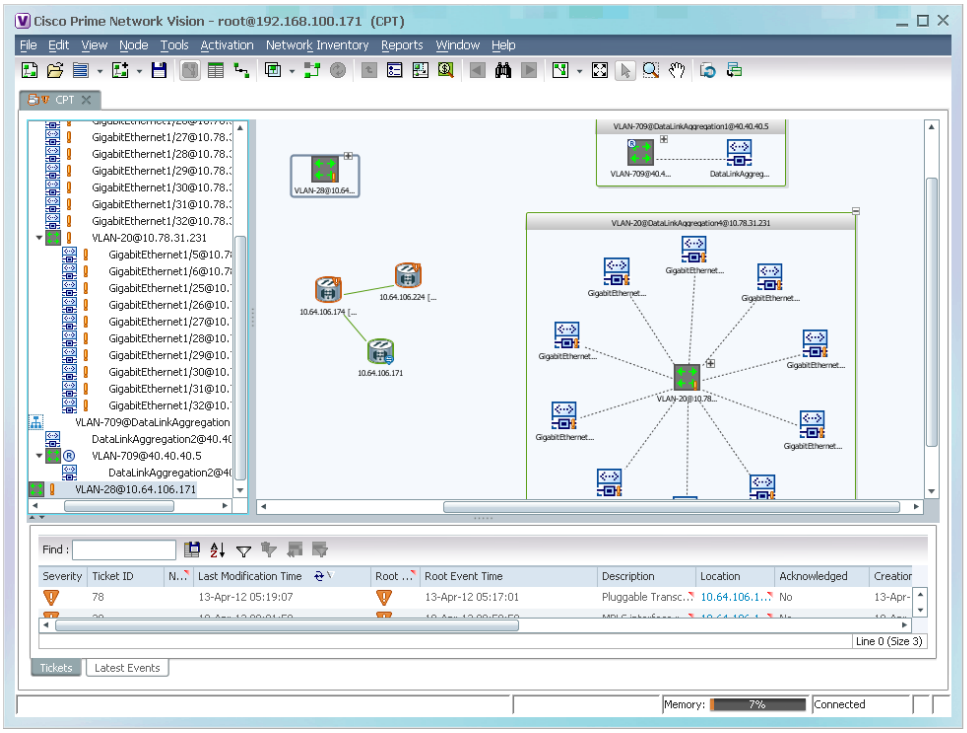
Figure 13-39 shows an example of the Add Unassociated Bridge dialog box.

*Figure 13-39 Add Unassociated Bridge Dialog Box*




**Step 3** In the Add Unassigned Bridge to *domain* dialog box, select the required bridge and click **OK**. The map is refreshed and displays the newly added bridge as shown in Figure 13-40.

*Figure 13-40 Unassociated Bridge in Prime Network Vision*




# Working with Ethernet Flow Point Cross-Connects

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

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

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

- Adding EFP Cross-Connects, page 13-75
- Viewing EFP Cross-Connect Properties, page 13-75

# 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 13-41).

*Figure 13-41 Local Switching Table in Logical Inventory*

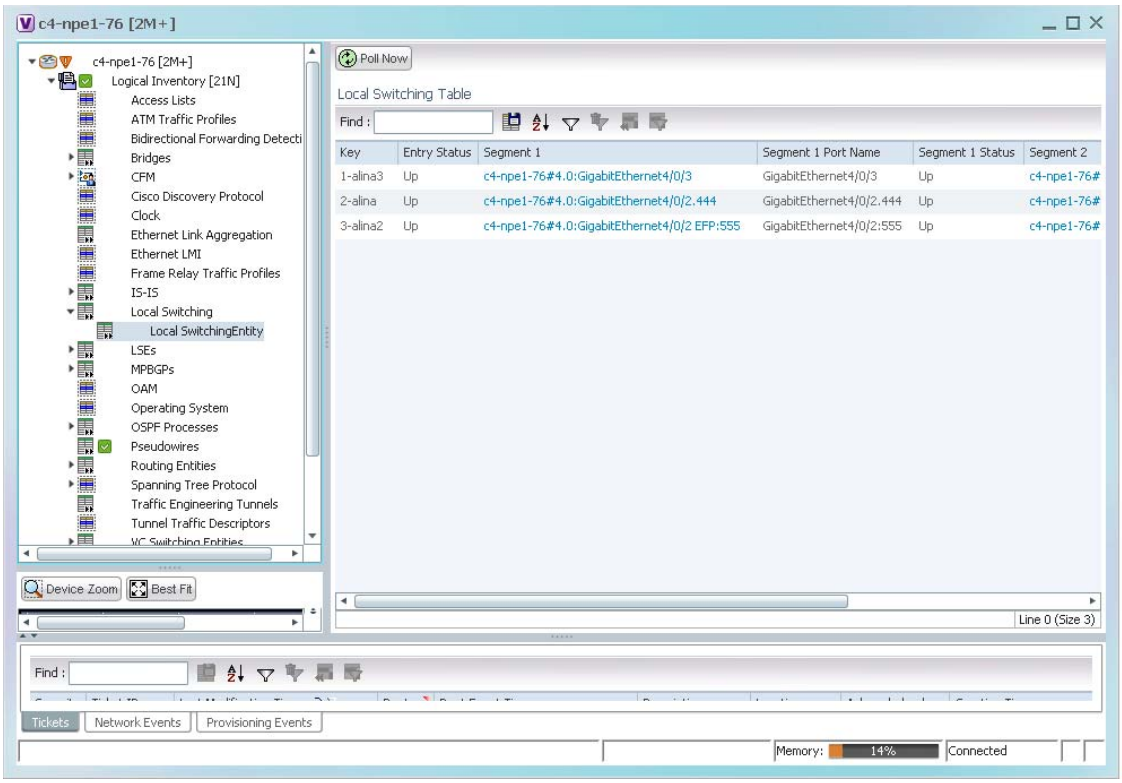



Table 13-36 describes the information displayed for the EFP cross-connects in the Local Switching Table.

*Table 13-36 EFP Cross-Connect Properties in Local Switching Table*

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

# Working with VPLS and H-VPLS Instances

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

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

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

- VSIs
- Pseudowires
- EFPs
- Switching entities

## 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 13-78.
- Apply VPLS overlays—See Applying VPLS Instance Overlays, page 13-79.
- View link details in VPLS overlays—See Viewing Pseudowire Tunnel Links in VPLS Overlays, page 13-81.
- View VPLS-related properties—See the following topics:
  - Viewing VPLS Instance Properties, page 13-83
  - Viewing Virtual Switching Instance Properties, page 13-84
  - Viewing VPLS Core or Access Pseudowire Endpoint Properties, page 13-86
  - Viewing VPLS Access Ethernet Flow Point Properties, page 13-88

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

# Adding VPLS Instances to a Map

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

To add a VPLS instance to a map:

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

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

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

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

- To search for specific elements:

  **a.** Choose **Search**.

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

  **c.** Click **Go**.

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

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

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

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

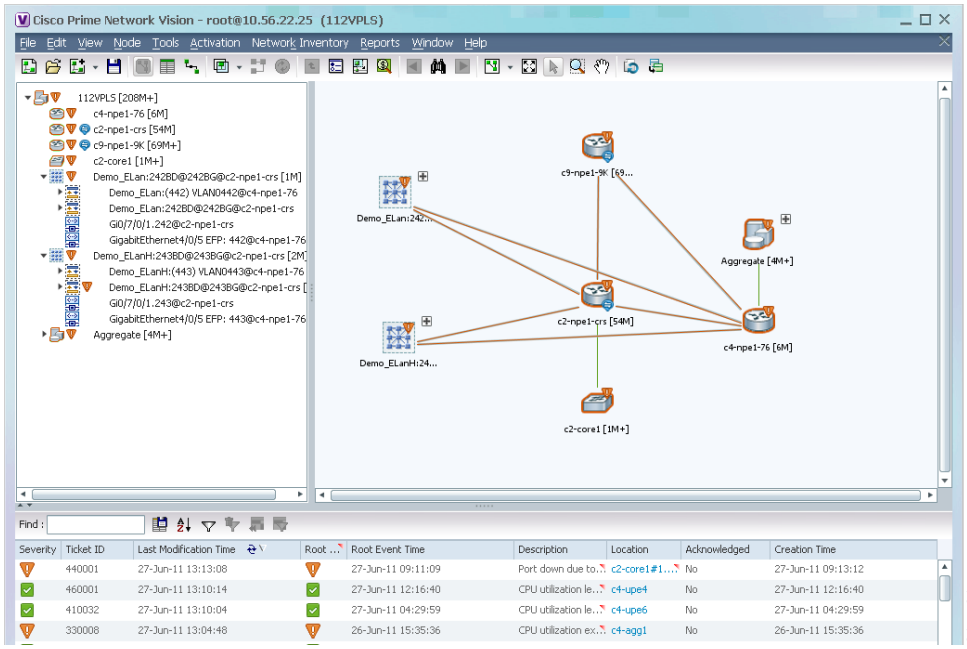
For information about sorting and filtering the table contents, see Filtering and Sorting Tabular Content, page 2-40.

**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 13-42.

*Figure 13-42 VPLS Instance in Prime Network Vision Map*




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

# Applying VPLS Instance Overlays

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

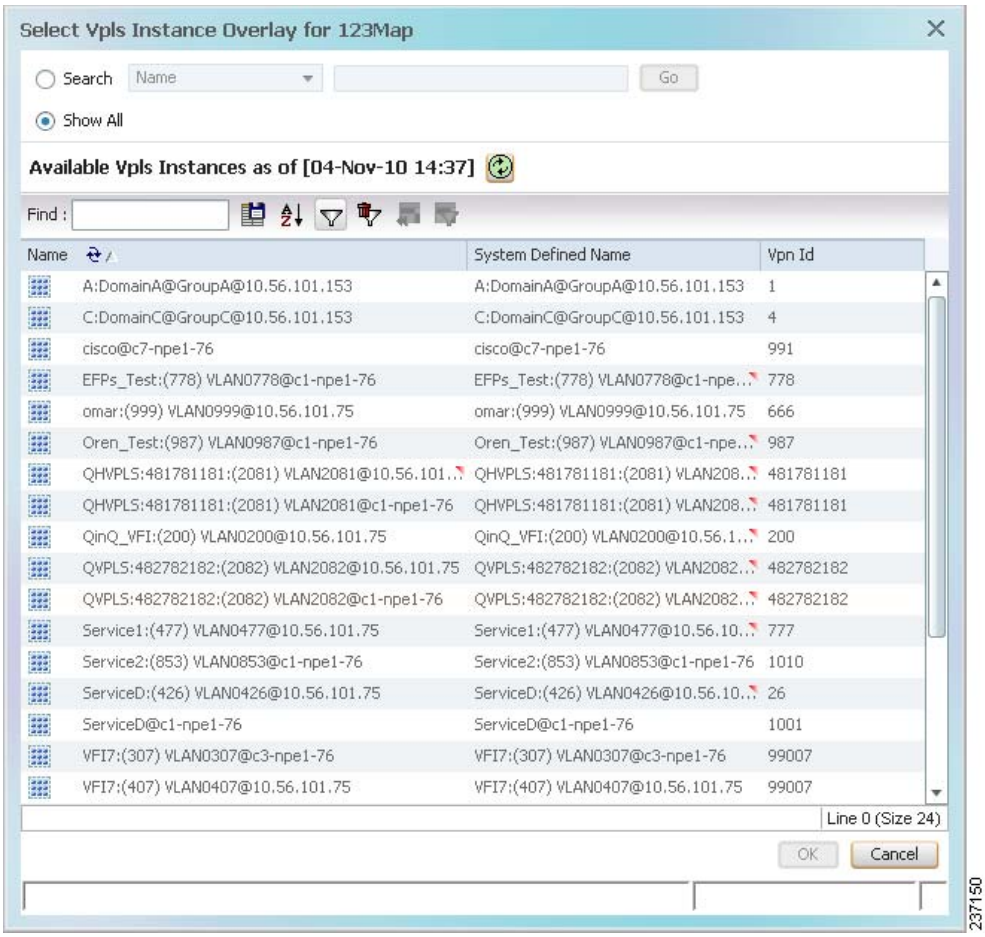
To apply a VPLS instance overlay:

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

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

Figure 13-43 shows an example of the Select VPLS Instance Overlay for *map* dialog box.

*Figure 13-43 Select VPLS Instance Overlay Dialog Box*

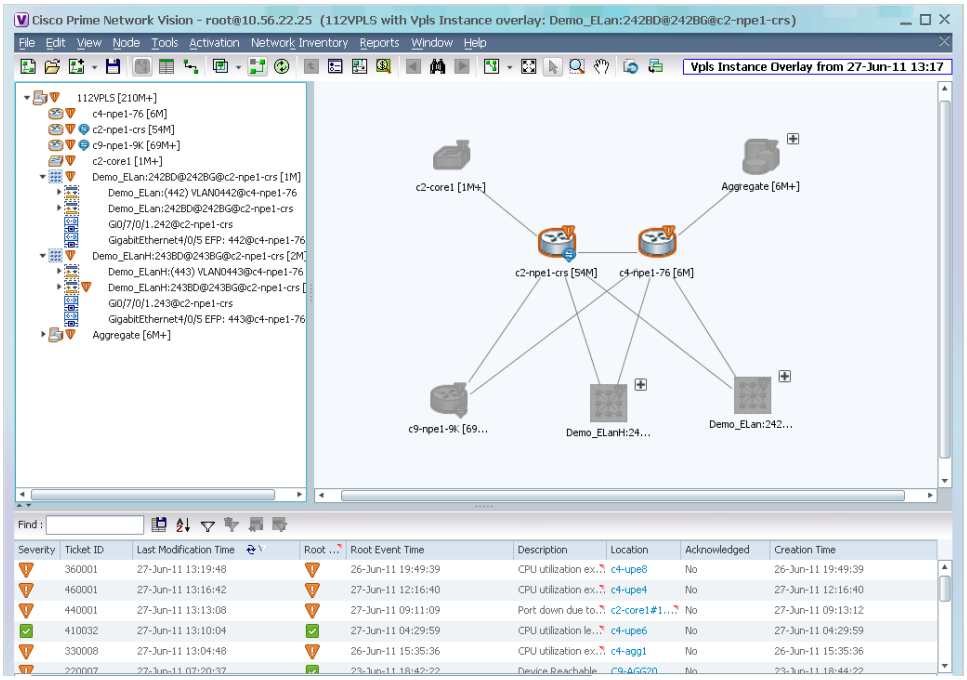



**Step 3** Select the required VPLS instance for the overlay.

**Step 4** Click **OK**.

The elements being used by the selected VPLS instance are highlighted in the map while the other elements are dimmed, as shown in Figure 13-44.

*Figure 13-44 VPLS Instance Overlay in Prime Network Vision*




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

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

# Viewing Pseudowire Tunnel Links in VPLS Overlays

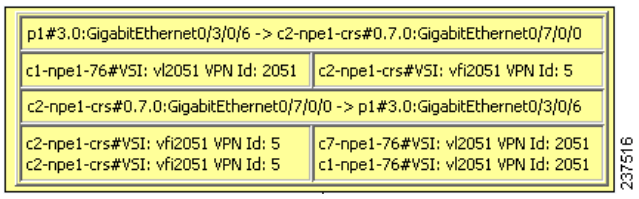
When a VPLS overlay is applied to a map in Prime Network Vision, you can view the details of the pseudowires that are interconnected through selected links.

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

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

Link information is displayed as shown in Figure 13-45.

*Figure 13-45 Link Callout Window for a VPLS Overlay*



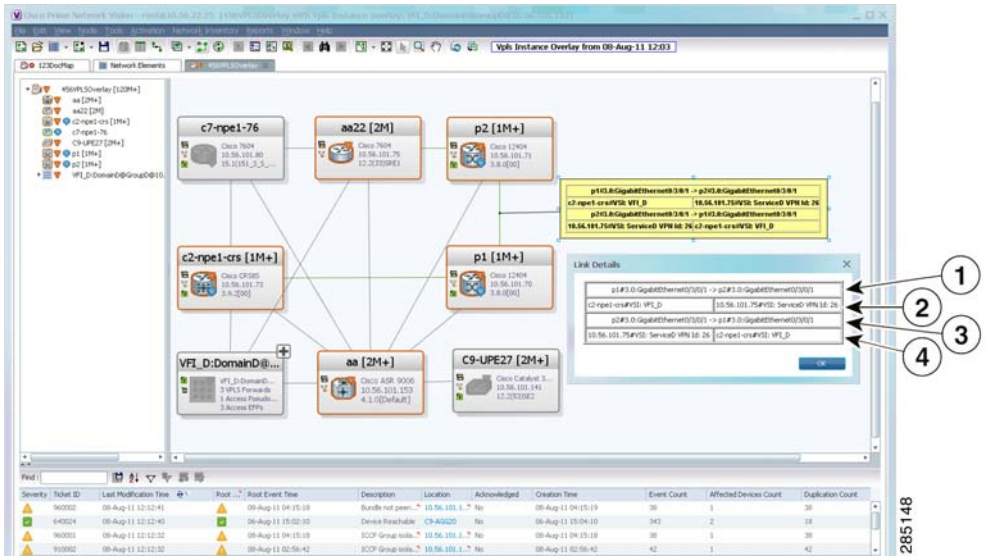
The callout window displays the following information for each link represented by the selected link:

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

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

The details about the link are displayed in the Link Details window as shown in Figure 13-46.

***Figure 13-46 Link Details Window for a VPLS Overlay***




The Link Details window provides the following information:

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

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

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

# Viewing VPLS-Related Properties

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

- VPLS instances—See Viewing VPLS Instance Properties, page 13-83.
- Virtual Switching Instances—Viewing Virtual Switching Instance Properties, page 13-84
- Tunnels—See Viewing VPLS Core or Access Pseudowire Endpoint Properties, page 13-86.
- Port connectors—See Viewing VPLS Access Ethernet Flow Point Properties, page 13-88.

## 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 13-47 shows an example of the VPLS Instance Properties window.

***Figure 13-47 VPLS Instance Properties Window***

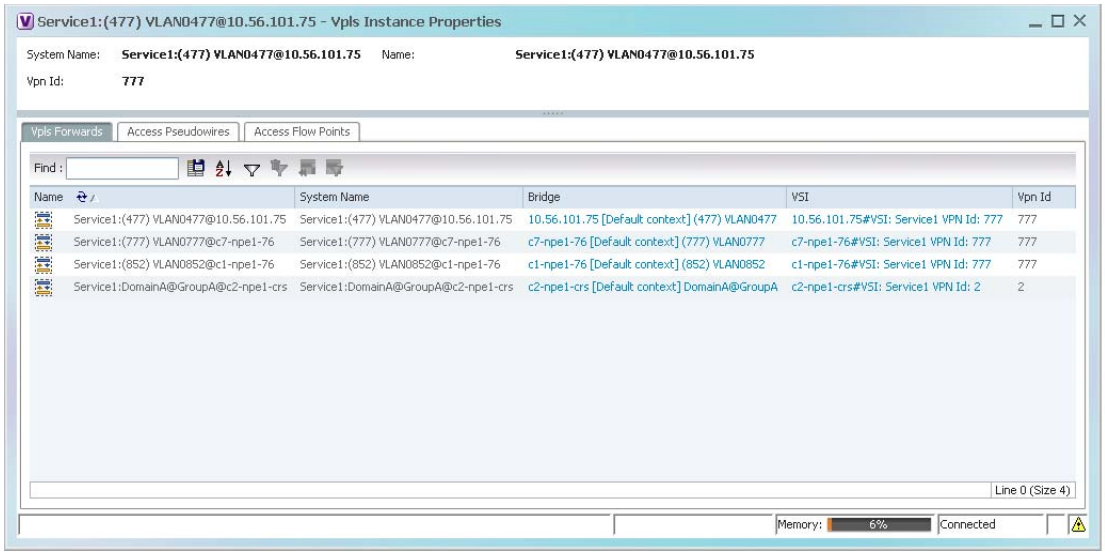



Table 13-37 describes the information that is displayed for VPLS instance properties.

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

***Table 13-37 VPLS Instance Properties***

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

*Table 13-37 VPLS Instance Properties (continued)*

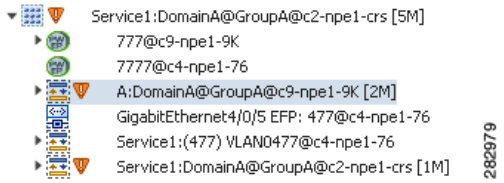
| Field | Description |
|---|---|
| VPN ID | VPN identifier for the VSI. |
| **Access Pseudowires Tab** | |
| Name | Pseudowire name. |
| Port | VSI on which the pseudowire is configured, hyperlinked to the entry in logical inventory. |
| Local Router IP | Local router IP address on which the pseudowire is configured. |
| Tunnel ID | Virtual circuit identifier of the pseudowire. |
| PTP Tunnel | Hyperlinked entry to the pseudowire properties in logical inventory. |
| Peer Router IP | Peer router IP address on which the pseudowire is configured. |
| Peer OID | Hyperlinked entry to the pseudowire properties of the peer. |
| Pseudowire Type | Type of pseudowire, such as Ethernet, Ethernet Tagged, CESoPSN Basic, PPP, or SAToP. |
| Pseudowire Edge Binding Type | Pseudowire endpoint association:<br>• 0—Unknown<br>• 1—Connection termination point<br>• 2—Ethernet flow point<br>• 3—Switching entity<br>• 4—Pseudowire switching entity<br>• 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 13-48.)

*Figure 13-48 VPLS Forward in Prime Network Vision Navigation Pane*




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

VSI properties are displayed as shown in Figure 13-49.

*Figure 13-49 VSI Properties in Logical Inventory*

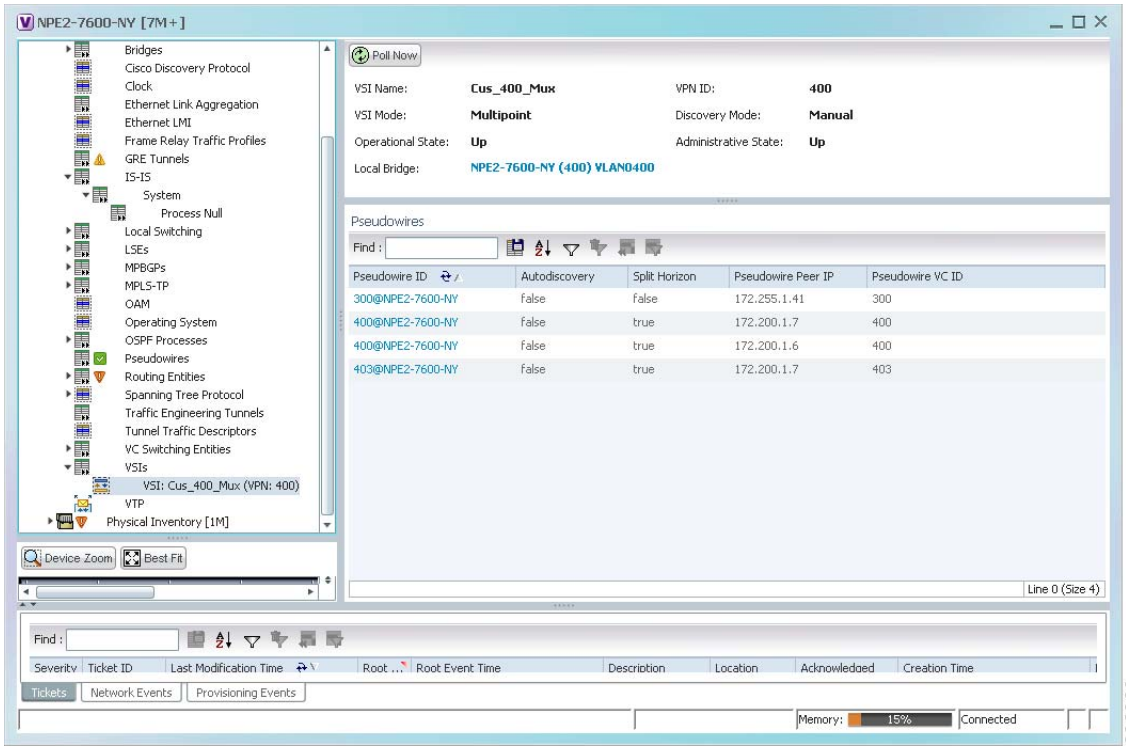


Table 13-38 describes the information that is displayed for the selected VSI.

*Table 13-38 VSI Properties in Logical Inventory*

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

## Viewing VPLS Core or Access Pseudowire Endpoint Properties

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

To view pseudowire endpoint properties for a VPLS instance, right-click the required pseudowire endpoint in the navigation pane, and choose **Properties**. (See Figure 13-50.)

*Figure 13-50 VPLS Pseudowire in Prime Network Vision Navigation Pane*

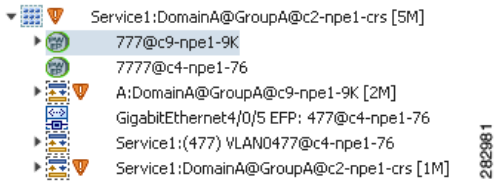



Figure 13-51 shows an example of the Tunnel Properties window that is displayed.

*Figure 13-51 VPLS Tunnel Properties Window*

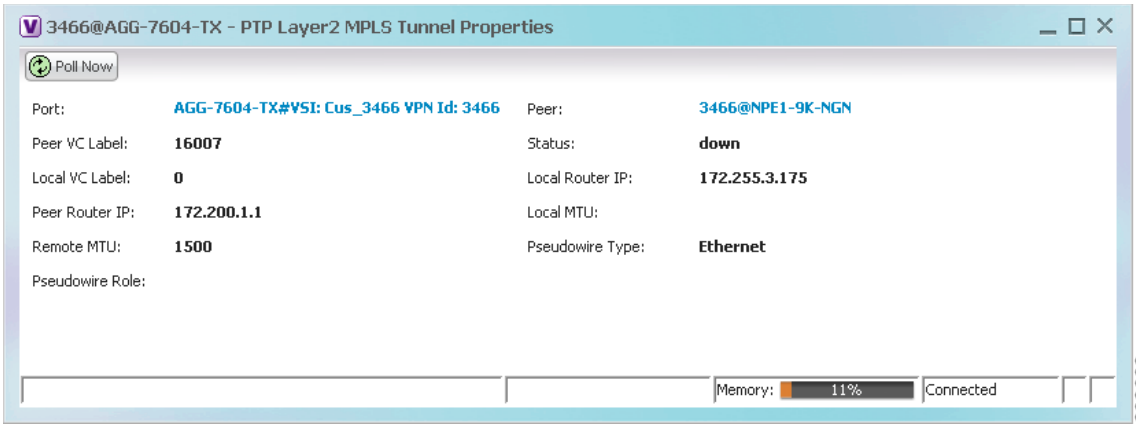



Table 13-39 describes the information that is displayed for pseudowire endpoint properties.

*Table 13-39 Tunnel Properties Window*

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

# Viewing VPLS Access Ethernet Flow Point Properties

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

To view the properties for the Access Ethernet Flow Points configured for a VPLS instance, right-click the required interface in the navigation pane, and choose **Inventory**. (See Figure 13-52.)

***Figure 13-52 VPLS Interface in Prime Network Vision Navigation Pane***

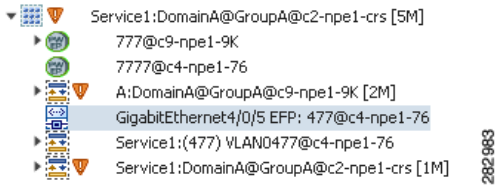
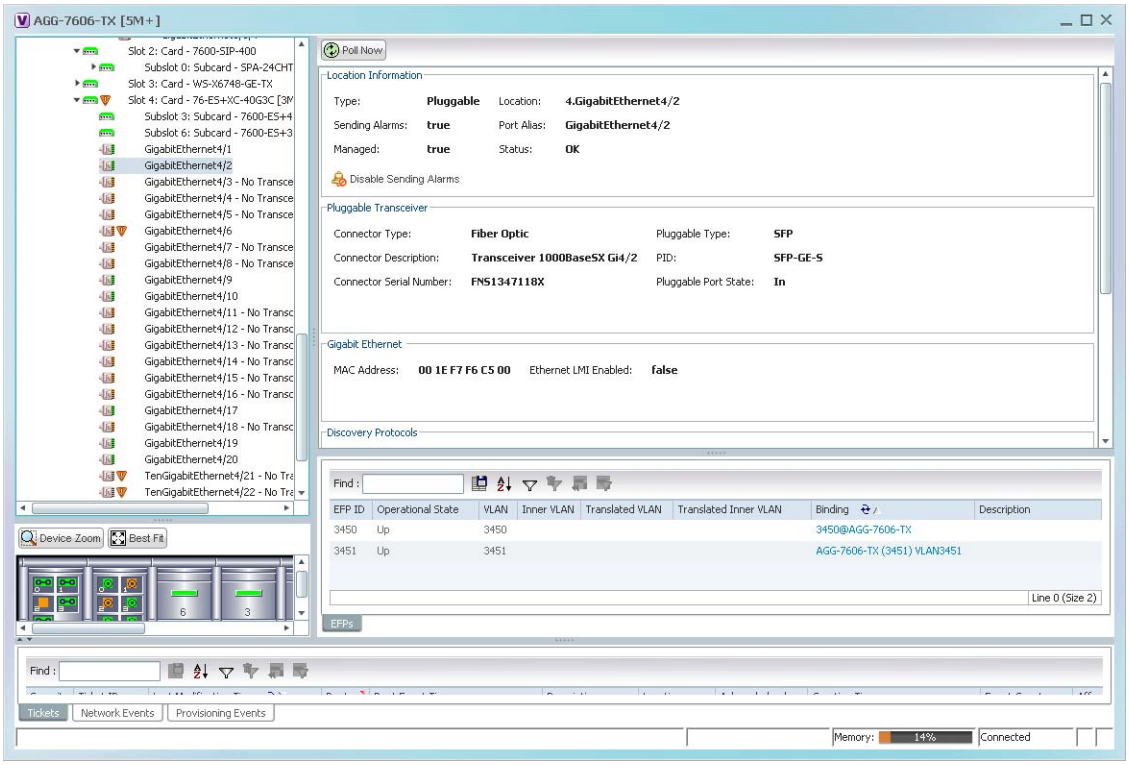



Figure 13-53 shows an example of the information displayed for the interface in physical inventory.

***Figure 13-53 EFP Properties in Physical Inventory***




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

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

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

- List of the configured subinterfaces on the port. For more information on the Subinterfaces table, see Viewing a Port Configuration, page 3-25.
- List of the configured EFPs on the port. For more information on the EFPs table, see Viewing EFP Properties, page 13-32.
- List of VLAN mappings configured on the port. For more information about the VLAN Mappings table, see Viewing VLAN Mappings, page 13-52.

# Working with Pseudowires

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

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

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

For details on the software versions Prime Network supports for these network elements, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*. To run the pseudowire commands, the software on the network element must support the pseudowire technology.

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

- Adding Pseudowires to a Map, page 13-89
- Viewing Pseudowire Properties, page 13-92
- Displaying Pseudowire Information, page 13-94
- Viewing Pseudowire Redundancy Service Properties, page 13-95
- Applying Pseudowire Overlays, page 13-97
- Monitoring the Pseudowire Headend, page 13-99

## 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.

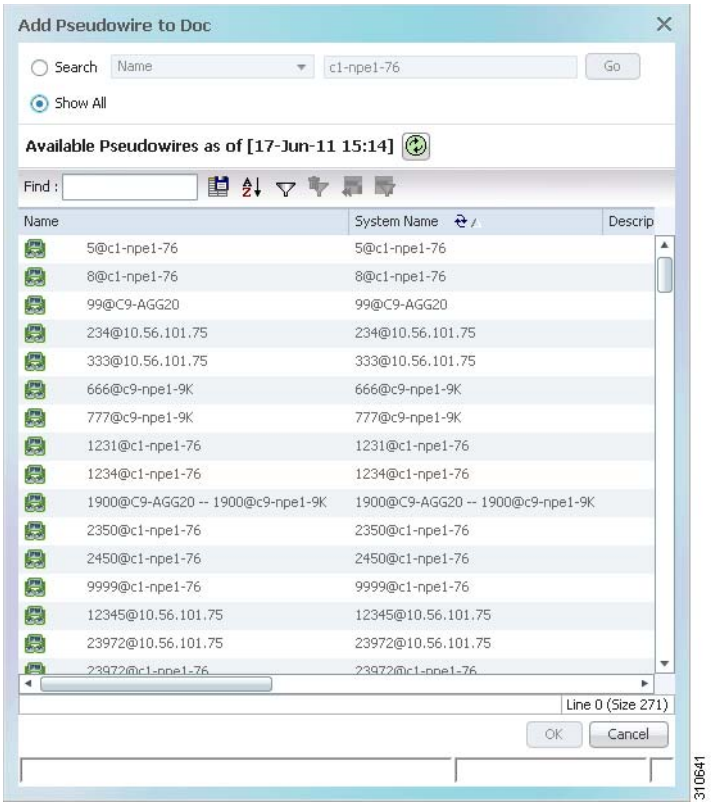
**Step 2** Open the Add Pseudowire to *map* dialog box in either of the following ways:

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

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

Figure 13-54 shows an example of the Add Pseudowire dialog box.

***Figure 13-54 Add Pseudowire Dialog Box***




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

- To search for specific elements:

  **a.** Choose **Search**.

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

  **c.** Click **Go**.

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

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

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

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

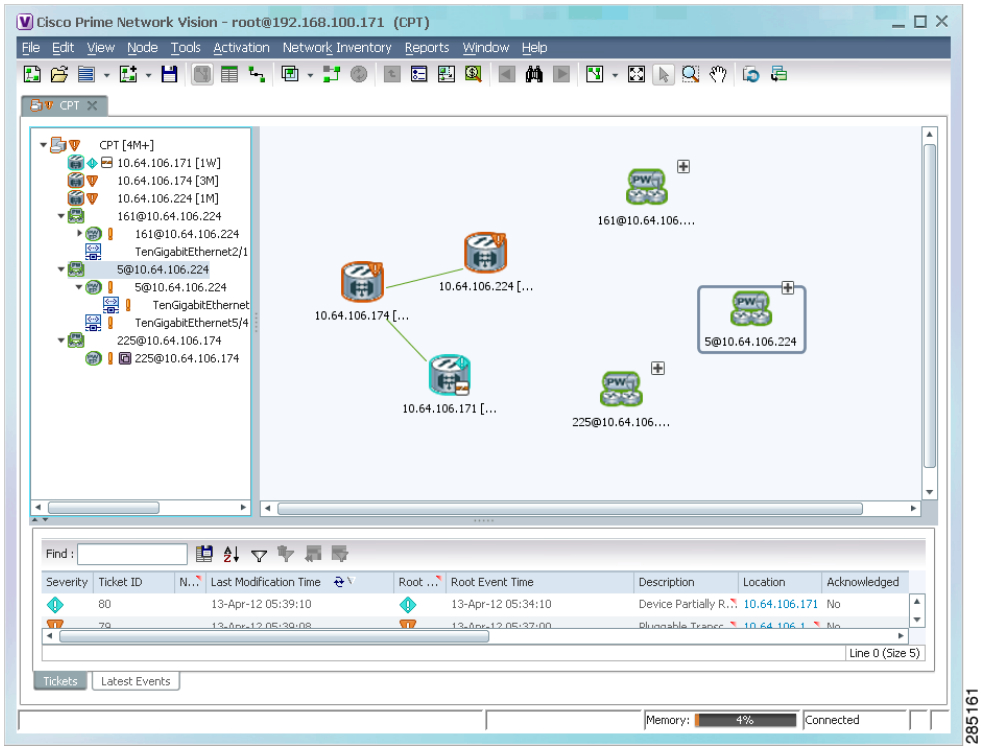
For information about sorting and filtering the table contents, see Filtering and Sorting Tabular Content, page 2-40.

**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 13-55.

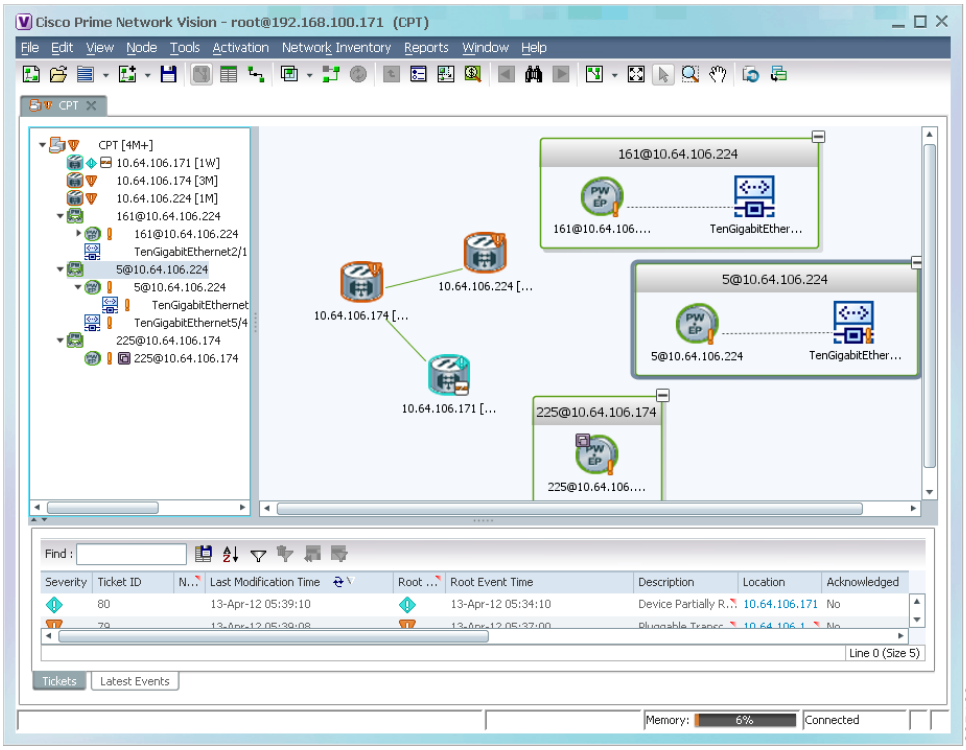
***Figure 13-55 Pseudowire in Prime Network Vision Map***




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

Figure 13-56 shows an example of an expanded pseudowire in Prime Network Vision.

*Figure 13-56 Pseudowire Components in Prime Network Vision Maps*




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

# Viewing Pseudowire Properties

To view pseudowire properties:

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

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

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

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

The Tunnel Edges table is displayed, listing the pseudowire endpoints configured on the selected element. For a description of the information contained in the Pseudowires Tunnel Edges table, see Table 19-27.

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

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

The Pseudowire Properties window is displayed as shown in Figure 13-57.

*Figure 13-57 Pseudowire Properties Window*

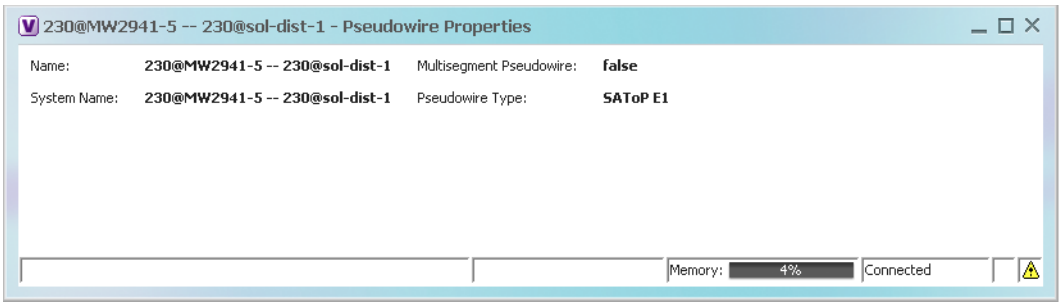



Table 13-40 describes the information presented in the Pseudowire Properties window.

*Table 13-40 Pseudowire Properties Window*

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

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

The Tunnel Properties window containing the pseudowire endpoint properties is displayed as shown in Figure 13-51 and described in Table 13-39.

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

The Local Switching table is displayed as shown in Figure 13-41.

Table 13-36 describes the information displayed in the Local Switching table.

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

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

Table 13-41 describes the information displayed in the Contained Current CTPs table.

*Table 13-41 Contained Current CTPs Table*

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

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

See Viewing EFP Properties, page 13-32 for the information that is displayed for EFPs.

# Displaying Pseudowire Information

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

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

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

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

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

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

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

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

**Step 5** The following information is displayed:

- The element name.
- The command issued.
- The results, including:
  - VCCV: CC Type—The types of CC processing that are supported. The number indicates the position of the bit that was set in the received octet. The available values are:
    - CW [1]—Control Word
    - RA [2]—Router Alert
    - TTL [3]—Time to Live
    - Unkn [x]—Unknown
  - Elapsed time—The elapsed time, in seconds.

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

# Viewing Pseudowire Redundancy Service Properties

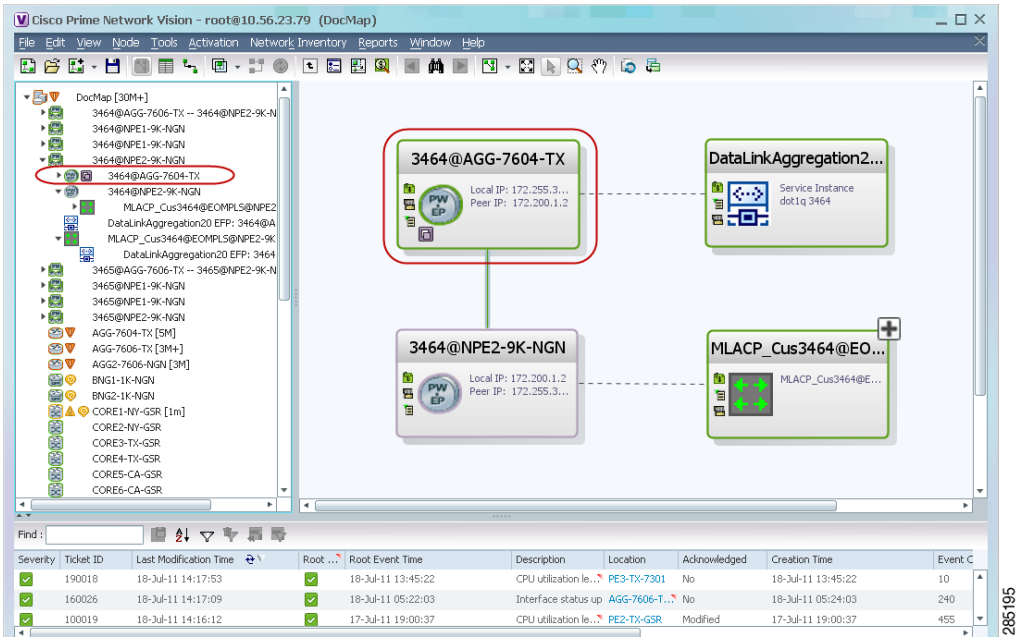
If a pseudowire is configured for redundancy service, a redundancy service badge is applied to the secondary (backup) pseudowire in the navigation and map panes in the Prime Network Vision window. Additional redundancy service details are provided in the inventory window for the device on which the pseudowire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

To view redundancy service properties for pseudowires:

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

If the pseudowire is configured for redundancy service, the redundancy service badge appears in the navigation and map panes as shown in Figure 13-58.

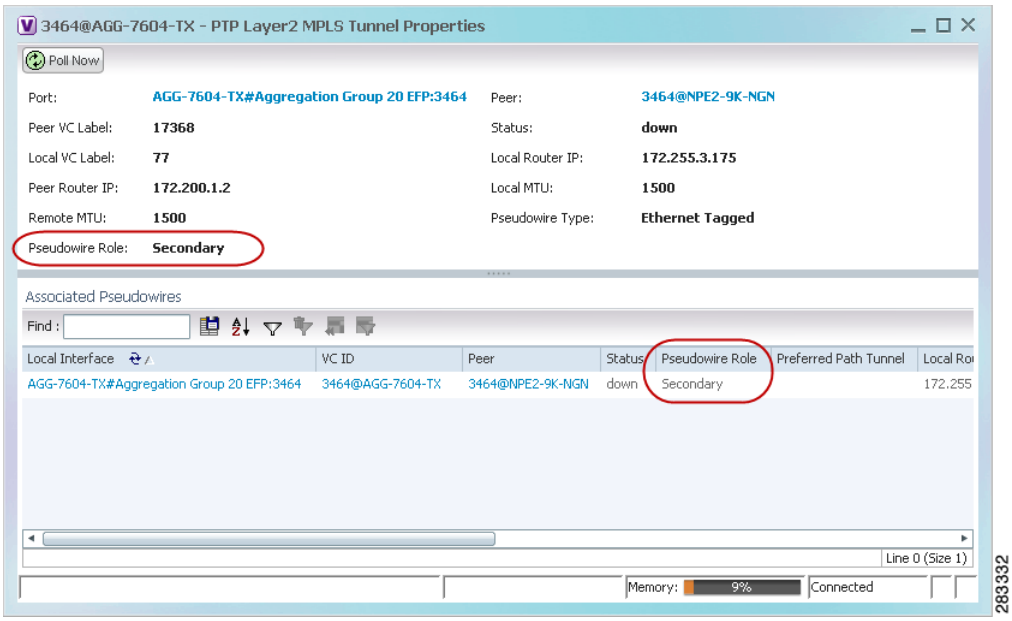
*Figure 13-58 Pseudowire Redundancy Service Badge in a Map*




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

The PTP Layer 2 MPLS Tunnel Properties window is displayed as shown in Figure 13-59 and shows that the selected pseudowire has a Secondary role in a redundancy service.

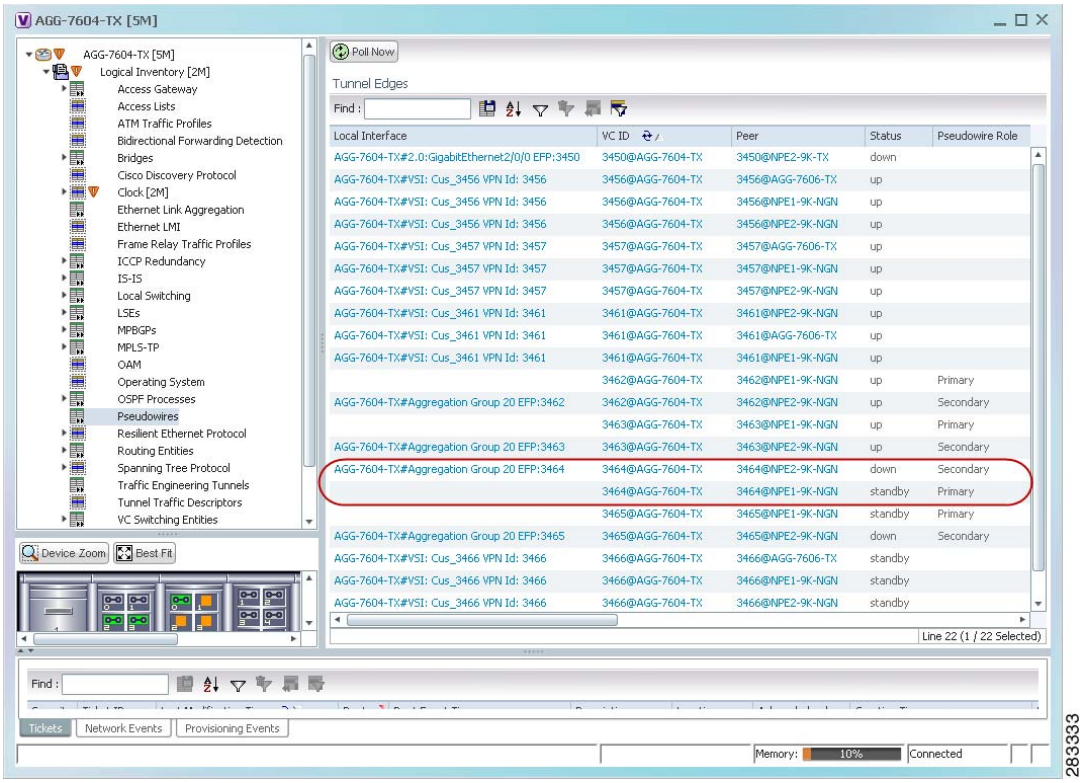
*Figure 13-59 Layer 2 MPLS Tunnel Properties for Pseudowire Redundancy Service*




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

The Tunnel Edges table in logical inventory is displayed, with the local interface selected in the table. (See Figure 13-60.)

*Figure 13-60 Pseudowire Redundancy Service in Logical Inventory*




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

For more information about the Pseudowires Tunnel Edges table, see Table 19-27.

# Applying Pseudowire Overlays

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

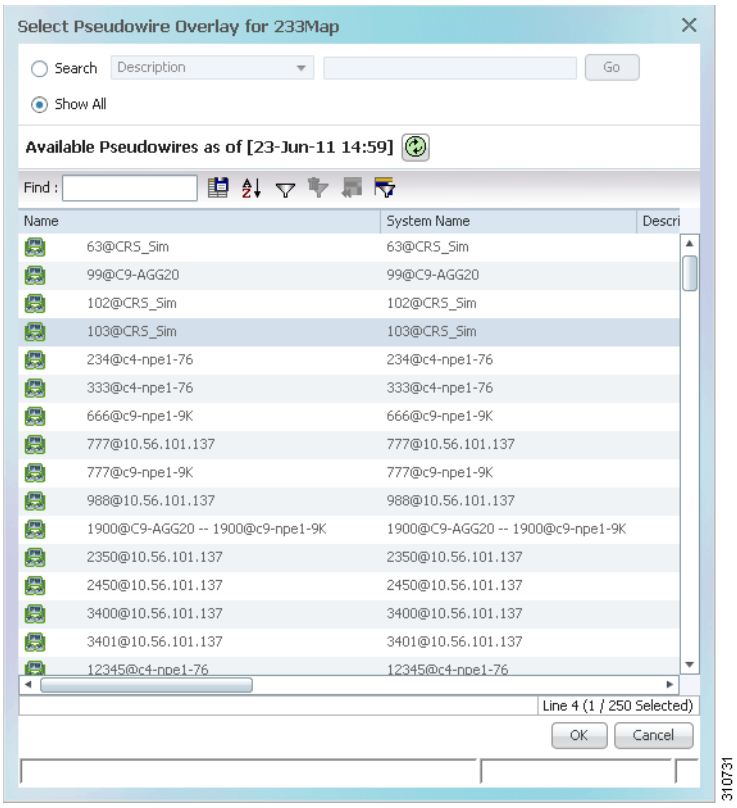
To apply a pseudowire overlay:

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

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

Figure 13-61 shows an example of the Select Pseudowire Overlay for *map* dialog box.

*Figure 13-61 Select Pseudowire Overlay Dialog Box*

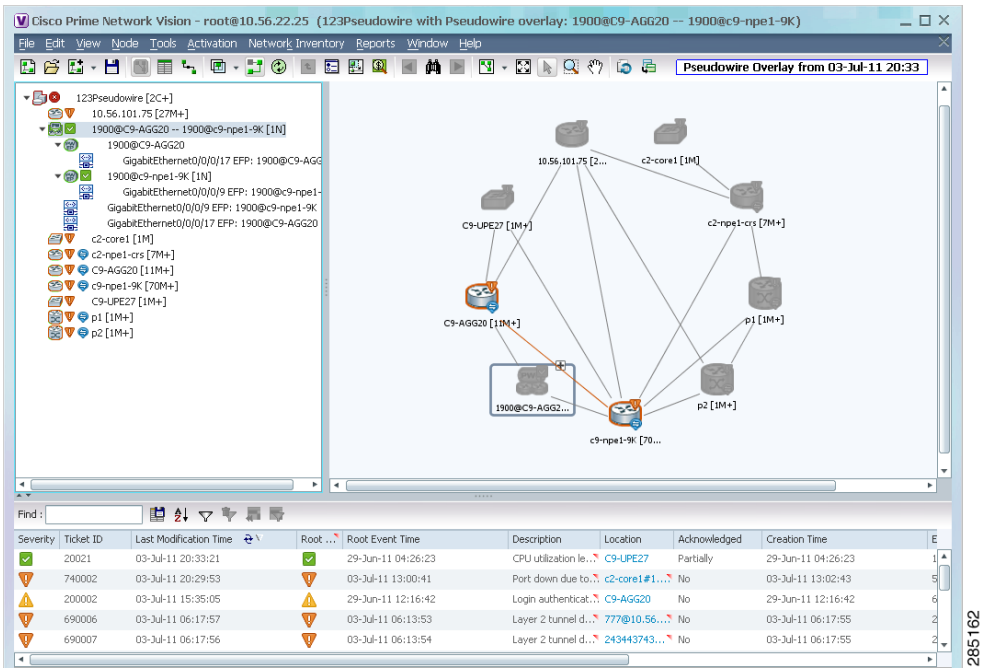



**Step 3** Select the required pseudowire for the overlay.

**Step 4** Click **OK**.

The elements being used by the selected pseudowire are highlighted in the map while the other elements are dimmed, as shown in Figure 13-62.

*Figure 13-62 Pseudowire Overlay in Prime Network Vision*




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

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

# Monitoring the Pseudowire Headend

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

Figure 13-63 displays a typical pseudowrie deployment over core network and Figure 13-64 displays a pseduowire deployment over access network.

*Figure 13-63 Pseudowire Deployment Over Core Network*

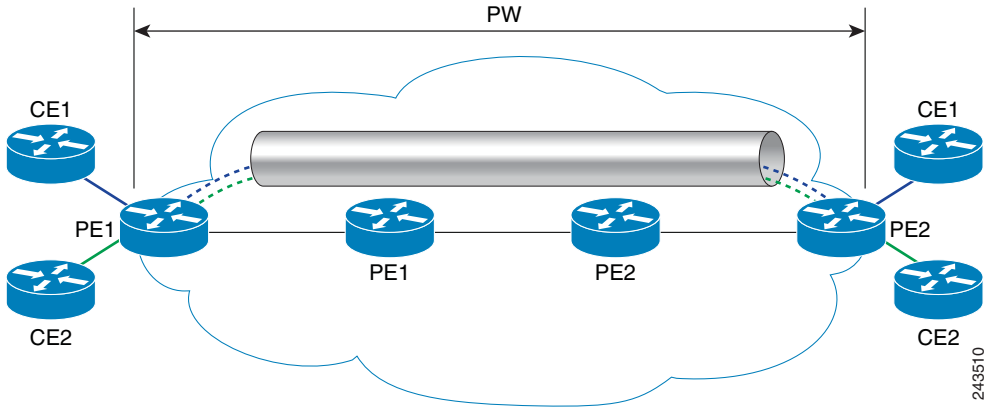
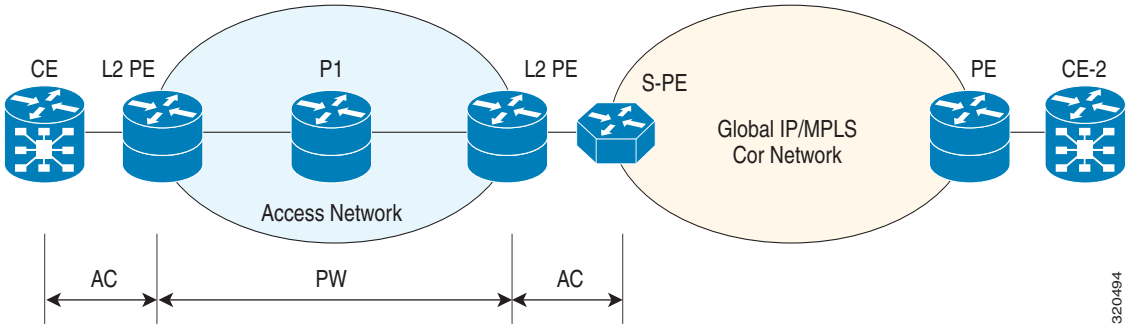



*Figure 13-64 Pseudowire Deployment Over Access Network*

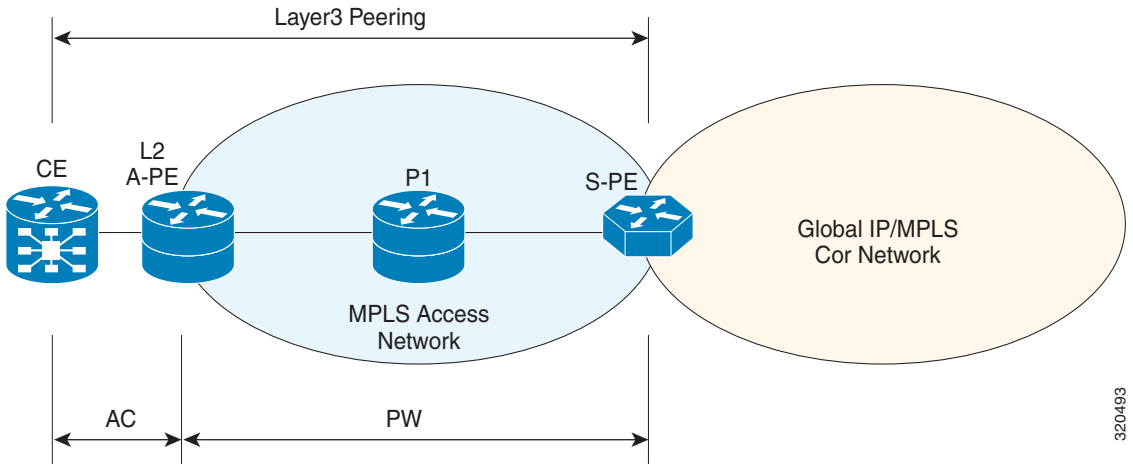



A pseudowire headend (PW-HE) virtual interface originates as a PW on an access node and terminates on a Layer 3 service instance on the service provider router. For example, a PWHE can originate on the Layer 2 PW feeder node and terminate on a VRF instance on the Cisco CRS Router. You can configure all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

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

The following figure displays the PW-HE interface:

*Figure 13-65 PW-HE Interface*




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

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

## Viewing the PW-HE configuration

To view the PW-HE configuration:

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

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

**Step 3** From the **PW-HE** node, choose a PW-HE interface. The PW-HE interface details are displayed in the content pane as shown in Figure 13-66.

*Figure 13-66 PW-HE Configuration Details*

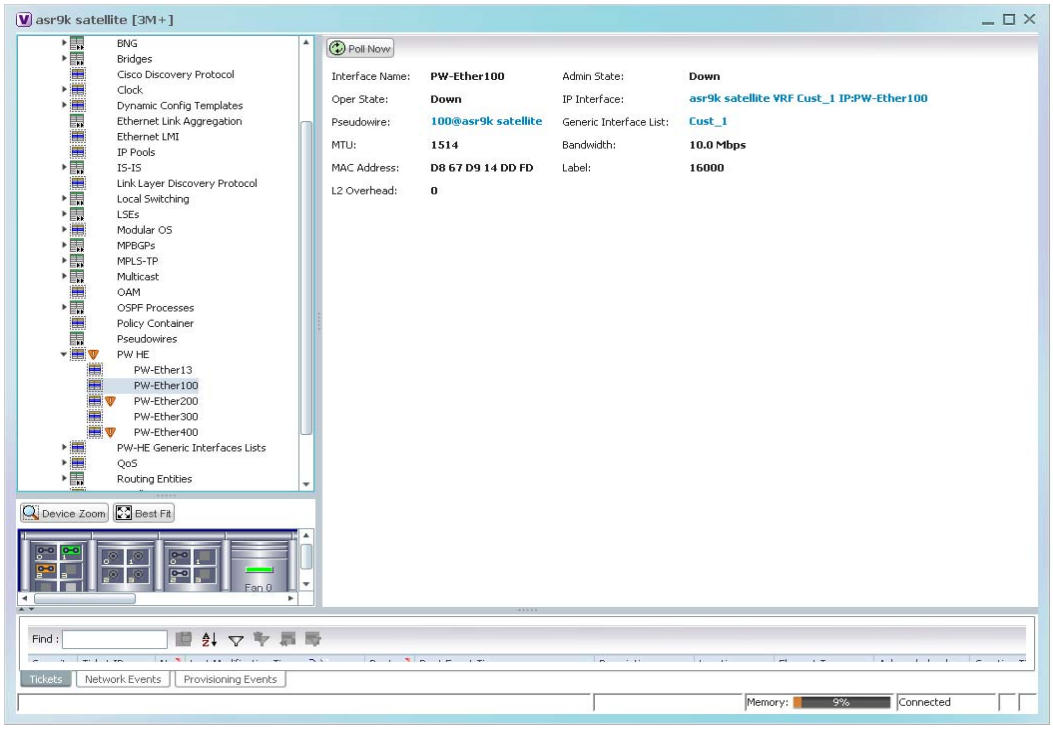



Table 13-42 displays the PW-HE interface details.

*Table 13-42 PW-HE Interface Details*

| Field | Description |
|---|---|
| Interface Name | The unique name to identify the PW-HE interface. |
| Admin State | The administrative state of the PW-HE, which can be any one of the following:<br>• Up<br>• Down |
| Oper State | The operational state of the PW-HE, which can be any one of the following:<br>• Up<br>• Down |
| IP Interface | The IP interface for the PW-HE, which when clicked will take you either to the associated VRF interface site under the VRF node or the associated IP Interface under the Routing Entity node. |
| Pseudowire | The pseudowire to which the PW-HE is associated with, which when clicked will take you to the **Pseudowire** node. |
| Generic Interface List | The generic interface list linked to the PW-HE, which when clicked will take you to the relevant node under the **PW-HE Generic Interfaces Lists** node. |
| MTU | The maximum number of transmission units (in bytes) for the PW-HE interface. |

*Table 13-42 PW-HE Interface Details (continued)*

| Field | Description |
|---|---|
| Bandwidth | The bandwidth (in kbits) for the PW-HE interface. |
| MAC Address | The MAC address specified for the PW-HE interface, which is generally in the xxx.xxx.xxx format. |
| Label | The MPLS label for the PW-HE interface. |
| L2 Overhead | The layer 2 overhead (in bytes) configured on the PW-HE interface, which can be any value between 0 and 64. This field defaults to 0. |

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

- Viewing PW-HE Configured as a Local Interface under Pseudowire, page 13-103
- Viewing PW-HE Generic Interface List, page 13-103
- Viewing PW-HE as an Associated Entity for a Routing Entity, page 13-104
- Viewing PW-HE as an Associated Entity for a VRF, page 13-104

## Viewing PW-HE Configured as a Local Interface under Pseudowire

To view the local interface details:

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

**Step 2** In the logical inventory window, choose **Logical Inventory > Pseudowire**. The list of Pseudowire interfaces configured in Prime Network are displayed in the content pane. For more information on Pseudowire properties, see Viewing Pseudowire Properties, page 13-92.

-

## Viewing PW-HE Generic Interface List

To view the PW-HE generic interface list:

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

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

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

Table 13-43 displays the PW-HE Generic Interface List details.

*Table 13-43 PW-HE Generic Interface List Details*

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

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

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

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

**Step 2** In the logical inventory window, choose **Logical Inventory > Routing Entities > Routing Entity**. The routing entity details for the PW-HE is displayed in the content pane. For more information on Routing entity details, see Viewing Routing Entities, page 19-31.

## Viewing PW-HE as an Associated Entity for a VRF

To view the VRF details for a PW-HE:

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

**Step 2** In the logical inventory window, choose **Logical Inventory > VRF >** *PW-HE node*. The VRF details for the PW-HE is displayed in the content pane. For more information on VRF details, see Viewing VRF Properties, page 19-27.

# Working with Ethernet Services

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

- Network VLAN and bridge domain are linked through a shared EFP.
- Network VLAN and VPLS instance are linked through either of the following:
  - A shared, standalone EFP.
  - A shared switching entity.
- Network VLAN and network pseudowire (single or multi-segment) are linked through either of the following:
  - A shared, standalone EFP.
  - A shared switching entity.

- VPLS-EoMPLS connected via a shared access pseudowire endpoint.
- Network VLAN and cross-connect are connected by a shared EFP.
- Network VLAN and service link are connected by a shared EFP.

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

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

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

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

- Adding Ethernet Services to a Map, page 13-105
- Applying Ethernet Service Overlays, page 13-106
- Viewing Ethernet Service Properties, page 13-108

# Adding Ethernet Services to a Map

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

To add an Ethernet service to a map:

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

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

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

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

- To search for specific elements:

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

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

  **c.** Click **Go**.

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

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

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

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

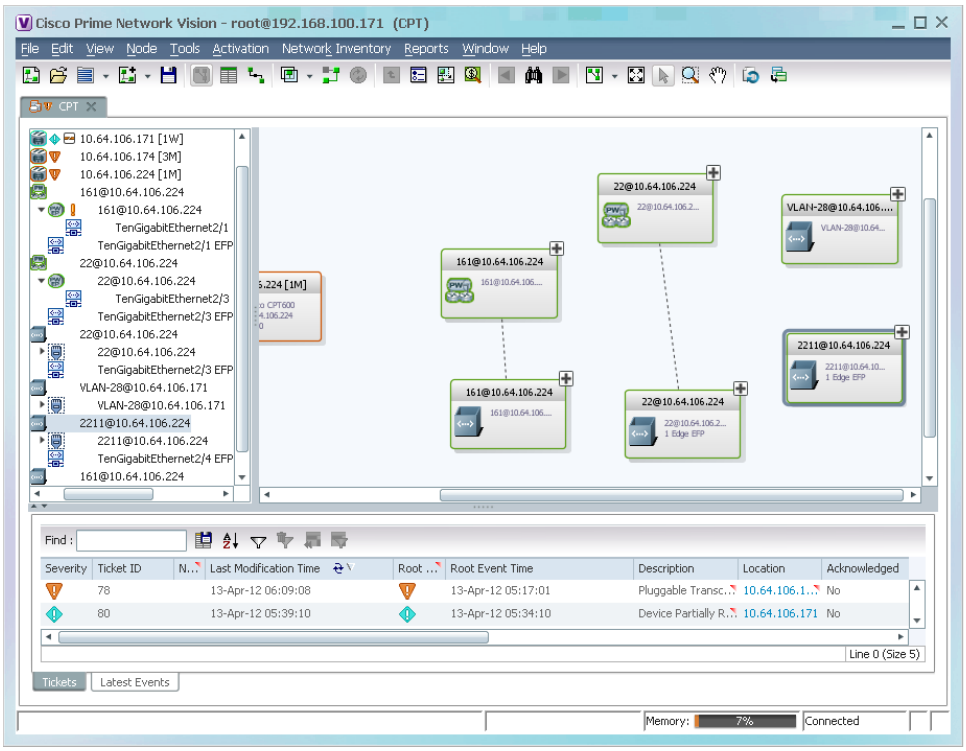
For information about sorting and filtering the table contents, see Filtering and Sorting Tabular Content, page 2-40.

**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 13-67.

***Figure 13-67 Ethernet Service in Prime Network Vision***




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

# Applying Ethernet Service Overlays

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

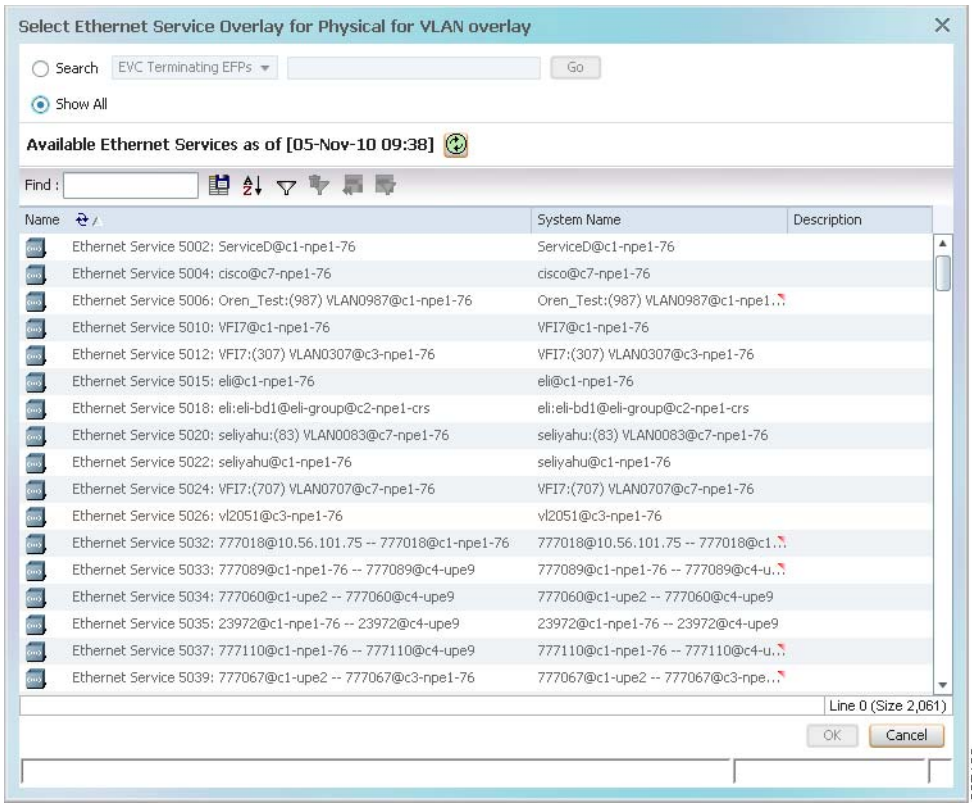
To apply an Ethernet service overlay:

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

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

Figure 13-68 shows an example of the Select Ethernet Service Overlay for *map* dialog box.

*Figure 13-68 Select Ethernet Service Overlay Dialog Box*

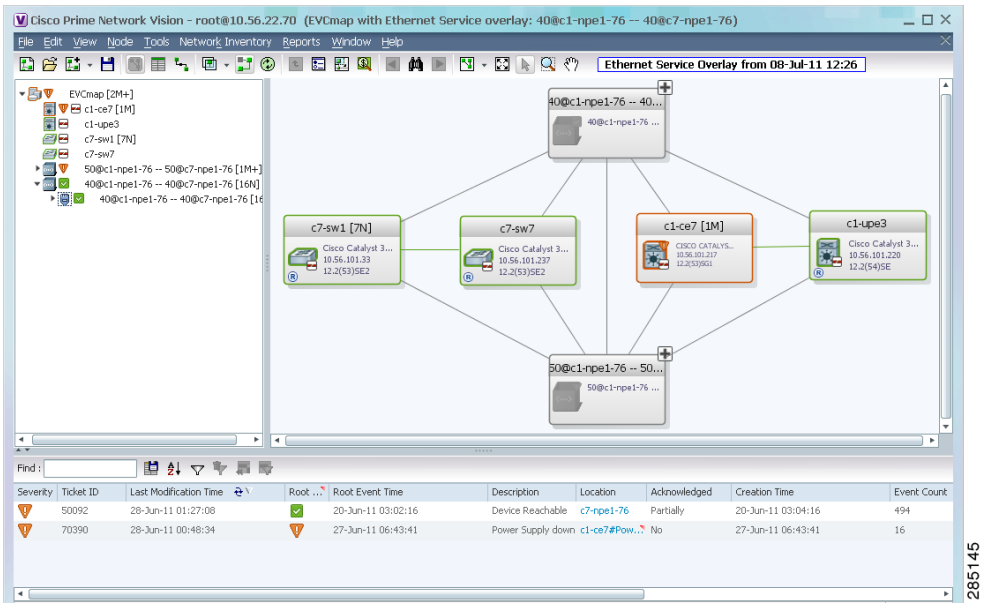



**Step 3** Select the required Ethernet Service for the overlay.

**Step 4** Click **OK**.

The elements being used by the selected Ethernet service are highlighted in the map while the other elements are dimmed, as shown in Figure 13-69.

*Figure 13-69 Ethernet Service Overlay in Prime Network Vision*




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

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

# Viewing Ethernet Service Properties

To view Ethernet service properties:

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

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

Figure 13-70 shows an example of an Ethernet Service Properties window with the EVC Terminating table. Depending on the types of service in the EVC, tabs might be displayed. For example, if the EVC contains two network VLANs and a VPLS, tabs are displayed for the following:

- EVC Terminating table
- Network VLANs
- VPLS

*Figure 13-70 Ethernet Service Properties Window*

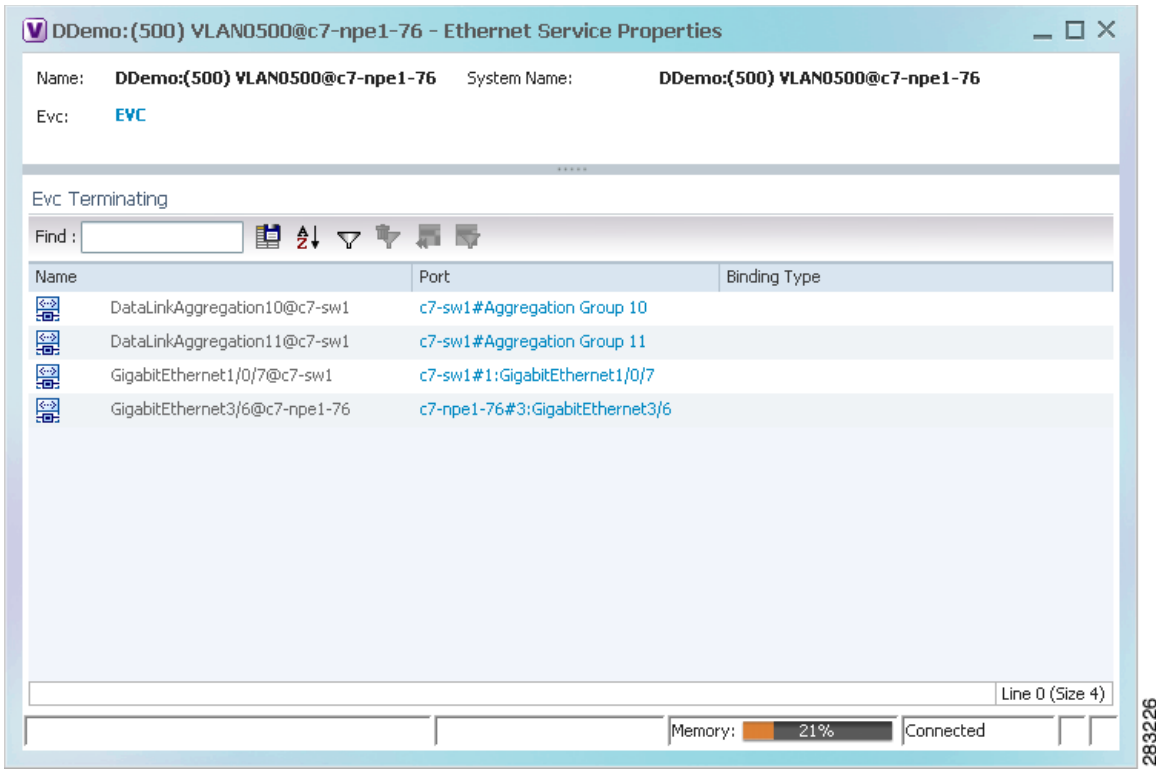



Table 13-44 describes the information that is displayed for an Ethernet service.

*Table 13-44 Ethernet Service Properties Window*

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

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

Figure 13-71 shows an example of the EVC Properties window.

*Figure 13-71 EVC Properties Window*

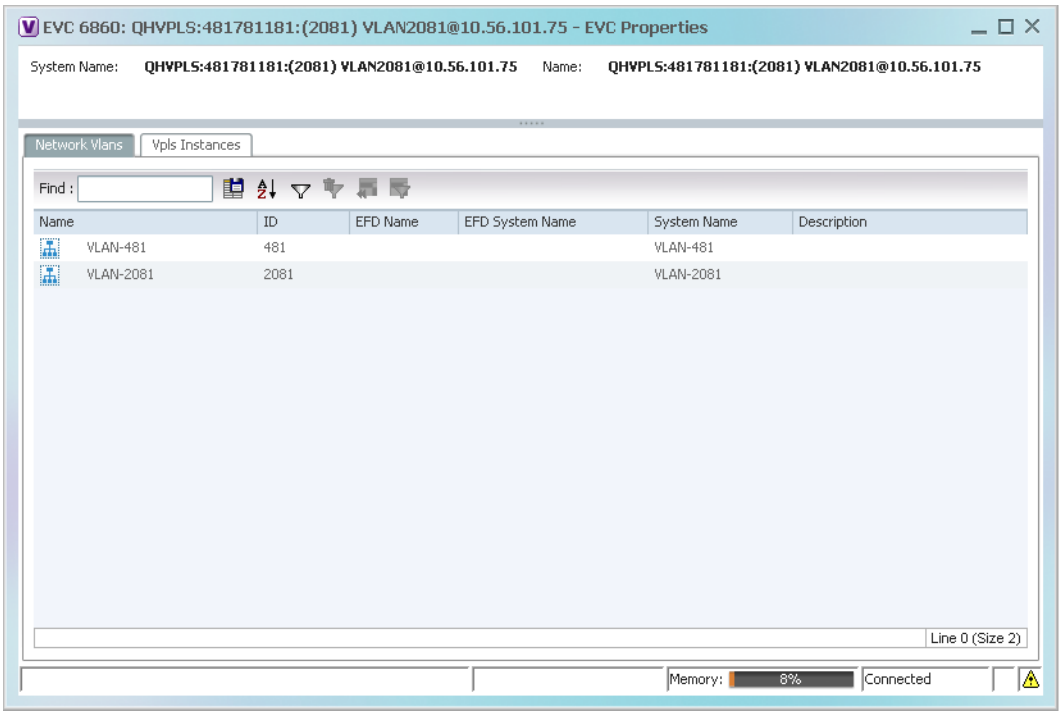



Table 13-45 describes the information that is displayed in the EVC Properties window. The tabs that are displayed depend on the services included in the EVC. For example, if the EVC contains two network VLANs and a VPLS, tabs are displayed for the following:

- EVC Terminating table
- Network VLANs
- VPLS

*Table 13-45 EVC Properties Window*

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

*Table 13-45 EVC Properties Window (continued)*

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

# Viewing IP SLA Responder Service Properties

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

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

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

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

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

To view IP SLA Responder service properties:

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

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

IP SLA Responder properties are displayed as shown in Figure 13-72.

*Figure 13-72 IP SLA Responder in Logical Inventory*

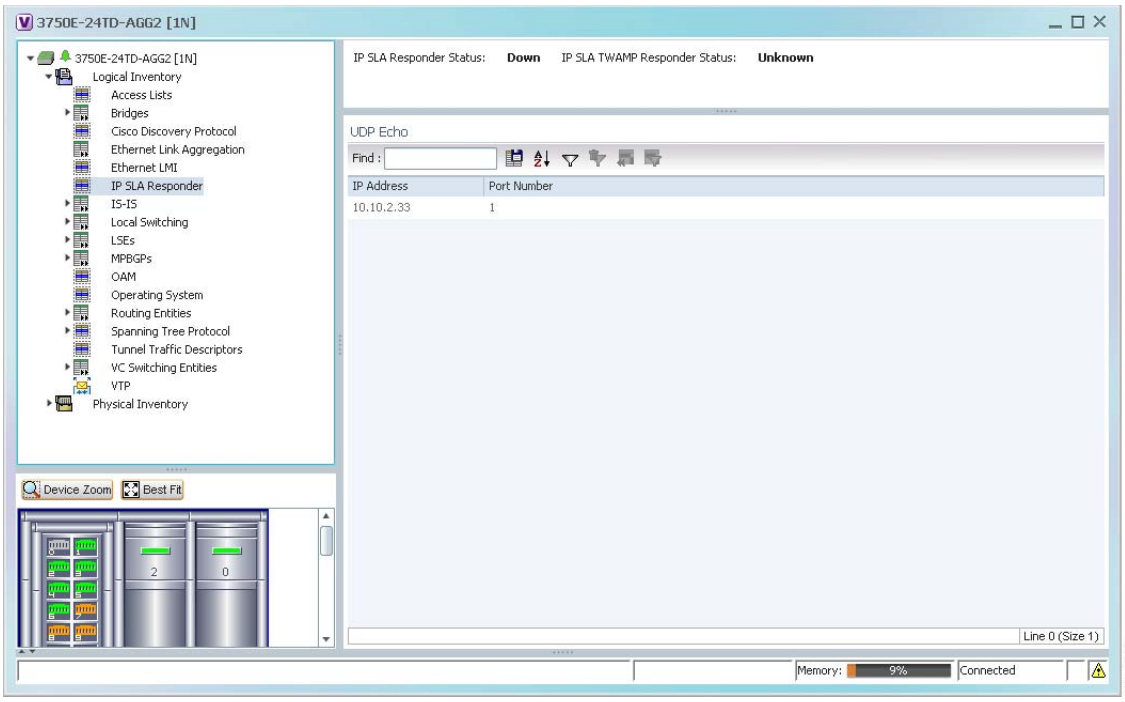



Table 13-46 describes the properties displayed for IP SLA Responder service.

*Table 13-46 IP SLA Responder Properties in Logical Inventory*

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

# Viewing IS-IS Properties

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

IS-IS networks contain end systems, intermediate systems, areas, and domains. End systems are user devices. Intermediate systems are routers. Routers are organized into local groups called areas, and areas are grouped into a domain. For configuring IS-IS, see Configuring IS-IS, page 13-120.

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 13-73 shows an example of the IS-IS window with the Process table in logical inventory.

***Figure 13-73 IS-IS Window in Logical Inventory***

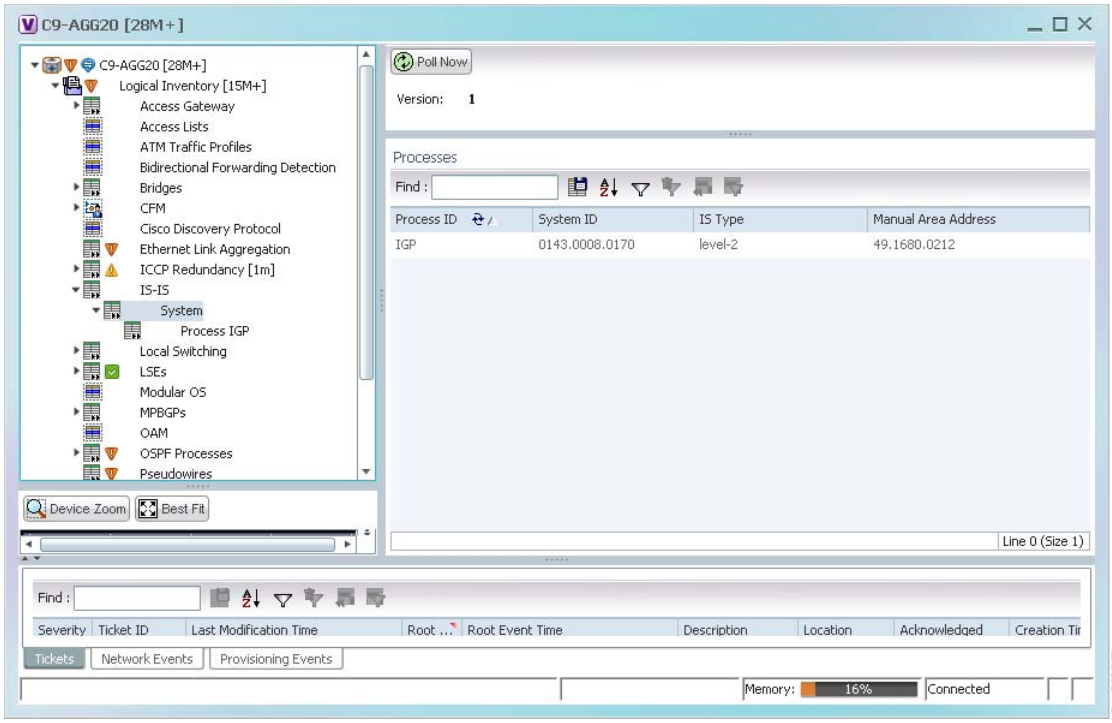


Table 13-47 describes the information that is displayed in this window and the Processes table.

*Table 13-47 IS-IS Properties in Logical Inventory - Processes Table*

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

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

Figure 13-74 shows an example of the information that is displayed for the IS-IS process.

*Figure 13-74 IS-IS Process Properties in Logical Inventory*

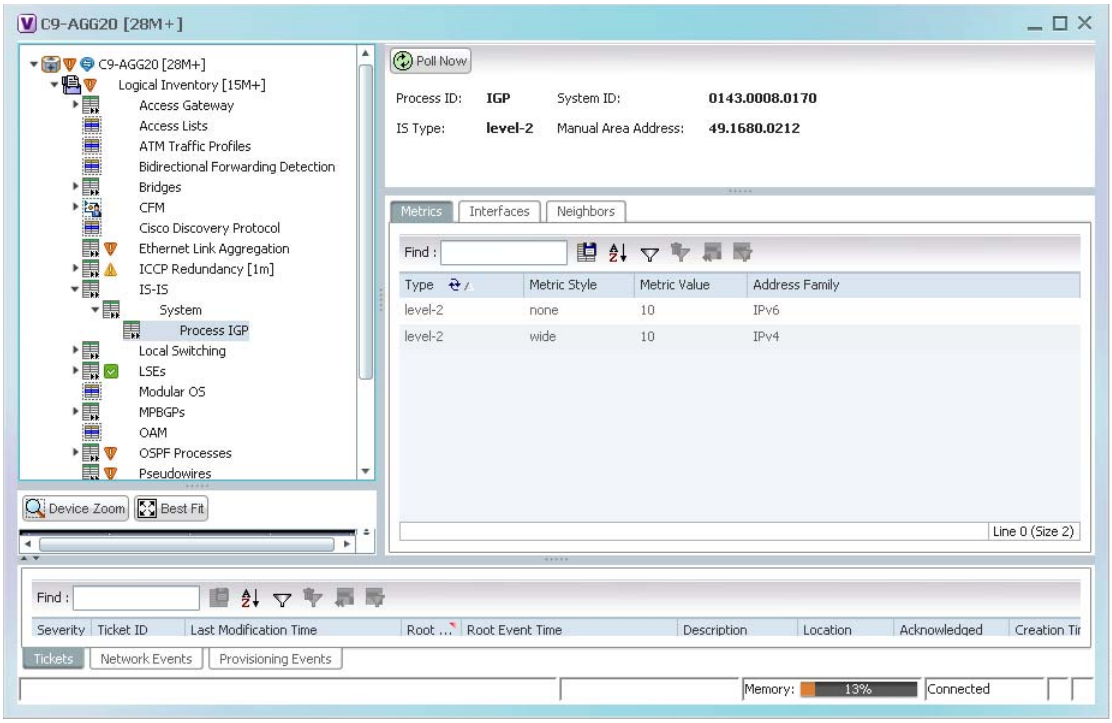


Table 13-48 describes the information that is displayed for the selected IS-IS process.

*Table 13-48 IS-IS Process Properties in Logical Inventory*

| Field | Description |
|---|---|
| Process | Unique identifier for the IS-IS process. |
| System ID | Identifier for this Intermediate System. |
| IS Type | Level at which the Intermediate System process is running: Level 1, Level 2, or Level 1-2. |
| Manual Area Address | Address assigned to the area. |
| **Metrics Tab** | |
| IS Type | Level at which the Intermediate System is running: Level 1, Level 2, or Level 1-2. |
| Metric Style | Metric style used: Narrow, Transient, or Wide. |
| Metric Value | Metric value assigned to the link. This value is used to calculate the path cost via the links to destinations. This value is available for Level 1 or Level 2 routing only.<br>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.<br>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 13-75, the entry in the navigation tree is OSPF Process (v2) 10.

***Figure 13-75 OSPF Processes in Logical Inventory***

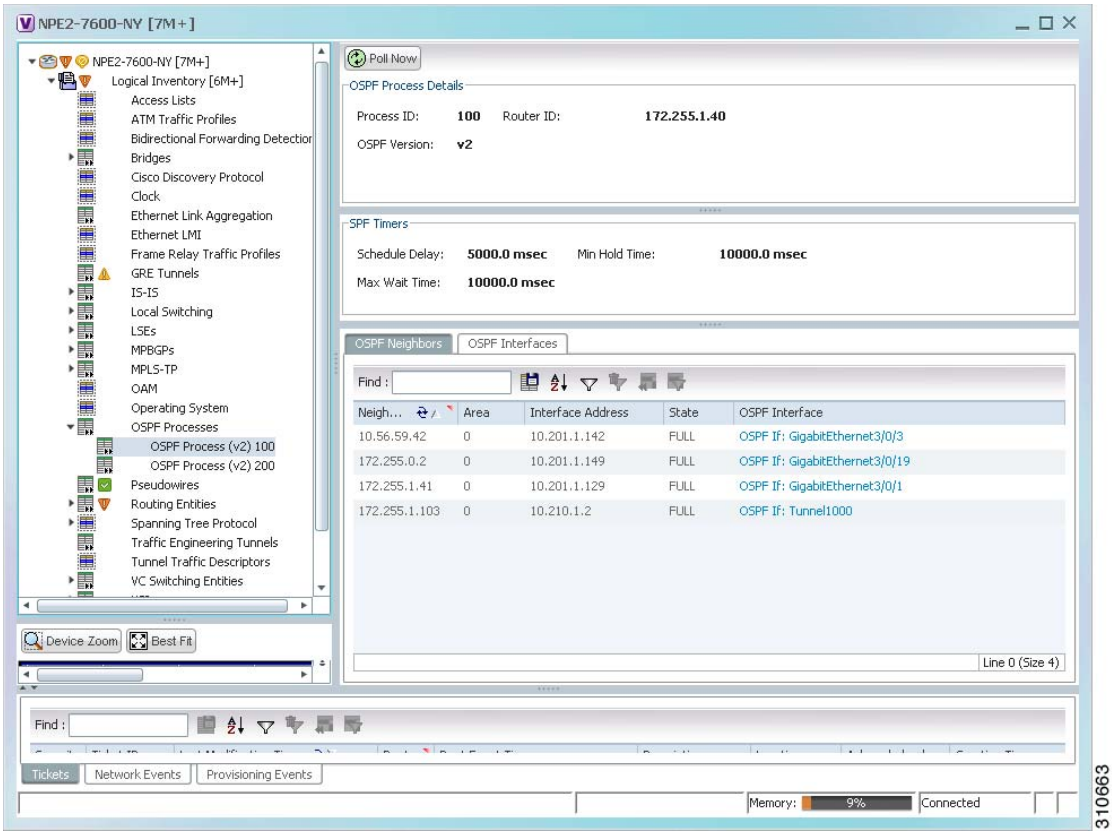



Table 13-49 describes the information that is displayed for OSPF processes.

*Table 13-49 OSPF Processes in Logical Inventory*

| Field | Description |
|---|---|
| **OSPF Process Details** | |
| Process ID | Unique process identifier. |
| Router ID | Router IP address. |
| OSPF Version | OSPF version: v1, v2, or v3. |
| **SPF Timers** | |
| Schedule Delay | Number of milliseconds to wait after a change before calculating the shortest path first (SPF). |
| Min Hold Time | Minimum number of milliseconds to wait between two consecutive SPF calculations. |
| Max Wait Time | Maximum number of milliseconds to wait between two consecutive SPF calculations. |
| **OSPF Neighbors Table** | |
| Neighbor ID | OSPF neighbor IP address. |
| Area | OSPF area identifier. |
| Interface Address | IP address of the interface on the neighbor configured for OSPF. |
| State | State of the communication with the neighbor: Down, Attempt, Init, 2-Way, Exstart, Exchange, Loading, and Full. |
| OSPF Interface | Hyperlinked entry to the OSPF Interface Properties window.<br>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.<br>For more information about the IP Interfaces table, see Table 19-12. |
| Internet Address | OSPF interface IP address. |
| Area ID | OSPF area identifier. |
| Priority | Eight-bit unsigned integer that specifies the priority of the interface. Values range from 0 to 255. Of two routers, the one with the higher priority takes precedence. |
| Cost | Specified cost of sending a packet on the interface, expressed as a metric. Values range from 1 to 65535. |
| Status | State of the interface: Up or Down. |
| State | OSPF state: BDR, DR, DR-Other, Waiting, Point-to-Point, or Point-to-Multipoint. |
| Network Type | Type of OSPF network: Broadcast, Nonbroadcast Multiple Access (NBMA), Point-to-Multipoint, Point-to-Point, or Loopback. |
| DR Address | Designated router IP address. |
| BDR Address | Backup designated router IP address. |

# Configuring REP and mLACP

The following commands can be launched from the inventory by right-clicking the appropriate node and selecting **Commands.** Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. For details on the software versions Prime Network supports for these network elements, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*. To run the REP and mLACP commands, the software on the network element must support these technology.

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

| Command | Navigation | Description | Supported on: |
|---|---|---|---|
| **REP Command** | | | |
| **Show REP Segment Information** | **Commands > Show** | This action performed at the command the launch point. | • Cisco 7600 Series Routers<br>• Cisco MWR 2941 Mobile Wireless Routers<br>• Cisco ME 3600X and Cisco ME 3800X Carrier Ethernet Switches<br>• Cisco Catalyst 3750 Metro Series Switches<br>• Cisco ME 6524 Ethernet Switch<br>• Cisco Carrier Packet Transport (CPT) System<br>• All Cisco Catalyst Switches |
| **mLACP Commands** | | | |
| **Show Group**<br>**Show MPLS LDP**<br>**Show Channel**<br>**Show LACP Internal** | **Commands > Show** | These actions are performed at the command the launch point. | • Cisco 7600 series devices<br>• Cisco 6509 NEB-A series devices<br>• Cisco ASR 9000 series routers. |

# Using Pseudowire Ping and Show Commands

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

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

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

# Configuring IS-IS

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

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

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

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

The table below lists the IS-IS configuration commands and the ISIS supported network elements.

To run the ISIS commands, the software on the network element must support ISIS technology. For details on the software versions Prime Network supports for the ISIS supported network elements, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

| Command | Navigation | Description | Supported on: |
|---|---|---|---|
| **Create ISIS Router** | **ISIS** > *right-click System* > **Commands** > **Configuration** | Use this command to create an IS-IS routing process and specify the area for each instance of the IS-IS routing process. An appropriate Network Entity Title (NET) must be configured to specify the area address for the IS-IS area and system ID of the router.<br>Multiple IS-IS processes can be configured. Up to eight processes are configurable. A maximum of five IS-IS instances on a system are supported. | • Cisco ASR 9000 series routers.<br>• Cisco ASR 901 Series Routers<br>• Cisco ASR903 Series Routers |
| **Modify ISIS Router**<br>**Delete ISIS Router** | **ISIS > System >** *right-click Process ID in content pane* **> Commands > Configuration >** | Use this command to modify or delete an exisiting IS-IS routing configuration for the specified routing process. | |

| Command | Navigation | Description | Supported on: |
|---|---|---|---|
| **Create ISIS Interface** | **ISIS > System >** *right-click Process ID in content pane* **> Commands > Configuration >** | Use these command to create or modify an IS-IS routing process and assign it to a specific interface, rather than to a network. | • Cisco ASR 9000 series routers.<br>• Cisco ASR 901 Series Routers<br>• Cisco ASR903 Series Routers |
| **Modify ISIS Interface**<br>**Delete ISIS Interface** | **ISIS >** *expand* **System >** *select a Process* **>** *select* **Interfaces** *tab***>** *right-click on a Interface Name* **> Commands > Configuration >** | | |
| **Create ISIS Address Family**<br>**Modify ISIS Address Family**<br>**Delete ISIS Address Family** | **ISIS > System >** *right-click Process ID in content pane* **> Commands > Configuration** | Configure or modify IS-IS routing to use standard IP Version 4 (IPv4) and IP Version 6 (IPv6) address prefixes. | |
| **Create ISIS Interface Address Family**<br>**Modify ISIS Interface Address Family**<br>**Delete ISIS Interface Address Family** | **ISIS >** expand **System >** *select a Process* **>** *select* **Interfaces** *tab***>** *right-click on a Interface Name* **> Commands > Configuration >** | Configure IS-IS routing to use standard IP Version 4 (IPv4) and IP Version 6 (IPv6) address prefixes on an interface. | Cisco ASR 9000 series routers. |
| **Show ISIS Configuration** | **ISIS >** *right-click* **System > Commands > Show** | The **show isis** command displays general information about an IS-IS instance and protocol operation. | • Cisco ASR 9000 series routers.<br>• Cisco ASR 901 Series Routers<br>• Cisco ASR903 Series Routers |

CHAPTER 14

# Monitoring Carrier Grade NAT Properties

Carrier Grade NAT is a large-scale Network Address Translation (NAT) that provides translation of millions of private IPv4 addresses to public IPv4 addresses. These translations support subscribers and content providers with a bandwidth throughput of at least 10 Gbps full-duplex.

Carrier Grade NAT addresses the IPv4 address completion problem. It employs Network Address and Port Translation (NAPT) to aggregate many private IPv4 addresses into fewer public IPv4 addresses. For example, a single public IPv4 address with a pool of 32,000 port numbers supports 320 individual private IP subscribers, assuming that each subscriber requires 100 ports. Carrier Grade NAT also offers a way to implement a graceful transition to IPv6 addresses.

Carrier Grade NAT attributes and instances are configured as a CRS-ADVSVC-PLIM card on Cisco CRS-1 routers. To route internal public addresses to external public addresses, a VPN Routing and Forwarding (VRF) instance is created. Interfaces are created for the VRF at the subscriber-side (private) and the Internet-side (public). The VRF enables static or dynamic routing of protocols on the interfaces.

Cisco Prime Network supports the following instances for Carrier Grade NAT:

- Stateful Address Translation- NAT44 Stateful
- Stateless Address Translation- NAT 64 Stateless (X-LAT)
- IPv6 rapid deployment (6rd)

Each Carrier Grade NAT instance has several attributes listed under them, such as preferred location, address pools, associated interfaces, and statistics. The attributes are grouped under related categories. The categories and attributes are listed below:

**Note** IPv4 Network Address Translation (NAT44) is not supported for devices running Cisco IOS XR software version 4.0.

The following topics describe how to use Prime Network Vision to view Carrier Grade NAT properties:


- User Roles Required to View Carrier Grade NAT Properties, page 14-2
- Viewing Carrier Grade NAT Properties in Logical Inventory, page 14-2
- Viewing Carrier Grade NAT Properties in Physical Inventory, page 14-5
- Configuring CG NAT Service, page 14-6

# 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 3.10 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 3.10 Administrator Guide*.

***Table 14-1 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 |
| Using CG NAT Configure, Delete, and Show Commands | — | — | — | X | X |

***Table 14-2 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 |
| Using CG NAT Configure, Delete, and Show Commands | — | — | — | 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 14-1.

***Figure 14-1 Carrier Grade NAT in Logical Inventory***

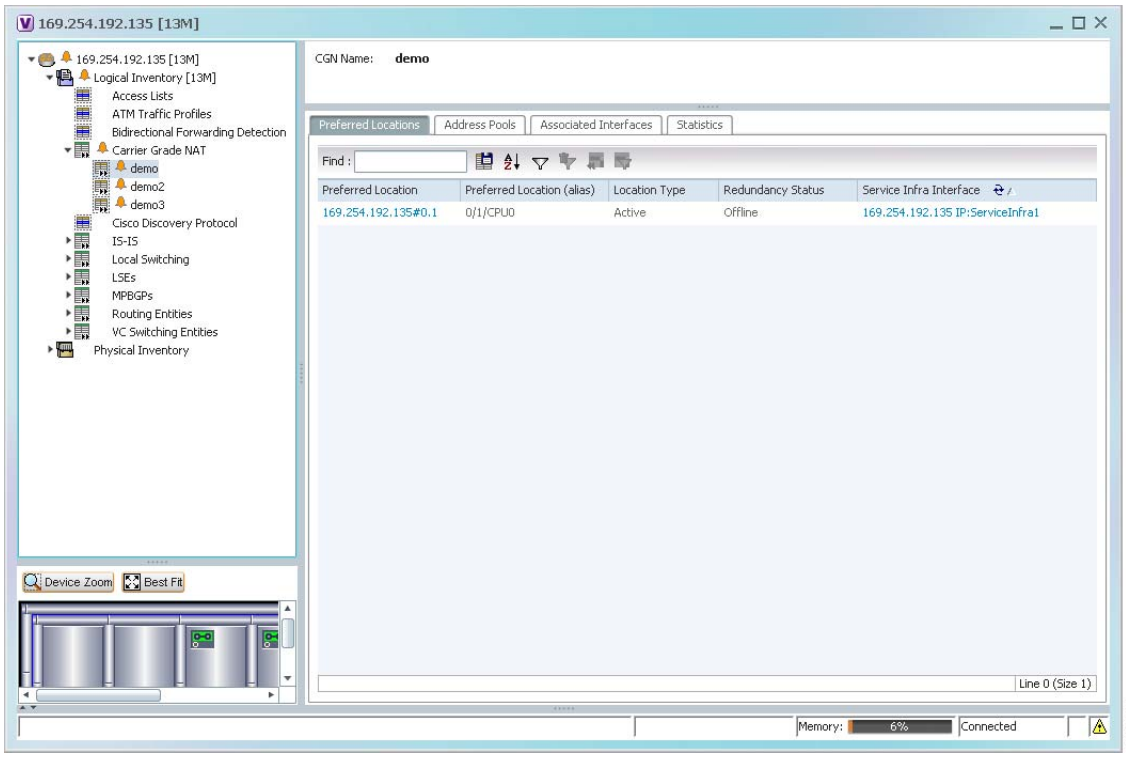



Table 14-3 describes the Carrier Grade NAT properties that are displayed.

***Table 14-3 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.<br>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.<br>For more information about routing entities in logical inventory, see Viewing Routing Entities, page 19-31. |

*Table 14-3 Carrier Grade NAT Properties in Logical Inventory (continued)*

| Field | Description |
|---|---|
| **Address Pools Tab** | |
| Inside VRF | Hyperlinked entry to the inside VRF in logical inventory.<br>For more information about VRF properties in logical inventory, see Viewing VRF Properties, page 19-27. |
| Address Family | Type of IP address in this pool: IPv4 or IPv6. |
| Outside VRF | Hyperlinked entry to the outside VRF in logical inventory.<br>For more information about VRF properties in logical inventory, see Viewing VRF Properties, page 19-27. |
| 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:<br>• For SVI service interfaces, hyperlinked entry to the routing entity in logical inventory.<br>• 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.<br>For statistic names and descriptions, see Table 14-4. |
| Statistics Value | Value of the statistic. |

You can also display pool utilization by right-clicking a VNE and choosing **Commands > Show > Pool Utilization.**

*Table 14-4 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:

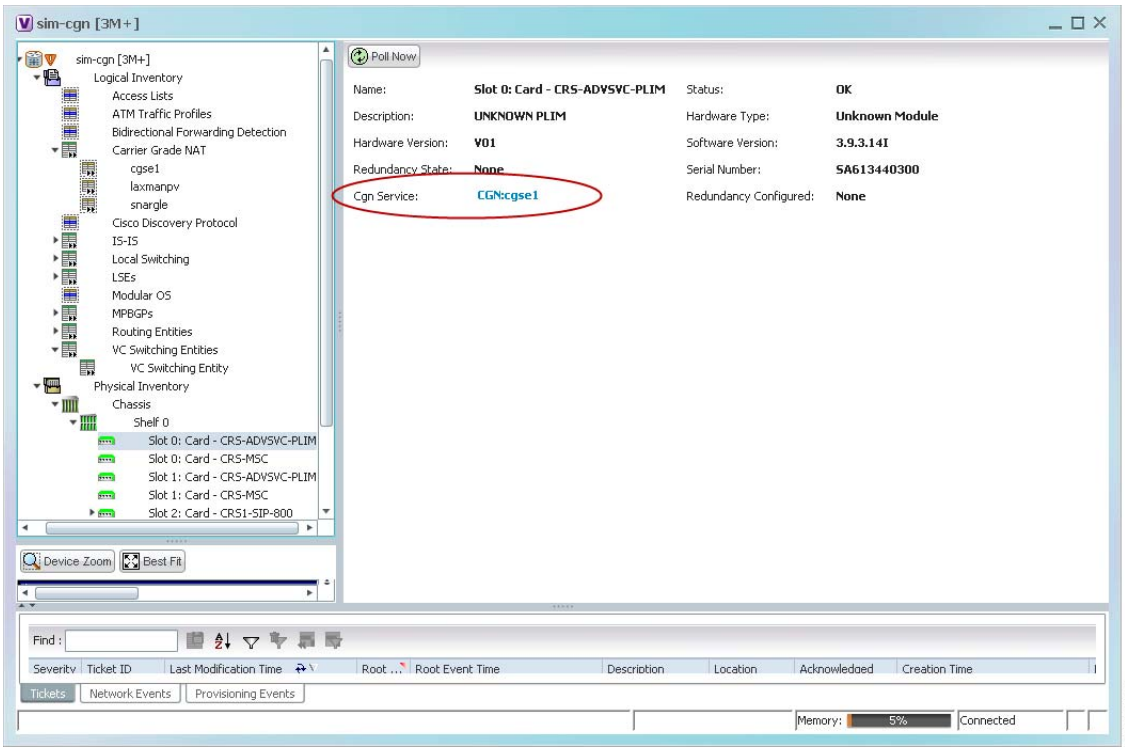
**Step 1** In Prime Network Vision, double-click the Cisco CRS device configured for Carrier Grade NAT.

**Step 2** To view Carrier Grade NAT properties configured on a specific interface, click **Physical Inventory > *chassis*** > *shelf* > *slot* > *card* > *interface*. See Table 3-11 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 14-2 shows an example of Carrier Grade NAT properties in physical inventory.

*Figure 14-2 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.

# Configuring CG NAT Service

The following commands can be launched from the inventory by right-clicking the appropriate node and selecting **Commands.**

The table below lists the configuration commands and the supported network elements. Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands.

For details on the software versions Prime Network supports for thes supported network elements, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*. To run the Carrier Grade NAT commands, the software on the network element must support the Carrier Grade NAT technology.

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

| Command | Navigation | Description | Supported on: |
|---|---|---|---|
| **Add Static Port Forwarding** | **Configure >** | To configure CG NAT service instance for static port forwarding. | Cisco CRS Series Routers including both the CRS-1 and CRS-3 Series Routers. |
| **Add NAT 64 Forwarding** | **Configure >** | To configure CG NAT service instance for NAT 64. | |
| **Add 6rd Forwarding** | **Configure >** | To configure CG NAT service instance for 6rd. | |
| **Static Port Forwarding** | **Delete >** | Click **Execute Now** to remove CG NAT instance. | |
| **Pool Utilization** | **Show >** | Display the CGN instance name, inside VRF name, start and end address | |

CHAPTER 15

# Monitoring DWDM Properties

The Cisco IP over dense wavelength division multiplexing (IPoDWDM) solution enables the convergence of the IP and DWDM core networks of the service providers. It increases service flexibility, operational efficiency and reliability while lowering operating expenses (OpEx) and capital expenditures (CapEx).

Cisco Prime Network discovers and displays the following DWDM attributes in the Physical Inventory tree of the Cisco Prime Network Vision:

- DWDM controllers. The controller location is same as the DWDM interface.
- Loopback information for the DWDM controller.
- DWDM controller status.
- DWDM port properties—Wavelength, Laser Status, Tx Power, and Rx Power.
- DWDM controller card status (G.709 status).

Prime Network also provides commands that support DWDM and Synchronous Optical Network (SONET) controllers. These commands help in configuring the device and in displaying device details. The commands are described in Configuring and Viewing DWDM, page 15-15. (For information on the SONET commands, see Configuring Clock, page 21-56.)

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 15-1
- Viewing DWDM in Physical Inventory, page 15-3
- Viewing G.709 Properties, page 15-5
- Viewing Performance Monitoring Configuration, page 15-11
- Configuring and Viewing DWDM, page 15-15


# 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 3.10 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 3.10 Administrator Guide*.

***Table 15-1 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 |
| Using IPoDWDM Configuration and Show Commands | — | — | — | X | X |

***Table 15-2 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 |
| Using IPoDWDM Configuration and Show Commands | — | — | — | 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 15-1.

***Figure 15-1 DWDM Properties in Physical Inventory***

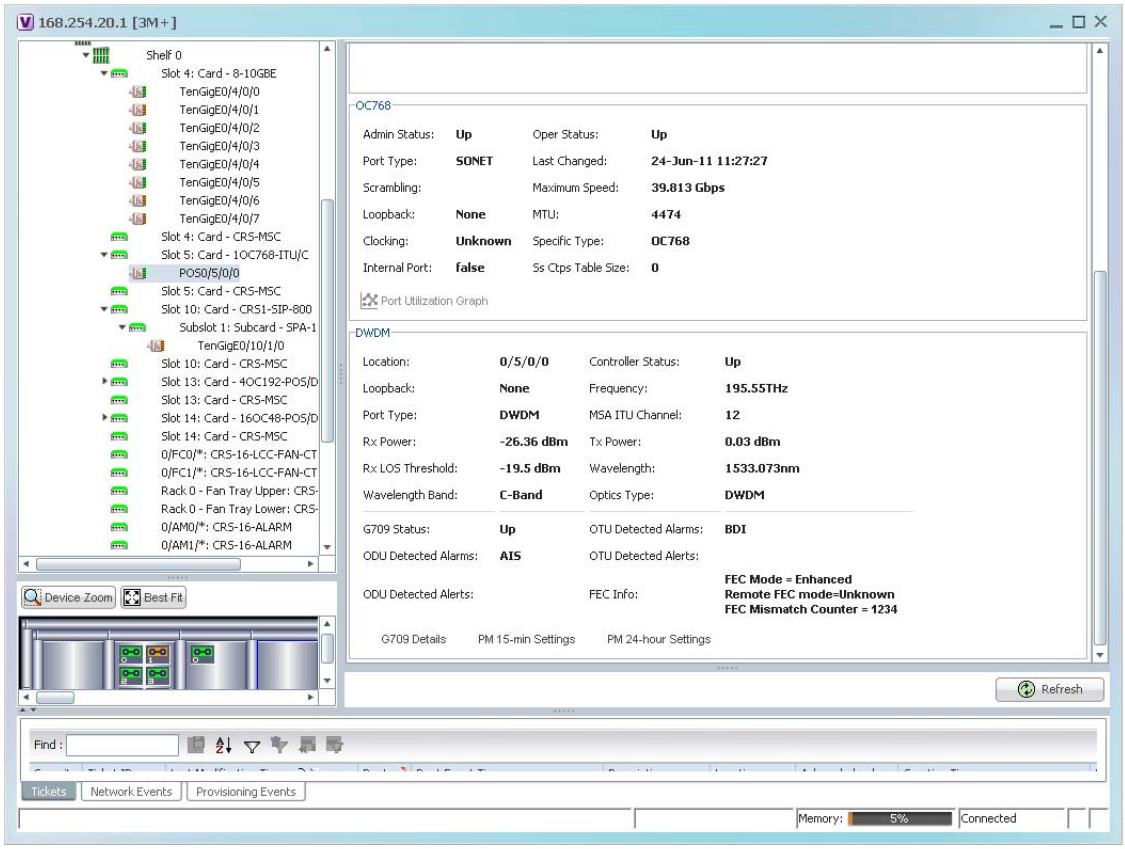


Table 15-3 describes the information displayed for DWDM.

***Table 15-3 DWDM Properties in Physical Inventory***

| Field | Description |
|---|---|
| Location | Physical interface using the format *rack*/*slot*/*module*/*port* where:<br>• *rack* is the chassis number of the rack.<br>• *slot* is the physical slot number of the line card.<br>• *module* is the module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number.<br>• *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. |
| 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:<br>• FEC mode of the controller: Disabled, Enhanced, Standard, or Unknown.<br>• FEC mode on the remote device: Disabled, Enhanced, Standard, or Unknown.<br>• 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 15-5. |

*Table 15-3 DWDM Properties in Physical Inventory (continued)*

| Field | Description |
|---|---|
| PM 15-min Settings | Click to view 15-minute performance monitoring properties. For more information, see Viewing Performance Monitoring Configuration, page 15-11. |
| PM 24-hour Settings | Click to view 24-hour performance monitoring properties. For more information, see Viewing Performance Monitoring Configuration, page 15-11. |

# 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 15-2 for all Cisco devices except the Cisco 7600 series devices.

*Figure 15-2 DWDM G709 Properties Window*

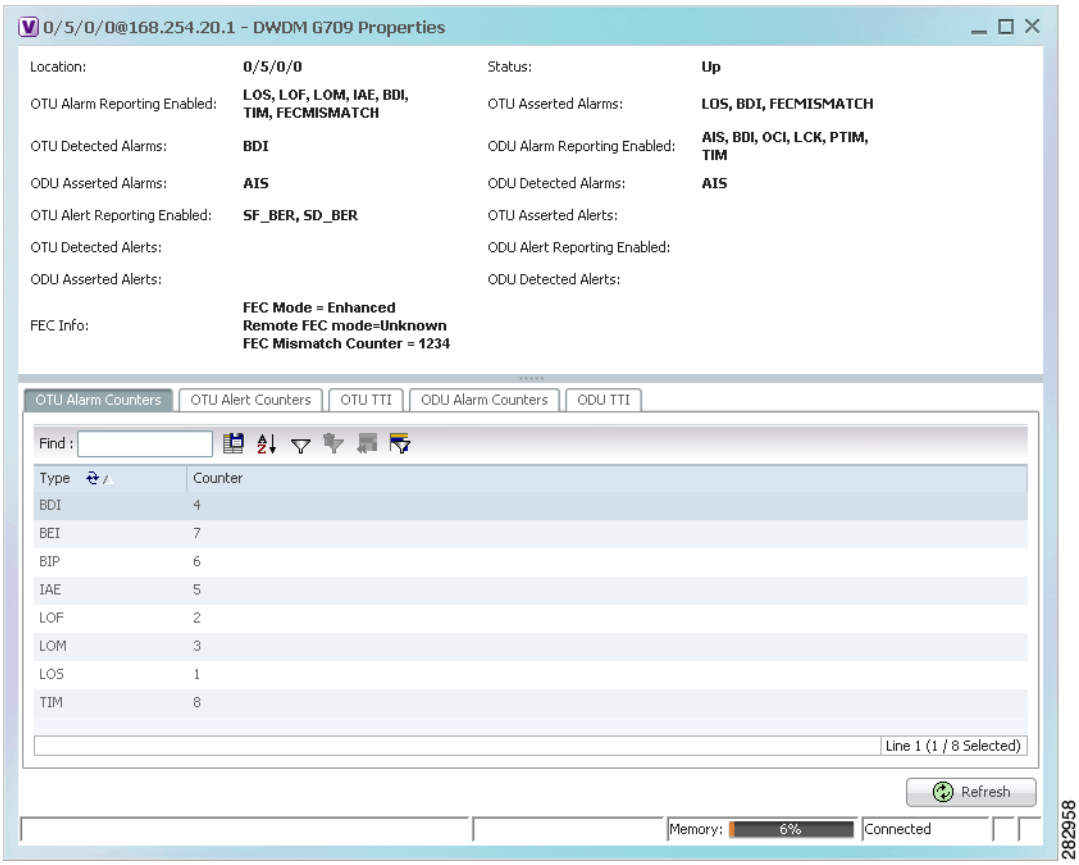



Figure 15-3 shows the tabs that are displayed in the G709 Info Properties window for Cisco 7600 series devices. For Cisco 7600 series devices:

- The ODU Alert Counters tab is displayed.
- The ODU TTI and OTU TTI tabs are not displayed.

*Figure 15-3 DWDM G709 Properties Window for Cisco 7600 Series Devices*

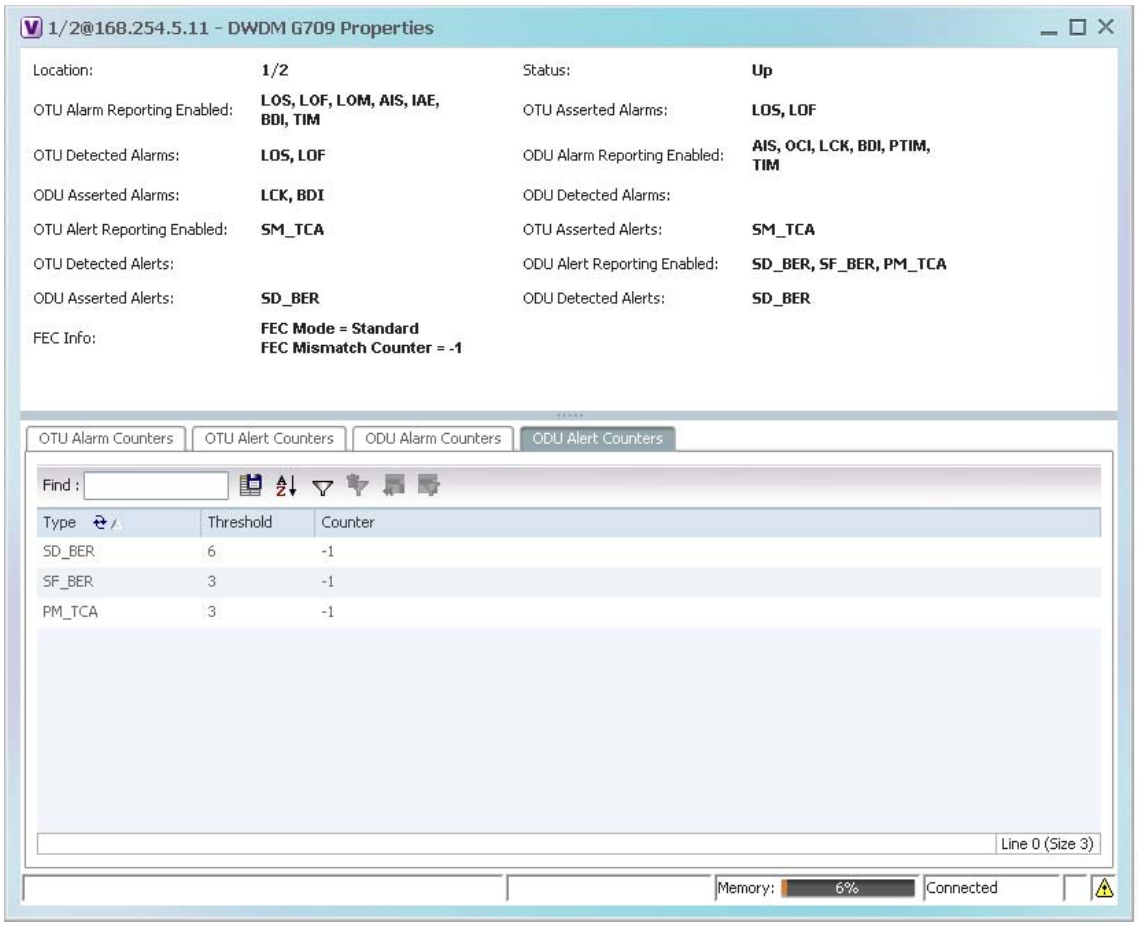



Table 15-4 describes the fields that are displayed above the tabs in the G709 Info Properties window.

*Table 15-4 DWDM G709 Properties Window*

| Field | Description |
|---|---|
| Location | Physical interface using the format *rack*/*slot*/*module*/*port* where:<br>• *rack* is the chassis number of the rack.<br>• *slot* is the physical slot number of the line card.<br>• *module* is the module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number.<br>• *port* is the physical port number of the interface. |

*Table 15-4 DWDM G709 Properties Window (continued)*

| Field | Description |
|---|---|
| **OTU Alarms** | |
| OTU Alarm Reporting Enabled for | The types of alarms enabled for reporting:<br>• AIS—Alarm indication signal (AIS) alarms.<br>• BDI—Backward defect indication (BDI) alarms.<br>• BEI—Backward error indication (BEI) alarms.<br>• BIP—Bit interleaved parity (BIP) alarms.<br>• FECMISMATCH—FEC mismatch alarms.<br>• IAE—Incoming alignment error (IAE) alarms.<br>• LOF—Loss of frame (LOF) alarms.<br>• LOM—Loss of multiple frames (LOM) alarms.<br>• LOS—Loss of signal (LOS) alarms.<br>• 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:<br>• AIS—Incoming SONET AIS error status.<br>• BDI—Path termination BDI error status.<br>• BEI—Backward error indication (BEI) error status.<br>• BIP—Bit interleaved parity (BIP) error status.<br>• LCK—Upstream connection locked (LCK) error status.<br>• OCI—Open connection indication (OCI) error status.<br>• PTIM—Payload TIM error status.<br>• 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 15-4 DWDM G709 Properties Window (continued)*

| Field | Description |
|---|---|
| **OTU Alerts** | |
| OTU Alert Reporting Enabled for | The types of alerts enabled for reporting:<br>• SD-BER—Section Monitoring (SM) bit error rate (BER) is in excess of the signal degradation (SD) BER threshold.<br>• SF-BER—SM BER is in excess of the signal failure (SF) BER threshold.<br>• PM-TCA—Performance monitoring (PM) threshold crossing alert (TCA).<br>• 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:<br>• SD-BER—SM BER is in excess of the SD BER threshold.<br>• SF-BER—SM BER is in excess of the SF BER threshold.<br>• PM-TCA—PM threshold crossing alert.<br>• 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:<br>• FEC mode for the controller—Disable, Enhanced, Standard, or Unknown.<br>• Remote FEC mode—FEC mode on the remote device: Disabled, Enhanced, Standard, or Unknown.<br>• 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 15-10
- OTU Alert Counters Tab, page 15-10
- ODU Alarm Counters Tab, page 15-10
- OTU TTI Tab, page 15-10
- ODU TTI Tab, page 15-10
- ODU Alert Counters Tab, page 15-11

**Step 4** To view additional G.709 properties, click the required tab. Table 15-5 describes the information displayed in each tab.

*Table 15-5 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**<br>This tab is not displayed for Cisco 7600 series devices. | |
| Type | Type of OTU Trail Trace Identifier (TTI) configured:<br>• Expected<br>• Received<br>• Sent |
| String Type | For each TTI type, the type of string:<br>• ASCII<br>• Hexadecimal |
| TTI String | For each TTI type, the specific TTI string configured. |
| **ODU TTI Tab**<br>This tab is not displayed for Cisco 7600 series devices. | |
| Type | Type of ODU TTI configured:<br>• Expected<br>• Received<br>• Sent |
| String Type | For each TTI type, the type of string:<br>• ASCII<br>• Hexadecimal |
| TTI String | For each TTI type, the specific TTI string configured. |

*Table 15-5 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 15-4.

*Figure 15-4 Client DWDM PM Settings Properties Window*

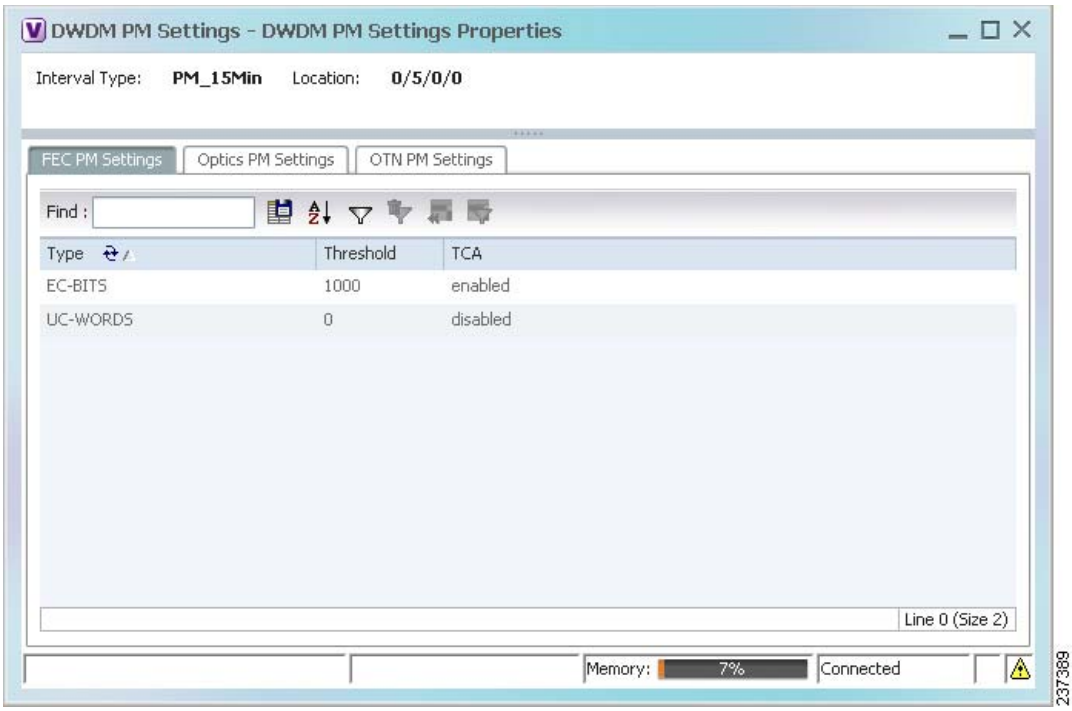



Table 15-6 describes the information displayed above the tabs in the Client DWDM PM Settings Properties window and in each of the tabs.

*Table 15-6 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:<br>• *rack* is the chassis number of the rack.<br>• *slot* is the physical slot number of the line card.<br>• *module* is the module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number.<br>• *port* is the physical port number of the interface. |
| **FEC PM Settings Tab** | |
| Type | FEC performance monitoring parameter being tracked:<br>• EC-BITS—The number of bit errors corrected (EC-BITS) in the DWDM trunk line during the performance monitoring time interval.<br>• 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. |

*Table 15-6 Client DWDM PM Settings Properties Window and Tabs (continued)*

| Field | Description |
|---|---|
| **Optics PM Settings Tab** | |
| Type | Optics performance monitoring parameter being tracked:<br>• LBC—Laser bias current.<br>• OPR—Optical power on the unidirectional port.<br>• 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 15-6 Client DWDM PM Settings Properties Window and Tabs (continued)*

| Field | Description |
|---|---|
| **OTN PM Settings Tab** | |
| Type | OTN performance monitoring parameter being tracked:<br>• 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.<br>• bbe-pm-ne—Near-end path monitoring background block errors (BBE-PM).<br>• 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.<br>• bbe-sm-ne—Near-end section monitoring background block errors (BBE-SM).<br>• 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.<br>• bber-pm-ne—Near-end path monitoring background block errors ratio (BBER-PM).<br>• 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.<br>• bber-sm-ne—Near-end section monitoring background block errors ratio (BBER-SM)<br>• 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.<br>• es-pm-ne—Near-end path monitoring errored seconds (ES-PM).<br>• 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.<br>• es-sm-ne—Near-end section monitoring errored seconds (ES-SM).<br>• 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.<br>• esr-pm-ne—Near-end path monitoring errored seconds ratio (ESR-PM).<br>• 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.<br>• esr-sm-ne—Near-end section monitoring errored seconds ratio (ESR-SM).<br>• 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.<br>• fc-pm-ne—Near-end path monitoring failure counts (FC-PM).<br>• 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.<br>• fc-sm-ne—Near-end section monitoring failure counts (FC-SM). |

*Table 15-6 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.<br>• ses-pm-ne—Far-end path monitoring severely errored seconds (SES-PM).<br>• 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.<br>• ses-sm-ne—Near-end section monitoring severely errored seconds (SES-SM).<br>• 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.<br>• sesr-pm-ne—Near-end path monitoring severely errored seconds ratio (SESR-PM).<br>• 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.<br>• sesr-sm-ne—Near-end section monitoring severely errored seconds ratio (SESR-SM).<br>• 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.<br>• uas-pm-ne—Near-end path monitoring unavailable seconds (UAS-PM).<br>• 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.<br>• 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. |

# Configuring and Viewing DWDM

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

The table below lists the configuration commands and the supported network elements. Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands.

For details on the software versions Prime Network supports for thes supported network elements, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*. To run the Carrier Grade NAT commands, the software on the network element must support the Carrier Grade NAT technology.

To find out if a device supports these commands, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

| Command | Navigation | Input Required and Notes | Supported on: |
|---|---|---|---|
| **Controller Data** | **Show >** | N/A; performed from command launch point | • Cisco 7600 Series Routers<br>• Cisco CRS Carrier Routing System<br>• Cisco CRS series includes Cisco CRS-1 and Cisco CRS-3 Carrier Routing Systems.<br>• Cisco IOS 12000 Series Gigabit Switch Router (GSR) |
| **PM History Data** | | PM interval type: 15-min or 24-hour | |
| | | Interval number | |
| **RTPM Counters** | | PM interval type: 15-min or 24-hour | |
| **RTPM Threshold** | | PM interval type: 15-min or 24-hour | |
| **Wavelength Map** | | N/A; performed from command launch point | |
| **IM Trace Details** | | Card location (for example, 0/5/CPU0) | |
| **Device Log** | | N/A; performed from command launch point | |
| **Counters** | **Clear >** | N/A; performed from command launch point | |
| **Channel** | **Configure >** | Channel number | |
| | | Option: Set or reset channel | |
| **FEC Mode** | | G.709 FEC mode: Disabled, enhanced, or standard | |
| **G.709 ODU** | | ODU alarm type: ais, bdi, lck, oci, ptim, or tim | |
| | | Option: Enable or disable alarm type | |
| **G.709 OTU** | | OTU alarm type: bdi, fecmismatch, iae, lof, lom, los, sd-ber, sf-ber, or tim | |
| | | Option: Enable or disable alarm type | |

| Command | Navigation | Input Required and Notes | Supported on: |
|---|---|---|---|
| **G.709 TTI** | **Configure >** | Optical channel unit type: ODU or OTU | • Cisco 7600 Series Routers<br>• Cisco CRS Carrier Routing System<br>• Cisco CRS series includes Cisco CRS-1 and Cisco CRS-3 Carrier Routing Systems.<br>• Cisco IOS 12000 Series Gigabit Switch Router (GSR) |
| | | TTI type: Expected or sent | |
| | | TTI string type: ASCII or hex | |
| | | TTI string | |
| | | Option: Set or reset TTI string | |
| **G.709 Wrapper** | | Option: Disable or enable G.709 wrapper | |
| **Laser State** | | Laser state: Switch off or on | |
| **Loopback** | | Loopback value: Internal or line | |
| | | Option: Set or remove | |
| **PM FEC Data** | | PM interval type | |
| | | FEC alarm type:<br>• Ec-bits—Bit errors corrected (BIEC); the number of bit errors corrected in the DWDM trunk line during the performance monitoring time interval<br>• Uc-words—Uncorrectable words; the number of uncorrectable words detected in the DWDM trunk line during the performance monitoring time interval | |
| | | TCA options: Enable or disable TCA generation | |
| | | Threshold option. Set configures the value on the device; reset is the default. If you select blank, the threshold value is not used. | |
| | | Threshold value | |

| Command | Navigation | Input Required and Notes | Supported on: |
|---|---|---|---|
| **PM Optics Data** | **Configure >** | PM interval: 15-min or 24-hour | • Cisco 7600 Series Routers<br>• Cisco CRS Carrier Routing System<br>• Cisco CRS series includes Cisco CRS-1 and Cisco CRS-3 Carrier Routing Systems.<br>• Cisco IOS 12000 Series Gigabit Switch Router (GSR) |
| | | Optics alarm type:<br>• lbc—Laser bias current<br>• opr—Optical power on the unidirectional port<br>• opt—Transmit optical power in dBm | |
| | | Maximum TCA option: Enable or disable | |
| | | Maximum threshold option: Choosing Set configures the value on the device; Reset is the default. If you select blank, the threshold value is not used. | |
| | | Maximum threshold | |
| | | Minimum TCA option: enable or disable | |
| | | Minimum threshold option: Choosing Set configures the value on the device; Reset is the default. If you select blank, the threshold value is not used. | |
| | | Minimum threshold | |
| **PM OTN Data** | | PM interval: 15-min or 24-hour | |
| | | OTN alarm type. For a list of types and their descriptions, see the OTN PN Settings Tab information in Table 15-6 on page 15-12. | |
| | | TCA option: Enable or disable | |
| | | Threshold option: Choosing Set configures the value on the device; Reset is the default. If you select blank, the threshold value is not used. | |
| | | Threshold value | |
| **Transmit Power** | | Transmit power in dBm | |
| | | Option: Set or reset transponder Tx threshold | |
| **Rx LOS Threshold** | | Rx LOS threshold value | |
| | | Option: Set or reset transponder Rx threshold | |

CHAPTER 16

# Monitoring 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 16-1
- Ethernet OAM Overview, page 16-2
- Viewing Connectivity Fault Management Properties, page 16-3
- Viewing Ethernet LMI Properties, page 16-10
- Viewing Link OAM Properties, page 16-14
- Configuring CFM, page 16-18
- Configuring E-LMI, page 16-21
- Configuring L-OAM, page 16-22


## 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 3.10 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 3.10 Administrator Guide*.

*Table 16-1 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 |
| Using CFM Configure and Enable Commands | — | — | — | X | X |
| Using E-LMI Configure and Enable Commands | — | — | — | X | X |
| Using L-OAM Configuration, Assign, Enable, and Show Commands | — | — | — | X | X |

*Table 16-2 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 |
| Using CFM Configure and Enable Commands | — | — | — | X | X |
| Using E-LMI Configure and Enable Commands | — | — | — | X | X |
| Using L-OAM Configuration, Assign, Enable, and Show Commands | — | — | — | 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. See Viewing Connectivity Fault Management Properties, page 16-3 and Configuring CFM, page 16-18.

- 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. See Viewing Ethernet LMI Properties, page 16-10 and Configuring E-LMI, page 16-21.
- 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. See Viewing Link OAM Properties, page 16-14 and Configuring L-OAM, page 16-22.

# Viewing Connectivity Fault Management Properties

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        Te0/2/0/3.110        Up MEP 2100 eb:7a:53!
```

CFM uses standard Ethernet frames. CFM frames are distinguishable by EtherType and for multicast messages, by MAC address. CFM frames are sourced, terminated, processed, and relayed by bridges. Routers support only limited CFM functions.

Bridges that cannot interpret CFM messages forward them as normal data frames. All CFM messages are confined to a maintenance domain and to an S-VLAN (PE-VLAN or Provider-VLAN). CFM supports three types of messages:

- Continuity check—Multicast heartbeat messages exchanged periodically among MEPs. They allow MEPs to discover other MEPs within a domain and allow maintenance intermediate points (MIPs) to discover MEPs. Continuity check messages (CCMs) are confined to a domain and S-VLAN.
- Loopback—Unicast frames that a MEP transmits, at the request of an administrator, to verify connectivity to a particular maintenance point. A reply to a loopback message indicates whether a destination is reachable but does not allow hop-by-hop discovery of the path. A loopback message is similar in concept to an Internet Control Message Protocol (ICMP) Echo (ping) message.
- Traceroute—Multicast frames that a MEP transmits, at the request of an administrator, to track the path (hop-by-hop) to a destination MEP. They allow the transmitting node to discover vital connectivity data about the path, and allow the discovery of all MIPs along the path that belong to the same maintenance domain. For each visible MIP, traceroute messages indicate ingress action, relay action, and egress action. Traceroute messages are similar in concept to User Datagram Protocol (UDP) traceroute messages.

From the Logical Inventory tree, you can troubleshoot MEPs using CFM ping, traceroute, MEP status, and MEP cross-check status. These commands, and all CFM commands, are described in Configuring CFM, page 16-18.

Prime Network associates alarms with the corresponding MEP or global CFM logical inventory objects. Prime Network correlates MEP down, MEP up, MEP missing, ETH-AIS, and ETH-RDI events with root cause alarms and corresponding tickets that exist along the path between the MEP on the reporting network element and the network element hosting the remote MEP.

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 16-1 shows an example of CFM in logical inventory.

*Figure 16-1 CFM in Logical Inventory*

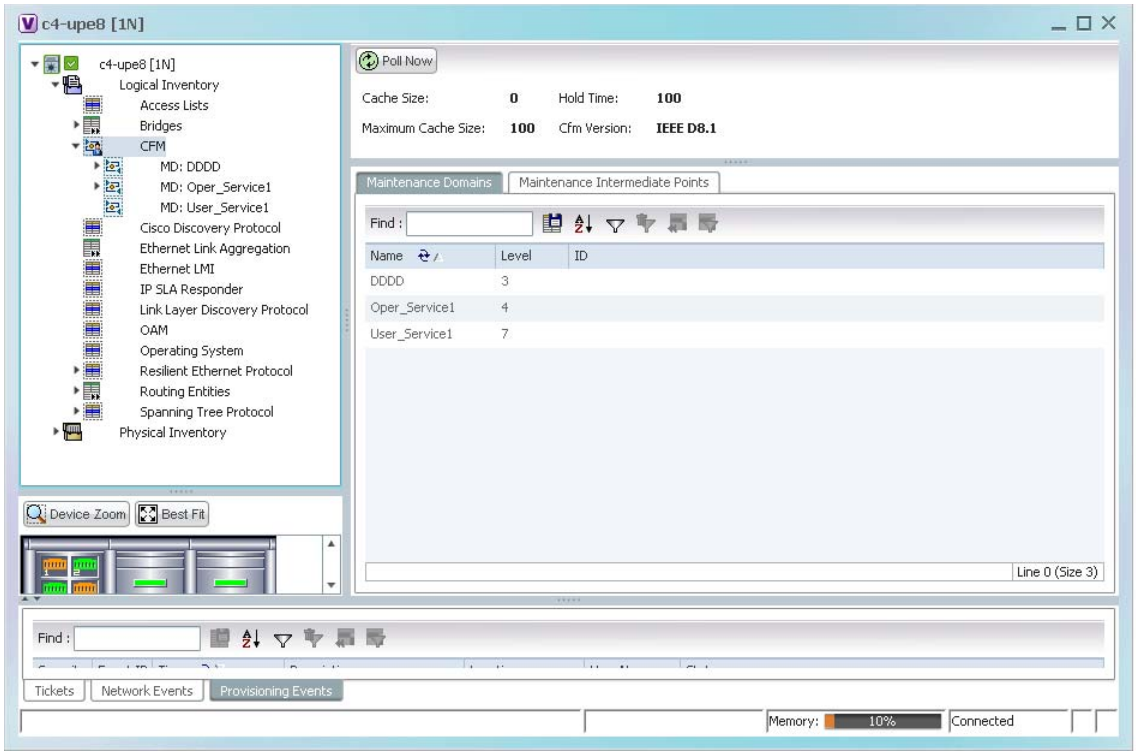



Table 16-3 describes the information displayed for CFM.

*Table 16-3 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 16-2.

*Figure 16-2 CFM Maintenance Intermediate Points Tab*

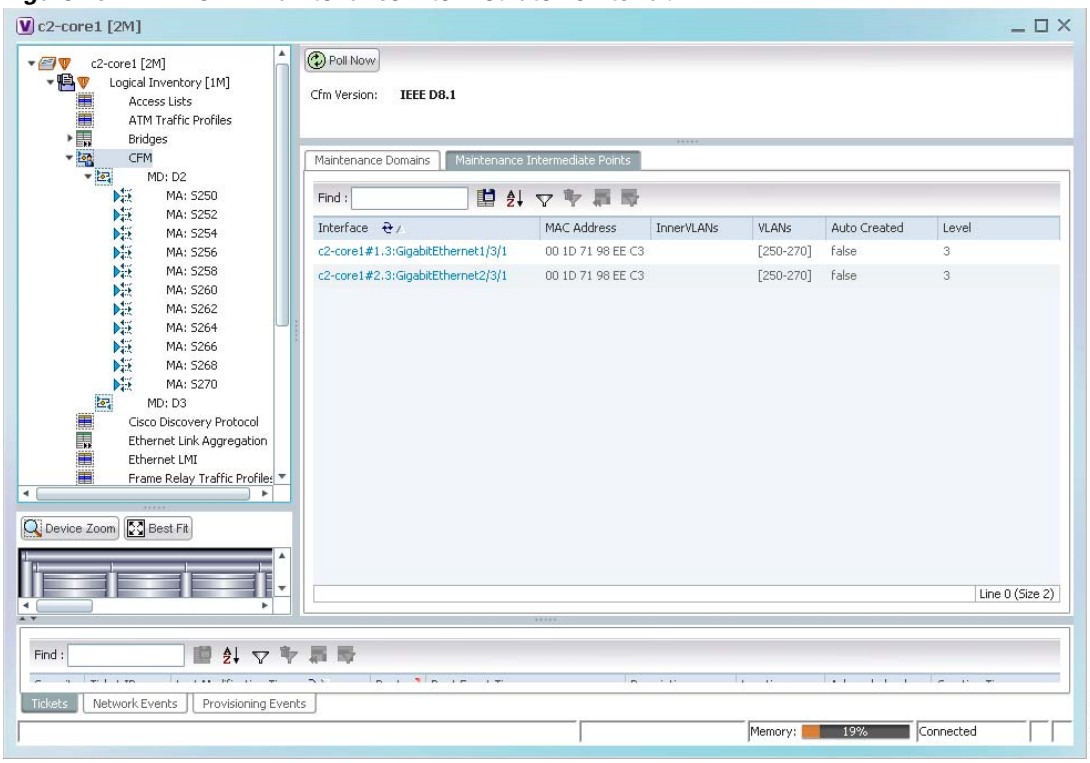



Table 16-4 describes the information that is displayed in the Maintenance Intermediate Points table.

*Table 16-4 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 16-3 shows an example of the information displayed for the maintenance domain.

*Figure 16-3 CFM Maintenance Domain Properties*

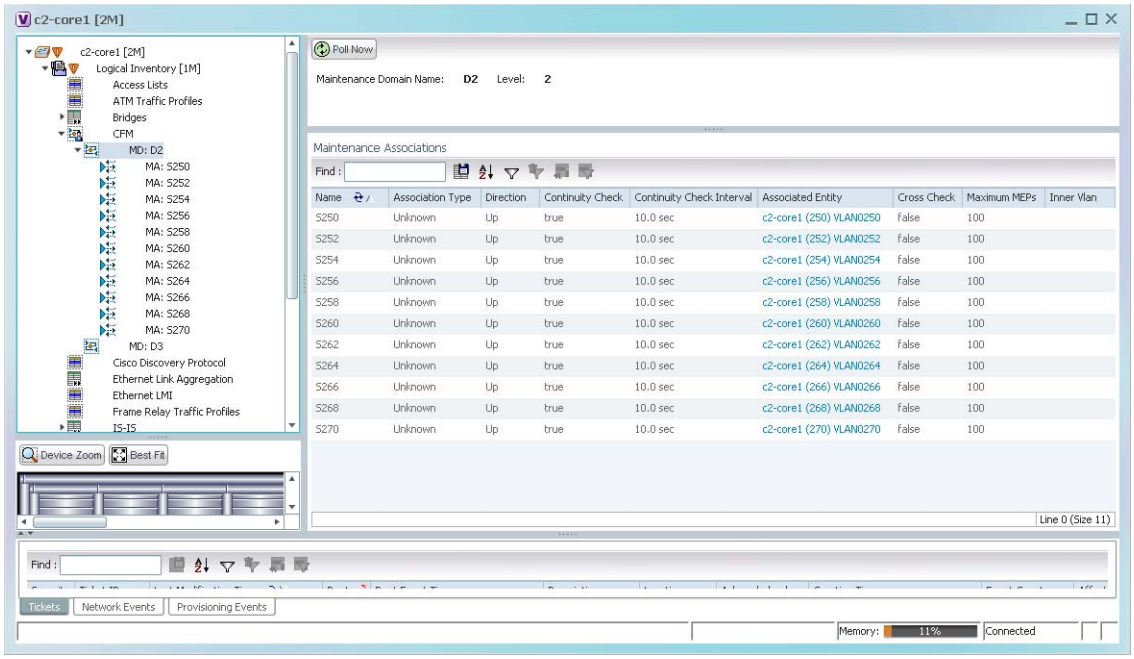



Table 16-5 describes the information that is displayed for CFM maintenance domains.

*Table 16-5 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 16-4 shows the information displayed for the maintenance association endpoints.

***Figure 16-4 CFM Maintenance Association - Endpoint Properties***

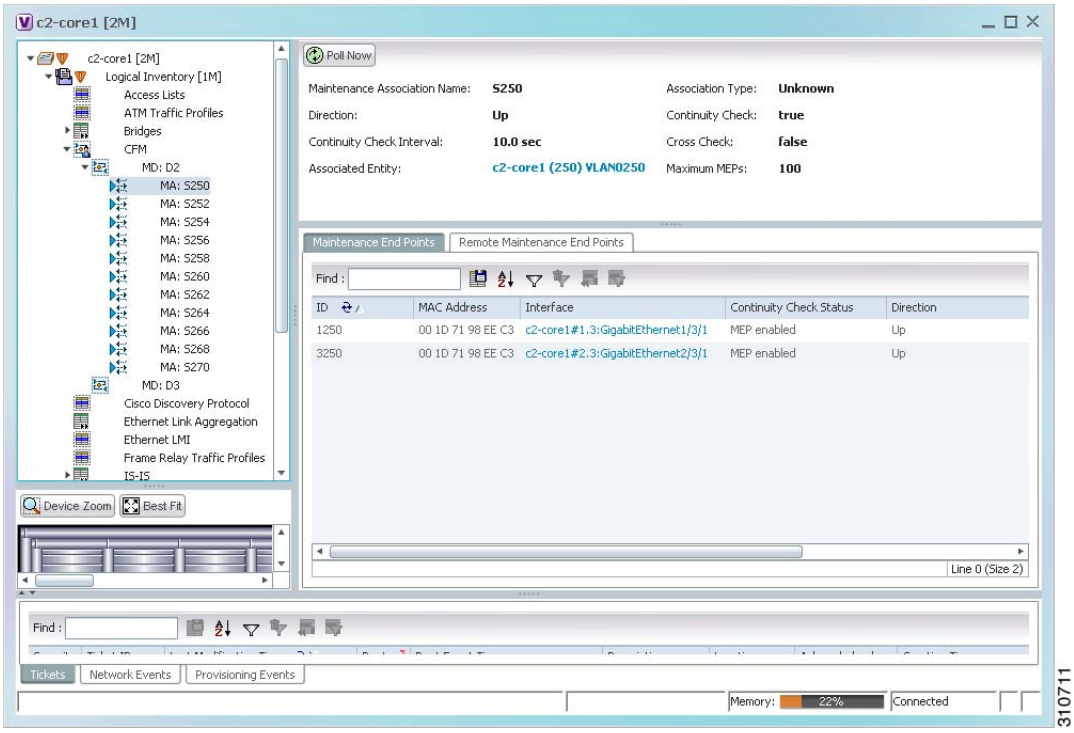



Table 16-6 describes the information that is displayed for CFM maintenance associations and MIPs.

***Table 16-6 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. |
| **Maintenance End Points Table** | |
| ID | Local identifier for the MEP. |
| MAC Address | MAC address that identifies the MEP. |

*Table 16-6 CFM Maintenance Association Properties (continued)*

| Field | Description |
|---|---|
| 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 16-5.

*Figure 16-5 Remote Maintenance End Points Table*

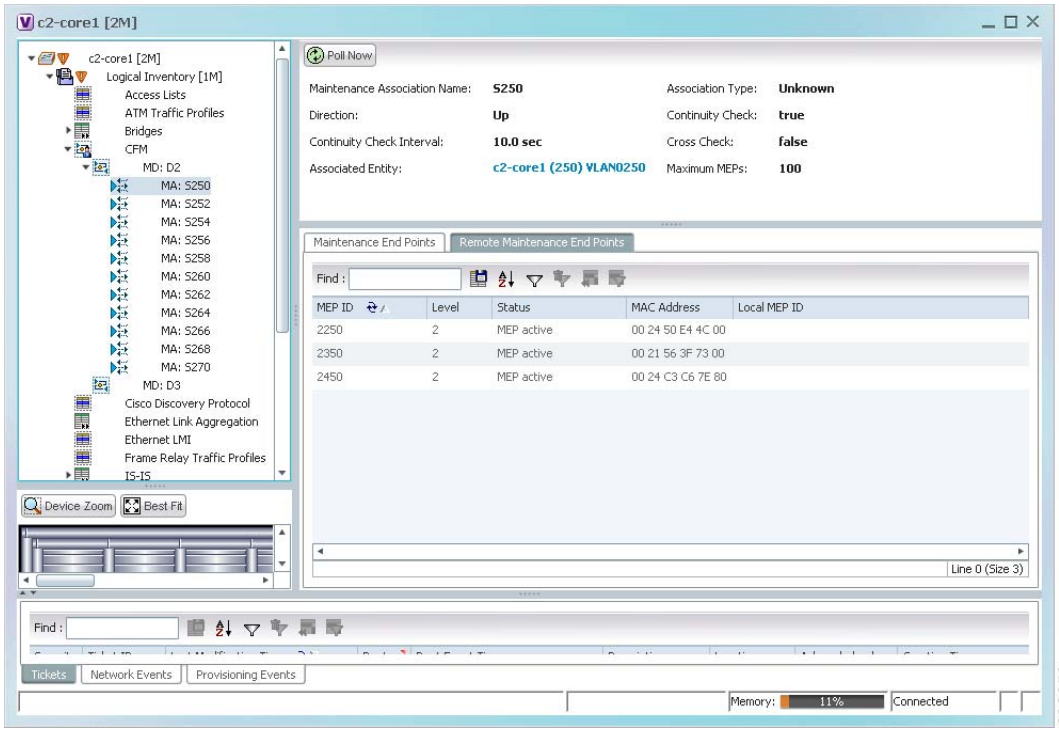


Table 16-7 describes the information presented for remote MEPs.

*Table 16-7 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.<br>**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 (E-LMI) is a protocol that operates between the customer edge (CE) network element and the provider edge (PE) network element. Ethernet LMI is a protocol between the CE network element and the provider edge (PE) network element. It runs only on the PE-CE UNI link and notifies the CE of connectivity status and configuration parameters of Ethernet services available on the CE port. Ethernet LMI interoperates with an OAM protocol, such as CFM, that runs within the provider network to collect OAM status. CFM runs at the provider maintenance level. Ethernet LMI relies on the OAM Ethernet Infrastructure (EI) to work with CFM for end-to-end status of EVCs across CFM domains. E-LMI commands are described in Configuring E-LMI, page 16-21.

The IOS OAM manager streamlines interaction between OAM protocols, and handles the interaction between CFM and E-LMI. Ethernet LMI interaction with the OAM manager is unidirectional, running only from the OAM manager to E-LMI on the U-PE side of the switch. Information is exchanged either as a result of a request from E- LMI or triggered by the OAM manager when it receives notification of a change from the OAM protocol. Information that is relayed includes the EVC name and availability status, remote UNI name and status, and remote UNI counts.

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 16-6 shows an example of Ethernet LMI properties in logical inventory.

*Figure 16-6 Ethernet LMI in Logical Inventory*

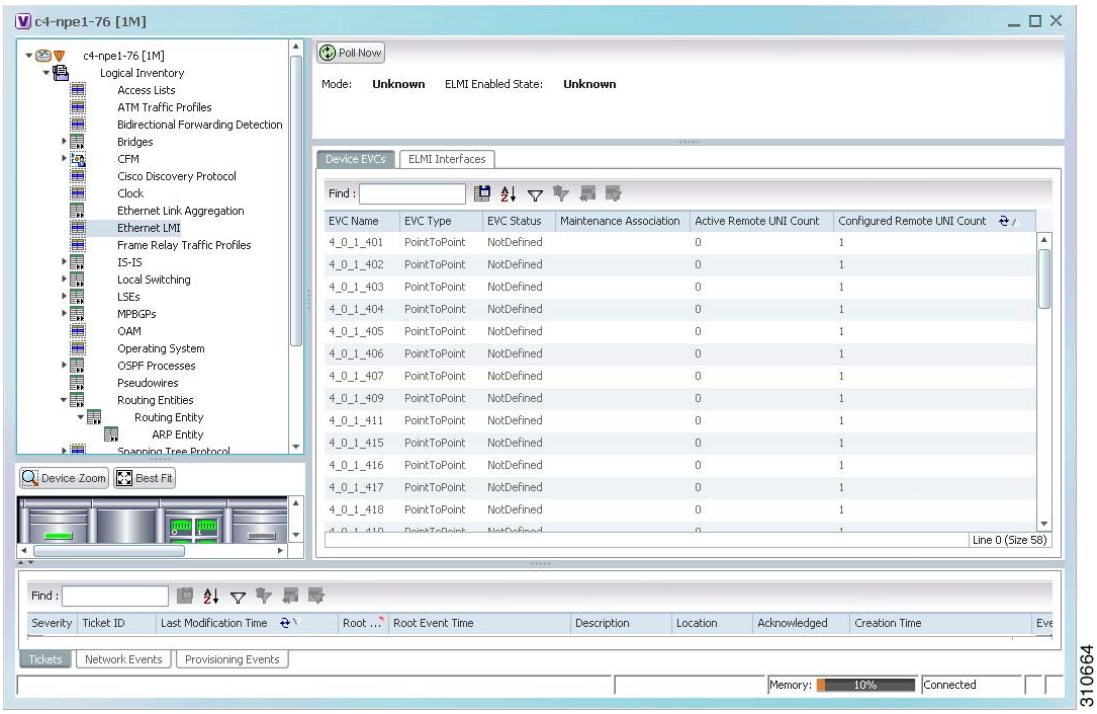



Table 16-8 describes the information displayed for Ethernet LMI.

*Table 16-8 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 16-6. |
| Active Remote UNI Count | Number of active remote UNIs. |
| Configured Remote UNI Count | Number of configured remote UNIs. |

*Table 16-8 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 16-7.

*Figure 16-7 Device EVC Properties Window*

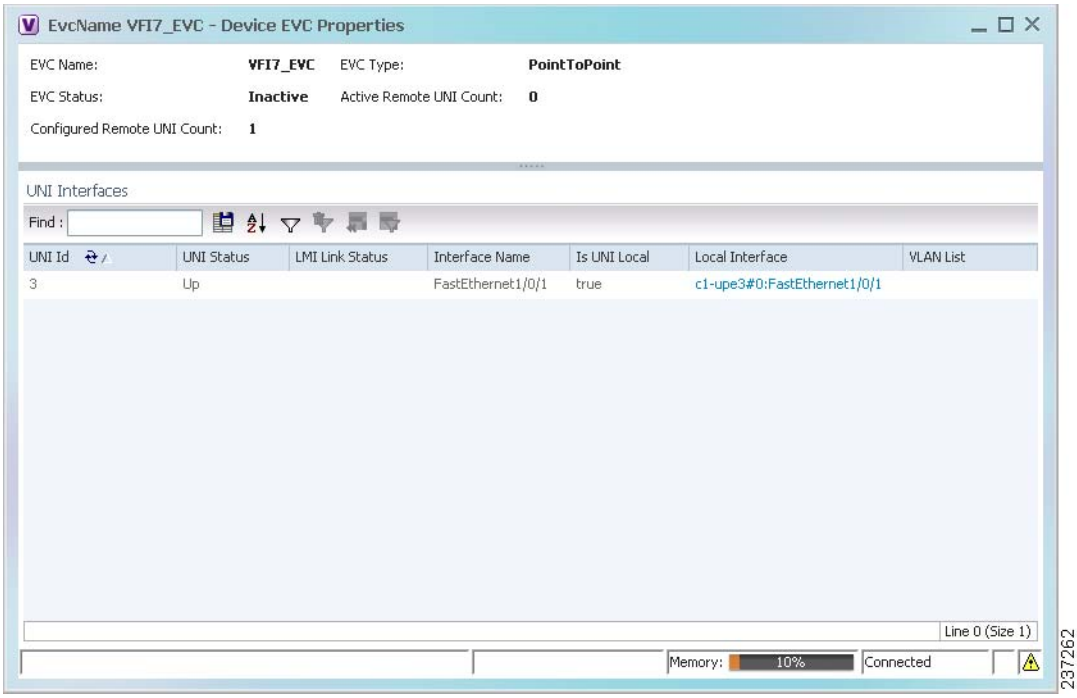



Table 16-9 describes the information displayed in the Device EVC Properties window.

*Table 16-9 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 16-6. |
| 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 16-10 describes the information displayed in the UNI Properties area in physical inventory.

*Table 16-10 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.<br>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. Link (802.3AH) OAM (L-OAM) can be implemented on any full-duplex point-to-point or emulated point-to-point Ethernet link.

The frames (OAM Protocol Data Units [OAMPDUs]) cannot propagate beyond a single hop within an Ethernet network and have modest bandwidth requirements (frame transmission rate is limited to a maximum of 10 frames per second).

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. You can also configure L-OAM using the commands described in Configuring L-OAM, page 16-22.

For information on CFM and Ethernet LMI, see Viewing Connectivity Fault Management Properties, page 16-3 and Viewing Ethernet LMI Properties, page 16-10.

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 16-8 shows an example of Link OAM properties in logical inventory.

***Figure 16-8 Link OAM Properties in Logical Inventory***

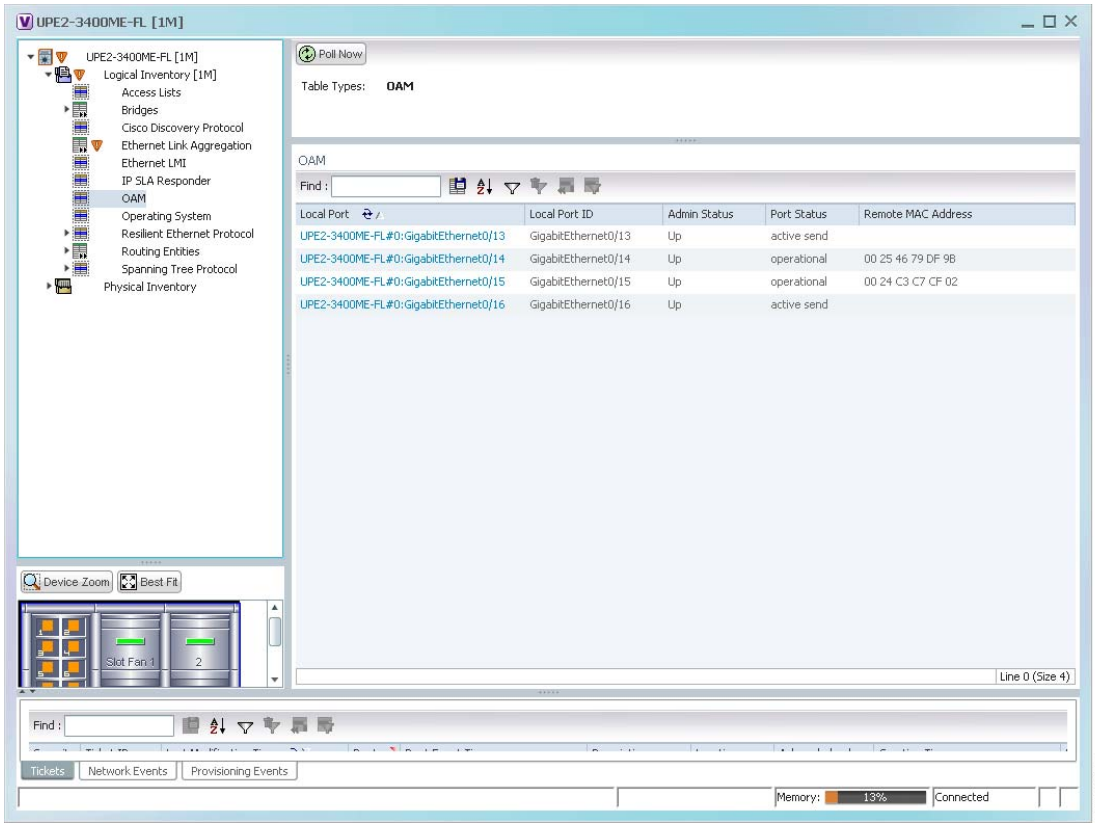



Table 16-11 describes the information displayed for Link OAM.

***Table 16-11 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 16-9.

***Figure 16-9 Link OAM Data Properties Window***

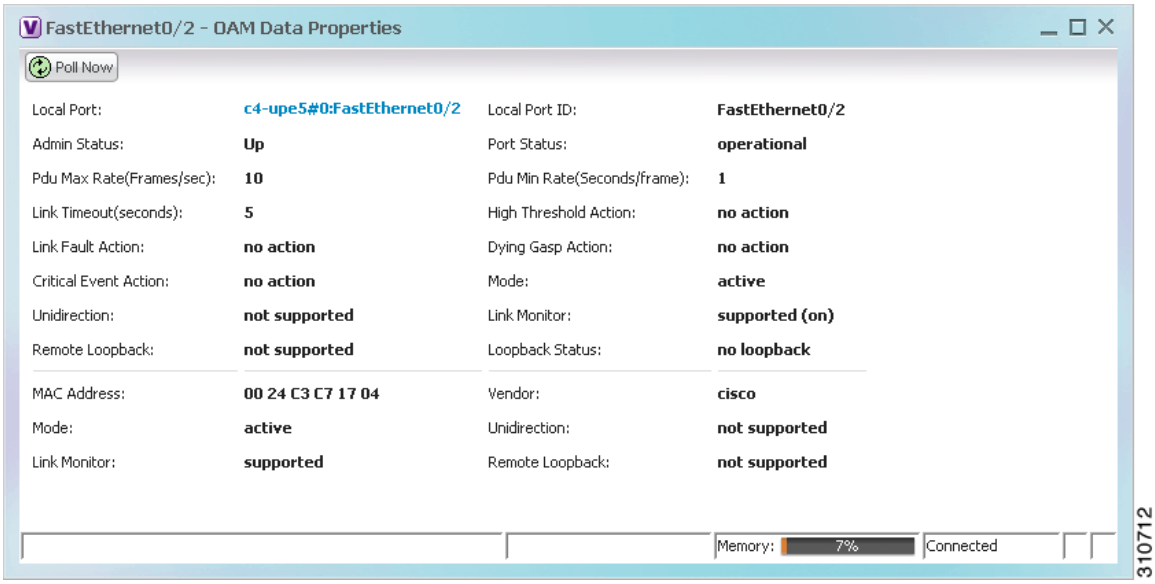



Table 16-12 describes the information that is displayed in the Link OAM Data Properties window.

***Table 16-12 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. |

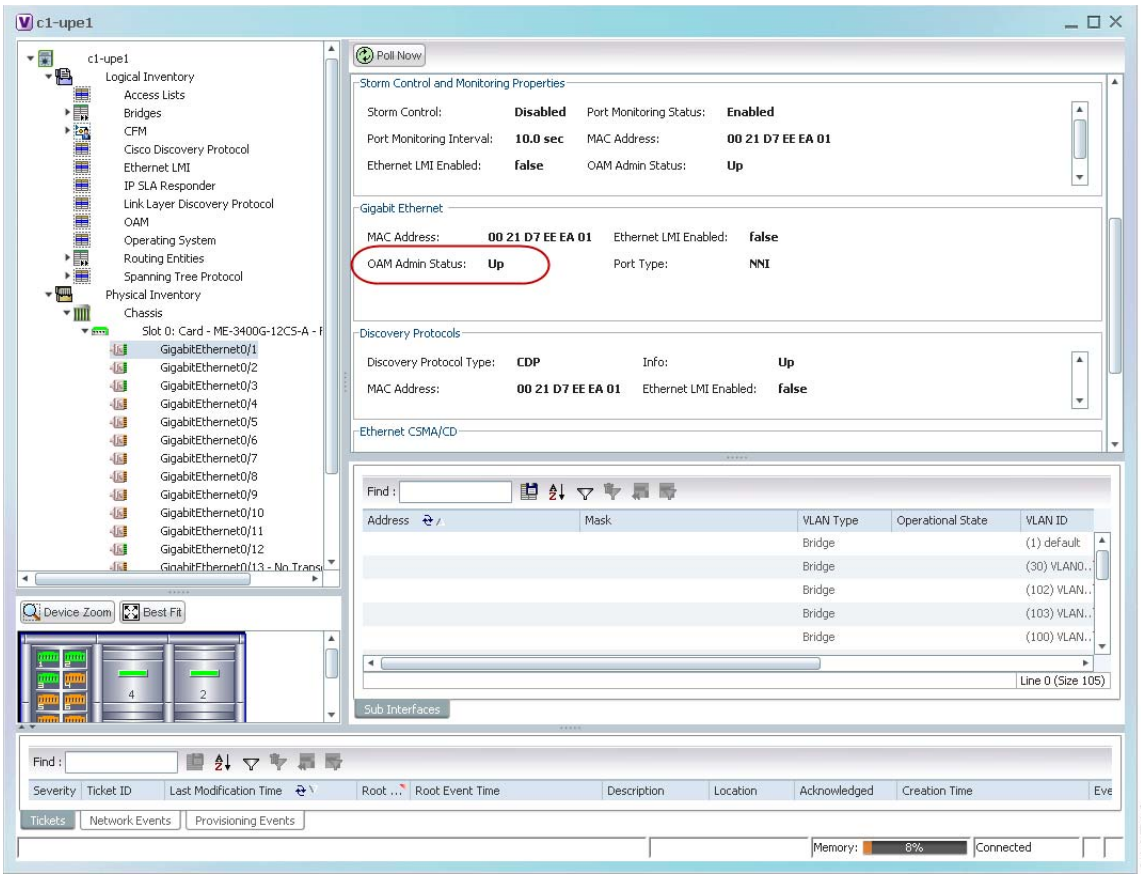
*Table 16-12 Link OAM Data Properties Window (continued)*

| 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 16-10.

*Figure 16-10 Link OAM Administrative Status in Physical Inventory*




# Configuring CFM

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.

The CFM commands can be launched from the inventory by right-clicking a CFM node and selecting **Commands**. Unless otherwise noted, all of the following commands are launched by right-clicking the device and choosing **Commands > Configure > Cisco**. You can navigate from the MEP logical inventory to the interface or port channel on which the MEP is configured.

To run the these commands, the software on the network element must support the technology. Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands.

For details on the software versions Prime Network supports for the listed supported network elements, see *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

| Command | Description | Supported on: |
|---|---|---|
| **Maintenance Domain > Configure CFM Maintenance Domain** | A maintenance domain is a management space for the purpose of managing and administering a network. A single entity owns and operates a domain and is defined by the set of ports internal to it and at its boundary. Each maintenance domain can contain any number of maintenance associations. Each maintenance association identifies a service that can be uniquely identified within the maintenance domain. The CFM protocol runs within a particular maintenance association.<br><br>Using this command, assign a unique maintenance level to each domain and a maintenance endpoint archived hold time. Maintenace level defines the hierarchical relationship among domains and MEP Archive Hold time acts as a demarcation point on an interface that participates in CFM. | • Cisco 7600 Series Routers<br>• Cisco ME 3400 Series Ethernet Access Switches<br>• Cisco ME 3750 Series Ethernet Access Switches<br>• Cisco ASR 9000 Series Aggregation Services Routers (supported only for the CFM IEEE 802.1ag<br>• (draft 8.1))<br>• Cisco Mobile Wireless Router 2941 (supported only for the CFM Cisco draft mode)<br>• Cisco Catalyst 6500 Series (IOS) Switches<br>• Cisco 3900 Series Integrated Services Routers<br>• Cisco XR 12000 Series Routers<br>• Cisco CRS Carrier Routing System<br>• Cisco ME3600X and Cisco ME3800X Carrier Ethernet Switches<br>• Cisco 3900 Series Integrated Services Routers<br>• Cisco MWR 2900 Series Mobile Wireless Routers<br>• Cisco Carrier Packet Transport (CPT) System<br>• Cisco ASR 903 Series Aggregation Services Routers |
| **Global Parameters > Configure CFM Global Parameters** | Enable CFM globally for a network element. Using this command you can configure the device to transmit traceroute and loopback messages with a hold-time value that indicates the validity of the messages. | |

| Command | Description | Supported on: |
|---|---|---|
| **Enable > Cisco >Continuity Check > Configure CFM Continuity Check**<br>**Enable > Cisco >Continuity Check > Enable CFM Continuity Check** | Enable continuity check parameters on the specified domain, service[1], bridge group, and bridge domain names. | • Cisco 7600 Series Routers<br>• Cisco ME 3400 Series Ethernet Access Switches<br>• Cisco ME 3750 Series Ethernet Access Switches<br>• Cisco ASR 9000 Series Aggregation Services Routers (supported only for the CFM IEEE 802.1ag<br>• (draft 8.1))<br>• Cisco Mobile Wireless Router 2941 (supported only for the CFM Cisco draft mode)<br>• Cisco Catalyst 6500 Series (IOS) Switches<br>• Cisco 3900 Series Integrated Services Routers<br>• Cisco XR 12000 Series Routers<br>• Cisco CRS Carrier Routing System<br>• Cisco ME3600X and Cisco ME3800X Carrier Ethernet Switches<br>• Cisco 3900 Series Integrated Services Routers<br>• Cisco MWR 2900 Series Mobile Wireless Routers<br>• Cisco Carrier Packet Transport (CPT) System<br>• Cisco ASR 903 Series Aggregation Services Routers |
| **MIP > Configure CFM MIP** | The Configure CFM MIP command configures an operator-level maintenance intermediate point (MIP) for the domain-level ID.<br>If the port on which a MIP is configured is blocked by Spanning-Tree Protocol (STP), the MIP cannot receive CFM messages or relay them toward the relay function side. The MIP can, however, receive and respond to CFM messages from the wire.<br>A MIP has only one level associated with it, and the command-line interface (CLI) does not allow you to configure a MIP for a domain that does not exist.<br>**Note** This command is not supported on the Cisco Carrier Packet Transport (CPT) System. | |
| **Service ID > Configure CFM Service ID** | Use the Configure CFM Service ID command to configure the CFM service ID. | |

| Command | Description | Supported on: |
|---|---|---|
| **MEP > Configure CFM MEP** | Use this command to configure maintenance endpoints (MEPs), which have the following characteristics:<br>• Per-maintenance domain (level) and service (S-VLAN or EVC)<br>• At the edge of a domain, define the boundary<br>• Within the bounds of a maintenance domain, confine CFM messages<br>• When configured to do so, proactively transmit CFM continuity check messages (CCMs)<br>• At the request of an administrator, transmit traceroute and loopback messages<br>**Note** This command is not supported on the Cisco Carrier Packet Transport (CPT) System. | • Cisco 7600 Series Routers<br>• Cisco ME 3400 Series Ethernet Access Switches<br>• Cisco ME 3750 Series Ethernet Access Switches<br>• Cisco ASR 9000 Series Aggregation Services Routers (supported only for the CFM IEEE 802.1ag<br>• (draft 8.1))<br>• Cisco Mobile Wireless Router 2941 (supported only for the CFM Cisco draft mode)<br>• Cisco Catalyst 6500 Series (IOS) Switches<br>• Cisco 3900 Series Integrated Services Routers<br>• Cisco XR 12000 Series Routers<br>• Cisco CRS Carrier Routing System<br>• Cisco ME3600X and Cisco ME3800X Carrier Ethernet Switches<br>• Cisco 3900 Series Integrated Services Routers<br>• Cisco MWR 2900 Series Mobile Wireless Routers<br>• Cisco Carrier Packet Transport (CPT) System<br>• Cisco ASR 903 Series Aggregation Services Routers |
| **Enable > Cisco > SNMP Server Traps > Enable CFM SNMP Server Traps** | Enables Ethernet CFM continuity check traps and Ethernet CFM cross-check traps | |

1. Applicable for Cisco ASR 9000 series that run on Cisco IOS XR software.

# Configuring E-LMI

E-LMI notifies the CE of connectivity status and configuration parameters of Ethernet services available on the CE port.

The following commands can be launched from the inventory by right-clicking an E-LMI node and selecting **Commands**. Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. The table below lists the Ethernet LMI commands and the supported network elements.

To run the these commands, the software on the network element must support the technology. Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands.

For details on the software versions Prime Network supports for the listed supported network elements, see *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

| Command | Description | Supported on: |
|---|---|---|
| **Enable > Global E-LMI** | Enable Ethernet LMI globally.<br>**Note** Not supported on Cisco IOS XR. | • Cisco 7600 Series Routers<br>• Cisco Catalyst 3750 Metro Series Switches<br>• Cisco Catalyst 6500 Series (IOS) Switches<br>• Cisco ME3600X and Cisco ME3800X Carrier Ethernet Switches<br>• Cisco ME 3400 Series Ethernet Access Switches<br>• Cisco MWR 2941 Mobile Wireless Routers<br>• Cisco ASR9000 Series Routers |
| **Enable On Interface** | If E-LMI is disabled globally, you can use this command to enable E-LMI on specific interfaces. | |
| **Configure MultiPoint To MultiPoint or Point To Point EVC** | UNI count indicates the range of the Unified network interface(UNI) is 2 to 1024; the default is 2. If you enter a value of 2, you have the option to select point-to-multipoint service. If you configure a value of 3 or greater, the service is point-to-multipoint. | |
| **Configure UNI in an Interface** | | |
| **Configure Service Instance Vlan Id on Interface** | Specify the service interface ID (Per-interface Ethernet service instance identifier that does not map to a VLAN). | |

# Configuring L-OAM

L-OAM commands monitors and troubleshoots a single Ethernet link. The following commands can be launched from the inventory by right-clicking a L-OAM node and selecting **Commands**. Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. The table below lists the L-OAM commands.

To run the these commands, the software on the network element must support the technology. Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands.

For details on the software versions Prime Network supports for the listed supported network elements, see *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

| Command | Description | Supported on: |
|---|---|---|
| **Assign Template on Interface** | Assign template name | • Cisco 7600 Series Routers<br>• Cisco Catalyst 3750 Metro Series Switches<br>• Cisco Catalyst 6500 Series (IOS) Switches<br>• Cisco ME 3400 Series Ethernet Access Switches<br>• Cisco MWR 2941 Mobile Wireless Routers<br>• Cisco ASR 9000 Series Aggregation Services Routers<br>• Cisco 2900 Series Integrated Services Routers<br>• Cisco 3900 Series Integrated Services Routers<br>• Cisco ME 3600X Ethernet Access Switches<br>• Cisco ME 3800X Carrier Ethernet Switch Routers<br>• Cisco 3900 Series Integrated Services Routers<br>• Cisco 2900 Series Integrated Services Routers<br>• Cisco 1900 Series Integrated Services Routers<br>• Cisco ASR 903 Series Aggregation Services Routers<br>• Cisco Carrier Packet Transport (CPT) System |
| **Configure MultiPoint To MultiPoint or Point To Point EVC** | Configure OAM (L-OAM) on any full-duplex point-to-point or emulated point-to-point Ethernet link. | |
| **Enable OAM on Interface**<br>**Disable OAM on Interface** | Enable or disable OAM on the specified interface. | |
| **Enable E-LMI On Interface** | Interface name (if E-LMI is disabled globally, you can use this command to enable E-LMI on specific interfaces) | |
| **Configure OAM Parameter on Interface** | Configure OAM parameters, like maximum and minimum transmission rate of OAM PDU , OAM client mode and remote loopback ability on an interface. | |
| **Start Remote Loopback**<br>**Stop Remote Loopback** | Specify the local interface name on which the remote loopback should be started and stopped. | |

CHAPTER 17

# Monitoring Y.1731 IPSLA Configuration

The following topics provide an overview of the Y.1731 technology and describe how to view and monitor Y.1731 configurations in Prime Network Vision:


- Y.1731 Technology - An Overview, page 17-1
- User Roles Required to Work with Y.1731 Probes, page 17-2
- Working with Y.1731 IPSLA Configurations, page 17-2


## Y.1731 Technology - An Overview

Y.1731 is an ITU-T recommendation that provides mechanisms for service-level Operation, Administration, and Maintenance (OAM) functionality in Ethernet networks. It covers mechanisms for Fault and Performance Management. Performance Management is the most sought-after functionality in this standard.

In Prime Network, devices that are configured using Y.1731 are detected, scanned for configurations, and monitored. A device configured using Y.1731 has probes, which are root objects or containers that hold single or multiple instances of Service Level Agreement (SLA) probes configured by the user.

In Prime Network, the Y.1731 technology is supported on the Cisco Aggregation Service Router (ASR) 9000 and Cisco Carrier Packet Transport (CPT) network elements.

### Y.1731 Performance Management Mechanisms

The OAM functions for performance monitoring according to Y.1731 allow measurement of the following performance parameters.

- Frame Loss Ratio—Expressed as a percentage. This ratio is defined as the number of frames not delivered divided by the total number of frames during a time interval.
- Frame Delay—A one-way delay for a frame, where one-way frame delay is defined as the time elapsed since the start of transmission of the first bit of the frame by a source node until the reception of the last bit of the same frame by the destination node.
- Frame Delay Variation—The measure of the variations in the frame delay between a pair of service frames. The service frames belong to the same CoS (Class of Service) instance on a point-to-point Ethernet (ETH) connection or multipoint ETH connectivity.
- Throughput—The average rate of successful traffic delivery over a communication channel. Typically used under test conditions, such as out-of service tests, when there is no traffic for the tested Ethernet connection.

# User Roles Required to Work with Y.1731 Probes

This topic identifies the roles that are required to work with Y.1731 probes. 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 3.10 Administrator Guide*.

***Table 17-1 Default Permission/Security Level Required for Y.1731 Probes***

| Task | Viewer | Operator | OperatorPlus | Configurator | Administrator |
|---|---|---|---|---|---|
| View the Y.1731 probe properties | X | X | X | X | X |
| Configure Y.1731 probes | — | — | — | X | X |

# Working with Y.1731 IPSLA Configurations

This topic contains the following sections:

- Viewing the Y.1731 Probe Properties, page 17-2
- Configuring Y.1731 Probes, page 17-4

## Viewing the Y.1731 Probe Properties

To view the Y.1731 probes and their properties for a device:

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

**Step 2** In the **Inventory** window, choose **Logical Inventory > Probes > Y1731 Probes**. A list of Y.1731 probes is displayed in the Y.1731 Probes content pane as shown in Figure 17-1.

*Figure 17-1 Y.1731 Probes Content Pane*

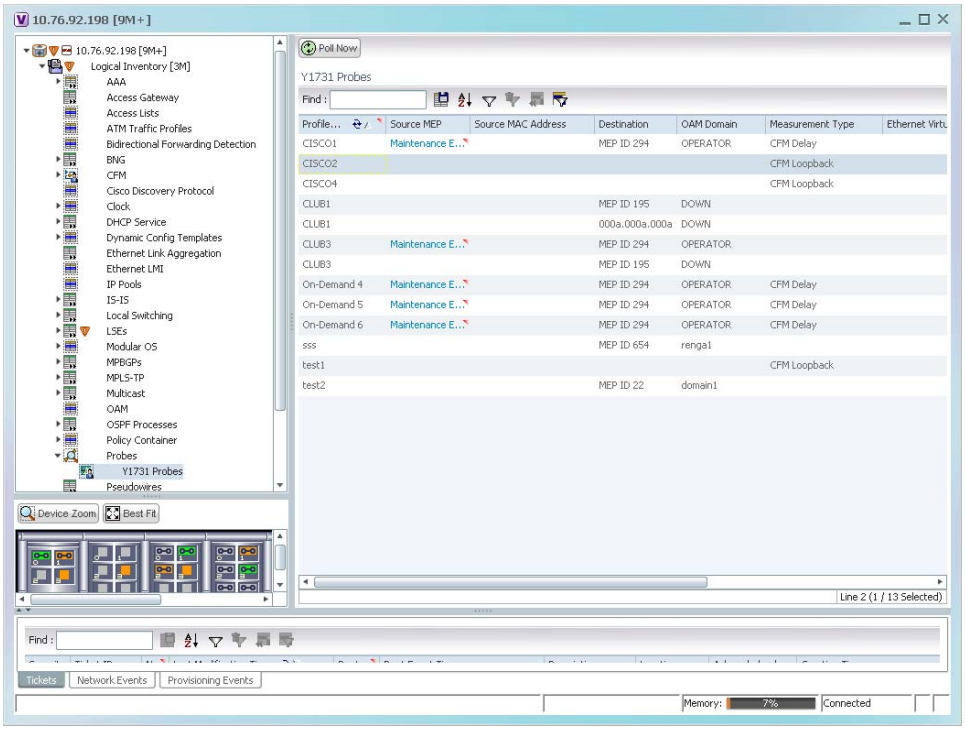



Table 17-2 describes the fields that are displayed in the content pane.

*Table 17-2 Y.1731 Content Pane*

| Field Name | Description |
|---|---|
| Profile Name | The name of the profile created for performance monitoring of the SLA configuration. |
| Source MEP | The maintenance endpoint (MEP) interface ID where the probe is getting initiated. |
| Source MAC Address | The source interface MAC address where the probe is getting initiated. |
| Destination | The interface ID or MAC address, which will help the probe to reach its destination. |
| OAM Domain | The name of the OAM domain. |
| Measurement Type | The type of performance operation, which could be cfm-delay-measurement or cfm-loopback. |
| Ethernet Virtual Connection | The name or identifier of the ethernet virtual connection, which connects two User-Network Interfaces (UNI). This is applicable only for the Cisco CPT devices. |
| Packet Size | The size of the service packet. This includes padding size when required. |
| Packets Per Burst | The number of packets transmitted per burst. |
| Burst Period | The time taken to send the packets from the source to their destination. This period is usually specified in terms of seconds or milliseconds. |

**Step 3** Right-click on a probe and choose **Properties** to view its properties. Additionally, the following information is displayed in the Probe Properties window for a Cisco CPT device.

Table 17-3 describes the additional fields that are displayed for a Cisco CPT device in the **Probe Properties** window.

*Table 17-3 Probe Properties Window*

| Field Name | Description |
|---|---|
| **Measurements** | |
| Statistics Type | The statistics type, which is Round Trip Delay or Round Trip Jitter. |
| Aggregate Bin Count | The aggregate count of bins to store the counter values of the result of each performance parameter.<br>**Note** The counter value refers to the counter of number of results that fall within a particular range specified for each performance attribute. |
| Aggregate Bin Boundaries | The bin boundary for the bins. For Cisco CPT devices, bin boundary is specified as comma separated intervals; whereas for ASR9K devices, it is an integer. Bin boundaries are specified in terms of milliseconds. |
| Bucket Size | The number of buckets required to store the performance attribute results gathered during a specified period. By default, a separate bucket is created for each probe, which will contain the results relating to measurements made by the probe. |

# Configuring Y.1731 Probes

You can configure Y.1731 probes using a certain set of commands. The following commands can be launched from the inventory by right-clicking the appropriate node and selecting **Commands.** Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

| Command | Navigation | Description | Supported On |
|---|---|---|---|
| Configure Probe EndPoint Association | *Right-click* **Y1731 Probes** *node* > **Commands** > **Configuration** | Use this command to configure endpoint association for a probe. | Cisco ASR 9000 devices |
| Configure Profile | | Use this command to configure a new profile for the probe. | |
| Create On Demand Probe Configuration | | Use this command to create an on demand probe configuration. | |
| Deassociate Profile | | Use this command to deassociate a profile from a probe. | |

| Command | Navigation | Description | Supported On |
|---|---|---|---|
| Delete Profile | *Right-click* **Y1731 Probes** *node* > **Commands** > **Configuration** | Use this command to delete a profile. | Cisco ASR 9000 devices |
| Show SLA Operations detail | *Right-click* **Y1731 Probes** *node* > **Commands** > **Diagnostics** | When service providers sell connectivity services to a subscriber, a Service Level Agreement (SLA) is reached between the buyer and seller of the service. The SLA defines the attributes offered by a provider and serves as a legal obligation on the service provider. As the level of performance required by subscribers increases, service providers need to monitor the performance parameters being offered.<br>Use this command to view the SLA operation details. | |
| Show SLA Profiles | | Use this command to view a list of the SLA profiles. | |
| Configure IP SLA parameters | *Right-click* **Y1731 Probes** *node* > **Commands** > **Configuration** | Use this command to configure an IP SLA parameter for the probe. | Cisco CPT devices |
| Delete IP SLA parameters | | Use this command to delete the IP SLA parameters for a probe. | |
| Show IP SLA | *Right-click* **Y1731 Probes** *node* > **Commands** > **Diagnostics** | Use this command to view the IP SLA schedule details. | |

CHAPTER 18

# 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.

This chapter contains the following topics:


- User Roles Required to Work with IPv6 and 6VPE, page 18-2
- Viewing IPv6 Information, page 18-2

# 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 3.10 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 3.10 Administrator Guide*.

***Table 18-1 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 18-2 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 18-3 describes where IPv6 information appears in logical and physical inventory.

*Table 18-3 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.<br>For more information, see Viewing 6rd Tunnel Properties, page 19-46. |
| Access Lists | • The Type field displays IPv6 for IPv6 access lists.<br>• 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.<br>For more information, see Viewing Carrier Grade NAT Properties in Logical Inventory, page 14-2. |
| GRE Tunnels | The IP Address field supports IPv6 addresses.<br>For more information, see Viewing MPLS Pseudowire over GRE Properties, page 21-31. |
| IS-IS | IS-IS properties support:<br>• IPv6 address families in the Metrics tab.<br>• IPv6 addresses in the Neighbors tab and the IS-IS Neighbor Properties window.<br>For more information, see Viewing IS-IS Properties, page 13-113. |
| MPBGPs | • IP address family identifiers indicate the BGP peer address family: IPv4, IPv6, Layer 2 VPN, VPNv4, or VPNv6.<br>• MP-BGP BGP neighbor entries display IPv6 addresses.<br>For information, see Viewing MP-BGP Information, page 19-45. |
| OSPFv3 | IPv6 addresses are displayed for OSPF neighbor interface addresses, OSPF interface internet addresses, OSPF neighbor properties window, and OSPF interface properties window.<br>For more information, see Viewing OSPF Properties, page 13-116. |
| Routing Entities | • IPv6 addresses appear in the IP Interfaces tab, the IPv6 Routing tab, and the interface properties window.<br>• IPv6 addresses are displayed in the NDP Table tab and the ARP Entry Properties window.<br>• VRRP groups using IPv6 display IPv6 addresses in the IP Interfaces Properties window in the VRRP group tab.<br>For more information, see Viewing Routing Entities, page 19-31. |
| VRFs | IPv6 addresses appear in the IPv6 tab, Sites tab, VRF Properties window, and IP Interface Properties window.<br>For more information, see Viewing VRF Properties, page 19-27. |

*Table 18-3 IPv6 Information in Inventory (continued)*

| Inventory Location | Description |
|---|---|
| **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 18-4.

*Table 18-4 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 18-1 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 18-1 Port with IPv4 and IPv6 Addresses*

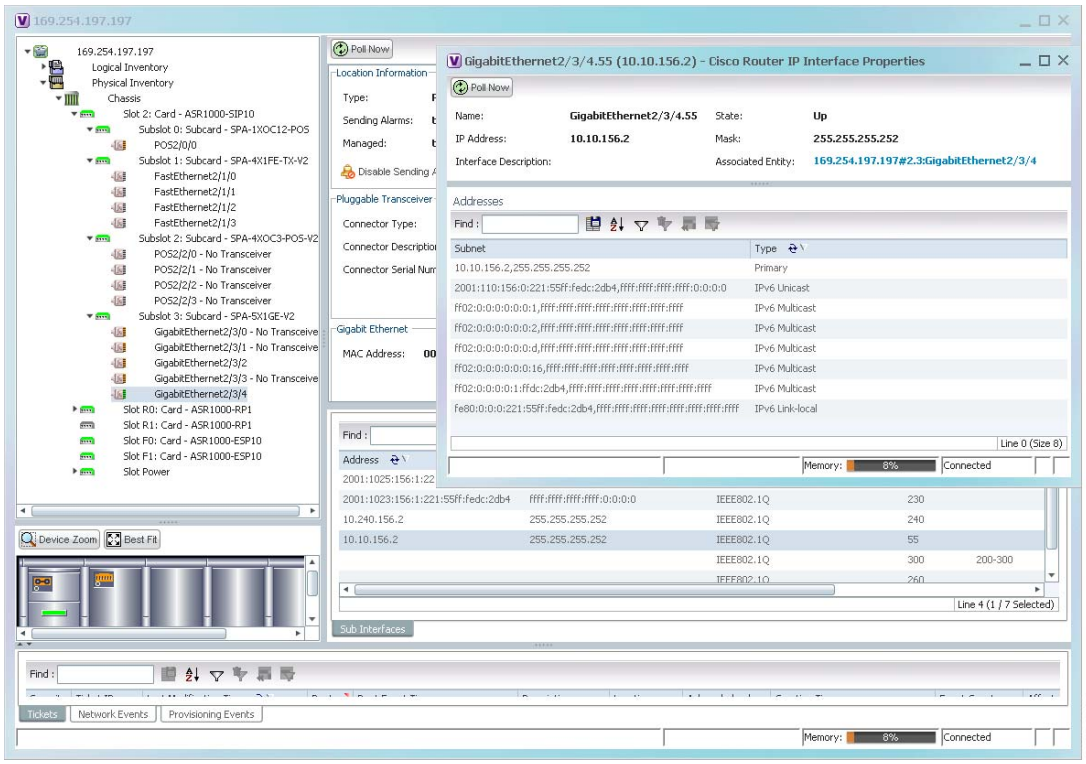
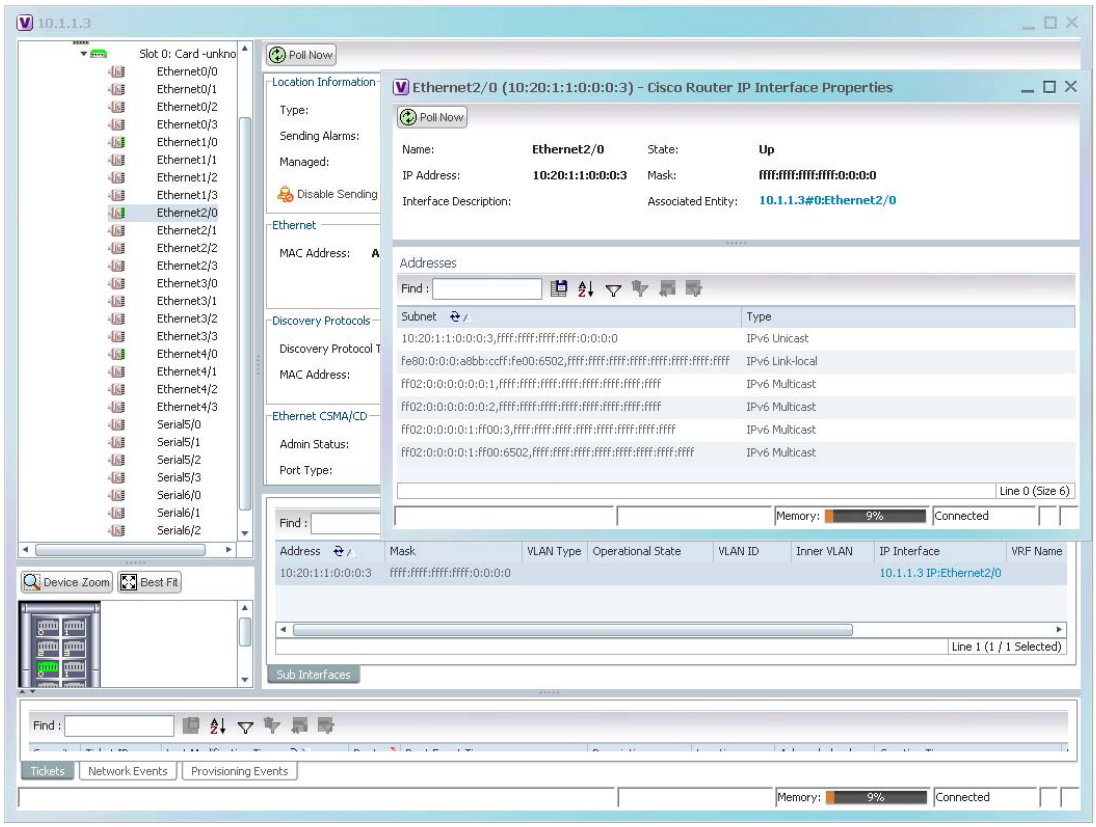



Figure 18-2 shows a port with only IPv6 addresses provisioned. In this example, the lowest IPv6 address is shown in the subinterface table, and all IPv6 addresses are shown in the interface properties window.

*Figure 18-2 Port with IPv6 Addresses*



CHAPTER 19

# 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 19-1
- Working with MPLS-TP Tunnels, page 19-4
- Viewing VPNs, page 19-18
- Managing VPNs, page 19-21
- Working with VPN Overlays, page 19-24
- Monitoring MPLS Services, page 19-26
- Configuring VRF, page 19-53
- Configuring IP Interface, page 19-54
- Configuring MPLS-TP, page 19-54
- Configuring MPLS-TE, page 19-57
- Configuring MPLS, page 19-57
- Configuring RSVP, page 19-58
- Configuring BGP, page 19-59
- Configuring VRRP, page 19-60
- Configuring Bundle Ethernet, page 19-61


## 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 3.10 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 3.10 Administrator Guide*.

***Table 19-1 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 |

*Table 19-1 Default Permission/Security Level Required for Working with MPLS Networks - Element Not in User's Scope (continued)*

| Task | Viewer | Operator | OperatorPlus | Configurator | Administrator |
|---|---|---|---|---|---|
| Display or hide VPN overlays | X | X | X | X | X |
| Remove VPN overlays | X | X | X | X | X |

*Table 19-2 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 |

*Table 19-2 Default Permission/Security Level Required for Working with MPLS Networks - Element in User's Scope (continued)*

| Task | Viewer | Operator | OperatorPlus | Configurator | Administrator |
|---|---|---|---|---|---|
| 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 19-5
- Viewing MPLS-TP Tunnel Properties, page 19-7
- Viewing LSPs Configured on an Ethernet Link, page 19-11
- Viewing LSP Endpoint Redundancy Service Properties, page 19-13
- Applying an MPLS-TP Tunnel Overlay, page 19-16
- Viewing MPLS-TP BFD session properties—See Viewing BFD Session Properties, page 19-47.

# 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.

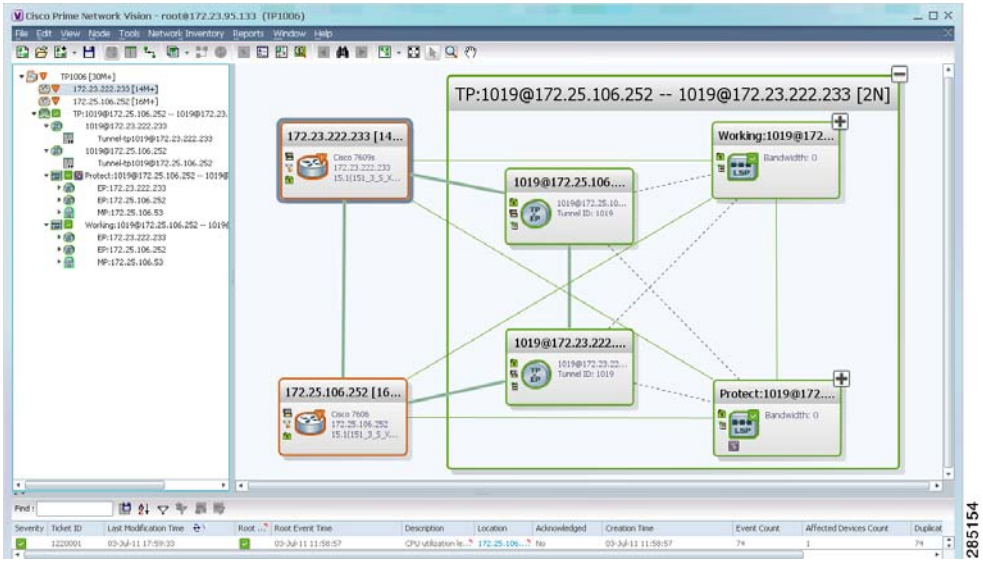
**Step 5** Click **OK**.

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

In Figure 19-1:

- 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 19-1 MPLS-TP Tunnel in Prime Network Vision Map*

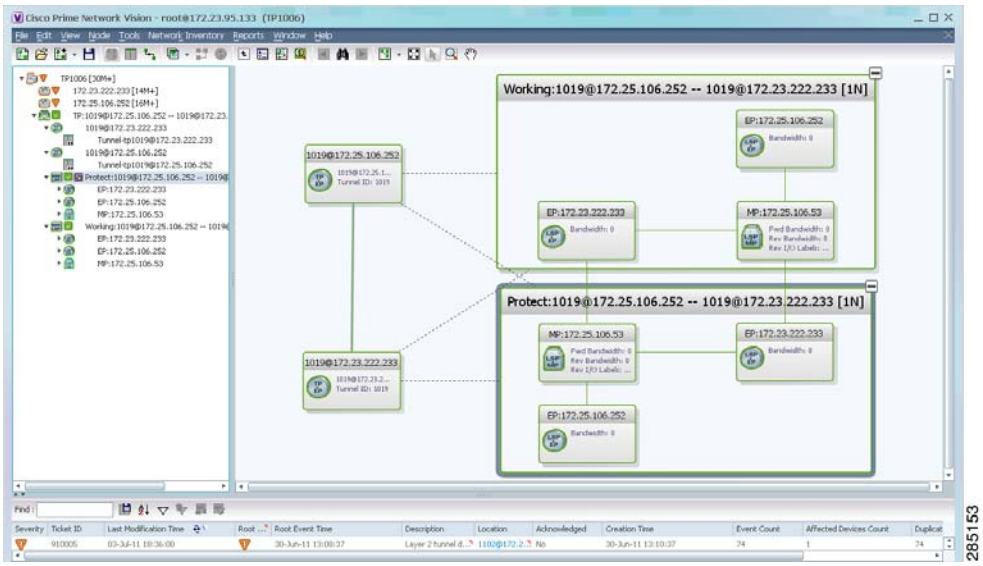



If an LSP is in lockout state, it is displayed with the lock badge ( ).

By expanding all aggregations in the MPLS-TP tunnel (see Figure 19-2), you can see components and links in the MPLS-TP tunnel, including:

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

*Figure 19-2 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 19-13.

# 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 19-31.
- LSEs—See Viewing Label Switched Entity Properties, page 19-39.
- Pseudowires— See Viewing Pseudowire End-to-End Emulation Tunnels, page 19-50.

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 19-3.

***Figure 19-3 MPLS-TP Tunnel Properties in Logical Inventory***

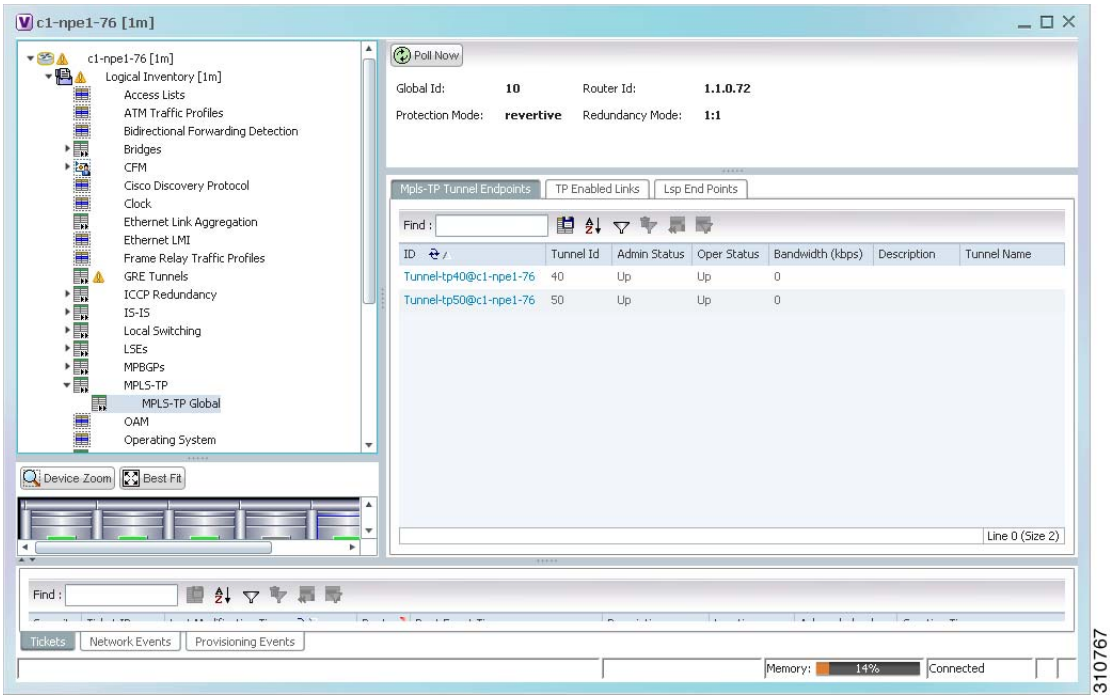



Table 19-3 describes the information that is available for MPLS-TP tunnels. The information that is displayed depends on the configuration.

*Table 19-3 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:<br>• Revertive—If the protection mode is revertive and a failed path is restored, the traffic automatically returns, or reverts, to the original path.<br>• 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:<br>• *src-node-ID* represents the identifier of the node originating the signal exchange.<br>• *src-tunnel-number* represents source tunnel identifier.<br>• *dest-node-ID* represents the identifier of the target node.<br>• *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 19-3 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:<br>• *src-node-ID* represents the identifier of the node originating the signal exchange.<br>• *src-tunnel-number* represents source tunnel identifier.<br>• *dest-node-ID* represents the identifier of the target node.<br>• *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 19-4.

*Figure 19-4 MPLS-TP Tunnel Properties Window*

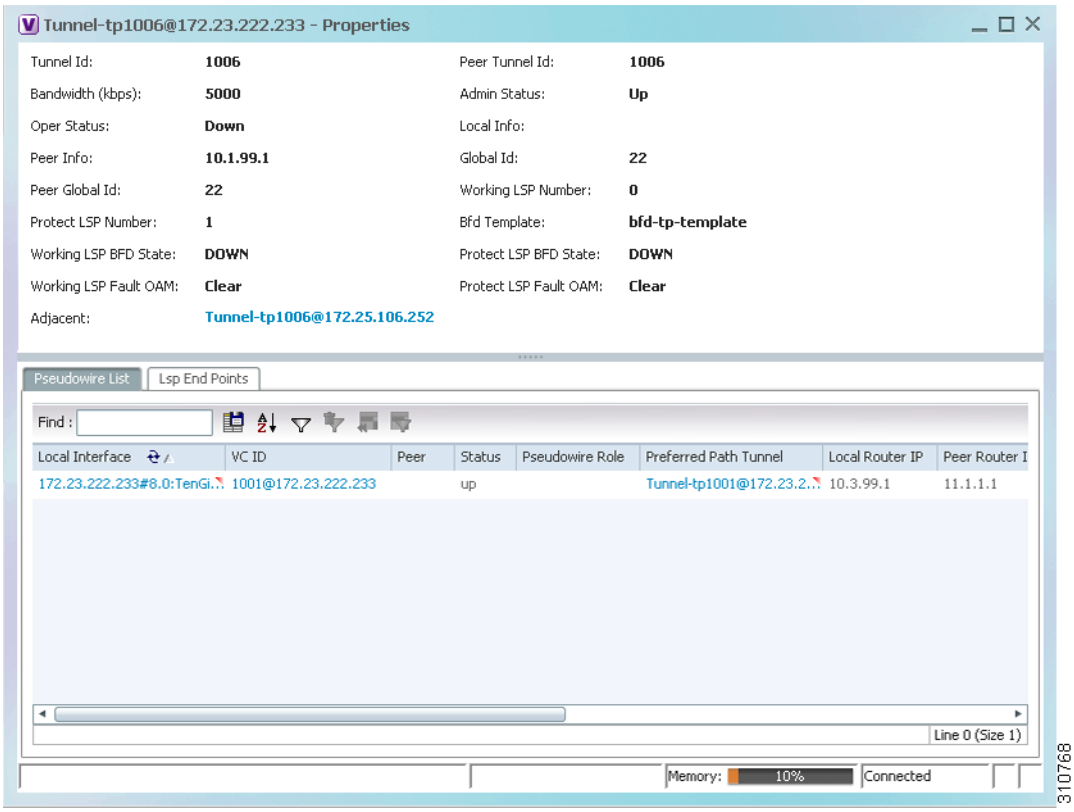



Table 19-4 describes the information available in the top portion of the MPLS-TP Tunnel Properties window. For information about the tabs that are displayed, see Table 19-3.

*Table 19-4 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 19-4 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.

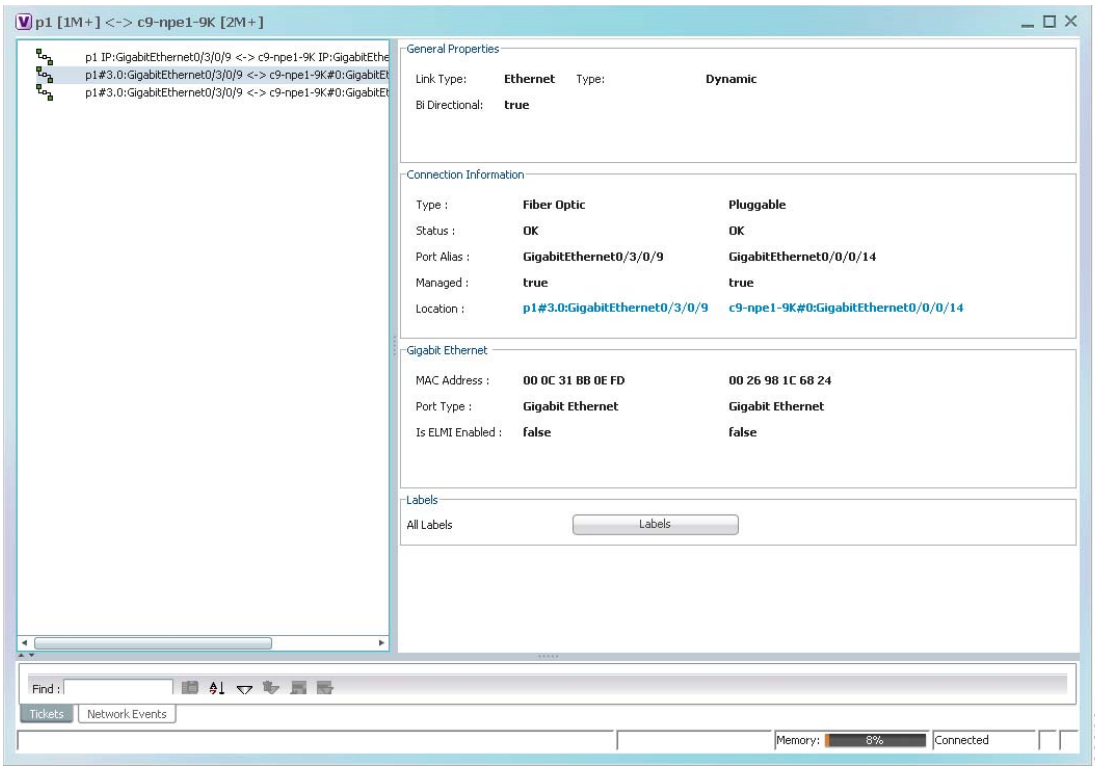
To view LSPs configured on an Ethernet link:

**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 19-5.

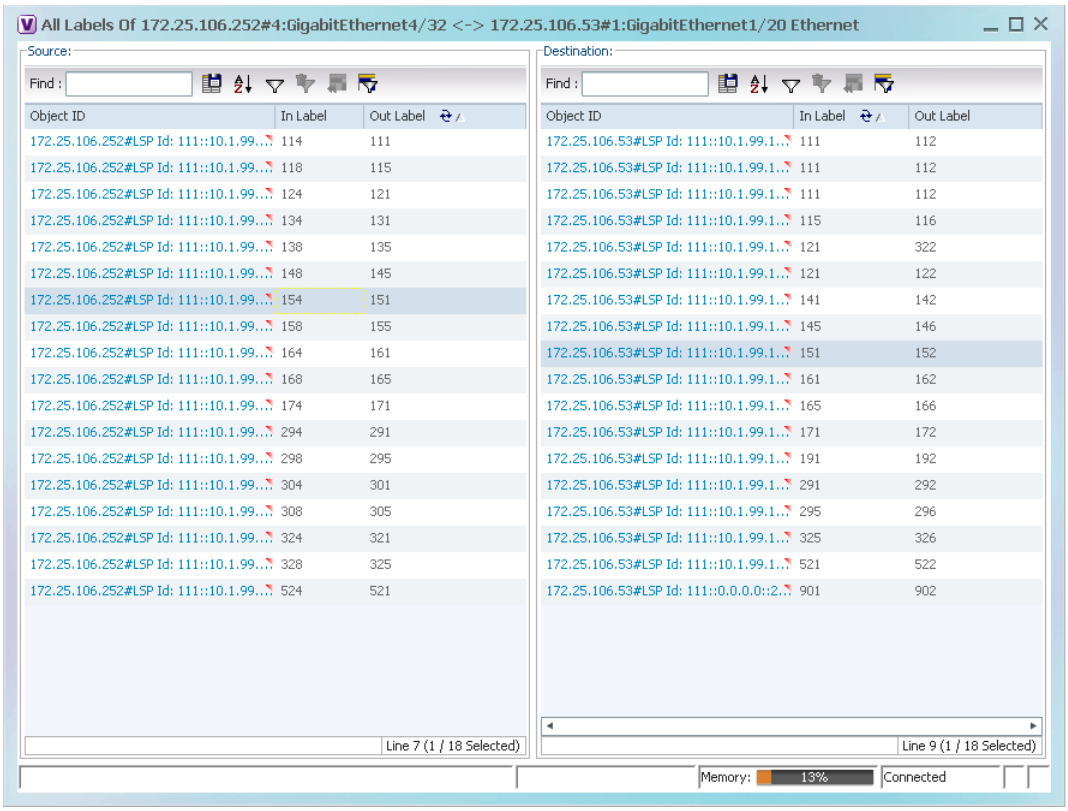
*Figure 19-5 Link Properties Window with All Labels Button*




**Step 3** Click **Labels**.

The All Labels window is displayed as shown in Figure 19-6 with the LSP sources and destinations.

*Figure 19-6 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

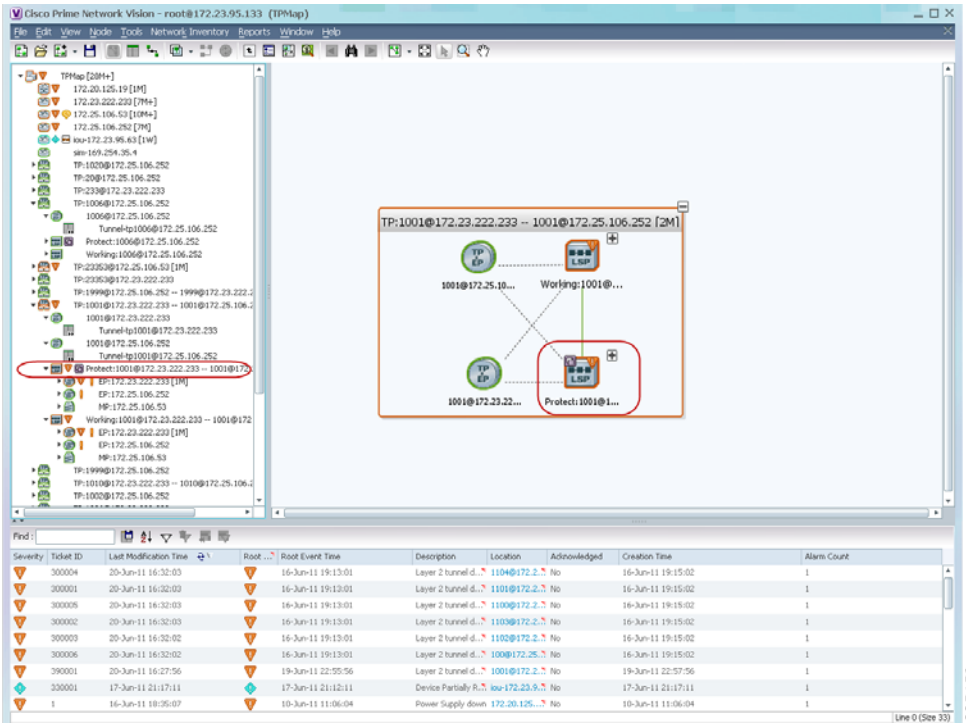
If an LSP endpoint in an MPLS-TP tunnel is configured for redundancy service, a redundancy service badge is applied to the secondary (backup) LSP endpoint in the navigation and map panes in Prime Network Vision. Additional redundancy service details are provided in the LSP endpoint properties window 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 19-7.

*Figure 19-7 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 19-8.

*Figure 19-8 LSP Endpoint Properties Window*

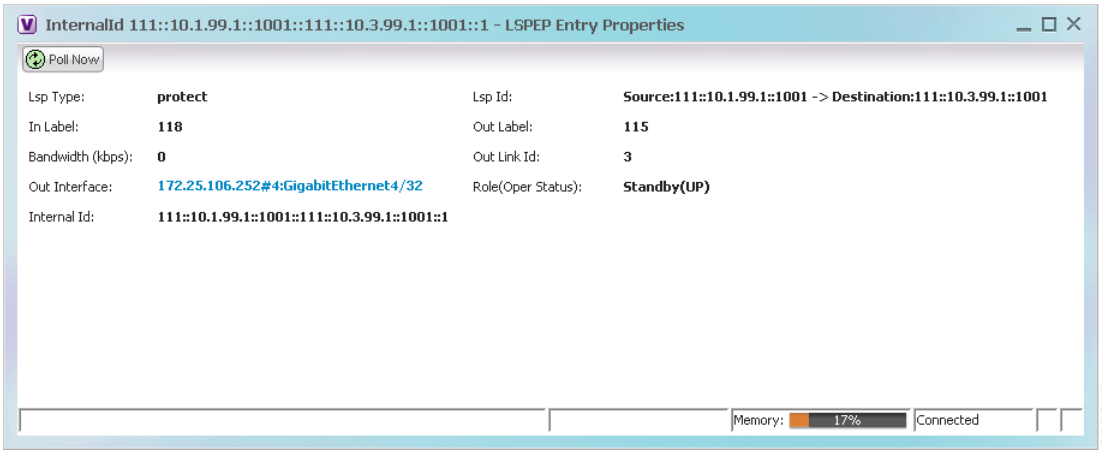



Table 19-5 describes the information displayed in the LSP Endpoint Properties window.

*Table 19-5 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:<br>• *src-node-ID* represents the identifier of the node originating the signal exchange.<br>• *src-tunnel-number* represents source tunnel identifier.<br>• *dest-node-ID* represents the identifier of the target node.<br>• *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) |

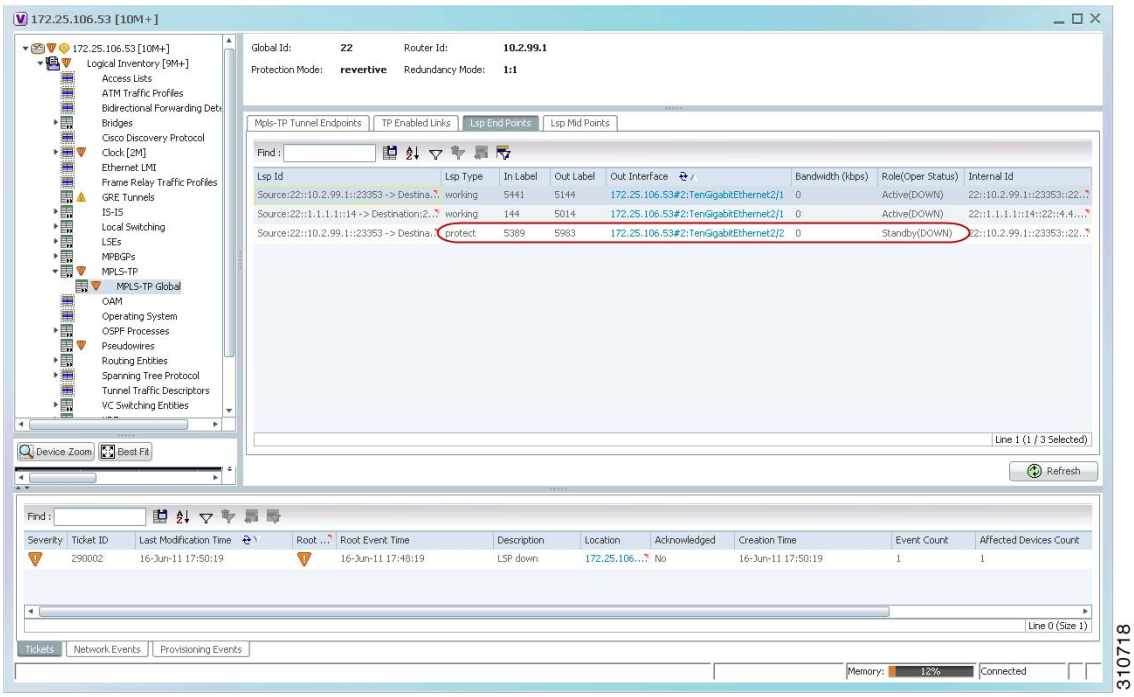
**Step 3** To view LSP endpoint redundancy status in inventory, double-click the element on which the MPLS-TP tunnel is configured.

**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 19-9):

- 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 19-9 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

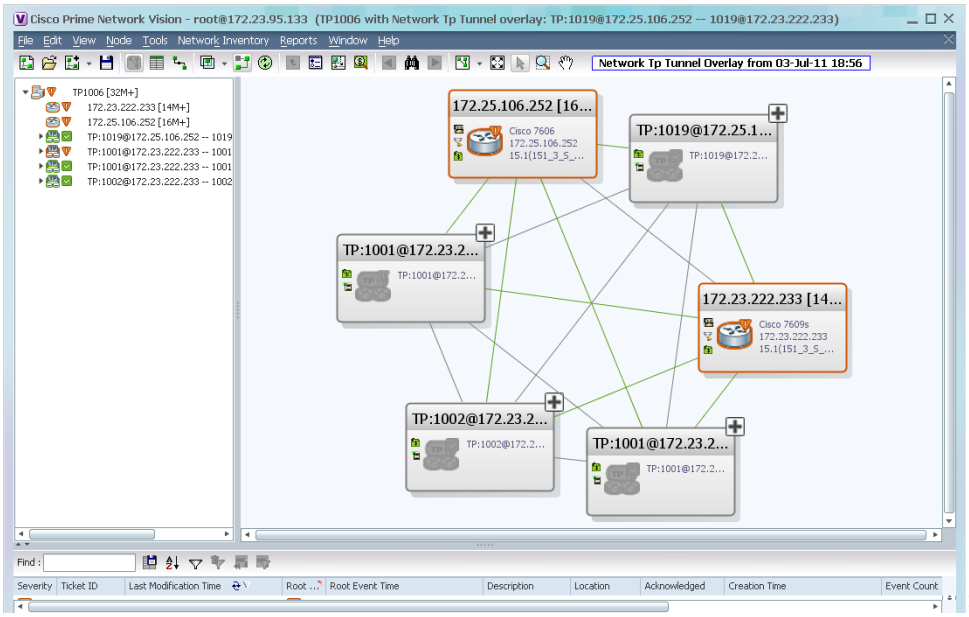
The search condition is “contains.” Search strings are case-insensitive. For example, if you choose the Name category and enter “net,” Prime Network Vision displays MPLS-TP tunnels that have “net” in their names whether net appears at the beginning of the name, the middle, or at the end: for example, 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 19-10.

***Figure 19-10 MPLS-TP Tunnel Overlay***

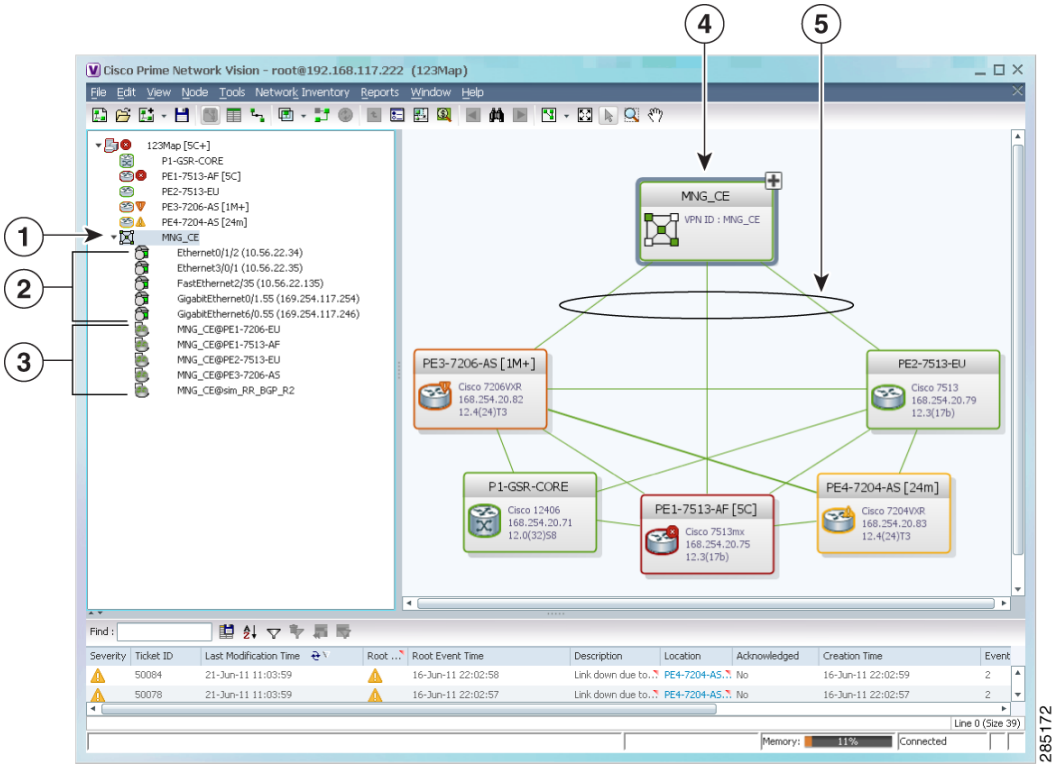



**Note** An overlay is a snapshot taken at a specific point in time and does not reflect changes that occur in the service. As a result, the information in an overlay can become stale. To update the overlay, click **Refresh Overlay** in the main toolbar.

# Viewing VPNs

Figure 19-11 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.

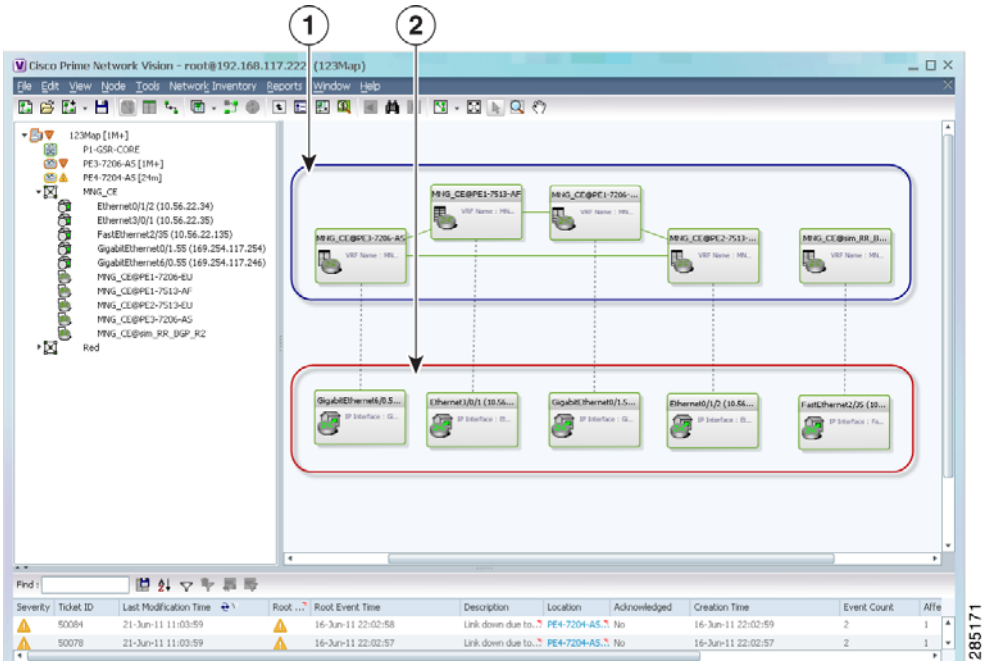
***Figure 19-11 VPN in Prime Network Vision Map View***




| | | | |
|---|---|---|---|
| **1** | VPN in the navigation tree | **4** | VPN in the map view |
| **2** | Sites | **5** | VPN links |
| **3** | Virtual routers | | |

Figure 19-12 shows a VPN with details, including virtual routers and sites, in the Prime Network Vision map view.

***Figure 19-12 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 2-16.

Table 19-6 shows the VPN icons in the Prime Network Vision map view.

*Table 19-6 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 19-7 shows the additional properties available for VPN entities.

*Table 19-7 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.<br>• Right-click a VPN and choose **Properties** to view the VPN Properties window. | Viewing VPN Properties, page 19-26 |
| VRF | Double-click a VRF to view the VRF properties window. | Viewing VRF Properties, page 19-27 |

*Table 19-7 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 19-27 |
| Link | Double-click a link to view the link properties window. The properties that are depend on the link type. | Chapter 6, "Working with Links" |

# Managing VPNs

The following topics describe:

- Creating a VPN, page 19-21
- Adding a VPN to a Map, page 19-22
- Removing a VPN from a Map, page 19-23
- Moving a Virtual Router Between VPNs, page 19-23

## 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 19-6 on page 19-20).

- 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 19-22.

# 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 19-24
- Managing a VPN Overlay Display in the Map View, page 19-25
- Displaying VPN Callouts in a VPN Overlay, page 19-25


## 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.

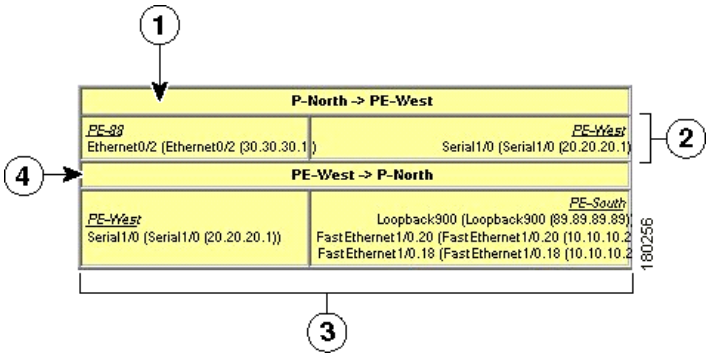
- To remove the VPN overlay, choose **Show Overlay Type > None**.

# 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 19-13) 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 19-13 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 19-26
- Viewing Site Properties, page 19-27
- Viewing VRF Properties, page 19-27
- Viewing VRF Egress and Ingress Adjacents, page 19-31
- Viewing Routing Entities, page 19-31
- Viewing Label Switched Entity Properties, page 19-39
- Viewing MP-BGP Information, page 19-45
- Viewing BFD Session Properties, page 19-47
- Viewing Cross-VRF Routing Entries, page 19-49
- Viewing Pseudowire End-to-End Emulation Tunnels, page 19-50
- Viewing MPLS TE Tunnel Information, page 19-52


## 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 19-8 describes the information that is displayed in the Router IP Interface Properties window:

*Table 19-8 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.<br>**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 18-2. |
| Type | Address type, such as Primary, Secondary, or IPv6 Unicast. |

# Viewing VRF Properties

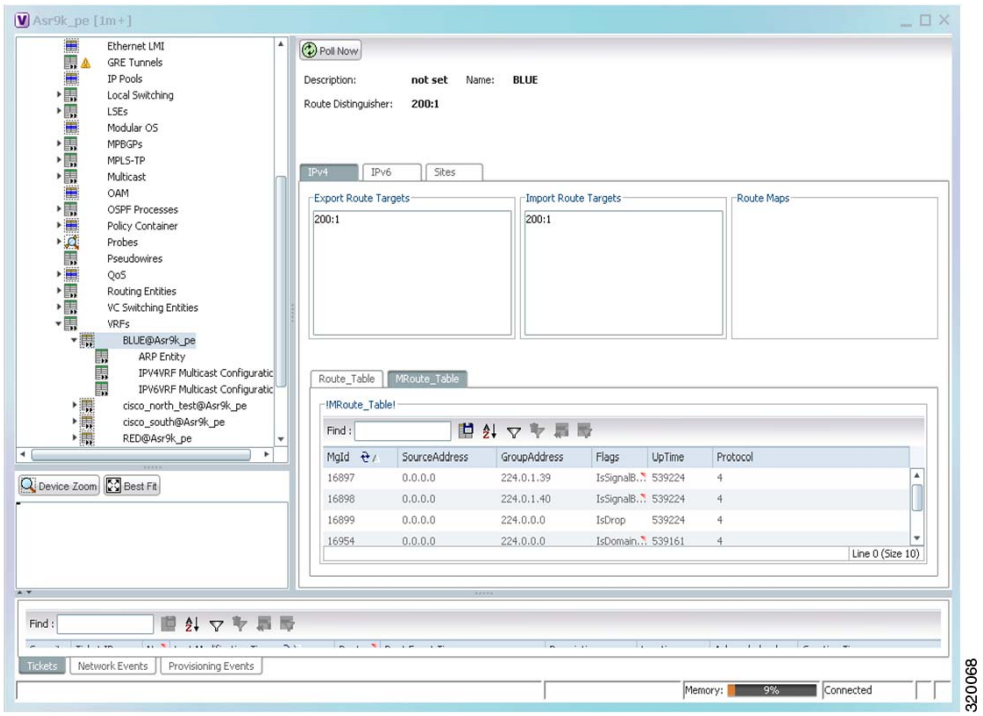
Prime Network Vision enables you to view VRF properties, including the VRF route distinguisher, import and export route targets, and any provisioned sites and VRF routes.

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 19-14.

***Figure 19-14 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 19-9 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 19-9.

***Table 19-9 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. |

*Table 19-9 VRF Properties (continued)*

| Field | Description |
|---|---|
| **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. |
| **MRoute_Table** | |
| Source Address | The source IP address from where the multicast information is sent. |
| Group Address | The group IP address of the multicast. |
| Flags | The flag information pertaining to the multicast. |
| Up Time | The amount of time the interface has been active. |
| Protocol | The protocol information, which can be 4 or 6. |
| **Sites Tab** | |
| Name | Site name. |
| IP Address | IP address of the interface. |
| Mask | Subnet mask. |
| State | State of the subinterface: Up or Down. |
| Associated Entity | Element and interface associated with the site, hyperlinked to its entry in physical inventory. |
| Description | Interface description. |
| Input Access List | Access list applied to the inbound traffic. |
| Output Access List | Access list applied to the outbound traffic. |

*Table 19-9 VRF Properties (continued)*

| Field | Description |
|---|---|
| Rate Limits | If a rate limit is configured on an IP interface, the limit is shown as an IP interface property. This option is checked when a rate limit is defined on the IP interface, meaning the access list is a rate limit access list. IP interface traffic is measured and includes the average rate, normal burst size, excess burst size, conform action, and exceed action.<br>**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 19-36.<br>**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 Multicast Configuration details

To view global multicast configuration details for a VRF:

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

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

Table 19-10 describes the information that is displayed in the Router IP Interface Properties window:

*Table 19-10 Global Multicast Configuration Details*

| Field | Description |
|---|---|
| VPN ID | The VPN ID configured for the VRF. |
| RoutePolicy | The name of the multicast route policy. |
| BgpAD | The BgpAd enabled on the device. |
| MdtSourceif | The Multicast Distribution Tree (MDT) source interface. |
| MdtPartioned | The MDT partitioned permission. |
| NSF | The non-stop forwarding (NSF) information configured for the VRF. |
| MdtAddress | The MDT address. |
| MdtData | The MDT data that can be handled. |
| Address Family | The address family, which can be IPV4 or IPV6. |
| RP Address | The rendezvous point (RP) address configured for the VRF. |

# 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 19-11 describes the information displayed in the Adjacents window.

***Table 19-11 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 19-15.

*Figure 19-15 Routing Entity Table*

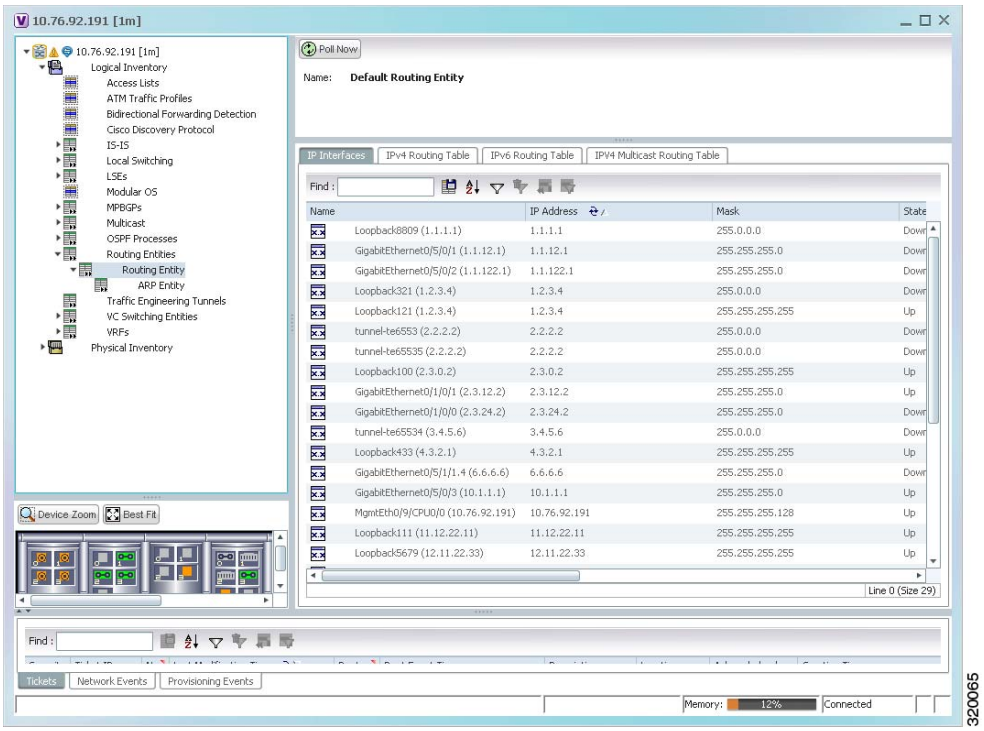



Table 19-12 describes the information that is displayed in the Routing Entity table.

*Table 19-12 Routing Entity Table*

| Field | Description |
|---|---|
| Name | Name of the routing entity. |
| **IP Interfaces Tab** | |
| Name | Site name. |
| IP Address | IP address of the interface. |
| Mask | Network mask. |
| State | State of the subinterface: Up or Down. |
| Associated Entity | Interface associated with the routing entity, hyperlinked to its location in physical inventory. |
| Description | Description of the interface. |
| Input Access List | If an input access list is assigned to an IP interface, the list is shown as an IP interface property, and a hyperlink highlights the related access list in the Access List table. When an access list is assigned to the inbound traffic on an IP interface, the actions assigned to the packet are performed. |

*Table 19-12 Routing Entity Table (continued)*

| Field | Description |
|---|---|
| VRRP Group | If a VRRP group is configured on an IP interface, the information is shown as an IP interface property. This option is checked when a rate limit is defined on the IP interface.<br>**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 19-37. |
| 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.<br>**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 19-36.<br>**Note** The Input Access, Output Access, and Rate Limits parameters apply only to Cisco IOS devices. |
| IP Sec Map Name | IP Security (IPsec) crypto map name. |
| Site Name | Name of the business element to which the interface is attached. |
| **IPv4 and IPv6 Routing Table Tabs** | |
| Destination | Destination of the specific network. |
| Outgoing If Name | Name of the outgoing interface; displayed if the Routing Protocol type is local. |
| Type | Routing type: Direct, Indirect, Static, Other, Invalid, or Unknown. |
| Next Hop | IP address from which to continue to get to a specific address. This field is empty when the routing entry goes to a PE router. |
| Prefix Length | Length of the network prefix in bits. |
| Route Protocol Type | Routing protocol used to communicate with other routers. |
| **IPv4 and IPv6 Multicast Routing Tabs** | |
| Source Address | The source IP address from where the multicast information is sent. |
| Group Address | The group IP address of the multicast. |
| Flags | The flag information pertaining to the multicast. |
| Up Time | The amount of time the interface has been active. |
| Protocol | The protocol information, which can be 4 or 6. |

## 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 19-13 describes the information that is displayed in the ARP table.

*Table 19-13 ARP Table*

| Field | Description |
|---|---|
| MAC | Interface MAC address. |
| Interface | Interface name. |
| IP Address | Interface IP address. |
| State | Interface state:<br>• Dynamic—The entry was learned by the device according to network traffic.<br>• Static—The entry was learned by a local interface or from a user configuring a static route.<br>• Other—The entry was learned by another method not explicitly defined.<br>• 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 19-16 shows an example of the NDP Table tab.

***Figure 19-16 NDP Table in Logical Inventory***

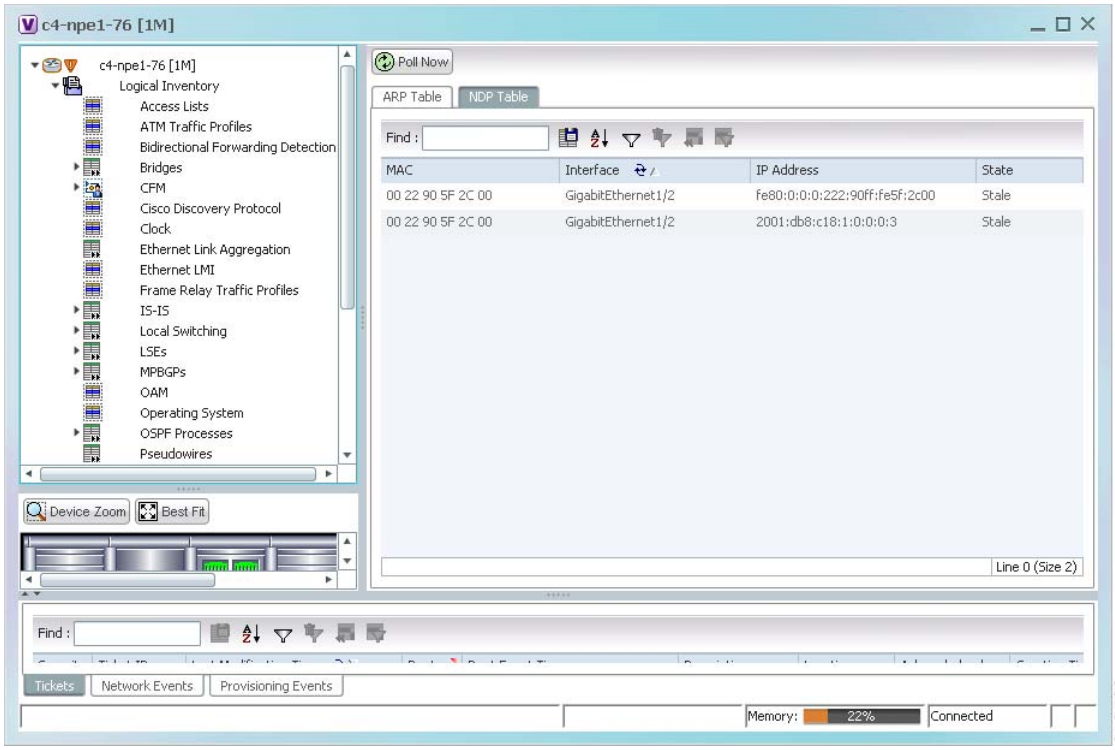



Table 19-14 describes the information displayed for NDP.

*Table 19-14 NDP Table*

| Field | Description |
|---|---|
| MAC | Interface MAC address. |
| Interface | Interface name. |
| IP Address | Interface IPv6 address. |
| Type | Entry type:<br>• 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.<br>• 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.<br>• 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.<br>• 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.<br>• PROBE—A reachability confirmation is actively sought by resending neighbor solicitation messages until a reachability confirmation is received. |

## 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 19-15 describes the information that is displayed in the Rate Limits tab of the IP Interface Properties dialog box.

*Table 19-15 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 19-17 VRRP Properties in IP Interface Properties Window*

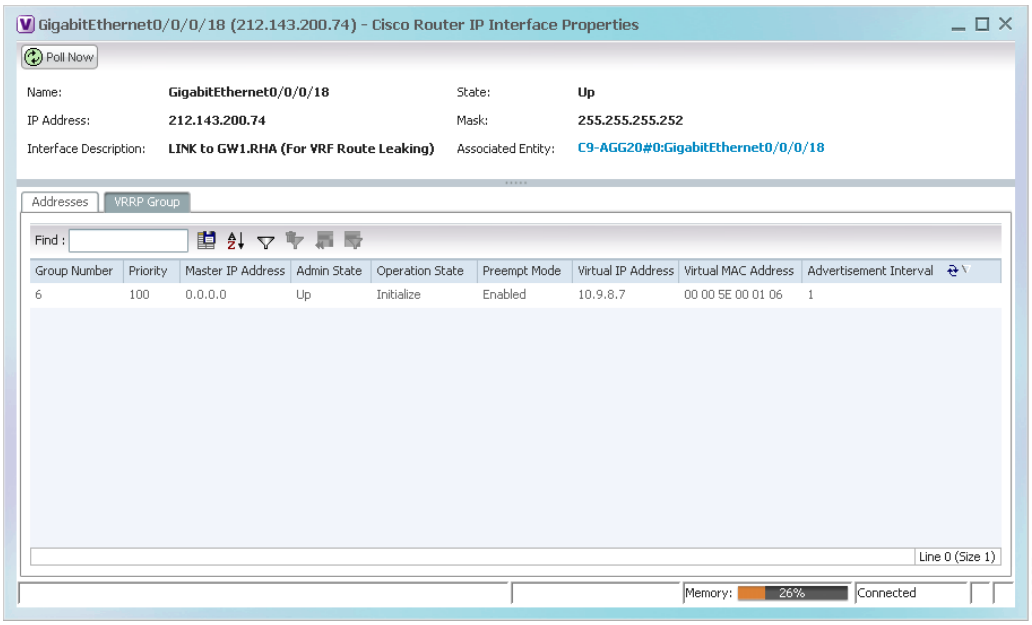



Table 19-16 describes the information in the VRRP Groups tab.

*Table 19-16 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.<br>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 19-17 describes the information that is displayed for label switched entities.

***Table 19-17 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. |

*Table 19-17 Label Switching Properties in Logical Inventory (continued)*

| Field | Description |
|---|---|
| MPLS TE Properties | Whether or not traffic engineering (TE) properties are configured on the interface:<br>• Checked—MPLS TE properties are configured on the interface.<br>• 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. |
| **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. |

*Table 19-17 Label Switching Properties in Logical Inventory (continued)*

| Field | Description |
|---|---|
| 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:<br>• Active—A failure exists in the primary tunnel and the backup is in use.<br>• Not Configured—The primary tunnel has no designated backup tunnel.<br>• Ready—The primary tunnel is in working condition. |
| **MPLS Label Range** | |
| MPLS Label Type | Type of MPLS label: Dynamic or Static. |
| Minimum Label Value | Lowest acceptable MPLS label in the range. |
| Maximum Label Value | Highest acceptable MPLS label in the range. |
| **LDP Neighbors** | |
| LDP ID | Identifier of the LDP peer. |
| Transport IP Address | IP address advertised by the peer in the hello message or the hello source address. |
| Session State | Current state of the session: Transient, Initialized, Open Rec, Open Sent, or Operational. |
| Protocol Type | Protocol used by the peer to establish the session: LDP, TDP, or Unknown. |
| Label Distribution Method | Method of label distribution: Downstream, Downstream On Demand, Downstream Unsolicited, or Unknown. |
| Session Keepalive Interval | Length of time (in milliseconds) between keepalive messages. |
| 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:<br>• Checked—Has one or more discovery sources.<br>• Unchecked—Has no discovery sources.<br>**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 19-18 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 |

# Multicast Label Switching

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

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

## Viewing MLDP Database Information

To view the MLDP database information:

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

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

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

Table 19-19 describes the information that is displayed for **MLDP Database Properties** dialog box.

*Table 19-19 MLDP Database Properties Dialog Box*

| Field | Description |
|---|---|
| LSM ID | The unique ID assigned to a LSP. |
| Tunnel Type | The tunnel type. |
| FEC Root | The root IP address of the MDT. |
| Opaque Value | The stream information that uniquely identifies the tree to the root.<br>To receive label switched multicast packets, the Egress Provider Edge (PE) indicates to the upstream router (the next hop closest to the root) which label it uses for the multicast source by applying the label mapping message. |
| Is Root | Indicates whether Forwarding Equivalence Class (FEC) is the root. |
| **Downstream Clients Tab** | |
| Egress Interface Name | The egress interface name. |
| Associated Entity | The entity associated with the LSP. Click this link to view the associated entity details. |
| Uptime | The amount of time from when the interface is active. |
| Table ID | The unique Table ID of the label through which the packet was received. |
| Ingress State | The status of the ingress interface, which can be **Enabled** or **Disabled**. |
| PPMP State | The status of the Point-to-Point Multipoint, which can be **Enabled** or **Disabled**. |
| Local Label | The label used to identify the label stack of the route within the local VPN network. |

## Viewing the MLDP Neighbors Information

To view information of MLDP neighbors:

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

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

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

Table 19-20 describes the information that is displayed for **Peer ID Properties** dialog box.

*Table 19-20 Peer ID Properties Dialog Box*

| Field | Description |
|---|---|
| Peer ID | The IP address of the MLDP peer. |
| Capabilities | The capabilities supported by the LDP LSR. |
| MLDP GR | Indicates whether graceful restart is enabled for the LDP.<br>**Note** LDP graceful restart provides a control plane mechanism to ensure high availability and allows detection and recovery from failure conditions while preserving Non Stop Forwarding (NSF) services. |
| Path Count | The number of LSP's configured. |
| Uptime | The amount of time from when the peer id is working. |
| **Peer Paths tab** | |
| IP Address | The IP address of the MLDP peer. |
| Interface Name | The interface name. |
| Associated Entity | The link to the associated entity, which when clicked will highlight the associated **Default routing entity** record under the **Routing Entity** node. |
| Protocol | The protocol type used for communication. |
| **Peer Adjacent List** | |
| IP Address | The IP address of the MLDP peer. |
| Interface Name | The interface name. |
| Associated Entity | The link to the associated entity, which when clicked will highlight the associated **Default routing entity** record under the **Routing Entity** node. |

# 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 19-21 describes the information that is displayed for MP-BGP.

*Table 19-21 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 19-18.

***Figure 19-18 6rd Tunnel Properties in Logical Inventory***

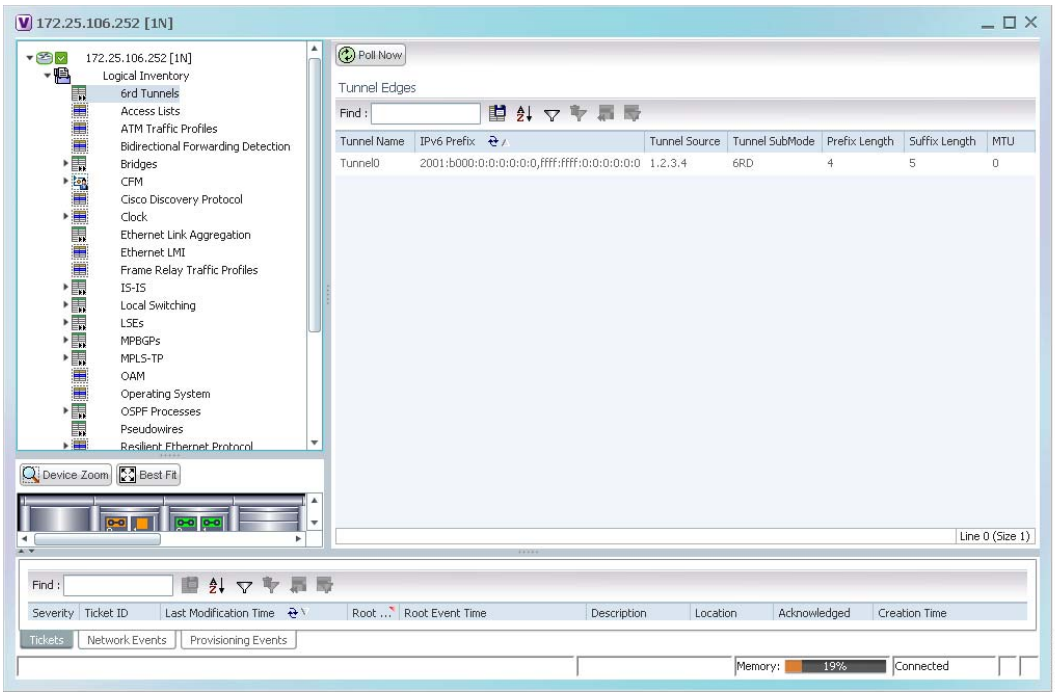



Table 19-22 describes the information displayed for 6rd tunnels.

*Table 19-22 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:<br>• 6rd—Static IPv6 interface.<br>• 6to4—IPv6 address with the prefix embedding the tunnel source IPv4 address.<br>• Auto-tunnel—IPv4-compatible IPv6 tunnel.<br>• 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 19-19.

*Figure 19-19 BFD Session Properties*

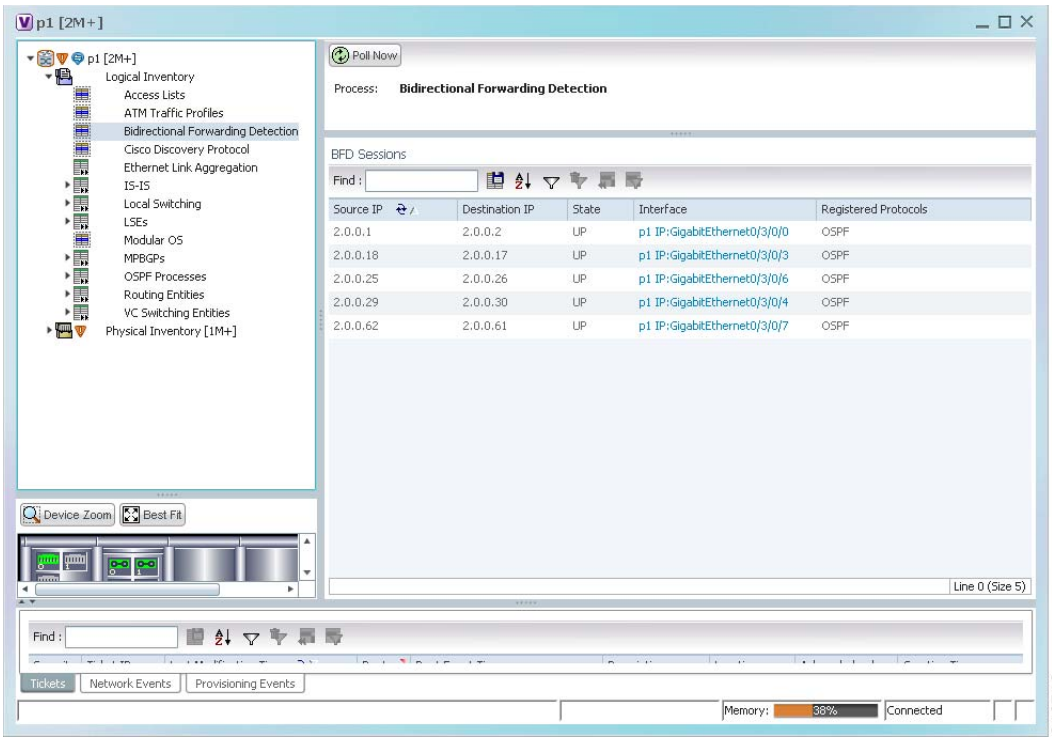



Table 19-23 describes the information displayed for BFD sessions.

*Table 19-23 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 19-24 is displayed.

*Table 19-24 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 19-25 describes the information that is displayed in the Session Properties window.

*Table 19-25 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 19-26.

*Table 19-26 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 19-27.

*Table 19-27 Pseudowires Branch Tunnel Edges Table*

| Field | Description |
|---|---|
| Local Interface | Name of the subinterface or port.<br>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:<br>• Aggregation groups are linked to Ethernet Link Aggregation in logical inventory.<br>• ATM interfaces are linked to the port in physical inventory and the ATM interface.<br>• ATM VCs are linked to the port in physical inventory and the Port IP Properties table.<br>• CEM groups are linked to the port in physical inventory and the CEM Group table.<br>• EFPs are linked to the port in physical inventory and the EFPs table.<br>• IMA groups are linked to IMA Groups in logical inventory.<br>• Local switching entities are linked to Local Switching Entity in logical inventory.<br>• VLANs are linked to Bridges in logical inventory.<br>• 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.<br>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 19-28 describes the information that is displayed in the Tunnel Edges table.

***Table 19-28 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:<br>• Enabled—The tunnel cannot be rerouted.<br>• Disabled—The tunnel can be rerouted. |
| Path Option | Tunnel path option:<br>• Dynamic—The tunnel is routed along the ordinary routing decisions after taking into account the tunnel constraints such as attributes, priority, and bandwidth.<br>• Explicit—The route is explicitly mapped with the included and excluded links. |
| Average Rate (Kbps) | Average bandwidth for this tunnel (in Kb/s). |

*Table 19-28 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 19-40.

# Configuring VRF

VRF commands configures routes that are available or reachable to all the destinations or networks in the VRF.

Unless otherwise noted, all of the following commands are launched by right-clicking the **VRF** node and choosing **Commands > Configuration**.

To run the these commands, the software on the network element must support the technology. Before executing any commands, you can preview them and view the results. For details on the software versions Prime Network supports for the listed supported network elements, see *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

| Command | Description |
|---|---|
| **Modify VRF**<br>**Delete VRF** | Configures VRF properties, including the VRF route distinguisher, import and export route targets, and any provisioned sites and VRF routes. |

# Configuring IP Interface

Unless otherwise noted, all of the following commands are launched by right-clicking the **Routing Entities** and choosing **Commands > Configuration**.

To run the these commands, the software on the network element must support the technology. Before executing any commands, you can preview them and view the results. For details on the software versions Prime Network supports for the listed supported network elements, see *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

| Command | Description |
|---|---|
| **Create Interface** | Configure IP interface as part of the routing entity. |
| **Modify Interface** | |
| **Delete Interface** | |
| **Configure Secondary IP Address** | |
| **Delete Secondary IP Address** | |

# Configuring MPLS-TP

Use these commands to configures MPLS transport profile (MPLS-TP) on the router.

Unless otherwise noted, all of the following commands are launched by right-clicking the appropriate node and selecting **MPLS-TP Global > Commands > Configuration**.

The table below lists the MPLS-TP configuration commands and the MPLS-TP supported network elements.

To run the these commands, the software on the network element must support the technology. Before executing any commands, you can preview them and view the results. For details on the software versions Prime Network supports for the listed supported network elements, see *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

Keep the following in mind:

- LSP Path Lockout can be accessed at both the tunnel level and endpoint level. If you run the command at the tunnel level, you must indicate whether the Lsp is protected or working.
- To run the Global Configuration, BFD Configuration, and Link Configuration commands on the Cisco Carrier Packet Transport (CPT) System, right-click the device in the Prime Network Vision List or Map View, and click **Logical Inventory > CPT Context Container**.

| Command | Description | Supported on: |
|---|---|---|
| **Tunnel Ping**<br>**Tunnel Trace**<br>**LSP Ping**<br>**LSP Trace**<br>**LSP Lockout**<br>**LSP Path Lockout**<br>**LSP Path No Lockout** | These actions are performed at the command the launch point. | • Cisco 7600 Series Routers<br>• Cisco Carrier Packet Transport (CPT) System<br>• Cisco ASR 9000 Series Aggregation Services Routers<br>• Cisco ASR 903 Series Aggregation Services Routers |
| **Add Global Configuration**<br>**Update Global Configuration**<br>**Remove Global Configuration** | Configure Global configuration with Router-id, Global-id, Fault OAM refresh timer value, Wait before restoring timer value.<br>The remove operation is performed at the command the launch point. | |
| **BFD Global Configuration** | BFD minimum interval and multiplier.<br>**Note** Only supported on Cisco ASR 9000. | |
| **Add Link Configuration Remove Link Configuration** | MPLS-TP link number, Next hop router address. Only the link number is require for the remove operation. | |
| **Add BFD Template Configuration**<br>**Remove BFD Template Configuration** | Template type and name, interval type and value, For compute hold down Check/UnCheck Multiplier, multiplier value.<br>The remove operation requires a template type and name. | |
| **Show BFD Template**<br>**Show BFD Template at Tunnel** | Show BFD Template requires a template name. The Show BFD Template at Tunnel is performed at the command launch point. | • Cisco 7600 Series Routers<br>• Cisco Carrier Packet Transport (CPT) System<br>• Cisco ASR 9000 Series Aggregation Services Routers<br>• Cisco ASR 903 Series Aggregation Services Routers |
| **Add Label Range Configuration**<br>**Remove Label Range Configuration** | Minimum and maximum values for dynamic and static labels. The remove operation is performed at the command the launch point.<br>**Note** Not supported on Cisco IOS. | |

# Locking/Unlocking MPLS-TP Tunnels in Bulk

An MPLS-TP network has one or multiple LSPs running between endpoint devices. If you want to shutdown one of the interfaces in the network, the MPLS-TP packet must be diverted through an alternative LSP. This can be achieved by locking the interface.

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

Before attempting to lock or unlock a tunnel, ensure that MPLS-TP tunnels have been configured for the link. Also, ensure that you have the appropriate rights (Configurator and above) to lock or unlock a tunnel.

### Locking MPLS-TP Tunnels

To lock MPLS-TP tunnels in bulk:

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

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

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

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

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

### Unlocking MPLS-TP Tunnels

To unlock MPLS-TP tunnels in bulk:

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

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

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

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

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

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

# Configuring MPLS-TE

Use these commands to configures MPLS-TE on the router. The table below lists the MPLS-TE configuration commands and the MPLS-TE supported network elements.

To run the these commands, the software on the network element must support the technology. Before executing any commands, you can preview them and view the results. For details on the software versions Prime Network supports for the listed supported network elements, see *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

| Command | Navigation | Description[1] | Supported on |
|---|---|---|---|
| **Configure MPLS-TE Global** | **LSEs >** *right-click* **Label Switching > Commands > Configuration >** | Configures MPLS at the device level or an interface level. Contains information on MPLS interfaces and whether traffic engineering tunnels are configured. | • Cisco ASR 9000 Series Routers<br>• Cisco ASR 901 Series Routers<br>• Cisco ASR 903 Series Routers |
| **Configure MPLS-TE Interface** | **Routing Entities > Routing Entity> IP Interfaces** *tab, right-click the required interface* **> Commands > Configuration >** | | Cisco ASR 9000 Series Routers |

1. Modify commands can be used to delete specific attributes, whereas the delete commands deletes the complete configuration.

# Configuring MPLS

Multiprotocol label switching (MPLS) is a high-performance packet forwarding technology that integrates the performance and traffic management capabilities of data link layer (Layer 2) switching with the scalability, flexibility, and performance of network layer (Layer 3) routing. Use these commands to enable MPLS protocol on Cisco routers

To run the these commands, the software on the network element must support the technology. Before executing any commands, you can preview them and view the results. For details on the software versions Prime Network supports for the listed supported network elements, see *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

| Command | Navigation | Description[1] | Supported on |
|---|---|---|---|
| **Configure MPLS Discovery** | **LSEs >** *right-click* **Label Switching > Commands > Configuration >** | Configure MPLS LDP discovery parameters to discover core MPLS networks. This also includes specifying the discovery method. | • Cisco ASR 9000 Series Routers<br>• Cisco ASR 901 Series Routers<br>• Cisco ASR 903 Series Routers |
| **Configure MPLS Label Range** | | Configures MPLS static and dynamic label range. | |
| **Enable MPLS on Interface** | **LSEs > Label Switching >** right-click on a selected ID in the **MPLS Interface** tab **Commands > Configuration >** | Enables/disables MPLS protocol on an interface. | |
| **Disable MPLS on Interface** | | Contains information on MPLS interfaces and whether traffic engineering tunnels are configured on an interface. | |

1. Modify commands can be used to delete specific attributes, whereas the delete commands deletes the complete configuration.

# Configuring RSVP

Use RSVP commands to establish a reserved-bandwidth path between hosts or the end systems to predetermine and ensure Quality of Service (QoS) for their data transmission.

To run the these commands, the software on the network element must support the technology. Before executing any commands, you can preview them and view the results. For details on the software versions Prime Network supports for the listed supported network elements, see *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

| Command | Navigation | Description[1] | Supported on: |
|---|---|---|---|
| **Configure RSVP** | **LSEs >** right-click **Label Switching > Commands > Configuration >** | Configure RSVP on a device or an interface. | • Cisco ASR 9000 Series Routers<br>• Cisco ASR 901 Series Routers<br>• Cisco ASR 903 Series Routers |
| **Delete RSVP** | | | Cisco ASR 9000 Series Routers |
| **Enable RSVP On Interface**<br>**Disable RSVP On Interface** | **Routing Entities > Routing Entity> IP Interfaces** *tab, right-click the required interface* **> Commands > Configuration** | | • Cisco ASR 9000 Series Routers<br>• Cisco ASR 901 Series Routers<br>• Cisco ASR 903 Series Routers |

1. Modify commands can be used to delete specific attributes, whereas the delete commands deletes the complete configuration.

# Configuring BGP

Multiprotocol BGP is an enhanced BGP that carries routing information for multiple network layer protocols and IP multicast routes. BGP commands configure the routing protocol to communicate with the other sites and VRFs.

**Note** BGP neighbors should be configured as part of BGP routing. At least one neighbor and at least one address family must be configured to enable BGP routing.

The table below lists the commands that will be used to configure BGP Routing Protocol on Cisco Routers.

To run the these commands, the software on the network element must support the technology. Before executing any commands, you can preview them and view the results. For details on the software versions Prime Network supports for the listed supported network elements, see *Cisco Prime Network Supported Cisco VNEs*.

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

| Command | Navigation | Description[1] | Supported on |
|---|---|---|---|
| **Create BGP Router**<br>**Modify BGP Router**<br>**Delete BGP Router** | **MPBGPs >** *right-click* **MPBGP > Commands > Configuration >** | Configures BGP routing and establish a BGP routing process with AS number and Router ID | • Cisco ASR 5000 Series Mobile-Gateway<br>• Cisco ASR 9000 Series Routers<br>• Cisco ASR 901 Series Routers<br>• Cisco ASR 903 Series Routers |
| **Create BGP Address Family**<br>**Modify BGP Address Family**<br>**Delete BGP Address Family** | | Enter various address family configuration modes that uses IPv4, IPv6, L2VPN, VPNV4 or VPNV6 address prefixes. | |
| **Create BGP Neighbor** | | Places the router in neighbor configuration mode for BGP routing and configures the neighbor IP address as a BGP peer. | |
| **Modify BGP Neighbor**<br>**Delete BGP Neighbor** | **MPBGP > MPBGP >** *right-click on the BGP neighbour in the content pane* **> Commands > Configuration >** | | |

1. Modify commands can be used to delete specific attributes, whereas the delete commands deletes the complete configuration.

# Configuring VRRP

The Virtual Router Redundancy Protocol (VRRP) feature allows for transparent failover at the first-hop IP router, enabling a group of routers to form a single virtual router. VRRP Command will be used to configure VRRP protocol on Cisco router.

These commands configures transparent failover at the first-hop IP router, enabling a group of routers to form a single virtual router.

To run the these commands, the software on the network element must support the technology. Before executing any commands, you can preview them and view the results. For details on the software versions Prime Network supports for the listed supported network elements, see *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

| Command | Navigation | Description[1] | Supported on: |
|---|---|---|---|
| **Create VRRP Group**<br>**Delete VRRP Interface** | **Routing Entities > Routing Entity> IP Interfaces** *tab, right-click the required interface* **> Commands > Configuration** | Configure a group of routers to form a single virtual router.<br>Example is using VRRP group as default router on the client. The LAN clients can be configured with the virtual router as their default gateway thus avoiding single point of failure, which was the case in dynamic discovery protocol. | Cisco ASR 9000 Series Routers |
| **Modify VRRP Group**<br>**Delete VRRP**<br>**Show VRRP** | **Routing Entities > Routing Entity> IP Interfaces** *tab, double-click on the VRRP configured interface* **>** *select* **VRRP Group** *tab* **>** *right-click on required group.* | | |

1. Modify commands can be used to delete specific attributes, whereas the delete commands deletes the complete configuration.

# Configuring Bundle Ethernet

Configure a bundle of one or more ports to form a single link using bundle ethernet commands.

To run the these commands, the software on the network element must support the technology. Before executing any commands, you can preview them and view the results. For details on the software versions Prime Network supports for the listed supported network elements, see *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

| Command | Navigation | Description[1] | Supported on: |
|---|---|---|---|
| **Bundle Ethernet** | | | |
| **Configure Bundle Ethernet** | **Physical Inventory > Chassis > Slot > Ethernet Port > Commands > Configuration >** | Configuring an Ethernet link bundle involves creating a bundle and adding member interfaces to that bundle. | • Cisco ASR 9000 Series Routers<br>• Cisco ASR 901 Series Routers<br>• Cisco ASR 903 Series Routers |

1. Modify commands can be used to delete specific attributes, whereas the delete commands deletes the complete configuration.

CHAPTER 20

# Viewing IP and MPLS Multicast Configurations

These topics provide an overview of the IP Multicast technology and describe how to view IP and multicast configurations in Prime Network Vision:


- IP and MPLS Multicast Configuration - An Overview, page 20-1
- User Roles Required to View IP and Multicast Configurations, page 20-2
- Viewing the Multicast Configurations, page 20-2


## IP and MPLS Multicast Configuration - An Overview

IP Multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to thousands of corporate recipients and homes. Applications that take advantage of multicast include video conferences, corporate communications, distance learning, and distribution of software, stock quotes, and news.

IP Multicast delivers source traffic to multiple receivers without adding any additional burden on the source or the receivers while using the least network bandwidth of any competing technology. Multicast packets are replicated in the network by Cisco routers enabled with Protocol Independent Multicast (PIM), Multicast Label Distribution Protocol (MLDP) and other supporting multicast protocols resulting in the most efficient delivery of data to multiple receivers possible.

Multicast is based on the concept of a group. An arbitrary group of receivers expresses an interest in receiving a particular data stream. This group does not have any physical or geographical boundaries—the hosts can be located anywhere on the Internet. Hosts that are interested in receiving data flowing to a particular group must join the group using Internet Group Management Protocol (IGMP). Hosts must be a member of the group to receive the data stream.

In Prime Network, IP and multicast support is available for the following network elements:

- Cisco Aggregation Service Router (ASR) 9000 series network elements
- Cisco Carrier Routing System (CRS) network elements
- Cisco Gigabit Switch Router (GSR) network elements

# User Roles Required to View IP and Multicast Configurations

This topic identifies the roles that are required to work with IP and Multicast Support. 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 3.10 Administrator Guide*.

***Table 20-1 Default Permission/Security Level Required for IP and Multicast Support***

| Task | Viewer | Operator | OperatorPlus | Configurator | Administrator |
|---|---|---|---|---|---|
| View multicast configuration details | X | X | X | X | X |
| View Multicast Label Switch details | X | X | X | X | X |
| View Routing entities | X | X | X | X | X |
| View VRF Properties | X | X | X | X | X |

# Viewing the Multicast Configurations

This topic contains the following sections:

- Viewing Multicast Node, page 20-2
- Viewing Multicast Protocols, page 20-4
- Multicast Label Switching, page 20-9
- Multicast Routing Entities, page 20-10

## Viewing Multicast Node

To view the Multicast node:

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

**Step 2** In the Inventory window, choose **Logical Inventory > Multicast**. The Route Policies and Multicast Global Interfaces tabs are displayed in the content pane as show in Figure 20-1. You can click on the tabs to view more details.

*Figure 20-1 Multicast Content Pane*

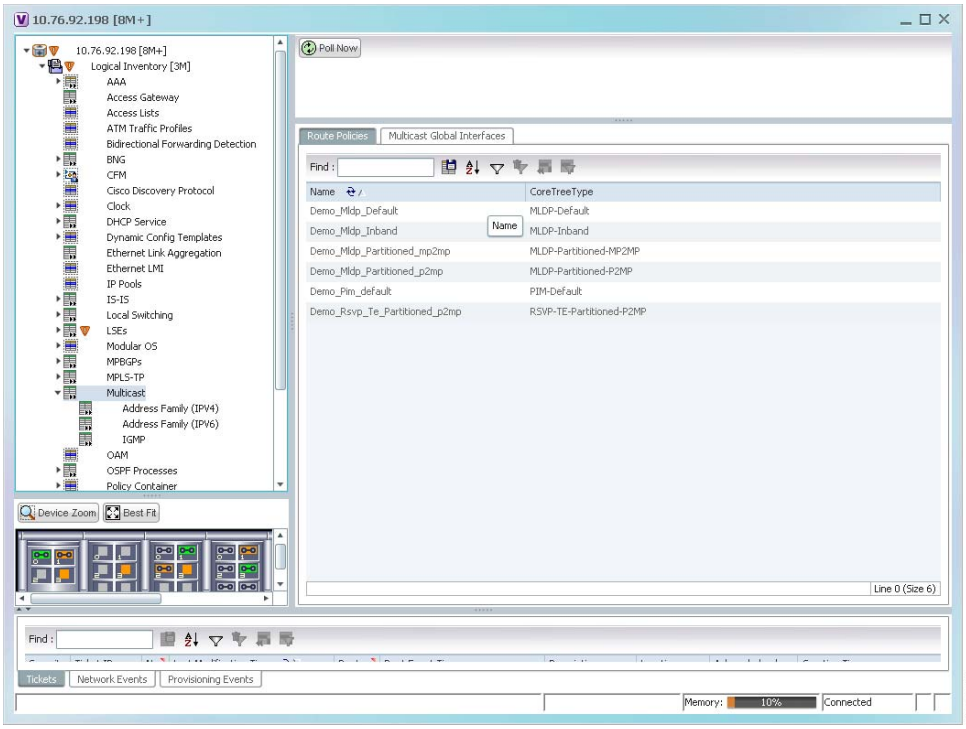



Table 20-2 describes the fields that are displayed in the Route Policies tab.

*Table 20-2 Route Policies Tab*

| Field Name | Description |
|---|---|
| Name | The name of the multicast route policy. |
| Core Tree Type | The type of the Multicast Distribution Tree (MDT) core tree configured in the route policy. Values are:<br>• MLDP-Default<br>• MLDP-Inband<br>• MLDP-Partitioned-MP2MP<br>• MLDP-Partitioned-P2MP<br>• PIM-Default<br>• RSVP-TE-Partitioned-P2MP |
| **Multicast Global Interfaces Tab** | |
| Interface Name | The name of the multicast enabled logical or physical interface. |
| Associated Entity | The link to the associated routing entity, which when clicked will highlight the associated **Default routing entity** record under the **Routing Entity** node. |

# Viewing Multicast Protocols

The following Multicast protocols are available in Prime Network:

- Address Family (IPv4)—See Viewing the Address Family (IPv4) Profile, page 20-4.
- Address Family (IPv6)—See Viewing the Address Family (IPv6) Profile, page 20-5.
- IGMP—Viewing the IGMP profile, page 20-5.
- PIM—Viewing the PIM Profile, page 20-7.

## Viewing the Address Family (IPv4) Profile

To view the Address Family (IPv4) profile:

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

**Step 2** In the Inventory window, choose **Logical Inventory > Multicast > Address Family (IPV4)**. The profile details are displayed in the content pane.

Table 20-3 describes the fields that are displayed in the **Address Family (IPV4)** profile**.**

*Table 20-3 Address Family (IPV4) Profile*

| Field Name | Description |
|---|---|
| MDT Source Interface | The source interface to set the multicast VPN data.<br>**Note** This interface can identify the root of the MDT in the service provider network. This interface and its corresponding address is used to update all Multicast VPN (MVPN) peers through multiprotocol Border Gateway Protocol (BGP). |
| MDT Static | The interface used for transporting MDT data. |
| Interface All | Indicates whether the multicast routing and protocols are enabled on the interfaces.<br>**Note** You must enable the interfaces using the Interface command in the multicast-routing configuration mode. |
| NSF Status | Indicates whether the non-stop forwarding capability is enabled for all the relevant components.<br>**Note** If this feature is enabled, then multicast forwarding will not stop on failure of the control plane multicast routing components. |
| Address Family | The address family, which in this instance is IPV4. |
| MDT MLDP | Indicates whether the Multicast Distribution Tree (MDT) Multipoint Extensions to Label Distribution Protocol (MLDP) in-band signalling is enabled. |

## Viewing the Address Family (IPv6) Profile

To view the Address Family (IPv6) profile:

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

**Step 2** In the Inventory window, choose **Logical Inventory > Multicast > Address Family (IPV6)**. The profile details are displayed in the content pane.

Table 20-4 describes the fields that are displayed in the **Address Family (IPV6)** profile**.**

*Table 20-4 Address Family (IPV6) profile*

| Field Name | Description |
|---|---|
| Interface All | Indicates whether the multicast routing and protocols are enabled on the interface.<br>**Note** You must enable the interfaces using the Interface command in the multicast-routing configuration mode. |
| NSF Status | Indicates whether the non-stop forwarding capability is enabled for all the relevant components.<br>**Note** If this feature is enabled, then multicast forwarding will not stop if the control plane multicast routing components fail. |
| Address Family | The address family, which in this instance is IPV6. |
| MDT MLDP | Indicates whether the Multicast Distribution Tree (MDT) Multipoint Extensions to Label Distribution Protocol (MLDP) in-band signalling is enabled. |
| MDT Static | The interface used for transporting MDT data. |
| MDT Source Interface | The source interface to set the multicast VPN data.<br>**Note** This interface can identify the root of the MDT in the service provider network. This interface and its corresponding address is used to update all Multicast VPN (MVPN) peers through multiprotocol Border Gateway Protocol (BGP). |

## Viewing the IGMP profile

The IGMP runs between hosts and their immediately neighboring multicast routers. The mechanisms of the protocol allow a host to inform its local router that it wishes to receive transmissions addressed to a specific multicast group. Also, routers periodically query the LAN to determine if known group members are still active. If there is more than one router on the LAN performing IP multicasting, one of the routers is elected querier and assumes the responsibility of querying the LAN for group members. Based on the group membership information learned from the IGMP, a router is able to determine which (if any) multicast traffic needs to be forwarded to each of its leaf sub networks. Multicast routers use this information, in conjunction with a multicast routing protocol, to support IP multicasting across the Internet.

There are three versions of IGMP:

- **IGMP Version 1**
- **IGMP Version 2**
- **IGMP Version 3**

To view the IGMP profile:

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

**Step 2** In the **Inventory** window, choose **Logical Inventory > Multicast > IGMP**. The IGMP details are displayed in the content pane. You can click on the tabs to view more details.

Table 20-5 describes the fields that are displayed in the **IGMP** profile**.**

***Table 20-5 IGMP Profile Details***

| Field Name | Description |
|---|---|
| NSF Status | The non-stop forwarding status, which can be **Normal** or **Non-Stop Forwarding Activated**.<br>**Note** The Non-Stop Forwarding Activated status implies that recovery of an IGMP failure is in progress. |
| **Interfaces Tab** | |
| Interface Name | The name of the interface. |
| Associated Entity | The link to the associated entity, which when clicked will highlight the associated **Default routing entity** record under the **Routing Entity** node. |
| Interface Address | The internet address of the interface. |
| VRF | The VRF to which the interface belongs. This is a link, which when clicked will take you to the relevant record under the **VRF** node. |
| IGMP Status | Indicates whether IGMP is enabled or disabled on the interface. |
| IGMP Version | The IGMP version installed on the interface. |
| **Groups Tab** | |
| Group Address | The address of the multicast group. |
| Interface Name | The name of the interface used to reach the group. |
| Associated Entity | The associated entity for the IGMP profile. Click this link to view the related record under the Subscriber Access Point node. |
| VRF | The VPN Routing and Forwarding (VRF) to which the interface belongs. This is a link, which when clicked will take you to the relevant record under the VRF node. |
| Up Time | The period from when the multicast group is available. This information is displayed in terms of hours, minutes, and seconds. |
| Expires | The duration after which the multicast group will be removed from the IGMP groups table. This information is displayed in terms of hours, minutes, and seconds. |
| Last Reporter | The most recent host that has reported being a member of the multicast group. |

*Table 20-5 IGMP Profile Details (continued)*

| Field Name | Description |
|---|---|
| **Group Ranges Tab** | |
| Group Range | The multicast group range in CDIR format, which is basically the Multicast Group IP address followed by the CDIR prefix. |
| Protocol | The PIM protocol that is used by the IGMP group range. |

## Viewing the PIM Profile

PIM is a family of multicast routing protocols for Internet Protocol (IP) networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN or the Internet. It is termed protocol-independent because PIM does not include its own topology discovery mechanism, but instead uses routing information supplied by other traditional routing protocols such as the Routing Information Protocol, Open Shortest Path First, Border Gateway Protocol and Multicast Source Discovery Protocol. There are four variants of PIM:

- PIM Sparse Mode (PIM-SM)
- PIM Dense Mode (PIM-DM)
- Bidirectional PIM
- PIM source-specific multicast (PIM-SSM)

Although PIM is called a multicast routing protocol, it actually uses the unicast routing table to perform the Reverse Path Forwarding (RPF) check function instead of building up a completely unrelated multicast routing table. PIM does not send and receive multicast routing updates between routers like other routing protocols.

To view the PIM profile:

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

**Step 2** In the Inventory window, choose **Logical Inventory > Multicast > PIM**. The profile details are displayed in the content pane. You can click on the tabs to view more details.

Table 20-6 describes the fields that are displayed in the **PIM** profile**.**

*Table 20-6 PIM Profile Details*

| Field Name | Description |
|---|---|
| NSF Status | The non-stop forwarding status, which can be **Normal** or **Non-Stop Forwarding Activated**.<br>**Note** The Non-Stop Forwarding Activated status implies that recovery of an IGMP failure is in progress. |
| **Interfaces Tab** | |
| Interface Name | The name or ID of the interface on which PIM is enabled. |
| Associated Entity | The link to the associated entity, which when clicked will highlight the associated **Default routing entity** record under the **Routing Entity** node. |

*Table 20-6 PIM Profile Details (continued)*

| Field Name | Description |
|---|---|
| IP Address | The IP address of the interface. |
| VRF | The name of the VRF associated to the interface. This is a link, which when clicked will take you to the relevant record under the **VRF** node. |
| PIM Status | Indicates whether the PIM is enabled (ON) or disabled (OFF) on the interface. |
| Hello Interval | The frequency at which PIM hello messages are sent over the PIM enabled interfaces.<br>These messages are sent at regular intervals by routers on all the PIM enabled interfaces. The router sends these messages to advertise their existence as a PIM router on the subnet. |
| Designated Router | The IP address of the designated router on the LAN.<br>**Note** Serial lines do not have a designated router. Hence, the IP address is displayed as 0.0.0.0. If the interface on the router is the designated router, then the words "This system" is displayed. If not, then the IP address of the external neighbor is displayed. |
| Designated Router Priority | The priority of the designated router, which is advertised by the neighbor in the hello messages. This value in this field will range from 0 to 4294967295 |
| **Rendezvous Points Tab** | |
| RP Address | The address of the interface serving as a rendezvous point for the group range or list.<br>A Rendezvous Point (RP) is a router in a multicast network domain that acts as a shared root for a multicast shared tree. Any number of routers can be configured to work as RPs and they can be configured to cover different group ranges. For correct operation, every multicast router within a Protocol Independent Multicast (PIM) domain must be able to map a particular multicast group address to the same RP. |
| Mode | The PIM protocol mode for which the router is advertised as a rendezvous point. The mode can be **PIM-SM** or **bidirectional PIM**. |
| Scope | The number of candidate announcement messages sent out from the rendezvous point. |
| Priority | The value of the candidate rendezvous point priority. |
| Uptime | The amount of time from when the rendezvous point is available. |
| Group List | The IP access list number or name of the group prefixes that are advertised in association with the rendezvous point address. |
| RP Type | The type of rendezvous point, which can be **BSR** or **Auto RP**.<br>**Note** The **Bootstrap Router** (BSR) is a mechanism for a router to learn RP information. It ensures that all routers in the PIM domain have the same RP cache as the BSR. **Auto-RP** is a mechanism to automate distribution of RP information in a multicast network. The Auto-RP mechanism operates using two basic components, the candidate RPs and the RP mapping agents. |

*Table 20-6 PIM Profile Details (continued)*

| Field Name | Description |
|---|---|
| **Topology Tab** | |
| Source Address | The IP address of the source of the multicast entry. In case the IP address is not available, a "*" or 0.0.0.0 is displayed here. |
| Group Address | The multicast group address or prefix for which the entry is associated with. |
| PIM Mode | The PIM mode of the topology entry, which can be Sparse, Source Specific, Dense, or Bidirectional. |
| Tree Type | The MDT tree type for the route entry, which can be **Shortest Path Tree** or Rendezvous Point Tree. |
| Uptime | The amount of time from which the topology is available. This value is displayed in terms of seconds. |
| RP Address | The Rendezvous Point address. This value is displayed only if the PIM Mode is SM or Bidirectional. |
| Join Prune Status | Indicates whether a join or prune message is sent to the RPF neighbor for the route. |
| RPF | The IP address and interface ID, along with the MoFFR information, of the Reverse Path Forwarding for the topology. |
| Flags | The comma separated flag information for this topology. |
| **Neighbors Tab** | |
| Neighbor IP Address | The IP address of the neighbor. |
| Interface Name | The interface name on which the neighbor can be reached. |
| Associated Entity | The link to the associated entity, which when clicked will highlight the associated **Default routing entity** record under the **Routing Entity** node. |
| VRF | The name of the VRF. |
| Flags | The flags that provide information about various states of the neighbor. |
| Designated Router Priority | The priority of the PIM interface for DR election. The default value is 1. |
| UpTime | The amount of time from which the interface is available. |

# Multicast Label Switching

Prime Network provides multicast support for MPLS services.

For more information on multicast label switching, see Multicast Label Switching, page 19-42.

# Multicast Routing Entities

Prime Network provides multicast support for routing entities. If you have configured multicast route information for a VRF, Prime Network displays a separate tab for the related VRF wherein you can view the multicast routing information.

For details on multicast routing entities, see Viewing Routing Entities, page 19-31 and Viewing VRF Properties, page 19-27.

CHAPTER 21

# 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 21-1
- Viewing SAToP Pseudowire Type in Logical Inventory, page 21-2
- Viewing CESoPSN Pseudowire Type in Logical Inventory, page 21-3
- Viewing Virtual Connection Properties, page 21-5
- Viewing IMA Group Properties, page 21-13
- Viewing TDM Properties, page 21-16
- Viewing Channelization Properties, page 21-17
- Viewing MLPPP Properties, page 21-26
- Viewing MLPPP Link Properties, page 21-29
- Viewing MPLS Pseudowire over GRE Properties, page 21-31
- Network Clock Service Overview, page 21-34
- Viewing CEM and Virtual CEM Properties, page 21-50
- Configuring SONET, page 21-54
- Configuring Clock, page 21-56
- Configuring TDM and Channelization, page 21-59
- Configuring Automatic Protection Switching (APS ), page 21-61


# 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 3.10 Administrator Guide*.

The following tables identify the tasks that you can perform:

- Table 21-1 identifies the tasks that you can perform if a selected element **is not in** one of your assigned scopes.
- Table 21-2 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 3.10 Administrator Guide*.

*Table 21-1 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 |
| Using SONET Configure, Clear, and Show Commands | — | — | — | X | X |

*Table 21-2 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 |
| Using SONET Configure, Clear, and Show Commands | — | — | — | 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:

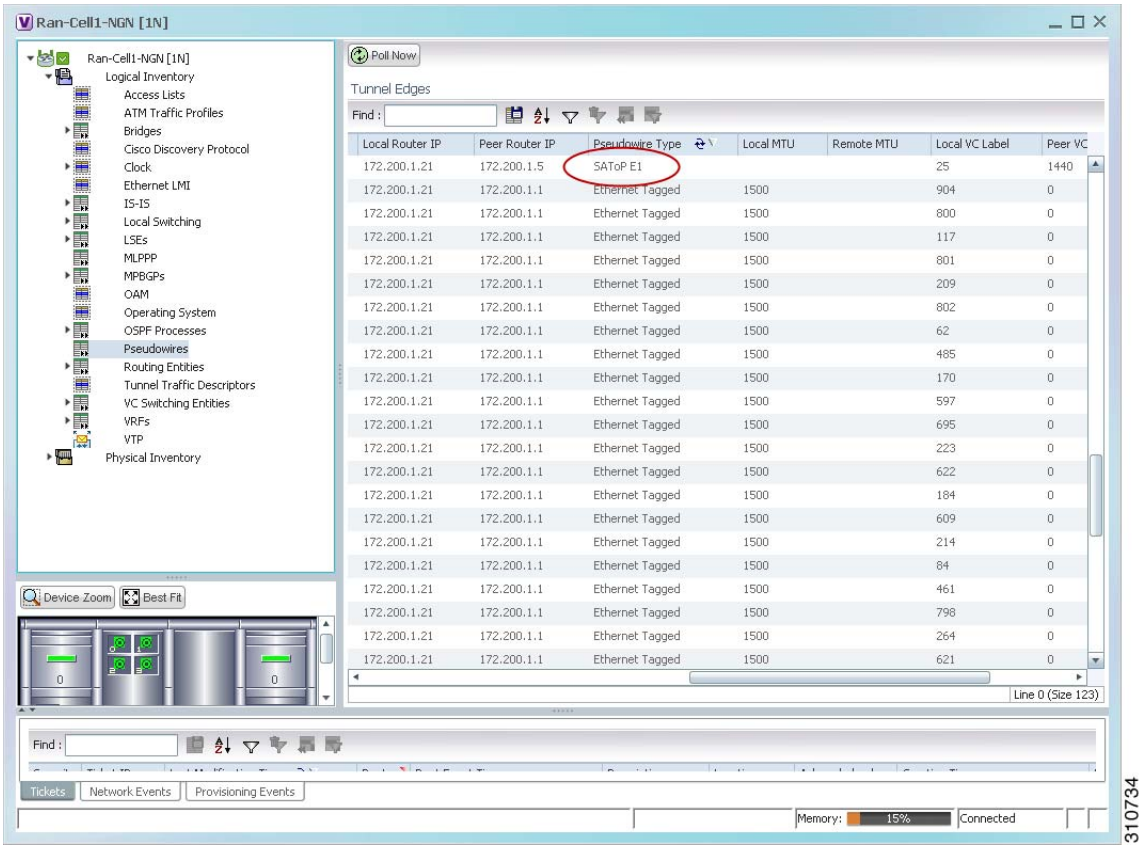
**Step 1** In Prime Network Vision, right-click the device on which SAToP is configured, then choose **Inventory**.

**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 21-1.

**Note** You can also view this information by right-clicking the entry in the table and choosing **Properties**.

*Figure 21-1 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:

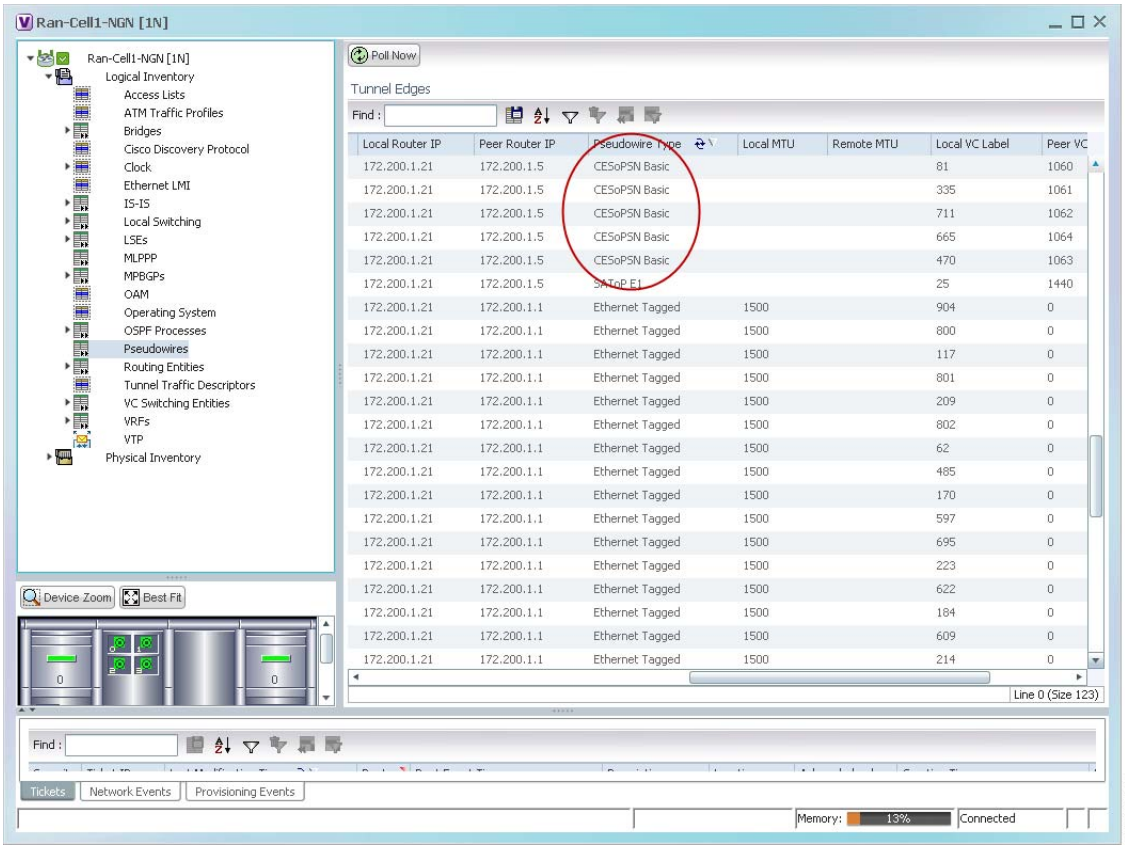
**Step 1** In Prime Network Vision, right-click the device on which CESoPSN is configured, then choose **Inventory**.

**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 21-2.

**Note** You can also view this information by right-clicking the entry in the table and choosing **Properties**.

*Figure 21-2 CESoPSN Pseudowire Type in Logical Inventory*




**Step 4** To view the physical inventory for the port, click the hypertext port link.

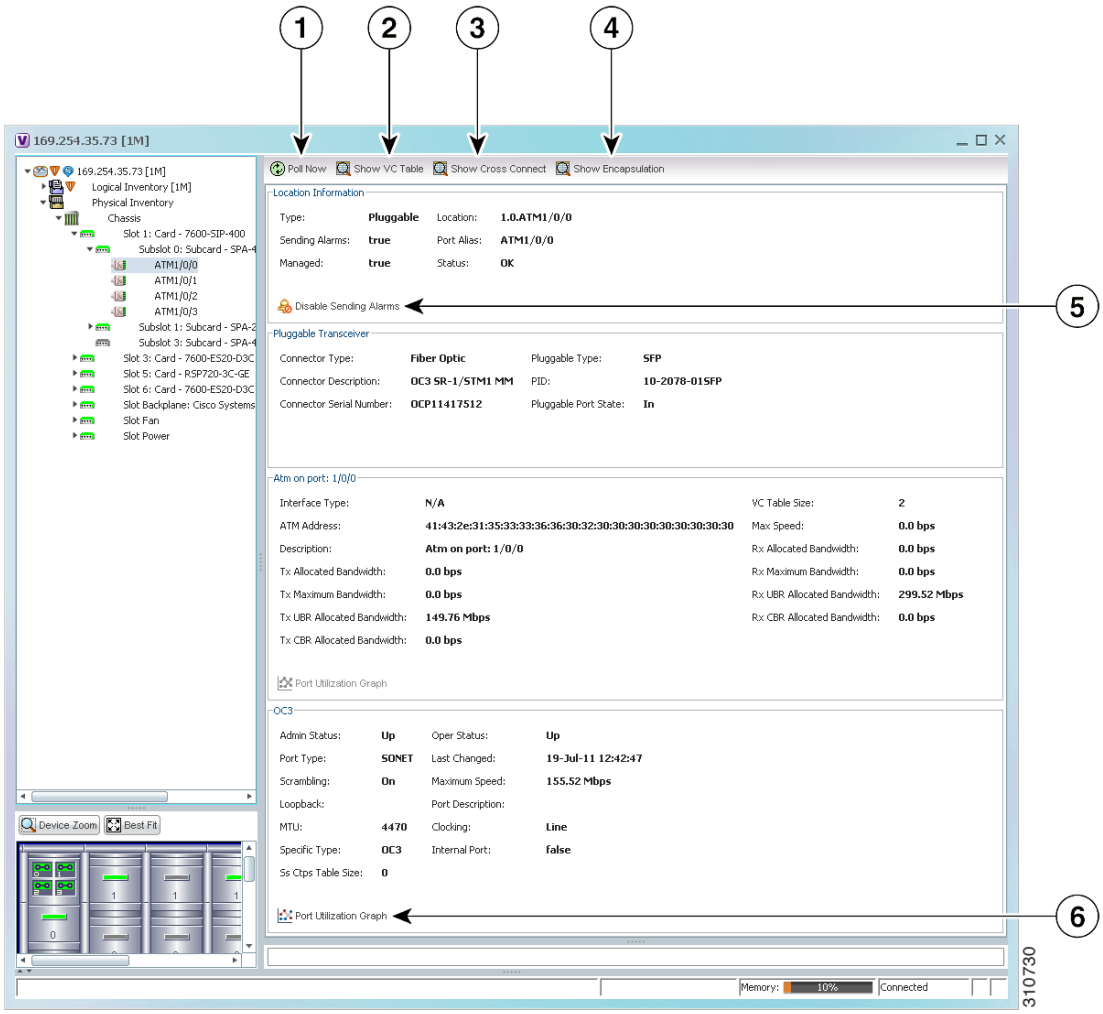
# Viewing Virtual Connection Properties

The following topics describe how to view properties related to virtual connections:

- Viewing ATM Virtual Connection Cross-Connects, page 21-6
- Viewing ATM VPI and VCI Properties, page 21-10
- Viewing Encapsulation Information, page 21-11

Buttons for viewing these properties are available at the top of the physical inventory window for the selected interface, as shown in Figure 21-3.

***Figure 21-3 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.<br>For more information, see Viewing ATM VPI and VCI Properties, page 21-10. |
| **3** | Show Cross Connect button | Displays cross-connect information for incoming and outgoing ports.<br>For more information, see Viewing ATM Virtual Connection Cross-Connects, page 21-6. |
| **4** | Show Encapsulation button | Displays encapsulation information for incoming and outgoing traffic for the selected item.<br>For more information, see Viewing Encapsulation Information, page 21-11. |
| **5** | Disable/Enable Sending Alarms button | Enables you to manage the alarms on a port.<br>For more information, see Working with Ports, page 3-23. |
| **6** | Port Utilization Graph button | Displays the selected port traffic statistics: Rx/Tx Rate and Rx/Tx Rate History.<br>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 21-10.

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 21-4.
- 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 21-4 ATM Virtual Connection Cross-Connect Properties***

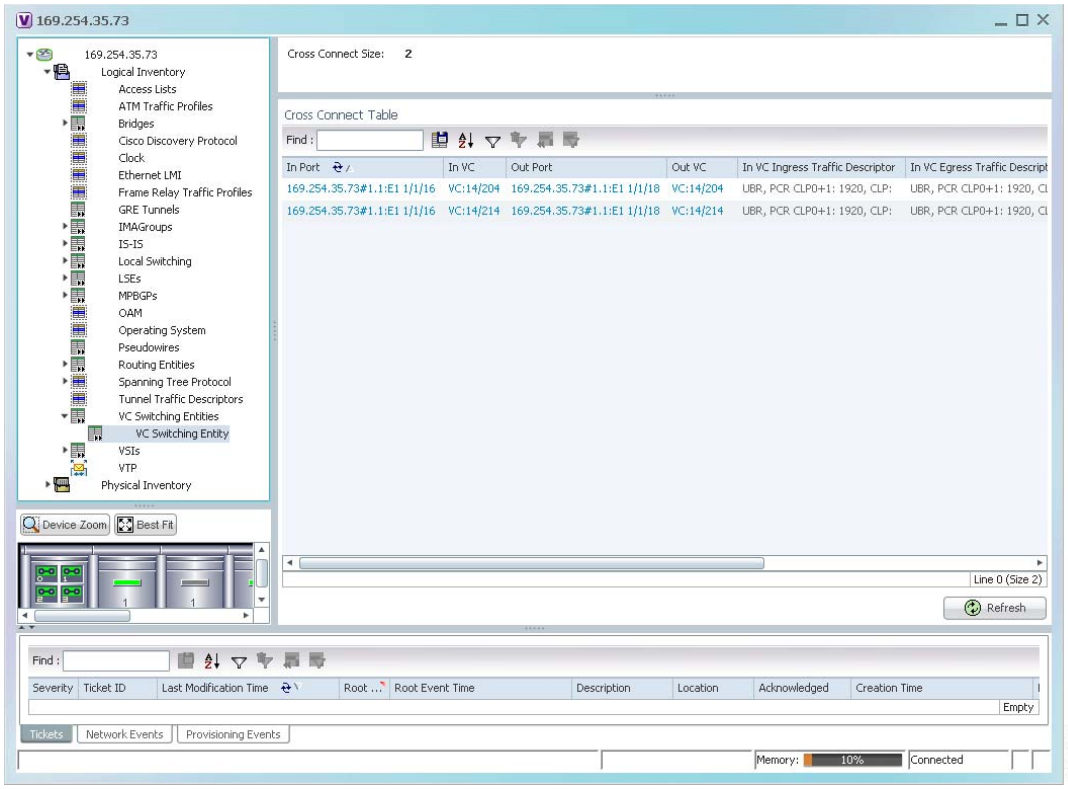



Table 21-3 identifies the properties that are displayed for ATM VC cross-connects.

*Table 21-3 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.<br>You can view additional details about the virtual connection in the following ways:<br>• Click the hyperlinked entry to view the VC table.<br>• 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.<br>You can view additional details about the virtual connection in the following ways:<br>• Click the hyperlinked entry to view the VC table.<br>• 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.<br>For information on VC traffic descriptors, see Table 21-4. |
| In VC Egress Traffic Descriptor | ATM traffic parameters and service categories for the outgoing traffic on the incoming VC cross-connect.<br>For information on VC traffic descriptors, see Table 21-4. |
| Out VC Egress Traffic Descriptor | ATM traffic parameters and service categories for the outgoing traffic on the outgoing VC cross-connect.<br>For information on VC traffic descriptors, see Table 21-4. |
| Out VC Ingress Traffic Descriptor | ATM traffic parameters and service categories for the incoming traffic on the outgoing VC cross-connect.<br>For information on VC traffic descriptors, see Table 21-4. |

*Table 21-4 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 21-5.

***Figure 21-5 VC Table***

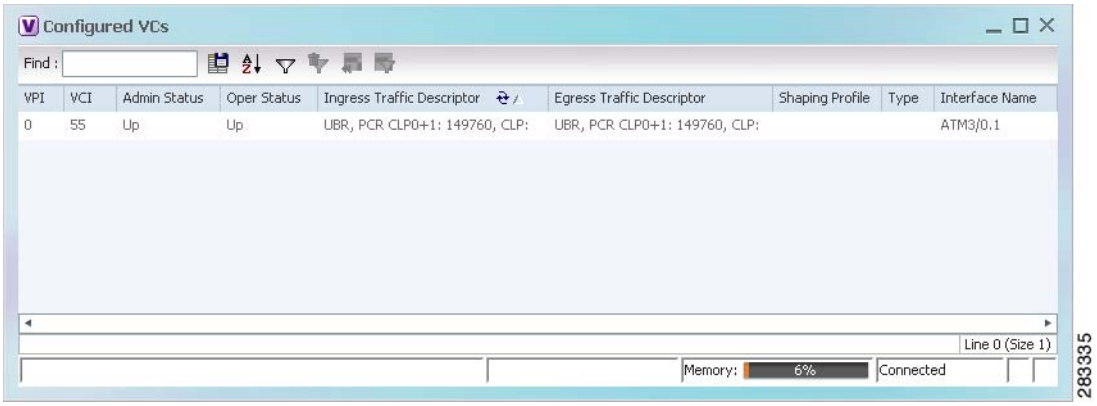



Table 21-5 describes the information displayed in the VC Table window.

*Table 21-5 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.<br>For information on VC traffic descriptors, see Table 21-4. |
| Egress Traffic Descriptor | Traffic parameters and service categories for the outgoing traffic.<br>For information on VC traffic descriptors, see Table 21-4. |
| 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 21-6.

*Figure 21-6 VC Encapsulation Properties*

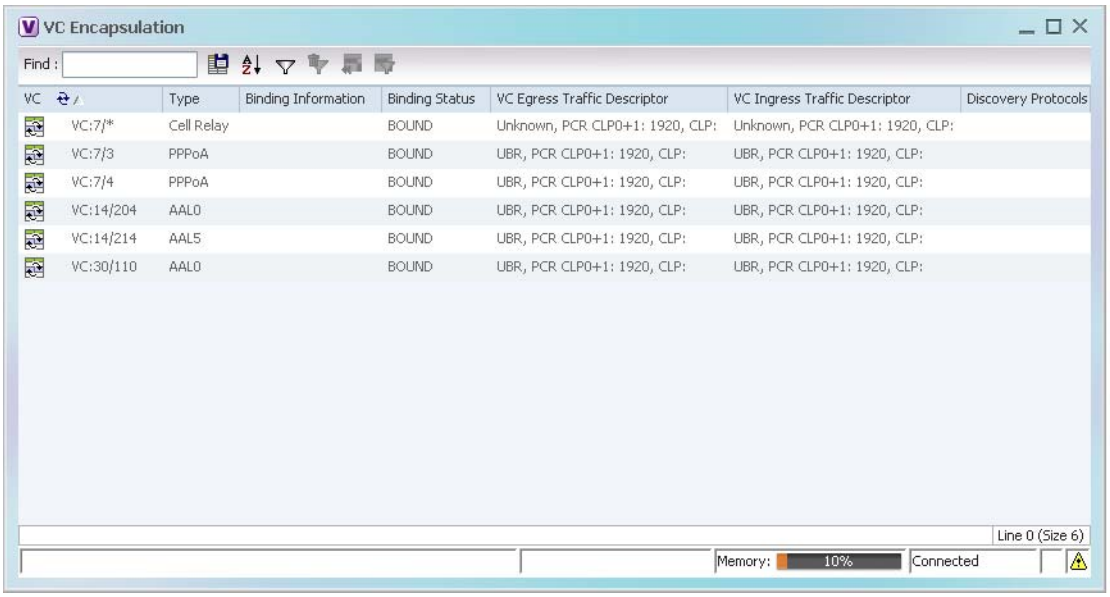



Table 21-6 describes the information displayed in the VC Encapsulation window.

*Table 21-6 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.<br>For information on VC traffic descriptors, see Table 21-4. |
| VC Ingress Traffic Descriptor | Traffic parameters and service categories for the incoming traffic.<br>For information on VC traffic descriptors, see Table 21-4. |
| 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 21-7.

***Figure 21-7 IMA Group Properties***

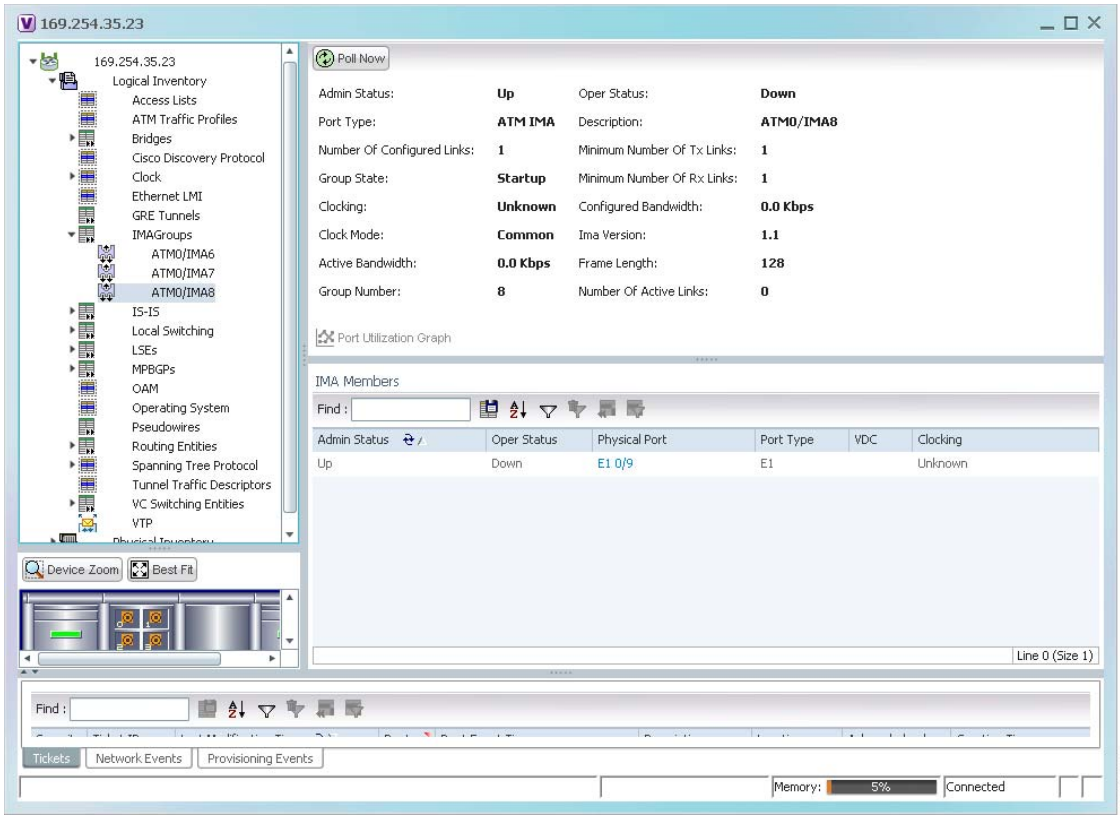



Table 21-7 describes the information displayed for the IMA group.

***Table 21-7 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:<br>• Common—Common transmit clocking (CTC).<br>• 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 21-7 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.<br>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:<br>• 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.<br>• Startup ACK—Both sides of the link are enabled.<br>• 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.<br>• 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.<br>• 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.<br>• 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:<br>• Dormant—The interface is dormant.<br>• Down—The interface is down.<br>• Not Present—An interface component is missing.<br>• Testing—The interface is in test mode.<br>• Unknown—The interface has an unknown operational status.<br>• Up—The interface is up. |
| Port Type | Type of port, such as ATM IMA. |

Table 21-8 describes the information displayed in the IMA Members table.

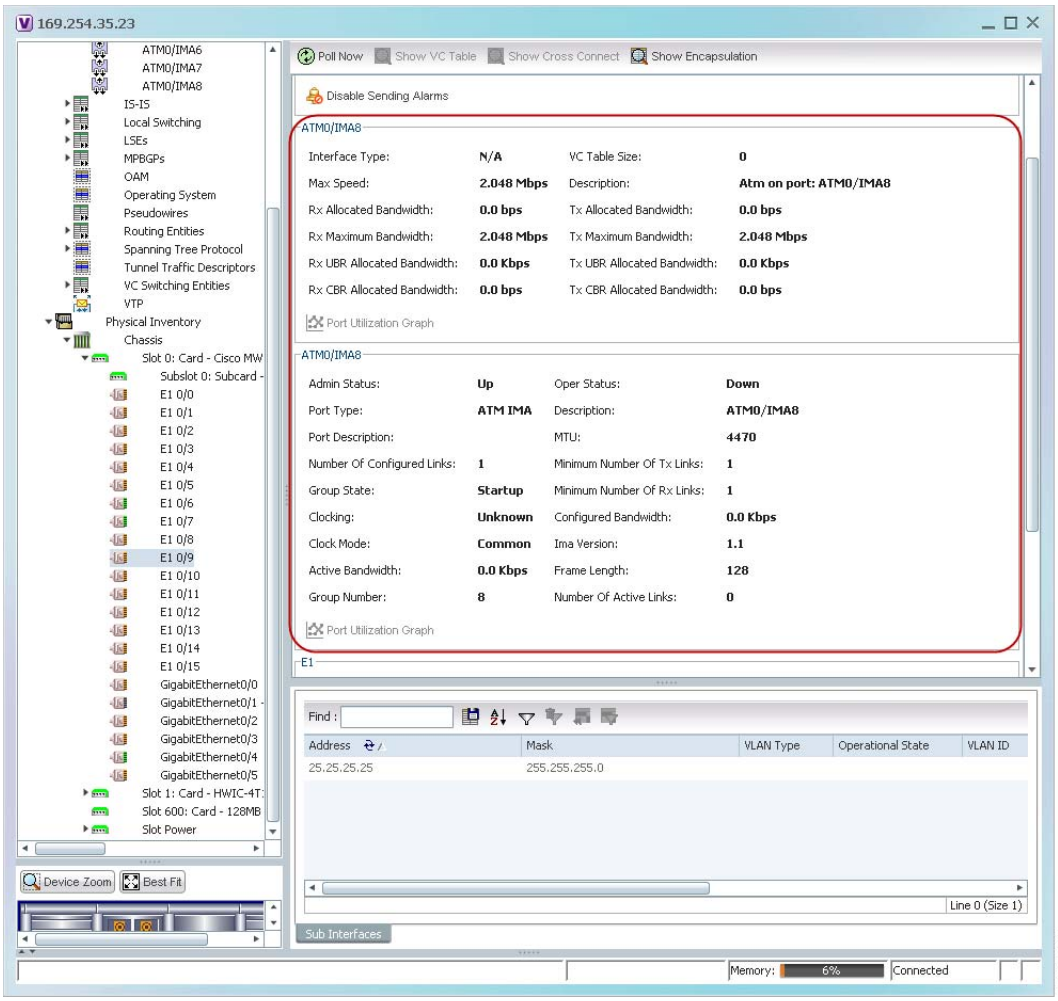
*Table 21-8 IMA Members Table*

| Column | Description |
|---|---|
| Admin Status | Administrative status of the IMA member. |
| Channelization | Channelization that occurs through the path, such as STS1-> VTG-> VT15.<br>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 21-8.

The information that is displayed for the port in physical inventory depends on the type of connection, such as SONET or ATM.

*Figure 21-8 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 21-9 are displayed in physical inventory in addition to the existing T1 or E1 properties.

*Table 21-9 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:<br>• 0—The international bit is not used.<br>• 1—The international bit is used.<br>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:<br>• 0—The national reserve bits are not used.<br>• 1—The national reserve bits are used.<br>This property applies only to E1. |
| Line Code | Line encoding method for the DS1 link:<br>• For E1, the options are Alternate Mark Inversion (AMI) and high-density bipolar of order 3 (HDB3).<br>• 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.

For SONET show and configuration commands, see Configuring SONET, page 21-54.

The following topics describe how to view channelization properties for SONET/SDH and T3 lines:

- Viewing SONET/SDH Channelization Properties, page 21-18
- Viewing T3 DS1 and DS3 Channelization Properties, page 21-21

# Viewing SONET/SDH Channelization Properties

SONET and SDH use the same concepts for channelization, but the terminology differs. Table 21-10 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 21-10 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 21-9.

***Figure 21-9 SONET/SDH Interface in Physical Inventory***

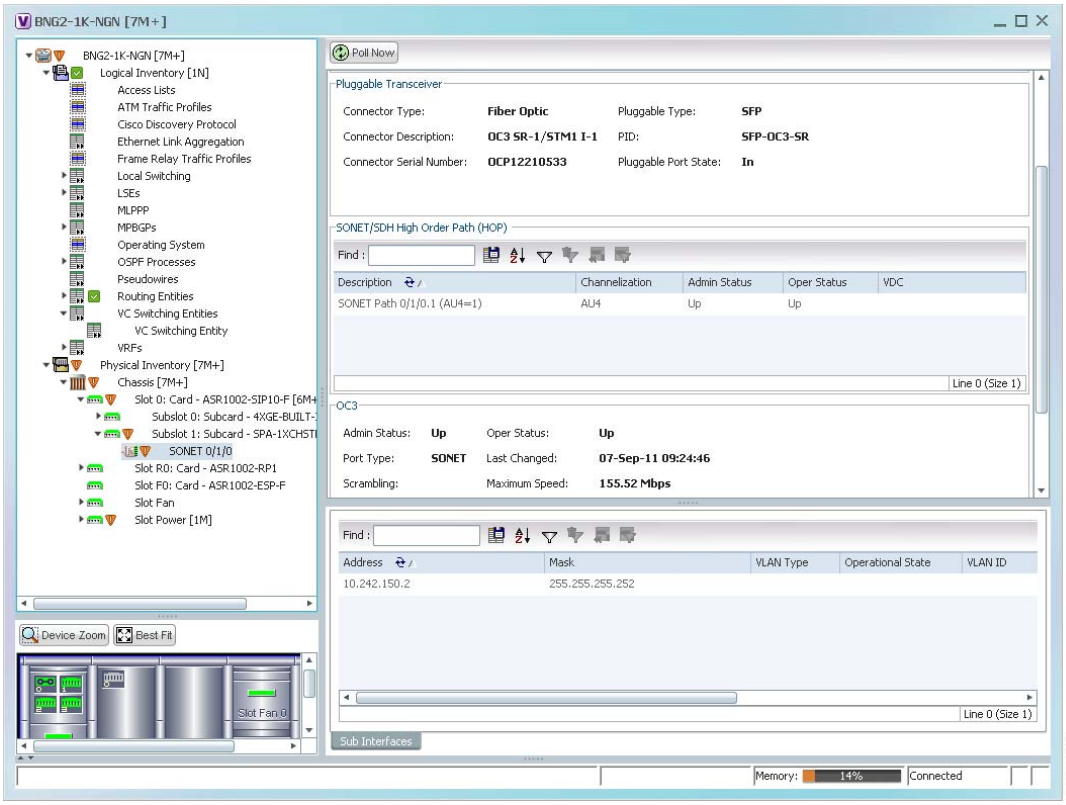


Table 21-11 describes the information that is displayed for SONET/SDH and OC3 in the content pane.

*Table 21-11 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 21-10.

*Figure 21-10 SONET/SDH High Order Path Properties Window*

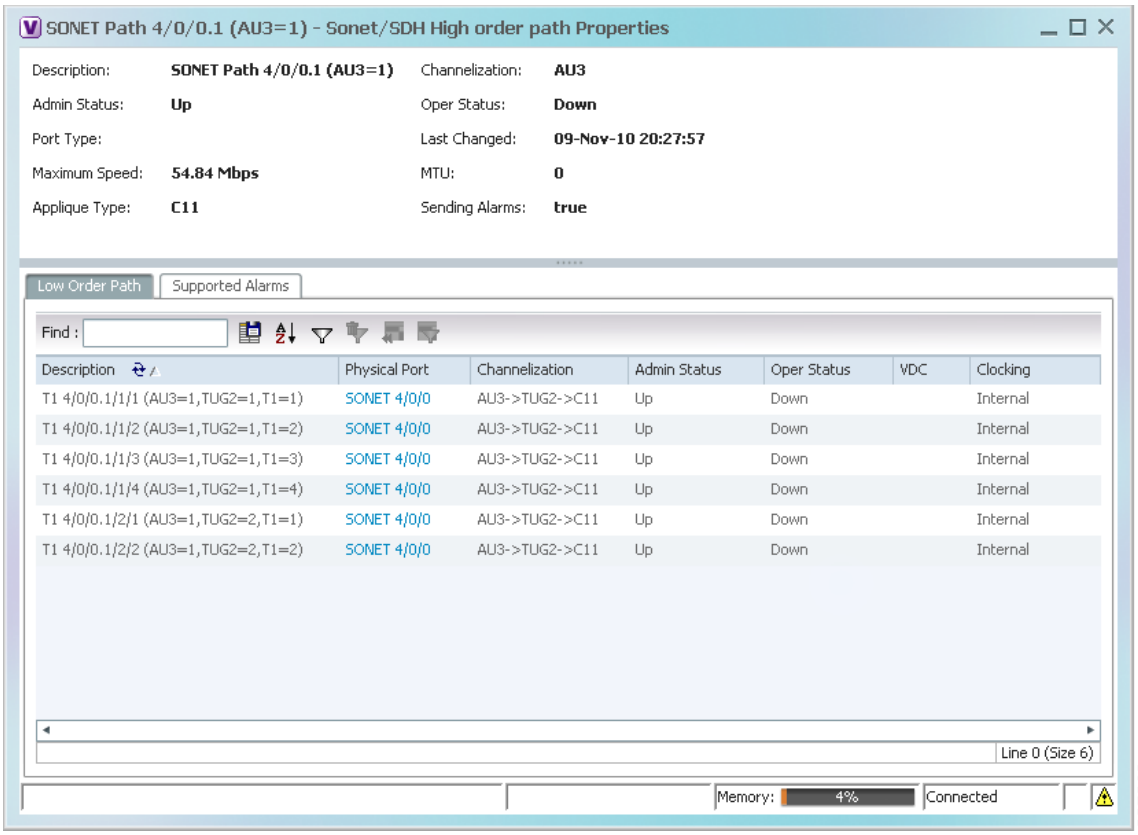



Table 21-12 describes the information displayed in SONET/SDH High Order Path Properties window.

*Table 21-12 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 21-12 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 21-11 shows DS1 channelization properties for T3 in physical inventory.

*Figure 21-11 T3 DS1 Channelization Properties in Physical Inventory*

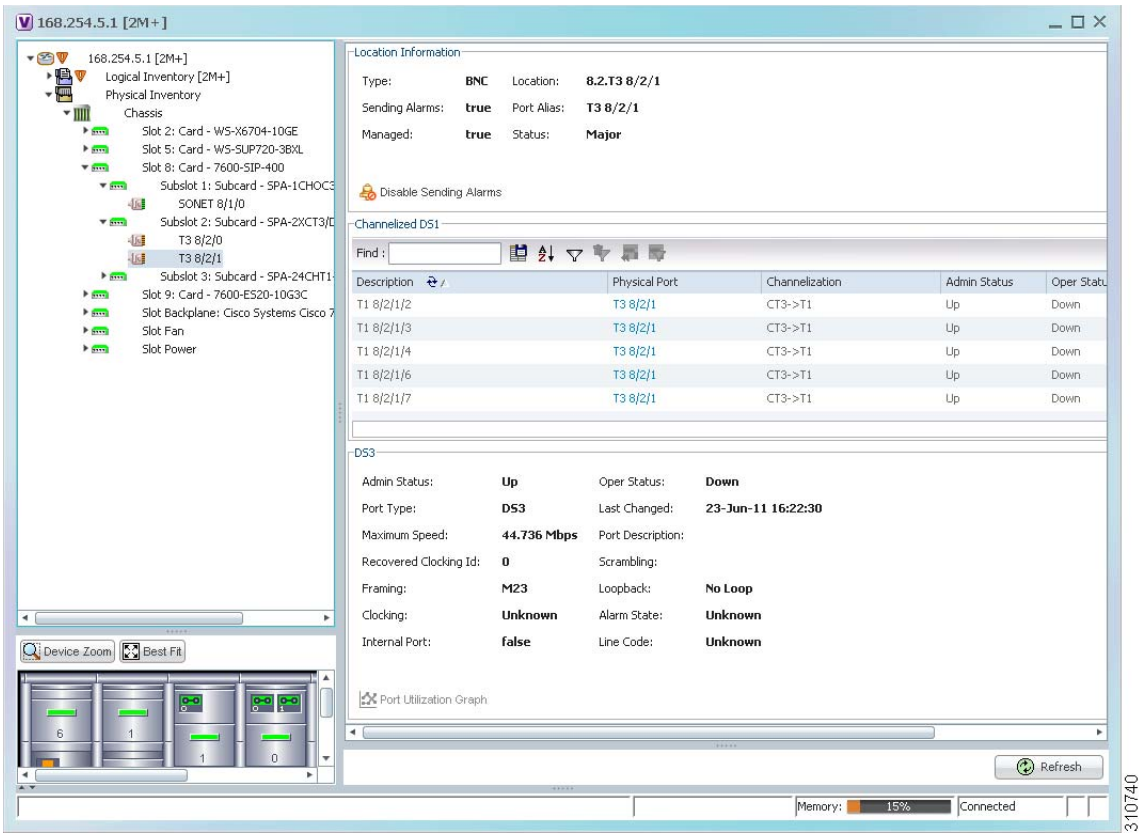



Table 21-13 describes the information that is displayed for Channelized DS1 and DS3 in the content pane.

*Table 21-13 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 21-13 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:<br>• Clear—The alarm state is clear.<br>• AIS—Alarm Indication Signal (AIS).<br>• LOS—Loss of signal (LOS) alarm.<br>• AIS_LOS—AIS loss of signal alarm.<br>• LOF—Loss of frame (LOF) alarm.<br>• AIS_LOF—AIS loss of frame alarm.<br>• LOS_LOF—Loss of signal and loss of frame alarm.<br>• AIS_LOS_LOF—AIS loss of signal and loss of frame alarm.<br>• 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 21-12 shows the information that is displayed in the Channelized DS1 PDH Properties window.

*Figure 21-12 Channelized DS1 PDH Properties Window*

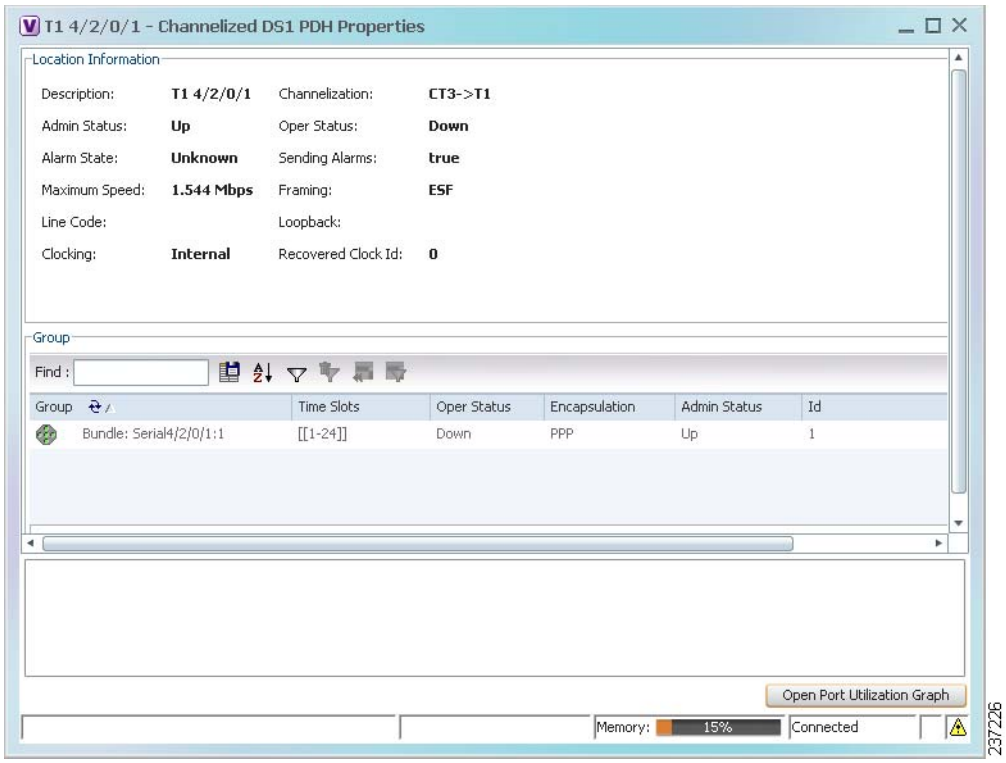



Table 21-14 describes the information that is displayed in the Channelized DS1 PDH Properties window.

*Table 21-14 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 21-14 Channelized DS1 PDH Properties Window (continued)*

| Field | Description |
|---|---|
| Alarm State | Alarm state of the DS1 line:<br>• Clear—The alarm state is clear.<br>• AIS—Alarm Indication Signal (AIS).<br>• LOS—Loss of signal (LOS) alarm.<br>• AIS_LOS—AIS loss of signal alarm.<br>• LOF—Loss of frame (LOF) alarm.<br>• AIS_LOF—AIS loss of frame alarm.<br>• LOS_LOF—Loss of signal and loss of frame alarm.<br>• AIS_LOS_LOF—AIS loss of signal and loss of frame alarm.<br>• 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 21-13.

***Figure 21-13 MLPPP Properties in Logical Inventory***

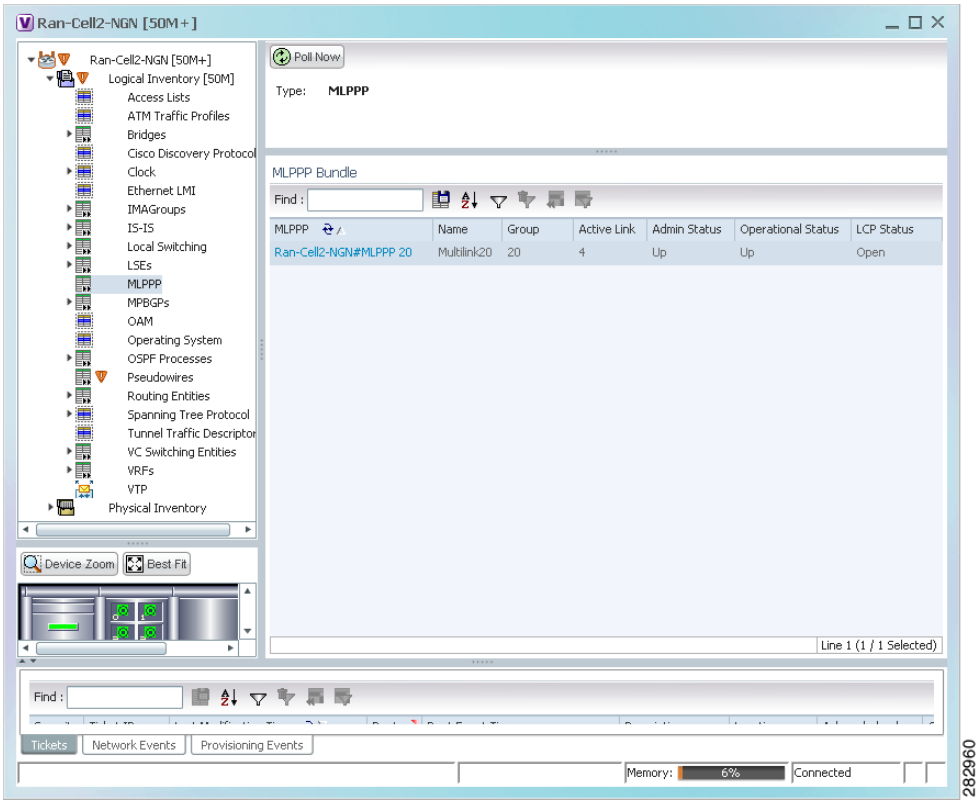


Table 21-15 describes the information that is displayed for MLPPP.

*Table 21-15 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 21-14.

*Figure 21-14 MLPPP Bundle Properties Window*

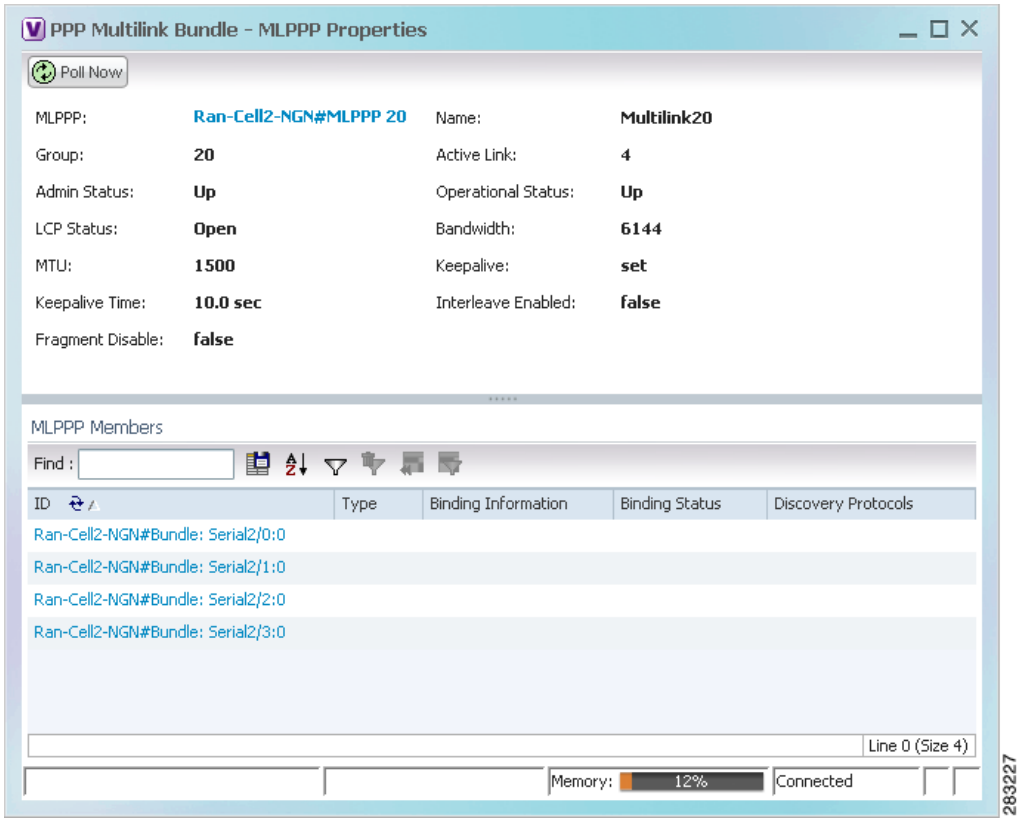


Table 21-16 describes the information that is displayed in the MLPPP Properties window.

*Table 21-16 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 21-16 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.

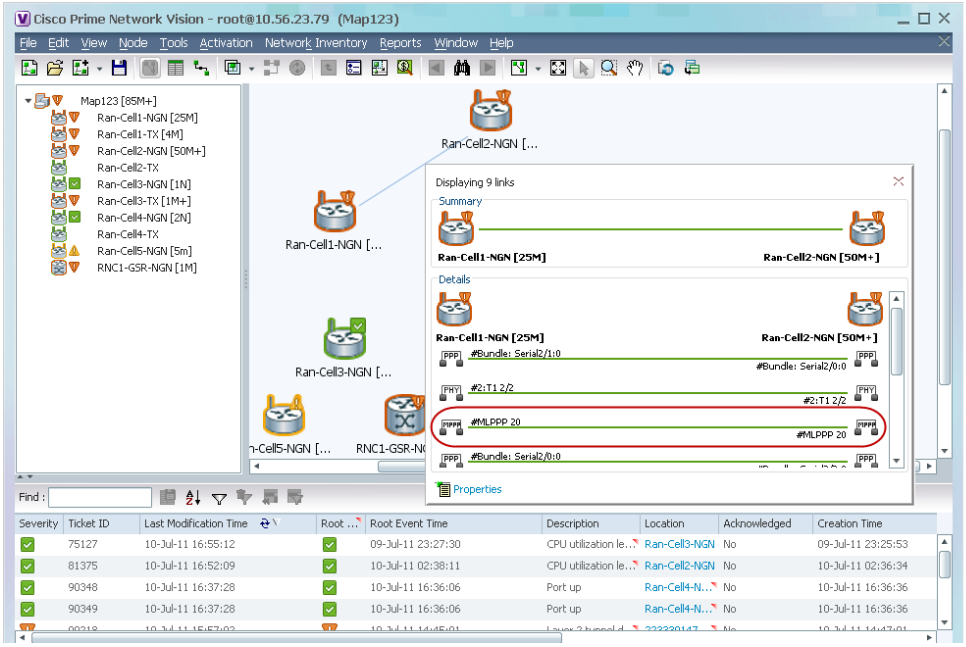
# Viewing MLPPP Link Properties

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 21-15.

*Figure 21-15 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 21-16.

***Figure 21-16 MLPPP Link Properties***

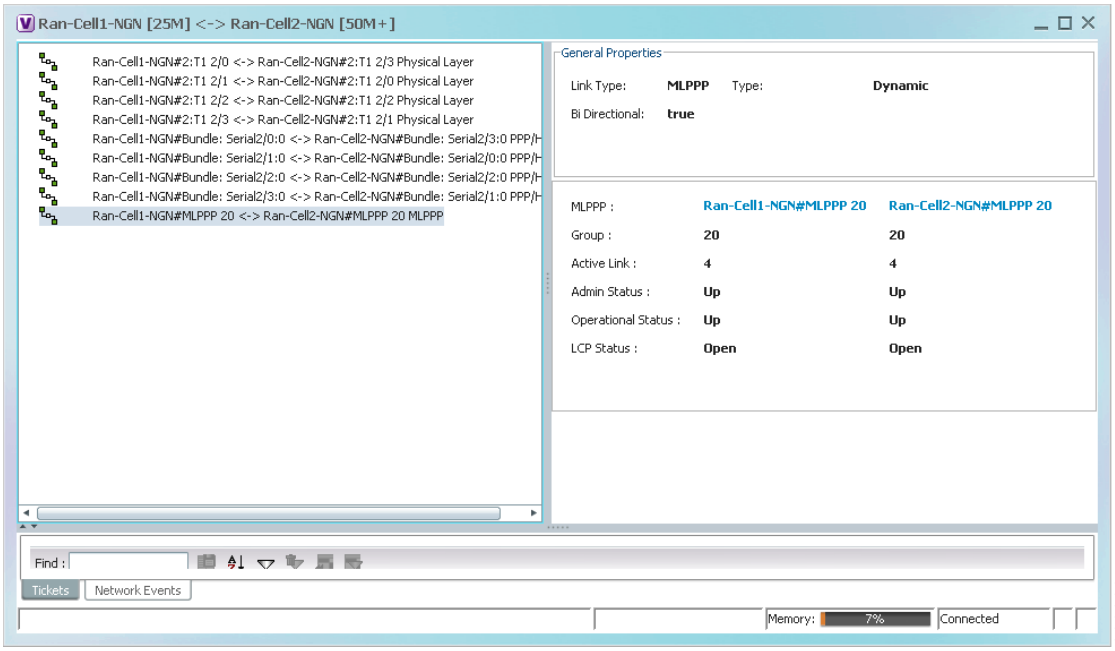



Table 21-17 describes the information that is displayed for the MLPPP link.

***Table 21-17 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 21-17.

**Step 3** Select the required entry and scroll horizontally until you see the required information.

***Figure 21-17 MPLS Pseudowire Tunnels over GRE Properties***

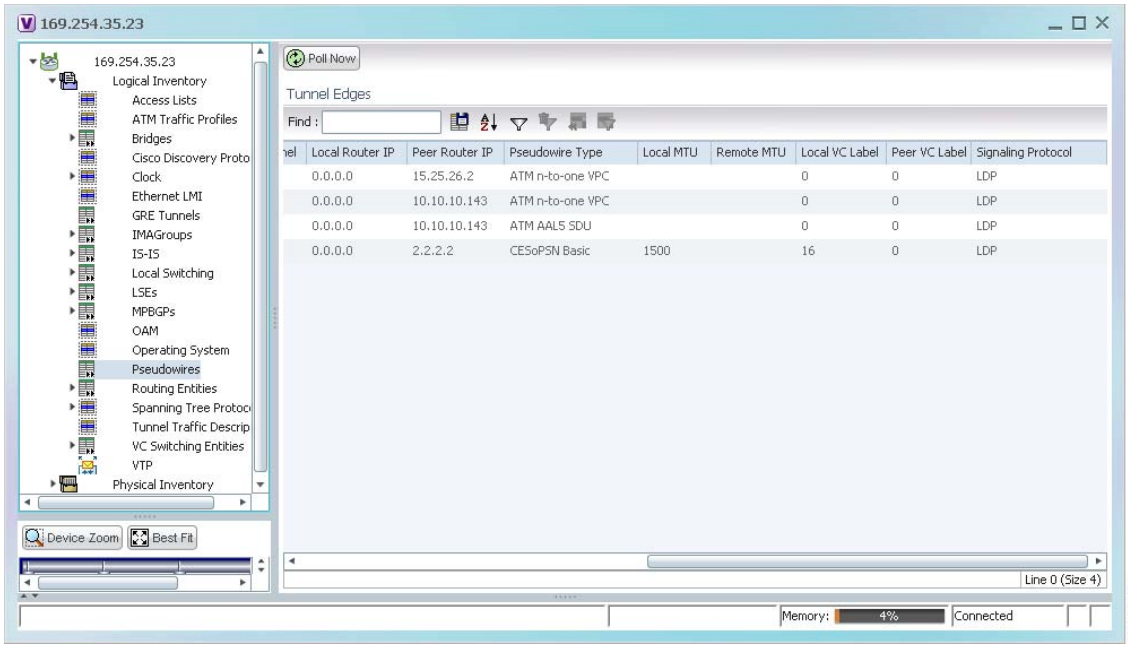


Table 21-18 describes the information included in the Tunnel Edges table specifically for MPLS pseudowire tunnels over GRE.

*Table 21-18 MPLS Pseudowire over GRE Properties*

| Field | Description |
|---|---|
| Pseudowire Type | Type of pseudowire relevant to MToP:<br>• ATM AAL5 SDU—ATM with ATM Adaptation Layer 5 (AAL5) service data units.<br>• ATM n-to-one VCC—ATM with n-to-one virtual channel connection (VCC).<br>• ATM n-to-one VPC—ATM with n-to-one virtual path connection (VPC).<br>• CESoPSN Basic—CESoPSN basic services with CAS.<br>• 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.<br>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 21-18 shows the Tunnel Edges table that is displayed for GRE tunnels.

*Figure 21-18 GRE Tunnel Properties in Logical Inventory*

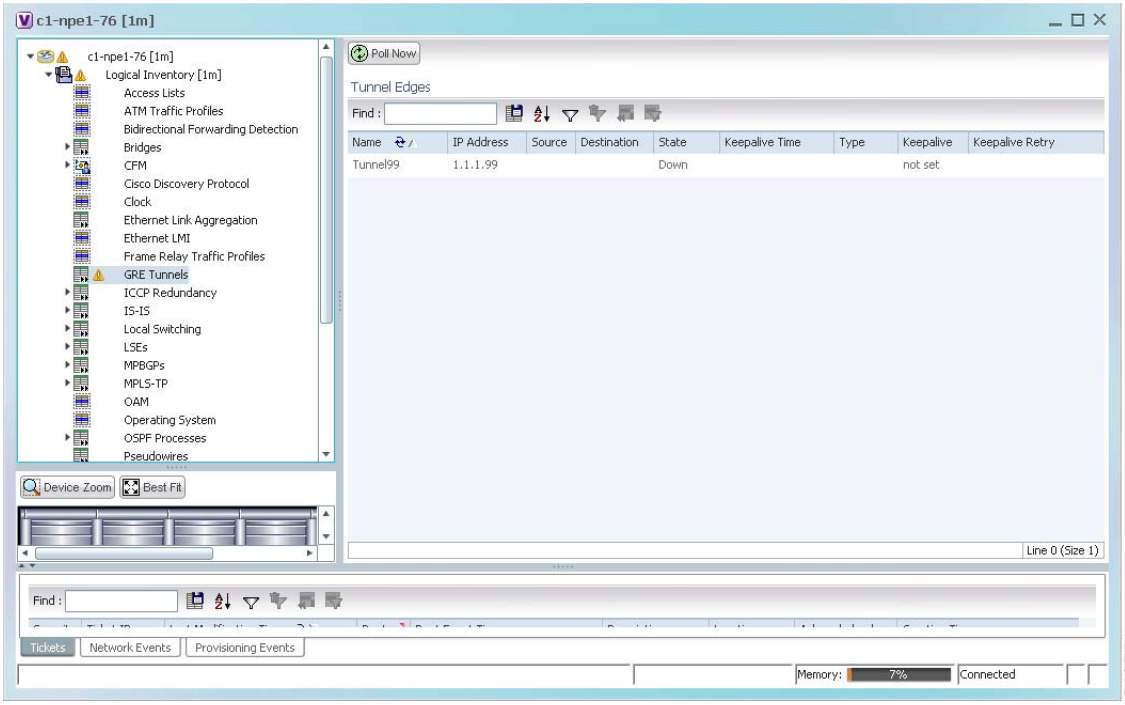



Table 21-19 describes the information that is displayed for GRE tunnels in logical inventory.

*Table 21-19 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 21-34
- Monitoring PTP Service, page 21-37
- Viewing Pseudowire Clock Recovery Properties, page 21-42
- Viewing SyncE Properties, page 21-46
- Applying a Network Clock Service Overlay, page 21-49
- Viewing CEM and Virtual CEM Properties, page 21-50

## 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 21-19.

*Figure 21-19 Clock Service Properties*

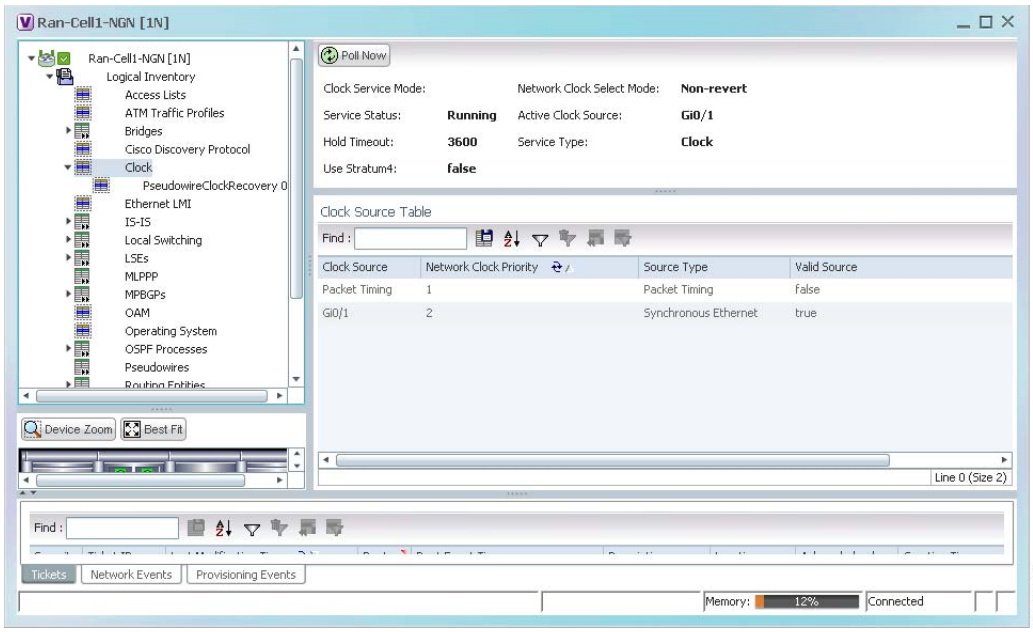



Table 21-20 describes the information displayed for clocking service.

*Table 21-20 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:<br>• Non-revert—Do not use the master device again after it recovers from the failure.<br>• Revert—Use the master device again after it recovers and functions correctly for a specified amount of time.<br>• Unknown—The network clock selection mode is unknown. |
| Service Status | Status of the system service:<br>• Initializing—The service is starting up.<br>• Down—The service is down.<br>• Reset—The service has been reset.<br>• Running—The service is running.<br>• 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. |

*Table 21-20 Clock Service Properties (continued)*

| Field | Description |
|---|---|
| Use Stratum4 | Quality of the clock source:<br>• True—Use Stratum 4, the lowest level of clocking quality.<br>• False—(Default) Use Stratum 3, a higher level of clocking quality than Stratum 4. |

*Table 21-20 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:<br>• BITS—Timing is supplied by a Building Integrated Timing Supply (BITS) port clock.<br>• E1/T1—Clocking is provided via an E1 or T1 interface.<br>• Packet-Timing—Clocking is provided over a packet-based network.<br>• Synchronous Ethernet—Clocking is provided by Synchronous Ethernet.<br>• Others—Clocking is provided by a source other than the above. |
| Valid Source | Validity of the clock source:<br>• True—The clock source is valid and operational.<br>• 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. For configuring PTP, see Configuring SONET, page 21-54.

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 21-20.

***Figure 21-20 PTP Service Properties***

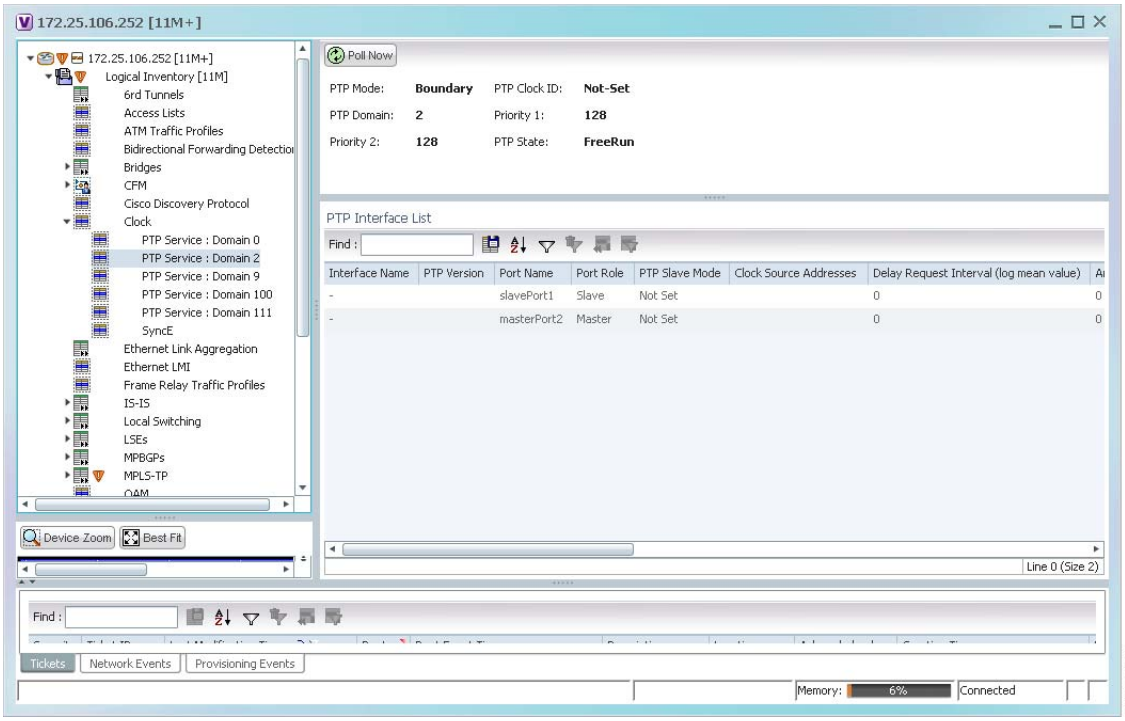



Table 21-21 describes the properties that are displayed for PTP service.

*Table 21-21 PTP Service Properties*

| Field | Description |
|---|---|
| PTP Mode | Mode of PTP operation:<br>• Boundary—Boundary clock mode.<br>• E2E Transparent—End-to-end transparent clock mode.<br>• Ordinary—Ordinary clock mode.<br>• P2P Transparent—Peer-to-peer transparent clock mode.<br>• Unknown—The clock mode is unknown.<br>**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:<br>• Freerun—The slave clock is not locked to a master clock.<br>• 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.<br>• Acquiring—The slave device is receiving packets from a master and is trying to acquire a clock.<br>• Freq locked—The slave device is locked to the master device with respect to frequency, but is not aligned with respect to phase.<br>• 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 21-21 PTP Service Properties (continued)*

| Field | Description |
|---|---|
| PTP Slave Mode | For an interface defined as a slave device, the mode used for PTP clocking:<br>• Not Set—The slave mode is not used.<br>• Multicast—The interface uses multicast mode for PTP clocking.<br>• Unicast—The interface uses unicast mode for PTP clocking.<br>• 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:<br>• 4—1 packet every 16 seconds.<br>• 3—1 packet every 8 seconds.<br>• 2—1 packet every 4 seconds.<br>• 1—1 packet every 2 seconds.<br>• 0—1 packet every second.<br>• -1—1 packet every 1/2 second, or 2 packets per second.<br>• -2—1 packet every 1/4 second, or 4 packets per second.<br>• -3—1 packet every 1/8 second, or 8 packets per second.<br>• -4—1 packet every 1/16 seconds, or 16 packets per second.<br>• -5—1 packet every 1/32 seconds, or 32 packets per second.<br>• -6—1 packet every 1/64 seconds, or 64 packets per second. |
| Announce Interval (log mean value) | Interval value for PTP announcement packets:<br>• 4—1 packet every 16 seconds.<br>• 3—1 packet every 8 seconds.<br>• 2—1 packet every 4 seconds.<br>• 1—1 packet every 2 seconds.<br>• 0—1 packet every second.<br>• -1—1 packet every 1/2 second, or 2 packets per second.<br>• -2—1 packet every 1/4 second, or 4 packets per second.<br>• -3—1 packet every 1/8 second, or 8 packets per second.<br>• -4—1 packet every 1/16 seconds, or 16 packets per second.<br>• -5—1 packet every 1/32 seconds, or 32 packets per second.<br>• -6—1 packet every 1/64 seconds, or 64 packets per second. |

*Table 21-21 PTP Service Properties (continued)*

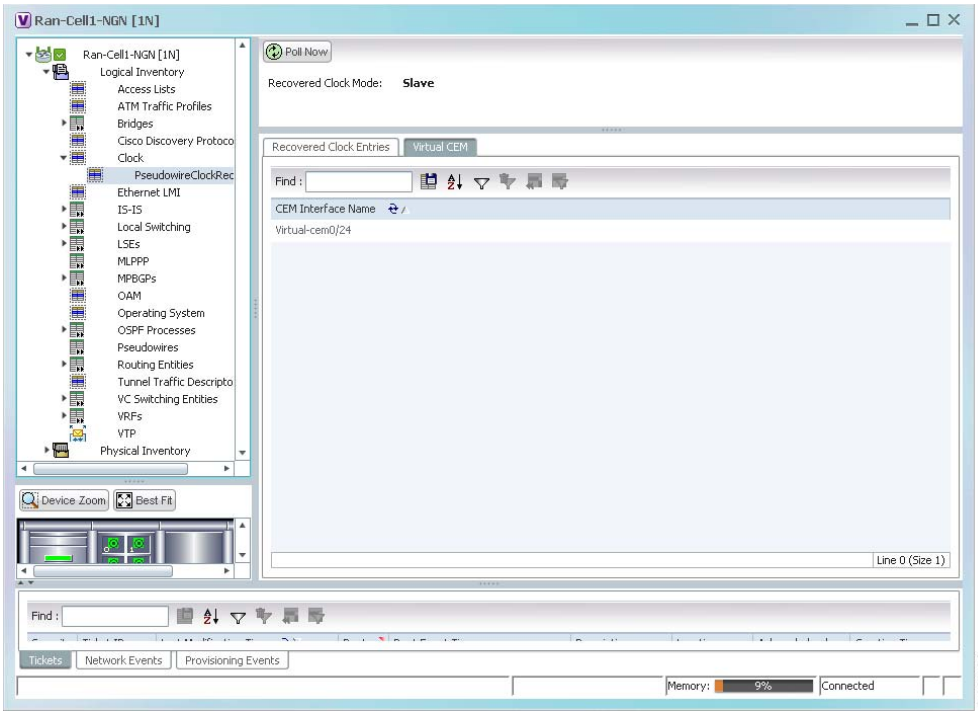
| Field | Description |
|---|---|
| Announce Timeout | Number of PTP announcement intervals before the session times out. Values are 2-10. |
| Sync Interval (log mean value) | Interval for sending PTP synchronization messages:<br>• 4—1 packet every 16 seconds.<br>• 3—1 packet every 8 seconds.<br>• 2—1 packet every 4 seconds.<br>• 1—1 packet every 2 seconds.<br>• 0—1 packet every second.<br>• -1—1 packet every 1/2 second, or 2 packets per second.<br>• -2—1 packet every 1/4 second, or 4 packets per second.<br>• -3—1 packet every 1/8 second, or 8 packets per second.<br>• -4—1 packet every 1/16 seconds, or 16 packets per second.<br>• -5—1 packet every 1/32 seconds, or 32 packets per second.<br>• -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:<br>• Not Set—The master mode is not used.<br>• Multicast—The interface uses multicast mode for PTP clocking.<br>• Unicast—The interface uses unicast mode for PTP clocking. This mode allows a single destination.<br>• 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 21-21.

***Figure 21-21 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 21-22.

*Table 21-22 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:<br>• 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.<br>• 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:<br>• Dormant—The interface is dormant.<br>• Down—The interface is down.<br>• Not Present—An interface component is missing.<br>• Testing—The interface is in test mode.<br>• Unknown—The interface has an unknown operational status.<br>• Up—The interface is up. |
| Admin Status | Administrative status of the CEM interface:<br>• Down—The CEM interface is administratively down.<br>• Testing—The administrator is testing the CEM interface.<br>• Unknown—The administrative status is unknown.<br>• Up—The CEM interface is administratively up. |

**Step 3** To view additional CEM group properties, double-click the required CEM group.

Table 21-23 describes the information displayed in the CEM Group Properties window.

*Table 21-23 CEM Group Properties*

| Field | Description |
|---|---|
| Oper Status | Operational status of the CEM interface:<br>• Dormant—The interface is dormant.<br>• Down—The interface is down.<br>• Not Present—An interface component is missing.<br>• Testing—The interface is in test mode.<br>• Unknown—The interface has an unknown operational status.<br>• 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:<br>• Down—The CEM interface is administratively down.<br>• Testing—The administrator is testing the CEM interface.<br>• Unknown—The administrative status is unknown.<br>• 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 21-22.

If no recovered clock entries exist, this tab is not displayed.

*Figure 21-22 Pseudowire Clock Recovery - Recovered Clock Entries Tab*

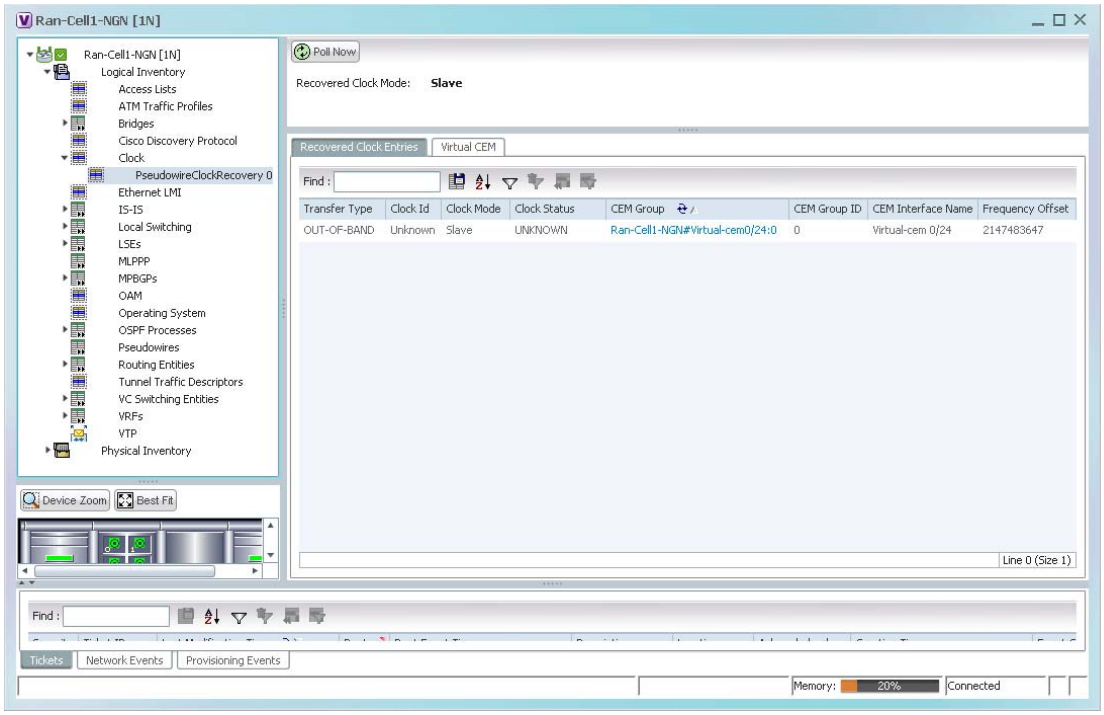



Table 21-24 describes the information displayed for pseudowire clock recovery.

*Table 21-24 Pseudowire Clock Recovery Properties*

| Field | Description |
|---|---|
| Recovered Clock Source | Interface (slot/subslot) in which clock recovery occurred.<br>Click the hyperlinked entry to view its properties in physical inventory. |
| Recovered Clock Mode | Recovered clock mode:<br>• Adaptive—The devices do not have a common clock source. The recovered clock is derived from packet arrival.<br>• 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.<br>• 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 21-24 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.<br>• 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:<br>• Adaptive—The recovered clock was obtained using ACR.<br>• Primary—The recovered clock was obtained from a clock with the highest priority.<br>• Secondary—The recovered clock was obtained from a clock with a lower priority than the primary clock. |
| Clock Status | Status of the clock:<br>• Acquiring—The clock is obtaining clocking information.<br>• Acquired—The clock has obtained the required clocking information.<br>• 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.

For configuring SyncE, see Configuring SONET, page 21-54.

To view SyncE properties, choose **Logical Inventory > Clock > SyncE**. (See Figure 21-23.)

*Figure 21-23 SyncE Properties in Logical Inventory*

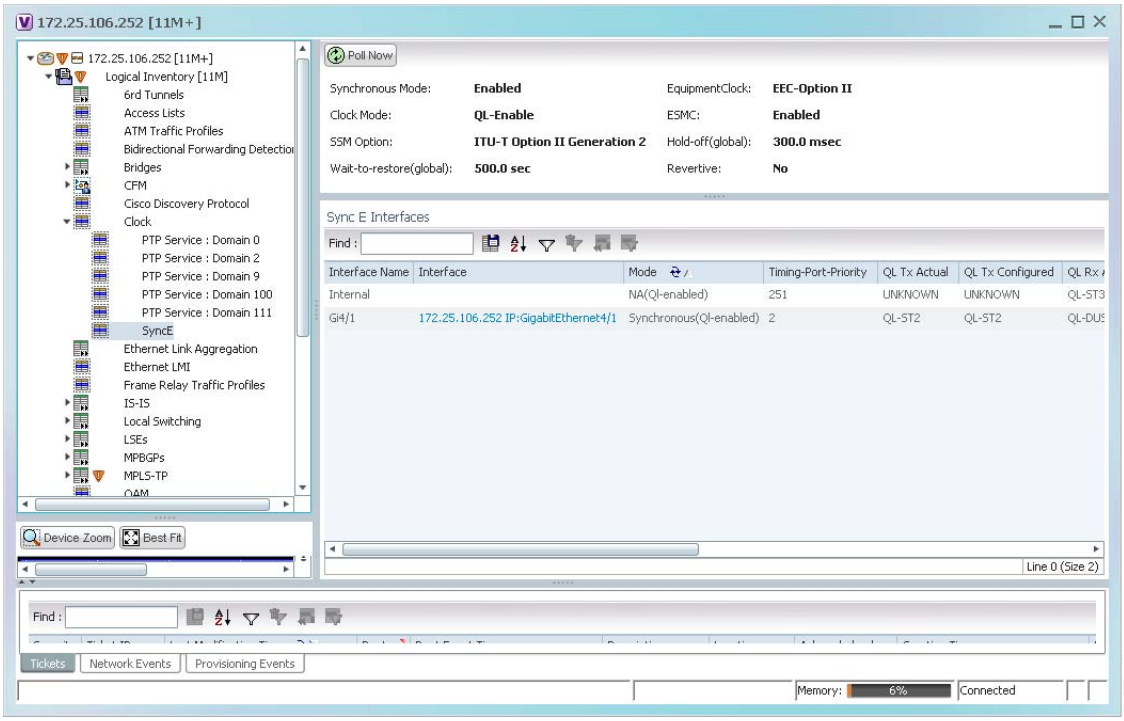



Table 21-25 describes the information that is displayed for SyncE.

*Table 21-25 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:<br>• ITU-T Option I<br>• ITU-T Option II Generation 1<br>• 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 21-25 SyncE Properties (continued)*

| Field | Description |
|---|---|
| **SyncE Interfaces Table** | |
| Interface Name | Name of the Gigabit or 10 Gigabit interface associated with SyncE.<br>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 19-31.<br>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:<br>• ITU-T Option I—Available values are QL-PRC, QL-SSU-A, QL-SSU-B, QL-SEC, and QL-DNU.<br>• ITU-T Option II Generation 1—Available values are QL-PRS, QL-STU, QL-ST2, QL-SMC, QL-ST4, and QL-DUS.<br>• 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.<br>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.<br>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.<br>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 21-25 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:

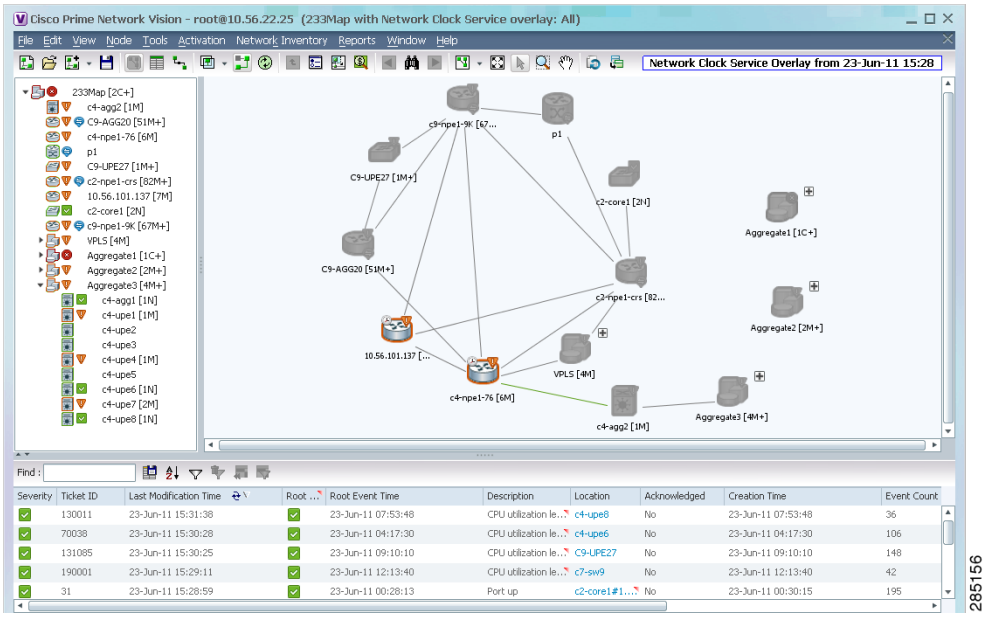
- Choose a search category, enter a search string, then click **Go** to narrow the search results to a range of network clock services or a specific network clock service. Search categories include:
  - Description
  - Name

  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.

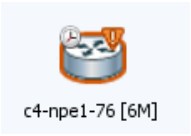
**Step 4** Select the network clock service overlay that you want to apply to the map.

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 21-24.)

*Figure 21-24 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 21-51
- Viewing Virtual CEMs, page 21-51
- Viewing CEM Groups, page 21-51

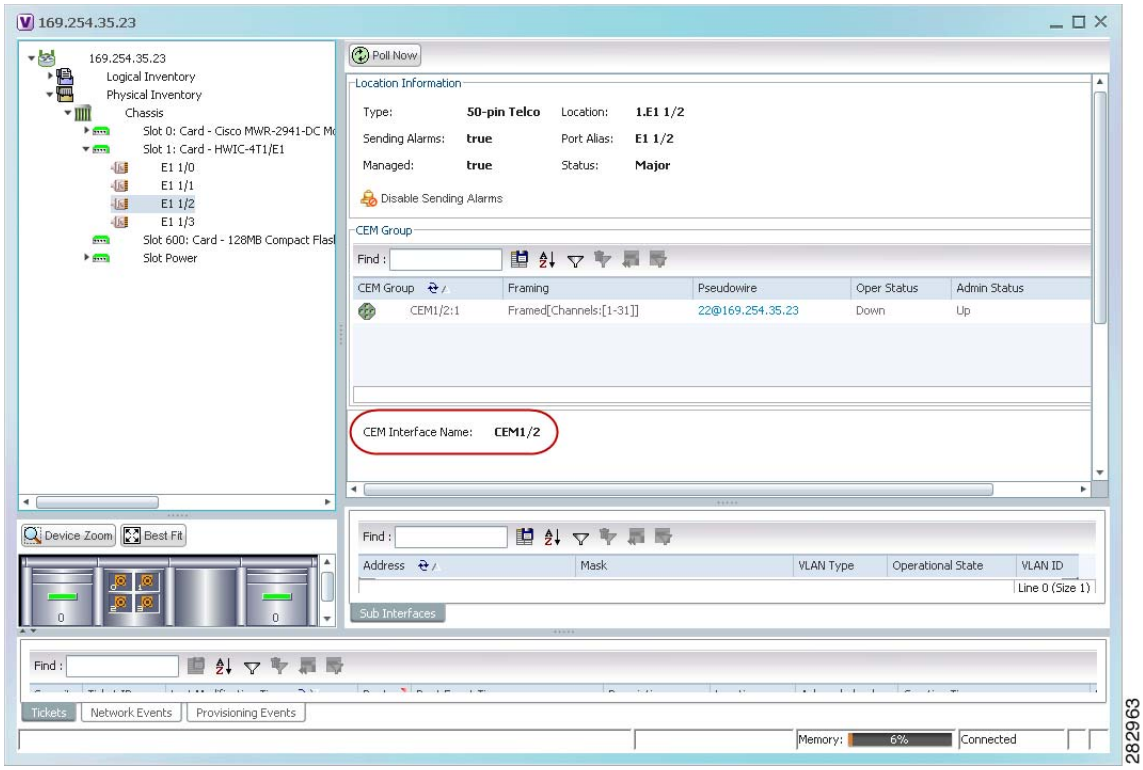
# Viewing CEM Interfaces

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 21-25.

***Figure 21-25 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 21-52
- Viewing CEM Groups on Virtual CEM Interfaces, page 21-53

## 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.

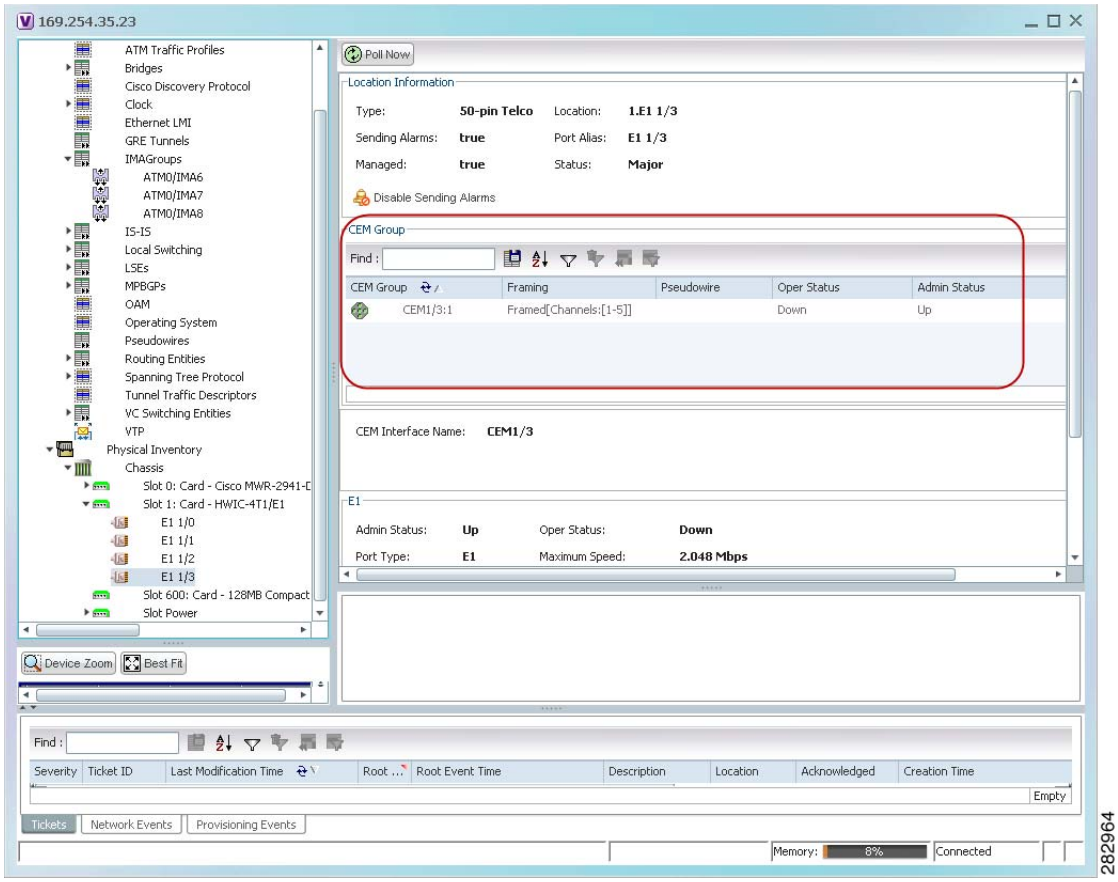
To view CEM groups configured on physical interfaces:

**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 21-26).

***Figure 21-26 CEM Group Information***

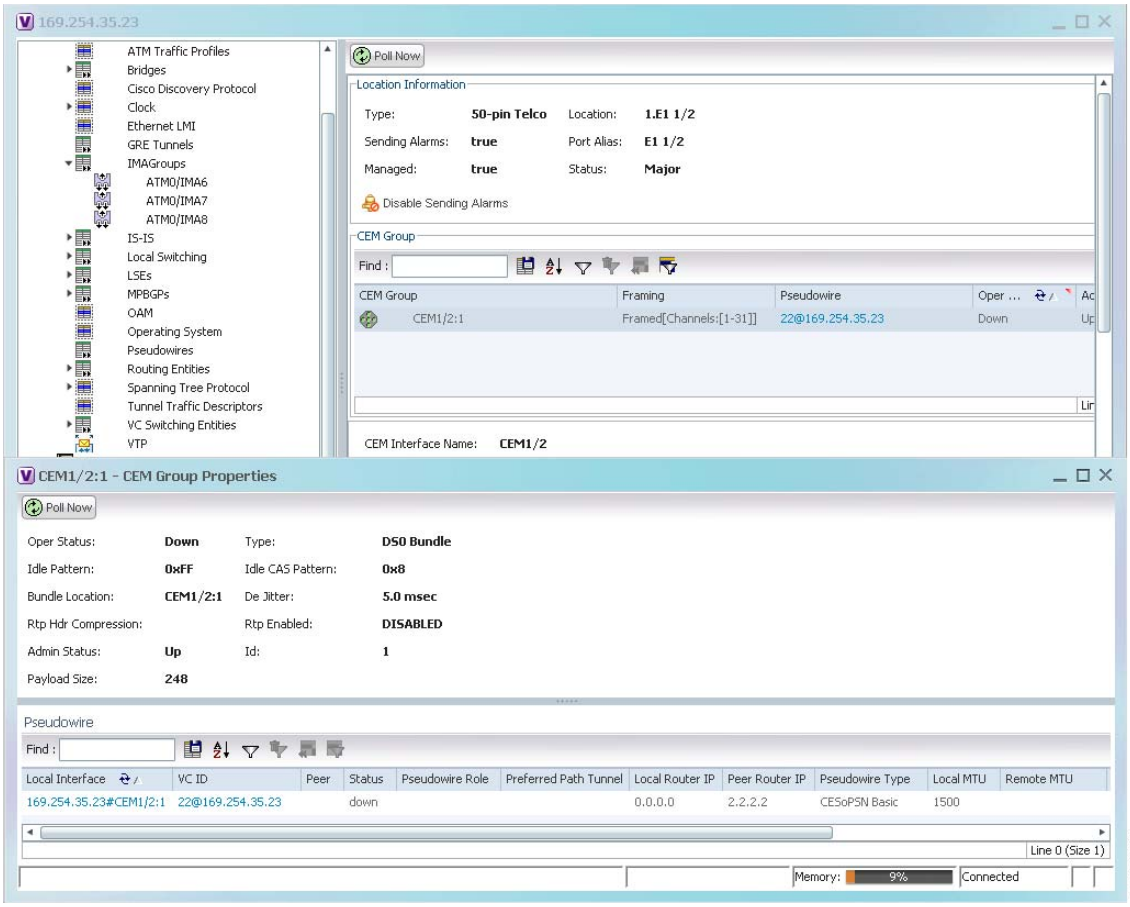



See Table 21-22 for a description of the properties displayed for CEM groups in the content pane.

**Step 3** To view additional information, double-click the required group.

The CEM Group Properties window is displayed as shown in Figure 21-27.

*Figure 21-27 CEM Group Properties Window*




See Table 19-27 on page 19-51 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.

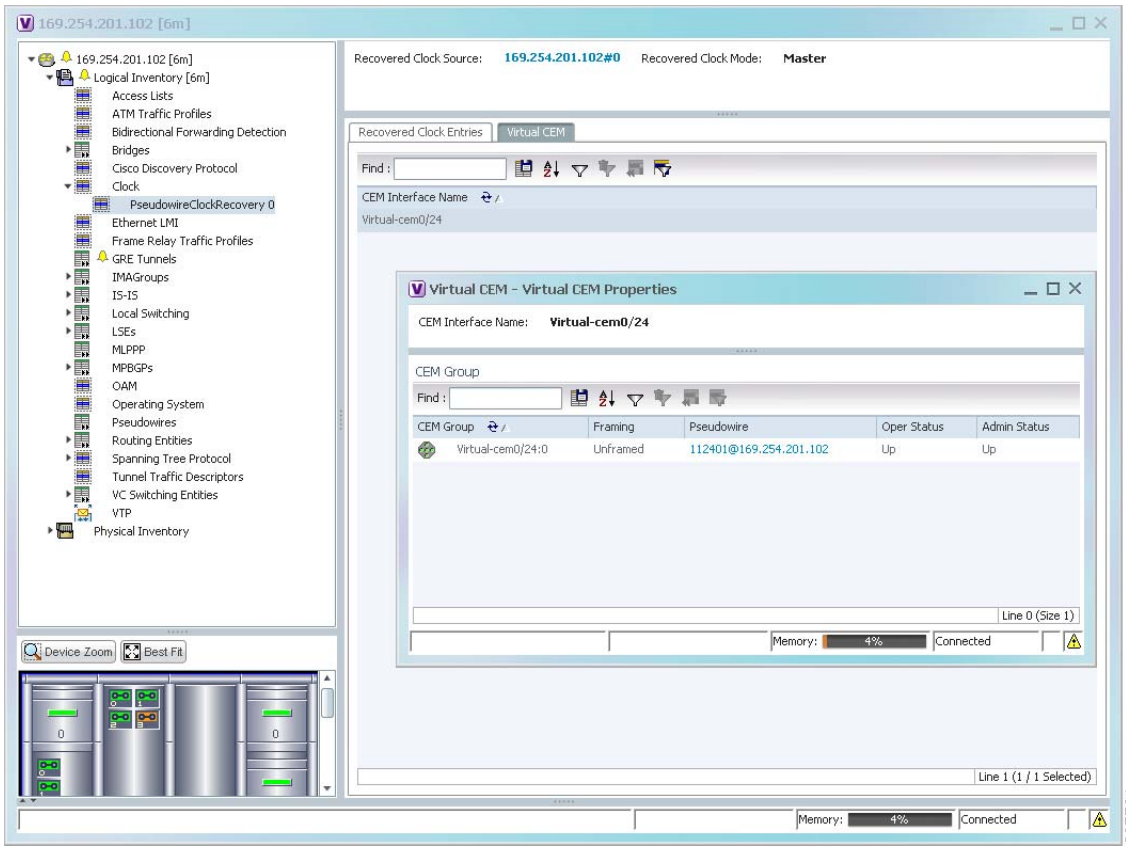
To view CEM groups on virtual CEM interfaces:

**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 21-28). If a pseudowire is configured on the CEM group for out-of-band clocking, the pseudowire VCID is also shown.

*Figure 21-28 CEM Group Properties*




**Step 4** To view additional CEM group properties, double-click the required CEM group.

Table 21-23 describes the information displayed in the CEM Group Properties window.

# Configuring SONET

These commands help in configuring the SONET device and in viewing device details.

The table below lists the SONET commands can be launched from the inventory by right-clicking a SONET port and selecting **Commands > SONET**.

To run the these commands, the software on the network element must support the technology. Before executing any commands, you can preview them and view the results. For details on the software versions Prime Network supports for the listed supported network elements, see *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

| Command | Navigation | Description | Supported on: |
|---|---|---|---|
| **BER Threshold** | *Right-click on SONET port and select* **Commands > SONET > Show >** | Performed from command launch point | • Cisco 7600 Series Routers<br>• Cisco CRS Carrier Routing System<br>• Cisco CRS series includes Cisco CRS-1 and Cisco CRS-3 Carrier Routing Systems.<br>• Cisco IOS 12000 Series GSR |
| **Controller Data** | | | |
| **TCA Threshold** | | | |
| **SDH Counters** | **Clear > SONET >** | N/A; performed from command launch point | |
| **BER Threshold** | *Right-click on SONET port and select* **Commands > SONET > Configure >** | BER threshold:<br>• sf-ber—Sets the signal failure BER threshold. Value in the range from 3 to 9. The default value is 6<br>• sd-ber—Sets the signal degrade BER threshold. Value in the range from 3 through 9. The default value is 3<br>Bit error rate: 3-9, or default. The default for sf-ber is 3, and the default for sd-ber is 9. | |
| **Line Counters** | *Right-click on SONET port and select* **Commands > SONET > Show > PM** | Line type: farendline, farendline-history, line, or line-history<br>History interval: 1-96; to view all, enter 0 | |
| **Medium Counters** | | N/A; performed from command launch point<br>Path type: farendpath, farendpath-history, path, path-history | |
| **Path Counters** | | Channelized path index: 1-48 (for a particular channel) or 0 (for all channels)<br>History interval: 1-96; to view all, enter 0 | |

| Command | Navigation | Description | Supported on: |
|---|---|---|---|
| **Section Counters** | *Right-click on SONET port and select* **Commands > SONET > Show > PM** | Section type: section or section-history<br>History interval: 1-96; to view all, enter 0 | • Cisco 7600 Series Routers<br>• Cisco CRS Carrier Routing System<br>• Cisco CRS series includes Cisco CRS-1 and Cisco CRS-3 Carrier Routing Systems.<br>• Cisco IOS 12000 Series GSR |
| **Trace Details** | | Card location (for example, 0/5/CPU0)<br>**Note** The device must be managed by Prime Network with device admin privileges. | |
| **Clock Source** | *Right-click on SONET port and select* **Commands > SONET > Configure >** | Clock source of sent signal on SONET ports:<br>• internal—Controller will clock its sent data using internal clock.<br>• line—Controller will clock its sent data using the clock recovered from the line's receive data stream.<br>• default—Cancels any clock source setting. | |
| **TCA Threshold** | | TCA threshold:<br>• b1-tca—Threshold for B1 BER TCA, between 3-9 (default is 6).<br>• b2-tca—Threshold for B2 BER TCA, between 3-9 (default is 6).<br>Bit error rate: Value from 3-9 (10 to the negative x), or default. | |

# Configuring Clock

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. SyncE and PTP are two widely used clock synchronization protocol used in ethernet based networks.

Clocking configuration commands allows you to configure SyncE and PTP clock configuration on Cisco router. SyncE and PTP clocking configuration is predominantly used in RAN Backhaul (or MToP) network where TDM traffic carried from cell site router to central office via packet switched network.

These commands can be launched from the logical inventory by right-clicking on **Clock** node. Before executing any commands, you can preview them and view the results.

To run the these commands, the software on the network element must support the technology. Before executing any commands, you can preview them and view the results. For details on the software versions Prime Network supports for the listed supported network elements, see *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

The table below lists the PTP and SyncE configuration commands and its supported network elements.

| Command | Navigation | Description | Supported on: |
|---|---|---|---|
| **Create PTP Clock Global** | (For ASR 901/903)<br>*Right-click* **Clock** *node* **> Commands > Configuration >**<br>(For ASR 9000)<br>*Right-click* **Clock** *node* **> Commands > Configuration > PTP >** | Identify the clock in the network with the highest priority. The clock with the highest priority is referred to as the master clock. All the other devices on the network synchronize their clocks with the master and are referred to as members. Constantly exchanged timing messages between master and members ensure continued synchronization.<br>The PTP clock port commands are used to modify PTP on individual interfaces. | • Cisco ASR 9000 Series Routers<br>• Cisco ASR 901 Series Routers<br>• Cisco ASR903 Series Routers |
| **Modify PTP Clock Global** | (For ASR 901/903)<br>*Expand* **Clock** *node* **>** *right-click PTP Service>* **Commands > Configuration >**<br>(For ASR 9000)<br>*Right-click* **Clock** *node* **> Commands > Configuration > PTP >** | | |
| **Delete PTP Clock Global** | *Expand* **Clock** *node* **>** *right-click PTP Service>* **Commands > Configuration >** | | • Cisco ASR 901 Series Routers<br>• Cisco ASR903 Series Routers |
| **Create PTP Clock Port** | *Expand* **Clock** *node* **>** *right-click PTP Service>* **Commands > Configuration >** | | |
| **Show PTP Clock Global** | *Expand* **Clock** *node* **>** *right-click PTP Service>* **Commands > Show >** | | |
| **Modify PTP Clock Port**<br>**Delete PTP Clock Port** | *Expand* **Clock** *node* **>** *select* **PTP** *node* **>** *right-click on the selected PTP interface* **> Commands > Configuration >** | | |

| Command | Navigation | Description | Supported on: |
|---|---|---|---|
| **Create PTP Interface**<br>**Modify PTP Interface** | **Physical inventory > Chassis > Slot > *Select an interface* > Commands > Configuration > PTP** | | • Cisco ASR 9000 Series Routers |
| **Create SyncE Global** | *Right-click* **Clock** *node* **> Commands > Configuration >** | Configure clock properties at the global level such as hold-off time, wait to restore, force switch, and so on, that helps routers to synchronize to the best available clock source.<br>Configure SyncE at the interface level using the SyncE interface commands. | • Cisco ASR 9000 Series Routers<br>• Cisco ASR 901 Series Routers<br>• Cisco ASR903 Series Routers |
| **Modify SyncE Global** | (For ASR901, ASR903):<br>*Expand* **Clock** *node* **>** *right-click* **SyncE> Commands > Configuration >**<br>(For ASR9000):<br>*Right-click* **Clock** *node* **> Commands > Configuration >** | | |
| **Create SyncE Interface**<br>**Modify SyncE Interface** | (For ASR901, ASR903):<br>*Expand* **Clock** *node* **>** *right-click* **SyncE> Commands > Configuration >**<br>(For ASR9000):<br>**Physical inventory > Chassis > Slot > *Select an interface* > Commands > Configuration > SyncE** | | |

| Command | Navigation | Description | Supported on: |
|---|---|---|---|
| **Create ESMC Global**<br>**Modify ESMC Global** | *Expand* **Clock** *node* **>** *right-click* **SyncE> Commands > Configuration >** | Configure ESMC for synchronous Ethernet (SyncE) clock synchronization.<br>Only ASR 9003 series router supports the Synchronization Status Message (SSM) and the Ethernet Synchronization Message Channel (ESMC) for synchronous Ethernet (SyncE) clock synchronization.<br>Configure ESMC for synchronous Ethernet (SyncE) clock synchronization on an interface using the ESMC interface commands. | • Cisco ASR903 Series Routers<br>• Cisco ASR 901 Series Routers<br>• Cisco ASR903 Series Routers |
| **Create ESMC Interface**<br>**Disable ESMC Interface** | *Expand* **Clock** *node* **>** *select* **SyncE >** *right-click on a SyncE Interface from the content pane* **> Commands > Configuration >** | | • Cisco ASR 901 Series Routers |
| **Modify ESMC Interface** | | | |

# Configuring TDM and Channelization

The table below lists the TDM and SONET/SDH channelization configuration commands , supported network elements, and navigation for the commands. These commands can be launched from the physical inventory.

To run the these commands, the software on the network element must support the technology. Before executing any commands, you can preview them and view the results. For details on the software versions Prime Network supports for the listed supported network elements, see *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

| Command | Navigation | Description | Supported on: |
|---|---|---|---|
| **TDM Commands** | | | |
| **Configure Card Type** | *Right-click the device* > **Commands > Configuration >** | • For ASR9000, configure the card type as SONET/SDH an specify the chassis, slot or the subslot number.<br>• For ASR 903 and 901, configure the card type as E1, T1, and specify the location using slot and bay number. | • Cisco ASR 9000 Series Routers<br>• Cisco ASR 901 Series Routers<br>• Cisco ASR903 Series Routers |
| **Modify E1 Controller**<br>**Modify T1 Controller** | (For ASR901, ASR903):<br>**Physical Inventory > Chassis > Slot >** *right-click on* **E1 or T1 > Commands > Configuration > E1T1 >**<br>or<br>(For ASR9000, ASR903):<br>**Physical Inventory > Chassis > Slot >** click on **SONET >** *double-click on a* **SONET/SDH High Order Path (HOP) >** *right-click* **LOP > Commands > Configuration > E1T1 >** | • In ASR 9000, E1 and T1 controller is configured as part of the channelization, when configuring the low order path (LOP) for the SONET controller.<br>• For ASR 903, you can configure E1 or T1 controller in either of the following ways:<br>– While configuring the card type<br>or<br>– During the channelization when configuring the low order path (LOP) for the SONET.<br>• For ASR 901, configure the card type to configure E1 or T1 controller. | |
| **Channelization Commands for SONET/SDH**<br>**Note** Channelization commands also include the TDM commands discussed above. Read the description to understand the scenario applicable to your device. | | | |
| **Configure Framing**<br>**Configure AUG Mapping** | **Physical Inventory > Chassis > Slot > Subslot >** *right-click on SONET/SDH-interface* **> Commands > Configuration > SONET >** | Configure SDH/SONET framing type using this command.<br>Configuring framing as SDH, configures AU4 by default, but if you want to change the mode of operation as AU3, use the **AUG Mapping** command. | Cisco ASR903 Series Routers |

| Command | Navigation | Description | Supported on: |
|---|---|---|---|
| **Configure Controller** | **Physical Inventory > Chassis > Slot > Subslot >** *right-click on SONET interface* **> Commands > Configuration > SONET >** | After configuring SONET/SDH type, configure the controller using additional parameters, like specifying the clock source. | • Cisco ASR 9000 Series Routers<br>• Cisco ASR903 Series Routers |
| **Configure AU3** | **Physical Inventory > Chassis > Slot > Subslot >** *click on SONET- interface* **>** *right-click on a SONET/SDH HOP* **> Commands > Configuration >** | Using these commands, you can configure the parameters for the SDH channelization.<br>When you are configuring the channelized E1/T1 line card for SDH framing, configure AU-3 or AU-4 as the mode of operation.<br>For SDH, both AU-3 and AU-4 AUG mappings are supported. | • Cisco ASR 9000 Series Routers<br>• Cisco ASR903 Series Routers |
| **Delete AU3** | | | • Cisco ASR 9000 Series Routers |
| **Configure AU4** | | | • Cisco ASR 9000 Series Routers<br>• Cisco ASR903 Series Routers |
| **Delete AU4** | | If the AUG mapping is configured to be AU-4, then the following mapping will be used:<br>TUG-3 <--> AU-4 <--> AUG<br>If the mapping is configured to be AU-3, then the following mapping will be used:<br>AU-3 <--> AUG | • Cisco ASR 9000 Series Routers |
| **Configure TUG3**<br>**Delete TUG3** | **Physical Inventory > Chassis > Slot > Subslot >** click on *SONET- interface* **>** *double-click on a* **SONET/SDH High Order Path (HOP) >** *right-click* **LOP > Commands > Configuration >** | | |
| **Delete STS**<br>**Configure STS** | **Physical Inventory > Chassis > Slot > Subslot >** *click on SONET- interface* **>** *right-click on a SONET/SDH HOP* **> Commands > Configuration >** | Using these commands, you can configure the STS path attributes for the SONET channelization mode. | |

# Configuring Automatic Protection Switching (APS )

APS refers to the mechanism of using a protect interface in the SONET network as the backup for working interface. When the working interface fails, the protect interface quickly assumes its traffic load. The working interfaces and their protect interfaces make up an APS group. SONET APS offers recovery from fiber (external) or equipment (interface and internal) failures at the SONET line layer.

The table below lists the APS configuration commands , supported network elements, and navigation for the commands.

To run the these commands, the software on the network element must support the technology. Before executing any commands, you can preview them and view the results. For details on the software versions Prime Network supports for the listed supported network elements, see *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

| Command | Navigation | Description | Supported on: |
|---|---|---|---|
| **Create APS**<br>**Modify APS** | **Physical Inventory > Chassis >** *slot* **>** *subslot* **>** *SONET interface* **> Commands > Configuration > APS >** | Adds an APS group with a specified number and assign a channel for the APS group. 0 designates a protect channel, and 1 designates a working channel. | • Cisco ASR 9000 Series Routers<br>• Cisco ASR903 Series Routers |

CHAPTER 22

# Viewing and Managing SBCs

This chapter identifies and describes the properties for Session Border Controllers (SBCs) that appear in Cisco Prime Network Vision (Prime Network Vision) logical inventory. It also describes commands you can run to manage SBCs.

Session Border Controllers (SBCs) control and manage real-time multimedia traffic flows between IP network borders, handling signaling, and media. SBCs perform native IP interconnection functions required for real-time communications such as admission control, firewall traversal, accounting, signaling interworking, and quality-of-service (QoS) management. This includes:

- 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

The Cisco Prime Network platform provides fault management, configuration, and performance monitoring for SBC services. Prime Network SBC commands allow you to configure SBC components.

An SBC consists of combined DBE and SBE functionality:

- Data Border Element (DBE)—Responsible for media-related functions.
- Signaling Border Element (SBE)—Responsible for call signaling-related functions.

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.

**Note** The existing Cisco SBC platforms support only DBE.

The following topics describe the SBC properties that are displayed in Prime Network Vision logical inventory:


- User Roles Required to View SBC Properties, page 22-2
- Viewing SBC Properties in Logical Inventory, page 22-3
- Viewing SBC DBE Properties, page 22-4
- Viewing SBC SBE Properties, page 22-5

- Viewing SBC Statistics, page 22-14
- Configuring SBC Components, page 22-14


# 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 3.10 Administrator Guide*.

The following tables identify the tasks that you can perform:

- Table 22-1 identifies the tasks that you can perform if a selected element **is not in** one of your assigned scopes.
- Table 22-2 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 3.10 Administrator Guide*.

***Table 22-1 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 |
| Using SBC Configuration and Monitoring Commands | — | — | — | X | X |
| Using SBC Show Commands | — | — | — | X | X |

***Table 22-2 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 |
| Using SBC Configuration and Monitoring Commands | — | — | — | X | X |
| Using SBC Show Commands | — | — | — | 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 22-1.

***Figure 22-1 SBC Properties in Logical Inventory***

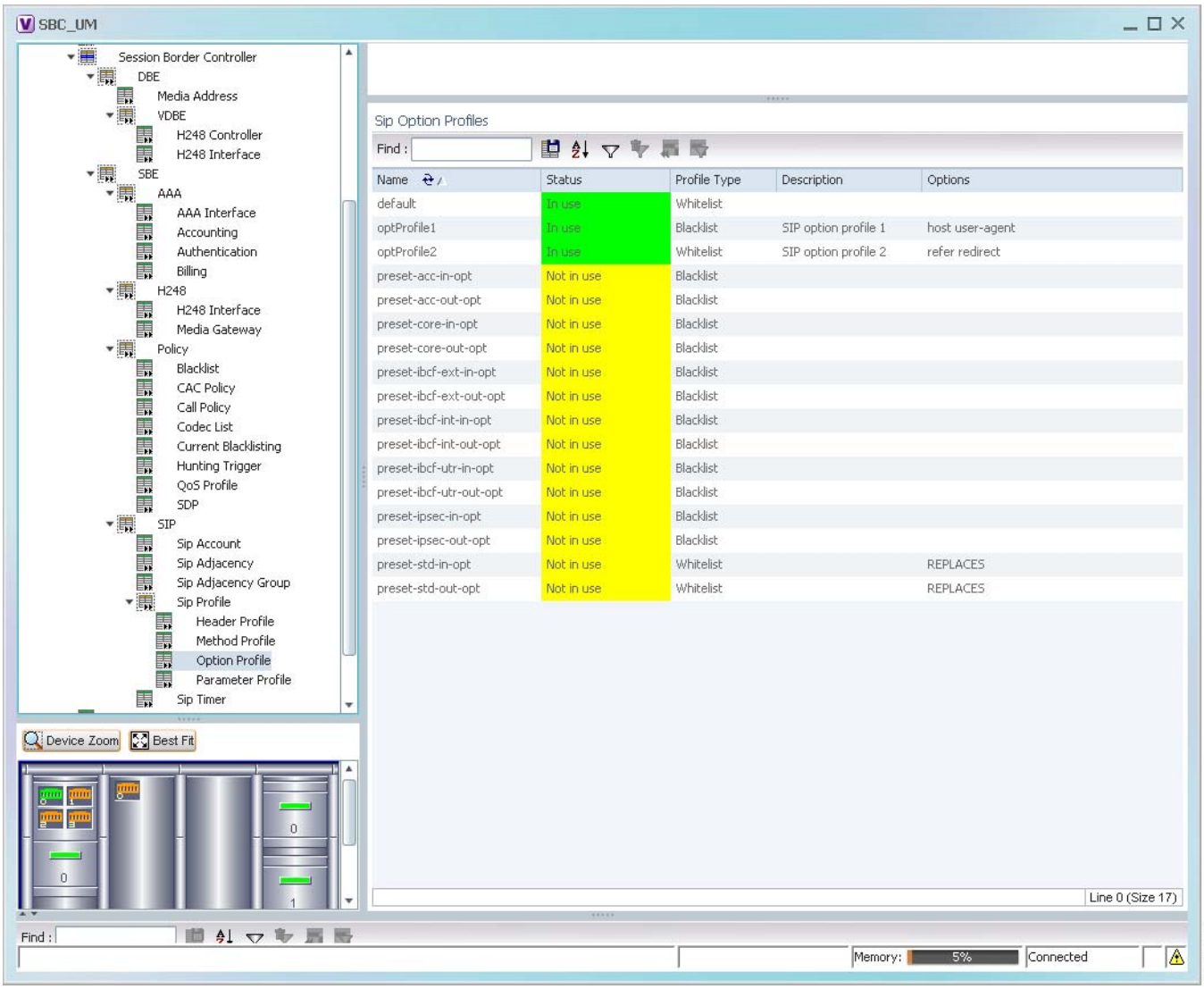



Table 22-3 describes the general SBC properties displayed in logical inventory.

***Table 22-3 SBC Properties***

| Field | Description |
|---|---|
| Process | Process name, such as Session Border Controller. |
| Process Status | Status of the process, such as Running. |

*Table 22-3 SBC Properties (continued)*

| Field | Description |
|---|---|
| Application Version | SBC version number. |
| Mode | Mode in which the SBC is operating:<br>• Unified<br>• 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 22-4 describes the DBE properties that appear in logical inventory.

*Table 22-4 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 22-5 describes the SBC media address properties that are displayed in logical inventory.

*Table 22-5 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 22-6 describes the VDBE H.248 properties that are displayed in logical inventory.

*Table 22-6 VDBE H.248 Properties*

| Branch | Description |
|---|---|
| H248 Controller | H.248 controller used by the DBE.<br>The Media Gateway Configuration (MGC) table displays the following information:<br>• Index—The number of the H.248 controller. The profile is used to interoperate with the SBE.<br>• Remote IP—The remote IP address for the H.248 controller.<br>• Remote Port—The remote port for the H.248 controller.<br>• Transport—The transport for communications with the remote device. |
| H248 Interface | The SBC H248 Control Interface table displays the following information:<br>• IP Address:<br>– In DM mode, the local IP address of the DBE used to connect to the SBE.<br>– In UM mode, the local IP address used to connect to the media gateway.<br>• Port—The port for the H.248 controller interface.<br>• Transport—The transport the H.248 controller interface uses.<br>• 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 22-7 describes the information displayed in logical inventory for an SBE.

*Table 22-7 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. |

*Table 22-7 SBC SBE Properties (continued)*

| Field | Description |
|---|---|
| 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 22-8 describes the AAA properties that appear in logical inventory for the SBC SBE.

*Table 22-8 AAA Properties*

| Branch | Description |
|---|---|
| AAA Interface | The SBE AAA Interface table displays the following information:<br>• AAA Address—The local AAA interface address.<br>• Network ID—A unique identifier for the SBE. |
| Accounting | The Accounting Radius Client table displays the following information:<br>• Name—The name of the accounting client.<br>• Client Type—The type of client, either Accounting or Authentication. |
| Authentication | The Authentication Radius Client table displays the following information:<br>• Name—The name of the authentication client.<br>• Client Type—The type of client, either Accounting or Authentication. |
| Billing | The SBE Billing table displays the following information related to billing:<br>• LDR Check Time—The time of day (local time) to run the long duration record check.<br>• 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.<br>• Admin Status—The configuration status, available with the **running-config** command.<br>• 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 22-9 describes the H.248 properties that appear in logical inventory for the SBC SBE.

***Table 22-9 H.248 Properties***

| Branch | Description |
|---|---|
| H248 Interface | The SBC H248 Control Interface table displays the following information:<br>• IP Address:<br>– In DM mode, the IP address used to connect the DBE and the MGC.<br>– In UM mode, the IP address used to connect the SBC and the media gateway.<br>• Port—The port for the H.248 controller interface.<br>• Transport—The transport the H.248 controller interface uses.<br>• Association—The relationship between the SBE and the media gateway. |
| Media Gateway | The Media Gateway table displays the following information:<br>• IP Address—The IP address of the media gateway.<br>• 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 22-10 describes the policy properties that appear in logical inventory for the SBC SBE.

*Table 22-10 Policy Properties*

| Branch | Description |
|---|---|
| Blacklist | The Blacklists table contains the following information:<br>• Name—The blacklist name.<br>• 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.<br>The SBE CAC Policy Set table contains the following information:<br>• Policy Set Number—An identifying number the SBE has assigned to the policy set.<br>• First Table—A CAC policy table.<br>• Status—Whether the policy is active or inactive. If the policy is active, the SBC applies the defined rules to events.<br>• 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.<br>• Description—A brief description of the policy set. |
| Call Policy | A call policy set is used for number analysis and routing.<br>The SBE Call Policy Set table contains the following information:<br>• Policy Set Number—An identifying number the SBE has assigned to the policy set.<br>• Status—Whether the policy is active or inactive. If the policy is active, the SBC applies the defined rules to events.<br>• First Call Table—The first call table used for call policy match.<br>• Description—A brief description of the policy set. |
| Codec List | The SBE Codec List table contains the following information:<br>• Name—The name of the codec list.<br>• Codecs—The codecs contained in each list. |

*Table 22-10 Policy Properties (continued)*

| Branch | Description |
|---|---|
| Current Blacklisting | The Current Blacklistings table contains the following information:<br>• Type—The type of source this blacklist applies to. Blacklists are used to block certain VoIP services that meet specified conditions.<br>• Event Type—The type of event this blacklist applies to, such as CORRUPT_MESSAGE.<br>• Is All Source Addresses—Whether the blacklist applies to all source IP addresses:<br>– True—Ignore any IP address in the Source Address field.<br>– False—Use the IP address in the Source Address field.<br>• Source Address—The IP address that this blacklist applies to.<br>• Source Port Number—The port number that this blacklist applies to.<br>• Source Port Type—The type of port this blacklist applies to. *All* is a valid entry.<br>• 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.<br>The Global Hunting Trigger List table contains the following information:<br>• Hunting Mode—Indicates the protocol to use to search for routes, such as Session Initiation Protocol (SIP).<br>• 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 22-10 Policy Properties (continued)*

| Branch | Description |
|---|---|
| QoS Profile | QoS profiles can be used by CAC policies and are used exclusively for marking IP packets.<br>The QoS Profile table contains the following information:<br>• Name—The name of the QoS profile.<br>• Class of Service—The type of call this profile applies to, such as voice, video, signaling, or fax.<br>• 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.<br>• IP Precedence—If the marking type is IP Precedence, the specified precedence, either 0 or 1.<br>• ToS—If the marking type is ToS, the ToS value.<br>• 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:<br>• SBE SDP Policy Table:<br>– Instance Name—The name of the policy table.<br>– SBE SDP Match Table—The name of the SDP match table.<br>• SBE SDP Match Table:<br>– Instance Name—The name of the SDP match table.<br>– Match Strings—The match criteria.<br>– 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 22-11 describes the SIP entries that appear in logical inventory for the SBC SBE.

*Table 22-11 SIP Properties*

| Branch | Description |
|---|---|
| SIP Account | The SBE Account table contains the following information:<br>• Name—The name of the account associated with the adjacencies.<br>• 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.<br>The SBC SIP Adjacencies table contains the following information:<br>• Name—The adjacency name.<br>• Status—The status of the adjacency, either Attached or Detached.<br>• Signaling Address—The local IP address and port (optional) for communications.<br>• Signaling Peer—The remote IP address and port (optional) for communications.<br>• Description—A brief description of the adjacency. |
| SIP Adjacency Group | The Adjacencies Groups table contains the following information:<br>• Name—The name of the SIP adjacency group.<br>• 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:<br>• Header profile—A profile based on SIP header information.<br>• Method profile—A profile based on SIP method strings.<br>• Option profile—A profile based on SIP option strings.<br>• Parameter profile—A profile based on SIP parameters. |
| SIP Profile > Header Profile | The SIP Header Profiles table contains the following information:<br>• Name—The name of the SIP header profile.<br>• Status—Whether or not the profile is in use.<br>• Profile Type—The type of profile:<br>– Whitelist—Accepts SIP requests that match the profile.<br>– Blacklist—Rejects SIP requests that match the profile.<br>• Description—A brief description of the profile. |

*Table 22-11 SIP Properties (continued)*

| Branch | Description |
|---|---|
| SIP Profile > Method Profile | The SIP Method Profiles table contains the following information:<br>• Name—The name of the SIP method profile.<br>• Status—Whether or not the profile is in use.<br>• Profile Type—The type of profile:<br>– Whitelist—Accepts SIP requests that match the profile.<br>– Blacklist—Rejects SIP requests that match the profile.<br>• Description—A brief description of the profile.<br>• Is Passthrough—Whether or not passthrough is enabled:<br>– True—Permits message bodies to be passed through for nonvital methods that match this profile.<br>– 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:<br>• Name—The name of the SIP option profile.<br>• Status—Whether or not the profile is in use.<br>• Profile Type—The type of profile:<br>– Whitelist—Accepts SIP requests that match the profile.<br>– Blacklist—Rejects SIP requests that match the profile.<br>• Description—A brief description of the profile.<br>• Options—The SIP option strings that define this profile, such as host user-agent, refer redirect, or replaces. |

*Table 22-11 SIP Properties (continued)*

| Branch | Description |
|---|---|
| SIP Profile > Parameter Profile | The SIP Parameter Profiles table contains the following information:<br>• Name—The name of the SIP parameter profile.<br>• Status—Whether or not the profile is in use.<br>• Description—A brief description of the profile. |
| SIP Timer | The SBE SIP Timer table contains the following information:<br>• 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.<br>• 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).<br>• TLS Idle Timeout—The minimum time, in milliseconds, that a Transport Layer Security (TLS) socket does not process traffic before it closes the connection.<br>• 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.<br>• 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.<br>• 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).<br>• 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). |

# Viewing SBC Statistics

The following commands can be launched from the inventory by right-clicking an SBC node and selecting **Commands**.

| Command | Navigation | Description |
|---|---|---|
| **Current 15 Min Statistics** | **Show > PM >** | Based on the command selected, the device's statistics are displayed. |
| **Current 5 Min Statistics** | | |
| **Current Day Statistics** | | |
| **Current Hour Statistics** | | |
| **H.248 Statistics** | | |
| **Previous 15 Minutes Statistics** | | |
| **Previous 5 Minutes Statistics** | | |
| **Previous Day Statistics** | | |
| **Previous Hour Statistics** | | |
| **CPS Data** | | |
| **Media Statistics** | **Show >** | |
| **Components** | | |

# Configuring SBC Components

The following commands can be launched from the logical inventory by right-clicking the Session Border Controller node. Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands.

**Note** SBC Commands are supported only on Cisco ASR 1000 Series Aggregation Services Routers

For details on the software versions Prime Network supports for the listed supported network elements, see *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

You can configure the following SBC components using the commands described in this section.

| Command | Navigation | Description |
|---|---|---|
| **SIP Adjancencies** | | |
| **Add SIP Adjacency** | *Right-click the SBC node* > **Commands > Add > SIP Adjacency** | Add an SIP adjacency or update an existing SIP adjacency. |
| **Update SIP Adjacency**<br>**Delete SIP Adjacency** | *In the SIP Adjacencies window, right-click the adjacency instance* > **Commands > Update /Delete > SIP Adjacency.** | |
| **Add SIP Adjacency Outbound AuthRealm**.<br>**Update SIP Adjacency Outbound AuthRealm**.<br>**Delete SIP Adjacency Outbound AuthRealm**. | *In the SIP Adjacencies window, right-click the SIP adjacency instance* > **Commands > Add /Update/Delete > SIP Adjacency Outbound AuthRealm**. | Use this command to add a SIP adjacency outbound authentication realm. |
| **SIP Header Profiles** | | |
| **Add SIP Header Profile** | *Right-click the SBE node* > **Commands > Add > SIP Header Profile** | Use the Add SIP Header Profile command to add a SIP header profile.<br>**Note** When you add a new SIP header profile, you can add three headers to it. You can add more headers to the new SIP header profile after it is discovered. |
| **Update SIP Header Profile**<br>**Delete SIP Header Profile** | *In the SIP Header Profiles window, right-click the profile* > **Commands > Update/Delete > SIP Header Profile** | |
| **Add SIP Header Profile Header** | *In the SIP Header Profiles window, right-click the SIP header profile instance* > **Commands > Add > SIP Header Profile Header** | Use the **Add Header** command to add a header to an existing header profile |
| **Delete SIP Header Profile Header** | *In the header profile properties window, right-click the header you want to remove and choose* > **Commands > Delete > SIP Header Profile Header** | Delete a header from a header profile. |
| **Add SIP Header Profile Entry** | *Right-click the SBE node* > **Commands > Add > SIP Header Profile Entry** | Use this command to add an entry to an existing SIP header profile header. |

| Command | Navigation | Description |
|---|---|---|
| **Update SIP Header Profile Entry**<br>**Delete SIP Header Profile Entry** | *Right-click an entry in the SIP Header Profile Header Properties window* > **Commands** > **Update/Delete** > **SIP Header Profile Entry** | Update or deletean existing SIP Header Profile entry in the **SIP Header Profile Header Properties** window. |
| **Add SIP Header Profile Condition** | *Expand the SBE node, SIP node, and SIP Profile node, and click the Header Profile node* > *double-click a header profile to open the SIP Header Profile Properties window* > *Double-click a header* > *Right-click an entry* > **Commands** > **Add** > **SIP Header Profile Condition** | Use this command to add a condition to a SIP header profile header. |
| **SIP Option Profiles** | | |
| **Add SIP Option Profile** | *Right-click the SBE node* > **Commands** > **Add** > **SIP Option Profile** | Configure SIP option profile paramters such as option profile type (whitelist or blacklist), profile options, and so on. |
| **Update SIP Option Profile**<br>**Delete SIP Option Profile** | *Right-click a profile in the SIP Option Profile window* > **Commands** > **Update/Delete** > **SIP Option Profile** | |
| **Add SIP Parameter Profile** | *Right-click the SBE node* > **Commands** > **Add** > **SIP Parameter Profile** | Configure SIP parameter profile. |
| **Delete SIP Parameter Profile** | *Click the Parameter Profile node, right-click the profile* > **Commands** > **Delete** > **SIP Parameter Profile** | |
| **Add SIP Parameter Profile Parameter** | *Expand the SBE node, SIP node, SIP Profile node* > *click the Parameter Profile* > *right-click the profile instance* > **Commands** > **Add** > **SIP Parameter Profile Parameter** | Add, update, or delete parameter in SIP parameter profiles.<br>Specify the parameter name to be updated and the name of the profile in which you want to add or update the parameter. |
| **Update SIP Parameter Profile Parameter**<br>**Delete SIP Parameter Profile Parameter** | *Double-click the profile that contains the parameter* > *right-click the parameter* > **Commands** > **Update/Delete** > **SIP Parameter Profile Parameter** | |
| **Blacklists** | | |

| Command | Navigation | Description |
|---|---|---|
| **Add Blacklist** | *Right-click the SBE node* > **Commands** > **Add** > **Blacklist** | Add or delete blacklist in the SBC node. Specify the IP address, port type, and the port number to be blacklisted. |
| **Delete Blacklist** | *In the Configured Blacklist Properties window, right-click the blacklist* > **Commands** > **Delete** > **Blacklist** | |
| **Add Blacklist Reason** | *Right-click the blacklist instance* > **Commands** > **Add** > **Blacklist Reason** | Add, modify, or delete a blacklist reason for the blacklisted node in SBC. |
| **Update Blacklist Reason**<br>**Delete Blacklist Reason** | *In the Configured Blacklist Properties window, right-click a blacklist reason* > **Commands** > **Update/Delete** > **Blacklist Reason** | |
| **Call Admission Control (CAC) Policies** | | |
| **Add CAC Policy Set** | *Right-click the SBE node* > **Commands** > **Add** > **CAC Policy Set** | Add, modify, or delete a CAC Policy Set |
| **Update CAC Policy Set**<br>**Delete CAC Policy Set** | *In the CAC Policy Set window, right-click the policy set instance* > **Commands** > **Update/Delete** > **CAC Policy Set** | |
| **Add CAC Policy Table** | *In the CAC Policy Set window, right-click the CAC policy instance* > **Commands** > **Add** > **CAC Policy Table** | Add or modify a CAC policy table in an existing CAC policy set. |
| **Update CAC Policy Table**<br>**Delete CAC Policy Table** | *Right-click a policy table in the CAC Policy Set Properties window* > **Commands** > **Update/Delete** > **CAC Policy Table** | |
| **Add CAC Rule Entry** | *Right-click a policy table* > **Commands** > **Add** > **CAC Rule Entry** | Add or modify a CAC rule entry in an existing CAC policy table. |
| **Update CAC Rule Entry**<br>**Delete CAC Rule Entry** | *Right-click an entry in the CAC Rule Entry tab* > **Commands** > **Update/Delete** > **CAC Rule Entry** | |
| **Add Call Policy Set** | *Right-click the SBE node* > **Commands** > **Add** > **Call Policy Set** | Add, modify, or delete a Call Policy Set.<br>**Note** When you add a new call policy set, you can add three call policy tables. You can add more tables after the call policy set you created is discovered. |
| **Update Call Policy Set**<br>**Delete Call Policy Set** | *Right-click a policy set in the Call Policy Set window* > **Commands** > **Update** > **Call Policy Set** | |

| Command | Navigation | Description |
|---|---|---|
| **Add Call Policy Table** | *In the Call Policy Set window, right-click the policy se*t > **Commands** > **Add** > **Call Policy Table** | Add, modify, or delete call policy tables |
| **Update Call Policy Table**<br>**Delete Call Policy Table** | Double-click a policy set, then right-click a policy table > **Commands** > **Update** > **Call Policy Table** | |
| **Add Call Rule Entry** | *Right-click a policy table* > **Commands** > **Add** > **Call Rule Entry** | Add, modify, or delete an entry from an existing call policy table. |
| **Update Call Rule Entry**<br>**Delete Call Rule Entry** | *Double-click a policy table, then right-click an entry* > **Commands** > **Update/Delete** > **Call Rule Entry** | |
| **Codec Lists** | | |
| **Add Codec List** | *Right-click the SBE node* > **Commands** > **Add** > **Codec List** | Add, or delete a Codec List |
| **Delete Codec List** | *In the Codec List window, right-click a list instance* > **Commands** > **Delete** > **Codec List** | |
| **Add Codec List Entry** | *In the Codec List window, right-click the codec list instance* > **Commands** > **Add** > **Codec List Entry** | Add, modify, or delete an entry in a codec list. |
| **Update Codec List Entry**<br>**Delete Codec List Entry** | *Double-click the codec list, then right-click the codec* > **Commands** > **Update /Delete> Codec List Entry** | |
| **Media Addresses** | | |
| **Add Media Address** | *Right-click the SBE node* > **Commands** > **Add** > **Media Address** | Add a media address or media Address DBE with parameters indicating that media address is managed by the Data Border Element (DBE) or Media Gateway Configuration (MGC). |
| **Add Media Address Dbe** | *Right-click the DBE node* > **Commands** > **Add** > **Media Address Dbe** | |
| **Delete Media Address** | *Expand the DBE node and click the Media Address node > right-click the media address* > **Commands** > **Delete** > **Media Address** | Delete an existing media address from the DBE node. |
| **QoS Profiles** | | |

| Command | Navigation | Description |
|---|---|---|
| **Add QoS Profile** | *Right-click the SBE node* > **Commands** > **Add** > **QoS Profile** | Configure QoS profile on a SBE node |
| **Update QoS Profile**<br>**Delete QoS Profile** | *Right-click the profile in the QoS Profile window* > **Commands** > **Update** > **QoS Profile** | |

CHAPTER 23

# Monitoring AAA Configurations

AAA refers to Authentication, Authorization, and Accounting, which is a security architecture for distributed systems that determines the access given to users for specific services and the amount of resources they have used.

- Authentication—This method identifies users, including their login and password, challenge and response, messaging support, and encryption. Authentication is the way to identify a subscriber before providing access to the network and network services.
- Authorization—This method provides access control, including authorization for a subscriber or domain profile. AAA authorization sends a set of attributes to the service describing the services that the user can access. These attributes determine the user's actual capabilities and restrictions.
- Accounting—This method collects and sends subscriber usage and access information used for billing, auditing, and reporting. For example, user identities, start and stop times, performed actions, number of packets, and number of bytes. Accounting enables an operator to analyze the services that the users access as well as the amount of network resources they consume. Accounting records comprise accounting Attribute Value Pairs (AVPs) and are stored on the accounting server. This accounting information can then be analyzed for network management, client billing, and/or auditing.

This chapter contains the following topics:


- Supported Network Protocols, page 23-1
- Viewing AAA Configurations in Prime Network Vision, page 23-2
- Configuring AAA Group, page 23-12


## Supported Network Protocols

AAA supports the following protocols:

- Diameter—This is a networking protocol that provides centralized AAA management for devices to connect and use a network service, and an alternative to RADIUS. Diameter Applications can extend the base protocol, by adding new commands and/or attributes.
- Remote Authentication Dial In User Service (RADIUS)—This is a networking protocol that provides centralized AAA management for devices to connect and use a network service. RADIUS is a client/server protocol that runs in the application layer, using UDP as transport. The Remote Access Server (RAS), the Virtual Private Network (VPN) server, the network switch with port-based authentication, and the Network Access Server (NAS), are all gateways that control access to the network, and all have a RADIUS client component that communicates with the RADIUS server.

# Viewing AAA Configurations in Prime Network Vision

Prime Network allows you to view the AAA configurations for Cisco ASR9000 and Cisco ASR5000 series network elements.

This topic contains the following sections:


- Viewing AAA Group Profile, page 23-2
- Viewing Dynamic Authorization Profile, page 23-3
- Viewing Radius Global Configuration Details, page 23-4
- Viewing AAA Configuration Details for an AAA group, page 23-5


## Viewing AAA Group Profile

To view the AAA group profile:

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

**Step 2** In the Inventory window, choose **Logical Inventory** > **AAA**. The AAA attribute details are displayed in the content pane.

**Note** These attributes are available only for Cisco ASR 9000 series network elements.

Table 23-1 describes the fields that are displayed in the content pane.

*Table 23-1 AAA Attributes*

| Field Name | Description |
|---|---|
| Type | Customization applied to the attribute. |
| Key | Unique format name applied to the attribute. |
| Value | Formatting applied to the attribute. |

**Step 3** In the Inventory window, choose **AAA group** node under the AAA node.

**Step 4** Under the **AAA group** node, select and expand the required group and choose the **Radius Configuration** option. The group details are displayed in the content pane.

Table 23-2 describes the fields that are displayed in the Radius Configuration dialog box.

*Table 23-2 Radius Configuration Details*

| Field Name | Description |
|---|---|
| Load Balancing Method | The load balancing method. |
| Ignore Preferred Server | Indicates if a transaction associated with a single AAA session should attempt to use the same server or not. |
| VRF | Virtual routing and forwarding (VRF) associated with the AAA group. Click the hyperlink to view the relevant node under the VRF node in the logical inventory. |
| Dead Time | The deadtime for the profile. |

# Viewing Dynamic Authorization Profile

To view the dynamic authorization profile:

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

**Step 2** In the Inventory window, choose **Logical Inventory > AAA > Dynamic Authorization**. The authorization details are displayed in the content pane. You can click on the tabs to view more details.

**Note** These attributes are available only for Cisco ASR 9000 series network elements.

Table 23-3 describes the fields that are displayed in the Dynamic authorization content pane.

*Table 23-3 Dynamic Authorization Details*

| Field Name | Description |
|---|---|
| Protocol | The name of the protocol. |
| Server Listen Port | The port number that receives service requests. |
| Ignore Server Key | Indicates whether the server key must be ignored. Values are:<br>• true<br>• false |
| **CoA Clients Tab** | |
| IP Address | The IP address of the Change of Authorization (CoA) client. |
| VRF | The associated VRF to which the CoA client belongs. Click the hyperlink to view the relevant node under the VRF node. |

# Viewing Radius Global Configuration Details

To view the radius global configuration details:

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

**Step 2** In the Inventory window, choose **Logical Inventory > AAA > Radius Global Configuration**. The authorization details are displayed in the content pane.

**Note** These attributes are available only for Cisco ASR 9000 series network elements.

Table 23-4 describes the fields that are displayed in the Radius global configuration content pane.

*Table 23-4 Radius Global Configuration Details*

| Field Name | Description |
|---|---|
| Load Balancing Method | The load balancing method using which the next host is selected. The server with the least transactions outstanding is generally picked as the next host. |
| Ignored Preferred Server | Indicates if a transaction associated with a single AAA session should attempt to use the same server or not. |
| Request Timeout | The request timeout value for the device. |
| Dead Time | The amount of time (in minutes) after which the dead RADIUS server will be treated as active. |
| Retransmit | Indicates whether retransmission of data is allowed. |
| Retransmit Count | The retransmission count. |
| Dead Criteria Time | The time interval after which the device is considered unavailable. |
| Dead Criteria Retransmit Count | The retransmission count after the dead criteria time. |
| **Accounting Servers/ Authentication Servers** | |
| Server IP | The IP address of the server. |
| Server Port | The server port. |
| Preference | The preferred server. |
| Operational State | The current operational state of the interface. |
| Administrative Status | The administrative status of the interface. |
| Retain Administrative Status After Reboot | Indicates whether the administrative status must be retained after the system reboots. |
| Keepalive Representative Group | The keepalive representative group. |
| Request Timeout | The request timeout value for the device. |
| Retransmit Count | The retransmission count. |

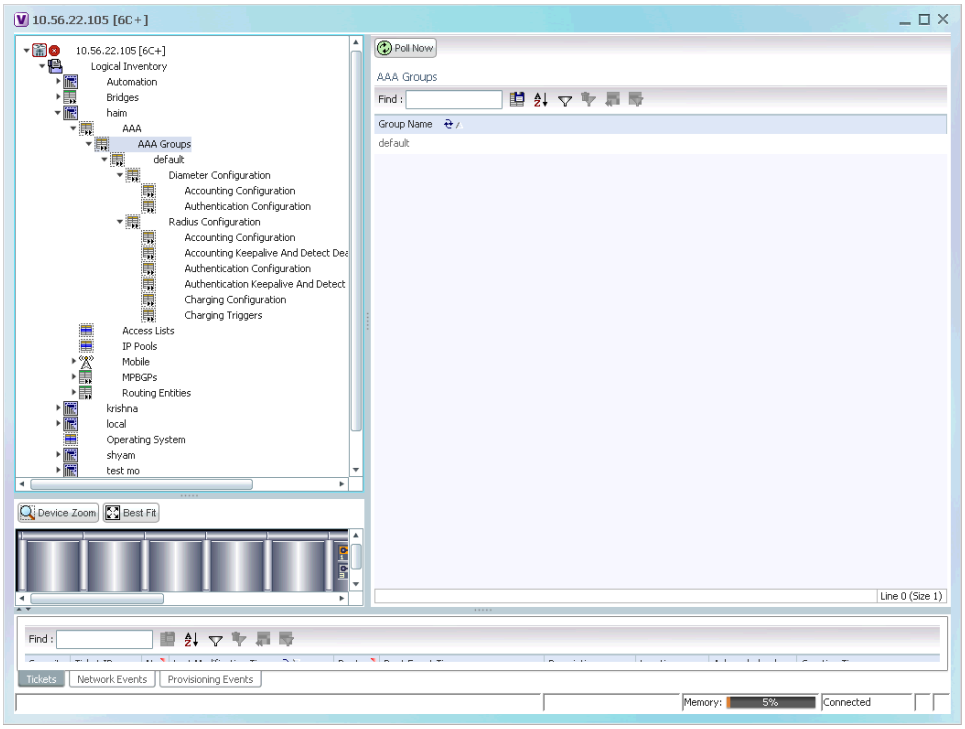
# Viewing AAA Configuration Details for an AAA group

For a Cisco ASR5000 device, Prime Network Vision allows you to view the following configurations for an AAA group:

- Diameter Configuration
  - Accounting Configuration
  - Authentication Configuration
- Radius Configuration
  - Accounting Configuration
  - Accounting Keepalive and Detect Dead Server Configuration
  - Authentication Configuration
  - Authentication Keepalive and Detect Dead Server Configuration
  - Charging Configuration
  - Charging Triggers

Prime Network Vision displays the AAA configuration details under the AAA container as shown in Figure 23-1. You can view the individual AAA group details by choosing **Logical Inventory** > *Context* > **AAA** > **AAA Groups**.

***Figure 23-1 AAA Groups in Logical Inventory***



## Viewing Diameter Configuration Details for an AAA group

To view the diameter configuration details for a AAA group:

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

**Step 2** In the Inventory window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Groups**.

You can view the AAA groups on the content pane.

**Step 3** Choose **Diameter Configuration** under a specific AAA group node. The diameter configurations made for accounting servers and authentication servers are displayed in the respective tabs on the content pane. Click on the tabs to view more details.

Table 23-5 describes the diameter configuration details for accounting and authentication servers.

*Table 23-5 Diameter Configuration*

| Field Name | Description |
|---|---|
| **Accounting Servers/Authentication Servers** | |
| Server Host | Host name of the diameter authentication/accounting server. |
| Priority | Relative priority of the diameter authentication/accounting server. |
| Number of Instances in Up State | Number of instances between the diameter authentication/accounting server and the AAA manager that are in UP status. |
| Number of Instances in Down State | Number of instances between the diameter authentication/accounting server and the AAA manager that are in DOWN status. |

**Step 4** In the Inventory window, choose **Accounting Configuration** or **Authentication Configuration** under the **Diameter Configuration** node. The configuration details are displayed on the content pane.

Table 23-6 describes the accounting/authentication diameter configuration details.

*Table 23-6 Accounting/Authentication Diameter Configuration*

| Field Name | Description |
|---|---|
| Dictionary | Diameter dictionary used for accounting/authentication. |
| Endpoint Name | Diameter endpoint used for accounting/authentication. |
| Maximum Transmissions | Maximum number of transmission attempts for diameter accounting/authentication. |
| Maximum Retries | Number of retry attempts for diameter accounting/authentication requests. |
| Request Timeout | Diameter accounting/authentication request timeout period. |
| Redirect Host AVP | Indicates whether to use:<br>• one returned AVP<br>• the first returned AVP as the primary host and the second returned AVP as the secondary host.<br>This field is applicable only for Authentication configuration. |

## Viewing Radius Configuration Details for an AAA Group

To view the radius configuration details for an AAA group:

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

**Step 2** In the Inventory window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Group**s > *AAA Group* > **Radius Configuration**. The configurations made for accounting, authentication, charging, and charging accounting servers are displayed in the respective tabs on the content pane. Click on the tabs to view more details.

Table 23-7 describes the radius configuration details for accounting, authentication, charging, and charging accounting servers.

***Table 23-7 Radius Configuration***

| Field Name | Description |
|---|---|
| Dictionary | The radius dictionary. |
| Strip Domain | Indicates whether the domain must be stripped from the user name prior to authentication or accounting. |
| Authenticator Validation | Indicates whether the MD5 authentication of the user is enabled or disabled. |
| Allow Server Down Authentication | Indicates whether subscriber sessions are allowed when RADIUS authentication is unavailable. |
| Allow Server Down Accounting | Indicates whether subscriber sessions are allowed when RADIUS accounting is unavailable. |
| **Accounting Servers/Authentication Servers/Charging Servers/Charging Accounting Servers** | |
| Server Name | IP address of the RADIUS server. |
| Server Port | Port used to communicate with the RADIUS server. |
| Preference | Preference of the RADIUS server. |
| Operational State | Status of the RADIUS server. |
| Administrative Status | Administrative status of the RADIUS server. |
| Retain Administrative Status after Reboot | Indicates whether the administrative status must be retained when the system reboots. |
| Keepalive Representative Group | Name of the Keepalive representative group. |

## Viewing Radius Accounting Configuration Details for an AAA group

To view the radius accounting configuration details for an AAA group:

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

**Step 2** In the Inventory window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Group**s > *AAA Group* > **Radius Configuration** > **Accounting Configuration**. The accounting configuration details are displayed in the content pane.

Table 23-8 describes the radius accounting configuration details.

*Table 23-8 Radius Accounting Configuration*

| Field Name | Description |
|---|---|
| Server Selection Algorithm | The algorithm to select the RADIUS accounting server(s) to which accounting data must be sent. Values are:<br>• first-n n Default<br>• first-server<br>• round-robin |
| Billing Version | The billing system version of RADIUS accounting servers. |
| Server Deadtime | The number of minutes after which communication must be attempted with a server that is not reachable. |
| Maximum Outstanding Messages | The maximum number of outstanding messages that can be queued with the AAA manager. |
| Fire and Forget | Indicates whether RADIUS Fire-and-Forget accounting is enabled for the AAA group. |
| Maximum Transmissions | The maximum number of transmissions attempted for a RADIUS accounting message, before it is declared FAILED. |
| Maximum Retries | The maximum number of attempts with the AAA server, before it is declared Not Responding and the detect dead server's consecutive failures count is incremented. |
| Maximum PDU Size (Bytes) | The maximum packed data unit size, in bytes, that can be accepted or generated. |
| Response Timeout | The time period, in seconds, to wait for a response from the RADIUS server, before resending the message. |
| Remote Address | Indicates whether the remote IP address lists are configured and the collection of accounting data for the addresses in these lists are enabled. |
| Archive Messages | Indicates whether archiving of the RADIUS accounting messages in the system (after retries to all available RADIUS accounting servers) is enabled. |
| APN To Be Included | The Access Point Name (APN) associated with the RADIUS accounting. |
| Interim Interval | The time interval (in seconds) between sending interim accounting records. |
| GTP Trigger Policy | The downlink volume that triggers interim RADIUS accounting. |

## Viewing the Radius Keepalive and Detect Dead Server Configuration Details for an AAA group

To view the radius accounting/authentication Keepalive and Detect Dead Server Configuration details:

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

**Step 2** In the Inventory window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Group**s > *AAA Group* > **Radius Configuration** > **Accounting Keepalive and Detect Dead Server Configuration** or **Authentication Keepalive and Detect Dead Server Configuration**. The configuration details are displayed in the content pane.

Table 23-9 describes the radius accounting keepalive and detect dead server configuration details.

***Table 23-9 Radius Accounting Keepalive and Detect Dead Server Configuration details***

| Field Name | Description |
|---|---|
| Keepalive Interval | The time interval (in seconds) between two keepalive access requests. |
| Keepalive Timeout | The time period to wait for a response from the RADIUS server, before resending the message. This value is displayed in seconds. |
| KeepAlive Maximum Retries | The maximum number of keepalive access requests to be sent, before the server is declared as not reachable. |
| Keepalive Consecutive Response | The number of consecutive accounting responses after which the server is declared as reachable. |
| Username | The accounting user name. |
| Calling Station ID | The calling station ID to be used for keepalive accounting. |
| Keepalive Password | The password to be used for authentication. This field is available only for authentication configuration. |
| Keepalive Allow Access Reject | Indicates the valid response for authentication request. This field is available only for authentication configuration. |
| Detect Dead Server Consecutive Failures | The number of consecutive failures for an AAA manager, before the status of an accounting server is changed from Active to Down. |
| Detect Dead Server KeepAlive | The number of seconds to wait for a response to any message, before the status of an accounting server is changed from Active to Down. |

## Viewing the Radius Authentication Configuration Details for an AAA group

To view the radius authentication configuration details for an AAA group:

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

**Step 2** In the Inventory window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Group**s > *AAA Group* > **Radius Configuration** > **Authentication Configuration**. The authentication configuration details are displayed in the content pane.

Table 23-10 describes the radius authentication configuration details.

*Table 23-10 Radius Authentication Configuration*

| Field Name | Description |
|---|---|
| Server Selection Algorithm | The algorithm to select the RADIUS accounting server(s) to which accounting data must be sent. Values are:<br>• first-server<br>• round-robin |
| Server Deadtime | The time period after which the status of the authentication server must be changed from Down to Active. |
| Maximum Outstanding Messages | The maximum number of outstanding messages that can be queued with the AAA manager. |
| Authentication Maximum Retries | The maximum number of attempts with the AAA server, before it is declared Not Responding and the detect dead server's consecutive failures count is incremented. |
| Authentication Maximum Transmissions | The maximum number of transmissions attempted for a RADIUS authentication message, before it is declared FAILED. |
| Authentication Response Timeout | The time period to wait for a response from the RADIUS server, before resending the message. This value is displayed in seconds. |
| APN To Be Included | The APN associated with the RADIUS authentication. |
| Authenticate Null User Name | Indicates whether the authentication of user names that are blank or empty is enabled. |
| Modify NAS IP | Indicates whether the RADIUS authentication is attempted after NAS IP is modified. |
| Probe Interval | The time interval (in seconds) before sending another probe authentication request to a RADIUS server. |
| Probe Timeout | The time period (in seconds) to wait for a response from a RADIUS server before resending the authentication probe. |
| Probe Maximum Retries | The number of retries for RADIUS authentication probe response before the authentication is declared as failed. |

## Viewing the Charging Configuration Details for an AAA group

To view the radius charging configuration details for an AAA group:

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

**Step 2** In the Inventory window, choose **Logical Inventory** > **AAA** > **AAA Group**s > *AAA Group* > **Radius Configuration** > **Charging Configuration**. The charging configuration details are displayed in the content pane.

Table 23-11 describes the charging configuration details.

*Table 23-11 Radius Charging Configuration*

| Field Name | Description |
|---|---|
| Authentication Server Selection Algorithm | The algorithm to select the RADIUS server(s) for active charging service to ensure proper load distribution amongst the available servers used for authentication requests. Value could be one of the following:<br>• first-server<br>• round-robin |
| Accounting Server Selection Algorithm | The algorithm to select the RADIUS server(s) for active charging service to ensure proper load distribution amongst the available servers for accounting requests. Value could be one of the following:<br>• first-n n Default<br>• first-server<br>• round-robin |
| Server Deadtime | The time period after which the status of the RADIUS server must be changed from Down to Active. |
| Maximum Outstanding Messages | The maximum number of outstanding messages that can be queued with the AAA manager. |
| Maximum Retries | The maximum number of attempts with the AAA server, before it is declared Not Responding and the detect dead server's consecutive failures count is incremented. |
| Response Timeout | The maximum number of retransmissions for RADIUS authentication requests. |
| Detect Dead Server Consecutive Retries | The number of consecutive failures for an AAA manager, before the status of an charging server is changed from Active to Down. |

## Viewing the Charging Trigger Configuration Details for an AAA group

To view the radius charging trigger configuration details for an AAA group:

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

**Step 2** In the Inventory window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Group**s > *AAA Group* > **Radius Configuration** > **Charging Trigger**. The charging configuration details are displayed in the content pane.

Table 23-12 describes the charging trigger configuration details.

*Table 23-12 Radius Charging Triggers Configuration*

| Field Name | Description |
|---|---|
| Serving Node Change | Indicates whether RADIUS trigger for serving node is enabled. |
| Radio Access Technology Change | Indicates whether RADIUS trigger for radio access technology change is enabled. |
| User Location Information Change | Indicates whether RADIUS trigger for user location information change is enabled. |
| Routing Area Information Change | Indicates whether RADIUS trigger for routing area information change is enabled. |
| Quality of Service Change | Indicates whether RADIUS trigger for quality of service change is enabled. |
| Mobile Station Timezone Change | Indicates whether RADIUS trigger for mobile station time zone change is enabled. |

# Configuring AAA Group

The following commands can be launched from the inventory by choosing *AAA Group* > **Commands > Configuration**. Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

| Command | Navigation | Description | Supported On |
|---|---|---|---|
| Create Diameter Accounting Server | *Right-click on AAA group* > **Commands > Configuration** | Use this command to create a new diameter accounting server. | Cisco ASR 9000 devices |
| Create Diameter Authentication Server | | Use this command to create a new diameter authentication server. | |
| Delete AAA Group | | Use this command to delete an AAA group. | |
| Modify AAA Group | | Use this command to modify the attributes of an AAA group. | |

CHAPTER 24

# Monitoring IP Pools

An IP pool is a sequential range of IP addresses within a certain network. We can have multiple pool configurations. Each pool can have a priority and can be assigned to a group.

IP addresses can be assigned dynamically from a single pool or from a group of pools. The Least Recently Used (LRU) method is used to assign IP addresses. In each pool, the addresses are placed in a queue. At the time of assigning, the address at the head of the queue is assigned, and when released is placed at the end of the queue.

When a group of pools have the same priority, an algorithm is used to determine a probability for each pool based on the number of available addresses. A pool is selected based on the probability determined. This method allocates addresses evenly from the group of pools.

IP pool supports both IPv4 and IPv6 addresses. With the IP Pool feature, Prime Network provides the flexibility of assigning IP addresses dynamically for services running on a network element. A service running on a network element can refer to an appropriate IP pool and an IP address gets assigned to the service from the IP pool.

This chapter contains the following topics:


- Viewing the IP Pool Properties, page 24-1
- Configuring IP Pool, page 24-3


## Viewing the IP Pool Properties

To view the IP pool properties for a device:

**Step 1** In Prime Network Vision, right-click the required device, and choose **Inventory**.

**Step 2** In the Inventory window, choose **Logical Inventory** > *Context* > **IP Pools**. A list of IP pools are displayed in the content pane.

Table 24-1 describes the fields that are displayed in the content pane.

***Table 24-1 IP Pool Properties***

| Field Name | Description |
|---|---|
| Table Types | Displays the type of table, which is **IP Pools**. |
| **IP Pools** | |
| Name | Name of the IP pool. |
| IP Pool Entries | Indicates whether entries exist for this pool. |

**Step 3** Right-click on an IP pool name and choose **Properties**. The IP Pool Properties dialog box is displayed as shown in Figure 24-1.

***Figure 24-1 IP Pool Properties***

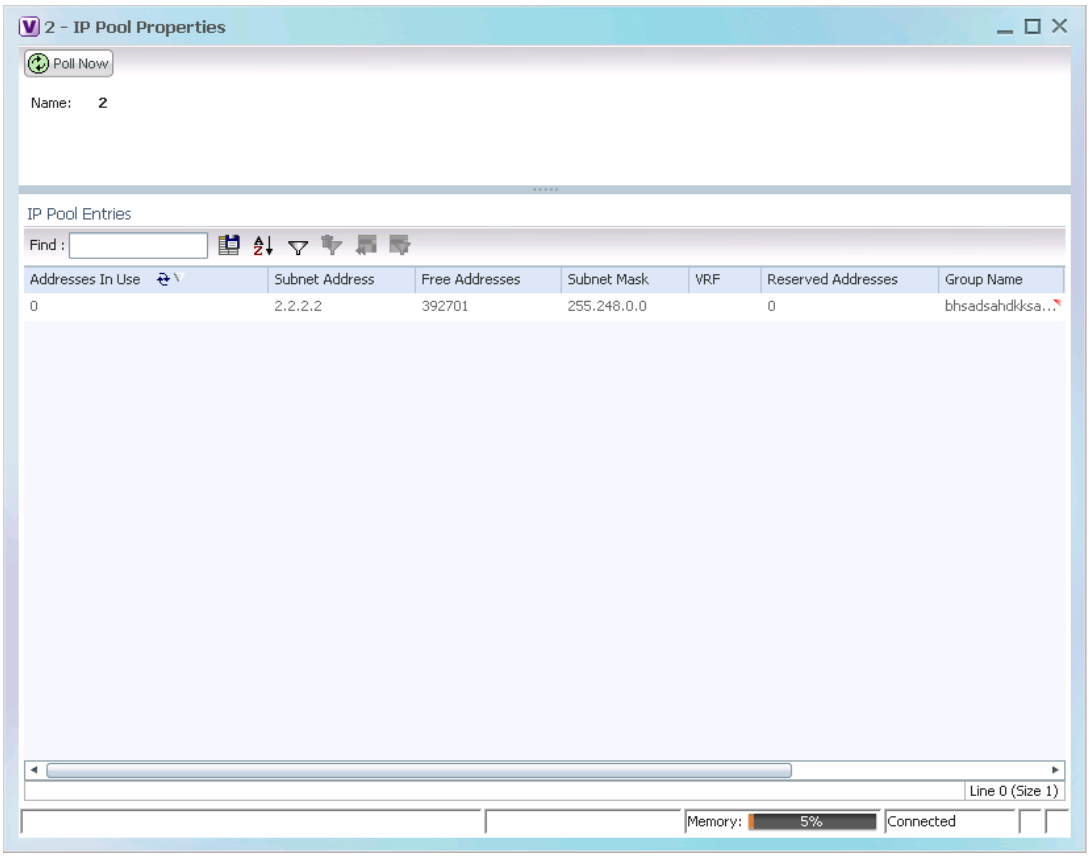


Table 24-2 describes the fields that are displayed in the IP Pool Properties dialog box.

*Table 24-2 IP Pool Properties*

| Field Name | Description |
|---|---|
| Name | Name of the IP pool. |
| **IP Pool Entries** | |
| Addresses In Use | Number of IP addresses assigned from the pool. |
| Start Address/Subnet Address | Could be one of the following:<br>• Starting IP address in the pool, if the pool is configured with a range.<br>• Subnet address, if the pool is configured with a subnet mask. |
| Free Addresses | Number of free addresses available in the pool. |
| End Address/Subnet Mask | Could be one of the following:<br>• Ending IP address in the pool, if the pool is configured with a range.<br>• Subnet mask, if the pool is configured with a subnet mask. |
| VRF | Virtual Routing and Forwarding (VRF) name, if the pool belongs to a VRF. |
| Reserved Addresses | Number of reserved addresses in the pool. |
| Group Name | Name of the group to which the pool belongs. |
| Pool Status | Status of the pool. |
| Pool Type | Type of the pool, which could be Public, Private, Static, Resource, or NAT. |
| Pool Priority | Priority of the pool, which is used when multiple pools are available. |

# Configuring IP Pool

The following commands can be launched from the inventory by right-clicking on an IP pool name and choosing **Commands > Configuration**. Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

| Command | Navigation | Description | Supported On |
|---|---|---|---|
| Delete IP Pool | *Right-click on IP Pool name* > **Commands > Configuration** | Use this command to delete an IP Pool | Cisco ASR 5000 devices |
| Modify IP Pool | | Use this command to modify IP Pool details. | |

CHAPTER 25

# Monitoring BNG Configurations

These topics provide an overview of the Broadband Network Gateway (BNG) technology and describe how to monitor and view BNG configurations in Prime Network Vision:


- Broadband Network Gateway (BNG) - An Overview, page 25-1
- User Roles Required to Work With BNG, page 25-2
- Working with BNG Configurations, page 25-3
- Viewing Policy Container, page 25-12
- Viewing QoS Profile, page 25-15


## Broadband Network Gateway (BNG) - An Overview

Broadband Network Gateway (BNG) provides capabilities that help to improve the service provider's ability to manage the subscriber's services, and simplify overall network operations. BNG is a functionality that comprises subscriber management at a logical aggregation point in the network, which manages the subscriber's user experience through identification, address assignment, authentication, authorization, accounting, and various other features such as security, Quality of Service (QoS), and subscriber forwarding.

BNG represents the subscriber as a session, which is a logical point to enable services for a given subscriber. A subscriber is usually identified with the protocol that provides the IP address of the subscriber for address assignment. For example, a subscriber that uses the Point-to-Point Protocol (PPP) to connect to the network, receives its IP address through the PPP IP Control Protocol (IPCP) negotiation, and is represented as a PPP session. A subscriber that uses Ethernet to connect to the network receives its IP address through Dynamic Host Control Protocol (DHCP) and is represented as an IP session.

The purpose of deploying BNG at the provider edge is to better manage and enrich the subscriber experience.

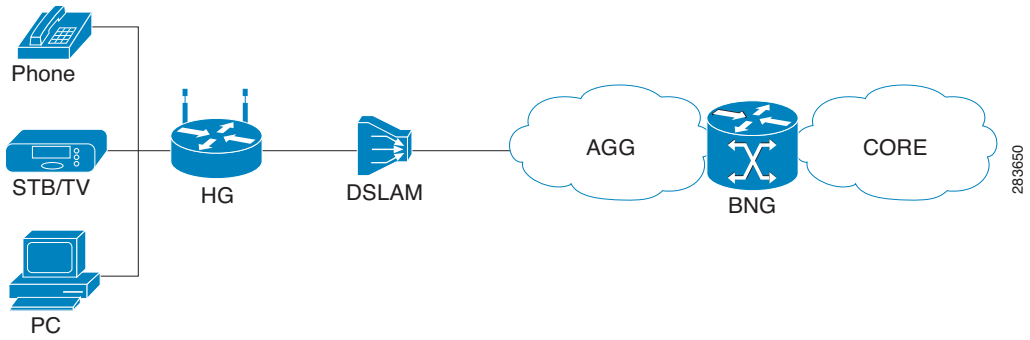
BNG separates subscriber access functions from provider services and yields these benefits:

- Comprehensive session management and billing functions are supported by means of communication with an authentication, authorization, and accounting (AAA) server that is separate from the BNG.
- Subscribers can obtain services based on their subscriber ID or a combination of their subscriber ID and access line.

The network topology for BNG can be explained using the following models:

- BNG Retail Model—The subscriber connects to the network over a digital subscriber line (DSL) circuit into a DSL access multiplexor (DSLAM), which aggregates a number of subscribers. The DSLAMs are connected to an aggregation network, which grooms the subscriber traffic and switches it to BNG. A sample of the retail model is shown in Figure 25-1.

***Figure 25-1 BNG Retail Model***




- BNG Wholesale Model—The subscriber's traffic is handed off by the carrier (who still owns the infrastructure) toone of the several Internet Service Providers (ISP). There are different ways to make this handoff, Layer 2 Tunneling Protocol (L2TP) or Layer 3 virtual private networking (VPN) being two such methods.

The BNG Retail model is used for deployment in Prime Network.

Prime Network provides BNG support for Cisco Aggregation Service Router (ASR) 9000 series network elements.

The following topics describe more about the BNG configuration details:

- User Roles Required to Work With BNG, page 25-2
- Working with BNG Configurations, page 25-3

# User Roles Required to Work With BNG

This topic identifies the roles that are required to work with BNG. 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 3.10 Administrator Guide*.

*Table 25-1 Default Permission/Security Level Required for BNG*

| Task | Viewer | Operator | OperatorPlus | Configurator | Administrator |
|---|---|---|---|---|---|
| View BBA profiles | X | X | X | X | X |
| View Subscriber Access Points | X | X | X | X | X |
| Diagnose Subscriber Access Points | — | — | — | X | X |
| View DHCP Service Profile | X | X | X | X | X |
| View IP Subscriber Template | X | X | X | X | X |
| View PPP Templates | X | X | X | X | X |
| View Service Templates | X | X | X | X | X |
| View policy details | X | X | X | X | X |
| View QoS profile | X | X | X | X | X |
| View AAA Group profile | X | X | X | X | X |
| View Dynamic Authorization profile | X | X | X | X | X |
| View Radius Global Configuration details | X | X | X | X | X |

# Working with BNG Configurations

This topic contains the following sections:


- View Broadband Access (BBA) Groups, page 25-3
- View Subscriber Access Points, page 25-5
- Diagnose Subscriber Access Points, page 25-6
- View Dynamic Host Configuration Protocol (DHCP) Service Profile, page 25-7
- View Dynamic Config Templates, page 25-9
- Viewing Policy Container, page 25-12
- Viewing QoS Profile, page 25-15
- Viewing AAA Configurations in Prime Network Vision, page 23-2


## View Broadband Access (BBA) Groups

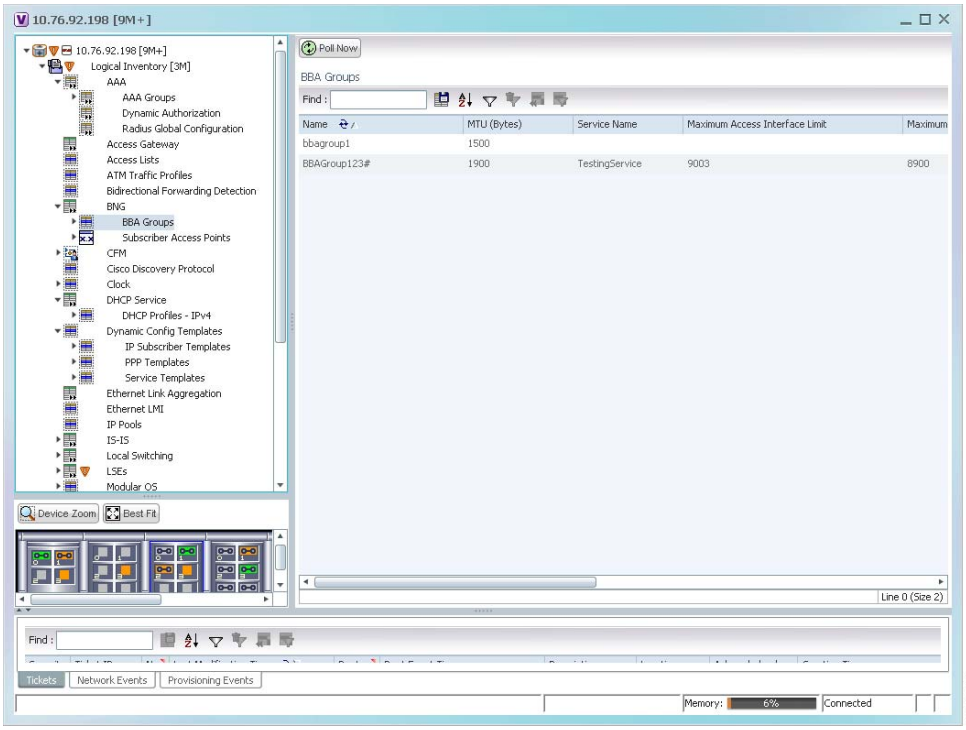
BBA groups refer to the configuration settings applicable to a subscriber session that are accessing the network through an access interface. The same group can be applied to multiple access interfaces. For example, the maximum session limit for an access interface.

To view the BBA group profile:

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

**Step 2** In the Inventory window, choose **Logical Inventory > BNG > BBA Groups**. A list of BBA groups is displayed in the content pane as shown in Figure 25-2.

*Figure 25-2 BBA Groups Content Pane*




**Step 3** Right-click on a group from the list and choose **Properties**. The BBA Group Properties dialog box is displayed.

Table 25-2 describes the fields that are displayed in the BBA Group Properties dialog box.

*Table 25-2 BBA Group Properties*

| Field Name | Description |
|---|---|
| Name | The name of the BBA Group. |
| MTU (Bytes) | The default maximum payload, which can be any value between 500 and 2000. |
| Service Name | The name of the service configured under the specified BBA group. |
| Maximum Access Interface Limit | The maximum limit of PPP over Ethernet (PPPoE) sessions on the access interface. |
| Maximum Circuit ID Limit | The maximum limit of PPPoE sessions for the circuit ID. |
| Maximum Session Limit | The maximum session limit per card. A warning is displayed if the session exceeds the limit specified here. |
| Maximum MAC Address Access Limit | The maximum limit for MAC address access. A warning is displayed if the access exceeds the limit specified here. |
| Maximum Payload Limit | The maximum payload limit. |
| Service Selection | Indicates the status of advertising of unrequested services names. By default, this service is enabled. |

*Table 25-2 BBA Group Properties (continued)*

| Field Name | Description |
|---|---|
| **Applied Interfaces** | |
| Interface Name | The name of the interface applied to the BBA Group. |
| Entity Association | The link to the applied interface. Click this hyperlink to view the relevant node under the Subscriber Access Point node. |

# View Subscriber Access Points

Subscriber access points refer to the access interfaces that are named based on the parent interface. For example, bundle-ether 2.100.pppoe312. The subscribers on bundles (or bundle-VLANs) interfaces allow redundancy and are managed on the route processor (RP). However, the subscribers over physical interfaces are created and managed on the line card (LC) and are not redundant.

To view the subscriber access points profile:

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

**Step 2** In the Inventory window, choose **Logical Inventory > BNG > Subscriber Access Points**. A list of access points is displayed in the content pane.

**Step 3** Right-click on an access point from the list and choose **Properties**. The Subscriber Access Point Properties dialog box is displayed.

Table 25-3 describes the fields that are displayed in the Subscriber Access Point Properties dialog box.

*Table 25-3 Subscriber Access Point Properties*

| Field Name | Description |
|---|---|
| Access Point | The name of the access point. |
| Associated Entity | The link to the associated entity. Click this hyperlink to view the associated Data Link Aggregation record under the Ethernet Link Aggregation node. |
| Access Type | The access type for the subscriber access point, which can be any one of the following:<br>• PPPOE_AND_IP<br>• PPPOE<br>• IP |
| Ingress Service Policy | The service policy for the access point, which when clicked will display the relevant policy under the Policy Container node. |
| Ingress QoS Policy | The Quality of Service policy for the inbound traffic, which when clicked will display the relevant policy under the Policy Container node. |

*Table 25-3 Subscriber Access Point Properties (continued)*

| Field Name | Description |
|---|---|
| Egress QoS Policy | The Quality of Service policy for the outbound traffic of the access point, which when clicked will display the relevant policy under the Policy Container node. |
| BBA Group | The BBA group to which the access point is associated. Click this hyperlink to view the relevant group under the BBA group node. |
| DHCP Profile | The DHCP profile to which the access point is associated. Click this hyperlink to view the relevant profile under the DHCP node. |
| IP Address | The destination address for User Datagram Protocol (UDP) broadcasts. |
| VRF | The Virtual Routing and Forwarding (VRF) in which the access points operates. |

# Diagnose Subscriber Access Points

The following commands can be launched from the inventory by right-clicking the **BNG > Subscriber Access Points** node and selecting the **Commands > Diagnose** option**.** Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

*Table 25-4 Diagnose Subscriber Access Points*

| Diagnose command | Input parameters |
|---|---|
| **Show DHCP Binding** | Binding Type |
| Show IP Subscriber Management Trace | • Trace Event Type<br>• Trace Count |
| Show PPoE Trace | • Trace Filter Type<br>• Trace Count |
| Show Subscriber Dynamic Template Trace All | • Trace Filter Type<br>• Trace Event Type<br>• Trace Count |
| Show Subscriber Manager Disconnect History | Disconnect History Filter Type |
| Show Subscriber Manager Session History | • Session Type<br>• ID Value |

*Table 25-4 Diagnose Subscriber Access Points (continued)*

| Diagnose command | Input parameters |
|---|---|
| Show Subscriber Manager Trace | • Trace Filter Type<br>• Trace Event Type<br>• Trace Count |
| Show Subscriber Session Details by Filter | • Session Filter Type<br>• Filter Value<br>• Filter State |

# View Dynamic Host Configuration Protocol (DHCP) Service Profile

DHCP is used to automate host configuration by assigning IP addresses, delegating prefixes (in IPv6), and providing extensive configuration information to network computers.

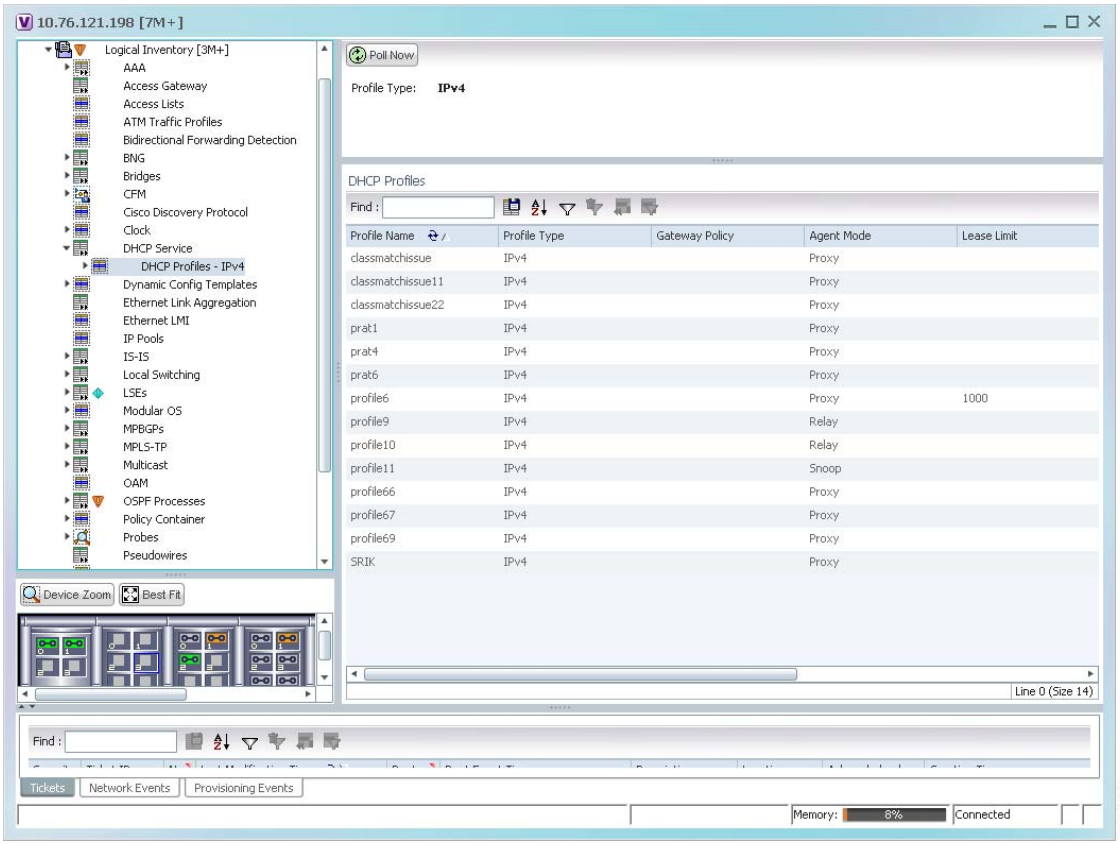
DHCP has the capability to allocate IP addresses only for a specified period of time, which is known as the lease period. If a client device wants to retain the IP addresses for a period longer than the lease period, then the client must renew the lease before it expires. A client can renew the lease depending on the configuration time sent from the server. A REQUEST message is unicast by the client using the server's IP address. On receiving the REQUEST message, the server responds with an acknowledgment, and the client's lease is extended by the lease time configured in the acknowledgment message.

To view the DHCP service profile:

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

**Step 2** In the Inventory window, choose **Logical Inventory > DHCP Service > DHCP Profiles - IPv4**. A list of DHCP profiles are displayed in the content pane as shown in Figure 25-3.

*Figure 25-3 DHCP Profiles*




**Step 3** Right-click on a service from the list and choose **Properties**. The DHCP Profile Properties dialog box is displayed.

Table 25-5 describes the fields that are displayed in the DHCP Profile Properties dialog box.

*Table 25-5 DHCP Profile Properties*

| Field Name | Description |
|---|---|
| Profile Name | The name of the DHCP profile. |
| Profile Type | The network protocol that the profile belongs to. The profile type can be IPV4 or IPV6. |
| Agent Mode | The DHCP agent mode, which can be Relay, Snoop or Proxy. |
| Lease Limit | The lease limit for the profile. |
| Lease Limit Type | The lease limit type. |
| Relay Information Check | Indicates whether the relay information check is enabled or disabled. |
| Relay Information Policy | The relay information policy. |
| **DHCP Agent Information Options** | |
| Option | The relay agent information options key parameter. |

*Table 25-5 DHCP Profile Properties (continued)*

| Field Name | Description |
|---|---|
| Value | The value of the relay agent information options. |
| **Applied Interfaces** | |
| Interface Name | The name of the interface applied to the DHCP Group. |
| Entity Association | The link to the applied interface. Click this hyperlink to view the relevant node under the Subscriber Access Point node. |
| **DHCP Servers** | |
| Profile Class | The profile class. |
| Server Address | The IP address of the profile, which is used to relay packets. |
| VRF | The VRF of the DHCP profile. Click this hyperlink to view the relevant node under the VRFs node. |
| Gateway Address | The IP address of the gateway. |
| Match Option | The match option of the DHCP profile. |
| Match Option Value | The value of the match option. |
| Match Option Mask | The match option mask. |

# View Dynamic Config Templates

A dynamic template is used to group configuration items, which are later applied to a group of subscribers. This template is globally configured through the command line interface (CLI). However, the template does not get applied to a subscriber interface as soon as it is configured. It must be activated using a control policy. Similarly, you must deactivate the template using a control policy to remove its association with the subscriber interface.

Ideally, you can activate more than one dynamic template on the same subscriber interface, for the same event or different events. The same dynamic-template can be activated on multiple subscriber interfaces through the same control policy.

Prime Network supports the following types of dynamic templates:

- IP subscriber templates
- PPP templates
- Service templates

To view the configuration templates:

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

**Step 2** In the Inventory window, choose **Logical Inventory > Dynamic Config Templates > IP Subscriber Templates** or **PPP template** or **Service template**. A list of templates is displayed in the content pane.

**Step 3** Select a template from the list, right-click and choose **Properties** to view its details.

Table 25-6 describes the fields that are displayed in the corresponding dialog box.

*Table 25-6 Template Properties*

| Field Name | Description |
|---|---|
| Name | The name of the subscriber template. |
| Template Type | The template type, which can be **IP Subscriber, PPP** or **Service** based on the selected template. |
| Ingress Policy | The name of the ingress service policy associated with the subscriber template. This field is applicable only for IP Subscriber and Service templates. |
| Associated Ingress Policy | The associated ingress policy. Click this hyperlink to view the relevant node under the Policy Container node. This field is applicable only for IP subscriber templates. |
| Egress Policy | The name of the egress service policy associated with the subscriber template. This field is applicable only for IP Subscriber and Service templates. |
| Associated Egress Policy | The associated egress policy. Click this hyperlink to view the relevant node under the Policy Container node. This field is applicable only for IP Subscriber and Service templates. |
| Ingress Access-List | The name of the ingress access-list associated with the subscriber template. This field is applicable only for IP subscriber templates. |
| Associated Ingress-ACL Entity | The associated ingress access list. Click this hyperlink to view the related list in the Access List node. This field is applicable only for IP subscriber templates. |
| Egress Access-List | The name of the egress access-list associated with the subscriber template. This field is applicable only for IP subscriber templates. |
| Associated Egress-ACL Entity | The associated egress access list. Click this hyperlink to view the related list in the Access List node. This field is applicable only for IP subscriber templates. |
| Mtu | The maximum transmission unit for IPv4. |
| Idle Timeout | The idle timeout for the subscriber template in seconds. This field is applicable only for IP Subscriber and Service templates. |
| Keep Alive Enabled | Indicates whether the Keep alive feature is enabled. This field is applicable only for PPP templates. |
| Keep Alive Interval | The keep alive interval time in terms of seconds. This field is applicable only for PPP templates. |
| Maximum Bad Authentication Request | The maximum number of authentication failures, which can be any value between 0 and 10. This field is applicable only for PPP templates. |
| Maximum Unacknowledged Request | The maximum number of unacknowledged configured requests, which can be any value between 4 and 20. This field is applicable only for PPP templates. |
| Maximum Negative Acknowledgement | The maximum number of consecutive configuration negative acknowledgements, which can be any value between 2 and 10. This field is applicable only for PPP templates. |

## Viewing the Settings for a PPP Template

In addition to the above details, you can also view the following settings for a PPP template:

- IPCP Settings
- LCP Settings
- Authentication Settings
- PPP Timeout Settings

To view the settings:

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

**Step 2** In the Inventory window, choose **Logical Inventory > Dynamic Config Templates > PPP template**. A list of templates is displayed in the content pane.

**Step 3** Select a template from the list, right-click and choose **Properties** to view its details. You can click on the tab to view more details. The IPCP tab is displayed by default.

Table 25-7 describes the fields that are displayed in the corresponding dialog box.

*Table 25-7 PPP Template Settings*

| Field Name | Description |
|---|---|
| DNS Server | The IPCP negotiation primary and secondary DNS IP address. |
| WINS Server | The IPCP negotiation primary and secondary WINS IP address. |
| IPAddress PoolName | The IPCP negotiation name of the peer-address pool. |
| Associated IP Pool Entity | The associated IP pool entity for the template. |
| ReNegotiation Enabled | Indicates whether the attempts by the peer to renegotiate IPCP is enabled. |
| **LCP Settings tab** | |
| Delay | The time period (in seconds or milliseconds) to delay before starting active LCP negotiations. |
| ReNegotiation Enabled | Indicates whether the attempts by the peer to renegotiate LCP is enabled. |
| **Authentication Settings tab** | |
| Authentication Type | The PPP link authentication method, which can be any one of the following:<br>• chap<br>• ms-chap<br>• pap |
| Chap Host Name | The Challenge Handshake Authentication Protocol (CHAP) host name. |
| MS Chap Host Name | The mobile station CHAP host name. |
| **PPP Timeout Settings** | |
| Absolute Session Timeout | The absolute timeout for a PPP session. |

*Table 25-7 PPP Template Settings (continued)*

| Field Name | Description |
|---|---|
| Maximum Authentication Response WaitTime | The maximum time (in seconds) to wait for an authentication response during a PPP negotiation. |
| Maximum Authentication Retry | The maximum time (in seconds) to wait for a response during a PPP negotiation. |

# Viewing Policy Container

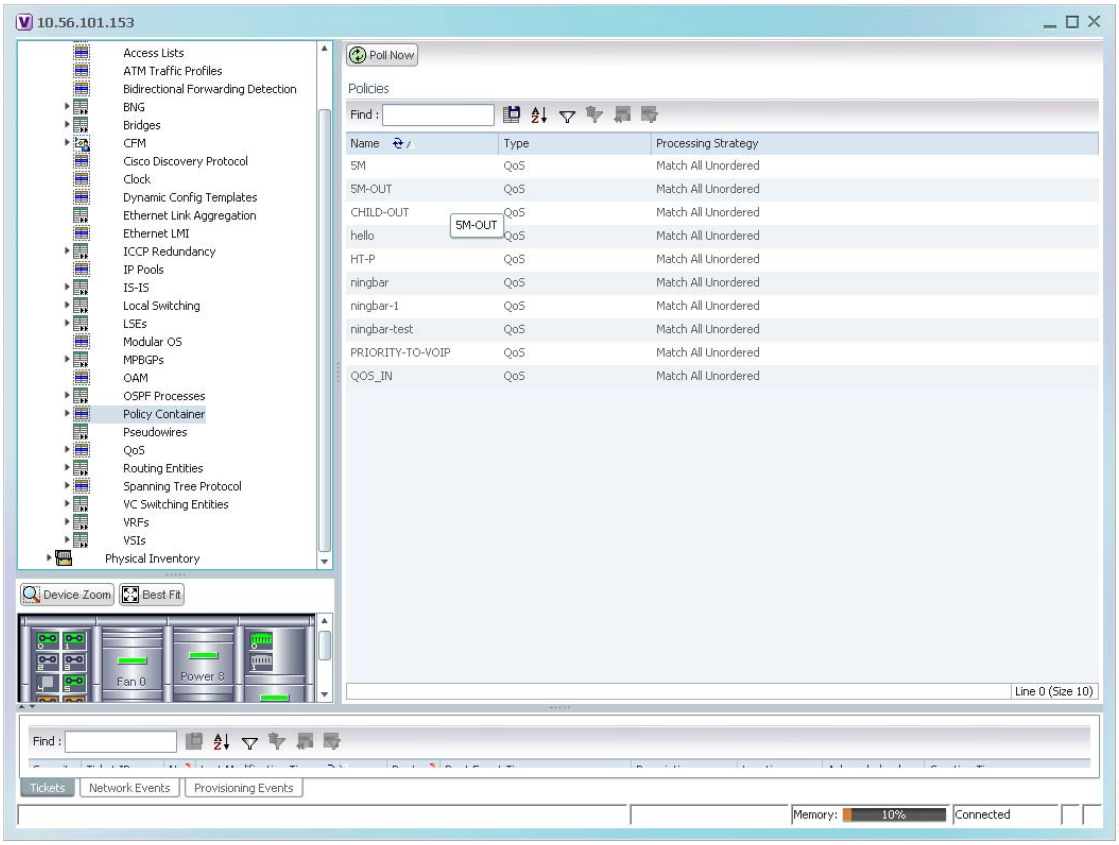
The Policy Container node in the logical inventory lists all the available service groups and service policies that are associated with service templates, BBA groups, and subscriber access points.

To view the service group and service policy profiles:

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

**Step 2** In the Inventory window, choose **Logical Inventory > Policy Container**. The Policies and Policy Group tabs are displayed in the content pane. In the Policies tab, a list of existing policies are displayed as shown in Figure 25-4.

*Figure 25-4 Policy Container*



**Step 3** Click the **Policy Group** tab. A list of existing groups are displayed.

**Step 4** Right-click on a group from the list and choose **Properties**. The Policy Group Properties dialog box is displayed.

Table 25-8 describes the fields that are displayed in the Policy Group Properties dialog box.

*Table 25-8 Policy Group Properties*

| Field Name | Description |
|---|---|
| Name | The name of the policy group. |
| Type | The type of policy group, which can be any one of the following:<br>• Accounting<br>• Control<br>• PBR<br>• Performance Traffic<br>• QoS<br>• Traffic<br>• Redirect |
| Processing Strategy | The strategy in applying the policy group, which can be any one of the following:<br>• Match First<br>• Match All Unordered<br>• Match All Ordered |
| **Policies** | |
| Name | The name of the service policy map. |
| Type | The type of policy map, which can be any one of the following:<br>• Accounting<br>• Control<br>• PBR<br>• Performance Traffic<br>• QoS<br>• Traffic<br>• Redirect |
| Processing Strategy | The strategy in applying the policies on the incoming traffic, which can be any one of the following:<br>• Match First<br>• Match All Unordered<br>• Match All Ordered |

**Step 5** Right-click on a policy from the Policies list and choose **Properties**. The **Service Policy Properties** dialog box is displayed.

Table 25-9 describes the fields that are displayed in the Service Policy Properties dialog box.

*Table 25-9 Service Policy Properties*

| Field Name | Description |
|---|---|
| Name | The name of the service policy map. |
| Type | The type of policy map, which can be any one of the following:<br>• Accounting<br>• Control<br>• PBR<br>• Performance Traffic<br>• QoS<br>• Traffic<br>• Redirect |
| Processing Strategy | The strategy in applying the policies on the incoming traffic, which can be any one of the following:<br>• Match First<br>• Match All Unordered<br>• Match All Ordered |
| **Policy Rules** | |
| Match Condition | The class map associated with the policy rule. |
| Type | The type of class map associated with the policy, which can be any one of the following:<br>• Control Subscriber<br>• QoS<br>• Traffic |
| Action Execution Strategy | The policy execution strategy, which can be any of the following:<br>• Execute All<br>• Execute Until Success<br>• Execute Until Failure |
| **Action Lists** | |
| Sequence Number | The sequence number of the policy action. |

*Table 25-9 Service Policy Properties (continued)*

| Field Name | Description |
|---|---|
| Action Type | The type of policy action, which can be any one of the following:<br>• Active<br>• Deactivate<br>• Apply<br>• Authenticate<br>• Authorize<br>• Set Timer<br>• Stop Timer<br>• Drop<br>• Accounting<br>• Conform Action<br>• Conform Color<br>• Exceed Action<br>• Exceed Color<br>• Child Conform Action<br>• Violation Action |
| Entity Type | The type of entity affected by the policy rule, which can be Dynamic template or Authorization list. |
| Entity Value | The value of the dynamic template or authorization list. |
| Entity Association | The associated entity. Click this hyperlink to view the relevant dynamic template or authorization list. |

# Viewing QoS Profile

QoS or Quality of services is the technique of prioritizing traffic flows and specifying preferences for forwarding packets with higher priority. The QoS node in the logical inventory lists all the services configured for the selected network element.

To view the QoS profile:

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

**Step 2** In the Inventory window, choose **Logical Inventory > QoS > Class of Services**. A list of existing policies are displayed in the content pane.

**Step 3** Right-click on a service in the list and choose **Properties**. The Class of Services Properties dialog box is displayed. You can click on the tabs to view more details.

Table 25-10 describes the fields that are displayed in the Class of Services Properties dialog box.

*Table 25-10 Class of Services Properties*

| Field Name | Description |
|---|---|
| Name | The name of the class of service. |
| Type | The type of the class of service. Values are:<br>• Control Subscriber<br>• QoS<br>• Traffic |
| Matching Condition | The matching condition for the service, which can be Match All or Match Any. |
| **Match Criteria Lists** | |
| Match Type | The match type, which can be any one of the following:<br>• Access group<br>• ATM<br>• Auth status<br>• COS<br>• DEI<br>• Destination-address<br>• Discard-class<br>• Domain<br>• DSCP<br>• Ethertype<br>• FR-DE<br>• Frame-relay<br>• MPLS<br>• Precedence<br>• Protocol<br>• Qos-group<br>• Source-address<br>• Timer<br>• Username<br>• VLAN<br>• VPLS |
| Match Value | The value associated with the match type. |
| Associated Entity | The entity associated to the selected access group. Click this hyperlink to view the related record in the Access List content pane. |

CHAPTER 26

# Monitoring Mobile Technologies

The following topics provide an overview of mobile technologies and describe how to work with mobile technologies in Prime Network Vision:


- User Roles Required to Work with Mobile Technologies, page 26-1
- GPRS/UMTS Networks - An Overview, page 26-4
- Working With GPRS/UMTS Network Technologies, page 26-6LTE Networks - An Overview, page 26-31
- Working with LTE Network Technologies, page 26-32
- Viewing Operator Policies, APN Remaps, and APN Profiles, page 26-105
- Working with Active Charging Service, page 26-116
- Configuring and Viewing Mobile Technologies, page 26-133


## User Roles Required to Work with Mobile Technologies

This topic identifies the GUI default permission or scope security level that is required to work with the mobile technologies 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 3.10 Administrator Guide*.

The following tables identify the tasks that you can perform:

- Table 26-1 identifies the tasks that you can perform if a selected element **is not in** one of your assigned scopes.
- Table 26-2 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 3.10 Administrator Guide*.

*Table 26-1 Default Permission/Security Level Required for Viewing GGSN, GTPU, and APN Properties - Element Not in User's Scope*

| Task | Viewer | Operator | OperatorPlus | Configurator | Administrator |
|---|---|---|---|---|---|
| Viewing GGSN properties | — | — | — | — | X |
| Viewing additional characteristics of a GGSN | — | — | — | — | X |
| Working with GGSN commands | — | — | — | — | X |
| Viewing GTPU properties | — | — | — | — | X |
| Working with GTPU commands | — | — | — | — | X |
| Viewing APN properties | — | — | — | — | X |
| Viewing additional characteristics of an APN | — | — | — | — | X |
| Working with APN commands | — | — | — | — | X |
| Viewing SAE-GW properties | — | — | — | — | X |
| Viewing P-GW properties | — | — | — | — | X |
| Working with P-GW commands | — | — | — | — | X |
| Viewing S-GW properties | — | — | — | — | X |
| Working with S-GW commands | — | — | — | — | X |
| Viewing GTPP properties | — | — | — | — | X |
| Viewing additional characteristics of a GTPP | — | — | — | — | X |
| Working with GTPP commands | — | — | — | — | X |
| Viewing EGTP properties | — | — | — | — | X |
| Working with EGTP commands | — | — | — | — | X |
| Viewing operator policies | — | — | — | — | X |
| Viewing APN remaps | — | — | — | — | X |
| Viewing APN profiles | — | — | — | — | X |
| Viewing additional characteristics of an APN profiles | — | — | — | — | X |
| Viewing active charging services (ACS) | — | — | — | — | X |
| Working with ACS commands | — | — | — | — | X |
| Viewing QCI-QoS mapping | — | — | — | — | X |
| Viewing the Layer 2 Tunnel Access Concentrator Configurations | — | — | — | — | X |
| Viewing the HSGW configuration | — | — | — | — | X |
| Viewing the Home Agent configuration | — | — | — | — | X |
| Viewing the Foreign Agent configuration details | — | — | — | — | X |

*Table 26-1 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 |
|---|---|---|---|---|---|
| Viewing the ePDG configuration details | — | — | — | — | X |
| Viewing the PDSN configuration details | — | — | — | — | X |
| Viewing the Local Mobility Anchor configuration | — | — | — | — | X |

*Table 26-2 Default Permission/Security Level Required for Viewing GGSN, GTPU, and APN Properties - Element in User's Scope*

| Task | Viewer | Operator | OperatorPlus | Configurator | Administrator |
|---|---|---|---|---|---|
| Viewing GGSN properties | X | X | X | X | X |
| Viewing additional characteristics of a GGSN | X | X | X | X | X |
| Working with GGSN commands | — | — | — | X | X |
| Viewing GTPU properties | X | X | X | X | X |
| Working with GTPU commands | — | — | — | X | X |
| Viewing APN properties | X | X | X | X | X |
| Viewing additional characteristics of an APN | X | X | X | X | X |
| Working with APN commands | — | — | — | X | X |
| Viewing SAE-GW properties | X | X | X | X | X |
| Viewing P-GW properties | X | X | X | X | X |
| Working with P-GW commands | — | — | — | X | X |
| Viewing S-GW properties | X | X | X | X | X |
| Working with S-GW commands | — | — | — | X | X |
| Viewing GTPP properties | X | X | X | X | X |
| Viewing additional characteristics of a GTPP | X | X | X | X | X |
| Working with GTPP commands | — | — | — | X | X |
| Viewing EGTP properties | X | X | X | X | X |
| Working with EGTP commands | — | — | — | X | X |
| Viewing operator policies | X | X | X | X | X |
| Viewing APN remaps | X | X | X | X | X |
| Viewing APN profiles | X | X | X | X | X |
| Viewing additional characteristics of an APN profiles | X | X | X | X | X |

*Table 26-2 Default Permission/Security Level Required for Viewing GGSN, GTPU, and APN Properties - Element in User's Scope (continued)*

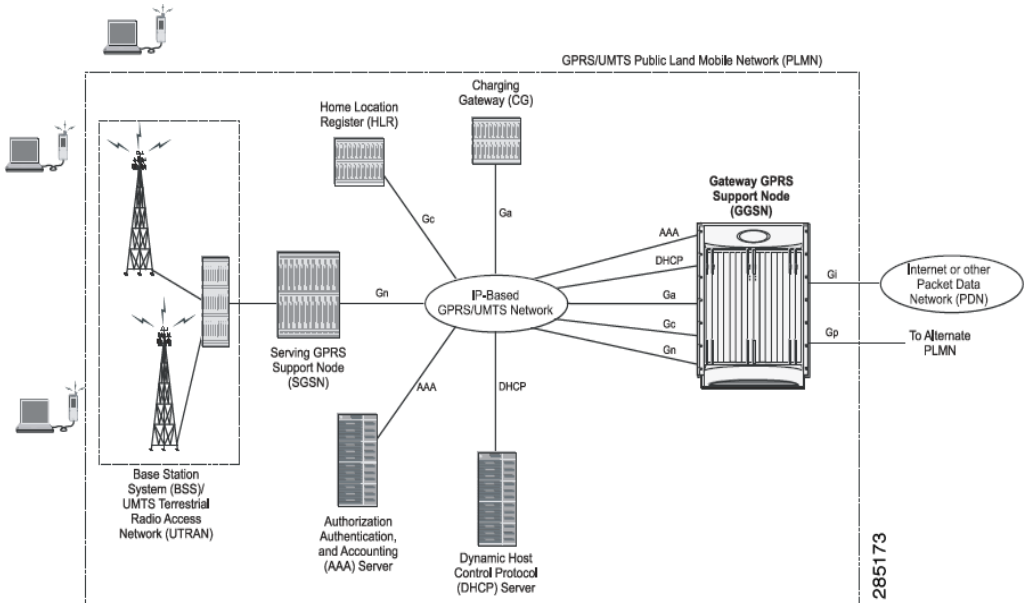
| Task | Viewer | Operator | OperatorPlus | Configurator | Administrator |
|---|---|---|---|---|---|
| Viewing active charging services (ACS) | X | X | X | X | X |
| Working with ACS commands | — | — | — | X | X |
| Viewing QCI-QoS mapping | X | X | X | X | X |
| Viewing the Layer 2 Tunnel Access Concentrator Configurations | X | X | X | X | X |
| Viewing the HSGW configuration | X | X | X | X | X |
| Viewing the Home Agent configuration | X | X | X | X | X |
| Viewing the Foreign Agent configuration details | X | X | X | X | X |
| Viewing the ePDG configuration details | X | X | X | X | X |
| Viewing the PDSN configuration details | X | X | X | X | X |
| Viewing the Local Mobility Anchor configuration | X | X | X | X | X |

# GPRS/UMTS Networks - An Overview

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 26-1 shows a basic GPRS/UMTS network topology.

*Figure 26-1 Basic GPRS/UMTS Network Topology*




The GPRS/UMTS packet core comprises two major network elements:

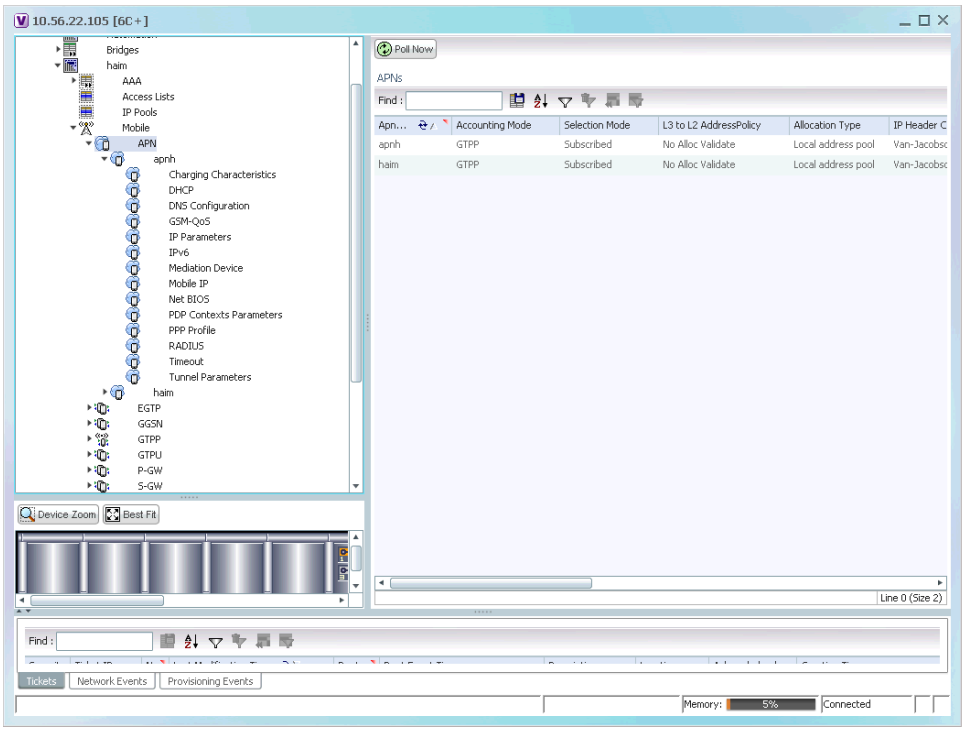
- Gateway GPRS support node (GGSN)—A gateway that provides mobile cell phone users access to a Packet Data Network (PDN) or specified private Internet Protocol (IP) networks.
- Serving GPRS support node (SGSN)—Connects the radio access network (RAN) to the GPRS/UMTS core and tunnels user sessions to 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 assignment is to be handled for that APN.

Prime Network Vision allows you to configure the mobile technologies by using commands and also view the properties configured for the mobile technologies. Figure 26-2 shows an example of the Inventory window with the mobile technology nodes/containers under the Mobile context.

From Prime Network 3.9, the mobile technologies are supported on Cisco Aggregation Service Router (ASR) 5000 series mobile gateways.

*Figure 26-2 Mobile Technology Nodes in Logical Inventory*




# Working With GPRS/UMTS Network Technologies

The following topics explain how to work with GPRS/UMTS network technologies in Prime Network Vision:

- Working with GGSN, page 26-6
- Working with GTPU, page 26-11
- Working with APN, page 26-13
- Working with GTPP, page 26-23
- Working with EGTP, page 26-29

## Working with GGSN

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.

The following topics explain how to work with GGSN in Prime Network Vision:


- Viewing GGSN Properties, page 26-7
- Viewing Additional Characteristics of a GGSN, page 26-8
- GGSN Commands, page 26-10


## 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. You can view the individual GGSN details from the table on the right pane or by choosing **Logical Inventory** > *Context* > **Mobile** > *GGSN Container* > *GGSN*.

Table 26-3 describes the details available for each GGSN.

***Table 26-3 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. |

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.

Table 26-4 describes the SGSN and PLMN information associated with the GGSN.

*Table 26-4 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. |

## Viewing Additional Characteristics of a GGSN

To view additional characteristics of a GGSN:

**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 >** *GGSN Container* **>***GGSN*.

**Step 3** Expand the *GGSN* node. The following list of characteristics configured for the GGSN are displayed:

- Charging Characteristics
- Timers And QoS

**Step 4** Choose **Charging Characteristics** to view the properties on the right pane. See Table 26-5 for more details on the charging characteristics configured for the GGSN.

*Table 26-5 GGSN Charging Characteristics*

| Field | Description |
|---|---|
| **Profiles** | |
| Profile No | Type of billing. For example:<br>• 1—Hot billing<br>• 2—Flat billing<br>• 4—Prepaid billing<br>• 8—Normal billing<br>All other profiles from 0 - 15 are customized billing types. |
| Buckets | Denotes container changes in the GGSN Call Detail Record (GCDR). |
| Prepaid | Prepaid type, which could be Prohibited or Use-rulebase-configuration. |
| Down Link Octets | Downlink traffic volume of the bucket. |
| Uplink Octets | Uplink traffic volume of the bucket. |
| Total Octets | Total traffic volume of the bucket. |
| **Tariff Time Triggers** | |
| Profile No | Type of billing. |
| Time1, Time2, and so on | First time-of-day time values, and so on, to close the current statistics container. |
| **Intervals** | |
| Profile No | Type of billing. |
| No. of SGSNs | Number of SGSN changes (inter-SGSN switchovers) resulting in a new Routing Area Identity (RAI) that can occur before closing an accounting record. |
| Interval | Normal time duration that must elapse before closing an accounting record. |
| Down Link Octets | Downlink traffic volume reached within the time interval. |
| Up Link Octets | Uplink traffic volume reached within the time interval. |
| Total Octets | Total traffic volume reached within the time interval. |

**Step 5** Under the *GGSN* node, choose **Timers and QoS** to view the properties on the right pane. See Table 26-6 for more details on the Timers and QoS parameters configured for the GGSN.

*Table 26-6 GGSN Timers and QoS*

| Field | Description |
|---|---|
| Retransmission Timeout | Timeout, in seconds, for retransmission of GTP control packets. |
| Max Retransmissions | Maximum retries for transmitting GTP control packets. |
| Setup Timeout | Maximum time, in seconds, allowed for session setup. |
| Echo Interval | Echo interval, in seconds, for GTP. |
| Guard Interval | Interval, in seconds, for which the GGSN maintains responses sent to SGSN. This optimizes the handling of retransmitted messages. |
| **QCI to DSCP Mapping** | |
| QoS class index | A set of transport characteristics used to differentiate various packet flows. |
| DSCP | Differentiated Services Code Point (DSCP), a mechanism for classifying and managing network traffic and providing QoS. |
| **QCI & ARP DSCP Mapping** | |
| QoS class index | A set of transport characteristics used to differentiate various packet flows. |
| Allocation retention priority | 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 | A mechanism for classifying and managing network traffic and providing QoS. |

## GGSN Commands

The following commands can be launched from the inventory by right-clicking a GGSN and choosing *GGSN* **> Commands > Configuration.** Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

*Table 26-7 GGSN Commands*

| Command | Navigation | Description |
|---|---|---|
| **Create PLMN Identifier** | *Right-click on a GGSN group* > Commands > Configuration | Use this command to create a PLMN Identifier. |
| **Create SGSN** | | Use this command to create an SGSN. |
| **Delete GGSN** | | Use this command to delete a GGSN profile. |
| **Modify GGSN** | | Use this command to modify a GGSN profile details. |

# Working with GTPU

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 configuration commands in Prime Network Vision. You can view the configured parameters for a GTPU in the logical inventory.

The following topics explain how to work with GTPU in Prime Network Vision:

- Viewing GTPU Properties, page 26-11
- GTPU Commands, page 26-12

## Viewing GTPU Properties

Prime Network Vision displays the GTPUs in a GTPU 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** > *GTPU Container*.

Prime Network Vision displays the list of GTPUs configured under the container. You can view the individual GTPU details from the table on the right pane or by choosing **Logical Inventory** >*Context* > **Mobile** > *GTPU Container* > *GTPU*.

Table 26-8 describes the details available for each GTPU.

*Table 26-8 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. |

## GTPU Commands

The following commands can be launched from the inventory by right-clicking a GTPU and choosing **Commands > Configuration.** Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

*Table 26-9 GTPU Commands*

| Command | Navigation | Description |
|---|---|---|
| **Create GTPU Bind IP Address** | *Right-click on a GTPU defined* > **Commands > Configuration** | Use this command to create a bind IP address for GTPU. |

*Table 26-9 GTPU Commands (continued)*

| Command | Navigation | Description |
|---|---|---|
| **Modify GTPU Bind IP Address** | Select the **GTPU** node > *right-click on an IP address in the content pane* > **Commands** > **Configuration** | Use this command to modify the Bind IP address for GTPU. |
| **Delete GTPU Bind IP Address** | | Use this command to delete the Bind IP address for GTPU. |
| **Delete GTPU** | *Right-click on a GTPU defined* > **Commands** > **Configuration** | Use this command to delete a GTPU group. |
| **Modify GTPU** | | Use this command to modify a GTPU group. |

# Working with APN

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 mobile station 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.
- Traffic policing that governs the subscriber traffic flow if it violates or exceeds configured peak or committed data rates. The traffic policing attributes represent a QoS data rate limit configuration for both uplink and downlink directions.

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 on the device. They are categorized as given below:

- Accounting—Various parameters regarding accounting possibilities, such as, charging characteristics, accounting mode (RADIUS server-based accounting, GTPP-based accounting, and so on.)
- Authentication—Various parameters regarding authentication, such as, protocols used, like, Challenge Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), or none, default username/password, server group to use, and limit for number of PDP contexts.
- Enhanced Charging—Name of rulebase to use, which holds the enhanced charging configuration (for example, 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 configure the APN parameters using Prime Network Vision. 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 Vendor Specific Attributes (VSAs) 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.

The following topics explain how to work with APN in Prime Network Vision:

- Viewing APN Properties, page 26-14
- Viewing Additional Characteristics of an APN, page 26-18
- APN Commands, page 26-23

## 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 26-18. 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*.

Table 26-10 describes the information that is available for the APN. The information that is displayed depends on the configuration of the APN.

***Table 26-10 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. |

*Table 26-10 APN Properties in Logical Inventory (continued)*

| Field | Description |
|---|---|
| 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.
- QoS Downlink Traffic Policing—Shows the attributes that represent QoS data rate limit configuration for downlink direction within the APN profile.
- QoS Uplink Traffic Policing—Shows the attributes that represent QoS data rate limit configuration for uplink direction within the APN profile.

*Table 26-11 Additional Configuration Details for APN*

| 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 (- ). |

*Table 26-11 Additional Configuration Details for APN (continued)*

| Field | Description |
|---|---|
| Rule Definition | The virtual APN rule definition can be one of the following:<br>• 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.<br>• bearer-access-service—Specifies the bearer access service name for the virtual APN.<br>• service name—Specifies the service name. Service name is unique across all the contexts. Value is a string of size 1 to 63.<br>• cc-profile—Specifies the APN for charging characteristics (CC) profile index. Value is an integer from 1 to 15.<br>• Domain name—Specifies the subscriber's domain name (realm). Domain name can be from 1 to 79 alpha and/or numeric characters.<br>• MCC—Specifies the MCC portion of the PLMN identifier. Value is an integer between 100 to 999.<br>• MNC—Specifies the MNC portion of the PLMN identifier. Value is an integer between 100 to 999.<br>• 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.<br>• Rat-Type—Specifies the rat-type option, which could be gan, geran, hspa, utran, or wlan.<br>• Roaming mode—Specifies the roaming mode, which could be Home, Visiting, or Roaming. |
| **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. |
| **QoS Downlink Traffic Policing** | |
| QCI | A scalar that denotes a set of transport characteristics and used to infer nodes specific parameters that control packet forwarding treatment. |

*Table 26-11 Additional Configuration Details for APN (continued)*

| Field | Description |
|---|---|
| Peak Data Rate | The peak data rate allowed, in bytes, for the downlink direction and QoS traffic class. |
| Committed Data Rate | The committed data rate allowed, in bytes, for the downlink direction and QoS traffic class. |
| Negotiate Limit | Indicates whether negotiation limit is enabled or disabled for the downlink direction and Qos traffic class. |
| Rate Limit | Indicates whether the rate limit is enabled or disabled for the downlink direction and Qos traffic class. |
| Burst Size Auto Readjust | Indicates whether the auto readjustment of burst size is enabled or disabled. This parameter is used in dynamic burst size calculation, for traffic policing, at the time of PDP activation of modification. |
| Burst Size Auto Readjust Duration | The burst size readjustment duration in seconds. This parameter indicates the number of seconds that the dynamic burst size calculation will last for. This allows the traffic to be throttled at the negotiated rates. |
| Peak Burst Size (bytes) | The peak burst size allowed, in bytes, for the downlink direction and QoS class. |
| Guaranteed Burst Size (bytes) | The guaranteed burst size allowed, in bytes, for the downlink direction and QoS class. |
| Exceed Action | The action to be taken on packets that exceed the committed data rate, but do not violate the peak data rate. The action could be one of the following:<br>• Drop<br>• Lower IP Precedence<br>• Transmit |
| Violate Action | The action to be taken on packets that exceed both committed and peak data rates. The action could be one of the following:<br>• Drop<br>• Lower IP Precedence<br>• Shape<br>• Transmit |
| **QoS Uplink Traffic Policing** | |
| QCI | A scalar that denotes a set of transport characteristics and used to infer nodes specific parameters that control packet forwarding treatment. |
| Peak Data Rate | The peak data rate allowed, in bytes, for the uplink direction and QoS traffic class. |
| Committed Data Rate | The committed data rate allowed, in bytes, for the uplink direction and QoS traffic class. |
| Negotiate Limit | Indicates whether negotiation limit is enabled or disabled for the uplink direction and Qos traffic class. |
| Rate Limit | Indicates whether the rate limit is enabled or disabled for the uplink direction and Qos traffic class. |

*Table 26-11 Additional Configuration Details for APN (continued)*

| Field | Description |
|---|---|
| Burst Size Auto Readjust | Indicates whether the auto readjustment of burst size is enabled or disabled. This parameter is used in dynamic burst size calculation, for traffic policing, at the time PDP. |
| Burst Size Auto Readjust Duration | The burst size readjustment duration in seconds. This parameter indicates the number of seconds that the dynamic burst size calculation will last for. This allows the traffic to be throttled at the negotiated rates. |
| Peak Burst Size (bytes) | The peak burst size allowed, in bytes, for the uplink direction and QoS class. |
| Guaranteed Burst Size (bytes) | The guaranteed burst size allowed, in bytes, for the uplink direction and QoS class. |
| Exceed Action | The action to be taken on packets that exceed the committed data rate, but do not violate the peak data rate. The action could be one of the following:<br>• Drop<br>• Lower IP Precedence<br>• Transmit |
| Violate Action | The action to be taken on packets that exceed both committed and peak data rates. The action could be one of the following:<br>• Drop<br>• Lower IP Precedence<br>• Shape<br>• Transmit |

## 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 >** *Context* **> 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.
- DHCP—Dynamic Host Control Protocol (DHCP) parameter configured, if the APN supports dynamic address assignment for PDP contexts.
- 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.

- Mediation Device—Represents the mediation device used by the APN for communication with the subscriber.
- Mobile IP—Represents mobile IP configuration of the APN.
- Net BIOS—Represents the NetBIOS server configuration used by the APN.
- PDP Contexts Parameters—Represents the PDP contexts supported by the APN.
- PPP Profile—Represents the PPP profile used by the APN.
- RADIUS—Represents the APN parameters related to communication with the RADIUS server.
- Timeout—Represents the timeout parameters of the APN.
- 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 26-12 for more details on the properties of each characteristics configured for the APN.

*Table 26-12 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. |
| Visiting 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. |
| **DHCP** | |
| Lease Expiration Policy | The action taken when leases for IP addresses assigned to PDP contexts that are facilitated by the APN, are about to expire. For example, auto renew. |
| **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. |

*Table 26-12 APN Characteristics (continued)*

| Field | Description |
|---|---|
| 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.<br>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. |
| **IPv6** | |
| Inbound Access Group Name | The name of the IPv6 access group for the APN when configured for inbound traffic. |
| Outbound 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 initial 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. |
| **Mediation Device** | |
| Mediation Accounting Enabled | Indicates whether mediation accounting is enabled or disabled. |
| No Early PDUs | Indicates whether protocol data units (PDUs) must be delayed or not until a response to the GGSN's accounting start request is received from the mediation device. If No Early PDUs is ‘true’, the chassis does not send any uplink or downlink data from or to a MS, until it receives a command from the mediation device. |
| No Interims | Indicates whether radius interim updates are sent to the mediation device or not for the APN for radius accounting. |

*Table 26-12 APN Characteristics (continued)*

| Field | Description |
|---|---|
| Delay GTP Response | Indicates whether the GTP response must be delayed or not. If this value is 'true', the GTP response is delayed and is sent to the SGSN only if the AAA server is up. If the value is 'false', the subscriber will be connected to the SGSN even if the AAA server is down. |
| **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. |
| **Net BIOS** | |
| Primary NBNS Address | Primary service address of the NetBIOS server. |
| Secondary NBNS Address | Secondary service address of the NetBIOS server. |
| **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. |
| **PPP Profile** | |
| Data Compression Protocols | The compression protocol used by the APN for compression of data packets. |
| Keep Alive | The frequency (in seconds) of sending the Link Control Protocol (LCP) keep alive messages. A value zero denotes that the keep alive messages are disabled completely. |
| Data Compression Mode | The compression mode used by the compression protocol which could be:<br>• Normal—Packets are compressed using the packet history.<br>• Stateless—Each packet is compressed individually. |
| MTU (bytes) | The maximum transmission unit (MTU) for packets accessing the APN. |
| Min. Compression Size (bytes) | The smallest packet to which compression may be applied. |
| **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. |

*Table 26-12 APN Characteristics (continued)*

| Field | Description |
|---|---|
| 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. |
| **Timeout** | |
| Absolute | Absolute timeout of a session, in seconds, for the APN. |
| Idle | Maximum duration, in seconds, after which the system considers the session as dormant or idle and invokes the long duration timer action. |
| Long Duration | Maximum duration, in seconds, before the system automatically reports or terminates the session. This is the maximum duration before the specified timeout action is activated for the session. |
| Long Duration Inactivity | Maximum duration, in seconds, before the session is marked as dormant. |
| Emergency Inactivity | Timeout duration, in seconds, to check inactivity on the emergency session. |
| Idle Activity Downlink State | Indicates whether the system must ignore the downlink traffic to consider as activity for idle-timeout. Only uplink packets will be able to reset the idle-timeout. |
| MBMS Bearer Absolute | Maximum time a Multimedia Broadcast and Multicast Server (MBMS) bearer can exist in active or idle state. |
| MBMS Bearer Idle | Maximum time an MBMS bearer context can be idle. |
| MBMS UE Absolute | Session timeout value for the MBMS user equipment. |
| IPv6 Init Solicit Wait | IPv6 initial router solicit wait timeout. |
| Long Duration Action Type | The action taken on long duration sessions. For example, the system performs any of the following actions:<br>• Detects a long duration session and sends an SNMP trap and CORBA notification.<br>• Disconnects the session after sending an SNMP trap and CORBA notification.<br>• Suppresses the SNMP trap and CORBA notification after detecting and disconnecting long duration session. |
| **Tunnel Parameters** | |
| Address Policy | The address allocation / validation policy for all tunneled calls except Layer 2 Tunneling Protocol (L2TP) calls. |
| 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. |

## APN Commands

The following commands can be launched from the inventory by right-clicking an APN and choosing **Commands > Configuration**. Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

*Table 26-13 APN Commands*

| Command | Navigation | Description |
|---|---|---|
| **Create QoS to DSCP Mapping** | *Right-click on an APN node* > **Commands > Configuration** | Use this command to create the mapping between QoS and DSCP. |
| **Create Virtual APN** | | Use this command to create a virtual APN. |
| **Delete APN** | | Use this command to delete an APN profile. |
| **Modify APN** | | Use this command to delete an APN profile. |

# Working with GTPP

GPRS Tunneling Protocol Prime (GTPP) is used for communicating accounting messages to CGs. Enhanced Ch7arging Service (ECS) supports different accounting and charging interfaces for prepaid and postpaid charging and record generation. GTPP accounting in ECS allows the collection of counters for different types of data traffic including the data in a GGSN CDR (G-CDR) that is sent to the CGF.

GTPP performs the following functions:

- Transfers CDRs between the Charging Data Function (CDF) and CGF.
- Redirects CDRs to another CGF.
- Advertises to peers about its CDR transfer capability; for example, after a period of service down time.
- Prevents duplicate CDRs that might arise during redundancy operations. The CDR duplication prevention function is carried out by marking potentially duplicated CDR packets, and delegating the final duplicate deletion task to a CGF or the billing domain, instead of handling the possible duplicates solely by GTPP messaging.

Prime Network provides support on gathering the GTPP accounting setup details that are configured in the mobile gateway for transferring the different types of CDRs from charging agent to a GTPP server or accounting server.

GTPP is configured within the accounting context of an APN and is also used by GGSN, P-GW, and S-GW to transmit CDRs to CGF.

The following topics provide details on how to work with GTPP in Prime Network Vision:

- Viewing GTPP Properties, page 26-24
- Viewing Additional Characteristics of a GTPP, page 26-25
- GTPP Commands, page 26-28

## Viewing GTPP Properties

Prime Network Vision displays the GTPPs in a GTPP container under the Mobile node in the logical inventory. The icon used for representing GTPPs in the logical inventory is explained in Logical Inventory Icons, page A-6.

To view GTPP 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** > *GTPP Container*.

Prime Network Vision displays the list of GTPP groups configured under the container. You can view the individual GTPP group details from the table on the right pane or by choosing **Logical Inventory** >*Context* > **Mobile** > *GTPP Container* > *GTPP Group*.

Table 26-14 describes the details available for each GTPP group.

***Table 26-14 GTPP Properties in Logical Inventory***

| Field | Description |
|---|---|
| Group Name | Name of the GTPP group. |
| CDR Storage Mode | Storage mode for CDRs, which could be Local or Remote. |
| CDR Timeout | Maximum amount of time the system waits for a response from the CGF before assuming the packet is lost. |
| CDR Max Retries | Number of times the system attempts to a CGF that is not responding. |
| Max CDR Size (bytes) | Maximum payload size of the GTPP packet. |
| Max CDR Wait Time | Maximum payload size of the GTPP packet. The payload includes the CDR and the GTPP header. |
| Max CDRs in Message | Maximum number of CDRs allowed in a single packet. |
| Recover Files Sequence Number | Indicates whether recovery of file sequence number is enabled or not. If enabled, everytime the machine is rebooted, the file sequence number continues from the last sequence number. |
| Data Request Start Sequence Number | The starting sequence number to be used in the GTPP data record transfer (DRT) record. |
| Start File Sequence Number | Starting value of the file sequence number. |
| Source Port Validation | Indicates whether port checking is enabled or disabled for node alive/echo/redirection requests from the CGF. |
| Dictionary | Dictionary supported by the GTPP group. |

*Table 26-14 GTPP Properties in Logical Inventory (continued)*

| Field | Description |
|---|---|
| **Accounting Server** | |
| Group | GTPP group, in which the accounting server is configured. |
| Context Name | Name of the context, in which the CGF is configured. |
| Primary Accounting Server Address | IPv4 or IPv6 address of the CGF. |
| Port | UDP port over which the GGSN communicates with the CGF. |
| State | Status of the CGF, which could be Active or Inactive. |
| Priority | Relative priority of the CGF. This priority determines which CGF server to send the accounting data to. |

## Viewing Additional Characteristics of a GTPP

To view additional characteristics of a GTPP:

**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** > *GTPP Container* >*GTPP*.

**Step 3** Expand the GTPP node. The following list of characteristics configured for the GGSN are displayed:

- Accounting Server Failure Detection—Attributes of the CGF accounting server within the GTPP server group.
- CDR Attributes Indicator—Indicates whether associated attributes are enabled or disabled for CDR generation.
- CDR Triggers—Attributes that trigger CDR generation.
- Charging Agent— IP address and port of the system interface within the current context used to communicate with the CGF or the GTPP Storage Server (GSS).
- EGCDR Data Generation Configuration—Attributes that represent the GTPP eG-CDR data generation configuration.
- Local Storage—Storage server information, if CDR storage mode is Local.
- MBMS CDR Triggers—Attributes that trigger the MBMS CDR generation.
- Storage Server—Configuration information for the GTPP backup storage server.

**Step 4** Click each of one of these characteristics to view its properties on the right pane. See Table 26-15 for more details on the properties of each characteristics configured for the GTPP.

*Table 26-15 GTPP Characteristics*

| Field | Description |
|---|---|
| **Accounting Server Failure Detection** | |
| Detect Dead Server Consecutive Failures | Number of failures that could occur before marking a CGF as dead (down). |
| Dead Server Suppress CDRs | Indicates whether suppression of CDRs is enabled or disabled when the GTPP server is detected as dead or unreachable. |
| Dead Time | Maximum duration, in seconds, before marking a CGF as dead on consecutive failures. |
| Echo Timeout | The amount of time that must elapse before the system attempts to communicate with a CGF that was previously unreachable. |
| Echo Max Retries | Number of times the system attempts to communicate with a GTPP backup storage server that is not responding. |
| Redirection Allowed | Indicates whether redirection of CDRs is allowed or not, when the primary CGF is unavailable. |
| Duplicate Hold Time Minutes | Number of minutes to hold on to CDRs that may be duplicates, when the primary CGF is down. |
| **CDR Attributes Indicator** | |
| Indicators | Indicates whether the following CDR attributes are enabled or not:<br>• PDP Type<br>• PDP Address<br>• Dynamic Flag<br>• Diagnostics<br>• Node ID<br>• Charging Characteristic Selection Mode<br>• Local Record Sequence Number<br>• MSISDN<br>• PLMN ID<br>• PGW PLMN ID<br>• IMEI<br>• RAT<br>• User Location Information<br>• List of Service Data<br>• Served MNAI<br>• Start Time<br>• Stop Time<br>• PDN Connection ID<br>• Served PDP PDN Address Extension<br>• Duration |

*Table 26-15 GTPP Characteristics (continued)*

| Field | Description |
|---|---|
| **CDR Triggers** | |
| **Triggers** | Indicates whether the following CDR triggers are enabled or not:<br>• Volume Limit<br>• Time Limit<br>• Tariff Time Change<br>• Serving Node Change Limit<br>• Intra SGSN Group Change<br>• Inter PLMN SGSN Change<br>• EGCDR Max LOSDV Limit<br>• QOS Change<br>• RAT Change<br>• MS Timezone Change<br>• Direct Tunnel |
| **Charging Agent** | |
| IP Address | IP address of the charging agent. |
| Port | Port of the charging agent. |
| **EGCDR Data Generation Configuration** | |
| Service Interval | The volume octet counts for the generation of the interim eG-CDRs to service data flow container in flow-based charging (FBC). |
| Service Idle Timeout | Time interval, in seconds, to close the eG-CDR, if the minimum time duration thresholds for service data flow containers are satisfied in FBC. |
| Delete Service Thresholds | Configured threshold in eG-CDR to be deleted in the service. |
| Include All LOSDVs | Indicates whether all content IDs are included in the final eG-CDR or not. |
| LOSDV Max Containers | Maximum number of List of Service Data Volume (LoSDV) containers in one eG-CDR. |
| LOTDV Max Containers | Maximum number of List of Service Data Volume (LoSDV) containers in one eG-CDR. |
| Closing Cause Unique | Indicates whether the same closing cause needs to be included for multiple final eG-CDRs or not. |
| **Local Storage** | |
| File Format | File format to store CDRs. |
| File Compression | Type of compression used on CDR files stored locally. None indicates that file compression is disabled. |
| File Rotation Time Interval | Time duration, in seconds, after which CDR file rotation happens. |
| File Rotation Volume Limit (MB) | Volume of CDR file, in MB, after which CDR file rotation happens. |

*Table 26-15 GTPP Characteristics (continued)*

| Field | Description |
|---|---|
| File Rotation CDR Count | Number of CDRs to include in a CDR file after which CDR file rotation happens. |
| Force File Rotation by Time Interval | Indicates whether file rotation is forced or not. If this is enabled, the system is forced to do a file rotation at specified interval, even if there are no CDRs generated. |
| Purge Processed Files | Indicates whether processed files must be processed or not. |
| **MBMS CDR Triggers** | |
| Interval | Specifies the normal time duration that must elapse before closing an accounting record provided that any or all of the following conditions are satisfied:<br>• Down link traffic volume is reached within the time interval<br>• Tariff time based trigger occurred within the time interval<br>• Data volume (uplink and downlink) bucket trigger occurred within the time interval |
| Buckets | Total number of data buckets configured for MBMS CDR trigger service. |
| **Storage Server** | |
| IP Address | IP address of the backup storage server. |
| Port | UDP port number over which the GGSN communicates with the backup storage server. |
| Timeout | Maximum amount of time, in seconds, the system waits for a response from the GTPP backup storage server before assuming the packet is lost. |
| Max Retries | Number of times the system attempts to communicate with a GTPP backup storage server that is not responding. |

## GTPP Commands

The following commands can be launched from the inventory by right-clicking a GTPP and choosing **Commands > Configuration** or **Commands > Show.** Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

*Table 26-16 GTPP Commands*

| Command | Navigation | Description |
|---|---|---|
| **Create CGF** | *Right-click on a GTPP group* > **Commands > Configuration** | The Charging Gateway Function (CGF) listens to GTP' messages sent from the GSNs on TCP/UDP port 3386. The core network sends charging information to the CGF, typically including PDP context activation times and the quantity of data which the end user has transferred. However, this communication which occurs within one network is less standardized and may, depending on the vendor and configuration options, use proprietary encoding or even an entirely proprietary system.<br>Use this command to create a new CGF. |
| **Create Storage Server** | | The GTPP Storage Server (GSS) provides an external management solution for the bulk storage of Charging Data Records (CDRs) coming from a GPRS Support Node (GSN) in a GPRS/UMTS network.<br>Use this command to create a storage server. |
| **Modify Storage Server** | *Right-click on a GTPP group* > **Storage Server** | Use this command to modify storage server configuration details. |
| **Delete Storage Server** | | Use this command to delete a storage server. |
| **Delete CGF** | *Right-click on a GTPP group* > **Commands > Configuration** | Use this command to delete a CGF. |
| **Delete GTPP** | | Use this command to delete a GTPP. |
| **Modify CGF** | | Use this command to modify CGF configuration details. |
| **Modify GTPP** | | Use this command to modify GTPP configuration details. |
| **Show CGF** | *Right-click on a GTPP group* > **Commands > Show** | Use this command to view and confirm CGF configuration details. |

# Working with EGTP

Evolved GPRS Tunneling Protocol (EGTP) formulates the primary bearer plane protocol within an LTE / EPC architecture. It provides support for tunnel management including handover procedures within and across LTE networks.

This topic contains the following sections:

- Viewing EGTP Properties, page 26-30
- EGTP Commands, page 26-31


## Viewing EGTP Properties

Prime Network Vision displays the EGTPs in an EGTP container under the Mobile node in the logical inventory. The icon used for representing EGTPs in the logical inventory is explained in Logical Inventory Icons, page A-6.

To view EGTP 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** > *EGTP Container*.

Prime Network Vision displays the list of EGTPs configured under the container. You can view the individual EGTP details from the table on the right pane or by choosing **Logical Inventory** >*Context* > **Mobile** > *EGTP Container* > *EGTP*.

Table 26-17 describes the details available for each EGTP.

***Table 26-17 EGTP Properties in Logical Inventory***

| Field | Description |
|---|---|
| Service Name | Name of the EGTP service. |
| Status | Status of the EGTP service. |
| Message Validation Mode | Mode of message validation for the EGTP service. |
| Interface Type | Interface type for the EGTP service. |
| Restart Counter | Restart counter value for the EGTP service. |
| GTPC Retransmission Timeout | Control packet retransmission timeout for the EGTP service. |
| GTPC Max Request Retransmissions | Maximum number of request retransmissions for the EGTP service. |
| GTPC IP QoS DSCP Value | The IP QoS DSCP value for the EGTP service. |
| GTPC Echo | Indicates whether GTPC echo is configured for the EGTP service or not. |
| GTPC Echo Interval | GTPC echo interval for the EGTP service. |
| GTPC Echo Mode | GTPC echo mode, which could be Dynamic or Default. |
| GTPC Smooth Factor | Smooth factor used in the dynamic echo timer for the EGTP service. |

## EGTP Commands

The following commands can be launched from the inventory by right-clicking an EGTP and choosing **Commands > Configuration.** Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

*Table 26-18 EGTP Commands*

| Command | Navigation | Description |
|---|---|---|
| **Modify EGTP** | *Right-click on a EGTP group* > **Commands > Configuration** | Use this command to modify EGTP configuration details. |
| **Delete EGTP** | | Use this command to delete the EGTP. |

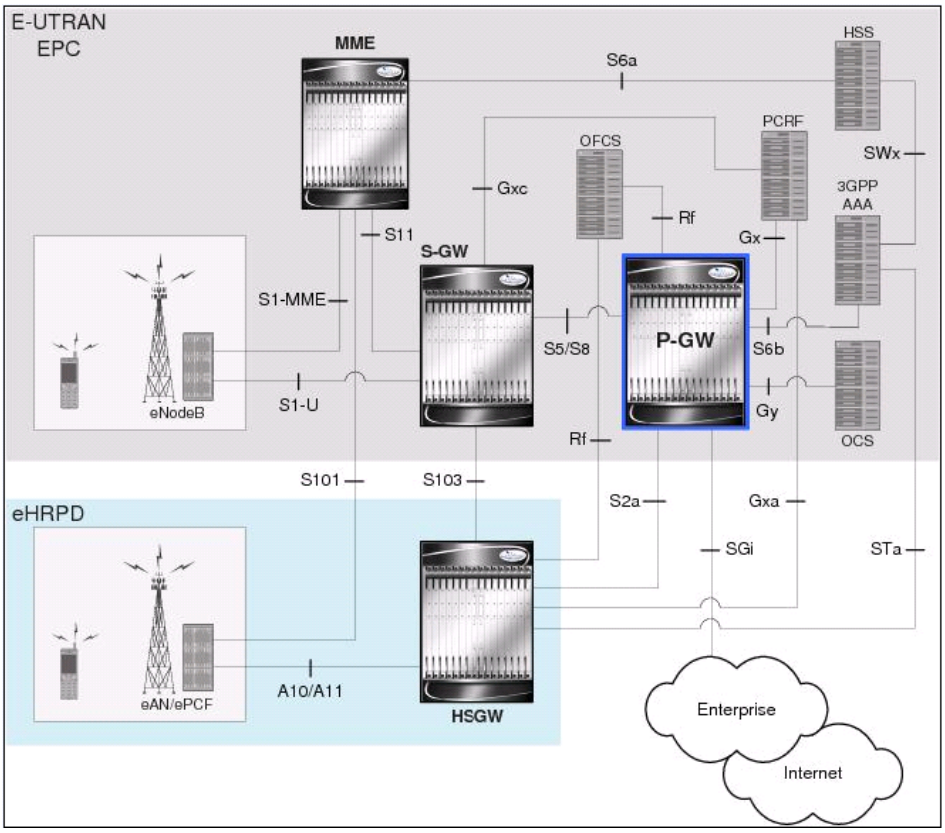
# LTE Networks - An Overview

Long Term Evolution (LTE) is the latest step in moving forward from the cellular 3G services, such as GSM to UMTS to HSPA to LTE or CDMA to LTE. LTE is based on standards developed by the Third Generation Partnership Project (3GPP). LTE may also be referred more formally as Evolved UMTS Terrestrial Radio Access Network (E-UTRAN). Following are the main objectives of an LTE network.

- Increased downlink and uplink peak data rates
- Scalable bandwidth
- Improved spectral efficiency
- All IP network

Figure 26-3 provides the topology of a basic LTE network.

*Figure 26-3 Basic LTE Network Topology*




# Working with LTE Network Technologies

The E-UTRAN uses a simplified single node architecture consisting of the eNodeBs (E-UTRAN Node B). The eNB communicates with the Evolved Packet Core (EPC) using the S1 interface, specifically with the Mobility Management Entity (MME) and Serving Gateway (S-GW) using S1-U interface. The PDN Gateway (P-GW0 provides connectivity to the external packet data networks.

Following sections provide more details on these services and their support in Prime Network:

- Monitoring SAE-GW, page 26-33
- Working with PDN-Gateway, page 26-34
- Working with Serving Gateway, page 26-36
- Viewing QCI-QoS Mapping, page 26-38
- Viewing the Layer 2 Tunnel Access Concentrator Configurations, page 26-39
- Monitoring the HRPD Serving Gateway, page 26-44
- Viewing the HSGW Configuration, page 26-46
- Monitoring Home Agent (HA), page 26-59
- Monitoring the Foreign Agent, page 26-65
- Monitoring Evolved Packet Data Gateway (ePDG), page 26-77
- Monitoring Packet Data Serving Node, page 26-87

- Viewing the Local Mobility Anchor Configuration, page 26-103

# Monitoring SAE-GW

Systems Architecture Evolution (SAE) has a flat all-IP architecture with separation of control plane and user plane traffic. The main component of SAE architecture is the Evolved Packet Core (EPC), also known as SAE Core. The EPC serves as an equivalent to GPRS networks by using its subcomponents Mobility Management Entities (MMEs), Serving Gateway (S-GW), and PDN Gateway (P-GW).

#### Mobility Management Entity (MME)

MME is the key control node for a Long Term Evolution (LTE) access network. It is responsible for idle mode User Equipment (UE) tracking and paging procedure including retransmissions. It is involved in the bearer activation/deactivation process and is also responsible for choosing the S-GW for a UE at the initial attach and at time of intra-LTE handover involving Core Network (CN) node relocation. The MME also provides the control plane function for mobility between LTE and 2G/3G access networks with the S3 interface terminating at the MME from the SGSN.

#### Serving Gateway (S-GW)

The S-GW routes and forwards user data packets, while also acting as the mobility anchor for the user plane during inter-eNodeB handovers and as the anchor for mobility between LTE and other 3GPP technologies. For idle state UEs, the S-GW terminates the downlink data path and triggers paging when downlink data arrives for the UE. It manages and stores UE contexts, such as parameters of the IP bearer service, network internal routing information, and so on. It also performs replication of the user traffic in case of lawful interception.

For more information, see Working with Serving Gateway, page 26-36.

#### PDN Gateway (P-GW)

The P-GW provides connectivity from the UE to external packet data networks by being the point of exit and entry of traffic for the UE. A UE may have simultaneous connectivity with more than one P-GW for accessing multiple PDNs. The P-GW performs policy enforcement, packet filtering for each user, charging support, lawful interception, and packet screening. Another key role of the P-GW is to act as the anchor for mobility between 3GPP and non-3GPP technologies such as WiMAX and 3GPP2.

For more information, see Working with PDN-Gateway, page 26-34.

Running S-GW and P-GW services together as a SAE-GW provides the following benefits:

- Higher capacity—For a UE with one PDN connection that is passing through standalone S-GW and P-GW services consumes 2 license units because both S-GW and P-GW services account for it separately. SAE-GW as a single node consumes only one license unit for the same, thus increasing the capacity.
- Cohesive configuration—Configuration and management of SAE-GW as a node is simpler to follow and logical to explain.

See Viewing SAE-GW Properties, page 26-33 for details on how to view SAE-GW properties in Prime Network Vision.

## Viewing SAE-GW Properties

Prime Network Vision displays the SAE-GWs in a SAE-GW container under the Mobile node in the logical inventory. The icon used for representing SAE-GW in the logical inventory is explained in Logical Inventory Icons, page A-6.

To view SAE-GW 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 >** *SAE-GW Container*.

Prime Network Vision displays the list of SAE-GW services configured under the container. You can view the individual SAE-GW service details from the table on the right pane or by choosing **Logical Inventory >** *Context* **> Mobile >** *SAE-GW* Container **>** *SAE-GW*.

Table 26-19 describes the details available for each SAE-GW.

***Table 26-19 SAE-GW Properties in Logical Inventory***

| Field | Description |
|---|---|
| Service Name | Name of the SAE-GW service. |
| Service ID | ID of the SAE-GW service. |
| Status | Status of the SAE-GW service. |
| P-GW Service | The P-GW service associated with the SAE-GW. |
| S-GW Service | The S-GW service associated with the SAE-GW. |
| New Call Policy | Specifies if the new call related behavior of SAE-GW service is enabled or disabled, when duplicate sessions with same IP address request is received. |

# Working with PDN-Gateway

PDN Gateway (P-GW) is the node that terminates the SGi interface towards the PDN. If a user equipment (UE) is accessing multiple PDNs, there may be more than one P-GW for that UE. The P-GW provides connectivity to the UE to external packet data networks by being the point of exit and entry of traffic for the UE. A UE may have simultaneous connectivity with more than one P-GW for accessing multiple PDNs.

The P-GW facilitates policy enforcement, packet filtering for each user, charging support, lawful interception, and packet screening. The features of P-GW include:

- Integration of multiple core network functions in a single node
- Multiple instances of P-GW can enable call localization and local breakout
- High performance across all parameters like, signaling, throughput, density, and latency
- Integrated in-line services
- Support for enhanced content charging, content filtering with blacklisting, dynamic network-based traffic optimization, application detection and optimization, stateful firewall, NAT translation, and lawful intercept
- High-availability helps to ensure subscriber satisfaction

The following topics explain how to work with P-GW in Prime Network Vision:

- Viewing P-GW Properties, page 26-35
- P-GW Commands, page 26-35

## Viewing P-GW Properties

Prime Network Vision displays the P-GWs in a P-GW container under the Mobile node in the logical inventory. The icon used for representing P-GW in the logical inventory is explained in Logical Inventory Icons, page A-6.

To view P-GW 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 >** *P-GW Container*.

Prime Network Vision displays the list of P-GW services configured under the container. You can view the individual P-GW service details from the table on the right pane or by choosing **Logical Inventory >***Context* **> Mobile >** *P-GW* Container **>** *P-GW*.

Table 26-20 describes the details available for each P-GW.

***Table 26-20 P-GW Properties in Logical Inventory***

| Field | Description |
|---|---|
| Service Name | Name of the P-GW service. |
| Service Status | Status of the P-GW service. |
| EGTP Service | Evolved GPRS Tunneling Protocol (EGTP) service associated with the P-GW. EGTP provides tunneling support for the P-GW. |
| GGSN Service | GGSN service associated with the P-GW. |
| LMA Service | Local Mobility Anchor (LMA) that facilitates proxy mobile IP on the P-GW. |
| QCI QoS Mapping Table Name | Table name of QoS class indices that enfore QoS parameters. |
| New Call Policy | Specifies if the new call related behavior of P-GW service is enabled or disabled, when duplicate sessions with same IP address request is received. |
| Session Delete Delay Timeout | Duration, in seconds, to retain a session before terminating it. |
| SAE-GW Service | Systems Architecture Evolution (SAE) gateway service associated with the P-GW. |

**Step 3** If the P-GW is associated with PLMNs, you can view the details of the PLMNs on clicking the specified P-GW.

## P-GW Commands

The following commands can be launched from the inventory by right-clicking a P-GW and choosing **Commands > Configuration.** Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

*Table 26-21 P-GW Commands*

| Command | Navigation | Description |
|---|---|---|
| **Create P-GW PLMN** | *Right-click on a P-GW service* > **Commands** > **Configuration** | Use this command to create a PLMN for P-GW. |
| **Delete P-GW** | | Use this command to delete a P-GW. |
| **Modify P-GW** | | Use this command to modify the configuration details for a P-GW. |

# Working with Serving Gateway

In a Long Term Evolution (LTE) / Systems Architecture Evolution (SAE) network, a Serving Gateway (S-GW) acts as a demarcation point between the Radio Access Network (RAN) and core network, and manages user plane mobility. It serves as the mobility anchor when terminals move across areas served by different eNode-B elements in Evolved UMTS Terrestrial Radio Access Network (E-UTRAN), as well as across other 3GPP radio networks such as GSM EDGE Radio Access Network(GERAN) and UTRAN. S-GW buffers downlink packets and initiates network-triggered service request procedures. Other functions include lawful interception, packet routing and forwarding, transport level packet marking in the uplink and the downlink, accounting support for per user, and inter-operator charging. The S-GW routes and forwards user data packets, while also acting as the mobility anchor for the user plane during inter-eNode-B handovers and as the anchor for mobility between LTE and other 3GPP technologies.

For idle state user equipment (UE), the S-GW terminates the downlink data path and triggers paging when downlink data arrives for the UE. It manages and stores UE contexts, such as parameters of the IP bearer service, network internal routing information, and so on. It also performs replication of the user traffic in case of lawful interception.

The following topics provide details on how to work with S-GWs in Prime Network Vision:

- Viewing S-GW Properties, page 26-36
- S-GW Commands, page 26-37

## Viewing S-GW Properties

Prime Network Vision displays the S-GWs in a S-GW container under the Mobile node in the logical inventory. The icon used for representing S-GW in the logical inventory is explained in Logical Inventory Icons, page A-6.

To view S-GW 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 >** *S-GW Container.*

Prime Network Vision displays the list of S-GW services configured under the container. You can view the individual S-GW service details from the table on the right pane or by choosing **Logical Inventory >***Context* **> Mobile >** *S-GW* Container **>** *S-GW.*

Table 26-22 describes the details available for each S-GW.

***Table 26-22 S-GW Properties in Logical Inventory***

| Field | Description |
|---|---|
| Service Name | Name of the S-GW service. |
| Service Status | Status of the S-GW service. |
| Accounting Context | Name of the context configured on the system that processes accounting for service requests handled by the S-GW service. |
| Accounting GTPP Group | Name of the accounting GTPP group associated with the S-GW service. This will hold the configured GTPP server group (for GTPP servers redundancy) on a S-GW service for CGF accounting functionality. |
| Accounting Mode | Accounting protocol, which could be GTPP or Radius-Diameter. |
| Egress Protocol | Egress protocol used for the S-GW service, which could be GTP, GTP-PMIP, or PMIP. |
| Ingress EGTP Service | Ingress EGTP service associated with the S-GW. EGTP provides tunneling support for the S-GW. |
| Egress Context | Context used for S-GW service egress. |
| Egress ETGP Service | Ingress EGTP service associated with the S-GW. EGTP provides tunneling support for the S-GW. |
| Egress Mag Service | Mobile Access Gateway (MAG) egress service through calls are routed to the S-GW. |
| IMS Authorization Service | IMS authorization service associated with the S-GW. |
| Accounting Policy | Accounting policy configured for the S-GW. |
| New Call Policy | Specifies if the new call related behavior of S-GW service is enabled or disabled, when duplicate sessions with same IP address request is received. |
| QCI QoS Mapping Table | Table name of QoS class indices that enfore QoS parameters. |
| SAE GW Service | Systems Architecture Evolution (SAE) gateway service associated with the S-GW. |

**Step 3** If the S-GW is associated with PLMNs, you can view the PLMN entries on clicking the specified S-GW.

## S-GW Commands

The following commands can be launched from the inventory by right-clicking an S-W and choosing **Commands > Configuration.** Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

*Table 26-23 S-GW Commands*

| Command | Navigation | Description |
|---|---|---|
| **Create S-GW PLMN** | *Right-click on a S-GW service* > **Commands** > **Configuration** | Use this command to create a PLMN for S-GW. |
| **Delete S-GW** | | Use this command to delete a S-GW. |
| **Modify S-GW** | | Use this command to modify the configuration details for a S-GW. |

# Viewing QCI-QoS Mapping

The QoS Class Index (QCI) to QoS mapping configuration mode is used to map Dices to enforceable QoS parameters. Mapping can occur between the RAN and the S-GW, the MME, and/or the P-GW in an LTE network or between the RAN and the harped Serving Gateway (HSGW) in an eHRPD network. This is a global configuration. These maps can be imported by P-gateway and S-gateway to enforce these parameters on upstream/downstream traffic.

Prime Network Vision displays the QCI-QoS mapping information under the Mobile node in the logical inventory. See Figure 26-18.

**Note** QCI-QoS mapping is applicable only for the ‘local’ context in the logical inventory.

To view QCI-QoS mapping:

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

**Step 2** In the logical inventory window, choose **Logical Inventory > *local* > Mobile > QCI-QoS Mapping**.

Prime Network Vision displays the list of QCI-QoS mapping records configured under the container. You can view the individual record from the table on the right pane or by choosing **Logical Inventory >***Context* **> Mobile > QCI-QoS Mapping >** *Mapping Name.*

Table 26-24 describes the QCI-QoS mapping details.

*Table 26-24 QCI-QoS Mapping*

| Field | Description |
|---|---|
| Mapping Name | Name of the QCI-QoS mapping record. |
| **QCI-QoS Mapping Table** | |
| QCI Number | QCI number. |
| QCI Type | QCI type. |
| Uplink | DSCP marking to be used for encapsulation and UDP for uplink traffic |
| Downlink | DSCP marking to be used for encapsulation and UDP for downlink traffic |
| Max Packet Delay | Maximum packet delay, in milliseconds, that can be applied to the data. |
| Max Error Rate | Maximum error loss rate of non congestion related packet loss. |
| Delay Class | Packet delay. |
| Precedence Class | Indicates packet precedence. |
| Reliability Class | Indicates packet reliability. |
| Traffic Policing Interval | Traffic policing interval. |

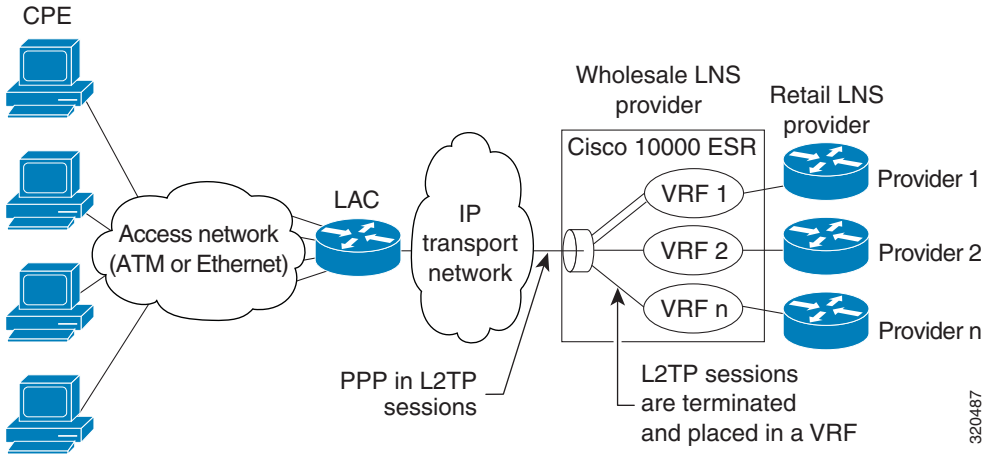
# Viewing the Layer 2 Tunnel Access Concentrator Configurations

In computer networking, Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself; it relies on an encryption protocol that it passes within the tunnel to provide privacy. The entire L2TP packet, including payload and L2TP header, is sent within a User Datagram Protocol (UDP) datagram. It is common to carry Point-to-Point Protocol (PPP) sessions within an L2TP tunnel.

The two endpoints of an L2TP tunnel are called the LAC (L2TP Access Concentrator) and the LNS (L2TP Network Server). The LAC is the initiator of the tunnel while the LNS is the server, which waits for new tunnels. Once a tunnel is established, the network traffic between the peers is bidirectional.

LAC allows users and telecommuters to connect to their corporate intranets or extranets using L2TP. In other words, it forwards packets to and from the LNS and a remote system. It connects to the LNS using a local area network or wide area network and directs subscriber sessions into L2TP tunnels based on the domain of each session. Figure 26-4 denotes the LAC architecture.

*Figure 26-4 LAC Architecture*




The packets that are exchanged within an L2TP tunnel can be categorized as control packets and data packets.

To view the LAC configuration details:

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

**Step 2** In the logical inventory window, choose **Logical Inventory >** *Context* **> LAC.** The list of LAC services configured in Prime Network is displayed in the content pane.

**Step 3** From the **LAC** node, choose an LAC service. The LAC service details are displayed in the content pane as shown in Figure 26-5.

*Figure 26-5 LAC Service Details*

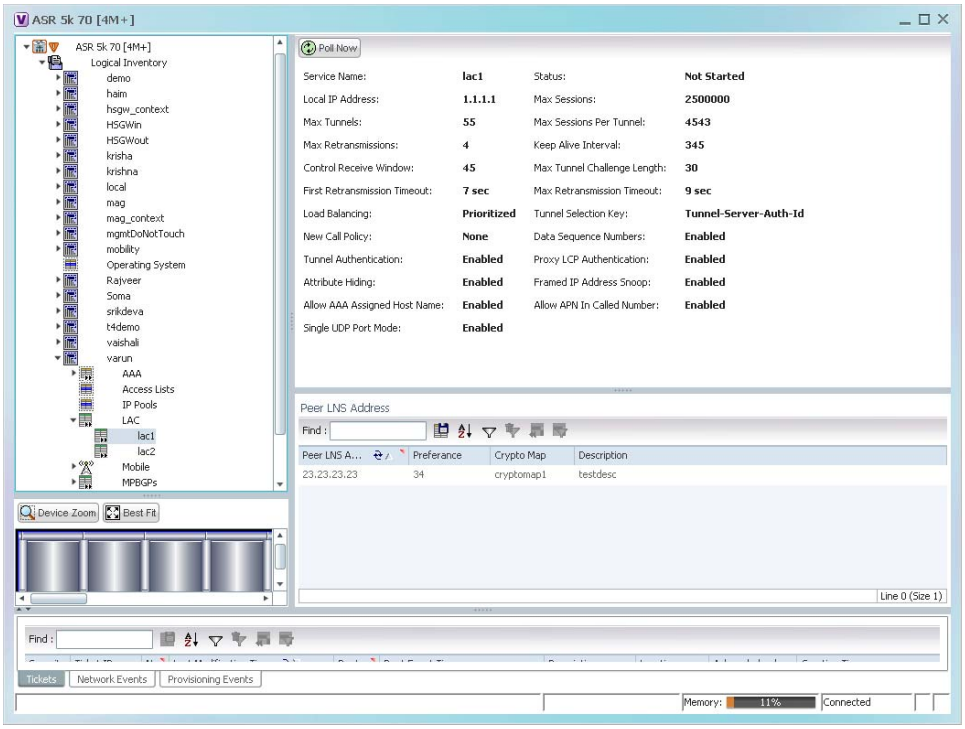



Table 26-25 displays the LAC configuration details.

*Table 26-25 LAC Configuration Details*

| Field | Description |
|---|---|
| Service Name | The unique identification string for the LAC service. |
| Status | The status of the LAC service, which can be any one of the following:<br>• Initiated<br>• Running<br>• Down<br>• Started<br>• Nonstarted<br>• Unknown |
| Local IP Address | The local IP address bound with the LAC service. |
| Max Sessions | The maximum number of subscribers connected to this service at any time, which can be any value between 1 and 2500000. This field defaults to 2500000. |

*Table 26-25 LAC Configuration Details*

| Field | Description |
|---|---|
| Max Tunnels | The maximum length (in bytes) of the tunnel challenge.<br>**Note** The tunnel challenge is basically used to authenticate tunnels at the time of creation. |
| Max Sessions Per Tunnel | The maximum number of sessions that can be handled by a single tunnel at one point of time, which can be any value between 1 and 65535. This field defaults to 512. |
| Max Retransmissions | The maximum number of times a control message is retransmitted to a peer, before clearing the tunnel and its sessions. |
| Keep Alive Interval | The amount of time after which a keep alive message is sent. |
| Control Receive Window | The number of control messages the remote peer LNS can send before an acknowledgement is received. |
| Max Tunnel Challenge Length | The maximum length (in bytes) of the tunnel challenge. |
| First Retransmission Timeout | The initial timeout before retransmitting a control message.<br>**Note** Each tunnel maintains a queue of control messages that must be transmitted to its peer. If an acknowledgement is not received after the specified period, then the control message is retransmitted. |
| Max Retransmission Timeout | The maximum amount of time between two retransmitted messages. |
| Load Balancing | The type of load balancing to select LNS for the LAC service, which can be any one of the following:<br>• Balanced<br>• Prioritized<br>• Random |
| Tunnel Selection Key | The selection key to create tunnels between the L2TP service and the LNS server, based on the value of the \u2015Tunnel-Server-Auth-ID\u2016 attribute received from the AAA server. |
| New Call Policy | The new call policy for busy-out conditions, which can be any one of the following:<br>• None<br>• Accept<br>• Reject |
| Data Sequence Numbers | Indicates whether data sequence numbering for sessions that use the current LAC service is enabled. This option is enabled by default. |

*Table 26-25 LAC Configuration Details*

| Field | Description |
|---|---|
| Tunnel Authentication | Indicates whether tunnel authentication is enabled.<br><br>**Note** If this option is enabled, a configured shared secret is used to ensure that the LAC service is communicating with an authorized peer LNS. The shared secret is configured by the command in the LAC service configuration mode, the command in the subscriber configuration mode, or the Tunnel-Password attribute in the subscribers RADIUS profile. |
| Proxy LCP Authentication | Indicates whether the option to send proxy LCP authentication parameters to the LNS is enabled. |
| Attribute Hiding | Indicates whether certain attributes in control messages sent from the LAC to the LNS is hidden.<br><br>**Note** The LAC hides these attributes only if the tunnel authentication option is enabled between the LAC and LNS. |
| Framed IP Address Snoop | Indicates whether the LAC can detect IPCP packets exchanged between the mobile node and the LNS and extract the framed-I-address assigned to the mobile node.<br><br>**Note** The address that is extracted is reported in the accounting start/stop messages and will be displayed for each subscriber session. |
| Allow AAA Assigned Host Name | Indicates whether the Tunnel-Client-Auth ID assigned by AAA is used as the Host name AVP in the L2TP tunnel setup message.<br><br>**Note** If the tunnel parameters are not received from the RADIUS server, then the parameters configured in APN are considered for LNS peer selection. When the parameters in APN are considered, the local-hostname configured with the APN command for the LNS peer is used as the LAC Host name. |
| Allow APN in Called Number | Indicates whether the APN name in Called number AVP is sent as part of the Incoming-Call Request (ICRQ) message sent to the LNS. If this keyword is not configured, then the Called number AVP will not be included in the ICRQ message sent to the LNS> |
| Single UDP Port Mode | Indicates whether the standard L2TP port 1701 is used as a source port for all L2TP control and data packets that originate from the LAC node. |
| **Peer LNS Address** | |
| Peer LNS Address | The IP address of the peer LNS for the current LAC service, which is usually in standard IPv4 dotted decimal notation. |
| Preference | The priority of the peer LNS, which can be any number between 1 and 128. This priority is used when multiple peer LNS are configured. |

*Table 26-25 LAC Configuration Details*

| Field | Description |
|---|---|
| Crypto Map | The name of crypto map that is configured for the selected context. |
| Description | The description of the specified peer LNS. |

# Monitoring the HRPD Serving Gateway

The HRPD Serving Gateway (HSGW) is a component in the evolved High Rate Packet Data (eHRPD) mobile network. It is an evolution option for CDMA operators that helps ensure converged mobility and management between HRPD and LTE networks.

The HSGW terminates the eHRPD access network interface from the Evolved Access Network (eAN) or Evolved Packet Core Function (ePCF) and routes UE-originated or terminated packet data traffic. It provides interworking with the eAN/ePCF and the PDN Gateway (P-GW) within the Evolved Packet Core (EPC) or LTE/SAE core network.

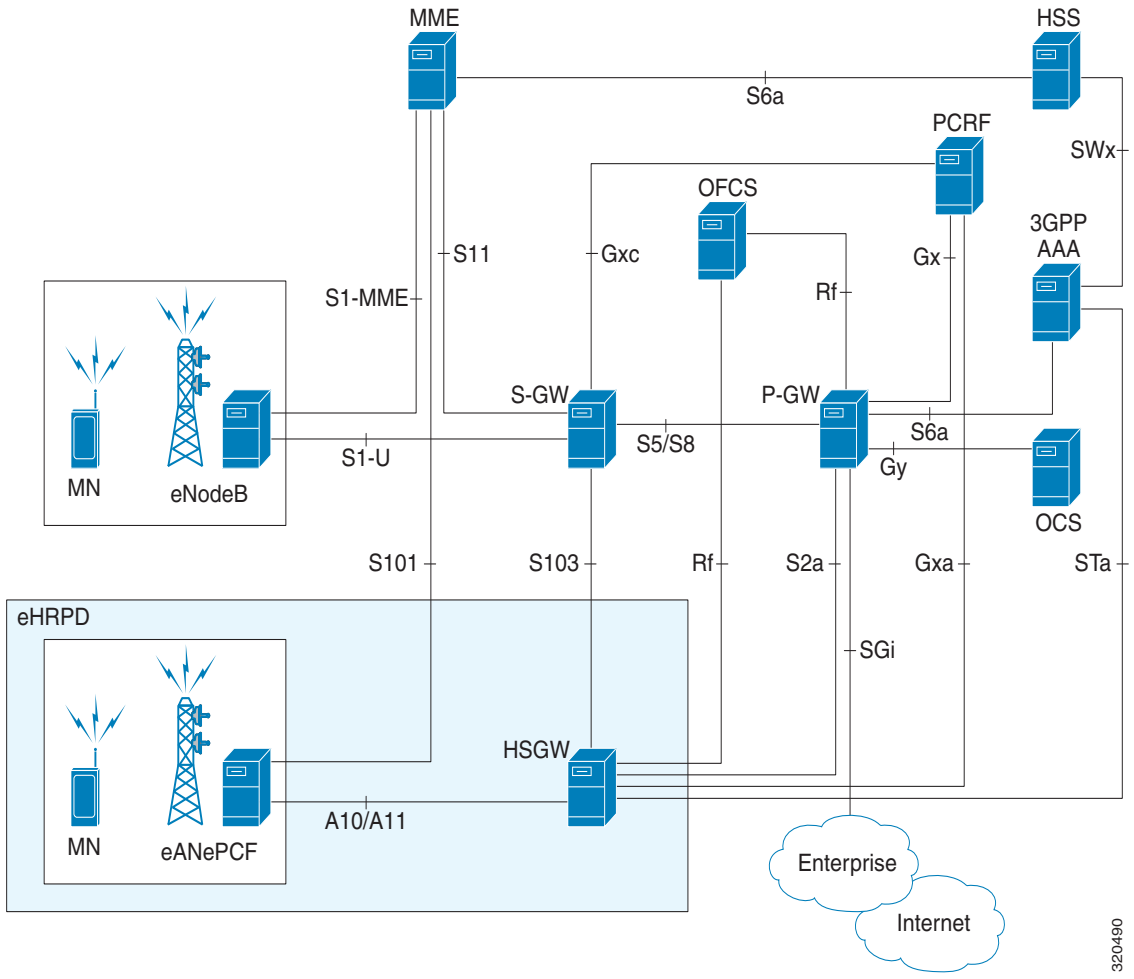
HSGW performs the following functions:

- Mobility anchoring for inter-eAN handoffs
- Transport level packet marking in the uplink and the downlink. For example, setting the DiffServ Code Point, based on the QCI of the associated EPS bearer
- Uplink and downlink charging per UE, PDN, and QCI
- Downlink bearer binding based on policy information
- Uplink bearer binding verification with packet dropping of UL traffic that does not comply with established uplink policy
- MAG functions for S2a mobility (i.e., Network-based mobility based on PMIPv6)
- Support for IPv4 and IPv6 address assignment
- EAP Authenticator function
- Policy enforcement functions defined for the Gxa interface
- Robust Header Compression (RoHC)
- Support for VSNCP and VSNP with UE
- Support for packet-based or HDLC-like framing on auxiliary connections
- IPv6 SLACC, generating RAs responding to RSs

An HSGW also establishes, maintains and terminates link layer sessions to UEs. The HSGW functionality provides interworking of the UE with the 3GPP EPS architecture and protocols. This includes support for mobility, policy control and charging (PCC), access authentication, and roaming. The HSGW also manages inter-HSGW handoffs.

The topology of the HSGW network is shown in the following figure:

*Figure 26-6 HSGW Topology*




## Basic Features of HSGW

The basic features supported by HSGW can be categorized as follows:

- Authentication
- IP Address Allocation
- Quality of Service
- AAA, Policy and Charging

The **Authentication** features supported by HSGW are:

- EAP over PPP
- UE and HSGW negotiates EAP as the authentication protocol during LCP
- HSGW is the EAP authenticator
- EAP-AKA' (trusted non-3GPP access procedure) as specified in TS 33.402
- EAP is performed between UE and 3GPP AAA over PPP/STa

The **IP Address Allocation** features supported by HSGW are:

- Support for IPv4 and IPv6 addressing
- Types of PDNs - IPv4, IPv6 or IPv4v6
- IPv6 addressing
  - Interface Identifier assigned during initial attach and used by UE to generate it's link local address
  - HSGW sends the assigned /64 bit prefix in RA to the UE
  - Configure the 128-bits IPv6 address using IPv6 SLAAC (RFC 4862)
  - Optional IPv6 parameter configuration via stateless DHCPv6(Not supported)
- IPv4 address
  - IPv4 address allocation during attach
  - Deferred address allocation using DHCPv4(Not supported)
  - Option IPv4 parameter configuration via stateless DHCPv4(Not supported)

The **Quality of Service** features supported by HSGW include:

- HRPD Profile ID to QCI Mapping
- DSCP Marking
- UE Initiated Dedicated Bearer Resource Establishment
- QCI to DSCP Mapping

The **AAA, Policy and Charging** features supported by HSGW include:

- EAP Authentication (STa)
- Rf Diameter Accounting
- AAA Server Groups
- Dynamic Policy and Charging: Gxa Reference Interface
- Intelligent Traffic Control

## Viewing the HSGW Configuration

To view the HSGW configuration:

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

**Step 2** In the logical inventory window, choose **Logical Inventory >** *Context* **> Mobile > HSGW**. The list of HSGW services configured in Prime Network are displayed in the content pane.

**Step 3** From the **HSGW** node, choose a HSGW service. The HSGW service details are displayed in the content pane as shown in Figure 26-7.

*Figure 26-7 HSGW Service Details*

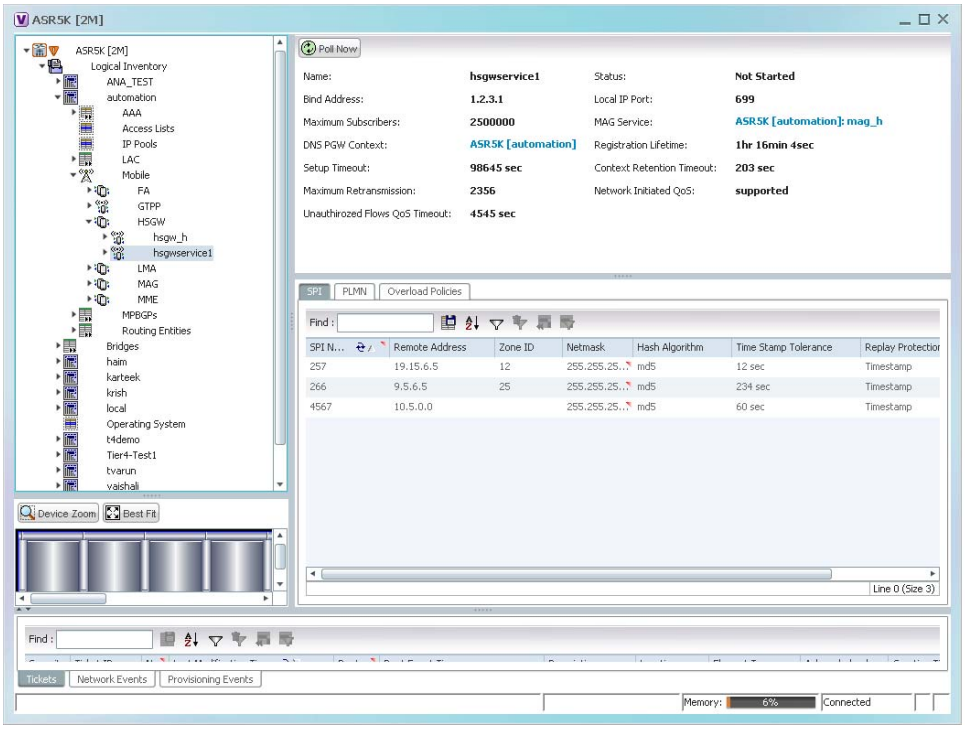



Table 26-26 displays the HSGW service details.

*Table 26-26 HSGW Service details*

| Field | Description |
|---|---|
| Name | The name of the HSGW service. |
| Status | The status of the service, which can be any one of the following:<br>• Started<br>• Not Started<br>This field defaults to **Not Started**. |
| Bind Address | The IPv4 address to which the service is bound to. This field defaults to Null if binding is not done. |
| Local IP Port | The User Datagram Protocol (UDG) port for the R-P interface of the IP socket. |
| Maximum Subscribers | The maximum number of subscriber sessions that the service can support. |
| MAG Service | The Mobile Access Gateway (MAG) service associated with the HSGW service. Clicking this link will take you to the relevant MAG service under the MAG node. |
| DNS PGW Context | The location of the Domain Name System (DNS) client, which is used to identify the Fully Qualified Domain Name (FQDN) for the peer P-GW. |
| Registration Lifetime | The registration lifetime that is configured for all the subscribers. |
| Setup Timeout | The maximum amount of time (in seconds) allowed for session setup. |
| Context Retention Timeout | The maximum number of time (in seconds) that the UE session context is maintained by the HSGW service before it is torn down.<br>**Note** The UE session context includes the Link Control Protocol (LCP), authentication and the A10 session context for a given UE. |
| Maximum Retransmission | The maximum number of times the HSGW service will try to communicate with the eAN or PCF before it declares it as unreachable. |
| Network Initiated QoS | Indicates whether the Network Initiated QoS feature is supported by the HSGW service. |
| Unauthorized Flow QoS Timeout | The amount of time (in seconds) the service must wait before a QoS update is triggered to downgrade an unauthorized flow. |
| **SPI tab** | |
| SPI Number | The unique Security Parameter Index (SPI) number, which indicates a security context between the services. |
| Remote Address | The IP address of the source service, which can be an IPv4 dotted decimal notation or IPv6 colon separated notation. |
| Zone ID | The PCF zone id that must be configured for the HSGW service. |
| Netmask | The subnet mask of the service. |
| Hash Algorithm | The hash algorithm used between the source and destination services. |
| Time Stamp Tolerance | The difference (tolerance) in timestamps that is acceptable. If the actual difference in the timestamps exceeds this difference, then the session is rejected. |

*Table 26-26 HSGW Service details*

| Field | Description |
|---|---|
| Replay Protection | The replay-protection scheme that must be implemented by the service. |
| Description | The description of the SPI. |
| **PLMN tab** | |
| PLMN ID | The unique id of the Public Land Mobile Network (PLMN), which is used to determine if a mobile station is visiting, roaming, or belongs to the network. |
| Primary | Indicates whether the PLMN Id must be used as the default and primary ID. |
| **Overload Policies tab** | |
| IP Address | The IP address of an alternate PDSN, which is in the IPv4 dotted decimal notation. |
| Weight | The weightage of the IP address, which determines the order in which the IP address is used in case of multiple IP addresses. |

You can also view the following configuration details for a HSGW service:

- A10/A11 Properties—The A10/A11 interface (also known as R-P interface for RAN-to-PDSN) supports the A10 protocol for user data transport between the PCF and PDSN, and the A11 protocol for the associated signaling. A11 signaling messages are also used for passing accounting related and other information from the PCF to the PDSN. The A10/A11 interfaces support mobility between PCFs under the same PDSN.
- GRE Parameters—Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco Systems that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol internetwork.
- IP Source Violation—IP source violations occur when the PDSN receives packets from a subscriber where the source address is not the same as the address given to the subscriber, and hence get discarded.

## Viewing the A10/A11 Configuration Details

To view the A10/A11 configuration details:

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

**Step 2** In the logical inventory window, choose **Logical Inventory >** *Context* **> Mobile > HSGW >** *HSGW service* **> A10/A11 Properties**. The configuration details are displayed in the content pane.

Table 26-27 displays the A10/A11 configuration details.

*Table 26-27 A10 A11 Configuration Details*

| Field | Description |
|---|---|
| Overload Policy | The method used by the HSGW service to handle overload conditions, which can be any one of the following:<br>• Reject<br>• Redirect |
| New Call Policy | The new call policy configured for the HSGW service, which can be any one of the following:<br>• None<br>• Reject<br>• Accept<br>This field defaults to **None**. |
| Data Available Indicator Enabled | Indicates whether the data available indicator in A10/A11 registration reply messages is enabled. |
| Data Over Signalling | Indicates whether the data over signaling marking feature for A10 packets is enabled. |
| Airlink Bad Sequence | The behavior for airlink related parameters configured for the HSGW service, which can be any one of the following:<br>• Accept<br>• Deny |
| Airlink Bad Sequence Deny Code | The reason for denying airlink bad sequence, which can be any one of the following:<br>• Unsupported vendor ID<br>• Poorly formed request |
| Handoff With No Connection Setup | Indicates whether the HSGW service must accept or deny handoff R-P sessions that do not have an Airlink Connection setup record in the A11 registration request. |
| RSVP Retransmission Timeout | The maximum amount of time (in seconds) in which RP control packets must be retransmitted. |
| RSVP Maximum Retransmission Count | The maximum number of times the RP control packets can be retransmitted. |

## Viewing the GRE Parameters

To view the GRE Parameters for the HSGW service:

**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 > HSGW >** *HSGW service* **> GRE Parameters**. The relevant details are displayed in the content pane.

Table 26-28 displays the GRE parameter details.

*Table 26-28 GRE Parameter Details*

| Field | Description |
|---|---|
| Checksum | Indicates whether insertion of GRE checksum in outgoing GRE data packets is enabled. |
| Checksum Verify | Indicates whether verification of GRE checksum in incoming GRE packets is enabled. |
| Reorder Timeout | The maximum amount of time (in milliseconds) to wait before reordered out-of-sequence GRE packets are processed. |
| Sequence Mode | The method to handle incoming out-of-sequence GRE packets, which can be any one of the following:<br>• Reorder<br>• None |
| Sequence Numbers | Indicates whether the option to insert or remove GRE sequence numbers in GRE packets is enabled. |
| Flow Control | Indicates whether flow control is supported by the selected HSGW service. By default, this option is disabled. |
| Flow Control Timeout | The amount of time (in milliseconds) to wait for an Transmitter On (XON) indicator from the RAN. This time can be any value between 1 and 1000000, and defaults to 10000 milliseconds. |
| Flow Control Action | The action that must be taken when the timeout limit is reached, which can be any one of the following:<br>• disconnect-session<br>• resume-session. |
| Protocol Type | The tunnel type for the GRE routing. This field defaults to **Any**. |
| Is 3GPP Extension Header QoS Marking | Indicates whether the 3GG Extension Header QoS Marking is enabled for the selected HSGW feature.<br>**Note** If this feature is enabled and the PCF negotiation feature is enabled in A11 RRQ, then the HSGW will include QoS optional data attribute in the GRE 3GPP2 Extension Header. |
| MTU | The maximum transmission unit (MTU) for packets accessing the APN. |
| IP Header DSCP | The Differential Service Code Point (DSCP) value in the IP header that marks the GRE IP Header encapsulation. This can be any value between 0x0F and 0X3F, and defaults to 0X0F. |

*Table 26-28 GRE Parameter Details*

| Field | Description |
|---|---|
| IP Header DSCP Packet Type | Indicates whether the IP Header DSCP Value packet type is specified for the packets, which can be any one of the following:<br>• all-control-packets—Indicates that DSCP marking for GRE IP header encapsulation will be applied for all control packets for the session.<br>• setup-packets-only—Indicates that DSCP marking for GRE IP header encapsulation willbe applied only for session setup packets. |
| GRE Segmentation | Indicates whether segmentation of GRE packets is enabled. By default, this option is disabled. |

### Viewing the IP Source Violation Details

To view the IP source Violation configuration details:

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

**Step 2** In the logical inventory window, choose **Logical Inventory >** *Context* **> Mobile > HSGW >** *HSGW service* **> IP Source Violation**. The configuration details are displayed in the content pane.

Table 26-29 displays the IP Source Violation configuration details.

*Table 26-29 IP Source Violation Configuration Details*

| Field | Description |
|---|---|
| Renegotiation Limit | The number of source violations that are allowed within a specified detection period, after which a PPP renegotiation is forced. |
| Drop Limit | The number of source violations that are allowed within a specified detection period, after which a call disconnect is forced. |
| Clear On Valid PDU | Indicates whether the service must reset the renegotiation limit and drop limit counters if a properly addressed packet is received. |
| Period | The amount of time (in seconds) for the source violation detection period. Once this value is reached, the drop limit and renegotiation limit counters are decremented. |

## Configuration Commands for HSGW

The HSGW commands allow you to configure HSGW services in your network. Please note that these commands are available only for Cisco ASR 5000 Mobile devices.

These commands can be launched from the logical inventory by choosing the **Context > Commands > Configuration** or **Context > Commands > Show**.

Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands.

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

**Note** In the GUI, parameters that are displayed in bold text are mandatory.

Table 26-30 lists the HSGW configuration commands.

*Table 26-30 HSGW Configuration Commands*

| Command | Navigation | Description |
|---|---|---|
| Create HSGW | *Right-click context* > **Commands** > **Configuration** | Use this command to create a new HSGW service. |
| Modify HSGW<br>Delete HSGW | Expand **HSGW** node > *right-click HSGW service* > **Commands** > **Configuration** | Use this command to modify/delete the configuration details of an HSGW service. |
| Show HSGW | Expand **HSGW** node > *right-click HSGW service* > **Commands** > **Show** | Use this command to view and confirm the configuration details of an HSGW service. |
| Create SPI | Expand **HSGW** node > *right-click HSGW service* > **Commands** > **Configuration** | Use this command to create a new Security Parameter Index (SPI) for the HSGW service. |
| Modify SPI<br>Delete SPI | Expand **HSGW** node > *HSGW service* > In content pane, click **SPI** tab > *right-click on SPI No. field* > **Commands** > **Configuration** | Use this command to modify/delete the SPI configuration details for the HSGW service. |

*Table 26-30 HSGW Configuration Commands*

| Command | Navigation | Description |
|---|---|---|
| Create PLMN entries | Expand **HSGW** node > *right-click HSGW service* > **Commands** > **Configuration** | Use this command to create a new Public Land Mobile Network (PLMN) for the HSGW service. |
| Modify PLMN entries<br>Delete PLMN entries | Expand **HSGW** node > *HSGW service* > In content pane, click **PLMN** tab > *right-click on PLMN ID field* > **Commands** > **Configuration** | Use this command to modify/delete the PLMN configuration details for the HSGW service. |
| Create Overload Policy | Expand **HSGW** node > *right-click HSGW service* > **Commands** > **Configuration** | Use this command to create a new overload policy for the HSGW service. |
| Modify Overload Policy<br>Delete Overload Policy | Expand **HSGW** node > *HSGW service* > In content pane, click **Overload Policies** tab > *right-click on IP address field* > **Commands** > **Configuration** | Use this command to modify/delete the overload policy details for the HSGW service. |
| Modify A10 A11 Interface | Expand **HSGW** node > *HSGW service* > *Right-click A10/A11 Properties* > **Commands** > **Configuration** | Use this command to modify the A10/A11 configuration details for the HSGW service. |

*Table 26-30 HSGW Configuration Commands*

| Command | Navigation | Description |
|---|---|---|
| Modify GRE | Expand **HSGW** node > *HSGW service* > *right-click GRE* > **Commands** > **Configuration** | Use this command to modify the GRE configuration details for the HSGW service. |
| Modify IP Source Violation | Expand **HSGW** node > HSGW service > *right-click IP Source Violation* > **Commands** > **Configuration** | Use this command to modify the IP source violation details for the HSGW service. |

## Viewing the MAG Configuration for HSGW

A Mobile Access Gateway (MAG) performs mobility-related signaling on behalf of the mobile nodes (MN) attached to its access links. MAG is the access router for the MN; that is, the MAG is the first-hop router in the localized mobility management infrastructure

A MAG performs the following functions:

- Obtains an IP address from a Local Mobility Anchor (LMA) and assigns it to an MN
- Retains the IP address of an MN when the MN roams across MAGs
- Tunnels traffic from an MN to LMA

To view the MAG configuration details:

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

**Step 2** In the logical inventory window, choose **Logical Inventory** > *Context* > **Mobile** > **MAG** > *MAG service*. The configuration details are displayed in the content pane.

Table 26-31 displays the configuration details for a MAG service.

*Table 26-31 MAG Service Configuration Details*

| Field | Description |
|---|---|
| Name | The unique name of the MAG service. |
| Status | The status of the MAG service, which can be any one of the following:<br>• Started<br>• Not Started<br>This field defaults to **Not Started**. |
| Bind Address | The IP address to which the MAG service is bound to. |

*Table 26-31 MAG Service Configuration Details*

| Field | Description |
|---|---|
| Maximum Subscribers | The maximum number of subscribers supported by the service. |
| PMIP Maximum Retransmission | The maximum number of times the MAG service will communicate with the LMA, before it is declared unreachable. |
| Registration Lifetime | The registration lifetime configured for all the subscribers who have subscribed to this service. |
| PMIP Retransmission Timeout | The maximum amount of time (in milliseconds) the MAG service must wait for a response from the LMA. |
| PMIP Renewal Time | Indicates the percentage of the registration lifetime when the registration renewal is sent to the LMA for subscribers using this service. |
| PMIP Retransmission Policy | The retransmission policy for PMIP control messages, which can be any one of the following:<br>• Normal<br>• Exponential backoff |
| New Call Policy | The method for handling new calls, which can be any one of the following:<br>• Accept<br>• Reject<br>This field defaults to **None**. |
| PMIPv6 Tunnel Encapsulation | The encapsulation type used for PMIPv6 tunnel data between the MAG and the LMA. |
| Information Set | The mobility options to be used in Proxy Binding Update (PBU) messages, for those messages sent between MAG and LMA. |
| Mobility Option Type | The mobility option type used in the mobility messages. |
| Signalling Packets IP Header DSCP | The Differential Services Code Point (DSCP) value in the IP Header of the signalling packets. |

## Viewing the Profile-QCI Mapping Details

You can view the configured mapping entries between a Rendezvous Point (RP) QoS Profile and the LTE QoS Class Index (QCI).

A QCI is a scalar that is used as a reference to access node-specific parameters that control bearer level packet forwarding treatment (e.g. scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, etc.), and that have been pre-configured by the operator owning the access node.

To view the Profile-QCI mapping 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 >** *local* **> Mobile > Profile** > **Profile-QCI Mapping** > *Profile-QCI Mapping*. The mapping details are displayed in the content pane.

Table 26-32 displays the Profile-QCI Mapping details.

*Table 26-32 Profile-QCI Mapping Details*

| Field | Description |
|---|---|
| Profile Name | The name of the Profile-QCI Mapping profile that is associated with the HSGW. |
| **Profile-QCI Mapping Table** | |
| QCI ID | The QCI ID to which the profile is mapped. |
| Profile ID | The profile ID to which the QCI ID is mapped. |
| Uplink GBR | The Guaranteed Bit Rate (GBR) for the uplink data flow, which can be any value between 0 and 4294967295. |
| Downlink GBR | The GBR for the downlink data flow, which can be any value between 0 and 4294967295. |
| Uplink MBR | The Maximum Bit Rate (MBR) for the uplink data flow, which can be any value between 0 and 4294967295. |
| Downlink MBR | The MBR for the downlink data flow, which can be any value between 0 and 4294967295. |
| Priority Level | The priority level of the profile for the QCI, which can be any value between 1 and 15. |
| Preemption Capability | The preemption capability of the profile. |

## Configuration Commands for MAG

The MAG commands allow you to configure MAG services in your network. Please note that these commands are available only for Cisco ASR 5000 Mobile devices.

These commands can be launched from the logical inventory by choosing the **Context > Commands > Configuration** or **Context > Commands > Show**.

Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands.

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

**Note** In the GUI, parameters that are displayed in bold text are mandatory.

Table 26-33 lists the MAG configuration commands.

*Table 26-33 MAG Configuration Commands*

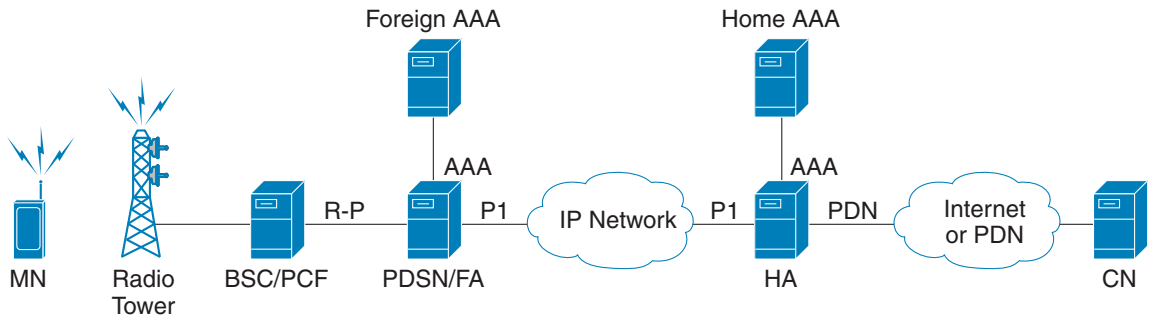
| Command | Navigation | Description |
|---|---|---|
| Create MAG | *Right-click context* > **Commands** > **Configuration** | Use this command to create a new Mobile Access Gateway (MAG) service for the selected context. |
| Modify MAG<br>Delete MAG | Expand **MAG** Node > *right-click MAG service* > **Commands** > **Configuration** | Use this command to modify the MAG configuration details/delete the MAG profile for the selected context. |
| Show MAG | Expand **MAG** Node > *right-click MAG service* > **Commands** > **Show** | Use this command to view and confirm the configuration details for the selected MAG service. |
| Create Profile ID QCI Mapping | Right-click on the context > **Commands** > **Configuration** | Use this command to create a QCI profile. |
| Delete Profile ID QCI Mapping | Expand **Profile** node > *right-click profile name* > **Commands** > **Configuration** | Use this command to delete QCI profile. |
| Create Profile | Expand **Profile** node > *right-click profile name* > **Commands** > **Configuration** | Use this command to create an entry for the QCI mapping profile. |
| Modify Profile<br>Delete Profile | Expand **Profile** node > Profile name > In content pane, *right-click on profile entry* > **Commands** > **Configuration** | Use these commands to modify/delete the entry for the QCI mapping profile. |

# Monitoring Home Agent (HA)

A Home Agent (HA) stores information about the mobile nodes whose permanent home address is in the home agent's network. When a node wants to communicate with the mobile node, it sends packets to the permanent address. Because the home address logically belongs to the network associated with the HA, normal IP routing mechanisms forward these packets to the home agent.

When a mobile node moves out of the home network, the HA still manages to deliver the packets to the mobile node. This is done by interacting with the Foreign Agent (FA) that the mobile node is communicating with using the Mobile IP (MIP) Standard. Such transactions are performed through the use of virtual private networks that create MIP tunnels between the HA and FA. The following figure displays the configuration between the FA and HA network deployment.

***Figure 26-8 Home Agent Topology***




When functioning as a HA, the system can either be located within the carrier's 3G network or in an external enterprise or ISP network. The FA terminates the mobile subscriber's PPP session, and then routes data to and from the appropriate HA on behalf of the subscriber.

In accordance with Request for Comments (RFC) 2002, the FA is responsible for mobile node registration with, and tunneling of data traffic from/to the subscriber's home network. The HA is also responsible for tunneling traffic, but it maintains subscriber location information separately in the Mobility Binding Records (MBR).

## Viewing the Home Agent Configuration

To view the Home Agent configuration:

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

**Step 2** In the logical inventory window, choose **Logical Inventory** > *Context* > **Mobile** > **Home Agent**. The list of home agent services configured in Prime Network are displayed in the content pane.

**Step 3** From the **Home Agent** node, choose a home agent service. The home agent service details are displayed in the content pane as shown in Figure 26-9.

*Figure 26-9 Home Agent Service Details*

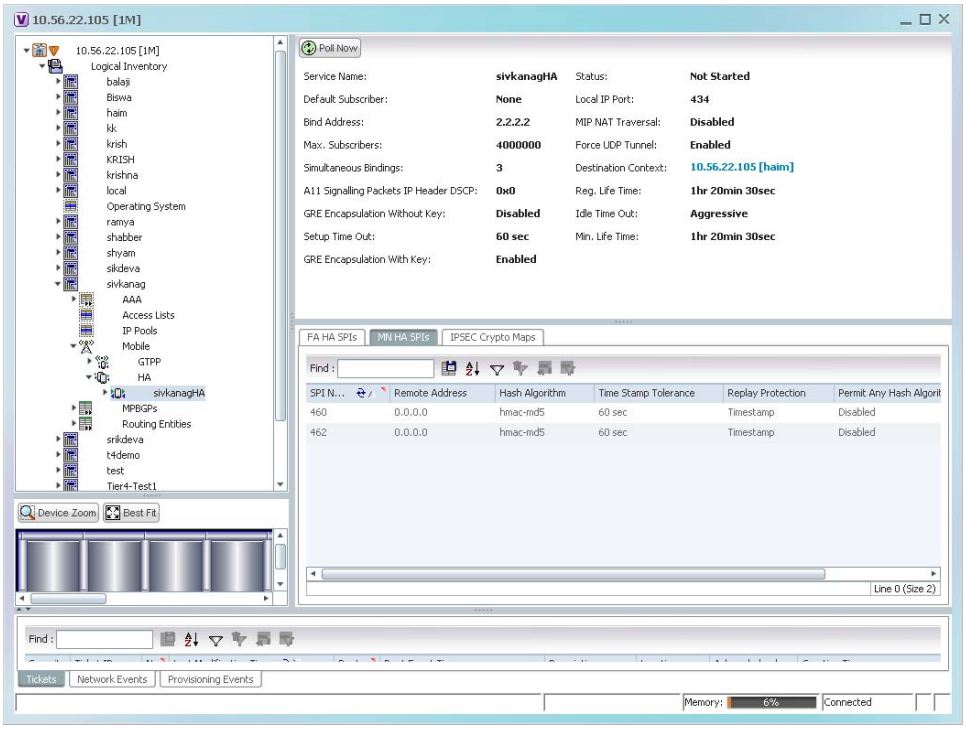



Table 26-34 displays the Home Agent service details.

*Table 26-34 Home Agent Service Details*

| Field | Description |
|---|---|
| Service Name | The name of the home agent service. |
| Status | The status of the home agent service, which can be any one of the following:<br>• Down<br>• Running<br>• Initiated<br>• Unknown<br>This field defaults to **Down**. |
| Default Subscriber | The name of the subscriber template that is applied to the subscribers. |
| Local IP Port | The User Datagram Protocol (UDP) port for the R-P interface of the IP socket. This IP port can be any value between 1 and 65535 and defaults to 699. |
| Bind Address | The IP address to which the service is bound to. This can be any address in the IPV4/IPv6 range. |
| MIP NAT Traversal | Indicates whether the acceptance of UDP tunnels for NAT traversal is enabled. |
| Max. Subscribers | The maximum subscriber sessions that could be supported. |

*Table 26-34 Home Agent Service Details (continued)*

| Field | Description |
|---|---|
| Force UDP Tunnel | Indicates whether HA would accept requests when Network Address Translation (NAT) is not detected but the Force bit is set in the Registration Request (RRQ) with the UDP Tunnel Request. |
| Simultaneous Bindings | The maximum number of care of addresses that can be simultaneously bound for the same user identified by Network Access Identifier (NAI) and Home address. |
| Destination Context | The name of the context to assign to the subscriber, after authentication. |
| A11 Signalling Packets IP Header DSCP | The Differential Services Code Point (DSCP) value in the IP header. |
| Registration Life Time | The registration lifetime configured for all the subscribers to the service. |
| GRE Encapsulation Without Key | Indicates whether Generic Routing Encapsulation (GRE) without encapsulation key is used during Mobile IP sessions with FA. |
| Idle Time Out | The method the HA service uses to determine the time to reset a session idle timer, which can be any one of the following:<br>• Aggressive<br>• Handoff<br>• Normal |
| SPI List | The Security Parameter Index (SPI) between the HA service and the FA. |
| Optimize Tunnel Reassembly | Indicates whether the option to optimize tunnel reassembly is enabled. |
| Wi-Max 3GPP | Indicates whether the Worldwide Interoperability for Microwave Acces (Wi-Max)-3GPP option is enabled for the Home agent service. |
| Setup Time Out | The maximum time (in seconds) allowed for session setup. |
| Reverse Tunnel | Indicates whether reverse tunnel feature is enabled for the home agent feature.<br>**Note** A reverse tunnel is a tunnel that starts at the care-of address of the mobile node and terminates at the home agent. A mobile node can request a reverse tunnel between the foreign agent and the home agent when the mobile node registers. |
| Min. Life Time | The minimum registration life time for a mobile IP session. |
| GRE Encapsulation With Key | Indicates whether GRE is used during mobile IP sessions with an FA. |
| **FA HA SPIs / MN HA SPIs tab** | |
| SPI Number | The number to indicate the security context between services. |
| Remote Address | The IP address of the source service. |
| Hash Algorithm | The hash algorithm used between the source and destination services. |
| Time Stamp Tolerance | The acceptable allowable difference in time stamps. If this difference is exceeded, then the session is rejected. |
| Replay Protection | The replay protection scheme that should be implemented by the service. |

*Table 26-34 Home Agent Service Details (continued)*

| Field | Description |
|---|---|
| Permit Any Hash Algorithm | Indicates whether verification of MN-HA authenticator using other hash algorithms is allowed, on failure of the configured hash algorithm.<br>**Note** This field is available only in the **MN HA SPIs** tab. |
| Description | The description of the SPI. |
| **IPSEC Crypto Maps** | |
| Map Name | The name of the crypto map that is configured in the same context that defines the IPSec tunnel properties. |
| Peer FA Address | The IP address of the Peer FA to which the IPSEC SA will be established. |
| Skey Expiry | The expiry information of the secret key. |

## Viewing the AAA Configuration for Home Agent Service

In order to support Packet Data Serving Node (PDSN), FA, and HA functionality, the system must be configured with at least one source context and at least two destination contexts as shown in the following figure.

The source context will facilitate the PDSN service(s), and the R-P interfaces. The AAA context will be configured to provide foreign/home AAA functionality for subscriber sessions and facilitate the AAA interfaces.

To view the AAA configuration:

**Step 1** In the logical inventory window, choose **Logical Inventory >** *Context* **> Mobile > Home Agent >** *Home agent service* **> AAA**. The AAA configuration details are displayed in the content pane.

Table 26-35 displays the AAA configuration for a home agent service.

*Table 26-35 AAA Configuration for Home Agent Service*

| Field | Description |
|---|---|
| AAA Context | The AAA context for the home agent service. Click this link to view the relevant AAA context. |
| AAA Accounting | Indicates whether the Home Agent can send AAA accounting information for subscriber sessions. |
| AAA Accounting Group | The AAA Accounting group for the Home agent service. |
| AAA Distributed MIP Keys | Indicates the usage of AAA distributed MIP keys for authenticating RRQ for WiMax HA calls. |
| DMU Refresh Key | Indicates whether the Home Agent is allowed to retrieve the MN-HA key again from the AAA during the call and use this freshly retrieved key value to recheck authentication. |

*Table 26-35 AAA Configuration for Home Agent Service*

| Field | Description |
|---|---|
| IMSI Authentication | Indicates whether MN-AAA or MN-FAC extensions are present in the RRQ. |
| MN HA Authentication Type | Indicates whether the HA service looks for an MN-HA authentication in the RRQ. |
| MN AAA Authentication Type | The method used to send authentication request to AAA for each re-registration attempt.<br>**Note** The initial registration request and de-registrations are handled normally. |
| PMIP Authentication | Indicates whether the HA service looks for an PMIP authentication in the RRQ. |
| Stale Key Disconnect | Indicates whether the call must be disconnected immediately on failure of MN-HA authentication. |
| Skew Lifetime | The IKE pre-shared key\u2018s time skew. |

## Viewing the GRE Configuration for Home Agent Service

To view the GRE configuration:

**Step 1** In the logical inventory window, choose **Logical Inventory >** *Context* **> Mobile > Home Agent >** *Home agent service* **> GRE**. The GRE configuration details are displayed in the content pane.

Table 26-36 displays the GRE configuration for a home agent service.

*Table 26-36 GRE Configuration for Home Agent Service*

| Field | Description |
|---|---|
| Checksum | Indicates whether insertion of GRE checksum in outgoing GRE data packets is enabled. |
| Checksum Verify | Indicates whether verification of GRE checksum in incoming GRE packets is enabled. |
| Reorder Timeout | The maximum amount of time (in milliseconds) to wait before reordered out-of-sequence GRE packets are processed. |
| Sequence Mode | The method to handle incoming out-of-sequence GRE packets, which can be any one of the following:<br>• Reorder<br>• None |
| Sequence Numbers | Indicates whether the option to insert or remove GRE sequence numbers in GRE packets is enabled. |

## Viewing the Policy Configuration for Home Agent Service

To view the Policy configuration:

**Step 1** In the logical inventory window, choose **Logical Inventory >** *Context* **> Mobile > Home Agent >** *Home agent service* **> Policy**. The Policy configuration details are displayed in the content pane.

Table 26-37 displays the Policy configuration for a home agent service.

*Table 26-37 Policy Configuration for Home Agent Service*

| Field | Description |
|---|---|
| BC Response Code | The response code for a binding cache (BC) query result in response to a network failure or error. |
| NW-Reachability Policy | The action to be taken on detection of an upstream network-reachability failure. |
| Over Load Policy | The overload policy within the HA service. |
| New Call Policy | The new call policy within the HA service. |
| **Over Load Redirect / NW-Reachability Redirect** | |
| IP Address | The IP address associated with the policy. |
| Weight | The weightage of the IP address associated with the policy. |

## Viewing the Registration Revocation Details for a Home Agent Service

To view the Registration revocation configuration details:

**Step 1** In the logical inventory window, choose **Logical Inventory >** *Context* **> Mobile > Home Agent >** *Home agent service* **> Registration Revocation**. The configuration details are displayed in the content pane.

Table 26-38 displays the Registration Revocation configuration for a home agent service.

*Table 26-38 Registration Revocation configuration for Home Agent Service*

| Field | Description |
|---|---|
| Registration Revocation State | Indicates whether the Registration Revocation Status is enabled. |
| Revocation IBit | Indicates whether the Revocation Ibit feature is enabled. |
| Send NAI Extension | Indicates whether the option to send NAI extension in the revocation message is enabled. |
| Handoff Old FA | Indicates whether the option to send a revocation message from the HA to the FA is enabled.<br>**Note** The revocation message is sent from the HA to the FA when an inter-access gateway or FA handoff of the MIP session occurs. |
| Idle Timeout | Indicates whether the HA must send a revocation message to the FA when the session times out. |

*Table 26-38 Registration Revocation configuration for Home Agent Service*

| Field | Description |
|---|---|
| Revocation Max Retries | The number of times the revocation message can be retransmitted. |
| Revocation Timeout | The maximum amount of time (in seconds) to wait for the receipt of an acknowledgement from the FA before the revocation message is transmitted again. |

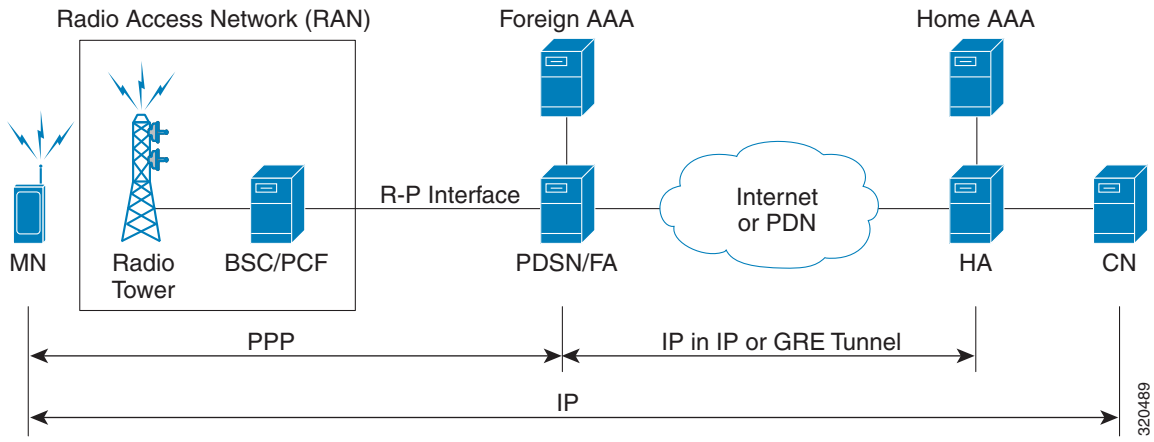
# Monitoring the Foreign Agent

A Foreign Agent (FA) is basically a router on a mobile node's visited network that provides routing services to the mobile node. The FA acts as a mediator between the mobile node and it's home agent (HA). When the mobile node moves out of its home network, the FA registers the mobile node with a Care of Address (CoA). It also facilitates routing information to the mobile node's home agent, which contains the permanent address of the node.

When a node tries to communicate with a mobile node that is roaming, it sends packets to the permanent address. The HA interacts with the FA and delivers the packets to the mobile node using the COA.

Figure 26-10 depicts the function of a foreign agent in a network and the different components that it interacts with.

*Figure 26-10 Foreign Agent Architecture*




## Viewing the Foreign Agent Configuration Details

To view the Foreign Agent configuration details:

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

**Step 2** In the logical inventory window, choose **Logical Inventory** > *Context* > **Mobile** > **FA.** The list of Foreign agents configured in Prime Network are displayed in the content pane.

**Step 3** From the **FA** node, choose a FA service. The FA service details are displayed in the content pane as shown in Figure 26-11.

***Figure 26-11 Foreign Agent Service Details***

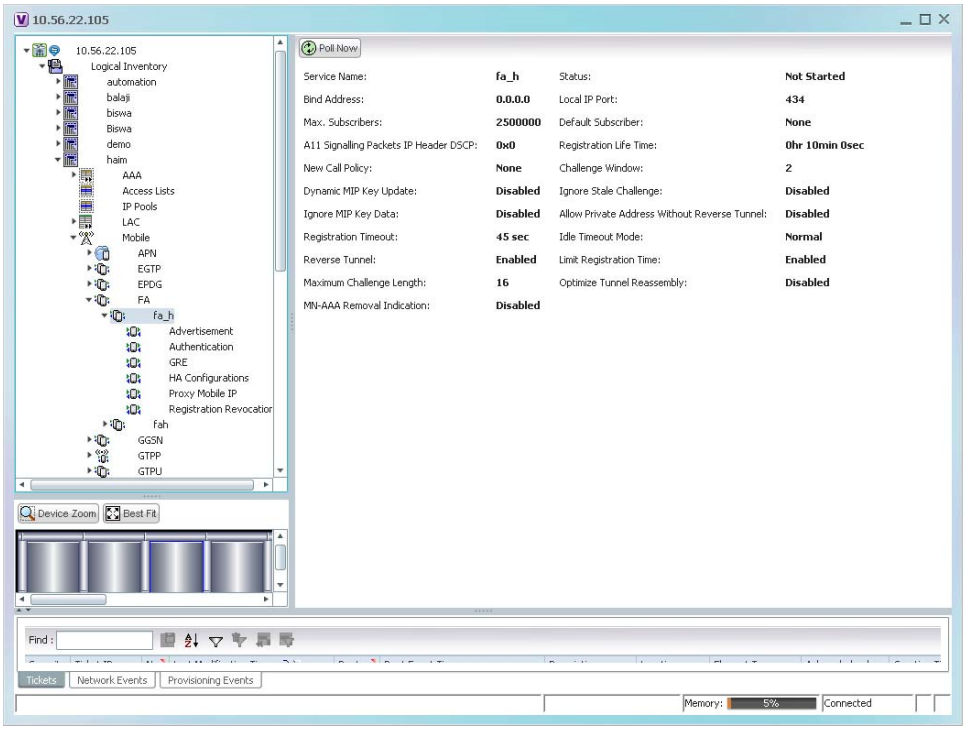



Table 26-39 displays the Foreign Agent configuration details.

***Table 26-39 FA Configuration Details***

| Field | Description |
|---|---|
| Service Name | The unique name to identify the FA service. |
| Status | The status of the FA service, which can be any one of the following:<br>• Down<br>• Running<br>• Initiated<br>• Unknown<br>This field defaults to **Down**. |
| Bind Address | The IPv4 address to which the service is bound. |
| Local IP Port | The UDP port for the R-P Interface of the IP socket. This port can be any value between 1 and 65535, and defaults to 434. |
| Max. Subscribers | The maximum subscriber sessions that is supported by the service. This can be any value between 0 and 2500000, and defaults to 2500000. |

*Table 26-39 FA Configuration Details (continued)*

| Field | Description |
|---|---|
| Default Subscriber | The name of the subscriber template that is applicable to the subscribers using this domain alias. |
| A11 Signalling Packets IP Header DSCP | The Differential Service Code Point (DSCP) value in the IP header. This value can range between 0x0 and 0x3F, and defaults to 0x0F.<br><br>**Note** The Differentiated Services (DS) field of a packet contains 6 bits that represents the DSCP value. Out of these 6 bits, five of them represent the DSCP. Hence, you can assign upto 32 DSCPs for various priorities. |
| Registration Life Time | The amount of time (in seconds) that an A10 connection can exist before its registration expires. This time can be any value between 1 and 65534, and defaults to 1800 seconds. |
| New Call Policy | The call policy for one or all the services, which can be any one of the following:<br>• Reject<br>• None<br>This field defaults to **None**. |
| Challenge Window | The number of challenges that can be handled by the FA. |
| Dynamic MIP Key Update | The status of the Dynamic Mobile IP Key update feature. This option is disabled by default. |
| Ignore Stale Challenge | The status of the Ignore Stale Challenge in MIP RRQ. This option is disabled by default. |
| Ignore MIP Key Data | The status of the Ignore MIP Key data. This option is disabled by default. |
| Allow Private Address Without Reverse Tunnel | Indicates whether the mobile node can use reverse tunnel for a private address. This option is disabled by default. |
| Registration Timeout | The amount of time (in seconds) for the registration reply timeout. |
| Idle Timeout Mode | The idle timeout method, which can be any one of the following:<br>• Normal<br>• Aggressive |
| Reverse Tunnel | Indicates whether reverse tunneling is applicable for client mobile IP sessions. This option is enabled by default. |
| Limit Registration Time | Indicates whether MIP registration lifetime is shorter than session idle, absolute, and long-duration timeouts. By default, this option is enabled. |
| Maximum Challenge Length | The maximum length of the FA challenge. |
| Optimize Tunnel Reassembly | Indicates whether tunnel reassembly is optimized for fragmented large packets passed between HA and FA. By default, this option is disabled. |
| MN-AAA Removal Indication | Indicates whether the FA can remove MN-FAC and MN-AAA extensions from RRQs. By default, this option is disabled. |

You can also view the following configuration details for a Foreign Agent service:

- Advertisement—Foreign agents advertise their presence on their attached links by periodically multicasting or broadcasting messages called agent advertisements. Mobile nodes listen to these advertisements and determine if they are connected to their home link or foreign link. Rather than waiting for agent advertisements, an MN can also send an agent solicitation. This solicitation forces any agents on the link to immediately send an agent advertisement.
- Authentication—Authentication verifies users before they are allowed access to the network and network services.
- GRE—Generic routing encapsulation (GRE) is a tunneling protocol used by Mobile IP. The GRE tunnel interface creates a virtual point-to-point link between two routers at remote points over an IP internetwork. If the GRE for Cisco Mobile Networks feature is enabled, the mobile router will request GRE encapsulation in the registration request only if the FA advertises that it is capable of GRE encapsulation (the G bit is set in the advertisement). If the registration request is successful, packets will be tunneled using GRE encapsulation. If the GRE for Cisco Mobile Networks feature is enabled and the mobile router is using collocated care-of address (CCoA), the mobile router will attempt to register with the HA using GRE encapsulation. If the registration request is successful, packets will be tunneled using GRE encapsulation.
- HA Configurations—Once the mobile node roams to a new network, it must register with the home agent as being away from home. Its registration is sent by way of the Foreign Agent (FA), the router providing service on the foreign network. A security association between the home agent (HA) and the foreign agent (FA) is mandatory.
- Proxy Mobile IP—Proxy Mobile IP supports Mobile IP for wireless nodes without requiring specialized software for those devices. The wireless access point acts as a proxy on behalf of wireless clients that are not aware of the fact that they have roamed onto a different Layer 3 network. The access point handles the IRDP communications to the foreign agent and handles registrations to the home agent.
- Registration Revocation—Registration Revocation is a method by which a mobility agent (one that provides Mobile IP services to a mobile node) can notify the other mobility agent of the termination of a registration due to administrative reasons or MIP handoff. When a mobile changes its point of attachment (FA), or needs to terminate the session administratively, the HA sends a registration revocation message to the old FA. The old FA tears down the session and sends a registration revocation acknowledgement message to the HA. Additionally, if the PDSN/FA needs to terminate the session administratively, the FA sends a registration revocation message to the HA. The HA deletes the binding for the mobile, and sends a registration revocation acknowledgement to FA.

### Viewing the Advertisement Configuration Details

To view the Advertisement configuration details for a foreign agent:

**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 > FA >** *FA service* **> Advertisement.** The details are displayed in the content pane.

Table 26-40 displays the Advertisement configuration details.

*Table 26-40 Advertisement Configuration Details*

| Field | Description |
|---|---|
| Advertisement Delay | The time delay (in milliseconds) for the first advertisement for a WiMax call. This time can be any value between 10 and 5000, and defaults to 1000. |
| Advertisement Interval | The advertisement interval time (in milliseconds). This time can be any value between 100 and 1800000, and defaults to 5000 milliseconds. |
| Advertisement Life Time | The maximum registration life time (in seconds) of the advertisement. This time can be any value between 1 and 65535, and defaults to 600 seconds. |
| Number of Advertisements Sent | The number of initial agent advertisements sent. This number can be any value between 1 and 65535, and defaults to 5. |
| Prefix Length Extension | Indicates whether the service address of the FA must be included in the Router Address field of the agent advertisement. If this field is set to **Yes**, then a prefix-length extension is appended to the router address field. By default, this option is set to **No**. |

## Viewing the Authentication Configuration Details

To view the Authentication configuration details for a foreign agent:

**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 > FA >** *FA service* **> Authentication.** The details are displayed in the content pane.

Table 26-41 displays the Authentication configuration details.

*Table 26-41 Authentication Configuration Details*

| Field | Description |
|---|---|
| MN AAA Authentication Policy | The MN AAA Authentication policy, which can be any one of the following:<br>• Ignore-after-handoff<br>• Init-reg<br>• Init-reg-except-handoff<br>• Always<br>• Renew-reg-noauth<br>• Renew-and-dereg-noauth<br>This field defaults to Always. |
| MN HA Authentication Policy | The policy to authenticate Mobile Node HA in the RRP, which can be any one of the following:<br>• Always<br>• Allow-noauth<br>This field defaults to **Allow-noauth**. |
| AAA Distributed MIP Keys Override | Indicates whether the AAA distributed MIP Keys Override option is enabled. In other words, if this feature is enabled, then the authentication parameters for the FA service will override the dynamic keys from AAA with static keys.<br>**Note** This feature supports those MIP registrations with an HA that does not support dynamic keys. |
| MN AAA Optimized Retries | Indicates whether the authentication request must be sent to the AA for each re-registration. |

## Viewing the GRE Configuration Details

To view the Generic Routing Encapsulation (GRE) configuration details for a foreign agent:

**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 > FA >** *FA service* **> GRE.** The details are displayed in the content pane.

Table 26-42 displays the GRE configuration details.

*Table 26-42 GRE Configuration Details*

| Field | Description |
|---|---|
| Checksum | Indicates whether the Checksum feature is enabled in outgoing GRE packets. By default, this option is disabled. |
| GRE Encapsulation | Indicates whether GRE is used when establishing a Mobile IP session.<br>If this option is enabled, the FA requests HA to use GRE when establishing a MIP session. If this option is disabled, the FA will not set the GRE bit in agent advertisements to the mobile node. |
| Checksum Verify | Indicates whether the checksum field must be verified in the incoming GRE packets. By default, this option is disabled. |
| Reorder Timeout | The maximum time (in milliseconds) to wait before processing the GRE packets that are out of sequence. This time can be any value between 0 and 5000, and defaults to 100 milliseconds. |
| Sequence Mode | The mode used to handle the incoming out-of-sequence packets, which can be any one of the following:<br>• Reorder<br>• None<br>This field defaults to **None**. |
| Sequence Numbers | Indicates whether GRE sequence numbers must be inserted into the data that is about to be transmitted over the A10 interface. This option is disabled by default. |

## Viewing the HA Configuration Details

To view the HA configuration details for a foreign agent:

**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 > FA >** *FA service* **> HA.** The details are displayed in the content pane.

Table 26-43 displays the HA configuration details.

*Table 26-43 HA Configuration Details*

| Field | Description |
|---|---|
| HA Monitoring | The HA monitoring status of the FA. This option is disabled by default. |
| AAA-HA Override | Indicates whether AAA HA can override Mobile Node during call establishment for HA assignment. |
| Dynamic HAFailover | Indicates whether failover during call establishment for Home Agent assignment is allowed. |
| HA Monitor Interval | The time interval (in seconds) to send HA monitoring requests. This time can be any value between 1 and 36000, and defaults to 30 seconds. |
| HA Monitor Maximum Inactivity Time | The maximum amount of time (in seconds) when there is no MIP traffic between FA and HA, which triggers the HA monitoring feature. This time can be any value between 30 and 600, and defaults to 60 seconds. |
| HA Monitor Retry Count | The number of times HA monitoring requests are sent before deciding that the HA is not reachable. This count can be any value between 0 and 10, and defaults to 5. |
| FA SPI List Name | The name of the SPI list linked with the FA service and configured for the selected context. Clicking on this link will take you to the relevant list under the **SPI** node. |
| **IKE** | |
| Peer HA Address | The IP address of the peer home agent. |
| Crypto Map Name | The IKE crypto map for the peer home agent. |
| **SPI** | |
| SPI Number | The unique SPI number that indicates a security context between the services. This number can be any value between 256 and 4294967295. |
| Remote Address | The IP address of the source service, which is expressed either in the IPv4 dotted decimal notation or IPv6 colon separated notation. |
| Hash Algorithm | The hash algorithm used between the source and destination services. |
| Time Stamp Tolerance | The acceptable time difference (in seconds) in timestamps, which can be any value between 0 and 65535.<br><br>**Note** If the actual timestamp difference exceeds the value here, then the session is rejected. If this value is 0, then the timestamp tolerance checking is disabled at the receiving end. |
| Replay Protection | The replay protection scheme that is implemented by the service. |
| Description | The description of the SPI. |
| Net Mask | The net mask for the IP address of the SPI. This field defaults to 255.255.255.255. |
| HA Monitor | Indicates whether HA monitoring is enabled. |

## Viewing the Proxy Mobile IP Configuration Details

To view the Proxy Mobile IP configuration details for a foreign agent:

**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 > FA >** *FA service* **> Proxy Mobile IP.** The details are displayed in the content pane.

Table 26-44 displays the Proxy Mobile IP configuration details.

***Table 26-44 Proxy Mobile IP Configuration Details***

| Field | Description |
|---|---|
| Proxy MIP | Indicates the status of the Proxy Mobile IP. |
| Encapsulation Type | The data encapsulation type to be used in PMIP call for specific FA services, which can be any one of the following:<br>• IPIP<br>• GRE<br>This field defaults to **IPIP**. |
| HA Failover | The failover status of the FA. This option is disabled by default. |
| HA Failover Max Attempts | The maximum number of times for HA Failover. This can be any value between 1 and 10, and defaults to 4. |
| HA Failover Timeout | The timeout (in seconds) for the HA failover. This time can be any value between 1 and 50, and defaults to 2. |
| HA Failover Attempts Before Switching | The number of times HA Failover was attempted, before switching over to an alternate HA. This can be any value between 1 and 5, and defaults to 2. |
| HA Failover Reply Code Trigger | The action to be taken on receipt of the configured reject code. |
| Max Retransmissions | The maximum number of times the FA is allowed to retransmit Proxy Mobile IP registration requests to the HA. This number can be any value between 1 and 4294967295, and defaults to 5. |
| Retransmission Timeout | The retransmission timeout (in seconds) for Proxy Mobile IP messages on event of failover. This time can be any value between 1 and 100, and defaults to 3. |
| Renew Time | The percentage of lifetime at which point the renewal is sent. This percent can be between 0 and 100, and defaults to 75. |

## Viewing the Registration Revocation Configuration Details

To view the Registration Revocation configuration details for a foreign agent:

**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 > FA >** *FA service* **> Registration Revocation.** The details are displayed in the content pane.

Table 26-45 displays the Registration Revocation configuration details.

*Table 26-45 Registration Revocation Configuration Details*

| Field | Description |
|---|---|
| Registration Revocation State | Indicates the status of the registration revocation. If this feature is enabled, then the FA can send a revocation message to the HA when revocation is negotiated with the HA and MIP binding is terminated. This feature is disabled by default. |
| Revocation IBit | The status of the Ibit on the registration revocation. If this feature is enabled, the FA can negotiate the Ibit via PRQ/RRP messages and process the Ibit revocation messages. This feature is disabled by default. |
| Internal Failure | Indicates whether a revocation message must be sent to the HA for those sessions that are affected by internal task failure. |
| Revocation Maximum Retries | The maximum number times a revocation message must be retransmitted before failure. This value can be any value between 0 and 10, and defaults to 3. |
| Revocation Timeout | The time period (in seconds) to wait for an acknowledgement from the HA before the revocation message is retransmitted. This time can be any value between 1 and 10, and defaults to 3. |

## Configuration Commands for Foreign Agent

To enable Mobile IP services on your network, you must determine which home agents will facilitate the tunneling for selected IP address, and where these devices or router will be allowed to roam. The areas, or subnets, into which the hosts are allowed to roam determine where foreign agent services need to be set up.

The foreign agent commands allow you to configure foreign agents in your network. Please note that these commands are available only for Cisco ASR 5000 Mobile devices.

These commands can be launched from the logical inventory by choosing the **Context > Commands > Configuration** or **Context > Commands > Show**.

Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands.

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

**Note** In the GUI, parameters that are displayed in bold text are mandatory.

Table 26-46 lists the Foreign Agent configuration commands.

*Table 26-46 Foreign Agent Configuration Commands*

| Command | Navigation | Description |
|---|---|---|
| Create FA | *Right-click on a context* > **Commands** > **Configuration** | Use this command to create a new foreign agent service for the selected context. |
| Modify FA<br>Delete FA | Expand **FA** node > *right-click FA service* > **Commands** > **Configuration** | Use these commands to modify/delete an existing foreign agent service configured for the selected context. |
| Show FA | Expand **FA** node > *right-click FA service* > **Commands** > **Show** | Use this command to view and confirm the foreign agent configuration details. |
| Create SPI | Expand **FA** node > *right-click FA service* > **Commands** > **Configuration** | Use this command to configure Security Parameter Index (SPI) for a foreign agent service. |
| Modify SPI<br>Delete SPI | Expand **FA** node > *expand FA service node* > **HA Configuration** > *right-click on SPI Number in content pane* > **Commands** > **Configuration** | Use these commands to modify and delete an existing SPI configured for a foreign agent service. |
| Create IKE | Expand **FA** node > *right-click FA service* > **Commands** > **Configuration** | Use this command to configure Internet Key Exchange (IKE) for a foreign agent service. If foreign agent reverse tunneling creates a tunnel that transverses a firewall, any mobile node that knows the addresses of the tunnel endpoints can insert packets into the tunnel from anywhere in the network. It is recommended to configure Internet Key Exchange (IKE) or IP Security (IPSec) to prevent this. |
| Modify IKE<br>Delete IKE | Expand **FA** node > *expand FA service node* > **HA Configuration** > *right-click on IKE Number in content pane* > **Commands** > **Configuration** | Use these commands to modify and delete an existing IKE configured for a foreign agent service. |

*Table 26-46 Foreign Agent Configuration Commands (continued)*

| Command | Navigation | Description |
|---|---|---|
| Modify Advertisement | Expand **FA** node > *FA service* > *right-click* **Advertisement** > **Commands** > **Configuration** | Use this command to modify the advertisement configuration settings specified for a foreign agent. |
| Modify Authentication | Expand **FA** node > *FA service* > *right-click* **Authentication** > **Commands** > **Configuration** | Use this command to modify the authentication configuration settings specified for a foreign agent. |
| Modify GRE | Expand **FA** node > *FA service* > *right-click* **GRE** > **Commands** > **Configuration** | Use this command to modify the Generic Routing Encapsulation (GRE) configuration settings specified for a foreign agent. |
| Modify HA Configuration | Expand **FA** node > *FA service* > *right-click* **HA Configuration** > **Commands** > **Configuration** | Use this command to modify the Home Agent configuration settings specified for a foreign agent. |
| Modify Proxy Mobile IP | Expand **FA** node > *FA service* > *right-click* **Proxy Mobile IP** > **Commands** > **Configuration** | Use this command to modify the Proxy Mobile IP configuration settings specified for a foreign agent. |
| Modify Registration Revocation | Expand **FA** node > *FA service* > *right-click* **Registration Revocation** > **Commands** > **Configuration** | Use this command to modify the Registration revocation configuration settings specified for a foreign agent. |

# Monitoring Evolved Packet Data Gateway (ePDG)

In today's market, there are multiple access networks for mobile technologies. For example, the following access networks are available for 3rd Generation Partnership Project (3GPP) network:

- General Packet Radio Service (GPRS). See GPRS/UMTS Networks - An Overview, page 26-4.
- Global System for Mobile communication (GSM)
- Universal Mobile Telecommunication System (UMTS). See GPRS/UMTS Networks - An Overview, page 26-4.

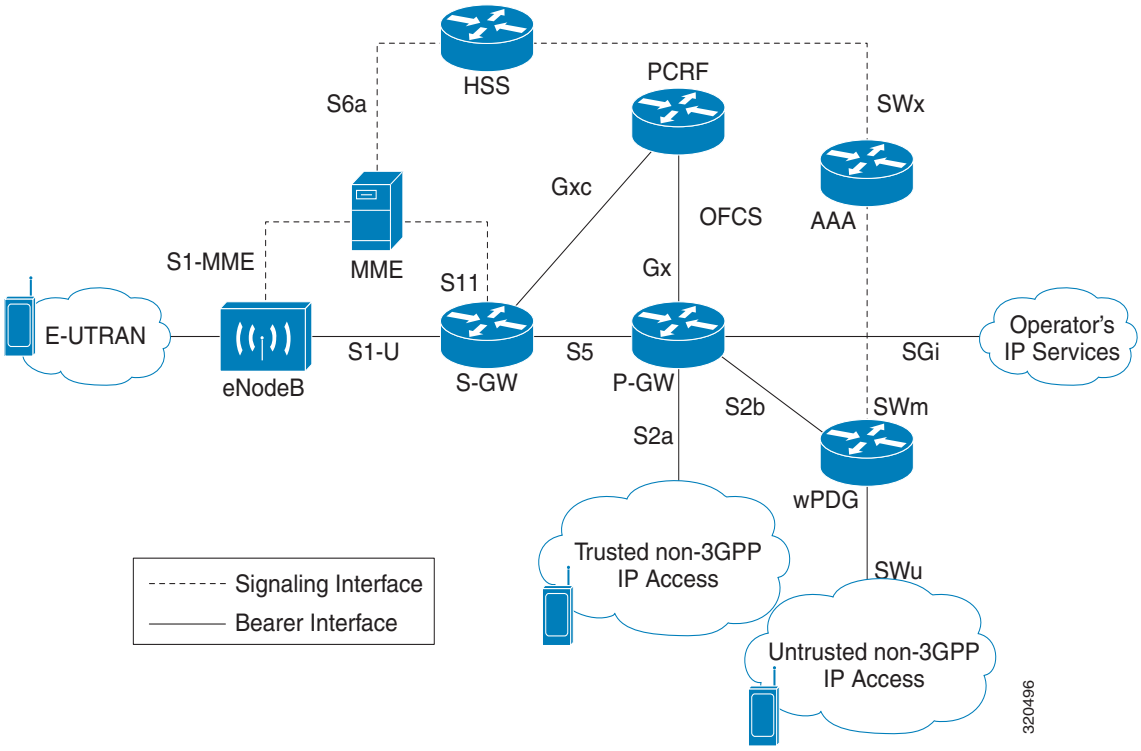
The following access network are available for Non-3GPP network:

- Worldwide Interoperability for Microwave Access (WiMAX)
- CDMA2000
- Wireless local area network (WLAN)
- Fixed networks

The Non-3GPP networks can be categorized into two—Trusted and Untrusted. While the trusted non-3GPP networks can interact directly with the Evolved Packet Core (EPC), the untrusted networks are required to pass through a security gateway to gain access to the EPC. This security gateway is called the Evolved Packet Data Gateway or ePDG.

When a user transmits data to the EPC using an untrusted non-3GPP network access, the ePDG must act as a termination node of IPSec tunnels established with the user equipment and secure the data being sent. Figure 26-12 shows the ePDG architecture.

***Figure 26-12 ePDG Architecture***



## IP Security (IPSec)

Internet Protocol Security or IPSec is a protocol suite that interacts with one another to provide secure private communications across IP networks. These protocols allow the system to establish and maintain secure tunnels with peer security gateways. In accordance with the following standards, IPSec provides a mechanism for establishing secure channels from mobile subscribers to pre-defined end points (such as enterprise or home networks):

- RFC 2401, Security Architecture for the Internet Protocol
- RFC 2402, IP Authentication Header (AH)
- RFC 2406, IP Encapsulating Security Payload (ESP)
- RFC 2409, The Internet Key Exchange (IKE)
- RFC-3193, Securing L2TP using IPSEC, November 2001

IPSec can be implemented for the following applications:

- **PDN Access**: Subscriber IP traffic is routed over an IPSec tunnel from the system to a secure gateway on the packet data network (PDN) as determined by access control list (ACL) criteria.
- **Mobile IP**: Mobile IP control signals and subscriber data is encapsulated in IPSec tunnels that are established between foreign agents (FAs) and home agents (HAs) over the Pi interfaces.

### IKEv2 and IPSec Encryption

ePDG supports Internet Key Exchange Version 2 (IKEv2) and IP Security Encapsulating Security Payload (IPSec ESP) encryption over IPv4 transport. The IKEv2 and IPSec encryption takes care of network domain security for all IP packet switched networks. It uses cryptographic techniques to ensure ensures confidentiality, integrity, authentication, and anti-replay protection.

## ePDG Security

In Prime Network, the following security services are available for ePDG:

- Crypto template—Used to define the IKEv2 and IPSec policies. In other words, it includes IKEv2 and IPSec parameters for keepalive, lifetime, NAT-T and cryptographic and authentication algorithms.
- EAP Profile—Defines the EAP authentication method and associated parameters.
- Transform Set—Define the negotiable algorithms for IKE SAs (Security Associations) and Child SAs to enable calls to connect to the ePDG.

### Viewing the Crypto Template Service Details

To view the Crypto template details:

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

**Step 2** In the logical inventory window, choose **Logical Inventory > *Context* > Security Association > Crypto Template.** The list of crypto templates are displayed in the content pane.

**Step 3** In the **Crypto Template** node, choose the crypto template. The template details are displayed in the content pane. Figure 26-13 displays the crytpo template details.

*Figure 26-13 Crypto Template Details*

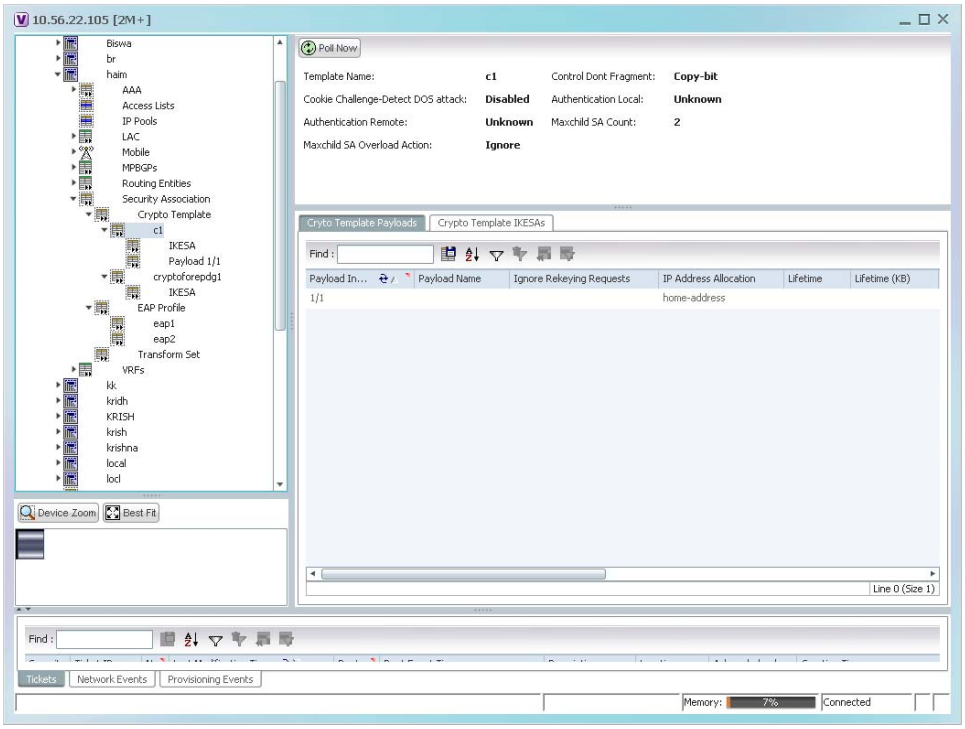



Table 26-47 displays the Crypto template details.

*Table 26-47 Crypto Template Details*

| Field | Description |
|---|---|
| Template Name | The unique name of the template. |
| Control Don't Fragment | The Don't Fragment (DF) bit in the IPSec tunnel data packet, which is encapsulated in the IPSec headers at both ends. The values for this field are:<br>• clear-bit—Clear DF Bit<br>• copy-bit—Copy DF bit from inner header<br>• set-bit—Set DF Bit<br>This field defaults to **copy-bit**. |
| Cookie Challenge-Detect DOS Attack | The cookie challenge parameters for the crypto template, which is used to prevent malicious Denial of Service (DOS) attacks against the server.<br>**Note** This feature prevents DOS attacks by sending a challenge cookie. If the response from the sender does not incorporate the expected cookie data, the packets are dropped. |

*Table 26-47 Crypto Template Details (continued)*

| Field | Description |
|---|---|
| Notify Payload - Half Open Session Start | The initial count of the number of half-open sessions per IPSec manager. Transmission of information will start only when the number of half-open sessions currently open exceed the starting count.<br><br>**Note** A session is considered half open if a Packet Data Interworking Function (PDIF) has responded to an IKEv2 INIT request with an IKEv2 INIT response, but no further messages were received on the particular IKE SA. |
| Notify Payload - Half Open Session End | The maximum count of half open sessions per IPSec manager. Transmission of information will stop when the number of half-open sessions currently open is less than this count. |
| Authentication Local | The local gateway key used for authentication. |
| Authentication Remote | The remote gateway key used for authentication. |
| Keepalive Interval | The period of time (in seconds) that must elapse before the next keepalive request is sent. |
| Keepalive Retries | The period of time (in seconds) that must elapse before the keepalive request is resent. |
| Keepalive Timeout | The keepalive time (in terms of seconds) for dead peer detection. |
| Maxchild SA Count | The maximum number of child SA per IKEv2 policy, which can be any value between 1 and 4. |
| Maxchild SA Overload Action | The action to be taken when the specified soft limit for the maximum number of SA is reached, which can be any one of the following:<br><br>Ignore—The IKEv2 stack ignores the specified soft limit for the SA and allows new SA to be created.<br><br>Terminate—The IKEv2 stack does not allow new child SA to be created when the specified soft limit is reached. |
| NAI CustomIDr | The unique user specified identification number to be used in the crypto template for Network Access Identifier (NAI). |
| **Crypto Template Payloads** | |
| Payload Instance | The payload instance configured for the crypto template. |
| Payload Name | The unique name of the crypto template payload. |
| Ignore Rekeying Requests | Indicates whether IKESA rekeying requests must be ignored. |
| IP Address Allocation | The IP Address Allocation scheme configured for the crypto template payload. |
| Lifetime | The lifetime (in seconds) for the IPSec Child Security Associations derived from the crypto template. |
| Lifetime (KB) | The lifetime (in kilo bytes) for the IPSec Child Security Associations derived from the crypto template. |
| Maximum Child SA | The maximum number of IPSec Child Security Associations (SA) that may be derived from a single IKEv2 IKE SA. |

*Table 26-47 Crypto Template Details (continued)*

| Field | Description |
|---|---|
| Rekey | Indicates whether IPSec Child Security Association rekeying must be enabled, after approximately 90% of the child SA lifetime has expired. |
| Rekey Keepalive | Indicates whether rekeying must be allowed if data is not received on the security association since the last rekey. |
| TSI Start Address | The IKEv2 Initiator Traffic Selector payload start address configured for the crypto template. |
| TSI End Address | The IKEv2 Initiator Traffic Selector payload end address configured for the crypto template. |
| TSR Start Address | The IKEv2 Responder Traffic Selector payload start address. |
| TSR End Address | The IKEv2 Responder Traffic Selector payload end address. |
| **Crypto Template IKESAs** | |
| IKESA Instance | The IKESA instance configured for the crypto template. |
| Allow Empty IKESA | Indicates whether empty IKESA is allowed. By default, empty IKESA is not allowed. |
| Certificate Sign | The certificate sign to be used. This field defaults to pkcs1.5. |
| Ignore Notify Protocol ID | Indicates whether the IKEv2 Exchange Notify Payload Protocol-ID values must be ignored for strict RFCA 4306 compliance. |
| Ignore Rekeying Requests | Indicates whether IKESA rekeying requests must be ignored. |
| Keepalive User Activity | Indicates whether the user inactivity timer must be reset when keepalive messages are received from the peer. |
| Max Retransmission | The maximum number of retransmissions of an IKEv2 IKE exchange request that is allowed if a response is not received. |
| Policy Congestion Rejection Notify Status | Indicates whether an error notification message must be sent in response to an IKE_SA INIT exchange, when IKESA sessions cannot be established anymore. |
| Policy Error Notification | Indicates whether an error notification message must be sent for invalid IKEv2 exchange message ID and syntax. |
| Rekey | Indicates whether IKESA rekeying must occur before the configured lifetime expires (which is approximately at 90% of the lifetime interval). By default, rekeying is not allowed. |
| Retransmission Timeout | The time period (in milliseconds) that must elapse before a retransmission of an IKEv2 IKE exchange request is sent when a corresponding response is not received. |
| Setup Timer | The number of seconds before a IKEv2 security association, which is not fully established, is terminated. |

## Viewing the EAP Profile Details

To view the EAP Profile details:

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

**Step 2** In the logical inventory window, choose **Logical Inventory > *Context* > Security Association > EAP Profile.** The list of profiles are displayed in the content pane.

**Step 3** In the **EAP Profile** node, choose the profile. The profile details are displayed in the content pane.

Table 26-48 displays the EAP Profile details.

***Table 26-48 EAP Profile Details***

| Field | Description |
|---|---|
| Name | The unique name of the EAP Profile. |
| Mode | The operative mode of the EAP profile, which can be any one of the following:<br>• **Authenticator Pass Through**—Indicates that the EAP Authentication Requests must be passed to an external EAP Server.<br>• **Authenticator Terminate**—Indicates that the EAP must act as an EAP Authentication Server. |
| Authentication Method | The EAP Authentication method to be used for the profile, which can be any one of the following:<br>• If the Mode is **Authenticator Pass Through**:<br>– eap-aka<br>– eap-gtc<br>– eap-md5<br>– eap-sim<br>– eap-tls<br>• If the Mode is Authenticator Terminate:<br>– eap-gtc<br>– eap-md5 |

## Viewing the Transform Set Details

To view the Transform Set details for IKEv2 IPSec/IKEv2:

**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* > Security Association > Transform Set > IKEv2 IPSec Transform Set** or **IKEv2 Transform set.** The list of profiles are displayed in the content pane.

**Step 3** In the **IKEv2 IPSec Transform Set** or **IKEv2 Transform set** node, choose the transform set. The relevant details are displayed in the content pane.

Table 26-49 displays the IKEv2 IPSec Transform set or IKEv2 Transform set details.

*Table 26-49 IKEv2 IPSec Transform Set/IKEv2 Transform set Details*

| Field | Description |
|---|---|
| Name | The name of the transform set. |
| DH Group | The Diffie-Hellman (DH) group for the transform set, which can be any one of the following:<br>• 1—Configure Diffie-Hellman Group 1:768-bit MODP Group<br>• 14—Configure Diffie-Hellman Group 14:2048-bit MODP Group<br>• 2—Configure Diffie-Hellman Group 2:1024-bit MODP Group<br>• 5—Configure Diffie-Hellman Group 5:1536-bit MODP Group<br>This field defaults to **2—Configure Diffie-Hellman Group 2:1024-bit MODP Group**.<br>**Note** The DH group is used to determine the length of the base Prime numbers used during the key exchange process in IKEv2. The cryptographic strength of any key derived, depends in part, on the strength of the DH group upon which the prime numbers are based. |
| Cipher | The appropriate encryption algorithm and encryption key length for the IKEv2 IKE security association, which can be any one of the following:<br>• 3des-cbc<br>• aes-cbc-128<br>• aes-cbc-256<br>• des-cbc<br>• Null<br>This field defaults to AESCBC-128. |
| HMAC | The Hash Message Authentication Code (HMAC) for the IKEv2 IPSec transform set,which can be any one of the following:<br>• aes-xcbc-96<br>• md5-96<br>• sha1-96<br>• sha2-256-128<br>• sha2-384-192<br>• sha2-512-256<br>This field defaults to **sha1-96**.<br>**Note** HMAC is a type of message authentication code calculated using a cryptographic hash function in combination with a secret key to verify both data integrity and message authenticity. A hash takes a message of any size and transforms it into a message of fixed size (the authenticator value), which is truncated and transmitted. |

*Table 26-49 IKEv2 IPSec Transform Set/IKEv2 Transform set Details*

| Field | Description |
|---|---|
| Mode | The encapsulation mode for the transform set, which can be any one of the following:<br>• transport<br>• tunnel |
| PRF | The Pseudo-random Function (PRF) for the transform set, which can be any one of the following:<br>• aes-xcbc-128<br>• md5<br>• sha1<br>• sha2-256<br>• sha2-384<br>• sha2-512<br>This field defaults to SHA1. This field is applicable only for IKEv2 transform sets.<br>**Note** This function is used to generate keying material for all cryptographic algorithms. It produces a string of bits that cannot be distinguished from random bit strings without the secret key. |
| Life Time | The time period for which the secret keys used for various aspects of a configuration is valid (before it times out). This field is applicable only for IKEv2 transform sets. |

## Viewing the ePDG Configuration Details

To view the ePDG configuration details:

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

**Step 2** In the logical inventory window, choose **Logical Inventory >** *Context* **> Mobile > EPDG.** The list of EPDG services configured in Prime Network are displayed in the content pane.

**Step 3** From the **EPDG** node, choose an EPDG service. The EPDG service details are displayed in the content pane.

Table 26-50 displays the EPDG service details.

*Table 26-50 EPDG Service Details*

| Field | Description |
|---|---|
| Service Name | The unique name of the ePDG service. |
| Status | The status of the ePDG service, which can be any one of the following:<br>• Initiated<br>• Running<br>• Down<br>• Started<br>• Nonstarted |
| IP Address | The IPV4 address of the ePDG service. |
| UDP Port | The User Datagram Protocol (UDP) port of the ePDG service. |
| Crypto Template | The name of the IKEv2 crypto template to be used by the ePDG service. This template is used to define the cryptographic policy for the ePDG service. |
| Max Sessions | The maximum number of sessions allowed for the ePDG service. |
| PLMN ID | The unique identification code of the Public Land Mobile Network (PLMN) for the ePDG service. This id is made up of the Mobile Country Code (MCC) and the Mobile Network Code (MNC). |
| MAG Service Context | The name of the context where the Mobile Access Gateway (MAG) services are configured. If a MAG service is not configured for the ePDG service, then one of the MAG services defined in the context is selected. |
| MAG Service | The name of the MAG service that handles the mobile IPv6 sessions. |
| Setup Timeout | The maximum time (in seconds) allowed for the session setup. |
| DNS PGWClient Context | The name of the context where the Domain Name System (DNS) client is configured for the Packet Data Network Gateway (PWG) selection. |
| DNS PGW Selection | The criteria to select a PGW service from the DNS. This criteria is based on the topology and/or weight from the DNS. |
| FQDN | The Fully Qualified Domain Name (FQDN), which is used for longest suffix match during dynamic allocation. |
| PGW Selection Agent Info Error Action | The action to be taken when the expected MIP6 agent information is not received from Authentication, Authorization, and Accounting (AAA) or Hosting Solution Software (HSS). |
| User Name MAC Address Stripping | Indicates whether the MAC address in the username obtained from the user equipment must be stripped. |
| User Name MAC Address Validation | Indicates whether the MAC address in the username obtained from the user equipment must be validated. |
| User Name MAC Address Validation Failure Action | Indicates the action that must be taken on failure of the validation of the MAC address in the user name obtained from the user equipment. |
| New Call Policy | Indicates the busy-out policy that must be followed to reject the incoming calls from individual users. |

## Configuration Commands for ePDG

The ePDG commands allow you to configure ePDG services in your network. Please note that these commands are available only for Cisco ASR 5000 Mobile devices.

These commands can be launched from the logical inventory by choosing the **Context > Commands > Configuration** or **Context > Commands > Show**.

Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands.

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

**Note** In the GUI, parameters that are displayed in bold text are mandatory.

Table 26-51 lists the ePDG configuration commands.

***Table 26-51 ePDG Configuration Commands***

| Command | Navigation | Description |
|---|---|---|
| Create ePDG Service | *Right-click context* > **Commands** > **Configuration** > | Use this command to create a new ePDG service. |
| Modify ePDG Service | Expand **EPDG** Node > *right-click EPDG service* > **Commands** > **Configuration** | Use this command to modify the configuration details for an ePDG service. |
| Delete ePDG Service | Expand **EPDG** Node > *right-click EPDG service* > **Commands** > **Configuration** | Use this command to delete an ePDG service. |
| Show ePDG Service | Expand **EPDG** Node > *right-click EPDG service* > **Commands** > **Show** | Use this command to view and confirm the configuration details of an ePDG Service. |

# Monitoring Packet Data Serving Node

Packet Data Serving Node, or PDSN, is a component of the Code Division Multiple Access (CDMA) 2000 mobile network. It acts as a connection point between the Radio Access Network (RAN) and IP Network. PDSN also manages PPP sessions between the mobile provider's core IP network and the mobile node.

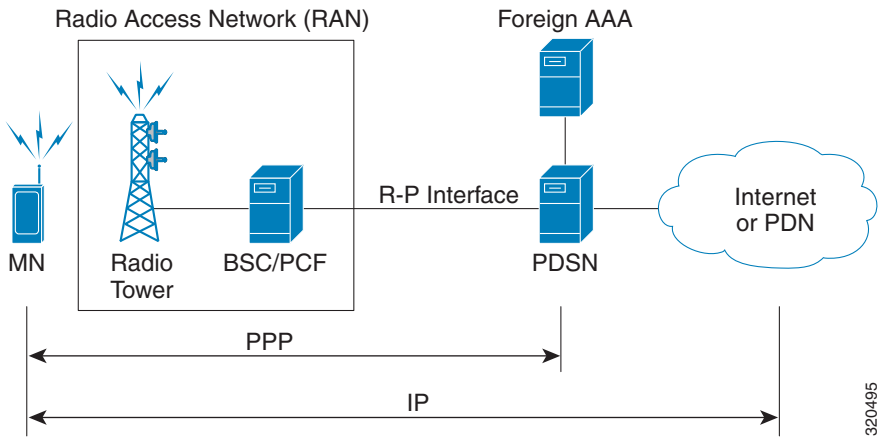
In other words, it provides access to the Internet, intranets, and applications servers for mobile stations that utilize a CDMA2000 RAN. Acting as an access gateway, PDSN provides simple IP and mobile IP access, foreign agent support, and packet transport for virtual private networking. It acts as a client for Authentication, Authorization, and Accounting (AAA) servers and provides mobile stations with a gateway to the IP network.

## PDSN Configurations

The following paragraphs list the different configurations for PDSN:

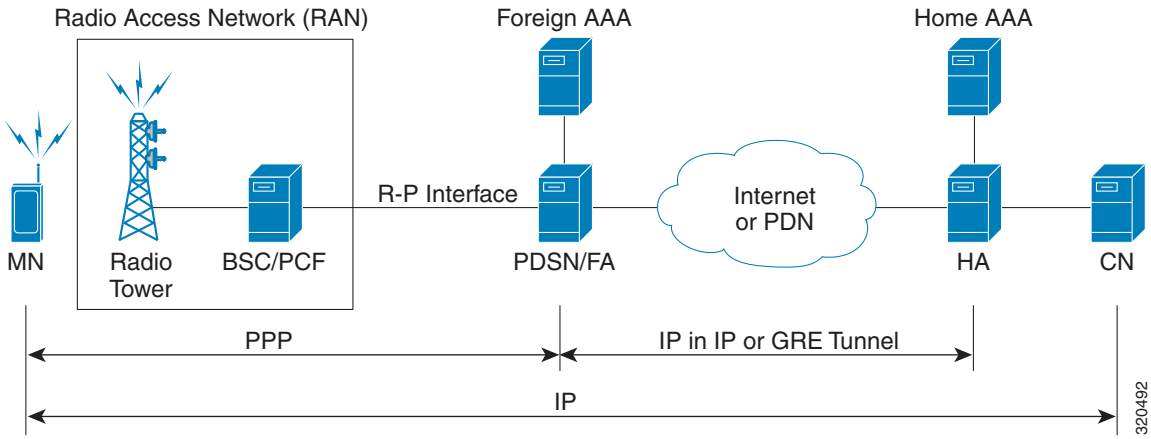
- Simple IP—In this protocol, the mobile user is assigned an IP address dynamically. The user can use this IP address within a defined geographical area, which is lost when the user moves out of the area. If the user moves out of the designated area, they must register with the service provider again to obtain a new IP address. Figure 26-14 depicts the working of this protocol.

***Figure 26-14 Simple IP configuration for PDSN***




- Mobile IP—In this protocol, the mobile user is assigned a static or dynamic IP address, which is basically the "home address" assigned by the user's Home Agent (HA). Even if the user moves out of the home network, the IP address does not change or is not lost. This enables the user to use applications that require seamless mobility such as transferring files. How does this work? The Mobile IP protocol provides a network-layer solution that allows mobile nodes to receive IP packets from their home network even when they are connected to a visitor network. The PDSN in the visitor's network performs as a Foreign Agent (FA), which assigns a Care-of-Address (CoA) to the mobile node and establishes a virtual session with the mobile node's HA. IP packets are encapsulated into IP tunnels and transported between the FA, HA and mobile node. Figure 26-15 depicts the working of this protocol.

*Figure 26-15 Mobile IP Configuration for PDSN*




- Proxy Mobile IP—This protocol provides a mobility solution for subscribers whose mobile nodes do not support the Mobile IP protocol. On behalf of the mobile node, PDSN proxies the Mobile IP tunnel with the HA. In turn, the service provider or the home agent assigns an IP address to the subscriber. This IP address does not change or is not lost even if the user moves out of the home network.

## Viewing the PDSN Configuration Details

To view the PDSN configuration details:

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

**Step 2** In the logical inventory window, choose **Logical Inventory >** *Context* **> Mobile > PDSN.** The list of PDSN services configured in Prime Network are displayed in the content pane.

**Step 3** From the **PDSN** node, choose a PDSN service. The PDSN service details are displayed in the content pane as shown in Figure 26-16.

*Figure 26-16 PDSN Service Details*

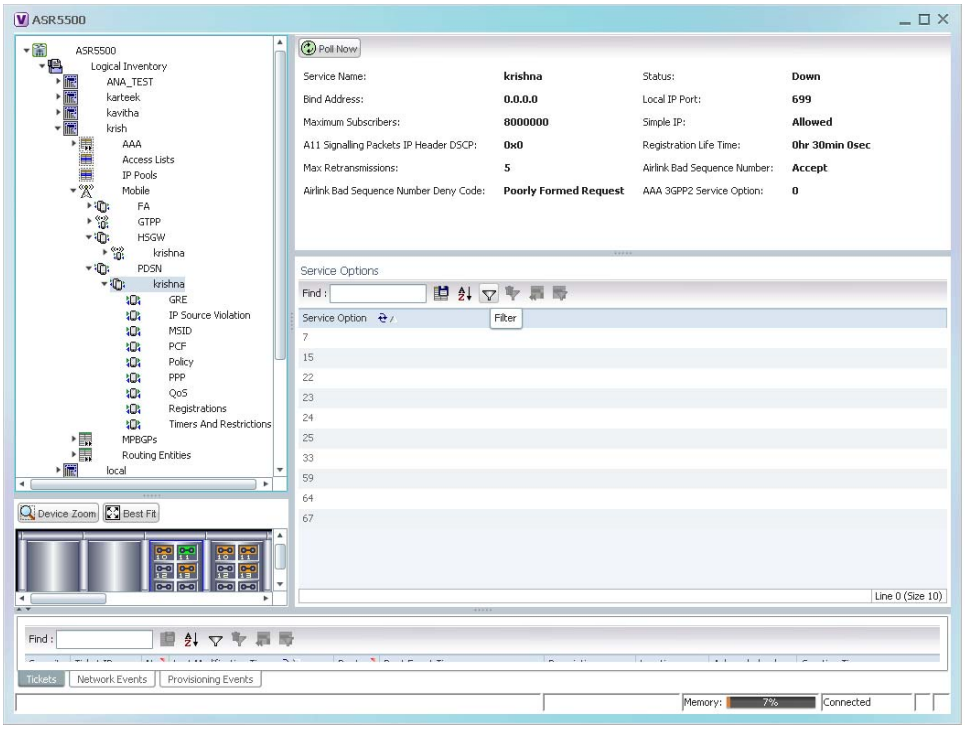



Table 26-52 displays the PDSN service details.

*Table 26-52 PDSN Service Details*

| Field | Description |
|---|---|
| Service Name | The unique name of the PDSN service. |
| Status | The status of the PDSN service, which can be any one of the following:<br>• Initiated<br>• Running<br>• Down<br>• Started<br>• Nonstarted<br>• Unknown |
| Bind Address | The IP address to which the service is bound. This can be a IPv4 or IPv6 address.<br>**Note** Multiple IP addresses belonging to the same IP interface can be bound to different PDSN services, but one address can be bound to only one service. |
| Local IP Port | The User Datagram Protocol (UDP) port for the R-P interface of the IP socket. This IP port can be any value between 1 and 65535 and defaults to 699. |

*Table 26-52 PDSN Service Details (continued)*

| Field | Description |
|---|---|
| Mobile IP | The IP address of the Foreign agent that is configured for the PDSN service. |
| Simple IP | Indicates whether the Simple IP configuration is available for the PDSN service, which can be any one of the following:<br>• Allowed<br>• Not Allowed (default value) |
| Max Subscribers | The maximum number of subscribers that the PDSN service can support. |
| Registration Life Time | The registration lifetime configured for all the subscribers to the service. |
| Max Retransmissions | Maximum retries for transmitting RP control packets. This count can be any value between 1 and 1000000 and defaults to 5. |
| A11 Signalling Packets IP Header DSCP | The Differential Services Code Point (DSCP) value in the IP header. |
| NAI Construction Domain | The Network Access Identifier for the PDSN service. This field is made up of the Mobile Station Identifier (MSID) of the subscriber, a separator character and a domain name.<br>**Note** The domain name used here can be either the name supplied as part of the subscriber's name or the domain alias. |
| Airlink Bad Sequence Number | The action to be taken when the PDSN receives an airlink record with a bad sequence number, which can be any one of the following:<br>• Accept (default value)<br>• Reject<br>**Note** At the time of the R-PA10 connection setup, an airlink record is assigned a unique sequence number. |
| Airlink Bad Sequence Number Deny Code | The reason for rejecting the airlink record with a bad sequence number, which can be any one of the following:<br>• Poorly Formed Request<br>• Unsupported Vendor ID |
| AAA 3GPP2 Service Option | The service options for which AAA 3GPP2 authentication is applicable. |
| **Service Option Entries** | |
| Service Option Number | The service option numbers applicable for the PDSN service.<br>**Note** Each service option relates to a standard data service. Hence, these numbers determine the data services that are supported by the PDSN service. |

You can also view the following configuration details for a PDSN service:

- GRE

- IP Source Violation
- MSID
- PCF
- Policy
- PPP
- QoS
- Registrations
- Timers and Restrictions

## Viewing the GRE Configuration Details

To view the Generic Routing Encapsulation (GRE) configuration details for a PDSN service:

**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 > PDSN** > *PDSN service* > **GRE.** The GRE details are displayed in the content pane.

Table 26-53 displays the GRE configuration details.

***Table 26-53 GRE Configuration Details***

| Field | Description |
|---|---|
| Checksum | Indicates whether the Checksum field is applicable for outgoing GRE packets.By default, this option is disabled. |
| Checksum Verify | Indicates whether the verification of the Checksum field is enabled for incoming GRE packets. |
| Reorder Time Out | The maximum time (in milliseconds) for processing the GRE packets that are coming out of order. This time can be any value between 0 and 5000, and defaults to 100 milliseconds. |
| Sequence Mode | The mode in which incoming out-of-sequence GRE packets are handled, which can be any one of the following:<br>• Reorder<br>• None<br>This field defaults to **None**. |
| Sequence Numbers | Indicates whether GRE sequence numbers are inserted in data that is about to be transmitted over the A10 interface. By default, this option is disabled. |
| Flow Control | Indicates whether flow control is supported by the selected PDSN service. If this option is enabled, PDSN sends flow control enabled Normal Vendor Specific Extensions (NSVE) in A11 RRPs. By default, this option is disabled. |
| Flow Control Time Out | The amount of time (in milliseconds) to wait for an Transmitter On (XON) indicator from the RAN. This time can be any value between 1 and 1000000, and defaults to 1000 milliseconds. |

*Table 26-53 GRE Configuration Details (continued)*

| Field | Description |
|---|---|
| Flow Control Action | The action that must be taken when the timeout limit is reached, which can be any one of the following:<br>• disconnect-session<br>• resume-session. |
| Protocol Type | The tunnel type for the GRE routing. This field defaults to **Any**. |
| Is 3GPP Ext Header QoS Marking | Indicates whether the 3GPP Extension Header QoS Marking is enabled for the selected PDSN feature.<br>**Note** If this feature is enabled and the PCF negotiation feature is enabled in A11 RRQ, then the PDSN will include QoS optional data attribute in the GRE 3GPP2 Extension Header. |
| IP Header DSCP Value | The Differential Service Code Point (DSCP) value in the IP header that marks the GRE IP Header encapsulation. This can be any value between 0x0F and 0X3F, and defaults to 0X0F. |
| IP Header DSCP Value Packet Type | Indicates whether the IP Header DSCP Value packet type is specified for the packets. By default, this option is disabled. |
| GRE Segmentation | Indicates whether segmentation of GRE packets is enabled. By default, this option is disabled. |

## Viewing the IP Source Violation Details

A Source violation occurs when a mobile device sources packets to the PDSN with a IP address that is different from the one specified during setup. Using this feature, the packets that need not be sent over the network are dropped when it tries to pass through PDSN.

To view the IP Source Violation configuration details for a PDSN service:

**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 > PDSN >** *PDSN service* **> IP Source Violation.** The details are displayed in the content pane.

Table 26-54 displays the IP Source Violation configuration details.

*Table 26-54 IP Source Violation Configuration Details*

| Field | Description |
|---|---|
| Clear on Valid Packet | Indicates whether the service to reset the negotiation and drop limit counters upon receipt of properly addressed packet is enabled. By default, this feature is disabled. |
| Drop Limit | The maximum number of IP source violations within the detection period, before the call is dropped. This number can be any value between 0 and 1000000, and defaults to 10. |
| Period | The detection period (in seconds) for the IP source violation. This field can be any value between 1 and 1000000, and defaults to 120. |
| Renegotiation Limit | The maximum number of IP source violations within the detection period before renegotiating PPP for the call. This field can be any value between 1 and 1000000, and defaults to 5. |

## Viewing the MSID Configuration Details

To view the Mobile Station ID (MSID) configuration details for a PDSN service:

**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 > PDSN** > *PDSN service* > **MSID.** The details are displayed in the content pane.

Table 26-55 displays the MSID configuration details.

*Table 26-55 MSID Configuration Details*

| Field | Description |
|---|---|
| MSID Length Max | The maximum length of the MSID configured for the PDSN service. This length can be any value between 10 and 15, and defaults to 15. |
| MSID Length Min | The minimum length of the MSID configured for the PDSN service. This length can be any value between 10 and 15, and defaults to 10. |
| MSID Authentication | Indicates whether the MSID authentication feature is enabled. |
| MSID Length Check | Indicates whether MSID length is enabled for the PDSN service. By default, this option is disabled.<br>**Note** This configuration is required to reject the A11-RRQs with illegal International Mobile Station Identification (IMSI). |

## Viewing the PCF Configuration Details

To view the Packet Control Function (PCF) configuration details for a PDSN service:

**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 > PDSN >** *PDSN service* **> PCF.** The details are displayed in the content pane.

Table 26-56 displays the PCF configuration details.

***Table 26-56 PCF Configuration Details***

| Field | Description |
|---|---|
| PCF Monitor Num Retries | The maximum number of retries before deciding that the PCF service is down. |
| PCF Session ID Change Restart PPP | Indicates whether the PPP must be restarted if there is a change in the session ID of an existing session. |
| New Call Conflict Terminate Old Session | Indicates whether the session with a PCF must be terminated when a new call request for an existing session is received from another PCF. |
| **PDSN Security Entries** | |
| SPI Number | The unique Security Parameters Index number that indicates a security context between the services. |
| Remote Address | The IP address of the source service. |
| Netmask | The subnet mask of the source service. |
| Zone ID | The ID of the zone to which the IP address belongs to. |
| Hash Algorithm | The hash algorithm used to encrypt the data. |
| Time Stamp Tolerance | The acceptable difference (in seconds) in the timestamps.<br>**Note** If the actual difference exceeds the difference specified here, then the session is rejected. If this difference is 0, the timestamp tolerance checking is disabled at the receiving end. |
| Replay Protection | The replay protection schemes that is implemented by the service. |
| Description | The description of the security profile. |

## Viewing the Policy Configuration Details

To view the Policy configuration details for a PDSN service:

**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 > PDSN >** *PDSN service* **> Policy.** The details are displayed in the content pane.

Table 26-57 displays the Policy configuration details.

*Table 26-57 Policy Configuration Details*

| Field | Description |
|---|---|
| Unknown CVSE Policy | Indicates whether the unknown Critical Vendor Specific Extension (CVSE) policy is enforced. |
| RRQ MEI From Current PCF | Indicates whether PPP must be restarted after getting MEI in RRQ. |
| New Call Policy | The call policy for one or all the services, which can be any one of the following:<br>• Accept<br>• Reject<br>• Redirect<br>• Reject on MSID<br>• Redirect on MSID<br>• None<br>This field defaults to **None**. |
| Overload Policy | The action to be taken by the PDSN service in case of an overload condition. |
| Overload Policy Reject Code | The reject code for the overload policy. |
| Service Option Policy | The policy followed by PDSN for configuring services. |
| Reject MSID | The Mobile Station Identifier (MSID) for which new calls are rejected.<br>**Note** If the **New Call Policy** field is set to **Reject MSID**, then this field will display the relevant MSID. |

## Viewing the PPP Configuration Details

To view the Point-to-Point Protocol details for a PDSN service:

**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 > PDSN** > *PDSN service* > **PPP.** The details are displayed in the content pane.

Table 26-58 displays the PPP configuration details.

*Table 26-58 PPP Configuration Details*

| Field | Description |
|---|---|
| Context Name | The destination context where the Layer 2 Tunneling protocol Access Concentrator (LAC) service is configured.<br><br>**Note** This context is the same as the PPP tunneling context. |
| Tunnel Type | The type of the PPP tunnel established between the PDSN and the PFC, which can be any one of the following values:<br>• L2TP<br>• None<br>This field defaults to **None**. |
| Fragment State | Indicates whether the PPP fragmentation is enabled. By default, this is option is disabled. |
| Alt PPP | Indicates whether the Alternate Point-to-Point (PPP) protocol sessions are enabled for the PDSN service. By default, this option is disabled. |
| Allow No Authentication | Indicates whether subscribers can gain network access even if they have not been authenticated. |
| Authentication | The authentication mode and priority when multiple modes are selected, which can be any one of the following:<br>• **chap**—Uses the Challenge Handshake Authentication Protocol (CHAP) for authentication. Must be followed by a priority value, which can be any value between 0 and 1000 with a lower number indicating higher preference. This protocol is enabled by default and commands the highest priority.<br>• **mschap**—Uses the Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) for authentication. Must be followed by a priority value, which can be any value between 0 and 1000 with a lower number indicating higher preference. This protocol is disabled by default.<br>• **pap**—Uses Password Authentication Protocol (PAP) for authentication. Must be followed by a priority value, which can be any value between 0 and 1000 with a lower number indicating higher preference. This protocol seconds CHAP in terms of priority. This protocol is enabled by default. |

## Viewing the QoS Configuration Details

To view the Quality of Service configuration details for a PDSN service:

**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 > PDSN >** *PDSN service* **> QoS.** The details are displayed in the content pane.

Table 26-59 displays the QoS configuration details.

*Table 26-59 QoS Configuration Details*

| Field | Description |
|---|---|
| Policy Mismatch | Indicates whether the PDSN must raise a Traffic FLow Template (TFT) violation if there is a policy mismatch of QoS. |
| Qos Wait | Indicates whether parameters related to QoS are enabled.<br>**Note** While configuring parameters for QoS, the minimum and maximum waiting time for transmission are also specified. Also, the action to be performed when the minimum time elapses is also specified. |
| Associate | The unique identification number of the associated QoS Profile that is configured for the selected context. |
| **QoS Profile tab** | |
| ID | The unique code of the QoS profile. |
| Description | The description of the QoS profile. |
| Uplink Bandwidth | The uplink bandwidth (in kbps) of your profile. |
| Downlink Bandwidth | The downlink bandwidth (in kbps) of your profile. |
| Latency | The latency (in milliseconds) of the profile. |
| Drop Rate | The maximum drop rate percent of the packet. |
| QoS Class | The type of QoS class associated with the profile. |

## Viewing the Registration Details

To view the Registration details for a PDSN service:

**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 > PDSN >** *PDSN service* **> Registrations.** The details are displayed in the content pane.

Table 26-60 displays the Registration details.

*Table 26-60 Registration Details*

| Field | Description |
|---|---|
| Accept Session Disconnect In Progress | Indicates whether A11 registration request messages must be accepted from the PCF when a session disconnection is in progress. |
| Ask Deny Terminate Session on Error | Indicates whether A11 sessions must be terminated when a registration acknowledgement is received from PCF with an error status. |
| Max Deny Reply Limit | Maximum number of retries for an erroneous registration request message from PCF, before PDSN terminates the session. |
| Deny Mismatched COA Address | Indicates whether RP Requests must be denied, when the Care of Address field does not match the source address of the requests. |
| Deny New Call Connection Setup Record Absent | Indicates whether new calls that do not have airlink connection setup record in the RRQ must be denied. |
| Deny New Call Connection Setup Record Absent Deny Code | The reason for denying new calls that do not have airlink connection setup record in RRQ. |
| Deny New Call Connection Reverse Tunnel Unavailable | Indicates whether new calls whose GRE key is the same as that of another user must be denied. |
| Deny Session Already Active | Indicates whether renew requests that have Airlink Start record for already active R-P sessions must be denied. |
| Deny Session Already Closed | Indicates whether renew and de registration requests for closed R-P sessions must be denied. |
| Deny Session Already Dormant | Indicates whether renew requests that have Airlink Start record for already dormant R-P sessions must be renewed. |
| Deny Terminate Session On Error | Indicates whether termination of session on receipt of erroneous registration request message must be denied. |
| Deny Use Zero GRE Key | Indicates whether the GRE key must be initialized to 0 when denying a new R-P session. |
| Discard Bad Extension | Indicates whether A11 registration request messages containing bad extensions must be discarded. |
| Discard GRE Key Change | Indicates whether A11 registration request messages for an existing A11 session that contain a different GRE key must be discarded. |
| Update Wait Timeout | The time taken (in seconds) by A11 RRQ for QoS changes. |

## Viewing the Timers and Restrictions Details

To view the Timers and Restrictions details for a PDSN service:

**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 > PDSN** > *PDSN service* > **Timers and Restrictions.** The details are displayed in the content pane.

Table 26-61 displays the Timers and Restrictions details.

***Table 26-61 Timers and Restrictions Details***

| Field | Description |
|---|---|
| Inter PDSN Handoff | Indicates whether the Inter-PDSN handoff feature off is enabled. Inter-PDSN handoff relates to the handoff between two PCFs with connectivity to different PDSNs.<br><br>**Note** Inter-PDSN handoff can be of two types: Fast Handoff and Dormant Handoff. Fast Handoff uses a GRE tunnel between two PDSNs to transport user data for a single service instance. Dormant Handoff occurs when a mobile station with a dormant packet session determines that it has crossed a packet zone boundary. |
| Inter PDSN Handover Use CANIDPANID | Indicates whether usage of Current Access Network ID (CANID) or Previous Access Network ID (PAN) is supported during an Inter-PDSN handover. |
| Data Available Indicator | Indicates whether data transfer is available. |
| PMA Capability Indicator | The Proxy Mobile Agent capability (PMA) indicator, which determines whether PMIP is supported by Prime Network.<br><br>**Note** PDSN sends the capability indicator through RADIUS to the AAA server as an access-request packet to indicate to the AAA server that PDSN supports PMIP. If the capability indicator attribute is missing, then PMIP is not supported by PDSN. |
| Direct LTE Indicator | Indicates whether PDSN can send Direct LTE indicator in the Access Request. |
| Data Over Signalling | Indicates whether data transfer over a10 signalling channel instead of bearer or subscriber channels from PCF or PDSN is allowed. By default, this feature is not allowed. |
| Dormant Transition | Indicates whether dormant transition of the RP link during the initial setup of the subscriber session is allowed. If this option is disabled, then the subscriber session will be disconnected if the RP link becomes dormant during the initial setup. |
| ROHC IP Header Compression | Indicates whether the Robust Header Compression (ROHC) is enabled for headers in the IP packets that are being sent by or sent to the PDSN. By default, this option is disabled. |
| Always On Indication | Indicates whether the Always On feature is enabled for a subscriber.<br><br>**Note** When the idle-time out limit runs out for a subscriber, the IP/PPP session remains connected as long as the subscriber is reachable. By default, this feature is disabled. |

*Table 26-61 Timers and Restrictions Details (continued)*

| Field | Description |
|---|---|
| Setup TimeOut | The maximum time (in seconds) allowed for a session to be setup between PCF and PDSN. This time can be any value between 1 and 1000000, and defaults to 60 seconds. |
| Retransmission TimeOut | The timeout period (in seconds) for retransmission of RP control packets. This time can be any value between 1 and 1000000 and defaults to 3 seconds. |
| Pdsn Type0 Tft | Indicates whether Traffic Flow Template (TFT) of the PDSN is changed from type 0 TFT to type 1 TFT. |
| Tft Validation TimeOut | The TFT validation timeout (in seconds) for QoS changes. This time can be any value between 1 and 100000, and defaults to 0. |
| Access Flow Traffic Violations | The number of violations that are permitted in the access flow traffic. |
| Access Flow Traffic Violations Interval | The time interval between two subsequent access flow traffic violations. |

## Configuration Commands for PDSN

The PDSN commands allow you to configure PDSNs in your network. Please note that these commands are available only for Cisco ASR 5000 Mobile devices.

These commands can be launched from the logical inventory by choosing the **Context > Commands > Configuration** or **Context > Commands > Show**.

Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands.

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

**Note** In the GUI, parameters that are displayed in bold text are mandatory.

Table 26-62 lists the PDSN configuration commands.

*Table 26-62 PDSN Configuration Commands*

| Command | Navigation | Description |
|---|---|---|
| Create PDSN | *Right-click on a context* > **Commands** > **Configuration** | Use this command to create a new PDSN service for the selected context. |
| Modify PDSN<br>Delete PDSN | Expand **PDSN** node > *right-click PDSN service* > **Commands** > **Configuration** | Use these commands to modify/delete an existing PDSN service configured for the selected context. |
| Show PDSN | Expand **PDSN** node > *right-click PDSN service* > **Commands** > **Show** | Use this command to view and confirm the PDSN service configuration details. |
| Modify GRE | Expand **PDSN** node > *PDSN service* > *right-click* **GRE** > **Commands** > **Configuration** | Use this command to modify the Generic Routing Encapsulation (GRE) configuration settings for a specified PDSN service. |
| Modify IP Source Violation | Expand **PDSN** node > *PDSN service* > *right-click* **IP Source Violation** > **Commands** > **Configuration** | Use this command to modify the IP Source Violation configuration details for the specified PDSN service. |
| Modify MSID | Expand **PDSN** node > *PDSN service* > *right-click* **MSID** > **Commands** > **Configuration** | Use this command to modify the mobile station ID (MSID) configuration details for the specified PDSN service. |
| Modify PCF Parameters | Expand **PDSN** node > *PDSN service* > *right-click* **PCF** > **Commands** > **Configuration** | Use this command to modify the Packet Control Function (PCF) configuration details for the specified PDSN service. |

*Table 26-62 PDSN Configuration Commands (continued)*

| Command | Navigation | Description |
|---|---|---|
| Create PCF Security Entry | Expand the **PDSN** node > *right-click PDSN service* > **Commands** > **Configuration** | Use this command to create a new PCF security entry. |
| Modify PCF Security Entry<br>Delete PCF Security Entry | Expand **PDSN** node > *PDSN service* > **PCF** > *Under* ***Security Profiles*** *tab n the content pane, right-click* ***SPI Number*** > **Commands** > **Configuration** | Use these commands to modify/delete the PCF security entry details. |
| Modify Policy | Expand **PDSN** node > *PDSN service* > *right-click* **Policy** > **Commands** > **Configuration** | Use this command to modify the policy configuration details for the PDSN service. |
| Modify PPP | Expand **PDSN** node > *PDSN service* > *right-click* **PPP**> **Commands** > **Configuration** | Use this command to modify the Point-to-Point Protocol configuration details for the selected PDSN service. |
| Modify Registrations | Expand **PDSN** node > *PDSN service* > *right-click* **Registrations** > **Commands** > **Configuration** | Use this command to modify the registration details for the selected PDSN service. |
| Modify Timers and Registrations | Expand **PDSN** node > *PDSN service* > *right-click* **Timers and Registrations** > **Commands** > **Configuration** | Use this command to modify the timers and registration details for the selected PDSN service. |

# Viewing the Local Mobility Anchor Configuration

Proxy Mobile IPv6 (or PMIPv6, or PMIP) is a network-based mobility management protocol for building a common access technology independent of mobile core networks, accommodating various access technologies such as WiMAX, 3GPP, 3GPP2 and WLAN based access architectures.

The PMIPv6 provides network-based IP Mobility management to a mobile node, without requiring the participation of the MN in any IP mobility-related signaling. The mobility entities in the network track the movements of the MN, initiate the mobility signaling, and set up the required routing state.

The major functional entities of PMIPv6 are Mobile Access Gateways (MAGs), Local Mobility Anchors (LMAs), and Mobile Nodes (MNs).

The Local Mobility Anchor (LMA) is the home agent for a mobile node in a Proxy Mobile IPv6 (PMIPv6) domain. It is the topological anchor point for mobile node home network prefixes and manages the binding state of an mobile node. An LMA has the functional capabilities of a home agent as defined in the Mobile IPv6 base specification (RFC 3775) along with the capabilities required for supporting the PMIPv6 protocol.

To view the LMA configuration details:

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

**Step 2** In the logical inventory window, choose **Logical Inventory >** *Context* **> Mobile > LMA.** The list of LMA services configured in Prime Network is displayed in the content pane.

**Step 3** From the **LMA** node, choose an LMA service. The LMA service details are displayed in the content pane as shown in Figure 26-17.

***Figure 26-17 LMA Service Details***

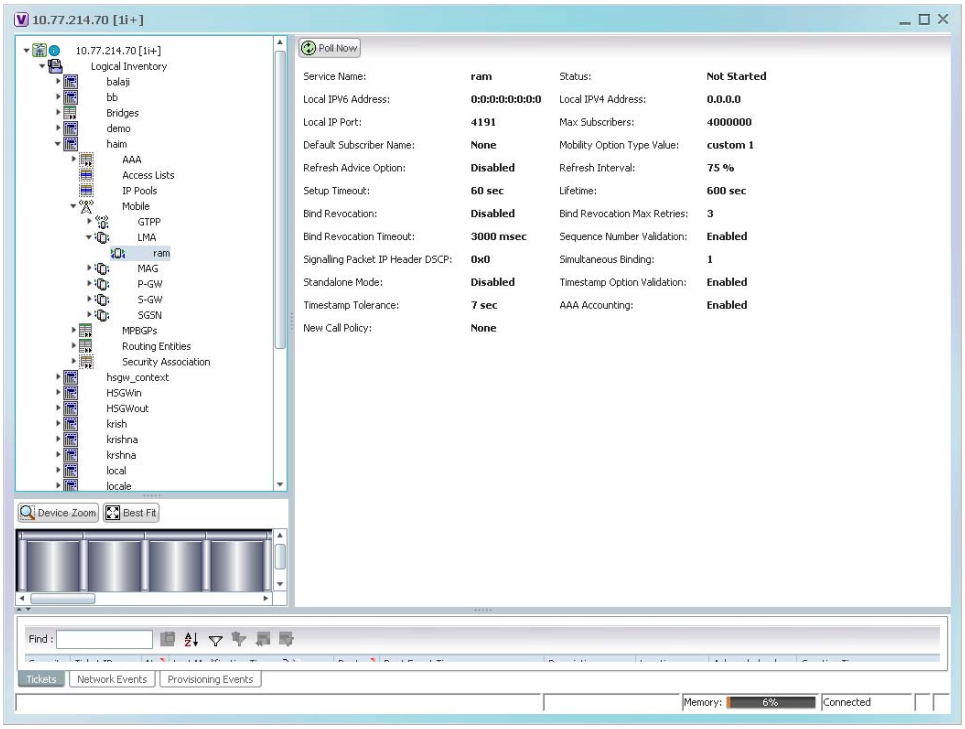



Table 26-63 displays the LMA service details.

*Table 26-63 LMA Service Details*

| Field | Description |
|---|---|
| Service Name | The unique service name of the LMA. |
| Status | The status of the LMA service, which can be any one of the following:<br>• Down<br>• Running<br>• Initiated<br>• Unknown.<br>This field defaults to **Down**. |
| Local IPv6 Address | The IP address of the interface serving as S2a (that is connected to HSGW) or S5/S8 (that is connected to S-GW) interface. |
| Local IPv4 Address | The IP address of the interface connected to HA/P-GW. |
| Local IP Port | The User Datagram Protocol (UDP) port for the LMA service. |
| Max Subscribers | The maximum number of subscribers that the LMA service can support. This number can be any value between 0 and 3000000. |
| Default Subscriber Name | The name of the subscriber template to be used for subscribers who are using this domain alias. |
| Mobility Option Type Value | The mobility option type used in mobility messages, which can be any one of the following:<br>• Custom 1<br>• Custom 2<br>• Standard |
| Refresh Advice Option | Indicates whether refresh advice option must be included in the Binding Acknowledgement sent by the LMA service. By default, this option is disabled. |
| Refresh Interval | The percent of granted lifetime to be used in the Refresh Interval Mobility option pertaining to the Binding Acknowledgement sent by the LMA service. This percentage can be any value between 1 and 99 and defaults to 75. |
| Setup Timeout | The maximum time (in seconds) allowed for the session to setup. This field defaults to 60. |
| Lifetime | The registration lifetime (in seconds) of the mobile IPv6 session. This number can be any value between 1 and 262140. |
| Bind Revocation | Indicates whether the binding revocation support is available for the LMA service. By default, this option is disabled. |
| Bind Revocation Max Retries | The maximum number of retries for the binding revocation, which can be any value between 1 and 10. This field defaults to 3. |
| Bind Revocation Timeout | The time interval (in milliseconds) of the retransmission of the binding revocation, which can be any value between 500 and 10000. This field defaults to 3000. |
| Sequence Number Validation | Indicates whether the sequence number of the MIPv6 control packet received by the LMA service must be validated. This option is enabled by default. |

*Table 26-63 LMA Service Details (continued)*

| Field | Description |
|---|---|
| Signalling Packet IP Header DSCP | The Differentiated Services Code Point (DSCP) marking that is applicable to the IP header that is carrying outgoing signalling packets. |
| Simultaneous Binding | The maximum number of Care of addresses that can be bound for the same user as identified by their Network Access Identifier (NAI) and home address. This can be any value ranging from 1 to 3. This field defaults to 1. |
| Standalone Mode | Indicates whether the LMA service can be started in the standalone mode. This option is disabled by default. |
| Timestamp Option Validation | Indicates whether the Timestamp option in the Binding Acknowledgement must be validated. This option is disabled by default. |
| Timestamp Tolerance | The time (in seconds) to validate Timestamp reply protection, which can be any value between 0 and 65535. This field defaults to 7 seconds. |
| AAA Accounting | Indicates whether the AAA Accounting information for subscriber sessions must be sent. This option is enabled by default. |
| New Call Policy | Indicates whether the new call policy must be accepted or rejected. By default, this field is set to **None**. |

# Viewing Operator Policies, APN Remaps, and APN Profiles

Operator policy provides mechanisms to fine tune the behavior of subsets of subscribers above and beyond the behaviors described in the user profile. It can also be used to control the behavior of visiting subscribers in roaming scenarios, enforcing roaming agreements, and providing a measure of local protection against foreign subscribers.

An operator policy associates APNs, APN profiles, an APN remap table, and a call-control profile to ranges of International Mobile Subscriber Identities (IMSIs). These profiles and tables are created and defined within their own configuration modes to generate sets of rules and instructions that can be reused and assigned to multiple policies. In this manner, an operator policy manages the application of rules governing the services, facilities, and privileges available to subscribers. These policies can override standard behaviors and provide mechanisms for an operator to get around the limitations of other infrastructure elements, such as DNS servers and HSSs.

**Note** Operator policies and APN profiles are applicable only for the ‘local’ context in the logical inventory.

The following topics explain how to view operator policies, APN remaps, and APN profiles in Prime Network Vision:

- Viewing Operator Policies, page 26-106
- Viewing APN Remaps, page 26-108
- Viewing APN Profiles, page 26-110

# Viewing Operator Policies

Operator policies provide an operator with a range of control to manage the services, facilities, and privileges available to subscribers. By configuring the various components of an operator policy, the operator fine tunes any desired restrictions or limitations needed to control call handling and this can be done for a group of callers within a defined IMSI range or per subscriber.

Besides enhancing operator control through configuration, the operator policy feature minimizes configuration by drastically reducing the number of configuration lines needed. Operator policy maximizes configurations by breaking them into the following reusable components that can be shared across IMSI ranges or subscribers:

- Call-control profiles
- IMEI profiles (SGSN only)
- APN profiles
- APN remap tables
- Operator policies
- IMSI ranges

To view operator policies in logical inventory:

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

**Step 2** In the logical inventory window, choose **Logical Inventory > *local* > Mobile > Policy > Operator Policies**

Prime Network Vision displays the list of operator policies configured under the container. You can view the individual policy details from the table on the right pane or by choosing **Logical Inventory > *local* > Mobile > Policy > Operator Policies >** *Policy*.

Table 26-64 describes the details available for each operator policy.

If an operator policy is configured with IMEI ranges and APN entries, the details are displayed in the respective tabs IMEI Ranges and APN Entries on the content pane.

*Table 26-64 Operator Policies in Logical Inventory*

| Field | Description |
|---|---|
| Name | Name of the operator policy. |
| Description | Description of the operator policy. |
| Call Control Profile Name | Name of the call control profile associated with the operator policy. |
| Call Control Validity | Indicates whether the call control profile name associated with the operator policy is valid or is not created yet (invalid). |
| APN Remap Table Name | Name of the APN remap table associated with the operator policy. |
| APN Remap Table Validity | Indicates whether the APN remap table name associated with the operator policy is valid or is not created yet (invalid). |
| Default APN Profile Name | Name of the default APN profile associated with the operator policy. |
| Default APN Profile Validity | Indicates whether the default APN profile name associated with the operator policy is valid or is not created yet (invalid). |
| **IMEI Ranges** | |
| Start Range | The starting number in the range of IMEI profiles. |
| To Range | The ending number in the range of IMEI profiles. |
| Software Version | Software version to fine tune the IMEI definition. |
| Profile Name | Name of the IMEI profile associated with the IMEI range. Displays ‘None’, if no profile is associated with the range. |
| Validity | Validity of the IMEI profile. |
| **APN Entries** | |
| NI | APN network identifier. |
| NI APN Profile | Name of the APN profile associated with the network identifier. An APN profile groups a set of APN-specific parameters that may be applicable to one or more APNs. When a subscriber requests an APN that has been identified in a selected operator policy, the parameter values configured in the associated APN profile are applied. |
| NI APN Profile Validity | Indicates whether the NI APN profile associated with the operator policy is valid or is not created yet (invalid). |
| OI | APN operator identifier. |
| OI APN Profile | Name of the APN profile associated with the operator identifier. An APN profile groups a set of APN-specific parameters that may be applicable to one or more APNs. When a subscriber requests an APN that has been identified in a selected operator policy, the parameter values configured in the associated APN profile are applied. |
| OI APN Profile | Indicates whether the OI APN profile associated with the operator policy is valid or is not created yet (invalid). |

# Viewing APN Remaps

An APN remap tables allow an operator to override an APN specified by a user, or the APN selected during the normal APN selection procedure, as specified by 3GPP TS 23.060. This level of control enables operators to deal with situations such as:

- An APN is provided in the activation request that does not match with any of the subscribed APNs; either a different APN was entered or the APN could have been misspelled. In such situations, the SGSN rejects the activation request. It is possible to correct the APN, creating a valid name so that the activation request is not rejected.
- In some cases, an operator might want to force certain devices or users to use a specific APN. For example, a set of mobile users may need to be directed to a specific APN. In such situations, the operator needs to override the selected APN.

An APN remap table group is a set of APN-handling configurations that may be applicable to one or more subscribers. When a subscriber requests an APN that has been identified in a selected operator policy, the parameter values configured in the associated APN remap table are applied. For example, an APN remap table allows configuration of the following:

- APN aliasing—Maps incoming APN to a different APN, based on partial string match (MME and SGSN) or matching charging characteristic (SGSN only).
- Wildcard APN—Allows APN to be provided by the SGSN, when wildcard subscription is present and the user has not requested an APN.
- Default APN—Allows a configured default APN to be used, when the requested APN cannot be used.

APN remap tables are configured with commands in the APN Remap Table configuration mode. A single APN remap table can be associated with multiple operator policies, but an operator policy can only be associated with a single APN remap table.

To view APN remap properties in logical inventory:

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

**Step 2** In the logical inventory window, choose **Logical Inventory > *local* > Mobile > > Profile > APN Remaps**

Prime Network Vision displays the list of APN remaps configured under the container. You can view the individual APN remap details from the table on the right pane or by choosing **Logical Inventory > *local* > Mobile > Profile > APN Remaps >** *APN Remap*.

Table 26-65 describes the details available for each APN remap.

If an APN remap is configured with charging characteristics and NI and OI entries, the details are displayed in the respective tabs Charging Characteristics and Network And Operator Identifier Entries on the content pane.

***Table 26-65 APN Remap Properties in Logical Inventory***

| Field | Description |
|---|---|
| Name | Name of the APN remap. |
| Description | Description of the APN remap. |
| APN When No APN Requested | APN network identifier that will be used when no APN is requested. |

*Table 26-65 APN Remap Properties in Logical Inventory (continued)*

| Field | Description |
|---|---|
| Wildcard APN for IPv4 | Wildcard APN included in the subscriber record, with PDP type as IPv4 context. |
| Wildcard APN for IPv6 | Wildcard APN included in the subscriber record, with PDP type as IPv6 context. |
| Wildcard APN for IPv4v6 | Wildcard APN included in the subscriber record, with PDP type as both IPv4 and IPv6 contexts. |
| Wildcard APN for PPP | Wildcard APN included in the subscriber record, with PDP type as PPP context. |
| **Charging Characteristics** | |
| Profile Index | Profile index in charging characteristics. |
| Behavior Bit Value | Behavior bit in charging characteristics. |
| APN For Overriding | Name of the APN profile that the charging characteristic attributes must be applied to, to generate CDRs. |
| **Network And Operator Identifier Entries** | |
| Requested NI | The old network identifier that is being mapped for replacement. |
| Mapped to NI | The new network identifier. |
| NI Wildcard Replace String | When a wildcard character is included in the old APN network identifier, this parameter identifies the information to replace the wildcard in the new APN network identifier. |
| Requested OI | The old operator identifier that is being mapped for replacement. |
| Mapped to OI | The new operator identifier. |
| OI MNC Replace String | When a wildcard character is included in the MNC portion of the old APN operator identifier, this parameter identifies the information to replace the wildcard in the new APN operator identifier. |
| OI MCC Replace String | When a wildcard character is included in the MCC portion of the old APN operator identifier, this parameter identifies the information to replace the wildcard in the new APN operator identifier. |

**Step 3** If a default APN is configured for the remap, click the **Default APN** node under the APN remap. You can view the following details on the content pane.

*Table 26-66 Default APN Properties in Logical Inventory*

| Field | Description |
|---|---|
| Default APN Name | Name of the default APN. |
| Use Default APN When No APN is Requested | Indicates whether the configured default APN can be used or not, if there is no APN in the request. |
| Use Default APN When DNS Query Fails | Indicates whether the configured default APN can be used or not, if DNS query fails. |
| Fallback APN to Use | A fallback APN to be used when the configured default APN is not present in the subscription, so that activation does not fail. |
| Fallback APN in First Subscription | Indicates whether APN from the first subscription record must be used, when the configured default APN is not available. |
| Use APN From Single Subscription Record | Indicates whether APN from the subscription record must be used, if it is the only record available and the normal APN selection fails. |

# Viewing APN Profiles

APN Profile defines a set of parameters controlling the SGSN or MME behavior, when a specific APN is received or no APN is received in a request. An APN profile is a key element in the Operator Policy feature. An APN profile is not used or valid unless it is associated with an APN and this association is specified in an operator policy.

Essentially, an APN profile is a template which groups a set of APN-specific commands that may be applicable to one or more APNs. When a subscriber requests an APN that has been identified in a selected operator policy, then the set of commands in the associated APN profile will be applied. The same APN profile can be associated with multiple APNs and multiple operator policies.

An APN profile groups a set of APN-specific parameters that may be applicable to one or more APNs. When a subscriber requests an APN that has been identified in a selected operator policy, the parameter values configured in the associated APN profile are applied. For example:

- Enable or disable a direct tunnel (DT) per APN (SGSN).
- Define charging characters for calls associated with a specific APN.
- Identify a specific GGSN to be used for calls associated with a specific APN (SGSN).
- Define various quality of service (QoS) parameters to be applied to calls associated with a specific APN.
- Restrict or allow PDP context activation on the basis of access type for calls associated with a specific APN.

A single APN profile can be associated with multiple operator policies.

To view APN profile properties in logical inventory:

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

**Step 2** In the logical inventory window, choose **Logical Inventory > *local* > Mobile > Profile > APN Profiles.**

Prime Network Vision displays the list of APN profiles configured under the container. You can view the individual APN profile details from the table on the right pane or by choosing **Logical Inventory > *local* > Mobile > Profile > APN Profiles >** *APN Profile*.

Table 26-67 describes the details available for each APN remap.

If additional properties are configured for the APN profile, you can click the respective tabs on the content pane to view the details:

- Gateway Entries
- RANAP ARP Entries
- QoS Class Entries
- Uplink Traffic Policing Entries/Downlink Traffic Policing Entries

***Table 26-67 APN Profile Properties in Logical Inventory***

| Field | Description |
|---|---|
| Name | Name of the APN profile. |
| Description | Description of the APN profile. |
| QoS Service Capping Prefer Type | Operational preferences for QoS parameters, specifically QoS bit rates. Value could be one of the following:<br>• both-hlr-and-local—Instructs the SGSN to use the locally configured QoS or HLR subscription.<br>• hlr-subscription—Instructs the SGSN to use QoS bit rate from HLR configuration and use the same for session establishment.<br>• local—Instructs the SGSN to use the locally configured QoS bit rate and use the same for session establishment. |
| Address Resolution Mode | Address resolution mode of the APN profile, which could be one of the following:<br>• fallback-for-dns—Uses DNS query for address resolution.<br>• local—Uses locally configured address. |
| CC Preferred Source | Charging characteristic settings to be used for S-CDRs, which could be one of the following:<br>• hlr-value-for-scdrs—Instructs the system to use charging characteristic settings received from the HLR for S-CDRs.<br>• local-value-for-scdrs—Instructs the profile preference to use only locally configured/stored charging characteristic settings for S-CDRs. |
| CC Local SCDR Behavior Bit | Value of the behavior bit for the charging characteristics for S-CDRs. |
| CC Local SCDR Behavior Profile Index | Value of the profile index for the charging characteristics for S-CDRs. |
| GGSN Algorithm Applicable | Selection algorithm for GGSNs. This parameter allows the operator to configure multiple GGSN pools by assigning the GGSN to a secondary pool of GGSNs. |

*Table 26-67 APN Profile Properties in Logical Inventory (continued)*

| Field | Description |
|---|---|
| IP Source Validation | Configures settings related to IP source violation detection with one of the following criteria:<br>• deactivate—Deactivates the PDP context with one of the following conditions:<br>– Deactivates all PDP contexts of the MS/UE. Default is to deactivate errant PDP contexts.<br>– Excludes packets having an invalid source IP address from the statistics used in the accounting records.<br>– Deactivates all assosiated PDP contexts (primary/secondary). Default is to deactivate errant PDP contexts.<br>– Configures maximum number of allowed IP source violations before the session is deactivated.<br>• discard—Discards errant packets and excludes packets having an invalid source IP address from the statistics used in the accounting records.<br>• ignore—Ignores checking of packets for MS/UE IP source violation. |
| IP Source Validation Tolerance Limit | Maximum number of allowed IP source violations before the session is deactivated. |
| Direct Tunnel | Permission for direct tunnel establishment by GGSNs, which could be not-permitted-by-ggsn or remove. |
| Private Extension LORC IE to GGSN | Indicates whether GTPC private extension is enabled or not for the over charging protection feature of the GGSN. |
| Private Extension LORC IE to SGSN | Indicates whether GTPC private extension is enabled or not for the over charging protection feature of the SGSN. |
| Idle Mode Access Control List IPV4 | Group of IPv4 Access Control Lists (ACLs) that define rules to apply to downlink data destined for UEs in an idle mode. |
| Idle Mode Access Control List IPV6 | Group of IPv6 ACLs that define rules to apply to downlink data destined for UEs in an idle mode. |
| DNS Query with MSISDN Start Offset Position | The position of the first digit in the MSISDN to start an offset and create a new APN DNS query string that is intended to assist roaming subscribers to use the local GGSN. |
| DNS Query with MSISDN End Offset Position | The position of the last digit in the MSISDN to be part of the offset. |
| DNS Query with LAC or RAC | Indicates whether geographical information must be appended to the APN string that is sent to the DNS query or not. This information is used during the DNS query process to select the geographically closest GGSN. |
| DNS Query with RNC ID | Indicates whether the SGSN must include the ID of the calling RNC in the APN DNS query string or not. |
| DNS Query with Charging Characteristics | Indicates whether charging characteristic configuration is enabled for the APN profile or not. |

*Table 26-67 APN Profile Properties in Logical Inventory (continued)*

| Field | Description |
|---|---|
| DNS Query Charging Characteristics ID Format | Format of the charging characteristic information to be included. |
| **Gateway Entries** | |
| Gateway Entry | Gateway entry configured for the APN profile. |
| IP Address | IPv4 or IPv6 addresses of the gateway configured. |
| Priority | Priority of the gateway to consider during address selection. |
| Weight | Weightage or importance assigned to the gateway for load balancing. |
| Pool | Gateway pool assigned. |
| Gateway Type | Type of gateway configured, which could be GGSN or P-GW. |
| **RANAP ARP Entries** | |
| Traffic Class | Traffic class of the Radio Access Network Application Part (RANAP) configuration. |
| Subscription Priority | Subscription priority of the traffic class; the lowest number denoting the highest priority. |
| Priority Level | Priority level for the subscription priority. |
| Preemption Capability | Preemption capability value of the traffic class. |
| Preemption Vulnerability | Preemption vulnerability value of the traffic class. |
| Queuing Allowed | Indicates whether queuing is allowed for the traffic class or not. |
| **QoS Class Entries** | |
| Class Name | Traffing class of the QoS configuration. |
| Service Delivery Unit Delivery Order | Indicates whether bearer should provide in-sequence delivery of service data units (SDUs) or not. |
| Delivery of Erroneous Service Delivery Units | Indicates whether SDUs detected as erroneous should be delivered or discarded. |
| Max Bit Rate Uplink | Maximum bit rate, in kbps, allowed for uplink between MS and the core network. |
| Max Bit Rate Downlink | Maximum bit rate, in kbps, allowed for downlink between MS and the core network. |
| Allocation Retention Priority | Relative importance compared to other Radio Access Bearers (RABs) for allocation and retention of the RAB. |
| Traffic Handling Priority | Relative importance for traffic handling when compared to other RABs. |
| SDU Max Size | Maximum allowed SDU size, in bytes. |
| SDU Error Ratio | Fraction of SDUs lost or detected as erroneous. |
| Guaranteed Bit Rate Uplink | Uplink bit rate, in kbps, that is assured for a given RAB between MS and the core network. |
| Guaranteed Bit Rate Downlink | Downlink bit rate, in kbps, that is assured for a given RAB between MS and the core network. |

*Table 26-67 APN Profile Properties in Logical Inventory (continued)*

| Field | Description |
|---|---|
| Minimum Transfer Delay | Minimum transfer delay, in milliseconds. |
| Residual BER | Undetected bit error ratio (BER) in the delivered SDUs. |
| MBR Map Down | Attribute that maps or converts the received HLR maximum bit rate (MBR) (from value) to a locally configured downlink MBR value (to value). |
| MBR Map Up | Attribute that maps or converts the received HLR MBR (from value) to a locally configured uplink MBR value (to value). |
| **Uplink Traffic Policing Entries/Downlink Traffic Policing Entries** | |
| Traffic Class | Traffic class of the QoS configuration. |
| Burst Size Auto Readjust | Indicates whether the auto readjustment of burst size is enabled or disabled. This parameter is used in dynamic burst size calculation, for traffic policing, at the time of PDP activation or modification. |
| Burst Size Auto Readjust Duration | The burst size readjustment duration in seconds. This parameter indicates the number of seconds that the dynamic burst size calculation will last for. This allows the traffic to be throttled at the negotiated rates. |
| Peak Burst Size (bytes) | The peak burst size allowed, in bytes, for the uplink/downlink direction and QoS class. |
| Guaranteed Burst Size (bytes) | The guaranteed burst size allowed, in bytes, for the uplink/downlink direction and QoS class. |
| Exceed Action | The action to be taken on packets that exceed the committed data rate, but do not violate the peak data rate. The action could be one of the following:<br>• Drop<br>• Lower IP Precedence<br>• Transmit |
| Violate Action | The action to be taken on packets that exceed both committed and peak data rates. The action could be one of the following:<br>• Drop<br>• Lower IP Precedence<br>• Shape<br>• Transmit |

## Viewing Additional Characteristics of an APN Profile

To view additional characteristics of an APN profile:

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

**Step 2** In the logical inventory window, choose **Logical Inventory > *local* > Mobile > Profile > APN Profiles >** *APN Profile*.

**Step 3** Expand the *APN Profile* node. The following list of characteristics configured for the APN profile are displayed:

- PDP Inactivity Actions—Attributes related to PDP data inactivity. Once a data communication is in progress there are cases where this data communication can be inactive after some time, for example, when the user has locked the phone after browsing the internet or when the battery suddenly drains out. In such a case, the SGSN can take a configured action based on this inactivity. The inactivity timeout and the actions that can be taken based on certain conditions are modeled in this configuration.
- QoS to DSCP Mapping (Downlink) / Qos to DSCP Mapping (Uplink)—Mapping of QoS parameters to DSCP. Configuration of the local values for the traffic class (TC) parameters for QoS configured for the APN.
- PDP Restrictions (UMTS) / PDP Restrictions (GPRS)—Activation restrictions on PDP.

**Step 4** Click each of one of these characteristics to view its properties on the right pane. See Table 26-68 for more details on the properties of each characteristics configured for the APN profile.

***Table 26-68 APN Profile Additional Characteristics***

| Field | Description |
|---|---|
| **PDP Inactivity Actions** | |
| PDP Inactivity Idle Timeout | Timeout duration for PDP inactivity. PDP context is deactivated, if it is inactive for the given duration. |
| PDP Inactivity Idle Timeout Action | Action to be taken when the PDP data communication is inactive for the timeout duration. |
| PDP Inactivity Idle Timeout Action Condition | Condition when the GPRS detach procedure should be executed on the PDP context, when the timeout is reached or exceeded. |
| PDP IPV4 IPV6 Override | PDP type to use, per APN, if dual PDP type addressing is not supported by the network. |
| **QoS to DSCP Mapping (Downlink) / Qos to DSCP Mapping (Uplink)** | |
| Conversational | Real time conversational traffic class of service, which is reserved for voice traffic. |
| Streaming | Streaming traffic class of service, which handes one-way, real-time data transmission, such as streaming video or audio. |
| Interactive Threshold Priority 1/2/3 | Interactive traffic class of service with threshold priorities 1, 2, and 3. |
| Background | Background traffic class of service. This best-effort class manages traffic that is handled as a background function, such as e-mail, where time to delivery is not a key factor. |
| Interactive TP1 Alloc P1/P2/P3 | Interactive traffic class of service, with threshold priority 1 and allocation priorities 1, 2, and 3. |
| Interactive TP2 Alloc P1/P2/P3 | Interactive traffic class of service, with threshold priority 2 and allocation priorities 1, 2, and 3. |
| Interactive TP3 Alloc P1/P2/P3 | Interactive traffic class of service, with threshold priority 3 and allocation priorities 1, 2, and 3. |
| **PDP Restrictions (UMTS) / PDP Restrictions (GPRS)** | |

*Table 26-68 APN Profile Additional Characteristics (continued)*

| Field | Description |
|---|---|
| QoS Class Background | Indicates whether background traffic class of service is enabled or not. |
| QoS Class Interactive | Indicates whether interactive traffic class of service is enabled or not. |
| QoS Class Streaming | Indicates whether streaming traffic class of service is enabled or not. |
| QoS Class Conversational | Indicates whether conversational traffic class of service is enabled or not. |

# Working with Active Charging Service

Enhanced Charging Service (ECS), also known as Active Charging Service (ACS), is an in-line service, which is integrated within the platform and provides mobile operators the ability to offer tiered, detailed, and itemized billing to subscribers. Data packets flow through the ECS subsystem and relevant actions are performed based on the configured rules. Charging records (xCDRs) will be generated and forwarded to ESS or billing systems for prepaid and post paid billing.

The major components and functions of an ECS solution are given below.

### Content Service Steering

Content Service Steering (CSS) enables directing selective subscriber traffic into the ECS subsystem. CSS uses Access Control Lists (ACLs) to redirect selective subscriber traffic flows. ACLs control the flow of packets into and out of the system. ACLs consist of rules (ACL rules) or filters that control the action taken on packets matching the filter criteria.

ACLs are configurable on a per-context basis and apply to a subscriber through either a subscriber profile (for PDSN) or an APN profile (for GGSN) in the destination context.

### Protocol Analyzer

Protocol analyzer stack is responsible for analyzing the individual protocol fields during packet inspection. The analyzer supports the following types of packet inspection:

- Shallow Packet Inspection—Inspection of the Layer 3 (IP header) and Layer 4 (for example, UDP or TCP header) information.
- Deep Packet Inspection—Inspection of Layer 7 and above information. This functionality includes:
  - Detection of Uniform Resource Identifier (URI) information at level 7 (example, HTTP)
  - Identification of true destination in the case of terminating proxies, where shallow packet inspection only reveals the destination IP address/port number of a terminating proxy

### Rule Definitions

Rule definitions (ruledefs) are user-defined expressions, based on protocol fields and protocol states, which define what actions to take when specific field values are true.

Most important rule definitions are related to Routing and Charging as explained below:

- Routing Ruledefs—Routing ruledefs are used to route packets to content analyzers. Routing ruledefs determine which content analyzer to route the packet to, when the protocol fields and/or protocol states in ruledef expression are true.

- Charging Ruledefs—Charging ruledefs are used to specify what action to take based on the analysis done by the content analyzers. Actions can include redirection, charge value, and billing record emission.

### Rule Base

A rule base is a collection of rule definitions and their associated billing policy. The rule base determines the action to be taken when a rule is matched. Rule bases can also be used to apply the same rule definitions for several subscribers, which eliminate the need to have unique rule definition for each subscriber. We can set priority, default bandwidth policy, type of billing for subscriber sessions, for a rule definition or group of rule definitions in the rule base.

### Content Filtering

ACS also offers a content filtering mechanism. Content filtering is an in-line service available for 3GPP and 3GPP2 networks to filter HTTP and WAP requests from mobile subscribers, based on the URLs in the requests. Content filtering uses the DPI feature of ECS to discern HTTP and WAP requests. This enables operators to filter and control the content that an individual subscriber can access, so that subscribers are inadvertently not exposed to universally unacceptable content and/or content inappropriate as per the subscribers' preferences.

The content filtering service offers the following solutions:

- URL Blacklisting—With this solution, all HTTP/WAP URLs in subscriber requests are matched against a database of blacklisted URLs. If there is a match, the flow is discarded, redirected, or terminated as configured. If there is no match, subscribers view the content as they would normally.
- Category-based Content Filtering
  - Category-based Static Content Filtering—In this method, all HTTP/WAP URLs in subscriber requests are matched against a static URL categorization database. Action is taken based on a URL's category, and the action configured for that category in the subscriber's content filtering policy. Possible actions include permitting, blocking, redirecting, and inserting content.
  - Category-based Static-and-Dynamic Content Filtering—In this method, each URL first undergoes static rating. If the URL cannot be rated by the static database or if the URL static rating categorizes a URL as either Dynamic or Unknown, the requested content is sent for dynamic rating; wherein the requested content is analyzed and categorized. Action is taken based on the category determined by dynamic rating, and the action configured for that category in the subscriber's content filtering policy. Possible actions include permitting, blocking, redirecting, and inserting content.

**Note** ACS is applicable only for the 'local' context in the logical inventory.

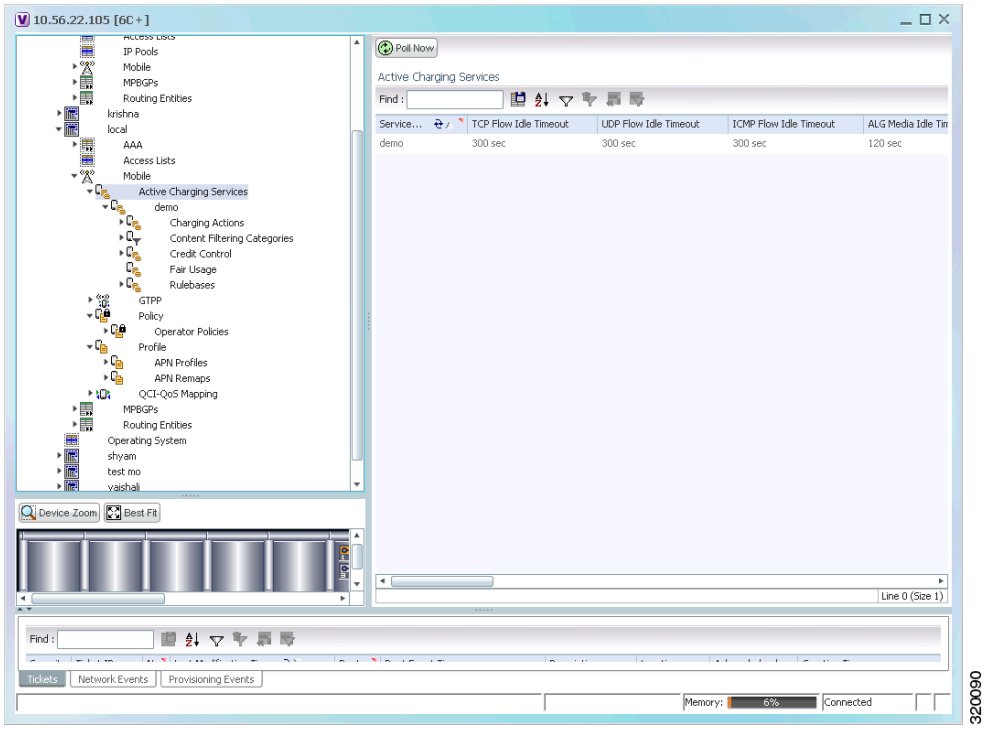
The following topics explain how to work with ACS in Prime Network Vision:

- Viewing Active Charging Services, page 26-118
- ACS Commands, page 26-131

# Viewing Active Charging Services

You can view the active charging services in logical inventory as shown in Figure 26-18.

***Figure 26-18 Mobile Technology Setup Nodes***




Additionally, you can also perform the following for each ACS:

- Viewing Content Filtering Categories, page 26-120
- Viewing Credit Control Properties, page 26-120
- Viewing Charging Action Properties
- Viewing Rule Definitions
- Viewing Rule Base for the Charging Action
- Viewing Bandwidth Policies
- Viewing Fair Usage Properties

To view ACS details in logical inventory:

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

**Step 2** In the logical inventory window, choose **Logical Inventory > *local* > Mobile > Active Charging Services**.

Prime Network Vision displays the list of active charging services configured under the container. You can view the individual ACS details from the table on the right pane or by choosing **Logical Inventory > *local* > Mobile > Active Charging Services >** *ACS*.

Table 26-69 describes the details available for each ACS.

*Table 26-69 Active Charging Services in Logical Inventory*

| Field | Description |
|---|---|
| Service Name | Name of the active charging service. |
| TCP Flow Idle Timeout | Maximum duration, in seconds, a TCP flow can remain idle. |
| UDP Flow Idle Timeout | Maximum duration, in seconds, a UDP flow can remain idle. |
| ICMP Flow Idle Timeout | Maximum duration, in seconds, an Internet Control Message Protocol (ICMP) flow can remain idle. |
| ALG Media Idle Timeout | Maximum duration, in seconds, an application level gateway (ALG) media flow can remain idle. |
| TCP Flow Mapping Idle Timeout | The time for which the TCP flow mapping timer holds the resources. |
| UDP Flow Mapping Idle Timeout | The time for which the UDP flow mapping timer holds the resources. |
| Deep Packet Inspection | Indicates whether configuration of DPI is enabled or disabled in the mobile video gateway. |
| Passive Mode | Indicates whether the ACS is in or out of passive mode operation. |
| CDR Flow Control | Indicates whether flow control is enabled or disabled between the ACS Manager (ACSMGR) and Charging Data Record Module (CDRMOD). |
| CDR Flow Control Unsent Queue Size | Flow control unsent queue size at ACSMGR level. |
| Unsent Queue High Watermark | Highest flow control unsent queue size at ACSMGR level. |
| Unsent Queue Low Watermark | Lowest flow control unsent queue size at ACSMGR level. |
| Content Filtering | Indicates whether content filtering is enabled or disabled for the ACS. |
| Dynamic Content Filtering | Indicates whether dynamic content filtering is enabled or disabled for the ACS. |
| URL Blacklisting | Indicates whether URL blacklisting is enabled or disabled for the ACS. |
| URL Blacklisting Match Method | Method to look up the URLs in the URL blacklisting database. |
| Content Filtering Match Method | Method to look up the URLs in the category-based content filtering database. |
| Interpretation of Charging Rulebase Name | Charging rulebase configured for the ACS. |
| Selected Charging Rulebase Name for AVP | Charging rulebase name for attribute value pair (AVP) configured for the ACS. |

## Viewing Content Filtering Categories

To view content filtering categories in logical inventory:

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

**Step 2** In the logical inventory window, choose **Logical Inventory > *local* > Mobile > Active Charging Services >***ACS*** >Content Filtering Categories**.

Prime Network Vision displays the list of content filtering categories configured under the container. You can view the individual content filtering category details from the table on the right pane or by choosing **Logical Inventory > *local* > Mobile > Active Charging Services >** *ACS* **>Content Filtering Categories** > *Content Filtering Category*.

Table 26-70 describes the details available for each content filtering category.

***Table 26-70 Content Filtering Categories in Logical Inventory***

| Field | Description |
|---|---|
| Policy ID | ID of the content filtering policy. |
| Failure Action | Action to take for the content filtering analysis result. |
| EDR File | The EDR file name. |
| Content Category | Name of the content filtering category. |
| Content Insert | Content string to insert in place of the message returned from prohibited or restricted site or content server. |
| Content Priority | Precedence of the category in the content filtering policy. |
| Content Failure Action | Action to take for the indicated result of the content filtering analysis, which could be one of the following:<br>• allow<br>• content-insert<br>• discard<br>• redirect URL<br>• terminate flow<br>• www-reply-code-and-terminate-flow |
| Content Redirect | Content string to redirect the subscriber to a specified URL. |
| Content Reply Code | Reply code to terminate flow. |
| EDR File Format | Predefined EDR file format. |

## Viewing Credit Control Properties

In a prepaid environment, the subscribers pay for a service prior to using it. While the subscriber is using the service, credit is deducted from subscriber's account until it is exhausted or the call ends. In prepaid charging, ECS performs the metering function. Credits are deducted in real time from an account balance or quota. A fixed quota is reserved from the account balance and given to the system by a prepaid rating and charging server, which interfaces with an external billing system platform. The system deducts

volume from the quota according to the traffic analysis rules. When the subscriber's quota gets to the threshold level specified by the prepaid rating and charging server, system sends a new access request message to the server and server updates the subscriber's quota. The charging server is also updated at the end of the call.

ECS supports the following credit control applications for prepaid charging:

- RADIUS Credit Control Application—RADIUS is used as the interface between ECS and the prepaid charging server.
- Diameter Credit Control Application—The Diameter Credit Control Application (DCCA) is used to implement real-time credit control for a variety of services, such as networks access, messaging services, and download services.

To view credit control properties in logical inventory:

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

**Step 2** In the logical inventory window, choose **Logical Inventory > *local* > Mobile > Active Charging Services >***ACS* **> Credit Control**.

Prime Network Vision displays the list of credit control groups configured under the container. You can view the individual credit control group details from the table on the right pane or by choosing **Logical Inventory > *local* > Mobile > Active Charging Services >** *ACS* **> Credit Control** > *Credit Control Group*.

You can also view the following details by clicking the respective node under the credit control group:

- Diameter
- Failure Handling
- Pending Traffic Treatment
- Quota
- Server Unreachable Failure Handling

Table 26-71 describes the details available for each credit control group.

***Table 26-71 Credit Control Properties in Logical Inventory***

| Field | Description |
|---|---|
| Group | Name of the credit control group for the subscriber. |
| Mode | Prepaid charging application mode, which could be Diameter or Radius. |
| APN Name to be Included | Type of APN name sent in the credit control application (CCA) message. |
| Trigger Type | Condition based on which credit reauthorization is triggered from the server. |
| Diameter MSCC Final Unit Action Terminate | Indicates whether to terminate a PDP session immediately when the Final-Unit-Action (FUA) in a particular multi service credit control (MSCC) is set as Terminate and the quota is exhausted for that service, or to terminate the session after all MSCCs (categories) have used their available quota. |
| Diameter Peer Select table | |
| Peer | Primary hostname. |
| Realm | Realm for the primary host. |
| Secondary Peer | Secondary hostname. |

*Table 26-71 Credit Control Properties in Logical Inventory (continued)*

| Field | Description |
|---|---|
| Secondary Realm | Realm for the secondary host. |
| IMSI Range Mode | Mode of peer selection based on IMSI prefix or suffix. |
| IMSI Start Value | Starting value of the IMSI range for peer selection. |
| IMSI End Value | Ending value of the IMSI range for peer selection. |
| **Diameter** | |
| End Point Name | Name of the diameter endpoint. |
| End Point Realm | Realm of the diameter endpoint. |
| Pending Timeout | Maximum time to wait for response from a diameter peer. |
| Session Failover | Indicates whether diameter session failover is enabled or not. |
| Dictionary | Diameter credit control dictionary for the ACS. |
| **Failure Handling** | |
| Initial Request | Failure handling behavior, if failure takes place during initial session establishment. Value could be continue, retry-and-terminate, and terminate. |
| Update Request | Failure handling behavior, if failure takes place during update request. Value could be continue, retry-and-terminate, and terminate. |
| Terminate Request | Failure handling behavior, if failure takes place during terminate request. Value could be continue, retry-and-terminate, and terminate. |
| **Pending Traffic Treatment** | |
| Trigger | Indicates whether to allow or drop a trigger while waiting for the credit information from the server. Value could be pass or drop. |
| Forced Reauth | Indicates whether to allow or drop reauthorization while waiting for the credit information from the server. Value could be pass or drop. |
| NoQuota | Indicates whether to allow or drop traffic, if there is no quota present. Value could be pass, drop, or buffer. |
| Quota Exhausted | Indicates whether to allow or drop traffic, if quota is exhausted. Value could be pass, drop, or buffer. |
| Validity Expired | Indicates whether to allow or drop traffic, if quota validity is expired. Value could be pass or drop. |
| **Quota** | |
| Request Trigger | Action taken on the packet that triggers the credit control application to request quota. Value could be exclude-packet-causing-trigger or include-packet-causing-trigger. |
| Holding Time | Duration for which ECS can hold the quota before returning to the credit control server. |
| Validity Time | Lifetime for which subscriber quota retrieved from the billing server is valid. |
| Time Threshold | Time threshold limit for subscriber quota in the prepaid credit control service. |
| Units Threshold | Unit threshold limit for subscriber quota in the prepaid credit control service. |
| Volume Threshold | Volume threshold limit for subscriber quota in the prepaid credit control service. |

*Table 26-71 Credit Control Properties in Logical Inventory (continued)*

| Field | Description |
|---|---|
| **Server Unreachable Failure Handling** | |
| Initial Request | Failure handling behavior if server is unreachable during initial session establishment. Value could be continue or terminate. |
| Update Request | Failure handling behavior if server is unreachable during update request. Value could be continue or terminate. |

## Viewing Charging Action Properties

Charging Action is an action taken on the incoming data packets once the data packets are treated by the routing and charging rule components. User can configure independent actions such as allow, forward, and block traffic, and bind these actions with other routing and charging rule components.

To view charging action properties in logical inventory:

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

**Step 2** In the logical inventory window, choose **Logical Inventory > *local* > Mobile > Active Charging Services >***ACS*** > Charging Action**.

Prime Network Vision displays the list of charging actions configured under the container as shown. You can view the individual charging action details from the table on the right pane or by choosing **Logical Inventory > *local* > Mobile > Active Charging Services >** *ACS* **> Charging Action** > *Charging Action.*

You can also view the following details by clicking the respective node under the Charging Action node:

- Allocation Retention Priority
- Bandwidth
- Flow Action
- QoS
- Video
- Billing Action

Table 26-72 describes the details available for each charging action record.

*Table 26-72 Charging Action Properties in Logical Inventory*

| Field | Description |
|---|---|
| Name | Name of the charging action. |
| Content ID | Content ID to use in the generated billing records as well the AVP used by the credit control application. |
| Service ID | Configured service ID used to associate the charging action in rule definitions configuration. |
| Charging EDR Name | Name of the EDR format for the billing action in the ACS. |

*Table 26-72 Charging Action Properties in Logical Inventory (continued)*

| Field | Description |
|---|---|
| EGCDRs | Indicates whether eG-CDRs must be generated when the subscriber session ends or an interim trigger condition occurs. |
| Rf | Indicates whether Rf accounting is enabled or not. |
| UDRs | Indicates whether UDRs must be generated based on the UDR format declared in the rule base. |
| Flow Idle Timeout | Maximum duration a flow can remain idle after which the system automatically terminates the flow. |
| Limit for Flow Type State | Indicates whether the limit for flow type is configured or not. |
| Limit for Flow Type Value | Maximum number of flows of a particular type. |
| Limit for Flow Type Action | Action to be taken, if the number of flows exceeds the maximum limit. |
| IP Type of Service | IP Type of Service (ToS) octets used in the charging action. |
| Retransmission Count | Indicates whether to count the number of packet retransmissions when the charging action is applied on the incoming data packets. |
| Content Filtering | Indicates whether content filtering must be applied on the incoming packets or not. |
| Credit Control | Indicates whether to apply credit control or not. |
| Credit Rating Group | Coupon ID used in prepaid charging as rating group. |
| Charge Volume | Method used for charge volume calculation based on the protocol and packet. |
| Next Hop Forwarding Address | Next hop forwarding address for a charging action. |
| VLAN ID | VLAN ID configured for the subscriber |
| Flow Mapping Idle Timeout | Maximum duration, in seconds, a flow can remain idle after which the system automatically terminates the flow. |
| **Allocation Retention Priority** | |
| Priority Level | Priority value that indicates whether to accept or reject a request for establishment or modification of a bearer in a limited resource condition. |
| Priority Vulnerability Indicator | Defines whether an active bearer can be preempted by a preemption-capable high priority bearer. |
| Priority Capability Indicator | Defines whether the bearer request can preempt the resources from the Low Priority Pre-empatable Active Bearers. |
| **Bandwidth** | |
| Bandwidth ID | The bandwidth policy ID for the ACS. |
| Uplink | Indicates whether uplink flow limit is configured for the subscriber or not. |
| Downlink | Indicates whether downlink flow limit is configured for the subscriber or not. |
| **Charging Action Bandwidth Direction** | |
| Direction | Direction of the packet flow: Uplink or Downlink |

*Table 26-72 Charging Action Properties in Logical Inventory (continued)*

| Field | Description |
|---|---|
| Peak Data Rate | Peak data rate configured for the uplink or downlink packet flow. |
| Peak Burst Size | Peak burst size allowed for the uplink or downlink packets. |
| Committed Data Rate | Committed data rate for the uplink or downlink packet flow. |
| Committed Burst Size | Committed burst size allowed for the uplink or downlink packets. |
| Exceed Action | Action to take on packets that exceed committed data rate but do not violate the peak data rate. |
| Violate Action | Action to take on packets that exceed both committed and peak data rates. |
| Bandwidth Limiting ID | Identifier for bandwidth limiting. |
| **Flow Action** | |
| Redirect URL | Indicates whether packets matched to the rule definition must be redirected to a specified URL or not. |
| Clear Quota Retry Timer | Indicates whether to reset the CCA quota retry timer for a specific subscriber upon redirection of data packets. |
| Conditional Redirect | Indicates whether packets matching to a configured user agent must be conditionally redirected to a specified URL. |
| Discard | Discards packets associated with the charging action. |
| Random Drop | Indicates whether to degrade voice quality and specify the time interval in seconds at which the voice packets will be dropped. |
| Readdress | Redirects unknown gateway traffic based on the destination IP address of the packets to known or trusted gateways. |
| Terminate Flow | Indicates whether to terminate the flow by terminating the TCP connection gracefully between the subscriber and external server. |
| Terminate Session | Indicates whether to terminate the session. |
| **QoS** | |
| Traffic Class | QoS traffic class for the charging action, which could be background, conversational, interactive, or streaming. |
| Class Identifier | The QCI value. |
| **Video** | |
| Bit Rate | Bits per second, at which the TCP video flow must be paced during video pacing. |
| CAE Readdressing | Indicates whether Content Adaptation Engine (CAE) readdressing is enabled, allowing video traffic to be fetched from the CAEs in the CAE group. |
| Transrating | Indicates whether transrating is enabled or not. Transrating is a mobile video feature that reduces the encoded bit rates by adjusting video encoding. |
| Target Rate Reduction | Percentage of the input bit rate of a video flow. |
| **Billing Action** | |
| EDR | Name of the EDR format for the billing action in the ACS. |
| EGCDR | Indicates whether eG-CDRs must be generated when the subscriber session ends or an interim trigger condition occurs. |

*Table 26-72 Charging Action Properties in Logical Inventory (continued)*

| Field | Description |
|---|---|
| Rf | Indicates whether Rf accounting is enabled or not. |
| UDRs | Indicates whether UDRs must be generated based on the UDR format declared in the rule base. |
| Radius Accounting Record | Indicates whether radius accounting is enabled or not. |

## Viewing Rule Definitions

Rule definitions are user-defined expressions, based on protocol fields and protocol states, which define what actions to take when specific field values are true. Each rule definition configuration consists of multiple expressions applicable to any of the fields or states supported by the respective analyzers.

Rule definitions are of the following types:

- Routing—Used to route packets to content analyzers. Routing rule definitions determine which content analyzer to route the packet to when the protocol fields and/or protocol states in the rule definition expression are true. Up to 256 rule definitions can be configured for routing.
- Charging—Used to specify what action to take based on the analysis done by the content analyzers. Actions can include redirection, charge value, and billing record emission. Up to 2048 charging rule definitions can be configured in the system.
- Post-processing—Used for post-processing purposes. Enables processing of packets even if the rule matching for them has been disabled.
- TPO—Used for Traffic Performance Optimization (TPO) in-line service match-rule and match advertisement features.

To view rule definitions in logical inventory:

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

**Step 2** In the logical inventory window, choose **Logical Inventory > *local* > Mobile > Active Charging Services >** *ACS* **> Rule Definitions**.

Prime Network Vision displays the list of rule definitions configured under the container. You can view the individual rule definition details from the table on the right pane or by choosing **Logical Inventory > *local* > Mobile > Active Charging Services >***ACS* **> Rule Definitions** > *Rule Definition.*

Table 26-73 describes the details available for each rule definition.

*Table 26-73 Rule Definition Group Properties in Logical Inventory*

| Field | Description |
|---|---|
| Name | Name of the rule definition group. |
| Application Type | Purpose of the rule definition, which could be charging, routing, post-processing, or Traffic Performance Optimization (TPO). |
| Copy Packet To Log | Indicates whether to copy every packet that matches the rule to a log file. |
| Tethered Flow Check | Indicates whether tethered flow check if enabled or not. Tethering detection flow check feature enables detection of subscriber data traffic flow originating from PC devices tethered to mobile smart phones, and also provides effective reporting to enable service providers take business decisions on how to manage such usage and to bill subscribers accordingly. |
| Multiline OR | Indicates whether to apply the OR operator to all lines in a rule definition. This allows a single rule definition to specify multiple URL expressions. |
| **Protocol Configuration** | |
| Protocol | The protocol that this rule definition is applied on. |
| Fields | Particular protocol field, which is applied on the data packets for inspection. Value could be, host, payload, or domain. |
| Operator | Logical operator that indicates how to logically match the value in the field analyzed based on the data type. |
| Value | Value of a particular protocol in a rule definition which has to be applied on the incoming data packets for inspection. |

## Viewing Rule Definition Groups

A rule definition group enables grouping the rule definitions into categories. A rule definition group may contain optimizable rule definitions. Whether a group is optimized or not is decided on whether all the rule definitions in the group can be optimized. When a new rule definition is added, it is checked if it is included in any rule definition group and whether it needs to be optimized or not.

To view rule definition groups in logical inventory:

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

**Step 2** In the logical inventory window, choose **Logical Inventory > *local* > Mobile > Active Charging Services >** *ACS* **> Group of Rule Definitions**.

Prime Network Vision displays the list of rule definition groups configured under the container. You can view the individual rule definition group details from the table on the right pane or by choosing **Logical Inventory > *local* > Mobile > Active Charging Services >***ACS* **> Group of Rule Definitions** > *Rule Definition Group.*

Table 26-74 describes the details available for each rule definition group.

*Table 26-74 Rule Definition Group Properties in Logical Inventory*

| Field | Description |
|---|---|
| Name | Name of the rule definition group. |
| Application Type | Purpose of the rule definition group, which could be charging, routing, content filtering, post-processing, or Traffic Performance Optimization (TPO). |
| Dynamic Command Content Filtering Policy ID | Content filtering policy ID to add or remove dynamic commands from the rule definition group. |

### Rule Definition Group Commands

The following commands can be launched from the inventory by right-clicking a rule definition group and choosing **Commands > Configuration** or **Commands > Show.** Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

*Table 26-75 Rule Definition Group Commands*

| Command Type | Command | Inputs Required and Notes |
|---|---|---|
| **Configuration** | **Delete Group of RuleDefs** | Click **Execute Now** to delete the rule definition group. |
| **Show** | **Show Group of RuleDefs** | Click **Execute Now** to display the group of rule definitions. |

## Viewing Rule Base for the Charging Action

A rule base is a collection of rule definitions and their associated billing policy. The rule base determines the action to be taken when a rule is matched. A maximum of 512 rule bases can be specified in the ECS service. It is possible to define a rule definition with different actions.

Rule bases can also be used to apply the same rule definitions for several subscribers, which eliminate the need to have unique rule definition for each subscriber. We can set priority, default bandwidth policy, type of billing for subscriber sessions, for a rule definition/ group of rule definitions in the rule base. Additionally we can configure content based billing and firewall/NAT constituent to rule base.

To view a rule base in logical inventory:

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

**Step 2** In the logical inventory window, choose **Logical Inventory > *local*** **> Mobile > Active Charging Services >** *ACS* **> Rulebase Container**.

Prime Network Vision displays the list of rule bases configured under the container. You can view the individual rule base details from the table on the right pane or by choosing **Logical Inventory > *local*** **> Mobile > Active Charging Services >***ACS* **> Rulebase Container** > *Rule Base.*

Table 26-76 describes the details available for each rule base record.

***Table 26-76 Rule Base Properties in Logical Inventory***

| Field | Description |
|---|---|
| Rulebase Name | Name of the rule base. |
| Flow Any Error Charging Action | Charging action to be used for packets dropped due to any error conditions after data session is created. |
| Limit for Total Flows | Maximum number of simultaneous uplink and downlink packet flows. |
| Limit for TCP Flows | Maximum number simultaneous TCP packet flows per subscriber or APN allowed for a rulebase. |
| Limit for Non TCP Flows | Maximum number simultaneous non-TCP packet flows per subscriber or APN allowed for a rulebase. |
| Charging Rule Optimization | Internal optimization level to use, for improved performance, when evaluating each instance of the action. |
| QoS Renegotiation Timeout | Timeout value after which QoS renegotiation is performed. |
| RTP Dynamic Routing | Indicates whether the Real Time Streaming Protocol (RTSP) and SDP analyzers are enabled to detect the start/stop of RTP (a Transport Protocol for Real-Time Applications) and RTP Control Protocol (RCP) flows. |
| Ignore Port Number In Application Header | Indicates whether to consider or ignore the port number embedded in the application. |
| Delayed Charging | Indicates how to charge for the control traffic associated with an application. |
| XHeader Certificate Name | Name of the encryption certificate to be used for x-header encryption. |
| XHeader Reencryption Period | Indicates how often to regenerate the encryption key for x-header encryption. |
| Default Bandwidth Policy | Name of the default bandwidth policy per subscriber. |
| P2P Dynamic Routing | Indicates whether P2P analyzer is enabled to detect the P2P applications flow configured in ACS. |
| Fair Usage Waiver Percentage | Waiver percent on top of the average available memory credits per session for the Fair Usage feature of active charging. |
| URL Blacklisting Action | Configured URL blacklisting action to take when the URL matches ones of the blacklisted URLs. |
| URL Blacklisting Content ID | Specific content ID for which URL blacklisting is enabled in the rulebase. |

*Table 26-76 Rule Base Properties in Logical Inventory (continued)*

| Field | Description |
|---|---|
| Charging Action Priorities tab | Charging rule definitions and their priorities in the rulebase. |
| Routing Action Priorities tab | Routing actions and their priorities in the rulebase. |
| Post Processing Action Priorities | Post-processing actions and their priorities in the rulebase. |

## Viewing Bandwidth Policies

Bandwidth policies are helpful in applying rate limit to potentially bandwidth intensive and service disruptive applications. Using this policy, the operator can police and prioritize subscribers' traffic to ensure that no single or group of subscribers' traffic negatively impacts another subscribers' traffic. Each policy will be identified by a unique ID, which will be associated to a particular group. Bandwidth policies are used to control the direction (uplink/downlink) of bandwidth, peak data rate, and peak burst size, and the actions that need to be taken on violation, if the bandwidth exceeds the burst size and data rate.

To view bandwidth policy in logical inventory:

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

**Step 2** In the logical inventory window, choose **Logical Inventory > *local* > Mobile > Active Charging Services >** *ACS* **> Bandwidth Policy Container**.

Prime Network Vision displays the list of bandwidth policies configured under the container. You can view the individual bandwidth policy details from the table on the right pane or by choosing **Logical Inventory > *local* > Mobile > Active Charging Services >** *ACS* **> Bandwidth Policy Container** > *Bandwidth Policy.*

Table 26-77 describes the details available for each bandwidth policy.

*Table 26-77 Bandwidth Policy Properties in Logical Inventory*

| Field | Description |
|---|---|
| Name | Name of the bandwidth policy configured. |
| Total Bandwidth ID Configured | Total number of bandwidth IDs configured. |
| Total Group Limit Configured | Total number of bandwidth group limits configured. |
| Flow Limit for Bandwidth ID and Group ID Associations and Group ID tables | Holds all bandwidth IDs and group IDs of the bandwidth policy. |

## Viewing Fair Usage Properties

To view fair usage properties configured for the ACS:

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

**Step 2** In the logical inventory window, choose **Logical Inventory > *local* > Mobile > Active Charging Services >** *ACS* **> Fair Usage**.

Prime Network Vision displays the details on the content pane.

Table 26-78 describes the fair usage properties.

***Table 26-78 Fair Usage Properties in Logical Inventory***

| Field | Description |
|---|---|
| CPU Threshold Percent | Percentage of system CPU resources that the dynamic inline transrating feature is allowed to use. |
| Threshold Percent | Percentage of system resources that the dynamic inline transrating feature is allowed to use. |
| Deactivate Margin Percent | Fair usage deactivate margin, below which monitor action is disabled. |

# ACS Commands

The following commands can be launched from the inventory by right-clicking an ACS and choosing **Commands > Configuration** or **Commands > Show.** Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

**Note** In the GUI, parameters that are displayed in bold text are mandatory.

Table 26-79 lists the Active Charging Services configuration commands.

*Table 26-79 Active Charging Services Configuration Commands*

| Command | Navigation | Description |
|---|---|---|
| Create Ruledef | Expand **Active Charging Services** node > *right-click ACS service* > **Commands** > **Configuration** | Rule definitions (Ruledefs) are user-defined expressions, based on protocol fields and/or protocol-states, which define what actions to take when specific field values are true.<br>Use this command to create a new rule definition for the selected ACS service. |
| Create group of Ruledefs | Expand **Active Charging Services** node > *right-click ACS service* > **Commands** > **Configuration** | Group-of-Ruledefs enable grouping ruledefs into categories. When a group-of-ruledefs is configured in a rulebase, if any of the ruledefs within the group matches, the specified charging-action is performed, any more action instances are not.<br>Use this command to create a new group of rule definitions for the selected ACS service. |
| Create Rulebase | Expand **Active Charging Services** node > *right-click ACS service* > **Commands** > **Configuration** | A rulebase is a collection of ruledefs and their associated billing policy. The rulebase determines the action to be taken when a rule is matched.<br>Use this command to create a new rule base for the selected ACS service. |
| Modify Active Charging Service<br>Delete Active Charging Service | Expand **Active Charging Services** node > *right-click ACS service* > **Commands** > **Configuration** | Use these commands to modify/delete an Active Charging service created for the selected context. |
| Create Access Ruledef<br>Delete Access Ruledef | Expand **Active Charging Services** node > *right-click ACS service* > **Commands** > **Configuration** > **Access Ruledef** | Use these commands to create/delete an access rule definition for the selected ACS service. |
| Show Access Ruledef | Expand **Active Charging Services** node > *right-click ACS service* > **Commands** > **Show** | Use this command to view and confirm the access rule definitions configured for the service. |

*Table 26-79 Active Charging Services Configuration Commands (continued)*

| Command | Navigation | Description |
|---|---|---|
| Create Host Pool<br>Modify Host Pool<br>Delete Host Pool | Expand **Active Charging Services** node > *right-click ACS service* > **Commands** > **Configuration** > **Host Pool** | Host pools allow operators to group a set of host or IP addresses that share similar characteristics together. Access rule definitions (ruledefs) can be configured with host pools. Up to ten sets of IP addresses can be configured in each host pool.<br>Use these commands to create/modify/delete a host pool for the selected ACS service. |
| Create Charging Action | Expand **Active Charging Services** node > *right-click ACS service* > **Commands** > **Configuration** | Charging Action is an action taken on the incoming data packets once the data packets are treated by the routing and charging rule components. You can configure independent actions such as allow, forward, and block traffic, and bind these actions with other routing and charging rule components.<br>Use this command to configure a charging action for a service. |
| Modify charging Action<br>Delete Charging Action | Expand **Active Charging Services** node > *ACS service* > **Charging Actions** > *right-click an charging action* > **Commands** > **Configuration** | Use these commands to modify/delete a charging action for a service. |
| Show Charging Action | Expand **Active Charging Services** node > *right-click ACS service* > **Commands** > **Show** | Use this command to view and confirm the charging action configuration details. |

# Configuring and Viewing Mobile Technologies

The following commands can be used to configure and view mobile technologies under a particular context in the Prime Network Vision. These commands can be launched from the logical inventory by choosing the *Context* **> Commands > Configuration** or *Context* **> Commands > Show.** Before executing any command, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

| Command | Navigation | Description |
|---|---|---|
| **Create AAA Group** | *Context* > **Commands > Configuration** | AAA refers to Authentication, Authorization, and Accounting, which is a security architecture for distributed systems that determines the access given to users for specific services and the amount of resources they have used.<br>Use this command to create a new AAA group. |
| **Create APN** | | APN is the access point name that is configured in the GGSN configurations.<br>Use this command to create a new APN service. |
| **Create Active Charging Service** | | Enhanced Charging Service (ECS), also known as Active Charging Service (ACS), is an in-line service, which is integrated within the platform and provides mobile operators the ability to offer tiered, detailed, and itemized billing to subscribers.<br>Use this command to create a new ACS service. |
| **Create EGTP** | | Evolved GPRS Tunneling Protocol (EGTP) formulates the primary bearer plane protocol within an LTE / EPC architecture. It provides support for tunnel management including handover procedures within and across LTE networks.<br>Use this command to create an EGTP service. |

| Command | Navigation | Description |
|---|---|---|
| **Create GGSN** | *Context* > **Commands > Configuration** | Gateway GPRS Support Node (GGSM) is the gateway between the GPRS wireless data network and other external packet data networks such as radio networks, IP networks, or private networks. GGSN provides network access to external hosts wishing to communicate with mobile subscribers (MS).<br>Use this command to create a GGSN service. |
| **Create GTPP** | | GPRS Tunneling Protocol Prime (GTPP) is used for communicating accounting messages to CGs.<br>Use this command to create a GTPP service. |
| **Create GTPU** | | GTPU carries user data within the GPRS core network and between the radio access network and the core network. The user data transported can be packets in any of IPv4, IPv6, or PPP formats.<br>Use this command to create a GTPU service. |
| **Create IP Pool** | | An IP pool is a sequential range of IP addresses within a certain network.<br>Use this command to create an IP Pool. |
| **Create P-GW** | | PDN Gateway (P-GW) is the node that terminates the SGi interface towards the PDN. If a UE is accessing multiple PDNs, there may be more than one P-GW for that UE.<br>Use this command to create a P-GW. |
| **Create QCI-QOS Mapping** | | The QoS Class Index (QCI) to QoS mapping configuration mode is used to map QCIs to enforceable QoS parameters.<br>Use this command to create a QCI-QOS Mapping. |
| **Create S-GW** | | A Serving Gateway (S-GW) acts as a demarcation point between the Radio Access Network (RAN) and core network, and manages user plane mobility.<br>Use this command to create a S-GW. |
| **Create VRF** | | Virtual routing and forwarding (VRF) is a technology included in IP (Internet Protocol) network routers that allows multiple instances of a routing table to exist in a router and work simultaneously.<br>Use this command to create a VRF. |
| **Delete Context** | | Use this command to delete a context under the Logical Inventory node. |
| **Modify License** | | Use this command to modify the license information. |

| Command | Navigation | Description |
|---|---|---|
| **Create DHCP** | *Context* > **Commands > Configuration > DHCP** | DHCP is used to automate host configuration by assigning IP addresses, delegating prefixes (in IPv6), and providing extensive configuration information to network computers.<br>Use this command to create a DHCP service. |
| **Delete DHCP** | | Use this command to delete a DHCP service. |
| **Modify DHCP** | | Use this command to modify the configuration details of a DHCP service. |
| **Create HA SPI List** | *Context* > **Commands > Configuration > HA SPI List** | Use this command to create the Security Parameter Index (SPI) between the HA service and the FA. |
| **Delete HA SPI List** | | Use this command to delete the HA SPI List. |
| **Modify HA SPI List** | | Use this command to modify the HA SPI List configuration details. |
| **Create HA Service** | *Context* > **Commands > Configuration > HA Service** | Use this command to create a new Home Agent service. |
| **Delete HA Service** | | Use this command to delete a HA Service. |
| **Modify HA Service** | | Use this command to modify the configuration details of a HA service. |
| **Create Network Requested PDP Context** | *Context* > **Commands > Configuration > PDP Context** | Packet Data Protocol (PDP) context is the connection or link between a mobile device and a network server that allows them to communicate with each other. A PDP context lasts only for the duration of a specific connection.<br>Use this command to create a network requested PDP context. |
| **Delete Network Requested PDP Context** | | Use this command to delete a network requested PDP context. |
| **Create Proxy DNS** | *Context* > **Commands > Configuration > Proxy DNS** | The proxy DNS listens for incoming DNS requests on the local interface and resolves remote hosts using an external PHP script, through http proxy requests.<br>Use this command to create a proxy DNS. |
| **Delete Proxy DNS** | | Use this command to delete a proxy DNS. |
| **Modify Proxy DNS** | | Use this command to modify the proxy DNS configuration details. |

| Command | Navigation | Description |
|---|---|---|
| **Create Route Access List** | *Context* > **Commands > Configuration > Route Map and Route Access List** | Access lists are a set of rules, organized in a rule table and are used to filter and identify traffic.<br>Use this command to create a new access list. |
| **Create Route Map** | | Route maps are similar to access lists; they both have criteria for matching the details of certain packets and an action of permitting or denying those packets. Unlike access lists, though, route maps can add to each "match" criterion a "set" criterion that actually changes the packet in a specified manner, or changes route information in a specified manner.<br>Use this command to create a route map. |
| **Delete Route Access List** | | Use this command to delete a route access list. |
| **Delete Route Map** | | Use this command to delete a route map. |
| **Modify Route Access List** | | Use this command to modify a route access list. |
| **Modify Route Map** | | Use this command to modify a route map. |
| **Create Subscribers** | *Context* > **Commands > Configuration > Subscriber** | Use this command to create a new subscriber. |
| **Delete Subscriber** | | Use this command to delete a subscriber. |
| **Modify Subscriber** | | Use this command to modify subscriber details. |
| **Show APN** | *Context* > **Commands > Show** | Use this command to view and confirm the APN configuration details. |
| **Show DHCP** | | Use this command to view and confirm the DHCP configuration details. |
| **Show EGTP** | | Use this command to view and confirm the EGTP configuration details. |
| **Show HA SPI List** | | Use this command to view and confirm the HA SPI List details. |
| **Show HA Service** | | Use this command to view and confirm the home agent service details. |
| **Show IP Pool** | | Use this command to view and confirm the IP Pool configuration details. |
| **Show License** | | Use this command to view and confirm the License details. |
| **Show Route Access List** | | Use this command to view and confirm the Access list details. |
| **Show Route Map** | | Use this command to view and confirm the Route Map details. |
| **Show Subscriber** | | Use this command to view and confirm the Subscriber details. |

| Command | Navigation | Description |
|---|---|---|
| **Create Policy Accounting** | Right-click on context > **Commands** > **Configuration** > **Policy Accounting** | Use this command to create a new accounting policy. |
| **Modify Policy Accounting**<br>**Delete Policy Accounting** | Right-click on context > **Commands** > **Configuration** > **Policy Accounting** | Use these commands to modify/delete an accounting policy. |

CHAPTER 27

# Monitoring Data Center Configurations

Data Center is a centralized repository, either physical or virtual for the storage, management, dissemination of data and information organized around a particular manner. In other words, it is a facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communication connections, environmental controls such as air conditioning or fire suppression, and security devices.

Cisco Prime Network supports the following network elements as part of data centers:

- Cisco Nexus 1000V network element
- Cisco Nexus 2000 network element
- Cisco Nexus 5000 network element
- Cisco Nexus 7000 network element
- Cisco Unified Computing System (UCS)

Prime Network supports the following technologies as part of data center:


- Virtual Port Channel (vPC), page 27-2
- Cisco FabricPath, page 27-6
- Virtualization, page 27-9


## User Roles Required to Work with Data Center Configurations

Table 27-1 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 3.10 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 3.10 Administrator Guide*.

*Table 27-1 Default Permission/Security Level Required for the Data Center Configurations*

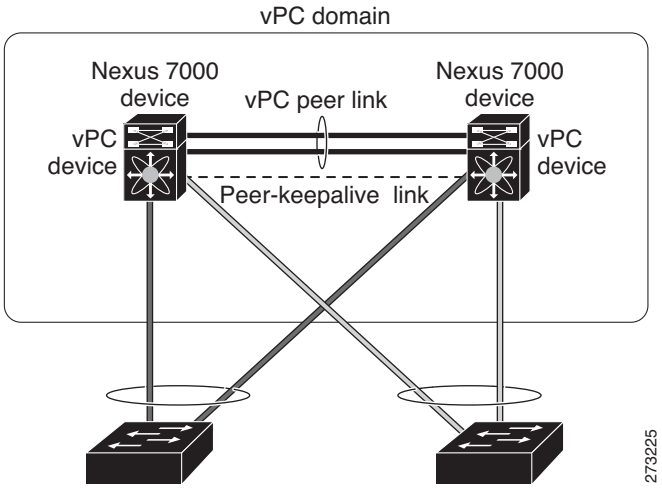
| Task | Viewer | Operator | OperatorPlus | Configurator | Administrator |
|---|---|---|---|---|---|
| Viewing Virtual Port Channel Configuration | X | X | X | X | X |
| Viewing vPC Configuration | X | X | X | X | X |
| Viewing Cisco FabricPath Configuration | X | X | X | X | X |
| Monitoring Cisco FabricPath Configuration | X | X | X | X | X |
| Viewing Virtual Data Centers | X | X | X | X | X |
| Viewing the Data Stores of a Data Center | X | X | X | X | X |
| Viewing the Host Servers of a Data Center | X[1] | X[1] | X[1] | X[1] | X[1] |
| Viewing the Virtual Machines of a Data Center | X[1] | X[1] | X[1] | X[1] | X[1] |

1. For users to be able to view VMs and hypervisors, a user's device scope must include all relevant vCenter VNEs.

# Virtual Port Channel (vPC)

A Virtual Port Channel (vPC) allows links that are physically connected to two different Cisco Nexus 7000 or Cisco Nexus 5000 series network elements to appear as a single port channel by a third device as shown in Figure 27-1. The third device can be a switch, server, or any other networking device that supports port channels. A vPC can provide Layer 2 multipathing, which allows you to create redundancy and increase bisectional bandwidth by enabling multiple parallel paths between nodes and allowing load balancing traffic. You can use only Layer 2 port channels in the vPC.

*Figure 27-1 vPC Architecture*




A vPC consists of the following components:

- Two vPC peer switches, among which one is primary and one is secondary. The system formed by the two peer switches is referred to as a vPC domain.
- A peer link, also known as multichassis EtherChannel trunk (MCT), which connects the vPC peer switches. A peer link is a redundant 10 Gigabit Ethernet Port Channel ,which is used to carry traffic from one system to the other when needed and to synchronize forwarding tables.
- vPC member ports that form the PortChannel and are split between the vPC peers.
- A routed link, called as a vPC peer-keepalive or fault-tolerant link is a Layer 3 Gigabit Ethernet link, used to resolve dual-active scenarios where the peer link connectivity is lost.

A vPC domain is associated to a single Virtual Device Context (VDC), so all vPC interfaces belonging to a given vPC domain must be defined in the same VDC. You must have a separate vPC peer link and peer keepalive link infrastructure for each VDC deployed. Consolidating a vPC pair (two vPC peer devices of the same domain) in two VDCs of the same physical device is not supported. The vPC peer link must use 10-Gigabit Ethernet ports for both ends of the link; otherwise, the link will not be formed.

A vPC provides the following benefits:

- Allows a single device to use a port channel across two upstream devices
- Eliminates STP blocked ports
- Provides a loop-free topology
- Uses all available uplink bandwidth
- Provides fast convergence in case of link or a device failure
- Provides link level resiliency
- Assures high availability

Prime Network supports vPC on Cisco Nexus 5000 series and Cisco Nexus 7000 series network elements.

This topic contains the following sections:

- Viewing Virtual Port Channel Configuration, page 27-4
- Viewing vPC Configuration, page 27-5

# Viewing Virtual Port Channel Configuration

To view the vPC configuration details in Prime Network Vision:

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

**Step 2** In the Inventory window, choose **Logical Inventory > VPC Domain**. The vPC domain details are displayed in the content pane as shown in Figure 27-2.

*Figure 27-2 vPC Domain in Logical Inventory*

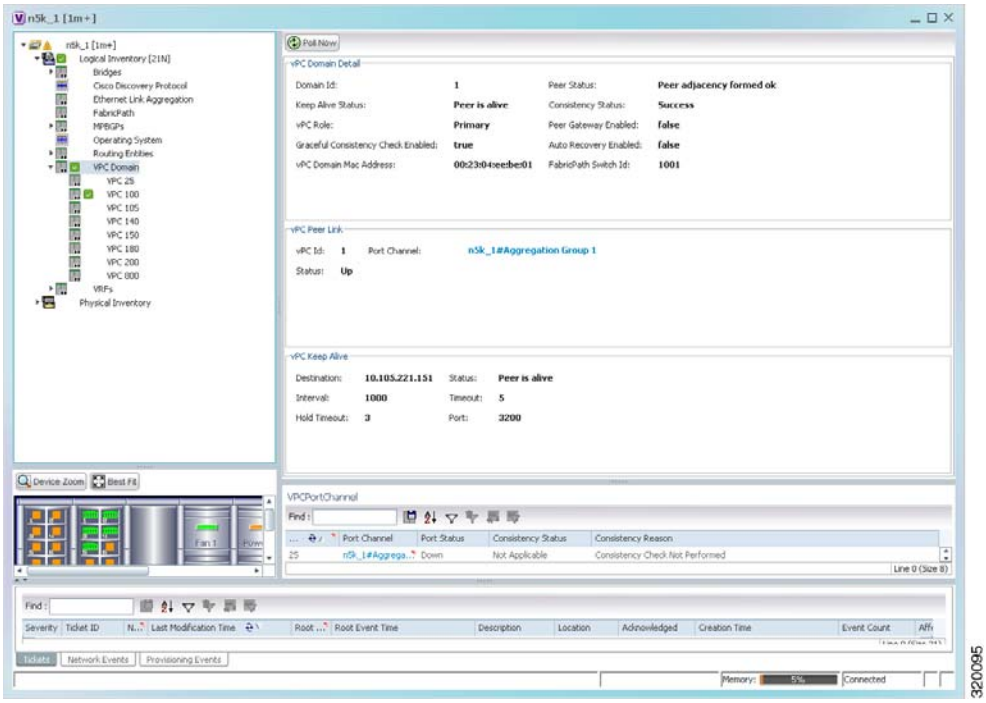



Table 27-2 describes the vPC domain details.

*Table 27-2 vPC Domain Properties*

| Field Name | Description |
|---|---|
| Domain ID | Unique ID that is used to identify the vPC peer links and ports connected to the vPC downstream devices. |
| Peer Status | Status of the peer link. |
| Keep Alive Status | Status of the keep alive link, which could be Alive or Down. |
| Consistency Status | Consistency status of the vPC, which could be Success or Failed. |
| vPC Role | Role of the vPC, which could be Primary or Secondary. |
| Peer Gateway Enabled | Status of the peer gateway, which could be Enabled or Disabled. |
| Graceful Consistency Check Enabled | Indicates whether graceful consistency check is enabled or disabled. This consistency check helps in preventing traffic drops. |
| Auto Recovery Enabled | Indicates whether auto recovery is enabled or disabled. |

*Table 27-2 vPC Domain Properties (continued)*

| Field Name | Description |
|---|---|
| vPC Domain Mac Address | MAC address of the vPC domain. |
| FabricPath Switch ID | ID of the FabricPath switch connected to the vPC. |
| **vPC Peer Link** | |
| vPC ID | Unique ID for vPC peer link. |
| Status | Status of the port channel used for communication, which could be Up or Down. |
| Port Channel | vPC used as the port channel for communication. Click the hyperlink, to view the relevant Ethernet link aggregation node in the physical inventory. |
| **vPC Keep Alive** | |
| Destination | Destination IP address of the peer switch. |
| Status | Status of the keep alive link, which could be Alive or Down. |
| Interval | Interval time required to check whether the peer switch is active or inactive. |
| Timeout | Time taken by the peer switch to respond. |
| Hold Timeout | Amount of time during which the peer switch information is stored. |
| Port | Interface used for the communication. |
| **VPC Port Channel** | |
| vPC ID | Unique virtual Port Channel ID. |
| Port Channel | Ethernet link used as the port channel for communication. Click the hyperlink, to view the relevant Ethernet link aggregation node in the physical inventory. |
| Port Status | Status of the vPC, which could be Up or Down. |
| Consistency Status | Consistency status of the vPC, which could be Success or Failed. |
| Consistency Reason | Reason for the consistency status. |

# Viewing vPC Configuration

The following commands can be launched from the inventory by right-clicking **VPC Domain** and choosing **Commands > Show.** Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

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

| Command | Navigation | Description |
|---|---|---|
| **Show Port Channel Capacity** | *Right-click on the VPC node* > **Commands** > **Show** | Use this command to view and confirm the port channel capacity details. |
| **Show vPC** | | Use this command to view the vPCs available for the selected domain. |
| **Show vPC Consistency Parameters** | | Use this command to view the vPC consistency parameters. |

# Cisco FabricPath

Cisco FabricPath is an innovation in Cisco NX-OS software that brings the stability and scalability of routing to Layer 2. It provides a foundation to build a scalable fabric—a network that itself looks like a single virtual switch from the perspective of its users. The switched domain does not have to be segmented anymore, providing data center–wide workload mobility. Because traffic is no longer forwarded along a spanning tree, the bisectional bandwidth of the network is not limited, and massive scalability is possible.

Cisco FabricPath introduces an entirely new Layer 2 data plane by encapsulating the frames entering the fabric with a header that consists of routable source and destination addresses. These addresses are the address of the switch on which the frame was received and the address of the destination switch to which the frame is heading. From there, the frame is routed until it is reaches the remote switch, where it is de-encapsulated and delivered in its original Ethernet format.

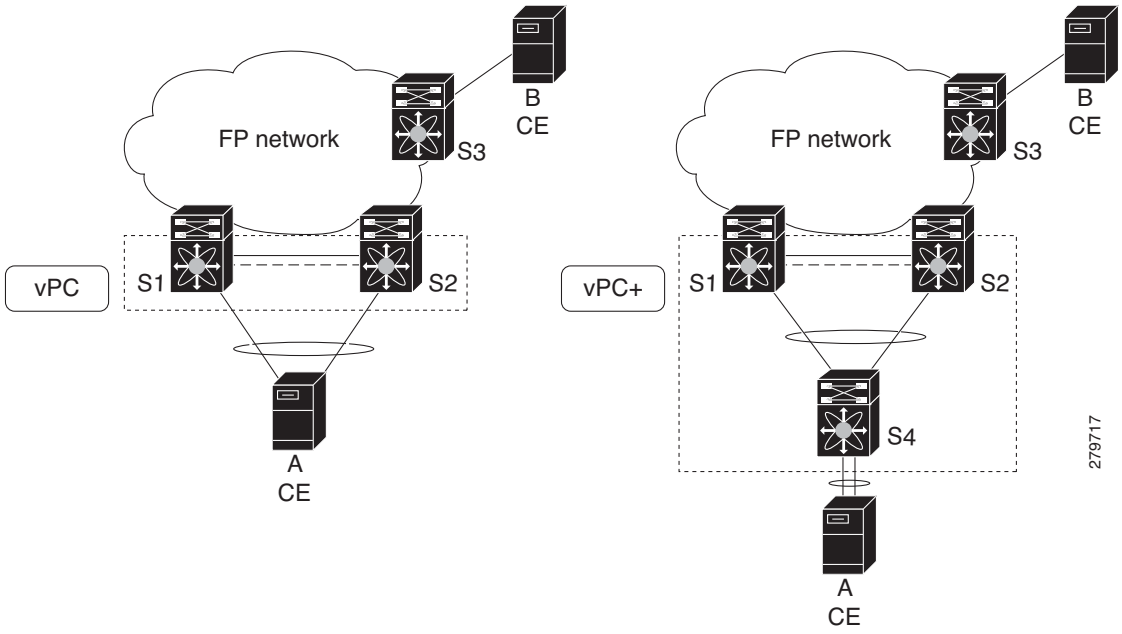
Cisco FabricPath provides the following features:

- Allows Layer 2 multipathing in the FabricPath network.
- Provides built-in loop prevention and mitigation with no need to use the Spanning Tree Protocol (STP).
- Provides a single control plane for unknown unicast, broadcast, and multicast traffic.
- Enhances mobility and virtualization in the FabricPath network.

The system randomly assigns a unique switch ID to each device that is enabled with FabricPath. After you enable FabricPath on the devices, you can configure an Ethernet interface or a port channel interface as a FabricPath interface. If one member of the port channel is in FabricPath mode, then all the other members will also be in FabricPath mode. After you configure the interface as a FabricPath interface, it automatically becomes a trunk port, capable of carrying traffic for multiple Virtual Local Area Networks (VLANs).

Prime Network supports Cisco FabricPath on Cisco Nexus 5000 series and Cisco Nexus 7000 series network elements. Figure 27-3 shows a Cisco FabricPath architecture.

***Figure 27-3 Cisco FabricPath Architecture***




This topic contains the following sections:


- Viewing Cisco FabricPath Configuration, page 27-7
- Monitoring Cisco FabricPath Configuration, page 27-9


# Viewing Cisco FabricPath Configuration

To view the FabricPath configuration in Prime Network Vision:

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

**Step 2** In the Inventory window, choose **Logical Inventory > FabricPath**. The FabricPath configuration details are displayed in the content pane as shown in Figure 27-4. You can also view the properties, by right-clicking the FabricPath node and choosing **Properties**.

*Figure 27-4 Cisco FabricPath Node in Logical Inventory*

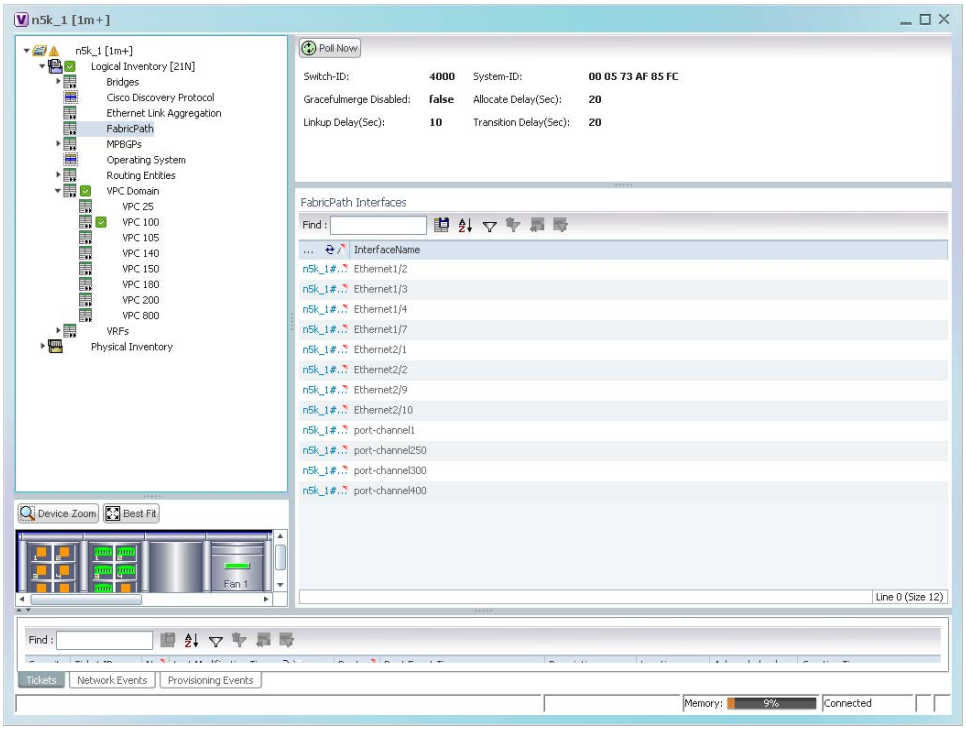



Table 27-3 describes the FabricPath configuration details.

*Table 27-3 Cisco FabricPath Configuration*

| Field Name | Description |
|---|---|
| Switch ID | Unique ID of the Cisco FabricPath virtual switch. |
| System-ID | System MAC address of the Cisco FabricPath. |
| Gracefulmerge Disabled | Indicates whether graceful merge feature is enabled are not. Value could be **True** or **False**. If this feature is enabled, the switch would be effectively linked to the Cisco FabricPath network. If disabled, you may experience traffic drops. |
| Allocate Delay (sec) | Time delay during new resource propagation. |
| Linkup Delay (sec) | Time delay for detecting conflicts during linkup sessions. |
| Transition Delay (sec) | Time delay during transition of value propagation. |
| **FabricPath Interfaces** | |
| Port | Ethernet link, which is configured as a Cisco FabricPath. Click the hyperlink to view the interface link in physical inventory. |
| Interface Name | Name of the interface for which switch port mode is configured as a Cisco FabricPath. |

# Monitoring Cisco FabricPath Configuration

The following commands can be launched from the inventory by right-clicking **FabricPath** and choosing **Commands > Show.** Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

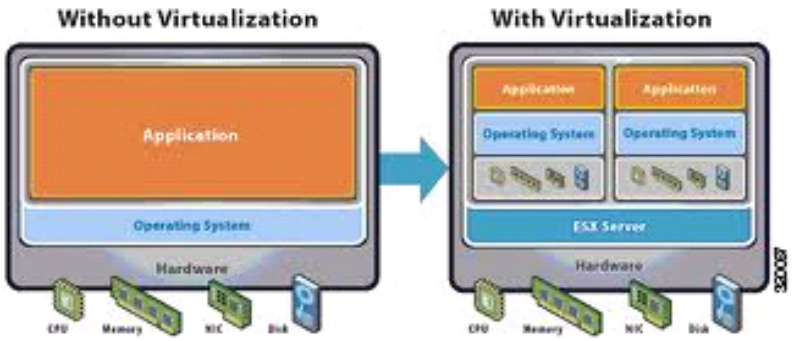
**Note** You might be prompted to enter your device access credentials while executing a command. Once you have entered them, these credentials will be used for every subsequent execution of a command in the same GUI client session. If you want to change the credentials, click **Edit Credentials**. The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

| Command | Navigation | Description |
|---|---|---|
| **FabricPath Conflict** | *Right-click on the FabricPath node* > **Commands > Show** | Use this command to view the Cisco FabricPath conflicts. |
| **MAC Address-Table Learning Mode** | | Use this command to view the MAC address-table learning mode. |

# Virtualization

Virtualization is a concept of creating a virtual version of any resource, such as hardware platform, operating system, storage device, or network resources, as shown in Figure 27-5. It provides a layer of abstraction between computing, storage and networking hardware, and the applications running on it. Virtual infrastructure gives administrators the advantage of managing pooled resources across the enterprise, allowing IT managers to be more responsive to dynamic organizational needs and to better leverage infrastructure investments.

***Figure 27-5 Virtualization Concept***



The various components of virtualization are:

**Hypervisor (Host Server)**

A hypervisor, also called a blade server, a virtual machine manager, or a host server, is a program that allows multiple operating systems to share a single hardware host. Each operating system appears to have the host's processor, memory, and other resources all to itself. However, the hypervisor is actually controlling the host processor and resources, allocating what is needed to each operating system in turn and making sure that the guest operating systems (called virtual machines) do not disrupt each other.

**Virtual Machine**

A virtual representation of a real machine using software that provides an operating environment, which can run or host a guest operating system.

**Guest Operating System**

An operating system running in a virtual machine environment that would otherwise run directly on a separate physical system.

**Data Store**

A data store represents a storage location for virtual machine files. It can be a Virtual Machine File System (VMFS) volume, a directory on Network Attached Storage, or a local file system path.

**Data Center**

Data Center serves as a container for hosts, virtual machines, networks, and data stores.

Prime Network supports virtualization on Cisco UCS network element.

The following topics explain how to view and monitor virtual data center properties in Prime Network Vision:

- Viewing Virtual Data Centers, page 27-10
- Viewing the Data Stores of a Data Center, page 27-11
- Viewing the Host Servers of a Data Center, page 27-11
- Viewing the Virtual Machines of a Data Center, page 27-14

# Viewing Virtual Data Centers

To view the virtual data centers in the logical inventory:

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

**Step 2** In the Inventory window, choose **Logical Inventory > Fabric Interconnect > Compute Virtualization**. The virtual data centers are listed in the content pane.

Table 27-4 describes the virtual data center properties.

*Table 27-4 Virtual Data Center Properties*

| Field Name | Description |
|---|---|
| Name | Name of the data center. |

*Table 27-4 Virtual Data Center Properties (continued)*

| Field Name | Description |
|---|---|
| Manager | IP address of the vCenter, which manages the virtual data center. |
| Description | The description of the data center. |

**Step 3** Right-click on a data center and choose **Properties** to view more details.

# Viewing the Data Stores of a Data Center

To view the details of data stores available for a data center:

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

**Step 2** In the Inventory window, choose **Logical Inventory** > **Fabric Interconnect** > **Compute Virtualization** > *Data Center* > **All Data Stores**. The available data stores are displayed in the content pane. You can view the data store properties from the table or by right-clicking the required data store and choosing **Properties**.

Table 27-5 describes the data store properties.

*Table 27-5 Data Store Properties*

| Field Name | Description |
|---|---|
| Name | Name of the data store. |
| Storage Type | Type of data storage for the data store. |
| Capacity | Capacity of the data store, in GB. |
| Free Space | Free space of the data store, in GB. |
| Accessible | Indicates whether the data store is accessible or not. Value could be True or False. |

# Viewing the Host Servers of a Data Center

To view the host centers of a data center:

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

**Step 2** In the Inventory window, choose **Logical Inventory** > **Fabric Interconnect** > **Compute Virtualization** > *Data Center* > **All Host Servers**. Choose a host server and the details are displayed in the content pane as shown in Figure 27-6.

*Figure 27-6 Host Server Details*

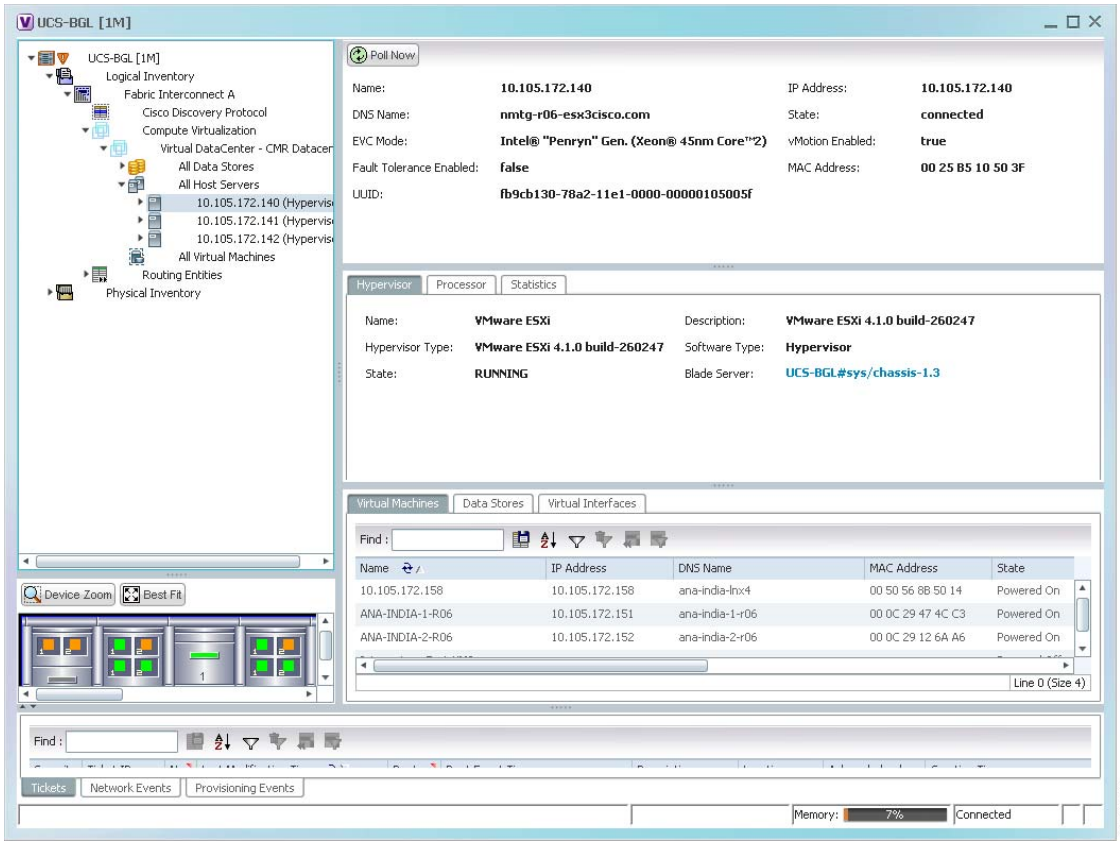



Table 27-6 describes the host server details.

*Table 27-6 Host Servers of a Data Center*

| Field Name | Description |
|---|---|
| Name | Name of the host server. |
| IP Address | The IP address of the host server. |
| DNS Name | The domain name of the host sever. |
| State | Management state of the host server. |
| EVC Mode | Enhanced vMotion Capability (Evc) of the host server. |
| VMotion Enabled | Indicates whether vMotion service is enabled or not. vMotion service helps in migrating the virtual machines from one host server to another, when a particular host server is down. |
| Fault Tolerance Enabled | Indicates whether fault tolerance service is enabled or not. This service provides continuous availability by protecting the primary virtual machine with a secondary virtual machine that runs simultaneously on a separate host. |
| MAC Address | MAC address of the host server. |
| UUID | The unique ID of the host server. |

*Table 27-6 Host Servers of a Data Center (continued)*

| Field Name | Description |
|---|---|
| **Hypervisor tab** | |
| Name | Name of the hypervisor running on the host server. |
| Description | Description of the hypervisor. |
| Hypervisor Type | Type of the hypervisor. |
| Software Type | Type of software used by the hypervisor. |
| State | State of the hypervisor, which could be Running, Runnable, Waiting, Exiting, or Other. |
| Blade Server | Link to the blade server in which the host server is located. Click the hyperlink to view the blade server details in the physical inventory. Click the **Associated Service** link in the blade server properties in the Physical Inventory window, to return to the host server properties. |
| **Processor tab** | |
| Name | Name of the processor used by the host server. |
| Description | Description of the processor used by the host server. |
| CPU | Number of central processing units (CPUs) available for the host server. |
| Cores per CPU | Number of cores per CPU available for the host server. |
| Rated Speed | Rated speed of the processor, in GHz. |
| Used Speed | Actual used speed of the processor, in GHz. |
| Hyper Threading Enabled | Indicates whether hyper threading is enabled for the host server or not. Hyper threading helps to improve parallelization of computations. |
| RAM Size | RAM size of the processor, in GB. |
| **Statistics tab** | |
| CPU Usage | CPU usage by the host server, in GHz. |
| Memory Usage | Memory usage by the host server, in GB. |
| **Virtual Machines tab** | |
| Name | Name of the virtual machine associated with the host server. |
| IP Address | IP address of the virtual machine. |
| DNS Name | Domain name of the virtual machine. |
| MAC Address | MAC address of the virtual machine. |
| State | Execution state of the virtual machine, which could be Powered On, Powered Off, or Suspended. |
| VM Version | Hardware version of the virtual machine. |
| Virtual CPU | Number of virtual CPUs configured for the virtual machine on the host server. |
| Minimum Required EVC Mode | Minimum required EvC of the virtual machine. |
| Software Type | Type of the software used by the virtual machine. |

*Table 27-6 Host Servers of a Data Center (continued)*

| Field Name | Description |
|---|---|
| **Data Stores tab** | |
| Data Store Name | Name of the data store associated with the host server. |
| Associated Data Store | Click the hyperlink to view the associated data store under the **All Data Stores** node. |
| **Virtual Interfaces tab** | |
| Name | Name of the network endpoint of the virtual entity. |
| Type | Type of the virtual entity network endpoint. |
| IP Address | Primary IP address of the virtual entity network endpoint. |
| MAC Address | MAC address of the virtual entity network endpoint. |
| Duplex Mode | Communication mode, which could be one of the following:<br>• Half—Transmit data in one direction at a time.<br>• Full—Transmit data in both the directions at the same time. |

# Viewing the Virtual Machines of a Data Center

To view the virtual machines for a data center:

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

**Step 2** In the Inventory window, choose **Logical Inventory** > **Compute Virtualization** > *Data Center* > **All Virtual Machines**. A list of virtual machines is displayed in the content pane as shown in Figure 27-7.

*Figure 27-7 Virtual Machine Details*

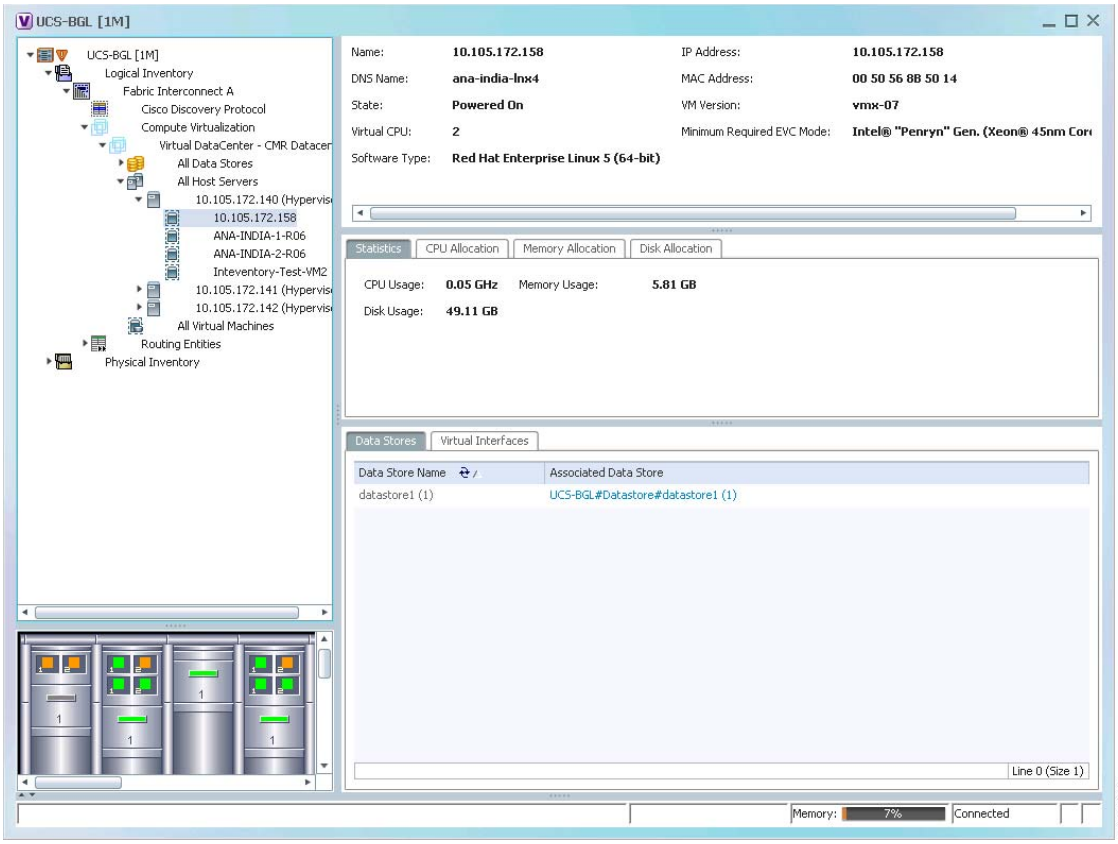



Table 27-7 describes the virtual machine details available in the list.

*Table 27-7 Virtual Machines*

| Field Name | Description |
|---|---|
| Name | Name of the associated data center. |
| **Virtual Machines** | |
| Virtual Machine | Name of the virtual machine. |
| Hypervisor | Name of the hypervisor associated with the virtual machine. |
| IP/DNS Name | IP address or the domain name of the virtual machine. |
| Mac Address | Mac address of the virtual machine. |

**Step 3** Click the hyperlinked virtual machine name to view more details about the virtual machine. Prime Network Vision takes you to the virtual machine node under the mapped host server in the logical inventory. You can view the virtual machine properties on the content pane or by right-clicking the virtual machine and choosing **Properties**.

Table 27-8 describes the properties of the virtual machine.

*Table 27-8 Virtual Machine Properties*

| Field Name | Description |
|---|---|
| Name | Name of the virtual machine. |
| IP Address | IP address of the virtual machine. |
| DNS Name | Domain name of the virtual machine. |
| MAC Address | MAC Address of the virtual machine. |
| State | Execution state of the virtual machine, which could be Powered On, Powered Off, or Suspended. |
| VM Version | Hardware version of the virtual machine. |
| Virtual CPU | Number of virtual CPUs configured for the virtual machine on the host server. |
| Minimum Required EVC Mode | Minimum required EvC of the virtual machine. |
| Software Type | Type of the software used by the virtual machine. |
| **Statistics tab** | |
| CPU Usage | CPU usage by the virtual machine, in GHz. |
| Memory Usage | Memory usage by the virtual machine, in GB. |
| Disk Usage | Amount of disk space used by the virtual machine, in GB. |
| Active Guest Memory Usage | Active guest memory used by the virtual machine, in GB. |
| **CPU Allocation tab** | |
| Resource Type | The type of resource, which in this instance is CPU. |
| Maximum Allocation | Maximum CPU allocation for the virtual machine, in GHz. |
| Unlimited Maximum Allocation | Unlimited maximum allocation capacity availability check for the virtual machine. Value could be true or false. |
| Expandable Allocation | Expandable allocation availability for the virtual machine. Value could be true or false. |
| Share | Relative importance of the virtual machine for CPU allocation, which could be High, Normal, or Low. |
| Custom Share Weight | Custom share weight assigned to the virtual machine. |
| **Memory Allocation tab** | |
| Maximum Allocation | Maximum memory allocation for the virtual machine, in GB. |
| Overhead Allocation | Overhead memory allocation for the virtual machine, in GB. |
| Unlimited Maximum Allocation | Unlimited maximum allocation capacity availability check for the virtual machine. Value could be true or false. |
| Expandable Allocation | Expandable allocation availability for the virtual machine. Value could be true or false. |
| Share | Relative importance of the virtual machine for memory allocation, which could be High, Normal, or Low. |

*Table 27-8 Virtual Machine Properties (continued)*

| Field Name | Description |
|---|---|
| Custom Share Weight | Custom share weight assigned to the virtual machine. |
| **Disk Allocation tab** | |
| Resource Type | The type of resource, which in this instance is Disk. |
| Guaranteed Allocation | Guaranteed resource allocation for the virtual machine, in GB. |
| Maximum Allocation | Maximum disk allocation for the virtual machine, in GB. |
| Unlimited Maximum Allocation | Unlimited maximum allocation capacity availability check for the virtual machine. Value could be true or false. |
| Expandable Allocation | Expandable allocation availability for the virtual machine. Value could be true or false. |
| Custom Share Weight | Custom share weight assigned to the virtual machine. |
| **Data Stores tab** | |
| Data Stores Name | Name of the data store associated with the virtual machine. |
| Associated Data Sore | Click the hyperlink to view the associated data store under the **All Data Stores** node. |
| **Virtual Interfaces tab** | |
| Name | Name of the network endpoint of the virtual entity. |
| Type | Type of the virtual entity network endpoint. |
| IP Address | Primary IP address of the virtual entity network endpoint. |
| MAC Address | MAC address of the virtual entity network endpoint. |
| Duplex Mode | Communication mode, which could be one of the following:<br>• Half—Transmit data in one direction at a time.<br>• Full—Transmit data in both the directions at the same time. |

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-9
- Severity Icons, page A-12
- Buttons, page A-12
- Badges, page A-18


## 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-9

# Network Element Icons

*Table A-1 Prime Network Vision Network Element Icons*

| Icon | Network Element |
|---|---|
| | Access pseudowire<br>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:<br>• A device has been deleted via Prime Network Administration, but remains in the map.<br>• 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)<br>Ethernet flow point (EFP)<br>MToP service |
| | Customer |
| | EFP cross-connect |
| | Ethernet service |
| | Ethernet virtual connection (EVC) |
| | Label-Switched Path (LSP) endpoint |
| | LSP midpoint |
| | 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 endpoint |
| | 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 |
| | IP Pool | BBA Groups |
| | Dynamic Config Templates | Policy Container |
| | QoS | |
| | Access Gateway | Multiple Spanning Tree protocol (MST) instance |
| | ARP Entity | OSPF Processes |
| | Bridges | Pseudowires |
| | Ethernet Link Aggregation | Routing Entities |
| | GRE Tunnels | Traffic Engineering Tunnels |
| | ICCP Redundancy container | VC Switching Entities |
| | IMA Groups | VRFs |
| | Local Switching | VSIs |
| | LSEs | VPC Domain |
| | MLPPP | BNG |
| | MPBGPs | DHCP Service |
| | Multicast | |
| | AAA Group | |
| | Probe | |
| | Y.1731 Probe | |
| | Bridge | |

*Table A-3 Logical Inventory Icons (continued)*

| Icon | Logical Inventory Item |
|---|---|
| | Connectivity Fault Management (CFM) Maintenance Association |
| | CFM Maintenance Domain |
| | 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 |
| | GGSN / SAE-GW / P-GW / S-GW / EGTP / GTPP container |

*Table A-3 Logical Inventory Icons (continued)*

| Icon | Logical Inventory Item |
|---|---|
| | GGSN / SAE-GW / P-GW / S-GW / EGTP / GTPP |
| | GTPU |
| | APN container |
| | APN |
| | ACS |
| | Operator policy |
| | APN profile / APN remap |
|  | Virtual data center |
| | Data store |
| | Data stores container |
| | Host server or hypervisor |
| | Host servers/hypervisor container |
| | Virtual machine |
| | Virtual machines container |

# Physical Inventory Icons

Table A-4 describes the icons used in physical inventory.

*Table A-4 Physical Inventory Icons*

| Icon | Device |
|---|---|
| | Chassis |
| | Satellite |
| | 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-11

# 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 |

*Table A-5 Prime Network Vision Link Icons (continued)*

| Icon | Description | Icon | Description |
|---|---|---|---|
| | 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 | | |

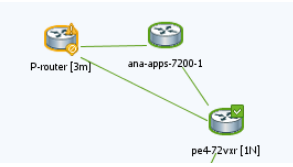
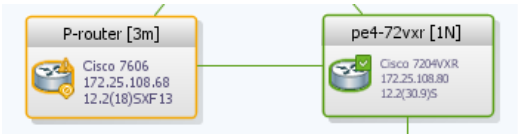
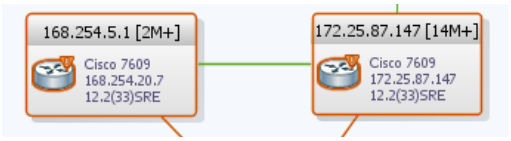
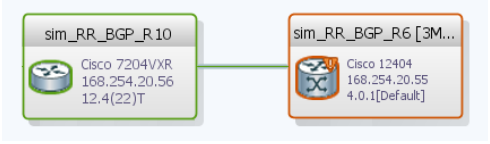
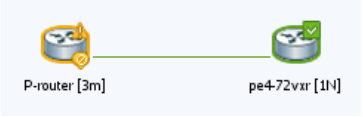
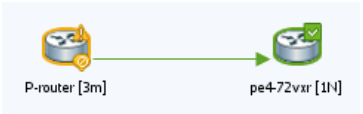
# Link Colors

*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:<br>• Business<br>• GRE<br>• MPLS-TP<br>• Pseudowire<br>• VLAN<br>• All others |
|  | Wide—Aggregated links that contain links of different groups.<br>When viewing a map at a low zoom level, aggregated links cannot be distinguished in the GUI. |
|  | 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 |
| | 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-13
- Table Buttons, page A-15
- Link Filtering Buttons, page A-16
- Prime Network Events Buttons, page A-16

- Ticket Properties Buttons, page A-17
- 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** | |
| | 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.<br>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. |

*Table A-9 Prime Network Vision Buttons (continued)*

| Button | Function |
|---|---|
| **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.<br>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.<br>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. |
| | 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. |

*Table A-9 Prime Network Vision Buttons (continued)*

| Button | Function |
|---|---|
| | 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. |

*Table A-10 Table Buttons (continued)*

| Icon | Name | Description |
|---|---|---|
| | 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*

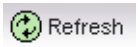
| Button | Function |
|---|---|
| | Displays the previous page of events in the Prime Network Events window. |
| | Displays the next page of events in the Prime Network Events window. |
| | Refreshes the events displayed in the log by querying the database. If a filter is active, the refresh is done 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. |

*Table A-12 Prime Network Events Buttons (continued)*

| Button | Function |
|---|---|
| | 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.<br>If a ticket was acknowledged, and some events were correlated to it afterward, then the ticket is considered to have not been acknowledged.<br>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.<br>This button is enabled only if the severity of the alarm is higher than Cleared or Normal. |
| | Saves the notes for the selected ticket.<br>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. |

*Table A-14 Report Manager Buttons (continued)*

| Icon | Name | Description |
|---|---|---|
| | 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-19
- 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. |

*Table A-15 VNE Communication State Badges (continued)*

| Badge | State Name | Description |
|---|---|---|
| | 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.)<br>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).<br>To extend Prime Network functionality so that it recognizes unsupported devices, use the VNE Customization Builder. See the *Cisco Prime Network 3.10 Customization 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. |
| 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 3.10 Administrator Guide*. |

*Table A-16 VNE Investigation State Badges (continued)*

| Badge | State Name | Description |
|---|---|---|
| | 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:<br>• Does not poll the device, but handles syslogs and traps.<br>• Maintains the status of any existing links.<br>• Does not fail on VNE reachability requests.<br>• 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.<br>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 3.10 Customization 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 |

*Table A-17 Network Element Technology-Related Badges (continued)*

| Icon | Description |
|---|---|
| | REP blocking primary |
| | REP primary |
| | Redundancy service |
| | STP root |

# Alarm and Ticket Badges

See Severity Icons, page A-12 for information about the icons used for alarm and ticket badges.

# GLOSSARY

## A

**AAA** — AAA refers to Authentication, Authorization, and Accounting, which is a security architecture for distributed systems that determines the access given to users for specific services and the amount of resources they have used.

**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.

**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; or 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.

## B

**BFD** — 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.

**BNG** — Broadband Network Gateway (BNG) provides capabilities that help to improve the service provider's ability to manage the subscriber's services, and simplify overall network operations.

**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.

## C

**carrier grade NAT** A large-scale Network Address Translation (NAT) that provides translation of millions of private IPv4 addresses to public IPv4 addresses.

**CCM** 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.

## D

**data center** A centralized repository, either physical or virtual for the storage, management, dissemination of data and information organized around a particular manner. In other words, it is a facility used to house computer systems and associated components, such as telecommunications and storage systems.

**DHCP** Dynamic Host Configuration Protocol is used to automate host configuration by assigning IP addresses, delegating prefixes (in IPv6), and providing extensive configuration information to network computers.

**dynamic links** The physical and logical links that exist between elements in the network. These links are discovered by Prime Network using various protocols (such as STP, CDP, and LLDP).

**dynamic templates** Used to group configuration items, which are later applied to a group of subscribers. This template is globally configured through the command line interface (CLI).

## E

**ePDG** Secures the data transmission with a UE connected to the EPC over an untrusted non-3GPP access. For this purpose, the ePDG acts as a termination node of IPsec tunnels established with the UE.

**event** In the context of network management, a discrete activity that occurred at a specific point in time.

**E-LMI** Ethernet Local Management Interface (E-LMI) is a protocol that operates between the customer edge (CE) network element and the provider edge (PE) network element. Ethernet LMI is a protocol between the CE network element and the provider edge (PE) network element.

## F

**FabricPath** An innovation in Cisco NX-OS software that brings the stability and scalability of routing to Layer 2. It provides a foundation to build a scalable fabric—a network that itself looks like a single virtual switch from the perspective of its users.

**Foreign Agent** A router on a mobile node's visited network that provides routing services to the mobile node. The FA acts as a mediator between the mobile node and it's home agent (HA).

## G

**GRE** 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.

## H

**Home Agent** A router on a mobile node's home network which tunnels datagrams for delivery to the mobile node when it is away from home. It maintains current location (IP address) information for the mobile node. It is used with one or more foreign agents.

**HSGW** HRPD Serving Gateway, a component in the evolved High Rate Packet Data (eHRPD) mobile network. It terminates the eHRPD access network interface from the Evolved Access Network (eAN) or Evolved Packet Core Function (ePCF) and routes UE-originated or terminated packet data traffic.

**HSRP** Hot Standby Router Protocol (HSRP) is a protocol that provides backup to a router in case of failure. Using HSRP, several routers are connected to the same Ethernet network segment and work together to present the appearance of a single virtual router.

**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.

## I

**IP Multicast** A bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to thousands of corporate recipients and homes.

**IP Pool** An IP pool is a sequential range of IP addresses within a certain network. IP addresses can be assigned dynamically from a single pool or from a group of pools for services running on a network element.

**IPSec** The Internet Protocol Security suite that interacts with one another to provide secure private communications across IP networks.

**IS-IS** 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.

## L

**LAC** Layer 2 Tunnel Access Concentrator, which allows users and telecommuters to connect to their corporate intranets or extranets using L2TP. In other words, it forwards packets to and from the LNS and a remote system.

**link** A physical or logical connection between two devices in the network, a device and an aggregation, or two aggregations.

**LMA** Local Mobility Anchor is the home agent for a mobile node in a Proxy Mobile IPv6 (PMIPv6) domain. It is the topological anchor point for mobile node home network prefixes and manages the binding state of an mobile node.

**logical link** An association between two network elements (based on a chain of physical links between the elements); for example, a tunnel.

## M

**managed element** A network element that is managed by Prime Network; for example, a device, cloud, or Internet Control Message Protocol (ICMP) VNE.

**MLPPP** Multilink PPP 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.

## N

**network clock service** 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 element** Any physical component or device in the network that can be managed through an IP address.

## P

**PDSN** Packet Data Serving Node is a component of the Code Division Multiple Access (CDMA) 2000 mobile network. It acts as a connection point between the Radio Access Network (RAN) and IP Network.

**physical link** A link between physical network objects; for example, a connection between two physical ports.

**provider** The party providing a service.

**pseudowire** An emulation of a point-to-point connection over a packet-switching network (PSN), which operates over a uniform packet-based access/aggregation networ

**pseudowire headend** A technology that allows termination of access or aggregation pseduowires into an L2 or L3 domain. It replaces a 2-node solution with a 1-node solution.

## Q

**QoS** Quality of services is the technique of prioritizing traffic flows and specifying preferences for forwarding packets with higher priority.

## S

**SBC** Session Border Controllers control and manage real-time multimedia traffic flows between IP network borders, handling signaling, and media.

**static links** Links that are created at the VNE level but are not updated. These links do not perform any configuration or provisioning on a device or in the network.

**subscriber** The party receiving a service.

**subscriber access points** The access interfaces that are named based on the parent interface.

## T

**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.

## U

**unassociated bridges** Switching Entities that do not belong to a flow domain, such as a network VLAN, a VPLS instance, or a network pseudowire.

## V

**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.

**virtualization** A concept of creating a virtual version of any resource, such as hardware platform, operating system, storage device, or network resources

**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.

**VPC** Virtual Port Channel (vPC) allows links that are physically connected to two different Cisco Nexus 7000 or Cisco Nexus 5000 series network elements to appear as a single port channel by a third device.

**VPLS** Virtual Private LAN Service 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.

**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.

**VRRP** Virtual Router Redundancy Protocol 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.

## Y

**Y.1731** Y.1731 is an ITU-T recommendation that provides mechanisms for service-level Operation, Administration, and Maintenance (OAM) functionality in Ethernet networks.

# INDEX

## Numerics


3.6.x tabs, in Prime Network Events 9-12
6rd tunnels, viewing properties 19-46
6VPE
  and IPv6 18-1
  IPv6 VPN over MPLS 18-1


## A


A 26-55, 26-65
AAA
  diameter configuration 23-6
  radius configuration 23-7
AAA configuration 23-1
  supported protocols 23-1
AAA configurations
  view 23-2
AAA group 23-2
aaa groups 23-2
access gateway
  badge 3-8, A-20
  viewing properties 13-19
accumulating affected parties
  in an alarm 10-23
  in the correlation tree 10-23
acknowledged tickets 10-7
acknowledging tickets 10-19
ACS
  overview 26-116
activating images on devices (NEIM)
  Cisco IOS XR devices and 4-35
  permissions 4-56, 4-57
activation script, launching 2-37, 5-1
active charging service 26-116
adding
  associated VLANs 13-54
  EFP cross-connects 13-75
  Ethernet services 13-105
  MPLS-TP tunnels 19-5
  pseudowires 13-89
  unassociated bridges 13-72
  VLANs 13-49
  VPLS instances 13-78
  VPNs
    existing 19-22
    new 19-21
address family ipv4 profile 20-4
address family ipv6 profile 20-5
administration
  global settings 4-47
Advanced tab
  events 9-17
  tickets 10-18
affected elements, finding 10-19
affected parties 10-22
  accumulating 10-23
  Affected Parties tab (tickets) 10-14
  calculating 10-22
  finding 10-19
affected severity, updating over time 10-24
Agent Not Loaded, VNE communication state 2-20
Agent Unreachable, VNE communication state 2-20
aggregation, definition 1-1
aggregations
  adding elements to 5-18

aggregating network elements 5-16
disaggregating 5-19
viewing thumbnails 5-16
working with thumbnail views 5-15, 5-18
alarm count, definition 10-6
alarms
badges A-21
customizing 2-39
definition 1-1
disabling on a port 3-26
severities 10-22
All tab, in Prime Network Events 9-3
APN
additional characteristics 26-18
overview 26-13
view properties 26-14
APN profiles 26-105
APN remaps 26-105
application, launching external 2-32, 2-37, 5-1
applying overlays
Ethernet service 13-106
MPLS-TP tunnels 19-16
network clock 21-49
pseudowire 13-97
VLAN 13-60
VPLS instance 13-79
VPN 19-24
ARP table 19-34
associated VLANs
adding 13-54
tag manipulations 13-54
viewing
mapping properties 13-56
service links 13-56
working with 13-54
association, definition 1-1
ATM cross-connects
in logical and physical inventory 21-6
overview 21-6
properties 21-7
viewing 21-6
audience, intended xxiii
audio options, customizing 2-39
Audit tab
events 9-17
in Prime Network Events 9-3
auto refresh, in Prime Network Events 9-21


## B


background images for maps 5-12
backing up files to archive (CM) 4-17, 4-56, 4-57
badges
access gateway 3-8, A-20
alarms 2-18, A-21
blocking 3-8, A-20
clock service 3-8, A-20
for elements and links 3-8
icons A-18
lock 3-8, 19-6, A-20
management states A-18
multiple links 3-8, A-20
reconciliation 3-9, 7-7, 13-49, A-20
redundancy service 3-9, A-21
REP primary 3-9, A-21
REP primary blocking 3-9, A-21
STP root 3-9, A-21
technology related A-20
tickets A-21
VNE communication states A-18
VNE investigation states A-19
VNE management states 2-18
bba groups 25-3
BFD
configuration commands 19-55
template commands 19-55
viewing BFD session properties 19-47
viewing MPLS-TP BFD session properties 19-49

BGP, viewing inventory details 19-45
Bidirectional Forwarding Detection. See BFD
blocked ports, using with Cisco PathTracer 12-4
blocking badge 3-8, A-20
bng 25-1
  retail model 25-2
  subscriber access points 25-5, 25-6
  user roles 25-2
  wholesale model 25-2
bridges
  understanding unassociated 13-72
  viewing properties for VLANs 13-69
broadband access groups 25-3
broadband network gateway
  overview 25-1
bulk lock mpls tp tunnels 19-55
bulk unlock mpls tp tunnels 19-55
business configurations 7-7
business elements
  definition 1-1
  icons 2-10, A-4
  roles required 7-1
business tag
  definition 1-1
  roles required 7-1
  searching for 7-4
  using Chinese characters 7-2
  working with 7-3
buttons A-16
  for filtering links A-16
  in table toolbars A-15
  Prime Network Events
    Auto Refresh 9-21
    Refresh Now 9-21
    Ticket Properties dialog box A-17
    toolbar A-16
  Prime Network Vision A-12
    link filtering A-16
    table toolbar A-15
    toolbar A-13
  Report Manager toolbar A-17

## C

callouts, VPN service overlay 19-25
Carrier Ethernet services, monitoring 13-1, 14-1
Carrier Grade NAT
  Add CGNAT or 6rd forwarding 13-118, 14-6
  Create CGNAT instance 13-118, 14-6
  Pool Utilization (command) 14-5
  roles required for viewing properties 14-2
  viewing properties
    logical inventory 14-2
    physical inventory 14-5
Carrier Supporting Carrier (CSC) path traces 12-31
CEM groups
  configured on
    physical interfaces 21-52
    virtual CEM interfaces 21-53
  viewing in
    logical inventory 21-53
    physical inventory 21-52
  viewing properties 21-51
CEM interfaces
  properties 21-52
  viewing in physical inventory 21-51
CESoPSN, viewing properties 21-3
CFM
  description
    maintenance domains 16-3
    maintenance endpoints (MEPs) 16-3
    maintenance intermediate points (MIPS) 16-3
  overview 16-3
  viewing properties for
    maintenance associations 16-8
    maintenance domains 16-5, 16-7
    MEPs 16-8
    MIPs 16-6

remote MEPs 16-10
Change and Configuration Management
global settings 4-47
change logs (CM) 4-23, 4-56, 4-57
Chinese characters
support for business tags 7-2
Circuit Emulation Services over PSN. See CESoPSN
Cisco.com credentials for NEIM 4-7
Cisco Discovery Protocol (CDP) properties
in logical inventory 13-6
in physical inventory 13-8
viewing 13-6
Cisco IOS XR devices
committing image changes (NEIM) 4-39
logical routers and 4-35
rolling back images (NEIM) 4-40
special notes for NEIM 4-35
Cisco PathTracer
across CSC configurations 12-31
comparing paths 12-27
counter values, saving 12-26
destinations 12-11
details pane 12-25
details window
menu options 12-22
toolbar 12-22
in MPLS networks 12-29
launching from
Ethernet Flow Point (EFP) 12-8
Ethernet port 12-12
examples 12-7
IP interface 12-9
MPLS-TP tunnel endpoint 12-13
pseudowire endpoint 12-12
VLAN bridge 12-10
Layer 2 VPNs 12-32
Layer 3 VPNs 12-32
menus 12-16
opening 12-3
overview 12-1, 12-2
path pane 12-18
path trace
from inventory 12-7
from map view 12-5
options for starting 12-5
path trace pane 12-18, 12-23
rerunning paths 12-27
right-click
options in path trace window 12-19
trace launch options 12-4
roles required 12-1
single-path window 12-16
starting points 12-30
tabs 12-18
toolbar 12-17
viewing
Layer 2 Tunnel Protocol path information 12-28
path trace details 12-20
path traces 12-14
QinQ path information 12-27
Cisco Prime Network
setup tasks 4-3
clear flash
image distribution 4-30
clearing and removing tickets 10-21
clearing tickets 10-7, 10-20
clock recovery, pseudowire properties 21-45
clock service
badge 3-8, A-20
properties 21-35
CM
archive, using 4-11, 4-56, 4-57
backing up files to archive 4-17
change logs 4-23
comparing files 4-13
deleting files from archive 4-22
exporting files 4-15
labels and 4-12

permissions 4-56, 4-57
restoring files from archive to devices 4-20
setup tasks 4-5
synchronizing files 4-16
color coding, severity icons 8-4
commands
fabricpath 27-9
mobile 26-133
vPC 27-5
committing image changes (NEIM) 4-39, 4-56, 4-57
communication status, for VNEs 3-17
comparing files (CM) 4-13, 4-56, 4-57
configuraiton audit
schedule 4-44
configuration audit 4-42
view result 4-45
configuration management
permissions 4-56, 4-57
configuration policy
create 4-43
manage 4-43
sample 4-43
sample CLIs 4-42
configuration scripts, launching 2-37, 5-1
Configuring Automatic Protection Switching (APS ), page 21-61 21-1
Configuring BGP, page 19-59 19-1
Configuring Bundle Ethernet, page 19-61 19-1
Configuring Clock, page 21-56 21-1
Configuring IP Interface, page 19-54 19-1
Configuring MPLS, page 19-57 19-1
Configuring MPLS-TE, page 19-57 19-1
Configuring MPLS-TP, page 19-54 19-1
Configuring RSVP, page 19-58 19-1
Configuring SONET, page 21-54 21-1
Configuring TDM and Channelization, page 21-59 21-1
Configuring VRF, page 19-53 19-1
Configuring VRRP, page 19-60 19-1
configuring y.1731 probes 17-4
Connecting, VNE communication state 2-20
Connectivity Fault Management. See CFM
content pane
in Prime Network Vision 2-7
in the Prime Network Vision inventory window 3-13
tabs in logical inventory 3-30
Control Channel (CC), viewing information for pseudowire endpoint 13-94
conventions, used in this document xxvi
Correlation tab (tickets) 10-17
CPU usage graph, opening 5-27
create
configuration policy 4-43
creating
maps 5-6
report folders 11-46
VPNs 19-21
cross-connects
ATM
overview 21-6
properties 21-7
viewing 21-6
EFP
adding 13-75
overview 13-74
properties 13-75
cross-VRF routing entries 19-49
Currently Unsynchronized, VNE investigation state 2-21
customizing
audio options 2-39
event history size 2-39


## D


Daily Average and Peak report 11-12
Daily Event Count by device report 11-15
data center 27-1
data store
view configuration 27-11

Defined Not Started, VNE investigation state 2-20
defining report types 11-46
deleting
business elements 7-7
report folders 11-48
reports 11-44
deleting files from archive (CM) 4-22
deleting images from repository (NEIM) 4-41
Dense Wavelength Division Multiplexing. See DWDM
destination, for Cisco PathTracer 12-11
Detailed Audit Events report 11-17
Detailed Provisioning Events report 11-17
Detailed Security Events report 11-18
Detailed Service Events report 11-15
Detailed Syslogs report 11-16
Detailed System Events report 11-18
Detailed Tickets report 11-16
Detailed Traps report 11-16
details pane, Cisco PathTracer 12-25
Details tab
events 9-15
tickets 9-19, 10-12
Device Partially Reachable, VNE communication state 2-20
devices
aggregations 5-16
CPU usage, checking 5-27
icons 2-7, A-2
in maps 5-16
pinging 5-28
severity indicator 2-17
status indicators 2-16
Telnet to a device 5-28
viewing
operating system information 3-31
properties 3-6
Devices with the Most Events report
by severity 11-12
by type 11-12
Devices with the Most Syslogs report 11-13
Devices with the Most Traps report 11-13
Device Unreachable, VNE communication state 2-20
device view pane
in the Prime Network Vision inventory window 3-13
toolbar 3-14
dhcp service 25-7
diagnose subscriber access points 25-6
disaggregating aggregations 5-19
Discovering, VNE investigation state 2-21
discovery
based on Link OAM 16-14
EFD 13-44
EVC multiplex services 13-105
MPLS-TP tunnels 19-5
VLAN 13-44
distributing images to devices (NEIM) 4-27, 4-35, 4-56, 4-57
document
audience xxiii
conventions xxvi
organization xxiv
related documentation xxvii
duplication count, definition 10-6
DWDM
channel, configure 15-15
commands 15-15
history (commands) 15-15
laser state, setting 15-15
loopback, setting 15-15
roles required for viewing properties 15-1
thresholds, setting 15-15
viewing
alert and alarm counters 15-10
G.709 properties 15-5
ODU alarm properties 15-8
ODU alert properties 15-9
OTU alarm properties 15-8
OTU alert properties 15-9
performance monitoring configuration 15-11

properties 15-3
dynamic authorization profile 23-3
dynamic config templates 25-9
ppp template 25-11
dynamic host configuration protocol 25-7


## E


EFD discovery 13-44
EFP
launching a path trace 12-8
overview 13-46
understanding severity and ticket badges 13-37
EFP cross-connects
adding 13-75
viewing properties 13-75
working with 13-74
egress adjacents, VRF 19-31
EGTP
overview 26-29
element icons, and information displayed 3-3
elements, business
deleting 7-7
renaming 7-7
elements, viewing operating system information 3-31
e-mail notification
configuration settings 4-6, 4-51
image management settings 4-7
Ethernet flow domains
renaming 13-41
viewing 13-41
Ethernet Flow Domains inventory tab 2-4
Ethernet flow point (EFP), viewing properties 13-32
Ethernet LAGs
viewing 13-22
viewing properties 13-23
Ethernet links, and configured LSPs 19-11
Ethernet LMI
commands 16-18, 16-21
Device EVC Properties window 16-12
enable 16-18, 16-21
EVC, configure 16-18, 16-21
overview 16-10
service instance, configure 16-18, 16-21
UNI, configure 16-18, 16-21
viewing properties
for device EVCs 16-11
for physical interfaces 16-12
for UNI interfaces 16-13
in logical inventory 16-11
Ethernet Local Management Interface. See Ethernet LMI
Ethernet OAM
overview 16-2
roles required for viewing properties 16-1
Ethernet Operations, Administration, and Maintenance. See Ethernet OAM
Ethernet port, launching a path trace 12-12
Ethernet Service report
detailed 11-21
options 11-36
summary 11-21
Ethernet services
adding overlays 13-106
adding to maps 13-105
viewing properties 13-108
working with 13-104
EVC (E-LMI), configure 16-18, 16-21
EVC (L-OAM), configuring 16-22
EVC multiplex services, discovery 13-105
EVCs
shared switching entities 13-39
viewing service properties 13-39
event history size, customizing 2-39
Event Reduction Statistics report 11-13
events
Advanced tab 9-17
Audit tab 9-17
categories 8-4

definition 1-2
Details tab 9-15
filtering 9-22, 9-23
Provisioning tab 9-17
refreshing list in Prime Network Events 9-21
removing filters 9-24
Security tab 9-17
Trap tab 9-18
viewing
in Prime Network Events 9-2
properties 9-14
events reports 11-11
detailed network events, report options 11-28
detailed non-network events, report options 11-31
generating from
Prime Network Vision 11-39
Report Manager 11-24
Reports menu 11-38
report options 11-26
Run Report dialog box 11-25
exporting data from
Prime Network Events 9-25
exporting files (CM) 4-15, 4-56, 4-57
external application, launching 2-32, 2-37, 5-1


## F


fabricpath 27-6
Fault Database vs. Event Archive Statistics report 11-13
FEC commands 15-15
filtering
events 9-22, 9-23
links
by type 5-26, 5-27
during map creation 5-26
in an existing map 5-27
using collection method 6-17
removing for events and tickets 9-24
tickets
by criteria 10-8
flickering links 6-3
foreign agent 26-65
advertisement 26-68
authentication 26-69
configuration 26-65
GRE configuration 26-70
HA configuration 26-71
proxy mobile 26-73
registration revocation 26-73


## G


G.709 commands 15-15
General tab, in inventory window 3-13
generated ticket 10-7
GGSN
overview 26-6
view properties 26-7
global settings 4-47
NEIM 4-53
GPRS/UMTS network 26-4
working technologies 26-6
graphical links, reducing number of in maps 2-11
GTPP
additional characteristics 26-25
overview 26-23
view properties 26-24, 26-30
GTPU
overview 26-11
view properties 26-11
GUI
overview of 4-1


## H


Hardware Summary By Selected Property 11-19
Hardware Summary Detailed report 11-19

History tab (tickets) 10-13
home agent 26-57, 26-59
AAA configuration 26-62
configuration 26-59
GRE configuration 26-63
policy configuration 26-63
registration revocation 26-64
topology 26-59
host server
view configuration 27-11
HSGW 26-44
a10/a11 configuration 26-49
basic features 26-45
GRE parameters 26-50
IP source violation 26-52
MAG configuration 26-52
MAG service 26-55
profile-qci mapping 26-56
topology 26-44
view configuration 26-46
HSRP
view properties 13-17
H-VPLS
working with 13-77
working with in Prime Network Vision 13-77

## I

icons
*See also* buttons *and* badges
alarm and ticket A-21
badges A-18
business elements 2-10, A-4
information displayed for elements 3-3
links A-9
logical inventory 3-30, A-6
management states 2-18, A-18
maps 19-20
map view 2-8
network elements 2-7, 2-9, A-2
physical inventory 3-19, A-9
Prime Network Events A-12
Prime Network Vision 2-8, A-1
reconciliation 3-9
reference A-1
REP 13-62
severities A-12
severity, color coding 2-17, 8-4
sizes 2-8, 3-3
tickets 2-22
VLAN domains 13-62
VLAN overlays 13-62
IGMP profile 20-5
image management
permissions 4-56, 4-57
IMA group
properties 21-13
viewing properties 21-13
impact analysis
accumulating affected parties 10-22
affected severities 10-22
automatic mode 10-22
links and 6-12
proactive mode 10-22
importing images into archive (NEIM) 4-24
In 26-62
Initializing management state 2-18
Inter-Chassis Communication Protocol (ICCP), viewing properties 13-28
inventory reports 11-19
generating from
Prime Network Vision 11-39
Report Manager 11-32
Reports menu 11-38
report options 11-33
Run Report dialog box 11-33
inventory tabs
Ethernet Flow Domains 2-4

in Prime Network Vision 2-4
Network Elements 2-4
types of 2-4
VTP Domains 2-4
inventory window
content pane 3-13
device view pane 3-13
device view pane toolbar 3-14
General tab 3-13
logical inventory 3-27
navigation pane 3-12
Network Events tab 3-15
opening 3-9
options
Disable Sending Alarms button 3-21, 21-6
Open Port Utilization Graph button 3-21, 21-6
Show Cross-Connect Table button 3-21, 21-6
Show DLCI Table button 3-21, 21-6
Show Encapsulation button 3-21, 21-6
Show VC Table button 3-21, 21-6
overview 3-9, 3-11
physical inventory 3-19, 3-21, 21-6
Ports tab 3-13, 3-23
Provisioning Events tab 3-15
ticket and events pane 3-15
Tickets tab 3-15
IOS-XR Software Package Summary report 11-20
IP 26-52
ip and mpls multicast configuration 20-1
IP interface, launching a path trace 12-9
IPoDWDM
See also DWDM
IPoDWDM commands 15-15
IP pools 24-1
IP SLA, viewing responder service properties 13-111
ip subscriber template 25-9
IPv6
addresses
in logical inventory 18-3
in physical inventory 18-4
in inventory 18-3
in Prime Network 18-2
notes, for viewing IPv6 addresses 18-4
support in Prime Network 18-1
viewing IPv6 information 18-2
IPv6 VPN over MPLS (6VPE) 18-1
IS-IS, viewing properties 13-113


## J


jobs
CM 4-56, 4-57
e-mail notification 4-55
NEIM 4-56, 4-57
jobs scheduler 11-40


## L


labeling files (CM) 4-12, 4-56, 4-57
labels, MPLS-TP tunnel (commands) 19-54
LAC 26-39
view configuration details 26-40
launching Prime Network Events
from Prime Central 8-2
in Find mode 8-3
launching Prime Network Vision
as a standalone application 2-2, 8-2
from Prime Central 2-2
Layer 2 Cisco PathTracer (VPN) 12-32
Layer 3 Cisco PathTracer (VPN) 12-32
link aggregation group. See Ethernet LAGs
Link Layer Discovery Protocol (LLDP), viewing properties 13-8
Link OAM
and topology discovery 16-14
commands 16-22
enabling and disabling 16-22
EVCs, configuring 16-22

overview 16-14
remote loopback, enabling and disabling 16-22
templates, managing 16-22
viewing properties in
logical inventory 16-15
physical inventory 16-18
link properties window
link list pane 6-11
overview 6-10
properties pane 6-11
ticket and events pane 6-12
links
adding 6-15
arrowheads 6-5, A-11
bidirectional vs. unidirectional 6-5, A-11
colors 6-5
dashed line 6-4, A-11
definition 1-4
dynamic 6-3
exceeding number that can be displayed 2-10
filtering A-16
by type 5-26, 5-27
in maps 5-25
using collection method 6-17
flickering 6-3
graphical representation 2-10
icons A-9
impact analysis 6-12
in maps 2-10
links view 6-8
normal vs. wide vs. tunnel 6-5
overview 6-1
properties 6-4
quick view 6-7
reducing number of in maps 2-11
selecting in maps 6-18
significance of
arrowheads A-11
characteristics A-11
color A-10
solid vs. dashed lines A-11
width A-11
solid line 6-4, A-11
static 6-3
tooltips 2-11, 6-6
tunnels 6-5
types A-9
use of arrowheads 6-5
user roles required for working with 6-1
viewing
between VLAN elements and devices 13-57
in links view 6-8
options 6-17
properties 6-4, 6-10
width 6-5
links, MPLS-TP tunnel (commands) 19-54
links view
filtering 2-16, A-16
information displayed 2-15
in Prime Network Vision 2-14
list view
in Prime Network Vision 2-11
overview 2-11
right-click options 2-13
toolbar 2-41, A-15
LLDP, viewing properties 13-8
lock badge 3-8, A-20
lock mpls tp tunnels 19-56
logical inventory
branches 3-29
content pane 3-30
content pane tabs 3-31
icons 3-30, A-6
navigation pane 3-29
tabs 3-31
viewing in Prime Network Vision 3-27
window 3-28
logical link, definition 1-4

logical routers (Cisco IOS XR) 4-35
loopback, remote (L-OAM), enabling/disabling 16-22
LSEs
  inventory details 19-39
  viewing 19-39
LSP
  LSP Lockout (commands) 19-54
  LSP Lookup (command 19-54
  LSP Ping and Trace (commands) 19-54
LSP endpoints 19-13
  properties 19-13
LSPs
  lockout state 19-6
  on Ethernet links 19-11
  properties 19-13
  redundancy service properties 19-13
  Working and Protected 19-5

## M

Maintenance, VNE investigation state 2-21
maintenance domains, in CFM 16-3
managed element, definition 1-4
management states
  badges A-18
  icons A-18
  overview 2-18
managing maps, roles required 5-2
managing report folders
  creating 11-46
  deleting 11-48
  moving 11-47
  renaming 11-47
  viewing properties 11-48
managing reports
  deleting 11-44
  moving reports 11-44
  renaming 11-42
  roles required 11-1
  saving 11-41
  sharing 11-43
  viewing
    report properties 11-45
    reports 11-41
managing tickets 10-19
managing VPNs 19-21
  adding to maps 19-22
  creating 19-21
  moving virtual routers between 19-23
  overlays
    adding 19-24
    displaying 19-25
    hiding 19-25
  removing from maps 19-23
maps
  adding VLANs 13-49
  aggregations 5-16
  applying background images 5-12
  Cisco PathTracer files 12-26
  closing 5-5
  creating 5-6
  customizing 2-39
  filtering links 5-25
  in Prime Network Vision 2-7
  link icons A-9
  network elements in 5-16
  opening 2-6, 5-5
  overlays
    callouts 19-25
    VPN 19-24
  overview 19-18, 19-19
  red border and graphical links 2-10
  removing
    VLANs 13-52
    VPNs 19-23
  roles required 5-2
  saving 5-15
  selecting views 5-12

using overview windows 5-14
viewing
aggregation thumbnails 5-16
thumbnails 5-16
VPNs
adding 19-22
overlays 19-24
viewing 19-18
working with 5-1
map view
adding VLAN overlays 13-60
in Prime Network Vision 2-7
multi chassis devices 5-19
Mean Time to Repair report 11-14
menus
Cisco PathTracer 12-16
Cisco PathTracer details window 12-22
Prime Network Events 8-6
Prime Network Vision 2-24
Report Manager 11-6
MEPs, in CFM 16-3
MIPS, in CFM 16-3
mldp database 19-42
mldp neighbors 19-43
MLPPP
viewing link properties 21-29
viewing properties 21-26
Mobile technologies 26-1
ACS 26-116
APN 26-13
commands 26-133
EGTP 26-29
GGSN 26-6
GTPP 26-23
GTPU 26-11
PDN-GW 26-34
SAE-GW 26-33
S-GW 26-36
mobile technologies
user roles 26-1
Mobile Transport over Packet. See MToP
modifying VNE properties 3-16
Modules Summary By Type 11-20
monitoring
Carrier Ethernet services 13-1
Carrier Grade NAT properties 14-1
network clocking service 21-34
PTP service 21-37
Most Common Daily Events report 11-14
Most Common Syslogs report 11-14
moving
report folders 11-47
reports between folders 11-44
MP-BGP properties in logical inventory 19-45
MPLS
ARP table 19-34
BGPs, viewing 19-45
Cisco PathTracer and 12-29
LSEs, viewing 19-39
monitoring services 19-26
NDP table 19-34
pseudowire end-to-end emulation tunnels, viewing 19-50
rate limit information 19-36
roles required for viewing properties 19-1
routing entities 19-31
TE tunnels, viewing 19-52
MPLS pseudowire over GRE, properties 21-32
MPLS TE tunnel, inventory details 19-52
MPLS-TP
BFD commands 19-55
MPLS-TP tunnel
label commands 19-54
MPLS-TP tunnel endpoint, launching a path trace 12-13
MPLS-TP tunnels
adding to maps 19-5
applying overlays 19-16
BFD sessions, viewing properties 19-49

commands supported 19-54
discovery 19-5
global configuration (commands)
Global Configuration Commands (MPLS-TP) 19-55
links, adding and removing 19-54
LSP commands 19-55
LSP lockout state 19-6
LSP Ping and Trace (commands) 19-54
overview 19-4
properties 19-7
Tunnel Ping and Trace (commands) 19-54
working with 19-4
mpls tp tunnels 19-55
MToP
channelized lines 21-17
IMA group properties 21-13
monitoring
network clocking service 21-34
PTP service 21-37
network clocking service 21-34
PTP service overview 21-37
roles required for working with 21-1
TDM
overview 21-16
viewing properties in physical inventory 21-17
viewing
ATM cross-connects 21-6
ATM VCI properties 21-10
ATM VPI properties 21-10
CEM groups 21-51, 21-52, 21-53
CEM interfaces 21-51
CEM properties 21-50
CESoPSN pseudowire properties 21-3
encapsulation information 21-11
IMA group properties 21-13
MLPPP link properties 21-29
MLPPP properties 21-26
network clocking service 21-34
pseudowire clock recovery properties 21-42
PTP service properties 21-37
SAToP pseudowire properties 21-2
SONET/SDH channelization properties 21-18
SyncE properties 21-46
T3 DS1 and DS3 channelization properties 21-21
TDM properties 21-17
virtual CEMs, list of 21-51
virtual CEMs properties 21-50
multicast configuration 19-30
overview 20-1
supported network elements 20-1
user roles required 20-2
multicast label distribution protocol 19-42
multicast label switching 19-42, 20-9
multicast profile
PIM profile 20-7
multicast protocol
IGMP profile 20-5
address family ipv6 20-5
multicast protocols 20-4
address family ipv4 20-4
multicast routing entities 20-10
multi chassis device
map view 5-19
Multichassis LACP (mLACP)
show commands 13-28
viewing properties 13-28
multiple links badge 3-8, A-20
multiplex services, discovery of 13-105


## N


navigation pane
logical inventory 3-29
physical inventory 3-19
Prime Network Vision 2-6
NDP table 19-34

NEIM
Cisco IOS XR devices and 4-35
committing image changes 4-39
deleting images from repository 4-41
distributing images to devices 4-27
global settings 4-53
importing images 4-24
permissions 4-56, 4-57
rolling back images on devices 4-40
setup tasks 4-6
upgrade analysis and 4-27
viewing repository 4-56, 4-57
Network Activation
Activation Framework 3-34
network clocking service
applying an overlay 21-49
clock service properties 21-35
monitoring 21-34
monitoring PTP service 21-37
overview 21-34
PTP interface properties 21-38
PTP service 21-37
network elements
adding to existing aggregations 5-18
aggregating 5-16
aggregations 5-16
CPU usage, checking 5-27
definition 1-4
icons 2-7, 2-9, A-2
information displayed in icons 3-3
in maps 5-16
management state 2-18
pinging 5-28
severity indicators and network elements 2-17
status indicators 2-16
Telnet to 5-28
viewing
operating system information 3-31
properties 3-6
Network Elements inventory tab 2-4
Network Events tab
inventory window 3-15
link properties window 6-12
network event tabs, in Prime Network Events 9-7
Network Pseudowire report
detailed 11-22
options 11-37
summary 11-22
network service reports 11-21
generating from
Prime Network Vision 11-39
Report Manager 11-35
Reports menu 11-38
report options 11-36
Run Report dialog box 11-35
Notes tab (tickets) 10-18, 10-19

## O

OAM
See also Link OAM
opening
maps 2-6
operating system information, viewing for devices 3-31
Operational, VNE investigation state 2-21
operator policy 26-105
options
working with aggregation thumbnails 5-15, 5-18
OSPF
supported versions 13-116
viewing properties 13-116
overlays
applying to
Ethernet services 13-106
maps 5-22
MPLS-TP tunnels 19-16
network clocks 21-49
pseudowire 13-97

VLANs 13-60
VPLS instances 13-79
VPNs 19-24
displaying and hiding
for VLANs 13-61
for VPNs 19-25
in maps 5-25
Ethernet service 13-106
pseudowire 13-89, 13-97
removing 13-61
viewing 5-25
pseudowire tunnel links in VPLS 13-81
REP information 13-62
STP information 13-65
VLAN
adding 13-60
removing 13-61
viewing STP link information 13-65
working with 13-44
VPLS
callouts 13-81
instance 13-79
viewing pseudowire tunnel links 13-81
VPN 19-24
adding 19-24
callouts 19-25
working with 5-21
overview
ATM cross-connects 21-6
CFM 16-3
Cisco PathTracer 12-1
EFP cross-connects 13-74
EFPs 13-46
Ethernet LMI 16-10
Ethernet OAM 16-2
Link OAM 16-14
MPLS-TP tunnels 19-4
network clocking service 21-34
Prime Network Events 1-2
Prime Network Vision inventory window 3-9
Prime Network Vision maps 2-5
PTP service 21-37
reports 11-1
SAToP 21-2
SBC 22-1
switching entities 13-45
TDM 21-16
unassociated bridges 13-72
VLANs 13-45
overview window 5-14


## P


package management, defined 4-35
Partially Discovered, VNE investigation state 2-21
password, changing 2-3
path pane, in Cisco PathTracer 12-18
path trace
and blocked ports 12-4
examples 12-7
launching from
EFP 12-8
Ethernet port 12-12
IP interface 12-9
MPLS-TP tunnel endpoint 12-13
pseudowire endpoint 12-12
VLAN bridge 12-10
starting 12-5
from inventory 12-7
from map view 12-5
viewing
in Cisco PathTracer 12-14
Layer 2 Tunnel Protocol path information 12-28
path trace details 12-20
QinQ path information 12-27
path trace details window 12-20
path trace pane, Cisco PathTracer 12-18, 12-23
PDN-GW

overview 26-34
P-GW
view properties 26-35
physical inventory
branches 3-19
buttons
Disable Sending Alarms 3-21, 21-6
Open Port Utilization Graph 3-21, 21-6
Show Encapsulation 3-21, 21-6
content pane 3-20
icons 3-19, A-9
navigation pane 3-19
viewing device properties 3-19
viewing in Prime Network Vision 3-19
window 3-14
physical link, definition 1-4
PIM profile 20-7
pinging
devices 5-28
network elements 5-28
ping pseudowire (command) 13-119
policy container 25-12
polling, initiating 3-18
Poll Now button 3-18
Pool Utilization (CG NAT command) 14-5
ports
alarms
disabling 3-26
viewing
configuration 3-25
status 3-23
with IPv4 and IPv6 addresses 18-5
Ports tab, in inventory window 3-13, 3-23
Port Utilization graph, generating 3-27
ppp template 25-9, 25-11
Prime Central
launching Prime Network Events 8-2
launching Prime Network Vision 2-2
Prime Network 3.6.x tabs, in Prime Network Events 9-12
Prime Network Command Builder
launching scripts 2-37, 5-1
Prime Network Events
All tab 9-3
Audit tab 9-3
buttons
Ticket Properties dialog box A-17
toolbar A-16
customizing 8-8
displaying all events 8-4
event categories 8-4
exporting data 9-25
icon severities A-12
launching
from Prime Central 8-2
in Find mode 8-3
options 8-2
menus 8-6
network event tabs 9-7
overview 1-2
Prime Network 3.6.x tabs 9-12
Provisioning tab 9-5
right-click options 8-7
roles required 8-1, 9-1
Security tab 9-6
Service tab 9-7
Syslog tab 9-8
system event tabs 9-3
System tab 9-6
Ticket tab 9-8
toolbar 8-5
toolbar buttons A-16
V1 Trap tab 9-10
V2 Trap tab 9-10
V3 Trap tab 9-11
viewing
all events 8-4
events and tickets 9-2
window 8-2

working with 9-14
Prime Network Vision
buttons A-12
filtering links A-16
table toolbar A-15
toolbar A-13
creating maps 5-6
customizing 2-39
generating reports 11-39
GUI overview 19-18, 19-19
icons 19-20, A-1
links A-9
logical inventory A-6
map A-2, A-4
physical inventory A-9
sizes 2-8
interface components 2-3
inventory tabs 2-4
launching
as a standalone application 2-2, 8-2
from Prime Central 2-2
options 2-2
links
characteristics A-11
colors A-10
icons A-9
list view toolbar A-15
maps 2-7, 2-39
closing 5-5
creating 5-6
opening 5-5
overview 2-5
saving 5-15
viewing options 5-12
menus 2-24
Activation 2-28
Edit 2-26
File 2-25
Help 2-29
Network Inventory 2-28
Node 2-27
Reports 2-29
right-click 2-29
Tools 2-27
View 2-26
Window 2-29
navigation 2-3
opening
the inventory window 3-9
overlays 19-25
port information 3-25
properties window 3-6
right-click menus 2-29
roles required 2-1, 3-1
tables
managing 2-40
toolbar buttons A-13
viewing tickets 10-3
VLAN elements and icons 13-45
windows 2-3
working with
H-VPLS 13-77
tickets 10-1
VPLS 13-77
Prime Network Vision window
content pane 2-7
inventory tabs 2-4
links view 2-14
list view
overview 2-11
toolbar 2-41
map view 2-7
icons 2-8
right-click options 2-11
severity indicators 2-11
navigation pane 2-6
right-click menus
aggregation 2-34

device 2-31
link 2-35
links view 2-37
list view 2-35
maps 2-30
ticket 2-38
ticket pane 2-16
toolbar 2-22
layout tools 2-24
map options 2-22
map zoom tools 2-24
navigation tools 2-23
overlay tools 2-23
viewing options 2-22
properties
6rd tunnels 19-46
CEM interface 21-52
clock service 21-35
ICCP 13-28
mLACP 13-28
MPLS pseudowire over GRE 21-32
MPLS-TP tunnels 19-7
MToP
ATM VCI 21-10
ATM VPI 21-10
pseudowire clock recovery 21-45
PTP interface 21-38
REP 13-14
report folders 11-48
report types 11-50
SBC 22-3
AAA 22-6
DBE 22-4
H.248 22-5, 22-7
media address 22-4
policy 22-7
SBE 22-5
SIP 22-10
virtual connections 21-5
properties window in Prime Network Vision 3-6
provider, definition 1-4
Provider Backbone Bridge (PBB), viewing properties 13-31
Provisioning Events tab, in the inventory window 3-15
Provisioning tab
events 9-17
in Prime Network Events 9-5
Proxy 26-73
proxy server
importing images from Cisco.com 4-7
pseudowire 13-99, 13-100
pseudowire clock recovery
properties 21-45
viewing properties 21-42
pseudowire endpoint, launching a path trace 12-12
pseudowire headend 13-100
associated routing entity 13-104
associated VRF entity 13-104
generic interface list 13-103
view configuration 13-101
pseudowires
adding 13-89
applying overlay 13-97
commands 13-119
overlays 13-89
pinging 13-119
redundancy service properties 13-95
viewing
endpoint properties 13-86
properties 13-92
redundancy service properties 13-95
tunnel links in VPLS overlays 13-81
VCCV and CC information 13-94
working with 13-89
PTP
interface properties 21-38
monitoring service 21-37
service overview 21-37

PWE3
inventory details 19-50
viewing 19-50

## Q

QCI-QoS mapping 26-38
QoS profile 25-15
quality of service profile 25-15
quick view, for links 6-7

## R

radius global configuration 23-4
rate limits, for routing entities 19-36
reconciliation badge A-20
aggregations 2-35
business elements 7-7
description 3-9
EFPs 13-49
switching entities 13-49
VPLS forwards 13-77
red border in maps, and graphical links 2-10
reduced polling 3-18
reduction count, definition 10-6
redundancy service 19-13
badge 3-9, A-21
on LSP endpoints 19-13
pseudowires 13-95
related documentation xxvii
removing
tickets 10-20
VLAN overlays 13-61
VLANs from maps 13-52
VPNs 19-23
renaming
Ethernet flow domains 13-41
report folders 11-47
reports 11-42
REP
icons and badges 13-62
viewing
for VLAN service link properties 13-63
in VLAN domain views 13-62
in VLAN overlays 13-62
report categories 11-11
report folders
creating 11-46
deleting 11-48
moving 11-47
renaming 11-47
viewing properties 11-48
working with 11-46
Report Manager
content pane 11-7
events reports 11-11
generating reports 11-24
inventory reports 11-19
menu options 11-6
navigation tree 11-7
network service reports 11-21
report categories 11-11
right-click options 11-9
roles required 11-1
toolbar buttons 11-6, A-17
using 11-4
report properties, viewing 11-45
reports
and database load 11-24
canceled 11-24
creating folders 11-46
defining types 11-46
deleting
folders 11-48
reports 11-44
events
Daily Average and Peak 11-12

Devices with the Most Events by severity 11-12
Devices with the Most Events by type 11-12
Devices with the Most Syslogs 11-13
Devices with the Most Traps 11-13
Event Reduction Statistics 11-13
Fault Database vs. Event Archive Statistics 11-13
Mean Time to Repair 11-14
Most Common Daily Events 11-14
Most Common Syslogs 11-14
Syslog Count by device 11-14
Syslog Count by type 11-14
Syslog Trend by severity 11-14
fail to generate 11-24
formats 11-41
generating 11-23
events reports 11-24
inventory reports 11-32
network service reports 11-35
generating from
Prime Network Vision 11-39
Report Manager 11-24
Reports menu 11-38
inventory
Hardware Summary By Selected Property 11-19
Hardware Summary Detailed 11-19
IOS-XR Software Package Summary 11-20
Modules Summary By Type 11-20
Software Version Summary by device 11-20
Software Version Summary by version 11-20
limiting access to 11-44
managing
maximum concurrent reports 11-40
options 11-40
maximum number of concurrent reports 11-40
moving
folders 11-47
reports between folders 11-44
network events
Detailed Event Count (by device) 11-15
Detailed Service Events 11-15
Detailed Syslogs 11-16
Detailed Tickets 11-16
Detailed Traps 11-16
network service
Ethernet Service Detailed 11-21
Ethernet Service Summary 11-21
Network Pseudowire Detailed 11-22
Network Pseudowire Summary 11-22
VPLS Detailed 11-23
VPLS Summary 11-23
non-network events
Detailed Audit Events 11-17
Detailed Provisioning Events 11-17
Detailed Security Events 11-18
Detailed System Events 11-18
options for
detailed network events reports 11-28
detailed non-network events reports 11-31
events reports 11-26
inventory reports 11-33
network service reports 11-36
overview 11-1
queued 11-40
renaming
folders 11-47
reports 11-42
Report Properties dialog box 11-45
roles required 11-1
saving 11-41
scheduling 11-39
sharing 11-43
using Report Manager 11-4
viewing 11-41
report folder properties 11-48
report properties 11-45
report type properties 11-50
working with folders 11-46
Reports menu, and generating reports 11-38

report types, viewing properties 11-50
REP primary badge 3-9, A-21
REP primary blocking badge 3-9, A-21
Resilient Ethernet Protocol (REP), viewing properties 13-14
restore mode (CM) 4-6
  merge 4-50
  overwrite 4-50
restoring files from archive to devices (CM) 4-20, 4-56, 4-57
right-click options
  aggregations 2-34
  Cisco PathTracer 12-4, 12-19
  devices 2-31
  links 2-35
  links view 2-37
  list view 2-13, 2-35
  maps 2-30
  Prime Network Events 8-7
  Prime Network Vision 2-11, 2-29
  Report Manager 11-9
  tickets 2-38
roles
  managing reports 11-1
  viewing
    Carrier Ethernet properties 13-2
    Carrier Grade NAT properties 14-2
    DWDM properties 15-1
    Ethernet OAM tool properties 16-1
    IPv6 information 18-2
    SBC properties 22-2
  working with
    business tags 7-1
    Cisco PathTracer 12-1
    links 6-1
    maps 5-2
    MPLS networks 19-1
    MToP 21-1
    Prime Network Events 8-1, 9-1
    Prime Network Vision 2-1, 3-1
    reports 11-1
    tickets 10-1
rolling back images on devices (NEIM) 4-35, 4-40, 4-56, 4-57
routers, logical (Cisco IOS XR) 4-35
routing entities 19-31
  ARP table 19-34
  NDP table 19-34
  rate limit information 19-36
  viewing properties 19-31
RTPM commands 15-15

## S

SAE-GW
  overview 26-33
SAToP, overview 21-2
saving
  maps 5-15
  reports 11-41
SBC
  AAA properties 22-6
  DBE properties 22-4
  H.248 properties 22-5, 22-7
  logical inventory properties 22-1
  media address properties 22-4
  overview 22-1
  policy properties 22-7
  properties 22-3
  SBE properties 22-5
  SIP properties 22-10
  user roles required for viewing properties 22-2
  viewing in logical inventory 22-3, 22-4
schedule configuration audit 4-44
scheduled jobs
  monitoring 11-40
scripts
  launching 2-37

launching for activation and configuration 5-1
Security tab
events 9-17
in Prime Network Events 9-6
service policy 25-12
Service tab, in Prime Network Events 9-7
service template 25-9
service view
overlays 19-25
removing VLANs 13-52
removing VPNs 19-23
virtual routers 19-23
VPNs 19-21, 19-26
Session Border Controller. See SBC
setup tasks
Cisco Prime Network 4-3
CM 4-5
global settings 4-47
NEIM 4-6
severity
color of device icon 2-18
icons A-12
indicators
in Prime Network Vision map view 2-11
overview 2-17
propagation 2-17
S-GW
overview 26-36
view properties 26-36
shared switching entities 13-39
sharing reports 11-43
Show Channel (mLACP command) 13-28
Show Group (mLACP command) 13-28
Show LACP Internal (mLACP command) 13-28
Show MPLS LDP (mLACP command) 13-28
Shutting Down, VNE investigation state 2-21
sites, viewing properties 19-27
Software Version Summary report
by device 11-20
by version 11-20
SONET/SDH, viewing properties 21-18
Spanning Tree Protocol. See STP
static link, adding 6-15
status indicators, for network elements 2-16
Stopped, VNE investigation state 2-21
STP
viewing
link information in VLAN overlay 13-65
properties 13-10
VLAN service link properties 13-66
viewing in
VLAN domain views 13-65
VLAN overlays 13-65
STP root badge 3-9, A-21
Structure-Agnostic TDM over Packet. See SAToP
subscriber, definition 1-5
subscriber access points 25-5
diagnose 25-6
switching entities
containing termination points 13-49
overview 13-45
synchronizing files (CM) 4-16, 4-56, 4-57
Synchronous Ethernet (SyncE), viewing properties 21-46
Syslog Count report
by device 11-14
by type 11-14
Syslog tab, in Prime Network Events 9-8
Syslog Trend report by severity 11-14
system event tabs, in Prime Network Events 9-3
System tab, in Prime Network Events 9-6

## T

T3 DS1 and DS3, viewing properties 21-21
tables
managing in Prime Network Vision 2-40
toolbar buttons A-15
tabs

in Cisco PathTracer window 12-18
tag manipulations, for associated VLANs 13-54
TDM
overview 21-16
viewing properties in physical inventory 21-17
Telnet to devices 5-28
termination points, in switching entities 13-49
TE tunnels and Cisco PathTracer 12-33
The 26-44
thumbnail views, options 5-15, 5-18
ticket and events pane, Prime Network Vision inventory window 3-15
ticket pane
information displayed 10-5
Prime Network Vision 2-16
ticket properties, Details tab 9-19
Ticket Properties dialog box
Advanced tab 10-18
Affected Parties tab 10-14
Correlation tab 10-17
Details tab 10-12
History tab 10-13
Notes tab 10-18, 10-19
toolbar 10-12
tickets
acknowledged 10-7
acknowledging 10-19
and EFP severities 13-37
badges A-21
clearing 10-7, 10-20
clearing and removing 10-21
definition 1-5
filtering
by criteria 10-8
finding
affected elements using the ticket pane 10-19
generated 10-7
icons 2-22
managing 10-19
propagating new 2-17
properties 10-10
removing 10-20
removing filters 9-24
right-click menu 2-38
roles required 10-1
status 10-6
viewing
in Prime Network Events 9-2
in Prime Network Vision 10-3
properties 10-12
working with in Prime Network Vision 10-1
Tickets tab
inventory window 3-15
link properties window 6-12
Prime Network Events 9-8
Time Division Multiplexing. See TDM or MToP TDM
To 13-103, 13-104, 26-49, 26-52, 26-59, 26-63, 26-64, 26-65, 26-68, 26-69, 26-70, 26-71, 26-73
toolbar buttons
Cisco PathTracer single-path window 12-17
for filtering links A-16
for tables A-15
Prime Network Vision list view A-15
Report Manager 11-6, A-17
Ticket Properties window 10-12
toolbars
Cisco PathTracer 12-17
Cisco PathTracer details window 12-22
device view pane 3-14
Prime Network Events 8-5
Prime Network Vision 2-22
Prime Network Vision list view 2-41
Report Manager 11-6
Ticket Properties window 10-12
tooltips for links 6-6
Tracking Disabled, VNE communication state 2-20
Trap tab (events) 9-18

## U


unassociated bridges
- adding 13-72
- overview 13-72

understanding
- EFP severity and ticket badges 13-37
- static and dynamic links 6-3
- unassociated bridges 13-72
- VLAN and EFD discovery 13-44

ungrouping aggregations 5-19
UNI (E-LMI), configure 16-18, 16-21
unlock mpls tp tunnels 19-56
unmanaged network, definition 1-5
Unsupported, VNE investigation state 2-20
updating
- affected severity 10-24
- VNE information 3-18

upgrade analysis (NEIM) 4-27
Up ticket 10-8
User-defined device groups
- permissions 4-56, 4-57

user roles
- mobile technologies 26-1
- viewing
  - Carrier Grade NAT properties 14-2
  - DWDM properties 15-1
  - Ethernet OAM properties 16-1
  - MToP properties 21-1
  - SBC properties 22-2
- working with
  - business elements 7-1
  - business tags 7-1
  - Carrier Ethernet services 13-2
  - Cisco PathTracer 12-1
  - IPv6 and 6VPE 18-2
  - links 6-1
  - maps 5-2
  - MPLS networks 19-1
  - Prime Network Events 8-1, 9-1
  - Prime Network Vision 2-1, 3-1
  - reports 11-1
  - tickets 10-1

user roles for bng 25-2


## V


V1 Trap tab, in Prime Network Events 9-10
V2 Trap tab, in Prime Network Events 9-10
V3 Trap tab, in Prime Network Events 9-11
View
- HSRP properties 13-17

viewing
- 6rd tunnel properties 19-46
- access gateway properties 13-19
- additional APN characteristics 26-18
- additional GTPP characteristics 26-25
- APN properties 26-14
- ATM cross-connects 21-6
- ATM VCI properties 21-10
- ATM VPI properties 21-10
- BFD session properties 19-47
- Carrier Ethernet properties, roles required 13-2
- Carrier Grade NAT properties 14-2, 14-5
- CDP properties 13-6
- CEM groups 21-51, 21-52, 21-53
- CEM interfaces 21-51
- CEM properties 21-50
- CESoPSN pseudowire properties 21-3
- CFM properties 16-3
- cross-VRF routing entries 19-49
- device operating system information 3-31
- device properties 3-6
- DWDM properties 15-3
- EFP cross-connect properties 13-75
- EFP properties 13-32
- encapsulation information 21-11
- Ethernet flow domains 13-41

Ethernet LAG properties 13-23
Ethernet LAGs 13-22
Ethernet Link Aggregation Groups 13-22
Ethernet services properties 13-108
EVC service properties 13-39
GGSN properties 26-7
GTPP properties 26-24, 26-30
GTPU properties 26-11
ICCP properties 13-28
IMA group properties 21-13
IP SLA responder service properties 13-111
IPv6 information 18-2
IS-IS properties 13-113
Layer 2 Tunnel Protocol path trace 12-28
Link Layer Discovery Protocol (LLDP) properties 13-8
Link Layer Discovery Protocol properties 13-8
Link OAM properties 16-14
link properties 6-10
links between VLAN elements and devices 13-57
LLDP properties 13-8
LSE properties 19-39
LSP endpoint properties 19-13
LSPs on Ethernet links 19-11
mLACP properties 13-28
MLPPP link properties 21-29
MLPPP properties 21-26
MPLS TE tunnel information 19-52
MPLS-TP BFD sessions 19-49
MPLS-TP tunnel properties 19-7
network element properties 3-6
operating system information for devices 3-31
OSPF properties 13-116
path trace details in Cisco PathTracer 12-20
path traces in Cisco PathTracer 12-14
PBB properties 13-31
P-GW properties 26-35
port configuration information 3-25
pseudowire
  clock recovery properties 21-42
  endpoint properties 13-86
  properties 13-92
  redundancy service properties 13-95
  VCCV and CC information 13-94
PWE3 tunnel information 19-50
QinQ path trace 12-27
REP information in
  VLAN domain views 13-62
  VLAN overlays 13-62
report folder properties 11-48
report properties 11-45
reports 11-41
report type properties 11-50
REP properties
  for VLAN service links 13-63
  in logical inventory 13-14
routing entities 19-31
SAToP pseudowire properties 21-2
SBC properties 22-3, 22-4
S-GW properties 26-36
SONET/SDH channelization properties 21-18
STP
  information in VLAN domain views 13-65
  information in VLAN overlays 13-65
  properties 13-10
  properties for VLAN service links 13-66
SyncE properties 21-46
T3 DS1 and DS3 channelization properties 21-21
TDM properties 21-17
ticket properties 9-18
tickets in Prime Network Vision 10-3
virtual CEMs
  list of 21-51
  properties 21-50
virtual connection properties 21-5
Virtual Switching Instance properties 13-84
VLAN
  bridge properties 13-69

mapping properties 13-56
mappings 13-52
service link properties 13-62
trunk group properties 13-67
VNE properties 3-16
VPLS
access Ethernet EFP properties 13-88
instance properties 13-83
properties 13-82
VPN
properties 19-26
site properties 19-27
VRF properties 19-27
VRRP information 19-37
VSI properties 13-84
viewing address family ipv4 profile 20-4
viewing address family ipv6 profile 20-5
viewing IGMP profile 20-5
viewing mldp database details 19-42
viewing mldp neighbor details 19-43
viewing multicast details 20-2
viewing multicast protocols 20-4
viewing the PIM profile 20-7
viewing VRF multicast configuration 19-30
viewing y.1731 probes 17-2
virtual CEMs
listing 21-51
viewing properties 21-50
Virtual Circuit Connectivity Verification (VCCV), viewing information for pseudowire endpoint 13-94
virtual cloud, definition 1-5
virtual connections
viewing encapsulation information 21-11
viewing properties 21-5
virtual data center
view configuration 27-10
virtualization 27-9
virtual machine
view configuration 27-14
Virtual Router Redundancy Protocol (VRRP), viewing information 19-37
virtual routers
moving 19-23
properties, viewing 19-27
VRF tables 19-31
Virtual Switching Instance. See VSI
VLAN bridge, launching a path trace 12-10
VLAN overlays
adding to maps 13-60
working with 13-44
VLANs
adding associated VLANs 13-54
adding to map view 13-49
associations 13-54
definition 1-5
discovery 13-44
elements
EFPs 13-46
icons in Prime Network Vision 13-45
network VLAN 13-45
overview 13-45
switching entities 13-45
overlays
STP link information 13-65
viewing REP information 13-62
viewing STP information 13-65
overview 13-45
removing
from maps 13-52
overlays 13-61
tag manipulations for associations 13-54
viewing
associated VLAN mapping properties 13-56
associated VLAN service links 13-56
bridge properties 13-69
links between elements and devices 13-57
mappings 13-52
REP properties 13-63

service link properties 13-62
STP properties 13-66
working with 13-44
VLAN trunk group, viewing properties 13-67
VNE/Agent Unreachable, VNE communication state 2-20
VNE communication states
Agent Not Loaded 2-20
Connecting 2-20
Device Partially Reachable 2-20
Device Unreachable 2-20
Tracking Disabled 2-20
VNE/Agent Unreachable 2-20
VNE investigation states
Currently Unsynchronized 2-21
Defined Not Started 2-20
Discovering 2-21
Maintenance 2-21
Operational 2-21
Partially Discovered 2-21
Shutting Down 2-21
Stopped 2-21
Unsupported 2-20
VNEs
communication state badges A-18
investigation state badges A-19
management state 2-18
modifying properties 3-16
updating information 3-18
viewing communication status 3-17
viewing properties 3-16
vPC 27-2
commands 27-5, 27-9
fabricpathconfiguration 27-7
view configuration 27-4
VPLS
adding instances to maps 13-78
instance overlays 13-79
overlays
link callout 13-81
viewing pseudowire tunnel links 13-81
viewing
access Ethernet EFP properties 13-88
instance properties 13-83
properties 13-82
pseudowire endpoint properties 13-86
working with 13-77
VPLS report
detailed 11-23
options 11-37
summary 11-23
VPNs
adding to maps 19-22
and virtual routers 19-23
creating 19-21
definition 1-6
managing 19-21
moving virtual routers between 19-23
overlays 19-24
callouts 19-25
creating 19-24
displaying 19-25
hiding 19-25
properties, viewing 19-26
removing from maps 19-23
sites 19-27
viewing in maps 19-18
virtual routers 19-27
VRF multicast configuration 19-30
VRFs
cross-VRF routing entries 19-49
tables
egress 19-31
ingress 19-31
viewing properties 19-27
with IPv4 and IPv6 addresses 18-6
VSI, viewing properties 13-84
VTP Domains inventory tab 2-4

## W

Working and Protected LSPs 19-5
working with
associated VLANs 13-54
business elements 7-1
business tags 7-1
EFP cross-connects 13-74
Ethernet services 13-104
H-VPLS 13-77
links, user roles required 6-1
MPLS-TP tunnels 19-4
overlays 5-21
Prime Network Events 9-14
pseudowire overlays 13-89
pseudowires 13-89
tickets in Prime Network Vision 10-1
VLAN overlays 13-44
VLANs 13-44
VPLS 13-77

## Y

y.1731
performance management mechanisms 17-1
y.1731 probes 17-1, 17-2, 17-4
user roles required 17-2
y.1731 technology
overview 17-1
You 26-56