



Cisco Active Network Abstraction 3.7.1 User Guide

Revised: January 31, 2011

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-21803-02

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 of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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 Active Network Abstraction 3.7.1 User Guide
© 1999-2011 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface xvii

New and Changed Information xviii

Audience xviii

Conventions xix

Related Documentation xx

Obtaining Documentation and Submitting a Service Request xx

CHAPTER 1

Cisco ANA Client Overview 1-1

Basic Cisco ANA Terminology 1-1

Cisco ANA Security: Permissions, Roles, and Scopes 1-3

Cisco ANA NetworkVision 1-4

Cisco ANA EventVision 1-7

CHAPTER 2

Working with the Cisco ANA NetworkVision Client 2-1

User Roles Required to Work with Cisco ANA NetworkVision 2-1

Starting Cisco ANA NetworkVision 2-2

Cisco ANA NetworkVision Window 2-4

Navigation Pane 2-5

Content Pane: Map, List, and Links Views 2-5

Map View 2-6

List View 2-10

Links View 2-13

Ticket Pane 2-15

Network Element Status Indicators 2-17

Severity 2-18

Network Element Management State 2-19

Tickets 2-22

Cisco ANA NetworkVision Toolbar 2-22

Cisco ANA NetworkVision Menu Bar 2-24

File Menu 2-25

Edit Menu 2-25

View Menu 2-26

Node Menu 2-26

Tools Menu 2-27

Activation Menu	2-28
Network Inventory Menu	2-28
Reports Menu	2-28
Window Menu	2-29
Help Menu	2-29
Cisco ANA NetworkVision Shortcut Menus	2-29
Device Shortcut Menu	2-30
Map Shortcut Menu	2-33
Aggregated Node Shortcut Menu	2-33
Link Shortcut Menu	2-34
List View Shortcut Menu	2-35
Links View Shortcut Menu	2-36
Ticket Shortcut Menu	2-37
Changing a User Password in Cisco ANA NetworkVision	2-38
Selecting Cisco ANA NetworkVision Map and Alarm Options	2-39
Working with Cisco ANA Tables	2-40
Table Toolbar Options	2-40
Finding Text in a Table	2-41
Sorting a Table	2-42
Filtering Table Contents	2-43
Viewing Selected Rows	2-45
Exporting Tables to a File	2-45

CHAPTER 3

Viewing Network Element Properties 3-1

User Roles Required to Work with Cisco ANA NetworkVision	3-1
Viewing the Properties of a Device	3-2
Viewing VNE Properties	3-4
Viewing VNE Communication Details	3-5
Opening the Inventory Window	3-6
Navigation Pane	3-8
Device View Pane	3-8
Device View Pane Toolbar	3-9
Ticket Pane	3-9
Content Pane	3-10
Viewing the Physical Properties of a Device	3-10
Opening the Port Utilization Graph	3-11
Managing Port Alarms	3-12
Disabling Alarms	3-12
Enabling Alarms	3-12

Viewing the Logical Properties of a Network Element	3-13
Logical Inventory Window	3-13
Logical Inventory Navigation Pane Branches	3-14
Logical Inventory Navigation Pane Icons	3-15
Logical Inventory Content Pane Tabs	3-17
Viewing Device Operating System Information	3-17

CHAPTER 4

Working with Cisco ANA NetworkVision Maps 4-1

User Roles Required for Working with Cisco ANA NetworkVision Maps	4-2
Opening Maps	4-3
Opening Commonly Used Maps	4-3
Opening a New Map from the Open Map Dialog Box	4-4
Closing a Map	4-5
Creating a New Map	4-6
Adding Elements to a Map	4-6
Removing Elements from a Map	4-9
Defining a Map Layout	4-10
Saving Maps	4-10
Saving a Map with Information	4-10
Saving a Map as a New Map	4-11
Saving a Map as an Image	4-11
Deleting a Map from the Cisco ANA Database	4-13
Renaming a Map	4-14
Resizing a Map Element	4-14
Viewing the Network Map	4-15
Viewing a Network Device	4-16
Selecting Map Views	4-16
Finding Elements Affected by a Ticket	4-17
Finding and Selecting Links in Maps	4-18
Finding a Network Device or Service	4-19
Working with Overlays	4-19
Applying an Overlay	4-20
Hiding or Viewing an Overlay	4-22
Removing an Overlay	4-22

Working with Aggregations	4-22
Grouping Network Elements into Aggregations	4-22
Ungrouping Aggregated Nodes	4-23
Renaming Aggregated Nodes	4-23
Filtering Links According to Type	4-24
Opening the CPU Usage Graph	4-26
Communicating with Devices Using Ping and Telnet	4-27
Previewing and Printing a Map	4-27

CHAPTER 5

Working with Links 5-1

User Roles Required to Work with Links	5-1
Understanding Dynamic and Static Links	5-2
Working with Flickering Topology Links	5-2
Viewing Link Properties	5-3
Viewing Link Properties in Cisco ANA NetworkVision Maps	5-3
Viewing Link Properties in the Links View	5-5
Viewing Link Properties in the Link Properties Window	5-7
Link List Pane	5-8
Properties Pane	5-9
Viewing Link Impact Analysis	5-10
Adding Static Links	5-12
Filtering Links Using the Collection Method	5-14
Selecting a Link	5-14

CHAPTER 6

Working with Business Tags and Business Elements 6-1

User Roles Required to Work with Business Tags and Business Elements	6-1
Using Chinese Characters	6-2
Creating a Business Tag	6-3
Searching for Business Tags and Viewing Their Properties	6-4
Renaming a Business Element	6-5
Deleting a Business Element	6-5

CHAPTER 7**Working with the Cisco ANA EventVision Client 7-1**

- User Roles Required to Work with Cisco ANA EventVision 7-1
- Starting Cisco ANA EventVision 7-2
- Cisco ANA EventVision Window 7-3
 - Cisco ANA EventVision Toolbar 7-5
 - Cisco ANA EventVision Menu Bar 7-6
- Right-Click Options 7-7
- Selecting Cisco ANA EventVision Viewing Options 7-8

CHAPTER 8**Tracking Faults Using Cisco ANA EventVision 8-1**

- User Roles Required to Work with Cisco ANA EventVision 8-1
- Viewing Events and Tickets in Cisco ANA EventVision 8-2
 - All Tab 8-2
 - System Event Tabs 8-3
 - Audit Tab 8-3
 - Provisioning Tab 8-4
 - Security Tab 8-5
 - System Tab 8-5
 - Network Event Tabs 8-6
 - Service Tab 8-6
 - Syslog Tab 8-7
 - Ticket Tab 8-8
 - V1 Trap Tab 8-8
 - V2 Trap Tab 8-9
 - V3 Trap Tab 8-10
- Viewing 3.6.x Tabs 8-11
- Working in Cisco ANA EventVision 8-14
 - Viewing Event Properties 8-14
 - Viewing Ticket Properties 8-18
 - Refreshing Cisco ANA EventVision Information 8-20
 - Filtering Events and Tickets 8-21
 - Defining Filters 8-21
 - Removing Filters 8-24
 - Exporting Displayed Data 8-24

CHAPTER 9

Working with Tickets in Cisco ANA NetworkVision 9-1

User Roles Required to Work with Tickets in Cisco ANA NetworkVision 9-1

Viewing Tickets in Cisco ANA NetworkVision 9-2

Ticket Status in the Ticket Pane 9-4

Filtering Tickets by Device 9-5

Filtering Tickets by Criteria 9-6

Viewing Ticket Properties 9-7

Toolbar 9-9

Details Tab 9-9

History Tab 9-10

Affected Parties Tab 9-11

Correlation Tab 9-14

Advanced Tab 9-15

Notes Tab 9-15

Managing Tickets 9-15

Finding Affected Elements 9-16

Acknowledging a Ticket 9-16

Clearing a Ticket 9-16

Removing a Ticket 9-17

Clearing and Removing Tickets 9-17

Impact Analysis in Cisco ANA 9-18

Status Values for Affected Parties 9-18

Accumulating Affected Parties 9-19

Accumulating the Affected Parties in an Alarm 9-19

Accumulating the Affected Parties in the Correlation Tree 9-19

Updating Affected Severity over Time 9-20

Disabling Impact Analysis 9-20

Viewing Detailed Information for the Affected Pair 9-20

CHAPTER 10

Working with Reports 10-1

User Roles Required to Manage Reports 10-1

Using the Report Manager 10-2

Menu Options 10-3

Toolbar Icons 10-4

Navigation Tree 10-4

Content Pane 10-5

Right-Click Options 10-6

Report Categories	10-8
Events Reports	10-8
Inventory Reports	10-11
Network Service Reports	10-12
Generating Reports	10-14
Generating Reports from Report Manager	10-15
Generating Events Reports	10-15
Generating Inventory Reports	10-19
Generating Network Service Reports	10-22
Generating Reports from the Reports Menu	10-25
Generating Reports from Cisco ANA NetworkVision	10-25
Managing Reports	10-26
Managing the Maximum Number of Concurrent Reports	10-26
Viewing and Saving Reports	10-27
Renaming Reports	10-28
Sharing Reports	10-29
Moving Reports Between Folders	10-30
Deleting Reports	10-30
Viewing Report Properties	10-31
Defining Report Types	10-33
Working with Report Folders	10-33
Creating Folders	10-34
Moving Folders	10-34
Renaming Folders	10-35
Deleting Folders	10-35
Viewing Folder and Report Type Properties	10-36
Viewing Report Folder Properties	10-36
Viewing Report Type Properties	10-37

CHAPTER 11

Using Cisco ANA PathTracer to Diagnose Problems	11-1
User Roles Required to Work with Cisco ANA PathTracer	11-2
Cisco ANA PathTracer Overview	11-2
Using Cisco ANA PathTracer	11-3
Cisco ANA PathTracer Right-Click Menu Options	11-4
Starting a Path Trace	11-4
From the Map View	11-5
From Logical or Physical Inventory	11-7
Examples of Launching Cisco ANA PathTracer	11-7

Cisco ANA PathTracer Multipath Window	11-12
Menus	11-14
Toolbar	11-14
Tabs	11-15
Paths Pane	11-16
Content Pane	11-16
Cisco ANA PathTracer Single-Path Window	11-16
Menus	11-18
Toolbar	11-18
Topological Map	11-19
Properties Table and Layer Tabs	11-19
Viewing Path Information	11-20
Saving and Opening Cisco ANA PathTracer Map Files	11-20
Saving Cisco ANA PathTracer Counter Values	11-21
Rerunning a Path and Comparing Results	11-22
Viewing Q-in-Q Path Information	11-22
Viewing L2TP Path Information	11-23
Using Cisco ANA PathTracer in MPLS Networks	11-24
Cisco ANA PathTracer MPLS Starting Points	11-25
Cisco ANA PathTracer MPLS Endpoints	11-25
Using Cisco ANA PathTracer for Layer 3 VPNs	11-26
Using Cisco ANA PathTracer for Layer 2 VPNs	11-26
Using Cisco ANA PathTracer for MPLS TE Tunnels	11-27
CHAPTER 12	
Monitoring Carrier Ethernet Services	12-1
User Roles Required to Work with Carrier Ethernet Services	12-2
Viewing CDP Properties	12-4
Viewing Link Layer Discovery Protocol Properties	12-5
Viewing Spanning Tree Properties	12-7
Viewing Resilient Ethernet Protocol Properties	12-10
Working with Ethernet Link Aggregation Groups	12-13
Viewing Ethernet LAG Properties	12-14
Viewing Provider Backbone Bridge Properties	12-19
Viewing EFP Properties	12-20
Understanding EFP Severity and Ticket Badges	12-22
Viewing EVC Service Properties	12-23

Viewing Virtual Switching Instance Properties	12-25
Viewing VPLS Core or Access Pseudowire Endpoint Properties	12-27
Viewing VPLS Access Ethernet Flow Point Properties	12-29
Viewing and Renaming Ethernet Flow Domains	12-30
Working with VLANs and VLAN Overlays	12-33
VLAN and EFD Discovery	12-33
VLAN Elements	12-34
Switching Entities Containing Termination Points	12-38
Adding VLANs to a Map	12-38
Removing VLANs from a Map	12-41
Viewing VLAN Mappings	12-41
Working with Associated VLANs	12-43
Adding an Associated VLAN	12-43
Viewing Associated Network VLAN Service Links and VLAN Mapping Properties	12-44
Viewing VLAN Links Between VLAN Elements and Devices	12-46
Adding a VLAN Overlay to a Map View	12-49
Displaying or Hiding VLAN Overlays	12-51
Removing a VLAN Overlay	12-51
Viewing VLAN Service Link Properties	12-52
Viewing REP Information in VLAN Domain Views and VLAN Overlays	12-52
Viewing REP Properties for VLAN Service Links	12-53
Viewing STP Information in VLAN Domain Views and VLAN Overlays	12-54
Viewing STP Properties for VLAN Service Links	12-56
Viewing VLAN Trunk Group Properties	12-57
Viewing VLAN Bridge Properties	12-59
Understanding Unassociated Bridges	12-61
Adding Unassociated Bridges	12-62
Working with Ethernet Flow Point Cross-Connects	12-64
Adding EFP Cross-Connects	12-65
Viewing EFP Cross-Connect Properties	12-66
Working with VPLS and H-VPLS Instances	12-69
Adding VPLS Instances to a Map	12-70
Using VPLS Instance Overlays	12-71
Viewing Pseudowire Tunnel Links in VPLS Overlays	12-73
Viewing VPLS-Related Properties	12-75
Viewing VPLS Instance Properties	12-75
Working with Pseudowires and Pseudowire Overlays	12-77
Adding Pseudowires to a Map	12-77
Pinging a Pseudowire	12-80

Displaying Pseudowire Information	12-83
Applying Pseudowire Overlays	12-85
Viewing Pseudowire Properties	12-86
Working with Ethernet Services	12-90
Adding Ethernet Services to a Map	12-91
Using Ethernet Service Overlays	12-92
Viewing Ethernet Service Properties	12-94
Viewing IP SLA Responder Service Properties	12-97
Viewing IS-IS Properties	12-98
Viewing OSPF Properties	12-101

CHAPTER 13

Monitoring Carrier Grade NAT Properties 13-1

User Roles Required to View Carrier Grade NAT Properties	13-1
Viewing Carrier Grade NAT Properties in Logical Inventory	13-2
Viewing Carrier Grade NAT Properties in Physical Inventory	13-4

CHAPTER 14

Monitoring DWDM Properties 14-1

User Roles Required to View DWDM Properties	14-1
Viewing DWDM in Physical Inventory	14-2
Viewing G.709 Properties	14-4
Viewing Performance Monitoring Configuration	14-10

CHAPTER 15

Viewing Ethernet Operations, Administration, and Maintenance Tool Properties 15-1

User Roles Required to View Ethernet OAM Tool Properties	15-1
Ethernet OAM Overview	15-2
Viewing Connectivity Fault Management Properties	15-2
Viewing Ethernet LMI Properties	15-8
Viewing Link OAM Properties	15-12

CHAPTER 16

IPv6 and IPv6 VPN over MPLS 16-1

User Roles Required to Work with IPv6 and 6VPE	16-1
Viewing IPv6 Information	16-2

CHAPTER 17

Monitoring MPLS Services 17-1

User Roles Required to Work with MPLS Networks	17-1
Viewing VPNs in Cisco ANA NetworkVision	17-3
Viewing Additional VPN Properties	17-5

Managing VPNs	17-6
Creating a VPN	17-6
Adding a VPN to a Map	17-7
Removing a VPN from a Map	17-8
Moving a Virtual Router Between VPNs	17-8
Working with VPN Overlays	17-9
Adding a VPN Overlay to a Map	17-9
Managing a VPN Overlay Display in the Map View	17-10
Displaying VPN Callouts in a VPN Overlay	17-10
Working with CE Devices	17-11
Connecting a CE Device	17-11
Disconnecting a CE Device	17-12
Showing or Hiding a CE Device	17-12
Working with Tunnels	17-13
Adding a Tunnel to a VPN	17-13
Removing a Tunnel	17-14
Working with LCAs and LCPs	17-15
Creating an LCA	17-15
Moving an LCA	17-15
Deleting an LCA	17-16
Moving an LCP	17-16
Jumping to an Adjacent LCP	17-16
Monitoring MPLS Services	17-17
Viewing VPN Properties	17-17
Viewing Site Properties	17-17
Viewing VRF Properties	17-18
Displaying VRF Egress and Ingress Adjacents	17-21
Viewing Routing Entities	17-22
Viewing the ARP Table	17-23
Viewing the NDP Table	17-24
Viewing Rate Limit Information	17-26
Viewing a Label Switched Entity	17-27
MPLS Interfaces Tab	17-27
Label Switching Table Tab	17-27
Traffic Engineering LSPs Tab	17-28
VRF Table Tab	17-29
LDP Neighbors Tab	17-29
Viewing MP-BGP Information	17-30
Viewing BFD Properties	17-31

Viewing a Port Configuration	17-33
Viewing Cross-VRF Routing Entries	17-34
Viewing Pseudowire End-to End Emulation Tunnels	17-35
Viewing MPLS TE Tunnel Information	17-36

CHAPTER 18
Monitoring MToP Services 18-1

User Roles Required to Work with MToP	18-1
Viewing SAToP Pseudowire Type in Logical Inventory	18-2
Viewing CESoPSN Pseudowire Type in Logical Inventory	18-3
Viewing ATM Virtual Connection Cross-Connects	18-4
Viewing IMA Group Properties	18-7
Viewing TDM Properties	18-10
Viewing Channelization Properties	18-11
Viewing SONET/SDH Channelization Properties	18-12
Viewing T3 DS1 and DS3 Channelization Properties	18-15
Viewing MLPPP Properties	18-19
Viewing MLPPP Link Properties	18-22
Viewing MPLS Pseudowire over GRE Properties	18-25
Network Clock Service Overview	18-28
Monitoring Clock Service	18-28
Monitoring PTP Service	18-30
Viewing Pseudowire Clock Recovery Properties	18-33
Viewing SyncE Properties	18-38
Viewing CEM and Virtual CEM Properties	18-40
Viewing CEM Interfaces	18-40
Viewing Virtual CEMs	18-41
Viewing CEM Groups	18-41
Viewing CEM Groups on Physical Interfaces	18-41
Viewing CEM Groups on Virtual CEM Interfaces	18-42

CHAPTER 19
Viewing SBC Properties 19-1

User Roles Required to View SBC Properties	19-2
Viewing SBC Properties in Logical Inventory	19-2
Viewing SBC DBE Properties	19-4
Viewing Media Address Properties	19-4
Viewing VDBE H.248 Properties	19-5

Viewing SBC SBE Properties	19-5
Viewing AAA Properties	19-6
Viewing H.248 Properties	19-7
Viewing Policy Properties	19-7
Viewing SIP Properties	19-11

APPENDIX A

Icon Reference A-1

Cisco ANA NetworkVision Icons	A-1
Map Icons	A-1
Link Colors	A-3
Link Badges	A-4
Cisco ANA NetworkVision Toolbar Icons	A-4
Table Toolbar Icons	A-6
Link Filtering Icons	A-6
Logical Inventory Icons	A-7
Physical Inventory Icons	A-8
Cisco ANA EventVision Icons	A-9
Severity Icons	A-9
Cisco ANA EventVision Toolbar Icons	A-10
Ticket Properties Toolbar Icons	A-10
Report Manager Icons	A-11
Icon Badges	A-11
Network Element Badges	A-12
Alarm and Ticket Badges	A-13

INDEX



Preface

This document describes Cisco Active Network Abstraction (Cisco ANA) 3.7.1. Cisco ANA 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, ANA 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 includes the following topics:

- [New and Changed Information, page xviii](#)
- [Audience, page xviii](#)
- [Conventions, page xix](#)
- [Related Documentation, page xx](#)
- [Obtaining Documentation and Submitting a Service Request, page xx](#)

New and Changed Information

[Table 1](#) describes the information that has been added or changed since the initial release of the *Cisco Active Network Abstraction 3.7.1 User Guide*.

Table 1 *New and Changed Information in This Guide*

Date Released	Revision	Location
January 31, 2011	Added the following note to the procedure for creating a business tag: Note Business tag names are case-sensitive.	Creating a Business Tag, page 6-3
	Added the following information to the procedure for searching for business tags: 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.	Searching for Business Tags and Viewing Their Properties, page 6-4
August 30, 2010	Initial version.	—

Audience

The intended audience for this documentation includes:

- Network viewers who monitor the network and perform basic (nonprivileged) system functions.
- Network operators who perform day-to-day operations such as creating business tags and maps, and managing alarms.
- Network configurators who activate services and configure network elements.
- System administrators who manage and configure users, network elements, the Cisco ANA system, and overall security.
- System managers or administrators who periodically review and manage the events list using Cisco ANA EventVision.
- Networking engineers who are interested in understanding how the Cisco ANA 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 ANA basic and administrative training.

Conventions

Table 2 describes the conventions used in this document.

Table 2 **Conventions**

Convention	Description
<i>string</i>	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.
<i>italic font</i>	Variables for which you supply values.
<i>italic screen font</i>	Variables you enter.
screen font	Courier plain shows an example of information displayed on the screen.
Option > Network Preferences	Choosing a menu item.

Related Documentation



Note

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

The following documentation is available for Cisco Active Network Abstraction 3.7.1:

Cisco Active Network Abstraction 3.7.1 Administrator Guide

Cisco Active Network Abstraction 3.7.1 Customization User Guide

Cisco Active Network Abstraction 3.7.1 Documentation Guide

Cisco Active Network Abstraction 3.7.1 Installation Guide

Cisco Active Network Abstraction 3.7.1 Release Notes

Cisco Active Network Abstraction 3.7.1 Reference Guide

Cisco Active Network Abstraction 3.7.1 Theory of Operations Guide

Cisco Active Network Abstraction 3.7.1 User Guide

Cisco Active Network Abstraction 3.7.1 Configuration and Image Management User and Administrator Guide

Cisco Active Network Abstraction Network Service Activation 1.1 User Guide

Cisco Active Network Abstraction Network Service Activation 1.1 Customization Guide

Open Source Used in Cisco Active Network Abstraction 3.7.1

Cisco Active Network Abstraction 3.7.1 Integration Developer Guide is available on the Cisco ANA Technology Center website. This guide describes how to use Cisco ANA integration interfaces.

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

Obtaining Documentation and Submitting a Service Request

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

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

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



CHAPTER 1

Cisco ANA Client Overview

Cisco ANA provides a suite of GUI tools that offer an intuitive interface for managing the network and services, and for performing required system administration activities. The Cisco ANA client application suite comprises Cisco ANA NetworkVision, Cisco ANA EventVision, and Cisco ANA Manage.

The following topics provide an introduction to Cisco ANA terminology and client applications:

- [Basic Cisco ANA Terminology, page 1-1](#)
- [Cisco ANA Security: Permissions, Roles, and Scopes, page 1-3](#)
- [Cisco ANA NetworkVision, page 1-4](#)
- [Cisco ANA EventVision, page 1-7](#)



Note

For information about the Cisco ANA Manage application, see the [Cisco Active Network Abstraction 3.7.1 Administrator Guide](#).

Basic Cisco ANA Terminology

[Table 1-1](#) provides a brief explanation of the terms used in the Cisco ANA clients and documentation.

Table 1-1 **Definitions**

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

Table 1-1 **Definitions (continued)**

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

Table 1-1 **Definitions (continued)**

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

Cisco ANA Security: Permissions, Roles, and Scopes

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

Permission

The user’s ability to perform certain tasks. There are two types of permissions: default and NE-related.

- **Default**—Applies only to the activities that are related to GUI functionality, and not the activities related to network elements. For example, a user with the default permission Viewer can view maps and the device list. For more information, see the [Cisco Active Network Abstraction 3.7.1 Administrator Guide](#).
- **NE-Related**—Enables the administrator to group a collection of managed network elements (in Cisco ANA Manage) to allow the user to view and manage the NEs based on the user’s role or permission. After the user is allocated a scope (list of network elements) and a role, the user can then perform various activities on the network elements, such as managing alarms in Cisco ANA NetworkVision. For more information, see the [Cisco Active Network Abstraction 3.7.1 Administrator Guide](#).

Roles

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

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



Note

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

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

The administrator is responsible for defining the types of activities that the user can view and perform using Cisco ANA Manage. For more information about user security and defining operational scopes, see the [Cisco Active Network Abstraction 3.7.1 Administrator Guide](#).

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

Scopes

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

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

Cisco ANA NetworkVision

Cisco ANA NetworkVision is the main GUI application used to visualize the network through network and service maps, to view device physical and logical inventories and connectivity, and to manage device configuration and software images. It provides total visibility for multiple-tier,

multiple-technology networks, and supports fault and configuration functionality. The highly optimized, customizable GUIs enable constant, system-wide surveillance of the network and service states, down to the node level.

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

Cisco ANA NetworkVision enables you to:

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

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

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

For details on using Cisco ANA NetworkVision when working with specific technologies, see the following topics:

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

Cisco ANA NetworkVision is also the launch point for:

- Cisco ANA PathTracer
- Cisco ANA Soft Properties Manager
- Cisco ANA Command Builder
- Cisco ANA Report Manager
- Cisco ANA Configuration and Image Management
- Cisco ANA Network Service Activation

Cisco ANA PathTracer

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

Cisco ANA Soft Properties Manager

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

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

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

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

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

For more information on the Cisco ANA Soft Properties Manager, see the [Cisco Active Network Abstraction 3.7.1 Customization User Guide](#).

For more information about using BQL with Cisco ANA, see the [Cisco Active Network Abstraction 3.7.1 Integration Developer Guide](#).

Cisco ANA Command Builder

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

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

For more information on the Cisco ANA Command Builder, see the [Cisco Active Network Abstraction 3.7.1 Customization User Guide](#).

Cisco ANA Report Manager

The Cisco ANA Report Manager enables you to generate, customize, view, and export a variety of reports about events, traps, tickets, syslogs, software versions, and devices. The Report Manager, available from Cisco ANA Manage, Cisco ANA NetworkVision, and Cisco ANA EventVision, provides out-of-the-box reports for events and inventory.

The Report Manager enables you to:

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

For information about reports and Report Manager, see [Chapter 10, “Working with Reports.”](#)

You can also retrieve reports using BQL. For more information, see the [Cisco Active Network Abstraction 3.7.1 Integration Developer Guide](#).

Cisco ANA Configuration and Image Management

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

For more information on the Cisco ANA Configuration and Image Management, see the [Cisco Active Network Abstraction 3.7.1 Configuration and Image Management User and Administrator Guide](#).

Cisco ANA Network Service Activation

Cisco ANA Network Service Activation (NSA) is a Cisco ANA service activation extension for users wanting to deploy Carrier Ethernet, IP Radio Access Network (RAN), and Mobile Transport over Pseudowire (MToP) services using a service activation wizard launched from the Cisco ANA NetworkVision GUI. Cisco ANA NSA provides:

- A predefined collection of service activation wizards, workflows, and scripts that allow you to begin activating services on Cisco network elements after Cisco ANA NSA is installed.
- The ability for service designers, network planners, and service integrators to customize the wizards and workflows to address service activation needs not provided in the delivered Cisco ANA NSA package.

Cisco ANA NSA provides a visual mechanism for end-to-end service activation on network elements. In addition, Cisco ANA NSA open APIs allow it to be integrated with northbound provisioning systems. Cisco ANA NSA therefore provides a GUI-based service activation solution that can also be integrated into existing operational support system (OSS) environments.

For more information about Cisco ANA NSA, see the [Cisco Active Network Abstraction Network Service Activation 1.1 User Guide](#).

Cisco ANA EventVision

Cisco ANA EventVision is the interface used by administrators for viewing system events and tickets that are generated within the Cisco ANA system.

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

You can configure Cisco ANA EventVision to display the following information:

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

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

All administrator activities in Cisco ANA Manage are logged and available in Cisco ANA EventVision. For more information on Cisco ANA Manage, see the [Cisco Active Network Abstraction 3.7.1 Administrator Guide](#).



CHAPTER 2

Working with the Cisco ANA NetworkVision Client

The following topics describe the user access roles required to use Cisco ANA NetworkVision, the Cisco ANA NetworkVision working environment, and how to access the Cisco ANA NetworkVision tools and commands:

- [User Roles Required to Work with Cisco ANA NetworkVision, page 2-1](#)
- [Starting Cisco ANA NetworkVision, page 2-2](#)
- [Cisco ANA NetworkVision Window, page 2-4](#)
- [Changing a User Password in Cisco ANA NetworkVision, page 2-38](#)
- [Selecting Cisco ANA NetworkVision Map and Alarm Options, page 2-39](#)
- [Working with Cisco ANA Tables, page 2-40](#)

User Roles Required to Work with Cisco ANA NetworkVision

[Table 2-1](#) identifies the GUI default permission or device scope security level that is required to work with Cisco ANA NetworkVision. Cisco ANA 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 device-based tasks (tasks that do affect devices), authorization is based on the default permission that is assigned to your account. That is, whether the device 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 Active Network Abstraction 3.7.1 Administrator Guide](#).

Table 2-1 *Default Permission/Security Level Required for Cisco ANA NetworkVision Functions*

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Start Cisco ANA NetworkVision	X	X	X	X	X
Change a user password in Cisco ANA NetworkVision	—	—	—	—	X ¹
Set Cisco ANA NetworkVision options	X	X	X	X	X
Work with Cisco ANA NetworkVision 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.

Starting Cisco ANA NetworkVision

This topic provides instructions for launching the Cisco ANA NetworkVision application. Cisco ANA NetworkVision is password protected to ensure security. Before you start working with Cisco ANA NetworkVision, make sure you know your username, password, and the Cisco ANA gateway IP address or hostname that you require.



Note

If you do not log into the Cisco ANA Manage, Cisco ANA NetworkVision, or Cisco ANA EventVision application during a specified period of time (the default is one month), your account is automatically locked. The default period can be changed per user in Cisco ANA Manage. The period of time is measured from the time you last logged out of any of the Cisco ANA client applications.



Note

When working intensively on Cisco ANA NetworkVision or Cisco ANA EventVision, you might experience a Java crash causing the GUI application to close. This issue does not affect the Cisco ANA server and is related only to the Java GUI applications running on a Windows machine with some models of graphics cards.

This situation can occur while working with multiple open windows of Cisco ANA applications and occurs sporadically with no specific scenario.

If you encounter this situation, do either of the following:

- Restart the Cisco ANA application.
- Consider updating your graphics card driver.

To start Cisco ANA NetworkVision:

Step 1 Choose **Start > Programs > Cisco ANA > Cisco ANA NetworkVision**.

The Cisco ANA NetworkVision Login dialog box is displayed. The last four Cisco ANA gateways you logged into are displayed in the Host drop-down list. The list is displayed in chronological order with the most recent Cisco ANA gateway at the top of the list.

Step 2 Enter your username and password.

Step 3 Choose a Cisco ANA gateway in either of the following ways:

- Enter an IP address or hostname in the Host field.
- Select a Cisco ANA gateway from the Host drop-down list. (The Cisco ANA gateway IP address or hostname that was used when you last logged in is automatically displayed at the top of the Host drop-down list.)



Note Make sure that you use the leading IP address (the IP address on which the Cisco ANA gateway was configured) when logging into the system.

Step 4 Click **OK**.

If any client updates are available, Cisco ANA automatically installs them.

When you launch Cisco ANA NetworkVision, messages are displayed if the server and client have different versions of the application that launches the client. For more information about these messages, see the [Cisco Active Network Abstraction 3.7.1 Installation Guide](#).

The Cisco ANA NetworkVision window appears empty when it is opened for the first time. You can create a new map or open a map that has been previously saved; see [Chapter 4, “Working with Cisco ANA NetworkVision Maps,”](#) for information on network maps.

After logging into Cisco ANA NetworkVision and launching the application, you can customize the Cisco ANA NetworkVision settings. For example, you can:

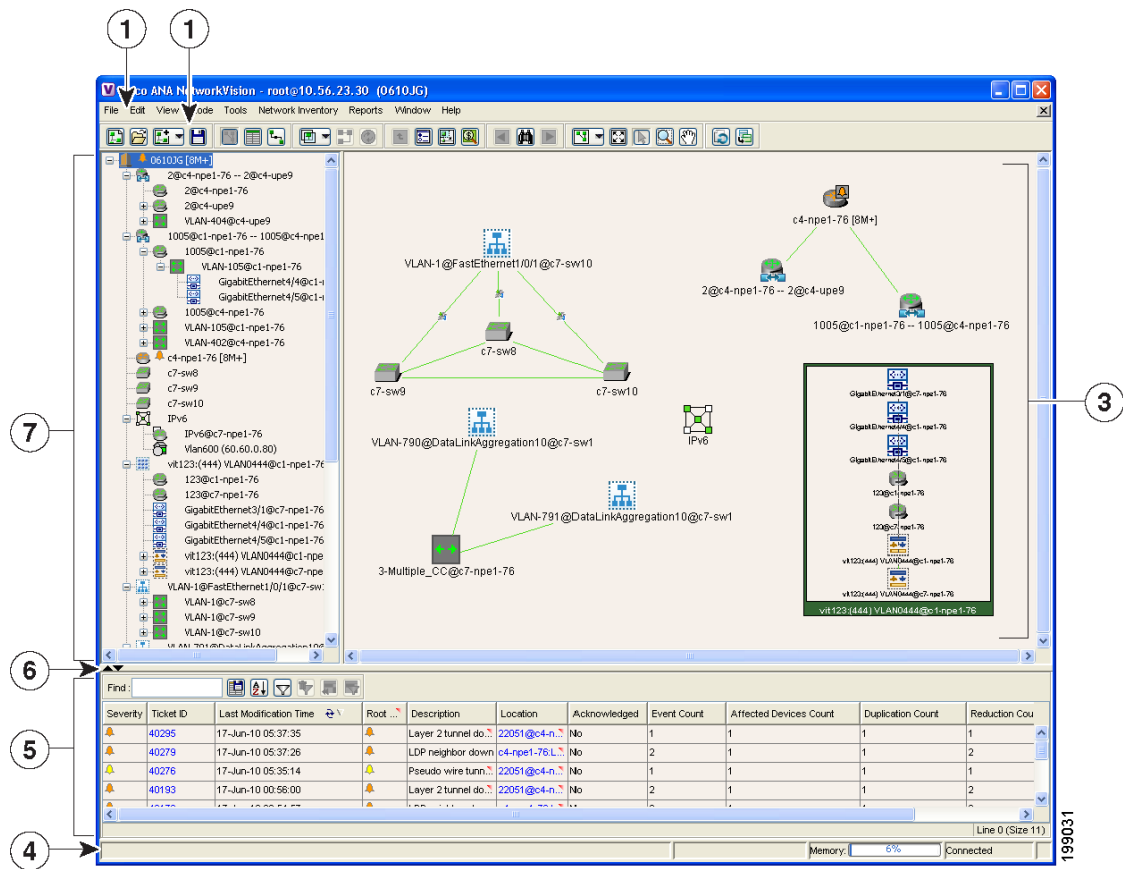
- Load the content pane with information when starting Cisco ANA NetworkVision.
- Display network elements in the Cisco ANA NetworkVision content pane and navigation pane.
- Configure audio responses when different alarms are triggered.

For more information on customizing Cisco ANA NetworkVision startup and display options, see [Selecting Cisco ANA NetworkVision Map and Alarm Options, page 2-39](#).

Cisco ANA NetworkVision Window

Figure 2-1 displays the Cisco ANA NetworkVision window with an open map.

Figure 2-1 Cisco ANA NetworkVision Window



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

The content pane, ticket pane, and navigation pane are the three main components of the Cisco ANA NetworkVision user interface.



Note The ticket pane can be displayed or hidden by clicking the arrows below the navigation pane.

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

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

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

Some of the functions that the Cisco ANA NetworkVision window enables you to perform are:

- View the network.
- View network element properties.
- View physical and logical inventory information.
- View a complete list of the physical links and their status.
- View link properties.
- View and manage tickets.

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 the map name (for example, the name of a geographic area). When the map name is changed, the Cisco ANA NetworkVision window is updated. The new map name is displayed, between brackets, at the top of the navigation tree, and in the title bar of the window.

The lowest level of the navigation tree displays a single NE (for example, a router and the device name, or the name of the business tag).

For information about the status of network objects, see [Network Element Status Indicators, page 2-17](#).

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 2-6](#).
- 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 2-10](#).
- Links view—Displays a complete list of the links shown in the map view and their status. For more information, see [Links View, page 2-13](#).

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

- The currently selected network elements or links.
- The sorting preferences.
- The filtering preferences, as defined using:
 - The Map Options dialog box—See [Filtering Links According to Type, page 4-24](#).
 - The Filter dialog box—See [Filtering Table Contents, page 2-43](#).
 - The links view collection method—See [Filtering Links Using the Collection Method, page 5-14](#).

Map View

Click **Show Map View** on the toolbar to display the map view in the Cisco ANA NetworkVision window.

In the map view, Cisco ANA NetworkVision displays:

- Managed network elements

Each NE is displayed using an NE icon, the color of which reflects severity, as described in [Severity Indicators, page 2-10](#). In addition, a management state or alarm icon is displayed with the IP address. A tooltip displays the NE name, NE type, and IP address.
- VLANs
- VPNs
- Links and link aggregations

The links (and link aggregations) that are presented in the map view:

- Display arrowheads if they are unidirectional.
 - Do not have arrowheads if they are bidirectional.
- Relationships between network elements, aggregations, and networks



Note

If the maximum number of links is exceeded, a warning message is displayed, all links are removed from the map, and the map is surrounded by a red border.

You can view the links in either of the following ways:

- Choose **Show Links view** in the toolbar.
- Filter the links to reduce the number of links that are to be displayed. This filtering allows the client to return to a normal state.

For more information on the maximum number of links, contact your Cisco account representative.

The links have tooltips that provide you with information regarding the number of links that are represented by a line, along with partial descriptions. Physical links are highlighted in bold. Because a single link may actually represent a number of links, you can use the links view to get more details (see [Links View, page 2-13](#)).

For more information about links in Cisco ANA NetworkVision, see [Chapter 5, “Working with Links.”](#)



Note

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

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

You can move the NEs manually on the map by dragging the required NE. You can also click **Layout Map** in the toolbar or choose **View > Zoom In** or **View > Zoom Out** to change the way NEs are displayed on the map.

Right-Click Functions

Table 2-2 describes some of the functions that can be performed using the right-click shortcut 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.

Table 2-2 Right-Click Functions in Map View

Right-Click Functions Available from Map View	For more information, see:
Go to Parent	Goes to the parent in the tree pane and map pane so you can view different information.
Go to Root	Goes to the root in the tree pane and map pane so you can view different information.
Aggregate network elements	Chapter 4, “Working with Cisco ANA NetworkVision Maps”
Change the view and content of network maps	Chapter 4, “Working with Cisco ANA NetworkVision Maps”
Communicate with network elements	Chapter 4, “Working with Cisco ANA NetworkVision Maps”
Configure the topology	Chapter 5, “Working with Links”
Create and attach business tags	Chapter 6, “Working with Business Tags and Business Elements”
Create and view tickets	Chapter 9, “Working with Tickets in Cisco ANA NetworkVision”
Filter tickets	Chapter 9, “Working with Tickets in Cisco ANA NetworkVision”
Generate reports on events, inventory, and networks services	Chapter 10, “Working with Reports”
Launch external applications or tools from Cisco ANA NetworkVision navigation tree, map pane, links view, and ticket pane	Cisco Active Network Abstraction 3.7.1 Customization User Guide
Launch components installed with Cisco ANA: • Cisco Active Network Abstraction Configuration and Image Management • Cisco Active Network Abstraction Network Service Activation	• Cisco Active Network Abstraction 3.7.1 Configuration and Image Management User and Administrator Guide • Cisco Active Network Abstraction Network Service Activation 1.1 User Guide
Launch available activation and configuration scripts, including those you create using Cisco ANA Command Builder (can be launched against multiple NEs)	Cisco Active Network Abstraction 3.7.1 Customization User Guide
View device inventory	Chapter 3, “Viewing Network Element Properties”
View NE information (device properties)	Chapter 3, “Viewing Network Element Properties”

Network Element Icons

Table 2-3 identifies the icons used to represent network elements in the Cisco ANA NetworkVision window's navigation pane and content pane.

Table 2-3 Network Element Icons

Icon	Device
	ATM switch
	Basic rate access (BRA)
	Connection termination point (TP) Ethernet flow point
	Cross-connect
	Digital subscriber line access multiplexer (DSLAM)
	Ethernet service
	Ethernet switch
	Ethernet virtual connection (EVC)
	Generic SNMP
	Logical Circuit Aggregation (LCA) business element
	Logical Circuit Peer (LCP) business element
	Logical Circuit Peer with one or more hidden connected devices
	Network pseudowire
	Network, subnetwork, or logical aggregation
	Pseudowire switching entity Switching entity

Table 2-3 *Network Element Icons (continued)*

Icon	Device
	Router
	Site
	Site with one or more hidden connected devices
	Unknown, or ghost, device
	Unmanaged network or cloud
	Viewable by a user with a higher permission level
	Virtual router
	VLAN
	VPLS
	VPN
	VSI

**Note**

When Cisco ANA NetworkVision detects a network device for which it does not have enough information available, Cisco ANA NetworkVision displays as a ghost device on the map. When this occurs, you cannot view the ghost device properties or communicate with it. When the information for the ghost device becomes available, Cisco ANA NetworkVision replaces its icon with the relevant device icon, and all the related device information and communication become available.

Severity Indicators

Table 2-4 shows the colors that are used to display the severity (or propagated severity) of a network device in the navigation, content, and ticket panes.

Table 2-4 Severity Indicators

Icon	Color	Severity
	Red	Critical
	Orange	Major
	Yellow	Minor
	Sky Blue	Warning
	Green	Cleared, Normal, or OK
	Dark Blue	Information
	White	Indeterminate

The same coloring conventions apply to the link severity displayed in the map and links views.



Note

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

When an aggregated node is selected in the navigation tree, the content pane displays the elements contained within the aggregation and the relationships between them.

For more information about how the status of a network element is displayed in a map, see [Network Element Status Indicators, page 2-17](#).

List View

Click **Show List View** in the toolbar to display the Cisco ANA NetworkVision list view. The list view displays the tabs described in Table 2-5, depending on the items included in the current map and the item selected in the navigation tree.

Table 2-5 Cisco ANA NetworkVision List View Tabs

Tab	Description
Aggregations	Aggregations contained in the current map.
Connection TP	Connection termination points (TPs) contained in the current map.

Table 2-5 Cisco ANA NetworkVision List View Tabs (continued)

Tab	Description
EFP Cross-Connect	EFP cross-connects contained in the current map.
Ethernet Flow Points	EFPs contained in the current map.
Ethernet Services	Ethernet services contained in the current map.
EVCs	EVCs contained in the current map.
Network Elements	Network elements contained in the current map.
Network Pseudowire	Network pseudowire contained in the current map.
Pseudowires	Pseudowires contained in the current map.
Pseudowire Edge	Pseudowire endpoints contained in the current map.
PW Switching Entity	Pseudowire switching entities contained in the current map.
Sites	Sites for the selected VLAN. Site properties include site name, description, location, and IP interface.
Switching Entities	Switching entities contained in the current map.
Virtual Routers	Virtual routers on the selected VLAN. Virtual router properties include the virtual router name and description.
VLANs	VLANs contained in the current map. VLAN properties include VLAN name, ID, description, and Ethernet flow points.
VPLS Forward	VPLS forwards contained in the current map.
VPLS Instance	VPLS instances contained in the current map.
VPNs	VPNs contained in the current map. VPN properties include VPN name and description

Table 2-6 describes the network element properties displayed in Network Elements tab. (Locked network elements display only managed element information and the locked device icon.)

Table 2-6 Network Element Information Displayed in List View

Field Name	Description
Name	Name of the network element managed by Cisco, as defined in Cisco ANA Manage. 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.
Communication State	Ability of the VNE to reach the network element, according to the health of the device. For more information about communication states, see the Cisco Active Network Abstraction 3.7.1 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 Active Network Abstraction 3.7.1 Administrator Guide .

Table 2-6 Network Element Information Displayed in List View (continued)

Field Name	Description
Element Category	Network element category, such as Router or Eth-Switch (Ethernet switch).
Element Type	Network element type including the manufacturer's name, such as Cisco 7200.
Vendor	Vendor name.
Up Since	Date and time when the network element was last reset.
System Description	Detailed description of the software installed on the network element.
Location	Location of the network element.
File Systems	Device file systems.
Sending Alarms	Whether the network element is configured for sending alarms: True or False. Reporting the status of alarms can be enabled on only part of the device.

**Tip**

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

Table 2-7 identifies the buttons that are displayed in the list view toolbar.

Table 2-7 List View Toolbar

Icon	Name	Description
	Export to CSV	Exports the information displayed in the table, or selected portions, to a CSV file. For more information, see Exporting Tables to a File, page 2-45
	Sort Table Values	Sorts the information displayed in the table by the criteria you specify. For more information, see Sorting a Table, page 2-42 .
	Filter	Filters the information displayed in the table by the criteria you specify. For more information, see Filtering Table Contents, page 2-43 .
	Clear Filter	Clears the existing filter.
	Show All Rows	Displays all table rows that meet the current filtering criteria.
	Show Only Selected Rows	Displays only the rows that you select. For more information, see Viewing Selected Rows, page 2-45 .

See [Working with Cisco ANA Tables, page 2-40](#), for more information about filtering, finding details about a network element in Cisco ANA NetworkVision tables, and the keyboard shortcuts used for accessing table functionality.

Some of the options that are available in the right-click shortcut menu in the list view are:

Option	Related Documentation
View network element properties	Chapter 3, “Viewing Network Element Properties”
View network element inventory	Chapter 3, “Viewing Network Element Properties”
Launch external applications or tools, such as an SSH client.	Cisco Active Network Abstraction 3.7.1 Customization User Guide
Launch available activation and configuration scripts, including those you create using Cisco ANA Command Builder (can be launched against multiple NEs).	Cisco Active Network Abstraction 3.7.1 Customization User Guide
Configure the topology.	Chapter 5, “Working with Links”
Configure and view business tag information.	Chapter 6, “Working with Business Tags and Business Elements”

**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 Cisco ANA NetworkVision window.

When you view a map, it might have many links, and some links might consist of a collection, or *aggregation*, of links. This can make it difficult for you to view the links you are interested in. The links view enables you to clearly view the links, search for a specific link, and view the status of a link.

**Note**

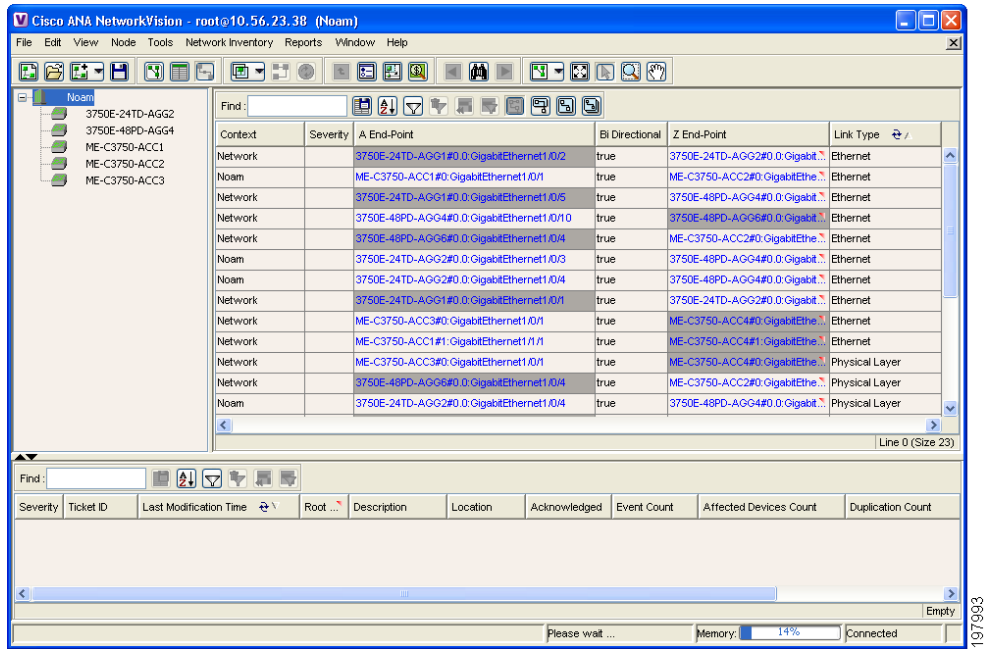
You can view and filter the links according to type using the Map Options dialog box. For more information, see [Filtering Links According to Type, page 4-24](#).

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 aggregated node is selected, the links in the selected aggregation are displayed in the links view.

Figure 2-2 shows a links view.

Figure 2-2 Links View



Note

An external link has a gray cell background in the table, and you can open the inventory window by clicking the hyperlink. For more information about external links, see [Viewing Link Properties in the Links View, page 5-5](#).

Table 2-8 describes the information that is displayed in the links view.

Table 2-8 Information Displayed in the Links View

Field Name	Description
Context	Name of the map or aggregated node containing the link.
Severity	Link alarm severity, represented by a bell icon. The color indicates the alarm severity and thereby the impact of the alarm on the network. For more information about severity, see Map View, page 2-6 .
A End-Point	Device or site that is the source of the link as a hyperlink to the inventory of the device or site.
Bi Directional	Whether the link is bidirectional or unidirectional: true (bidirectional) or false (unidirectional). If the link is unidirectional (false), the traffic is from A to Z.
Z End-Point	Device or site that is the destination of the link as a hyperlink to the inventory of the device or site.
Link Type	Type of link, such as Physical Layer, VPN, or MPLS.

**Note**

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

The links view toolbar includes the tools described in [Table 2-7](#) and the link filtering buttons described in [Table 2-9](#).

Table 2-9 Link Filtering Buttons

Button	Name	Description
	All Links	Displays the complete list of links for the selected context (map or aggregated node). 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 aggregated node) and the other side either not in the map or outside the selected context.
	Flat Links (Surface)	Displays the links currently visible on the map for the selected context (map or aggregated node), excluding any thumbnails.
	Deep Links	Displays the links for the current aggregated node where both endpoints are within the currently selected context.

For more information about filtering and sorting links in the links view, see [Viewing Link Properties in the Links View, page 5-5](#).

Ticket Pane

When Cisco ANA detects faulty behavior in the network, the VNEs and their internal device components initiate an internal, end-to-end message flow, resulting in the full understanding and containment of the fault across all relevant network elements and network layers.

The ticket pane enables you to view and manage tickets as well as identify elements or links that are affected by a ticket. All the tickets that are reported by Cisco ANA are stored in the Cisco ANA gateway database.

The ticket pane is displayed beneath the navigation and content panes in the Cisco ANA NetworkVision window. You can view or hide the ticket pane by clicking the arrows displayed below the navigation pane.

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.

**Note**

For detailed definitions of the key concepts in fault management, such as tickets, alarms, and events, see the [Cisco Active Network Abstraction 3.7.1 Theory of Operations Guide](#). For information on managing tickets, see [Chapter 9, “Working with Tickets in Cisco ANA NetworkVision.”](#)

Cisco ANA 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 Ticket Properties window enables you to view all correlated alarms.

**Note**

The root cause alarm severity is the top-most severity of its contained alarms.

The ticket pane enables you to perform the following functions:

- View all tickets or only the filtered tickets of a selected device. For more information, see [Filtering Tickets by Device, page 9-5](#).
- View and filter all tickets that meet specified criteria. See [Filtering Tickets by Criteria, page 9-6](#).
- View and acknowledge tickets.
- View the properties of a ticket, including the history, correlated alarms, severity of the root cause alarm, and affected parties.
- Clear a ticket.
- Remove a ticket.
- Clear and remove a ticket.
- Locate the elements or links affected by the ticket in the map or links view.
- Sort the tickets displayed.

[Table 2-10](#) describes the information displayed in the ticket pane.

Table 2-10 Ticket Information Displayed in the Ticket Pane

Field Name	Description
Severity	Severity of alarm, represented by a bell icon. The color indicates the alarm severity and thereby the impact of the alarm on the network. For more information about severity, see Map View, page 2-6 . • Red—Critical • Orange—Major • Yellow—Minor • Sky Blue—Warning • Green—Cleared, Normal, or OK • Dark Blue—Informational • White—Indeterminate
Ticket ID	Ticket identifier, assigned sequentially. Click the hyperlinked entry to view ticket properties, and to acknowledge, clear, or refresh the ticket. For more information, see Chapter 9, “Working with Tickets in Cisco ANA NetworkVision.”
Last Modification Time	Date and time the ticket was last modified. The ticket is modified when a user acknowledges the ticket or when an event is correlated.
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.
Description	Supported ticket name.

Table 2-10 Ticket Information Displayed in the Ticket Pane (continued)

Field Name	Description
Location	Entity that triggered the ticket, as a hyperlink that displays the relevant location in the inventory.
Acknowledged	Whether or not the ticket has been acknowledged: Yes or No.
Event Count	Number of events associated with the ticket.
Affected Devices Count	Number of devices affected by the ticket, including the sources of the alarm and their subsequent alarms.
Duplication Count	For network events, the duplication count is calculated by the VNE and pertains only to flapping events. The duplication count represents the number of noncleared events aggregated by the flapping event. For tickets, the duplication count is the sum of the duplication counts of all events that are associated with the root alarm.
Reduction Count	For network events, the reduction count is calculated by the VNE and pertains only to flapping events. The reduction count represents the number of events that are aggregated by the flapping event. Ticket reduction count is the sum of reduction counts of all the events that are associated to the ticket. The History tab in the Windows Properties window displays one reduction count for each event listed. For more information, see Chapter 9, “Working with Tickets in Cisco ANA NetworkVision.”
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 Ticket ID. For information about tickets, see [Chapter 9, “Working with Tickets in Cisco ANA NetworkVision.”](#)

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 Cisco ANA NetworkVision tables and table functionality, see [Working with Cisco ANA Tables, page 2-40](#).

The Location bar below the table displays:

- The location of the selected rows in the table; for example, Line 3.
- The number of selected rows and the total number of rows in the table; for example, 2/16 Selected.

For more information about network element status indicators, see [Network Element Status Indicators, page 2-17](#).

Network Element Status Indicators

The following topics describe the ways in which the status of a network element is displayed in Cisco ANA NetworkVision:

- [Severity, page 2-18](#)
- [Network Element Management State, page 2-19](#)
- [Tickets, page 2-22](#)

Severity

Severity indicates the operational health of the network element. An icon has only one severity value at any given time, and this value is displayed using the severity colors. For more information about the colors used to display the severity (or propagated severity) of network elements and links, see [Severity Indicators](#), page 2-10.

Propagation

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

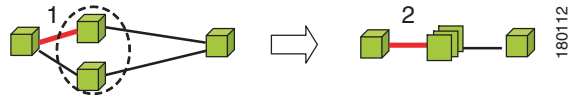
The same severity propagation rules that are used for network elements apply to links. A link is a child object of an aggregation *only* if it is fully contained in the aggregation; that is, the network elements on both sides of the link are part of the aggregation, as shown in [Figure 2-3](#) and [Figure 2-4](#).

Figure 2-3 Link Severity Example 1



[Figure 2-3](#) shows critical link 1 between two NEs 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 2-4 Link Severity Example 2



[Figure 2-4](#) shows critical link 1 that forms part of a link aggregation. This affects the severity of link 2 because it contains a link with a critical severity.

New Ticket Propagation

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

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

$n\ s\ [+]$

where:

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

For example:

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

A bell represents unacknowledged tickets, and the bell color is that of the most severe, unacknowledged ticket.

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

Network Element Management State

The management state indicates the state or mode of the software component (a VNE) managing an NE 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 network elements.

The management state indication applies only to network elements and network element components. A network object can have only one state (for example, Unsupported or Initializing).

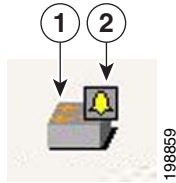
A managed network element icon consists of a managed element icon and one or two overlay icons, or *badges*:

- 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. For more information about network element icons, see [Network Element Icons, page 2-8](#). For more information about severity colors, see [Severity Indicators, page 2-10](#).
- An alarm badge (a bell) 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 2-5](#) 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 Minor, as indicated by the yellow alarm badge.

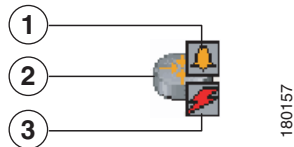
Figure 2-5 Element with Ticket and Alarm Severity Indicators



1	Element icon with severity Major (orange)
2	Alarm badge with severity minor (yellow)

- A VNE management state badge is displayed on top of the managed element icon to indicate the management state in the navigation tree and map. For example, a router that Cisco ANA failed to access (the router is unreachable) is displayed as illustrated in Figure 2-6.

Figure 2-6 Element with Overlay Badges



1	Alarm badge
2	Managed element icon
3	VNE management state badge

Table 2-11 describes network element communication and management states and shows the related badge for each state.

Table 2-11 Network Element Communication and Management States

State Name	Description	Badge
Communication States		
Device Reachable	All element protocols are enabled and connected.	None
Device Partially Reachable	The element is not fully reachable because: - At least one protocol is not operational. - All protocols are not operational but the element is still sending syslogs or traps.	
Device Unreachable	No protocols are responding and the element has not sent traps or syslogs in the last three minutes.	
VNE/Agent Unreachable	The VNE is not responding to the gateway. This can occur if the unit or AVM is overutilized or the connection between the gateway and unit or AVM was lost.	

Table 2-11 Network Element Communication and Management States (continued)

State Name	Description	Badge
Connecting	The VNE is starting and the initial connection has not yet been made to the device. This is a momentary state.	None
Investigation States		
Defined Not Started	The initial state of the VNE, as soon as it is created. The VNE was created but not started, or an existing VNE was stopped. A VNE remains in this state until it is started by a user. In this state, the VNE is managed but does not yet have any device information because the VNE has not yet connected to the device.	None
Unsupported	The device type is not supported by Cisco ANA, specifically because no VNE driver was found for the device.	
Discovering	The VNE is building the model of the device (the device type was found and is supported by Cisco ANA).	
Operational	The VNE has a stable model for the device. Modeling might not be fully complete, but enough information exists to monitor the device.	None
Currently Unsynchronized	The VNE model is inconsistent with the element for one of the following reasons: - A required, recoverable device command failed. - The device did not respond in a timely manner. - The VNE was in maintenance state but has restarted and is now resynchronizing with the network element. - The VNE was in the Device Unreachable state and is now resynchronizing with the network element.	
Maintenance	The VNE is no longer polling the device; therefore, the VNE does not know the device status. This can occur when a user moves the VNE to maintenance mode, or the VNE is using adaptive polling and CPU information is too high.	
Partially Discovered	The VNE model is inconsistent with the device because a required device command failed three times. A common cause of this state is that the device contains an unsupported module.	
Reconciliation	The business 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.	
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 Active Network Abstraction 3.7.1 Administrator Guide](#).

Tickets

A bell icon is displayed in the navigation, map, and ticket panes to indicate one or more tickets. Every alarm is assigned a severity level, representing the impact of the fault on the network device. The bell icon displays the severity level of the top-most alarm. The following is an example:

Value	Navigation Pane	Map
Ticket		

Cisco ANA NetworkVision Toolbar

The Cisco ANA NetworkVision toolbar is context-sensitive and the options vary depending on your selection in the application.


Note

The functionality that a user can access from the toolbar and in menus depends on the permissions defined for the user.

Table 2-12 identifies the icons and describes the functions that are available in the Cisco ANA NetworkVision toolbar.

Table 2-12 Cisco ANA NetworkVision Toolbar

Button	Name	Function
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 Cisco ANA NetworkVision content pane (the button toggles when selected or deselected).
	Show List View	Displays the list view in the Cisco ANA NetworkVision content pane (the button toggles when selected or deselected).
	Show Links View	Displays the links view in the Cisco ANA NetworkVision content pane (the button toggles when selected or deselected).

Table 2-12 Cisco ANA NetworkVision Toolbar (continued)

Button	Name	Function
Overlay Tools		
	Choose Overlay Type	Chooses and displays an overlay of a specific type on top of the elements displayed in the content pane in a map view. Available overlay options are: • Ethernet Service • Pseudowire • VLAN • VPLS • VPN • None—Removes the existing overlays.
	Show Overlay / Hide Overlay	Displays or hides a previously defined overlay on top of the elements displayed in the map view. Note Overlays do not reflect changes that occur in the selected service. As a result, the information in an overlay can become stale.
	Refresh Overlay	Refreshes the overlay that was last selected.
Navigation Tools		
	Go to Parent	Moves up a branch in the navigation pane and content pane to enable you to view different information.
	Link Filter	Opens the Map Options dialog box, enabling you to display or hide different types of links in the map and links views.
	Overview	Opens a window displaying an overview of the network.
	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 a device or aggregated node 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.
	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.
Map Zoom and Layout Tools		
	Layout Map	Defines the way in which the NEs are arranged in the Cisco ANA PathTracer window: circular, symmetric, tree, or hierarchical.
	Fit in Window	Fits the entire subnetwork or map in the content pane.

Table 2-12 Cisco ANA NetworkVision Toolbar (continued)

Button	Name	Function
	Normal Selection Mode	Activates the normal selection mode (the button toggles when selected or deselected).
	Zoom Selection Mode	Activates the zoom selection mode, which enables you to select a pane in the map to enlarge by clicking and dragging (the button toggles when selected or deselected).
	Pan Mode	Activates the pan mode, which enables you to move around in the map by clicking and dragging (the button toggles when selected or deselected).
Application-Specific Tools		
	Open Activation	Displayed if Cisco ANA Network Service Activation is installed with Cisco ANA. Opens the Activation dialog box. For more information, see the Cisco Active Network Abstraction Network Service Activation 1.1 User Guide.
	Show Recent Activations	Displayed if Cisco ANA Network Service Activation is installed with Cisco ANA. Opens the Service Activation List dialog box. For more information, see the Cisco Active Network Abstraction Network Service Activation 1.1 User Guide.

Cisco ANA NetworkVision Menu Bar

The following topics describe the options that are available in each Cisco ANA NetworkVision menu:

- [File Menu, page 2-25](#)
- [Edit Menu, page 2-25](#)
- [View Menu, page 2-26](#)
- [Node Menu, page 2-26](#)
- [Tools Menu, page 2-27](#)
- [Network Inventory Menu, page 2-28](#)
- [Reports Menu, page 2-28](#)
- [Window Menu, page 2-29](#)
- [Help Menu, page 2-29](#)



Note

Based on the security level and access permissions assigned to a user, some of the menu options may not be available.



Note

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

File Menu

Table 2-13 describes the options that are available in the Cisco ANA NetworkVision File menu. For more information, see Chapter 4, “Working with Cisco ANA NetworkVision Maps.”

Table 2-13 File Menu Options

File Menu Option	Description
New Map	Creates a new empty map in the database.
Open	Opens a map saved in the database using the Open dialog box.
Close	Closes the map that is currently displayed.
Load MultiPath	Loads a Cisco ANA PathTracer map from a previously saved file in the Cisco ANA PathTracer Multi-Path window.
Add to Map	Opens the Add dialog box and enables you to add any of the following to the map or to the subnetwork selected in the navigation pane and displayed in the content pane: • Cross-Connect • Ethernet Service • Network Element • Pseudowire • Unassociated Bridge • VLAN • VPLS • VPN This option is enabled when a map is open and you have the required security level (OperatorPlus).
Save Map	Saves the appearance of the map (the background and the location of devices) to the database. This option is enabled when a map is open and you have the relevant security level (OperatorPlus).
Save As Image	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	Displays each map as it will look when printed.
Print	Prints the active map as displayed in the Print Preview dialog box.
Exit	Exits the Cisco ANA NetworkVision application and saves the content pane.

Edit Menu

Table 2-14 identifies the options available in the Cisco ANA NetworkVision Edit menu. For more information, see Chapter 4, “Working with Cisco ANA NetworkVision Maps.”

Table 2-14 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	Displays the Resize dialog box, enabling you to define the percentage used to resize device icons or aggregated nodes in the map. Note The Resize option is only available when device icons or aggregated nodes are selected.

View Menu

Table 2-15 identifies the options available in the Cisco ANA NetworkVision View menu. For more information, see [Viewing the Network Map, page 4-15](#).

Table 2-15 View Menu Options

View Menu Option	Description
Layout	Defines the way in which the map is displayed in the Cisco ANA NetworkVision content pane: circular, symmetric, tree, or hierarchical.
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 be enlarged by clicking and dragging to view the selected area. The selected option is dimmed.

Node Menu

Table 2-16 describes the Node menu options.



Note

Most of the functionality available in this menu is only available when a device icon or an aggregated node is selected in the navigation pane or a map.

Table 2-16 Node Menu Options

Node Menu Option	Description
Inventory	Displays a dialog box that enables you to view the physical and logical inventory. For physical inventory, you can view all the components of the device, such as modules and ports. In addition, you can view the status of each component. For logical inventory, you can view all the profiles and virtual channels or routing tables of the device. For more information, see Chapter 3, “Viewing Network Element Properties.”
Aggregate	Groups selected items into an aggregation in the Cisco ANA NetworkVision content pane, and enables you to define a name for the aggregation. For more information, see Chapter 4, “Working with Cisco ANA NetworkVision Maps.”
Disaggregate	Ungroups the selected aggregated node in the navigation pane and a map of the Cisco ANA NetworkVision window. All the aggregations in the selected node move up one level, and the original aggregated node is removed. For more information, see Chapter 4, “Working with Cisco ANA NetworkVision Maps.” Note This option is available only when an aggregated node is selected in the navigation or a map.
Mark as A Side	Starts the process of creating a new static link. This option is enabled when a device, port or unmanaged network is selected.
Mark as Z Side	Launches the Add Static Link dialog box, enabling you to create a static link between the two selected nodes. This option is enabled after a device, port or unmanaged network is selected and after the Mark as A Side option is selected. Note If you select two ports, the Add Static Link dialog box is not displayed.
Properties	Displays a dialog box enabling you to view the properties of the selected device, such as the severity, IP address, and communication state. For more information, see Chapter 3, “Viewing Network Element Properties.”

Tools Menu

[Table 2-17](#) describes the Tools menu options.

Table 2-17 Tools Menu Options

Tools Menu Option	Description
Change User Password	Enables you to change the password used when logging in to the Cisco ANA client application suite. The change takes effect the next time you log into the application. Note The administrator can also change a user password in Cisco ANA Manage.
Options	Enables you to customize several of Cisco ANA NetworkVision’s options, such as whether or not to load the content upon startup. For more information, see Selecting Cisco ANA NetworkVision Map and Alarm Options, page 2-39 .
Config and Image Mgmnt	Displays the Cisco Active Network Abstraction Configuration and Image Management dashboard. For more information, see the Cisco Active Network Abstraction 3.7.1 Configuration and Image Management User and Administrator Guide .

Activation Menu

The Activation menu is displayed if the Cisco ANA Network Service Activation application is installed with Cisco ANA.

See the [Cisco Active Network Abstraction Network Service Activation 1.1 User Guide](#) for more information about any of the options in this menu.

[Table 2-18](#) describes the Activation menu options.

Table 2-18 Activation Menu Options

Activation Menu Option	Description
Activation	Opens the Activation dialog box.
Show Recent Activations	Opens the Service Activation List dialog box.
Service Modification Utility	Opens the Service Metadata Modification Utility dialog box.

Network Inventory Menu

[Table 2-19](#) describes the Network Inventory menu options.

Table 2-19 Network Inventory Menu Options

Network Inventory Menu Option	Description
Ethernet Flow Domains	Opens the Ethernet Flow Domain List Properties window, which lists the domains. For more information, see Viewing and Renaming Ethernet Flow Domains, page 12-30
VTP Domains	Enables you to view a current snapshot of the VLAN Trunk Protocol (VTP) domains. See Viewing VLAN Trunk Group Properties, page 12-57 .

Reports Menu

[Table 2-20](#) describes the Reports menu options.

Table 2-20 Reports Menu Options

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

For more information about Report Manager and reports, see [Chapter 10, “Working with Reports.”](#)

Window Menu

The Cisco ANA NetworkVision Window menu displays the names of all the maps open in the Cisco ANA NetworkVision content pane, enabling you to move between the maps.

Help Menu

Table 2-21 describes the Help menu options.

Table 2-21 Help Menu Options

Help Menu Option	Description
Cisco ANA NetworkVision Help	Opens the online help for Cisco ANA NetworkVision and Cisco ANA EventVision.
Icon Legend	Opens a window that identifies and describes the icons used in Cisco ANA.
Cisco ANA NSA Help	This option appears only if Cisco ANA Network Service Activation is installed with Cisco ANA. Opens the online help for the Cisco ANA Network Service Activation application.
Cisco.com	This option is unavailable in this version.
About Cisco ANA NetworkVision	Displays application information about Cisco ANA NetworkVision and any additionally installed applications.

Cisco ANA NetworkVision Shortcut Menus

Right-clicking a specific area, link, network element, device, or alarm in the Cisco ANA NetworkVision window opens the following menus:

- [Device Shortcut Menu, page 2-30](#)
- [Map Shortcut Menu, page 2-33](#)
- [Aggregated Node Shortcut Menu, page 2-33](#)
- [Link Shortcut Menu, page 2-34](#)
- [List View Shortcut Menu, page 2-35](#)
- [Links View Shortcut Menu, page 2-36](#)
- [Ticket Shortcut Menu, page 2-37](#)

A menu is displayed when you right-click in many of the Cisco ANA NetworkVision windows or tables. For example, you can open a map from the Open Map dialog box using the right-click menu. The options displayed vary depending on the window or table currently displayed and the selection as described in the following topics.

**Note**

- Based on the security level and access permissions assigned to a user, some menu options might not be available.
- The menus are context-sensitive and the options vary according to your selection in the application; for example, the shortcut menus for NEs and aggregated nodes are different.

Device Shortcut Menu

The Device shortcut menu is displayed when you right-click a device in the navigation pane or in the content pane.

**Note**

The Device shortcut menu is context-sensitive and the options vary depending on your selection in the application. Some options might not be available when multiple devices are selected.

[Table 2-22](#) describes the options available in the device shortcut menu.

Table 2-22 *Device Shortcut Menu Options*

Device Shortcut Menu Option	Description
Open VRF Table	Opens the VRF Table window. For more information, see Viewing VRF Properties, page 17-18 .
Inventory	Displays a window enabling you to view the physical and logical inventory. For physical inventory, you can view all the components of the device, such as the modules, ports, and its IP address or configured VLANs. In addition, you can view the status of each component. For logical inventory, you can view all the profiles and VC tables of the device. For more information, see Chapter 3, “Viewing Network Element Properties.”
Aggregate	Groups the selected devices into an aggregation in the Cisco ANA NetworkVision content pane, and enables you to define a name for the new aggregated node. For more information, see Chapter 4, “Working with Cisco ANA NetworkVision Maps.”
Disaggregate	Ungroups the devices in the selected aggregated node in the navigation pane and a map of the Cisco ANA NetworkVision window. For more information, see Chapter 4, “Working with Cisco ANA NetworkVision Maps.” Note This option is available only when an aggregated node is selected in the navigation or a map.
Attach Business Tag	Attaches a business tag to the selected network element. For more information, see Chapter 6, “Working with Business Tags and Business Elements.”
Detach / Edit	You can detach or edit a business tag from the selected NE. For more information, see Chapter 6, “Working with Business Tags and Business Elements.” Note The Detach and Edit options are only displayed when a business tag is attached to an NE.

Table 2-22 Device Shortcut Menu Options (continued)

Device Shortcut Menu Option	Description
Config Mgmnt	Displays the Configuration Management page for the selected device in Cisco Active Network Abstraction Configuration and Image Management. For more information, see the Cisco Active Network Abstraction 3.7.1 Configuration and Image Management User and Administrator Guide .
Image Mgmnt	Displays the Image Management page for the selected device in Cisco Active Network Abstraction Configuration and Image Management. For more information, see the Cisco Active Network Abstraction 3.7.1 Configuration and Image Management User and Administrator Guide .
Filter Tickets	Filters the tickets shown in the ticket pane so that only the tickets of a selected device or network element are displayed.
Resize	Enables you to resize an object on the map by percentage or predefined sizes.
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.
Save as New Map	Creates a new map and places the selected aggregation as the root, while leaving the original map intact.
Run Report	Enables you to run standard or user-defined events, inventory, and network service reports on demand.
Add Associated VLAN	Opens the Add Associated VLAN dialog box so that you can add an associated VLAN to the selected VLAN. For more information, see Adding an Associated VLAN, page 12-43 .
Delete	Deletes the selected item from the map.
Modify	Displays the Modify dialog box so that you can change the selected item's name, description, or icon.
Rename	Renames the selected item.
Show VRF Egress Adjacents	Displays the Adjacents window for the selected VRF.
Show VRF Ingress Adjacents	Displays the Adjacents window for the selected VRF.
Edit	Move the selected item to the location you specify.
Show as Aggregation / Show Thumbnail	Displays the selected item as a single entity or as a collection of items.
Tools	The Tools option contains the following choices: • CPU Usage—Displays memory and CPU usage information for a device or network element. • Ping—Pings the device from the client station. • Telnet—Communicates with the device using the Telnet window from the client station.

Table 2-22 **Device Shortcut Menu Options (continued)**

Device Shortcut Menu Option	Description
Topology	The Topology option enables you to add: • A static link between two devices. • A static topology between a device and an unmanaged network. • A tunnel to a VPN. When working with static links, the following submenu options enable you to define the A Side and Z Side of the link: • Mark as A Side • Mark as Z Side When working with VPNs in VPN Service View, the Add Tunnel submenu option allows you define and configure tunnels.
<i>Launch external applications</i>	Starts an external application or tool that has been configured for access via the shortcut menu. For more information, see the Cisco Active Network Abstraction 3.7.1 Customization User Guide .
<i>Script names</i>	Launches available activation and configuration scripts, including those you create using Command Builder (can be launched against multiple NEs). For more information, see the Cisco Active Network Abstraction 3.7.1 Customization User Guide .
PathTracer	Launches a path trace from the selected item.
Properties	Displays the properties of the selected item, such as the IP address and system name. In addition, you can open the VNE Properties dialog box and manage VNE properties. For more information, see Chapter 3, “Viewing Network Element Properties.”
VNE Tools	Changes the status of the VNE by starting or stopping it. For more information, see Chapter 3, “Viewing Network Element Properties.”
Management	Contains the following submenu options: • Command Builder—Defines commands and scripts using the Cisco ANA Command Builder tool (Configurator security level required). • Soft Properties Management—Extends VNEs by adding SNMP MIB or Telnet/SSH/TL-1 properties to the device’s collected information model using the Cisco ANA Soft Properties Manager (Administrator security level required). For more information about Command Builder and Soft Properties Manager, see the Cisco Active Network Abstraction 3.7.1 Customization User Guide.

Map Shortcut Menu

The Map shortcut menu is displayed when you right-click anywhere on a map in the content pane.

[Table 2-23](#) describes the map shortcut menu options.

Table 2-23 Map Shortcut Menu Options

Map Shortcut Menu Option	Description
Go to Parent	Goes to the parent in the navigation pane and content pane to enable you to view different information.
Go to Root	Goes to the root in the navigation pane and content pane to enable you to view different information.
Aggregate	Creates an aggregation of the selected nodes in the navigation pane and a map in the Cisco ANA NetworkVision window and enables you to define a name for the aggregation. For more information, see Chapter 4, “Working with Cisco ANA NetworkVision Maps.”
Filter Tickets	Filters the tickets shown in the ticket pane so that only the tickets of a selected device or network element are displayed.
Launch external applications	Launch external applications or tools, such as an SSH client. See the Cisco Active Network Abstraction 3.7.1 Customization User Guide .
Script names	Launches available activation and configuration scripts, including those you create using Command Builder (can be launched against multiple NEs). For more information, see the Cisco Active Network Abstraction 3.7.1 Customization User Guide .
Add Associated VLAN	Opens the Add Associated VLAN dialog box so that you can add an associated VLAN to the selected VLAN. For more information, see Adding an Associated VLAN, page 12-43 .

Aggregated Node Shortcut Menu

The Aggregated Node shortcut menu is displayed when you right-click an aggregated node in a map.

[Table 2-24](#) describes the aggregated node shortcut menu options.

Table 2-24 Aggregated Node Shortcut Menu Options

Aggregated Node Shortcut Menu Option	Description
Aggregate	Groups the selected aggregated nodes into an aggregation in the Cisco ANA NetworkVision content pane, and enables you to define a name for the new aggregated node. For more information, see Chapter 4, “Working with Cisco ANA NetworkVision Maps.”
Disaggregate	Ungroups the selected aggregated node in the navigation pane and map in the Cisco ANA NetworkVision window. All the aggregations in the selected node move up one level, and the original aggregated node is removed. For more information, see Chapter 4, “Working with Cisco ANA NetworkVision Maps.”

Table 2-24 **Aggregated Node Shortcut Menu Options (continued)**

Aggregated Node Shortcut Menu Option	Description
Attach Business Tag	Attaches a business tag to the selected network element. For more information, see Chapter 6, “Working with Business Tags and Business Elements.”
Filter Tickets	Filters the tickets shown in the ticket pane so that only the tickets of the selected aggregated node are displayed.
Rename	Renames the selected aggregated node.
Resize	Defines the size of selected aggregated nodes in a map according to predefined sizes or according to a percentage of the current size.
Remove from Map	Removes the selected aggregated node 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.
Add Associated VLAN	Opens the Add Associated VLAN dialog box so that you can add an associated VLAN to the selected VLAN. For more information, see Adding an Associated VLAN, page 12-43 .
Run Report	Enables you to run standard or user-defined events, inventory, and network service reports.
Show Thumbnail	Displays a thumbnail of the selected aggregated node in the content pane, including all aggregated devices.
Show as Aggregation	Displays the aggregated node in a map. Note The Show as Aggregation option is displayed in the shortcut menu when a thumbnail is displayed in content pane.
Delete	Deletes the selected item.
Rename	Enables you to rename the selected item.

Link Shortcut Menu

The Link shortcut menu is displayed when you right-click a link in the map view. For more information, see [Chapter 5, “Working with Links.”](#)

[Table 2-25](#) describes the link shortcut menu options.

Table 2-25 **Link Shortcut Menu Options**

Link Shortcut Menu Option	Description
Filter Tickets	Filters the tickets shown in the ticket pane so that only the tickets of a selected network element are displayed.
Properties	Displays the properties of the selected link.

List View Shortcut Menu

The list view shortcut menu is displayed when you right-click an entry in the list view table displayed in the Cisco ANA NetworkVision content pane. For more information, see [List View, page 2-10](#).

[Table 2-26](#) describes the list view shortcut menu options.

Table 2-26 List View Shortcut Menu Options

List View Shortcut Menu Option	Description
Inventory	Displays a window enabling you to view the physical and logical inventory. For physical inventory, you can view all the components of the device, such as the modules, ports, and its IP address or configured VLANs. In addition, you can view the status of each component. For logical inventory, you can view all the profiles and VC tables of the device. For more information, see Chapter 3, “Viewing Network Element Properties.”
Attach Business Tag	Attaches a business tag to the selected link. For more information, see Chapter 6, “Working with Business Tags and Business Elements.”
Detach/Edit	Detaches or edits a business tag from the selected link. For more information, see Chapter 6, “Working with Business Tags and Business Elements.” Note The Detach and Edit options are only displayed when a business tag is attached to a link.
Run Report	Enables you to run standard or user-defined events, inventory, and network service reports.
Show Only Selected Rows	Displays only the rows that you select. For more information, see Viewing Selected Rows, page 2-45 .
Show All Rows	Displays all table rows that meet the current filtering criteria.
Tools	Contains the following submenu options: - CPU Usage—Displays memory and CPU usage information for a device or network element. - Ping—Pings the device from the client station. - Telnet—Communicates with the device using the Telnet window from the client station.
Topology	Enables you to add: - A static link between two devices. - A static topology between a device and an unmanaged network. - A tunnel to a VPN. When working with static links, the following submenu options enable you to define the A Side and Z Side of the link: - Mark as A Side - Mark as Z Side When working with VPNs in VPN Service View, the Add Tunnel submenu option allows you define and configure tunnels.

Table 2-26 List View Shortcut Menu Options (continued)

List View Shortcut Menu Option	Description
<i>Launch external applications</i>	Launches external applications or tools, such as an SSH client. See the Cisco Active Network Abstraction 3.7.1 Customization User Guide .
Properties	Displays the properties of the selected item, such as the IP address and system name. In addition, you can open the VNE Properties dialog box and manage VNE properties. For more information, see Chapter 3, “Viewing Network Element Properties.”
<i>Script names</i>	Launches available activation and configuration scripts, including those you create using Command Builder (can be launched against multiple NEs). For more information, see the Cisco Active Network Abstraction 3.7.1 Customization User Guide .
VNE Tools	Changes the status of the VNE by starting or stopping it. For more information, see Chapter 3, “Viewing Network Element Properties.”
Management	Contains the following submenu options: - Command Builder—Defines commands and scripts using the Cisco ANA Command Builder tool (Configurator security level required). - Soft Properties Management—Extends VNEs by adding SNMP MIB or Telnet/SSH/TL-1 properties to the device’s collected information model using the Cisco ANA Soft Properties Manager (Administrator security level required). For more information about Command Builder and Soft Properties Manager, see the Cisco Active Network Abstraction 3.7.1 Customization User Guide.

Links View Shortcut Menu

The links view shortcut menu is displayed when you right-click a link in the links view table displayed in the Cisco ANA NetworkVision content pane. For more information, see [Chapter 5, “Working with Links.”](#)

[Table 2-27](#) describes the links view shortcut menu options.

Table 2-27 Links View Shortcut Menu Options

Links View Shortcut Menu Option	Description
Attach Business Tag	Attaches a business tag to the selected link. For more information, see Chapter 6, “Working with Business Tags and Business Elements.”
Detach/Edit	Detaches or edits a business tag from the selected link. For more information, see Chapter 6, “Working with Business Tags and Business Elements.” Note The Detach and Edit options are only displayed when a business tag is attached to a link.
Select Link in Map	Highlights the selected link in the content pane.

Table 2-27 Links View Shortcut Menu Options (continued)

Links View Shortcut Menu Option	Description
Show Only Selected Rows	Displays only the rows that you select. For more information, see Viewing Selected Rows, page 2-45 .
Show All Rows	Displays all table rows that meet the current filtering criteria.
Properties	Displays the properties of the selected link.

Ticket Shortcut Menu

The Ticket shortcut menu is displayed when you right-click a ticket in the ticket pane. The Ticket shortcut menu enables you to view ticket properties and highlights the links or elements that are affected by a ticket. The Ticket menu also enables you to acknowledge, clear, and remove a ticket. For more information, see [Chapter 9, “Working with Tickets in Cisco ANA NetworkVision.”](#)

[Table 2-28](#) describes the ticket shortcut menu options.

Table 2-28 Ticket Shortcut Menu Options

Ticket Shortcut Menu 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 Cisco ANA. The ticket is displayed as Clear in the ticket pane. Note When a Card Out or Link Down alarm occurs, the relevant information is displayed in the inventory and maintained in the VNE.
Remove	Removes the ticket and all its active subtickets from the ticket pane (this option is only available after the ticket has been cleared). The deleted tickets can be viewed using Cisco ANA EventVision. Multiple tickets can be removed at the same time. Note When a ticket is removed, the information is no longer displayed in the inventory and is removed from the VNE.
Clear and Remove	Approves the reported faulty ticket and clears the faulty networking entity from Cisco ANA. In addition, the ticket and all its active subtickets are removed from the ticket pane.
Find Affected Elements	Finds any elements affected by the selected ticket: - If only one element is affected, it is selected in the Cisco ANA NetworkVision navigation pane and content area. - If multiple elements are affected, they are displayed in the Affected Elements window.
Show Only Selected Rows	Displays only the rows that you select. For more information, see Viewing Selected Rows, page 2-45 .

Table 2-28 Ticket Shortcut Menu Options (continued)

Ticket Shortcut Menu Option	Description
Show All Rows	Displays all table rows that meet the current filtering criteria.
Properties	Displays the Ticket Properties dialog box, enabling you to view ticket information, including impact analysis details of the affected parties and correlated alarms. See Viewing Ticket Properties, page 9-7 .

Changing a User Password in Cisco ANA NetworkVision

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

- If Cisco ANA provides login authentication, Cisco ANA NetworkVision enables you to change your login password. If needed, the administrator can also change your password in Cisco ANA Manage.
- If Cisco ANA uses an LDAP server for authentication, you cannot change your password in Cisco ANA NetworkVision. Only users with Administrator privileges can change your password, which must be done on the LDAP server.
 - For more information about external authentication, see the [Cisco Active Network Abstraction 3.7.1 Customization User Guide](#).
 - For more information about password guidelines, see the [Cisco Active Network Abstraction 3.7.1 Administrator Guide](#).

To change your password:

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



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

Step 2 Enter the following information:

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

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

Selecting Cisco ANA NetworkVision Map and Alarm Options

Cisco ANA NetworkVision enables you to select map, display, and audio options.

To select Cisco ANA NetworkVision options:

- Step 1** Choose **Tools > Options** from the main menu.
- Step 2** In the Startup tab, check the Load Workspace on Startup check box to automatically view the content pane when you log in. Uncheck the check box if you do not want to view the content pane when you log in.
- Step 3** Click the **Display** tab. Set the display options using the information in the following table.

Table 2-29 Cisco ANA NetworkVision Display Options

Field	Description
Preferences	
Map Labels Font Size	In the drop-down list, choose the preferred font size for labels on maps. Font sizes range from 10 to 14, with a default of 12.
Severity	
Show Severity Text (e.g. [3M+])	Check the check box to view severity labels in the navigation pane and maps, using the formula described in New Ticket Propagation, page 2-18 . Uncheck the check box to hide severity labels.
Show Acknowledged	Check the check box to view the number of both acknowledged and unacknowledged alarms in the network element display name. Uncheck the check box to view only the number of unacknowledged alarms in the network element display name. For example, assume that device NE1 has two alarms with the severity M. One of these two alarms is acknowledged, and the other is not. If you check the Show Acknowledged check box, the display name will be NE1 [2M]. If you uncheck the Show Acknowledged check box, the display name will be NE1 [1M].
Show Propagated	Check the check box to view propagated alarms on the specific entity. Uncheck the check box to view only the alarms on the specific entity.
Display Name	
Display Name	Select the preferred setting for network element names: - Do not use Business Tag—Displays the original network element name only. - Add Business Tag to name—Displays the original network element name and the name of the business tag. - Replace name with Business Tag—Replaces the network element name with the name of the business tag. When a subscriber is attached to a port, the name of the subscriber is also added.

- Step 4** Click the **Audio** tab.

- Step 5** Select your preferences for audio notifications:
- Check the Enable Audio Response for Alarm check box to indicate that a sound is to be issued when an alarm is triggered. Uncheck the check box to prevent a sound from being issued when an alarm is triggered.
 - In the Critical field, specify the .wav file to use for critical alarms.
 - In the Major field, specify the .wav file to use for major alarms.
 - In the Minor field, specify the .wav file to use for minor alarms.
 - Check the Loop Sound on Critical Alarm check box to play the critical alarm sound continuously when a critical alarm is triggered. Uncheck the check box to play the critical alarm sound only once when a critical alarm is triggered.
- Step 6** Click **Apply** to apply your selections.
- Step 7** Click **OK**.
-

Working with Cisco ANA Tables

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

- [Table Toolbar Options, page 2-40](#)
- [Finding Text in a Table, page 2-41](#)
- [Sorting a Table, page 2-42](#)
- [Filtering Table Contents, page 2-43](#)
- [Viewing Selected Rows, page 2-45](#)
- [Exporting Tables to a File, page 2-45](#)

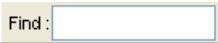
To view all text in a table cell, you can do either of the following:

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

Table Toolbar Options

[Table 2-30](#) describes the options available in table toolbars.

Table 2-30 Table Toolbar Options

Option	Name	Description
	Find	Searches the current table for the string you enter. For more information, see Finding Text in a Table, page 2-41 .
	Export to CSV	Exports the information displayed in the table, or selected portions, to a CSV file. For more information, see Exporting Tables to a File, page 2-45
	Sort Table Values	Sorts the information displayed in the table by the criteria you specify. For more information, see Sorting a Table, page 2-42 .
	Filter	Filters the information displayed in the table by the criteria you specify. For more information, see Filtering Table Contents, page 2-43 .
	Clear Filter	Clears the existing filter.
	Show All Rows	Displays all table rows that meet the current filtering criteria.
	Show Only Selected Rows	Displays only the rows that you select. For more information, see Viewing Selected Rows, page 2-45 .

Finding Text in a Table

Cisco ANA enables you to search for information about a specific network object in a table by entering search criteria, such as a partial IP address.

[Table 2-31](#) lists the keyboard shortcuts that you can use when working with tables.

Table 2-31 Keyboard Shortcuts for Tables

Keyboard Shortcut	Description
Ctrl + A	Selects all the rows in the table.
Ctrl + Space	Deselects all the rows in the table.
Enter	On a selected row, opens the default action.
Arrow Navigation Keys	Navigates up and down in the rows.
Ctrl + Up/Down	Keeps the selected row and moves up or down.
Ctrl + Up/Down + Space	Keeps the selected row and moves up or down. The space selects the required row.

Table 2-31 Keyboard Shortcuts for Tables (continued)

Keyboard Shortcut	Description
Shift + Up/Down	Keeps the selected row and selects all the rows that are above or below it.
Shift + F10	Opens the shortcut menu.
F3	Finds next.
Shift + F3	Finds previous.

To find text in a table:

-
- Step 1** In the Find field on the toolbar, enter the search criterion for the entity that you want to find and press **Enter**.
- Step 2** Press **F3** to continue searching the table or press **Ctrl + F** to return to the Find field.
-

Sorting a Table

Cisco ANA NetworkVision enables you to sort a table in one or more of the following ways:

- According to a column, by clicking the required column heading. The  icon is displayed next to the selected column heading, indicating continuous sorting.
- In ascending or descending order, by clicking a column heading.
- By clicking **Sort Table Values** in the toolbar and specifying sort criteria.

A triangle next to the column heading indicates the property by which the table is sorted.

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.
- Step 2** Enter the required information as defined in [Table 2-32](#):

Table 2-32 Sort Table Values Dialog Box

Field	Description
Sort By	Specify the first sort criterion: 1. In the drop-down list, select the column to use for the first sort criterion. 2. Click the Ascending or Descending radio button to indicate the sort order.

Table 2-32 Sort Table Values Dialog Box (continued)

Field	Description
Then By	(Optional) Specify the next sort criterion: 1. In the drop-down list, select the column to use for the second sort criteria. 2. Click the Ascending or Descending radio button to indicate the sort order.
Sort Operation	Specify the frequency of the sort operation by clicking the appropriate radio button: • Only Once—Sorts the information in the table only once according to the specified criteria. • 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 Click **OK**. The table information is sorted according to the filter defined.

Filtering Table Contents

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



Note

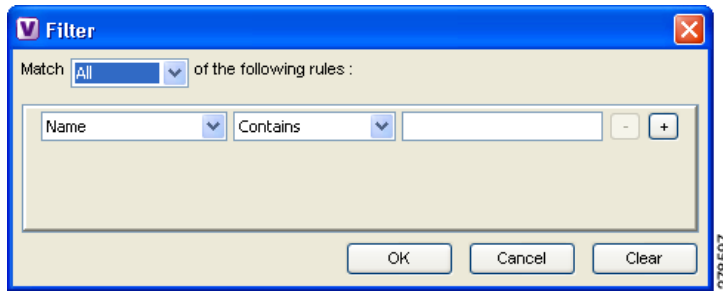
If you load a table with many entries, (for example, thousands of entries), it can take a while for the complete table to load. The filtering options in the table toolbar are unavailable until the table has completely loaded.

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

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

To define a filter:

Step 1 In the toolbar above the table, click **Filter**. The Filter dialog box is displayed as shown in [Figure 2-7](#).

Figure 2-7 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, list choose the rule to use for this criterion. The options are:
 - Contains
 - Does not contain
 - Equals
 - Does not equal
 - Greater than
 - Less than
- c. The third field either lists the available values or allows you to enter text:
 - If a drop-down list is displayed, choose the required entry.
 - If an entry field is displayed, enter a string or regular expression for the criterion. Any entry that is not a regular expression is treated as a string.

Step 4 Click  to add another criterion for this filter.

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

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

The table data is displayed using the defined filter.

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

The table is refreshed and all entries are displayed.

The following tables have additional filtering capabilities:

- Cisco ANA NetworkVision ticket pane. For more information, see [Filtering Tickets by Criteria, page 9-6](#).
- Links view in the content pane. For more information, see [Links View, page 2-13](#).

Viewing Selected Rows

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

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

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

Filter: 'Name' Contains ME

The status bar below the table also displays the:

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

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

Line 4 (1/6 Selected)

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

Line 0 (Size 6)

To view selected rows:

-
- Step 1** Select the appropriate line or lines in the table using standard Windows mouse or keystroke operations.
 - Step 2** Click **Show Only Selected Rows**.
The table displays the selected rows, and the Show All Rows option becomes active.
 - Step 3** Click **Show All Rows** to view all rows in the table.
-

Exporting Tables to a File

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

To export a table to a file:

-
- Step 1** Press **Ctrl + Space** to clear any existing selection.
 - Step 2** Identify the content you want to export:
 - To export specific rows, select the required rows.
 - To export the entire table, ensure that nothing is selected.
 - Step 3** In the toolbar above the table, click **Export to CSV**. The Export Table to File dialog box is displayed.
 - Step 4** Browse to the directory where you want to save the table.

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

Step 6 Click **Save**. The content specified in [Step 2](#) is saved in the selected directory.



CHAPTER 3

Viewing Network Element Properties

The following topics describe the user access roles required to use Cisco ANA NetworkVision and how to view network element physical and logical properties in any mapped network:

- [User Roles Required to Work with Cisco ANA NetworkVision, page 3-1](#)
- [Viewing the Properties of a Device, page 3-2](#)
- [Viewing VNE Properties, page 3-4](#)
- [Viewing VNE Communication Details, page 3-5](#)
- [Opening the Inventory Window, page 3-6](#)



Note The inventory window also enables you to view all the tickets that are collected on the selected NE in the ticket pane. For more information, see [Ticket Pane, page 3-9](#).

- [Viewing the Physical Properties of a Device, page 3-10](#)
- [Viewing the Logical Properties of a Network Element, page 3-13](#)
- [Viewing Device Operating System Information, page 3-17](#)



Note

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

User Roles Required to Work with Cisco ANA NetworkVision

[Table 3-1](#) identifies the roles that are required to work with Cisco ANA NetworkVision. Cisco ANA 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 device-based tasks (tasks that do affect devices), authorization is based on the default permission that is assigned to your account. That is, whether the device 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 Active Network Abstraction 3.7.1 Administrator Guide](#).

Table 3-1 *Default Permission/Security Level Required for Cisco ANA NetworkVision Functions*

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View maps	X	X	X	X	X
View device properties	X	X	X	X	X
View network element properties in logical and physical inventory	X	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	X

Viewing the Properties of a Device

Cisco ANA NetworkVision enables you to view the properties of a selected device using the Properties window. For example, in the Properties window you can view the vendor and location of a device.

To view device properties:

- Step 1

Right-click a device in the navigation pane, content pane, or device view, and choose **Properties**.
The Properties window is displayed as shown in [Figure 3-1](#).

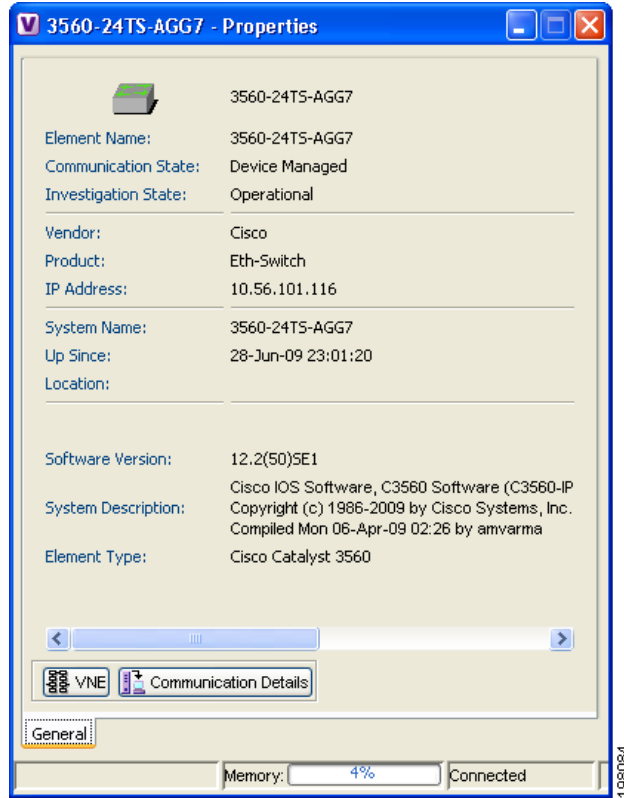
Figure 3-1 *Properties Window*

Table 3-2 describes the information displayed in the Properties window.

Table 3-2 *Properties Window*

Field	Description
Communication State	The ability of the VNE to reach the network element, according to the health of the device. For more information about communication states, see the Cisco Active Network Abstraction 3.7.1 Administrator Guide .
Investigation State	The 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 Active Network Abstraction 3.7.1 Administrator Guide .
Device icon	An icon representing the device in Cisco ANA and displaying the current color associated with the device operational health. For more information on severity colors, see Network Element Status Indicators , page 2-17. The device icon might include a badge (such as a bell or other symbol) that indicates an alarm or another item of interest associated with the device.
Vendor	The vendor name, as defined in the device MIB.
Product	The product name of the device, as defined in the device MIB; for example, Router.

Table 3-2 *Properties Window (continued)*

Field	Description
Element Name	A name assigned to the element for ease of identification.
IP Address	The IP address used for managing the device.
System Name	The name of the device, as defined in the device MIB.
Up Since	The date and time the device was last reset.
Location	The physical location of the device, as defined in the device MIB.
Software Version	The software version running on the device.
Software Description	A description of the system taken from the device.
Element Type	The device type with the manufacturer's name, such as Cisco 7200.
Buttons	
VNE	Opens the VNE Properties dialog box, where you can edit the VNE's properties, start and stop the VNE, perform maintenance, and configure polling rates. For more information, see: • Viewing VNE Properties, page 3-4 • Cisco Active Network Abstraction 3.7.1 Administrator Guide
Communication Details	Opens the Communication Details window, which displays the status of the device protocols and whether the device is sending traps and syslogs. For more information, see Viewing VNE Communication Details, page 3-5.

Step 2 To close the Properties window, click .

Viewing VNE Properties

To view VNE properties, open the inventory window (**Node > Inventory**) or Properties window (**Node > Properties**) for the required element, and then click **VNE**.

If the VNE for the element has been stopped, a message is displayed at the top of the inventory window letting you know that the VNE was stopped. The message includes a Refresh button so that you can refresh the information if the VNE has restarted. If the VNE is still down when you click **Refresh**, a VNE Unreachable message is displayed and the inventory window is closed. For more information about starting VNEs, stopping VNEs, adding new VNEs to a network, or modifying the status of a VNE, see the [Cisco Active Network Abstraction 3.7.1 Administrator Guide](#).



Note

The window displayed for all the devices is similar in appearance, but the information that is displayed varies according to the selected entity.

The inventory window also enables you to view all tickets that are collected on the selected NE in the ticket pane. For more information, see [Ticket Pane, page 3-9](#).

Viewing VNE Communication Details

To view VNE communication details:

- Step 1** In Cisco ANA NetworkVision, select the required element.
- Step 2** Open the inventory window (**Node > Inventory**) or Properties window (**Node > Properties**) for the selected item.
- Step 3** Click **Communication Details**.

The Communication Details window is displayed as shown in [Figure 3-2](#).

Figure 3-2 Communication Details Window



The Communication Details window provides information about:

- Management connectivity state
- SNMP connectivity
- Telnet connectivity
- ICMP connectivity
- Syslog connectivity
- Trap connectivity

For more information about the Communication Detail window, see the [Cisco Active Network Abstraction 3.7.1 Administrator Guide](#).

Opening the Inventory Window

The inventory window enables you to:

- View physical and logical inventory information.
- View tickets for a device.
- Open the Port Utilization graph for physical ports.
- Open Cisco ANA PathTracer.
- Add or remove links.
- Manage the alarms being sent on a port.
- Open the Cisco ANA Command Builder to create customized commands.
- Open the Cisco ANA Soft Properties Manager to extend the amount of information displayed. For more information, see the [Cisco Active Network Abstraction 3.7.1 Customization User Guide](#).
- View VNE properties. For more information, see [Viewing VNE Properties, page 3-4](#).
- View VNE communication details. For more information, see [Viewing VNE Communication Details, page 3-5](#).

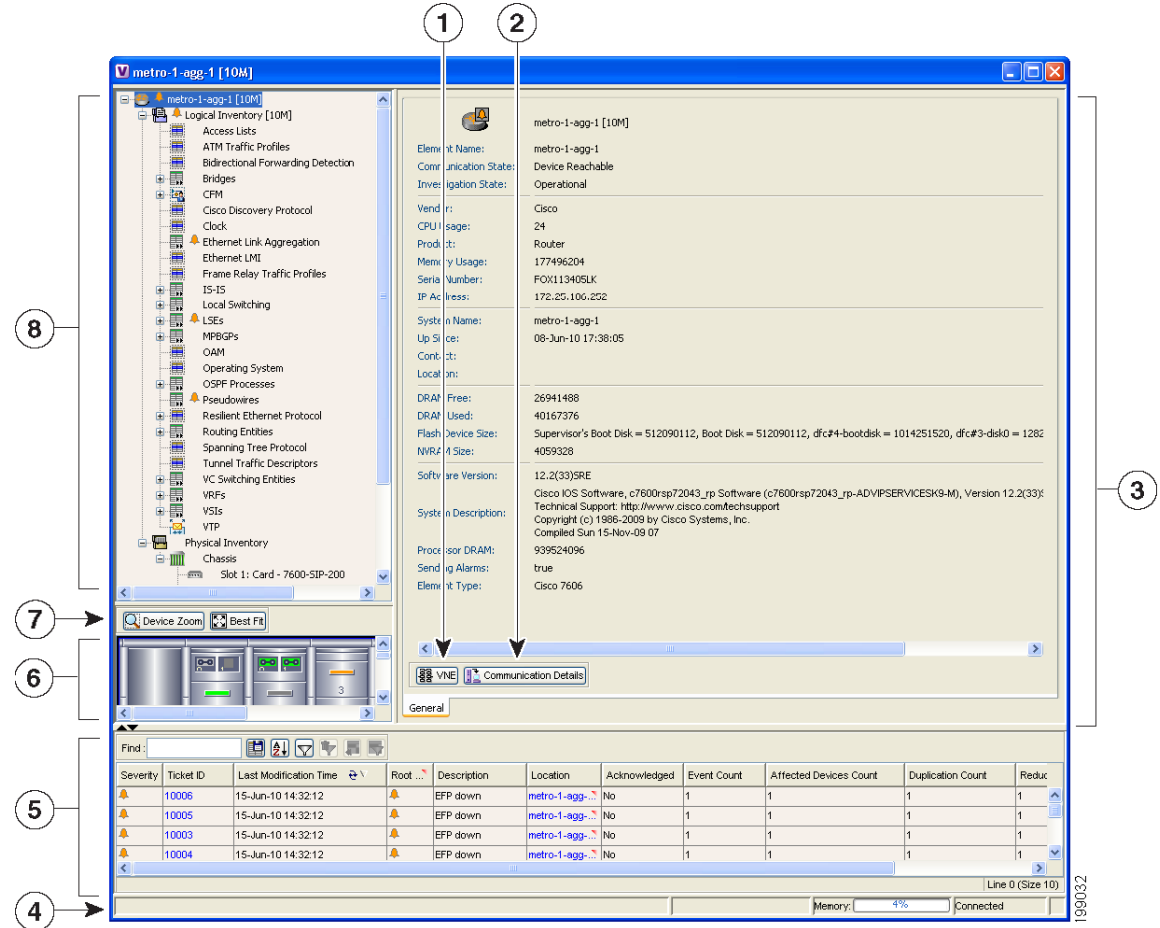
For more information on specific technologies, see:

- [Chapter 12, “Monitoring Carrier Ethernet Services”](#)
- [Chapter 13, “Monitoring Carrier Grade NAT Properties”](#)
- [Chapter 14, “Monitoring DWDM Properties”](#)
- [Chapter 15, “Viewing Ethernet Operations, Administration, and Maintenance Tool Properties”](#)
- [Chapter 16, “IPv6 and IPv6 VPN over MPLS”](#)
- [Chapter 17, “Monitoring MPLS Services”](#)
- [Chapter 18, “Monitoring MToP Services”](#)
- [Cisco Active Network Abstraction 3.7.1 Reference Guide](#)

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

- Select an element in the navigation pane or in a map, and then choose **Node > Inventory**.
- Double-click an item in the navigation pane or in a map.
- Right-click an element in the navigation pane or in a map to display the shortcut menu and then choose **Inventory**.

[Figure 3-3](#) shows an example of an inventory window.

Figure 3-3 *Inventory Window*

1	VNE button	5	Ticket pane
2	Communication Details button	6	Device view pane
3	Content pane	7	Device view pane toolbar
4	Status bar	8	Navigation pane

The inventory window displays the physical and logical inventory for the selected item. The inventory window is divided into the following areas:

- [Navigation Pane](#), page 3-8
- [Device View Pane](#), page 3-8
- [Device View Pane Toolbar](#), page 3-9
- [Ticket Pane](#), page 3-9
- [Content Pane](#), page 3-10

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 physical inventory information, open the physical inventory branch.

To view logical inventory information, open the logical inventory branch. For more information about logical inventory information, see [Viewing the Logical Properties of a Network Element, page 3-13](#).

If the selected VNE is shutting down when the inventory window is opened, a Refresh button is displayed in the inventory window so you can refresh the display when the VNE is available again.

Click the top right corner to close the inventory window.

For more information about the right-click shortcut menus that are available in the inventory window, see [Cisco ANA NetworkVision Shortcut Menus, page 2-29](#).

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 and physical inventory.

The logical inventory branch includes logical items related to the selected element, such as access lists, ATM traffic profiles, and routing entities. The physical inventory branch includes the different NE components, such as chassis, cards, slots, and so on. When you select an NE component in the navigation pane, the information displayed in the content pane is updated. The branches in the navigation pane can be expanded and collapsed 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 device as defined in Cisco ANA Manage. The highest level in the navigation pane also displays the device icon and status.

The color of the device icon in the navigation pane reflects its operational health and is the same as the color of the NE component in the device view panel. For more information about indicators of operational health and status, see [Network Element Status Indicators, page 2-17](#).

You can attach a business tag to an NE component by right-clicking it and then choosing **Attach Business Tag**. For more information about business tags, see [Chapter 6, “Working with Business Tags and Business Elements.”](#)

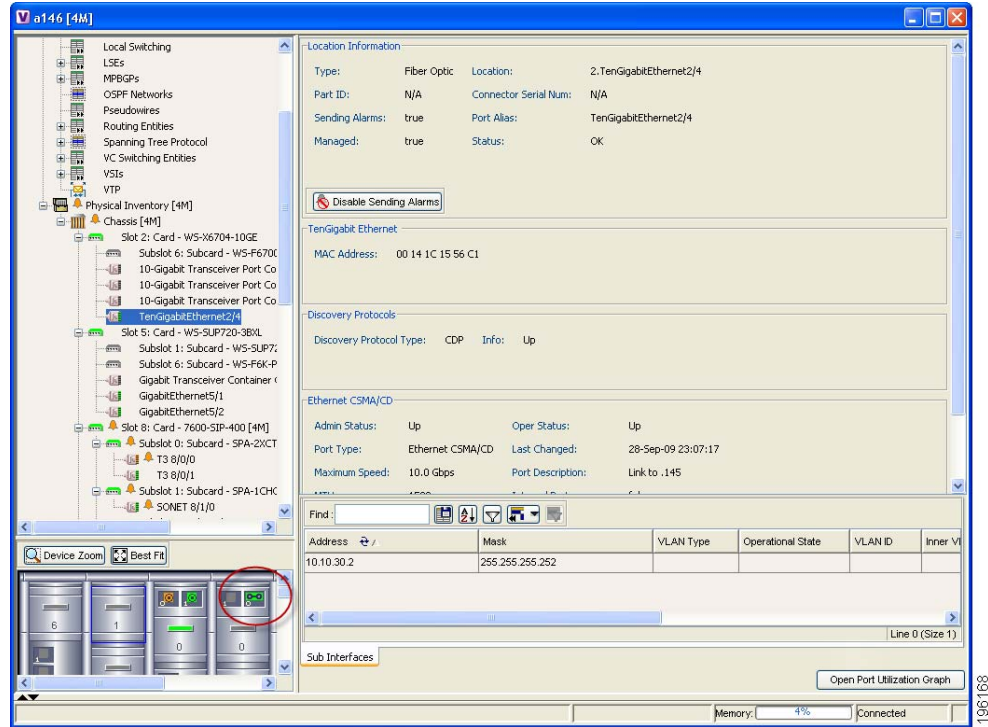
For more information about the right-click menus that are available, see [Cisco ANA NetworkVision Shortcut Menus, page 2-29](#).

Device View Pane

The device view pane enables you to visually locate NEs 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 3-4](#) provides an example of the device view pane for a Cisco device. The four slots in the device view pane correspond to the four slots in the physical inventory navigation pane. If you click a port in the device view pane (see the circled port), Cisco ANA displays both the element’s properties and its location in the physical inventory.

Figure 3-4 Device View Pane



Device View Pane Toolbar

The inventory window contains the following tools for working with the device view pane:

Icon	Description
	Displays an enhanced view of the network element 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 device displayed in the device view panel.

Ticket Pane

The ticket pane is displayed at the bottom of the inventory window. The tickets displayed relate to the element selected in the navigation pane. For more information about the ticket pane, see [Ticket Pane, page 2-15](#).



Note

The ticket pane can be displayed or hidden by clicking the arrows displayed below the device view panel.

Content Pane

The content pane contains physical or logical inventory information specific to the item you select in the navigation pane or device view panel; for example, chassis or port information.

The content pane can also display context-sensitive tabs and toolbars; the tools displayed depend on your selection in the navigation pane or device view panel. For example, when an ATM port is selected, the Show VC Table tool is displayed on the toolbar.

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

For information about tables that appear in the content pane, see [Working with Cisco ANA Tables, page 2-40](#).

Viewing the Physical Properties of a Device

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

- Device
- Chassis
- Shelves
- Slots
- Subslots
- Ports, including logical ports

[Table 3-3](#) identifies the icons used to display physical inventory components in the navigation pane.

Table 3-3 Physical Inventory Icons

Icon	Device
	Chassis
	Shelf
	Slot/Subslot
	Port/Logical Port
	Unmanaged Port

Pluggable transceiver modules on Cisco equipment are displayed in a three-level hierarchy:

Container object

Module (such as an SFP container)

Port (such as an SFP or GBIC 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.

For Cisco CRS devices only, fans and power supplies are displayed in physical inventory if they are field replaceable units (FRUs). The manner in which the fans are displayed depends on whether the fans are separable or not:

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

The system also includes built-in system properties for each network element. This includes information such as MAC address, maximum transmission unit (MTU), and media type.

**Note**

The window displayed for all the devices is similar in appearance. However, the components contained in each device can vary.

The information displayed in the content area changes according to the device type, device, and component selected in the navigation pane.

The following buttons might be displayed in the inventory window for physical inventory:

- **Disable Sending Alarms**—Enables you to manage the alarms on a port. For more information, see [Managing Port Alarms, page 3-12](#).
- **Open Port Utilization Graph**—Displays the selected port traffic statistics: Rx/Tx Rate and Rx/Tx Rate History. For more information, see [Opening the Port Utilization Graph, page 3-11](#).
- **Show Encapsulation**—Displays encapsulation information for incoming and outgoing traffic for the selected item; for example, for L2 or ATM encapsulation.
- **Show Cross-Connect Table**—Displays cross-connect information for incoming and outgoing ports.
- **Show DLCI Table**—Displays data-link connection identifier (DCLI) information for the selected port.
- **Show VC Table**—Displays virtual circuit (VC) information for the selected port.

For information about configuring topology from a port, see [Adding Static Links, page 5-12](#).

For a detailed description of device properties, see [Viewing the Properties of a Device, page 3-2](#).

Opening the Port Utilization Graph

Cisco ANA NetworkVision 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 double-click the required port.
- Step 2** Click **Open Port Utilization Graph** in the Port Connector Properties window.
- 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.
-

Managing Port Alarms

You can enable or disable the alarms on a selected port. 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 pane.

Disabling Alarms

To disable alarms:

-
- Step 1** Open the inventory window for the required device.
- Step 2** Do one of the following in the navigation pane:
- Right-click the required port and choose **Disable Sending Alarms**,
 - Select the port and then click **Disable Sending Alarms** in the context pane.

The Sending Alarms field in the Location Information section of the content pane displays the value false. This indicates that the alarm for the required port has been disabled. In addition, the toolbar in the content pane displays the Enable Sending Alarms tool.

Enabling Alarms

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

To enable alarms:

-
- Step 1** Open the inventory window for the required device.
- Step 2** In the navigation pane, select the port and then click **Enable Sending Alarms**.

The Sending Alarms field in the Location Information section of the content pane displays the value true. This indicates that the alarm for the required port has been enabled. In addition, the toolbar in the content pane now displays the Disable Sending Alarms tool.

Viewing the Logical Properties of a Network Element

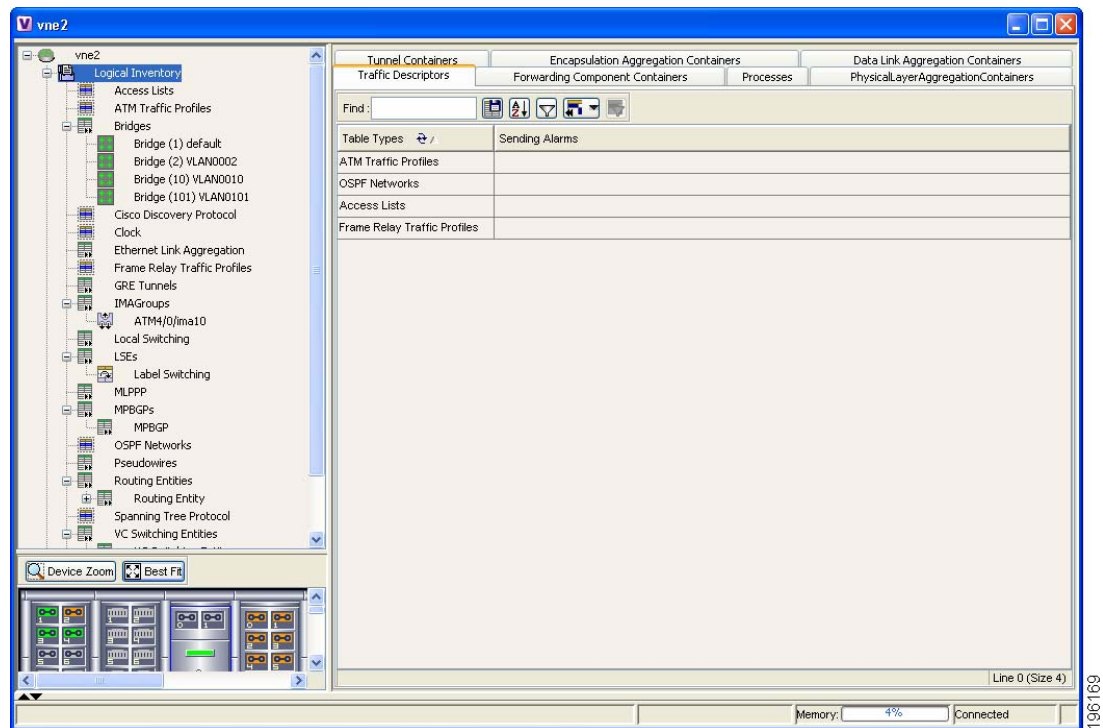
Cisco ANA NetworkVision enables you to view logical inventory information. Cisco ANA maintains logical inventory for each device. The logical inventory reflects dynamic data such as configuration data, forwarding, and service-related components that affect traffic handling in the device.

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

Logical Inventory Window

Logical inventory information is displayed in the inventory window as shown in [Figure 3-5](#).

Figure 3-5 Logical Inventory Information Displayed in the Inventory Window



Note

For more information about opening the inventory window, see [Opening the Inventory Window](#), page 3-6.

Logical Inventory Navigation Pane Branches

Table 3-4 describes the branches that appear in the logical inventory navigation pane.

Table 3-4 Logical Inventory Navigation Pane Branches

Name	Description
Access Lists	Provides details on access lists.
ATM Traffic Profiles	Provides details on traffic profiles for ATM.
Bidirectional Forwarding Detection	Provides details related to Bidirectional Forwarding Detection.
Bridges	Provides details on configured VLANs.
Carrier Grade NAT	Provides details on Carrier Grade Name Address Translation (NAT).
CFM	Provides details related to Connectivity Fault Management (CFM).
Cisco Discovery Protocol	Provides details on NEs using Cisco Discovery Protocol (CDP).
Clock	Provides details on network clock service, clock recovery, and Precision Time Protocol (PTP) configuration.
Ethernet Link Aggregation	Provides details on Ethernet aggregation groups.
Frame Relay Traffic Profiles	Provides details on traffic profiles for Frame Relay.
GRE Tunnels	Provides details on generic routing encapsulation (GRE) tunneling protocol for IP tunnels.
IMA Groups	Provides details on Inverse Multiplexing over ATM (IMA) groups.
Link Layer Discovery Protocol	Provides details on Link Layer Discovery Protocol (LLDP).
Local Switching	Provides details on local switching.
LSEs	Provides details on local switching for MPLS interfaces.
MLPPP	Provides details on Multilink Point-to-Point (MLPPP) configurations.
Modular OS	Provide details on modular operating systems for Cisco IOX XR devices.
MPBGPs	Details 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.
Operating System	Provides information on the operating system for Cisco IOS devices.
OSPF Processes	Provides details on OSPF processes, such as the Shortest Path First (SPF) timer settings, OSPF neighbors, and OSPF interfaces.
Pseudowires	Provides details on pseudowire end-to-end emulation (PW3E) tunnels.
Resilient Ethernet Protocol	Provides details on Resilient Ethernet Protocol (REP).
Routing Entities	Provides details on routing table entries and IP interfaces.

Table 3-4 Logical Inventory Navigation Pane Branches (continued)

Name	Description
Session Border Controller	Provides details on Session Border Controller (SBC) configuration.
Spanning Tree Protocol	Provides details on STP and Multiple Spanning Tree Protocol (MSTP) configurations.
Traffic Engineering Tunnels	Provides details on traffic engineering (TE) tunnels.
VC Switching Entities	Provides details on cross-connects and VC traffic.
VRFs	Provides details on Virtual Routing and Forwarding (VRF).
VSIs	Provides details on Virtual Switch Interface (VSI) instance names, associated pseudowire information, virtual circuit IDs, and so on.
VTP	Provides details on VLAN Trunk Protocol domain names, modes, version numbers, and so on.

Logical Inventory Navigation Pane Icons

Table 3-5 describes the icons used in the logical inventory navigation pane.

Table 3-5 Logical Inventory Navigation Pane 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
	ARP Entity	MPBGPs
	Bridges	OSPF Processes
	Ethernet Link Aggregation	Pseudowires
	GRE Tunnels	Routing Entities
	IMA Groups	Traffic Engineering Tunnels
	Local Switching	VC Switching Entities
	LSEs	VRFs
	MLPPP	VSIs
	Bridge	

Table 3-5 *Logical Inventory Navigation Pane Icons (continued)*

Icon	Logical Inventory Item
	Connectivity Fault Management (CFM)
	CFM Maintenance Association
	CFM Maintenance Domain
	Cross-VRF
	Encapsulation
	Inverse Multiplexing over ATM (IMA) group
	Label switching
	Logical inventory
	Multiple Spanning Tree protocol (MST) instance
	Virtual Switch Interface (VSI)
	VLAN Trunk Protocol (VTP)

Logical Inventory Content Pane Tabs

[Table 3-6](#) describes the tabs that can appear in the logical inventory content pane, depending on your selection in the navigation pane.

Table 3-6 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.
Forwarding Component Containers	Lists the context profiles for which logical inventory information can be displayed, such as routing entities and bridges.
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 pseudowire or GRE tunnels.

Viewing Device Operating System Information

Cisco ANA discovers and automatically displays operating system information for Cisco IOS and Cisco IOS XR devices in logical inventory.

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

-
- Step 1** In Cisco ANA NetworkVision, double-click the required device.
- Step 2** For a Cisco IOS device, in the inventory window, choose **Logical Inventory > Operating System**. [Table 3-7](#) describes the information that is displayed for the Cisco IOS operating system:

Table 3-7 Operating System Information in Logical Inventory

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

- Step 3** For a Cisco IOS XR device, in logical inventory, choose **Logical Inventory > Modular OS**. [Figure 3-6](#) shows an example of the information that is displayed for Cisco IOS XR devices.

Figure 3-6 Modular OS Information in Logical Inventory

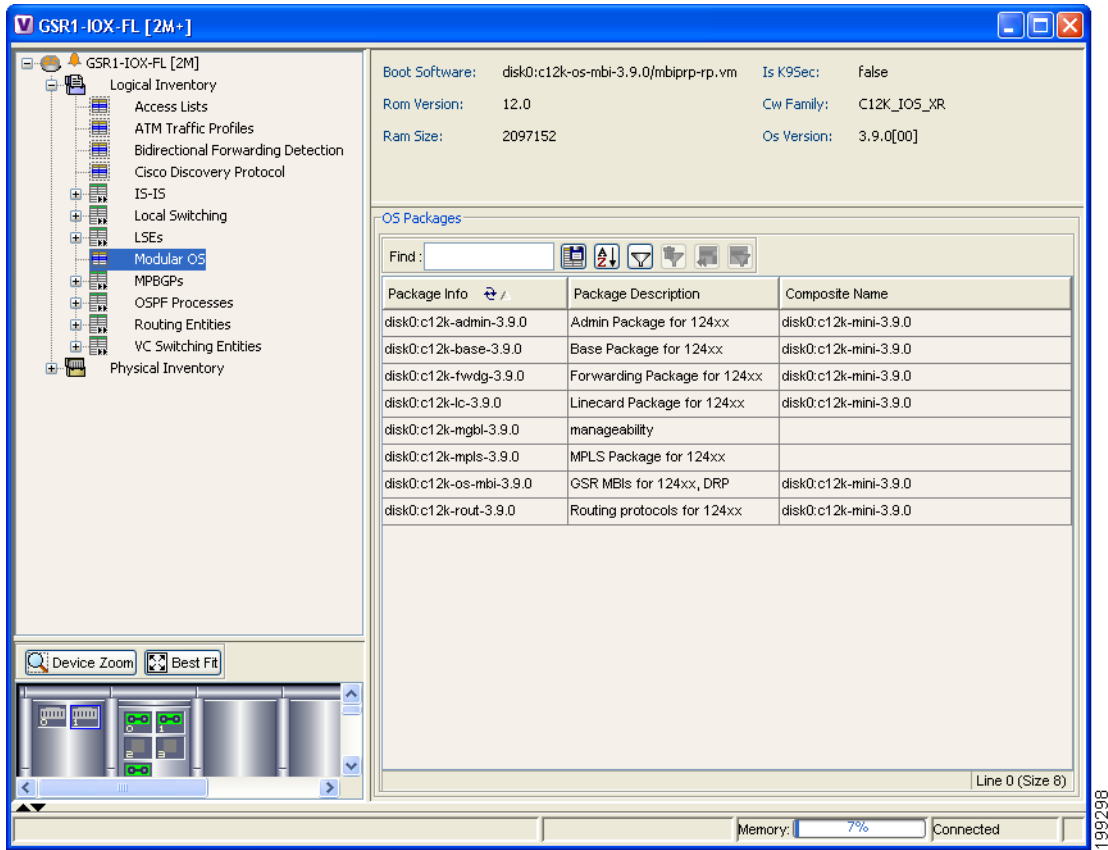


Table 3-8 describes the information that is displayed for Cisco IOS XR system.

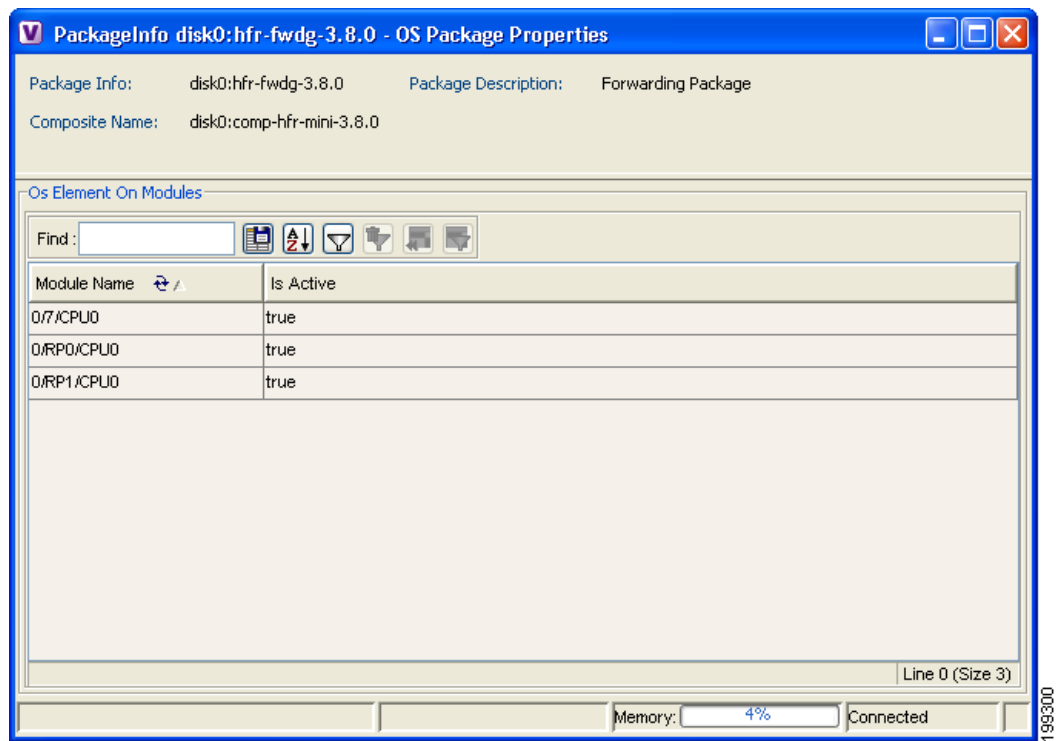
Table 3-8 Modular OS Information in Logical Inventory

Field	Description
Boot Software	Cisco IOS XR system image information.
Is K9Sec	Whether or not the K9 security feature is enabled on the operating system: True or False
ROM Version	Cisco IOS XR bootstrap software version, such as 1.51.
Cw Family	Cisco software family, based on the device platform, such as CRS_IOS_XR or C12K_IOS_XR.
RAM Size	Size, in kilobytes, of the device processor RAM.
OS Version	Cisco IOS XR software version, such as 3.8.0[00].
OS Packages Table	
Package Info	Information on the individual package and its version, such as disk0:hfr-admin-3.8.0.

Table 3-8 *Modular OS Information in Logical Inventory (continued)*

Field	Description
Package Description	Description of the package, such as FPD (Field Programmable Device) Package.
Composite Name	Composite package name of the package, such as disk0:comp-hfr-mini-3.8.0.

Step 4 To view details about an individual package, double-click the package in the OS Packages table. The OS Package Properties window is displayed as shown in [Figure 3-7](#).

Figure 3-7 *OS Package Properties Window*

[Table 3-9](#) describes the information displayed in the OS Package Properties window.

Table 3-9 OS Package Properties Window

Field	Description
Package Info	Information on the individual package and its version, such as disk0:hfr-admin-3.8.0.
Package Description	Description of the package, such as FPD (Field Programmable Device) Package.
Composite Name	Composite package name of the package, such as disk0:comp-hfr-mini-3.8.0.
OS Element on Modules	
Module Name	Name of the module on which the package is installed.
Is Active	Whether or not the package is active: Yes or No.



CHAPTER 4

Working with Cisco ANA NetworkVision Maps

The topological map is the main tool used by Cisco ANA NetworkVision to display the links and relationships between the network elements and aggregated nodes. The following topics describe how to work with the topological maps displayed in the content pane of the Cisco ANA NetworkVision window:

- [User Roles Required for Working with Cisco ANA NetworkVision Maps, page 4-2](#)
- [Opening Maps, page 4-3](#)
- [Creating a New Map, page 4-6](#)
- [Adding Elements to a Map, page 4-6](#)
- [Removing Elements from a Map, page 4-9](#)
- [Defining a Map Layout, page 4-10](#)
- [Saving Maps, page 4-10](#)
- [Deleting a Map from the Cisco ANA Database, page 4-13](#)
- [Renaming a Map, page 4-14](#)
- [Resizing a Map Element, page 4-14](#)
- [Viewing the Network Map, page 4-15](#)
- [Viewing a Network Device, page 4-16](#)
- [Selecting Map Views, page 4-16](#)
- [Finding Elements Affected by a Ticket, page 4-17](#)
- [Finding and Selecting Links in Maps, page 4-18](#)
- [Finding a Network Device or Service, page 4-19](#)
- [Working with Aggregations, page 4-22](#)
- [Filtering Links According to Type, page 4-24](#)
- [Opening the CPU Usage Graph, page 4-26](#)
- [Communicating with Devices Using Ping and Telnet, page 4-27](#)
- [Previewing and Printing a Map, page 4-27](#)

You can also perform the following functions from the map and list views if they are configured for your client. These are described in the [Cisco Active Network Abstraction 3.7.1 Customization User Guide](#).

- Launch external applications or tools, such as an SSH client.
- Launch available activation and configuration scripts, including those you create using Command Builder. These scripts can be launched against multiple NEs at the same time.

User Roles Required for Working with Cisco ANA NetworkVision Maps

Table 4-1 identifies the roles that are required to work with Cisco ANA NetworkVision maps. Cisco ANA 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 device-based tasks (tasks that do affect devices), authorization is based on the default permission that is assigned to your account. That is, whether the device 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 Active Network Abstraction 3.7.1 Administrator Guide](#).

Table 4-1 Default Permission/Security Level Required for Working with Cisco ANA NetworkVision Maps

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Map-Related Tasks					
Add elements to a map	—	—	X	X	X
Create maps	—	—	X	X	X
Define a map layout	X	X	X	X	X
Delete maps	—	—	X	X	X
Group and ungroup aggregations	—	X	X	X	X
Preview and print maps	X	X	X	X	X
Remove elements from a map	—	—	X	X	X
Rename maps	—	—	X	X	X
Resize elements in a map	X	X	X	X	X
View maps ¹	X	X	X	X	X
Link-Related Tasks					
Filter links	—	—	X	X	X
Find and select a link in a map	—	—	X	X	X

Table 4-1 *Default Permission/Security Level Required for Working with Cisco ANA NetworkVision Maps (continued)*

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Other Tasks					
Open the CPU Usage Graph	—	—	—	—	X
Use Ping and Telnet to communicate with devices	—	—	—	—	X

1. A user with Viewer, Operator, OperatorPlus, or Configurator access can view objects in a map, but the objects are generic in their representation and are displayed with a locked icon on them.

Opening Maps

Cisco ANA provides two methods for opening maps:

- You can open commonly used maps (if you left the maps open when you last exited Cisco ANA NetworkVision). See [Opening Commonly Used Maps, page 4-3](#).
- You can view all existing maps and choose the ones you want to open. See [Opening a New Map from the Open Map Dialog Box, page 4-4](#).

For information on how to close a map, see [Closing a Map, page 4-5](#).

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

Opening Commonly Used Maps

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



Note

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

To open a commonly used map that you did not close previously:

- Step 1** Launch Cisco ANA NetworkVision as described in [Starting Cisco ANA NetworkVision, page 2-2](#). The Cisco ANA NetworkVision window opens, and the Last Open Maps dialog box is displayed.
- Step 2** Check the check boxes for the maps you want to open, and uncheck the check boxes for the maps you do not want to open.
- Step 3** Click **OK**.

Opening a New Map from the Open Map Dialog Box

You can open any maps that are in the Open Map dialog box, even if you have never accessed them before.

To open a new map:

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

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

The Open Map dialog box lists the existing maps.

The Find field enables you to search for a map containing the string that you enter. For more information, see [Finding Text in a Table, page 2-41](#).

You can use the tools described in [Table 4-2](#) to manage maps in the Open Map dialog box.

Table 4-2 Open Map Dialog Box Options

Tool	Description
	Export to CSV—Exports the information displayed in the table. For more information, see Exporting Tables to a File, page 2-45 .
	Delete Map—Deletes the selected map from the Open Map dialog box, the Cisco ANA NetworkVision window and the database. If a map that is opened is deleted, the map closes. For more information, see Deleting a Map from the Cisco ANA Database, page 4-13 .
	Rename Map—Renames the selected map in the Open Map dialog box and Cisco ANA NetworkVision window. For more information, see Renaming a Map, page 4-14 .
	Sort Table Values—Sorts the information displayed in the table.
	Filter—Defines a filter for the information displayed in the table. For more information, see Filtering Table Contents, page 2-43 . Note When a filter is applied, the Clear Filter button is activated.
	Clear Filter—Clears the existing filter.
	Show All Rows—Displays all table rows that meet the current filtering criteria.
	Show Only Selected Rows—Displays only the rows that you select. For more information, see Viewing Selected Rows, page 2-45 .

- Step 2** Select the maps you want to open using one of the following methods. You can select multiple maps by pressing **Ctrl** while you select individual maps.
- Select the maps in which you are interested, and then click **Open**.
 - Right-click the required maps and choose **Open**.
 - Double-click the required maps.

Use the Window menu in the Cisco ANA NetworkVision window to move between the open maps. For more information on the Cisco ANA NetworkVision window, see [Cisco ANA NetworkVision Window, page 2-4](#).



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

Closing a Map

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

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

To close a map:

-
- Step 1** (Optional) To save more than the default map information, use one of the following methods:
- Click **Save Map Appearance** in the main toolbar.
 - Choose **File > Save Map** from the main menu.

- Step 2** Do one of the following:
- Choose **File > Close**.
 - Click  in the upper right corner of the content pane.

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

- Step 3** Click **Yes**. The map is saved and closed. An empty Cisco ANA NetworkVision window is displayed, or the map that was last opened is displayed.
-

Creating a New Map

Cisco ANA NetworkVision enables you to create multiple network maps to represent specific network views. Views can cover specific network segments, customer networks, or any other mix of network elements desired. When you create a map, it is available to other users if they have sufficient access and security privileges.

The network maps provide a graphic display of active faults and alarms, and serve as an easy access point for activating services.

Keep the following in mind when creating a new map:

- You cannot specify the same name for two or more maps.
- If you use non-US characters for a map name, they are not displayed correctly in the navigation pane. However, the names are displayed correctly in the Window menu.

To create a new map:

Step 1 Do one of the following:

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

The Create Map dialog box is displayed.

The Advanced button enables you to filter the links displayed in the map pane. For more information, see [Filtering Links According to Type, page 4-24](#).

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

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

Step 3 Add elements to your new map as described in [Adding Elements to a Map, page 4-6](#).

See the following topics for information on adding elements to and removing elements from a map:

- [Adding Elements to a Map, page 4-6](#)
- [Removing Elements from a Map, page 4-9](#)

Adding Elements to a Map

When you add a network element to a map, the map is automatically saved in the Cisco ANA database.



Note

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

To add a network element:

Step 1 Do one of the following:

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

Figure 4-1 shows the elements available for adding to maps.

Figure 4-1 Available Elements to Add to Maps

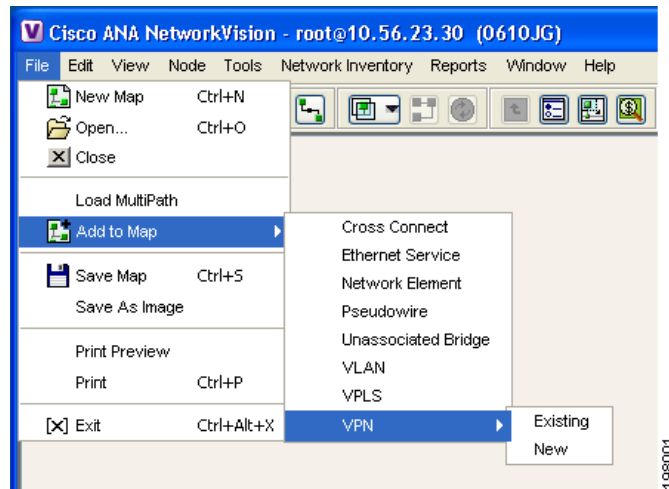


Table 4-3 describes the types of elements that you can add to a map and the available search criteria for each type.

Table 4-3 Network Elements to Add to Maps

Name	Description
Cross-Connect	EFP cross-connects that can be added to the map. The Search field allows you to search for an EFP cross-connect by name.
Ethernet Service	Ethernet services that can be added to the map. The Search field allows you to search for an Ethernet Service by any of the following categories: • EVC-terminating EFPs • Name • System name
Network Element	Devices that can be added to the map. The Search field allows you to search for a device by any of the following categories: • Element Category • Element Type • IP Address • Name • System Name • Vendor

Table 4-3 **Network Elements to Add to Maps (continued)**

Name	Description
Pseudowire	Pseudowires that can be added to the map. The Search field allows you to search for a pseudowire by any of the following categories: • Description • Is Multisegment Pseudowire • Name • Pseudowire Type • System Name
Unassociated Bridge	Unassociated bridges that can be added to the map. The Search field allows you to search for unassociated bridges by name.
VLAN	VLANs that can be added to the map. The Search field allows you to search for a VLAN by any of the following categories: • Ethernet Flow Domain • ID • Name
VPLS	VPLS instances that can be added to the map. The Search field allows you to search for a VPLS instance by name.
VPN > Existing	Existing VPNs that can be added to the map. The Search field allows you to search for a VPN by either of the following categories: • Description • Name
VPN > New	Opens the Create VPN dialog box so that you can create a new VPN to add to the map. For information on creating a VPN, see Creating a VPN, page 17-6.

After you select the required type of element, the *Add element to map* dialog box is displayed. For example, if you are adding a pseudowire to a map named CompanyEast, the dialog box is named Add Pseudowire to CompanyEast.

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

- To search for specific elements:
 - a. In the Search field, choose a search category.
 - b. Enter a search string to narrow the display to a range of elements or to a specific element. [Table 4-3](#) identifies the search categories available for each type of element.

c. Click **Go**.

For example, if you choose IP Address and enter **254**, the network elements that have IP addresses beginning with 254 are displayed. If you choose Vendor and enter Cisco, only Cisco network elements are displayed.

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



Note If you choose **Show All** and the number of elements for that type is large, it might take a while for all elements to be displayed.

The available elements that meet the specified search criteria 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**.



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

For information about sorting and filtering the table contents, see [Working with Cisco ANA Tables, page 2-40](#).

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

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

The network element information is saved with the map in the Cisco ANA database.

Removing Elements from a Map

When you delete an element or aggregated node from a map, it is removed from the map in the database, but the elements are still managed by Cisco ANA.



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 aggregated node from a map:

-
- Step 1** In the navigation pane or map, select the network element or aggregated node that you want to delete.
- Step 2** Right-click to display the shortcut menu and choose **Remove from Map**. The selected network element or aggregated node is removed from the map.
-

The network element is removed from the map in the database, but is still managed by Cisco ANA and can be added again.

Defining a Map Layout

Cisco ANA NetworkVision enables you to select the way in which the network object topology is displayed. The map view displays the objects in the selected layout: circular, symmetric, tree, or hierarchical.

You can select the map layout by using either of the following methods:

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

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

Saving Maps

Cisco ANA provides three options for saving maps:

- To save more map information than Cisco ANA saves by default, see [Saving a Map with Information, page 4-10](#).
- To save a copy of a map so you can use it as a template for another map, see [Saving a Map as a New Map, page 4-11](#).
- To save a map as an image, see [Saving a Map as an Image, page 4-11](#).

Saving a Map with Information

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

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

To save these changes, do one of the following:

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

Saving a Map as a New Map

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

To save a map as a new map:

-
- Step 1** Make sure that the map that you want to save is displayed in the Cisco ANA NetworkVision content pane.
 - Step 2** Select the required map, elements, or aggregated nodes in the navigation tree or the map.
 - Step 3** Right-click in the navigation pane or one of the selected items in the map pane, and choose **Save as New Map**.
 - Step 4** In the Create Map dialog box, enter a new name for the map.
 - Step 5** Click **OK**. The new map is created.
-

**Note**

For information about opening the new map, see [Opening a New Map from the Open Map Dialog Box, page 4-4](#).

Saving a Map as an Image

To save a map as an image:

-
- Step 1** Display the required map in Cisco ANA NetworkVision.
 - Step 2** Choose **File > Save As Image** from the main menu.
 - Step 3** In the Save as Image dialog box, define the image characteristics as described in [Table 4-4](#).

Figure 4-2 Save as Image Dialog Box

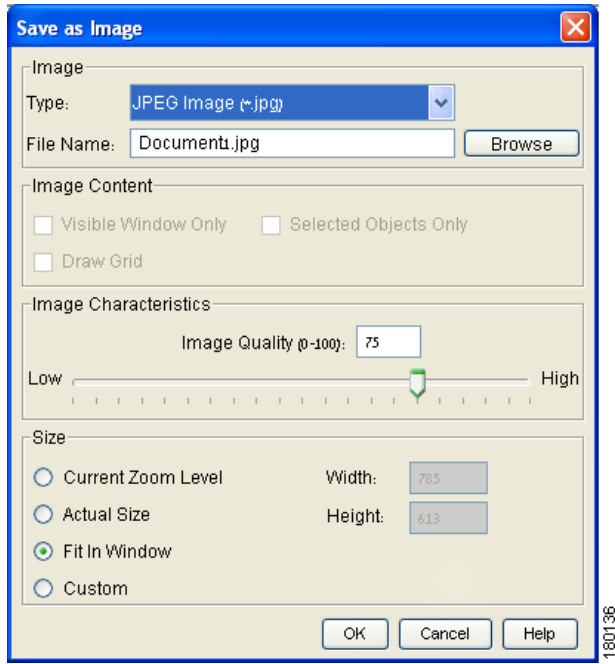


Table 4-4 Save as Image Dialog Box Options

Attribute	Description
Image	Specify the image type and filename: - Type—In the drop-down list, select JPEG Image (*.jpg). The file types .svg and .png are not available. - File Name—Enter a filename for the image.
Image Content	Check the appropriate check box for the content to be included in the image: - Visible Window Only—Saves the currently selected map as an image, even if the content area displays the list view or the links view. - Draw Grid—This option is not available. - Selected Objects Only—Saves the selected network objects as an image.

Table 4-4 *Save as Image Dialog Box Options (continued)*

Attribute	Description
Image Characteristics	Define the quality of the image using one of the following methods. Both methods use values of 0 to 100 where 0 is the lowest quality and 100 is the highest quality. • Image Quality (0-100)—Enter a value from 0 to 100. • Low-High—Click and drag the slider to the required level of quality.
Size	Specify the required zoom level for the image: • Current Zoom Level—Saves the image at the currently selected zoom level. Selecting this option enables the Visible Window Only check box. • Actual Size—Saves the image at the actual size. • Fit in Window—Saves the image so that it fits in the window. • Custom—Saves the image at an enlarged or reduced size. Selecting this option enables the Width and Height options, so that you can enter the required size.

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

Deleting a Map from the Cisco ANA Database

Cisco ANA NetworkVision enables you to delete a map from all the views in the Cisco ANA NetworkVision window.

If another client is using a map that you are deleting, Cisco ANA displays a message to those clients advising them that the map is being closed and deleted from the database.

To delete a map from Cisco ANA NetworkVision and the Cisco ANA database:

Step 1 Open the Open Map dialog box in one of the following ways:

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

Step 2 In the Open Map dialog box, complete the following steps:

- a. In the Open Map dialog box, select the map that 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 Cisco ANA NetworkVision window, and the database.
- d. Click **Cancel** to close the Open Map dialog box.

Renaming a Map

Cisco ANA NetworkVision enables you to rename a map that is displayed in the Cisco ANA NetworkVision window. The name change affects all users of the map and the new name is displayed in the Cisco ANA NetworkVision window of all users.

To rename a map:

-
- Step 1** Do one of the following:
- Click **Open Map** in the main toolbar.
 - Choose **File > Open** from the main menu.
- Step 2** In the Open Map dialog box, select the map that you want to rename.
- Step 3** Click **Rename Map** in the toolbar.
- Step 4** Enter the new map name.
- Step 5** Click **OK**. The selected map is renamed in the Open Map dialog box, in the Cisco ANA NetworkVision window, and in the database.
- Step 6** Click **Cancel** to close the Open Map dialog box.
-

Resizing a Map Element

Cisco ANA NetworkVision enables you to define the size of selected devices or aggregated nodes in the map view, according to predefined sizes or according to a percentage of the current size.



Note

You can manually resize a node by selecting it and dragging the corner (handle).

To resize a device or aggregated node:

-
- Step 1** In the map, select the devices or aggregated node that you want to resize.
-  **Note** The Resize option is enabled only when devices or aggregated nodes are selected. Links cannot be resized.
-
- Step 2** Do one of the following:
- Choose **Edit > Resize** from the main menu.
 - Right-click the selected devices or aggregated node in the map, and choose **Resize**.
- Step 3** In the Resize Nodes Controller dialog box, set the size of the devices or nodes:
- In the Resize Node field, select a resizing percentage from the drop-down list.
 - In the Set Nodes Sizes field, select a fixed size from the drop-down list.
- Step 4** Click **OK**. The selected devices or aggregated node are resized.
-

Viewing the Network Map

Cisco ANA NetworkVision enables you to display the entire network map or any part of the map in the Cisco ANA NetworkVision map view.

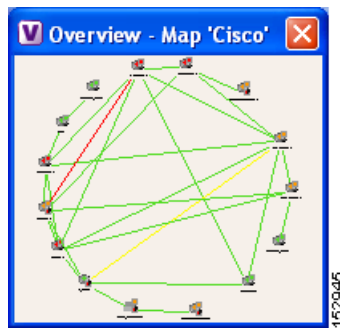
Use the Zoom tools or the Overview window to display the part of the map that you require. Viewing the Overview window enables you to see all the changes and alarms taking place in the network. In addition, you can display an aggregated node in a thumbnail.

Viewing a Network Overview

To open an overview of the network:

- Step 1** Do one of the following:
- Click **Overview** in the main toolbar.
 - Choose **View > Overview** from the main menu.

Figure 4-3 Overview Window



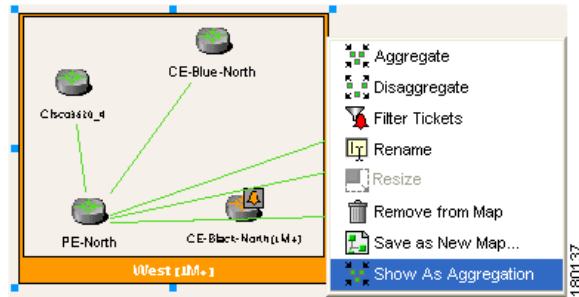
- Step 2** In the Overview window, select the required area by clicking and dragging the mouse, thereby enlarging it in the map pane. A blue rectangle is displayed around the selected area. You can move the selected area by placing the mouse within the rectangle. The mouse icon changes to a hand, and you can then click and drag the mouse to move the rectangle over the required area.
- Step 3** Click and drag the rectangle again to select or resize a different network area.
- Step 4** Click the upper right corner to close the Overview window.

Viewing an Aggregated Node Thumbnail

In addition, you can display a thumbnail of the selected aggregated node in the map pane, including all aggregated devices. Thumbnails can also be nested.

To display a thumbnail of the node:

- Step 1** Right-click an aggregated node, and choose **Show Thumbnail**. The thumbnail is displayed in the map pane.

Figure 4-4 Thumbnail

Step 2 From here you can do the following:

- To redisplay the aggregated node in the map, right-click the thumbnail frame and choose **Show As Aggregation**.
- To resize the thumbnail, select the thumbnail frame and then click and drag any of the thumbnail handles.

Viewing a Network Device

To view a network device, select the device in the navigation tree or in the map. You can:

- Use the Zoom tools when viewing the network (see [Cisco ANA NetworkVision Toolbar, page 2-22](#)).
- Click **Overview** in the main toolbar to display the network in the Overview window.

For more information, see:

- [Finding a Network Device or Service, page 4-19](#)
- [Chapter 3, “Viewing Network Element Properties”](#)

Selecting Map Views

Cisco ANA NetworkVision provides you with various selection and display tools that can be used to view and analyze maps in the content area.

You can view graphical representations of NEs and various links that appear in the map view in the Cisco ANA NetworkVision content area by using the toolbar buttons.

The Show List View and Show Links View icons open dynamic tables that present network element information, device information, and respective map context links.

Table 4-5 identifies and describes the tools that you can use to view and manipulate maps in the Cisco ANA NetworkVision content area.

Table 4-5 Cisco ANA NetworkVision Map Viewing Options

Button	Name	Function
Viewing Options		
	Show Map View	Displays the map view in the Cisco ANA NetworkVision content area. The button toggles when selected or deselected.
	Show List View	Displays the list view in the Cisco ANA NetworkVision content area. The button toggles when selected or deselected.
	Show Links View	Displays the links view in the Cisco ANA NetworkVision content area. The button toggles when selected or deselected.
Map Zoom and Layout Tools		
	Layout Map	Defines the way in which the map is displayed in the map pane of the Cisco ANA NetworkVision window: circular, symmetric, tree, or hierarchical.
	Fit in Window	Fits the entire subnetwork or map in the map pane.
	Normal Selection Mode	Activates the normal selection mode. The button toggles when selected or deselected.
	Zoom Selection Mode	Activates the zoom selection mode, which enables you to select an area in the map pane to be enlarged by clicking and dragging to view the selected area. The button toggles when selected or deselected.
	Pan Mode	Activates the pan mode, which enables you to move around in the map pane by clicking and dragging. The button toggles when selected or deselected.

To select a tool, do one of the following:

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

Finding Elements Affected by a Ticket

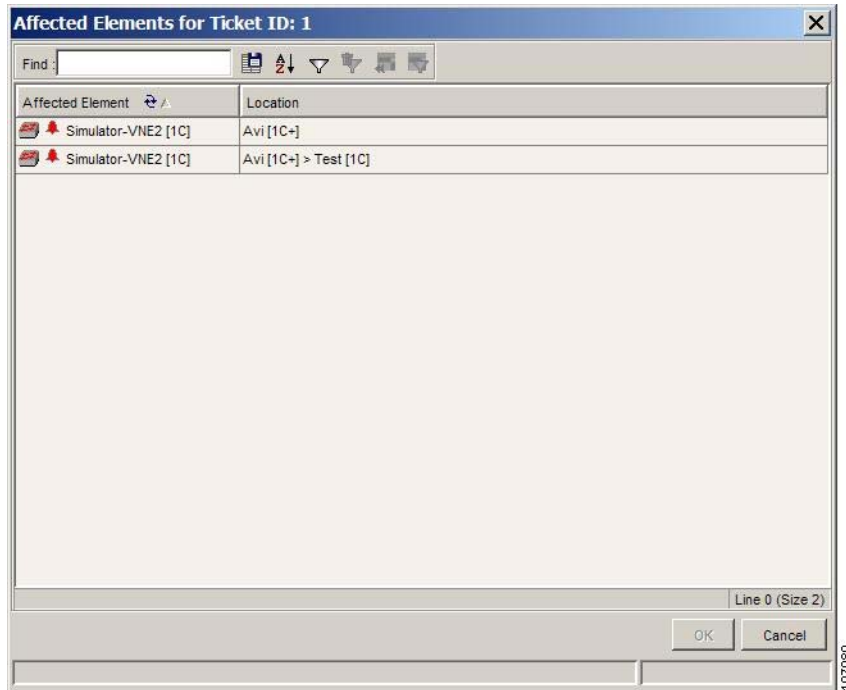
Cisco ANA NetworkVision enables you to find the elements that might be affected by a ticket displayed in the ticket pane.

To find elements affected by a ticket:

-
- Step 1** In the ticket pane, right-click the required ticket and choose **Find Affected Elements**. Depending on the number of affected elements, the information is displayed in one of the following ways:
- If only one element is affected, the affected element is selected in the navigation pane and the content area.

- If two or more elements are affected, the affected elements are displayed in the Affected Elements window as shown in [Figure 4-5](#).

Figure 4-5 Affected Elements Window



Step 2 Do one of the following, as appropriate:

- Click in the navigation pane or the map pane to remove the highlight from the selected device or link.
- Close the Affected Elements table.

Finding and Selecting Links in Maps

Cisco ANA NetworkVision enables you to find a specific link and select it in the map pane.

To find and select a link:

Step 1 In the Links view, right-click the required link and choose **Select Link in Map**.

The link is highlighted in the map pane.

Step 2 If two or more lines represent the same link (such as a VRF link), the Select Link Context dialog box is displayed. Select the required link context from the drop-down list and click **OK**. The link is highlighted in the map pane.

Step 3 Click in the content area to remove the highlight from the selected link.

For more information about links in Cisco ANA NetworkVision, see [Chapter 5, “Working with Links.”](#)

Finding a Network Device or Service

Cisco ANA NetworkVision enables you to find a device or service (such as a VPN or VLAN) in the map by entering the device or service name, the device IP address, or any part of the name or IP address.

To find a device or service in a map:

Step 1 Do one of the following:

- Click **Find** in the main toolbar.
- Choose **Edit > Find in Map** from the main menu.

Step 2 In the Find in Map dialog box, enter the device name or the IP address.



Note You can enter a partial name (case sensitive) or IP address. For example, entering **xx** finds devices or services with names containing the letters XY.

The Search all map levels check box enables you to search for a device, name, or IP address at all levels of the map. When disabled, this option searches for the device or service, but excludes aggregations from the search. This option is disabled by default.

Step 3 Check or uncheck the Search all map levels check box, as required.

Step 4 Click **OK**. A device or service matching the search criteria is displayed on the map.

Step 5 Continue searching using the following methods:

- To view the next device or service that matches the search criteria, click **Find Next** in the toolbar or press **F3**.
 - To view the previous device or service that matches the search criteria, click **Find Previous** in the toolbar or press **Shift + F3**.
-

Working with Overlays

Cisco ANA NetworkVision enables you to apply overlays to a map and thus isolate the parts of a network that are being used by a specific service.

The following topics discuss the overlay options in more detail:

- [Applying an Overlay, page 4-20](#)
- [Hiding or Viewing an Overlay, page 4-22](#)
- [Removing an Overlay, page 4-22](#)

Applying an Overlay

To apply an overlay:

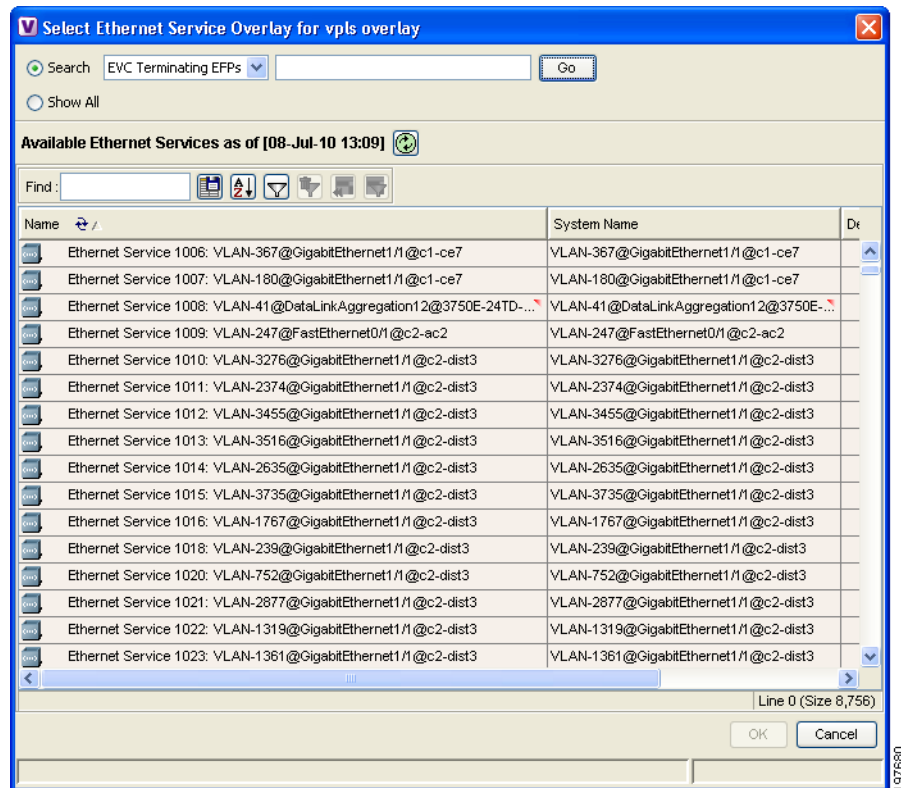
- Step 1** In Cisco ANA NetworkVision, choose the map in which you want to apply an overlay.
- Step 2** From the toolbar, choose **Choose Overlay Type** > *overlay-type* where *overlay-type* is one of the following options:

Overlay Option	Description
Ethernet Service	Applies an Ethernet service overlay to the map.
None	Removes any existing overlays on the map.
Pseudowire	Applies a pseudowire overlay to the map.
VLAN	Applies a VLAN overlay to the map.
VPLS	Applies a VPLS instance overlay to the map.
VPN	Applies a VPN overlay to the map.

With the exception of the None option, a dialog box is displayed that allows you to select the specific overlay to apply.

Figure 4-6 shows an example of the Select Ethernet Service Overlay dialog box.

Figure 4-6 Select Overlay Dialog Box



Each overlay type allows you to search for specific overlays. [Table 4-6](#) identifies the fields you can search for each overlay type.

Table 4-6 **Overlay Type Search Fields**

Overlay Type	Search Fields
Ethernet Service	• EVC Terminating EFPs • Name • System Name
Pseudowire	• Description • Is Multisegment Pseudowire • Name • Pseudowire Type • System Name
VLAN	• Ethernet Flow Domain • ID • Name
VPLS	Name
VPN	• Description • Name

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

- To search for specific overlays:
 - a. In the Search field, choose a search category.
 - b. Enter a search string to narrow the display to a range of overlays or to a specific overlay. [Table 4-6](#) identifies the search categories available for each type of overlay.
 - c. 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** and click **Go**.

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.

**Note**

The overlay is a snapshot taken at a specific point in time and does not reflect changes that occur in the service. As a result, the information in an overlay can become stale. To update the overlay, click **Refresh Overlay** in the toolbar.

Hiding or Viewing an Overlay

When an overlay is applied to a map, the Show Overlay/Hide Overlay button becomes active in the toolbar.

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

Removing an Overlay

To remove an overlay, choose **Choose Overlay Type > None**. The overlays are removed from the map.

Working with Aggregations

Cisco ANA NetworkVision enables you to group network elements and display them as an aggregated node. Aggregations can contain devices, VPNs, other aggregated nodes, and so forth.

For more information, see the following topics:

- [Grouping Network Elements into Aggregations, page 4-22](#)
- [Ungrouping Aggregated Nodes, page 4-23](#)
- [Renaming Aggregated Nodes, page 4-23](#)

Grouping Network Elements into Aggregations

To aggregate network elements:

-
Step 1	Select the network elements using one of the following methods: • Select a single item in the map pane or navigation tree. • Select multiple items in the map pane or navigation tree while pressing Ctrl.
Step 2	Aggregate the network elements using one of the following methods: • Choose Node > Aggregate from the main menu. • Right-click in the navigation pane or map pane and choose Aggregate.
Step 3	In the Aggregation dialog box, enter a unique name for the aggregated node and click OK . The aggregated node is displayed in the navigation pane and the map pane. Aggregated nodes are displayed as a single entity with the Aggregation icon.

The aggregated node icon changes color according to the alarm severity. For more information about device colors, see [Network Element Status Indicators, page 2-17](#).

Ungrouping Aggregated Nodes

All aggregated nodes can be ungrouped. If the node you disaggregate contains any child aggregations, the child aggregations move up one level, and the original aggregated node 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 aggregated node is ungrouped. As a result, no elements are represented twice at the same level.

To disaggregate a node:

Step 1 Select the required aggregation in Cisco ANA NetworkVision.

Step 2 Disaggregate the node using one of the following methods:

- Choose **Node > Disaggregate** from the main menu.
- Right-click the aggregated node in the navigation tree or map pane and choose **Disaggregate**.

If the aggregation contains elements that already exist at the parent level, a confirmation message is displayed, stating that any duplicate elements will be removed.

Step 3 Confirm the disaggregation.

The node is disaggregated. Any aggregations in the selected node move up one level, and the original aggregated node is removed.

For more information about resizing an aggregated node, see [Resizing a Map Element, page 4-14](#).

Renaming Aggregated Nodes

You can rename aggregated nodes that are displayed in Cisco ANA NetworkVision. The name change affects all users of the map, and the new name is displayed in the Cisco ANA NetworkVision window of all users.

To rename an aggregated node:

Step 1 Select the aggregated node that you want to rename in the navigation tree or the map.

Step 2 Right-click the aggregated node and choose **Rename**.

Step 3 In the Rename Node dialog box, enter a new name for the aggregated node and click **OK**. The selected aggregated node is renamed in the navigation tree, map pane, and database.

Filtering Links According to Type

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. You can do either of the following:

- (Method 1) 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.
- (Method 2) 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.

The links filter applies to all aspects of Cisco ANA NetworkVision: the map view, links view, ticket pane, severity calculation, and other items, such as memory consumption and thresholds. Cisco ANA NetworkVision 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 Cisco ANA NetworkVision, see [Chapter 5, “Working with Links.”](#)

Method 1

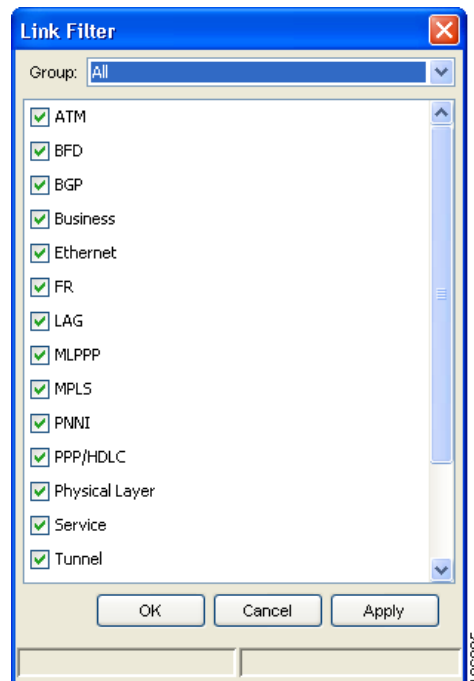
To filter links according to type (method 1):

Step 1 Open the Create Map dialog box using one of the following methods:

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

The Create Map dialog box is displayed. For more information, see [Creating a New Map, page 4-6](#).

Step 2 Click **Advanced**. The Link Filter dialog box is displayed.

Figure 4-7 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 the VPN links are displayed in the map view and links view.



Note You can customize the Group drop-down list options by selecting an option and adding or removing the required link types. The next time the Link Filter dialog box is opened, the Custom option is displayed with the specified link types.

- Step 4** Check the check boxes for the links that you want to display in the map view and links view. Uncheck the check boxes for the links you do not want to display in the map view and links view.
- Step 5** Click **Apply** to apply the defined link filter settings and continue with more selections.
- Step 6** Click **OK** when you have completed your selections.

- Step 7** In the Create Map dialog box, enter a name for the new map and click **OK**. An empty new map is displayed in the navigation pane and content area.
- Step 8** Add the required devices to the map. For more information, see [Creating a New Map, page 4-6](#).
The links are displayed in the map view and links view according to your selections.
-

Method 2

You can also create a map and add the devices with all the 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.

To filter links according to type (method 2):

- 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.
-

Opening the CPU Usage Graph

Cisco ANA NetworkVision enables you to display memory and CPU usage information for a device or network element, including its history.

To open the CPU usage graph:

- Step 1** Right-click a network element in the navigation tree and choose **Tools > CPU Usage**.
The CPU Usage dialog box displays the following information:
- CPU Usage—The CPU usage rate as a percentage.
 - CPU Usage History—The CPU usage rate history is graphically displayed.
 - Memory Usage—The memory usage rate as a percentage.
 - Memory Usage History—The memory usage rate history is graphically displayed.
- Step 2** If desired, click **Save to CSV File** to export the displayed data. For more information, see [Exporting Tables to a File, page 2-45](#).
- Step 3** Click the upper right corner to close the CPU Usage dialog box.
-

Communicating with Devices Using Ping and Telnet

Cisco ANA NetworkVision enables you to communicate with devices in the following ways:

- [Pinging a Device, page 4-27](#)
- [Telneting a Device, page 4-27](#)

Pinging a Device

Cisco ANA NetworkVision enables you to ping a device to verify that the device is responding.

**Note**

The ping is performed from the client to the device, and not from the Cisco ANA 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**.

Telneting a Device

Cisco ANA NetworkVision enables you to communicate with a device using the Telnet window.

**Note**

The telnet is performed from the client to the device, and not from the Cisco ANA unit hosting the VNE to the device.

To telnet a device:

- Step 1** Right-click a device in the navigation tree or map, and choose **Tools > Telnet**.
- Step 2** Log in and use the Telnet window as needed.

Previewing and Printing a Map

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

- [Previewing a Map Before Printing It, page 4-27](#)
- [Defining the Print Setup for a Map, page 4-28](#)

Previewing a Map Before Printing It

Using Cisco ANA NetworkVision, you can preview a map before printing it.

To preview a map:

- Step 1** In Cisco ANA NetworkVision, display the map that you want to print.
- Step 2** From the main menu, choose **File > Print Preview**. The Print Preview dialog box is displayed with the active map.

The following buttons are displayed in the Print Preview dialog box:

Button	Description
Print	Prints the displayed network or map to the selected printer.
Print Setup	Opens the Print Setup dialog box, enabling you to define how the network or map is printed. For more information, see Defining the Print Setup for a Map, page 4-28 .
Zoom In	Zooms in on the network or map.
Zoom Out	Zooms out of the network or map.
Zoom %	Zooms in to get a close-up view of your network or map or zooms out to see more of the network or map at a reduced size. Use the drop-down list to choose the zoom setting that you want.
Fit In Window	Displays the entire network or map in the Print Preview dialog box.
Close	Closes the Print Preview dialog box.

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

Defining the Print Setup for a Map

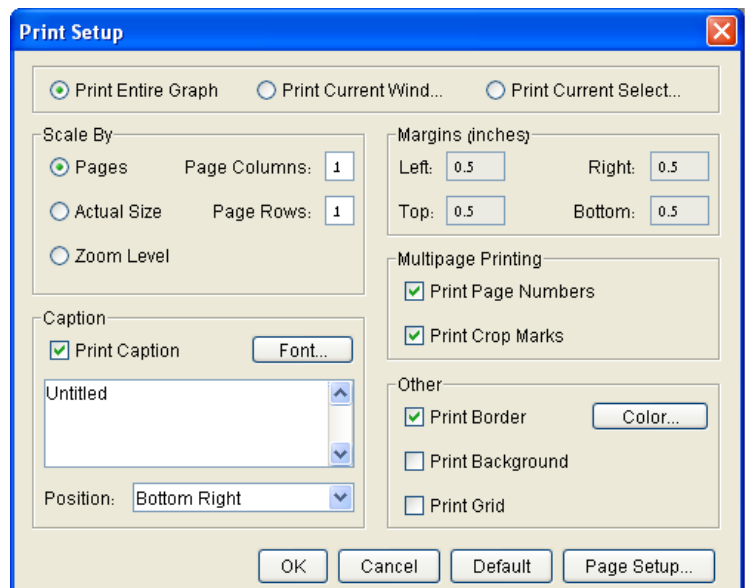
Cisco ANA NetworkVision enables you to define the print setup of a map before it is printed.

To define the print setup:

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

Step 2 Click **Print Setup**. The Print Setup dialog box is displayed.

Figure 4-8 *Print Setup Dialog Box*



Step 3 Define the print setup, using the information in [Table 4-7](#).

Table 4-7 Print Setup Dialog Box Options

Option	Description
Print Selection	
Print Entire Graph	Prints the currently displayed map, including aggregated nodes.
Print Current Window	Prints the currently displayed map, excluding aggregated nodes.
Print Current Selection	Prints the area selected in the currently displayed map.
Page and Scale	
Pages	Prints the currently displayed map according to the numbers specified in the Page Columns and Page Rows fields.
Actual Size	Prints the currently displayed map at the actual size.
Zoom Level	Prints the currently displayed map according to the selected zoom level.
Caption	
Print Caption	Adds the specified caption to the printed map.
Position	Defines the position of the caption in the printed map.
Page Margins	
Margins	Prints the map with the specified page margins.
Multipage Printing	
Print Page Numbers	Prints the map with page numbers.
Print Crop Marks	Prints the map with crop marks.
Border, Background, and Grid	
Print Border	Prints a border around the printed map.
Print Background	Prints the background of the currently displayed map.
Print Grid	Prints a grid for the printed map.
Page Layout	
Page Setup	Offers standard printer options, such as printing in portrait or landscape mode.

Step 4 Click **OK** to save your settings, or **Default** to restore the default settings.

The Print Preview dialog box is refreshed with the current settings.

Step 5 If you are satisfied with your settings, click **Print**. Otherwise, click **Print Setup** and revise your settings.



CHAPTER 5

Working with Links

The following topics describe how to view information about static and dynamic links using the Cisco ANA NetworkVision user interface:

- [User Roles Required to Work with Links, page 5-1](#)
- [Understanding Dynamic and Static Links, page 5-2](#)
- [Working with Flickering Topology Links, page 5-2](#)
- [Viewing Link Properties, page 5-3](#)
- [Viewing Link Impact Analysis, page 5-10](#)
- [Adding Static Links, page 5-12](#)
- [Filtering Links Using the Collection Method, page 5-14](#)
- [Selecting a Link, page 5-14](#)

User Roles Required to Work with Links

[Table 5-1](#) identifies the GUI default permission or device scope security level that is required to work with links in Cisco ANA NetworkVision. Cisco ANA 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 device-based tasks (tasks that do affect devices), authorization is based on the default permission that is assigned to your account. That is, whether the device 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 Active Network Abstraction 3.7.1 Administrator Guide](#).

Table 5-1 Default Permission/Security Level Required for Working with Links

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

Table 5-1 Default Permission/Security Level Required for Working with Links (continued)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View link properties in the Link Properties window	—	—	—	—	X
View link impact analysis	—	—	—	—	X
Add static links	—	—	—	—	X
Filter links	—	X	X	X	X
Find and select a link in a map	—	—	—	—	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.

Understanding Dynamic and Static Links

Cisco ANA NetworkVision provides a topological model of the physical and logical links that exist between elements in the network. Cisco ANA automatically discovers these links, and the ongoing process of autodiscovery maintains this topological information. Cisco ANA NetworkVision discovers any new links that are added and continues to verify that the discovered links still exist; for this reason, they are called *dynamic* links.

Property information is provided for links that are:

- Between two devices.
- Between a device and an aggregated node that connects this device to another device inside the aggregation.
- Between two aggregated nodes that contain devices that cross the aggregations.

If a link is unidirectional, Cisco ANA NetworkVision displays an arrowhead on the link. If it is bidirectional, an arrowhead is not displayed.

Cisco ANA NetworkVision also provides functionality that allows you to create links on the VNE level. These links do not perform any configuration or provisioning on a device or in the network. Because the links do not really exist in the network, the links are not updated. For this reason they are called *static links*. Static links are useful for map visualization and network correlation; for example, if Cisco ANA 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, Cisco ANA treats the static link as if it were a physical or logical link and allows correlation flows to go through the static link. For information on creating static links, see [Adding Static Links](#), page 5-12.

Working with Flickering Topology Links

A link is considered flickering when it is connected, disconnected, and reconnected because the topology information is conflicting. When this situation occurs, Cisco ANA generates a system event with the message “Physical Link discovery inconsistent.”

To remedy the situation, we recommend that you wait until the link disappears from the map and then create a static link.

Viewing Link Properties

Cisco ANA NetworkVision provides information about links in the following ways:

- Through the physical characteristics of the link in a map and tooltips—See [Viewing Link Properties in Cisco ANA NetworkVision Maps](#), page 5-3.
- In the Links view—See [Viewing Link Properties in the Links View](#), page 5-5.
- In the link properties window—See [Viewing Link Properties in the Link Properties Window](#), page 5-7.

Viewing Link Properties in Cisco ANA NetworkVision Maps

The representation of a link in a map provides information about that link. The characteristics that provide information about a link are:

- Whether the link is solid or dashed.
- Whether or not the link displays an arrow at one end.
- Link color.

[Table 5-2](#) describes the link variations that can be displayed in a map and provides examples of each.

Table 5-2 *Link Properties in Cisco ANA NetworkVision Maps*

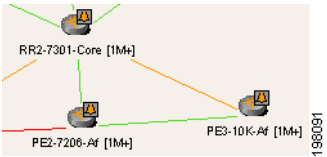
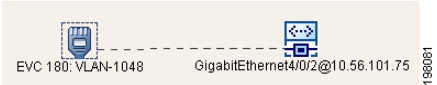
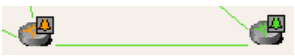
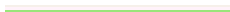
Link Characteristic	Description	Example
Solid Line vs. Dashed Line		
Solid line	Physical or topological link, such as a link between two devices.	
Dashed line	Association between such elements as EVCs, a VPLS service instances (VSIs), or components of a VPN.	
Arrowhead vs. No Arrowhead		
No arrowhead	Bidirectional link.	
Arrowhead	Unidirectional link, with the flow in the direction of the arrowhead.	
Link Color		
Red	Critical alarm is on the link.	

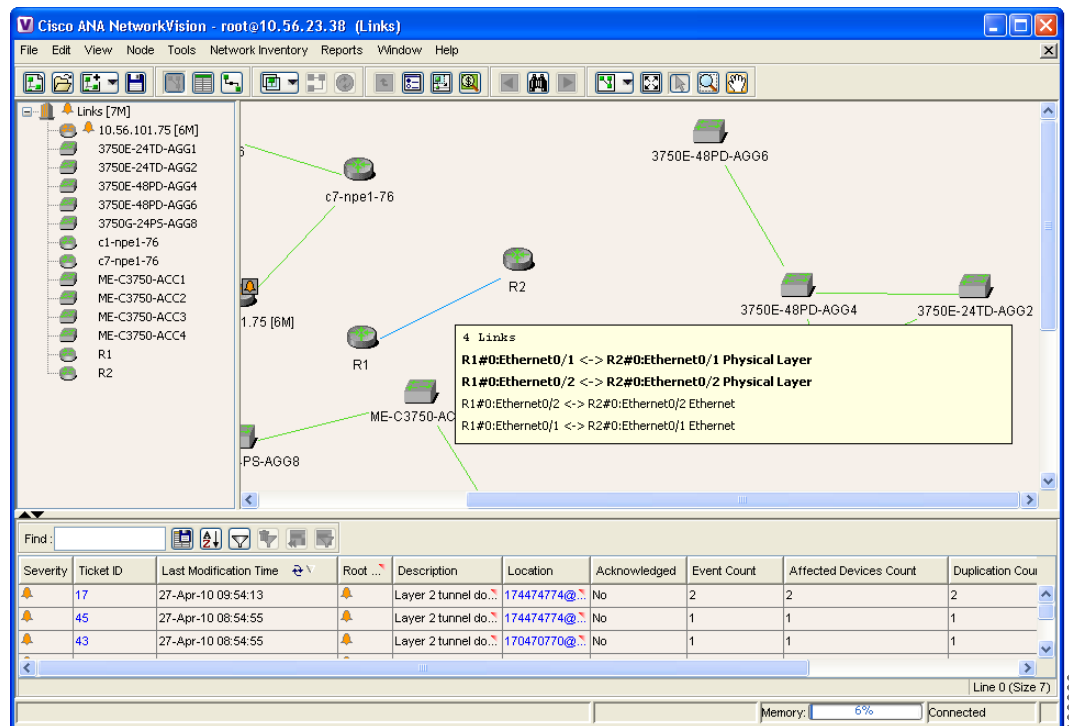
Table 5-2 *Link Properties in Cisco ANA NetworkVision Maps (continued)*

Link Characteristic	Description	Example
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 2-6](#).

If you hover your mouse cursor over a link, you can view additional information about the link in a tooltip as shown in [Figure 5-1](#).

Figure 5-1 *Link Tooltip in Cisco ANA NetworkVision*

The tooltip can contain the following information about the link:

- Link endpoints.
- The protocols being used on the link, such as Ethernet, BFD, or MPLS.
- Whether the link represents a tunnel.
- Whether the link is a physical link.
- The number of links represented by the line on the map.

Links use the format *end1 <-> end2 protocol/layer* where:

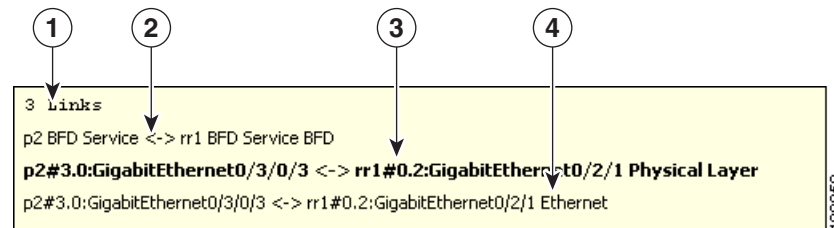
- *end1* is one end of the link and includes the element name and interface or service.
- *end2* is the other end of the link and includes the element name and interface or service.
- *protocol/layer* indicates the protocol used on the link or the layer of communication, such as Ethernet or the physical layer.

For example, a link identified as `p2 BFD Service <-> rr1 BFD service BFD` indicates a BFD service between devices p2 and rr1, using the BFD protocol.

Similarly, a link identified as `p2#3.0:GigabitEthernet0/3/0/3 <-> rr1#0.2:GigabitEthernet0/2/1 Physical Layer` indicates a link at the physical layer between device p2 on slot 3, subslot 0, interface GigabitEthernet0/3/0/3 and device rr1 on slot 0, subslot 3, interface GigabitEthernet0/2/1.

Figure 5-2 shows an example of the information that is displayed in a link tooltip.

Figure 5-2 Link Tooltip Example

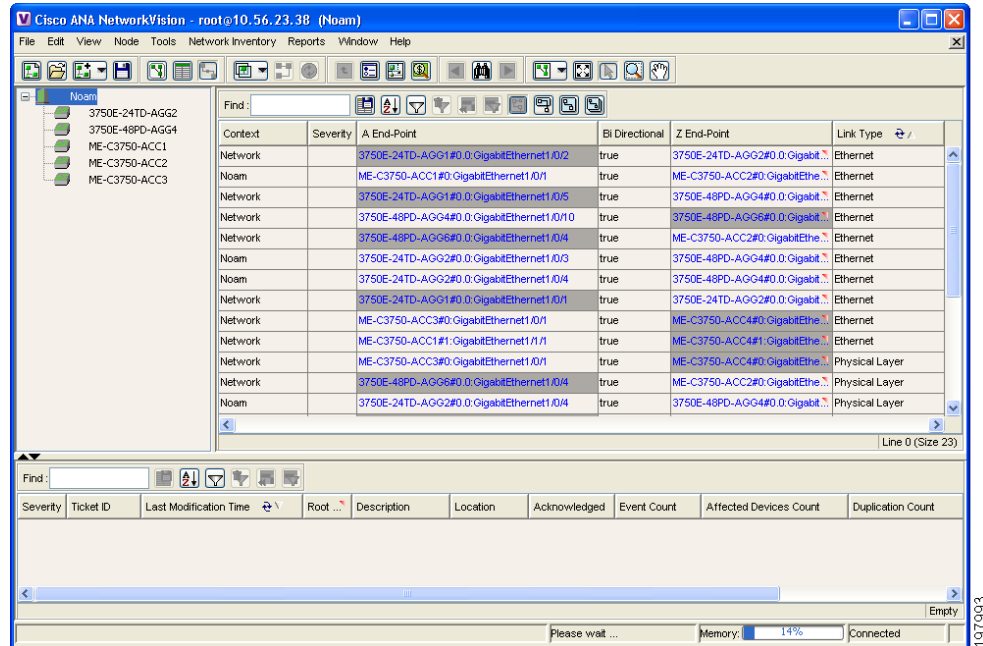


1	Number of links represented by the single link in the map. In this example, three links.
2	Any service being used by the link. In this example, BFD service.
3	Boldface type indicates a physical link between devices. In this example, the link is between device p2 on slot 3, subslot 0, interface GigabitEthernet0/3/0/3 and device rr1 on slot 0, subslot 3, interface GigabitEthernet0/2/1.
4	Protocol used on the interface. In this example, Ethernet.

Viewing Link Properties in the Links View

The links shown in a map are a summary of the many links starting from one side and ending at the other side of the link. However, with the links view, you can view a list of all physical links included in a map and their status.

To display the links view in the Cisco ANA NetworkVision window, click **Show Links View** in the main toolbar. Figure 5-3 shows an example of a links view.

Figure 5-3 Links View**Note**

A link external to the network has a gray 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.

The following columns are displayed in the links view:

- **Context**—The name of the map or aggregated node containing the link; there can be multiple contexts.
- **Severity**—Displays a severity bell icon, which is colored according to the severity of the alarm on the link. This indicates the impact of the alarm on the network. For more information about severity, see [Network Element Status Indicators, page 2-17](#).
- **A End-Point**—The device or site that is the source of the link, as a hyperlink to the inventory of the device or site.
- **Bi Directional**—Whether the link is bidirectional or unidirectional: True (bidirectional) or False (unidirectional).
- **Z End-Point**—The device or site that is the destination of the link, hyperlinked to the relevant entry in inventory.
- **Link Type**—The type of link, such as Physical Layer, VPN, MLPPP, or MPLS.

By default, the links displayed in the links view are sorted according to link type and the deep collection method.

The buttons in [Table 5-3](#) 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 toolbar are unavailable until the table has completely loaded.

Table 5-3 **Links View Tools**

Icon	Name	Description
	All Links	The complete list of links for the selected map or aggregated node.
	External Links	The links with one side of the link in the selected map or aggregated node and the other side of the link outside the currently selected map or aggregated node.
	Flat Links (Surface)	The links currently visible in the map pane for the selected map or aggregated node, excluding any thumbnails.
	Deep Links	The links for the selected aggregated node and any child aggregated nodes, with both endpoints within the currently selected map or aggregated node.

For more information about filtering links using the collection method, see [Filtering Links Using the Collection Method](#), page 5-14.

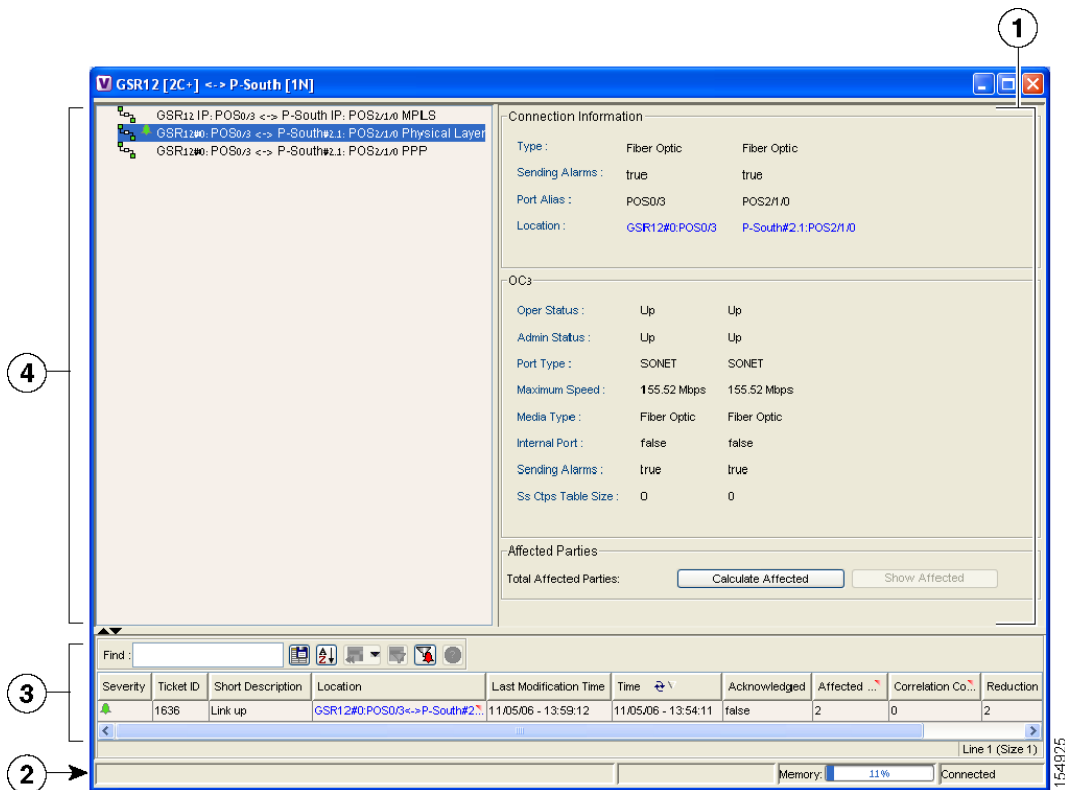
Viewing Link Properties in the Link Properties Window

The link properties window contains general information about the selected link, details of the link connection, and technology-specific information appropriate for the link.

To open the link properties window:

- Step 1** In a Cisco ANA NetworkVision map, double-click a link between two elements.
The link properties window is displayed as shown in [Figure 5-4](#).

Figure 5-4 Link Properties Window



1	Properties pane	3	Ticket pane
2	Status bar	4	Link List pane



Note If there are a few links between the elements or aggregated nodes, the link properties window displays information for all the links.

See the following topics for more information about each of the panes in the link properties window:

- [Link List Pane, page 5-8](#)
- [Properties Pane, page 5-9](#)
- [Ticket Pane, page 2-15](#)

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 a branch 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 [Network Element Status Indicators, page 2-17](#).

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
- Hyperlink to port inventory access
- Status

The properties pane displays the connection information type, port alias, and port location (a hyperlink), all of which uniquely identify the port. The port location information is also displayed as a hyperlink to the inventory window.

The properties pane displays the parameters for the different sides of the link, aligned under the relevant link identifier. Any discrepancies between the link's ports are colored red.

The properties pane enables you to view the statistics of the traffic on the link. The following fields are displayed in the Connection Information area:

- Type—The type of connector, such as fiber optic.
- Sending Alarms—Whether the port is configured to send alarms: True or False.
- Status—The status of the link, such as OK.
- Port Alias—The name used in the device CLI or EMS for the selected port.
- Managed—Whether the link is managed: True or False.
- Location—The 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
- MPBGP
- MPLS Link Information
- Pseudowire
- VRF

IP addresses are displayed in IPv4 or IPv6 format as appropriate.

The following buttons are displayed in the Affected Parties area for physical links:

- Calculate Affected—Calculates and retrieves the total number of potentially affected entities.
- Show Affected—Displays the properties of the affected parties. This button is enabled after you click **Calculate Affected**.

Viewing Link Impact Analysis

Cisco ANA NetworkVision enables you to select a network link and calculate the parties 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.



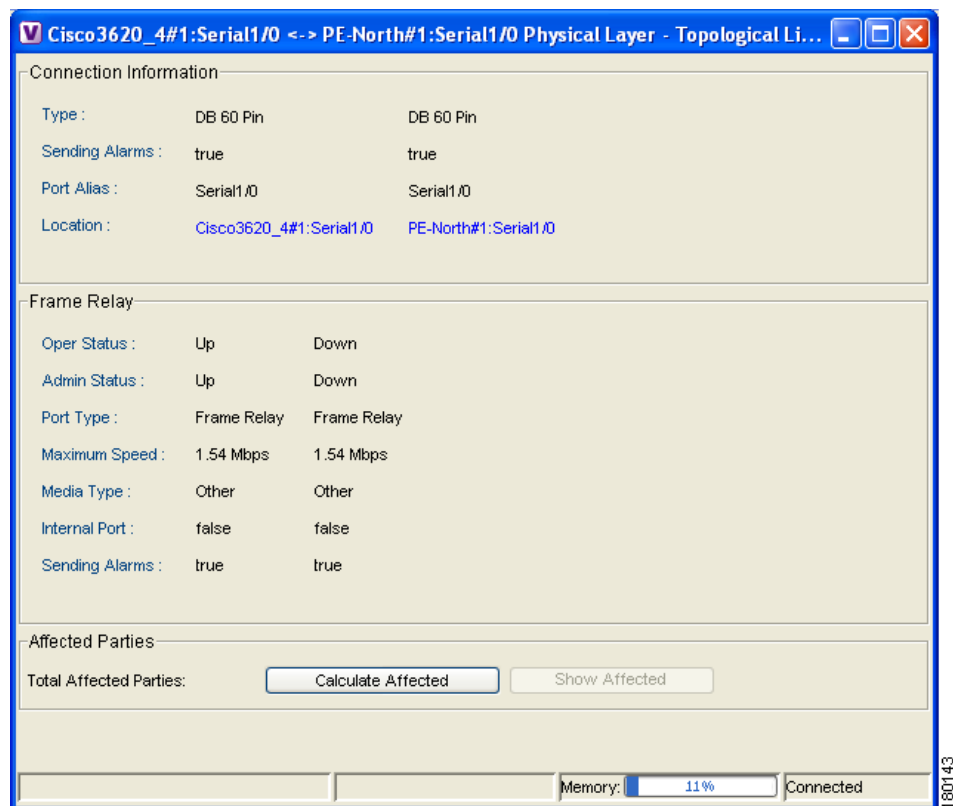
Note

This topic applies only to physical links.

To calculate impact analysis:

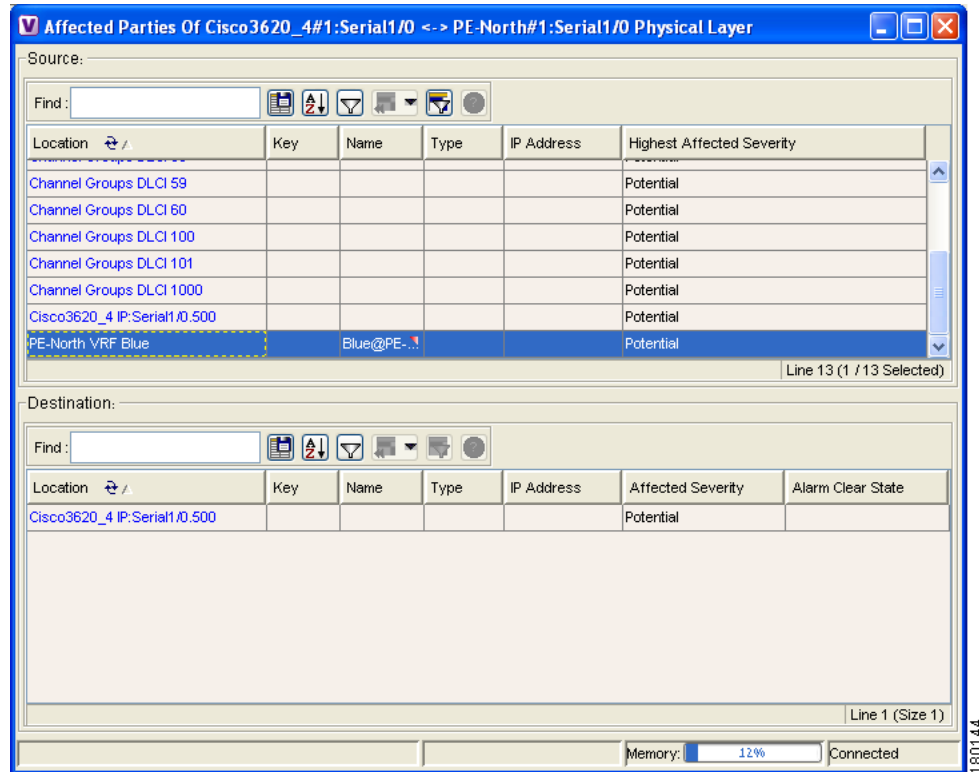
- Step 1** Select a map or aggregated node in the navigation pane, and click **Show Links View** in the main toolbar. The links view is displayed in the content pane.
- Step 2** In the Cisco ANA NetworkVision main toolbar, click **Link Filter**. The Link Filter dialog box is displayed. For information about the Link Filter dialog box, see [Filtering Links According to Type](#), page 4-24.
- Step 3** From the Group drop-down list, choose **Physical** and then click **OK**. Only physical links are displayed in the links view.
- Step 4** In the links view, right-click the selected link and choose **Properties**. The Topological Link Properties window is displayed.

Figure 5-5 Topological Link Properties Window



- Step 5** Click **Calculate Affected**. The total number of potentially affected parties is displayed in the Affected Parties area.
- Step 6** Click **Show Affected**. The Affected Parties dialog box is displayed as shown in [Figure 5-6](#).

Figure 5-6 Affected Parties Dialog Box



- Step 7** To view the potentially affected destinations if a link were to go 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 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.

Adding Static Links

Cisco ANA NetworkVision enables you to create static links that exist only on the VNE level. Static links are useful for visualization and network correlation because Cisco ANA 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. Cisco ANA 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).

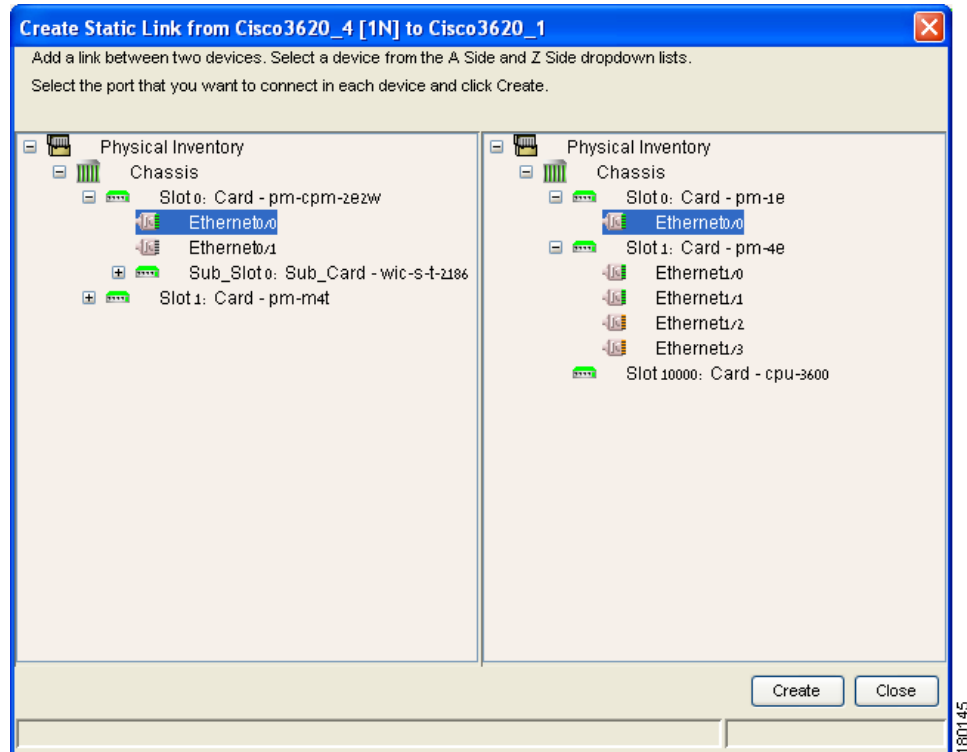
Beginning with Cisco ANA 3.7.1, you can also create static links between Ethernet Link Aggregation Groups (LAGs) by choosing a LAG and the desired port channel for the A or Z side as described in the following procedure.

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 Cisco ANA NetworkVision window's navigation and a map (method 1), or from the inventory window navigation pane (method 2).

In addition, you can add a new link using Cisco ANA Manage. For more information, see the [Cisco Active Network Abstraction 3.7.1 Administrator Guide](#).

Adding a Link (Method 1)

-
Step 1	Right-click the required A Side device in the navigation pane or in a map, and choose Topology > Mark as A Side .
Step 2	Right-click the required Z Side device or LAG in the navigation pane or properties pane to display the right-click shortcut menu and choose Topology > Mark as Z Side . The Create Static Link dialog box is displayed, so that you can select the ports to connect.

Figure 5-7 Create Static Link Dialog Box

Step 3 Select the required port on both the A Side device and the Z Side device.

Step 4 Click **Create** to validate the connection and create the new link. A success message is displayed. A warning message is displayed if any of the following apply:

- A validation check fails.
- The operation status of one port is Up and the other port is Down.
- The selected ports are not of the same type.
- The Layer 2 technology type is not the same.
- One of the ports is part of another link.

Adding a Link (Method 2)

Step 1 Open the inventory window for the required A Side device.

Step 2 In the navigation pane, navigate to the required port for the A Side device.

Step 3 Right-click the required A Side port and choose **Topology > Mark as A Side**.

Step 4 Repeat [Step 1](#) and [Step 2](#) for the Z Side device.

Step 5 Right-click the required Z Side port 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 apply:

- 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 Active Network Abstraction 3.7.1 Administrator Guide](#).

Filtering Links Using the Collection Method

The links view table enables you to view links that are not displayed graphically in the Cisco ANA NetworkVision 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 Cisco ANA NetworkVision.
-

To filter links according to the collection method:

-
- Step 1** Click **Show Links View** in the Cisco ANA NetworkVision main toolbar.
- Step 2** Select a map or aggregated node 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

Cisco ANA NetworkVision 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), the Select Link Context dialog box is displayed. Select the required link 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 in the map background.
-



CHAPTER 6

Working with Business Tags and Business Elements

A business tag is a string that is meaningful to the business, and which can be used to label a component of a network element for use in ANA screens and reports.

A business element is a construction or organization of certain network elements and their properties into a logical entity, to provide the ability to track them in a way that makes sense from a business perspective. Examples of business elements include Layer 2 VPNs, Layer 3 VPNs, and virtual routers.

The following topics describe how to manage and view Cisco ANA business tags and business elements:

- [User Roles Required to Work with Business Tags and Business Elements, page 6-1](#)
- [Using Chinese Characters, page 6-2](#)
- [Creating a Business Tag, page 6-3](#)
- [Searching for Business Tags and Viewing Their Properties, page 6-4](#)
- [Renaming a Business Element, page 6-5](#)
- [Deleting a Business Element, page 6-5](#)

User Roles Required to Work with Business Tags and Business Elements

[Table 6-1](#) identifies the roles that are required to work with business tags and business elements. Cisco ANA 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 device-based tasks (tasks that do affect devices), authorization is based on the default permission that is assigned to your account. That is, whether the device 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 Active Network Abstraction 3.7.1 Administrator Guide](#).

Table 6-1 *Default Permission/Security Level Required for Working with Business Tags and Business Elements*

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Create a business tag	—	—	—	Partial ¹	X
Delete 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 devices only if the devices are in the user's scope.

Using Chinese Characters

Beginning with Cisco ANA 3.7, business tags support Chinese characters, enabling you to perform the following activities using Chinese characters:

- [Creating a Business Tag, page 6-3.](#)
- [Searching for Business Tags and Viewing Their Properties, page 6-4.](#)
- Generating a list of business tags.
- Editing the details of a business tag.
- Writing business tag notes.
- Removing business tags.
- Creating aggregations.
- Exporting 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 Active Network Abstraction 3.7.1 Installation Guide](#)
- Integration over northbound interfaces—[Cisco Active Network Abstraction 3.7.1 Integration Developer Guide](#)

Creating a Business Tag

Cisco ANA NetworkVision enables you to create a business tag, for example, a new subscriber to a port. In addition, you can detach existing subscribers from ports.

Attaching a Business Tag

To attach a business tag:

Step 1 In the Cisco ANA NetworkVision window or in any of the dialog boxes, right-click a network object and choose **Attach Business Tag**.

Step 2 In the Attach Business Tag dialog box, provide the required information:

- Unique Key—Enter a unique identifier for the business tag.
- Name—Enter a name for the business tag.



Note Business tag names are case-sensitive.

- Type—Choose the type of business tag: Subscriber, Provider Connection, or Label.



Note If you select Label, the name of the network object changes to display the business tag name if the Replace name with Business Tag option is selected in the Options dialog box (**Tools > Options**). For more information about display options, see [Selecting Cisco ANA NetworkVision Map and Alarm Options, 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 ANA NetworkVision, such as in the navigation pane, maps, and Cisco ANA PathTracer.



Note The Edit and Detach options are displayed in the right-click shortcut menu when a business tag is attached to a network element.

You can search and edit business tag information attached to a network object using tools available from the appropriate Business Tag dialog box.

Detaching a Business Tag

A business tag that has been attached to a network object can also be detached. You can detach one more more business tags at a time.

To detach a business tag:

- Step 1

In the Cisco ANA NetworkVision window, navigate to the network object that contains the business tag you want to delete. You can also search for the business tag as described in [Searching for Business Tags and Viewing Their Properties, page 6-4](#).
- Step 2

Right-click the network object and choose **Detach Business Tag**.
The business tag is detached from the network object and is no longer displayed.

Searching for Business Tags and Viewing Their Properties

Cisco ANA NetworkVision enables you to find a business tag by entering the full or partial business tag name and the business tag key. If you use the full or partial business tag name for the search, the search results provide a list of business tags meeting the search criteria. If you use the business tag key, the search results provide information about the particular business tag.



Note

If you know the location of the business tag, you can view its properties by opening the Business Tag tab in the device inventory window.

To search for a business tag:

- Step 1

Open the Find Business Tag dialog box in one of the following ways:
 - Click **Find** in the main toolbar.
 - Choose **Edit > Find Business Tag** from the main menu.

[Table 6-2](#) describes the tools available in the Find Business Tag dialog box.

Table 6-2 Find Business Tag Dialog Box Tools

Icon	Name	Function
	Find	Finds the business tag according to a name, key, or type entered in the Find Business Tag dialog box.
	Clear	Clears the search information entered in fields in the Find Business Tag dialog box.
	Help	Displays online help for Cisco ANA NetworkVision and Cisco ANA EventVision.

- Step 2** Specify your search criteria:
- **Unique Key**—Enter the key you are searching for.
 - **Name**—Enter a full or partial entry of the name you are searching for. The search function is case-insensitive, so entering the string **biz tag** in the Name field results in business tags with names containing Biz Tag, Biz tag, and biz tag.
 - **Type**—From the drop-down list, select the type of business tag you are searching for.
- Step 3** Click **Find**. The search results are displayed in a table at the bottom of the Find Business Tag dialog box. The table displays the business tag unique key, name, type, and a hyperlink to the network element the business tag is attached to.
- Step 4** View additional details as required:
- To view the business tag's properties, double-click the business tag in the search results table.
 - To go to the business tag's location, click the hyperlink provided in the search results table.
-

Renaming a Business Element

The following caveats apply when renaming a business element:

- Except for network VLANs, the original name of the business element is not saved, so you cannot revert to the original name.
- Renaming a business element affects all users who have the business element loaded in their service view maps.

To rename business elements in service view maps:

-
- Step 1** In the Cisco ANA NetworkVision navigation pane or a map, right-click the business element and choose **Rename**.
- Step 2** In the Rename Node dialog box, enter a new name.
- Step 3** Click **OK**.

The changed business element name appears in the Cisco ANA NetworkVision navigation pane and map.

Deleting a Business Element

You can delete business elements from the database. However, if you delete a business element from the database, it can no longer be viewed in Cisco ANA NetworkVision. We recommend that you delete a business element only when the physical element no longer exists.



Caution

Deleting business elements affects all users who have the business elements loaded in their service view map.

Table 6-3 lists the requirements that must be met before you can delete a business element.

Table 6-3 Business Element Deletion Requirements

Business Element	Requirements
Layer 3 VPN	The VPN has no virtual routers, or, if it does, the virtual routers and sites 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.
Site	No sites or interfaces are connected or bound to the VRF, or, if they are connected, they display the reconciliation icon.
Layer 2 VPN	The Layer 2 VPN has no Logical Circuit Peers (LCPs), or, if it does, the LCPs display the reconciliation icon.
LCA	The Logical Circuit Aggregation (LCA) has no LCPs, or, if it does, the LCPs display the reconciliation icon.

To delete a business element:

-
- Step 1** Verify that the business element meets all requirements specified in Table 6-3. You cannot delete the element if all requirements are not met.
 - Step 2** In the Cisco ANA NetworkVision navigation pane or a map, right-click the business element, and choose **Delete**.
 - Step 3** In the confirmation message, click **Yes** to delete the currently selected element, or click **Yes to All** to delete multiple selected elements.

The selected business element is deleted from the business configuration of all users.



CHAPTER 7

Working with the Cisco ANA EventVision Client

These topics describe the Cisco ANA EventVision application and the options you can use to view system events and tickets that are generated within the Cisco ANA system:

- [User Roles Required to Work with Cisco ANA EventVision, page 7-1](#)
- [Starting Cisco ANA EventVision, page 7-2](#)
- [Cisco ANA EventVision Window, page 7-3](#)
- [Selecting Cisco ANA EventVision Viewing Options, page 7-8](#)

User Roles Required to Work with Cisco ANA EventVision

[Table 7-1](#) identifies the roles that are required to work with Cisco ANA EventVision. Cisco ANA 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 device-based tasks (tasks that do affect devices), authorization is based on the default permission that is assigned to your account. That is, whether the device 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 Active Network Abstraction 3.7.1 Administrator Guide](#).

Table 7-1 **Default Permission/Security Level Required for Cisco ANA EventVision**

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Opening Cisco ANA EventVision	—	—	—	—	X
Selecting Cisco ANA event viewing options	—	—	—	—	X

Starting Cisco ANA EventVision

This section provides instructions for starting Cisco ANA EventVision. Cisco ANA EventVision is password protected to ensure security. Before you start working with Cisco ANA EventVision, make sure you know your username and password, and the Cisco ANA gateway IP address or hostname that you require.

**Note**

Only users with the administrator role can log into Cisco ANA EventVision.

**Note**

If you do not log into the Cisco ANA Manage, Cisco ANA NetworkVision, or Cisco ANA EventVision application during a specified period of time (the default is 30 days), your account is automatically locked. The default period can be changed in Cisco ANA Manage. The period of time is measured from the time you last logged out of any of the Cisco ANA client applications. For more information about changing the default period and unlocking an account, see the [Cisco Active Network Abstraction 3.7.1 Administrator Guide](#).

To start Cisco ANA EventVision:

Step 1 Choose **Start > Programs > Cisco ANA > Cisco ANA EventVision**.

The login dialog box appears.

Step 2 Enter your username and password.

Step 3 Do one of the following:

- Enter the required Cisco ANA gateway information in the Host field, as an IP address or hostname.
- Select a Cisco ANA gateway from the Host list.

**Note**

- The Cisco ANA gateway IP address or hostname that was used when you last logged in is automatically displayed at the top of the Host list.
- Make sure that you use the leading IP address (the IP address on which the Cisco ANA gateway was configured) when logging into the system.

Step 4 Click **OK**.

When you launch Cisco ANA EventVision, messages are displayed if the server and client have different versions of the application that launches the client. For more information about these messages, see the [Cisco Active Network Abstraction 3.7.1 Installation Guide](#).

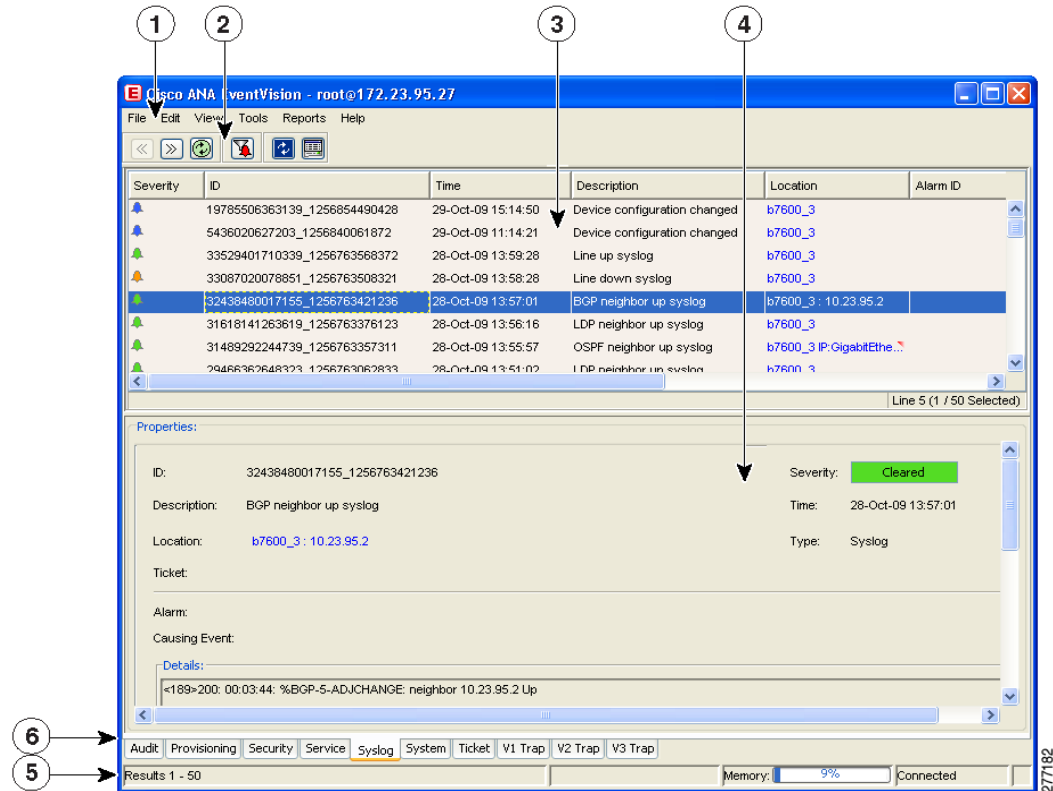
The first time you log in, the Ticket tab is displayed in the Cisco ANA EventVision window.

When you log in again, the tab and filter that were visible when you last logged out of the application are displayed.

Cisco ANA EventVision Window

The Cisco ANA EventVision window displays the events generated in the system. [Figure 7-1](#) shows an example of the Cisco ANA EventVision window.

Figure 7-1 Cisco ANA EventVision Window



1	Menu bar	4	Properties pane
2	Toolbar	5	Status bar
3	Table pane	6	Cisco ANA EventVision tabs

Cisco ANA EventVision displays events for the last two days by default. To modify the default number of days for which events are displayed, see [Selecting Cisco ANA EventVision Viewing Options](#), [page 7-8](#). As you increase the number of days, it might take longer for the events to be displayed.

You can display the events list only (without the Event Properties pane), and select the required tab to display events, such as Provisioning events only.

You can also the Cisco ANA EventVision window toolbar and menu options to:

- Filter results so that events meeting your criteria are displayed. See [Filtering Events and Tickets](#), [page 8-21](#).
- View selected event properties in a separate window. See [Viewing Event Properties](#), [page 8-14](#).

Event Status Indicators

The events list is color coded according to the severity of the event. An icon appears for each ticket or event in the Cisco ANA EventVision tabs (based on its severity) as shown in [Table 7-2](#).

Table 7-2 *Event Status Indicators*

Icon	Color	Severity
	Red	Critical
	Orange	Major
	Yellow	Minor
	Sky Blue	Warning
	Green	Cleared, Normal, or OK
	Dark Blue	Information
	White	Indeterminate

Event Types and Categories

Every event that occurs in the Cisco ANA system and the Cisco ANA gateway is logged. This includes events that are performed as part of the normal operation of the Cisco ANA system, as well as events that may need further attention. Events are categorized, and any of the log entries can be viewed in the Cisco ANA EventVision tabs as described in [Table 7-3](#).

Table 7-3 *Event Categories in Cisco ANA EventVision*

Tab	Description
Audit	Related to commands running in the Cisco ANA gateway.
Provisioning	Related to configuration and provisioning activities.
Security	Related to client login and user activity when managing the system and the environment.
Service	Related to the alarms that are generated by the Cisco ANA system.
Syslog	Related to the predefined set of syslogs received from the devices by the VNEs, which are used to generate the syslog events.
System	Related to the everyday working of the internal system and its components. These events may be related to Cisco ANA and Cisco ANA gateway resources, representing the system log.
Ticket	Related to all the tickets that were opened in Cisco ANA.

Table 7-3 *Event Categories in Cisco ANA EventVision (continued)*

Tab	Description
V1 Trap	Related to SNMPv1 traps that are generated by a network element and received by Cisco ANA; Cisco ANA uses these traps to generate the trap events.
V2 Trap	Related to SNMPv2 traps that are generated by a network element and received by Cisco ANA; Cisco ANA uses these traps to generate the trap events.
V3 Trap	Related to SNMPv3 traps that are generated by a network element and received by Cisco ANA; Cisco ANA uses these traps to generate the trap events.
All	Displayed when you choose File > Open All Tab . Provides a flat list of all events and tickets, sorted by time. To disable the All option, follow the instructions provided in the Cisco Active Network Abstraction 3.7.1 Installation Guide .
3.6.x Type	Five tabs where <i>Type</i> represents one of the following: • Ticket • Service • Syslog • V1 Trap • V2-V3 Trap These tabs are: • Available only if Cisco ANA was upgraded from version 3.6.7 to Cisco ANA 3.7 or 3.7.1. • Displayed when you choose File > Open 3.6.x Tabs.

Cisco ANA EventVision Toolbar

[Table 7-4](#) describes the tools that are displayed in the Cisco ANA EventVision toolbar.

Table 7-4 *Cisco ANA EventVision Tools*

Button	Function
	Displays the previous page of events in the Cisco ANA EventVision window.
	Displays the next page of events in the Cisco ANA EventVision 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 ANA EventVision Information, page 8-20 .

Table 7-4 Cisco ANA EventVision Tools (continued)

Button	Function
	Displays the Cisco ANA EventVision Filter dialog box, which enables you to define a filter for the events displayed in the Cisco ANA EventVision log. For more information, see Filtering Events and Tickets, page 8-21 .
	Toggles automatic refresh of event data on and off. You define the refresh-time period (in seconds) in the Cisco ANA EventVision Options dialog box. The default is 60 seconds. If a filter is active, the refresh is done according to the filter. For more information, see Selecting Cisco ANA EventVision Viewing Options, page 7-8 .
	Displays the properties of the selected event or ticket in the Properties pane.

Cisco ANA EventVision Menu Bar

[Table 7-5](#) describes the options available in the Cisco ANA EventVision main menus. In addition to these options, Cisco ANA EventVision displays a shortcut Properties option when you right-click an event or ticket (see [Viewing Event Properties, page 8-14](#)).

Table 7-5 Cisco ANA EventVision Menu Options

Menu Option	Description
File Menu	
Export	Exports the log event information displayed in the Cisco ANA EventVision window according to the criteria defined in the Cisco ANA EventVision Options dialog box.
Open 3.6.x Tabs	Displays the following tabs: 3.6.x Ticket 3.6.x Service 3.6.x Syslog 3.6.x V1 Trap 3.6.x V2-V3 Trap This option is available only if Cisco ANA was upgraded from version 3.6.7 to Cisco ANA 3.7 or 3.7.1.
Open All Tab	Displays the All tab so you can view a flat list of all events and tickets sorted only by time. To disable the All option, follow the instructions provided in the Cisco Active Network Abstraction 3.7.1 Installation Guide .
Exit	Exits Cisco ANA EventVision.
Edit Menu	
Filter	Defines a filter for the events displayed in the Cisco ANA EventVision window according to the tab selected. See Filtering Events and Tickets, page 8-21 .
Purge	This option is unavailable in this version.

Table 7-5 Cisco ANA EventVision Menu Options (continued)

Menu Option	Description
View Menu	
Refresh	Refreshes the information displayed in the Cisco ANA EventVision window.
Go To	Navigates through the pages of the Cisco ANA EventVision window.
Properties	Displays the properties of the selected event, such as the root cause and source. For more information, see Viewing Event Properties, page 8-14 .
Details Pane	Displays or hides the Properties pane. If an event is selected, the properties of the selected event are displayed in the Properties pane.
Tools Menu	
Change User Password	Allows you to change the password used when logging into the Cisco ANA client application suite. The change takes effect the next time you log into the application.
Options	Defines the display options for the Cisco ANA EventVision window. For more information, see Selecting Cisco ANA EventVision Viewing Options, page 7-8
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 and inventory reports on demand.
Help Menu	
Cisco ANA EventVision Help	Opens the online help for Cisco ANA EventVision and Cisco ANA NetworkVision.
Cisco.com	This option is unavailable.
About Cisco ANA EventVision	Displays application information, such as the version number.

Right-Click Options

Cisco ANA EventVision offers the following right-click options in its 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 Cisco ANA EventVision. For more information, see the [Cisco Active Network Abstraction 3.7.1 Customization User Guide](#).
- Properties—Displays the properties window for the selected event or ticket.

Selecting Cisco ANA EventVision Viewing Options

The Cisco ANA EventVision Options dialog box enables you to define the options for displaying events in the Cisco ANA EventVision window.

To define Cisco ANA EventVision options:

-
- Step 1** From the main menu, choose **Tools > Options**.
- Step 2** In the Cisco ANA EventVision Options dialog box, select the required settings as described in [Table 7-6](#).

Table 7-6 *Cisco ANA EventVision Options Dialog Box*

Option	Description
Save last filter	Saves the filter criteria defined per event type in the Filter Events dialog box. The filter criteria are available the next time you log into Cisco ANA EventVision. Note Events are not filtered automatically when you next log into Cisco ANA EventVision unless the Open using filter option is selected as well.
Open EventVision with saved filter	When enabled, applies the previously defined filter to the events as soon as you log into Cisco ANA EventVision. The events are continuously filtered according to the defined settings, even after you close the application.
Show <i>n</i> events per page	Specifies the number of events to be displayed per page.
Export <i>n</i> events in total	Sets the maximum number of events to be exported to a file.
Run auto refresh every <i>n</i> secs	Automatically refreshes the Cisco ANA EventVision display after the specified number of seconds. Note If you modify this option, you are prompted to confirm your choice. Confirmation is required because this option uses rapid refresh from the database, which can slow down other vital database options.
Display events for the last <i>n</i> days	Displays past events from the specified number of days. Values range from 1 to 14 days, with a default of 2 days. If you increase the number of days, it might take longer for the events to be displayed.

-
- Step 3** Click **OK**.
-



CHAPTER 8

Tracking Faults Using Cisco ANA EventVision

The following topics describe how to use Cisco ANA EventVision to track faults:

- [User Roles Required to Work with Cisco ANA EventVision, page 8-1](#)
- [Viewing Events and Tickets in Cisco ANA EventVision, page 8-2](#)
- [Viewing 3.6.x Tabs, page 8-11](#)
- [Working in Cisco ANA EventVision, page 8-14](#)



Note

For detailed information about alarms and event management, see the [Cisco Active Network Abstraction 3.7.1 Theory of Operations Guide](#).

User Roles Required to Work with Cisco ANA EventVision

[Table 8-1](#) identifies the roles that are required to work with Cisco ANA EventVision. Cisco ANA 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 device-based tasks (tasks that do affect devices), authorization is based on the default permission that is assigned to your account. That is, whether the device 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 Active Network Abstraction 3.7.1 Administrator Guide](#).

Table 8-1 Default Permission/Security Level Required for Cisco ANA EventVision

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Viewing events and tickets	—	—	—	—	X
Viewing events and ticket properties	—	—	—	—	X
Refreshing information displayed in tables	—	—	—	—	X

Table 8-1 Default Permission/Security Level Required for Cisco ANA EventVision (continued)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Filtering events and tickets	—	—	—	—	X
Exporting displayed data	—	—	—	—	X

Viewing Events and Tickets in Cisco ANA EventVision

Events are displayed according to event categories, which are represented by tabs in the Cisco ANA EventVision 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.

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. You can define a filter to be used as well as the number of items to be displayed in the list, by using the Cisco ANA EventVision Options dialog box. Each tab displays the specified number of entries per page as defined in the Cisco ANA EventVision Options dialog box.

For more information, see [Selecting Cisco ANA EventVision Viewing Options, page 7-8](#).

Because the lists of events and tickets can be lengthy, you can use the left and right arrows on the navigation toolbar 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 ANA EventVision, 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 Cisco ANA database for all category events.

You can disable the All tab by following the instructions provided in the [Cisco Active Network Abstraction 3.7.1 Installation Guide](#).

[Table 8-2](#) describes the information that is displayed in the All tab.

Table 8-2 All Tab

Column	Description
Severity	Icon of a bell, colored according to the severity of the alarm on the event (the color and type of alarm are displayed in the Properties window Severity field). See Event Status Indicators, page 7-4 .
Event ID	Event identifier, assigned sequentially.

Table 8-2 All Tab (continued)

Column	Description
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 ANA EventVision window display the system events:

- [Audit Tab, page 8-3](#)
- [Provisioning Tab, page 8-4](#)
- [Security Tab, page 8-5](#)
- [System Tab, page 8-5](#)

Audit Tab

The Audit tab displays all events generated for each command or request in Cisco ANA; for example, opening Cisco ANA EventVision displays the **Get** command as shown in [Figure 8-1](#).

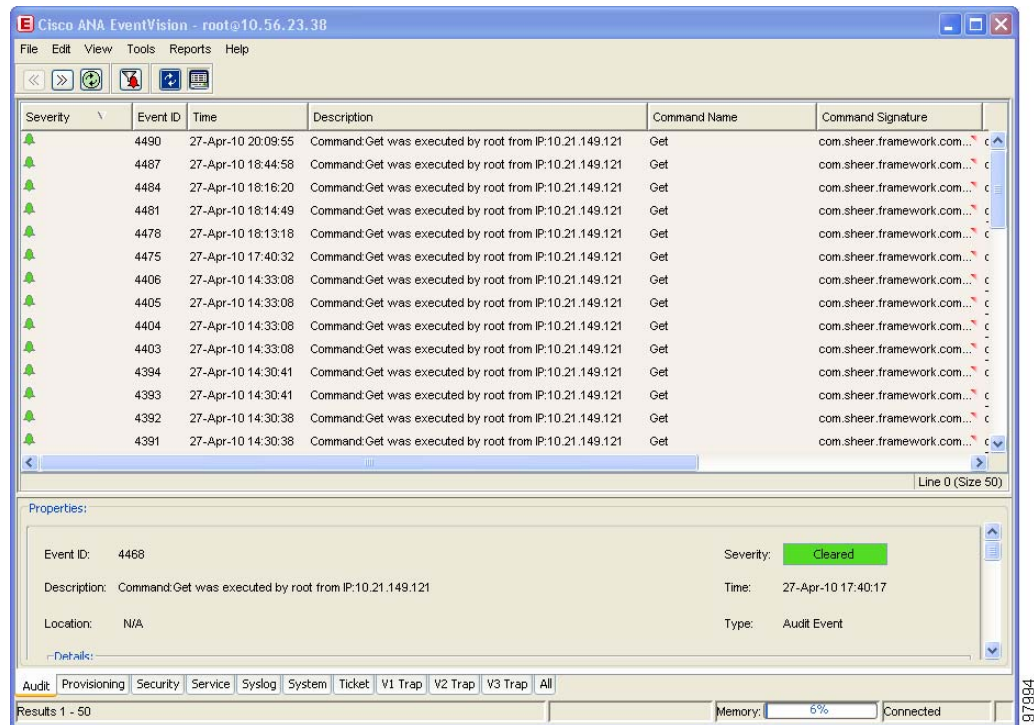
Figure 8-1 Audit Tab

Table 8-3 describes the information that is displayed in the Audit tab.

Table 8-3 Audit Tab

Column	Description
Severity	Icon of a bell, colored according to the severity of the alarm on the event (the color and type of alarm are displayed in the Properties window Severity field). See Event Status Indicators, page 7-4 .
Event ID	Sequential ID number of the event.
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 Cisco ANA, 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. Cisco ANA 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 both Cisco ANA Command Builder and Cisco ANA Workflow Editor¹.

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, Cisco ANA 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 ANA=====

For more information about activation scripts, see the [Cisco Active Network Abstraction 3.7.1 Integration Developer Guide](#).

Table 8-4 describes the information that is displayed in the Provisioning tab.

1. The Workflow Editor is based on LiquidBPM by Autonomy, Inc.

Table 8-4 Provisioning Tab

Column	Description
Severity	Icon of a bell, colored according to the severity of the alarm on the event (the color and type of alarm are displayed in the Properties window Severity field). See Event Status Indicators , page 7-4.
Event ID	Sequential ID number of the event.
Time	Date and time when the event happened and was logged and recorded.
Description	Description of the event, such as “Script Show has failed.”
Location	Entity that triggered the event.
Username	Name of the user who performed the provisioning operations.
Status	Status, such as Success or Fail.

Security Tab

The Security tab displays detailed information specific to this event category. Security events are related to client login and user activity when managing the system and the environment. Additional information specific to this event category can be viewed in the Event Properties window.

[Table 8-5](#) describes the information that is displayed in the Security tab.

Table 8-5 Security Tab

Column	Description
Severity	Icon of a bell, colored according to the severity of the alarm on the event (the color and type of alarm are displayed in the Properties window Severity field). See Event Status Indicators , page 7-4.
Event ID	Sequentially assigned identifier of the event.
Time	Date and time when the event happened and was logged and recorded.
Description	Description of the event, such as “Successful login root.”
Location	Entity that triggered the event.
Username	Name of the user who triggered the event.
Originating IP	IP address of the client where the event was triggered.

For more information about the system security events displayed in this tab, see the [Cisco Active Network Abstraction 3.7.1 Reference Guide](#).

System Tab

The System tab displays all the system events related to the everyday working of the internal system and its components. These events can be related to Cisco ANA and Cisco ANA gateway resources, representing the system log. Additional information specific to this event category can be viewed in the Event Properties window.

[Table 8-6](#) describes the information that is displayed in the System tab.

Table 8-6 **System Tab**

Column	Description
Severity	Icon of a bell, colored according to the severity of the alarm on the event (the color and type of alarm are displayed in the Properties window Severity field). See Event Status Indicators, page 7-4 .
Event ID	Sequential ID number of the event.
Time	Date and time when the event happened and was logged and recorded.
Description	Description of the event, such as “Dropped Events Report.”
Location	Entity that triggered the event.

For more information about the system error and event messages displayed in this tab, see the [Cisco Active Network Abstraction 3.7.1 Reference Guide](#).

Network Event Tabs

The following topics describe the information displayed in Cisco ANA EventVision for network events:

- [Service Tab, page 8-6](#)
- [Syslog Tab, page 8-7](#)
- [Ticket Tab, page 8-8](#)
- [V1 Trap Tab, page 8-8](#)
- [V2 Trap Tab, page 8-9](#)
- [V3 Trap Tab, page 8-10](#)

Service Tab

The Service tab displays all the events generated by Cisco ANA, such as Link Down. Service events are related to the alarms that are generated by the Cisco ANA system. Additional information specific to this event category can be viewed in the Event Properties window.

[Table 8-7](#) describes the information that is displayed in the Service tab.

Table 8-7 **Service Tab**

Column	Description
Severity	Icon of a bell, colored according to the severity of the alarm on the event (the color and type of alarm are displayed in the Properties window Severity field). See Event Status Indicators, page 7-4 .
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 “BGP neighbor found.”
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.

Table 8-7 Service Tab (continued)

Column	Description
Ticket ID	Hyperlinked identifier of the ticket associated with the event. Click the link to view the Ticket Properties window.
Causing Event ID	Identifier of the causing event.
Duplication Count	For network events, the duplication count is calculated by the VNE and pertains only to flapping events. The duplication count represents the number of noncleared events aggregated by the flapping event.
Reduction Count	For network events, the reduction count is calculated by the VNE and pertains only to flapping events. The reduction count represents the number of events that are aggregated by the flapping event.

For more information about the service alarms that are displayed in this tab, see the [Cisco Active Network Abstraction 3.7.1 Reference Guide](#).

Syslog Tab

The Syslog tab displays all the syslog events. These events are related to the predefined set of syslogs received from the devices by the VNEs, which are used to generate the syslog events. Additional information specific to this event category can be viewed in the Event Properties window.

[Table 8-8](#) describes the information that is displayed in the Syslog tab.

Table 8-8 Syslog Tab

Column	Description
Severity	Icon of a bell, colored according to the severity of the alarm on the event (the color and type of alarm are displayed in the Properties window Severity field). See Event Status Indicators, page 7-4 .
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	Entity that triggered the event.
Alarm ID	Identifier of the alarm associated with the event.
Ticket ID	Identifier of the ticket associated with the event.
Causing Event ID	Identifier of the causing event.
Duplication Count	For network events, the duplication count is calculated by the VNE and pertains only to flapping events. The duplication count represents the number of noncleared events aggregated by the flapping event.
Reduction Count	For network events, the reduction count is calculated by the VNE and pertains only to flapping events. The reduction count represents the number of events that are aggregated by the flapping event.

Ticket Tab

The Ticket tab displays detailed information specific to tickets. A ticket contains a single root alarm (the root cause alarm can be of any alarm type, such as syslog or service), and all its subsequent correlated alarms. Additional information specific to tickets can be viewed in the Ticket Properties window.

A *Tickets capacity overflow, red threshold reached* system alarm is generated when the maximum number of tickets is exceeded. The alarm severity is defined as critical.

[Table 8-9](#) describes the information that is displayed in the Ticket tab.

Table 8-9 ***Ticket Tab***

Column	Description
Severity	Icon of a bell, colored according to the severity of the alarm on the ticket (the color and type of alarm are displayed in the Ticket Properties window Severity field). See Event Status Indicators, page 7-4 .
Ticket ID	Sequentially assigned identifier of the ticket, hyperlinked to the Ticket Properties window.
Last Modification Time	Date and time when the ticket was last modified.
Description	Description of the event, such as “BGP neighbor found.”
Location	Hyperlink to the entity that triggered the event.
Acknowledged	Status of the ticket: Acknowledged or Not Acknowledged.
Event Count	Number of events associated with the ticket.
Affected Devices Count	Number of devices affected by the ticket (the sources of the alarm and their subsequent alarms).
Duplication Count	For tickets, the duplication count is the sum of the duplication counts of all events that are associated with the root alarm.
Reduction Count	Ticket reduction count is the sum of reduction counts of all the events that are associated to the ticket. The History tab in the Ticket Properties window displays one reduction count for each event listed. For more information, see Chapter 9, “Working with Tickets in Cisco ANA NetworkVision.”
Alarm Count	Total number of alarms associated with the ticket, including the root alarm.

For information about viewing ticket properties, see [Viewing Ticket Properties, page 8-18](#).

V1 Trap Tab

This event is triggered when the network element sends a trap message to Cisco ANA because of a network event, such as Link Down. The V1 Trap tab displays detailed information specific to this category. Additional information specific to each event category can be viewed in the Event Properties window.

Table 8-10 describes the information that is displayed in the V1 Trap tab.

Table 8-10 V1 Trap Tab

Column	Description
Severity	Icon of a bell, colored according to the severity of the alarm on the event (the color and type of alarm are displayed in the Properties window Severity field). See Event Status Indicators, page 7-4 .
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 the [Cisco Active Network Abstraction 3.7.1 Reference Guide](#).

V2 Trap Tab

This event is triggered when the network element sends a trap message to Cisco ANA because of a network event. The V2 Trap tab displays detailed information specific to this category. Additional information specific to each event category can be viewed in the Event Properties window.

Table 8-11 describes the information that is displayed in the V2 Trap tab.

Table 8-11 V2 Trap Tab

Column	Description
Severity	Icon of a bell, colored according to the severity of the alarm on the event (the color and type of alarm are displayed in the Properties window Severity field). See Event Status Indicators, page 7-4 .
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.

Table 8-11 V2 Trap Tab (continued)

Column	Description
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.
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.dismanEventMIBNotificationPrefix.
Trap Type OID	Trap object identifier.
Enterprise	Enterprise OID for the trap, representing the company or organization that is associated with the trap.

For more information about the Cisco IOS and Cisco IOX traps displayed in this tab, see the [Cisco Active Network Abstraction 3.7.1 Reference Guide](#).

V3 Trap Tab

This event is triggered when the network element sends a trap message to Cisco ANA because of a network event. The V3 Trap tab displays detailed information specific to this category. Additional information specific to each event category can be viewed in the Event Properties window.

[Table 8-12](#) describes the information that is displayed in the V3 Trap tab.

Table 8-12 V3 Trap Tab

Column	Description
Severity	Icon of a bell, colored according to the severity of the alarm on the event (the color and type of alarm are displayed in the Properties window Severity field). See Event Status Indicators, page 7-4 .
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.

Table 8-12 V3 Trap Tab (continued)

Column	Description
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.
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.dismanEventMIBNotificationPrefix.
Trap Type OID	Trap object identifier.
Enterprise	Enterprise OID for the trap, representing the company or organization that is associated with the trap.

For more information about the Cisco IOS and Cisco IOX traps displayed in this tab, see the [Cisco Active Network Abstraction 3.7.1 Reference Guide](#).

Viewing 3.6.x Tabs

If you upgrade to Cisco ANA 3.7 or 3.7.1 from version 3.6.7, 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

[Figure 8-2](#) shows an example Cisco ANA EventVision when the 3.6.x tabs are displayed.

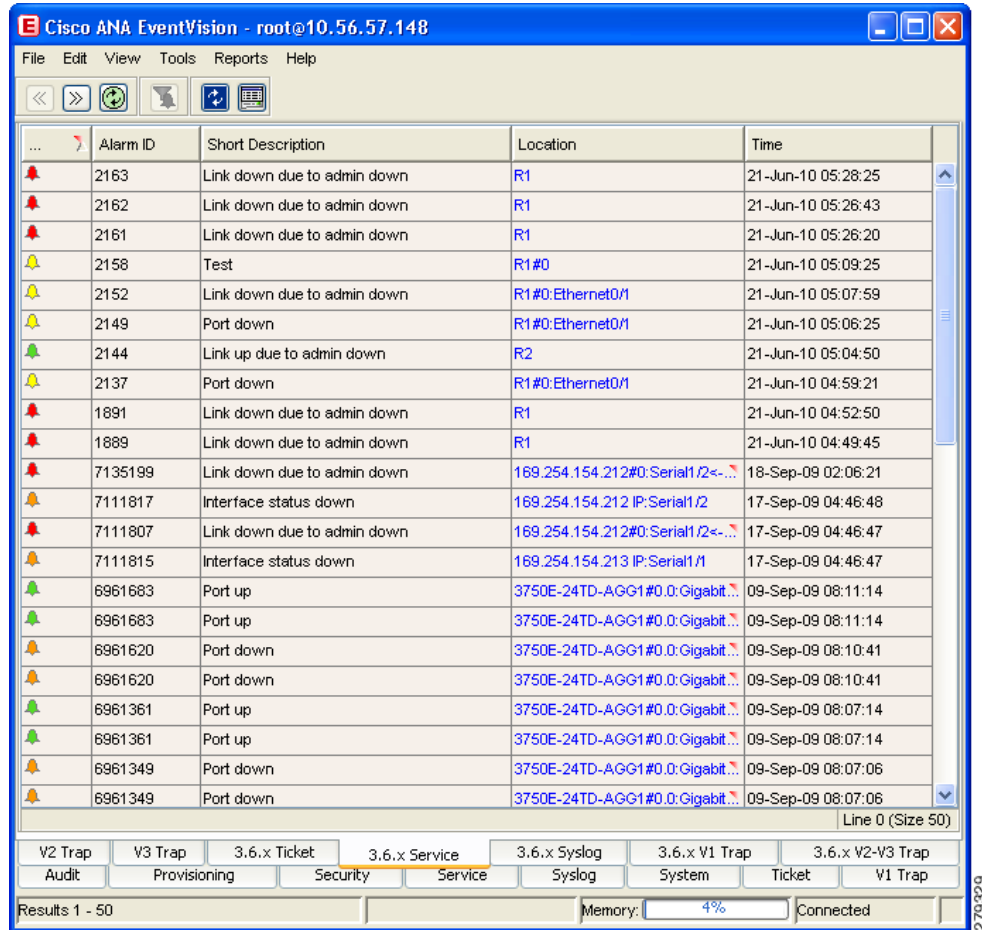
Figure 8-2 Cisco ANA EventVision with 3.6.x Tabs

Table 8-13 describes the information that is displayed in each of the 3.6.x tabs.

Table 8-13 3.6.x Tab Contents in EventVision

Field	Description
3.6.x Ticket Tab	
Severity	Icon of a bell, colored according to the severity of the alarm on the ticket. For more information, see Event Status Indicators, page 7-4 .
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 when the ticket was last modified.
Time	Date and time recorded when the first event happened.
Acknowledged	Status of the ticket: Acknowledged, Not Acknowledged, or Partly Acknowledged.
Affected Devices Count	Number of devices affected by the ticket (the sources of the alarm and their subsequent alarms).

Table 8-13 3.6.x Tab Contents in EventVision (continued)

Field	Description
Correlation Count	Number of correlated alarms included in the ticket.
Reduction Count	Ticket reduction count is the sum of reduction counts of all the events that are associated to the ticket. The History tab in the Ticket Properties window displays one reduction count for each event listed. For more information, see Chapter 9, “Working with Tickets in Cisco ANA NetworkVision.”
Duplication Count	For tickets, the duplication count is the sum of the duplication counts of all events that are associated with the root alarm.
3.6.x Service Tab	
Severity	Icon of a bell, colored according to the severity of the alarm. For more information, see Event Status Indicators, page 7-4 .
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 7-4 .
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 V1 Trap Tab	
Severity	Icon of a bell, colored according to the severity of the alarm. For more information, see Event Status Indicators, page 7-4 .
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 7-4 .
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 in Cisco ANA EventVision

The following sections describe how to view, filter, and display the properties of specific events and tickets, and how to refresh and export events:

- [Viewing Event Properties, page 8-14](#)
- [Viewing Ticket Properties, page 8-18](#)
- [Refreshing Cisco ANA EventVision Information, page 8-20](#)
- [Filtering Events and Tickets, page 8-21](#)
- [Exporting Displayed Data, page 8-24](#)

Viewing Event Properties

Cisco ANA EventVision 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 **Details Pane** on the toolbar displays the properties of the selected ticket or event in the Properties pane.

To view event properties:

Step 1 Select the required tab for the specific event type and the event in the Cisco ANA EventVision window.

Step 2 Do one of the following:

- Double-click the event in the events list.
- Choose **View > Properties** from the main menu.
- Right-click the event and choose **Properties**.

The Event Properties tabbed window is displayed for the selected event, as shown in [Figure 8-3](#). The Details tab is displayed by default.

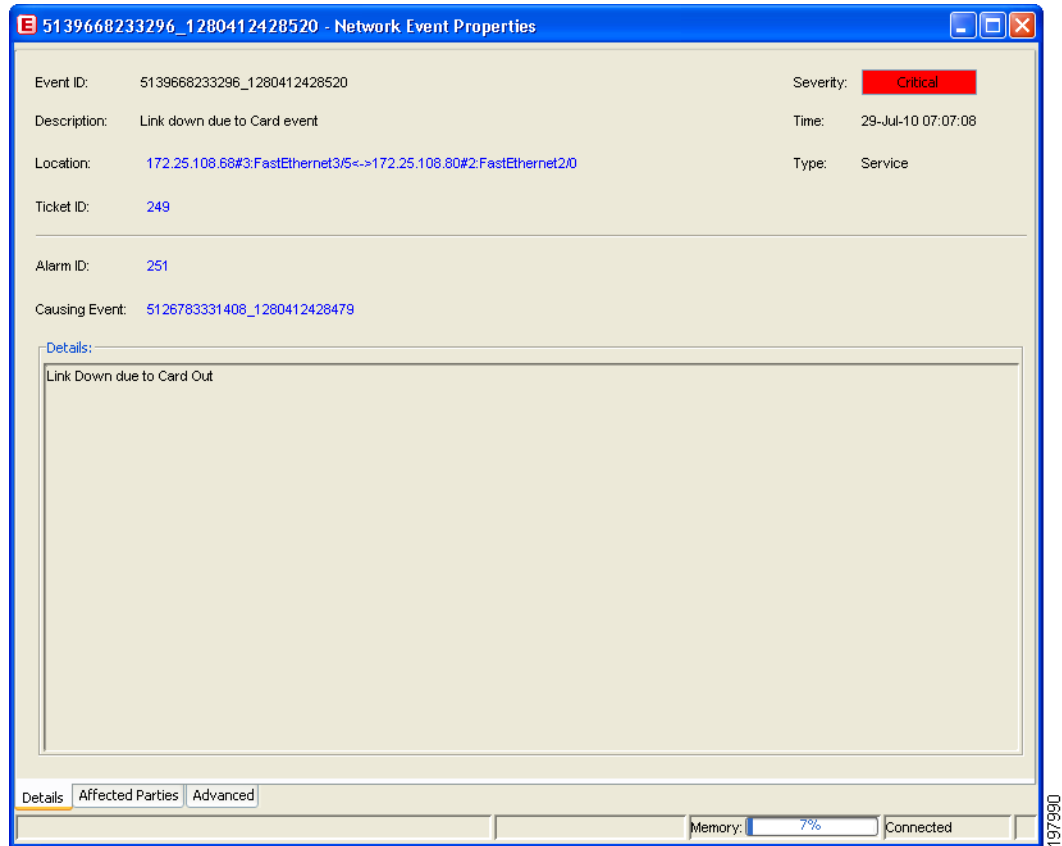
Figure 8-3 Event Properties Window - Details Tab

Table 8-14 describes the information that is displayed in the Event Properties window in the Details tab.

Table 8-14 Details Tab for Events

Field	Description
Event ID	Unique identifier for the selected event.
Severity	Severity of the event, indicated by color and text label.
Description	Description of the event.
Time	Date and time when the event happened and was logged and recorded.
Location	Entity that triggered the event, hyperlinked to its entry in physical inventory.
Type	Type of event, such as Security or Service.
Ticket ID	This field is displayed only for network events. Sequential identifier of the ticket, hyperlinked to the Ticket Properties window.
Alarm ID	This field is displayed only for network events. Alarm identifier, hyperlinked to the Ticket Properties window.

Table 8-14 *Details Tab for Events (continued)*

Field	Description
Causing Event	This field is displayed only for network events. The identifier of the causing event.
Details	Detailed description of the event.

Step 3 As required, view additional properties for the event.

[Table 8-15](#) identifies the tabs that are available for each type of event and a link to the relevant information.

Table 8-15 *Event Properties Window - Available Tabs by Event Type*

Event Types and Tabs	Related Topic
Audit Events	
Details	Details Tab for Events, page 8-15
Audit	Audit Tab, page 8-17
Provisioning Events	
Details	Details Tab for Events, page 8-15
Provisioning	Provisioning Tab, page 8-17
Security Events	
Details	Details Tab for Events, page 8-15
Security	Security Tab, page 8-17
Service Events	
Details	Details Tab for Events, page 8-15
Affected Parties	Affected Parties Tab, page 9-11
Advanced	Advanced Tab, page 9-15
Syslog Events	
Details	Details Tab for Events, page 8-15
Affected Parties	Affected Parties Tab, page 9-11
Advanced	Advanced Tab, page 9-15
System Events	
Details	Details Tab for Events, page 8-15
Trap Events	
Details	Details Tab for Events, page 8-15
Affected Parties	Affected Parties Tab, page 9-11
Advanced	Advanced Tab, page 9-15
Trap	Trap Tab, page 8-18

Audit Tab

Table 8-16 describes the information that is displayed in the Audit tab for audit-related events.

Table 8-16 **Audit Tab**

Field	Description
User Name	Name of user who initiated the command.
Result	Command result, if available.
Originating IP	IP address of the client that issued the command.
Command Signature	Actual command run by Cisco ANA, such as GetEventViewerProperties .
Command Parameters	Parameters applied to the command.

Provisioning Tab

Table 8-17 describes the information that is displayed in the Provisioning tab for provisioning-related events.

Table 8-17 **Provisioning Tab**

Field	Description
User Name	Name of the user who performed the provisioning operation.
Status	Status of the operation: Success or Fail.

Security Tab

Table 8-18 describes the information that is displayed in the Security tab for security-related events.

Table 8-18 **Security Tab**

Field	Description
User Name	Name of the user who triggered the event.
Client Type	Client that triggered the event: Cisco ANA NetworkVision, Cisco ANA Manage, Cisco ANA EventVision, or Unknown.
Originating IP	IP address of the client where the event was triggered.

Trap Tab

[Table 8-19](#) describes the information that is displayed in the Trap tab for trap-related events.

Table 8-19 Trap Tab

Field	Description
Version	The SNMP version: version-1, version-2c, or version-3.
Community String	The community that the device sends in the Protocol Data Unit (PDU).
Error Status	The error status: No Error, Too Big, No Such Name, Bad Value, Read Only, and Gen Err.
Values	
Translated Oid	A string representation of the OID. For example, 1.3.6 is translated into iso.org.dod where: 1 represents iso. 3 represents org. 6 represents dod.
Translated Value	A 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	The OID that is not translated. It is a dot notation representation of the OID, such as 1.3.6.1.4.1.9.
Value	The 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 9-7](#).

Viewing Ticket Properties

The properties of a selected ticket can be viewed in detail by displaying the Ticket Properties window.

To view ticket properties:

-
- Step 1** In the Ticket tab in the Cisco ANA EventVision window, select the required ticket.
- Step 2** Do one of the following:
- Double-click the ticket.
 - Choose **View > Properties** from the main menu.
 - Right-click the ticket and choose **Properties**.

The Ticket Properties tabbed window is displayed for the selected ticket, as shown in Figure 8-4.

Figure 8-4 Ticket Properties Window - Details Tab

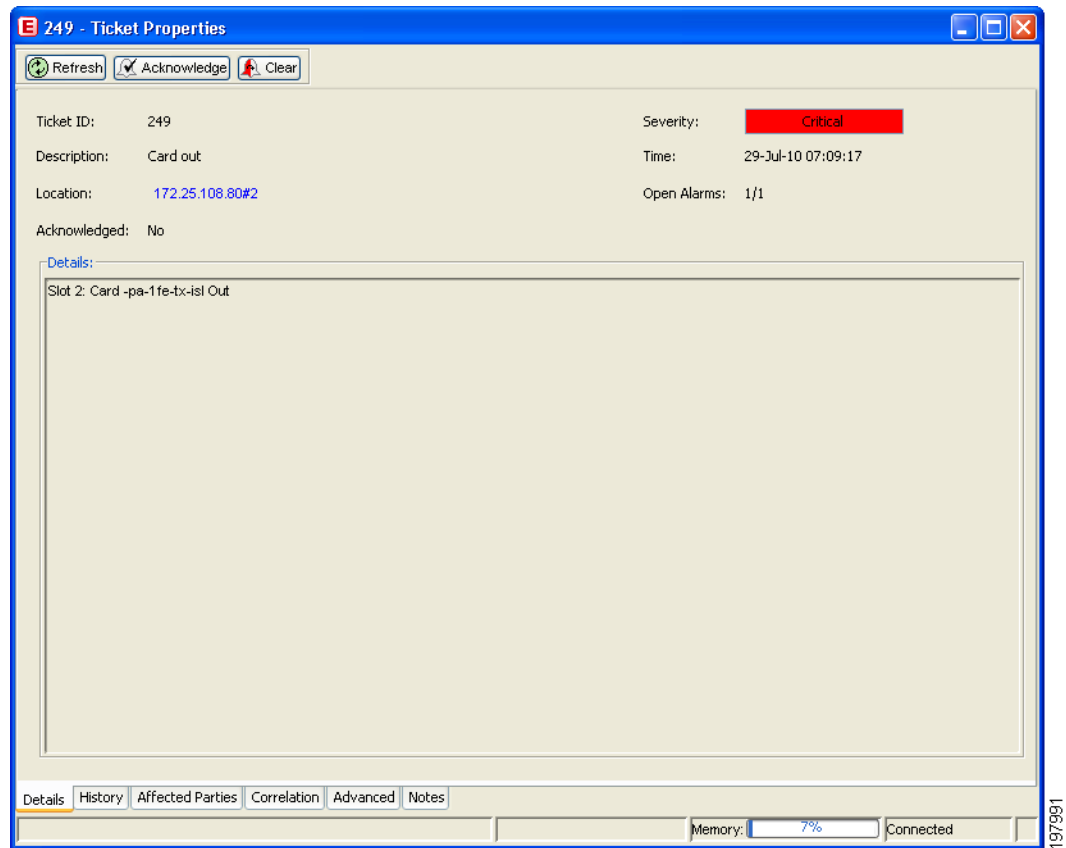


Table 8-20 describes the information that is displayed in the Details tab in the Ticket Properties window.

Table 8-20 Ticket Properties Window - Details Tab

Field	Description
Details Tab	
Ticket ID	Sequentially assigned identifier of the ticket.
Severity	Severity of the ticket, indicated by color and text label.
Description	Description of the ticket.
Time	Date and time when the ticket and was logged and recorded.
Location	Hyperlink to the entity that triggered the event. Note If the entity that triggered the event is outside your scope, a message is displayed that states you do not have permission to access the selected item.
Open Alarms	Number of open alarms out of all alarms, such as 3/4.
Acknowledged	Whether or not the ticket has been acknowledged: Yes or No.
Details	Detailed description of the ticket.

Step 3 As required, review additional properties for the ticket.

[Table 8-21](#) identifies the additional tabs that are displayed in the Ticket Properties window and links to the relevant information.

Table 8-21 Ticket Properties Window - Additional Tabs

Tab	Description
History	Contains the history of the ticket, including all the events. For more information, see History Tab, page 9-10 .
Affected Parties	The services (affected pairs) that are potentially affected (potential impact analysis) by the ticket. For more information, see Affected Parties Tab, page 9-11 .
Correlation	Displays all the alarms that are correlated to the selected ticket. For more information, see Correlation Tab, page 9-14 .
Advanced	The number of affected devices, correlations, duplications, and reductions for the selected ticket. In addition, it provides any other additional information available about the ticket. For more information, see Advanced Tab, page 9-15 .
Notes	Enables you to add and save notes for the selected ticket. The Notes tab is not available for tickets that have been archived. For more information, see Notes Tab, page 9-15 .

Refreshing Cisco ANA EventVision Information

Cisco ANA EventVision displays current information in lists in each tab. While you view a list, the information is not updated unless you manually refresh the list or activate autorefresh. The default autorefresh setting is 60 seconds and can be adjusted (see [Selecting Cisco ANA EventVision Viewing Options, page 7-8](#)). Your filter settings remain intact.

Table 8-22 shows the refresh icons.

Table 8-22 Cisco ANA EventVision Refresh Icons

Button	Name	Function
	Refresh Now	Manually refreshes the events list.
	Auto Refresh	Automatically refreshes the events list. The Auto Refresh icon toggles to indicate whether auto refresh is on or off. This icon indicates auto refresh is on.

To manually refresh a list, do one of the following:

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

To automatically refresh a list, click **Auto Refresh** in the toolbar.

Filtering Events and Tickets

The Filter Events dialog box allows you to filter events and tickets according to severity, identifier, date and time, and text in the description field. 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 ANA EventVision Options dialog box also affect your filters:

- If you check the Keep Last Filter check box, the currently defined filter settings are saved in the registry and are displayed the next time you log in, but are not applied.
- If you check the Open Using Filter check box, the events are continuously filtered according to the defined settings, even when you log out of and back into the application.

For more information, see [Selecting Cisco ANA EventVision Viewing Options, page 7-8](#).

See the following topics for more information about filtering events and tickets:

- [Defining Filters, page 8-21](#)
- [Removing Filters, page 8-24](#)

Defining Filters

To define a filter:

Step 1

Do one of the following:

- Choose **Edit > Filter** from the main menu.
- Click **Filter** in the main toolbar.

Figure 8-5 Cisco ANA EventVision Filter Events Dialog Box

Filter Events

Aggregated Severity

☐ Indeterminate

☐ Information

☐ Cleared

☐ Warning

☐ Minor

☒ Major

☒ Critical

General

☒ ID

Contains

☒ Description

Does Not Contain

☒ Location

☒ Last Modification Time

From:

Sat 26 / Dec / 2009

11 : 3 : 31

To:

Sat 26 / Dec / 2009

11 : 3 : 31

Advanced

☒ Acknowledged

Partly Acknowled...

☒ Event Count

Greater Than

☒ Affected Devices Count

Less Than

☒ DuplicationCount

Equal

☒ ReductionCount

Not Equal

☒ AlarmCount

Greater Than

OK

Cancel

Clear

Step 2 In the Filter Events dialog box, specify the filter criteria as described in Table 8-23.

Table 8-23 Cisco ANA EventVision Filter Events Options

Field	Description
Aggregated Severity	Check the check box of each event severity to include in the filter.
General	
ID	To filter by ticket identifier: 1. Check the ID check box. 2. In the drop-down list, choose the required operator: – Contains – Does Not Contain 3. Enter the value to include or exclude from the filter.
Description	To filter by a string in the description: 1. Check the Description check box. 2. In the drop-down list, choose the required operator: – Contains – Does Not Contain 3. Enter the string to include or exclude from the filter.

Table 8-23 Cisco ANA EventVision Filter Events Options (continued)

Field	Description
Location	To filter events by location: 1. Check the Location check box. 2. Specify the location in one of the following ways: – In the Location field, enter the name of the network element to include in the filter. – Click the ... button to select the required element from a list.
Last Modification Time	To filter events according the time they were last modified: 1. Check the Last Modification Time check box. 2. In the From field, specify the beginning date and time to filter events by. 3. In the To field, specify the ending date and time to use for filtering events.
Advanced	
Acknowledged	To filter events according to their acknowledgement status: 1. Check the Acknowledged check box. 2. In the drop-down list, choose the acknowledgement status: – Acknowledged – Not Acknowledged – Partly Acknowledged
Event Count	To filter events according to their event count: 1. Check the Event Count check box. 2. In the drop-down list, choose the operator for comparing the event count: Greater Than, Less Than, Equal, or Not Equal. 3. In the Event Count field, enter the number of events to use for filtering.
Affected Devices Count	To filter events according to their affected devices count: 1. Check the Affected Devices Count check box. 2. In the drop-down list, choose the operator for comparing the affected devices count: Greater Than, Less Than, Equal, or Not Equal. 3. In the Affected Devices Count field, enter the number of affected devices to use for filtering.
Duplication Count	To filter events according to their duplication count: 1. Check the Duplication Count check box. 2. In the drop-down list, choose the operator for comparing the duplication count: Greater Than, Less Than, Equal, or Not Equal. 3. In the Duplication Count field, enter the value to use for filtering.

Table 8-23 Cisco ANA EventVision Filter Events Options (continued)

Field	Description
Reduction Count	To filter events according to their reduction count: 1. Check the Reduction Count check box. 2. In the drop-down list, choose the operator for comparing the reduction count: Greater Than, Less Than, Equal, or Not Equal. 3. In the Reduction Count field, enter the value to use for filtering.
Alarm Count	To filter events according to their alarm count: 1. Check the Alarm Count check box. 2. In the drop-down list, choose the operator for comparing the alarm count: Greater Than, Less Than, Equal, or Not Equal. 3. In the Alarm Count field, enter the value 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 ANA EventVision enables you to export the currently displayed data from the Cisco ANA EventVision table according to the criteria defined in the Cisco ANA EventVision Options dialog box. You can then import and view at a later time.

To export a table to a file:

- Step 1** Choose **File > Export**.
- Step 2** In the Export Table to File dialog box, browse to the directory where you want to save the list.
- Step 3** In the File name field, enter a name for the list.
- Step 4** Click **Save**. The displayed events list or rows are saved in the selected directory.



CHAPTER 9

Working with Tickets in Cisco ANA NetworkVision

The following topics describe viewing tickets in Cisco ANA NetworkVision, how to manage tickets that represent fault scenarios of selected devices or network elements, and fault impact analysis:

- [User Roles Required to Work with Tickets in Cisco ANA NetworkVision, page 9-1](#)
- [Viewing Tickets in Cisco ANA NetworkVision, page 9-2](#)
- [Viewing Ticket Properties, page 9-7](#)
- [Managing Tickets, page 9-15](#)
- [Impact Analysis in Cisco ANA, page 9-18](#)



Note

For detailed information about alarms and fault management, see the [Cisco Active Network Abstraction 3.7.1 Theory of Operations Guide](#).

User Roles Required to Work with Tickets in Cisco ANA NetworkVision

[Table 9-1](#) identifies the roles that are required to work with tickets in Cisco ANA NetworkVision. Cisco ANA 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 device-based tasks (tasks that do affect devices), authorization is based on the default permission that is assigned to your account. That is, whether the device 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 Active Network Abstraction 3.7.1 Administrator Guide](#).



Note

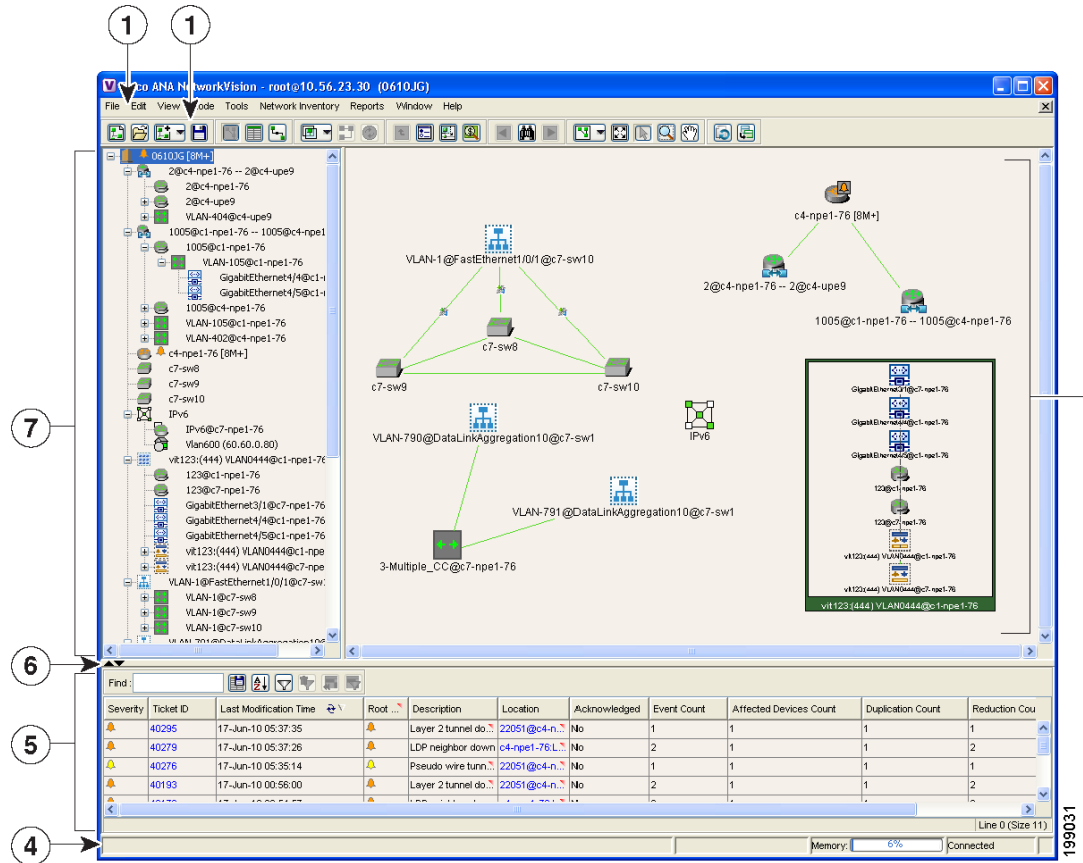
If a device that is outside of your scope is the root cause of a ticket that affects a device in your scope, you can view the ticket Cisco ANA NetworkVision, but the ticket will indicate that the root cause is outside of your scope.

Table 9-1 *Default Permission/Security Level Required for Working with Tickets in Cisco ANA NetworkVision*

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View tickets	—	—	—	—	X
Filter tickets	—	—	—	—	X
View ticket properties	—	—	—	—	X
Find affected elements	—	—	—	—	X
Acknowledge tickets	—	—	—	—	X
Clear tickets	—	—	—	—	X
Remove tickets	—	—	—	—	X
Clear and remove tickets	—	—	—	—	X
Disable impact analysis	—	—	—	—	X
View information for an affected pair	—	—	—	—	X

Viewing Tickets in Cisco ANA NetworkVision

Tickets are displayed in the ticket pane in Cisco ANA NetworkVision as shown in [Figure 9-1](#).

Figure 9-1 Cisco ANA NetworkVision Window

1	Menu bar	5	Ticket pane
2	Toolbar	6	Hide/Display ticket pane
3	Content area	7	Navigation pane
4	Status bar		

The ticket pane enables you to view and manage tickets as well as find the elements affected by a ticket. All tickets that are reported by Cisco ANA are stored in the Cisco ANA gateway database.

The ticket pane is displayed beneath the navigation and content panes in the Cisco ANA NetworkVision window. You can view or hide the ticket pane by clicking the arrows displayed below the navigation pane.

For more information about the information available in the ticket pane, see [Table 2-10 on page 2-16](#).

The ticket pane enables you to perform the following tasks:

Task	Related Topic
View all tickets or only the filtered tickets of a selected device.	Filtering Tickets by Device, page 9-5
View and filter all tickets that meet specified criteria.	Filtering Tickets by Criteria, page 9-6
View the properties of a ticket, including the history, correlated alarms, and affected parties.	Viewing Ticket Properties, page 9-7
Find the elements affected by a ticket in the map.	Finding Affected Elements, page 9-16
View and acknowledge tickets.	Acknowledging a Ticket, page 9-16
Clear a ticket.	Clearing a Ticket, page 9-16
Remove a ticket.	Removing a Ticket, page 9-17
Clear and remove a ticket.	Clearing and Removing Tickets, page 9-17

Ticket Status in the Ticket Pane

The appearance of a ticket displayed in the ticket pane depends on the severity of the ticket and the operations that have been performed on the ticket. Tickets detailed in the ticket pane change when:

- A ticket is generated.
- A ticket is cleared.
- A ticket is acknowledged.
- An Up ticket is generated.
- A ticket is cleared and removed.
- A ticket is removed.
- Other properties are updated, such as severity, description, or counters.

Generated Ticket

[Table 9-2](#) shows an example of the appearance of the ticket pane when a ticket is generated.

Table 9-2 **Generated Ticket**

Icon	Severity	Ticket ID	Short Description	Acknowledged
	(Major)	27	Port down	Yes

Cleared Ticket

Table 9-3 shows an example of the appearance of the ticket pane when a ticket is cleared.

Table 9-3 **Cleared Ticket**

Icon	Severity	Ticket ID	Short Description	Acknowledged
	(Normal)	27	Cleared due to Force Clear	Yes

A ticket that has been cleared can be removed from the ticket pane.

When a ticket is cleared, its definition automatically changes to acknowledged in the ticket pane and its definition in the Acknowledged column is Acknowledged.

Acknowledged Ticket

Table 9-4 shows an example of the appearance of the ticket pane when a ticket is acknowledged. When a ticket is acknowledged it can then be cleared and the severity changes to Normal.

Table 9-4 **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 Cisco ANA Gateway and from the ticket pane.

Generated Up Ticket

The cause of the alarm is fixed; therefore an Up ticket is automatically generated with a Normal severity. Table 9-5 shows an example of the appearance of the ticket pane when an Up ticket is generated.

Table 9-5 **Generated Up Ticket**

Icon	Severity	Ticket ID	Short Description	Acknowledged
	(Normal)	27	Port up	Yes

Filtering Tickets by Device

Cisco ANA NetworkVision enables you to filter the tickets that are shown in the ticket pane so that only the tickets of a selected device or network element are displayed.

To filter tickets for a specific network element:

- Step 1** Right-click the required device or network element in the navigation pane or a map in the Cisco ANA NetworkVision window to display the Device shortcut menu.

- Step 2** Choose **Filter Tickets**. The ticket pane displays the tickets of the selected device or network element only.



Note The Filter button in the ticket pane toggles to indicate that a filter has been applied.

The filter can be removed to display all the tickets in the system.

Filtering Tickets by Criteria

Cisco ANA NetworkVision enables you to define a filter for the tickets displayed in the ticket pane according to various criteria. For example, tickets can be filtered according to the number of affected parties or acknowledged tickets.

To define a ticket filter:

- Step 1** Click **Ticket Filter** in the ticket pane toolbar. The Ticket Filter dialog box is displayed ([Figure 9-2](#)).

Figure 9-2 Ticket Filter Dialog Box

Ticket Filter

Aggregated Severity

☐ Indeterminate ☐ Information ☐ Cleared ☐ Warning

☐ Minor ☐ Major ☐ Critical

General

☒ ID Contains

☒ Description Contains

☒ Location ...

☒ Last Modification Time From: Sun 20 / Dec / 2009 14 : 20 : 41 To: Sun 20 / Dec / 2009 14 : 20 : 41

Advanced

☒ Acknowledged Not Acknowledged

☒ Event Count Greater Than

☒ Affected Devices Count Greater Than

☒ DuplicationCount Greater Than

☒ ReductionCount Greater Than

☒ AlarmCount Greater Than

OK Cancel Clear

- Step 2** Select the required filter values, and provide any required criteria. For more information about specifying filter criteria, see [Table 8-23](#).

- Step 3** Click **OK**. The filtered 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.

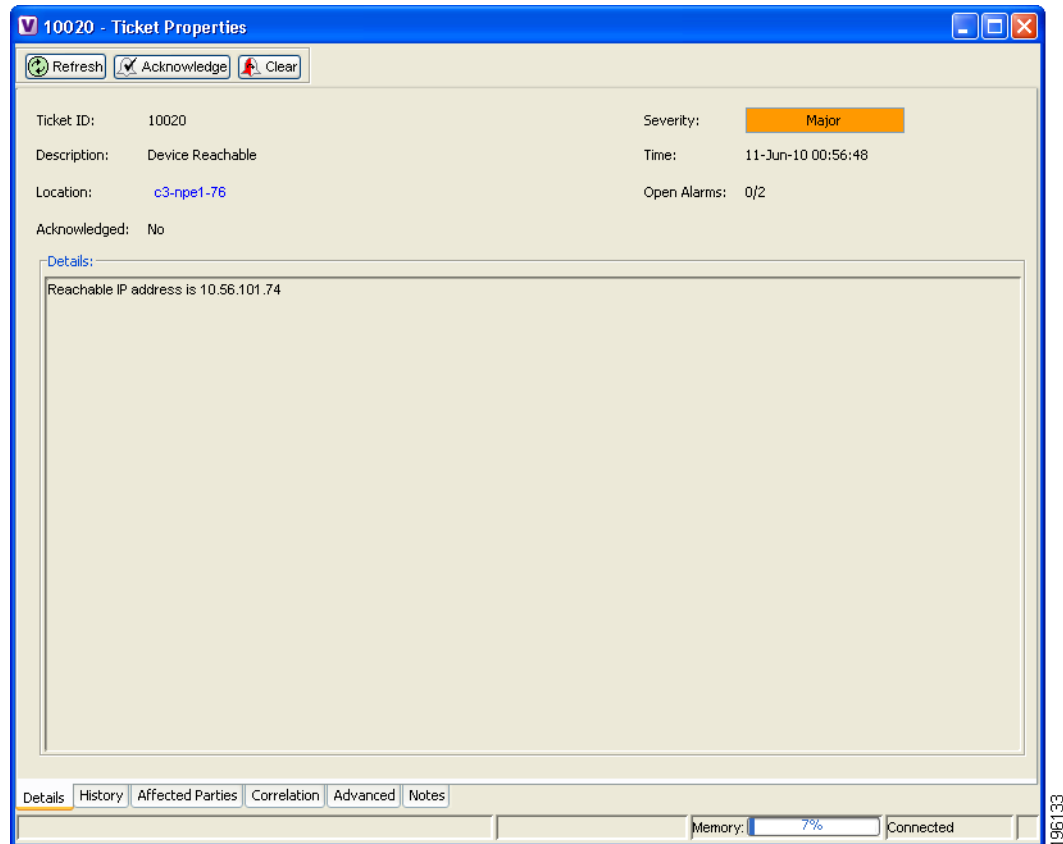
Viewing Ticket Properties

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 Cisco ANA NetworkVision, open the Ticket Properties window in one of the following ways:

- Open the required map and then double-click the required ticket ID in the ticket pane.
- Open the required map, right-click a ticket in the ticket pane, and choose **Properties**.

[Figure 9-3](#) shows the Ticket Properties window.

Figure 9-3 Ticket Properties Window

The information displayed in the Ticket Properties window corresponds with the information displayed in the Cisco ANA NetworkVision ticket pane or the Cisco ANA EventVision window. The ID number displayed in the header corresponds to the ID number of the ticket selected in the ticket pane.

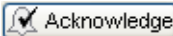
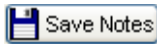
The Ticket Properties window contains the following components:

- [Toolbar, page 9-9](#)
- [Details Tab, page 9-9](#)
- [History Tab, page 9-10](#)
- [Affected Parties Tab, page 9-11](#)
- [Correlation Tab, page 9-14](#)
- [Advanced Tab, page 9-15](#)
- [Notes Tab, page 9-15.](#)

Toolbar

The Ticket Properties dialog box contains the tools described in [Table 9-6](#).

Table 9-6 Ticket Properties Window Toolbar

Icon	Description
 Refresh	Refreshes the information displayed in the Ticket Properties dialog box.
 Acknowledge	Acknowledges that the ticket is being handled. The status of the ticket is displayed as true in the ticket pane and in the Ticket Properties dialog box. For more information, see Acknowledged Ticket, page 9-5 . If a ticket was acknowledged, and some events were correlated to it afterward, then the ticket is considered to have not been acknowledged. This button is enabled only if the ticket is not acknowledged.
 Clear	Requests the relevant Cisco ANA to remove the faulty network element from the Cisco ANA networking inventory. In addition, it sets the ticket to Cleared severity or status (the icon is displayed in green) and automatically changes the acknowledged status of the ticket to true. For more information, see Cleared Ticket, page 9-5 . This button is enabled only if the severity of the alarm is higher than Cleared or Normal.
 Save Notes	Saves the notes for the selected ticket. This button is enabled only when text is entered in the Notes field of the Notes tab.

Details Tab

[Table 9-7](#) describes the information that is displayed in the Details tab about the compiled alarm.

Table 9-7 Event Properties Window - Details Tab

Field	Description
Alarm ID	Alarm identifier.
Severity	Severity propagated from all the correlated alarms.
Description	Description of the ticket.
Time	Date and time when the initial root-cause alarm was generated. The time is taken from Cisco ANA.
Location	Entity that triggered the root-cause alarm, as a hyperlink that opens the relevant location. Note If the entity that triggered the alarm is outside your scope, a message is displayed that states you do not have permission to access the selected item.

Table 9-7 Event Properties Window - Details Tab (continued)

Field	Description
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.
Acknowledged	Whether the alarm has been acknowledged: Yes or No.
Details	Detailed description of the alarm.

History Tab

The History tab enables you to display the history of the ticket, including all the events. [Figure 9-4](#) shows the History tab.

Figure 9-4 History Tab

Severity	Event ID	Time	Description	Location	Alarm ID	Causing Event ID	Duplication Count	Reduction Count
Warning	3831282296134_1...	11-Jun-10 00:50:25	LDP neighbor down	p1.LSE	10038	3534929552714_12...	1	1
Warning	5648053462342_1...	11-Jun-10 00:55:36	LDP neighbor up	p1.LSE	10038		1	1
Warning	3534929552714_1...	11-Jun-10 00:49:48	Link down on unreachable	p1#3.0:GigabitEthernet...	10028	3891411838282_12...	1	1
Warning	4402512946506_1...	11-Jun-10 00:52:27	Link up	p1#3.0:GigabitEthernet...	10028		1	1
Warning	3363130860870_1...	11-Jun-10 00:49:15	Link down syslog	p1#3.0:GigabitEthernet...	10033	3534929552714_12...	1	1
Warning	3367425828166_1...	11-Jun-10 00:49:15	Line down syslog	p1#3.0:GigabitEthernet...	10032	3534929552714_12...	1	1
Warning	4376743142726_1...	11-Jun-10 00:52:24	Link up syslog	p1#3.0:GigabitEthernet...	10033		1	1
Warning	4381038110022_1...	11-Jun-10 00:52:24	Line up syslog	p1#3.0:GigabitEthernet...	10032		1	1
Warning	3247166743878_1...	11-Jun-10 00:48:43	OSPF neighbor down syslog	p1 OSPF Process (v2...	10039	3326771122502_12...	1	1
Warning	3328771122502_1...	11-Jun-10 00:49:02	OSPF Neighbor Down	p1 OSPF Process (v2...	10031	3534929552714_12...	1	1
Warning	4621556278598_1...	11-Jun-10 00:53:11	OSPF neighbor up syslog	p1 OSPF Process (v2...	10039		1	1
Warning	4862074447174_1...	11-Jun-10 00:53:28	OSPF Neighbor Up	p1 OSPF Process (v2...	10031		1	1
Warning	3414670468422_1...	11-Jun-10 00:49:17	Interface status down	p1 IP:GigabitEthernet...	10036	3534929552714_12...	1	1
Warning	4393923011910_1...	11-Jun-10 00:52:25	Interface status up	p1 IP:GigabitEthernet...	10036		1	1
Warning	3577879225674_1...	11-Jun-10 00:50:00	BFD connectivity down	p1 BFD Service <->...	10037	3534929552714_12...	1	1
Warning	3242871776582_1...	11-Jun-10 00:48:43	bfd session down syslog	p1 BFD Service : 2.0...	10040	3577879225674_12...	1	1
Warning	4307456234618_1...	11-Jun-10 00:53:17	bfd session up syslog	p1 BFD Service : 2.0...	10040		1	1

Line 11 (1 / 98 Selected)

11 07:08:11.133 : ospf[317] : %ROUTING-OSPF-5-ADJCHG : Process 10, Nbr 1.1.0.74 on GigabitEthernet0/3/0/4 in area 0 from LOADING to FULL, Loading Done,vrrf default vrrf id:60000000

Details History Affected Parties Correlation Advanced Notes

Memory: 8% Connected

[Table 9-8](#) describes the information that is displayed in the History tab.

Table 9-8 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 when the ticket changed.

Table 9-8 *Ticket Properties Window - History Tab (continued)*

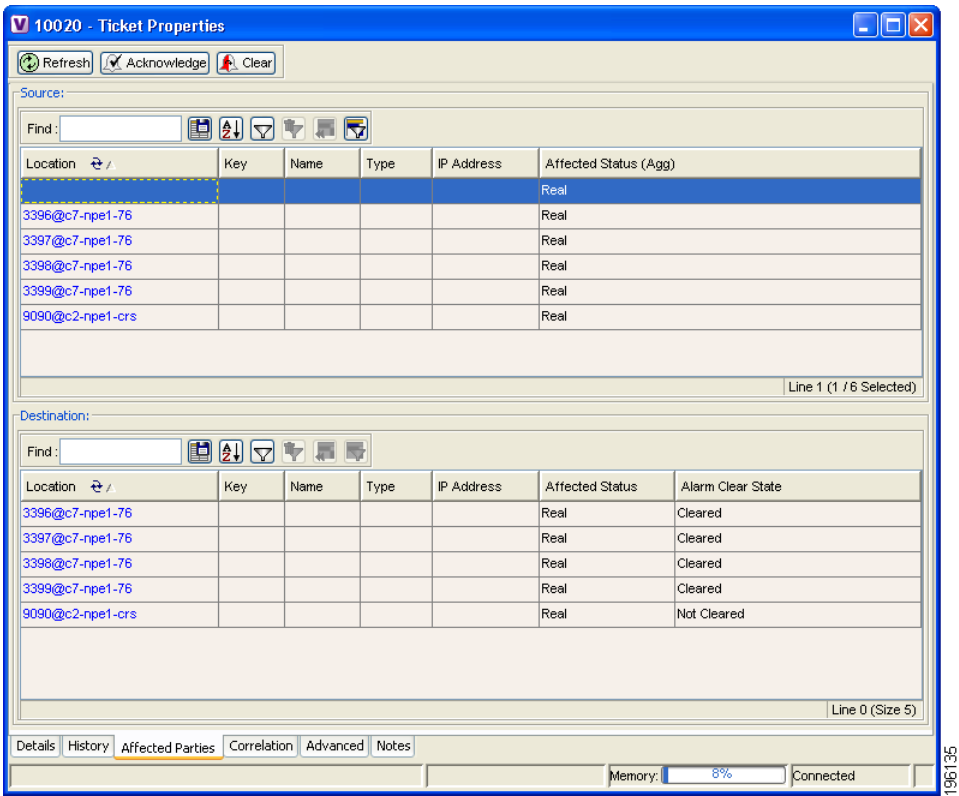
Field	Description
Description	Description of the event.
Location	Entity that triggered the alarm, as a hyperlink that opens the relevant location. Note If the entity that triggered the alarm is outside your scope, a message is displayed that states you do not have permission to access the selected item.
Alarm ID	Alarm identifier.
Ticket ID	Ticket identifier. This field appears in the History tab only in Cisco ANA EventVision.
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, Cisco ANA automatically calculates the affected parties and embeds this information in the ticket along with all the correlated faults. You can view a list of all the endpoints that are affected.

The Affected Parties tab displays the service resources (affected pairs) that are affected by the ticket.

Figure 9-5 Affected Parties Tab



The Affected Parties tab contains two tables: Source and Destination. Table 9-9 describes the information that is displayed in the Affected Properties tab.

Table 9-9 Ticket Properties Window - Affected Properties Tab

Field	Description
Source Table	
Location	Hyperlinked entry to the port with the affected parties.
Key	Unique value taken from the affected element’s business tag key, if it exists.
Name	Subinterface (site) name or business tag name of the affected element, if it exists.
Type	Business tag type.
IP Address	If the affected element is an IP interface, the IP address of the subinterface site.

Table 9-9 Ticket Properties Window - Affected Properties Tab (continued)

Field	Description
Affected Status (Agg)	Status for the affected pair (destination). The same source can be part of multiple pairs, and therefore each pair can have a different affected status. The highest affected status reflects the highest among these. The affected status can be one of the following: • Potential • Real • Recovered • N/A—From the links view, this indicates <i>Not Applicable</i>.
Destination Table	
Location	Hyperlinked entry to the port with the affected parties.
Key	Unique value taken from the affected element's business tag key, if it exists.
Name	Subinterface name or business tag name of the affected element, if it exists.
Type	Business tag type.
IP Address	If the affected element is an IP interface, the IP address of the subinterface site.
Affected Status	Status of the affected pair as calculated by the client according to the rules defined in Status Values for Affected Parties, page 9-18 .
Alarm Clear State	For each pair, an indication of the clear state of the alarm: • Cleared—All related alarms for this pair have been cleared. • Not Cleared—One or more alarms for this pair have not been cleared.

When an affected side is selected in the Source table, the Destination table lists all endpoints with services that have been affected between them and the entry selected in the Source table.

In addition, for every affected pair, you can view detailed information that includes a list of the events that contributed to this affected pair. For more information, see [Viewing Detailed Information for the Affected Pair, page 9-20](#).

**Note**

The Affected Parties dialog box occasionally displays entries that start with the word *Misconfigured*. Entries that start with Misconfigured indicate that the flow has stopped unexpectedly between the source and destination points. An unexpected termination point can be a routing entity, bridge, or VC switching entity. The significant aspects of Misconfigured entries are:

- Because the link does not terminate as expected, the link is not actually impacted.
- An error might exist in the configuration or status of the termination points. We recommend that you check the configuration and status of the affected termination points.

Correlation Tab

The Correlation tab displays all the alarms that are correlated to the selected ticket.

Figure 9-6 Correlation Tab

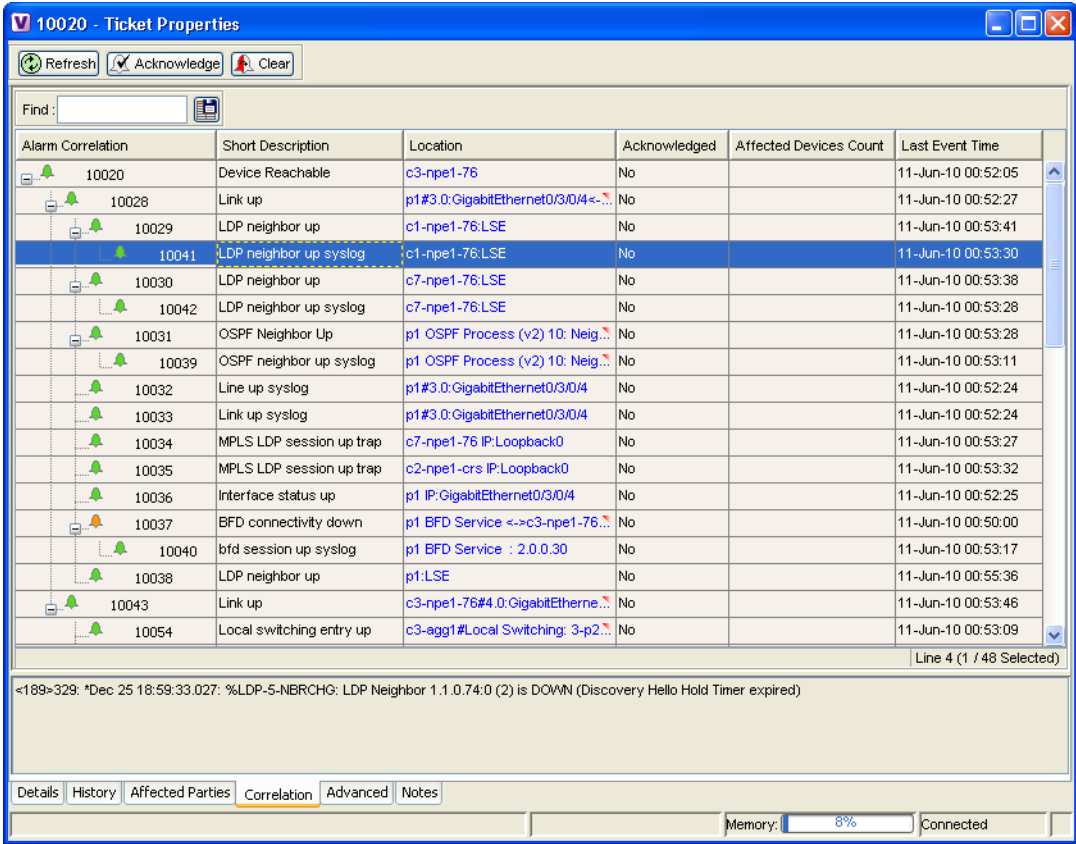


Table 9-10 describes the information that is displayed in the Correlation tab.

Table 9-10 Ticket Properties Window - Correlation Tab

Field	Description
Alarm Correlation	Alarms correlated with the ticket. Expand or collapse the branch to display or hide information as needed. The severity displayed is the severity of the root alarm.
Short Description	Description of the alarm.
Location	Hyperlinked entry that opens an window displaying the selected node along with the affected parties. Note If the entity that triggered the alarm is outside your scope, a message is displayed that states you do not have permission to access the selected item.
Acknowledged	Whether or not the root alarm has been acknowledged: Yes or No.
Affected Devices Count	Number of devices affected by the alarm.

Table 9-10 Ticket Properties Window - Correlation Tab (continued)

Field	Description
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 Windows 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.

The following restrictions apply to the Notes tab:

- 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.

Managing Tickets

The following topics describe how to manage tickets:

- [Finding Affected Elements, page 9-16](#)
- [Acknowledging a Ticket, page 9-16](#)
- [Clearing a Ticket, page 9-16](#)

- [Removing a Ticket, page 9-17](#)
- [Clearing and Removing Tickets, page 9-17](#)

Finding Affected Elements

To locate elements affected by a ticket in Cisco ANA NetworkVision, 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. Cisco ANA NetworkVision enables you to handle the status of a ticket by acknowledging it. This acknowledges the fault.

The change is reported to the Cisco ANA gateway and all open Cisco ANA NetworkVision applications. You can acknowledge multiple tickets at the same time.

An acknowledged ticket returns to a status of Not Acknowledged when a new event is correlated to it.



Note

You cannot undo this operation.

To acknowledge one or more tickets, do one of the following:

- Select one or more tickets in the ticket pane, and then right-click and choose **Acknowledge**.
- Double-click a ticket in the ticket pane and click **Acknowledge**.

For more information, see [Ticket Status in the Ticket Pane, page 9-4](#).

Clearing a Ticket

When an alarm occurs, a warning or ticket is displayed in the ticket pane. Cisco ANA NetworkVision 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 Cisco ANA gateway and all open Cisco ANA NetworkVision applications. This operation cannot be reversed.

You can clear multiple tickets at the same time.



Note

Before using **Clear and Remove** (which might also be available when you right-click a ticket), be sure you understand the results of *removing* a ticket. Like clearing a ticket, removing a ticket cannot be reversed. See [Removing a Ticket, page 9-17](#).

Clearing an open ticket performs the following operations:

- For certain network elements, such as cards and links, sends a request to the Cisco ANA system to remove the faulty network element from the Cisco ANA networking inventory.
- Sets the alarm to Cleared or Normal severity or status by issuing a corresponding Clear alarm.

- Automatically sets the alarm severity or status to acknowledged (true).

To clear one or more tickets, do one of the following:

- Select one or more tickets in the ticket pane, and then right-click and choose **Clear**.
- Double-click a ticket in the ticket pane and click **Clear**.

For more information, see [Ticket Status in the Ticket Pane, page 9-4](#).

Removing a Ticket

When an alarm occurs, a warning or ticket is displayed in the ticket pane. Cisco ANA NetworkVision enables you to completely remove the ticket and all of its active alarms and business tags. The change is reported to the Cisco ANA gateway and all instances of Cisco ANA NetworkVision 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 Cisco ANA EventVision.

Removing a ticket performs the following operations:

- For certain network elements, such as cards or links, sends a request to the Cisco ANA system to remove the faulty network element from the Cisco ANA networking inventory.
- Archives the ticket and active alarms.
- Notifies all open instances of Cisco ANA clients (Cisco ANA NetworkVision or BQL) that are registered on the ticket that the ticket has been removed and deletes the ticket from the ticket pane.



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 [Ticket Status in the Ticket Pane, page 9-4](#).

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 shortcut menu, see [Ticket Shortcut Menu, page 2-37](#).

Clearing and Removing Tickets

Clearing and removing a ticket:

- Approves the reported faulty ticket.
- Clears the faulty networking entity from Cisco ANA.
- Archives the ticket.

You can clear and remove multiple tickets at the same time.

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 Cisco ANA

Impact analysis enables you to identify the network elements and services that are impacted by a network fault or outage.

Cisco ANA offers two modes of impact analysis:

- Automatic impact analysis—When a fault occurs that has been identified as potentially service affecting, Cisco ANA 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—Cisco ANA 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, Cisco ANA 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 relates 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, Cisco ANA might identify the services as either potentially or real affected. As time progresses and more information is accumulated from the network, Cisco ANA updates the information to indicate which of the potentially affected parties are real or recovered.

The indications for these states are available both through the API and in the GUI.



Note

There is no clear state for the affected services when the alarm is cleared.

Accumulating Affected Parties

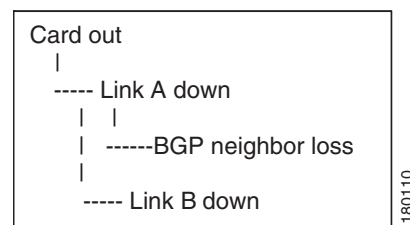
During automatic impact analysis, Cisco ANA NetworkVision automatically calculates the accumulation of affected parties. This information is embedded in the ticket along with all of the correlated faults.

In the following example, these alarm types exist in the correlation tree:

- Ticket root-cause alarm (Card Out).
- An alarm which is correlated to the root cause and has other alarms correlated to it (Link A Down).
- An alarm with no other alarms correlated to it (Link B Down and BGP Neighbor Loss).

An event sequence is correlated to each of these alarms.

Figure 9-7 Correlation Tree Example



Cisco ANA NetworkVision identifies the affected parties for each type of alarm and accumulates the following information:

- The affected parties reported on all the events in the alarm event sequence, including flapping alarms.
- The affected parties reported on the alarms that are correlated to it.

The gathered information includes the accumulation of the affected report of all the events in its own correlation tree.

For example, in [Figure 9-7](#):

- BGP neighbor loss includes the affected parties of all events in its own event sequence.
- Link A Down includes the affected parties of its own event sequence and the accumulated information of the BGP Neighbor Loss event.

Accumulating the Affected Parties in an Alarm

If two events form part of the same event sequence in a specific alarm, the recurring affected pairs are displayed only once in the Affected Parties tab. If different affected severities are reported for the same pair, the pair is marked with the severity that was reported by the latest event, according to the time stamp.

Accumulating the Affected Parties in the Correlation Tree

If two or more alarms that are part of the same correlation tree report on the same affected pair of edgepoints and have different affected severities, the recurring affected pairs are displayed only once in the Affected Parties tab. If different affected severities are reported for the same pair, the pair is marked with the highest severity.

For example, assume that X and Y are the OIDs of edgepoints in the network, and a service is running between them. Both alarms, Link B Down and BGP Neighbor Loss, report on the pair X < > Y as affected:

- Link B Down reports on X < > Y as potentially affected.
- BGP Neighbor Loss reports on X < > Y as real affected.

The affected severity priorities are:

- Real—Priority 1
- Recovered—Priority 2
- Potential—Priority 3

Card Out reports on X < > Y as real, affected only once.

Updating Affected Severity over Time

In some cases, Cisco ANA 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.

Disabling Impact Analysis

You can disable impact analysis for a specific alarm. If impact analysis is disabled, the system reports the event with no impact information. The settings can be changed dynamically during system runtime.

For more information about disabling impact analysis for specific alarms, see the [Cisco Active Network Abstraction 3.7.1 Customization User Guide](#).

Viewing Detailed Information for the Affected Pair

You can view detailed information for every affected pair in Cisco ANA NetworkVision. The detailed information includes a list of the events that contributed to the affected pair.

To view detailed information for the affected pair:

-
- Step 1** Open the Ticket Properties window for the required ticket, as described in [Affected Parties Tab, page 9-11](#).
 - Step 2** Click the **Affected Parties** tab.

- Step 3** In the Source table, click the required entry.
- Step 4** In the Destination table, right-click the required entry, then choose **Detailed List**.
The Affected Parties Destination Properties window is displayed.

Figure 9-8 Affected Parties Destination Properties Window

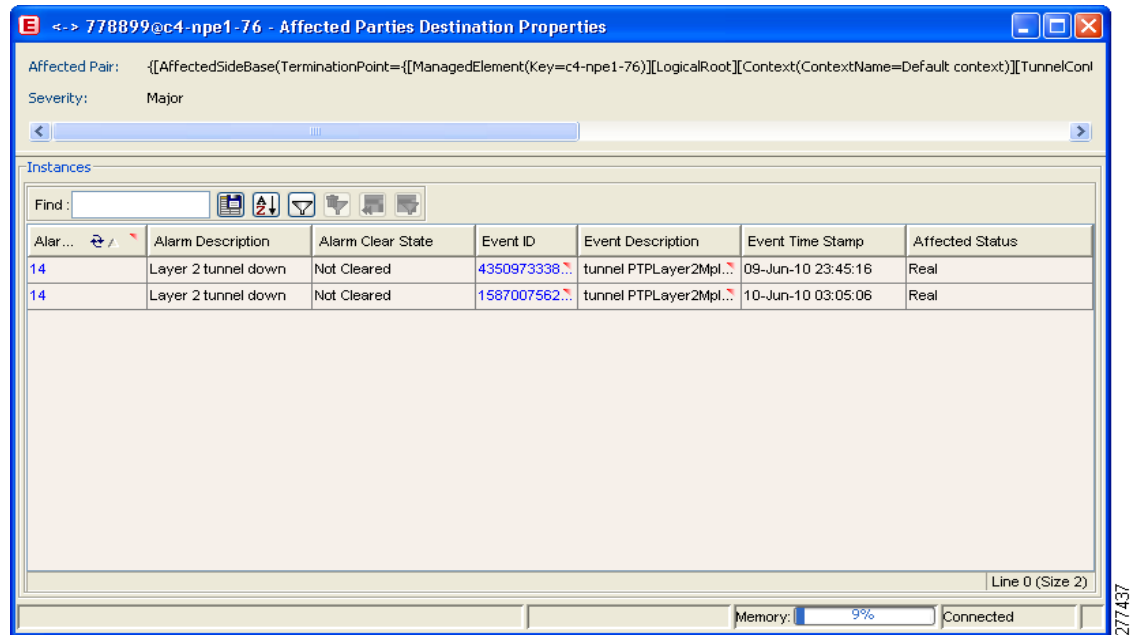


Table 9-11 describes the information that is displayed in the Affected Parties Destination Properties window. Each row in the Instances table represents an event that was reported for the affected pair. The contains a list of pairs of endpoints when the service between them has been affected.

Table 9-11 Affected Parties Destination Properties Window

Field	Description
Affected Pair	Identifiers for the affected pair.
Affected Severity	The status of the selected link as calculated by the client according to the rules defined in Status Values for Affected Parties, page 9-18 . Possible values include: - Potential - Real - Recovered
Severity	The severity of the alarm, such as Major, Minor, or Normal. For more information, see Severity Indicators, page 2-10 .
Instances Table	
Alarm OID	Identifier of the alarm to which the event is correlated as a hyperlink to the alarm's properties.
Alarm Description	Description of the alarm to which the event is correlated.

Table 9-11 *Affected Parties Destination Properties Window (continued)*

Field	Description
Alarm Clear State	For each pair, the clear state of the alarm: • Cleared—All the related alarms for this pair have been cleared. • Not Cleared—One or more alarms for this pair have not been cleared.
Event ID	Event identifier as a hyperlink to the relevant event's properties.
Event Description	Description of the event.
Event Timestamp	Date and time at which the event was created.
Affected Status	Status of the affected pair as calculated by the client according to the rules defined Status Values for Affected Parties , page 9-18.



CHAPTER 10

Working with Reports

Cisco ANA provides a Report Manager that enables you to generate, view, and export reports of the information managed by Cisco ANA. You can save the generated reports in any of the following formats: PDF, CSV, HTML, XLS, and XML.

In addition to a variety of standard reports for events and inventory, you can define reports as required for your environment. The following topics discuss the Report Manager and reports in more detail:

- [User Roles Required to Manage Reports, page 10-1](#)
- [Using the Report Manager, page 10-2](#)
- [Report Categories, page 10-8](#)
- [Generating Reports, page 10-14](#)
- [Managing Reports, page 10-26](#)
- [Defining Report Types, page 10-33](#)
- [Working with Report Folders, page 10-33](#)

User Roles Required to Manage Reports

Table 10-1 identifies the roles that are required to manage reports. Cisco ANA 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 device-based tasks (tasks that do affect devices), authorization is based on the default permission that is assigned to your account. That is, whether the device 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 Active Network Abstraction 3.7.1 Administrator Guide](#).

Table 10-1 Default Permission/Security Level Required for Working with Reports

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Generate reports	X	X	X	X	X
View reports	X	X	X	X	X
Export reports	X	X	X	X	X

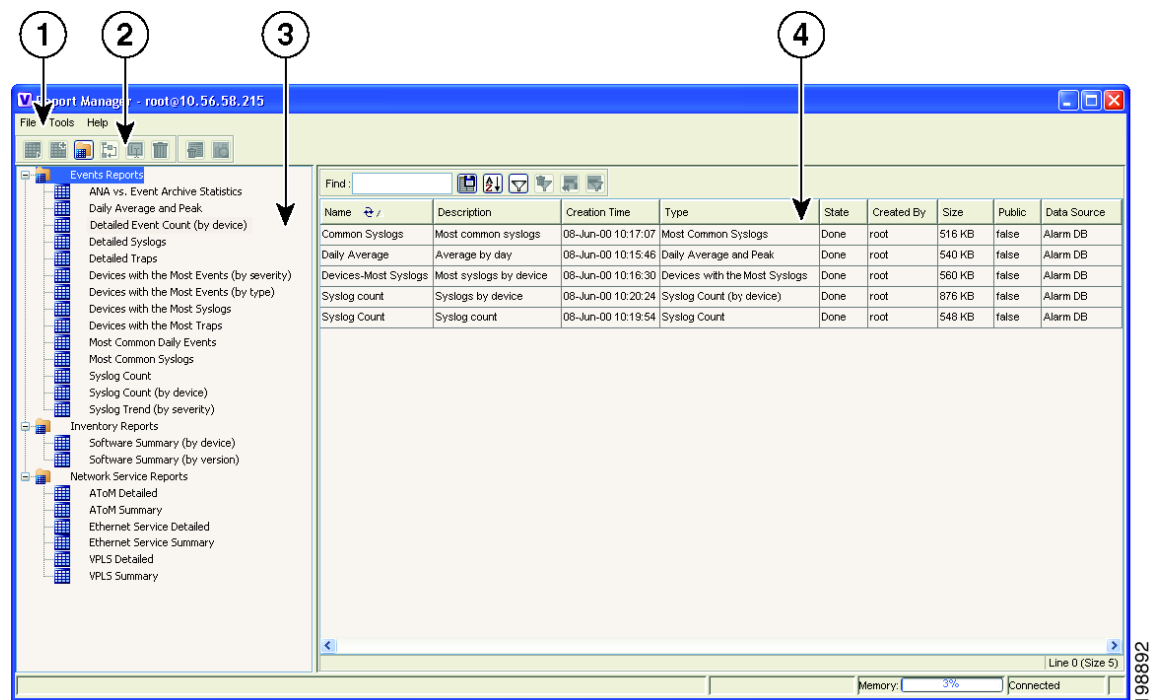
Table 10-1 Default Permission/Security Level Required for Working with Reports (continued)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Save reports	X	X	X	X	X
Print reports	X	X	X	X	X
Delete reports	X	X	X	X	X
Set report preferences for purging and sharing	—	—	—	—	X

Using the Report Manager

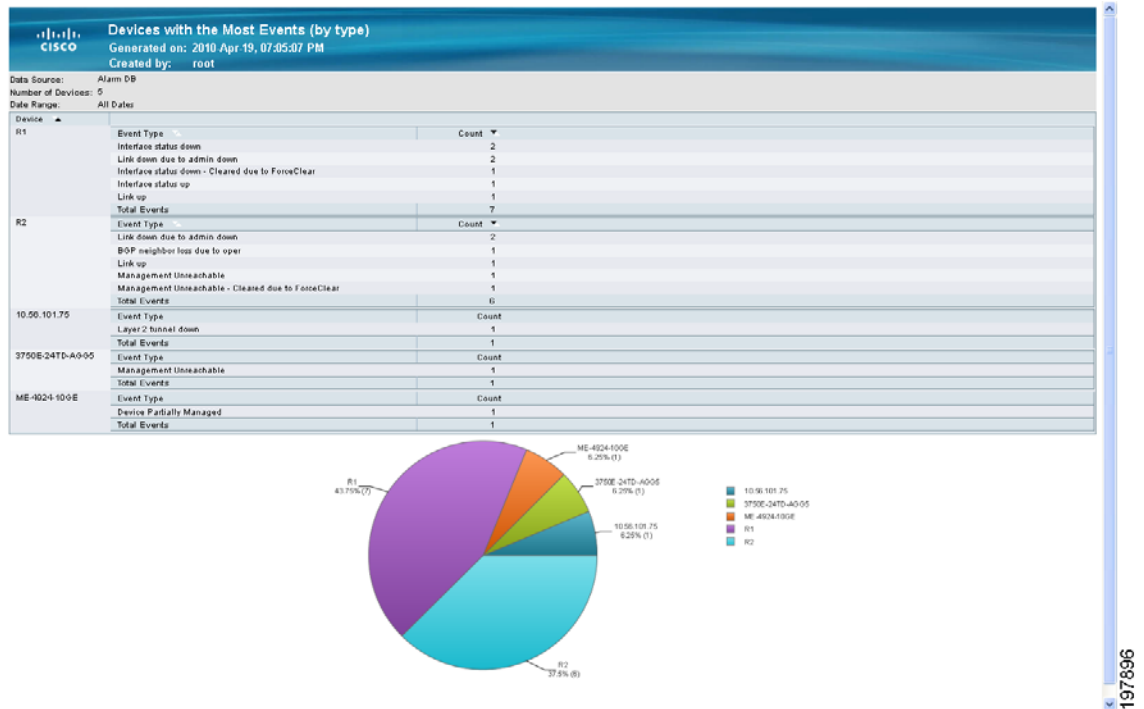
The Report Manager is available from Cisco ANA NetworkVision, Cisco ANA EventVision, and Cisco ANA Manage by choosing **Reports > Report Manager**. The Report Manager (shown in Figure 10-1) enables you to run standard reports, such as the number of syslogs by device.

The Report Manager also enables you to create reports and folders, view previously generated reports, define report types for your use, and organize reports in a manner suited to your environment and needs.

Figure 10-1 Report Manager Window

1	Menu bar	3	Navigation tree with report types and folders
2	Toolbar	4	Content pane

Figure 10-2 shows an example of a generated report with a pie chart.

Figure 10-2 Sample Report

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, and percentage of total events.

**Note**

Not all reports include pie charts. In addition, reports that normally include a pie chart do not display a pie chart if the chart exceeds 25 slices.

Menu Options

Table 10-2 describes the menu options available in the Report Manager window.

Table 10-2 Report Manager Menu Options

Option	Description
File Menu	
Exit	Exits the Cisco ANA NetworkVision application.
Tools Menu	
Change User Password	Enables you to change the password used when logging into the Cisco ANA client application suite. The change takes effect the next time you log into the application.
	Note The administrator can also change a user password in Cisco ANA Manage.

Table 10-2 Report Manager Menu Options (continued)

Option	Description
Help Menu	
Cisco ANA Report Manager Help	Opens the online help for Cisco ANA NetworkVision and Cisco ANA EventVision.
Cisco.com	Unavailable.
About Cisco Report Manager	Displays application information about Cisco ANA NetworkVision.

Toolbar Icons

Table 10-3 identifies the icons that appear in the Report Manager toolbar.

Table 10-3 Report Manager Toolbar Icons

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.
	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 Cisco ANA and any user-defined reports. For more information on the standard report types, see [Table 10-8](#).

When you select an item in the tree, the content pane displays the generated reports as follows:

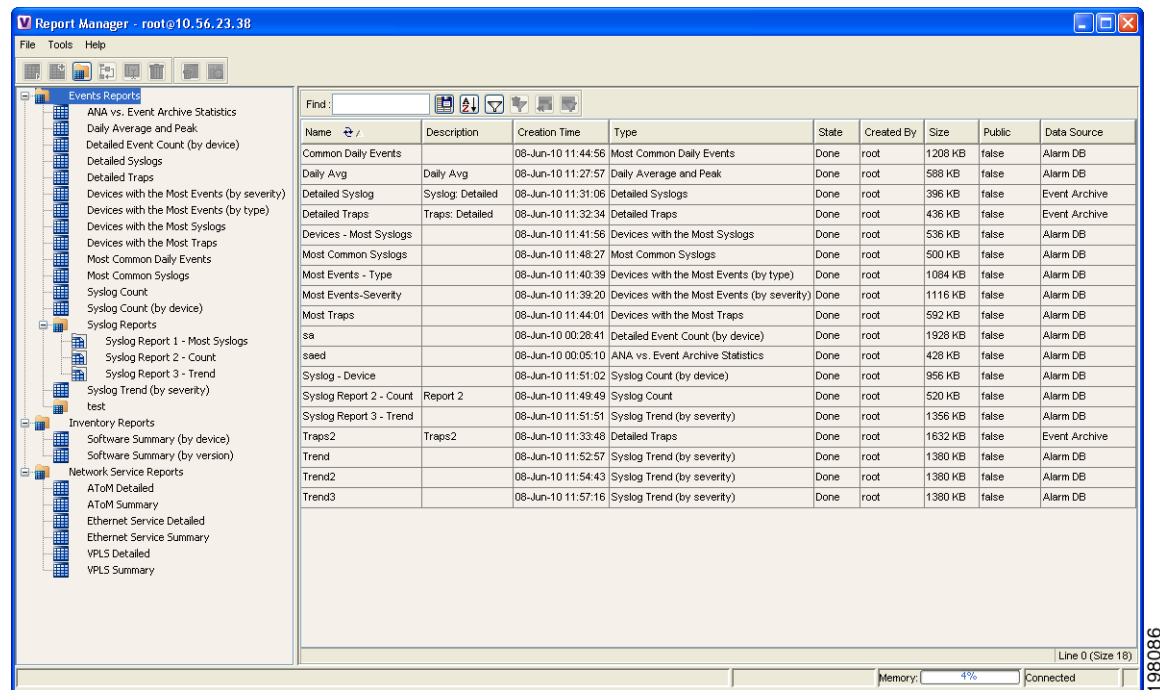
- If you select a folder, the content pane lists all reports that have been generated using any of the report types in that folder.
- If you select a report type, the content pane lists all reports that have been generated of that report type.

Content Pane

The content pane lists all reports generated for the folder or report type selected in the navigation tree. You can double-click a report to view the report in HTML format.

[Figure 10-3](#) shows an example of the content pane.

Figure 10-3 Reports Manager Content Pane



The screenshot shows the Reports Manager interface with a navigation tree on the left and a content pane on the right. The content pane displays a table of reports with columns: Name, Description, Creation Time, Type, State, Created By, Size, Public, and Data Source. The table lists various reports such as 'Common Daily Events', 'Daily Avg', 'Detailed Syslog', 'Detailed Traps', 'Devices - Most Syslogs', 'Most Common Syslogs', 'Most Events - Type', 'Most Events-Severity', 'Most Traps', 'sa', 'saed', 'Syslog - Device', 'Syslog Report 2 - Count', 'Syslog Report 3 - Trend', 'Traps2', 'Trend', 'Trend2', and 'Trend3'.

Name	Description	Creation Time	Type	State	Created By	Size	Public	Data Source
Common Daily Events		08-Jun-10 11:44:56	Most Common Daily Events	Done	root	1208 KB	false	Alarm DB
Daily Avg	Daily Avg	08-Jun-10 11:27:57	Daily Average and Peak	Done	root	588 KB	false	Alarm DB
Detailed Syslog	Syslog: Detailed	08-Jun-10 11:31:06	Detailed Syslogs	Done	root	396 KB	false	Event Archive
Detailed Traps	Traps: Detailed	08-Jun-10 11:32:34	Detailed Traps	Done	root	436 KB	false	Event Archive
Devices - Most Syslogs		08-Jun-10 11:41:56	Devices with the Most Syslogs	Done	root	536 KB	false	Alarm DB
Most Common Syslogs		08-Jun-10 11:48:27	Most Common Syslogs	Done	root	500 KB	false	Alarm DB
Most Events - Type		08-Jun-10 11:40:39	Devices with the Most Events (by type)	Done	root	1084 KB	false	Alarm DB
Most Events-Severity		08-Jun-10 11:39:20	Devices with the Most Events (by severity)	Done	root	1116 KB	false	Alarm DB
Most Traps		08-Jun-10 11:44:01	Devices with the Most Traps	Done	root	592 KB	false	Alarm DB
sa		08-Jun-10 00:28:41	Detailed Event Count (by device)	Done	root	1928 KB	false	Alarm DB
saed		08-Jun-10 00:05:10	ANA vs. Event Archive Statistics	Done	root	428 KB	false	Alarm DB
Syslog - Device		08-Jun-10 11:51:02	Syslog Count (by device)	Done	root	956 KB	false	Alarm DB
Syslog Report 2 - Count	Report 2	08-Jun-10 11:49:49	Syslog Count	Done	root	520 KB	false	Alarm DB
Syslog Report 3 - Trend		08-Jun-10 11:51:51	Syslog Trend (by severity)	Done	root	1356 KB	false	Alarm DB
Traps2	Traps2	08-Jun-10 11:33:48	Detailed Traps	Done	root	1632 KB	false	Event Archive
Trend		08-Jun-10 11:52:57	Syslog Trend (by severity)	Done	root	1380 KB	false	Alarm DB
Trend2		08-Jun-10 11:54:43	Syslog Trend (by severity)	Done	root	1380 KB	false	Alarm DB
Trend3		08-Jun-10 11:57:16	Syslog Trend (by severity)	Done	root	1380 KB	false	Alarm DB

[Table 10-4](#) describes the information displayed in the content pane for each report.

Table 10-4 Reports Manager Content Pane Information

Attribute	Description
Name	Name of the report. Double-click the report to view the report in HTML format.
Description	Brief description of the report.
Creation Time	Date and time when the report was generated.

Table 10-4 Reports Manager Content Pane Information (continued)

Attribute	Description
Type	Report type.
State	State of the report: Running, Done, or Failed.
Created By	User who created the report.
Size	Report size.
Public	Availability of the report to other users: • True—The report is available to all users. • False—The report is available to only the user who generated the report and the administrator.
Data Source	Source of the information for the report: ANA Database or Event Archive.

**Note**

Reports are purged from Cisco ANA after 90 days by default. This setting can be modified by changing the setting in Cisco ANA Manage. For more information, see the [Cisco Active Network Abstraction 3.7.1 Administrator Guide](#).

Right-Click Options

Right-click options are available for:

- [Navigation Pane Folders, page 10-6](#)
- [Navigation Pane Reports, page 10-7](#)
- [Content Pane Reports, page 10-7](#)

Navigation Pane Folders

[Table 10-5](#) describes the options available when you right-click a folder in the navigation pane.

Table 10-5 Report Manager Navigation Pane Folder Right-Click Options

Option	Description
New Folder	Creates a new folder.
Delete	Deletes a user-defined folder.
Rename	Renames a user-defined folder.
Move	Moves a user-defined folder.
Properties	Displays the Folder Properties window which lists the folder contents. For more information on the Reports Category Properties window, see Viewing Folder and Report Type Properties, page 10-36 .

Navigation Pane Reports

[Table 10-6](#) describes the options available when you right-click a report in the navigation pane.

Table 10-6 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	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.
Move	Moves a user-defined report.
Properties	Displays the Reports Type Properties window which includes a brief description of the report and enables you to generate the report. For more information on the Reports Type Properties window, see Viewing Report Properties, page 10-31 .

Content Pane Reports

[Table 10-7](#) describes the options available when you right-click a report in the content pane.

Table 10-7 Report Manager Content Pane Report Right-Click Options

Option	Description
View As	Displays the report in the selected format: - HTML - PDF - CSV - XLS - XML The default option, HTML, is displayed in bold font. For more information on viewing reports, see Viewing and Saving Reports, page 10-27 .
Rename	Renames the selected report.
Share or Unshare	Shares the selected reports or limits them to your viewing only. The option toggles between Share and Unshare, as appropriate for the selected reports. By default, the Share and Unshare options are available only to users with administrator access. These options are available to other users only if an administrator has enabled sharing in Cisco ANA Manage. For more information, see the Cisco Active Network Abstraction 3.7.1 Administrator Guide .
Delete Report	Deletes the selected reports.

Table 10-7 Report Manager Content Pane Report Right-Click Options (continued)

Option	Description
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

Cisco ANA provides reports related to:

- Events—See [Events Reports, page 10-8](#).
- Inventory—See [Inventory Reports, page 10-11](#).
- Network services—See [Network Service Reports, page 10-12](#).

Events Reports

[Table 10-8](#) describes the standard events report types provided by Cisco ANA.

Table 10-8 Standard Events Report Types

Report Name	Description
ANA vs. Event Archive Statistics	For each day in the specified time period, the number of each of the following items in the alarm database and the Cisco ANA Event Collector (AEC): • Syslogs • Traps • Tickets • Correlated events • Uncorrelated events • Nonnetwork events • Network-originated events • Network-originated and service events

Table 10-8 **Standard Events Report Types (continued)**

Report Name	Description
Daily Average and Peak	For each day of the specified time period, the peak number and average rate of syslogs and traps for each of the following time periods: • Second • Ten seconds • Minute • Hour • Day
Detailed Event Count (by device)	For each device, the following information for the specified time period: • Number of syslogs for each severity, including – Syslog type – Number of each syslog type • Number of traps for each severity, including: – Trap type – Number of each trap type • Number of tickets, including: – Ticket type – Number of each ticket type
Detailed Syslogs	For each device, the following information from the event archive for the specified time period: • Date and time of each syslog, in ascending order • Raw syslog The maximum number of syslogs retrieved for this report is 250,000.
Detailed Traps	For each device, the following information for the specified time period: • IP address • Time of trap • SNMP version • Generic or device-specific trap OID • Detailed trap description The maximum number of traps retrieved for this report is 250,000.

Table 10-8 **Standard Events Report Types (continued)**

Report Name	Description
Devices with the Most Events (by severity)	For the specified number of devices with the most events, the following information for each device for the specified time period: - Severity of the events associated with the device, sorted by severity - Number of events for each severity A pie chart presents the information by device and percentage in a graphical format
Devices with the Most Events (by type)	For the specified number of devices with the most events, the following information for each device for the specified time period: - Type of events associated with the device - Number of events received for each event type A pie chart presents the information by device and percentage in a graphical format.
Devices with the Most Syslogs	For the specified number of devices with the most syslogs, the number of syslog messages for each device for the specified time period. You can run this report on the Cisco ANA alarm database or the event archive. A pie chart presents the information by device and percentage in a graphical format.
Devices with the Most Traps	For the specified number of devices with the most traps, the number of traps associated with each device for the specified time period. You can run this report on the Cisco ANA database or the event archive. A pie chart presents the information by device and percentage in a graphical format.
Most Common Daily Events	For each day in the specified time period: - The specified number of most common syslogs, traps, tickets, and service events - The number of each type of syslog, trap, ticket, and service event - If selected, a pie chart that presents the events by percentage in a graphical format
Most Common Syslogs	Most common syslog messages and the number of each for the specified time period and devices. A pie chart presents the information by syslog message and percentage in a graphical format.

Table 10-8 **Standard Events Report Types (continued)**

Report Name	Description
Syslog Count	Number of syslog messages by type for the specified time period with the times of the first and last occurrences. A pie chart presents the information by syslog message and percentage in a graphical format.
Syslog Count (by device)	For each device, the type and number of each syslog message and the times of the first and last occurrences for each type. A pie chart presents the information by device and percentage in a graphical format.
Syslog Trend (by severity)	For the specified devices, the trend of specified syslog messages in graph format: • By priority • For the specified time period • At the specified intervals

Inventory Reports

Table 10-9 describes the standard inventory report types provided by Cisco ANA.

Table 10-9 **Standard Inventory Report Types**

Report Name	Description
Software Summary (by device)	For each device included in the report: • Device name • Element type • IP address • Serial number • Software version on the device • Name of image file
Software Summary (by version)	For each software version included in the report: • Number of devices running the version • Device names • Element types • Device IP address • Device serial number • Name of image file

Network Service Reports

Table 10-10 describes the standard network service report types provided by Cisco ANA.

Table 10-10 **Standard Network Service Report Types**

Report Name	Description
AToM Detailed	For each pseudowire in the report: • Pseudowire name • Pseudowire type • Business tag assigned to the pseudowire • Maps that contain the pseudowire • Pseudowire endpoints • Switching entities • Ethernet flow points • Connection termination points (TPs) You can filter report content by specifying part or all of the: • Pseudowire name • Pseudowire type • Business tag • Map name
AToM Summary	For each pseudowire in the report: • Pseudowire name • Pseudowire type • Business tag assigned to the pseudowire • Maps that contain the pseudowire You can filter the report content by specifying part or all of the: • Pseudowire name • Pseudowire type • Business tag • Map name

Table 10-10 **Standard Network Service Report Types (continued)**

Report Name	Description
Ethernet Service Detailed	For each Ethernet service in the report: • Ethernet service or Layer 2 VPN name • Business tag assigned to the Ethernet service or Layer 2 VPN instance • EVC name • Business tag assigned to the EVC • Maps that contain the Ethernet service or Layer 2 VPN • Edge EFPs associated with the EVC or Layer 2 VPN • EFD fragment names • EFD fragment types You can filter report content by specifying part or all of the: • Ethernet service name • EVC name • Ethernet service business tag • EVC business tag • Map name
Ethernet Service Summary	For each Ethernet service in the report: • Ethernet service or Layer 2 VPN name • Business tag assigned to the Ethernet service or Layer 2 VPN instance • EVC name • Business tag assigned to the EVC • Maps that contain the Ethernet service or Layer 2 VPN You can filter report content by specifying part or all of the: • Ethernet service name • EVC name • Ethernet service business tag • EVC business tag • Map name

Table 10-10 **Standard Network Service Report Types (continued)**

Report Name	Description
VPLS Detailed	For each VPLS or H-VPLS instance in the report: • VPLS or H-VPLS name • Business tag associated with the VPLS or H-VPLS instance • Maps that contain the VPLS or H-VPLS instance • VPLS forwarders that represent the device-level VPLS switching entities • Access pseudowire endpoints • Access EFPs • Core pseudowires You can filter report content by specifying part or all of the: • VPLS or H-VPLS name • Business tag • Map name
VPLS Summary	For each VPLS or H-VPLS instance in the report: • VPLS or H-VPLS name • Business tag assigned to the VPLS or H-VPLS instance • Maps that contain the VPLS or H-VPLS instance You can filter report content by specifying part or all of the: • VPLS or H-VPLS name • Business tag • Map name

Generating Reports

You can generate reports in any of the following ways:

- [Generating Reports from Report Manager, page 10-15](#)
- [Generating Reports from the Reports Menu, page 10-25](#)
- [Generating Reports from Cisco ANA NetworkVision, page 10-25](#)

Generating Reports from Report Manager

Cisco ANA provides three types of reports as described in [Report Categories, page 10-8](#). The information that you need to provide when generating a report depends on the report type. The following topics describe the information required to generate each report type:

- [Generating Events Reports, page 10-15](#)
- [Generating Inventory Reports, page 10-19](#)
- [Generating Network Service Reports, page 10-22](#)

Generating Events Reports

To generate an events report using Report Manager:

-
- Step 1** In Cisco ANA NetworkVision, Cisco ANA EventVision, or Cisco ANA Manage, choose **Reports > Report Manager**.
- Step 2** In the Report Manager window, choose **Events Reports > report-type**.
For information on the standard reports available for events, see [Table 10-8](#).
- Step 3** Generate the report in either of the following ways:
- Click **Run** in the toolbar.
 - Right-click the report type, then choose **Run**.

The Run Report dialog box is displayed as shown in [Figure 10-4](#). The fields displayed in the Run Report dialog box vary depending on the type of report.

Figure 10-4 Events Report - Run Report Dialog Box

Run Report - Most Common Syslogs

Report Settings

Report Name: Syslogs - Most Common

Description: Most common syslogs

Display: 8 Most Common Syslogs

Report Security: ☒ Private ☐ Public

Date Selection

☐ Last: 1 Days

☒ From date: Thu 10 / Jun / 2010 8 : 32 : 8

To date: Mon 14 / Jun / 2010 8 : 32 : 8

Device Selection

☒ Select Devices ☐ All Devices

Selected Devices:

- 3750E-48PD-AGG6
- 3750E-24TD-AGG1
- 3750E-48PD-AGG4
- 3750E-24TD-AGG2
- PE-East
- 10.56.101.241
- R1
- P-North
- ATF_ROUTER
- 3560-24TS-AGG7
- R2
- 3750G-24PS-AGG8

Add... Remove Clear

OK Cancel

Memory: 2% Connected

Step 4 In the Run Report dialog box, specify the report settings as described in [Table 10-11](#).

Table 10-11 Events Report - Run Report Dialog Box Fields

Option	Description
Report Settings	
Report Name	Enter a unique name for the report.
Description	Enter a brief description of the report.
Display	This field does not appear for all reports. Enter the number of items to be displayed in the generated report.
Include pie charts in report output	This field does not appear for all reports. Check this check box to view pie charts in the report with the standard numerical output.

Table 10-11 Events Report - Run Report Dialog Box Fields (continued)

Option	Description
Report Security	Indicate the level of security for the report by clicking the appropriate option: • Private—The report can be viewed and used only by the report creator and the administrator. • Public—The report can be viewed and used by all other users, regardless of whether the devices are listed in the report are in the user's scope. Note You can share reports with others only if sharing is enabled in Cisco ANA Manage. For more information, see the Cisco Active Network Abstraction 3.7.1 Administrator Guide.
Data Source	Depending on the report, this field: • Does not appear. • Is a read-only field. • Allows you to specify the source of information to use for the report: ANA Database or Event Archive.
Date Selection	
Last	Specify the length of time before the current date and time, and the unit of measure: seconds, minutes, hours, days, weeks, or months.
From Date To Date	Specify the date range for the report: 1. Click From Date. 2. In the From date field, enter the start date for the time period, or click the drop-down arrow to select the start date from a calendar. 3. Enter a time for the start date, using the format HH MM SS. 4. In the To Date field, enter the end date for the time period, or click the drop-down arrow to select the end date from a calendar. 5. Enter a time for the end date, using the format HH MM SS.
Version	
Version	This field does not appear for all reports. Specify the SNMP version to include in the report: All, 1, 2, or 3.

Table 10-11 **Events Report - Run Report Dialog Box Fields (continued)**

Option	Description
Generic	
Generic	This field does not appear for all reports. Specify the generic traps to include in the report: 1. Select the generic traps to include in the report: - All—Include all generic traps - 0—coldStart - 1—warmStart - 2—linkDown - 3—linkUp - 4—authenticationFailure - 5—egpNeighborLoss - 6—enterpriseSpecific 2. If you select generic type 6, enter the OIDs (comma separated) in the Display field.
Device Selection	
Select Devices	Select devices to include in the report: 1. Click Select Devices. 2. Click Add. 3. In the Add Network Element dialog box, select devices using either of the following methods: - To select a specific network element or category of network elements: a. Click Search. b. In the drop-down list, choose the search category: Element Category, Element Type, IP Address, System Name, or Vendor. c. In the Search field, enter the string that you want to match. d. Click Go. - To select from all network elements, click Show All. 4. In the Available Network Elements table, select the network elements that you want to include in the report. You can select multiple network elements at a time. 5. Click OK.
All devices	Click All Devices to include all devices in your scope in the report.

Table 10-11 Events Report - Run Report Dialog Box Fields (continued)

Option	Description
Intervals	
Intervals	This field does not appear for all reports. In the Grouped by drop-down list, choose the unit of time to use for tracking the trend: Seconds, Minutes, Hours, Days.
Severity	
Severity	This field does not appear for all reports. Check the check boxes of the syslog message severities to be included in the report: All, Critical, Major, Minor, Warning, Cleared, Information, and Indeterminate.
Syslog Messages	
Syslog Messages	This field does not appear for all reports. Specify the syslog messages to be included in the report: - To include selected syslog messages in the report, in the list of syslog messages on the left, select the required syslog messages, and then click Add Selected to move them to the list of syslog messages on the right. - To include all syslog messages in the report, click Add All. To find syslog messages that match a string, enter the string in the Find field. The list of syslog messages is automatically updated to include only those messages that contain the string you enter. Click the Sort Order button to sort the syslog messages alphabetically or in reverse alphabetic order.

Step 5 Click **OK**.

The report appears in the table in the content pane with a state of Running. 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 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 Cisco ANA NetworkVision, Cisco ANA EventVision, or Cisco ANA Manage, choose **Reports > Report Manager**.

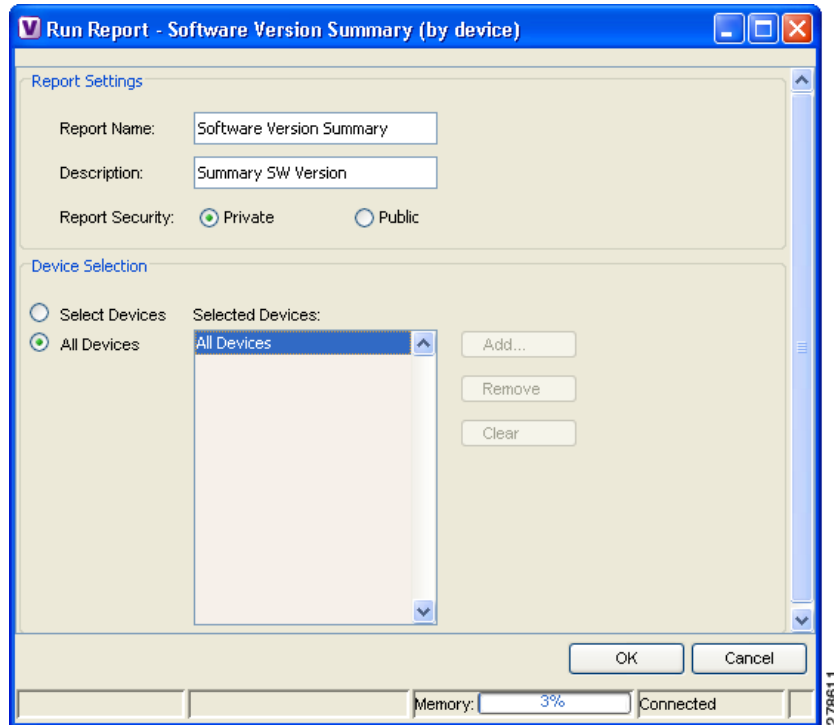
Step 2 In the Report Manager window, choose **Inventory Reports > report-type**.
For information on the standard reports available for inventory, see [Table 10-8](#).

Step 3 Generate the report in either of the following ways:

- Click **Run** in the toolbar.
- Right-click the report type, then choose **Run**.

The Run Report dialog box is displayed as shown in [Figure 10-5](#).

Figure 10-5 *Inventory Report - Run Report Dialog Box*



Step 4 Enter the required information in the Run Report dialog box as described in [Table 10-12](#).

Table 10-12 *Inventory Report - Run Report Dialog Box Fields*

Field	Description
Report Settings	
Report Name	Enter a unique name for the report.
Description	Enter a brief description of the report.

Table 10-12 *Inventory Report - Run Report Dialog Box Fields (continued)*

Field	Description
Report Security	Indicate the level of security for the report by clicking the appropriate option: • Private—The report can be viewed and used only by the report creator and the administrator. • Public—The report can be viewed and used by all other users, regardless of whether the devices are listed in the report are in the user's scope. Note You can share reports with others only if sharing is enabled in Cisco ANA Manage. For more information, see the Cisco Active Network Abstraction 3.7.1 Administrator Guide.
Device Selection	
Select Devices	Select devices to include in the report: 1. Click Select Devices. 2. Click Add. 3. In the Add Network Element dialog box, select devices using either of the following methods: – To select a specific network element or category of network elements: a. Click Search. b. In the drop-down list, choose the search category: Element Category, Element Type, IP Address, System Name, or Vendor. c. In the Search field, enter the string that you want to match. d. Click Go. – To select from all network elements, click Show All. 4. In the Available Network Elements table, select the network elements that you want to include in the report. You can select multiple network elements at a time. 5. Click OK.
All devices	Click All Devices to include all devices in your scope in the report.

Step 5 Click **OK**.

The report appears in the table in the content pane with a state of Running. 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 no data is found for the report, the report states that no results were found.

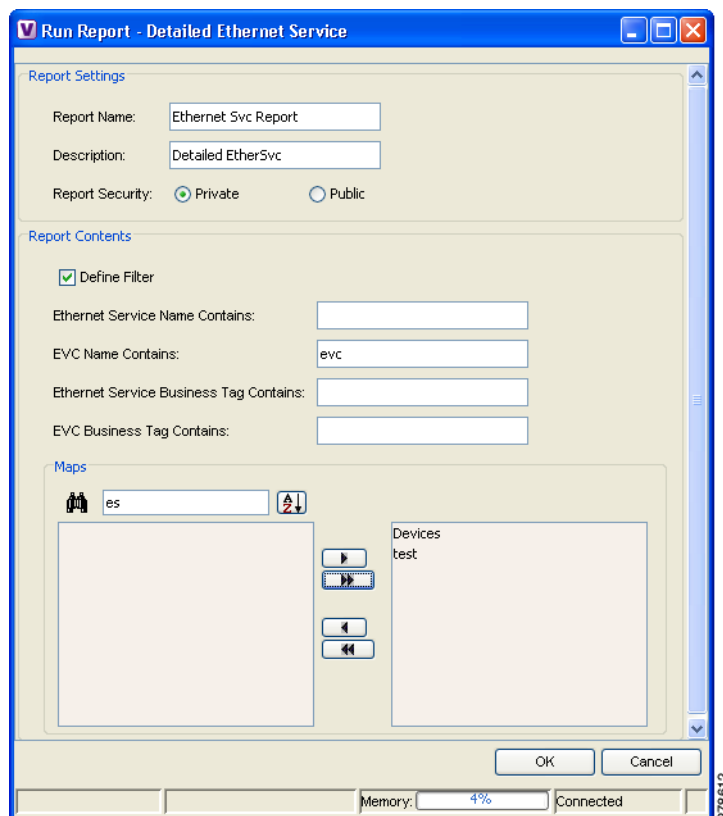
Generating Network Service Reports

To generate a network service report using Report Manager:

- Step 1** In Cisco ANA NetworkVision, Cisco ANA EventVision, or Cisco ANA Manage, choose **Reports > Report Manager**.
- Step 2** In the Report Manager window, choose **Network Service Reports > report-type**.
For information on the standard reports available for network services, see [Table 10-8](#).
- Step 3** Generate the report in either of the following ways:
 - Click **Run** in the toolbar.
 - Right-click the report type, then choose **Run**.

The Run Report dialog box is displayed as shown in [Figure 10-6](#).

Figure 10-6 Network Service Report - Run Report Dialog Box



Step 4 Enter the required information the Run Report dialog box as described in [Table 10-13](#).

Table 10-13 Network Service Report - Run Report Dialog Box Fields

Field	Description
Report Settings	
Report Name	Enter a unique name for the report.
Description	Enter a brief description of the report.
Report Security	Indicate the level of security for the report by clicking the appropriate option: - Private—The report can be viewed and used only by the report creator and the administrator. - Public—The report can be viewed and used by all other users, regardless of whether the devices are listed in the report are in the user's scope. Note You can share reports with others only if sharing is enabled in Cisco ANA Manage. For more information, see the Cisco Active Network Abstraction 3.7.1 Administrator Guide.
Report Contents - AToM Reports	
Define Filter	Check the Define Filter check box to enter criteria that must be matched for inclusion in the report.
Pseudowire Name Contains	Enter a string that must appear in the pseudowire name for the pseudowire to be included in the report.
Pseudowire Type Contains	Enter a string that must appear in the pseudowire type for the pseudowire to be included in the report.
Pseudowire Business Tag Contains	Enter a string that must appear in the pseudowire business tag for the pseudowire to be included in the report.
Maps	Specify the maps to include in the report: - To include specific maps in the report, in the list of maps on the left, select the required maps, and then click Add Selected to move them to the list of maps on the right. - To include all maps in the report, click Add All. To find maps that match a string, enter the string in the Find field. The list of maps is automatically updated to include only those maps that contain the string you enter. Click the Sort Order button to sort the maps alphabetically or in reverse alphabetic order.
Report Contents - Ethernet Service Reports	
Define Filter	Check the Define Filter check box to enter criteria that must be matched for inclusion in the report.
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.

Table 10-13 Network Service Report - Run Report Dialog Box Fields (continued)

Field	Description
Ethernet Service Business Tag Contains	Enter a string that must appear in the Ethernet service business tag for the Ethernet service to be included in the report.
EVC Business Tag Contains	Enter a string that must appear in the EVC business tag for the EVC to be included in the report.
Maps	Specify the maps to include in the report: - To include specific maps in the report, in the list of maps on the left, select the required maps, and then click Add Selected to move them to the list of maps on the right. - To include all maps in the report, click Add All. To find maps that match a string, enter the string in the Find field. The list of maps is automatically updated to include only those maps that contain the string you enter. Click the Sort Order button to sort the maps alphabetically or in reverse alphabetic order.
Report Contents - VPLS Reports	
Define Filter	Check the Define Filter check box to enter criteria that must be matched for inclusion in the report.
VPLS Name Contains	Enter a string that must appear in the VPLS name for the VPLS or H-VPLS to be included in the report.
VPLS Business Tag Contains	Enter a string that must appear in the VPLS business tag for the VPLS or H-VPLS to be included in the report.
Maps	Specify the maps to be included in the report: - To include specific maps in the report, in the list of maps on the left, select the required maps, and then click Add Selected to move them to the list of maps on the right. - To include all maps in the report, click Add All. To find maps that match a string, enter the string in the Find field. The list of maps is automatically updated to include only those maps that contain the string you enter. Click the Sort Order button to sort the maps alphabetically or in reverse alphabetic order.

Step 5 Click **OK**.

The report appears in the table in the content pane with a state of Running. 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 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.

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 [Table 10-11](#).
- Step 3** Click **OK**.
- Step 4** In the Running Report dialog box, specify the 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 5** Click **OK**.
- Depending on your selections in [Step 4](#), the Report Manager window is displayed, the report is displayed, or the report is available for viewing at a later time.
-

Generating Reports from Cisco ANA NetworkVision

Cisco ANA NetworkVision enables you to run reports on selected devices from the map and list views.

To generate a report from Cisco ANA NetworkVision:

-
- Step 1** In Cisco ANA NetworkVision, 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 [Table 10-11](#).
The devices that you select in the navigation pane or content pane are automatically included in the report.
- Step 4** Click **OK**.
- Step 5** In the Running Report dialog box, specify the 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 5](#), the Report Manager window is displayed, the report is displayed, or the report is available for viewing at a later time.

Managing Reports

Cisco ANA provides the following options for working with reports:

- [Managing the Maximum Number of Concurrent Reports, page 10-26](#)
- [Viewing and Saving Reports, page 10-27](#)
- [Renaming Reports, page 10-28](#)
- [Sharing Reports, page 10-29](#)
- [Moving Reports Between Folders, page 10-30](#)
- [Deleting Reports, page 10-30](#)
- [Viewing Report Properties, page 10-31](#)

Managing the Maximum Number of Concurrent Reports

Cisco ANA enables you to run multiple reports at the same time, with the maximum number of concurrent reports 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 Active Network Abstraction 3.7.1 Administrator Guide](#).

Viewing and Saving Reports

You can view any reports that appear in the Report Manager content pane as long as the state is Done. After viewing a report, you can save it in any of the available formats.

**Note**

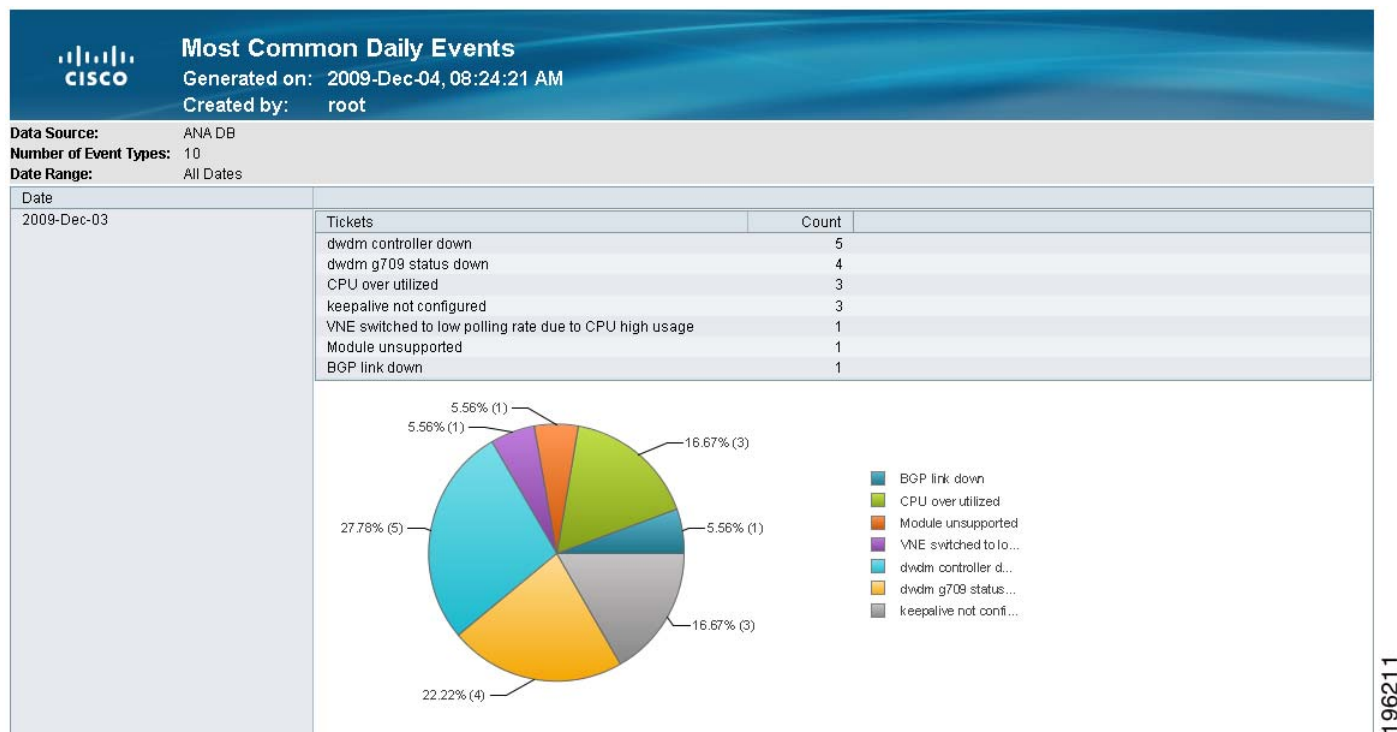
Reports are purged from Cisco ANA after 90 days by default. This setting can be modified by changing the setting in Cisco ANA Manage. For more information, see the [Cisco Active Network Abstraction 3.7.1 Administrator Guide](#).

To view and save a report:

-
- Step 1** Choose **Reports > Report Manager**.
- Step 2** In the navigation pane, locate the required report in either of the following ways:
- Select the folder containing the report.
 - Select the report type.
- Step 3** In the content pane, right-click the report, then choose **View As > format** where *format* is one of the following:
- **HTML**—Displays the report in a browser window. Clicking a column heading in the report sorts the report by that value; clicking the column heading again sorts the data in the reverse order. HTML is the default format.
 - **PDF**—Displays a PDF version of the report.
 - **CSV**—Creates a CSV version of the report that you can either save to a specific location or view using another application. The CSV version contains only the report data; it does not contain the header information, layout, or formatting information that is available in other formats.
 - **XLS**—Creates an XLS version of the report that you can either save to a specific location or view using another application, such as Microsoft Excel.
 - **XML**—Creates an XML version of the report that you can either save to a specific location or view using an XML editor or viewer.

[Figure 10-7](#) is an example of the Most Common Daily Events report in HTML format. The data is sorted by the Count column, in descending order.

Figure 10-7 Most Common Daily Events Report Example



Step 4 Save the report as required.

Renaming Reports

You can rename:

- Any report type that you defined.
- Any generated report that you have access to.

You cannot rename any of the Cisco ANA 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.

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 navigation pane, locate the required report in either of the following ways:

- Select the folder containing the report.
- Select the report type.

Step 3 In the content pane, right-click the report that you want to rename, then choose **Rename**.

Step 4 In the Rename Report dialog box, enter the new name for the report.

Step 5 Click **OK**.

The content pane is refreshed and the report is displayed with the new name.

Sharing Reports

Cisco ANA 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 Cisco ANA Manage. For more information, see the [Cisco Active Network Abstraction 3.7.1 Administrator Guide](#).

Sharing a Report

To share access to a report that you generated:

Step 1 Choose **Reports > Report Manager**.

Step 2 In the navigation pane, locate the required report in either of the following ways:

- Select the folder containing the report.
- Select the report type.

Step 3 In the content pane, right-click the report that you want to share, then choose **Share**.

The report is available to all system users for viewing and using.

Limiting Access to a Report

To limit access to a report that you generated and subsequently shared:

-
- Step 1** Choose **Reports > Report Manager**.
- Step 2** In the navigation pane, locate the required report in either of the following ways:
- Select the folder containing the report.
 - Select the report type.
- Step 3** In the content pane, right-click the report that you want to limit access to, then choose **Unshare**.
The report can be viewed and used by only you and the administrator.
-

Moving Reports Between Folders

You can move a report type that you have defined from the current folder to another folder in the navigation tree.

**Note**

You cannot move a standard report type from one folder to another.

To move a report type to a new folder:

-
- Step 1** Choose **Reports > Report Manager**.
- Step 2** In the navigation tree, select the required report that you have defined.
- Step 3** Do either of the following:
- Click **Move** in the toolbar.
 - Right-click the report, then choose **Move**.
- Step 4** In the Move To dialog box, select the folder to which you want to move the report.
- Step 5** Click **OK**.
The Report Manager window is refreshed and the report appears in the specified folder.
-

Deleting Reports

You can delete reports to which you have access.

To delete a report:

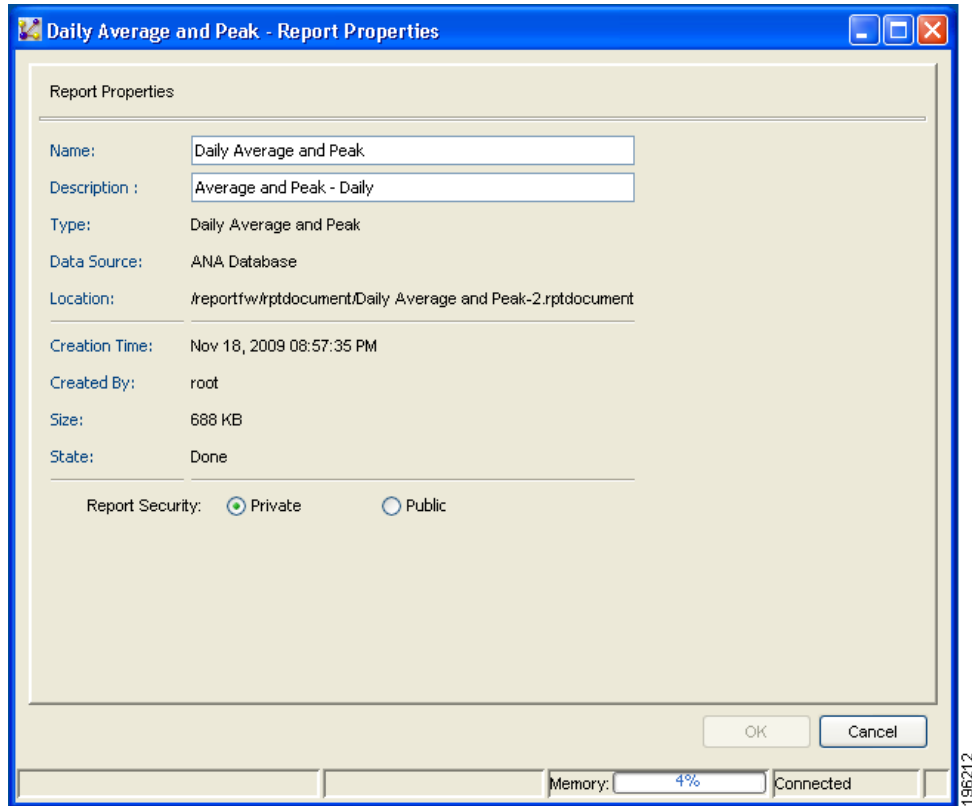
-
- Step 1** Choose **Reports > Report Manager**.
- Step 2** In the navigation pane, locate the required report in either of the following ways:
- Select the folder containing the report.
 - Select the report type.

- Step 3** In the content pane, select the required report.
- Step 4** Delete the report in either of the following ways:
- Right-click the report, then choose **Delete Report**.
 - Click **Delete Report** in the toolbar.
- Step 5** In the Delete Report confirmation window, click **Yes** to confirm deletion.
- The Report Manager window is refreshed and the deleted report no longer appears.
-

Viewing Report Properties

The Report Properties dialog box enables you to view the report settings and to modify some of them. To view report properties, and optionally change the name, description, or access:

-
- Step 1** Choose **Reports > Report Manager**.
- Step 2** In the navigation pane, locate the required report in either of the following ways:
- Select the folder containing the report.
 - Select the report type.
- Step 3** In the content pane, right-click the selected report, then choose **Properties**.
- The Report Properties dialog box is displayed, as shown in [Figure 10-8](#).

Figure 10-8 Report Properties Dialog Box

The Report Properties dialog box contains the following information about the report:

- Name
- Description
- Type
- Source of the information
- Location of the report on the gateway
- Date and time it was created
- User who created it
- Size
- State
- Access

Step 4 Change the information in the following fields as required:

- Name
- Description

Step 5 Click **OK**.

Defining Report Types

You can modify any of the report types provided by Cisco ANA so that it better suits your needs and environment. This is extremely beneficial if you generate a particular type of report for specific devices or events on a regular basis.

To define a report type:

-
- Step 1** Choose **Reports > Report Manager**.
 - Step 2** In the navigation pane, select the existing report type on which you want to base your report type and then do either of the following:
 - Right-click the existing report type, then choose **Define Report of This Type**.
 - Click **Define Report of This Type** in the toolbar.
 - Step 3** In the Define report of type dialog box, specify the options using the information in [Table 10-11](#).
 - Step 4** In the Location field, do either of the following:
 - Use the specified reports folder.
 - Click **Browse** to select a different folder:
 - a. In the Move to dialog box, select the required folder.
 - b. Click **OK**.
 - Step 5** Click **OK**.

The newly defined report type appears in the navigation tree in the specified folder.

Working with Report Folders

Cisco ANA provides the following options for working with report folders:

- [Creating Folders, page 10-34](#)
- [Moving Folders, page 10-34](#)
- [Renaming Folders, page 10-35](#)
- [Deleting Folders, page 10-35](#)
- [Viewing Folder and Report Type Properties, page 10-36](#)

Creating Folders

Cisco ANA enables you to create additional report folders in Report Manager.

To create a report folder:

-
- Step 1** Choose **Reports > Report Manager**.
- Step 2** Select the location of the new folder as follows:
- To create a folder at the top level in the hierarchy (at the same level as the Events Reports, Inventory Reports, and Network Service Reports folders), click in the navigation pane.
 - To create a folder in an existing folder, select the folder.
- Step 3** Depending on your selection in [Step 2](#), continue with one of the following:
- Click **New Folder** in the toolbar.
 - Right-click the folder, then choose **New Folder**.
- Step 4** In the New Folder dialog box, enter a name for the folder.
- Step 5** Click **OK**.

The navigation pane is refreshed and the new folder is displayed.

Moving Folders

Cisco ANA enables you to move folders that you have created in Report Manager. You cannot move the Events Reports, Inventory Reports, or Network Service Reports folder.

To move a report folder:

-
- Step 1** Choose **Reports > Report Manager**.
- Step 2** In the navigation pane, select the folder you want to move, and then do one of the following:
- Click **Move** in the toolbar.
 - Right-click the folder, then choose **Move**.
- Step 3** In the Move To dialog box, select the location where you want the folder to reside.



Tip To move the folder to the same level as the folders provided by Cisco ANA, click the white space in the Move To dialog box so that none of the top-level folders are selected.

- Step 4** Click **OK**.

The navigation pane is refreshed and the folder is displayed in the new location.

Renaming Folders

Cisco ANA enables you to rename folders that you have created in Report Manager. You cannot:

- Rename a folder that resides at the highest level in the hierarchy, such as the Events Reports, Inventory Reports, or Network Service Reports folder.
- Use the same name for different folders that reside at the same level in the hierarchy.

To rename a report folder:

-
- Step 1** Choose **Reports > Report Manager**.
- Step 2** In the navigation pane, select the folder you want to rename, and then do one of the following:
- Click **Rename** in the toolbar.
 - Right-click the folder, then choose **Rename**.
- Step 3** In the Rename Folder dialog box, enter the new name for the folder.
- Step 4** Click **OK**.

The navigation pane is refreshed and the folder is displayed with the new name.

Deleting Folders

You can delete folders that you have created in Report Manager if they are empty. You cannot delete the following folders:

- Events Reports folder
- Inventory Reports folder
- Network Service Reports folder
- User-created folders that contain other folders or report types

To delete a report folder:

-
- Step 1** Choose **Reports > Report Manager**.
- Step 2** In the navigation pane, select the folder you want to delete, and then do one of the following:
- Click **Delete** in the toolbar.
 - Right-click the folder, then choose **Delete**.
- Step 3** In the Confirm Folder Delete dialog box, click **Yes** to confirm the deletion.

The navigation pane is refreshed and the folder no longer appears.

Viewing Folder and Report Type Properties

The following topics describe how to view properties for folders and report types:

- [Viewing Report Folder Properties, page 10-36](#)
- [Viewing Report Type Properties, page 10-37](#)

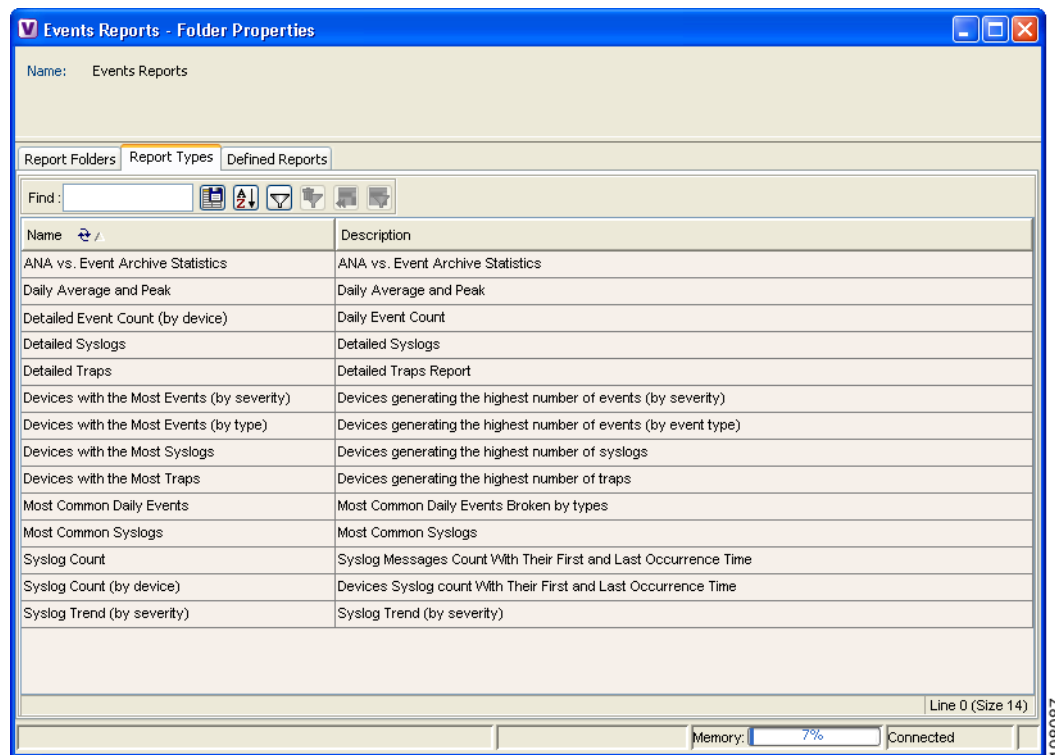
Viewing Report Folder Properties

The Report Properties window enables you to view report properties and to add folders.

To view report properties:

-
- Step 1** Choose **Reports > Report Manager**.
- Step 2** In the navigation pane, right-click the required folder, then choose **Properties**.
The Folder Properties window is displayed, as shown in [Figure 10-9](#).

Figure 10-9 Folder Properties



[Table 10-14](#) describes the information that is displayed in each tab, depending on the folder's contents.

Table 10-14 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 Cisco ANA:
- 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.
 - Cisco ANA-provided report type—The Report Type Properties window is displayed with the report name and description. Click **Run** to generate the report.
- Step 2** Click the upper right corner to close the window.
-



CHAPTER 11

Using Cisco ANA PathTracer to Diagnose Problems

Cisco ANA enables you to view a network path between two network objects using Cisco ANA PathTracer in the following types of networks:

- Circuit-switched network, such as Frame Relay or ATM
- Packet-switched networks, such as Ethernet and IP

In addition, beginning with Cisco ANA 3.7, you can specify either IPv4 or IPv6 addresses for the source or destination of a path trace.

The following topics describe the Cisco ANA PathTracer working environment and the functionality available when using Cisco ANA PathTracer:

- [User Roles Required to Work with Cisco ANA PathTracer, page 11-2](#)
- [Cisco ANA PathTracer Overview, page 11-2](#)
- [Using Cisco ANA PathTracer, page 11-3](#)
- [Cisco ANA PathTracer Multipath Window, page 11-12](#)
- [Cisco ANA PathTracer Single-Path Window, page 11-16](#)
- [Viewing Path Information, page 11-20](#)
- [Saving and Opening Cisco ANA PathTracer Map Files, page 11-20](#)
- [Saving Cisco ANA PathTracer Counter Values, page 11-21](#)
- [Rerunning a Path and Comparing Results, page 11-22](#)
- [Viewing Q-in-Q Path Information, page 11-22](#)
- [Viewing L2TP Path Information, page 11-23](#)
- [Using Cisco ANA PathTracer in MPLS Networks, page 11-24](#)

User Roles Required to Work with Cisco ANA PathTracer

Table 11-1 identifies the roles that are required to work with Cisco ANA PathTracer. Cisco ANA 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 device-based tasks (tasks that do affect devices), authorization is based on the default permission that is assigned to your account. That is, whether the device 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 Active Network Abstraction 3.7.1 Administrator Guide](#).

Table 11-1 Default Permission/Security Level Required for Working with Cisco ANA PathTracer

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Launch a path trace	—	—	—	—	X
View path information	—	—	—	—	X
Save Cisco ANA PathTracer map files	—	—	—	—	X
Save Cisco ANA PathTracer counter values	—	—	—	—	X
Rerun a path and compare results	—	—	—	—	X

Cisco ANA PathTracer Overview

Cisco ANA PathTracer enables end-to-end route tracing to be performed with informative performance information displayed simultaneously for the multiple networking layers. Upon receiving a path's start and endpoint, Cisco ANA PathTracer visually traces the route through the network. For example, in an ATM network environment, Cisco ANA 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 ANA 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 ID.

Cisco ANA PathTracer can also be used for the following MPLS and Carrier Ethernet technologies:

- Path trace across VLANs—Follows the path based on forwarding table, which means the trace follows ports in Forwarding STP state.
- Path trace across Q-in-Q—Creates a single path trace (if the MAC address is learned) or 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 ID. A

MAC/VLAN path trace can be conducted from a CE-VLAN interface across an SP-VLAN, that is, across Q-in-Q configurations with the CE-VLAN ID as inner VLAN ID and Cisco ANA PathTracer detecting the outer SP-VLAN ID that encapsulates the CE-VLAN.

- Path trace across 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 path trace—A multi-point MAC/VLAN path trace can be conducted on CE-VLANs across service provider VPLS transport from a VLAN interface that attaches to the VPLS.
- MAC address not reachable— If Cisco ANA PathTracer cannot complete a MAC/VLAN path trace to a specified destination MAC address across an MPLS core, VPLS, or H-VPLS, then Cisco ANA PathTracer displays the portion of the path that Cisco ANA PathTracer was able to trace toward the destination MAC address.
- Simulated Ethernet frame—Cisco ANA 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.

Cisco ANA derives the various paths on the network from its up-to-date knowledge of the network. After a user has selected a source and destination, Cisco ANA PathTracer finds and retrieves the path of a specified service. 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.

Cisco ANA PathTracer enables you to view multiple paths between the source and the destination in the Cisco ANA PathTracer multipath window, or to view a selected single-path in the Cisco ANA PathTracer single-path window.

Using Cisco ANA PathTracer

Cisco ANA PathTracer can be launched from a bridge, switching entity, Ethernet interface, Ethernet flow point, VLAN interface, ATM VC, DLCI, or IP interface entry point. 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.

To view a specific path, you must specify an initial point, such as a VPI/VCI, DLCI, VLAN, Ethernet port, or IP interface and optionally a destination, such as an IP or MAC address. If you specify VC or DLCI information, which ends in a router, Cisco ANA PathTracer finds the next hop according to the destination IP address. If you do not specify a destination IP or MAC address, Cisco ANA PathTracer uses the default gateway in the router. The business tags that have been referred to the physical or logical entities are also displayed.



Note

The path can also be opened if there is a business tag attached to an endpoint that can be used as the starting point for opening the Cisco ANA PathTracer.

The Cisco ANA PathTracer tool provides two windows in which to view the path:

- [Cisco ANA PathTracer Multipath Window, page 11-12](#)—Displays all the paths available between the selected source and destination.
- [Cisco ANA PathTracer Single-Path Window, page 11-16](#)—Displays a single path available between the selected source and destination, as well as the subscribers and properties.

Cisco ANA PathTracer Right-Click Menu Options

Cisco ANA PathTracer is launched by using right-click menu options. [Table 11-2](#) identifies the launching points for the different types of elements.

Table 11-2 *Cisco ANA PathTracer Right-Click Menu Options*

Element	Location
Affected Parties	- Inventory window - Ticket Properties window (Affected Parties tab)
Bridge	Inventory window
Business tag	The path can be found using a business tag, which is attached to the VPI/VCI, or using an IP interface by entering its key; it can then be opened from the Find Business Tag dialog box.
Ethernet flow point	Map view (Ethernet Flow Domain Properties window)
IP interface	- Inventory window - Affected entry
Layer 2 MPLS Tunnel	Inventory window
MPLS-TE Tunnel	Inventory window
Port	Inventory window
Site	Map view
Switching entity	Map view
VC Cross Connect Table	Inventory window (Cross Connect dialog box)
VC Table	Inventory window (VC Table dialog box)
VLAN	- Navigation pane - Map view

Starting a Path Trace

You can start a path trace in the following ways:

- [From the Map View, page 11-5](#)
- [From Logical or Physical Inventory, page 11-7](#)

From the Map View

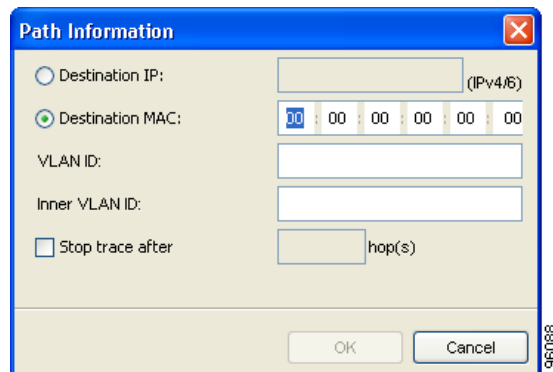
To start a path trace from the map view:

- Step 1** In the Cisco ANA NetworkVision map view, 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 and then drill down to a switching entity or Ethernet flow point.
 - b. Right-click the required item.
 - c. 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 and then drill down to the required site.
 - b. Right-click the site.
 - c. 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.
 - d. Choose **PathTracer > From Here to Destination** or **PathTracer > Start Here**.

The next step depends on your choice in [Step 1](#):

- If you chose **PathTracer > From Here to Destination**, the Path Information dialog box is displayed ([Figure 11-1](#)). Continue with [Step 2](#).
- If you chose **PathTracer > Start Here**, continue with [Step 3](#).

Figure 11-1 Path Information Dialog Box



- Step 2

To specify a destination:

a.

In the Path Information dialog box, enter the required information, as described in [Table 11-3](#).



Note

Depending on the launch point, the Path Information dialog box might not contain all of the following fields.

Table 11-3 Cisco ANA 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 ANA 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 chose **Start Here**, navigate to the destination interface, port, or bridge, right-click it, and choose **End Here**.

The PathTracer multipath window is displayed showing the paths that were found. For more information about this window, see [Cisco ANA PathTracer Multipath Window, page 11-12](#).

- Step 4

If the multipath window displays more than one path, select a path in the Paths pane.



Note

If multiple paths are selected in the Paths pane, they will be opened. If nothing is selected in the Paths pane, then all the available paths will be opened automatically, and each one will be displayed in a separate PathTracer single-path window.

- Step 5

On the multipath window toolbar, click **Cisco PathTracer**. The PathTracer single-path window is displayed showing the end-to-end path.
- For more information about the single-path window, see [Cisco ANA PathTracer Single-Path Window, page 11-16](#).

From Logical or Physical Inventory

To start a path trace from logical or physical inventory:

-
- Step 1** In Cisco ANA NetworkVision, open the inventory window for the required device using one of the following methods:
- Double-click a device or element in the navigation pane or in a map.
 - Right-click a device or element in the navigation pane or in a map and choose **Inventory**.
- Step 2** Select one of the following launch points in logical or physical inventory:
- IP Interface
 - VLAN Bridge
 - Port
- Step 3** Right-click the selected item and choose one of the following:
- **PathTracer > From Here to Destination**—If you choose this option, continue with [Step 2 in From the Map View, page 11-5](#).
-  **Note** If you select an IP interface as the launch point, the right-click menu displays IPv4 and IPv6 options. These options are enabled or dimmed, depending on whether the IP interface has an IPv4 IP address, an IPv6 address, or both IPv4 and IPv6 addresses. For an example, see [Figure 11-3](#).
-
- **PathTracer > Start Here**—If you choose this option, continue with [Step 3 in From the Map View, page 11-5](#).
-

Examples of Launching Cisco ANA PathTracer

The following topics provide examples for launching Cisco ANA PathTracer from different points in Cisco ANA NetworkVision:

- [Using an Ethernet Flow Point, page 11-7](#)
- [Using an IP Interface, page 11-8](#)
- [Using a VLAN Bridge, page 11-10](#)
- [Using an Ethernet Port, page 11-11](#)
- [Using a Pseudowire, page 11-11](#)

Using an Ethernet Flow Point

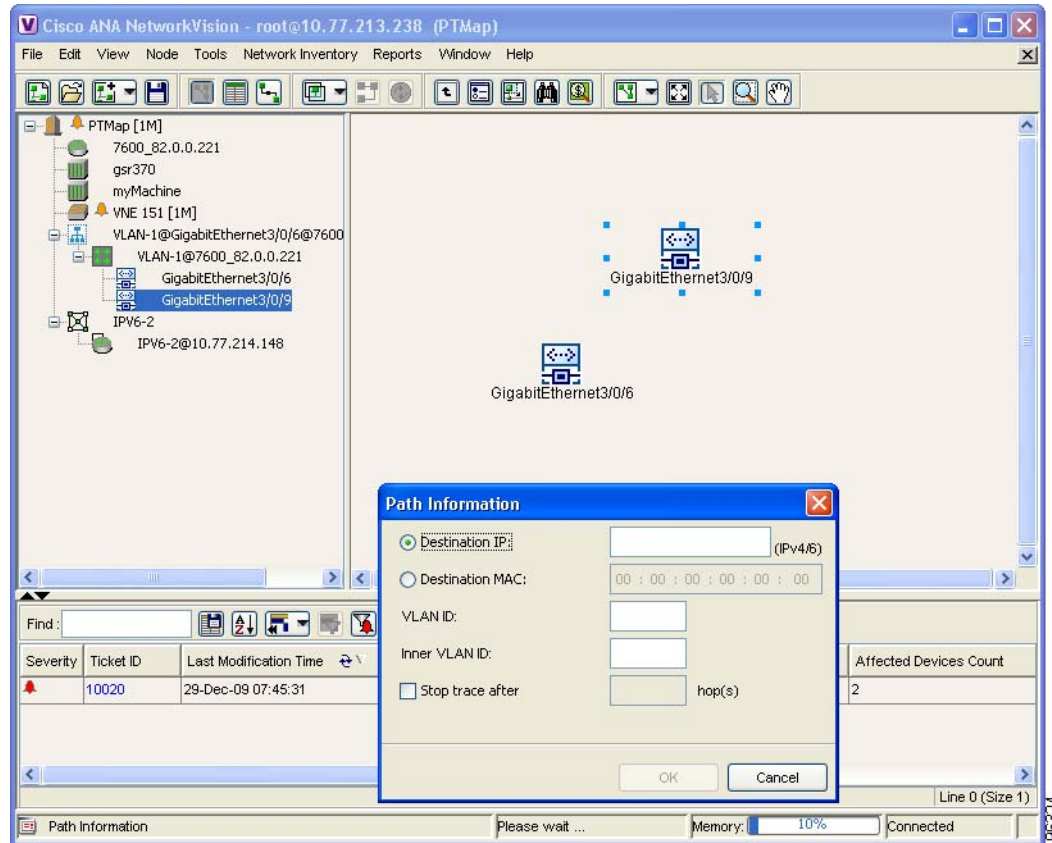
A network VLAN is required for you to start a path trace using an Ethernet flow point.

To launch a path trace from an Ethernet flow point:

-
- Step 1** In the Cisco ANA NetworkVision navigation pane or map pane, select the required network VLAN.
- Step 2** Navigate down to an Ethernet flow point and right-click it.

- Step 3** Choose **PathTracer > From Here to Destination**. The Path Information dialog box is displayed as shown in [Figure 11-2](#).

Figure 11-2 Ethernet Flow Point Path Trace Example



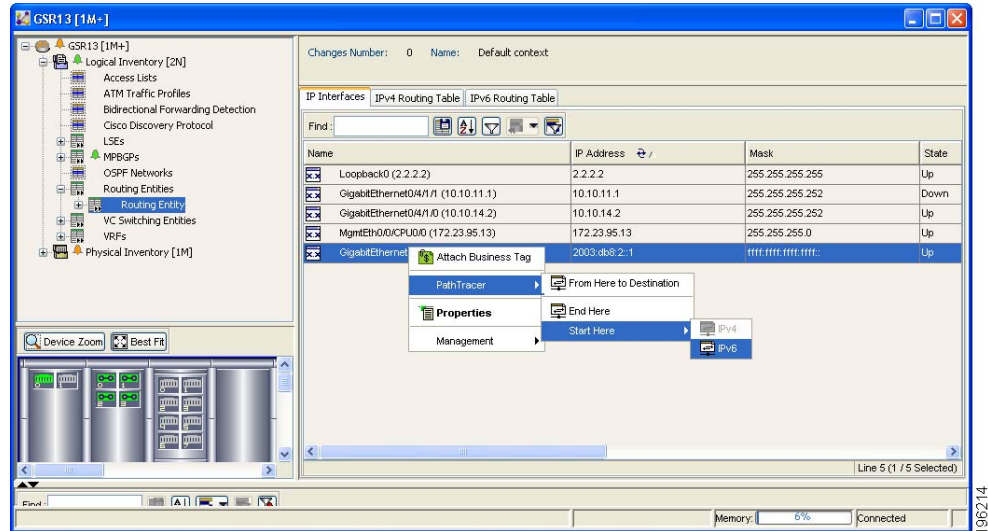
- Step 4** Specify the destination and maximum number of hops using the information in [Table 11-3](#).
- Step 5** Click **OK**. The Cisco ANA PathTracer window is displayed with the resulting path trace.

Using an IP Interface

Both IPv4 and IPv6 addresses are supported as valid path trace sources and destinations as illustrated in the following procedure.

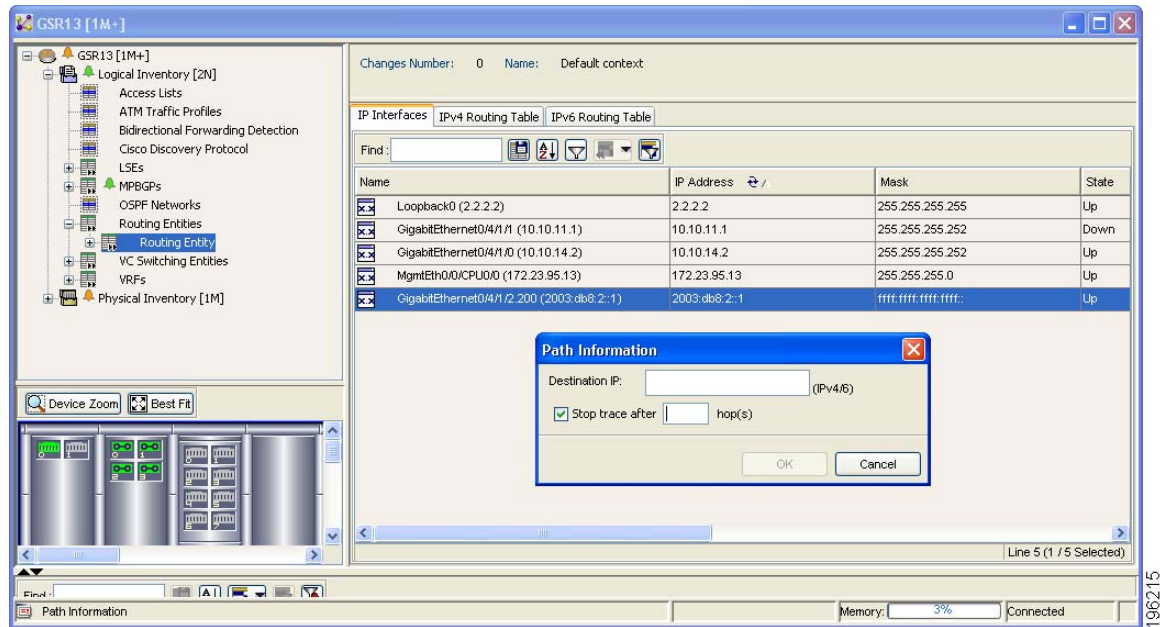
To launch a path trace from an IP interface:

- Step 1** In logical inventory, select the required IP interface (**Logical Inventory > Routing Entities > Routing Entity > ip-interface**).
- Step 2** Right-click the selected interface.
- The right-click menu displays IPv4 and IPv6 options. These options are enabled or dimmed, depending on whether the IP interface has an IPv4 address, an IPv6 address, or both IPv4 and IPv6 addresses. See [Figure 11-3](#).

Figure 11-3 IP Interface Path Trace Launch Point

Step 3 Choose **PathTracer > From Here to Destination**.

The Path Information dialog box is displayed as shown in Figure 11-4.

Figure 11-4 IP Interface Path Trace Launch Point Path Information Dialog Box

Step 4 In the Destination IP field, enter the IPv4 or IPv6 address.

Step 5 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 6 Click **OK**. The Cisco ANA PathTracer window appears, displaying the resulting path trace.

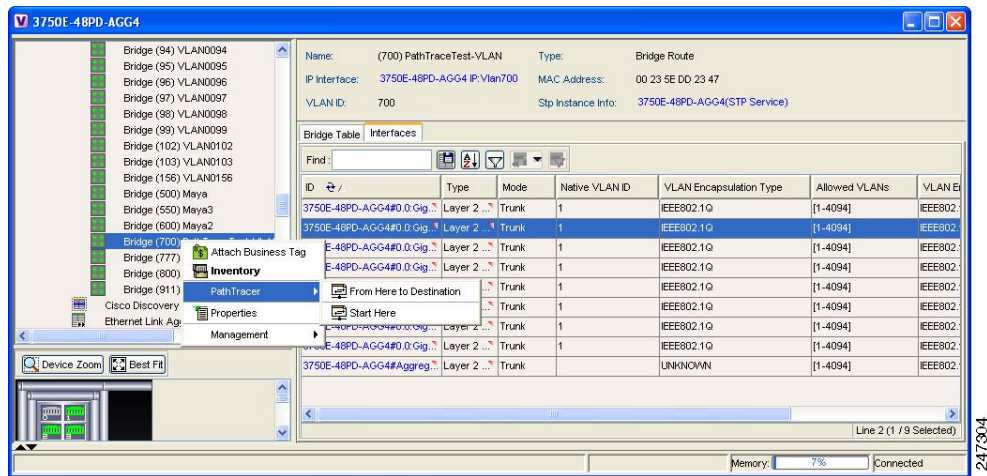
Using a VLAN Bridge

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, select the required bridge (**Logical Inventory** > **Bridges** > *bridge*).
- Step 2** Right-click the selected bridge, then choose one of the following options as shown in [Figure 11-5](#):
 - **PathTracer** > **From Here to Destination**
 - **PathTracer** > **Start Here**

Figure 11-5 VLAN Bridge Path Trace Launch Point



- Step 3** If you chose **From Here to Destination** in [Step 2](#), the Path Information dialog box is displayed. Specify the required destination using the information in [Table 11-3](#).
- Step 4** If you chose **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.

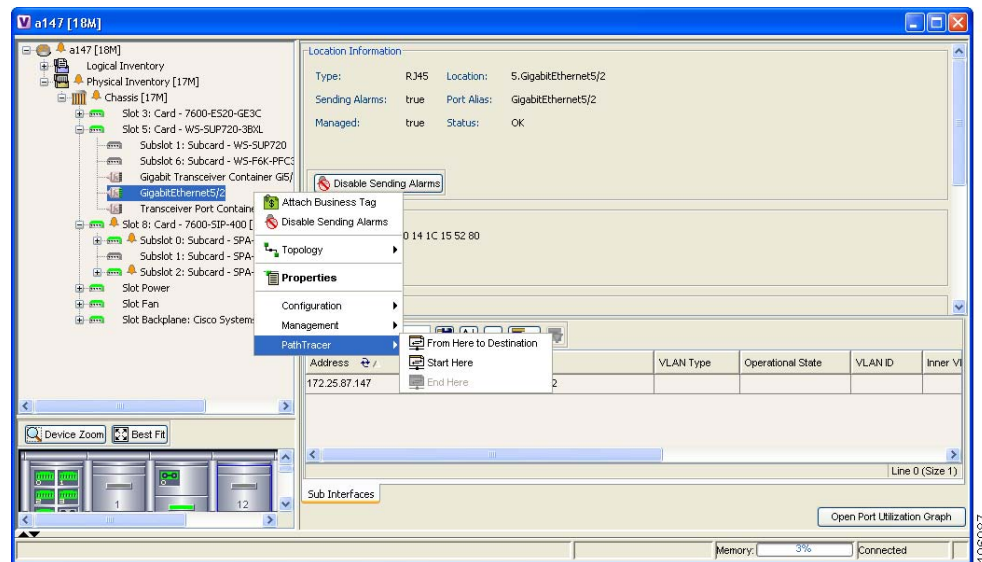
The Cisco ANA PathTracer window is displayed with the resulting path trace.

Using an Ethernet Port

To launch a path trace from an Ethernet port:

- Step 1** In physical inventory, select the required port (**Physical Inventory > Chassis > slot > subslot > port**).
- Step 2** Right-click the selected port and choose one of the following as shown in [Figure 11-6](#):
 - **PathTracer > From Here to Destination**
 - **PathTracer > Start Here**

Figure 11-6 Ethernet Port Path Trace Launch Point



- Step 3** Depending on your choice in [Step 2](#), specify the required destination information or select the path trace end point.

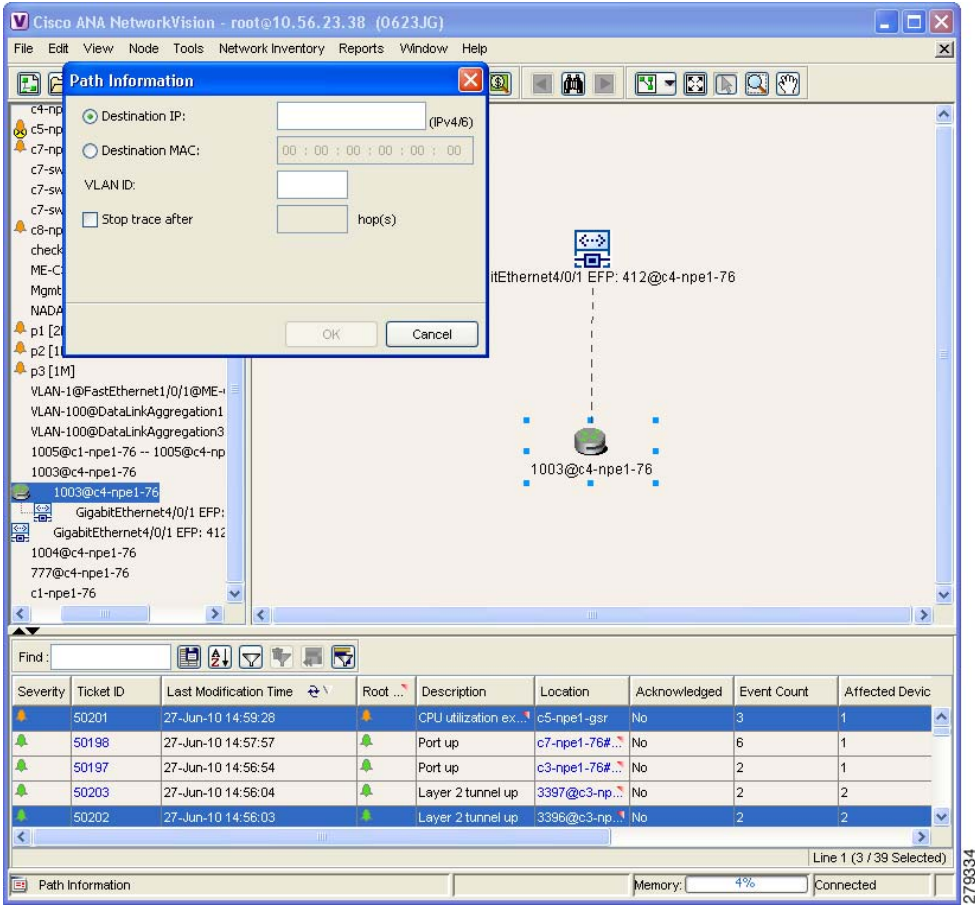
The Cisco ANA PathTracer window appears, displaying the resulting path trace.

Using a Pseudowire

To launch a path trace from network pseudowire:

- Step 1** In the Cisco ANA NetworkVision navigation pane or map pane, select the required network pseudowire.
- Step 2** Navigate down to the required pseudowire endpoint and right-click it.
- Step 3** In the right-click menu, choose **PathTracer > From Here to Destination**.

The Path Information dialog box is displayed as shown in [Figure 11-7](#).

Figure 11-7 Path Information Dialog Box

Step 4 Specify the destination using the information in [Table 11-3](#).
The Cisco ANA PathTracer window appears, displaying the resulting path trace.

Cisco ANA PathTracer Multipath Window

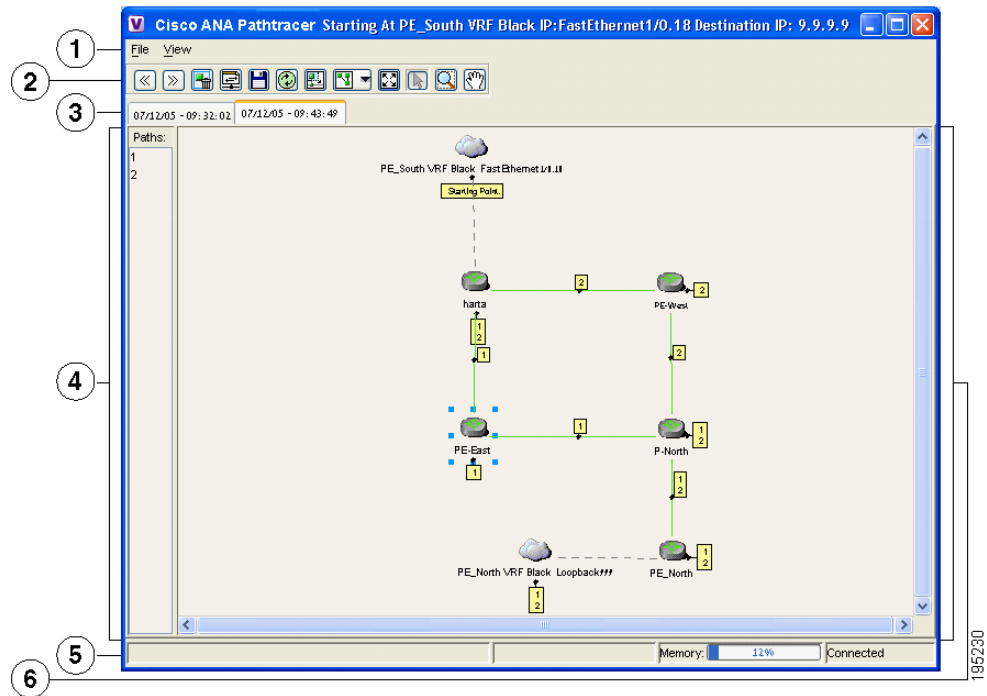
The Cisco ANA PathTracer multipath window displays all the discovered paths for the selected context, including devices and physical links.

The Cisco ANA PathTracer multipath window enables you to:

- View a previous path or view the next path.
- Open the Cisco ANA PathTracer single-path window in order to view a single selected path.
- Save the multipath map to a file.
- Run the Cisco ANA PathTracer again.

An example of the Cisco ANA PathTracer multipath window is displayed in [Figure 11-8](#).

Figure 11-8 Cisco ANA PathTracer Multipath Window



1	Menu bar	4	Paths pane
2	Toolbar	5	Status bar
3	Map pathtraced at...tabs	6	Content pane

The Cisco ANA PathTracer multipath window contains the following elements:

- [Menus, page 11-14](#)
- [Toolbar, page 11-14](#)
- [Tabs, page 11-15](#)
- [Paths Pane, page 11-16](#)
- [Content Pane, page 11-16](#)

Menus

The menus in the Cisco ANA PathTracer multipath window provide the options described in [Table 11-4](#).

Table 11-4 Cisco ANA PathTracer Window Menu Options

Menu Option	Description
File Menu	
Run Again	Runs the Cisco ANA PathTracer again, using the same source and destination parameters.
Save	Saves the map displayed in the multipath window.
Close	Closes the multipath window.
View Menu	
Layout	Defines the way in which the NEs are arranged in the Cisco ANA PathTracer window: circular, symmetric, tree, or hierarchical.
Overview	Opens a window displaying an overview of the network.
Zoom In	Enables you to zoom in for a closer view of the map.
Zoom Out	Enables you to zoom out for a higher-level view of the map.
Fit in Window	Fits the entire subnetwork or map in the content pane.
Normal Select	Activates the normal selection mode (the button toggles when selected or deselected).
Pan	Activates the pan mode, which enables you to move around in the map by clicking and dragging (the button toggles when selected or deselected).
Zoom Selection	Activates the zoom selection mode, which enables you to select an pane in the map to enlarge by clicking and dragging (the button toggles when selected or deselected).

You can also right-click views and network elements in the multipath window and choose items from a shortcut menu. The shortcut menu is context sensitive depending on the view and the network element selected. For more information about the Device shortcut menu and for a detailed description of the menu options available, see [Device Shortcut Menu, page 2-30](#).

Toolbar

The Cisco ANA PathTracer multipath window contains the following tools:

Button	Function
	Selects the previous path viewed in the content pane.
	Selects the next path viewed in the content pane.

Button	Function
	Clears the path selection made in the content pane.
	Opens the Cisco ANA PathTracer single-path window based on the path selected in the Cisco ANA PathTracer multipath window. A map is displayed for the selected path, including NE details, links, and property information. For more information, see Cisco ANA PathTracer Single-Path Window, page 11-16 .
	Saves the multipath map displayed in the content pane. For more information, see Saving and Opening Cisco ANA PathTracer Map Files, page 11-20 .
	Defines the way in which the map is displayed in the content pane (circular, symmetric, tree, or hierarchical).
	Opens a window displaying an overview of the network displayed in the content pane.
	Offers the following options for running Cisco ANA PathTracer again for the same source and destination: • Change Hop Count—Enables you to enter a new hop count. • Repeat Last Trace—Runs the previous trace with the same settings. • Run Full Path Trace—Runs the previous trace without a hop count limitation. The new path trace map is displayed in the content pane. A new tab with the up-to-date (or refreshed) path map is created for each run, with each tab representing a run and the tab label indicating the snapshot time.
	Fits the entire subnetwork or map in the content pane.
	Activates the normal selection mode (the button toggles when selected or deselected).
	Activates the zoom selection mode, which enables you to select an pane in the map to enlarge by clicking and dragging (the button toggles when selected or deselected).
	Activates the pan mode, which enables you to move around in the map by clicking and dragging (the button toggles when selected or deselected).

Tabs

The path is initially displayed in the content pane in a tab that displays the date and time when Cisco ANA 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 displays all of the paths available for the selected source and destination. A new path is created for each source and destination pair. The paths are identified by number, such as 1, 2, and 3. Selecting a path in the Paths pane enables you to view each individual path in the content pane of the Cisco ANA PathTracer single-path window, and the selected path is highlighted in the map.

If the path trace was launched with a specific hop count, the paths pane displays First n Hops where n is the number of hops specified.

Content Pane

The content pane enables you to view a route map of the intermediate network elements. The map displays devices, links, and topological paths.

Icons are used in the content pane to display the network objects and their status. For more information about the icons used, see [Chapter 2, “Working with the Cisco ANA NetworkVision Client.”](#)

All links and nodes are labeled with the relevant paths numbers. The starting point is labeled with a special Starting Point label. All other edge points are displayed as clouds.

Cisco ANA PathTracer Single-Path Window

The Cisco ANA PathTracer single-path window displays the devices and links of the discovered path, as well as path layer properties and subscriber information.



Note

This section refers to single-path view only.

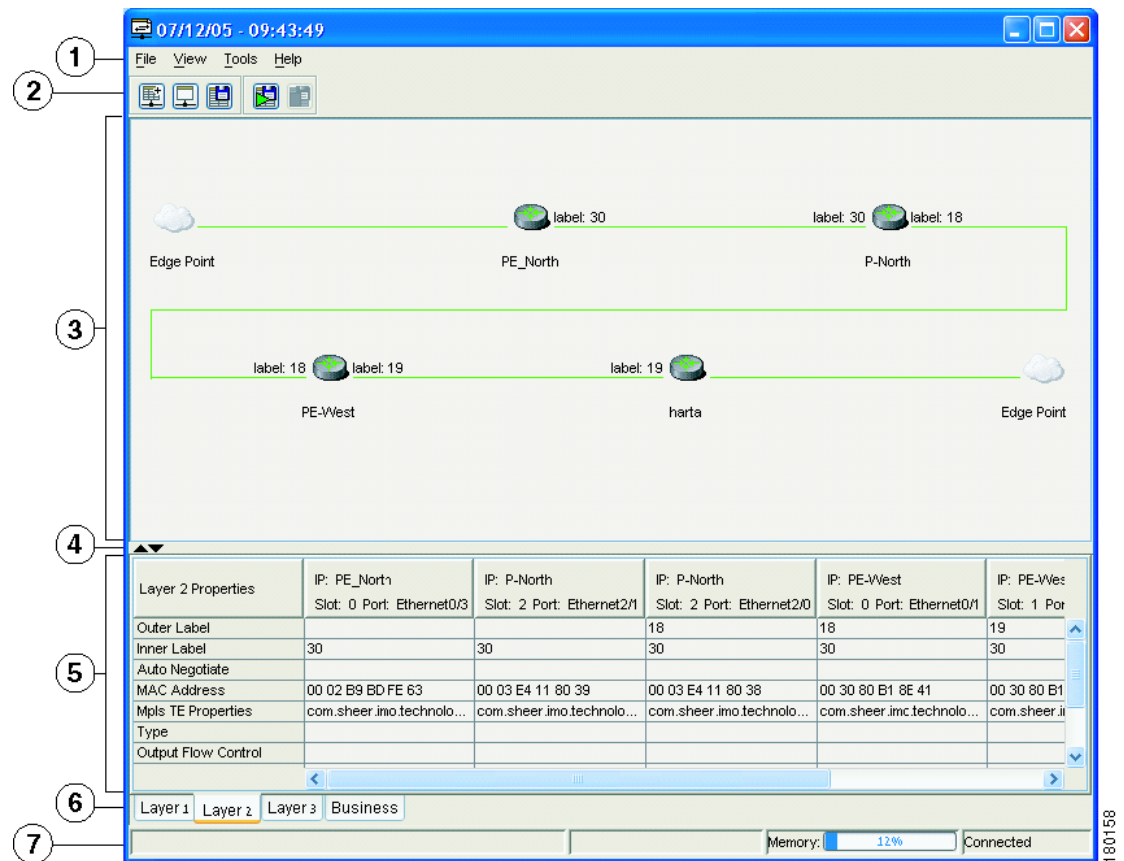
The Cisco ANA PathTracer single-path window enables you to:

- View a map of the intermediate network elements.
- 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.

In addition, right-clicking on an item in Cisco ANA PathTracer enables you to perform certain functions. For example, you can view device information, including device properties, and attach business tags.

Figure 11-9 shows an example of the Cisco ANA PathTracer single-path window.

Figure 11-9 Cisco ANA PathTracer Single-Path Window



1	Menu bar	5	Properties table
2	Toolbar	6	Layer tabs
3	Content pane	7	Status bar
4	Hide/Display Properties table		

The Cisco ANA PathTracer single-path window contains the following items:

- [Menus, page 11-18](#)
- [Toolbar, page 11-18](#)
- [Topological Map, page 11-19](#)
- [Properties Table and Layer Tabs, page 11-19](#)

Menus

The following table provides a description of each option available in the Cisco ANA PathTracer single-path window menus.

Menu Name	Options
File	Close—Closes the single-path window.
View	- Show All—Displays all of the information contained in the Properties table. - Hide All—Hides all of the information contained in the Properties table.
Tools	- Export to File—Exports the currently displayed data to a file. - Start Saving to File—Starts exporting the counter values of the path displayed in the Cisco ANA PathTracer single-path window to a CSV file. - Stop Saving to File—Stops exporting the counter values of the path displayed in the Cisco ANA PathTracer single-path window to a CSV file.
Help	- Help Contents—Opens the online help for Cisco ANA NetworkVision and Cisco ANA EventVision. - Help About—Displays application information, such as the version number.

In addition, you can right-click views and network elements in the single-path window and choose items from a shortcut menu. The shortcut menu is context sensitive depending on the view and the network element selected. The following right-click menu options are available only when you select a network element in the single-path window:

- Show ‘In’ Port—In the Properties table, highlights the In Port information of the selected network element.
- Show ‘Out’ Port—In the Properties table, highlights the Out Port information of the selected network element.

Toolbar

The Cisco ANA PathTracer single-path window contains the following tools:

Table 11-5 Cisco ANA PathTracer Single-Path Window Tools

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.

Table 11-5 Cisco ANA PathTracer Single-Path Window Tools (continued)

Button	Name	Function
	Start Saving to File	Starts exporting the counter values of the path displayed in the Cisco ANA PathTracer single-path window to a CSV file.
	Stop Saving to File	Stops exporting the counter values of the path displayed in the Cisco ANA PathTracer single-path window to a CSV file.

Topological Map

The topological map displays the devices and links that are part of the path. Icons are used in Cisco ANA PathTracer to display the network objects and their status. For more information about the icons used, see [Chapter 2, “Working with the Cisco ANA NetworkVision Client.”](#)

For more information about the colors used to indicate severities, see [Map View, page 2-6](#).

The same coloring conventions that are used in maps in the Cisco ANA NetworkVision content pane are used to display links in the Cisco ANA PathTracer single-path window. Selecting a device or link on the map automatically highlights the related parameters in the table.



Note

The color of a selected link is customizable. The default color is blue.

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 [Network Element Status Indicators, page 2-17](#).

Properties Table and Layer Tabs

The Properties table and tabs display the supported parameters of the specified NE. The Cisco ANA PathTracer single-path window is divided into tabs as shown in the example in [Cisco ANA PathTracer Single-Path Window, page 11-16](#).

The information parameters are displayed in a table, with the ingress and egress ports on 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 Cisco ANA PathTracer information parameters are arranged in groups as follows:

- **Networking Layers**—This group provides information about each network element, including ingress and egress port information. The information is either plain data that was extracted from the device or calculated data such as rates or statistics. This information is displayed in the Layer 1, Layer 2, and Layer 3 tabs.

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**—This area provides the name and key of the business tags that have been attached to the network entities displayed; for example, the port or the entire device (physical entity), VC, VP, DLCI, context (logical entity), or MPLS. This information is displayed in the Business Tag area.

The Cisco ANA PathTracer window is divided into the following tabs; all tabs appear empty when the window opens:

- **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. In addition, it enables you to view the link and connection parameters. For each of the devices, 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 ANA PathTracer single-path window is displayed with the Layer 2 tab active.
- **Layer 3**—Displays the Layer 3 information selected path and enables you to view the link parameters. The name of each device is displayed.
- **Business Parameter**—Displays the name and the key of the business tags that have been attached to the network entities displayed; for example, the port or the entire device (physical entity), VC, VP, DLCI, IP interface, or context (logical entity).

Viewing Path Information

The Cisco ANA PathTracer tabs display information regarding each network element, including ingress and egress port information. The information is either plain data that was extracted from the device or calculated data such as rates or statistics. This information is displayed in the Layer 1, Layer 2, and Layer 3 tabs of the Cisco ANA PathTracer single-path window.

To view path information, select the required tab, and click **Show All**. The path information is displayed in the active tab of the Cisco ANA PathTracer single-path window.



Note

Selecting a device or link on the map automatically highlights the related parameters in the table.

Saving and Opening Cisco ANA PathTracer Map Files

Cisco ANA NetworkVision enables you to export the maps displayed in the Cisco ANA PathTracer multipath window to an .xml file. You can view the data at a later time to assess whether anything has changed.

Saving Cisco ANA PathTracer Map Files

To save Cisco ANA PathTracer Map Files:

- Step 1** Open the Cisco ANA PathTracer multipath window as described in [Using Cisco ANA PathTracer, page 11-3](#).
- Step 2** Save the map in one of the following ways:
 - Click **Save MultiPath** in the multipath window toolbar.
 - Choose **File > Save** from the multipath window menu.
- Step 3** In the Save dialog box, browse to the directory where you want to save the file.

- Step 4** In the File name field, enter a name for the map file.
- Step 5** Click **Save**. The map file is saved in the selected directory.
-

Opening Cisco ANA PathTracer Map Files

Cisco ANA NetworkVision enables you to open saved XML-formatted path-tracing maps.



Note

- When you load a multipath file, Cisco ANA queries the file (not the network), and loads all the persisted information.
 - When you load a multipath file that does not contain the same Start Here and End Here destination information, the map is automatically opened in another instance of Cisco ANA PathTracer.
-

To open Cisco ANA PathTracer Map Files:

- Step 1** In Cisco ANA NetworkVision, choose **File > Load PathTracer** from the main menu. The Open dialog box is displayed.
- Step 2** Browse to the directory of the saved file and select the file.
- Step 3** Click **Open**. The Cisco ANA PathTracer multipath window is displayed with the previously saved map file.
-

Saving Cisco ANA PathTracer Counter Values

Cisco ANA NetworkVision enables you to export, over a period of time, the counter values of the path displayed in the Cisco ANA PathTracer single-path window to a CSV file. The data can then be viewed at a later stage.



Note

This topic applies to the single-path view only.

To save Cisco ANA PathTracer counter values that are generated over a period of time:

- Step 1** Open the Cisco ANA PathTracer single-path window as described in [Using Cisco ANA PathTracer, page 11-3](#).
- Step 2** Start saving counter values to a file in one of the following ways:
- Click **Start Saving to File** in the single-path window toolbar.
 - Choose **Tools > Start Saving to File** from the single-path window main menu.
- Step 3** In the Export Table to File dialog box, browse to the directory where you want to save the Cisco ANA 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 ANA PathTracer starts saving the counter values to the specified file.

- Step 6** Stop exporting counter values to the file in one of the following ways:
- Click **Stop Saving to File** in the single-path window toolbar.
 - Choose **Tools > Stop Saving to File** from the single-path window main menu.

Cisco ANA NetworkVision 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 ANA PathTracer Map Files, page 11-20](#)), you can use the file a later time to rerun the same path automatically with the same source and destination. If required, you can then compare the saved path and the 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 ANA PathTracer Map Files, page 11-20](#). The Cisco ANA PathTracer multipath window is displayed with the previously saved map file.
- Step 2** Rerun the path in the file in one of the following ways:
- Click **Run Again** in the multipath window toolbar.
 - Choose **File > Run Again** from the multipath window main menu.
- The path runs automatically using the same source and destination as the loaded map file, and a new tab is displayed in the Cisco ANA PathTracer multipath window with the updated map. The tab also displays the updated details of the date and time when the path was rerun.
- Step 3** Compare the previous map with the updated one by switching between the tabs in the Cisco ANA PathTracer multipath window.
-



Note

- If you load a Cisco ANA 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 another instance of the Cisco ANA PathTracer multipath window.
 - If you load a Cisco ANA 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 an additional VLAN tag in a packet, in addition to an existing one. Either VLAN tag is considered an 802.1Q header.

Cisco ANA 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, the tool lets you:

- 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 ANA PathTracer windows when a path is traced over Ethernet ports with Dot1q and a Q-in-Q configuration.

As described in [Using Cisco ANA PathTracer, page 11-3](#), to view a specific path, you must specify an initial start point, such as an IP interface, and then an endpoint, such as a destination IP address.

To trace a Q-in-Q path, you start the path from any:

- Router or switch that is part of the Ethernet domain with Dot1q and Q-in-Q configurations.
- IP destination that can be reached from that point of the network.

As soon as you select the endpoint, the Cisco ANA PathTracer Multipath window is displayed. From this window, you can open the Cisco ANA PathTracer Single-Path 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 ANA uses VC ID encapsulation information to trace the path from one tunnel interface to another over the network. The Cisco ANA 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.

Layer 2 and Layer 3 L2TP information is displayed in the Cisco ANA PathTracer windows when a path is traced over L2TP tunnels for Redback devices.

The Layer 3 tab displays the peer name for L2TP tunnels.

[Table 11-6](#) describes the information that is displayed in the Layer 2 tab for L2TP tunnels.

Table 11-6 Layer 2 Tab Information for L2TP Tunnels

Field	Description
Encapsulation Type	The encapsulation type, such as Point-to-Point Protocol over ATM (PPPoA).
Binding Information	The name of the subscriber.

Table 11-6 Layer 2 Tab Information for L2TP Tunnels (continued)

Field	Description
Binding Status	The binding status: bound or unbound.
Tunnel Session Count	The number of current sessions.
Tunnel Remote ID	The remote tunnel identifier.
Tunnel ID	The local tunnel identifier.
Tunnel Name	The name of the subscriber and the tunnel ID.
Session ID	The session identifier.
Traffic > L2TPSessionCounters	The number of traffic packets passing through the L2TP tunnel.
Traffic < L2TPSessionCounters	The number of traffic packets passing through the L2TP tunnel.
Tunnel Ctl Errors	The number of control errors.
Tunnel State	The tunnel state: unknown, idle, connecting, established, or disconnecting.
Session Type	The session type: unknown, LAC, or LNS.
Peer Name	The peer name.
Tunnel Remote IP	The remote IP address of the tunnel.
Last Error Code	The value of the last error code that caused the tunnel disconnection.
Session State	The session state: unknown, idle, connecting, established, or disconnecting.
Remote Session ID	The remote session identifier.

Using Cisco ANA PathTracer in MPLS Networks

You can open and view Cisco ANA 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

The LSP can be traced and displayed by Cisco ANA PathTracer as part of an end-to-end tracing of a service, as well; for example, when viewing a path between one CE device and another. Cisco ANA 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 circuit (for example, a VC or VLAN) ends in a router, Cisco ANA PathTracer finds the next hop according to the destination IP address. When you select an endpoint, Cisco ANA extracts the relevant IP address from this point and uses it as the destination.

Cisco ANA PathTracer MPLS Starting Points

You can open Cisco ANA PathTracer by right-clicking a starting point and entering the required destination IP address. [Table 11-7](#) lists the Cisco ANA PathTracer starting points.

Table 11-7 Cisco ANA PathTracer Starting Points

Element	Location	Start Options
IP Interface	- Inventory window. - Affected entity (enabled only if the affected entity has an IP interface).	- From Here to Destination - Start Here
Site	Service view map.	- From Here to Destination - To Subnet Destination - Start Here
Business tag attached to the VPI/VCI or IP interface	The path can be found using a business tag, which is attached to the VPI/VCI or IP interface by entering its key. It can then be opened from the Find Business Tag window.	From Here to Destination
Layer 2 MPLS Tunnel	Inventory window.	From Here to Destination
LCP	Service view map.	- From Here to Destination - Start Here

Cisco ANA PathTracer MPLS Endpoints

If you choose the Start Here option, [Table 11-8](#) lists the endpoints that can be selected as path destinations.

Table 11-8 Cisco ANA PathTracer Endpoints

Element	Location	End Options
IP Interface	- Inventory window - Affected entity (enabled only if the affected entity has an IP interface)	End Here
Site	Service view map	End Here
LCP	Service view map	End Here

The Cisco ANA PathTracer multipath window is displayed. From this window you can open the Cisco ANA PathTracer single-path window with the appropriate 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 ANA PathTracer single-path window.

Using Cisco ANA PathTracer for Layer 3 VPNs

Cisco ANA PathTracer uses VRF routing and label switching information to trace the path from one VRF interface to another. If you choose a start and endpoint from the right-click menu, you can open the Cisco ANA PathTracer for Layer 3 VPNs. The Cisco ANA PathTracer multipath window shows the VPN topology map. From this window, you can open the Cisco ANA PathTracer single-path window with the appropriate VPN information displayed in the Layer 2 and Layer 3 tabs.

For Layer 3 path information, Cisco ANA uses VRF routing and label switching information to trace the path from one VRF interface to another. Layer 3 Cisco ANA PathTracer information is displayed in the Cisco ANA 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 ANA 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.



Note Selecting a device or link on the map automatically highlights the related parameters in the table.

The Cisco ANA PathTracer single-path window with the Layer 3 tab is displayed. 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.
- **Sending Alarms**—Whether or not the interface is configured for sending alarms: True or False.

Cisco ANA PathTracer does not display or trace EXP bits for L3 VPNs that use policy-based tunnel selection (PBTS).

Using Cisco ANA PathTracer for Layer 2 VPNs

Cisco ANA uses VC ID and label switching information to trace the path from one tunnel interface to another over the MPLS network.

The Cisco ANA 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 ANA PathTracer multipath window shows the VPN topology map for the relevant devices and links. From this window, you can open the Cisco ANA PathTracer single-path window with the appropriate VPN information displayed in the Layer 2 and Layer 3 tabs.

For Layer 2 path information, Cisco ANA uses VC ID and label switching information to trace the path from one tunnel interface to another. Layer 2 Cisco ANA PathTracer information is displayed in the Cisco ANA 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.



Note Selecting a device or link on the map automatically highlights the related parameters in the table.

Table 11-9 describes the Layer 2 properties that can be displayed in the Layer 2 tab specifically for VPNs.

Table 11-9 Cisco ANA PathTracer Layer 2 Properties for VPNs

Field	Description
Outer Label	The details of the outer MPLS label.
Inner Label	The details of the inner MPLS label.
MAC Address	The MAC address.
Tunnel ID	The tunnel identifier. The identifier and the router IP address of the two tunnel edges identify the pseudowire tunnel
Tunnel Type	The tunnel type: 0—Unknown 1—PWE3 2—TE
Tunnel Status	The operational state of the tunnel: Up or Down.
Tunnel Local VC Label	The 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	The 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	The IP address of the tunnel edge, which is used as the MPLS router identifier.
Tunnel Peer Router IP	The IP address of the peer tunnel edge, which is used as the MPLS router identifier.
Distribution Protocol Type	The protocol used by MPLS to build the tunnel, such as LDP or TDP.
Peer OID	The tunnel identifier and device name.

Using Cisco ANA PathTracer for MPLS TE Tunnels

Cisco ANA Path Tracer 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 ANA 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 ANA PathTracer multipath window is displayed showing the MPLS TE tunnel topology map. From this window, you can open the Cisco ANA PathTracer single-path window with the appropriate MPLS TE tunnel information displayed in the Layer 2 tab.

**Note**

Cisco ANA PathTracer does not display or trace EXP bits for L3 VPNs that use PBTS.

Layer 2 and Layer 3 Cisco ANA PathTracer information is displayed in the Cisco ANA PathTracer 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.

**Note**

Selecting a device or link on the map automatically highlights the related parameters in the table.

[Table 11-10](#) describes the Layer 2 properties that can be displayed in the Layer 2 tab specifically for MPLS TE tunnels.

Table 11-10 Cisco ANA PathTracer Layer 2 Properties for MPLS TE Tunnels

Field	Description
MPLS TE Properties	The MPLS TE data set in an MPLS interface, primarily bandwidth allocation levels and signaling protocol.
Tunnel Oper Status	The operational status of the tunnel: Up or Down. If this value is Up, the Tunnel Admin Status must also be Up. See Tunnel Admin Status properties for additional information.
Tunnel Bandwidth Kbps	The configured bandwidth (in Kb/s) for the tunnel.
Tunnel Description	A description of the tunnel.
Tunnel Name	The interface name.
Tunnel Admin Status	The administrative status of the tunnel (Up or Down) with the following caveats: - If the Tunnel Oper Status value is Up, the Tunnel Admin Status value must also be Up. - If the Tunnel Admin Status value is Down, the Tunnel Oper Status value must also be Down.
Tunnel Lockdown	Whether or not the tunnel can be rerouted: - Enabled—The tunnel cannot be rerouted. - Disabled—The tunnel can be rerouted.
Tunnel LSP ID	The LSP identifier.
Tunnel Auto Route	Whether or not destinations behind the tunnel are routed through the tunnel: Enabled or disabled.
Tunnel Hold Priority	The tunnel priority after path setup.
Tunnel Setup Priority	The tunnel's priority upon path setup.

Table 11-10 Cisco ANA PathTracer Layer 2 Properties for MPLS TE Tunnels (continued)

Field	Description
Tunnel Path Option	The tunnel path option: - Dynamic—The tunnel is routed along the ordinary routing decisions after taking into account the tunnel constraints such as attributes, priority, and bandwidth. - Explicit—The route is explicitly mapped with the included and excluded links.
Tunnel Out Label	The TE tunnel MPLS label distinguishing the LSP selection in the adjacent device.
Tunnel Affinity	The tunnel's preferential bits for specific links.
Tunnel Destination Address	The 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	The interface through which the tunnel exits the device.
Tunnel Burst Kbps	Burst flow specification (in Kb/s) for this tunnel.
Tunnel Average Rate Kbps	The tunnel average rate in Kb/s.
Tunnel Affinity Mask	The tunnel affinity bits that should be compared to the link attribute bits.



CHAPTER 12

Monitoring Carrier Ethernet Services

The following topics describe how you can use Cisco ANA to monitor Carrier Ethernet services:

- [User Roles Required to Work with Carrier Ethernet Services, page 12-2](#)
- [Viewing CDP Properties, page 12-4](#)
- [Viewing Link Layer Discovery Protocol Properties, page 12-5](#)
- [Viewing Spanning Tree Properties, page 12-7](#)
- [Viewing Resilient Ethernet Protocol Properties, page 12-10](#)
- [Working with Ethernet Link Aggregation Groups, page 12-13](#)
- [Viewing Provider Backbone Bridge Properties, page 12-19](#)
- [Viewing EFP Properties, page 12-20](#)
- [Understanding EFP Severity and Ticket Badges, page 12-22](#)
- [Viewing EVC Service Properties, page 12-23](#)
- [Viewing Virtual Switching Instance Properties, page 12-25](#)
- [Viewing and Renaming Ethernet Flow Domains, page 12-30](#)
- [Working with VLANs and VLAN Overlays, page 12-33](#)
- [Understanding Unassociated Bridges, page 12-61](#)
- [Working with Ethernet Flow Point Cross-Connects, page 12-64](#)
- [Working with VPLS and H-VPLS Instances, page 12-69](#)
- [Working with Pseudowires and Pseudowire Overlays, page 12-77](#)
- [Working with Ethernet Services, page 12-90](#)
- [Viewing IP SLA Responder Service Properties, page 12-97](#)
- [Viewing IS-IS Properties, page 12-98](#)
- [Viewing OSPF Properties, page 12-101](#)

User Roles Required to Work with Carrier Ethernet Services

Table 12-1 identifies the roles that are required to work with to Carrier Ethernet services in Cisco ANA NetworkVision. Cisco ANA 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 device-based tasks (tasks that do affect devices), authorization is based on the default permission that is assigned to your account. That is, whether the device 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 Active Network Abstraction 3.7.1 Administrator Guide](#).

Table 12-1 Default Permission/Security Level Required for Working with Carrier Ethernet Services

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Bridges and Bridge Domains					
Add unassociated bridges	—	—	X	X	X
EFP Cross-Connects					
Add EFP cross-connects	—	—	X	X	X
View EFP cross-connect properties	Partial ¹	Partial ¹	Partial ¹	Partial ¹	X
Ethernet Flow Domains					
Rename Ethernet flow domains	X	X	X	X	X
View EFD properties	—	—	—	—	X
View EFP properties	—	—	—	—	X
View Ethernet flow domains	X	X	X	X	X
View Ethernet LAG properties	—	—	—	—	X
View LAG link discovery information	—	—	—	—	X
Ethernet Services					
Add Ethernet services to a map	—	—	X	X	X
Add Ethernet service overlays	X	X	X	X	X
View Ethernet service properties	X	X	X	X	X
Pseudowires and Pseudowire Overlays					
Add pseudowires to a map	—	—	X	X	X
Apply pseudowire overlays	X	X	X	X	X
View EVC service properties	—	—	—	—	X
View pseudowire properties	Partial ²	Partial ²	Partial ²	Partial ²	X
Resilient Ethernet Protocol (REP)					
View REP information in VLAN domain views and VLAN overlays	—	—	—	—	X
View REP properties	—	—	—	—	X

Table 12-1 *Default Permission/Security Level Required for Working with Carrier Ethernet Services (continued)*

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View REP properties for VLAN service links	—	—	—	—	X
Spanning Tree Protocol (STP)					
View STP information in VLAN domain views and VLAN overlays	—	—	—	—	X
View STP properties	—	—	—	—	X
View STP properties for VLAN service links	—	—	—	—	X
VLANs					
Add VLANs to a map	—	—	X	X	X
Remove VLANs from a map	—	—	X	X	X
View associated VLAN network VLAN service links and VLAN mapping properties	—	—	—	—	X
View VLAN bridge properties	—	—	—	—	X
View VLAN mappings	—	—	—	—	X
View VLAN trunk group properties	—	—	—	—	X
VLAN Overlays					
Add VLAN overlays to a map	X	X	X	X	X
Display or hide VLAN overlays	X	X	X	X	X
Remove VLAN overlays	X	X	X	X	X
VPLS / H-VPLS					
Add VPLS instances to a map	—	—	X	X	X
Use VPLS instance overlays	X	X	X	X	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
View VSI properties	—	—	—	—	X
Other Tasks					
View CDP properties	—	—	—	—	X
View IP SLA responder service properties	—	—	—	—	X
View IS-IS properties	—	—	—	—	X
View Link Layer Discovery Protocol (LLDP) properties	—	—	—	—	X

Table 12-1 *Default Permission/Security Level Required for Working with Carrier Ethernet Services (continued)*

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View OSPF properties	—	—	—	—	X
View Provider Backbone Bridge (PBB) properties	—	—	—	—	X

1. The user with this role can view EFP cross-connect properties, but not local switching properties configured on an element unless the element is in the user's scope.
2. The user with this role can view properties for individual pseudowires added to a map, but not for pseudowire endpoint properties configured on an element unless the element is in the user's scope.

Viewing CDP Properties

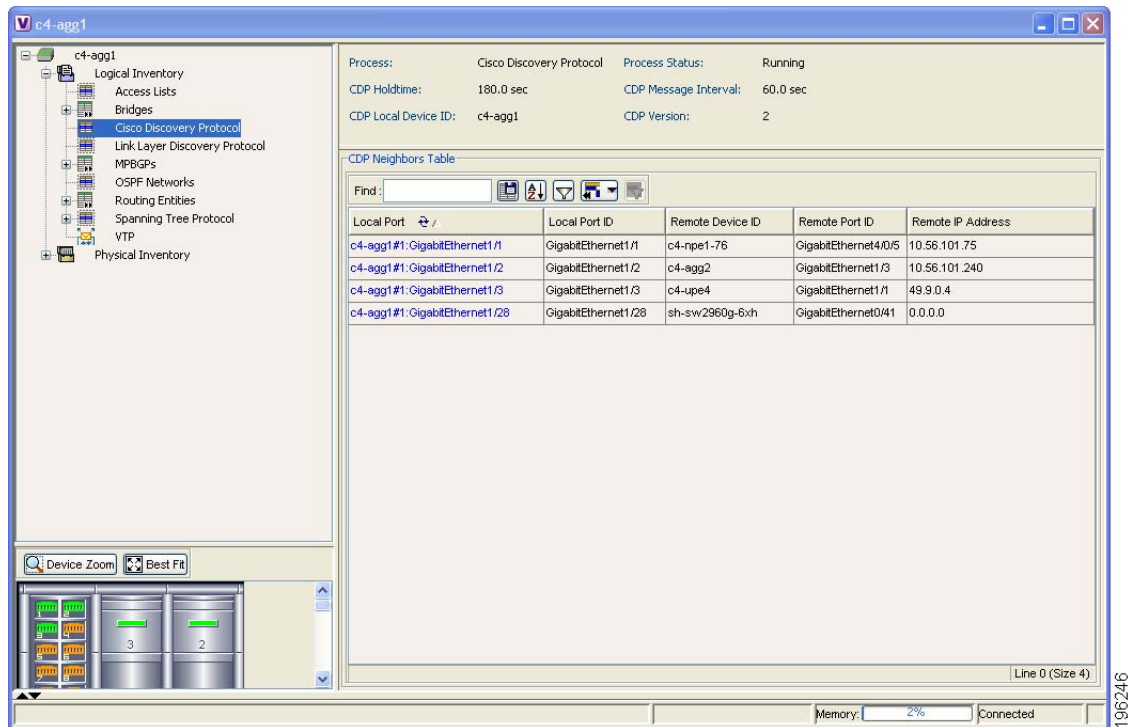
Cisco Discovery Protocol (CDP) is primarily used to obtain protocol addresses of neighboring devices and discover the platform of those devices.

To view CDP properties:

- Step 1** In Cisco ANA NetworkVision, double-click the device whose CDP properties you want to view.
- Step 2** In the inventory window, click **Logical Inventory > Cisco Discovery Protocol**.

The CDP properties are displayed in logical inventory as shown in [Figure 12-1](#).

Figure 12-1 *CDP in Logical Inventory*



[Table 12-2](#) describes the CDP instance properties that are displayed.

Table 12-2 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.

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

Viewing Link Layer Discovery Protocol Properties

LLDP stores and maintains the local device information, including a list of devices directly connected to the device.

In Logical Inventory

To view LLDP properties:

Step 1 In Cisco ANA NetworkVision, double-click the device with the LLDP information you want to view.

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

The LLDP properties are displayed in logical inventory as shown in [Figure 12-2](#).

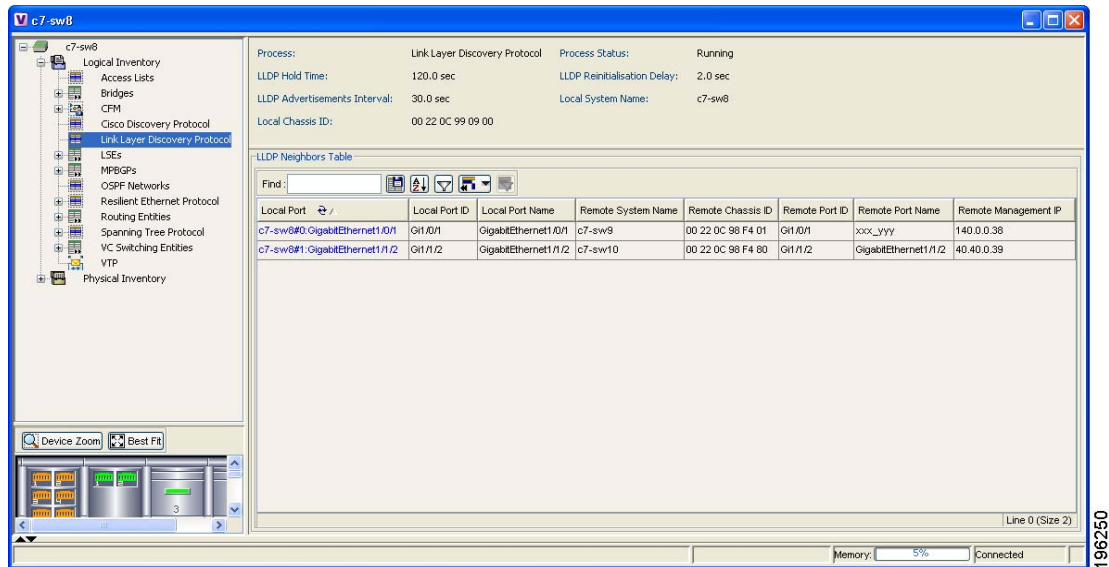
Figure 12-2 LLD in Logical Inventory

Table 12-3 describes the properties that are displayed for LLDP.

Table 12-3 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.
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.

Step 3 When finished, press **Ctrl + F4** to close the LLDP properties window.

In Physical Inventory

To view LLDP on a Layer 2 port:

-
- Step 1** In Cisco ANA NetworkVision, 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 Cisco ANA NetworkVision content pane:
- Discovery Protocol Type—LLDP
 - Info—Tx (Enabled or Disabled), Rx (Enabled or Disabled).
- Step 3** When finished, press **Ctrl + F4** to close the Port properties window.
-

Viewing Spanning Tree Properties

STP is a link management protocol that provides path redundancy while preventing undesirable loops in the network.

To view Spanning Tree properties:

-
- Step 1** In Cisco ANA NetworkVision, double-click the element whose STP properties you want to view.
- Step 2** In the inventory window, choose **Logical Inventory > Spanning Tree Protocol Service**.
- Step 3** STP properties are displayed in logical inventory as shown in [Figure 12-3](#).

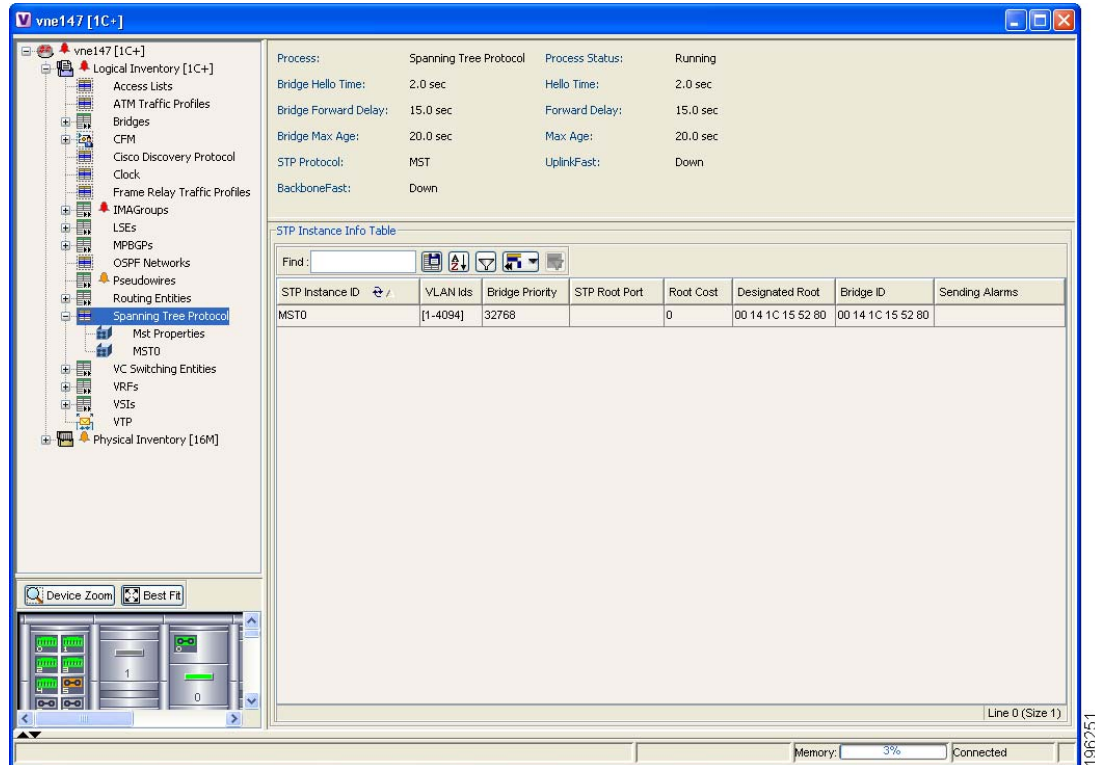
Figure 12-3 STP in Logical Inventory

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

Table 12-4 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 hundredths of seconds) when the port is the root.
Hello Time	Current hello time (in hundredths of seconds).
Bridge Forward Delay	When the port is the root and in listening or learning state, amount of time to wait (in hundredths of seconds) before proceeding to the forwarding state.
Forward Delay	Current bridge forward delay (in hundredths of seconds).
Bridge Max Age	When the port is the root, maximum age of learned Spanning Tree Protocol port information (in hundredths of seconds).
Max Age	Current maximum age (in hundredths of seconds).
STP Protocol	STP version: RSTP, PVSTP, MSTP, or RPVST.
UplinkFast	PVSTP Uplink Fast function status: Up or Down.
BackboneFast	PVSTP BackboneFast function status: Up or Down.

Table 12-4 *STP Properties (continued)*

Field	Description
STP Instance Info Table	
STP Instance ID	STP instance name.
VLAN Id	VLAN identifier.
Bridge Priority	Bridge priority.
STP Root Port	Hyperlinked entry to the STP port in 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 hundredths of seconds) when the port is the root.
Hello Time	Current hello time (in hundredths of seconds).
Bridge Forward Delay	When the port is the root and in the listening or learning state, amount of time to wait (in hundredths of seconds) before proceeding to the forwarding state.
Forward Delay	Current bridge forward delay (in hundredths of seconds).
Bridge Max Age	When the port is the root, maximum age of learned Spanning Tree Protocol port information (in hundredths of seconds).
Max Age	Current maximum age (in hundredths of seconds).
Sending Alarms	Whether or not the STP instance is sending alarms.

Step 4 To view the properties of an STP instance, double-click it.

[Table 12-5](#) describes the information that is displayed in the STP Instance Information Properties window.

Table 12-5 *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 hundredths of seconds) when the port is the root.
Hello Time	Current hello time (in hundredths of seconds).
Bridge Forward Delay	When the port is the root and in listening or learning state, amount of time to wait (in hundredths of seconds) before proceeding to the forwarding state.
Forward Delay	Current bridge forward delay (in hundredths of seconds).

Table 12-5 STP Instance Information Properties (continued)

Field	Description
Bridge Max Age	When the port is the root, the maximum age of learned Spanning Tree Protocol port information (in hundredths of seconds).
Max Age	Current maximum age (in hundredths of seconds).
STP Protocol Specification	STP version, such as PVSTP or RSTP.
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.
Port Identifier	STP port identifier.
Portfast	STP PortFast status: 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.
Sending Alarms	Whether or not the port is configured for sending alarms: True or False.

Step 5 When finished, press **Ctrl + F4** to close each STP properties window.

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

- VLAN domain views and overlays—See [Viewing STP Information in VLAN Domain Views and VLAN Overlays](#), page 12-54.
- VLAN service link properties—See [Viewing STP Properties for VLAN Service Links](#), page 12-56.

Viewing Resilient Ethernet Protocol Properties

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

To view REP properties in logical inventory:

- Step 1** In Cisco ANA NetworkVision, double-click the device configured for REP.
- Step 2** In the inventory window, choose **Logical Inventory > Resilient Ethernet Protocol**.

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

Figure 12-4 REP in Logical Inventory

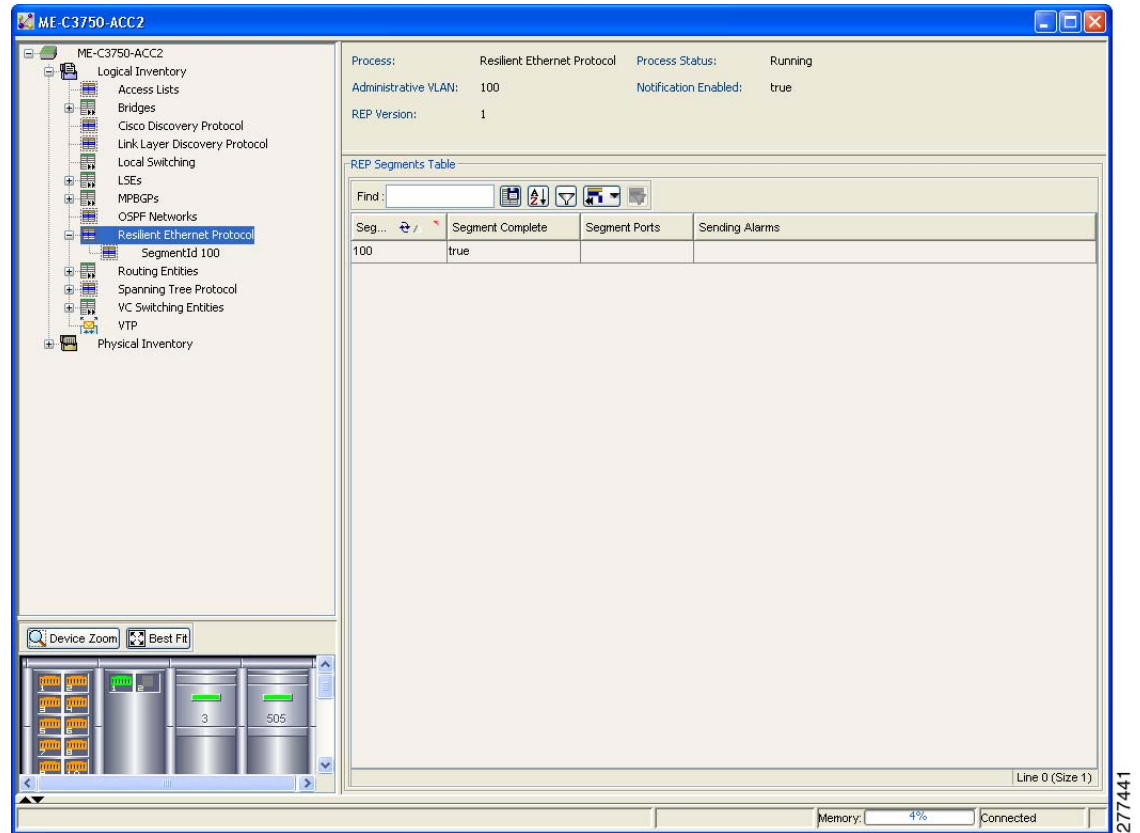


Table 12-6 describes the information that is displayed for REP.

Table 12-6 REP Properties

Field	Description
Process	Process name; in this case, Resilient Ethernet Protocol.
Process Status	State of the REP process, such as Running or Down.
Administrative VLAN	Administrative VLAN used by REP to transmit its hardware flooding layer messages. Values range from 1 to 4094.
Notification Enabled	Whether or not notification is enabled: True or False.
REP Version	Version of REP being used.

Table 12-6 REP Properties (continued)

Field	Description
REP Segments Table	
Segment ID	Segment identifier.
Segment Complete	Indicates whether the segment is complete; that is, that no port in the segment is in a failed state: True or False.
Segment Ports	This column is empty.
Sending Alarms	Whether or not the segment is configured for sending alarms: True or False.

Step 3 To view REP segment properties, double-click the required entry in the REP Segments table. Figure 12-5 shows an example of REP segment properties in logical inventory.

Figure 12-5 REP Segment Properties

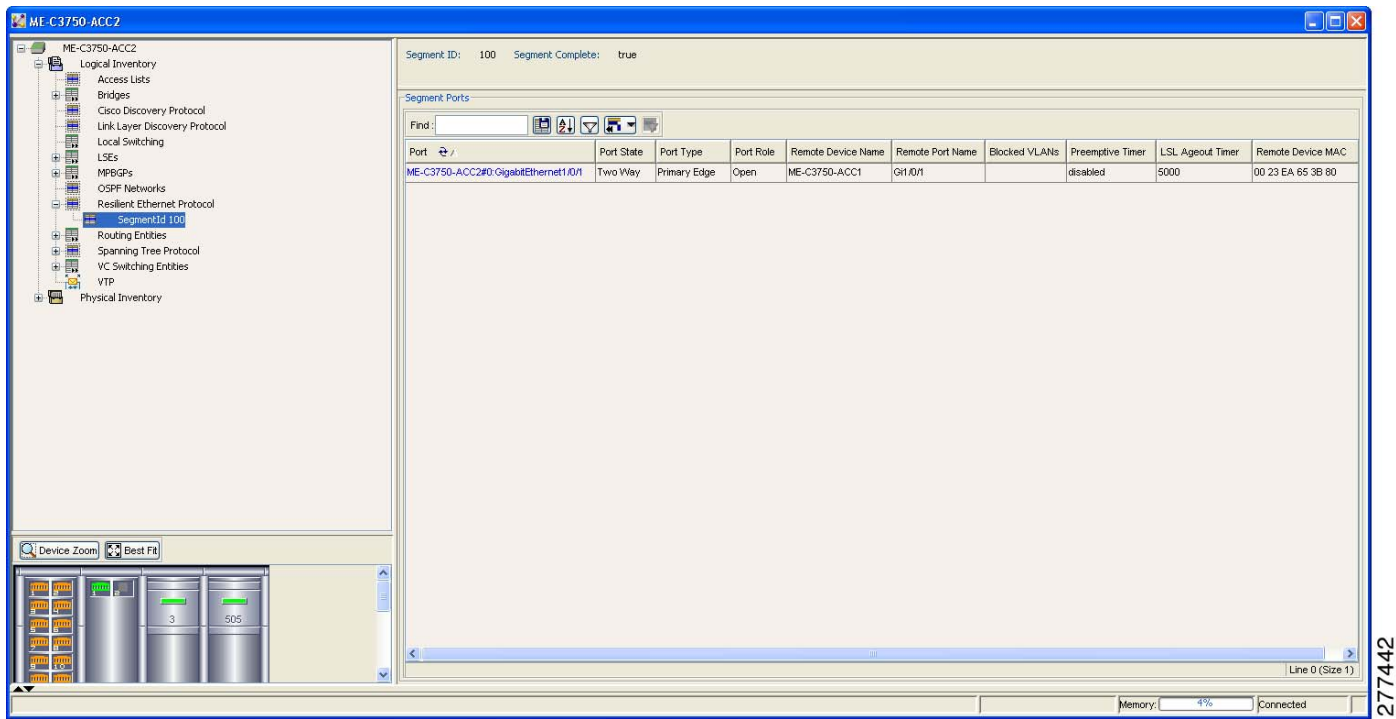


Table 12-7 describes the information that is displayed for REP segments.

Table 12-7 REP Segment Properties

Field	Description
Segment ID	Segment identifier.
Segment Complete	Indicates whether the segment is complete; that is, that no port in the segment is in a failed state: True or False.

Table 12-7 REP Segment Properties (continued)

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

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

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

- VLAN domain views and overlays—See [Viewing REP Information in VLAN Domain Views and VLAN Overlays](#), page 12-52.
- VLAN service link properties—See [Viewing REP Properties for VLAN Service Links](#), page 12-53.

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.

Beginning with Cisco ANA 3.7.1:

- LAG links are discovered automatically for devices that support LAG technology and use VNEs that model Link Aggregation Control Protocol (LACP) attributes.
- You can create static links between Ethernet LAGs by choosing a LAG and the desired port channel for the A or Z side as described in [Adding Static Links, page 5-12](#).

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

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

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

- An aggregation service alarm is generated.

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

Viewing Ethernet LAG Properties

To view properties for Ethernet link aggregation groups:

-
- Step 1** In Cisco ANA NetworkVision, double-click the device with the link aggregation group you want to view.
- Step 2** In the inventory window, choose **Logical Inventory > Ethernet Link Aggregation**.
The link aggregation properties are displayed as shown in [Figure 12-6](#).

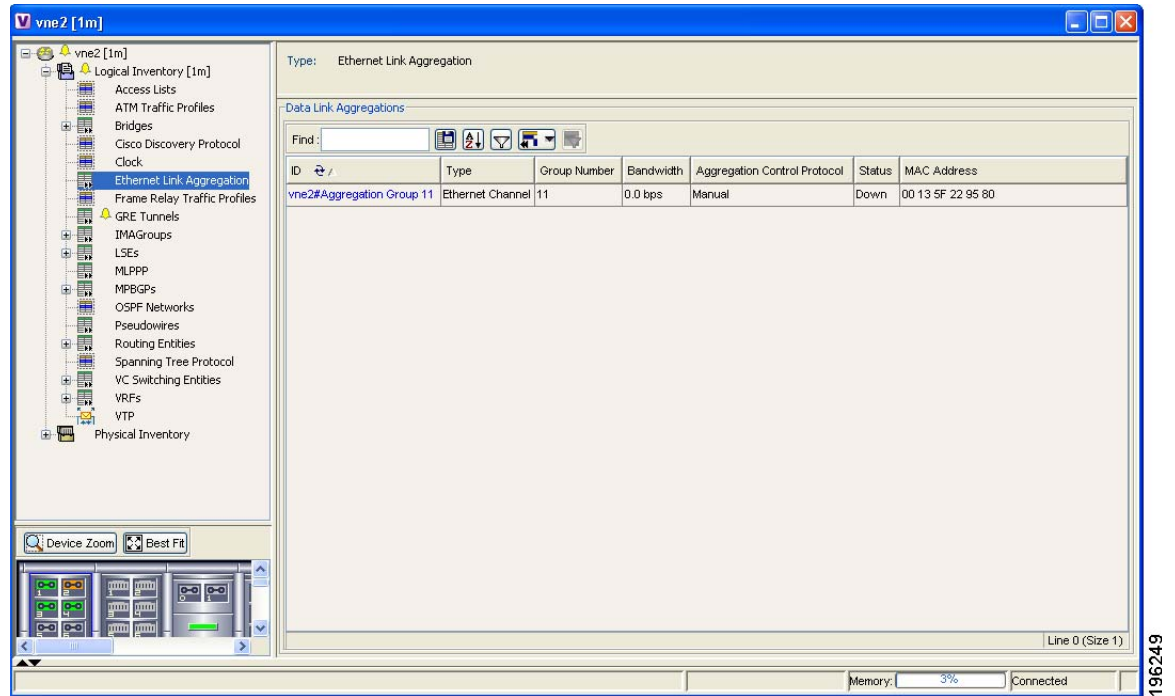
Figure 12-6 Ethernet Link Aggregation in Logical Inventory

Table 12-8 describes the aggregation group properties that are displayed in the Data Link Aggregations table.

Table 12-8 Data Link Aggregations Table

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

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

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

- For Ethernet Channel aggregations, see Table 12-9.
- For IEEE 802.3 AD aggregations, see Table 12-10.

Table 12-9 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.
Aggregated Ports Table	
ID	Aggregated port identifier, hyperlinked to the interface in physical inventory.
Type	Aggregation type, such as Layer 2 VLAN.
Mode	VLAN mode, such as Trunk.
Native VLAN ID	VLAN identifier (VID) associated with this VLAN. The range of VLANs is 1 to 4067.
VLAN Encapsulation Type	Type of encapsulation configured on the VLAN, such as IEEE 802.1Q.
Allowed VLANs	List of VLANs allowed on this interface.
VLAN Encapsulation Admin Type	VLAN administration encapsulation type, such as IEEE 802.1Q.
Subinterfaces Table	
Address	IP address of the subinterface.
Mask	Subnet mask applied to the IP address.
VLAN Type	Type of VLAN, such as Bridge or IEEE 802.1Q.
Operational State	Operational state of the subinterface: Up or Down.
VLAN ID	VLAN identifier.
Inner VLAN	CE-VLAN identifier.
IP Interface	IP interface configured as part of the subinterface, hyperlinked to the routing entity or VRF in logical inventory.
VRF Name	VRF associated with the subinterface.
Is MPLS	Whether the subinterface is enabled for MPLS: True or False. This column is displayed when at least one interface is MPLS-enabled.
Sending Alarms	Whether the interface is configured for alarms: True or False.
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.

Table 12-9 LAG Ethernet Channel Properties (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 bridge in logical inventory.
Description	Description for the EFP.

Table 12-10 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.
Aggregated Ports Table	
ID	Port identifier, hyperlinked to the interface in physical inventory.
Type	Type of VLAN, such as Layer 2 VLAN.
Sending Alarms	Whether or not the interface is configured for sending alarms: True or False.
Discovery Protocols	Discovery protocols used on this port.

Table 12-10 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	
Dot3ad Agg Port Partner Admin Key	Administrative key for the partner port.
Dot3ad Agg Port Partner Admin Port Priority	Administrative port priority for the partner.
Dot3ad Agg Port Partner Oper Port Priority	Priority assigned to the aggregation port by the partner.
Dot3ad Agg Port Actor Admin State	Local administrative state as transmitted by the local system in LACP data units (LACPDUs).
Dot3ad Agg Port Actor Oper State	Local operational state for the port.
Dot3ad Agg Port Partner Oper Key	Operational key for the partner port.
Dot3ad Agg Port Selected Agg ID	Selected identifier for the aggregation 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 Attached Agg ID	Identifier of the aggregator that the port is attached to.
Dot3ad Agg Port Partner Oper State	Partner administrative state as transmitted by the partner in the most recently transmitted LAPCDU.
Dot3ad Agg Port Actor Admin Key	Administrative key for the local port.

Table 12-10 LAG IEEE 802.3 AD Properties (continued)

Field	Description
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.

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

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.

Cisco ANA 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

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

To view PBB properties:

- Step 1** In Cisco ANA NetworkVision, double-click the element configured for PBB.
- Step 2** In the inventory window, choose **Logical Inventory > BridgeILans > PBB-bridge**.

Figure 12-7 shows an example of PBB properties in logical inventory.

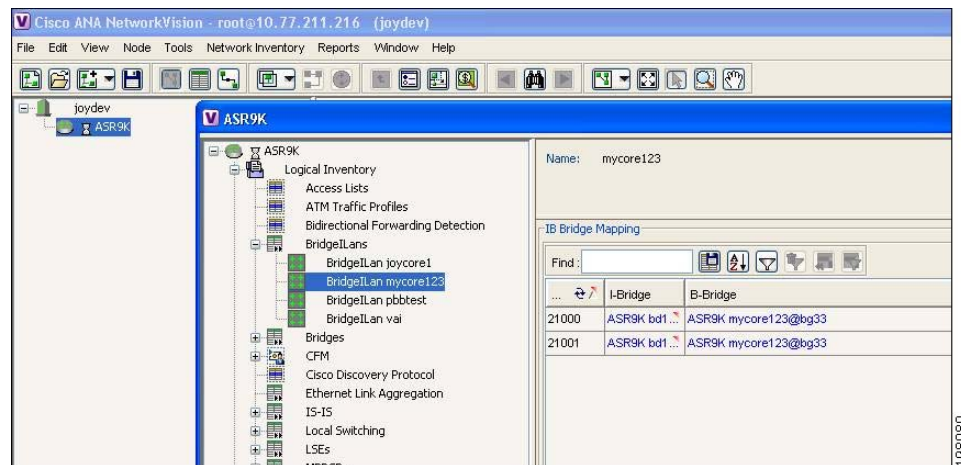
Figure 12-7 PBB Properties in Logical Inventory

Table 12-11 describes the information displayed for PBB.

Table 12-11 PBB Properties in Logical Inventory

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

Viewing EFP Properties

Cisco ANA provides information about EFPs in a number of ways. For example:

- EFP names displayed in Cisco ANA NetworkVision 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 Cisco ANA NetworkVision 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 Cisco ANA NetworkVision 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**.

The EFP Properties window displays the information described in Table 12-12.

Table 12-12 EFP Properties Window

Field	Description
EFP ID	Identifier for the EFP.
VLAN Match Criteria	Match criteria configured on the EFP for forwarding decisions.
Operational State	Operational status of the EFP: Up or Down.
Administrative State	Administrative status of the EFP: Up or Down.

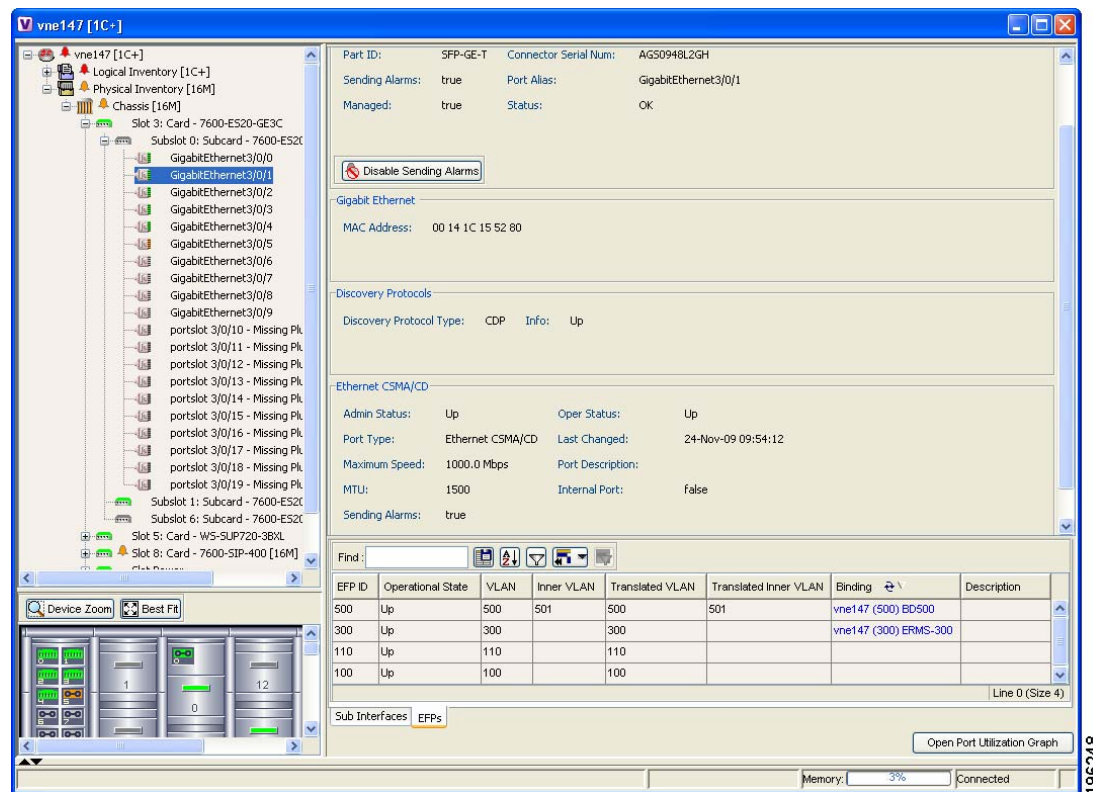
Table 12-12 EFP Properties Window (continued)

Field	Description
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 To view EFP properties in physical inventory, navigate to the required interface in either of the following ways:

- Use the procedure described in [Viewing and Renaming Ethernet Flow Domains](#), page 12-30 to navigate to the individual interface.
- In physical inventory, navigate to and then select the required interface.

The EFPs tab is displayed in the content pane next to the Subinterfaces tab as shown in [Figure 12-8](#).

Figure 12-8 EFPs Tab in Physical Inventory

[Table 12-13](#) describes the information displayed in the EFPs tab.

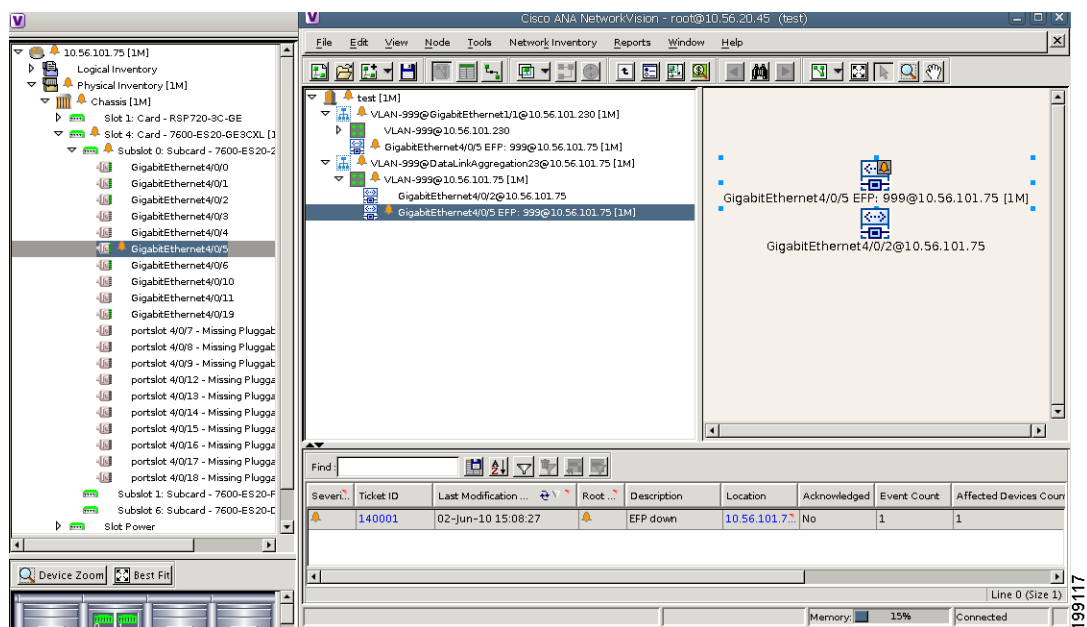
Table 12-13 EFPs Tab

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

Understanding EFP Severity and Ticket Badges

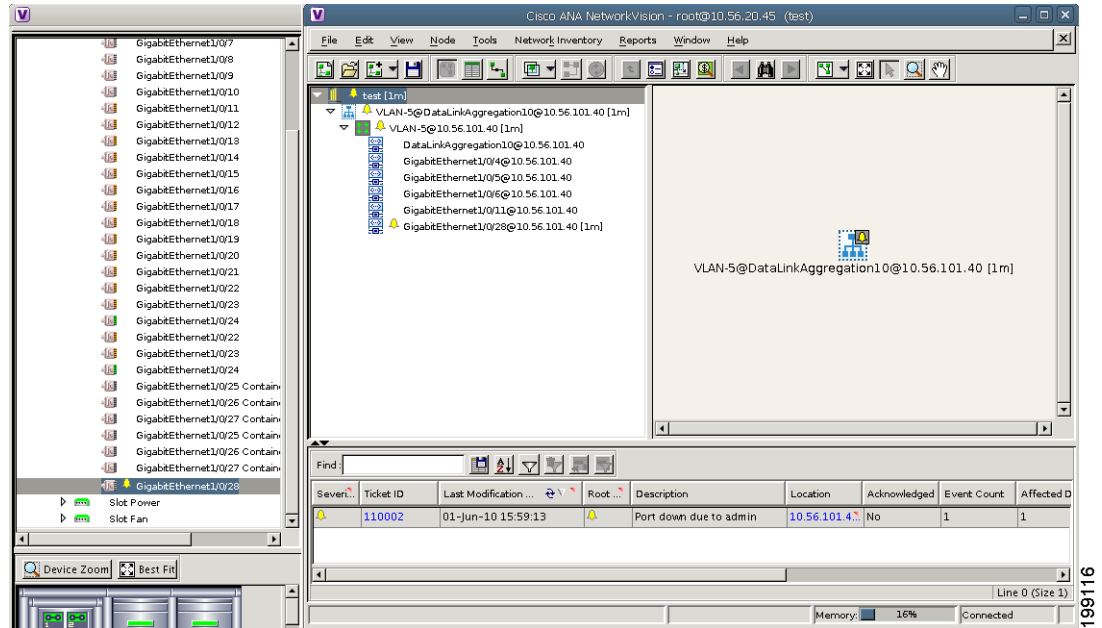
Severity and ticket badges are displayed on EFP icons as follows:

- If the EFP element represents an EFP 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 VNE EFP configuration service instance. See [Figure 12-9](#).

Figure 12-9 EFP Severity and Ticket Badges Based on Underlying Service Instance

- If the EFP element represents a VLAN interface for a regular switch port, the severity and ticket badges are based on the corresponding port. See [Figure 12-10](#).

Figure 12-10 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. Cisco ANA 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.

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

- Step 1** In Cisco ANA NetworkVision, double-click the required device.
- Step 2** In the inventory window, choose **Physical Inventory** > **Chassis** > *module* > *port*.

[Figure 12-11](#) shows an example of a port in physical inventory configured with these EVC properties.

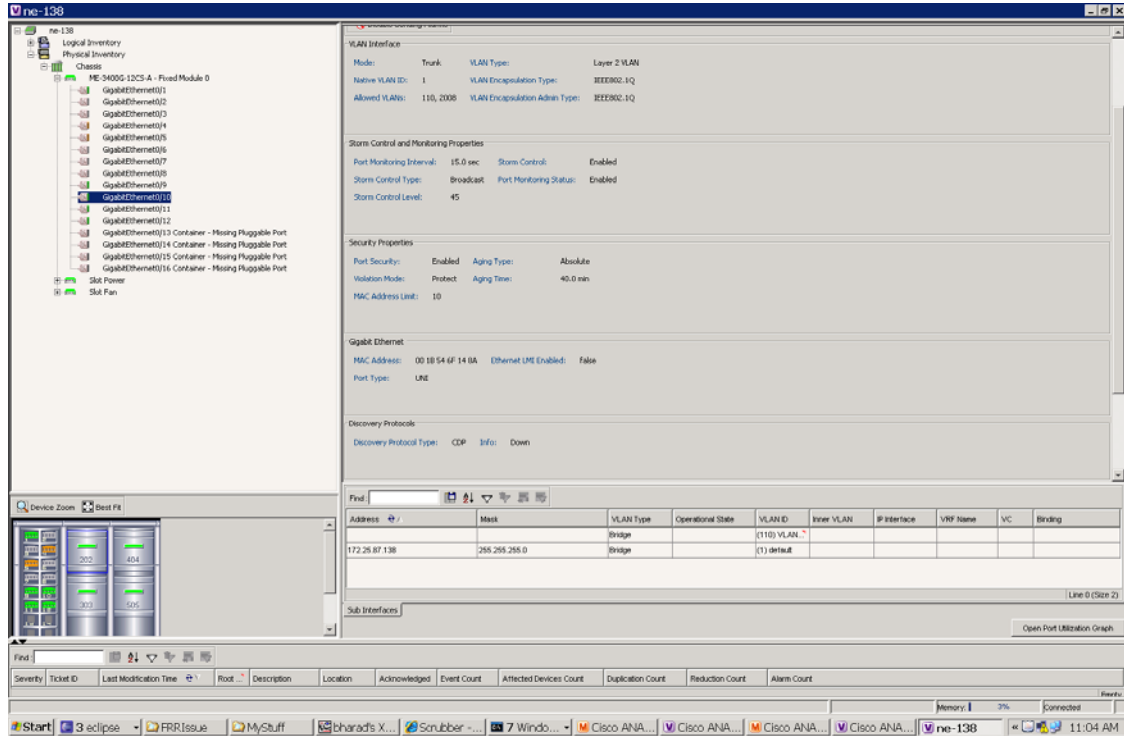
Figure 12-11 EVC Port Properties in Physical Inventory

Table 12-14 describes the information displayed for these properties.

Table 12-14 EVC Port Properties in Physical Inventory

Field	Description
Storm Control and Monitoring Properties Area	
Port Monitoring Interval	Keepalive interval in seconds. The default value is ten seconds.
Storm Control	Status of storm control on the port: Enabled or Disabled.
Storm Control Type	Type of storm the port is configured for protection from: Broadcast, Multicast, or Unicast.
Port Monitoring Status	Status of port monitoring: - Enabled—The switch sends keepalive messages on user network interfaces (UNIs) and enhanced network interfaces (ENIs) and does not send keep alive messages on network node interfaces (NNIs). - Disabled—The switch does not send keepalive messages.
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.

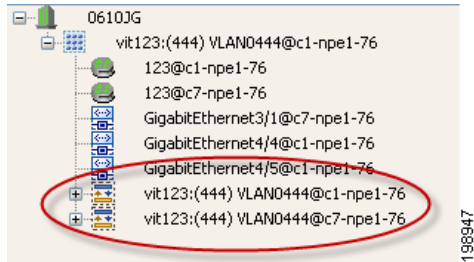
Table 12-14 EVC Port Properties in Physical Inventory (continued)

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

Viewing Virtual Switching Instance Properties

To view VSI properties in Cisco ANA NetworkVision, 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 **Properties**. (See [Figure 12-12](#).)

Figure 12-12 VPLS Forward in Cisco ANA NetworkVision Navigation Pane

The first option opens the inventory window, while the second option opens a standalone VSI Properties window. The information that is displayed is the same for both options.

VSI properties are displayed as shown in Figure 12-13.

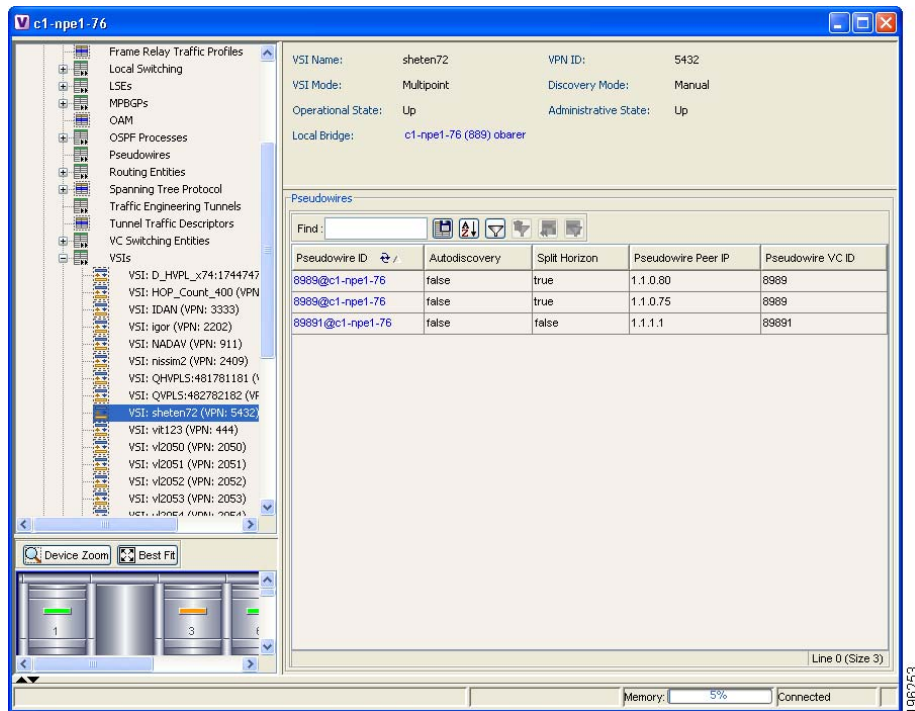
Figure 12-13 VSI Properties in Logical Inventory

Table 12-15 describes the information that is displayed for the selected VSI.

Table 12-15 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.

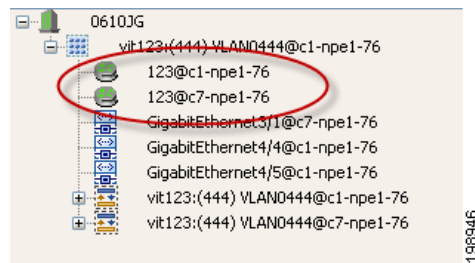
Table 12-15 VSI Properties in Logical Inventory (continued)

Field	Description
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 Cisco ANA NetworkVision navigation pane.

To view pseudowire endpoint properties for a VPLS instance, right-click the required pseudowire endpoint in the navigation pane, and choose **Properties**. (See [Figure 12-14](#).)

Figure 12-14 VPLS Pseudowire in Cisco ANA NetworkVision Navigation Pane

[Figure 12-15](#) shows an example of the Tunnel Properties window that is displayed.

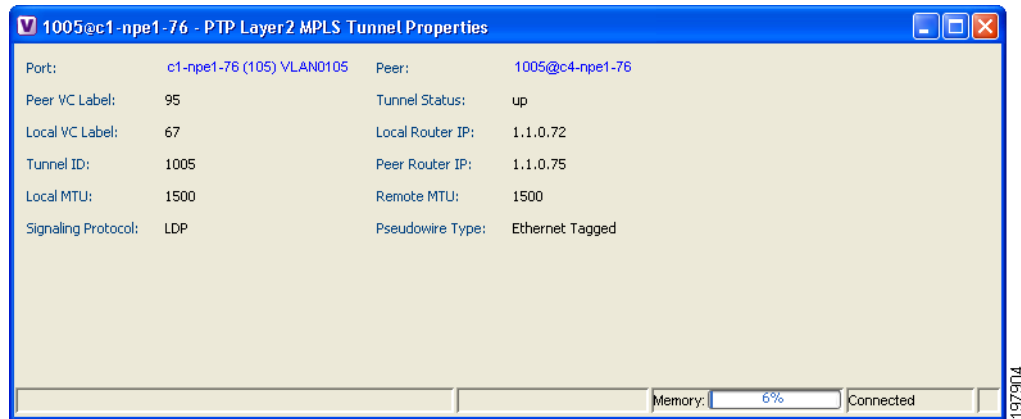
Figure 12-15 VPLS Tunnel Properties Window

Table 12-16 describes the information that is displayed for pseudowire endpoint properties.

Table 12-16 Tunnel Properties Window

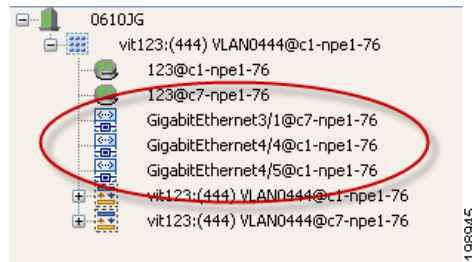
Field	Description
Port	VSI on which the pseudowire is configured, hyperlinked to the VSI in logical inventory.
Peer	Hyperlinked entry to the pseudowire endpoint peer pseudowires in logical inventory.
Peer VC Label	MPLS label that is used by this router to identify or access the tunnel. It is inserted 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. For a complete list of pseudowire types, see the Cisco Active Network Abstraction 3.7.1 Theory of Operations Guide .

Viewing VPLS Access Ethernet Flow Point Properties

The ports that represent the attachment circuits to VPLS instances are displayed under VPLS instances in the Cisco ANA NetworkVision navigation pane.

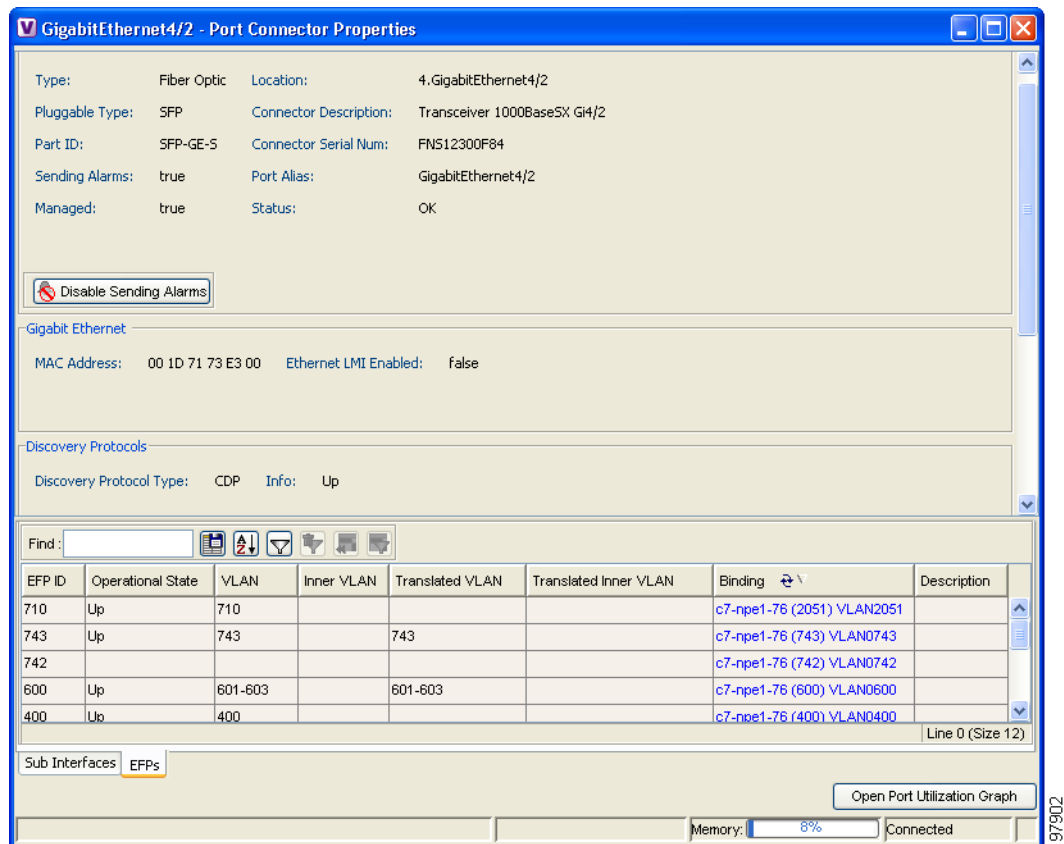
To view the properties for the Access Ethernet Flow Points configured for a VPLS instance, right-click the required interface in the navigation pane, and choose **Properties**. (See [Figure 12-16](#).)

Figure 12-16 VPLS Interface in Cisco ANA NetworkVision Navigation Pane



[Figure 12-17](#) shows an example of the Port Connector Properties window.

Figure 12-17 Port Connector Properties Window



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 17-33](#).
- List of the configured EFPs on the port. For more information on the EFPs table, see [Viewing EFP Properties, page 12-20](#).
- List of VLAN mappings configured on the port. For more information about the VLAN Mappings table, see [Viewing VLAN Mappings, page 12-41](#).

Viewing and Renaming Ethernet Flow Domains

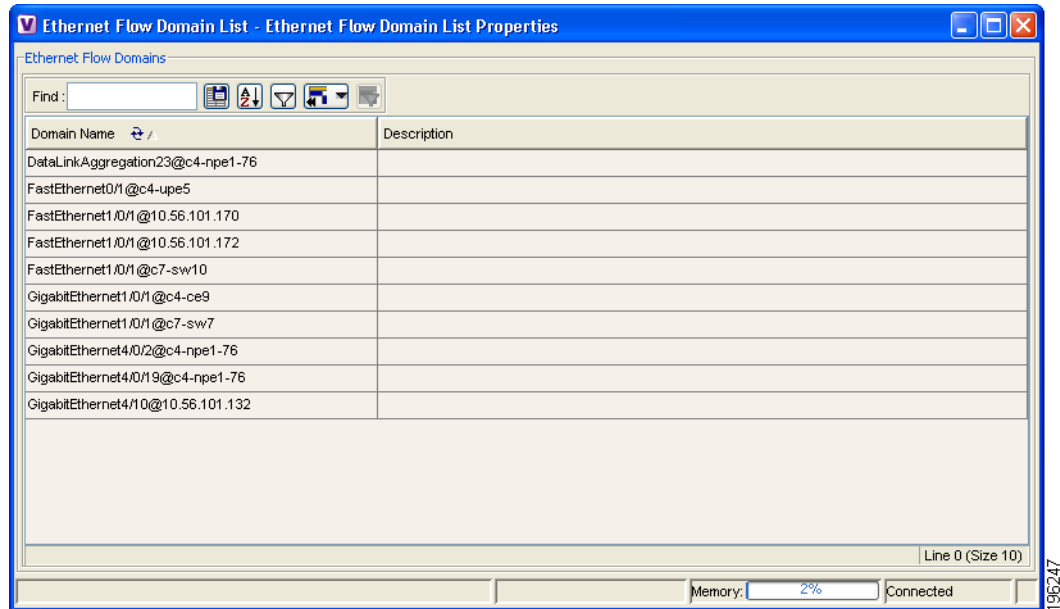
An Ethernet flow domain represents an Ethernet access domain. The Ethernet flow domain holds all network elements between the CE (inclusive, if managed by the SP), up to the SP core (exclusive). This includes CE, access, aggregation, and distribution network elements.

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 NE 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 Cisco ANA NetworkVision, choose **Network Inventory > Ethernet Flow Domains**.

The Ethernet Flow Domain List window is displayed with the name and a brief description for each Ethernet flow domain as shown in [Figure 12-18](#).

Figure 12-18 Ethernet Flow Domains in Logical Inventory

- Step 2** To rename an Ethernet flow domain:
- Right-click the required domain, then choose **Rename**.
 - In the Rename Node dialog box, enter a new name for the domain.
 - Click **OK**.

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

- Step 3** To view Ethernet flow domain properties, do either of the following:
- Right-click the required domain, then choose **Properties**.
 - Double-click the required domain.

The Ethernet Flow Domain Properties window is displayed as shown in [Figure 12-19](#).

Figure 12-19 Ethernet Flow Domain Properties Window

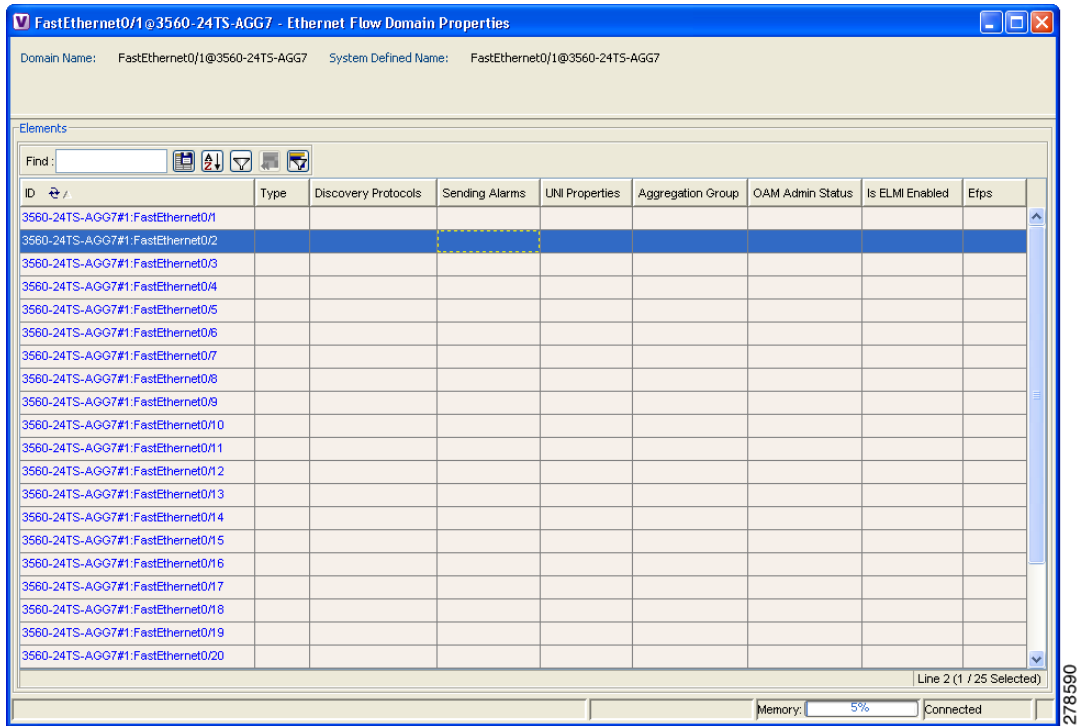


Table 12-17 describes the information displayed in the Ethernet Flow Domain Properties window.



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

Table 12-17 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 Protocol	Discovery protocol used on the interface.
Sending Alarms	Whether the interface is configured for sending alarms: True or False.

- Step 4** To navigate to the individual interface or link aggregation group, click an interface ID 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:

- [VLAN and EFD Discovery, page 12-33](#)
- [VLAN Elements, page 12-34](#)
- [Switching Entities Containing Termination Points, page 12-38](#)
- [Adding VLANs to a Map, page 12-38](#)
- [Removing VLANs from a Map, page 12-41](#)
- [Viewing VLAN Mappings, page 12-41](#)
- [Working with Associated VLANs, page 12-43](#)
- [Viewing VLAN Links Between VLAN Elements and Devices, page 12-46](#)
- [Adding a VLAN Overlay to a Map View, page 12-49](#)
- [Displaying or Hiding VLAN Overlays, page 12-51](#)
- [Removing a VLAN Overlay, page 12-51](#)
- [Viewing VLAN Service Link Properties, page 12-52](#)
- [Viewing REP Information in VLAN Domain Views and VLAN Overlays, page 12-52](#)
- [Viewing REP Properties for VLAN Service Links, page 12-53](#)
- [Viewing STP Information in VLAN Domain Views and VLAN Overlays, page 12-54](#)
- [Viewing STP Properties for VLAN Service Links, page 12-56](#)
- [Viewing VLAN Trunk Group Properties, page 12-57](#)
- [Viewing VLAN Bridge Properties, page 12-59](#)

VLAN and EFD Discovery

When you start the Cisco ANA gateway the first time, Cisco ANA 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.

Similarly, when you restart the gateway, Cisco ANA uses this stabilization period to add existing information on VLANs, VLAN associations, and EFDs to maps and logical inventory. EFDs that were previously stored in the database can be viewed in inventory, and VLANs can be viewed in maps.

During this delay, Cisco ANA does not add VNEs or apply updates to existing VLANs or EFDs.

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

VLAN Elements

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

- [VLAN Elements in Cisco ANA NetworkVision, page 12-34](#)
- [VLANs, page 12-34](#)
- [Switching Entities, page 12-34](#)
- [Ethernet Flow Points, page 12-35](#)

VLAN Elements in Cisco ANA NetworkVision

[Table 12-18](#) describes the icons that Cisco ANA uses to represent VLAN elements.

Table 12-18 *VLAN Elements and Icons in Cisco ANA NetworkVision*

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

VLANs

As described in the [Cisco Active Network Abstraction 3.7.1 Theory of Operations Guide](#), Cisco ANA discovers and allows you to display maps with a network-level view of VLANs.

In Cisco ANA, 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 Cisco ANA NetworkVision 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

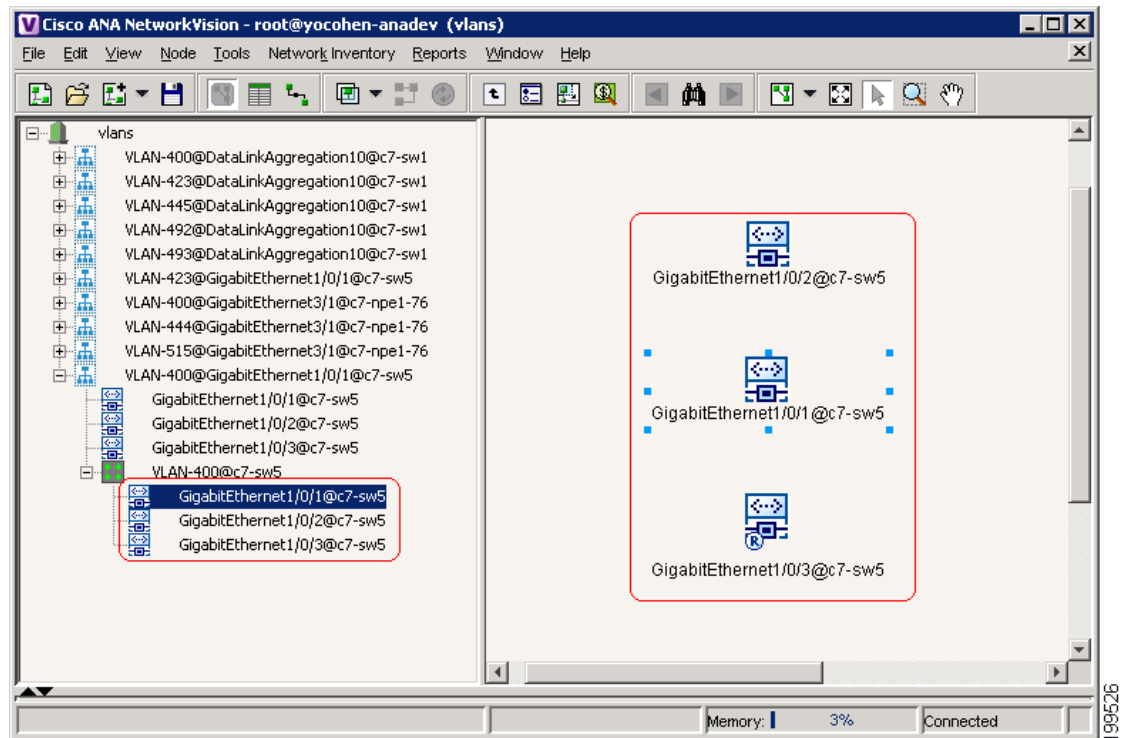
An Ethernet flow point (EFP) can represent a port that is configured for participation in a specific VLAN.

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

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

Figure 12-20 shows an example of EFPs configured as switch ports in Cisco ANA NetworkVision.

Figure 12-20 EFPs in a Cisco ANA NetworkVision Map

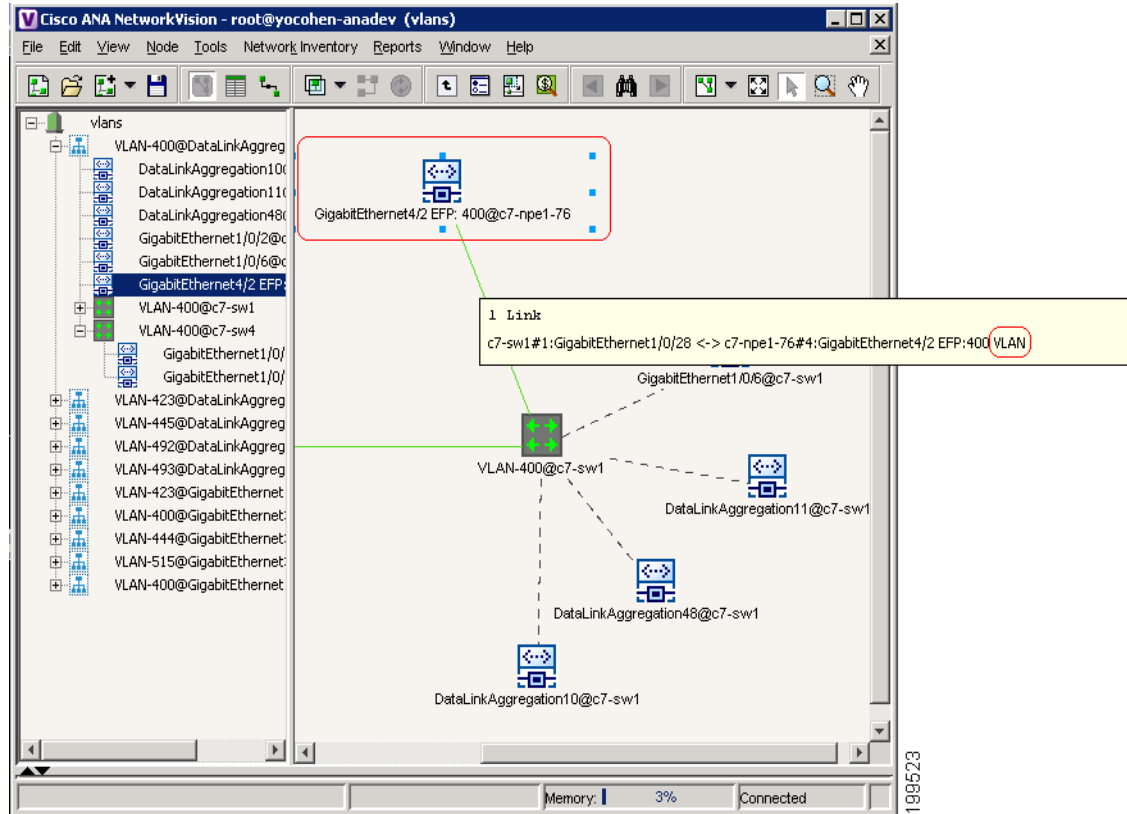


EFPs that are located directly inside a VLAN represent one of the following:

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

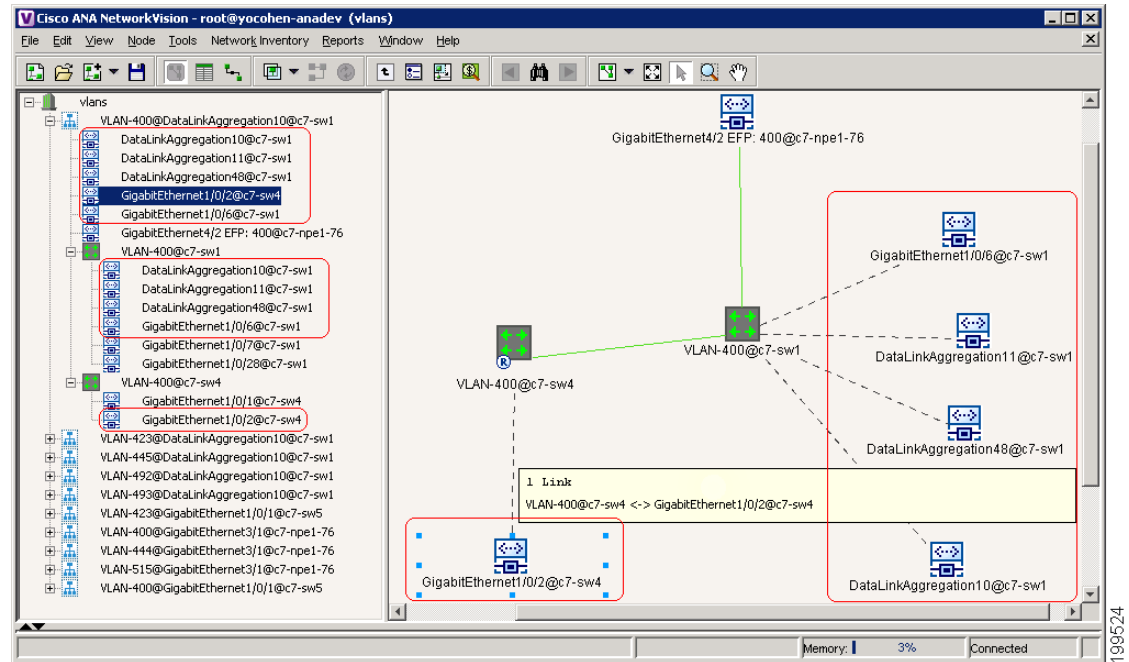
These EFPs are typically connected to a switching entity inside the VLAN by a VLAN link, as shown in Figure 12-21.

Figure 12-21 Termination Point EFP Inside a VLAN



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

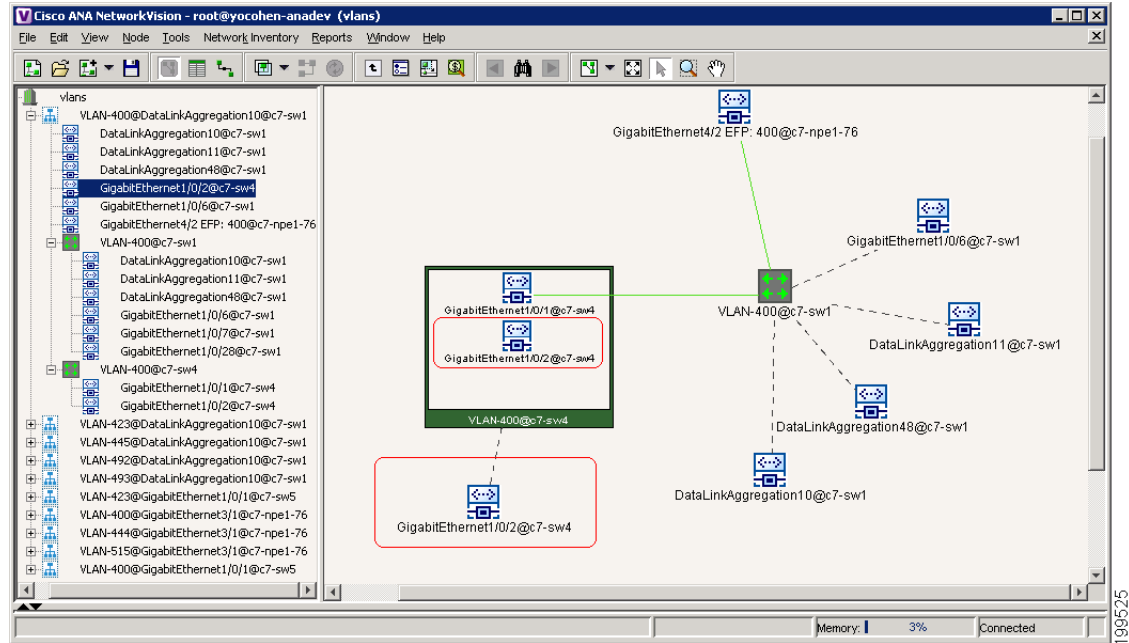
In Cisco ANA, edge EFPs are displayed directly under the VLAN at the same level as their switching entities and are connected to their corresponding switching entities by a dotted link, as shown in Figure 12-22.

Figure 12-22 Edge EFP Inside a VLAN

Expanding the switching entity VLAN-400@c7-sw4 in [Figure 12-22](#) allows us to see in [Figure 12-23](#) that the highlighted EFP (GigabitEthernet1/0/2@c7-sw4) is:

- Not connected to any other EFP by a VLAN link (as opposed to EFP GigabitEthernet1/0/1@c7-sw4).
- Displayed both inside and outside its switching entity.

Figure 12-23 Edge EFP Displayed Inside and Outside of Switching Entity



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 Cisco ANA NetworkVision 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 Cisco ANA and are not currently displayed in the map. For more information about VLANs, see the [Cisco Active Network Abstraction 3.7.1 Theory of Operations Guide](#).

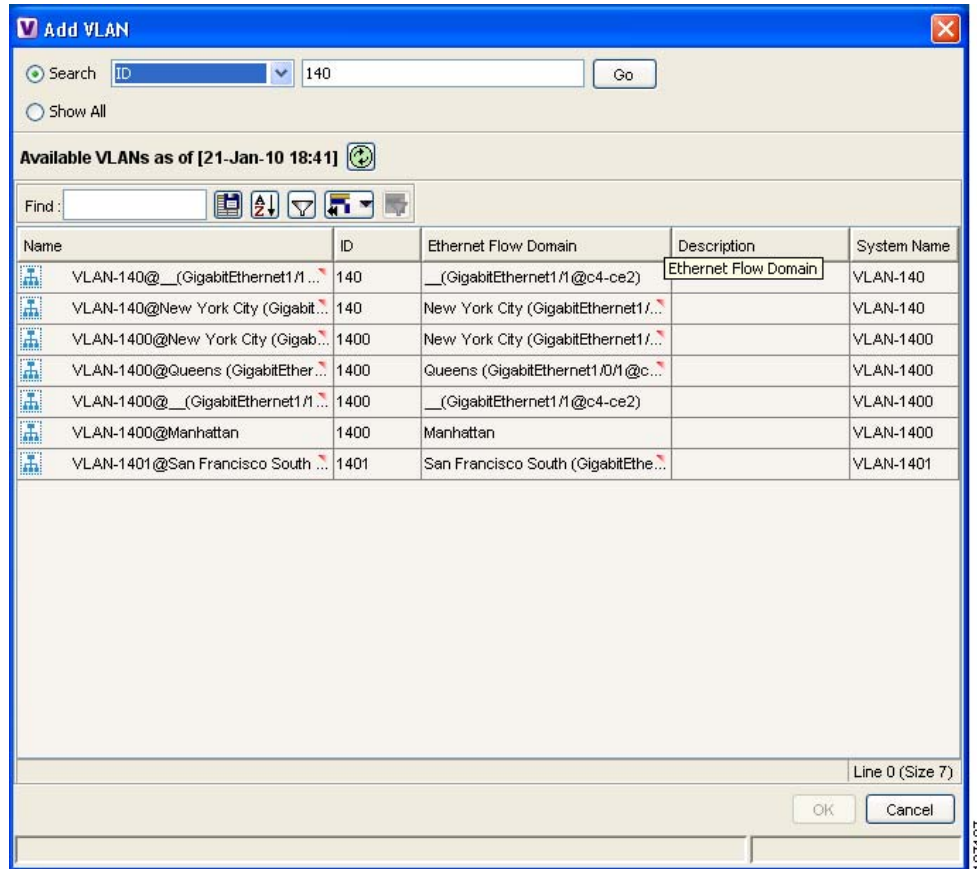


Note

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

To add VLANs to a map:

- Step 1** In Cisco ANA NetworkVision, display the map to which you want to add the VLANs.
- Step 2** Choose **File > Add to Map > VLAN**. The Add VLAN dialog box is displayed as shown in [Figure 12-24](#).

Figure 12-24 Add VLAN Dialog Box

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

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

The search condition is “contains.” Search strings are case-insensitive. For example, if you choose the Name category and enter “net,” Cisco ANA 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.

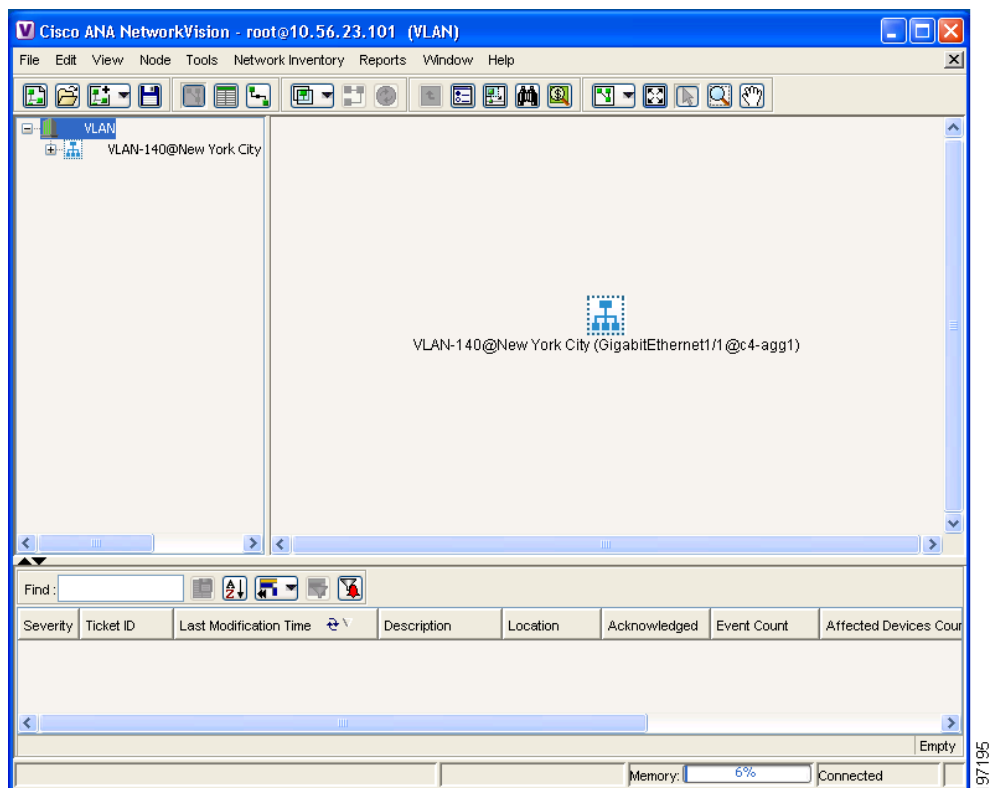
Step 4 Select the VLANs that you want to add to the map.



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

Step 5 Click **OK**.

The VLANs are displayed in the Cisco ANA NetworkVision content pane as shown in [Figure 12-25](#). Any tickets that apply to the VLANs are displayed in the ticket pane.

Figure 12-25 Network VLAN in Cisco ANA NetworkVision Map View

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

- [Viewing and Renaming Ethernet Flow Domains, page 12-30](#)
- [Viewing EFP Properties, page 12-20](#)

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

For REP, see:

- [Viewing Resilient Ethernet Protocol Properties, page 12-10](#)
- [Viewing REP Information in VLAN Domain Views and VLAN Overlays, page 12-52](#)
- [Viewing REP Properties for VLAN Service Links, page 12-53](#)

For STP, see:

- [Viewing Spanning Tree Properties, page 12-7](#)
- [Viewing STP Information in VLAN Domain Views and VLAN Overlays, page 12-54](#)
- [Viewing STP Properties for VLAN Service Links, page 12-56](#)

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 Cisco ANA 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, sites, LCAs, or LCPs from the map without removing the VLAN.

To remove a VLAN, in the Cisco ANA NetworkVision 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 Cisco ANA NetworkVision, double-click the device with VLAN mappings configured.
- Step 2** In the inventory window, choose **Physical Inventory > Chassis > slot > port**.
- Step 3** Click **VLAN Mappings** next to the Subinterfaces tab in the lower portion of the content pane.
- The VLAN Mappings tab is displayed as shown in [Figure 12-26](#).

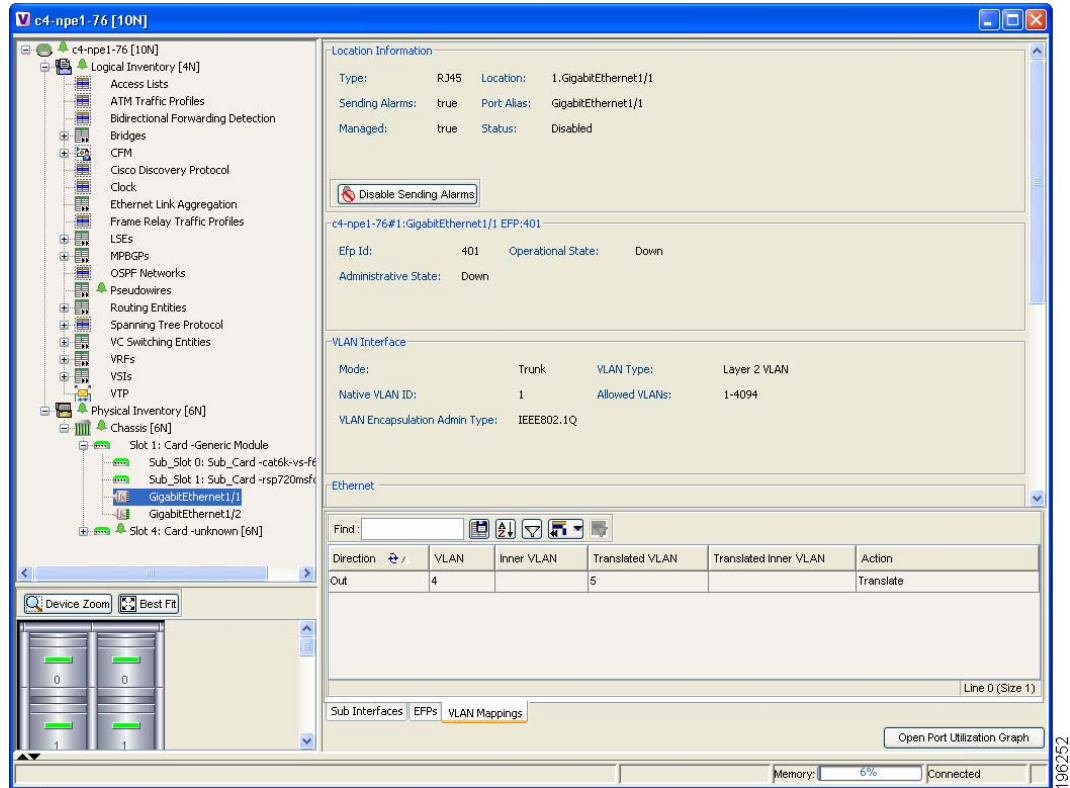
Figure 12-26 VLAN Mappings Tab in Physical Inventory

Table 12-19 describes the information that is displayed in the VLAN Mappings table.

Table 12-19 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

Cisco ANA discovers associations between network VLANs and displays the information in Cisco ANA NetworkVision. Network VLAN associations are represented by VLAN service links, and can be any of the tag manipulation types described in [Table 12-20](#).

Table 12-20 *Types of Tag Manipulations in VLAN Associations*

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

When working with VLANs, you can:

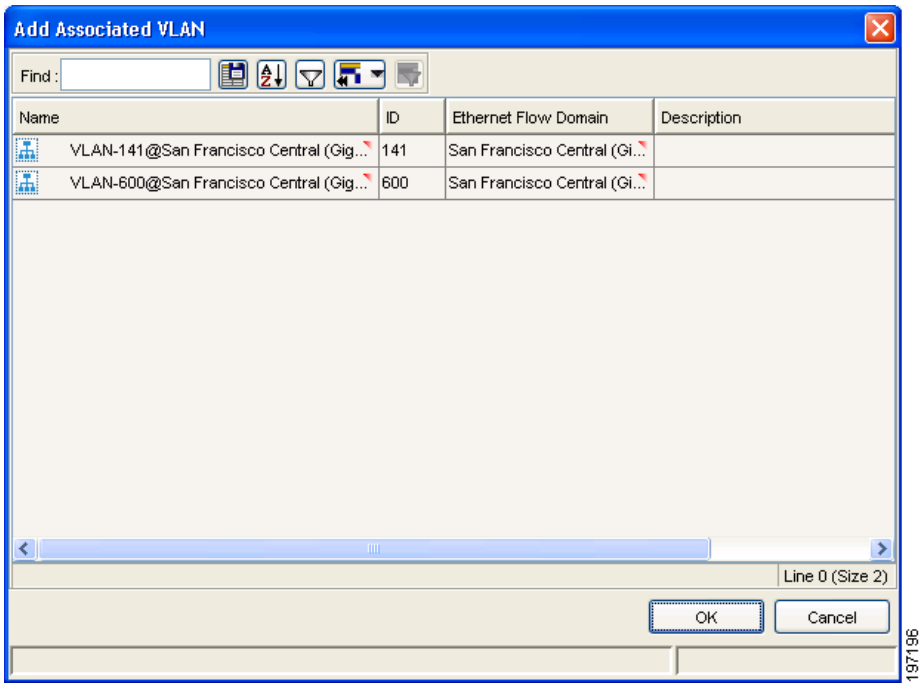
- Add an associated VLAN—See [Adding an Associated VLAN](#), page 12-43.
- View properties for associated VLANs—See [Viewing Associated Network VLAN Service Links and VLAN Mapping Properties](#), page 12-44.

Adding an Associated VLAN

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

-
- Step 1** In Cisco ANA NetworkVision, select the required VLAN in the map view.
- Step 2** Right-click the VLAN and choose **Add Associated VLAN**.
- The Add Associated VLAN table is displayed as shown in [Figure 12-27](#).

Figure 12-27 Add Associated VLAN Window



In this example, the selected network VLAN has two associated VLANs: VLAN-141 and VLAN-600. Table 12-21 describes the information displayed in the Add Associated VLAN table.

Table 12-21 Add Associated VLAN Table

Field	Description
Name	Name of the VLAN.
ID	VLAN identifier.
Ethernet Flow Domain	Name of the Ethernet flow domain.
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 Cisco ANA NetworkVision.

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 Cisco ANA NetworkVision in the thumbnail view.
 - View VLAN mapping properties in the Link Properties window.

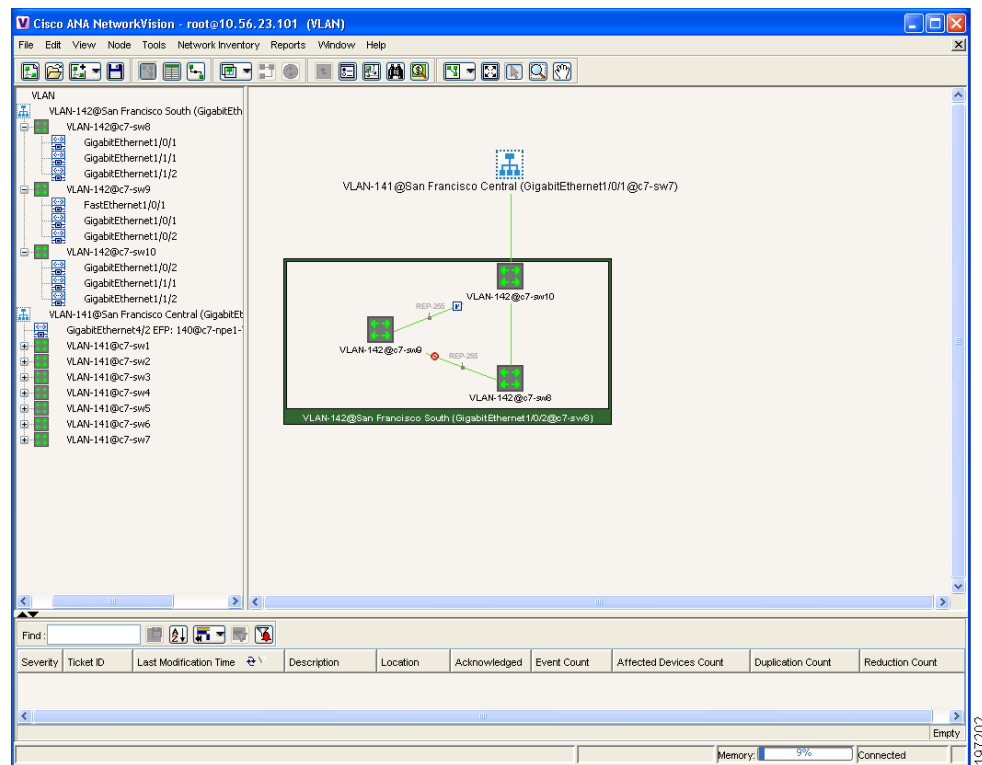
To view associated network VLAN service links and VLAN mapping properties:

- Step 1** Select the required network VLAN in the map view.
- Step 2** Right-click the VLAN, then choose **Show Thumbnail**.

Figure 12-28 shows an example of a network VLAN in the thumbnail view.

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

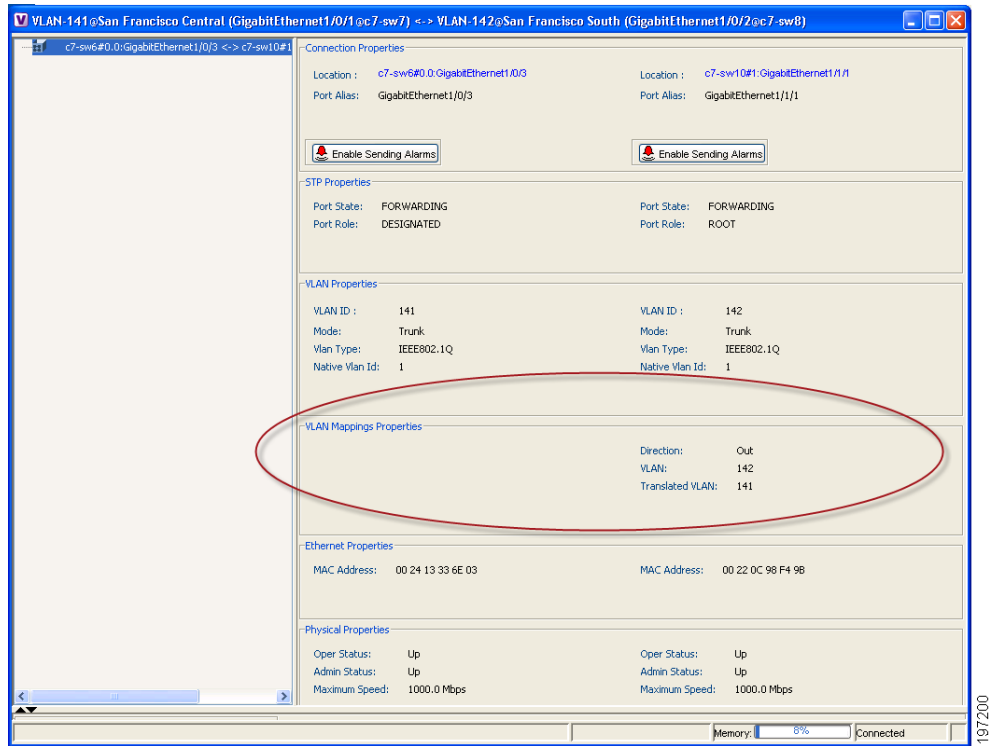
Figure 12-28 VLAN Service Links Between Associated Network VLANs



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

The Link Properties window is displayed as shown in Figure 12-29.

If VLAN tag manipulation is configured on the link, the VLAN Mapping Properties area in the Link Properties window displays the relevant information. For example, in Figure 12-29, the VLAN Mapping Properties area shows that a one-to-one VLAN mapping for VLAN tag 142 to VLAN tag 141 is configured on port GigabitEthernet1/1/1 on c7-sw10 on the egress direction.

Figure 12-29 VLAN Mapping Properties in Link Properties Window

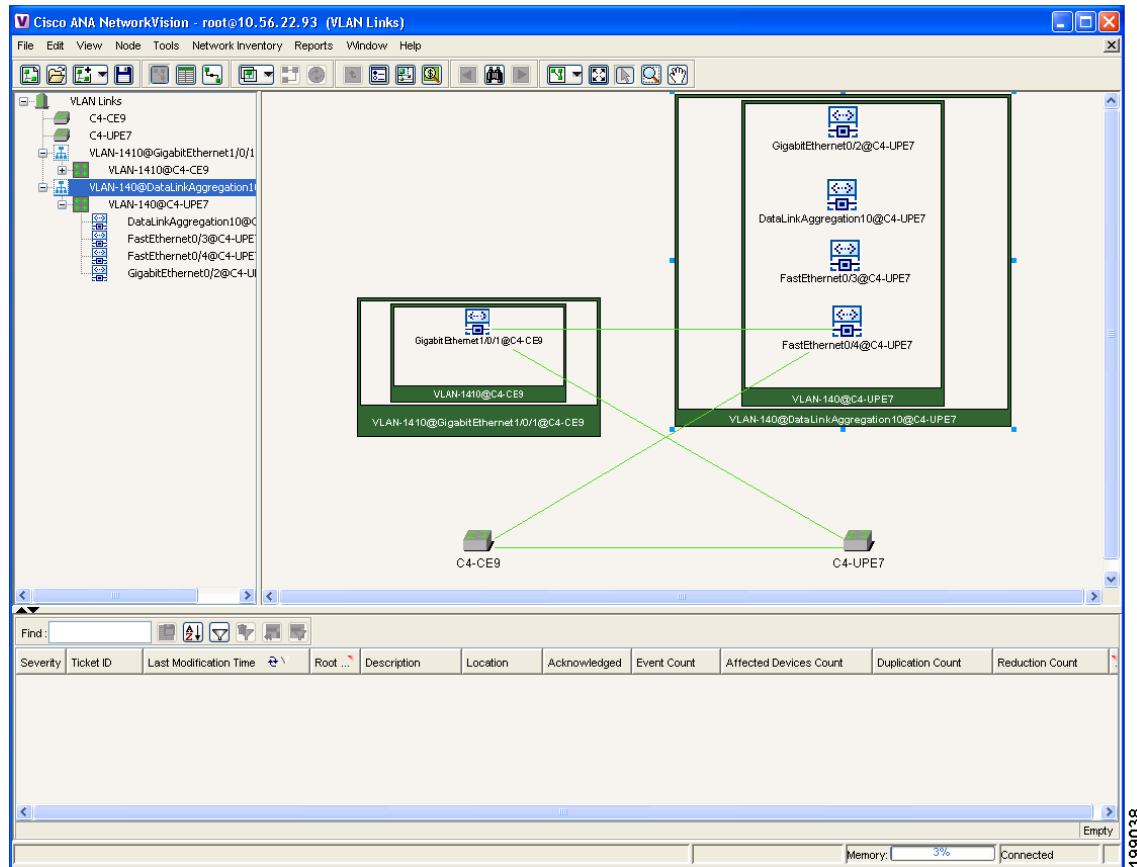
For additional information about viewing network VLAN service link properties, see:

- [Viewing REP Properties for VLAN Service Links, page 12-53](#)
- [Viewing STP Properties for VLAN Service Links, page 12-56](#)

Viewing VLAN Links Between VLAN Elements and Devices

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

For example, assume that you have the following situation, as shown in [Figure 12-30](#) and described in the following paragraphs.

Figure 12-30 VLAN Elements and Devices in Cisco ANA NetworkVision

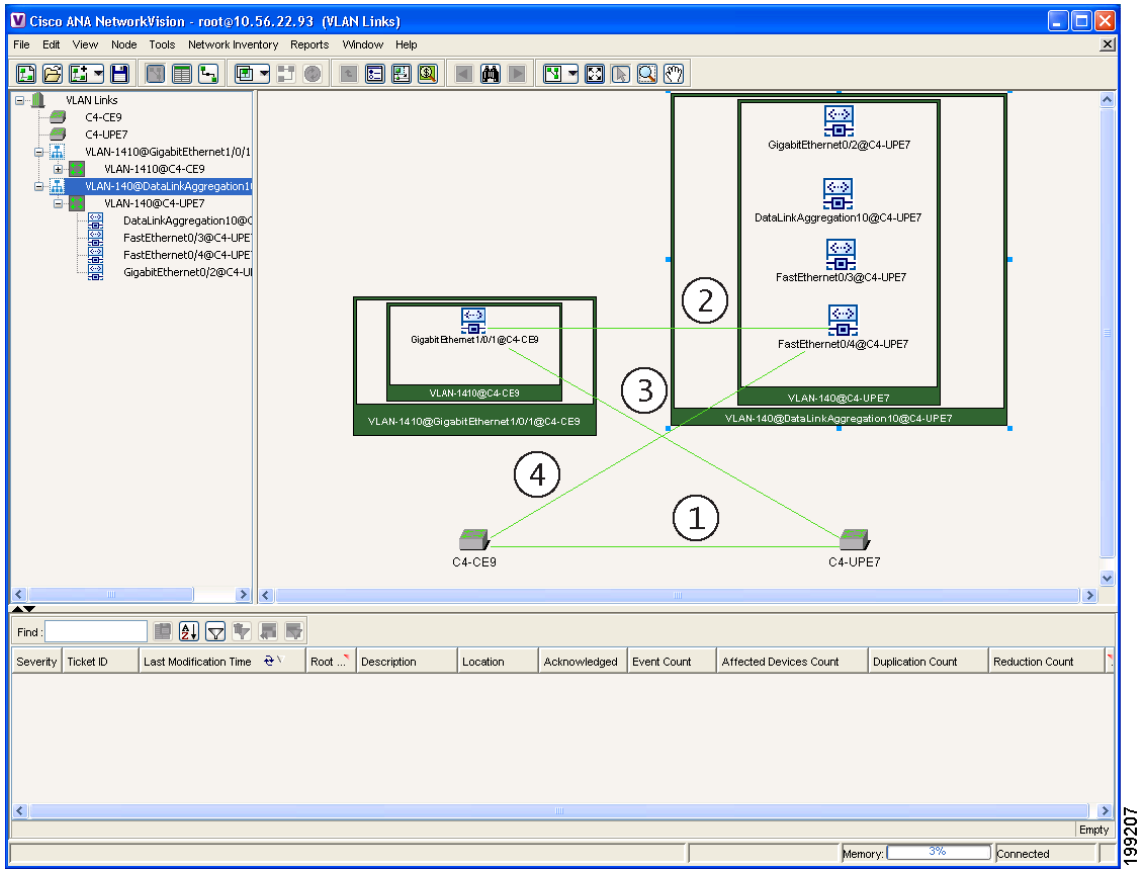
The elements are configured as follows:

- Port GigaEthernet1/0/1 on element C4-CE9 is connected to port FastEthernet0/4 on element C4-UPE7 by an Ethernet topology link.
- Port GigaEthernet1/0/1 on element C4-CE9 is a trunk port associated with VLAN-1410 which is configured on element C4-CE9.
- Port FastEthernet0/4 on element C4-UPE7 is a trunk port associated with VLAN-140 which is configured on element C4-UPE7.
- Port FastEthernet0/4 on element C4-UPE7 has a VLAN mapping to tunnel VLAN-1410 (C-VLAN) in VLAN-140 (SP-VLAN).

In this example, VLAN discovery identified two network VLANs: VLAN-1410 and VLAN-140. Each of these network VLANs contains a switching entity and an EFP that represent the connected ports, GigaEthernet1/0/1 and FastEthernet0/4, respectively.

The four links in the map are identified in [Figure 12-31](#) and described in the following table.

Figure 12-31 Links Between VLAN Elements and Devices



1	The Ethernet topological link between port GigaEthernet1/0/1 on VNE C4-CE9 and portFastEthernet0/4 on VNE C4-UPE7.
2	The VLAN link between GigaEthernet1/0/1@C4-CE9 EFP and FastEthernet0/4@C4-UPE7 EFP.
3	Another view of the VLAN link (link 2), shown as a link between VNE C4-CE9 and FastEthernet0/4@C4-UPE7 EFP.
4	Another view of the VLAN link (link 2), shown as a link between VNE C4-UPE7 and GigaEthernet1/0/1@C4-CE9 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.

Adding a VLAN Overlay to a Map View

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. For more information about VLAN overlays, see the [Cisco Active Network Abstraction 3.7.1 Theory of Operations Guide](#).

To add a VLAN overlay:

-
- Step 1** Display the network map for which you want to create an overlay in Cisco ANA NetworkVision.
 - 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,” Cisco ANA displays overlays that have “net” in their names. The string “net” can be at the beginning, middle, or end of the name, such as Ethernet.
 - Choose **Show All** to view all overlays.
 - Step 4** Select an overlay, then click **OK**.

The network elements and physical links used by the selected VLAN overlay are highlighted in the network map. All other network elements and links are dimmed. The VLAN name is displayed in the title of the window. See [Figure 12-32](#).

Figure 12-32 VLAN Overlay Example

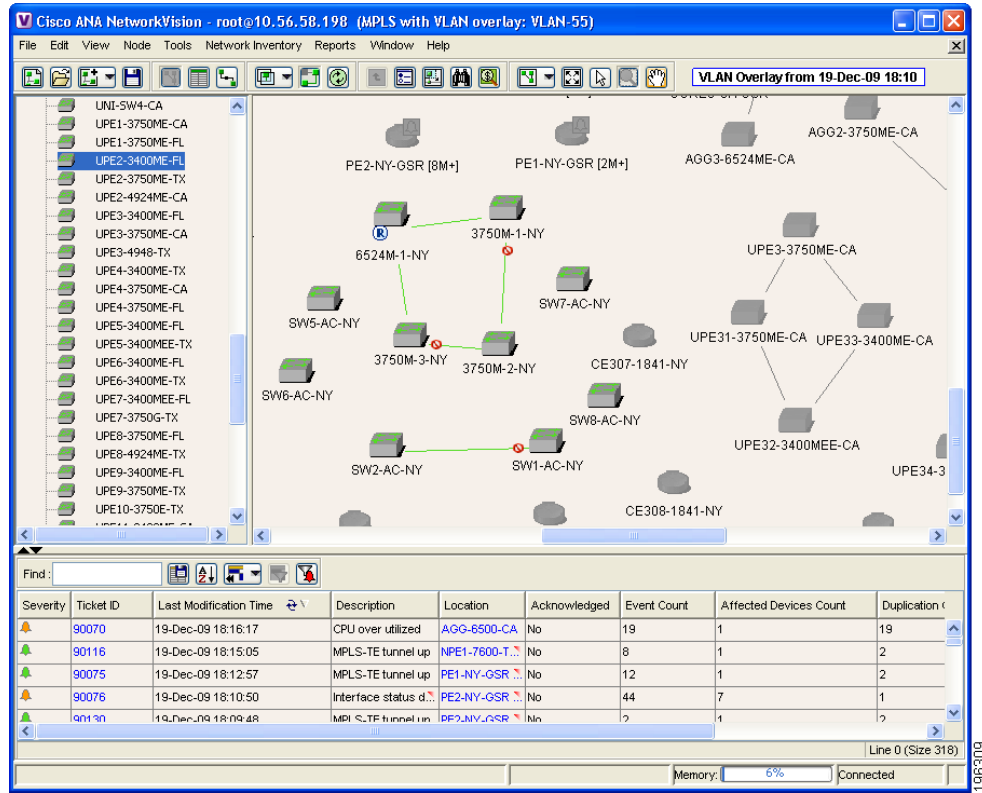
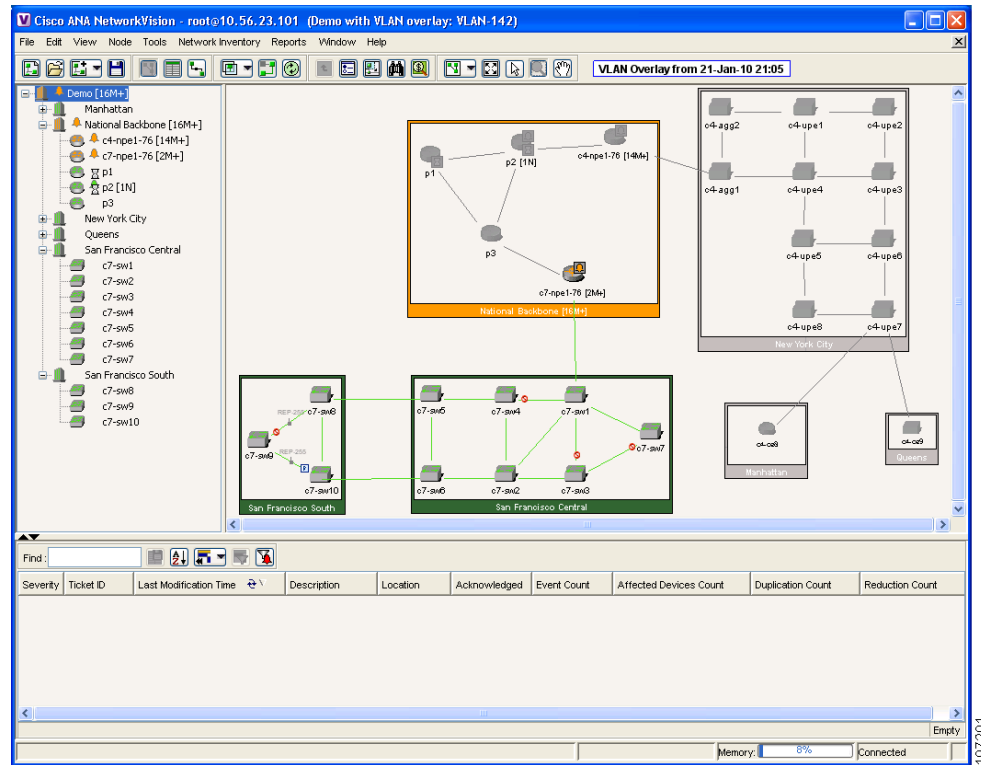


Figure 12-33 shows an example of a VLAN with associated VLANs. In this example:

- VLAN 142 is configured on devices in the San Francisco South aggregation.
- VLAN 141 is configured on devices in the San Francisco Center aggregation and on c7-npe1-76.

Figure 12-33 VLAN Overlay with VLAN Associations**Note**

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

Displaying or Hiding VLAN Overlays

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

**Note**

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

Removing a VLAN Overlay

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

Viewing VLAN Service Link Properties

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

- [Viewing REP Properties for VLAN Service Links, page 12-53](#)
- [Viewing STP Properties for VLAN Service Links, page 12-56](#)
- [Viewing Associated Network VLAN Service Links and VLAN Mapping Properties, page 12-44](#)

Viewing REP Information in VLAN Domain Views and VLAN Overlays

You can view REP segment and port information in Cisco ANA NetworkVision in the map view. The icons displayed depend on whether you view the REP information in the VLAN domain view or in a VLAN overlay. [Table 12-22](#) describes the icons and badges used to represent REP segment and port information.

Table 12-22 REP Icons and Badges in VLAN Domain Views and Overlays

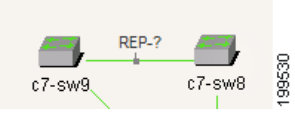
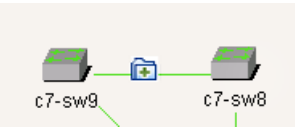
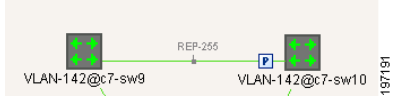
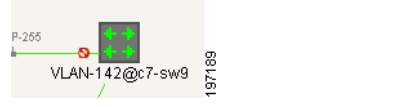
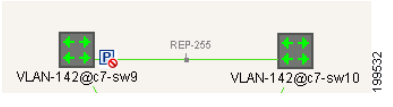
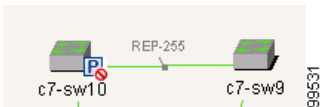
Item	Description	VLAN Domain View	VLAN Overlay
	REP identifier—Uses the format REP- <i>id</i> where <i>id</i> represents the REP segment identifier, such as REP-255.	 The REP identifier is displayed in the domain view if the visual link represents only one link. If the visual link represents more than one link, no REP identifier is displayed.	 The REP identifier is displayed in a VLAN overlay view if all the links represented by the visual link are from the same source to the same destination.
	REP identifier for incorrect configuration—Indicates that the two sides of the link are configured differently or incorrectly.		
	Multiple links icon—Indicates that multiple links or badges are represented by a single visual link.	 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 has a REP identifier or badge.	 The multiple links icon is displayed in a VLAN overlay view if either of the following is true: • More than one link is represented by the visual link and the links have different sources or destinations. • A badge or REP identifier exists on a sublink.

Table 12-22 REP Icons and Badges in VLAN Domain Views and Overlays (continued)

Item	Description	VLAN Domain View	VLAN Overlay
	REP primary badge—Indicates a REP primary port.		
	Blocking badge—Indicates a REP alternate port.		
	Primary and blocking badge—Indicates a REP primary port that is also blocking.		

Viewing REP Properties for VLAN Service Links

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

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

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

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

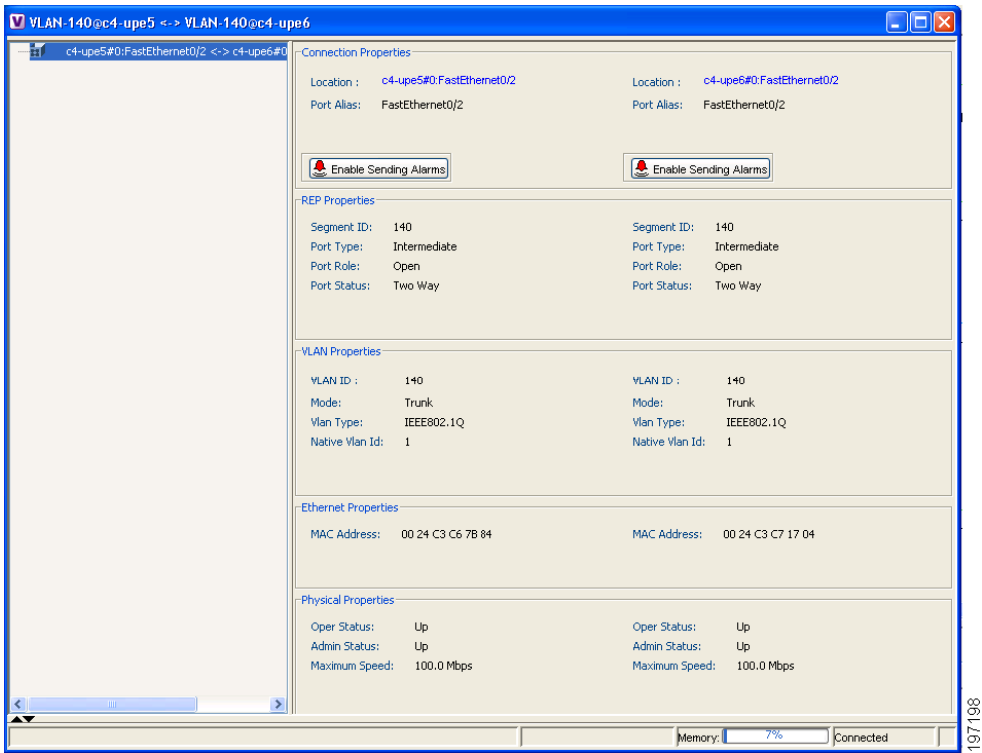


Table 12-23 describes the information that is displayed for REP for each end of the link.

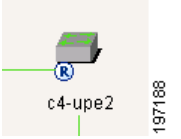
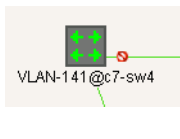
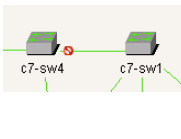
Table 12-23 REP Properties in VLAN Service Link Properties Window

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

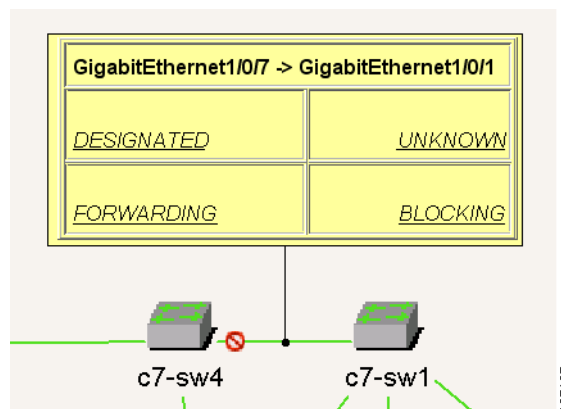
You can view STP segment and port information in Cisco ANA NetworkVision in the map view. The icons displayed depend on whether you view the STP information in the VLAN domain view or in a VLAN overlay. Table 12-22 describes the icons and badges used to represent STP link and port information.

Table 12-24 STP Information in VLAN Domain Views and Overlays

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

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

- Port name
- Port role
- Port state

Figure 12-35 STP Link Information in a VLAN Overlay

- [Viewing VLAN Trunk Group Properties, page 12-57](#)
- [Viewing VLAN Bridge Properties, page 12-59](#)

Viewing STP Properties for VLAN Service Links

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

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

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

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

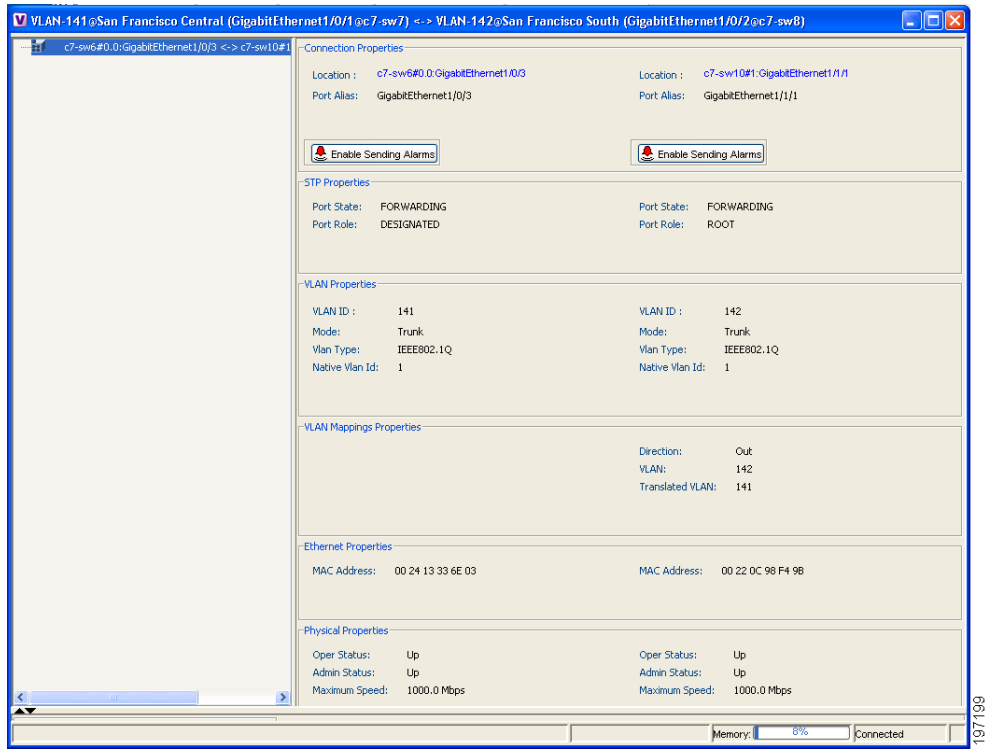


Table 12-25 describes the information that is displayed for STP for the VLAN service link.

Table 12-25 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.

Cisco ANA displays VTP information in the Cisco ANA NetworkVision 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.

Cisco ANA shows all VTP modes: Server, Client, Transparent, and Off. For each mode, Cisco ANA displays the relevant mode information such as VTP domain, VTP mode, VTP version, VLAN trunks, and the trunk encapsulation. Cisco ANA 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.

For additional information about VTP, see the [Cisco Active Network Abstraction 3.7.1 Theory of Operations Guide](#).

To view VTP properties:

-
- Step 1** In Cisco ANA NetworkVision, choose **Network Inventory > VTP Domains**.
- Step 2** Double-click the VTP domain you want to view.
- The VTP Domain Properties window is displayed as shown in [Figure 12-37](#).

Figure 12-37 VTP Domain Properties Window in Logical Inventory

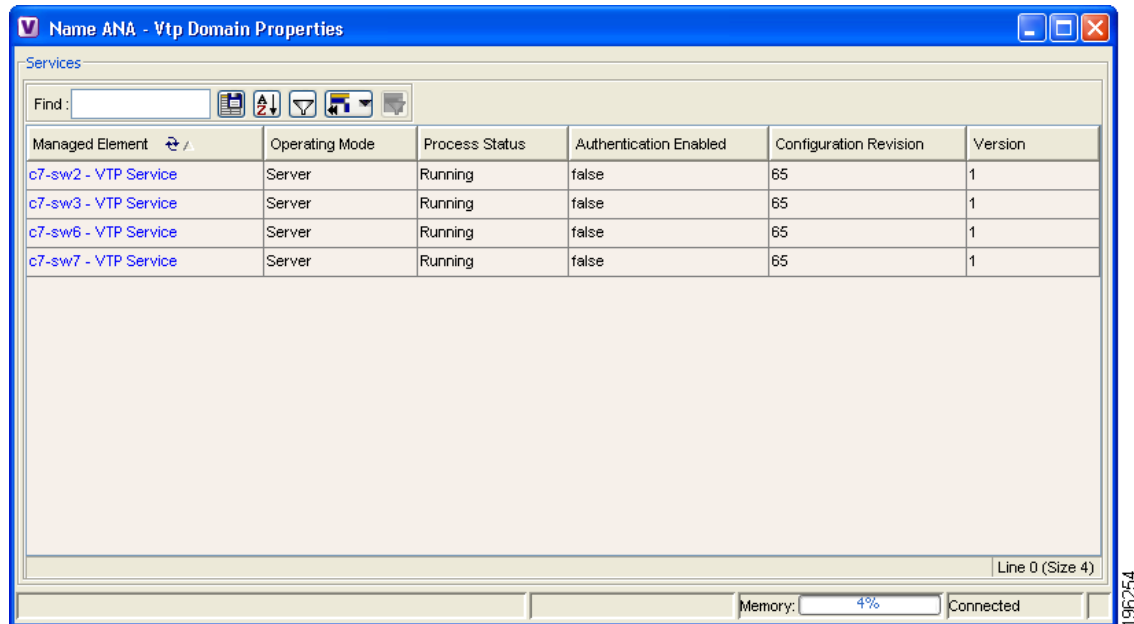


Table 12-26 describes the information that is displayed in the VTP Domain Properties window.

Table 12-26 VTP Domain Properties Window

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

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

Table 12-27 describes the VTP information that is displayed in the inventory window content pane.

Table 12-27 VTP Properties in Inventory

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

Table 12-27 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 Cisco ANA NetworkVision inventory window and choosing Bridges in the Logical Inventory tree. To view VLAN bridge properties:

- Step 1** In Cisco ANA NetworkVision, double-click the device containing the VLAN bridges you want to view.
- Step 2** In the inventory window, choose **Logical Inventory > Bridges > bridge**.
VLAN bridge properties are displayed as shown in [Figure 12-38](#).

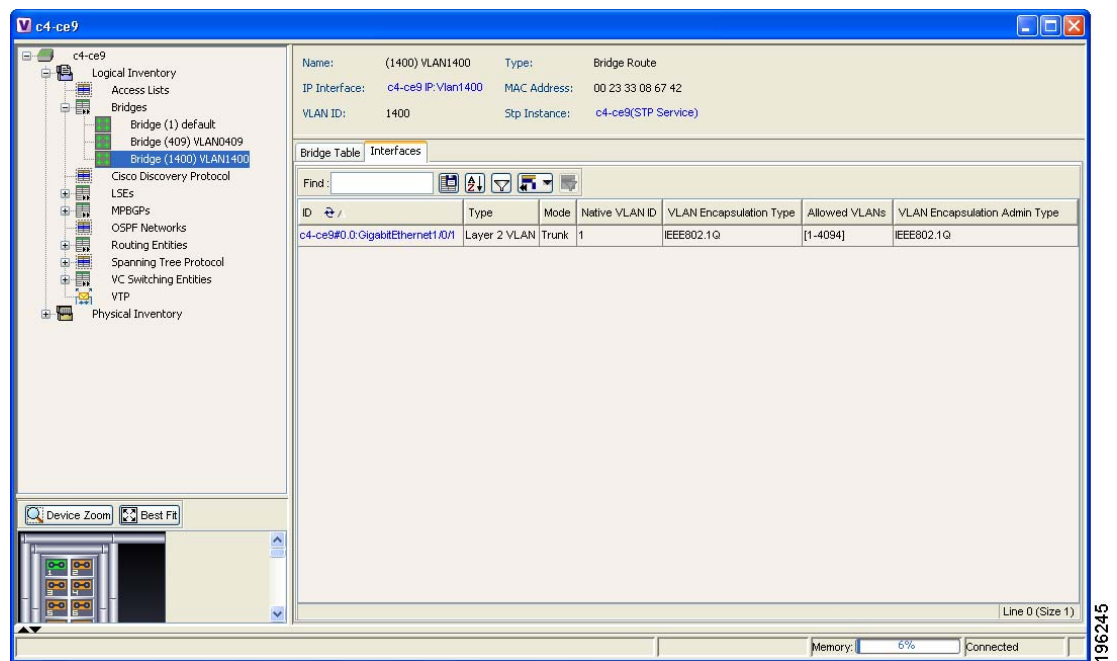
Figure 12-38 VLAN Bridge Properties in Logical Inventory

Table 12-28 describes the information that is displayed. Depending on the bridge configuration, any of the tabs might be displayed for the selected bridge.

Table 12-28 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.
Sending Alarms	Whether or not the port is configured for sending alarms: True or False.
Interfaces Tab	
ID	VLAN interface identifier, hyperlinked to the interface in physical inventory.
Type	VLAN interface type, such as Layer 2 VLAN.
Mode	VLAN interface configuration mode: - Unknown—The interface is not VLAN aware. - Access—Puts the interface into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The interface becomes nontrunking. - Dynamic Auto—The interface can convert the link to a trunk link. The interface becomes a trunk if the neighbor interface is set to Trunk or Dynamic Desirable mode. - Dynamic Desirable—The interface actively attempts to convert the link to a trunk link. The interface becomes a trunk if the neighboring interface is set to Trunk, Dynamic Desirable, or Dynamic Auto mode. Dynamic Desirable is the default mode for all Ethernet interfaces. - Trunk—Puts the interface into permanent trunking mode and negotiates to convert the link into a trunk link. The interface becomes a trunk interface even if the neighbor interface is not a trunk interface. - Dot1Q Tunnel—Configures the interface as a tunnel (nontrunking) port to be connected in an asymmetric link with an 802.1Q trunk port. 802.1Q tunneling is used to maintain customer VLAN integrity across a service provider network.
Native VLAN ID	VLAN Identifier (VID) associated with this VLAN. The range of the VLAN ID is (1 to 4067).
VLAN Encapsulation Type	Type of encapsulation configured on the VLAN, such as IEEE 802.1Q.

Table 12-28 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.

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

Understanding Unassociated Bridges

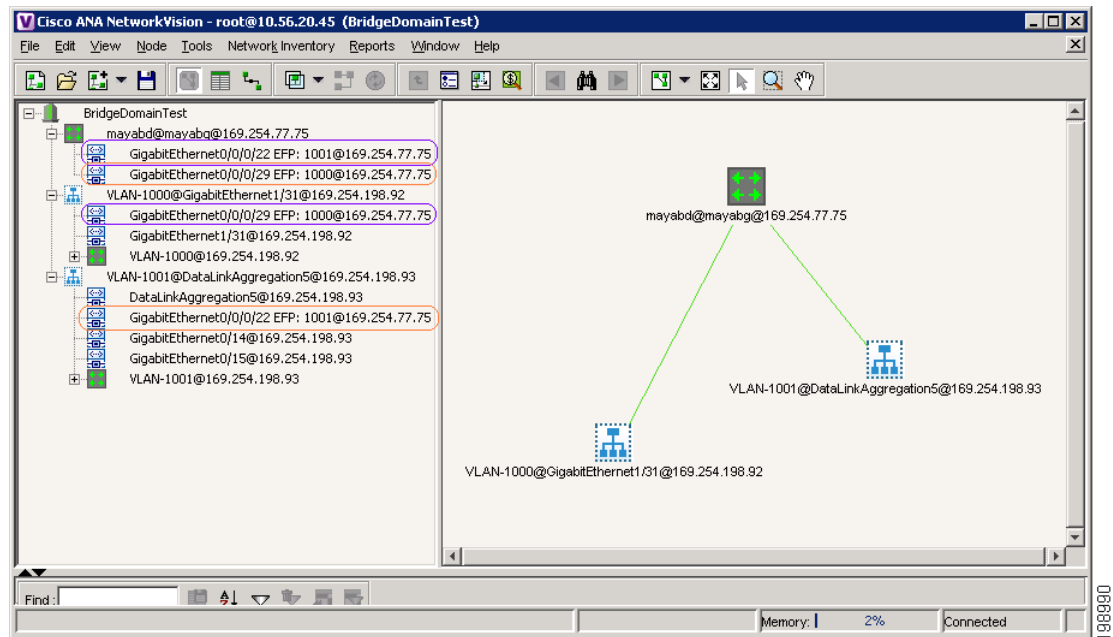
Some switching entities might not belong to a flow domain, such as a network VLAN, a VPLS instance, or a network pseudowire. These switching entities are referred to as *unassociated bridges*.

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

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

Unassociated bridge switching entities can hold Ethernet flow points that serve as termination points on different network VLANs. If these switching entities are added to a map with the relevant VLANs, the links are displayed as shown in [Figure 12-39](#).

Figure 12-39 Switching Entity with EFPs on Different Network VLANs



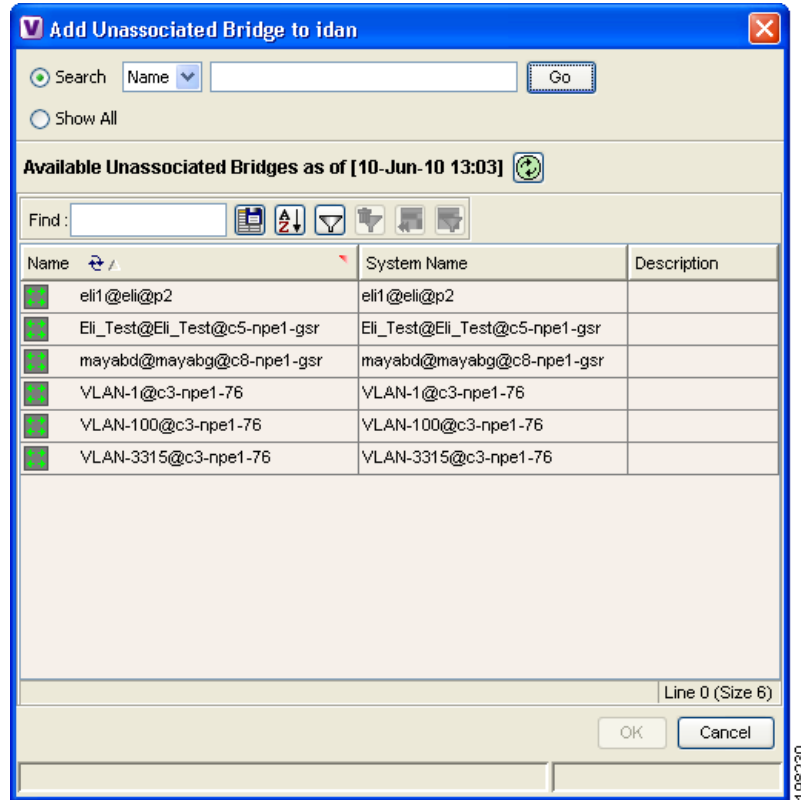
Adding Unassociated Bridges

Cisco ANA enables you to add unassociated bridges to maps and to view their properties in Cisco ANA NetworkVision.

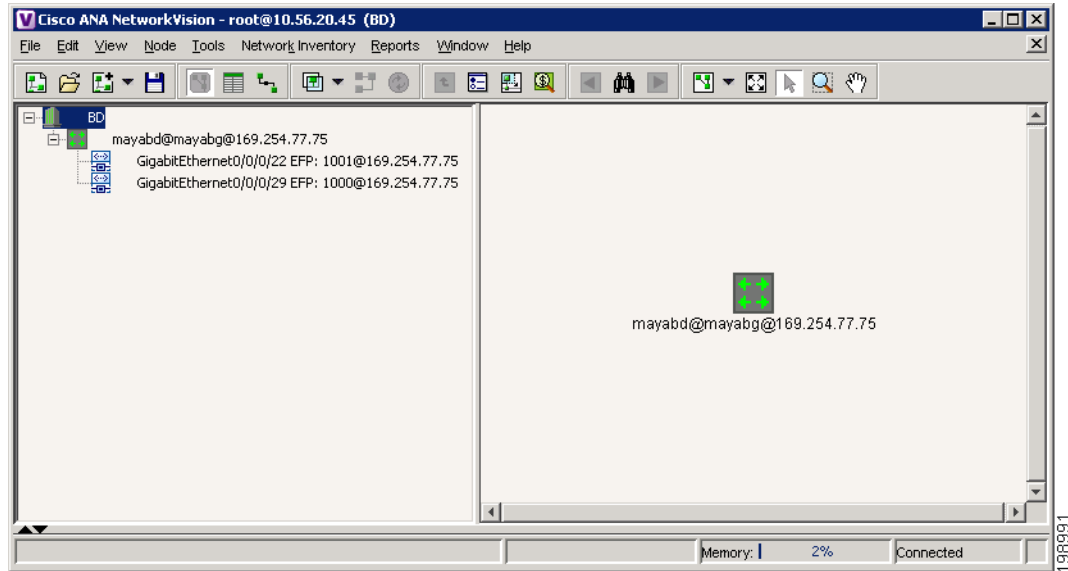
To add an unassociated bridge to a map:

- Step 1** In Cisco ANA NetworkVision, select the required map or domain.
- Step 2** Open the Add Unassociated Bridge dialog box in one of the following ways:
 - Choose **File Add to Map > Unassociated Bridge**.
 - In the toolbar, click **Add to Map** and choose **Unassociated Bridge**.

Figure 12-40 shows an example of the Add Unassociated Bridge dialog box.

Figure 12-40 Add Unassociated Bridge Dialog Box

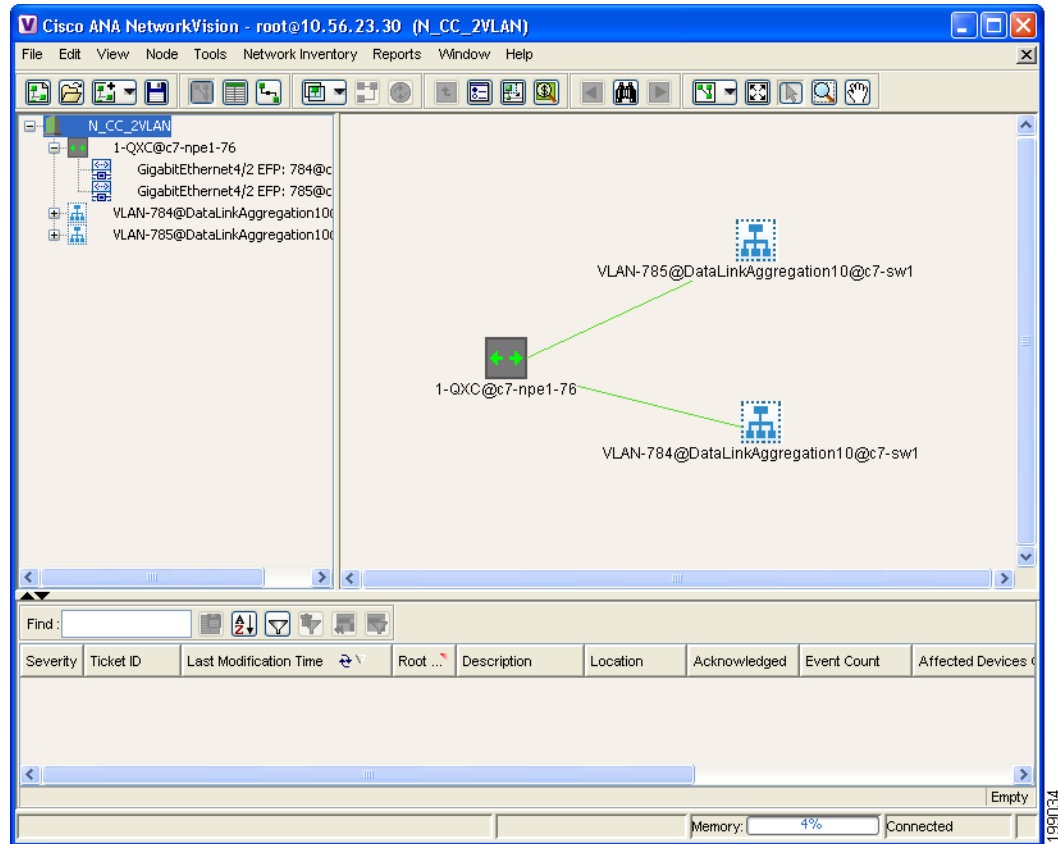
- Step 3** In the Add Unassigned Bridge to *domain* dialog box, select the required bridge and click **OK**. The map is refreshed and displays the newly added bridge as shown in [Figure 12-41](#).

Figure 12-41 Unassociated Bridge in Cisco ANA NetworkVision

Working with Ethernet Flow Point Cross-Connects

Cisco ANA automatically discovers Ethernet flow point (EFP) cross-connects, also known as locally switched EFPs. Cisco ANA 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.

Cisco ANA 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, Cisco ANA displays the links between them and the cross-connect as well. [Figure 12-42](#) shows an example of a cross-connect, two related VLANs, and the links between the cross-connect and the VLANs.

Figure 12-42 EFP Cross-Connect Linked to VLANs in Cisco ANA NetworkVision

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

- [Adding EFP Cross-Connects](#), page 12-65
- [Viewing EFP Cross-Connect Properties](#), page 12-66

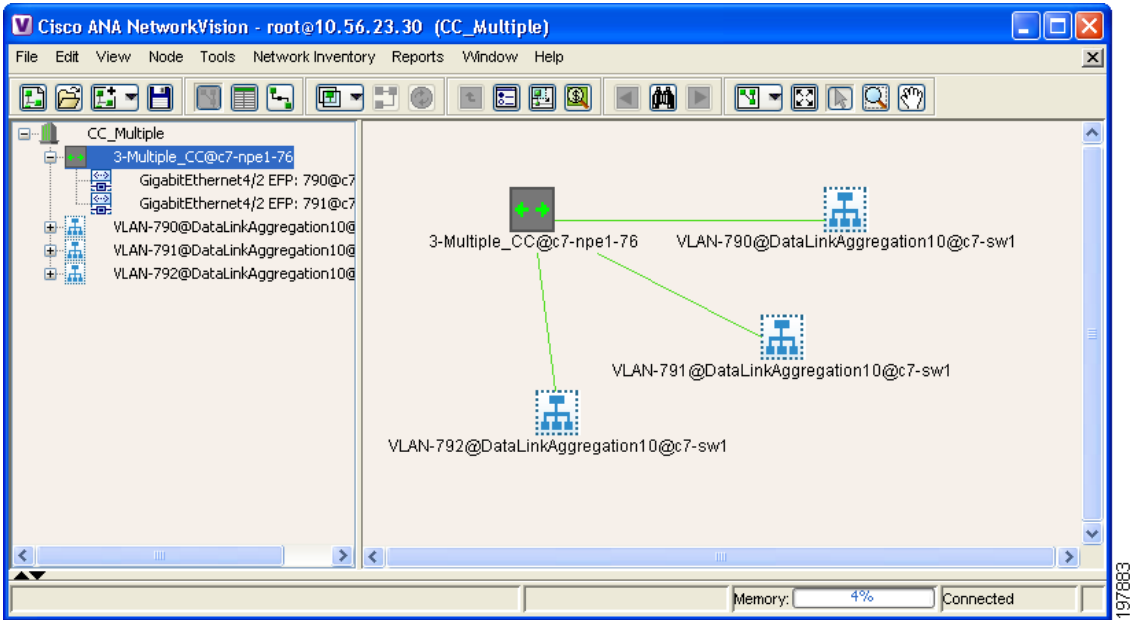
Adding EFP Cross-Connects

To add an EFP cross-connect to a map:

- Step 1** In Cisco ANA NetworkVision, 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 as shown in [Figure 12-43](#).

Figure 12-43 EFP Cross-Connect in Cisco ANA NetworkVision



Viewing EFP Cross-Connect Properties

To view EFP cross-connect properties:

- Step 1 In Cisco ANA NetworkVision, select the EFP cross-connect with the properties you want to view.
 - Step 2 To open the EFP Cross-Connect Properties window, choose **Node > Properties**.
- Figure 12-44 shows an example of the EFP Cross-Connect Properties window.

Figure 12-44 EFP Cross-Connect Properties Window

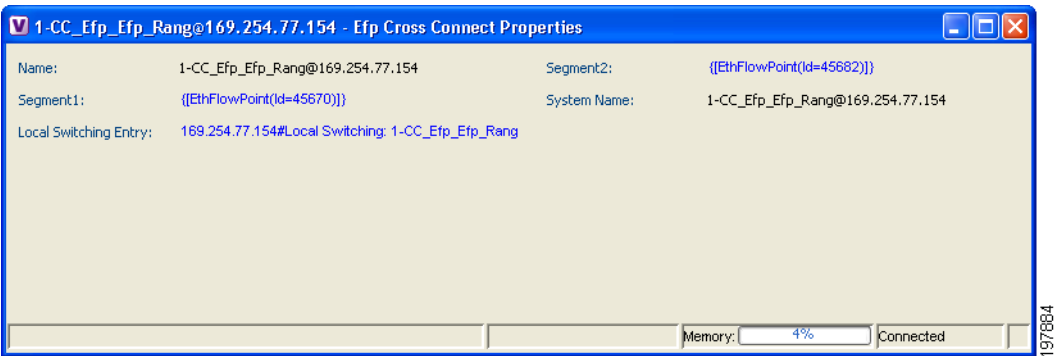


Table 12-29 describes the information displayed in the EFP Cross-Connect Properties window.

Table 12-29 EFP Cross-Connect Properties

Field	Description
Name	EFP cross-connect name.
Segment 1	Identifier of the first cross-connect segment, hyperlinked to its entry in physical inventory.
Segment 2	Identifier of the second cross-connect segment, hyperlinked to its entry in physical inventory.
System Name	Name of system on which the EFP cross-connect is configured.
Local Switching Entry	Hyperlink to the relevant entry in the Local Switching table in logical inventory.

Step 3 To view the Local Switching Entry Properties window, right-click the required EFP cross-connect in Cisco ANA NetworkVision and then choose **Properties**.

Figure 12-45 shows an example of the Local Switching Entry Properties window.

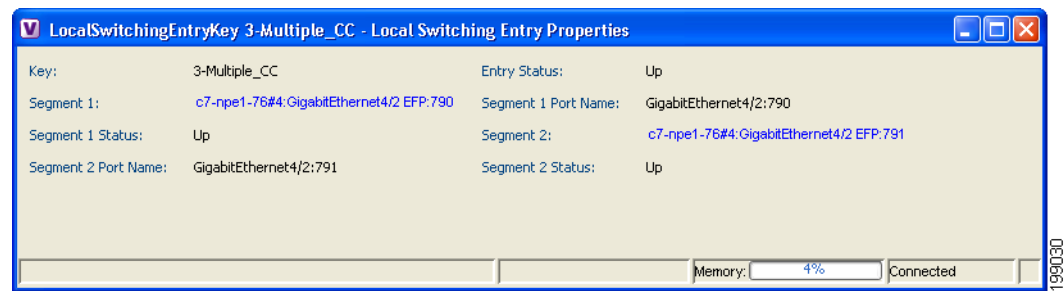
Figure 12-45 Local Switching Entry Properties Window

Table 12-30 describes the information displayed for the EFP cross-connect in the Local Switching Entry Properties window.

Table 12-30 Local Switching Entry Properties

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.

Step 4 To view the EFP cross-connect properties in logical inventory, double-click the required element in Cisco ANA NetworkVision, then choose **Logical Inventory > Local Switching > Local Switching Entity**.

Figure 12-46 shows an example of the Local Switching Table.

Figure 12-46 Local Switching Table in Logical Inventory

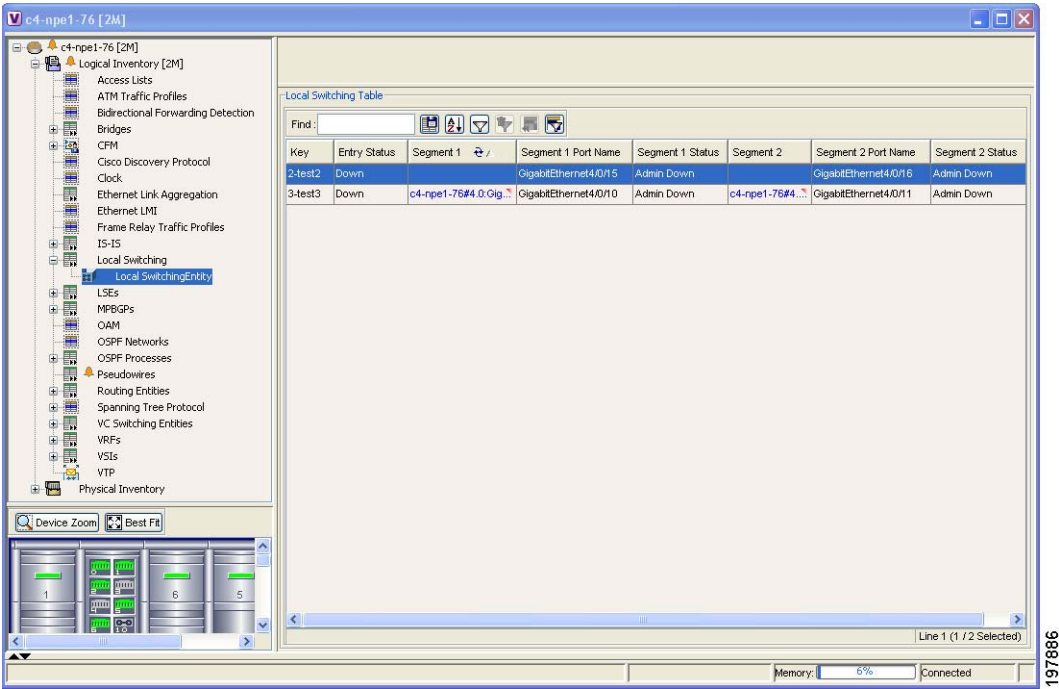


Table 12-31 describes the information displayed in the Local Switching Table.

Table 12-31 Local Switching Table in Logical Inventory

Field	Description
Local Switching Table	
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.

Table 12-31 Local Switching Table in Logical Inventory (continued)

Field	Description
PW Switching Table	
Key	Entry key for the pseudowire.
Entry Status	Status of the pseudowire: Down, Unresolved, or Up.
Segment 1	Identifier of the first segment, hyperlinked to the relevant entry in the Pseudowires Tunnel Edges table in logical inventory.
Segment 1 Port Name	Identifier of the first segment port.
Segment 1 Status	Status of the first segment, such as Admin Up, Admin Down, Oper Down, or Up.
Segment 2	Identifier of the second segment, hyperlinked to the relevant entry in the Pseudowires Tunnel Edges table in logical inventory.
Segment 2 Port Name	Identifier of the second segment port.
Segment 2 Status	Status of the second 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.

Cisco ANA discovers the following VPLS-related information from the network and constructs VPLS instances:

- VSIs
- Pseudowires
- Switching entities
- EFPs

By using the identified VPLS instances, you can:

- Add VPLS instances to a map—See [Adding VPLS Instances to a Map](#), page 12-70.
- Apply VPLS overlays—See [Using VPLS Instance Overlays](#), page 12-71.

- View link details in VPLS overlays—See [Viewing Pseudowire Tunnel Links in VPLS Overlays, page 12-73](#).
- View VPLS-related properties—See [Viewing VPLS-Related Properties, page 12-75](#).
- View VPLS instance properties—See [Viewing VPLS Instance Properties, page 12-75](#).

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

Adding VPLS Instances to a Map

You can add the VPLS instances that Cisco ANA discovers to maps as required.

To add a VPLS instance to a map:

-
- Step 1** In Cisco ANA NetworkVision, select the required map or domain.
- Step 2** Open the Add VPLS Instance to *map* dialog box in either of the following ways:
- In the toolbar, choose **Add to Map > VPLS**.
 - In the menu bar, choose **File > Add to Map > VPLS**.
- Step 3** In the Add VPLS Instance dialog box, do either of the following:
- To search for specific elements:
 - a. Choose **Search**.
 - b. To narrow the display to a range of VPLS instances or a group of VPLS instances, enter a search string in the search field.
 - c. Click **Go**.

For example, if you enter **vpls1**, the VPLS instances that have names containing the string VPLS1 are displayed.
 - To view all available VPLS instances, choose **Show All** and click **Go**.

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

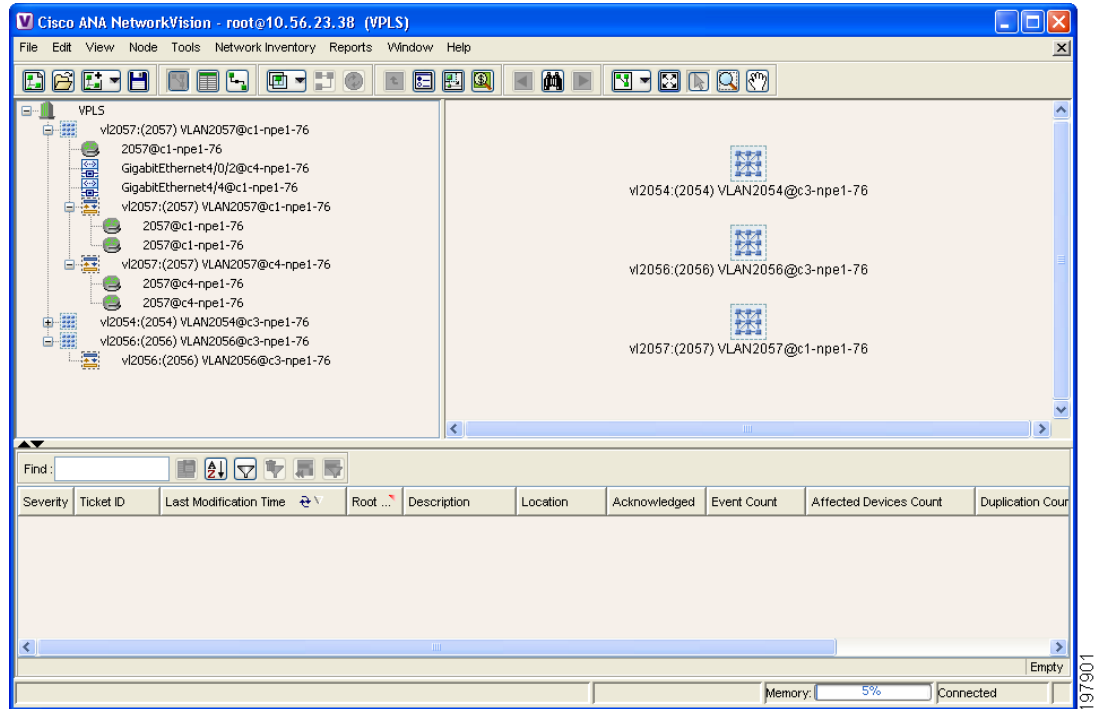


Note If an element is not included in your scope, it is displayed with the locked device icon.

For information about sorting and filtering the table contents, see [Working with Cisco ANA Tables, 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 12-47](#).

Figure 12-47 VPLS Instance in Cisco ANA NetworkVision Map

The VPLS instance information is saved with the map in the Cisco ANA database.

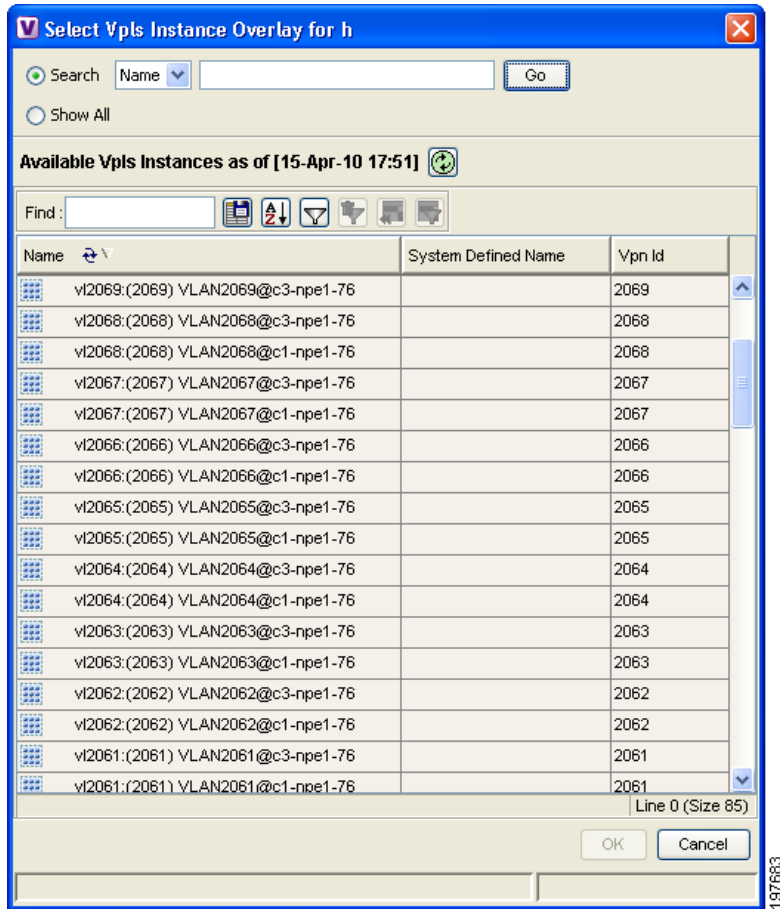
Using VPLS Instance Overlays

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 Cisco ANA NetworkVision, choose the map in which you want to apply an overlay.
- Step 2** From the toolbar, choose **Choose Overlay Type > VPLS**.

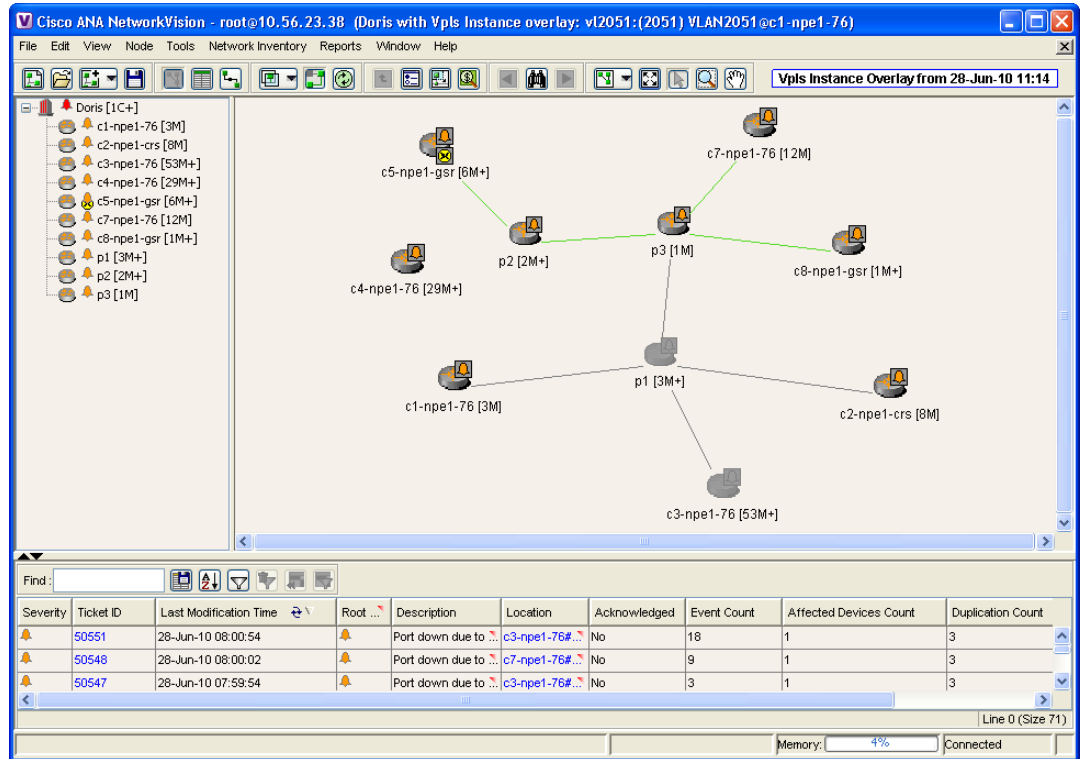
Figure 12-48 shows an example of the Select VPLS Instance Overlay for *map* dialog box.

Figure 12-48 Select VPLS Instance Overlay Dialog Box

Step 3 Select the required VPLS instance for the overlay.

Step 4 Click **OK**.

The elements being used by the selected VPLS instance are highlighted in the map while the other elements are dimmed, as shown in [Figure 12-49](#).

Figure 12-49 VPLS Instance Overlay in Cisco ANA NetworkVision

- 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**.

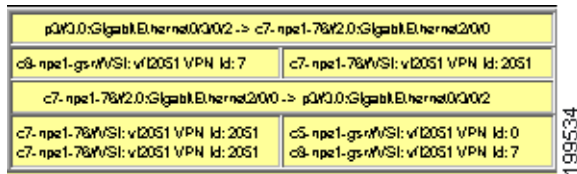
Viewing Pseudowire Tunnel Links in VPLS Overlays

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

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

- Step 1** Right-click the required link in the overlay, and choose **Show Callouts**. The link must be visible (not dimmed) in the map.
- Link information is displayed as shown in [Figure 12-50](#).

Figure 12-50 Link Callout Window for a VPLS Overlay



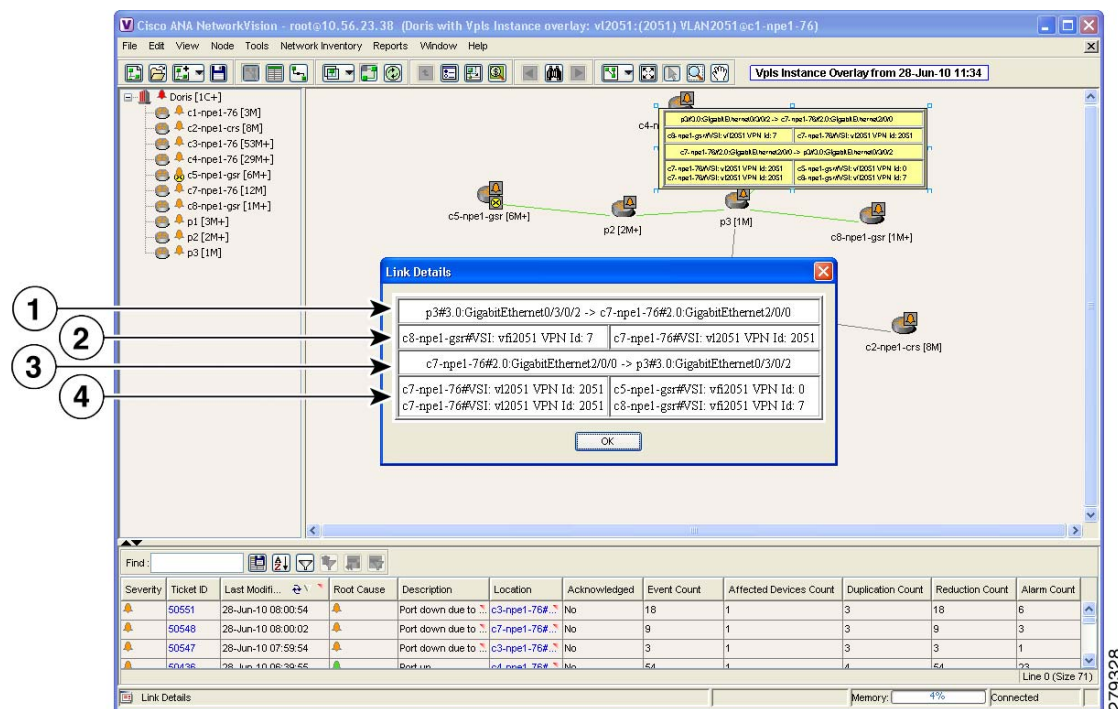
The callout window displays the following information for each link represented by the selected link:

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

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

The details about the link are displayed in the Link Details window as shown in Figure 12-51.

Figure 12-51 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 p3 to c7-npe1-76.
3	Link details and direction. In this example, the link is from c7-npe1-76 to p3.
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

Cisco ANA NetworkVision enables you to view the properties of the following VPLS-related elements:

- VPLS instances—See [Viewing VPLS Instance Properties](#), page 12-75.
- Tunnels—See [Viewing VPLS Core or Access Pseudowire Endpoint Properties](#), page 12-27.
- Port connectors—See [Viewing VPLS Access Ethernet Flow Point Properties](#), page 12-29.

Viewing VPLS Instance Properties

To view the properties of a VPLS instance in Cisco ANA NetworkVision, open the VPLS Instance Properties window in either of the following ways:

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

Figure 12-52 shows an example of the VPLS Instance Properties window.

Figure 12-52 VPLS Instance Properties Window

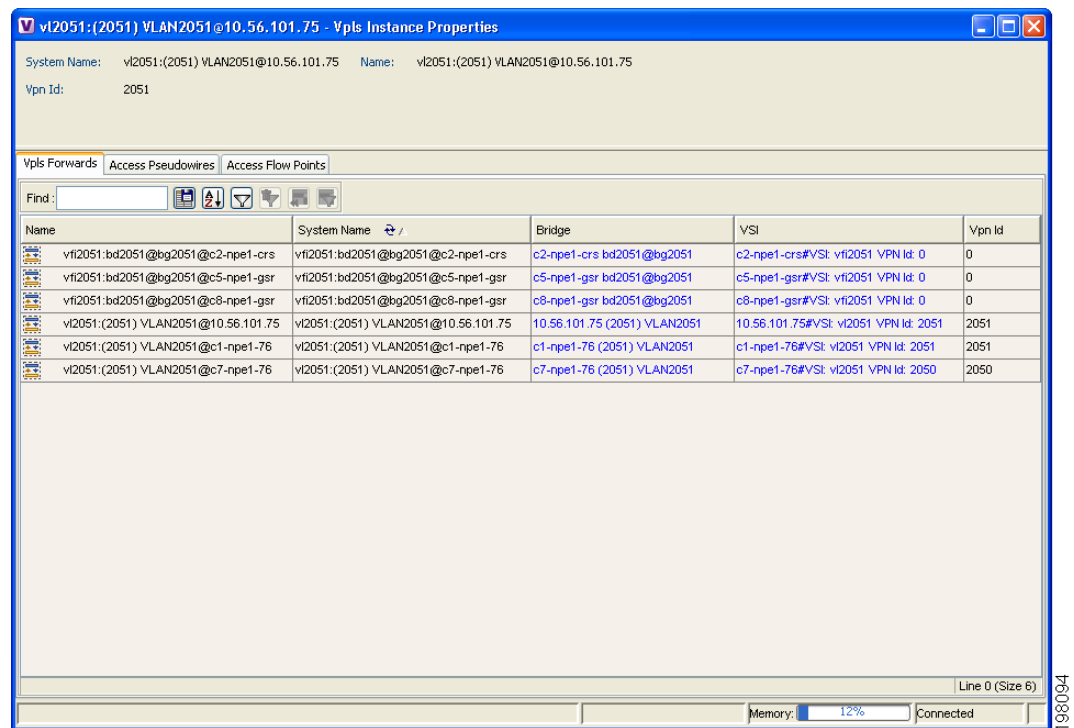


Table 12-32 describes the information that is displayed for VPLS instance properties.

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

Table 12-32 VPLS Instance Properties

Field	Description
System Name	Name that Cisco ANA assigns to the VPLS instance.
Name	User-defined name of the VPLS instance. When the VPLS instance is created, the system name and this name are the same. If you change the name of the VPLS instance (right-click, then choose Rename), the changed name appears in this field whereas the system name retains the original name.
VPN ID	VPN identifier used in an MPLS network to distinguish between different VPLS traffic.
VPLS Forwards Tab	
Name	User-defined name of the VPLS forward.
System Name	Name that Cisco ANA assigns to the VPLS forward.
Bridge	Bridge that the VSI is configured to use, hyperlinked to the bridge table in logical inventory.
VSI	VSI hyperlinked to the relevant entry in logical inventory.
VPN ID	VPN identifier for the VSI.
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. For a complete list of pseudowire types, see the Cisco Active Network Abstraction 3.7.1 Theory of Operations Guide .
Pseudowire Edge Binding Type	Pseudowire endpoint association: • 0—Unknown • 1—Connection termination point • 2—Ethernet flow point • 3—Switching entity • 4—Pseudowire switching entity • 5—VPLS forward

Table 12-32 VPLS Instance Properties (continued)

Field	Description
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.

Working with Pseudowires and Pseudowire Overlays

Cisco ANA supports the discovery and modeling of Any Transport over MPLS (AToM) and Ethernet over MPLS (EoMPLS) domains that span multisegment pseudowires. This support enables you to:

- Add discovered pseudowires to a map—See [Adding Pseudowires to a Map](#), page 12-77.
- Ping a pseudowire—See [Pinging a Pseudowire](#), page 12-80.
- View information about pseudowires—See [Displaying Pseudowire Information](#), page 12-83.
- Apply pseudowire overlays—See [Applying Pseudowire Overlays](#), page 12-85.
- View multisegment pseudowire properties—See [Viewing Pseudowire Properties](#), page 12-86.

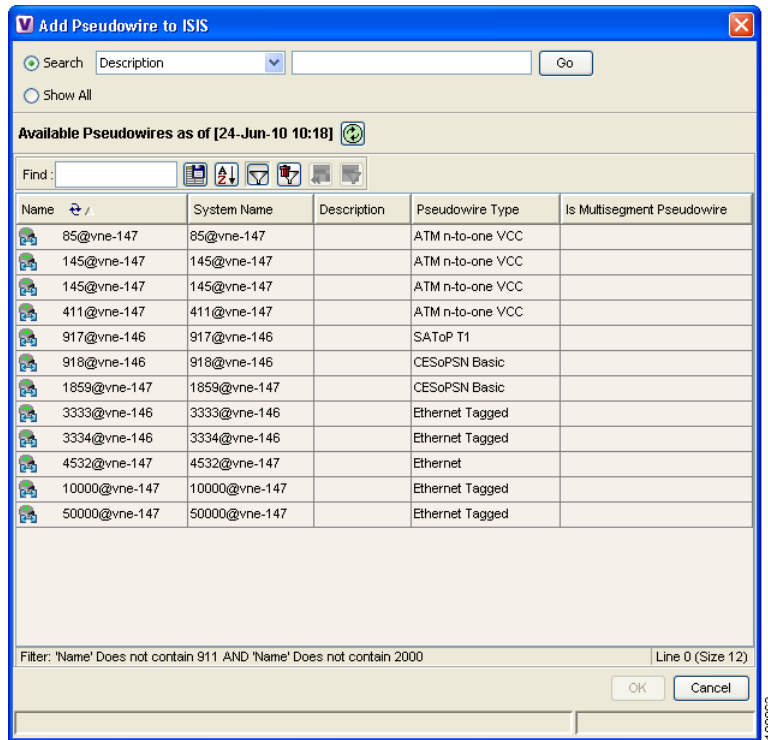
Adding Pseudowires to a Map

You can add a pseudowire that Cisco ANA discovers to maps as required.

To add a pseudowire to a map:

-
- Step 1** In Cisco ANA NetworkVision, select the required map or domain.
- Step 2** Open the Add Pseudowire to *map* dialog box in either of the following ways:
- In the toolbar, choose **Add to Map > Pseudowire**.
 - In the menu bar, choose **File > Add to Map > Pseudowire**.

[Figure 12-53](#) shows an example of the Add Pseudowire dialog box.

Figure 12-53 Add Pseudowire Dialog Box

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

- To search for specific elements:
 - a. Choose **Search**.
 - b. To narrow the display to a range of pseudowire or a group of pseudowires, enter a search string in the search field.
 - c. Click **Go**.

For example, if you enter **pseudo1**, the pseudowires that have names containing the string “pseudo1” are displayed.
- To view all available pseudowires, choose **Show All** and click **Go**.

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



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

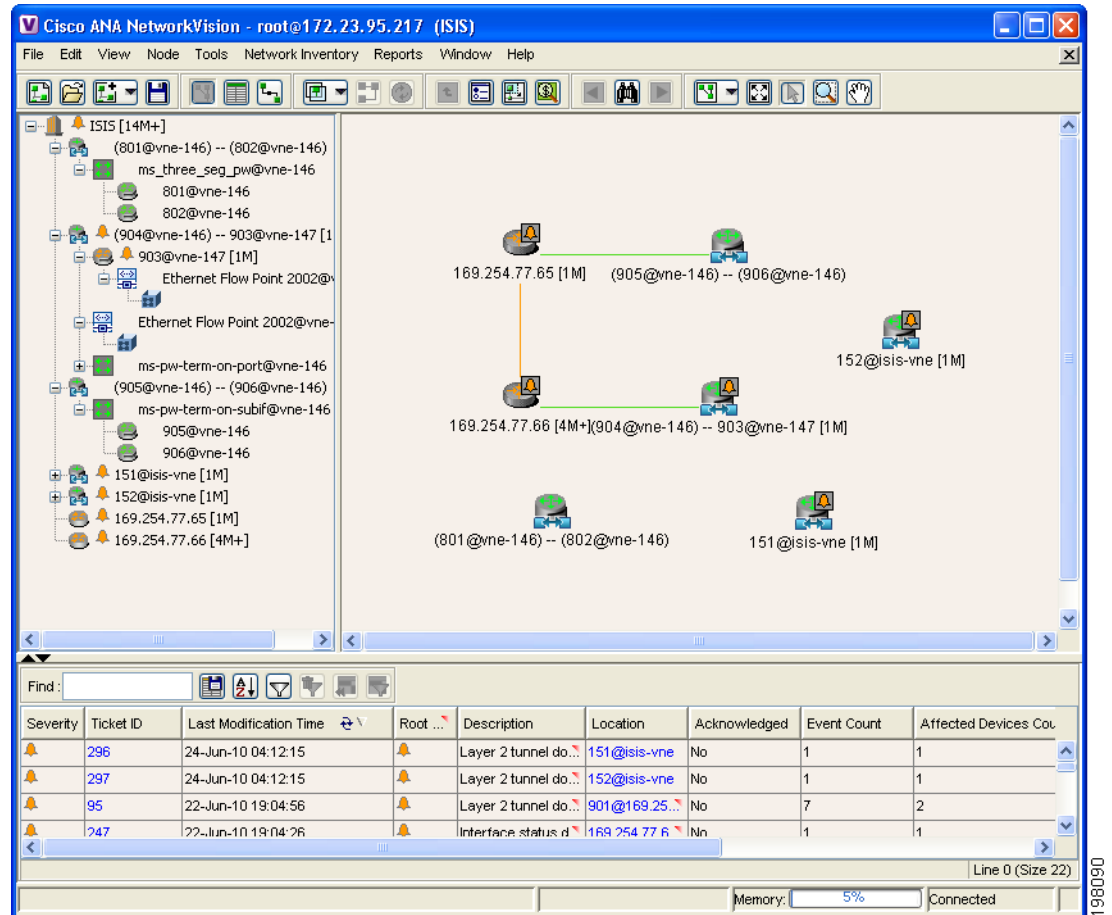
For information about sorting and filtering the table contents, see [Working with Cisco ANA Tables, page 2-40](#).

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**.

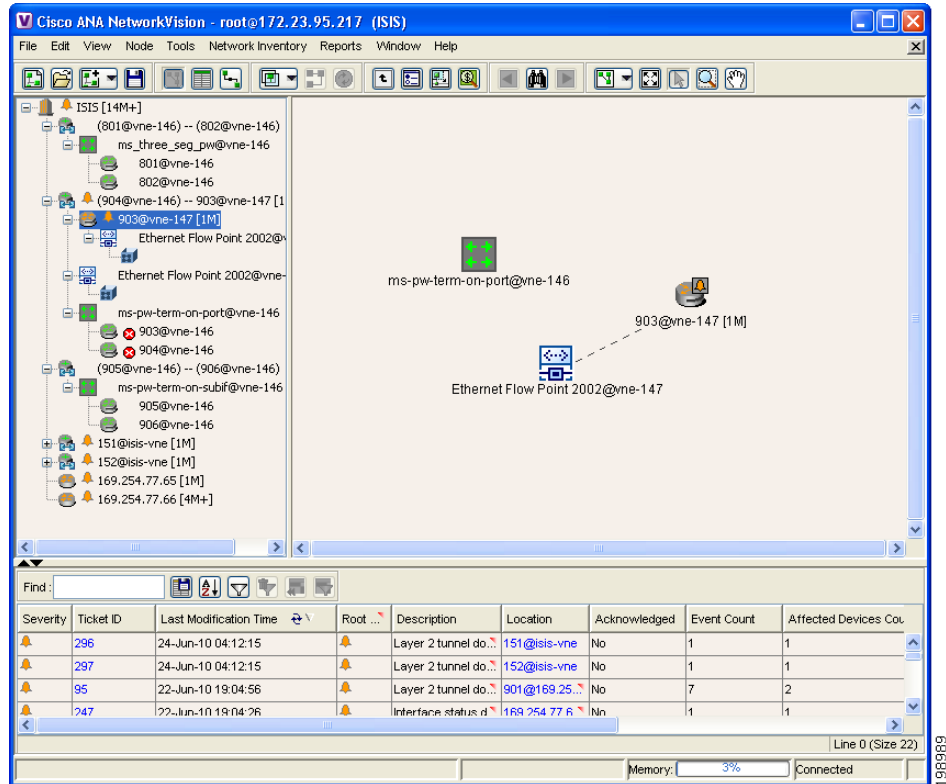
The pseudowire is displayed in the navigation pane and in the content area. In addition, any associated tickets are displayed in the ticket pane. See [Figure 12-54](#).

Figure 12-54 Pseudowire in Cisco ANA NetworkVision Map



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

[Figure 12-55](#) shows an example of an expanded pseudowire in Cisco ANA NetworkVision.

Figure 12-55 Pseudowire Components in Cisco ANA NetworkVision Maps

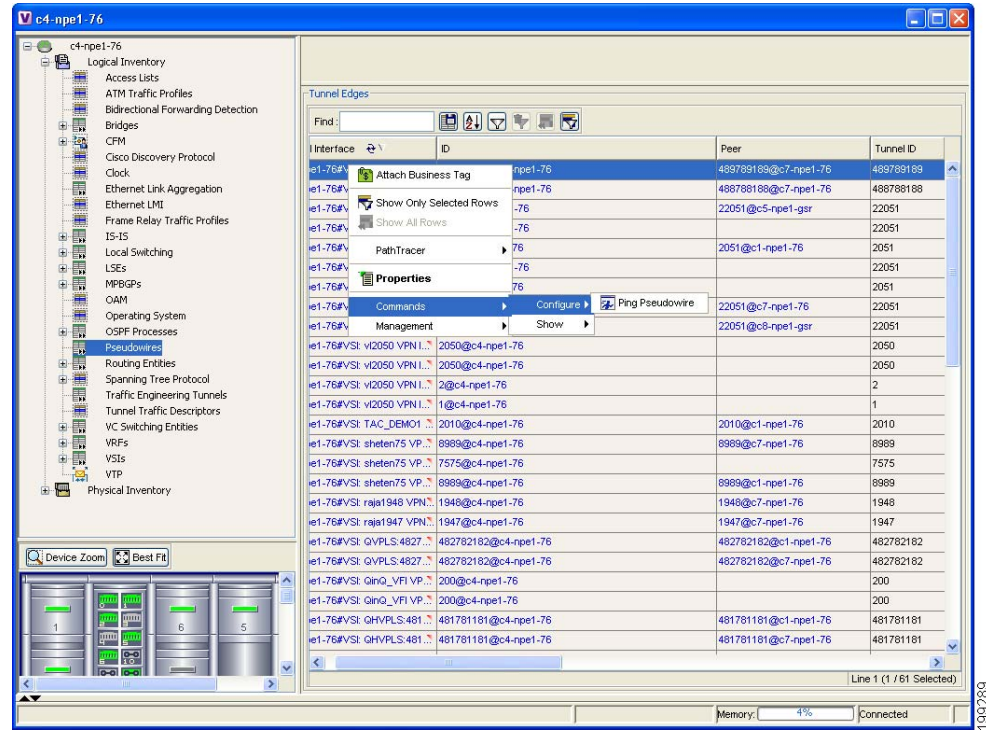
The pseudowire information is saved with the map in the Cisco ANA database.

Pinging a Pseudowire

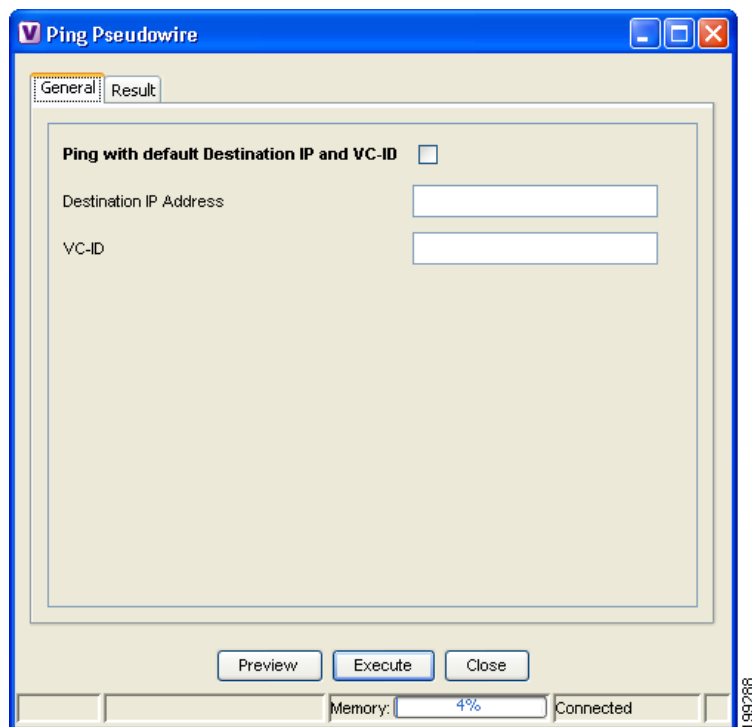
Cisco ANA enables you to ping a peer router to ensure that the pseudowire tunnel is available.

To ping a pseudowire peer router:

- Step 1** In the require map, double-click the required device configured for pseudowire.
- Step 2** In the inventory window, choose **Logical Inventory > Pseudowire**.
- Step 3** In the Tunnel Edges table, select the interface with the peer edge that you want to ping, and make sure that the tunnel status is up.
- Step 4** Right-click the interface and choose **Commands > Configure > Ping Pseudowire** as shown in [Figure 12-56](#).

Figure 12-56 Ping Pseudowire Command

The Ping Pseudowire dialog box is displayed with the General tab as shown in [Figure 12-57](#).

Figure 12-57 Ping Pseudowire Dialog Box - General Tab

Step 5 In the General tab, specify the destination as follows:

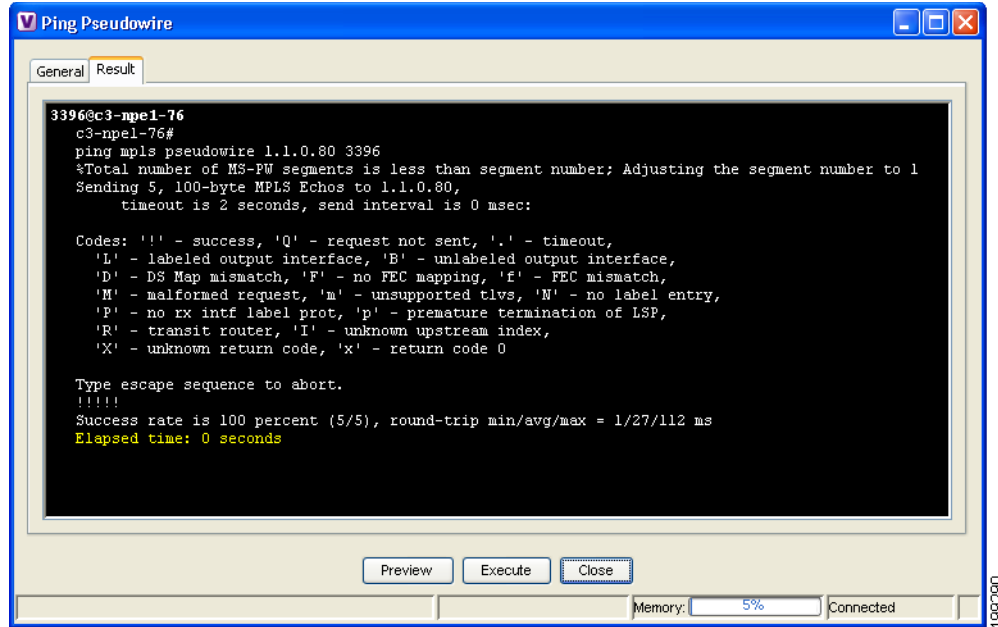
- **Ping with default Destination IP and VC-ID**—Check this check box to ping the selected peer pseudowire endpoint using the default destination IP address and VC identifier. You do not need to enter a destination IP address or tunnel identifier if you choose this option.
- **Destination IP Address**—Enter the required destination IP address if you do not want to use the default destination IP address. If you enter a destination IP address, you must enter the tunnel identifier in the VC-ID field.
- **VC-ID**—Enter the required tunnel identifier if you do not want to use the default VC identifier. If you enter a tunnel identifier, you must enter the destination IP address in the Destination IP Address field.

Step 6 To preview the command to ensure it is right, click **Preview**.

The command is displayed in the Result tab for your review.

Step 7 To execute the command, click **Execute**.

The result of the command is displayed in the Result tab, as shown in [Figure 12-58](#).

Figure 12-58 Ping Pseudowire Dialog Box - Result Tab

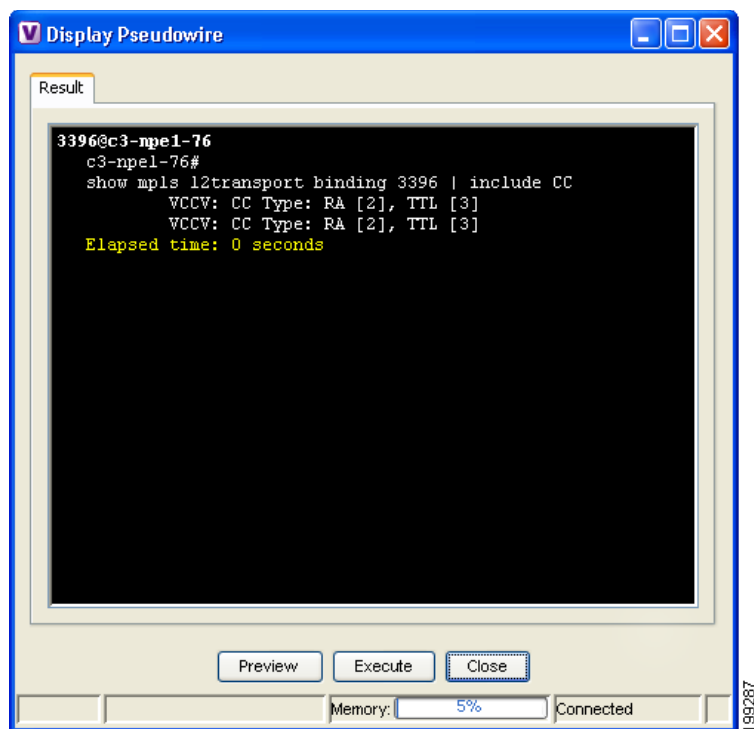
Step 8 Click **Close** to close the Ping Pseudowire dialog box.

Displaying Pseudowire Information

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

- Step 1** In the require map, double-click the required device configured for pseudowire.
- Step 2** In the inventory window, choose **Logical Inventory > Pseudowire**.
- Step 3** In the Tunnel Edges table, right-click the required interface and choose **Commands > Show > Display Pseudowire**.
- Step 4** In the Display Pseudowire dialog box, do either of the following:
 - To view the command before running it, click **Preview**.
 - To run the command, click **Execute**.

When you click **Execute**, the results are displayed in the dialog box as shown in [Figure 12-59](#).

Figure 12-59 Display Pseudowire Dialog Box

Step 5 The following information is displayed:

- The element name.
- The command issued.
- The results, including:
 - VCCV: CC Type—The types of CC processing that are supported. The number indicates the position of the bit that was set in the received octet. The available values are:
 - CW [1]—Control Word
 - RA [2]—Router Alert
 - TTL [3]—Time to Live
 - Unkn [x]—Unknown
 - Elapsed time—The elapsed time, in seconds.

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

Applying Pseudowire Overlays

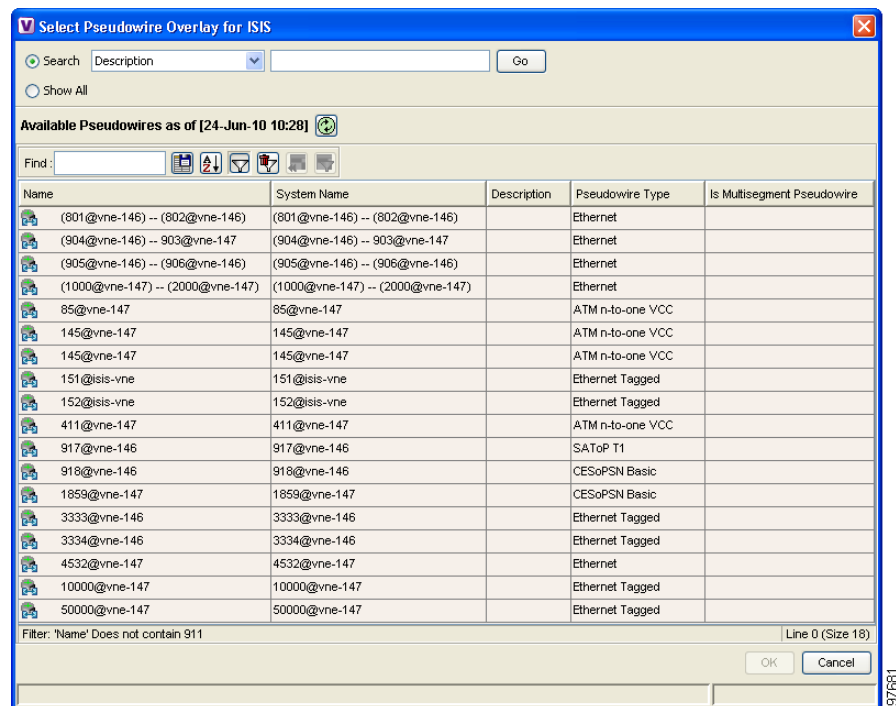
A pseudowire overlay allows you to isolate the parts of a network that are being used by a specific pseudowire.

To apply a pseudowire overlay:

- Step 1** In Cisco ANA NetworkVision, choose the map in which you want to apply an overlay.
- Step 2** From the toolbar, choose **Choose Overlay Type > Pseudowire**.

Figure 12-60 shows an example of the Select Pseudowire Overlay for *map* dialog box.

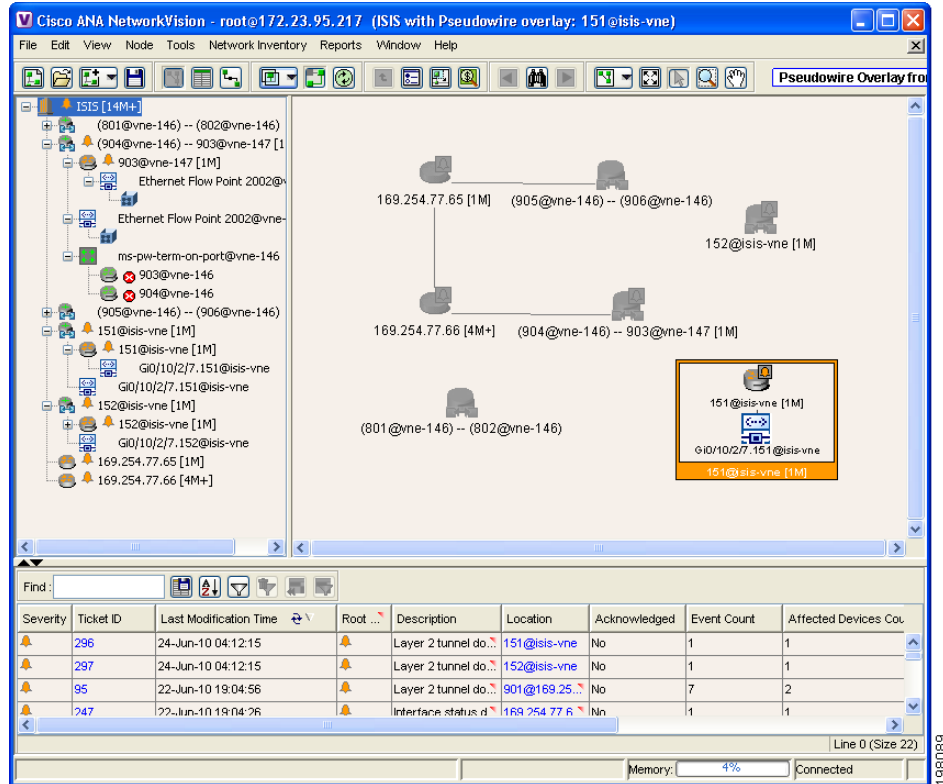
Figure 12-60 Select Pseudowire Overlay Dialog Box



- Step 3** Select the required pseudowire for the overlay.
- Step 4** Click **OK**.

The elements being used by the selected pseudowire are highlighted in the map while the other elements are dimmed, as shown in Figure 12-61.

Figure 12-61 Pseudowire Overlay in Cisco ANA NetworkVision



- 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 Properties

To view pseudowire properties:

- Step 1** In Cisco ANA NetworkVision, select the required map or domain.
- Step 2** To view pseudowire endpoint properties configured on an element:
- In the navigation or map pane, right-click the required element and then choose **Inventory**.
 - 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 Tunnel Edges table, see [Table 17-15 on page 17-36](#).
- Step 3** To view the properties of a pseudowire that you added to a map, right-click the element, and then choose **Properties**.
- The Pseudowire Properties window is displayed as shown in [Figure 12-62](#).

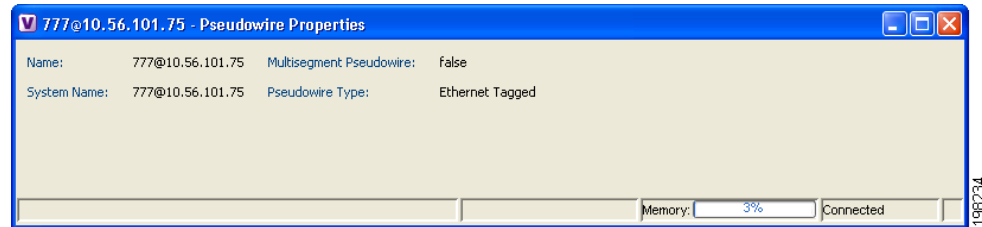
Figure 12-62 Pseudowire Properties Window

Table 12-33 describes the information presented in the Pseudowire Properties window.

Table 12-33 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. For a complete list of pseudowire types, see the Cisco Active Network Abstraction 3.7.1 Theory of Operations Guide .

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

The Tunnel Properties window containing the pseudowire endpoint properties is displayed as shown in Figure 12-15 and described in Table 12-16.

- 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 PW Switching table is displayed as shown in Figure 12-63.

Figure 12-63 PW Switching Table in Logical Inventory

Key	Entry Status	Segment 1	Segment 1 Port Name	Segment 1 Status	Segment 2	Segment 2 Port Name	Segment 2 Status
ms-pw-term-on-port	Up	904@ana-dev-7609-1	10.10.20.4.904	Up	903@ana-dev-7609-1	10.10.20.1.903	Up
ms-pw-term-on-subif	Up	905@ana-dev-7609-1	10.10.20.1.905	Down	906@ana-dev-7609-1	10.10.20.4.906	Down
ms_pw_on_eip	Up	912@ana-dev-7609-1	10.10.20.4.912	Down	911@ana-dev-7609-1	10.10.20.1.911	Down
ms_three_seg_pw	Up	802@ana-dev-7609-1	10.10.20.1.802	Down	801@ana-dev-7609-1	10.10.20.2.801	Down

Table 12-34 describes the information displayed in the PW Switching table.

Table 12-34 PW Switching Table in Logical Inventory

Field	Description
Key	Entry key for the pseudowire.
Entry Status	Status of the pseudowire: Down, Unresolved, or Up.
Segment 1	Identifier of the first segment, hyperlinked to the relevant entry in the Pseudowires Tunnel Edges table in logical inventory.
Segment 1 Port Name	Identifier of the first segment port.
Segment 1 Status	Status of the first segment, such as Admin Up, Admin Down, Oper Down, or Up.
Segment 2	Identifier of the second segment, hyperlinked to the relevant entry in the Pseudowires Tunnel Edges table in logical inventory.
Segment 2 Port Name	Identifier of the second segment port.
Segment 2 Status	Status of the second segment, such as Admin Up, Admin Down, Oper Down, or Up.

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

The Contained Current CTPs table is displayed as shown in Figure 12-64.



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

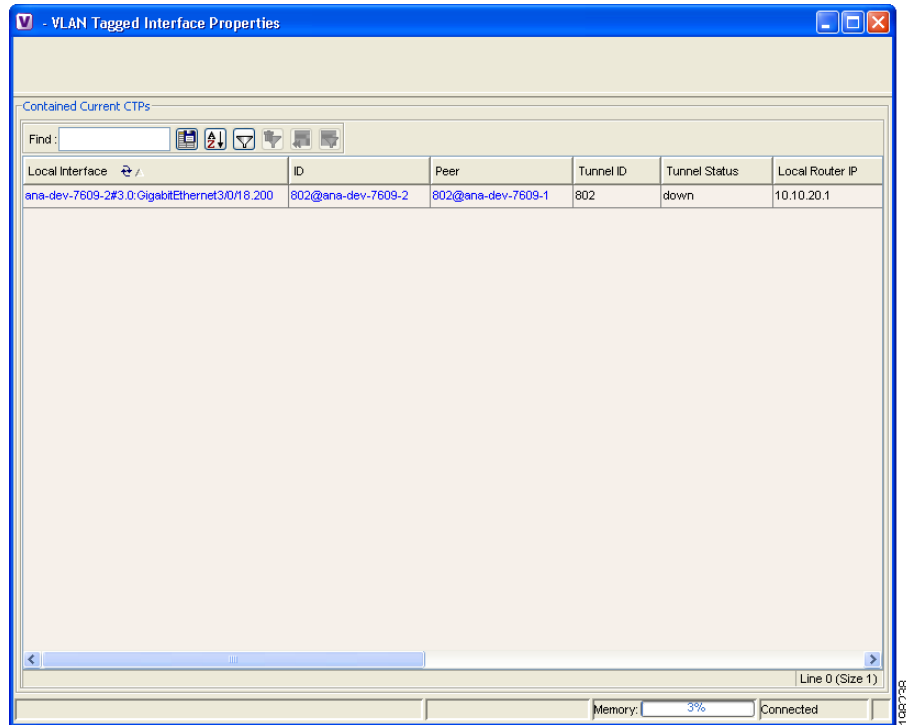
Figure 12-64 Contained Current CTPs Table

Table 12-35 describes the information displayed in the Contained Current CTPs table.

Table 12-35 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. For a complete list of pseudowire types, see the Cisco Active Network Abstraction 3.7.1 Theory of Operations Guide .
Local MTU	The size, in bytes, of the MTU on the local interface.

Table 12-35 Contained Current CTPs Table (continued)

Field	Description
Remote MTU	The size, in bytes, of the MTU on the remote interface.
Local VC Label	The MPLS label that is used by this router to identify or access the tunnel. It is inserted in the MPLS label stack by the local router.
Peer VC Label	The MPLS label that is used by this router to identify or access the tunnel. It is inserted in the MPLS label stack by the peer router.
Signaling Protocol	The protocol used to build the tunnel, such as LDP or TDP.
Preferred Path Tunnel	The path to be used for pseudowire traffic.

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

See [Viewing EFP Properties, page 12-20](#) for the information that is displayed for EFPs.

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 (either 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 connected by a shared EFP.
- Network VLAN and service link 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.

For more information about Cisco ANA and Ethernet services, see the [Cisco Active Network Abstraction 3.7.1 Theory of Operations Guide](#).

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

- [Adding Ethernet Services to a Map, page 12-91](#)
- [Using Ethernet Service Overlays, page 12-92](#)
- [Viewing Ethernet Service Properties, page 12-94](#)

Adding Ethernet Services to a Map

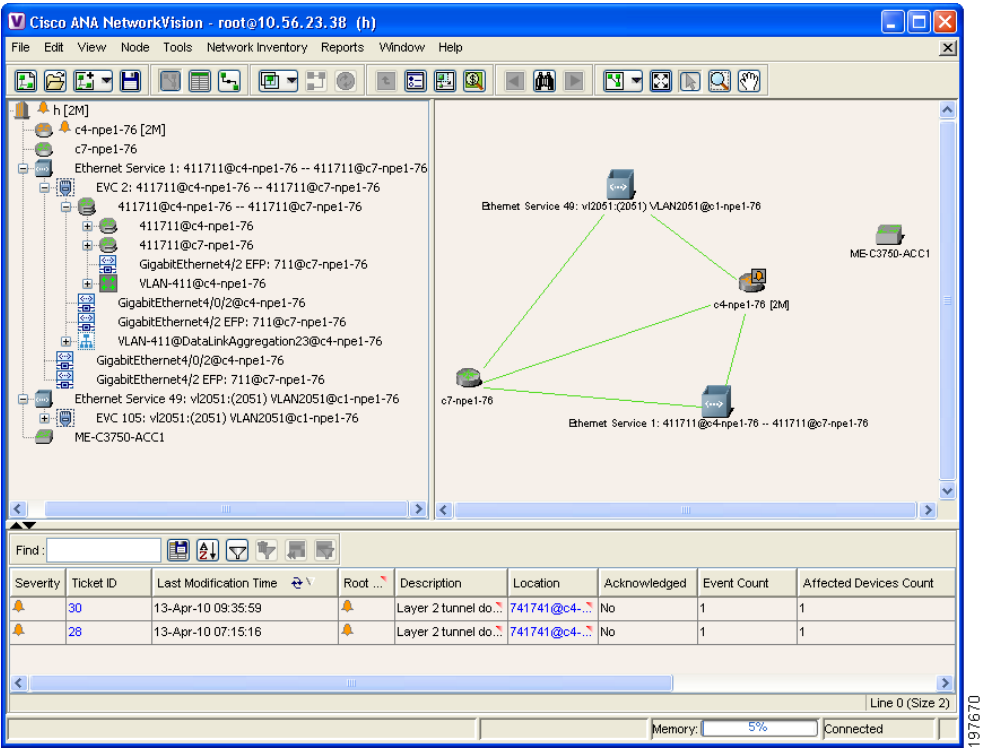
You can add the Ethernet services that Cisco ANA discovers to maps as required.

To add an Ethernet service to a map:

-
- Step 1** In Cisco ANA NetworkVision, select the required map or domain.
- Step 2** Open the Add Ethernet Service to *map* dialog box in either of the following ways:
- In the toolbar, choose **Add to Map > Ethernet Service**.
 - In the menu bar, choose **File > Add to Map > Ethernet Service**.
- Step 3** In the Add Ethernet Service dialog box, do either of the following:
- To search for specific elements:
 - a. Choose **Search**, and then choose a search category: EVC Terminating EFPs, Name, or System Name.
 - b. To narrow the display to a range of Ethernet services or a group of Ethernet services, enter a search string in the search field.
 - c. Click **Go**.

For example, if you choose Name and enter **EFP1**, the network elements that have names beginning with EFP1 are displayed.
 - To view all available Ethernet services, choose **Show All** and click **Go**.
- The available elements that meet the specified search criteria are displayed in the Add Ethernet Service dialog box in table format. The dialog box also displays the date and time at which the list was generated. To update the list, click **Refresh**.
-  **Note** If an element is not included in your scope, it is displayed with the locked device icon.
-
- For information about sorting and filtering the table contents, see [Working with Cisco ANA Tables, 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 12-65](#).

Figure 12-65 Ethernet Service in Cisco ANA NetworkVision Map



The Ethernet service information is saved with the map in the Cisco ANA database.

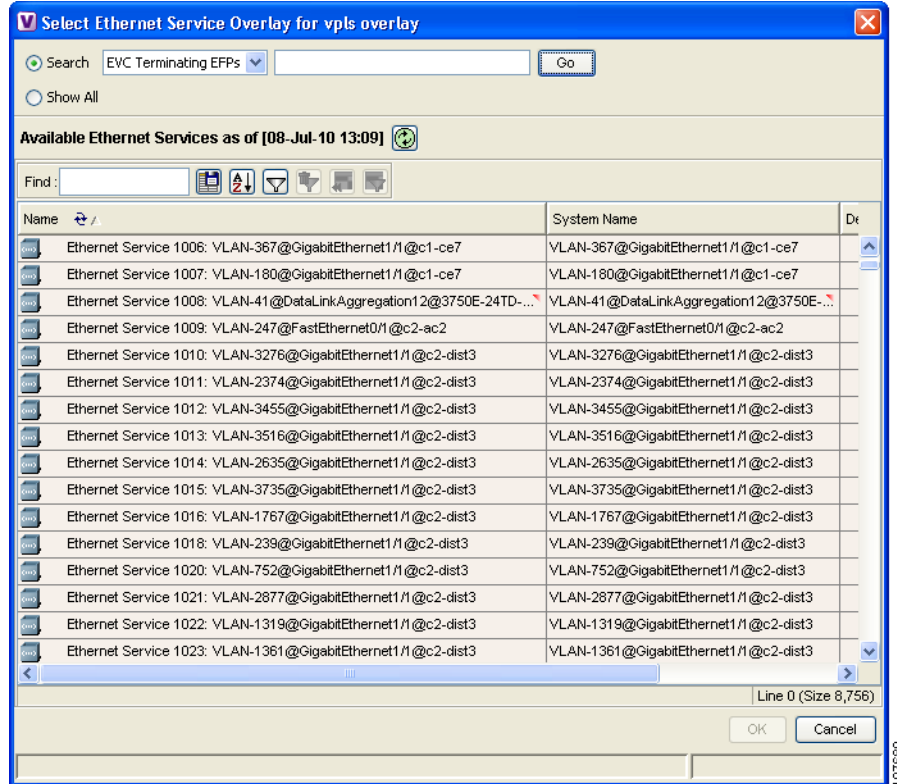
Using Ethernet Service Overlays

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 Cisco ANA NetworkVision, choose the map in which you want to apply an overlay.
- Step 2** From the toolbar, choose **Choose Overlay Type > Ethernet Service**.

Figure 12-66 shows an example of the Select Ethernet Service Overlay for *map* dialog box.

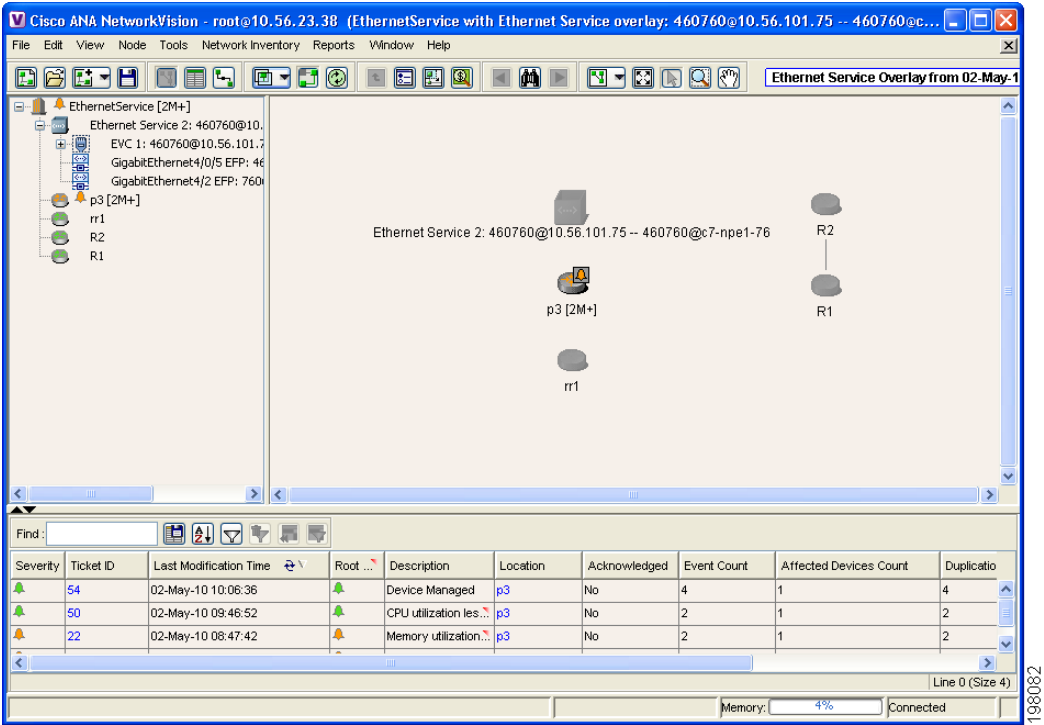
Figure 12-66 Select Ethernet Service Overlay Dialog Box

Step 3 Select the required Ethernet Service for the overlay.

Step 4 Click **OK**.

The elements being used by the selected Ethernet service are highlighted in the map while the other elements are dimmed, as shown in [Figure 12-67](#).

Figure 12-67 Ethernet Service Overlay in Cisco ANA NetworkVision



- 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 Cisco ANA NetworkVision, select the map containing the required Ethernet service.
- Step 2

In the navigation or map pane, right-click the Ethernet service and choose **Properties**.
- Figure 12-68 shows an example of an Ethernet Service Properties window.

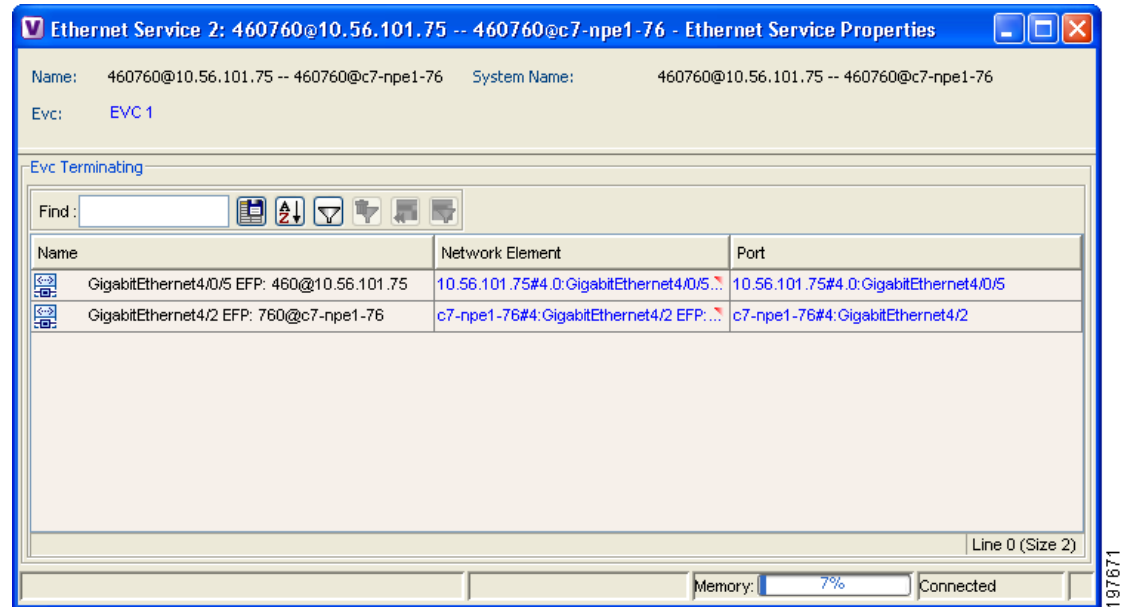
Figure 12-68 Ethernet Service Properties Window

Table 12-36 describes the information that is displayed for an Ethernet service.

Table 12-36 Ethernet Service Properties Window

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

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

Figure 12-69 shows an example of the EVC Properties window.

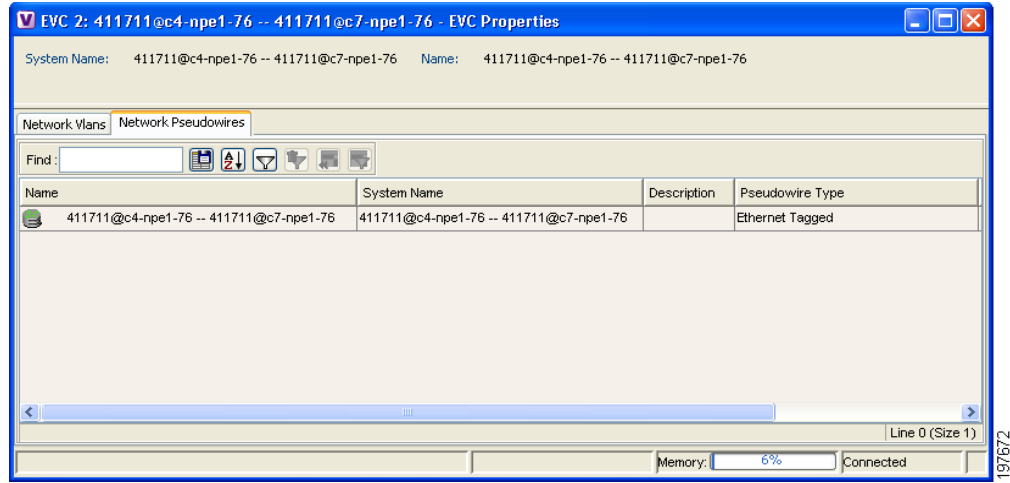
Figure 12-69 EVC Properties Window

Table 12-37 describes the information that is displayed in the EVC Properties window. The tabs that are displayed in the window depend on the EVC links.

Table 12-37 EVC Properties Window

Field	Description
System Name	Name of the system on which the EVC is configured.
Name	EVC name.
Network VLANs Tab	
Name	VLAN name.
ID	VLAN identifier.
Ethernet Flow Domain	Name of the Ethernet flow domain.
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. For a complete list of pseudowire types, see the Cisco Active Network Abstraction 3.7.1 Theory of Operations Guide .
Is Multisegment Pseudowire	Whether or not the pseudowire is multisegment: True or False.
VPLS Instances Tab	
Name	VPLS name.
System Defined Name	VPLS system name.
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.

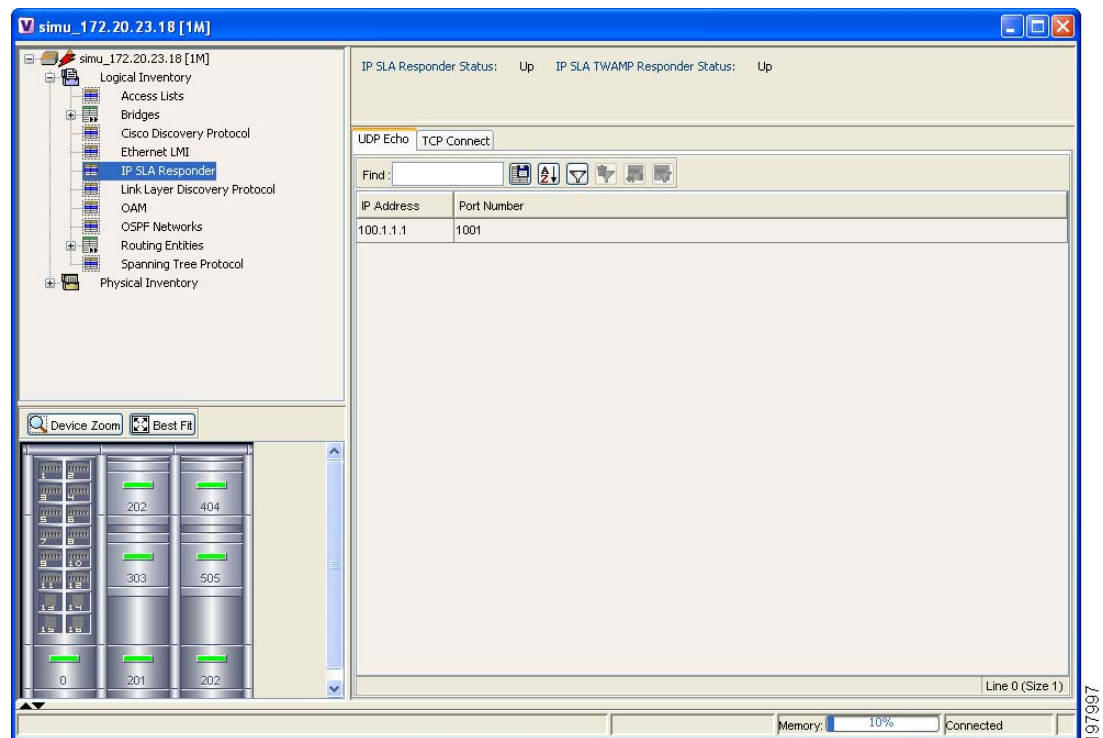
In Cisco ANA 3.7.1, IP SLA Responder service is supported on the following devices:

- 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 Cisco ANA NetworkVision, double-click the device configured for IP SLA Responder service.
- Step 2** In the inventory window, choose **Logical Inventory > IP SLA Responder**.
- IP SLA Responder properties are displayed as shown in [Figure 12-70](#).

Figure 12-70 IP SLA Responder in Logical Inventory



[Table 12-38](#) describes the properties displayed for IP SLA Responder service.

Table 12-38 *IP SLA Responder Properties in Logical Inventory*

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

Viewing IS-IS Properties

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

IS-IS networks contain end systems, intermediate systems, areas, and domains. End systems are user devices. Intermediate systems are routers. Routers are organized into local groups called areas, and areas are grouped into a domain.

To view IS-IS properties:

-
- Step 1** In Cisco ANA NetworkVision, double-click the device configured for IS-IS.
- Step 2** In the inventory window, choose **Logical Inventory > IS-IS > System**.

[Figure 12-71](#) shows an example of the ISIS window with the Process table in logical inventory.

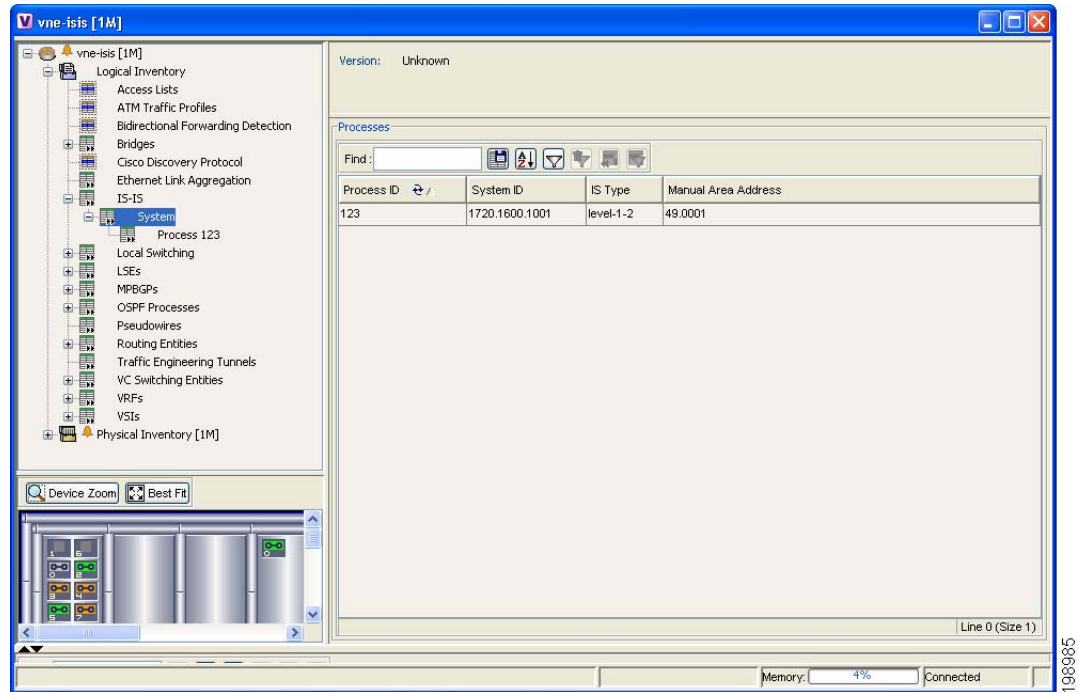
Figure 12-71 *ISIS Window in Logical Inventory*

Table 12-39 describes the information that is displayed in this window and the Processes table.

Table 12-39 *IS-IS Properties in Logical Inventory - Processes Table*

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

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

Figure 12-72 shows an example of the information that is displayed for the IS-IS process.

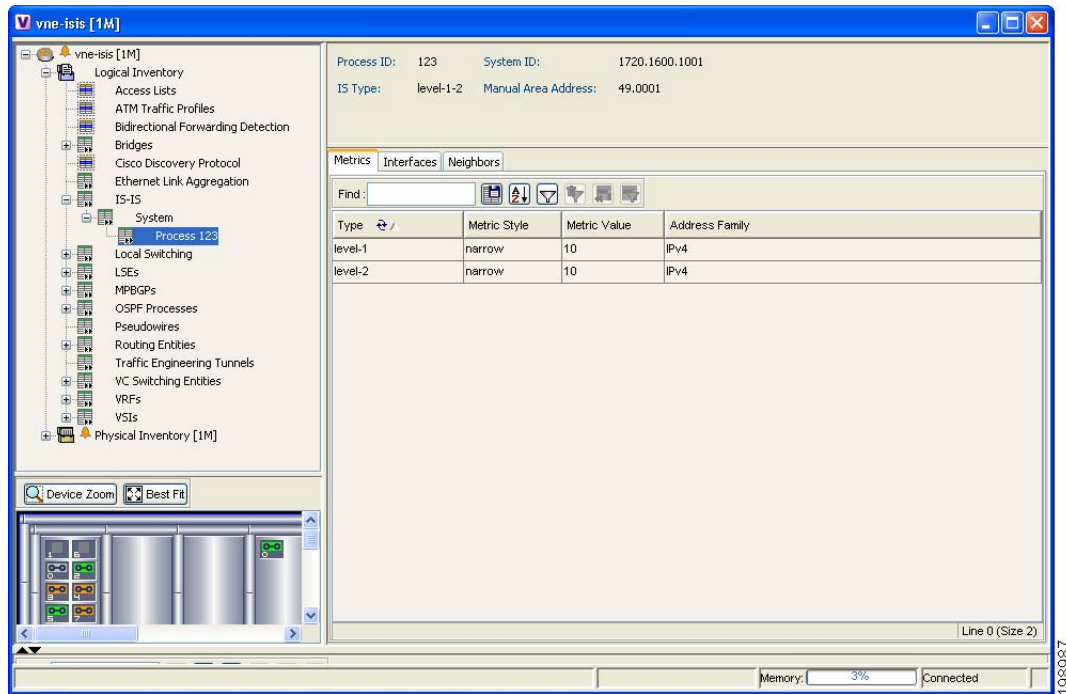
Figure 12-72 IS-IS Process Properties in Logical Inventory

Table 12-40 describes the information that is displayed for the selected IS-IS process.

Table 12-40 IS-IS Process Properties in Logical Inventory

Field	Description
Process	Unique identifier for the IS-IS process.
System ID	Identifier for this Intermediate System.
IS Type	Level at which the Intermediate System process is running: Level 1, Level 2, or Level 1-2.
Manual Area Address	Address assigned to the area.
Metrics Tab	
IS Type	Level at which the Intermediate System is running: Level 1, Level 2, or Level 1-2.
Metric Style	Metric style used: Narrow, Transient, or Wide.
Metric Value	Metric value assigned to the link. This value is used to calculate the path cost via the links to destinations. This value is available for Level 1 or Level 2 routing only. If the metric style is Wide, the value can range from 1 to 16777214. If the metric style is Narrow, the value can range from 1 to 63. The default value for active IS-IS interfaces is 10, and the default value for inactive IS-IS interfaces is 0.
Address Family	IP address type used: IPv4 or IPv6.

Table 12-40 IS-IS Process Properties in Logical Inventory (continued)

Field	Description
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

Cisco ANA supports the following versions of OSPF:

- OSPFv1
- OSPFv2
- OSPFv3

Using Cisco ANA NetworkVision you can view OSPF properties for:

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

To view OSPF properties:

- Step 1** In Cisco ANA NetworkVision, double-click the device configured for OSPF.
- Step 2** To view OSPF processes, choose **Logical Inventory > OSPF Processes > OSPF Process (vn) ID** where *vn* represents the OSPF version and *ID* is the OSPF process identifier.
- For example, in [Figure 12-73](#), the entry in the navigation tree is OSPF Process (v2) 1.

Figure 12-73 OSPF Processes in Logical Inventory

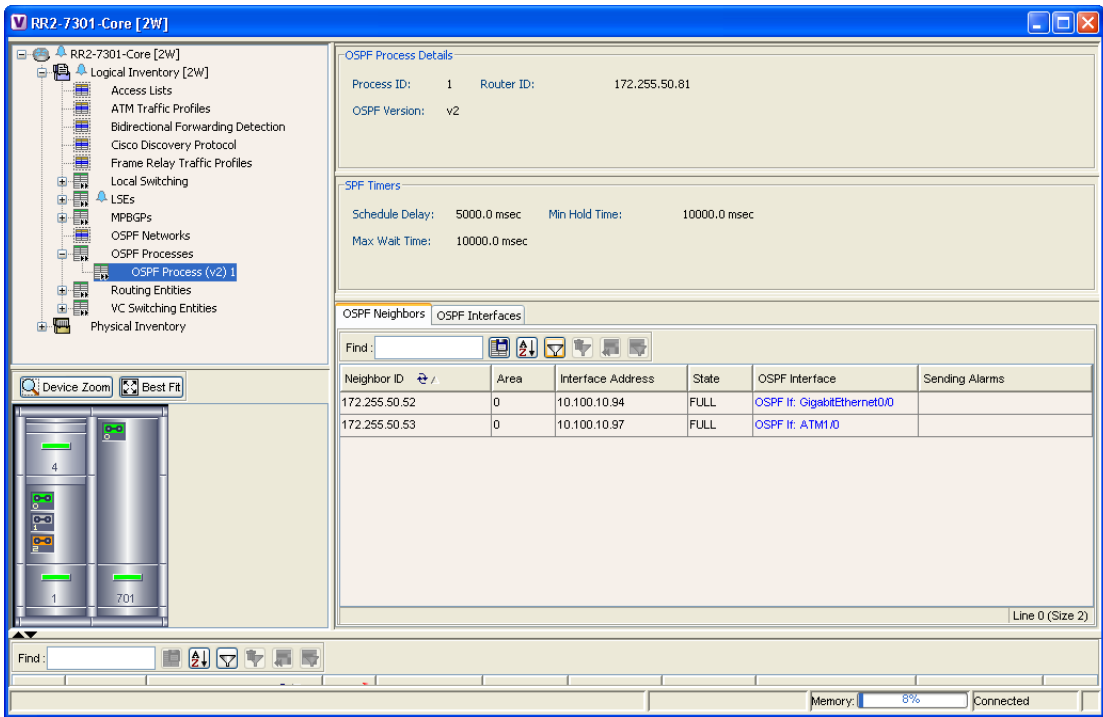


Table 12-41 describes the information that is displayed for OSPF processes.

Table 12-41 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 performing the shortest path first (SPF) calculation.
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.

Table 12-41 OSPF Processes in Logical Inventory (continued)

Field	Description
OSPF Interface	Hyperlinked entry to the OSPF Interface Properties window. The OSPF Interfaces window displays the same information as in the OSPF Interfaces Table below.
Sending Alarms	Status of sending alarms on the interface: True or False.
OSPF Interfaces Table	
IP Interface	OSPF interface, hyperlinked to relevant entry in the routing entity IP Interfaces table in logical inventory. For more information about the IP Interfaces table, see Table 17-6 .
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.
Sending Alarms	Status of sending alarms on the interface: True or False.



CHAPTER 13

Monitoring Carrier Grade NAT Properties

Carrier Grade NAT is a large-scale NAT, capable of providing private-IPv4-to-public-IPv4 translation in the order of millions of translations. Carrier Grade NAT can support several hundred thousand subscribers with the bandwidth throughput of at least 10Gb/s full-duplex. With IPv4 addresses reaching depletion, Carrier Grade NAT is vital in providing private IPv4 connectivity to the public IPv4 internet. In addition, Carrier Grade NAT is not limited to IPv4 NAT; it can also translate between IPv4 and IPv6 addresses.

In Cisco ANA 3.7.1, Carrier Grade NAT is supported on Cisco CRS-1 routers containing a Cisco CRS-ADVSVC-PLIM card.

The following topics describe using Cisco ANA NetworkVision to view Carrier Grade NAT properties:

- [User Roles Required to View Carrier Grade NAT Properties, page 13-1](#)
- [Viewing Carrier Grade NAT Properties in Logical Inventory, page 13-2](#)
- [Viewing Carrier Grade NAT Properties in Physical Inventory, page 13-4](#)

User Roles Required to View Carrier Grade NAT Properties

[Table 13-1](#) identifies the roles that are required to view Carrier Grade NAT properties in Cisco ANA NetworkVision. Cisco ANA 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 device-based tasks (tasks that do affect devices), authorization is based on the default permission that is assigned to your account. That is, whether the device 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 Active Network Abstraction 3.7.1 Administrator Guide](#).

Table 13-1 Default Permission/Security Level Required for Viewing Carrier Grade NAT Properties

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Viewing Carrier Grade NAT properties	X	X	X	X	X

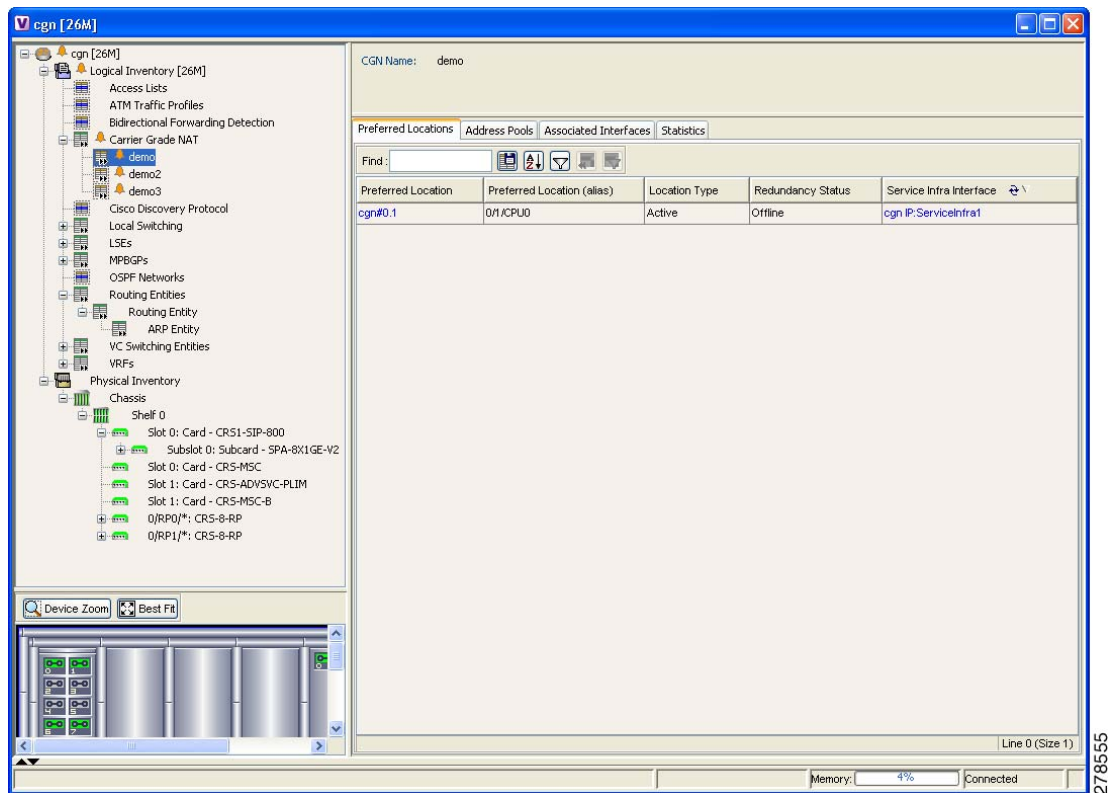
Viewing Carrier Grade NAT Properties in Logical Inventory

To view Carrier Grade NAT properties in logical inventory:

- Step 1** In Cisco ANA NetworkVision, double-click the Cisco CRS-1 device configured for Carrier Grade NAT.
- Step 2** In the inventory window, click **Logical Inventory > Carrier Grade NAT**.

The Carrier Grade NAT properties are displayed in logical inventory as shown in [Figure 13-1](#).

Figure 13-1 Carrier Grade NAT in Logical Inventory



[Table 13-2](#) describes the Carrier Grade NAT properties that are displayed.

Table 13-2 Carrier Grade NAT Properties in Logical Inventory

Field	Description
CGN Name	Name of the Carrier Grade NAT service.
Preferred Location Tab	
Preferred Location	Hyperlinked entry to the card in physical inventory.
Preferred Location (alias)	Location of module in clear text.
Location Type	Configured type of location: Active or Standby
Redundancy Status	Redundancy state: Online or Offline. If the field is empty, it means the data was not collected from the device.
Service Infra Interface	Hyperlinked entry to the routing entity in logical inventory. For more information about routing entities in logical inventory, see Viewing Routing Entities, page 17-22 .
Address Pools Tab	
Inside VRF	Hyperlinked entry to the inside VRF in logical inventory. For more information about VRF properties in logical inventory, see Viewing VRF Properties, page 17-18 .
Address Family	Type of IP address in this pool: IPv4 or IPv6.
Outside VRF	Hyperlinked entry to the outside VRF in logical inventory. For more information about VRF properties in logical inventory, see Viewing VRF Properties, page 17-18 .
Address Pool	Range of IP addresses that can be used for the service instance. If an end address is not specified, the entire range of 255 addresses is used for the address pool.
Associated Interfaces Tab	
Interface	Hyperlinked entry to the associated entry in logical inventory: - For SVI service interfaces, hyperlinked entry to the routing entity in logical inventory. - For SVI service applications, hyperlinked entry to the VRF entity in logical inventory.
Statistics Tab	
Statistics Name	Name of the statistic. For statistic names and descriptions, see Table 13-3 .
Statistics Value	Value of the statistic.

Table 13-3 Carrier Grade NAT Statistics in Logical Inventory

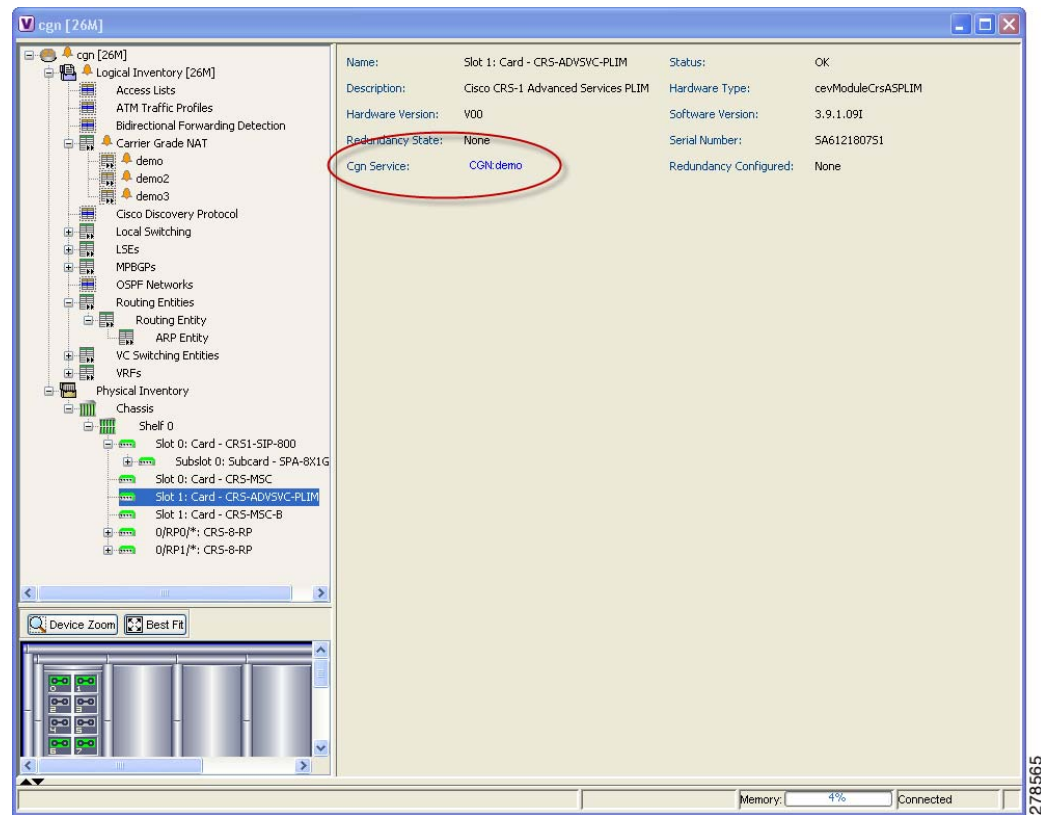
Statistic Name	Description
Inside to outside drops port limit exceeded	Number of packets dropped because the port limit has been exceeded. The value is calculated from the time Carrier Grade NAT was configured and running on the card.
Inside to outside drops resource depletion	Number of packets that 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 Cisco ANA NetworkVision, double-click the Cisco CRS-1 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 17-13](#) for a description of the information displayed in the Subinterfaces table.
- Step 3** To view Carrier Grade NAT properties configured on a Cisco CRS-ADVSVC-PLIM card, click **Physical Inventory > chassis > shelf > slot > PLIM-card**.

[Figure 13-2](#) shows an example of Carrier Grade NAT properties in physical inventory.

Figure 13-2 Carrier Grade NAT Properties in Physical Inventory

The field CGN Service is displayed, and the entry is hyperlinked to the associated Carrier Grade NAT service in logical inventory.



CHAPTER 14

Monitoring DWDM Properties

The following topics describe how you can view and monitor IP over dense wavelength division multiplexing (DWDM) properties configured on network elements by using Cisco ANA:

- [User Roles Required to View DWDM Properties, page 14-1](#)
- [Viewing DWDM in Physical Inventory, page 14-2](#)
- [Viewing G.709 Properties, page 14-4](#)
- [Viewing Performance Monitoring Configuration, page 14-10](#)

User Roles Required to View DWDM Properties

[Table 14-1](#) identifies the roles that are required to view DWDM properties using Cisco ANA. Cisco ANA 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 device-based tasks (tasks that do affect devices), authorization is based on the default permission that is assigned to your account. That is, whether the device 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 Active Network Abstraction 3.7.1 Administrator Guide](#).

Table 14-1 Default Permission/Security Level Required for Viewing DWDM Properties

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View DWDM properties	X	X	X	X	X
View G.709 properties	X	X	X	X	X
View performance monitoring configuration information	X	X	X	X	X

Viewing DWDM in Physical Inventory

Cisco ANA NetworkVision 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 the Cisco ANA NetworkVision right-click the device on which DWDM is configured, then choose **Inventory**.
- Step 2** In the inventory window, choose **Physical Inventory > Chassis** and navigate to the interface configured for DWDM. DWDM details are displayed in the DWDM area in the content pane as shown in [Figure 14-1](#).

Figure 14-1 DWDM Properties in Physical Inventory

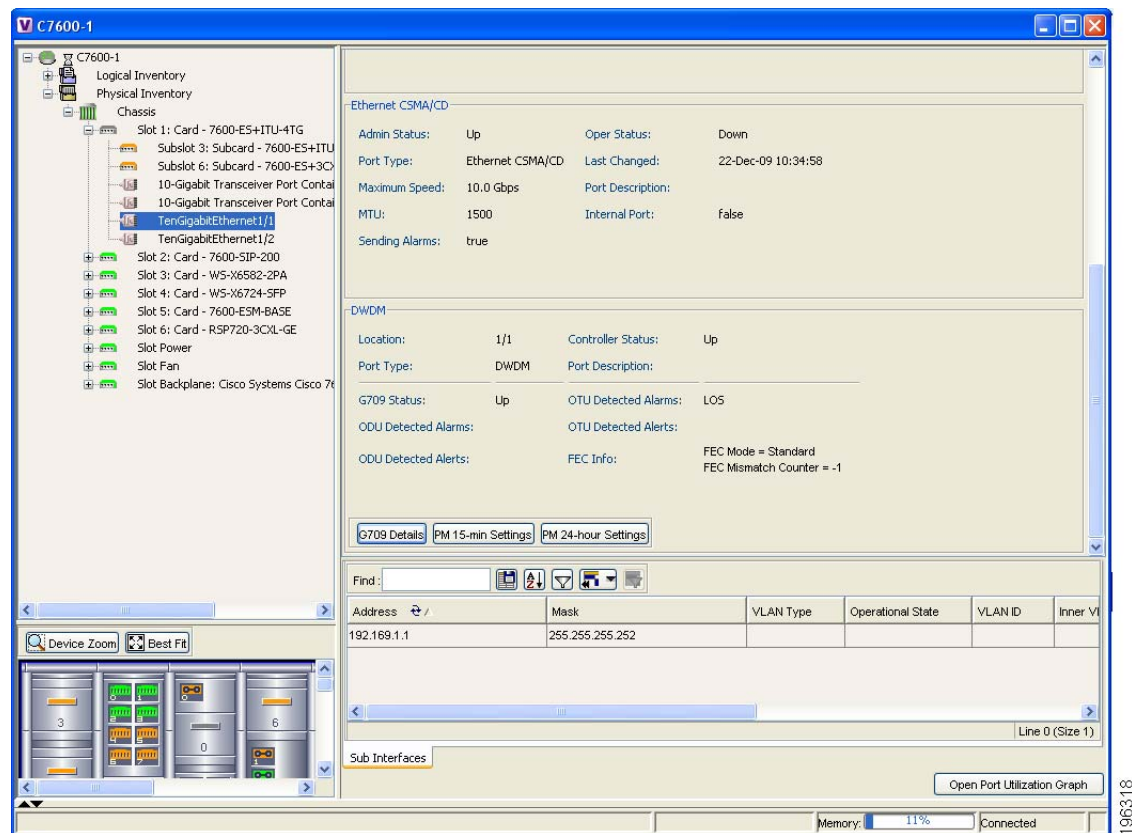


Table 14-2 describes the information displayed for DWDM.

Table 14-2 DWDM Properties in Physical Inventory

Field	Description
Location	Physical interface using the format <i>rack/slot/module/port</i> where: <i>rack</i> is the chassis number of the rack. <i>slot</i> is the physical slot number of the line card. <i>module</i> is the module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number. <i>port</i> is the physical port number of the interface.
Controller Status	Status of the controller: Up or Down.
Loopback	Indicates 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	Indicates whether the G.709 wrapper is enabled or disabled: Up or Down.
OTU Detected Alarms	OTU overhead alarms.
ODU Detected Alarms	Optical channel data unit (ODU) alarms.
OTU Detected Alerts	OTU alerts.
ODU Detected Alerts	ODU alerts.
FEC Info	Indicates the: - FEC mode of the controller: Disabled, Enhanced, Standard, or Unknown. - FEC mode on the remote device: Disabled, Enhanced, Standard, or Unknown. - Number of sync word mismatches found during the tracking phase.
G709 Details	Click to view G709 properties. For more information, see Viewing G.709 Properties, page 14-4 .

Table 14-2 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 14-10 .
PM 24-hour Settings	Click to view 24-hour performance monitoring properties. For more information, see Viewing Performance Monitoring Configuration, page 14-10 .

Viewing G.709 Properties

The Telecommunication Standardization Sector (ITU-T) Recommendation G.709 provides a standardized method for transparently transporting services over optical wavelengths end to end. A significant component of G.709 is the FEC code that improves performance and extends the distance that optical signals can span.

To view G.709 properties:

-
- Step 1** In the Cisco ANA NetworkVision right-click the device on which DWDM is configured, then choose **Inventory**.
 - Step 2** In the inventory window, choose **Physical Inventory > Chassis** and navigate to the interface configured for DWDM.
 - Step 3** In the content pane, click **G709 Details**.

The G709 Info Properties window is displayed as shown in [Figure 14-2](#) for all Cisco devices except the Cisco 7600 series devices.

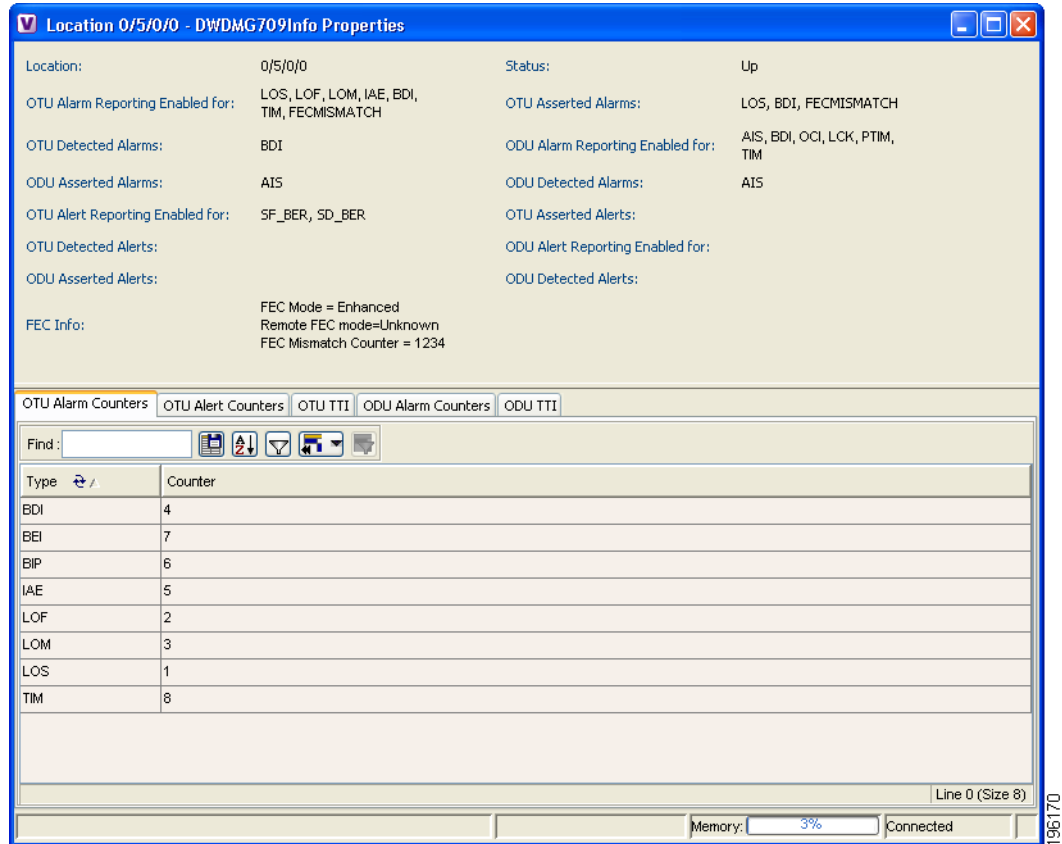
Figure 14-2 DWDM G709 Properties Window

Figure 14-3 shows the tabs that are displayed in the G709 Info Properties window for Cisco 7600 series devices. For Cisco 7600 series devices:

- The ODU Alert Counters tab is displayed.
- The ODU TTI and OTU TTI tabs are not displayed.

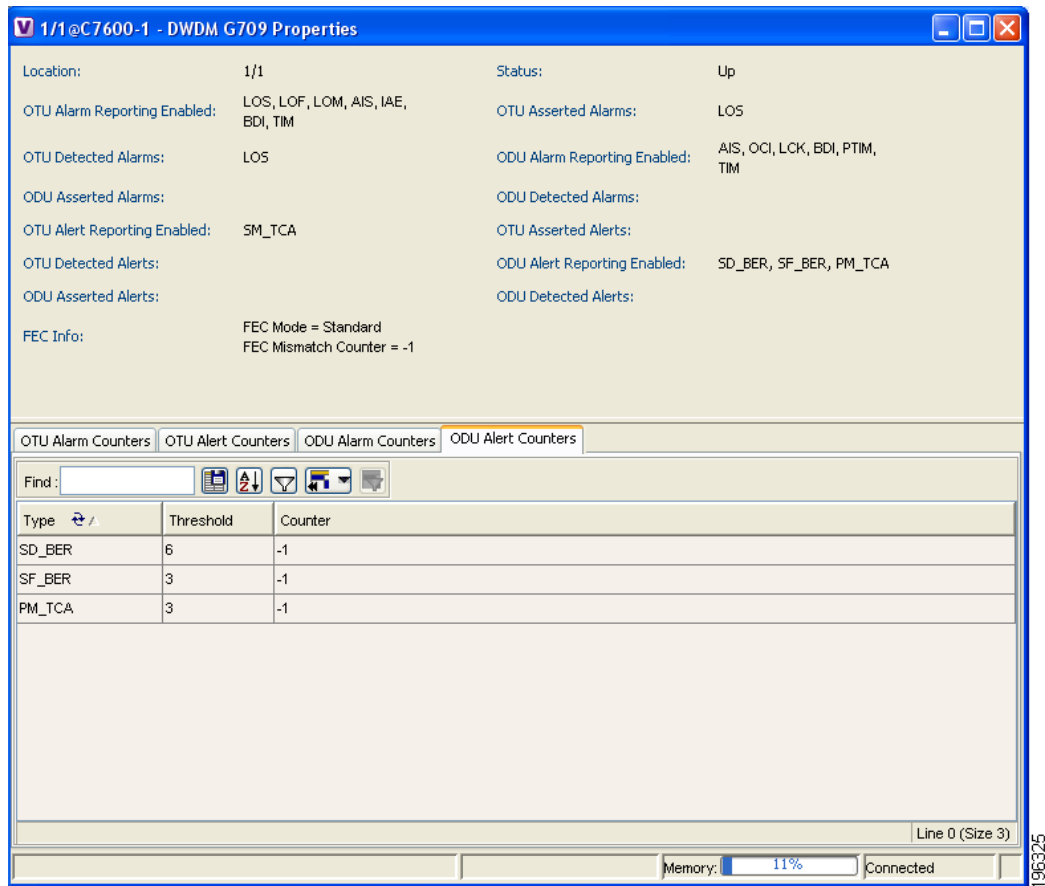
Figure 14-3 DWDM G709 Properties Window for Cisco 7600 Series Devices

Table 14-3 describes the fields that are displayed above the tabs in the G709 Info Properties window.

Table 14-3 DWDM G709 Properties Window

Field	Description
Location	Physical interface using the format <i>rack/slot/module/port</i> where: <i>rack</i> is the chassis number of the rack. <i>slot</i> is the physical slot number of the line card. <i>module</i> is the module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number. <i>port</i> is the physical port number of the interface.

Table 14-3 DWDM G709 Properties Window (continued)

Field	Description
OTU Alarms	
OTU Alarm Reporting Enabled for	The types of alarms enabled for reporting: • AIS—Alarm indication signal (AIS) alarms. • BDI—Backward defect indication (BDI) alarms. • BEI—Backward error indication (BEI) alarms. • BIP—Bit interleaved parity (BIP) alarms. • FECMISMATCH—FEC mismatch alarms. • IAE—Incoming alignment error (IAE) alarms. • LOF—Loss of frame (LOF) alarms. • LOM—Loss of multiple frames (LOM) alarms. • LOS—Loss of signal (LOS) alarms. • TIM—Type identifier mismatch (TIM) alarms.
OTU Asserted Alarms	OTU alarms indicated to be reported by the user.
OTU Detected Alarms	OTU alarms detected by the hardware.
ODU Alarms	
ODU Alarm Reporting Enabled for	The types of ODU alarms enabled for reporting: • AIS—Incoming SONET AIS error status. • BDI—Path termination BDI error status. • BEI—Backward error indication (BEI) error status. • BIP—Bit interleaved parity (BIP) error status. • LCK—Upstream connection locked (LCK) error status. • OCI—Open connection indication (OCI) error status. • PTIM—Payload TIM error status. • TIM—Data stream TIM error status.
ODU Asserted Alarms	ODU alarms indicated to be reported by the user.
ODU Detected Alarms	ODU alarms detected by the hardware.
OTU Alerts	
OTU Alert Reporting Enabled for	The types of alerts enabled for reporting: • SD-BER—Section Monitoring (SM) bit error rate (BER) is in excess of the signal degradation (SD) BER threshold. • SF-BER—SM BER is in excess of the signal failure (SF) BER threshold. • PM-TCA—Performance monitoring (PM) threshold crossing alert (TCA). • SM-TCA—SM threshold crossing alert.
OTU Asserted Alerts	OTU alerts indicated to be reported by the user.

Table 14-3 DWDM G709 Properties Window (continued)

Field	Description
OTU Detected Alerts	OTU alerts detected by the hardware.
ODU Alerts	
ODU Alert Reporting Enabled for	The types of ODU alerts enabled for reporting: - SD-BER—SM BER is in excess of the SD BER threshold. - SF-BER—SM BER is in excess of the SF BER threshold. - PM-TCA—PM threshold crossing alert. - SM-TCA—SM threshold crossing alert.
ODU Asserted Alerts	ODU alerts indicated to be reported by the user.
ODU Detected Alerts	ODU alerts detected by the hardware.
Other	
FEC Info	FEC properties: - FEC mode for the controller—Disable, Enhanced, Standard, or Unknown. - Remote FEC mode—FEC mode on the remote device: Disabled, Enhanced, Standard, or Unknown. - FEC mismatch counter—Number of sync word mismatches found during the tracking phase.
Status	G.709 wrapper administrative status: Up or Down.

The G709 Info Properties window contains the following tabs, depending on the selected network element:

- [OTU Alarm Counters Tab, page 14-8](#)
- [OTU Alert Counters Tab, page 14-9](#)
- [ODU Alarm Counters Tab, page 14-9](#)
- [OTU TTI Tab, page 14-9](#)
- [ODU TTI Tab, page 14-9](#)
- [ODU Alert Counters Tab, page 14-9](#)

Step 4 To view additional G.709 properties, click the required tab. [Table 14-4](#) describes the information displayed in each tab.

Table 14-4 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.

Table 14-4 G709 Properties Window Tabs (continued)

Field	Description
OTU Alert Counters Tab	
Type	Type of OTU alert, such as SD-BER or SF-BER.
Threshold	Threshold set for the type of alert.
Counter	Number of alerts reported for each alert type. A value of -1 indicates that no value has been set up.
ODU Alarm Counters Tab	
Type	Type of ODU alarm, such as AIS or BDI.
Counter	Number of alarms reported for each alarm type.
OTU TTI Tab	
This tab is not displayed for Cisco 7600 series devices.	
Type	Type of OTU Trail Trace Identifier (TTI) configured: - Expected - Received - Sent
String Type	For each TTI type, the type of string: - ASCII - Hexadecimal
TTI String	For each TTI type, the specific TTI string configured.
ODU TTI Tab	
This tab is not displayed for Cisco 7600 series devices.	
Type	Type of ODU TTI configured: - Expected - Received - Sent
String Type	For each TTI type, the type of string: - ASCII - Hexadecimal
TTI String	For each TTI type, the specific TTI string configured.
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.

Cisco ANA 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 the Cisco ANA NetworkVision right-click the device on which DWDM is configured, then choose **Inventory**.
- Step 2** In the inventory window, choose **Physical Inventory > Chassis** and navigate to the interface configured for DWDM.
- Step 3** In the content pane, select the performance monitoring configuration settings you want to view:
- To view the performance monitoring 15-minute configuration settings, click **PM 15-min Settings**.
 - To view the performance monitoring 24-hour configuration settings, click **PM 24-hour Settings**.

The Client DWDM PM Settings Properties window is displayed as shown in [Figure 14-4](#).

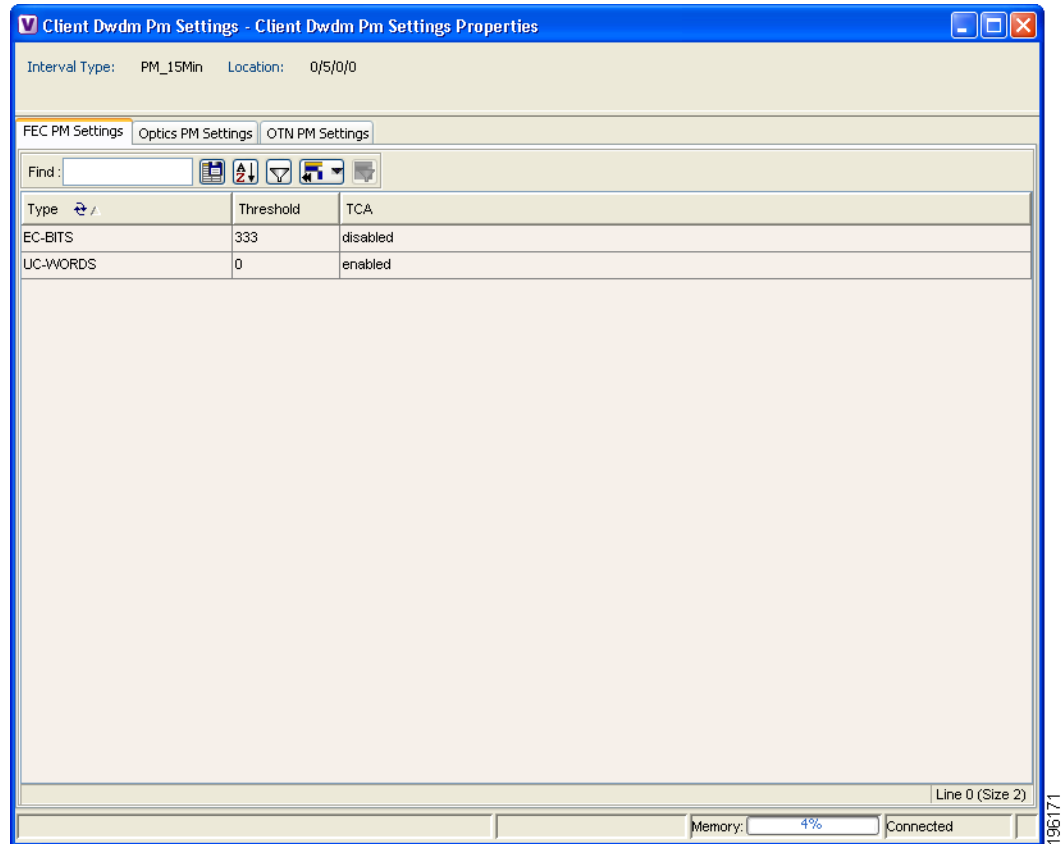
Figure 14-4 Client DWDM PM Settings Properties Window

Table 14-5 describes the information displayed above the tabs in the Client DWDM PM Settings Properties window and in each of the tabs.

Table 14-5 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 <i>rack/slot/module/port</i> where: <i>rack</i> is the chassis number of the rack. <i>slot</i> is the physical slot number of the line card. <i>module</i> is the module number. A physical layer interface module (PLIM) is always 0. Shared port adapters (SPAs) are referenced by their subslot number. <i>port</i> is the physical port number of the interface.

Table 14-5 Client DWDM PM Settings Properties Window and Tabs (continued)

Field	Description
FEC PM Settings Tab	
Type	FEC performance monitoring parameter being tracked: • EC-BITS—The number of bit errors corrected (EC-BITS) in the DWDM trunk line during the performance monitoring time interval. • UC-WORDS—The number of uncorrectable words (UC-WORDS) detected in the DWDM trunk line during the performance monitoring time interval.
Threshold	Threshold for the performance monitoring parameter.
TCA	Indicates whether TCA generation for the specified parameter on the DWDM controller is enabled or disabled.
Optics PM Settings Tab	
Type	Optics performance monitoring parameter being tracked: • LBC—Laser bias current. • OPR—Optical power on the unidirectional port. • OPT—Transmit optical power in dBm.
Max Threshold	Maximum threshold configured for the parameter.
Max TCA	If enabled, indicates a TCA is generated if the value of the parameter exceeds the maximum threshold during the performance monitoring period. If disabled, TCAs are not generated if the maximum threshold is exceeded.
Min Threshold	Minimum threshold configured for the parameter.
Min TCA	If enabled, indicates a TCA is generated if the value of the parameter drops below the minimum threshold during the performance monitoring period. If disabled, TCAs are not generated if the value drops below the minimum threshold.
OTN PM Settings Tab	
Type	OTN performance monitoring parameter being tracked: • bbe-pm-fe—Far-end path monitoring background block errors (BBE-PM). Indicates the number of background block errors recorded in the optical transport network (OTN) path during the performance monitoring time interval. • bbe-pm-ne—Near-end path monitoring background block errors (BBE-PM). • bbe-sm-fe—Far-end section monitoring background block errors (BBE-SM). Indicates the number of background block errors recorded in the OTN section during the performance monitoring time interval. • bbe-sm-ne—Near-end section monitoring background block errors (BBE-SM).

Table 14-5 *Client DWDM PM Settings Properties Window and Tabs (continued)*

Field	Description
Type (cont.)	• bber-pm-fe—Far-end path monitoring background block errors ratio (BBER-PM). Indicates the background block errors ratio recorded in the OTN path during the performance monitoring time interval. • bber-pm-ne—Near-end path monitoring background block errors ratio (BBER-PM). • bber-sm-fe—Far-end section monitoring background block errors ratio (BBER-SM). Indicates the background block errors ratio recorded in the OTN section during the performance monitoring time interval. • bber-sm-ne—Near-end section monitoring background block errors ratio (BBER-SM) • es-pm-fe—Far-end path monitoring errored seconds (ES-PM). Indicates the errored seconds recorded in the OTN path during the performance monitoring time interval. • es-pm-ne—Near-end path monitoring errored seconds (ES-PM). • es-sm-fe—Far-end section monitoring errored seconds (ES-SM). Indicates the errored seconds recorded in the OTN section during the performance monitoring time interval. • es-sm-ne—Near-end section monitoring errored seconds (ES-SM). • esr-pm-fe—Far-end path monitoring errored seconds ratio (ESR-PM). Indicates the errored seconds ratio recorded in the OTN path during the performance monitoring time interval. • esr-pm-ne—Near-end path monitoring errored seconds ratio (ESR-PM). • esr-sm-fe—Far-end section monitoring errored seconds ratio (ESR-SM). Indicates the errored seconds ratio recorded in the OTN section during the performance monitoring time interval. • esr-sm-ne—Near-end section monitoring errored seconds ratio (ESR-SM). • fc-pm-fe—Far-end path monitoring failure counts (FC-PM). Indicates the failure counts recorded in the OTN path during the performance monitoring time interval. • fc-pm-ne—Near-end path monitoring failure counts (FC-PM). • fc-sm-fe—Far-end section monitoring failure counts (FC-SM). Indicates the failure counts recorded in the OTN section during the performance monitoring time interval. • fc-sm-ne—Near-end section monitoring failure counts (FC-SM). • 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.

Table 14-5 *Client DWDM PM Settings Properties Window and Tabs (continued)*

Field	Description
Type (cont.)	• ses-pm-ne—Far-end path monitoring severely errored seconds (SES-PM). • ses-sm-fe—Far-end section monitoring severely errored seconds (SES-SM). Indicates the severely errored seconds recorded in the OTN section during the performance monitoring time interval. • ses-sm-ne—Near-end section monitoring severely errored seconds (SES-SM). • sesr-pm-fe—Far-end path monitoring severely errored seconds ratio (SESR-PM). Indicates the severely errored seconds ratio recorded in the OTN path during the performance monitoring time interval. • sesr-pm-ne—Near-end path monitoring severely errored seconds ratio (SESR-PM). • sesr-sm-fe—Far-end section monitoring severely errored seconds ratio (SESR-SM). Indicates the severely errored seconds ratio recorded in the OTN section during the performance monitoring time interval. • sesr-sm-ne—Near-end section monitoring severely errored seconds ratio (SESR-SM). • uas-pm-fe—Far-end path monitoring unavailable seconds (UAS-PM). Indicates the unavailable seconds recorded in the OTN path during the performance monitoring time interval. • uas-pm-ne—Near-end path monitoring unavailable seconds (UAS-PM). • uas-sm-fe—Far-end section monitoring unavailable seconds (UAS-SM). Indicates the unavailable seconds recorded in the OTN section during the performance monitoring time interval. • uas-sm-ne—Near-end section monitoring unavailable seconds (UAS-SM).
Threshold	Threshold configured for the parameter.
TCA	If enabled, indicates a TCA is generated if the value of the parameter crosses the threshold during the performance monitoring period. If disabled, TCAs are not generated if the value crosses the threshold.

Step 4 To close the Client DWDM PM Settings Properties window, click the upper right corner.



CHAPTER 15

Viewing Ethernet Operations, Administration, and Maintenance Tool Properties

The following topics describe how you can use Cisco ANA to monitor Ethernet operations, administration, and maintenance (OAM) tools:

- [User Roles Required to View Ethernet OAM Tool Properties, page 15-1](#)
- [Ethernet OAM Overview, page 15-2](#)
- [Viewing Connectivity Fault Management Properties, page 15-2](#)
- [Viewing Ethernet LMI Properties, page 15-8](#)
- [Viewing Link OAM Properties, page 15-12](#)

User Roles Required to View Ethernet OAM Tool Properties

[Table 15-1](#) identifies the roles that are required to view Ethernet OAM tool properties. Cisco ANA 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 device-based tasks (tasks that do affect devices), authorization is based on the default permission that is assigned to your account. That is, whether the device 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 Active Network Abstraction 3.7.1 Administrator Guide](#).

Table 15-1 **Default Permission/Security Level Required for Viewing Ethernet OAM Tool Properties**

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View CFM properties	X	X	X	X	X
View Ethernet LMI properties	X	X	X	X	X
View Link OAM properties	X	X	X	X	X

Ethernet OAM Overview

Cisco ANA supports three, interrelated OAM components, including:

- **Connectivity Fault Management**—Connectivity Fault Management (CFM) is an end-to-end per-service-instance (per VLAN) Ethernet layer OAM protocol that includes connectivity monitoring, fault verification, and fault isolation. CFM allows you to manage individual customer service instances. Ethernet Virtual Connections (EVCs) are the services that are sold to customers and are designated by service VLAN tags. CFM operates on a per-service-VLAN (or per-EVC) basis. It lets you know when an EVC fails and provides tools to isolate the failure.
- **Ethernet Local Management Interface**—Ethernet Local Management Interface (Ethernet LMI) operates between the customer edge (CE) and the user-facing provider edge (U-PE) devices. Ethernet LMI allows you to automatically provision CEs based on EVCs and bandwidth profiles.
- **Link OAM**—Link OAM allows you to monitor and troubleshoot a single Ethernet link. It is an optional sublayer implemented in the Data Link Layer between the Logical Link Control (LLC) and MAC sublayers of the Open Systems Interconnect (OSI) model. You can monitor a link for critical events and, if needed, put a remote device into loopback mode for link testing. Link OAM also discovers unidirectional links, which are created when one transmission direction fails.

Viewing Connectivity Fault Management Properties

CFM provides capabilities for detecting, verifying, and isolating connectivity failures in networks with bridges operated by multiple independent organizations, each with restricted management access to each other's equipment. CFM allows you to discover and verify end-to-end, Carrier Ethernet PE-to-PE or CE-to-CE paths through bridges and LANs.

CFM consists of maintenance domains. Maintenance domains are administrative regions used to manage and administer specific network segments. Maintenance domains are organized in a hierarchy. The administrator assigns a maintenance level to the domain from 0 (lowest level) to 7 (highest level); the maintenance level determines the domain's position within the CFM hierarchy.

CFM maintenance domain boundaries are indicated by maintenance points. A maintenance point is an interface point that participates within a CFM maintenance domain. Maintenance point types include:

- **Maintenance Endpoints**—Maintenance endpoints (MEPs) are active CFM elements residing at the edge of a domain. MEPs can be inward or outward facing. They periodically transmit continuity check messages and expect to periodically receive similar messages from other MEPs within a domain. If requested, MEPs can also transmit traceroute and loopback messages. MEPs are responsible for keeping CFM messages within the boundaries of a maintenance domain.
- **Maintenance Intermediate Points**—Maintenance intermediate points (MIPs) are passive elements that catalog information received from MEPs and other MIPs. MIPs only respond to specific CFM messages such as traceroute and loopback, and they forward those messages within the maintenance domain.

**Note**

Cisco ANA does not display information for CFM maintenance endpoints or maintenance intermediate points for Cisco Viking devices if errors exist in their configurations. An error in the configuration is indicated by an exclamation point (!) in the CLI output.

For example, if you enter the command `show ethernet cfm local maintenance-points`, a configuration error is indicated as follows:

```
cfm_d100/2          cfm_s100          Te0/2/0/3.100          Up MEP 2100 eb:7a:53!
```

To view CFM properties:

Step 1 In Cisco ANA NetworkVision, double-click the required device for CFM.

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

Figure 15-1 shows an example of CFM in logical inventory.

Figure 15-1 CFM in Logical Inventory

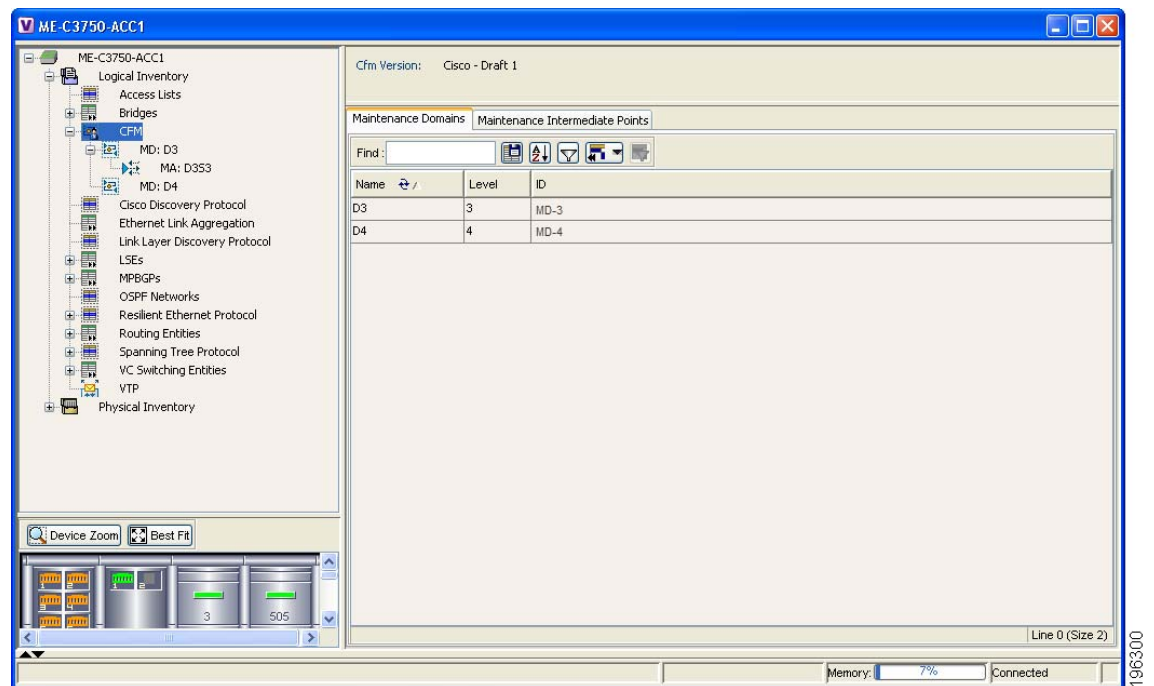
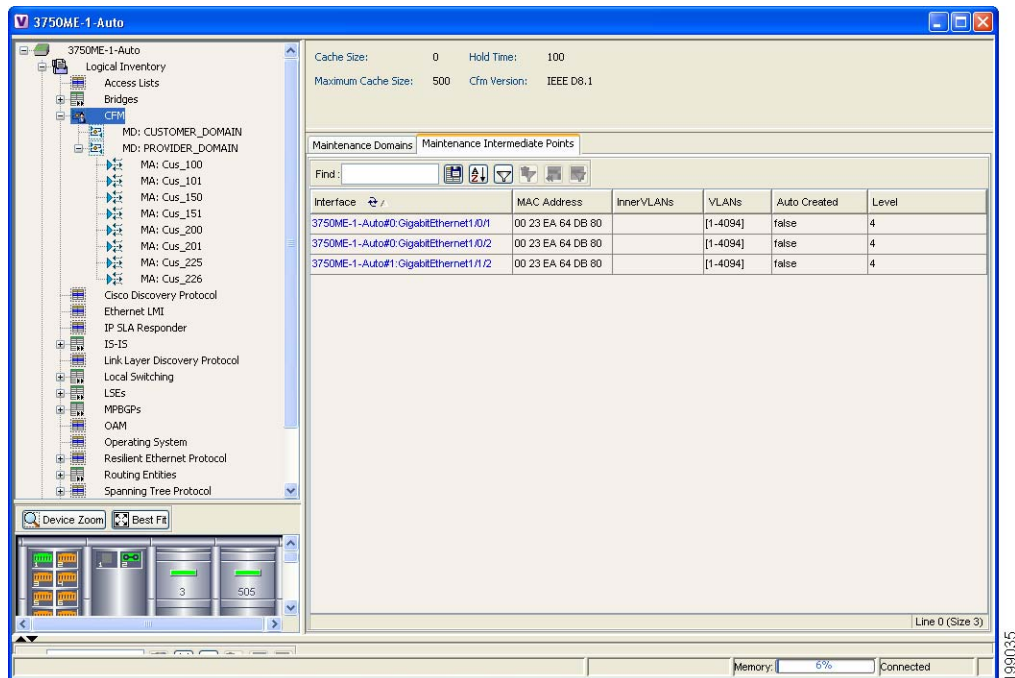


Table 15-2 describes the information displayed for CFM.

Table 15-2 CFM Properties

Field	Description
CFM Version	CFM version, such as IEEE D8.1.
Maintenance Domains Table	
Name	Domain name.
Level	Unique level the domain is managed on. Values range from 0 to 7.
ID	Optional domain identifier.

Step 3 Click the Maintenance Intermediate Points tab to view MIP information. See [Figure 15-2](#).

Figure 15-2 CFM Maintenance Intermediate Points Tab

[Table 15-3](#) describes the information that is displayed in the Maintenance Intermediate Points table.

Table 15-3 CFM Maintenance Intermediate Point Properties

Field	Description
Interface	Interface configured as a MIP, hyperlinked to its entry in physical inventory.
MAC Address	MAC address of the interface.
Inner VLANs	Inner VLAN identifiers.
VLANs	VLANs associated with the interface.
Auto Created	Whether or not the MIP was automatically created: True or False.
Level	Unique level the domain is managed on. Values range from 0 to 7.

Step 4 To view the details of a specific maintenance domain, do one of the following:

- Choose **Logical Inventory > CFM > domain**.
- Double-click the required entry in the Maintenance Domains table.

Figure 15-3 shows an example of the information displayed for the maintenance domain.

Figure 15-3 CFM Maintenance Domain Properties

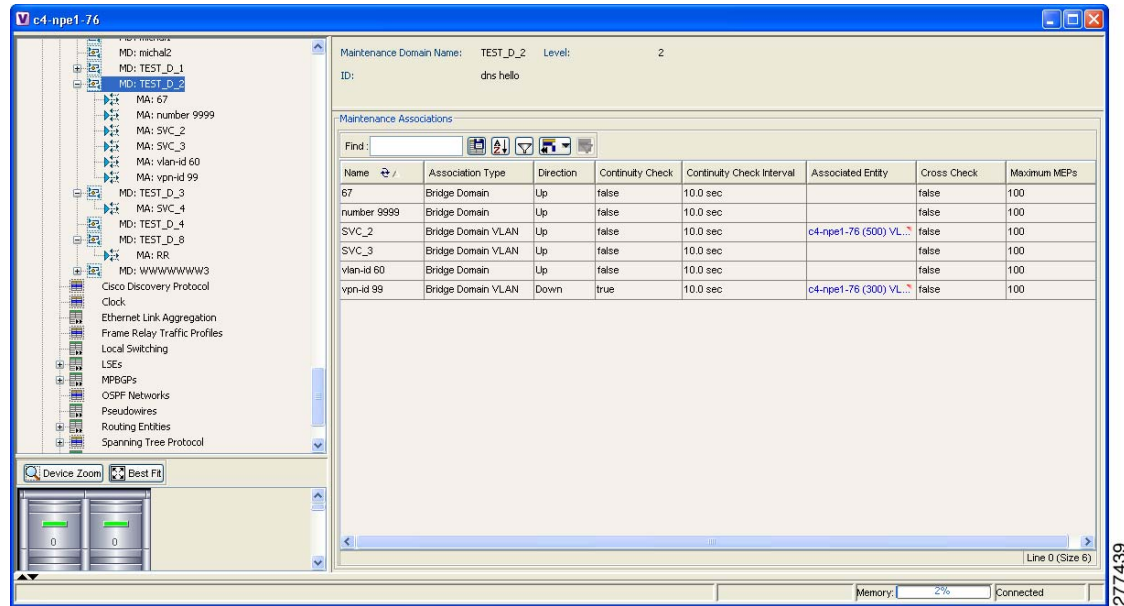


Table 15-4 describes the information that is displayed for CFM maintenance domains.

Table 15-4 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.

Table 15-4 CFM Maintenance Domain Properties (continued)

Field	Description
Maximum MEPs	Maximum number of maintenance endpoints (MEPs) that can be configured on the maintenance association.
Inner VLAN	Inner VLAN identifier.

Step 5 To view the properties for a maintenance association's endpoints, do one of the following:

- Choose **Logical Inventory > CFM > domain > association**.
- In the Maintenance Associations table, double-click the required association.

Figure 15-4 shows the information displayed for the maintenance association endpoints.

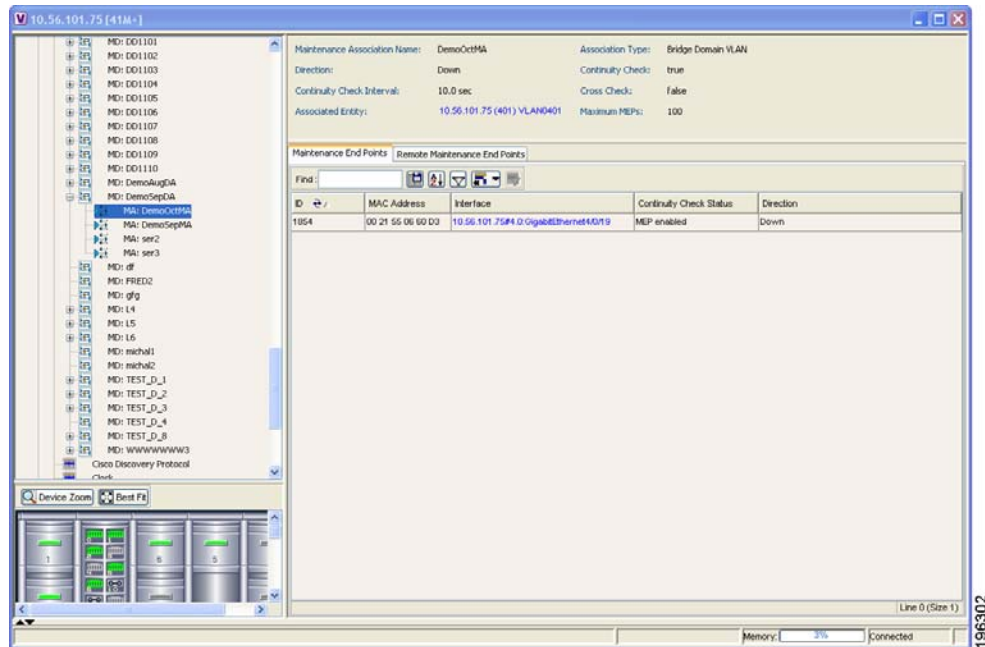
Figure 15-4 CFM Maintenance Association - Endpoint Properties

Table 15-5 describes the information that is displayed for CFM maintenance associations and MIPs.

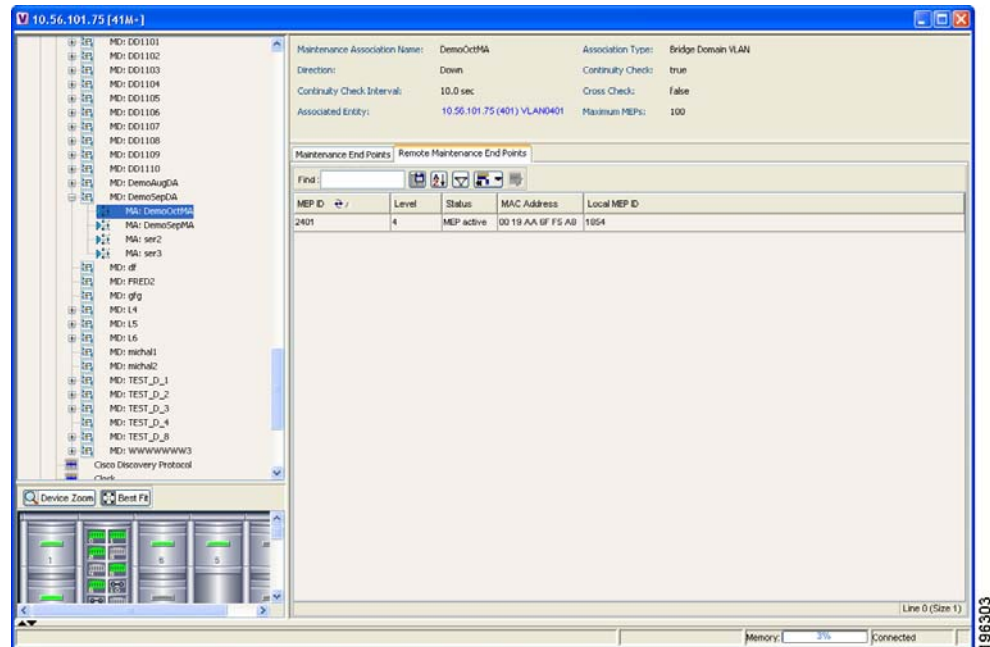
Table 15-5 CFM Maintenance Association Properties

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.

Table 15-5 CFM Maintenance Association Properties (continued)

Field	Description
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.
Interface	Interface on which the MEP is configured, hyperlinked to the respective EFP, VSI or interface in inventory.
Continuity Check Status	CFM continuity check status: MEP Active, MEP Inactive, MEP Enabled, MEP Disabled, or Unknown.
Direction	Direction of traffic on which the MEP is defined: Up, Down, or Unknown.

Step 6 Click the **Remote Maintenance End Points** tab to view the information displayed for remote MEPs. See [Figure 15-5](#).

Figure 15-5 Remote Maintenance End Points Table

[Table 15-6](#) describes the information presented for remote MEPs.

Table 15-6 CFM Remote Maintenance End Points Table

Field	Description
MEP ID	Remote MEP identifier.
Level	Level at which the remote MEP is managed: 0-7.
Status	Status of the remote MEP, such as MEP Active.
MAC Address	MAC address of the remote MEP.
Local MEP ID	Numeric identifier assigned to the local MEP. Values range from 1 to 8191. Note If the remote MEP is in Up mode, the remote MEP is not associated to the local MEP. As a result, the Local MEP ID column is empty.

Viewing Ethernet LMI Properties

Ethernet Local Management Interface (LMI) is a protocol that operates between the customer edge (CE) network element and the provider edge (PE) network element.

Ethernet LMI:

- Runs only on the PE-CE User Network Interface (UNI) link.
- Notifies the CE of connectivity status and configuration parameters of Ethernet services available on the CE port.

Ethernet LMI interoperates with CFM, another OAM protocol that runs within the provider network, to collect OAM status. CFM runs at the provider maintenance level with inward-facing MEPs at the UNI. Using the OAM Ethernet infrastructure, Ethernet LMI works with CFM to provide end-to-end status of Ethernet virtual connections (EVCs) across CFM domains.

To view Ethernet LMI properties:

-
- Step 1** In Cisco ANA NetworkVision, double-click the device configured for Ethernet LMI.
- Step 2** In the inventory window, choose **Logical Inventory > Ethernet LMI**.

Figure 15-6 shows an example of Ethernet LMI properties in logical inventory.

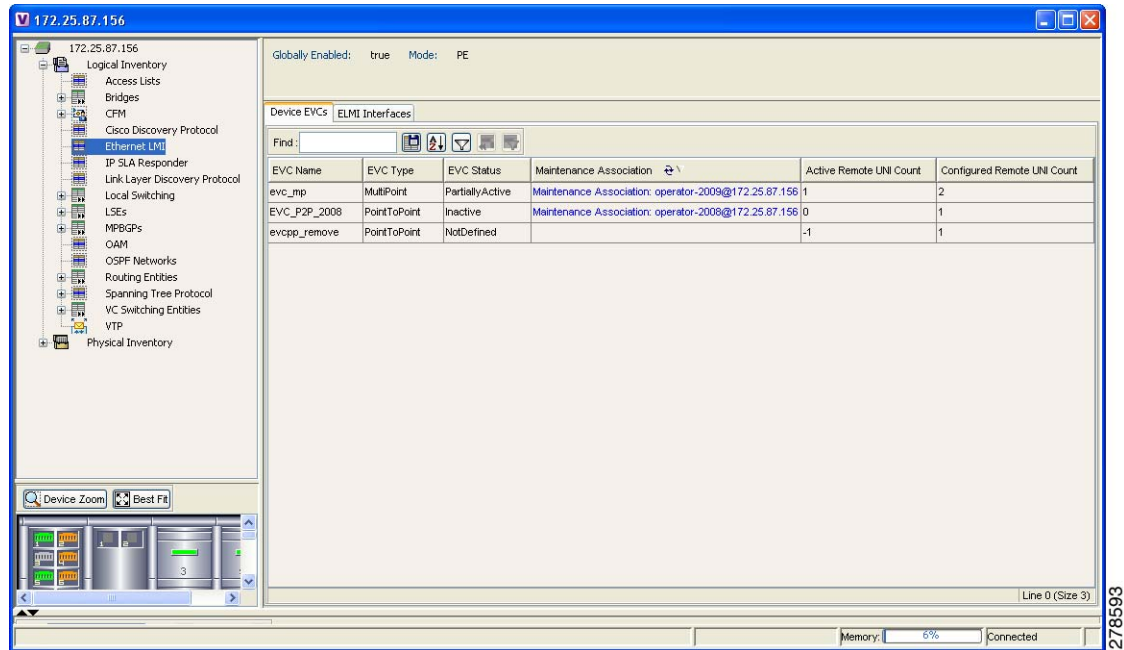
Figure 15-6 Ethernet LMI in Logical Inventory

Table 15-7 describes the information displayed for Ethernet LMI.

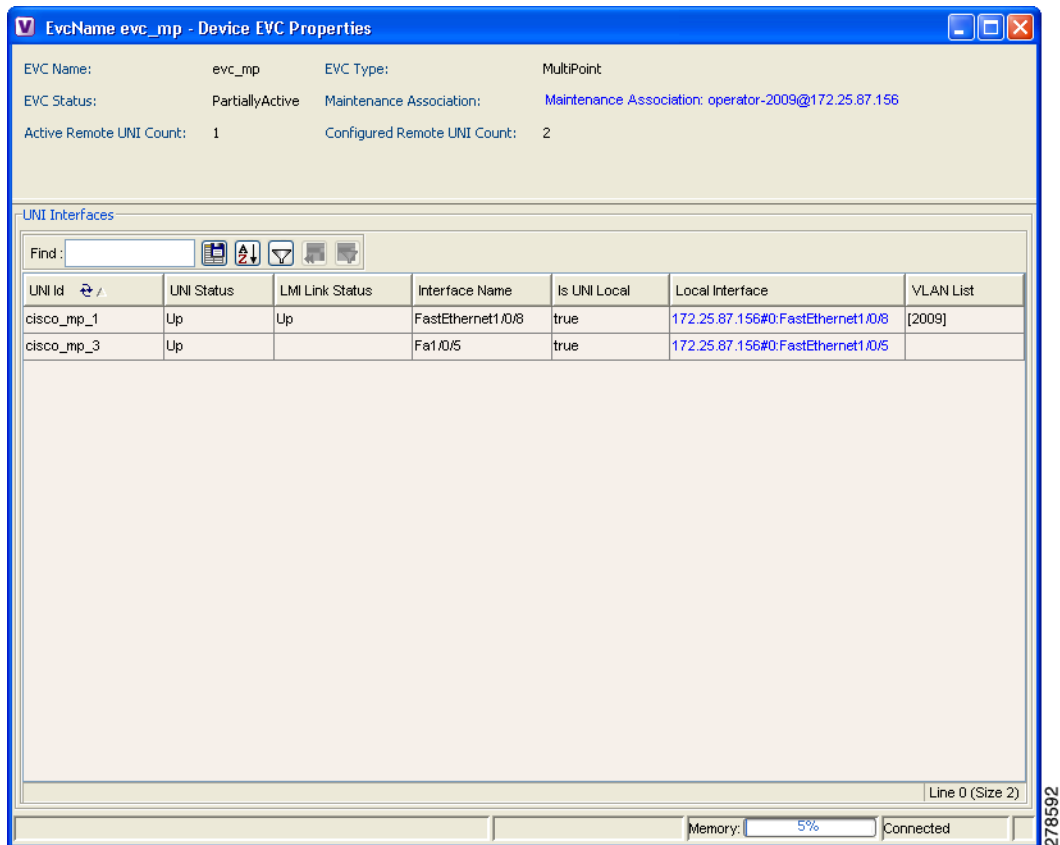
Table 15-7 Ethernet LMI Properties in Logical Inventory

Field	Description
Globally Enabled	Whether or not Ethernet LMI is enabled globally: True or False.
Mode	Ethernet LMI mode: CE or PE.
Device EVCs Tab	
EVC Name	Name of the EVC.
EVC Type	Type of EVC: Point-to-point or Multipoint.
EVC Status	EVC status: Active, Inactive, Not Defined, or Partially Active.
Maintenance Association	Hyperlinked entry to the maintenance association in CFM in logical inventory. For more information about maintenance associations, see Table 15-5 .
Active Remote UNI Count	Number of active remote UNIs.
Configured Remote UNI Count	Number of configured remote UNIs.
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.

Table 15-7 Ethernet LMI Properties in Logical Inventory (continued)

Field	Description
N391	Frequency at which the customer equipment polls the status of the UNI and all EVCs. The range is 1-65000 seconds, with a default of 360 seconds.
N393	Error count for the metro Ethernet network. The range is 1-10, with a default of 4.

Step 3 To view device EVC properties, double-click an EVC name in the Device EVCs tab. The Device EVC Properties window is displayed as shown in [Figure 15-7](#).

Figure 15-7 Device EVC Properties Window

[Table 15-8](#) describes the information displayed in the Device EVC Properties window.

Table 15-8 Device EVC Properties in Logical Inventory

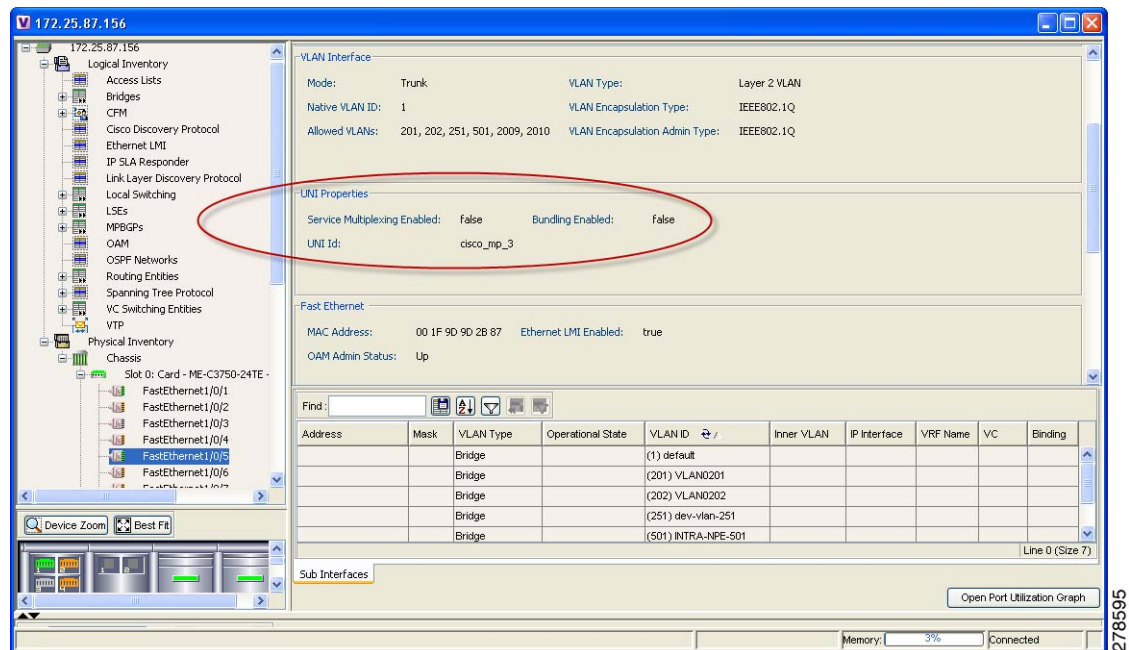
Field	Description
EVC Name	Name of the EVC.
EVC Type	Type of EVC: Point-to-point or Multipoint.
EVC Status	EVC status: Active, Inactive, Not Defined, or Partially Active.

Table 15-8 Device EVC Properties in Logical Inventory (continued)

Field	Description
Maintenance Association	Hyperlinked entry to the maintenance association in CFM in logical inventory. For more information about maintenance associations, see Table 15-5 .
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 ELMUI Interfaces table (see [Step 2](#)).

The UNI properties are displayed as shown in [Figure 15-8](#).

Figure 15-8 Ethernet LMI UNI Properties in Physical Inventory

[Table 15-9](#) describes the information displayed in the UNI Properties area in physical inventory.

Table 15-9 Ethernet LMI UNI Properties in Physical Inventory

Field	Description
Service Multiplexing Enabled	Whether or not the interface is configured for UNI multiplexing: True or False.
Bundling Enabled	Whether or not the interface is configured for UNI bundling: True or False.
UNI Id	UNI identifier.
Bundling Type	Type of bundling applied: All-to-One or None. This field appears only when a bundling type is set.

Viewing Link OAM Properties

Link OAM is an optional sublayer implemented in the OSI Data Link Layer between the Logical Link Control and MAC sublayers.

The Link OAM frames, OAM Protocol Data Units (OAMPDUs), cannot propagate beyond a single hop within an Ethernet network. Link OAM processes include:

- **Discovery**—Discovery is the first Link OAM process. During discovery, Link OAM identifies the devices at each end of the link and learns their OAM capabilities.
- **Link monitoring**—Link OAM link monitoring includes:
 - Monitoring links and issuing notifications when error thresholds are exceeded or faults occur.
 - Collecting statistics on the number of frame errors (or percent of frames that have errors) and the number of coding symbol errors.
- **Remote MIB Variable Retrieval**—Provides 802.3ah MIB polling and response (but not writing).
- **Remote Failure indication**—Informs peers when a received path goes down. Because link connectivity faults caused by slowly deteriorating quality are difficult to detect, Link OAM communicates such failure conditions to its peer using OAMPDU flags. The failure conditions that can be communicated are a loss of signal in one direction on the link, an unrecoverable error (such as a power failure), or some other critical event.
- **Remote Loopback**—Puts the peer device in (near-end) intrusive loopback mode using the OAMPDU loopback control. Statistics can be collected during the link testing. In loopback mode, every frame received is transmitted back unchanged on the same port (except for OAMPDUs, which are needed to maintain the OAM session). Loopback mode helps ensure the quality of links during installation or troubleshooting. Loopback mode can be configured so that the service provider device can put the customer device into loopback mode, but the customer device cannot put the service provider device in loopback mode.

To view Link OAM properties:

-
- Step 1** In Cisco ANA NetworkVision, double-click the device configured for Link OAM.
- Step 2** In the inventory window, choose **Logical Inventory > OAM**.

Figure 15-9 shows an example of Link OAM properties in logical inventory.

Figure 15-9 Link OAM Properties in Logical Inventory

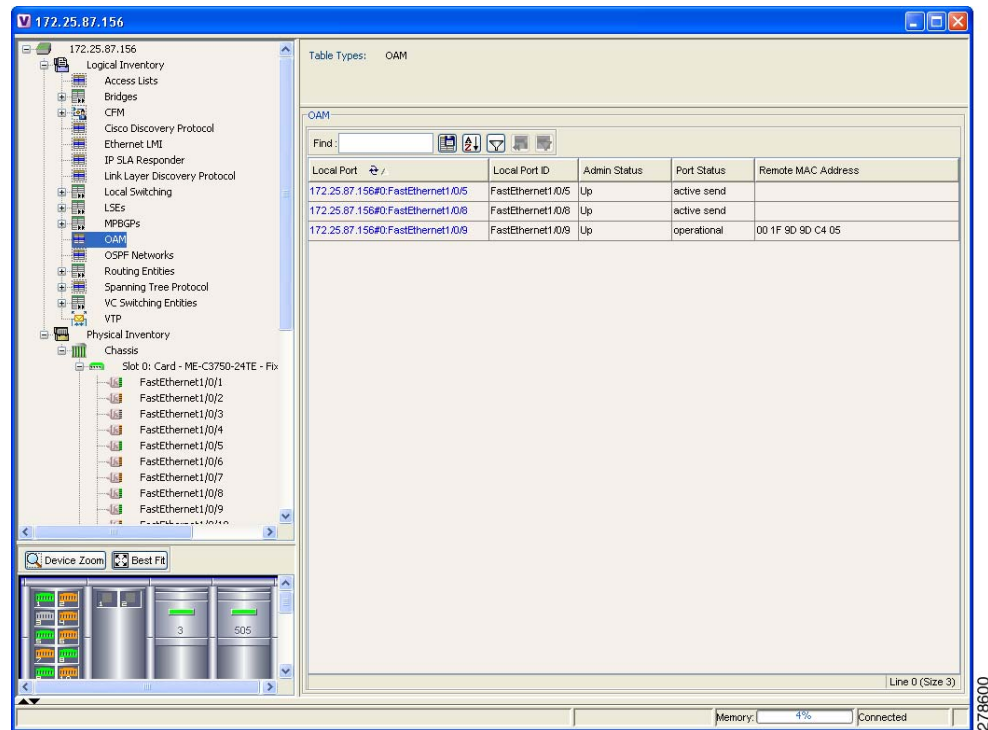


Table 15-10 describes the information displayed for Link OAM.

Table 15-10 Link OAM Properties in Logical Inventory

Field	Description
Table Types	Type of table. In this case, it is OAM.
OAM Table	
Local Port	Name of the OAM-supported interface, hyperlinked to the location in physical inventory.
Local Port ID	Local port identifier, such as FastEthernet1/0/9.
Admin Status	Administrative status of the interface.
Port Status	Status of the port.
Remote MAC Address	Remote client MAC address.

Step 3 To view detailed information about an entry in the table, double-click the required entry. The Link OAM Data Properties window is displayed as shown in Figure 15-10.

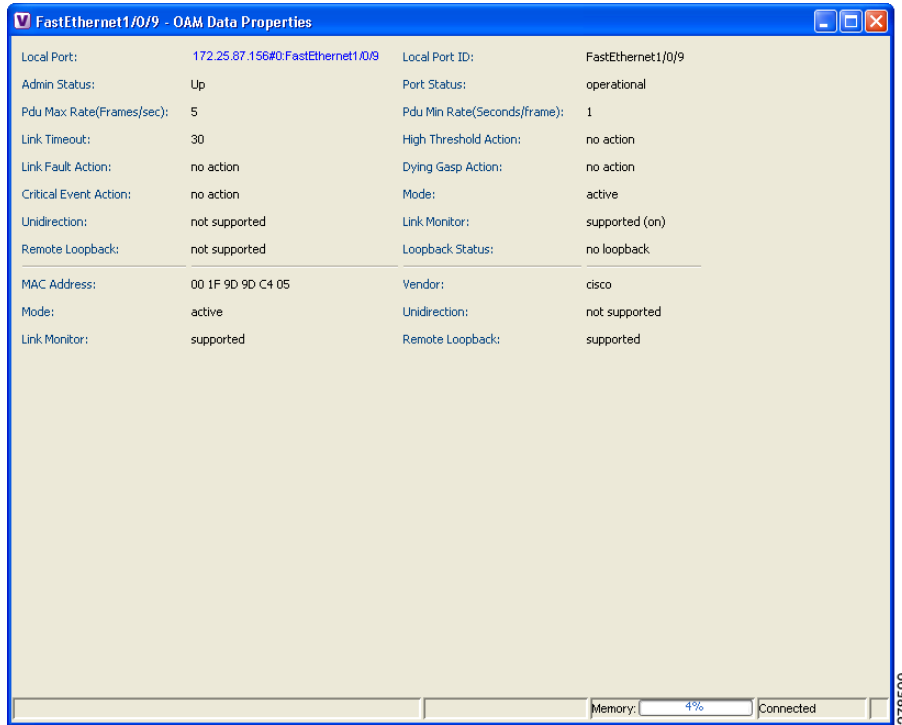
Figure 15-10 Link OAM Data Properties Window

Table 15-11 describes the information that is displayed in the Link OAM Data Properties window.

Table 15-11 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 rate 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.
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.

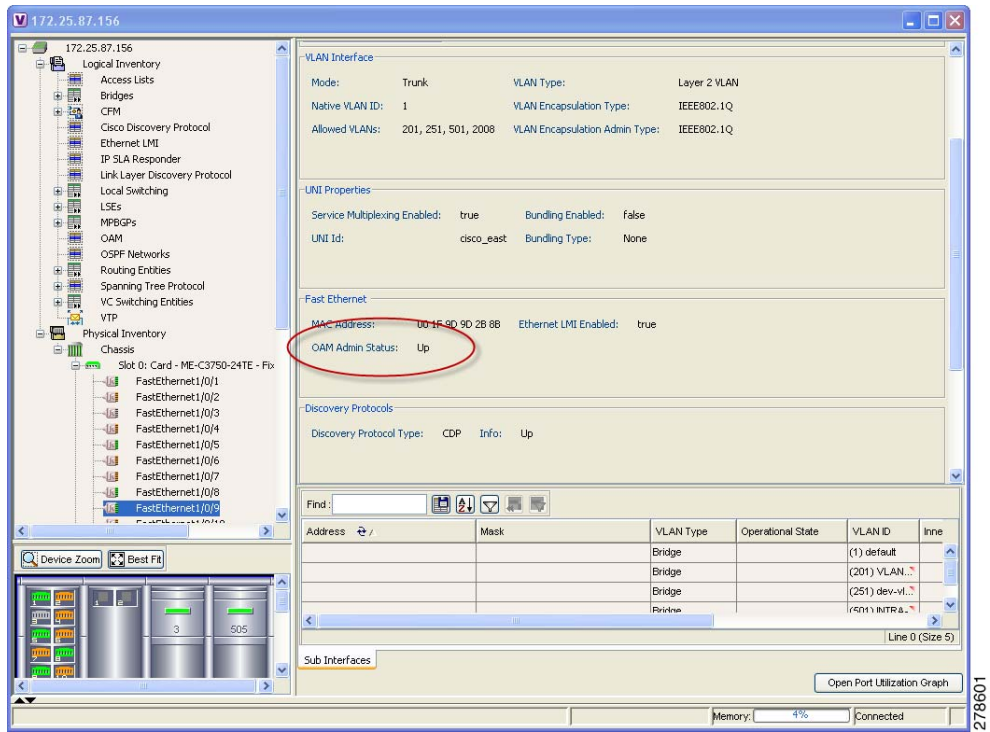
Table 15-11 *Link OAM Data Properties Window (continued)*

Field	Description
Unidirection	Status of unidirectional Ethernet on the local interface: Supported or Not supported.
Link Monitor	Status of link monitoring on the local interface: Supported or Not supported.
Remote Loopback	Status of remote loopback on the local interface: Supported or Not supported.
Loopback Status	Status of loopback on the local interface: Supported or No loopback.
Remote Client	
MAC Address	MAC address for the remote client.
Vendor	Vendor of the remote client.
Mode	Mode of the remote client: Active or Passive.
Unidirection	Status of unidirectional Ethernet on the remote client interface: Supported or Not supported.
Link Monitor	Status of link monitoring on the remote client interface: Supported or Not supported.
Remote Loopback	Status of loopback on the remote client interface: Supported or Not supported.

Step 4 To view Link OAM status in physical inventory, choose **Physical Inventory** > *chassis* > *slot* > *interface*.

The Link OAM administrative status is displayed as shown in [Figure 15-11](#).

Figure 15-11 Link OAM Administrative Status in Physical Inventory





CHAPTER 16

IPv6 and IPv6 VPN over MPLS

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.

The following topics tell you how you can use Cisco ANA to view 6VPE properties:

- [User Roles Required to Work with IPv6 and 6VPE, page 16-1](#)
- [Viewing IPv6 Information, page 16-2](#)

User Roles Required to Work with IPv6 and 6VPE

[Table 16-1](#) identifies the roles that are required to work with IPv6 and 6VPE in Cisco ANA. Cisco ANA 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 device-based tasks (tasks that do affect devices), authorization is based on the default permission that is assigned to your account. That is, whether the device 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 Active Network Abstraction 3.7.1 Administrator Guide](#).

Table 16-1 Default Permission/Security Level Required for Viewing IPv6 Properties

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View IPv6 properties	X	X	X	X	X

Viewing IPv6 Information

Cisco ANA NetworkVision displays IPv6 addresses when they are configured on PE and CE routers in the Cisco ANA NetworkVision IP interface table. IPv6 addresses are:

- Displayed in the Cisco ANA NetworkVision 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 ANA PathTracer to trace paths and present path trace results.

IPv6 information appears in the following locations in logical and physical inventory:

Inventory Location	Description
Logical Inventory	
MPBGPs	IP address family identifiers indicate the BGP peer address family: IPv4, IPv6, VPNv4, or VPNv6. For information, see Viewing MP-BGP Information, page 17-30 .
Routing Entities	IPv6 addresses appear under the IP Interfaces tab in the table view when applicable, and the interface properties window.
VRFs	IPv6 addresses appear under the Sites tab in the interface table and interface properties popup window, and in the VRF IPV6 Routing Table tab. See Figure 17-5 on page 17-19 .
Physical Inventory	
Port	IPv6 addresses appear in the Subinterfaces tab and interface properties popup window.

The IP addresses that appear depend on whether the interface has only IPv4 addresses, only IPv6 addresses, or both IPv4 and IPv6 addresses, as shown in [Table 16-2](#).



Note

To display the properties window, right-click the IP address in the interface table and choose **Properties**.

Table 16-2 *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.

Be aware of the following when working with IPv6 addresses:

- Cisco ANA NetworkVision MPLS label switching and Label Switching Entities (LSEs) do not display IPv6 addresses. However, the Neighbor Discovery Protocol (NDP) table does display IPv6 addresses.
- Cisco ANA supports all the textual presentations of address prefixes. However, Cisco ANA NetworkVision 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 Cisco ANA NetworkVision.

Figure 16-1 shows a port inventory view of a port with IPv4 and IPv6 addresses. In this example, one IPv4 address and multiple IPv6 addresses are provisioned on the interface.

- The primary IPv4 address appears in the interface table and properties window. If secondary IPv4 addresses were provisioned on the interface, they would appear in the properties window.
- IPv6 addresses provisioned on the interface appear in the properties window and Sub Interface tab.

Figure 16-1 Port with IPv4 and IPv6 Addresses

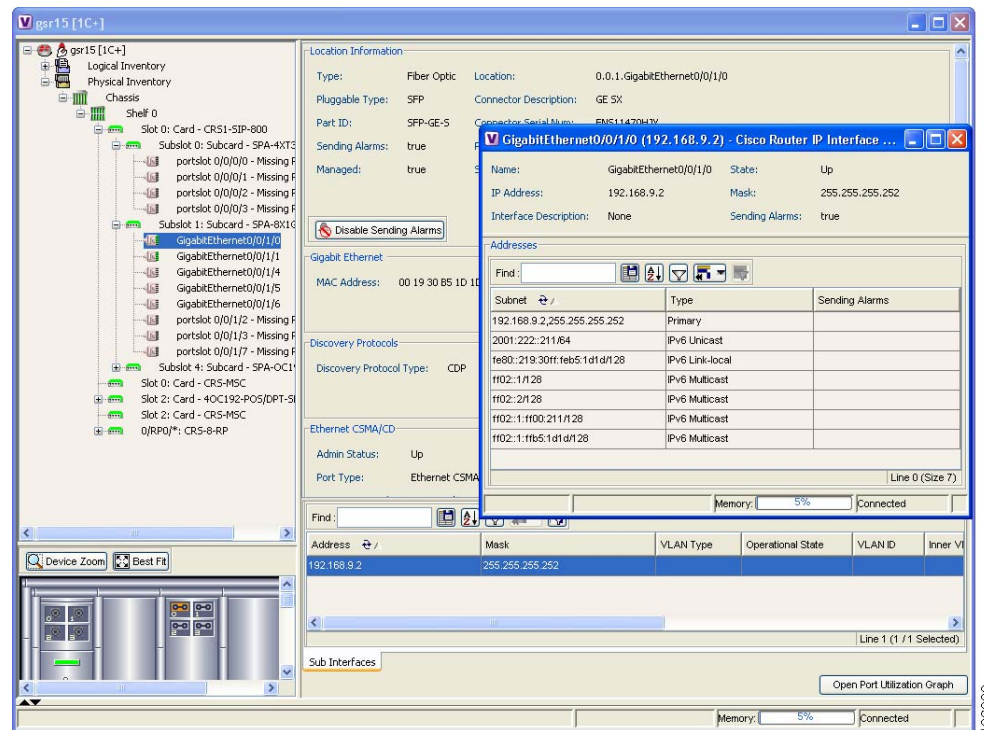


Figure 16-2 shows a port with only IPv6 addresses provisioned. In this example, the lowest IPv6 address is shown in the subinterface table, and all IPv6 addresses are shown in the interface properties window.



Note

For information on the IPv6 addressing format, see the [Cisco Active Network Abstraction 3.7.1 Theory of Operations Guide](#).

The screenshot displays the vgs15 [1C+] network management interface. The left sidebar shows a tree view of the network topology, including Logical Inventory, Physical Inventory, Chassis, and Slot 0. The main window shows the configuration for GigabitEthernet0/0/1/1.2 on a Cisco Router. The configuration parameters are as follows:

- Port ID: SFP-GE-5
- Connector Serial Num: FNS11470HK5
- Sending Alarms: true
- Port Alias: GigabitEthernet0/0/1/1
- Managed: true
- Status: OK

The detailed view of the interface configuration shows the following parameters:

- Name: GigabitEthernet0/0/1/1.2
- State: Down
- IP Address: 2001:210:10:15::15
- Mask: ffff.ffff.ffff.ffff
- Interface Description: None
- Sending Alarms: true

The interface also displays a table of addresses and a table of sub-interfaces.

Subnet	Type	Sending Alarms
2001:210:10:15::15/64	Pv6 Unicast	
fe80::219:30ff:feb5:1d1e1f28	Pv6 Link-local	
ff02::1:1/28	Pv6 Multicast	
ff02::2/28	Pv6 Multicast	

Address	Mask	VLAN Type	Operational State	VLAN ID	Inne
2001:210:10:15::15	ffff.ffff.ffff.ffff				
2001:1023:156:550:219:30ff:feb5:1	ffff.ffff.ffff.ffff	IEEE802.1Q	Up	550	
2001:1025:156:1:219:30ff:feb5:1d1e	ffff.ffff.ffff.ffff	IEEE802.1Q	Up	250	

The interface also displays a table of sub-interfaces:

Sub Interfaces
Open Port Utilization Graph



CHAPTER 17

Monitoring MPLS Services

The following topics describe how to view and manage aspects of Multiprotocol Label Switching (MPLS) services using Cisco ANA NetworkVision, including the MPLS service view, business configuration, and maps. The topics also describe the device inventory specific to MPLS VPNs, including routing entities, label switched entities (LSEs), BGP neighbors, Multiprotocol BGP (MP-BGP), VRF instances, pseudowires, and TE tunnels. Topics include:

- [User Roles Required to Work with MPLS Networks, page 17-1](#)
- [Viewing VPNs in Cisco ANA NetworkVision, page 17-3](#)
- [Managing VPNs, page 17-6](#)
- [Working with VPN Overlays, page 17-9](#)
- [Working with CE Devices, page 17-11](#)
- [Working with Tunnels, page 17-13](#)
- [Working with LCAs and LCPs, page 17-15](#)
- [Monitoring MPLS Services, page 17-17](#)

For more information about MPLS and Cisco ANA, see the [Cisco Active Network Abstraction 3.7.1 Theory of Operations Guide](#).

User Roles Required to Work with MPLS Networks

[Table 17-1](#) identifies the roles that are required to work with MPLS networks. Cisco ANA 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 device-based tasks (tasks that do affect devices), authorization is based on the default permission that is assigned to your account. That is, whether the device 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 Active Network Abstraction 3.7.1 Administrator Guide](#).

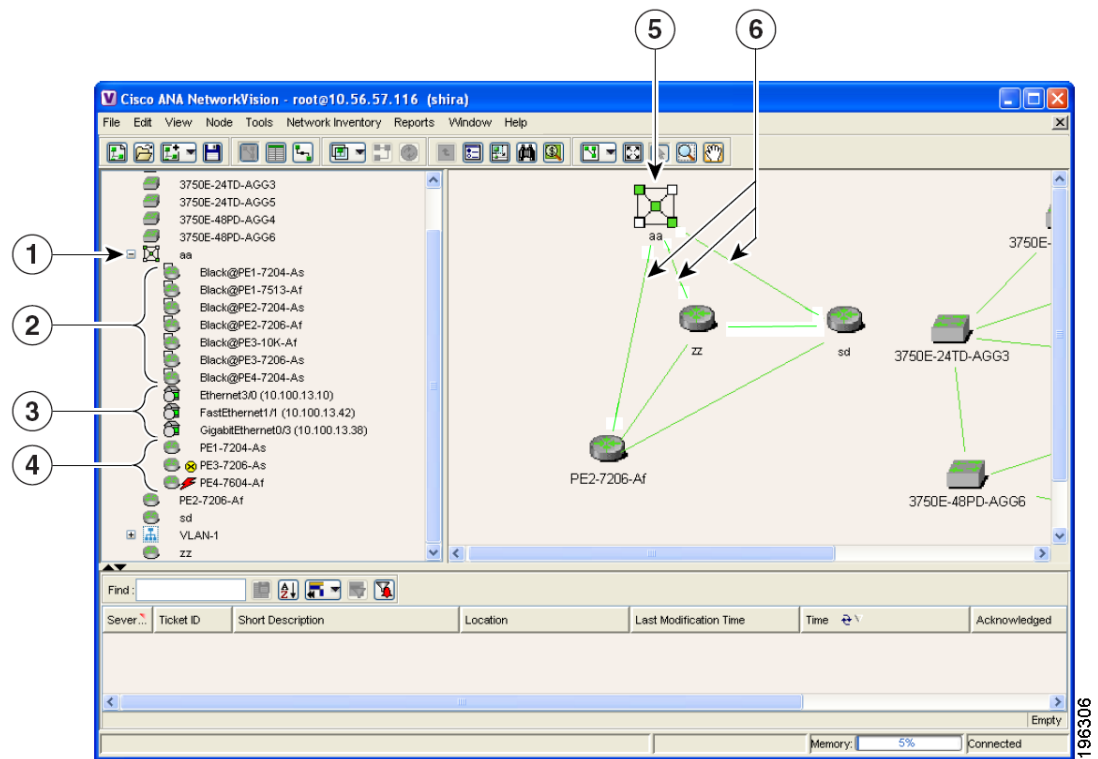
Table 17-1 *Default Permission/Security Level Required for Working with MPLS Networks*

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
VPNs					
Add tunnels to VPNs	—	—	—	—	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
Remove VPNs from a map	—	—	X	X	X
View VPN properties	—	—	—	—	X
View VPNs in Cisco ANA NetworkVision	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
View the NDP table	—	—	—	—	X
View rate limit information	—	—	—	—	X
Other					
View BFD properties	—	—	—	—	X
View cross-VRF routing entries	—	—	—	—	X
View LSE properties	—	—	—	—	X
View MP-BDP information	—	—	—	—	X
View MPLS TE tunnel information	—	—	—	—	X
View port configurations	—	—	—	—	X
View pseudowire end-to-end emulation tunnels	—	—	—	—	X

Viewing VPNs in Cisco ANA NetworkVision

Figure 17-1 shows a VPN displayed in the Cisco ANA NetworkVision map view. In this example, the VPN is selected in the navigation pane, so the VPN details, such as virtual routers and IP interfaces, are not shown in the map view.

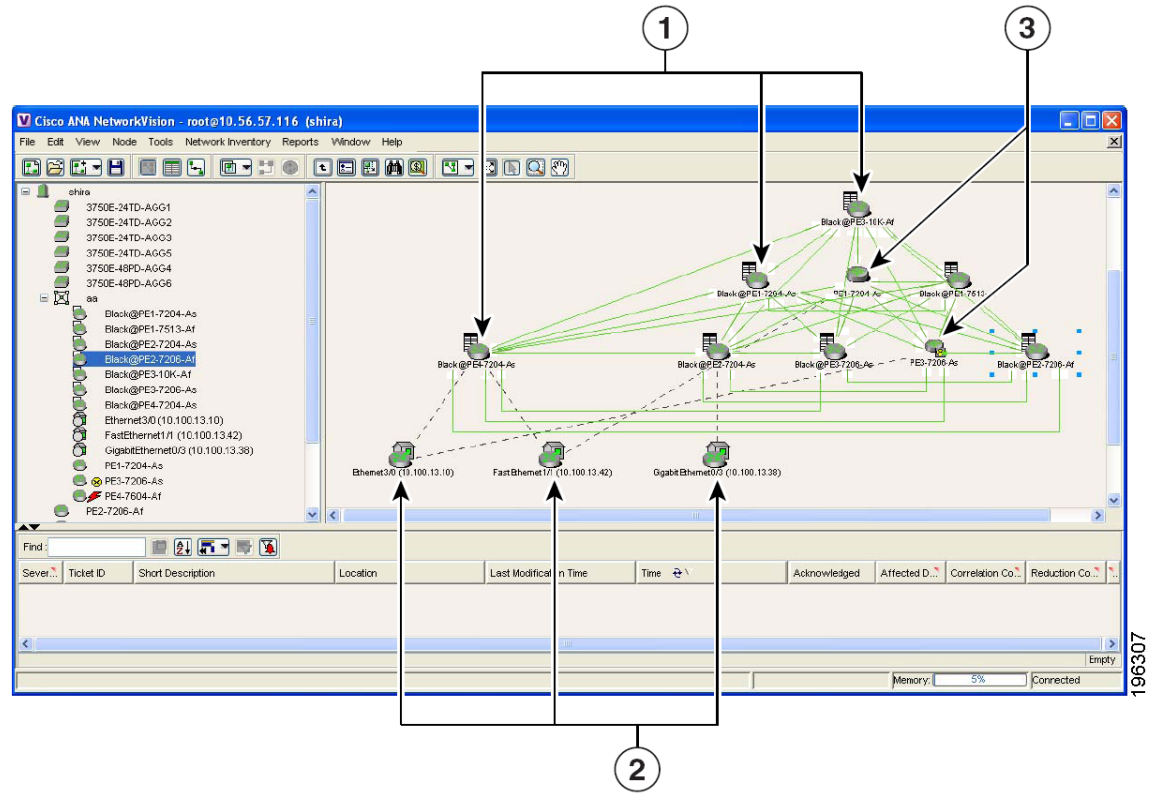
Figure 17-1 VPN in Cisco ANA NetworkVision Map View



1	VPN in the navigation tree	4	Network elements
2	Virtual routers	5	VPN in the map view
3	Sites	6	VPN links (IPv4 and IPv6 aware)

Figure 17-2 shows a VPN with details, including virtual routers, IP interfaces, and network elements, displayed in the Cisco ANA NetworkVision map view.

Figure 17-2 VPN in Cisco ANA NetworkVision Map View with VRFs and Sites



1	Virtual router
2	Sites
3	Network elements

The Cisco ANA NetworkVision 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 [Network Element Status Indicators](#), page 2-17.

Table 17-2 shows the VPN icons in the Cisco ANA NetworkVision map view.

Table 17-2 VPN Icons in Cisco ANA NetworkVision Map View

Icon	Description
	Root (map name) or aggregation
	VPN

Table 17-2 VPN Icons in Cisco ANA NetworkVision Map View (continued)

Icon	Description
	Virtual router
	Site
	Site business element with an actively associated, hidden CE device
	LCA business element
	LCP business element
	LCP business element with an actively assigned tunnel edge for a hidden CE device

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 also be displayed in the Layer 3 VPN sub-branches. The Layer 2 VPN sub-branches display the LCAs and LCPs contained in the VPN along with the names of the business elements. In addition, CE devices can also be displayed in the Layer 2 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 Cisco ANA NetworkVision 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.

Cisco ANA presents tickets related to the map in the ticket area, which allows you to view and manage the VPN tickets.

Viewing Additional VPN Properties

Cisco ANA NetworkVision allows you to select any element in the navigation pane or map view and view additional underlying properties. To view additional properties for an object, either double-click it or right-click it and choose **Properties**. [Table 17-3](#) shows the additional properties available for VPN entities.

Table 17-3 *Displaying Additional VPN Properties*

Object	Drill-Down Display	For Additional Information
VPN	- Double-clicking a VPN displays the participating VRFs, sites, and network elements in the navigation pane and map view. - Right-clicking a VPN and choosing Properties displays the VPN Properties window.	Viewing VPN Properties, page 17-17
VRF	Double-clicking a VRF displays the VRF properties window	Viewing VRF Properties, page 17-18
Site	Double-clicking a site displays the IP Interface Properties window	Viewing Site Properties, page 17-17
Link	Double-clicking a link displays the link properties window. The properties depend on the link type.	Chapter 5, “Working with Links”

Managing VPNs

The following topics describe:

- [Creating a VPN, page 17-6](#)
- [Adding a VPN to a Map, page 17-7](#)
- [Removing a VPN from a Map, page 17-8](#)
- [Moving a Virtual Router Between VPNs, page 17-8](#)

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 Cisco ANA NetworkVision navigation pane, select the map root.
- Step 2** From the File menu, choose **Add to Map > VPN > New**.
- Step 3** In the Create VPN dialog box, enter the following:
- Name—A unique name for the new VPN.

**Note**

VPN business element names are case sensitive.

- **Icon**—To use a custom icon for the VPN, click the button next to the Icon field and navigate to the icon file.

**Note**

If a path is not specified to an icon, the default VPN icon is used (for more information about icons, see [Table 17-2 on page 17-4](#)).

- **Description**—(Optional) An additional VPN description.

Step 4 Click **OK**.

The new VPN is added to the VPN list in the Add VPN dialog box.

For more information about loading the newly created VPN in the service view map, see [Adding a VPN to a Map, page 17-7](#).

Adding a VPN to a Map

You can add VPNs to a map view if the VPNs were previously discovered by Cisco ANA and are not currently displayed in the map.

**Note**

Adding VPNs will affect other users if they are working with the same map.

To add an existing VPN to a map:

Step 1 In Cisco ANA NetworkVision, 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,” Cisco ANA 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 **Add**.

The VPN is loaded in the map view that is displayed in the Cisco ANA NetworkVision content pane.

Step 6 Click **Close**.

The VPN is displayed in the navigation pane and the selected map or subnetwork in the Cisco ANA NetworkVision 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 Cisco ANA 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 will affect 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, sites, LCAs, or LCPs from the map without removing the VPN.

To remove a VPN, in the Cisco ANA NetworkVision 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 the overlay is run, the changes do not appear in the current overlay.

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 Cisco ANA NetworkVision 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:

- [Adding a VPN Overlay to a Map, page 17-9](#)
- [Managing a VPN Overlay Display in the Map View, page 17-10](#)
- [Displaying VPN Callouts in a VPN Overlay, page 17-10](#)

Adding a VPN Overlay to a Map

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 create a VPN overlay:

-
- Step 1** In Cisco ANA NetworkVision, display the network map for which you want to create 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 either 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,” Cisco ANA 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 that you want to add 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 added to a map, you can manage its display using the overlay tools in the main toolbar using any of the following options:

- To display the overlay, click **Show Overlay** on the main toolbar.
- To hide an active overlay, click **Hide Overlay** on the main toolbar.

**Note**

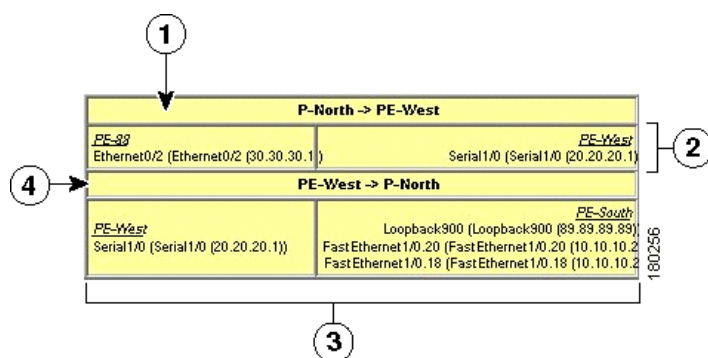
The Show Overlay toolbar button is a toggle. When clicked, the overlay is displayed. When clicked again, the overlay is hidden.

- To remove the VPN overlay, choose **Show Overlay Type > None**.

Displaying VPN Callouts in a VPN Overlay

You can display or hide the callouts for VPN links displayed in a VPN overlay to show the details of the sites that are interlinked through the selected links. The callouts (see [Figure 17-3](#)) enable you to view the VPN traffic links for a specific link (either bidirectional or unidirectional).

Figure 17-3 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 Cisco ANA NetworkVision 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**.
-

Working with CE Devices



Note

The information in this section applies only to pseudowires that existed before upgrading to Cisco ANA 3.7.1. For information on managing pseudowires that were added after upgrading to Cisco ANA 3.7.1, see [Working with Pseudowires and Pseudowire Overlays, page 12-77](#).

The following topics describe:

- [Connecting a CE Device, page 17-11](#)
- [Disconnecting a CE Device, page 17-12](#)
- [Showing or Hiding a CE Device, page 17-12](#)

Connecting a CE Device



Note

The information in this section applies only to pseudowires that existed before upgrading to Cisco ANA 3.7.1. For information on managing pseudowires that were added after upgrading to Cisco ANA 3.7.1, see [Working with Pseudowires and Pseudowire Overlays, page 12-77](#).

The connect CE functionality enables you to create a symbolic link to the overall link between the CE device and the site (IP interface) or Logical Circuit Peers (LCPs). The CE device belongs to the currently displayed map only.

To connect a CE device:

-
- Step 1** Do either of the following:
- To add a CE device to a site, choose the VPN in the Cisco ANA NetworkVision navigation pane or map view.
 - To add a CE device to an LCP, choose the Logical Circuit Aggregation (LCA).
- Step 2** Choose **File > Add to Map**.
- Step 3** From the Add dialog box, choose the device that you want to add.
- Step 4** Click **OK**.

The device is displayed in the navigation pane and the selected map or subnetwork in the Cisco ANA NetworkVision content pane.



Note Device alarm tickets do not appear in the ticket area of the Cisco ANA NetworkVision content pane until the device is added to the VPN map view.

- Step 5** Right-click the site or LCP in the navigation pane or map view and choose **Topology > Connect CE Devices**.
- Step 6** Right-click the device in the navigation pane or map view and choose **Topology > Connect to Site/LCP**, where *Site* or *LCP* displays the details of the site or LCP to be connected.

The site or LCP is connected to the CE device, and the CE device is displayed in the navigation pane and map view. A dashed, dark-gray line indicates the association.



Note The **Topology > Connect to Site/LCP** menu option is not available until after you choose the **Topology > Connect CE Device** menu option.

Disconnecting a CE Device



Note The information in this section applies only to pseudowires that existed before upgrading to Cisco ANA 3.7.1. For information on managing pseudowires that were added after upgrading to Cisco ANA 3.7.1, see [Working with Pseudowires and Pseudowire Overlays, page 12-77](#).

You can disconnect a CE device from its sites or LCPs. To disconnect a CE device, right-click the required CE device or link in the map view and choose **Topology > Disconnect CE Device**.

The association with the CE device is no longer displayed in the map view.

Showing or Hiding a CE Device



Note The information in this section applies only to pseudowires that existed before upgrading to Cisco ANA 3.7.1. For information on managing pseudowires that were added after upgrading to Cisco ANA 3.7.1, see [Working with Pseudowires and Pseudowire Overlays, page 12-77](#).

You can show the CE device for a site or LCP in the Cisco ANA NetworkVision navigation pane and map view. You can also display the device associations on the map view after the CE is connected. In addition, you can manually add connected devices (some or all of them) to view them along with the links to sites or LCPs.

To show a connected device, right-click one of the following and choose **Show CE Devices**:

- A site in the map view displaying the site business element with an actively associated CE device icon (see [Table 17-2 on page 17-4](#)).
- An LCP in the map view displaying the LCP business element with an actively assigned tunnel edge for the CE device icon.

The connected devices are shown in the navigation pane and map view including the associations.

To hide a connected device, right-click the site or LCP in the Cisco ANA NetworkVision pane or map view connected to the CE device and choose **Hide Connected Devices**.

The site or LCP with hidden connected devices icon appears. [Table 17-4](#) shows the displayed icons.

Table 17-4 *Hidden Device Icons*

Icon	Description
	Site with one or more hidden connected devices.
	LCP with one or more one hidden connected devices.

You can also manually remove some or all of the connected devices in order to hide them along with the links to sites or LCPs.

**Note**

Tickets associated with a device are displayed in the ticket pane only when a device or logical part of the device is added to the map view.

Working with Tunnels

The following topics describe:

- [Adding a Tunnel to a VPN, page 17-13](#)
- [Removing a Tunnel, page 17-14](#)

Adding a Tunnel to a VPN

**Note**

The information in this section applies only to pseudowires that existed before upgrading to Cisco ANA 3.7.1. For information on managing pseudowires that were added after upgrading to Cisco ANA 3.7.1, see [Working with Pseudowires and Pseudowire Overlays, page 12-77](#).

You can add tunnels or partially configured tunnels to a VPN. LCPs with a missing peer are marked with the stranded icon. (For more information about icons, see [Table 17-2](#).) Each tunnel can be associated with only one VPN.

**Note**

The topology state between LCPs is a logical link. It does not reflect the actual state of the network.

You can do either of the following:

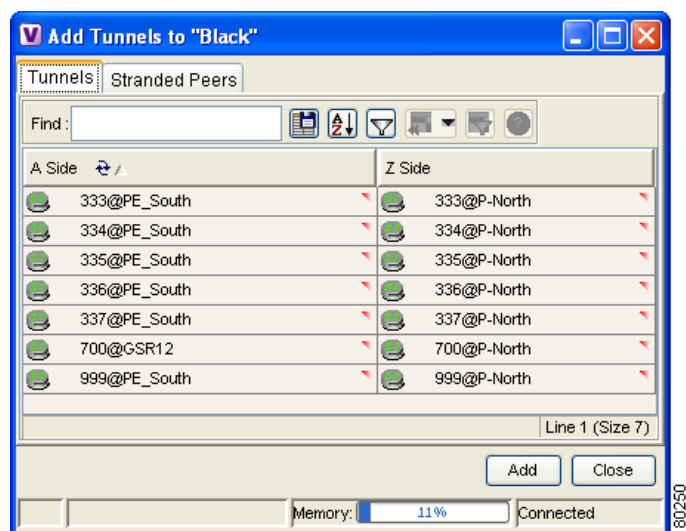
- Add a tunnel (LCP) to an LCA that has been manually created (see [Creating an LCA, page 17-15](#)).
- Add a tunnel (LCP) directly to a VPN, in which case the LCA is automatically created beneath the VPN.

To add a tunnel to a VPN:

- Step 1** In the Cisco ANA NetworkVision navigation pane or a map, right-click an LCA or VPN and choose **Topology > Add Tunnel**.

The Add Tunnels dialog box (Figure 17-4) displays tunnels not currently attached to a VPN. The Tunnels tab displays the list of pseudowire tunnels (including both tunnel edges). The Stranded Peers tab displays the list of partially configured tunnel edges, so you can add an LCP without its peer, for example, if a tunnel is partially managed, an agent fails to load, or a device is incorrectly configured.

Figure 17-4 Add Tunnels Dialog Box



- Step 2** Select the tunnel or stranded peer and click **Add**.

One of the following occurs:

- If the tunnel or stranded peer is added under an LCA, the link between the peers appears in the map.
- If the tunnel or stranded peer is added under a VPN, Cisco ANA detects the starting point of the PWE3 tunnel edges and groups all of the LCPs that start at the same device into an LCA under the VPN.



Note If a tunnel exists between VPNs (for example, an extranet tunnel), add a tunnel to one VPN and then move one LCP to the VPN with which you want to create the extranet tunnel.

Removing a Tunnel



Note

The information in this section applies only to pseudowires that existed before upgrading to Cisco ANA 3.7.1. For information on managing pseudowires that were added after upgrading to Cisco ANA 3.7.1, see [Working with Pseudowires and Pseudowire Overlays](#), page 12-77.

To remove a tunnel that was added to an LCA or VPN, in the Cisco ANA NetworkVision navigation pane or a map, right-click the LCA or VPN and choose **Topology > Remove Tunnel**.

Both tunnel sides are removed from the map. You view them in the Add Tunnels dialog box. If the deleted tunnel formed part of an LCA that was created manually, the LCA is still displayed in the navigation or map. If the deleted tunnel formed part of an LCA that was created automatically, the LCA is removed from the navigation and the map, provided no other LCPs exist in the LCA.

**Note**

You cannot view MPLS TE tunnels in VPN service view maps; however, you can view the device and topology information. For more information, see [Viewing MPLS TE Tunnel Information, page 17-36](#).

Working with LCAs and LCPs

The following topics describe:

- [Creating an LCA, page 17-15](#)
- [Moving an LCA, page 17-15](#)
- [Deleting an LCA, page 17-16](#)
- [Moving an LCP, page 17-16](#)

Creating an LCA

You can manually create an LCA and populate it by moving LCPs and tunnels to it. For more information, see [Moving an LCP, page 17-16](#) and [Adding a Tunnel to a VPN, page 17-13](#).

To create an LCA:

-
- Step 1** In the Cisco ANA NetworkVision window navigation or a map, right-click the VPN and choose **Create LCA**.
- Step 2** In the Create LCA dialog box, enter a unique name for the new LCA.
- Step 3** Click **OK**.

The new LCA is created. It appears in the navigation pane in the Cisco ANA NetworkVision window, beneath the selected VPN, and also appears in the map.

Moving an LCA

You can move the LCA to another VPN in the service view map. When you move an LCA, all of the LCPs it contains also move.

To move an LCA:

-
- Step 1** In the Cisco ANA NetworkVision navigation or a map, right-click the LCA and choose **Edit > Move selected**.
- Step 2** Right-click the VPN to which you want to move the LCA and choose **Edit > Move here**.

The LCA moves to the selected VPN and is displayed in the navigation pane and map for the selected VPN.



Note All the LCPs move with the LCA.

Deleting an LCA

You can delete an LCA if it was manually created and either has no LCPs or all the LCPs have reconciliation icons. (To move an LCA to another VPN, see [Jumping to an Adjacent LCP, page 17-16.](#))

To delete the LCA:

Step 1 In the Cisco ANA NetworkVision navigation or a map, right-click the required LCA and choose **Delete**.

Step 2 Click **Yes** on the confirmation.

The selected LCA is deleted from the database and service view maps of all users.

Moving an LCP

You can move an LCP to another VPN or LCA in the service view map.

To move an LCP:

Step 1 In the Cisco ANA NetworkVision navigation pane or a map, right-click the LCA and choose **Edit > Move selected**.

Step 2 Right-click the VPN or LCA to which you want to move the LCP and choose **Edit > Move here**.

The LCP moves to the VPN or LCA and is displayed in the navigation and map of the selected VPN or LCA.



Note If an LCP is moved to a VPN, an LCA is automatically created for it.

Jumping to an Adjacent LCP

If a service view map displays multiple tunnels, you can quickly access the selected LCP peer appearing in the same map.

To jump to the adjacent LCP, in the Cisco ANA NetworkVision navigation pane or map, right-click the required LCP and choose **Jump to Adjacent**.

The adjacent LCP is highlighted in the navigation pane and map.

Monitoring MPLS Services

This section provides details for viewing MPLS services and technologies. Topics include:

- [Viewing VPN Properties, page 17-17](#)
- [Viewing Site Properties, page 17-17](#)
- [Viewing VRF Properties, page 17-18](#)
- [Displaying VRF Egress and Ingress Adjacents, page 17-21](#)
- [Viewing Routing Entities, page 17-22](#)
- [Viewing a Label Switched Entity, page 17-27](#)
- [Viewing MP-BGP Information, page 17-30](#)
- [Viewing BFD Properties, page 17-31](#)
- [Viewing a Port Configuration, page 17-33](#)
- [Viewing Cross-VRF Routing Entries, page 17-34](#)
- [Viewing Pseudowire End-to End Emulation Tunnels, page 17-35](#)
- [Viewing MPLS TE Tunnel Information, page 17-36](#)

Viewing VPN Properties

To view the properties of a VPN:

-
Step 1	In the Cisco ANA NetworkVision navigation pane or map view, right-click the VPN and choose Properties .
Step 2	In the VPN Properties window, view the following VPN properties: • Name—The name of the VPN. • ID—The unique key automatically assigned to the VPN.
Step 3	Click Close to close the VPN Properties dialog box.
-

Viewing Site Properties

Cisco ANA enables you to view site properties, including the interfaces that are configured on the PE device. The displayed properties reflect the configuration that Cisco ANA automatically discovered for the device.

To view site properties:

-
Step 1	In the Cisco ANA NetworkVision navigation pane or map view, right-click a site and choose Properties .
Step 2	In the Router IP Interface Properties window, view the following site properties: • 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.

- Mask—The mask of the specific network.
- Sending Alarms—Whether the alarm for the required port has been enabled (true) or disabled (false).
- IP Address—The IP address of the interface.
- State—The state of the interface, either Up or Down.
- Addresses—A table that displays PE-side IP interface details. Address properties include:
 - Subnet—A combination of the IP address and the subnet mask.



Note If the site is an IPv6 VPN over MPLS with IPv6 addresses provisioned, the IPv6 addresses are displayed. For more information, see [Viewing IPv6 Information, page 16-2](#).

- Type—The address type; for example, Primary, Secondary, or IPv6 Unicast.
- Sending Alarms—Indicates whether the interface is sending alarms.

Step 3 When finished, click **Close** in the Router IP Interface Properties window.

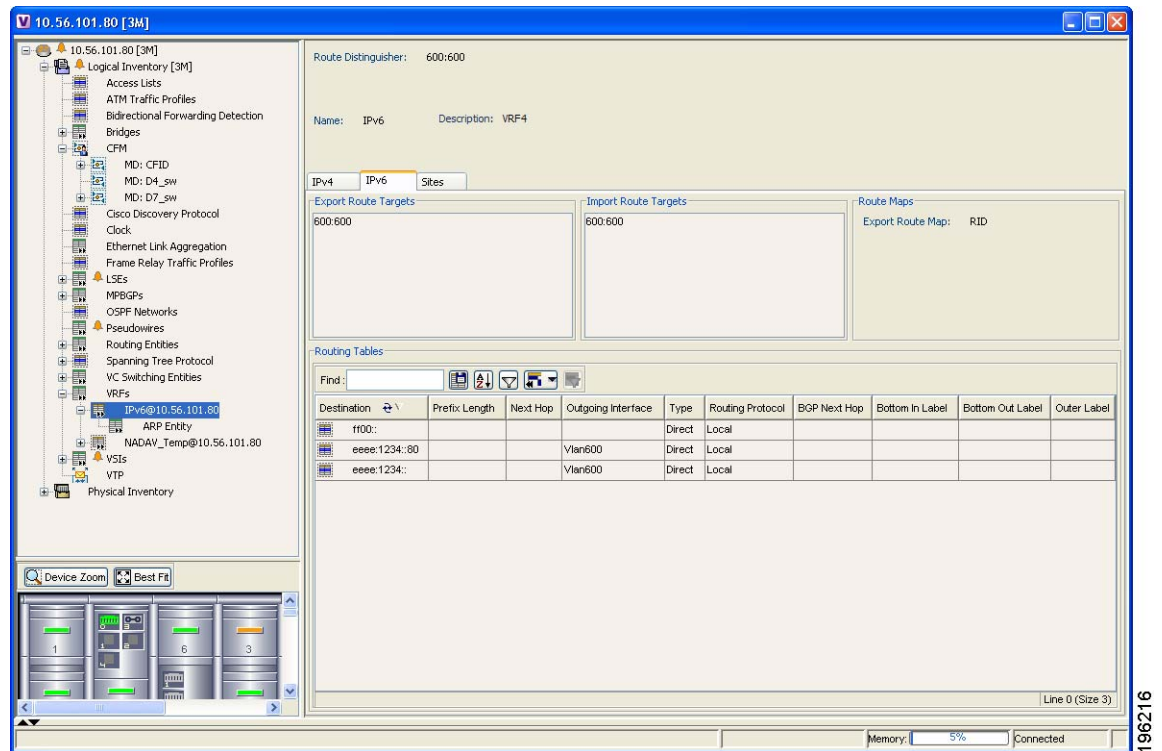
Viewing VRF Properties

Cisco ANA NetworkVision 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:

Step 1 Right-click a VRF in the Cisco ANA NetworkVision navigation pane or map view and choose **Properties**.

The VRF Properties window is displayed ([Figure 17-5](#)).

Figure 17-5 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. In addition, the forwarding table also contains MPLS encapsulation information.

Table 17-5 describes the VRF properties that are displayed.



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 here.

Table 17-5 VRF Properties

Field	Description
Route Distinguisher	The route distinguisher configured in the VRF.
Name	The name of the VRF.
Description	A description of the VRF, if available.
IPv4 Tab	
Export Route Targets	The IPv4 export route targets contained by the VRF.
Import Route Targets	The IPv4 import route targets contained by the VRF.
Route Maps	The route maps for the VRF.
IPv6 Tab	
Export Route Targets	The IPv6 export route targets contained by the VRF.
Import Route Targets	The IPv6 import route targets contained by the VRF.

Table 17-5 VRF Properties (continued)

Field	Description
Route Maps	The route maps for the VRF.
IPv4 and IPv6 Route Tables	
Destination	The destination of the specific network.
Prefix Length	The length of the network prefix in bits.
Next Hop	The next routing hop.
Outgoing Interface	The name of the outgoing interface; displayed if the Routing Protocol type is local.
Type	The type: Direct (local), Indirect, or Static.
Routing Protocol	The routing protocol used to communicate with the other sites and VRFs: BGP or local.
BGP Next Hop	The 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	The innermost label that is expected when MPLS traffic is received.
Bottom Out Label	The innermost label sent with MPLS traffic.
Outer Label	The outermost or top label in the stack used for MPLS traffic.
Sites Tab	
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.
IP Address	The IP address of the interface.
Mask	The subnet mask.
State	The state of the subinterface: Up or Down.
Associated Entity	Hyperlinked entry to the associated entry in inventory: - For SVI service interfaces, hyperlink to the Carrier Grade NAT entry in logical inventory. - For physical interfaces, hyperlink to the interface in physical inventory. - For link aggregations, hyperlink to the LAG list of interfaces.
Description	A description of the interface.
Input Access List	The access list applied to the inbound traffic of the interface.
Output Access List	The access list applied to the outbound traffic of the interface.
Rate Limits	Measures traffic for the IP interfaces on Cisco devices, including the average rate, normal burst size, excess burst size, conform-action, and exceed action.
	 Note Input access list, output access list, and rate limits parameters apply only to Cisco IOS devices.
IP Sec Map Name	The IP Security (IPsec) map name.

Table 17-5 VRF Properties (continued)

Field	Description
Site Name	The name of the business element to which the interface is attached.
Sending Alarms	Whether or not the interface is configured for sending alarms: True or False.

Step 2 When finished, press **Ctrl + F4** to close the VRF Properties window.

**Note**

You can also open a VRF table by right-clicking the virtual router in the Cisco ANA NetworkVision navigation pane or map view and selecting **Open VRF Table**. For more information about the columns displayed in the VRF Table window, see [Viewing VRF Properties, page 17-18](#).

Displaying VRF Egress and Ingress Adjacents

Cisco ANA 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:

Step 1 Right-click a VRF in the Cisco ANA NetworkVision navigation pane or map view and choose **Show VRF Egress Adjacents** or **Show VRF Ingress Adjacents**.

The Adjacents window is displayed.

Step 2 View the ingress and egress adjacent properties:

- Name—The name of the VRF as it appears in the device.
- Route Distinguisher—The route distinguisher configured in the VRF.
- Vrf V6 Table—The IPv6 route distinguisher, if IPv6 is provisioned.
- Sending Alarms—Indicates whether or not the VRF is sending alarms.

**Note**

Selecting a specific VRF in the Cisco ANA NetworkVision navigation pane displays the VRF properties. For more information, see [Viewing VRF Properties, page 17-18](#).

Step 3 When finished, press **Ctrl + F4** to close the Adjacents window.

Viewing Routing Entities

To view routing entities, choose **Logical Inventory > Routing Entities > Routing Entity**. The routing information is displayed as shown in [Figure 17-6](#).

Figure 17-6 Routing Entity Table

Name	IP Address	Mask	State	Associated Entity	Description	Input Access List
GigabitEthernet20/2 (172.16.0.65)	172.16.0.65	255.255.255.252	Up	NPE1-7604-Auto#20.0.1	### To PEB-GS...	
Loopback0 (169.255.6.12)	169.255.6.12	255.255.255.255	Up		### MNG ###	
Tunnel100 (10.100.0.2)	10.100.0.2	255.255.255.252	Up		### Test GRE T...	
Tunnel1000 (169.255.6.12)	169.255.6.12	255.255.255.255	Down			
Vlan99 (172.17.0.49)	172.17.0.49	255.255.255.240	Up	NPE1-7604-Auto (99)		

[Table 17-6](#) describes the information that is displayed in the Routing Entity table.

Table 17-6 Routing Entity Table

Field	Description
Changes Number	The number of changes to the currently displayed routing entity.
Name	The name of the routing entity.
IP Interfaces Tab	
Name	The site name; for example, ATM4/0.100(10.0.0.1) is a combination of the interface name and IP address used to reach the site.
IP Address	The IP address of the interface.
Mask	The details of the dotted decimal mask.
State	The state of the subinterface: Up or Down.
Associated Entity	Interface associated with the routing entity, hyperlinked to its location in physical inventory.
Description	A description of the interface.
Input Access List	If an input access list is assigned to an IP interface, the list is shown as an IP interface property, and a hyperlink highlights the related access list in the Access List table. When an access list is assigned to the inbound traffic on an IP interface, the actions assigned to the packet are performed.

Table 17-6 Routing Entity Table (continued)

Field	Description
Output Access List	If an output access list is assigned to an IP interface, the list is shown as an IP interface property, and a hyperlink highlights the related access list in the Access List table. When an access list is assigned to the outbound traffic on an IP interface, the actions assigned to the packet are performed.
Rate Limits	If a rate limit is configured on an IP interface, the limit is shown as an IP interface property. This option is checked when a rate limit is defined on the IP interface, meaning the access list is a rate limit access list. IP interface traffic is measured and includes the average rate, normal burst size, excess burst size, conform action, and exceed action. Note Double-clicking a row displays the properties of the IP interface. When a rate limit is configured on the IP interface, the Rate Limits tab is displayed. For more information about rate limits, see Viewing Rate Limit Information, page 17-26. Note The Input Access, Output Access, and Rate Limits parameters apply only to Cisco IOS devices.
IP Sec Map Name	The IP Security (IPsec) crypto map name.
Site Name	The name of the business element to which the interface is attached.
Sending Alarms	Whether or not the interface is configured to send alarms: True or False.
IPv4 and IPv6 Routing Table Tabs	
Destination	Destination of the specific network.
Sending Alarms	This option is unavailable.
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	CE router address from which to continue to get to a specific address. This field is empty when the routing entry goes to a PE router.
Prefix Length	Length of the network prefix in bits.
Route Protocol Type	Routing protocol used to communicate with other routers.

Viewing the ARP Table

[Table 17-7](#) describes the information that is displayed in the ARP table (**Logical Inventory > Routing Entities > Routing Entity > ARP**).

Table 17-7 ARP Table

Field	Description
MAC	The interface MAC address.
Interface	The interface name.
IP Address	The interface IP address.

Table 17-7 **ARP Table (continued)**

Field	Description
Type	The interface type: • Dynamic—An entry that was learned by the device according to network traffic. • Static—An entry that was learned by a local interface or by configuring a static route. • Other—An entry that was learned by another method not explicitly defined. • Invalid—In SNMP, this type is used to remove an ARP entry from the table.
Sending Alarms	This option is unavailable.

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, choose **Logical Inventory > Routing Entities > Routing Entity > ARP Entity > NDP Table**. [Figure 17-7](#) shows an example of the NDP Table tab.

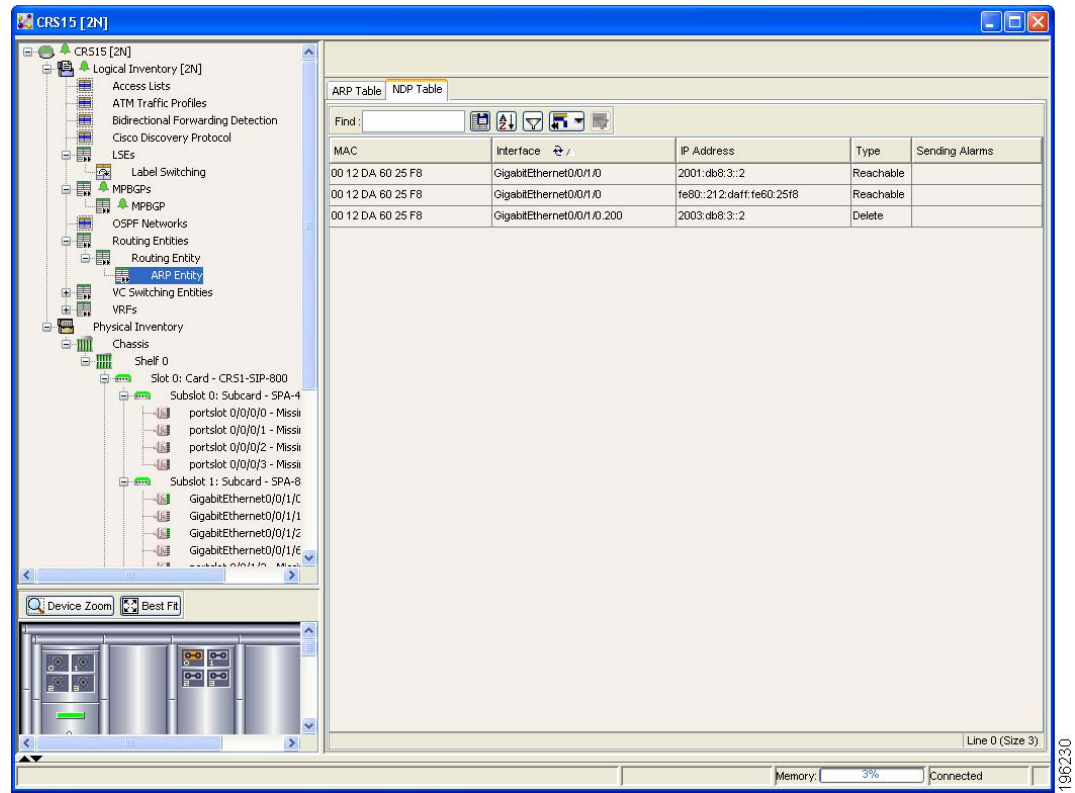
Figure 17-7 **NDP Table**

Table 17-8 describes the information displayed for NDP.

Table 17-8 **NDP Table**

Field	Description
MAC	The interface MAC address.
Interface	The interface name.
IP Address	The interface IPv6 address.

Table 17-8 **NDP Table (continued)**

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

Viewing Rate Limit Information

Choose **Routing Entities > Routing Entity > IP Interfaces** and double-click a specific row in the IP Interfaces tab to display 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.

The following information is displayed in the Rate Limits tab of the IP Interface Properties dialog box:

Field	Description
Type	The 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	The 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.

Field	Description
Exceed Action	The 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	A hyperlink that highlights the related access list in the Access List table.
Sending Alarms	This option is unavailable.

Viewing a Label Switched Entity

The LSEs logical inventory branch displays incoming and outgoing label information. The Label Switching Properties window includes the following information:

- Local LDP ID—The local Label Distribution Protocol (LDP) identifier.
- LDP Process State—The state of the LDP process, such as Running.

The Label Switching Properties window can contain the following tabs, depending on the configuration:

- [MPLS Interfaces Tab, page 17-27](#)
- [Label Switching Table Tab, page 17-27](#)
- [Traffic Engineering LSPs Tab, page 17-28](#)
- [VRF Table Tab, page 17-29](#)
- [LDP Neighbors Tab, page 17-29](#)

MPLS Interfaces Tab

The MPLS Interfaces tab provides information about the MPLS interfaces. The following information is displayed:

- ID—The interface identification.
- Distribution Protocol Type—The protocol used to establish the session, which may be LDP or TDP (Tag Distribution Protocol).
- MPLS TE Properties—Indicates whether or not MPLS traffic engineering (TE) properties are included, either checked (included) or unchecked (not included).
- Discovery Protocols—The discovery protocols used on this interface.
- Sending Alarms—Indicates whether or not the interface is sending alarms.

Label Switching Table Tab

The Label Switching Table tab describes the MPLS label switching entries used for traversing the MPLS core networks. [Table 17-9](#) describes the information that is displayed in the Label Switching Table tab.

Table 17-9 **Label Switching Table Tab**

Field	Description
Incoming Label	The details of the incoming MPLS label.
Action	The type of action; POP, swap, aggregate, or untagged. 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.

Table 17-9 *Label Switching Table Tab (continued)*

Field	Description
Outgoing Label	The details of the outgoing MPLS label.
Out Interface	The name of the outgoing interface, displayed as a hyperlink to the port subinterface in the device physical inventory.
IP Destination	The IP address of the destination network.
Destination Mask	The subnet mask of the destination network.
Next Hop	The IP address of the next MPLS interface in the path. The IP address is used for resolving the MAC address of the next MPLS interface that you want to reach.
Sending Alarms	This option is unavailable.

When a TE tunnel starts, you can view the initial TE tunnel information by choosing **Logical Inventory > LSEs > Label Switching > Traffic Engineering LSPs**. For more information, see [Viewing MPLS TE Tunnel Information, page 17-36](#).

Traffic Engineering LSPs Tab

The Traffic Engineering LSPs tab 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. [Table 17-10](#) describes the information displayed in the Traffic Engineering LSPs tab.

Table 17-10 *Traffic Engineering LSPs Tab*

Field	Description
LSP Name	The LSP name.
LSP Type	The LSP role: Head, Tail, Middle, All, or Remote.
Source Address	The source IP address.
Destination Address	The destination IP address.
In Label	The input label.
In Interface	The input interface.
Out Interface	The output interface.
Out Label	The output label.
Average Bandwidth (Kbps)	The average tunnel bandwidth in Kb/s.
LSP ID	The LSP identifier.
Burst (Kbps)	The tunnel burst rate, in Kb/s.
Peak (Kbps)	The tunnel peak rate, in Kb/s.
FRR TE Tunnel	The Fast Reroute (FRR) TE tunnel name, hyperlinked to the routing entity in logical inventory.
FRR TE Tunnel State	The state of the FRR TE tunnel: Not Configured, Ready, or Active.
Sending Alarms	Indicates whether or not the entity is sending alarms.

VRF Table Tab

The VRF Table tab describes the MPLS paths that terminate locally at a VRF. [Table 17-11](#) describes the information that is displayed in the VRF Table tab.

Table 17-11 VRF Table Tab

Field	Description
Incoming Label	The details of the incoming VRF label.
Action	The action that will be invoked: push, pop, swap, or untagged.
VRF	The VRF name as a hyperlink; displays the VRF properties.
IP Destination	The destination IP address.
Destination Mask	The destination IP subnet mask.
Next Hop	The next hop.
Out Interface	The out interface.
Sending Alarms	This option is unavailable.

LDP Neighbors Tab

The LDP Neighbors tab provides details of 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 for 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.

**Note**

If two LSRs are connected with two separate interfaces, two LDP discoveries are performed.

The following properties are displayed on the LDP Neighbors tab for each LDP peer:

Field	Description
LDP ID	The LDP identifier of the neighbor (peer) for the session.
Transport IP Address	The IP address advertised by the peer in the hello message or the hello source address.

Field	Description
Session State	The current state of the session, which can be one of the following: • Transient • Initialized • Open Rec • Open Sent • Operational
Protocol Type	The protocol used to establish the session, which may be LDP or TDP (Tag Distribution Protocol).
Label Distribution Method	The method of label distribution. This might be Downstream or Downstream On Demand.
Session Keepalive Interval	The negotiated number of seconds between keepalive messages.
Session Hold Time	The amount of time (in seconds) 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	An indication of whether the peer has one or more discovery sources.  Note To see the discovery sources in the LDP Neighbor Properties window, double-click the row of the peer in the table.
Sending Alarms	This option is unavailable.

Double-clicking an entry (peer) in the table opens the LDP Neighbor Properties window that displays the basic and targeted discovery sources for the peer. Each peer can have several discovery sources. The following information is displayed:

- Interface Name—The interface on which LDP is configured.
- Source IP Address—The IP address of the peer that sends the targeted hello messages for extended discovery.
- Adjacency Type—The type of LDP adjacency used for discovery, which may be Link (basic) or Targeted (extended).
- Sending Alarms—This option is unavailable.

Viewing MP-BGP Information

The MP-BGP branch displays information about a router's BGP neighbors. Clicking the high-level MP-BGP category displays the MP-BGP peer running on the local router. Right-clicking MP-BGPs and choosing Properties displays the same property in the MPBGPs - FW Component Container Properties window.

Clicking a MP-BGP entity displays a list of the routers used in the MP-BGP network and includes the configuration and status of the links between the router displayed in the inventory and all other BGP members. Right-clicking the MP-BGP entity and choosing Properties displays the same properties in the MPBGP Properties window. The Autonomous System (AS) to which the router belongs is displayed. The BGP Neighbors table contains the following information:

Field	Description
Peer Remote Address	The BGP peer remote IP address used by the BGP peer to exchange routing information with the local BGP peer.
Peer ID	The IP address by which the BGP recognizes and converses with its neighbor.
VRF Name	The remote peer VRF name.
Peer Keep Alive	The time interval, in seconds, between successive keepalive messages. The keepalive time is negotiated with the neighbor after the link is established.
Peer State	The state of the link between the local and remote BGP peers. Valid values are Idle, Connect, Active, Open Set, Open Confirm, and Established.
BGP Neighbor Type	The BGP neighbor type, either client or nonclient. Route reflector advertising is based on the BGP neighbor type. To client peers, a route reflector advertises all routes learned from both client and nonclient peers. To nonclient peers, the route reflector advertises only the routes received from client peers.
Peer Hold Time	The BGP Hold Time value (in seconds) that is used when negotiating with peers. If the router does not receive successive keepalive, update, or notification messages within the period specified in the Hold Time field of the open message, the BGP link to the peer is closed.
Peer Remote AS	The the remote peer AS.
AFI	Address family identifier: IPv4, IPv6, VPNv4, or VPNv6.
AF Peer State	The address family peer state: Established (up), or Idle (down).
Distribute Through Interface	The local interface through which BGP information is distributed to BGP neighbors.
Sending Alarms	This option is unavailable.

Viewing BFD Properties

Bidirectional Forwarding Detection (BFD) is used to expedite detection of communication failures of other protocols, such as BGP and OSPF.

To view BFD properties that are configured on a device:

-
- Step 1** In Cisco ANA NetworkVision, double-click the required device.
- Step 2** In the inventory window, choose **Logical Inventory > Bidirectional Forwarding Detection**.
The properties for BFD are displayed as shown in [Figure 17-8](#).

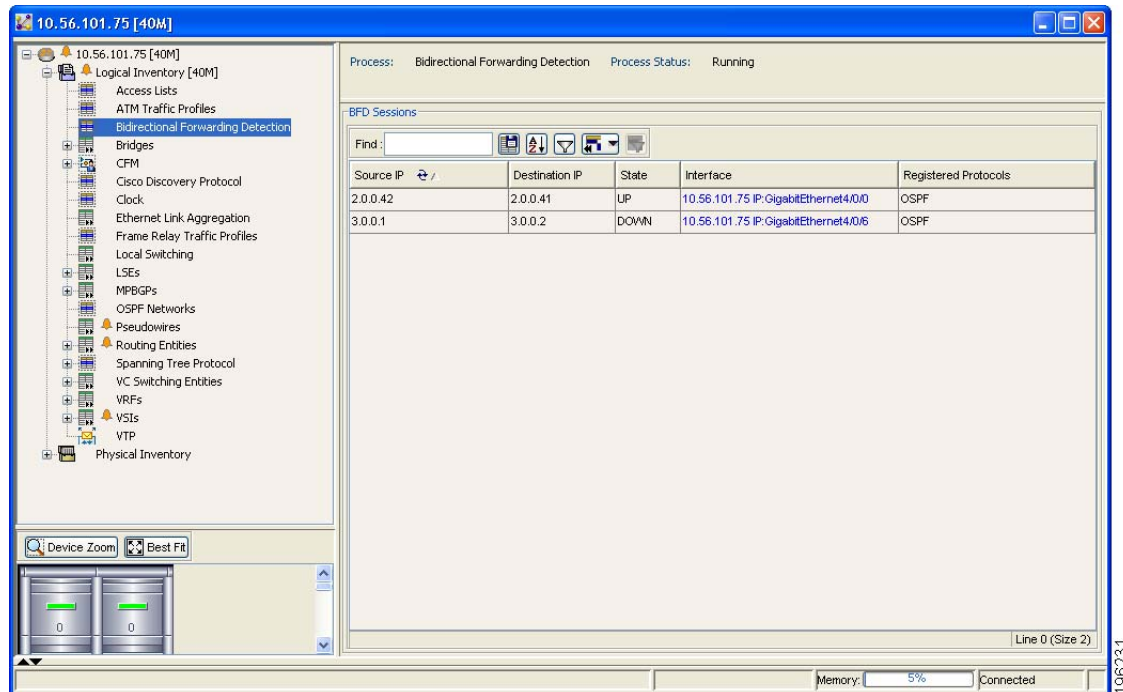
Figure 17-8 BFD Properties

Table 17-12 describes the information displayed for BFD.

Table 17-12 BFD Properties

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

Viewing a Port Configuration

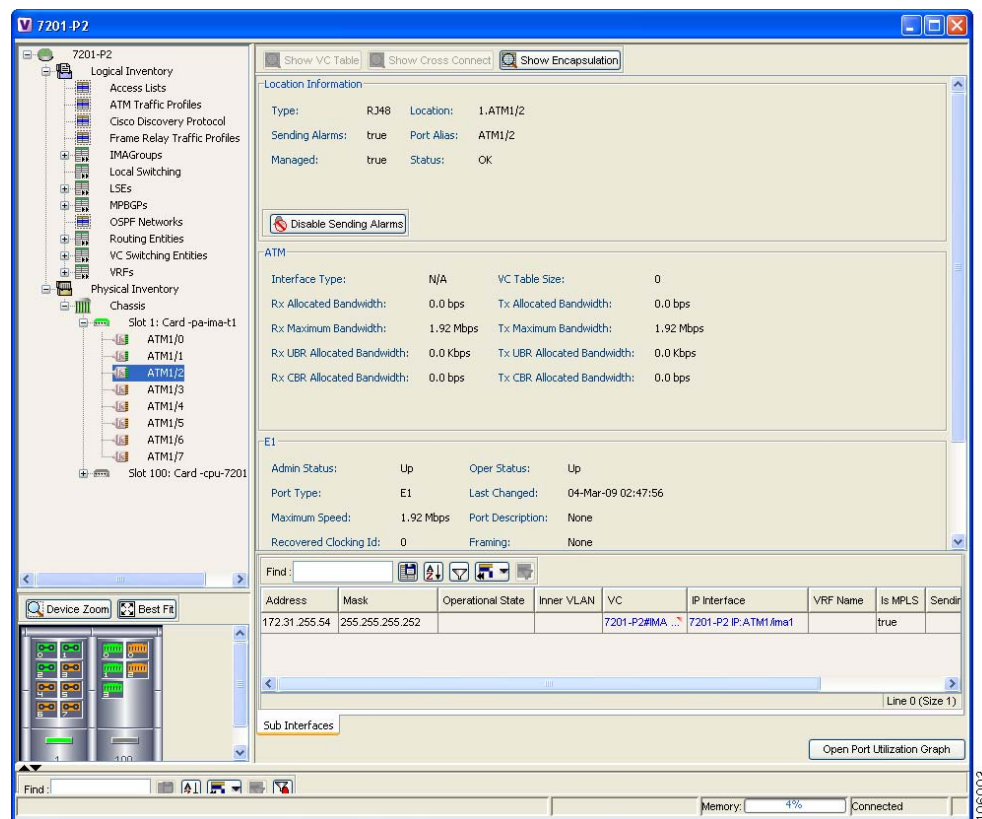
In addition to viewing logical inventory information from the logical inventory branch, you can also view services provisioned on physical ports by clicking a physical port in the physical inventory branch. Information that is displayed includes:

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

For detailed information on viewing physical inventory information, see [Chapter 3, “Viewing Network Element Properties.”](#)

[Figure 17-9](#) shows an example of port information (including the subinterfaces) displayed when a port is selected in the physical inventory branch of the inventory window.

Figure 17-9 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 17-13](#) describes the information that is displayed in the Subinterfaces table.

Table 17-13 Subinterfaces Table

Field	Description
Address	The IP address defined in the subinterface.
Mask	The subnet mask.
VLAN Type	The type of VLAN, such as Bridge or IEEE 802.1Q. Double-click the entry to view the Port IP VLAN Properties window containing: - VLAN type - VLAN identifier - Operational status - A brief description of the VLAN
Operational State	The operational state of the subinterface.
VLAN ID	The VLAN identifier.
Inner VLAN	The CE-VLAN identifier.
IP Interface	A hyperlink that displays the VRF properties in the inventory window for the IP interface.
VRF Name	The name of the VRF.
Is MPLS	Whether this is an MPLS interface: True or False.
Sending Alarms	Whether the alarm for the required port has been enabled (true) or disabled (false).
Tunnel Edge	Whether this is a tunnel edge: enabled (true) or disabled (false).
Binding	A hyperlinked entry to the specific bridge in logical inventory.

Viewing Cross-VRF Routing Entries

The Cross-VRF routing entries display routing information learned from the BGP neighbors (BGP knowledge base). The cross-VRF routing entry parameters are displayed in the Cross-VRF Properties window. To display the cross-VRF routing entries, double-click an entry (row) in the Cross-VRFs tab of the MP BGP Properties area. The following information is displayed:

Field	Description
Destination	The destination of the specific network.
Mask	The mask of the specific network.
Next Hop	The PE address from which to continue to get to a specific address.
Out Going VRF	The VRF routing entry that points to the other VRF in the same PE. The outgoing VRF is the VRF that is pointed to by the Cross-VRF entry.
Out Tag	The MPLS label inserted in the MPLS label stack by this PE router to reach the destination address that is connected to the other VRF.

Field	Description
In Tag	The MPLS label used by this router to identify traffic arriving at the destination address, it was advertised by this PE router and is inserted in the MPLS label stack by the PE from which the traffic originated.
Sending Alarms	This option is unavailable.

Viewing Pseudowire End-to End Emulation Tunnels

The Pseudowires branch (**Logical Inventory > Pseudowires**) displays a list of the Layer 2 tunnel edge properties (per edge), including tunnel status and VC labels. [Table 17-14](#) describes the information that is displayed in the Tunnel Edges table for pseudowires.

Table 17-14 Pseudowires Branch Tunnel Edges Table

Field	Description
Local Interface	The name of the subinterface or port. Strings, such as Aggregation Group, EFP, VLAN, and VSI, are included in the interface name, and the entry is hyperlinked to the relevant entry in logical or physical inventory: • Aggregation groups are linked to Ethernet Link Aggregation in logical inventory. • ATM interfaces are linked to the port in physical inventory and the ATM interface. • ATM VCs are linked to the port in physical inventory and the Port IP Properties table. • CEM groups are linked to the port in physical inventory and the CEM Group table. • EFPs are linked to the port in physical inventory and the EFPs table. • IMA groups are linked to IMA Groups in logical inventory. • Local switching entities are linked to Local Switching Entity in logical inventory. • VLANs are linked to Bridges in logical inventory. • VSIs are linked to the VSI entry in logical inventory.
ID	The tunnel identifier, hyperlinked to the PTP Layer 2 MPLS Tunnel Properties window.
Peer	The details of the selected LCP peer (edge peer), 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 PWE3 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 MPLS router ID.
Peer Router IP	The IP address of the peer tunnel edge, which is used as the MPLS router ID.

Table 17-14 Pseudowires Branch Tunnel Edges Table (continued)

Field	Description
Pseudowire Type	Type of pseudowire, such as Ethernet, Ethernet Tagged, CESoPSN Basic, PPP, or SAToP. For a complete list of pseudowire types, see the Cisco Active Network Abstraction 3.7.1 Theory of Operations Guide .
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 by MPLS to build the tunnel, for example, LDP or TDP.
Preferred Path Tunnel	The path to be used for MPLS pseudowire traffic.

Viewing MPLS TE Tunnel Information

The Traffic Engineering Tunnels branch displays specific TE tunnel information. The name of the table is displayed at the top of the Properties window in the title bar. [Table 17-15](#) describes the information that is displayed in the Tunnel Edges table.

Table 17-15 Tunnel Edges Table

Field	Description
Name	The name of the TE tunnel (in Cisco devices it is the interface name).
Tunnel Destination	The IP address of the device in which the tunnel ends.
Administrative Status	The administrative state of the tunnel: Up or Down.
Operational Status	The operational state of the tunnel: Up or Down.
Outgoing Label	The TE tunnel's MPLS label distinguishing the LSP selection in the next device.
Description	A description of the tunnel.
Outgoing Interface	The interface through which the tunnel exits the device.
Bandwidth (Kbps)	Bandwidth specification for this tunnel in Kb/s.
Setup Priority	The tunnel's priority upon path setup.
Hold Priority	The tunnel priority after path setup.
Affinity	The tunnel's preferential bits for specific links.
Affinity Mask	The 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.

Table 17-15 Tunnel Edges Table (continued)

Field	Description
Lockdown	Whether or not the tunnel can be rerouted: • Enabled—The tunnel cannot be rerouted. • Disabled—The tunnel can be rerouted.
Path Option	The tunnel path option: • Dynamic—The tunnel is routed along the ordinary routing decisions after taking into account the tunnel constraints such as attributes, priority, and bandwidth. • Explicit—The route is explicitly mapped with the included and excluded links.
Average Rate (Kbps)	Average bandwidth for this tunnel (in Kb/s).
Burst (Kbps)	Burst flow specification (in Kb/s) for this tunnel.
Peak Rate (Kbps)	Peak flow specification (in Kb/s) for this tunnel.
LSP ID	LSP identification number.
Policy Class	Value of Policy Based Tunnel Selection (PBTS) configured. This value ranges from 1-7.
FRR	The TE Fast Reroute (FRR) status: Enabled or Disabled.
Egress Traffic Descriptor	Name of the VC egress descriptor.
Sending Alarms	This option is unavailable.
Ingress Traffic Descriptor	Name of the VC ingress descriptor.

The Traffic Engineering LSPs Label Switching sub-branch displays the TE tunnel LSP information. Devices that have LSPs running TE tunnels (either as a head end, midpoint, or tail end), display the following information:

Field	Description
LSP Type	The type of LSP: • Head—A tunnel starting at this device. • Midpoint—A tunnel passing through this device. • Tail—A tunnel terminating at this device.
Source Address	IP address of the device where the tunnel begins, that is, the tunnel head.
In Interface and Label	Occupied only for midpoint or tail LSPs, this label is advertised to the previous device on this interface as the LSP's next label.
Out Interface and Label	Occupied only for head or midpoint LSPs, this label is appended to tunnel packets going out through this interface to the next hop along the tunnel's path.
Destination Address	The IP address of the device at the end of the tunnel.
LSP name	A name identifying the tunnel.

Field	Description
LSP ID	LSP identification number.
Average Bandwidth	Average bandwidth for this tunnel (in Kb/s).
Burst	Burst flow specification for this tunnel (in Kb/s).
Peak	Peak flow specification for this tunnel (in Kb/s).
Sending Alarms	This option is unavailable.



CHAPTER 18

Monitoring MToP Services

The following topics describe Mobile Transport over Packet (MToP) services and how you can view and manage them:

- [User Roles Required to Work with MToP, page 18-1](#)
- [Viewing SAToP Pseudowire Type in Logical Inventory, page 18-2](#)
- [Viewing CESoPSN Pseudowire Type in Logical Inventory, page 18-3](#)
- [Viewing ATM Virtual Connection Cross-Connects, page 18-4](#)
- [Viewing IMA Group Properties, page 18-7](#)
- [Viewing TDM Properties, page 18-10](#)
- [Viewing Channelization Properties, page 18-11](#)
- [Viewing MLPPP Properties, page 18-19](#)
- [Viewing MPLS Pseudowire over GRE Properties, page 18-25](#)
- [Network Clock Service Overview, page 18-28](#)
- [Viewing CEM and Virtual CEM Properties, page 18-40](#)

For more information about MToP, see the *Cisco Active Network Abstraction 3.7.1 Theory of Operations Guide*.

User Roles Required to Work with MToP

[Table 18-1](#) identifies the roles that are required to work with MToP in Cisco ANA NetworkVision. Cisco ANA 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 device-based tasks (tasks that do affect devices), authorization is based on the default permission that is assigned to your account. That is, whether the device 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 Active Network Abstraction 3.7.1 Administrator Guide*.

Table 18-1 Default Permission/Security Level Required for Viewing MToP Properties

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View MToP properties	—	—	—	—	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 Cisco ANA NetworkVision, right-click the device on which SAToP is configured, then choose **Inventory**.
 - Step 2** In the inventory window, choose **Logical Inventory > Pseudowires**.
 - Step 3** In the Tunnel Edges table, select the required entry and scroll horizontally until you see the Pseudowire Type column. See [Figure 18-1](#).



Note You can also view this information by right-clicking the entry in the table and choosing **Properties**.

- Step 4** To view the physical inventory for the port, click the hypertext port link.

Figure 18-1 SAToP Pseudowire Type in Logical Inventory

ID	Peer	Tunnel ID	Tunnel Status	Local Router IP	Peer Router IP	Pseudowire Type
50001@vne-146		50001	down	10.10.20.3	10.10.20.2	CESoPSN Basic
10@vne-146		10	down	10.10.20.3	10.2.2.2	CESoPSN Basic
146147@vne-146	500@vne-147	146147	down	10.10.20.3	10.10.20.4	SAToP E1
500@vne-146		500	down	10.10.20.3	10.10.20.4	Ethernet
40801@vne-146		40801	down	10.10.20.3	10.10.20.1	Ethernet
40802@vne-146		40802	down	10.10.20.3	10.10.20.4	Ethernet
4321@vne-146		4321	admin down	10.10.20.3	4.3.2.1	Ethernet
4322@vne-146		4322	admin down	10.10.20.3	4.3.2.2	Ethernet
60001@vne-146		60001	down	10.10.20.3	10.10.20.1	Ethernet
60002@vne-146		60002	down	10.10.20.3	10.10.20.4	Ethernet

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 Cisco ANA NetworkVision:

- Step 1** In Cisco ANA NetworkVision, right-click the device on which CESoPSN is configured, then choose **Inventory**.
- Step 2** In the inventory window, choose **Logical Inventory > Pseudowires**.
- Step 3** In the Tunnel Edges table, select the required entry and scroll horizontally until you see the Pseudowire Type column. See [Figure 18-2](#).



Note

You can also view this information by right-clicking the entry in the table and choosing **Properties**.

Step 4 To view the physical inventory for the port, click the hypertext port link.

Figure 18-2 CESoPSN Pseudowire Type in Logical Inventory

Local Interface	ID	Peer	Tunnel ID	Tunnel Status	Local Router IP	Peer Router IP	Pseudowire Type
Bundle Location CEM8/1/0:1	1234@a146	1234@a147	1234	down	10.10.20.3	10.10.20.4	CESoPSN Basic
Bundle Location CEM8/3/0:2	10@a146		10	down	10.10.20.3	10.2.2.2	CESoPSN Basic
Bundle Location CEM8/3/1:2	50001@a146		50001	down	10.10.20.3	10.10.20.2	CESoPSN Basic
Bundle Location Virtual-cem8/3/24:0	146147@a146		146147	down	10.10.20.3	10.10.20.4	SAToP E1
	500@a146	500@a147	500	down	10.10.20.3	10.10.20.4	Ethernet
a146#VSt: lax-pw VPN Id: 0	4321@a146		4321	admin down	10.10.20.3	4.3.2.1	Ethernet
a146#VSt: lax-pw VPN Id: 0	4322@a146		4322	admin down	10.10.20.3	4.3.2.2	Ethernet
a146#VSt: ms-pw VPN Id: 0	60001@a146		60001	down	10.10.20.3	10.10.20.1	Ethernet
a146#VSt: ms-pw VPN Id: 0	60002@a146	60002@a147	60002	down	10.10.20.3	10.10.20.4	Ethernet

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.

To view ATM cross-connects:

- Step 1** In Cisco ANA NetworkVision, right-click the required device, then choose **Inventory**.
- Step 2** In the inventory window, choose **Logical Inventory > VC Switching Entities > VC Switching Entity**. The Cross-Connect Table is displayed in the content pane as shown in Figure 18-3.
- Step 3** Select an entry and scroll horizontally until you see the required information.

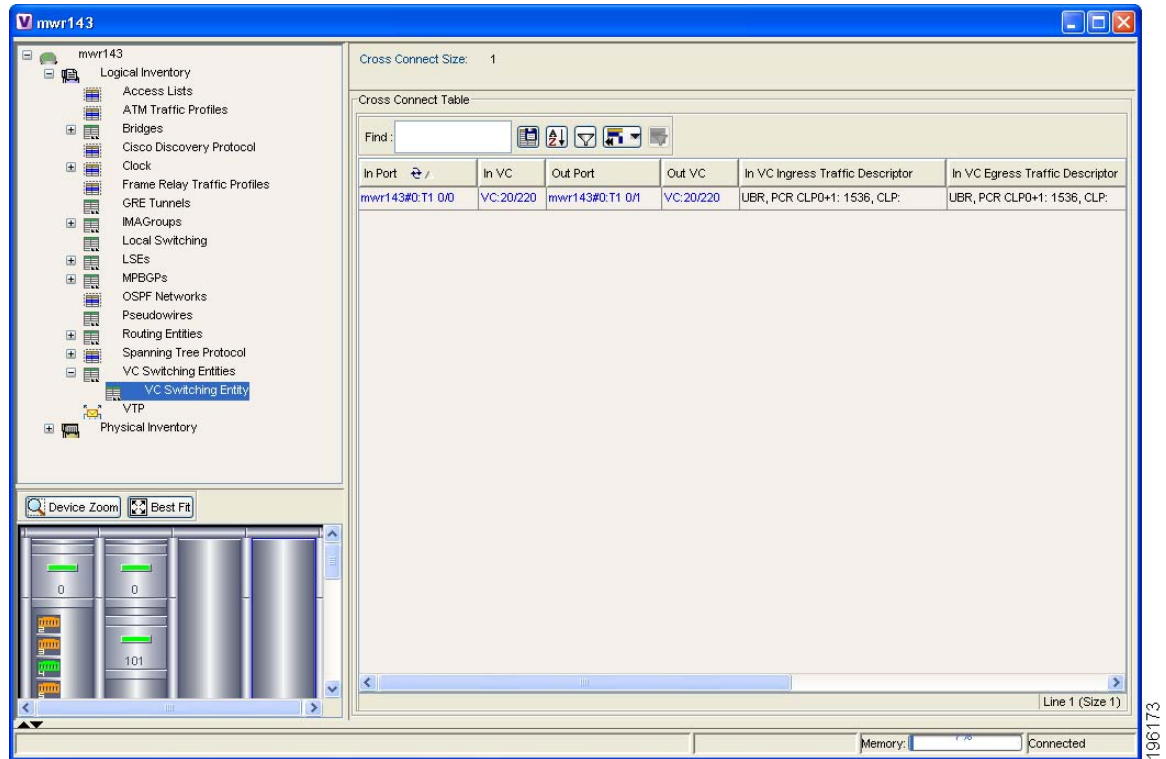
Figure 18-3 ATM Virtual Connection Cross-Connect Properties

Table 18-2 identifies the properties that are displayed for ATM VC cross-connects.

Table 18-2 ATM Virtual Connection Cross-Connect Properties

Field	Description
In Port	The incoming port for the cross-connect.
In VC	The incoming virtual connection for the cross-connect. You can view additional details about the virtual connection in the following ways: - Click the hyperlinked entry to view the VC table. - Right-click the entry, then choose Properties to view information about the incoming and outgoing VCIs, VPI, service category, and traffic descriptors.
Out Port	The outgoing port for the cross-connect.
Out VC	The outgoing virtual connection for the cross-connect. You can view additional details about the virtual connection in the following ways: - Click the hyperlinked entry to view the VC table. - Right-click the entry, then choose Properties to view information about the incoming and outgoing VCIs, VPI, service category, and traffic descriptors.
In VC Ingress Traffic Descriptor	ATM traffic parameters and service categories for the incoming traffic on the incoming VC cross-connect. For information on VC traffic descriptors, see Table 18-3.

Table 18-2 *ATM Virtual Connection Cross-Connect Properties (continued)*

Field	Description
In VC Egress Traffic Descriptor	ATM traffic parameters and service categories for the outgoing traffic on the incoming VC cross-connect. For information on VC traffic descriptors, see Table 18-3 .
Out VC Egress Traffic Descriptor	ATM traffic parameters and service categories for the outgoing traffic on the outgoing VC cross-connect. For information on VC traffic descriptors, see Table 18-3 .
Out VC Ingress Traffic Descriptor	ATM traffic parameters and service categories for the incoming traffic on the outgoing VC cross-connect. For information on VC traffic descriptors, see Table 18-3 .
Sending Alarms	Indicates whether the cross-connect is sending alarms: True or False.

Table 18-3 *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.

Table 18-3 Virtual Connection Traffic Descriptors (continued)

Value	Description
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 IMA Group Properties

To view IMA group properties:

- Step 1** In Cisco ANA NetworkVision, right-click the required device, then choose **Inventory**.
- Step 2** In the inventory window, choose **Logical Inventory > IMA Groups > group**. IMA group properties and the IMA Members table are displayed in the content pane as shown in [Figure 18-4](#).

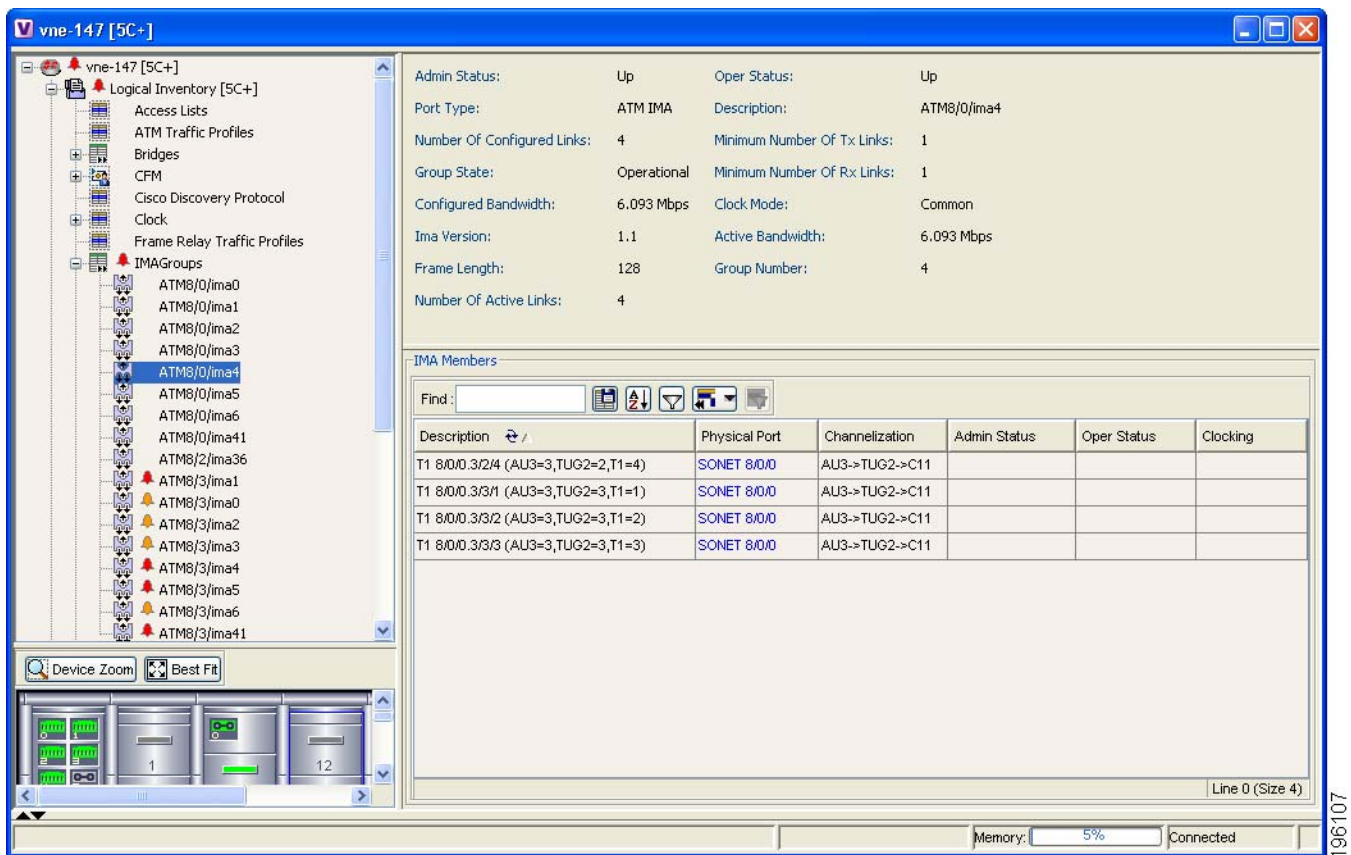
Figure 18-4 IMA Group Properties

Table 18-4 describes the information displayed for the IMA group.

Table 18-4 IMA Group Properties

Field	Description
Active Bandwidth	The active bandwidth of the IMA group.
Admin Status	The administrative status of the IMA group.
Clock Mode	The clock mode the IMA group is using: - Common—Common transmit clocking (CTC). - Independent—Independent transmit clocking (ITC).
Configured Bandwidth	The total bandwidth of the IMA group, which is the sum of all individual links in the group.
Description	The IMA group interface name.
Frame Length	The length of the IMA group transmit frames, in the number of cells: 32, 64, 128, or 256. A small frame length causes more overhead but loses less data if a problem occurs. We recommend a frame length of 128 cells.
Group Number	The IMA group number.
Group State	The IMA group status, in the order of usual appearance: - Startup—The near end is waiting to receive indication that the far end is in Startup. The IMA group moves to the Startup-Ack state when it can communicate with the far end and has recorded IMA ID, group symmetry, and other IMA group parameters. - Startup ACK—Both sides of the link are enabled. - Config Aborted—The far end has unacceptable configuration parameters, such as an unsupported IMA frame size, an incompatible group symmetry, or an unsupported IMA version. - Insufficient Links—The near end has accepted the far end group parameters, but the far end does not have sufficient links to move into the Operational state. - Operational—The group is not inhibited and has sufficient links in both directions. The IMA interface can receive ATM layer cells and pass them from the IMA sublayer to the ATM layer. - Blocked—The group is blocked, even though sufficient links are active in both directions.
IMA Version	The IMA version configured, either 1.0 or 1.1.
Minimum Number of Rx Links	The minimum number of Rx links needed for the IMA group to be operational.
Minimum Number of Tx Links	The minimum number of Tx links needed for the IMA group to be operational.
Number of Active Links	The number of DS1 (E1 or T1) links that are active in the group.

Table 18-4 IMA Group Properties (continued)

Field	Description
Number of Configured Links	The number of DS1 (E1 or T1) links that are configured in the IMA group.
Oper Status	The operational state of the IMA group interface: • Dormant—The interface is dormant. • Down—The interface is down. • Not Present—An interface component is missing. • Testing—The interface is in test mode. • Unknown—The interface has an unknown operational status. • Up—The interface is up.
Port Type	Type of port, such as ATM IMA.

Table 18-5 describes the information displayed in the IMA Members table.

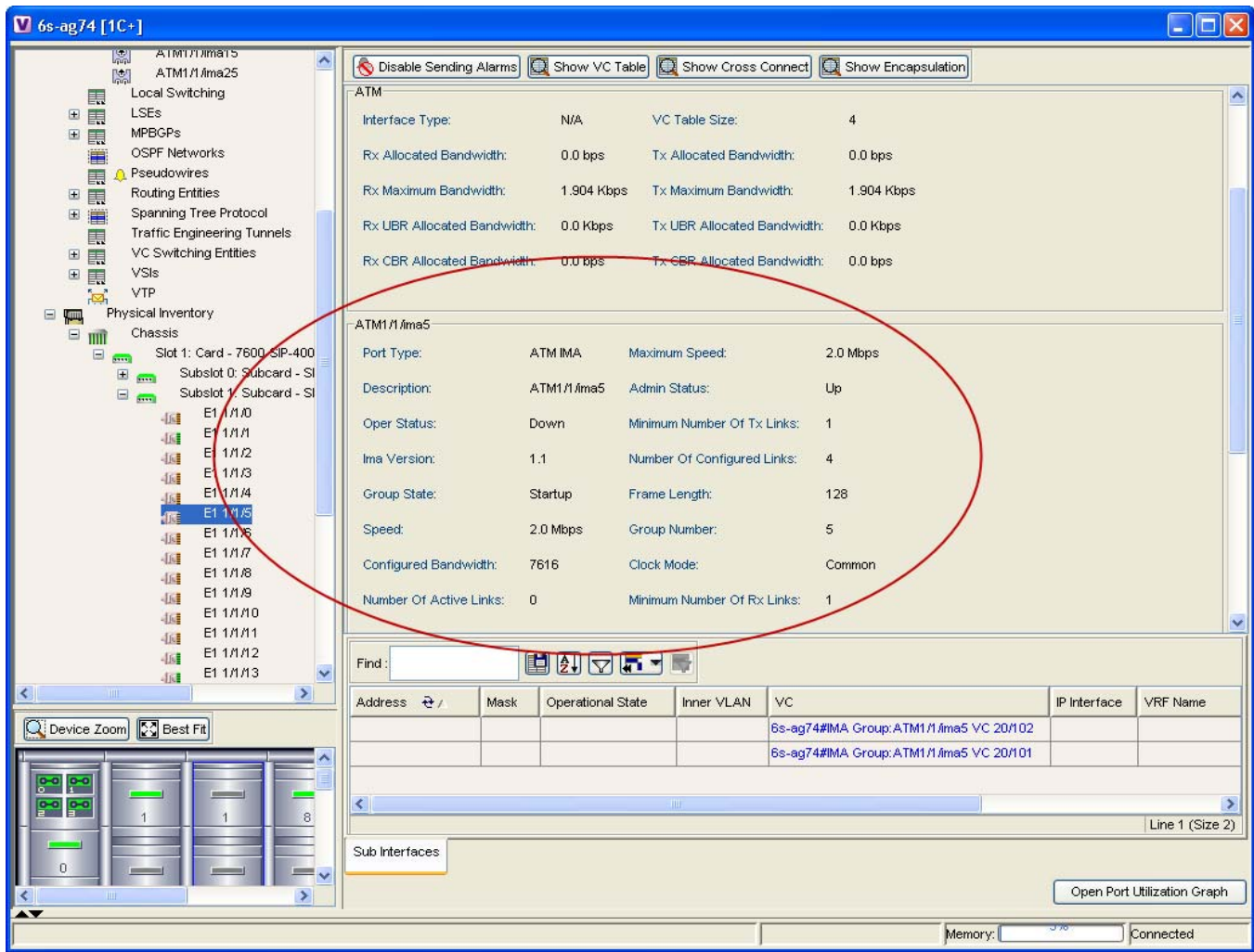
Table 18-5 IMA Members Table

Column	Description
Admin Status	The administrative status of the IMA member.
Channelization	The channelization that occurs through the path, such as STS1-> VTG-> VT15. Information is displayed in this field only if the T1 or E1 path was channelized. If the line was not channelized, this field is not displayed. For example, if the IMA group is configured on a T1 or E1 card, this field is not displayed.
Clocking	The source of the clocking mechanism: Internal or Line.
Description	The type of channelization, such as Synchronous Transport Signal 1 (STS-1) or Synchronous Transport Module level 1 (STM-1).
Oper Status	The operational state of the IMA member:
Physical Port	Hyperlinked entry to the port in physical inventory.
Port Type	The type of port, such as E1 or T1.

Step 3 In the IMA Members table, click a hyperlinked port entry to view the port properties in physical inventory. See [Figure 18-5](#).

The information that is displayed for the port in physical inventory depends on the type of connection, such as SONET or ATM.

Figure 18-5 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 broken into segments that are transmitted in a defined sequence. Each incoming data stream is allocated a timeslot of a fixed length, and the data from each stream is transmitted in turn. For example, data from data stream 1 is transmitted during timeslot 1, data from data stream 2 is transmitted during timeslot 2, and so on. After each incoming stream has transmitted data, the cycle begins again with data stream 1. The transmission order is maintained so that the input streams can be reassembled at the destination.

MToP encapsulates TDM streams for delivery over packet-switching networks (PSNs) using the following methods:

- SAToP—A method for encapsulating TDM bit-streams (T1, E1, T3, or E3) as pseudowires over PSNs.
- CESoPSN—A method for encapsulating structured (NxDS0) TDM signals as pseudowires over PSNs.

For T1 or E1 entries, the TDM properties presented in [Table 18-6](#) are displayed in physical inventory in addition to the existing T1 or E1 properties.

Table 18-6 TDM-Specific Properties for DS1 (T1 or E1) in Physical Interfaces

Field	Description
International Bit	Indicates whether or not the international bit is used by the controller: • 0—The international bit is not used. • 1—The international bit is used. This property applies only to E1.
National Bits	Indicates whether or not the national reserve bits (sa4, sa5, sa6, sa7, and sa8) are used by the controller: • 0—The national reserve bits are not used. • 1—The national reserve bits are used. This property applies only to E1.
Line Code	The line encoding method for the DS1 link: • For E1, the options are Alternate Mark Inversion (AMI) and high-density bipolar of order 3 (HDB3). • For T1, the options are AMI and bipolar with 8 zero substitution (B8ZS).
Cable Length	For T1 ports in short-haul mode, the length of the cable in feet.

Viewing Channelization Properties

Beginning with version 3.7, Cisco ANA supports the channelization of SONET/SDH and T3 lines. When a line is channelized, it is logically divided into smaller bandwidth channels called paths. These paths (referred to as high order paths or HOPs) can, in turn, contain low order paths, or LOPs. The sum of the bandwidth on all paths cannot exceed the line bandwidth.

The following topics describe how to view channelization properties for SONET/SDH and T3 lines:

- [Viewing SONET/SDH Channelization Properties, page 18-12](#)
- [Viewing T3 DS1 and DS3 Channelization Properties, page 18-15](#)

Viewing SONET/SDH Channelization Properties

SONET and SDH use the same concepts for channelization, but the terminology differs. [Table 18-7](#) describes the equivalent terms for SONET and SDH channelization. The information displayed in Cisco ANA NetworkVision reflects whether SONET or SDH is configured on the interface.

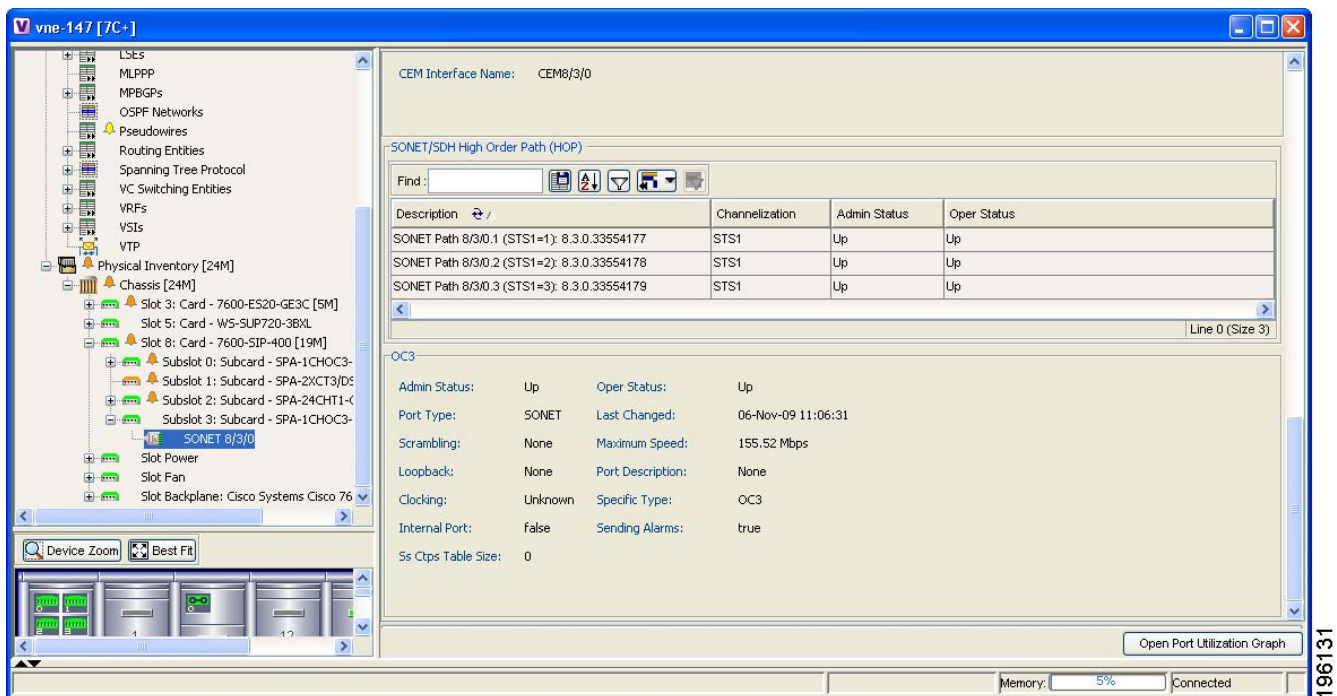
Table 18-7 *SONET and SDH Channelization Terminology*

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- <i>n</i>)
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 Cisco ANA NetworkVision, right-click the required device, then choose **Inventory**.
- Step 2** Choose **Physical Inventory > Chassis > slot > subslot > SONET/SDH-interface**. The properties for SONET/SDH and OC-3 are displayed in the content pane. See [Figure 18-6](#).

Figure 18-6 *SONET/SDH Interface in Physical Inventory*



[Table 18-8](#) describes the information that is displayed for SONET/SDH and OC3 in the content pane.

Table 18-8 SONET/SDH and OC3 Properties

Field	Description
SONET/SDH High Order Path (HOP) Area	
Description	The SONET/SDH path description including the interface and high order path. Double-click an entry to view additional details about the path.
Channelization	The type of channelization, such as STS-1 or STM-1.
Admin Status	The administrative status of the HOP.
Oper Status	The operational status of the HOP.
OC3 Area	
Admin Status	The administrative status of the OC-3 line.
Oper Status	The operational status of the OC-3 line.
Port Type	The type of port.
Last Changed	The date and time of the last status change of the line.
Scrambling	Identifies any scrambling that has been applied to the SONET payload.
Maximum Speed	The maximum bandwidth for the line.
Loopback	The loopback setting configured on the line.
Port Description	The description of the port defined by the user.
Clocking	The clocking configured on the line.
Specific Type	The specific type of line; in this case, OC3.
Internal Port	Whether or not the line includes an internal port: True or False.
Sending Alarms	Whether or not the line is sending alarms: True or False.
Ss Ctps Table Size	The size of the SONET/SDH Connection Termination Point (CTP) table.

- Step 3** To view additional information about a channelized path, double-click the required entry in the Description column. The SONET/SDH High Order Path Properties window is displayed as shown in [Figure 18-7](#).

Figure 18-7 SONET/SDH High Order Path Properties Window

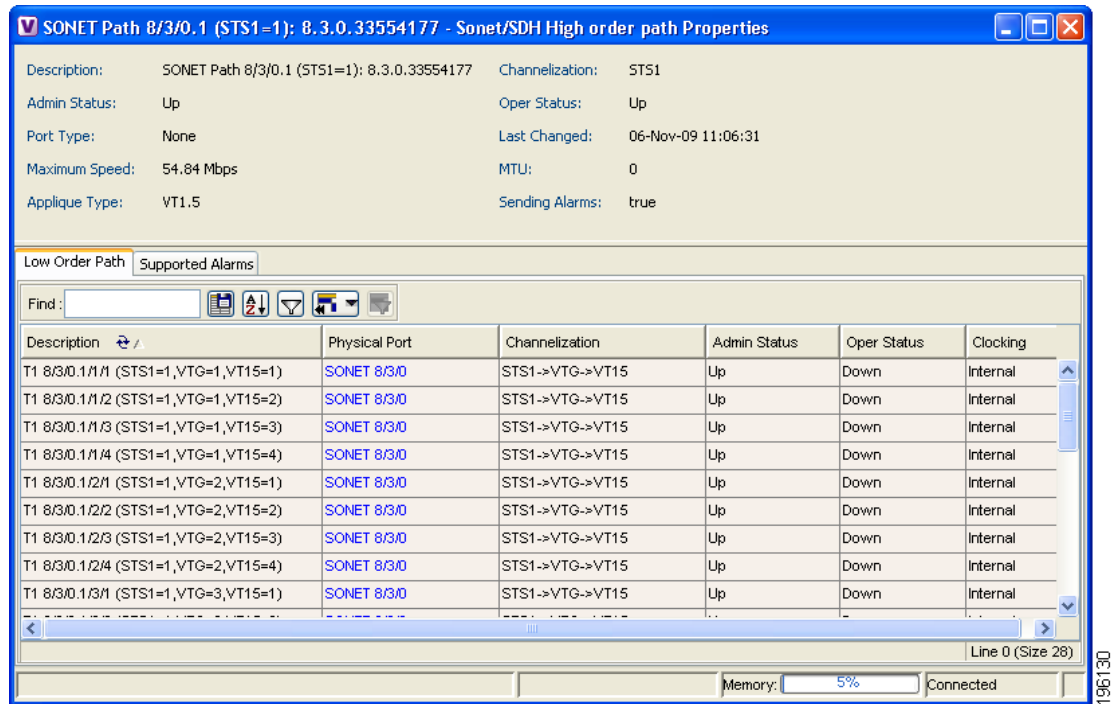


Table 18-9 describes the information displayed in SONET/SDH High Order Path Properties window.

Table 18-9 SONET/SDH High Order Path Properties

Field	Description
Description	The SONET/SDH path description including the interface and high order path. Double-click an entry to view additional details about the path.
Channelization	The type of channelization, such as Synchronous Transport Signal 1 (STS-1) or Synchronous Transport Module level 1 (STM-1).
Admin Status	The administrative status of the HOP.
Oper Status	The operational status of the HOP.
Port Type	The type of port.
Last Changed	The date and time of the last status change of the path.
Maximum Speed	The maximum bandwidth for the line.
MTU	The MTU for the path.
Applique Type	A 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.
Low Order Path Tab	
Description	A 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.

Table 18-9 SONET/SDH High Order Path Properties (continued)

Field	Description
Channelization	The channelization that occurs through the path, such as STS1-> VTG-> VT15.
Admin Status	The administrative status of the path.
Oper Status	The operational status of the path.
Clocking	The source of the clocking mechanism: Internal or Line.
Supported Alarms Tab	
Name	The 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 Cisco ANA NetworkVision, right-click the required device, then choose **Inventory**.
- Step 2** Choose **Physical Inventory > Chassis > slot > subslot > T3-interface**.

[Figure 18-8](#) shows DS1 channelization properties for T3 in physical inventory, and [Figure 18-9](#) shows DS3 channelization properties for T3 in physical inventory.

Figure 18-8 T3 DS1 Channelization Properties in Physical Inventory

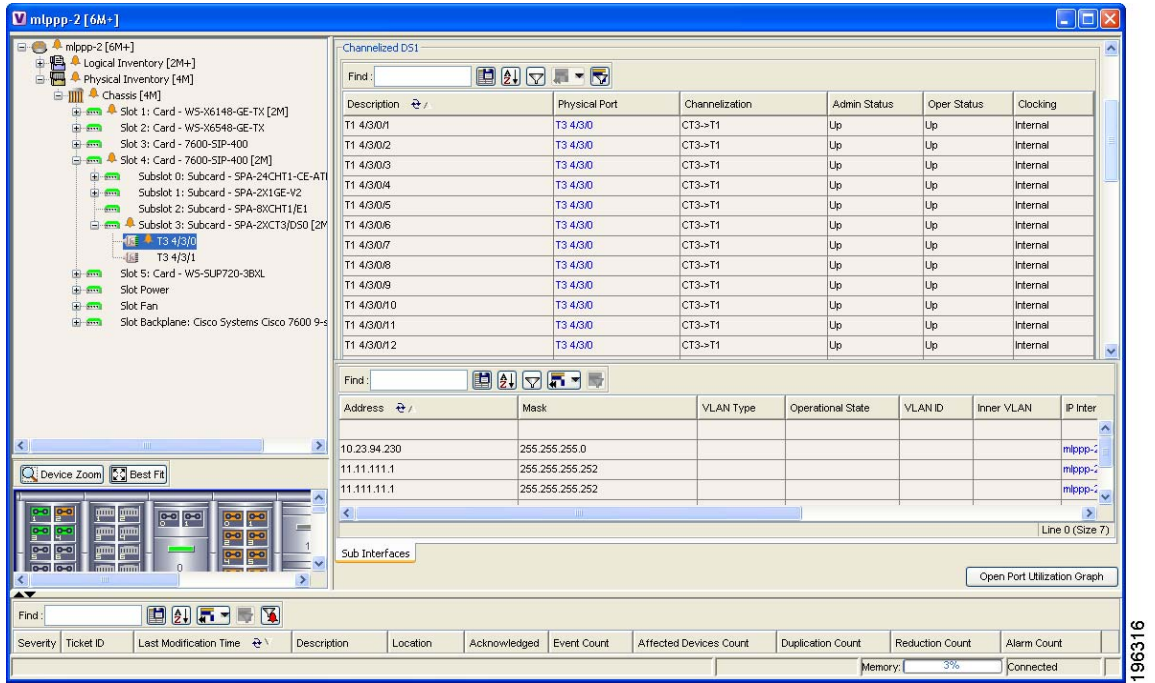


Figure 18-9 T3 DS3 Channelization Properties in Physical Inventory

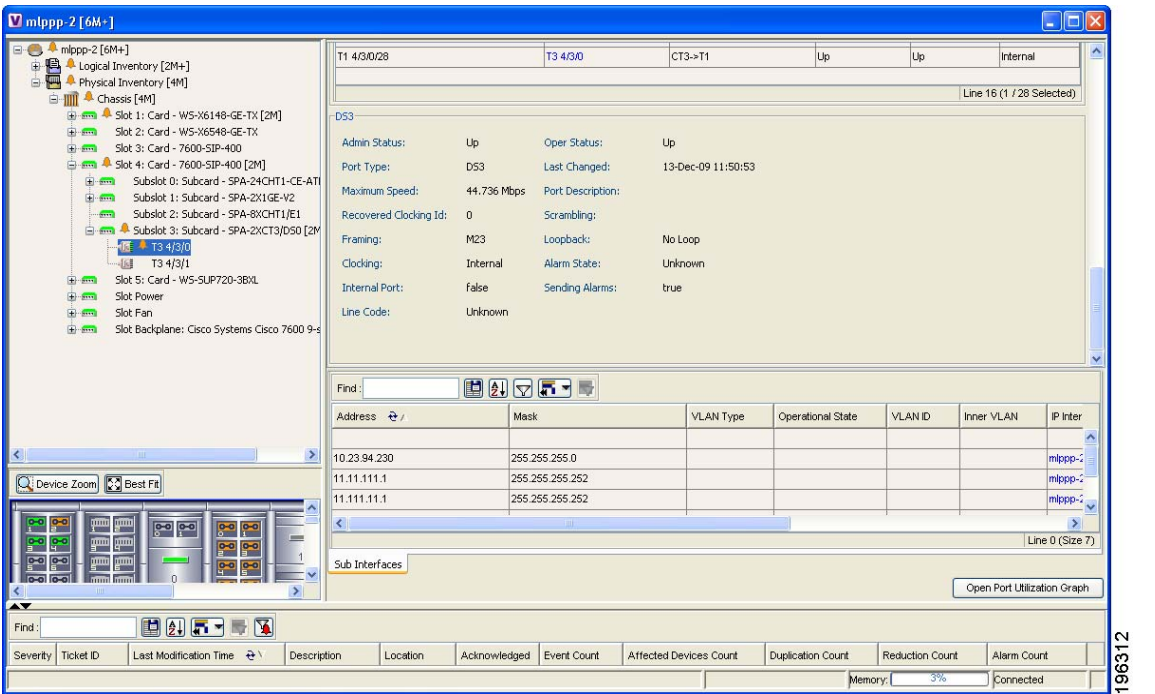


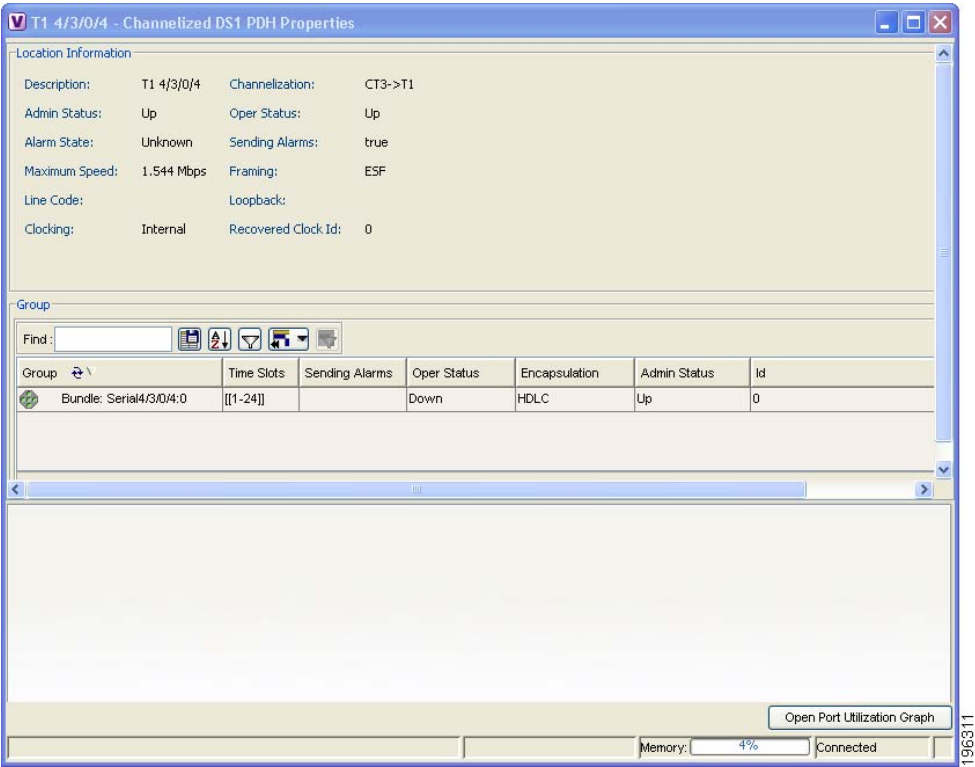
Table 18-10 describes the information that is displayed for Channelized DS1 and DS3 in the content pane.

Table 18-10 **Channelized DS1 and DS3 Properties**

Field	Description
Channelized DS1 Table	
Description	The path description including the physical interface and the channel number. Double-click an entry to view additional details about the path.
Physical Port	The physical port for the channelized line.
Channelization	The type of channelization, such as channelized T3 (CT3) to T1.
Admin Status	The administrative status of the channelized line.
Oper Status	The operational status of the channelized line.
Clocking	The clocking configured on the line: Internal or Line.
DS3 Area	
Admin Status	The administrative status of the DS3 line.
Oper Status	The operational status of the DS3 line.
Port Type	The type of port.
Last Changed	The date and time of the last status change of the line.
Maximum Speed	The maximum bandwidth for the line.
Port Description	The description of the port configured on the interface.
Recovered Clocking ID	The recovered clock identifier, if known.
Scrambling	Identifies any scrambling that has been applied to the SONET payload.
Framing	The type of framing applied to the line.
Loopback	The loopback setting configured on the line.
Clocking	The clocking configured on the line: Internal or Line.
Alarm State	The alarm state of the DS3 line: • Clear—The alarm state is clear. • AIS—Alarm Indication Signal (AIS). • LOS—Loss of signal (LOS) alarm. • AIS_LOS—AIS loss of signal alarm. • LOF—Loss of frame (LOF) alarm. • AIS_LOF—AIS loss of frame alarm. • LOS_LOF—Loss of signal and loss of frame alarm. • AIS_LOS_LOF—AIS loss of signal and loss of frame alarm. • Unknown—Unknown alarm.
Internal Port	Whether or not the line includes an internal port: True or False.
Sending Alarms	Whether or not the line is sending alarms: True or False.
Line Code	The line coding applied to the line.

Step 3 To view additional information about a DS1channelized path, double-click the required entry in the Channelized DS1 table. [Figure 18-10](#) shows the information that is displayed in the Channelized DS1 PDH Properties window.

Figure 18-10 Channelized DS1 PDH Properties Window



[Table 18-11](#) describes the information that is displayed in the Channelized DS1 PDH Properties window.

Table 18-11 Channelized DS1 PDH Properties Window

Field	Description
Location Area	
Description	The path description including the physical interface and the channel number.
Channelization	The type of channelization used on the line, such as CT3-> T1.
Admin Status	The administrative status of the channelized line.
Oper Status	The operational status of the channelized line.

Table 18-11 Channelized DS1 PDH Properties Window (continued)

Field	Description
Alarm State	The alarm state of the DS1 line: • Clear—The alarm state is clear. • AIS—Alarm Indication Signal (AIS). • LOS—Loss of signal (LOS) alarm. • AIS_LOS—AIS loss of signal alarm. • LOF—Loss of frame (LOF) alarm. • AIS_LOF—AIS loss of frame alarm. • LOS_LOF—Loss of signal and loss of frame alarm. • AIS_LOS_LOF—AIS loss of signal and loss of frame alarm. • Unknown—Unknown alarm.
Sending Alarms	Whether or not the line is sending alarms: True or False.
Maximum Speed	The maximum bandwidth for the line.
Framing	The type of framing applied to the line.
Line Code	The line coding applied to the line.
Loopback	The loopback setting configured on the line.
Clocking	The clocking configured on the line: Internal or Line.
Recovered Clock ID	The 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	The name of the DS0 bundle.
Time Slots	The range of timeslots (DS0 channels) allotted to the group.
Sending Alarms	Whether or not the group is sending alarms: True or False.
Oper Status	The operational status of the group.
Encapsulation	The type of encapsulation used, such as High-Level Data Link Control (HDLC).
Admin Status	The administrative status of the group.
ID	The 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 Cisco ANA NetworkVision, right-click the required device, then choose **Inventory**.
- Step 2

In the inventory window, choose **Logical Inventory** > **MLPPP**. See [Figure 18-11](#).

Figure 18-11 MLPPP Properties in Logical Inventory

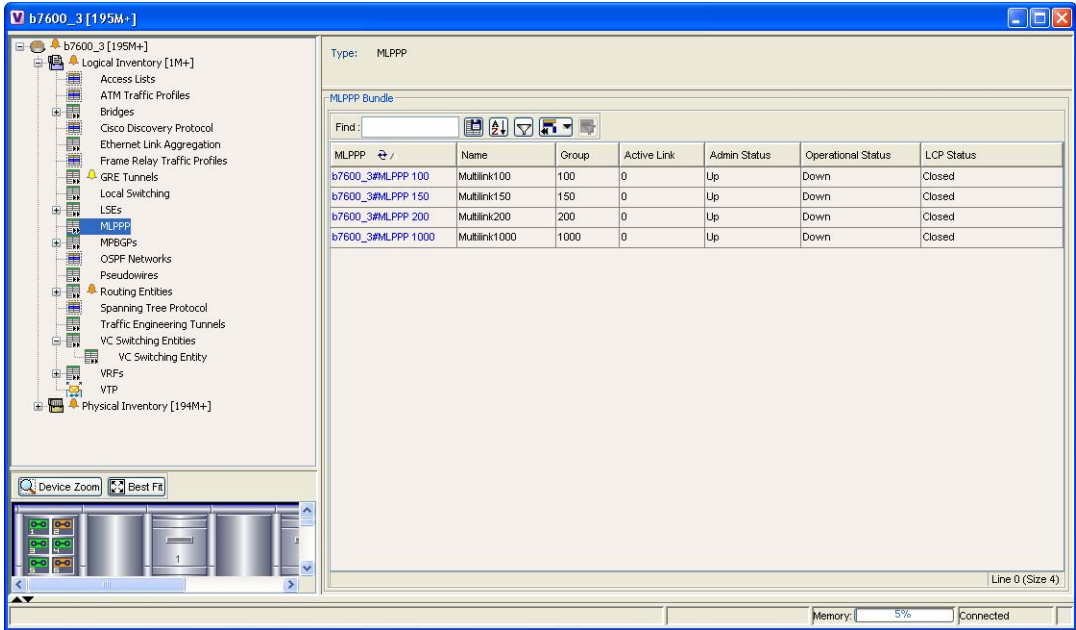


Table 18-12 describes the information that is displayed for MLPPP.

Table 18-12 MLPPP Properties

Field	Description
Type	The type of properties; in this case, MLPPP.
MLPPP Bundle Table	
MLPPP	The MLPPP bundle name, hyperlinked to the MLPPP Properties window.
Name	The MLPPP interface name.
Group	The MLPPP group to which the bundle belongs.
Active Link	The number of active interfaces participating in MLPPP.
Admin Status	The administrative status of the MLPPP bundle: Up or Down.
Operational Status	The administrative status of the MLPPP bundle: Up or Down.
LCP Status	The Link Control Protocol (LCP) status of the MLPPP bundle: Closed, Open, Started, or Unknown.

- Step 3

To view properties for individual MLPPP bundles, double-click the hyperlinked entry in the MLPPP Bundle table.
- The MLPPP Properties window is displayed as shown in [Figure 18-12](#).

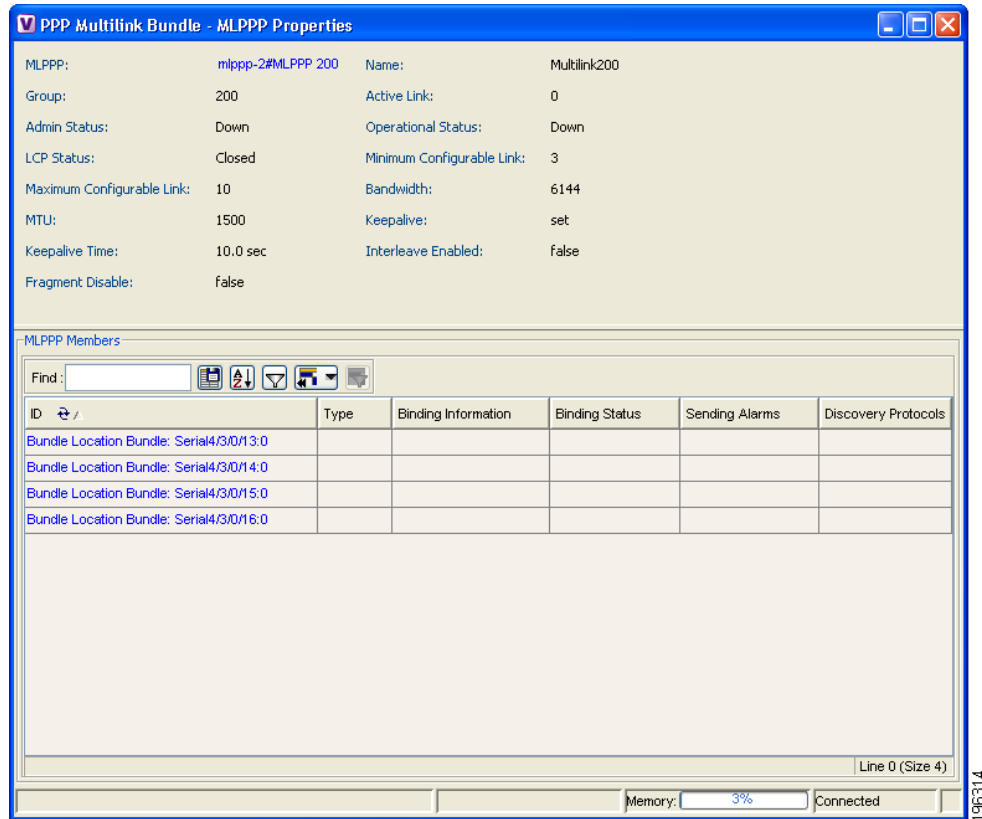
Figure 18-12 MLPPP Bundle Properties Window

Table 18-13 describes the information that is displayed in the MLPPP Properties window.

Table 18-13 MLPPP Bundle and Member Properties

Field	Description
MLPPP	The MLPPP bundle name, hyperlinked to MLPPP in logical inventory.
Name	The MLPPP interface name.
Group	The MLPPP group to which the bundle belongs.
Active Link	The number of active interfaces participating in MLPPP.
Admin Status	The administrative status of the MLPPP bundle: Up or Down.
Operational Status	The operational status of the MLPPP bundle: Up or Down.
LCP Status	The Link Control Protocol (LCP) status of the MLPPP bundle: Closed, Open, Started, or Unknown.
Bandwidth	The bandwidth allocated to the MLPPP bundle.
MTU	The size of the Maximum Transmission Unit (MTU), from 1 to 2147483647 bytes.
Keepalive	The 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.

Table 18-13 MLPPP Bundle and Member Properties (continued)

Field	Description
Fragment Disable	Whether fragmentation is enabled or disabled: True or False.
Fragment Delay	The maximum size, in units of time, for packet fragments on an MLPPP bundle. Values range from 1 to 999.
Fragment Maximum	The maximum number of MLPPP bundle fragments.
Keepalive Retry	The number of times that the device sends keepalive packets without response before closing the MLPPP bundle protocol. Values range from 2 to 254.
Minimum Configured Link	The minimum number of configured links for an MLPPP bundle.
Maximum Configured Link	The maximum number of configured links for an MLPPP bundle.
Load Threshold	The minimum load threshold for the MLPPP bundle. If the traffic load falls below the threshold, the link is removed.
MLPPP Members Table	
ID	The MLPPP bundle member identifier, hyperlinked to the interface in physical inventory.
Type	No value is displayed in this field.
Binding Information	The binding information to which the interface is associated. The value is null.
Binding Status	No value is displayed in this field.
Sending Alarms	Whether or not the interface is sending alarms: True or False.
Discovery Protocols	The 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.

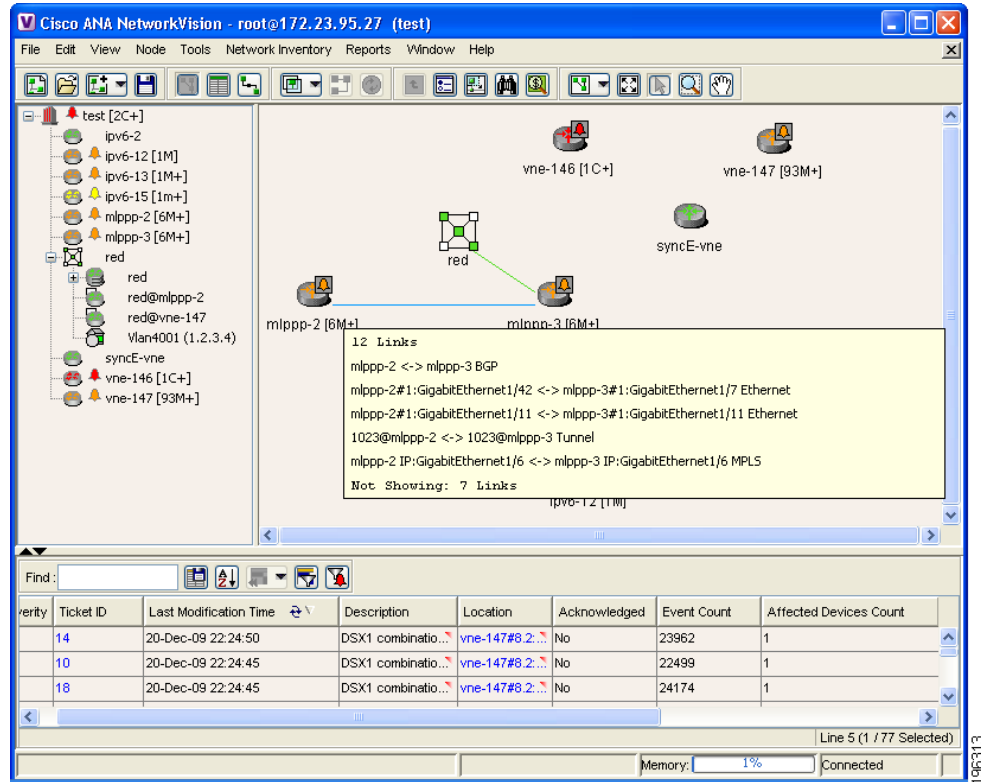
Viewing MLPPP Link Properties

An MLPPP link is a link that connects two MLPPP devices.

To view MLPPP link properties:

Step 1 In the Cisco ANA NetworkVision map view, select a link connected to two MLPPP devices. The link information is displayed as shown in [Figure 18-13](#).

Figure 18-13 MLPPP Link in Cisco ANA NetworkVision



Step 2 To view the MLPPP link properties, right-click the link and then choose **Properties**. The link properties are displayed as shown in Figure 18-14.

Figure 18-14 MLPPP Link Properties

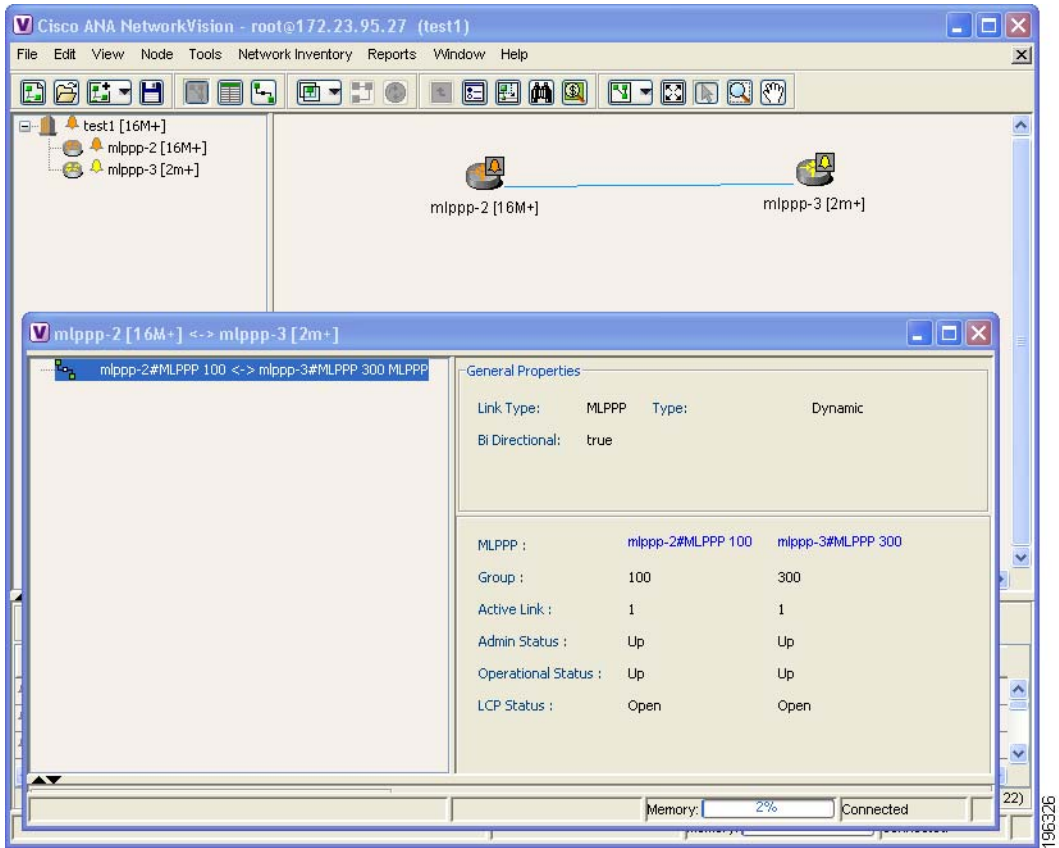


Table 18-14 describes the information that is displayed for the MLPPP link.

Table 18-14 MLPPP Link Properties

Field	Description
General Properties	
Link Type	The link protocol. In this case, MLPPP.
Type	The type of link: Dynamic or Static.
Bi Directional	Whether the link is bidirectional: True or False.
MLPPP Properties	
The properties are displayed for both ends of the MLPPP link.	
MLPPP	The interface configured for MLPPP, hyperlinked to the entry in physical inventory.
Group	The MLPPP group to which the interface belongs.
Active Link	The number of active interfaces participating in the MLPPP link for each device.
Admin Status	The administrative status of the interface: Up or Down.

Table 18-14 *MLPPP Link Properties (continued)*

Field	Description
Operational Status	The operational status of the interface: Up or Down.
LCP Status	The 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 Cisco ANA NetworkVision, right-click the required device, then choose **Inventory**.
 - Step 2** In the inventory window, choose **Logical Inventory > Pseudowires**. The Tunnel Edges table is displayed in the content pane as shown in [Figure 18-15](#).
 - Step 3** Select the required entry and scroll horizontally until you see the required information.

Figure 18-15 MPLS Pseudowire Tunnels over GRE Properties

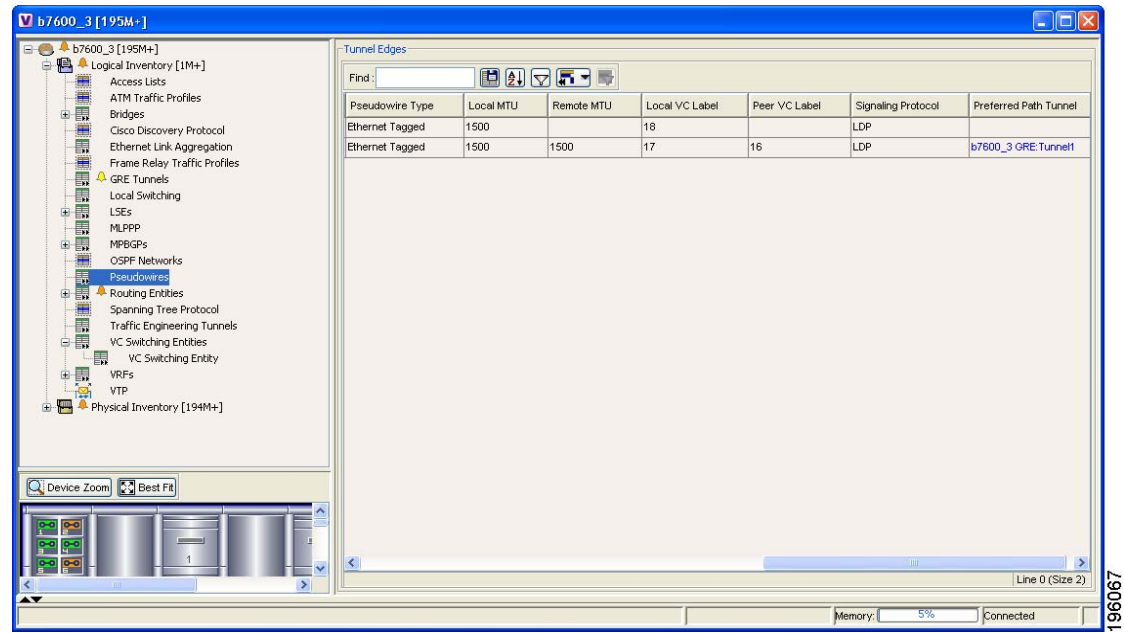


Table 18-15 describes the information included in the Tunnel Edges table specifically for MPLS pseudowire tunnels over GRE.

Table 18-15 MPLS Pseudowire over GRE Properties

Field	Description
Local MTU	The size, in bytes, of the MTU on the local interface.
Preferred Path Tunnel	The path to be used for MPLS pseudowire traffic. Click the hyperlinked entry to view the tunnel details in logical inventory.
Pseudowire Type	Type of pseudowire relevant to MToP: - ATM AAL5 SDU—ATM with ATM Adaptation Layer 5 (AAL5) service data units. - ATM n-to-one VCC—ATM with n-to-one virtual channel connection (VCC). - ATM n-to-one VPC—ATM with n-to-one virtual path connection (VPC). - CESoPSN Basic—CESoPSN basic services with CAS. - SAToP E1—SAToP on an E1 interface. For a complete list of pseudowire types, see the Cisco Active Network Abstraction 3.7.1 Theory of Operations Guide .
Remote MTU	The size, in bytes, of the MTU on the remote interface.

Step 4 To view GRE Tunnel properties, choose **Logical Inventory > GRE Tunnels**.

Figure 18-16 shows the Tunnel Edges table that is displayed for GRE tunnels.

Figure 18-16 GRE Tunnel Properties in Logical Inventory

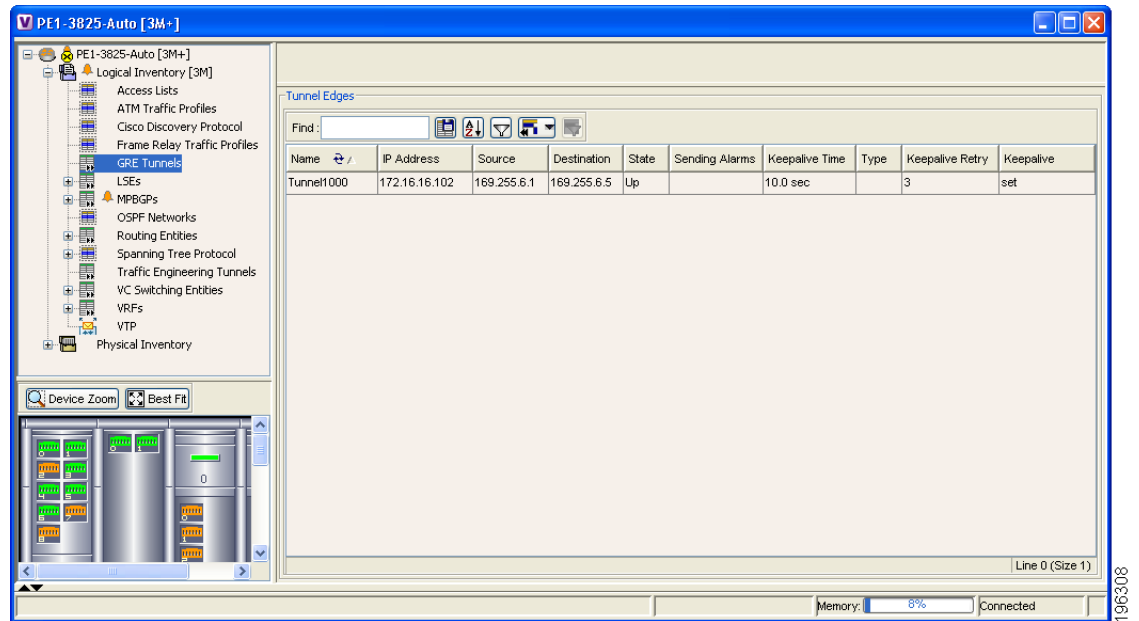


Table 18-16 describes the information that is displayed for GRE tunnels in logical inventory.

Table 18-16 GRE Tunnel Properties in Logical Inventory

Field	Description
Name	The tunnel name.
IP Address	The tunnel IP address.
Source	The IP address local to the device.
Destination	The IP address of the remote router.
State	The state of the tunnel: Up or Down.
Sending Alarms	Whether the tunnel is configured for sending alarms: True or False.
Keepalive Time	If keepalive is enabled, the amount of time, in seconds, to wait before sending a keepalive message.
Type	The tunnel type.
Keepalive Retry	The 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.
Keepalive	The status of the keepalive function: Set, Not Set, or Unknown.

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 Cisco ANA, *clock service* refers to *network clock service*.

Monitoring Clock Service

To monitor clock service:

- Step 1** In Cisco ANA NetworkVision, right-click the required device, then choose **Inventory**.
- Step 2** In the inventory window, choose **Logical Inventory > Clock**. Clock service information is displayed in the content pane as shown in [Figure 18-17](#).

Figure 18-17 Clock Service Properties

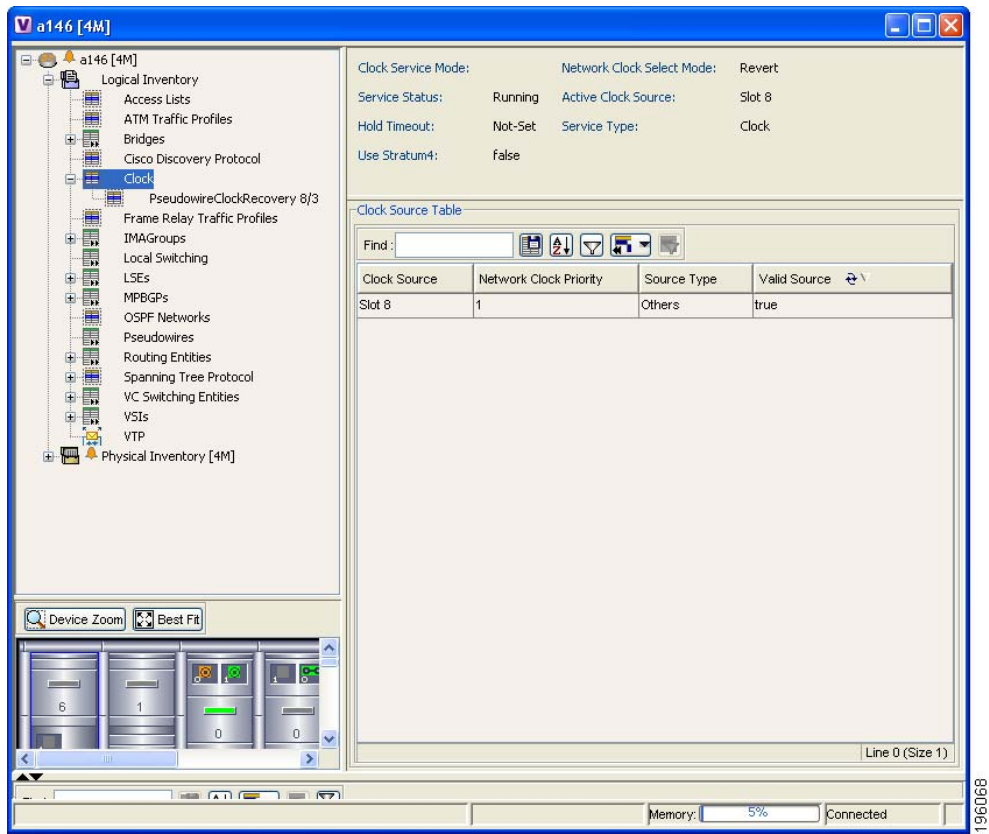


Table 18-17 describes the information displayed for clocking service.

Table 18-17 Clock Service Properties

Field	Description
Clock Service Mode	This field is not populated.
Network Clock Select Mode	The action to take if the master device fails: - Non-revert—Do not use the master device again after it recovers from the failure. - Revert—Use the master device again after it recovers and functions correctly for a specified amount of time. - Unknown—The network clock selection mode is unknown.
Service Status	The status of the system service: - Initializing—The service is starting up. - Down—The service is down. - Reset—The service has been reset. - Running—The service is running. - Other—A status other than those listed.
Active Clock Source	The current active clock source used by the NE.
Hold Timeout	How long the NE waits before reevaluating the network clock entry. Values can be from 0-86400 seconds, Not Set, or infinite.
Service Type	Indicates the type of system service, such as Clock or Cisco Discovery Protocol.
Use Stratum4	The quality of the clock source: - True—Use Stratum 4, the lowest level of clocking quality. - False—(Default) Use Stratum 3, a higher level of clocking quality than Stratum 4.
Clock Source Table	
Clock Source	The current active clock source used by the NE.
Network Clock Priority	The priority of the clock source with 1 being the highest priority.

Table 18-17 Clock Service Properties (continued)

Field	Description
Source Type	The method by which clocking information is provided: • BITS—Timing is supplied by a Building Integrated Timing Supply (BITS) port clock. • E1/T1—Clocking is provided via an E1 or T1 interface. • Packet-Timing—Clocking is provided over a packet-based network. • Synchronous Ethernet—Clocking is provided by Synchronous Ethernet. • Others—Clocking is provided by a source other than the above.
Valid Source	Validity of the clock source: • True—The clock source is valid and operational. • False—The clock source is not valid or is not operational.

Monitoring PTP Service

In networks that employ TDM, periodic synchronization of device clocks is required to ensure that the receiving device knows which channel is which for accurate reassembly of the data stream. The Precision Time Protocol (PTP) standard:

- Specifies a clock synchronization protocol that enables this synchronization.
- Applies to distributed systems that consist of one or more nodes communicating over a network.

Defined by IEEE 1588-2008, PTP Version 2 (PTPv2) allows device synchronization at the nanosecond level.

PTP uses the concept of master and slave devices to achieve precise clock synchronization. Using PTP, the master device periodically starts a message exchange with the slave devices. After noting the times at which the messages are sent and received, each slave device calculates the difference between its system time and the system time of the master device. The slave device then adjusts its clock so that it is synchronized with the master device. When the master device initiates the next message exchange, the slave device again calculates the difference and adjusts its clock. This repetitive synchronization ensures that device clocks are coordinated and that data stream reassembly is accurate.

To monitor PTP service:

-
- Step 1** In Cisco ANA NetworkVision, right-click the required device, then choose **Inventory**.
- Step 2** In the inventory window, choose **Logical Inventory > Clock > PTP Service**. The PTP service properties are displayed in the content pane as shown in [Figure 18-18](#).

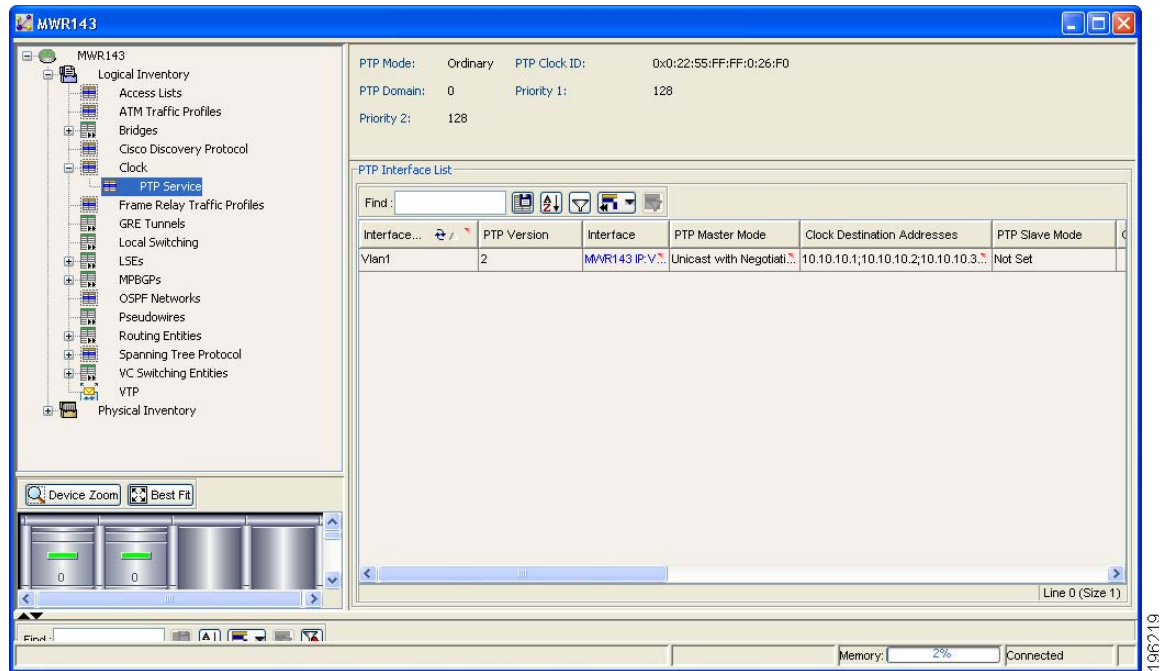
Figure 18-18 PTP Service Properties

Table 18-18 describes the properties that are displayed for PTP service.

Table 18-18 PTP Service Properties

Field	Description
PTP Mode	The mode of PTP operation: - Boundary—Boundary clock mode. - E2E Transparent—End-to-end transparent clock mode. - Ordinary—Ordinary clock mode. - P2P Transparent—Peer-to-peer transparent clock mode. - Unknown—The clock mode is unknown. Note Cisco MWR-2941 routers support Ordinary mode only.
PTP Clock ID	The clock identifier derived from the device interface.
PTP Domain	The number of the domain used for PTP traffic. A single network can contain multiple separate domains.
Priority 1	The 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.
PTP Interface List Table	
Interface Name	The interface identifier.
PTP Version	The version of PTP used. The default value is 2, indicating PTPv2.

Table 18-18 PTP Service Properties (continued)

Field	Description
Interface	The physical interface identifier, hyperlinked to the routing information for the interface.
PTP Master Mode	For an interface defined as a master device, the mode used for PTP clocking: • Not Set—The master mode is not used. • Multicast—The interface uses multicast mode for PTP clocking. • Unicast—The interface uses unicast mode for PTP clocking. This mode allows a single destination. • Unicast with Negotiation—The interface uses unicast mode with negotiation for PTP clocking. This mode allows up to 128 destinations.
Clock Destination Addresses	The IP addresses of the clock destinations. This field contains IP addresses only when Master mode is enabled.
PTP Slave Mode	For an interface defined as a slave device, the mode used for PTP clocking: • Not Set—The slave mode is not used. • Multicast—The interface uses multicast mode for PTP clocking. • Unicast—The interface uses unicast mode for PTP clocking. • Unicast with Negotiation—The interface uses unicast mode with negotiation for PTP clocking.
Clock Source Addresses	The IP addresses of the clock source.
Delay Request Interval (log mean value)	When the interface is in PTP master mode, the interval specified to member devices for delay request messages. The intervals use base 2 values, as follows: • 4—1 packet every 16 seconds. • 3—1 packet every 8 seconds. • 2—1 packet every 4 seconds. • 1—1 packet every 2 seconds. • 0—1 packet every second. • -1—1 packet every 1/2 second, or 2 packets per second. • -2—1 packet every 1/4 second, or 4 packets per second. • -3—1 packet every 1/8 second, or 8 packets per second. • -4—1 packet every 1/16 seconds, or 16 packets per second. • -5—1 packet every 1/32 seconds, or 32 packets per second. • -6—1 packet every 1/64 seconds, or 64 packets per second.

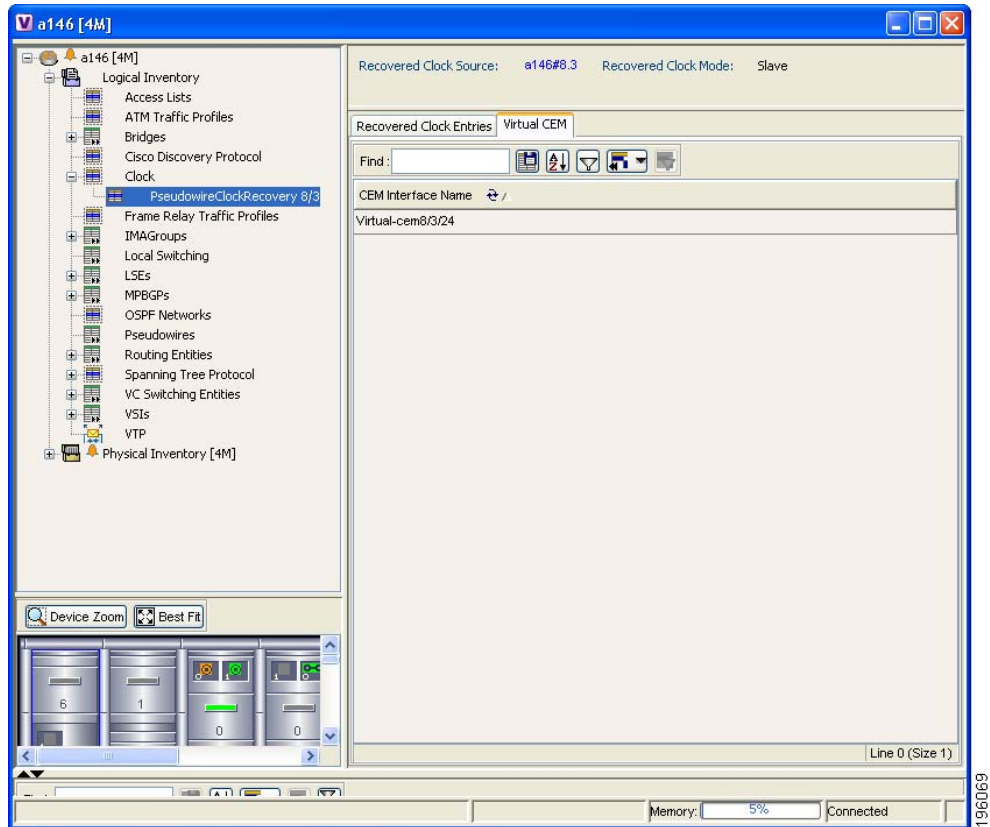
Table 18-18 PTP Service Properties (continued)

Field	Description
Announce Interval (log mean value)	The interval value for PTP announcement packets: • 4—1 packet every 16 seconds. • 3—1 packet every 8 seconds. • 2—1 packet every 4 seconds. • 1—1 packet every 2 seconds. • 0—1 packet every second. • -1—1 packet every 1/2 second, or 2 packets per second. • -2—1 packet every 1/4 second, or 4 packets per second. • -3—1 packet every 1/8 second, or 8 packets per second. • -4—1 packet every 1/16 seconds, or 16 packets per second. • -5—1 packet every 1/32 seconds, or 32 packets per second. • -6—1 packet every 1/64 seconds, or 64 packets per second.
Announce Timeout	The number of PTP announcement intervals before the session times out. Values are 2-10.
Sync Interval (log mean value)	The interval for sending PTP synchronization messages: • 4—1 packet every 16 seconds. • 3—1 packet every 8 seconds. • 2—1 packet every 4 seconds. • 1—1 packet every 2 seconds. • 0—1 packet every second. • -1—1 packet every 1/2 second, or 2 packets per second. • -2—1 packet every 1/4 second, or 4 packets per second. • -3—1 packet every 1/8 second, or 8 packets per second. • -4—1 packet every 1/16 seconds, or 16 packets per second. • -5—1 packet every 1/32 seconds, or 32 packets per second. • -6—1 packet every 1/64 seconds, or 64 packets per second.
Sync Limit (nanoseconds)	The maximum clock offset value, in nanoseconds, before PTP attempts to resynchronize.

Viewing Pseudowire Clock Recovery Properties

To view Pseudowire Clock Recovery properties:

- Step 1** Choose **Logical Inventory > Clock > Pseudowire Clock Recovery**. Cisco ANA NetworkVision displays the Virtual CEM tab by default. See [Figure 18-19](#).

Figure 18-19 Pseudowire Clock Recovery - Virtual CEM Tab

Step 2 To view more information about a virtual CEM, right-click the virtual CEM, then choose **Properties**. The Virtual CEM Properties window is displayed.

The information that is displayed in the Virtual CEM Properties window depends on whether or not the virtual CEM belongs to a group:

- If a CEM group is not configured on the virtual CEM, the Virtual CEM Properties window contains only the CEM interface name.
- If a CEM group is configured on the virtual CEM, the Virtual CEM Properties window contains the information described in [Table 18-19](#).

Table 18-19 Virtual CEM Group Properties

Field	Description
CEM Interface Name	The CEM interface name.
CEM Group Table	
CEM Group	Name of the virtual CEM group.
Framing	The framing mode used for the CEM channel: - Framed—Specifies the channels used for the controller, such as Channels: (1-8), (10-14). The channels that are available depend on the type of controller: T1, E1, T3, or E3. - Unframed—Indicates that a single CEM channel is used for all T1/E1 timeslots. SAToP uses the unframed mode.
Pseudowire	The name of the pseudowire configured on the CEM interface, hyperlinked to the pseudowire properties in logical inventory.
Oper Status	The operational status of the CEM interface: - Dormant—The interface is dormant. - Down—The interface is down. - Not Present—An interface component is missing. - Testing—The interface is in test mode. - Unknown—The interface has an unknown operational status. - Up—The interface is up.
Admin Status	The administrative status of the CEM interface: - Down—The CEM interface is administratively down. - Testing—The administrator is testing the CEM interface. - Unknown—The administrative status is unknown. - Up—The CEM interface is administratively up.

Step 3 To view additional CEM group properties, double-click the required CEM group.

[Table 18-20](#) describes the information displayed in the CEM Group Properties window.

Table 18-20 CEM Group Properties

Field	Description
Oper Status	The operational status of the CEM interface: • Dormant—The interface is dormant. • Down—The interface is down. • Not Present—An interface component is missing. • Testing—The interface is in test mode. • Unknown—The interface has an unknown operational status. • Up—The interface is up.
Idle Pattern	The 8-bit hexadecimal number that is transmitted on a T1 or E1 line when missing packets are detected on the pseudowire (PW) circuit.
Type	The 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	The associated card and slot for the virtual CEM, using the virtual CEM port 24; for example virtual-cem/8/3/24:0.
Dejitter	The size of the dejitter buffer in milliseconds (ms). The range is 4 to 500 ms with a default of 4 ms.
RTP Hdr Compression	Indicates whether RTP header compression is enabled or disabled.
RTP Enabled	Indicates whether RTP compression is enabled or disabled.
Admin Status	The administrative status of the CEM interface: • Down—The CEM interface is administratively down. • Testing—The administrator is testing the CEM interface. • Unknown—The administrative status is unknown. • Up—The CEM interface is administratively up.
ID	The DS0 bundle CEM group identifier.
Payload Size	The size of the payload for packets on the CEM interface. The range is 32 to 1312 bytes.

Step 4 To view recovered clock entries, click the Recovered Clock Entries tab. See [Figure 18-20](#).
If no recovered clock entries exist, this tab is not displayed.

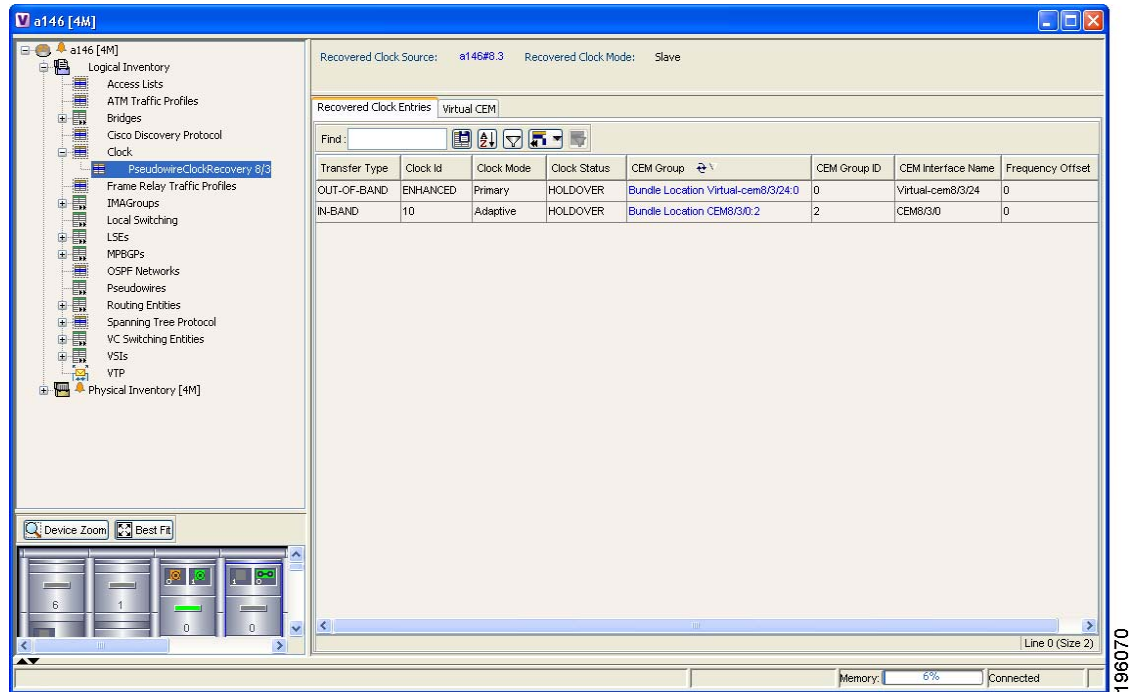
Figure 18-20 Pseudowire Clock Recovery - Recovered Clock Entries Tab

Table 18-21 describes the information displayed for pseudowire clock recovery.

Table 18-21 Pseudowire Clock Recovery Properties

Field	Description
Recovered Clock Source	The interface (slot/subslot) in which clock recovery occurred. Click the hyperlinked entry to view its properties in physical inventory.
Recovered Clock Mode	Identifies the recovered clock mode: - Adaptive—The devices do not have a common clock source. The recovered clock is derived from packet arrival. - Differential—The edge devices have a common clock source, and the recovered clock is derived from timing information in packets and the related difference from the common clock. - Synchronous—A GPS or BITS clock source externally synchronizes both end devices. This method is extremely accurate, but is rarely available for all network devices. For more information about clock recovery methods, see the Cisco Active Network Abstraction 3.7.1 Theory of Operations Guide .

Table 18-21 Pseudowire Clock Recovery Properties (continued)

Field	Description
Virtual CEM Tab	
CEM Interface Name	The virtual CEM interface associated with the clock.
Recovered Clock Entries Tab	
This tab appears if recovered entries exist.	
Transfer Type	• In-band—The clocking information is sent over the same pseudowire as the bearer traffic. • Out-of-band—The clocking information is sent over a dedicated pseudowire between the sending and receiving SPAs.
Clock ID	The clock identifier, if known.
Clock Mode	The clock mode of the recovered clock: • Adaptive—The recovered clock was obtained using ACR. • Primary—The recovered clock was obtained from a clock with the highest priority. • Secondary—The recovered clock was obtained from a clock with a lower priority than the primary clock.
Clock Status	The status of the clock: • Acquiring—The clock is obtaining clocking information. • Acquired—The clock has obtained the required clocking information. • Holdover—The current primary clock is invalid and a holdover timer has started to check whether or not the clock becomes valid within the specified holdover time.
CEM Group	The CEM group associated with the clock.
CEM Group ID	The ID of the CEM group associated with the clock.
CEM Interface Name	The virtual CEM interface associated with the clock.
Frequency Offset	The offset to the clock frequency, in Hz.

Viewing SyncE Properties

With Ethernet equipment gradually replacing SONET and SDH equipment in service-provider networks, frequency synchronization is required to provide high-quality clock synchronization over Ethernet ports. Synchronous Ethernet (SyncE), a recently adopted standard, provides the required synchronization at the physical level.

In SyncE, Ethernet links are synchronized by timing their bit clocks from high-quality, stratum-1-traceable clock signals in the same manner as SONET/SDH. Operations messages maintain SyncE links, and ensure a node always derives timing from the most reliable source.

To view SyncE properties, choose **Logical Inventory > Clock > SyncE**. (See [Figure 18-21](#).)

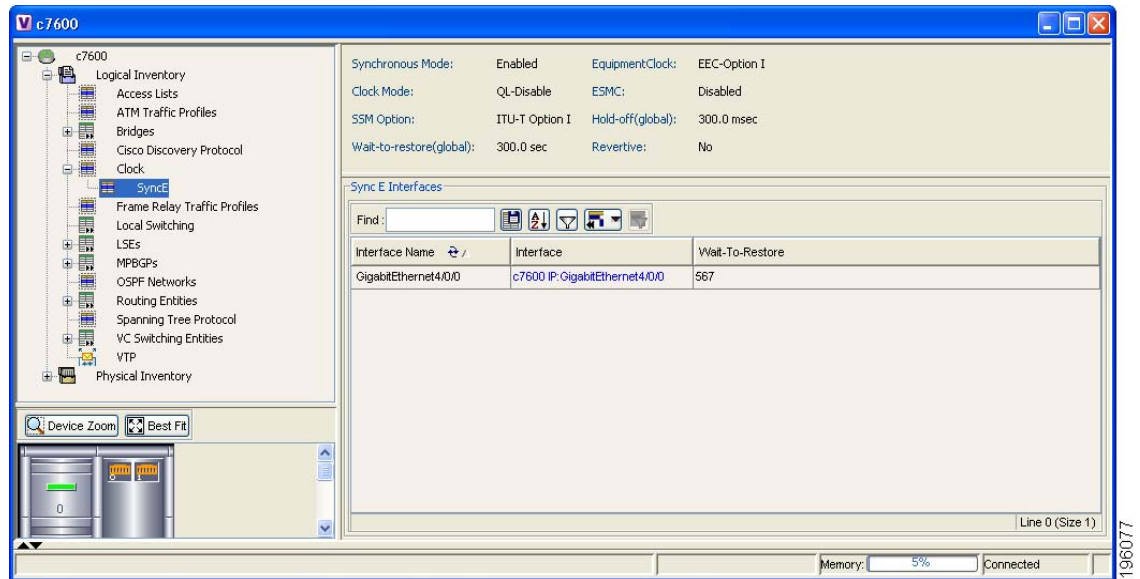
Figure 18-21 SyncE Properties in Logical Inventory

Table 18-22 describes the information that is displayed for SyncE.

Table 18-22 SyncE Properties

Field	Description
Synchronous Mode	The 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	The Ethernet Synchronization Message Channel (ESMC) status: Enabled or Disabled.
SSM Option	The type of Synchronization Status Message (SSM) option being used: - ITU-T Option I - ITU-T Option II generation 1 - ITU-T Option II generation 2
Hold-off (global)	The length of time (in milliseconds) to wait before issuing a protection response to a failure event.
Wait-to-restore (global)	The length of time (in seconds) to wait after a failure is fixed before the span returns to its original state.
Revertive	Whether the network clock is to use revertive mode: Yes or No.

Table 18-22 *SyncE Properties (continued)*

Field	Description
SyncE Interfaces Table	
Interface Name	The interface name.
Interface	A hyperlinked entry to the interface routing information in the Routing Entity Controller window. For more information, see Viewing Routing Entities, page 17-22 .
Wait-to-Restore	The length of time (in seconds) to wait after a failure is fixed before the interface returns to its original state.

Viewing CEM and Virtual CEM Properties

The following topics describe how to view CEM and virtual CEM properties and interfaces:

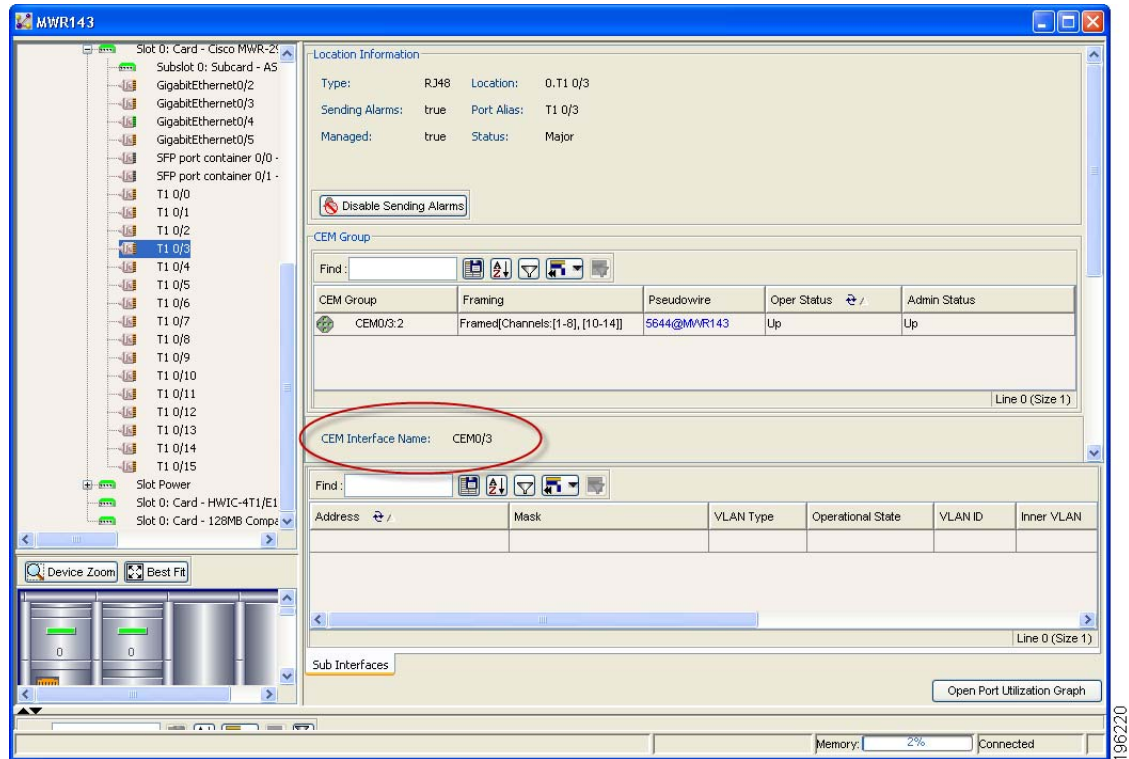
- [Viewing CEM Interfaces, page 18-40](#)
- [Viewing Virtual CEMs, page 18-41](#)
- [Viewing CEM Groups, page 18-41](#)

Viewing CEM Interfaces

To view CEM interfaces:

-
Step 1	In Cisco ANA NetworkVision, right-click the required device, then choose Inventory .
Step 2	In the inventory window, choose Physical Inventory > Chassis > slot > subslot > interface . The CEM interface is displayed in the content pane as shown in Figure 18-22 .

Figure 18-22 CEM Interface



Viewing Virtual CEMs

To view virtual CEMs, choose **Logical Inventory > Clock > Pseudowire Clock Recovery** (Figure 18-19).

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 Cisco ANA NetworkVision:

- [Viewing CEM Groups on Physical Interfaces, page 18-41](#)
- [Viewing CEM Groups on Virtual CEM Interfaces, page 18-42](#)

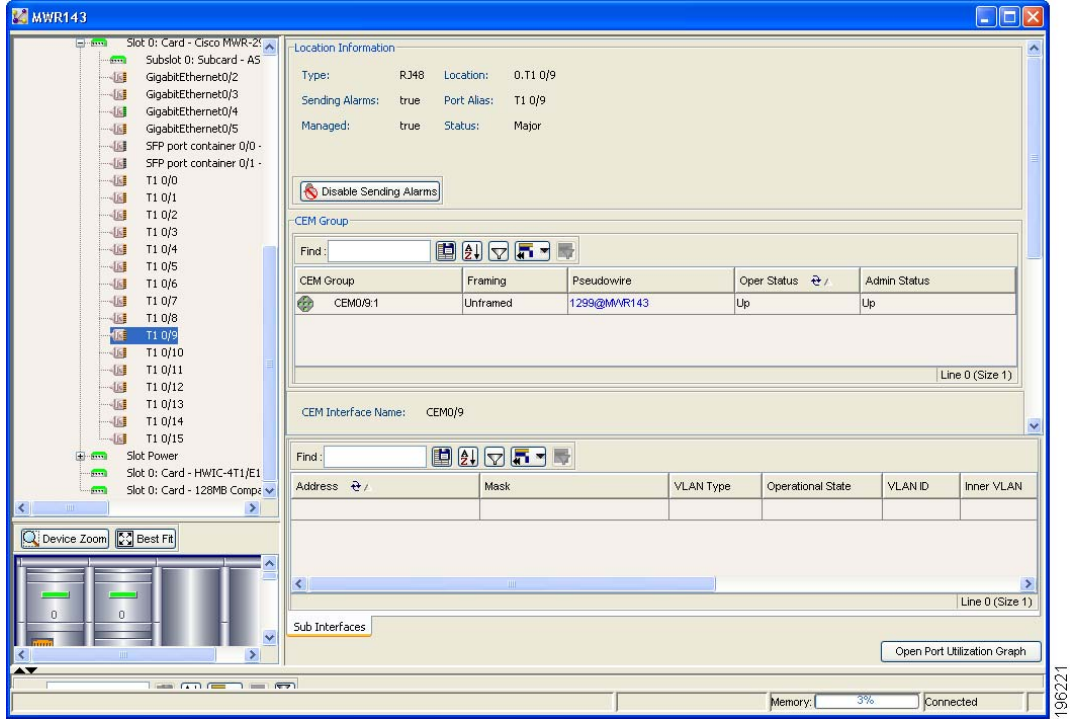
Viewing CEM Groups on Physical Interfaces

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 Cisco ANA NetworkVision, right-click the required device, then choose **Inventory**.
- Step 2** In the navigation pane, choose **Physical Inventory > Chassis > slot > subslot > interface**.
The CEM group information is displayed in the content pane with other interface properties (Figure 18-23).

Figure 18-23 CEM Group Information



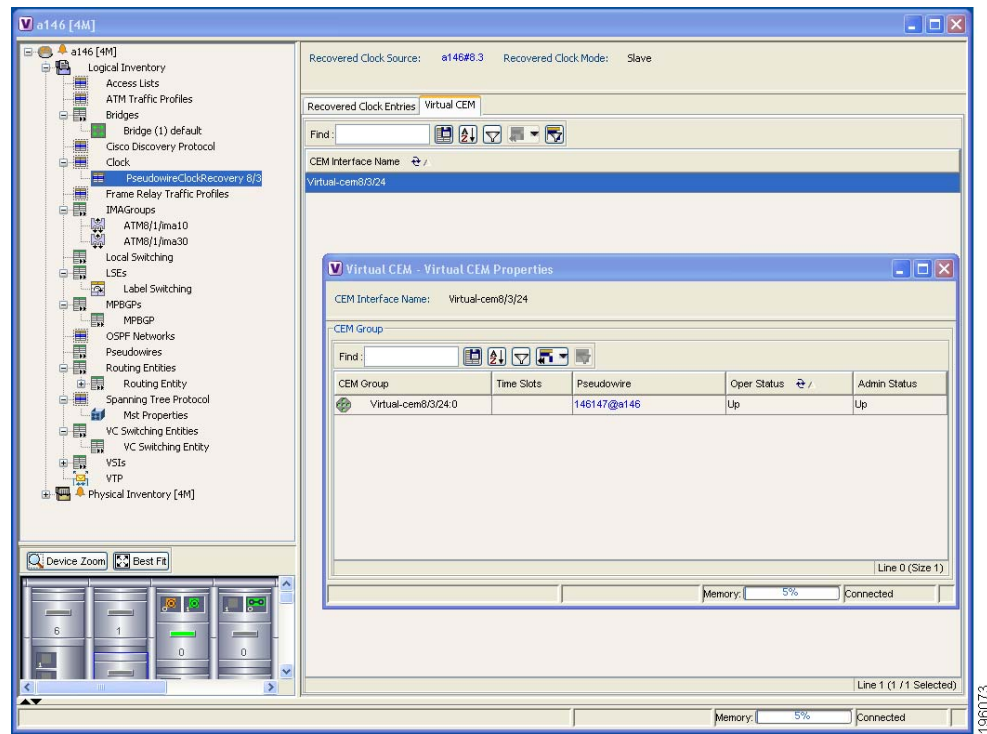
See Table 18-19 for a description of the properties displayed for CEM groups in the content pane.

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 Cisco ANA NetworkVision, right-click the required device, then choose **Inventory**.
- Step 2** In the inventory window, choose **Logical Inventory > Clock > Pseudowire Clock Recovery**.
- Step 3** In the Virtual CEM tab, right-click the CEM interface name and choose **Properties**. The CEM group properties are displayed in a separate window (Figure 18-24). If a pseudowire is configured on the CEM group for out-of-band clocking, the pseudowire VCID is also shown.

Figure 18-24 CEM Group Properties

- Step 4** To view additional CEM group properties, double-click the required CEM group.
- [Table 18-20](#) describes the information displayed in the CEM Group Properties window.



CHAPTER 19

Viewing SBC Properties

This topic identifies and describes the properties for Session Border Controllers (SBCs) that appear in Cisco ANA NetworkVision logical inventory.

An SBC can provide the following types of services:

- Protocol and media interworking
- Session routing
- Hosted Network Address Translation (NAT) and firewall traversal
- Security and AAA
- Intra- and inter-VPN interconnections and optimization
- Media transcoding with an external media server

SBC services are divided into the following components:

- Data Border Element (DBE)—Responsible for media-related functions.
- Signaling Border Element (SBE)—Responsible for call signaling-related functions.



Note

The existing Cisco SBC platforms support only DBE.

An SBC itself consists of the combined DBE and SBE functionality.

In addition, the SBC can operate in the following deployment models:

- Distributed Model (DM)—Contains only the SBE or DBE, resulting in a distributed SBC.
- Unified Model (UM)—Contains both the SBE and DBE, thereby implementing the SBE and DBE as a single device.

The following topics describe the SBC properties that are displayed in Cisco ANA NetworkVision logical inventory:

- [User Roles Required to View SBC Properties, page 19-2](#)
- [Viewing SBC Properties in Logical Inventory, page 19-2](#)
- [Viewing SBC Properties in Logical Inventory, page 19-2](#)
- [Viewing SBC DBE Properties, page 19-4](#)
- [Viewing SBC SBE Properties, page 19-5](#)

User Roles Required to View SBC Properties

Table 19-1 identifies the GUI default permission or device scope security level that is required to view SBC properties in Cisco ANA NetworkVision. Cisco ANA 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 device-based tasks (tasks that do affect devices), authorization is based on the default permission that is assigned to your account. That is, whether the device 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 Active Network Abstraction 3.7.1 Administrator Guide](#).

Table 19-1 Default Permission/Security Level Required for Viewing SBC Properties

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Viewing SBC properties	—	—	—	—	X

Viewing SBC Properties in Logical Inventory

To view SBC properties Cisco ANA NetworkVision logical inventory, right-click the element configured for SBC, then choose **Inventory > Logical Inventory > Session Border Controller**.

The SBC properties are displayed as shown in [Figure 19-1](#).

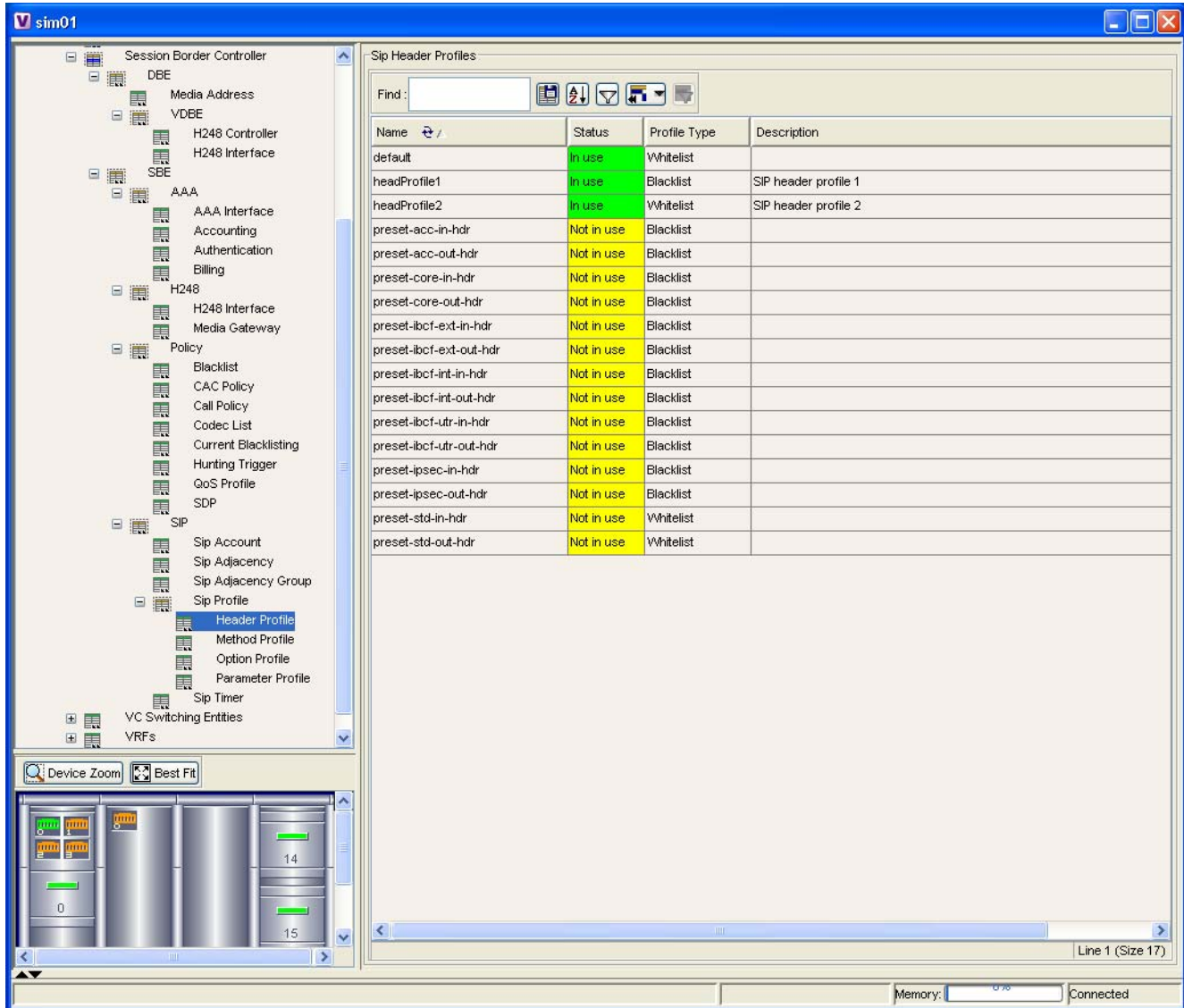
Figure 19-1 SBC Properties in Cisco ANA NetworkVision Logical Inventory

Table 19-2 describes the general SBC properties displayed in Cisco ANA NetworkVision logical inventory.

Table 19-2 SBC Properties

Field	Description
Process	The process name, such as Session Border Controller.
Process Status	The status of the process, such as Running.
Mode	The mode in which the SBC is operating: - Unified - Distributed DBE

Table 19-2 SBC Properties (continued)

Field	Description
SBC Service Name	The name of the service.
Application Version	The SBC version number.

Viewing SBC DBE Properties

The DBE controls media packet access to the network, provides differentiated services and QoS for different media streams, and prevents service theft.

To view SBC DBE properties, choose **Logical Inventory > Session Border Controller > DBE**.

[Table 19-3](#) describes the DBE properties that appear in logical inventory.

Table 19-3 SBC DBE Properties

Field	Description
Process	The process name, such as DBE.
Process Status	The status of the process, such as Running.
Name	A name assigned to the DBE.
Type	The type of DBE, either DBE or virtual DBE (vDBE).
DBE Location Id	A unique identifier configured on each vDBE within a UM DBE.

Viewing Media Address Properties

A DBE uses a pool of sequential IPv4 media addresses as local media addresses.

To view SBC media address properties, choose **Logical Inventory > Session Border Controller > DBE > Media Address**.

[Table 19-4](#) describes the SBC media address properties that are displayed in logical inventory.

Table 19-4 Media Address Properties

Branch	Description
Media Address	The Media Address table contains the following information: - Address Range—The IP addresses defined for the pool. - Port Range Lower—The 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—The upper end of the port range for the interface. - VRF Name—The VRF the interface is assigned to. - Service Class—The class of service (CoS) for each port range. Options include fax, signaling, voice, or any.

Viewing VDBE H.248 Properties

To view VDBE H.248 properties, choose **Logical Inventory > Session Border Controller > DBE > VDBE**.

Table 19-5 describes the VDBE H.248 properties that are displayed in logical inventory.

Table 19-5 VDBE H.248 Properties

Branch	Description
H248 Controller	The H.248 controller used by the DBE. The Media Gateway Configuration (MGC) table displays the following information: • Index—The number of the H.248 controller. The profile is used to interoperate with the SBE. • Remote IP—The remote IP address for the H.248 controller. • Remote Port—The remote port for the H.248 controller. • Transport—The transport for communications with the remote device.
H248 Interface	The SBC H248 Control Interface table displays the following information: • IP Address: – In DM mode, the local IP address of the DBE used to connect to the SBE. – In UM mode, the local IP address used to connect to the media gateway. • Port—The port for the H.248 controller interface. • Transport—The transport the H.248 controller interface uses. • Association—The relationship between the SBE and the media gateway.

Viewing SBC SBE Properties

The SBE controls the access of VoIP signaling messages to the network core and manipulates the contents of these messages. It does this by acting as a SIP B2BUA or H.323 gateway.

To view SBC SBE properties, choose **Logical Inventory > Session Border Controller > SBE**.

Table 19-6 describes the information displayed in logical inventory for an SBE.

Table 19-6 SBC SBE Properties

Field	Description
Process	The name of the process, such as SBE.
Process Status	The status of the process, such as Running or Idle.
Name	A name assigned to this SBE.

Table 19-6 SBC SBE Properties (continued)

Field	Description
Call Redirect Limit	The 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	The amount of time, in milliseconds, that the SBE waits after receiving a media timeout notification from the DBE for an on-hold call before tearing down the call.

Viewing AAA Properties

For devices that support local and remote billing, the SBC can send billing records to a AAA server using the RADIUS protocol.

To view AAA properties, choose **Logical Inventory > Session Border Controller > SBE > AAA**.

[Table 19-7](#) describes the AAA properties that appear in logical inventory for the SBC SBE.

Table 19-7 AAA Properties

Branch	Description
AAA Interface	The SBE AAA Interface table displays the following information: - AAA Address—The local AAA interface address. - Network ID—A unique identifier for the SBE.
Accounting	The Accounting Radius Client table displays the following information: - Name—The name of the accounting client. - Client Type—The type of client, either Accounting or Authentication.
Authentication	The Authentication Radius Client table displays the following information: - Name—The name of the authentication client. - Client Type—The type of client, either Accounting or Authentication.
Billing	The SBE Billing table displays the following information related to billing: - LDR Check Time—The time of day (local time) to run the long duration record check. - Local Billing Address—The local IP address for SBE billing. This IP address can be different from the local AAA IP address and is the IP address written in the bill records. - Admin Status—The configuration status, available with the running-config command. - Operational Status—The running status, available from the CLI. This entry indicates whether the billing interface is up. The status is derived from the interworking of the SBC and the AAA server.

Viewing H.248 Properties

The H.248 interface is used for signaling between an SBE and a DBE in distributed mode and between an SBE and a transcoding media gateway. The SBE or SBC acts as an H.248 MGC, and the transcoding device acts as an H.248 media gateway. The connection between the MGC and the media gateway is an H.248 link.

To view H.248 properties, choose **Logical Inventory > Session Border Controller > H248**.

[Table 19-8](#) describes the H.248 properties that appear in logical inventory for the SBC SBE.

Table 19-8 H.248 Properties

Branch	Description
H248 Interface	The SBC H.248 Control Interface table displays the following information: • IP Address: – In DM mode, the IP address used to connect the DBE and the MGC. – In UM mode, the IP address used to connect the SBC and the media gateway. • Port—The port for the H.248 controller interface. • Transport—The transport the H.248 controller interface uses. • Association—The relationship between the SBE and the media gateway.
Media Gateway	The Media Gateway table displays the following information: • IP Address—The IP address of the media gateway. • Codec List—A comma-separated list of the codecs supported.

Viewing Policy Properties

An SBC policy is a set of rules that define how the SBC treats different kinds of VoIP events. An SBC policy allows control of the VoIP signaling and media that pass through the SBC at an application level.

A *policy set* is a group of policies that can be active on the SBC at any one time. If a policy set is active, the SBC uses the rules defined within it to apply policy to events. Multiple policies can be set on a single SBC.

To view policy properties, choose **Logical Inventory > Session Border Controller > Policy**.

[Table 19-9](#) describes the policy properties that appear in logical inventory for the SBC SBE.

Table 19-9 Policy Properties

Branch	Description
Blacklist	The Blacklists table contains the following information: • Name—The blacklist name. • Type—The type of source that this blacklist applies to, such as critical or normal.
CAC Policy	A Call Admission Control (CAC) policy is used to define admission control. The SBE CAC Policy Set table contains the following information: • Policy Set Number—An identifying number the SBE has assigned to the policy set. • Status—Whether the policy is active or inactive. If the policy is active, the SBC applies the defined rules to events. • First Table—A CAC policy table. • First CAC Scope—The scale that the CAC applies for, such as source adjacency or destination adjacency. This is the first CAC table used for CAC policy match. • Description—A brief description of the policy set.
Call Policy	A call policy set is used for number analysis and routing. The SBE Call Policy Set table contains the following information: • Policy Set Number—An identifying number the SBE has assigned to the policy set. • Status—Whether the policy is active or inactive. If the policy is active, the SBC applies the defined rules to events. • First Call Table—The first call table used for call policy match. • Description—A brief description of the policy set.
Codec List	The SBE Codec List table contains the following information: • Name—The name of the codec list. • Codecs—The codecs contained in each list.

Table 19-9 Policy Properties (continued)

Branch	Description
Current Blacklisting	The Current Blacklistings table contains the following information: • Type—The type of source this blacklist applies to. Blacklists are used to block certain VoIP services that meet specified conditions. • Event Type—The type of event this blacklist applies to, such as CORRUPT_MESSAGE. • Is All Source Addresses—Whether the blacklist applies to all source IP addresses: – True—Ignore any IP address in the Source Address field. – False—Use the IP address in the Source Address field. • Source Address—The IP address that this blacklist applies to. • Source Port Number—The port number that this blacklist applies to. • Source Port Type—The type of port this blacklist applies to. <i>All</i> is a valid entry. • Time Remaining—The amount of time, in hours, minutes, or seconds, before the blacklist is removed.
Hunting Trigger	The hunting trigger enables the SBC to search for other routes or destination adjacencies if an existing route fails. The Global Hunting Trigger List table contains the following information: • Hunting Mode—Indicates the protocol to use to search for routes, such as Session Initiation Protocol (SIP). • Hunting Triggers—The SIP responses, such as 468 or 503, that indicate the SBC is to search for an alternate route or destination adjacency. SIP responses are defined in RFC3261.

Table 19-9 *Policy Properties (continued)*

Branch	Description
QoS Profile	QoS profiles can be used by CAC policies and are used exclusively for marking IP packets. The QoS Profile table contains the following information: • Name—The name of the QoS profile. • Class of Service—The type of call this profile applies to, such as voice, video, signaling, or fax. • Marking Type—The type of marking to be applied to the IP packet. Options include Passthrough, Differentiated Service Code Point (DSCP), and IP Precedence/ToS. • IP Precedence—If the marking type is IP Precedence, the specified precedence, either 0 or 1. • ToS—If the marking type is ToS, the ToS value. • DSCP—If the marking type is DSCP, the DSCP value.
SDP	The Session Description Protocol (SDP) content pane contains the following tabs, each with their respective table: • SBE SDP Policy Table: – Instance Name—The name of the policy table. – SBE SDP Match Table—The name of the SDP match table. • SBE SDP Match Table: – Instance Name—The name of the SDP table. – Match Strings—The match criteria. – Table Type—The type of table, either Blacklist or Whitelist.

Viewing SIP Properties

To view SIP properties, choose **Logical Inventory > Session Border Controller > SIP**.

Table 19-10 describes the SIP entries that appear in logical inventory for the SBC SBE.

Table 19-10 SIP Properties

Branch	Description
SIP Account	The SBE Account table contains the following information: • Name—The name of the account associated with the adjacencies. • Adjacencies—The identified adjacencies.
SIP Adjacency	An adjacency represents a signaling relationship with a remote call agent. One adjacency is defined per external call agent. Each adjacency belongs within an account. Each incoming call is matched to an adjacency, and each outgoing call is routed out over a second adjacency. The SBC SIP Adjacencies table contains the following information: • Name—The adjacency name. • Status—The status of the adjacency, either Attached or Detached. • Signaling Address—The local IP address and port (optional) for communications. • Signaling Peer—The remote IP address and port (optional) for communications. • Description—A brief description of the adjacency.
SIP Adjacency Group	The Adjacencies Groups table contains the following information: • Name—The name of the SIP adjacency group. • Adjacencies—The adjacencies that belong to the group.
SIP Profile	The SBC can be configured with whitelist and blacklists profiles on SIP messages. The following types of SIP profiles are available: • Header profile—A profile based on SIP header information. • Method profile—A profile based on SIP method strings. • Option profile—A profile based on SIP option strings. • Parameter profile—A profile based on SIP parameters.
SIP Profile > Header Profile	The SIP Header Profiles table contains the following information: • Name—The name of the SIP header profile. • Status—Whether or not the profile is in use. • Profile Type—The type of profile: – Whitelist—Accepts SIP requests that match the profile. – Blacklist—Rejects SIP requests that match the profile. • Description—A brief description of the profile.

Table 19-10 *SIP Properties (continued)*

Branch	Description
SIP Profile > Method Profile	The SIP Method Profiles table contains the following information: • Name—The name of the SIP method profile. • Status—Whether or not the profile is in use. • Profile Type—The type of profile: – Whitelist—Accepts SIP requests that match the profile. – Blacklist—Rejects SIP requests that match the profile. • Description—A brief description of the profile. • Is Passthrough—Whether or not passthrough is enabled: – True—Permits message bodies to be passed through for nonvital methods that match this profile. – False—Strips the message body out of any nonvital SIP messages that match this profile.
SIP Profile > Option Profile	The SIP Option Profiles table contains the following information: • Name—The name of the SIP option profile. • Status—Whether or not the profile is in use. • Profile Type—The type of profile: – Whitelist—Accepts SIP requests that match the profile. – Blacklist—Rejects SIP requests that match the profile. • Description—A brief description of the profile. • Options—The SIP option strings that define this profile, such as host user-agent, refer redirect, or replaces.

Table 19-10 SIP Properties (continued)

Branch	Description
SIP Profile > Parameter Profile	The SIP Parameter Profiles table contains the following information: • Name—The name of the SIP parameter profile. • Status—Whether or not the profile is in use. • Description—A brief description of the profile.
SIP Timer	The SBE SIP Timer table contains the following information: • TCP Connect Timeout—The time, in milliseconds, that the SBC waits for a SIP TCP connection to a remote peer to complete before failing that connection. The default is 1000 milliseconds. • TCP Idle Timeout—The minimum time, in milliseconds, that a TCP socket does not process any traffic before it closes the connection. The default is 120000 milliseconds (2 minutes). • TLS Idle Timeout—The minimum time, in milliseconds, that a Transport Layer Security (TLS) socket does not process traffic before it closes the connection. • Invite Timeout—The time, in seconds, that the SBC waits for a final response to an outbound SIP invite request. The default is 180 seconds. If no response is received during that time, an internal request timeout response is generated and returned to the caller. • UDP First Retransmit Interval—The time, in milliseconds, that the SBC waits for a UDP response or ACK before sending the first retransmission of a signal. The default value is 500 milliseconds. • UDP Max Retransmit Interval—The maximum time interval, in milliseconds, for an SBC to retransmit a signal. The maximum retransmission interval is 4000 milliseconds (4 seconds). • UDP Response Linger Period—The time, in milliseconds, for which the SBC retains negative UDP responses to invite requests. The default value is 32000 milliseconds (32 seconds).



APPENDIX A

Icon Reference

The following topics provide a quick reference to Cisco ANA NetworkVision and Cisco ANA EventVision icons:

- [Cisco ANA NetworkVision Icons, page A-1](#)
- [Cisco ANA EventVision Icons, page A-9](#)
- [Report Manager Icons, page A-11](#)
- [Icon Badges, page A-11](#)

Cisco ANA NetworkVision Icons

The following topics describe the icons used in Cisco ANA NetworkVision:

- [Map Icons, page A-1](#)
- [Link Colors, page A-3](#)
- [Cisco ANA NetworkVision Toolbar Icons, page A-4](#)
- [Table Toolbar Icons, page A-6](#)
- [Link Filtering Icons, page A-6](#)
- [Logical Inventory Icons, page A-7](#)
- [Physical Inventory Icons, page A-8](#)

Map Icons

Table A-1 *Cisco ANA NetworkVision Map Icons*

Icon	Device
	ATM switch
	Basic rate access (BRA)

Table A-1 Cisco ANA NetworkVision Map Icons (continued)

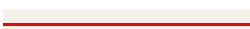
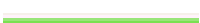
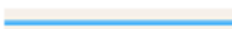
Icon	Device
	Connection termination point (TP) Ethernet flow point (EFP)
	Cross-connect
	Digital subscriber line access multiplexer (DSLAM)
	Ethernet service
	Ethernet switch
	Ethernet virtual connection (EVC)
	Generic SNMP
	Logical Circuit Aggregation (LCA) business element
	Logical Circuit Peer (LCP) business element
	Logical Circuit Peer with one or more one hidden connected devices.
	Network pseudowire
	Network, subnetwork, or logical aggregation
	Pseudowire switching entity Switching entity
	Router
	Site

Table A-1 Cisco ANA NetworkVision Map Icons (continued)

Icon	Device
	Site with one or more hidden connected devices.
	Unknown, or ghost, device
	Unmanaged network, cloud
	Viewable by a user with a higher permission level
	Virtual router
	VLAN
	VPLS
	VPN
	VSI

Link Colors

Table A-2 Link Colors

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 Badges

Table A-3 **Link Badges**

Icon	Description
	Blocking
	Multiple links
	REP primary
	REP primary and blocking
	STP root

Cisco ANA NetworkVision Toolbar Icons

Table A-4 **Cisco ANA NetworkVision Toolbar Icons**

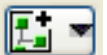
Button	Function
Map Options	
	Creates a new map in the database.
	Opens a map saved in the database using the Open dialog box.
	Adds a network element to the map or to the subnetwork selected in the navigation pane and displayed in the content pane.
	Saves the current map (the background and the location of devices) to the database.
Viewing Options	
	Displays the map view in the Cisco ANA NetworkVision content pane (the button toggles when selected or deselected).
	Displays the list view in the Cisco ANA NetworkVision content pane (the button toggles when selected or deselected).

Table A-4 Cisco ANA NetworkVision Toolbar Icons (continued)

Button	Function
	Displays the links view in the Cisco ANA NetworkVision content pane (the button toggles when selected or deselected).
Overlay Tools	
	Chooses and displays an overlay of a specific type on top of the elements displayed in the content pane in the map view. When an overlay is selected, all the elements and links that are part of the overlay are colored, and those that are not part of the overlay are dimmed.
	Displays or hides a previously defined overlay of a specific type on top of the elements displayed in the content pane in map view.
	Refreshes the overlay.
Navigation Tools	
	Moves up a branch in the navigation pane and map pane to enable you to view different information.
	Opens the Map Options dialog box, enabling you to display or hide different types of links in the map and links views.
	Opens a window displaying an overview of the network.
	Finds a device or aggregated node in the map according to the name.
	Opens the Find Business Tag dialog box, enabling you to find and delete 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 Cisco ANA NetworkVision map view: circular, symmetric, tree, or hierarchical.
	Fits the entire subnetwork or map in the map pane.
	Activates the normal selection mode (the button toggles when selected or deselected).

Table A-4 Cisco ANA NetworkVision Toolbar Icons (continued)

Button	Function
	Activates the zoom selection mode, which enables you to select an area in the map pane to enlarge by clicking and dragging (the button toggles when selected or deselected).
	Activates the pan mode, which enables you to move around in the map pane by clicking and dragging (the button toggles when selected or deselected).

Table Toolbar Icons

Table A-5 Table Toolbar

Icon	Name	Description
	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 <i>element category</i>).
	Filter	Filters the information displayed in the table by the criteria you specify.
	Clear Filter	Clears the existing filter.
	Show All Rows	Displays all table rows that meet the current filtering criteria.
	Show Only Selected Rows	Displays only the rows that you select.

Link Filtering Icons

Table A-6 Link Filtering Icons

Button	Name	Description
	All Links	Displays the complete list of links for the selected context (map or aggregated node). 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 aggregated node) and the other side either not in the map or outside the selected context.

Table A-6 *Link Filtering Icons (continued)*

Button	Name	Description
	Flat Links (Surface)	Displays the links currently visible on the map for the selected context (map or aggregated node), excluding any thumbnails.
	Deep Links	Displays the links for the current aggregated node where both endpoints are within the currently selected context.

Logical Inventory Icons

Table A-7 describes the icons used in the logical inventory navigation pane.

Table A-7 *Logical Inventory Navigation Pane 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
	ARP Entity	MPBGPs
	Bridges	OSPF Processes
	Ethernet Link Aggregation	Pseudowires
	GRE Tunnels	Routing Entities
	IMA Groups	Traffic Engineering Tunnels
	Local Switching	VC Switching Entities
	LSEs	VRFs
	MLPPP	VSIs
	Bridge	
	Connectivity Fault Management (CFM)	

Table A-7 *Logical Inventory Navigation Pane Icons (continued)*

Icon	Logical Inventory Item
	CFM Maintenance Association
	CFM Maintenance Domain
	Cross-VRF
	Encapsulation
	Inverse Multiplexing over ATM (IMA) group
	Label switching
	Logical inventory
	Multiple Spanning Tree protocol (MST) instance
	Virtual Switch Interface (VSI)
	VLAN Trunk Protocol (VTP)

Physical Inventory Icons

Table A-8 *Physical Inventory Icons*

Icon	Device
	Chassis
	Shelf
	Slot/Subslot

Table A-8 *Physical Inventory Icons (continued)*

Icon	Device
	Port/Logical Port
	Unmanaged Port

Cisco ANA EventVision Icons

This topic includes:

- [Severity Icons, page A-9](#)
- [Cisco ANA EventVision Toolbar Icons, page A-10](#)
- [Ticket Properties Toolbar Icons, page A-10](#)

Severity Icons

The severity indicators in [Table A-9](#) are also used for alarm and ticket badges.

Table A-9 *Severity Indicators*

Icon	Color	Severity
	Red	Critical
	Orange	Major
	Yellow	Minor
	Sky Blue	Warning
	Green	Cleared, Normal, or OK
	Dark Blue	Information
	White	Indeterminate

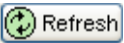
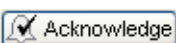
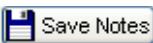
Cisco ANA EventVision Toolbar Icons

Table A-10 Cisco ANA EventVision Toolbar Icons

Button	Function
	Displays the previous page of events in the Cisco ANA EventVision window.
	Displays the next page of events in the Cisco ANA EventVision 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 Cisco ANA EventVision Filter dialog box, which enables you to define a filter for the events displayed in the Cisco ANA EventVision log.
	Toggles automatic refresh of event data on and off. You define the refresh-time period (in seconds) in the Cisco ANA EventVision 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 Toolbar Icons

Table A-11 Ticket Properties Window Toolbar Icons

Icon	Description
 Refresh	Refreshes the information displayed in the Ticket Properties dialog box.
 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. If a ticket was acknowledged, and some events were correlated to it afterward, then the ticket is considered to have not been acknowledged. This button is enabled only if the ticket is not acknowledged.
 Clear	Requests the relevant Cisco ANA to remove the faulty network element from the Cisco ANA networking inventory. In addition, it sets the ticket to Cleared severity or status (the icon is displayed in green) and automatically changes the acknowledged status of the ticket to true. This button is enabled only if the severity of the alarm is higher than Cleared or Normal.
 Save Notes	Saves the notes for the selected ticket. This button is enabled only when text is entered in the Notes field of the Notes tab.

Report Manager Icons

Table A-12 *Report Manager Toolbar Icons*

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.
	Rename	Renames a folder that you created.
	Delete	Deletes one or more folders that you created.
	Delete Report	Deletes the selected report.
	View	Displays the selected report in HTML format.

Icon Badges

This topic includes:

- [Network Element Badges, page A-12](#)
- [Alarm and Ticket Badges, page A-13](#)

Network Element Badges

Table A-13 **Network Element Icon Badges**

Badge	State	Description
	Currently Unsynchronized	The VNE model is inconsistent with the element for one of the following reasons: - A required, recoverable device command failed. - The device did not respond in a timely manner. - The VNE was in maintenance state but has restarted and is now resynchronizing with the network element. - The VNE was in the Device Unreachable state and is now resynchronizing with the network element.
	Device Partially Reachable	The element is not fully reachable because: - At least one protocol is not operational. - All protocols are not operational but the element is still sending syslogs or traps.
	Device Unreachable	No protocols are responding and the element has not sent traps or syslogs in the last three minutes.
	Discovering	The VNE is building the model of the device.
	Maintenance	The VNE is no longer polling the device; therefore, the VNE does not know the device status. This can occur when a user moves the VNE to maintenance mode, or the VNE is using adaptive polling and CPU information is too high.
	Partially Discovered	The VNE model is inconsistent with the device because a required device command failed three times. A common cause of this state is that the device contains in unsupported module.
	Reconciliation	The business 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.
	Shutting Down	The VNE has been stopped or deleted by the user, and the VNE is terminating its connection to the device.
	Unsupported	The device type is not supported by Cisco ANA, specifically because no VNE driver was found for the interface.
	VNE/Agent Unreachable	The VNE is not responding to the gateway. This can occur if the unit or AVM is overutilized or the connection between the gateway and unit or AVM was lost.

Alarm and Ticket Badges

The severity icons in [Table A-9 on page A-9](#) are also used for alarm and ticket badges.



INDEX

Numerics

6VPE, and Cisco ANA [16-2](#)

A

accumulating affected parties

 in an alarm [9-19](#)

 in the correlation tree [9-19](#)

acknowledged tickets [9-5](#)

acknowledging tickets [9-16](#)

activation script, launching [2-7, 2-32, 2-33, 2-36, 4-2](#)

adding

 associated VLANs [12-43](#)

 EFP cross-connects [12-65](#)

 Ethernet services to maps [12-91](#)

 pseudowires to maps [12-77](#)

 unassociated bridges [12-62](#)

 VLANs to maps [12-38](#)

 VPLS instances [12-70](#)

 VPNs to a map [17-7](#)

Advanced tab (tickets) [9-15](#)

affected elements, finding [9-16](#)

Affected Elements window [4-18](#)

affected parties [9-18](#)

 accumulating [9-5, 9-19](#)

 affected pair, viewing reports [9-20](#)

 Affected Parties tab (tickets) [9-11](#)

 calculating [9-19](#)

affected severity, updating over time [9-20](#)

aggregated node

 aggregating devices [4-22](#)

 disaggregating [4-23](#)

renaming [4-23](#)

viewing thumbnail [4-15](#)

aggregating network elements [4-22](#)

aggregation, definition [1-1, 1-2](#)

alarm

 badges [A-13](#)

 customizing [2-39](#)

 disabling on a port [3-12](#)

 enabling on a port [3-12](#)

 severities [9-18](#)

alarm count, definition [2-17](#)

All tab, in Cisco ANA EventVision [8-2](#)

application, launching external [2-7, 2-13, 2-32, 2-33, 2-36, 4-2](#)

applying Ethernet service overlays [12-92](#)

ARP table [17-23](#)

associated VLANs

 adding [12-43](#)

 tag manipulations [12-43](#)

 viewing

 mapping properties [12-44](#)

 service links [12-44](#)

 working with [12-43](#)

association, definition [1-2](#)

ATM cross-connects

 overview [18-4](#)

 properties [18-5](#)

 viewing [18-4](#)

AToM report

 detailed [10-12](#)

 options [10-23](#)

 summary [10-12](#)

audience, intended [xviii](#)

Audit tab

events [8-17](#)in Cisco ANA EventVision [8-3](#)auto refresh, in Cisco ANA EventVision [8-20](#)

B

badge

alarms [2-19, A-13](#)icons [A-11](#)network element [A-12](#)tickets [A-13](#)VNE management state [2-19](#)

BGP

inventory details [17-30](#)viewing [17-30](#)Bidirectional Forwarding Detection (BFD), viewing properties [17-31](#)

bridges

understanding unassociated [12-61](#)viewing properties for VLANs [12-59](#)business configurations [6-5](#)

business element

definition [1-2](#)roles required [6-1](#)

business tag

detaching [6-4](#)roles required [6-1](#)searching for [6-4](#)using Chinese characters [6-2](#)working with [6-3](#)buttons [A-6](#)

Ccallouts, VPN service overlay [17-10](#)Carrier Ethernet services, monitoring [12-1, 13-1](#)

Carrier Grade NAT

roles required for viewing properties [13-1](#)

viewing properties

logical inventory [13-2](#)physical inventory [13-4](#)CC, viewing information for pseudowire endpoint [12-83](#)

CE

disconnecting in maps [17-12](#)displaying and hiding [17-12](#)linking in maps [17-11](#)

CEM groups

configured on physical interfaces [18-41](#)configured on virtual CEM interfaces [18-42](#)viewing [18-41](#)in logical inventory [18-42](#)in physical inventory [18-41](#)

CEM interfaces

properties [18-42](#)viewing [18-40](#)CESoPSN, viewing properties [18-3](#)Chinese character support for business tags [6-2](#)

Circuit Emulation Services over PSN. See CESoPSN

Cisco ANA 3.6.x tabs, in Cisco ANA EventVision [8-11](#)

Cisco ANA Command Builder

launching scripts [2-7, 2-32, 2-33, 2-36, 4-2](#)overview [1-6](#)

Cisco ANA EventVision

All tab [8-2](#)Audit tab [8-3](#)Cisco ANA 3.6.x tabs [8-11](#)customizing [7-8](#)displaying all events [7-4](#)event categories [7-4](#)exporting data [8-24](#)

icons

severities [A-9](#)Ticket Properties dialog box [A-10](#)toolbar [A-10](#)

- launching [7-2](#)
 - menus [7-6](#)
 - overview [1-7](#)
 - Provisioning tab [8-4](#)
 - right-click options [7-7](#)
 - roles required [7-1, 8-1](#)
 - Security tab [8-5](#)
 - Service tab [8-6](#)
 - Syslog tab [8-7](#)
 - System tab [8-5](#)
 - Ticket tab [8-8](#)
 - toolbar [7-5](#)
 - toolbar icons [A-10](#)
 - V1 Trap tab [8-8](#)
 - V2 Trap tab [8-9](#)
 - V3 Trap tab [8-10](#)
 - viewing
 - all events [7-4](#)
 - events and tickets [8-2](#)
 - window [7-3](#)
- Cisco ANA NetworkVision
- adding network elements [4-6](#)
 - customizing [2-39](#)
 - deleting maps [4-13](#)
 - exporting data [2-45](#)
 - generating reports [10-25](#)
 - GUI overview [17-3, 17-4](#)
 - icons [17-4, A-1](#)
 - filtering links [A-6](#)
 - logical inventory [A-7](#)
 - map [A-1](#)
 - physical inventory [A-8](#)
 - table toolbar [A-6](#)
 - toolbar [A-4](#)
 - interface components [2-4](#)
 - links
 - badges [A-4](#)
 - colors [A-3](#)
 - list view toolbar [A-6](#)
 - maps [2-6, 2-39](#)
 - adding network elements [4-6](#)
 - closing [4-5](#)
 - deleting [4-13](#)
 - layout [4-10](#)
 - opening [4-3](#)
 - renaming [4-14](#)
 - resizing elements [4-14](#)
 - saving [4-10](#)
 - saving as an image [4-11](#)
 - saving as new map [4-11](#)
 - saving information [4-10](#)
 - viewing options [4-16](#)
 - menus [2-24](#)
 - Edit [2-25](#)
 - File [2-25](#)
 - Help [2-29](#)
 - Network Inventory [2-28](#)
 - Node [2-26](#)
 - Reports [2-28](#)
 - Tools [2-27](#)
 - View [2-26](#)
 - Window [2-29](#)
 - navigation [2-4](#)
 - opening the inventory window [3-6](#)
 - overlays [17-10](#)
 - overview [1-4](#)
 - port information [17-33](#)
 - properties window [3-3](#)
 - removing network elements [4-9](#)
 - renaming maps [4-14](#)
 - resizing map elements [4-14](#)
 - roles required [2-1, 3-1](#)
 - shortcut menus [2-29](#)
 - starting [2-2](#)
 - tables
 - defining filters [2-43](#)
 - finding text in [2-41](#)
 - managing [2-40](#)

- setting selection filters [2-45](#)
 - sorting [2-42](#)
 - toolbar icons [A-4](#)
 - viewing tickets [9-2](#)
 - VLAN elements and icons [12-34](#)
 - windows [2-4](#)
 - working with tickets [9-1](#)
- Cisco ANA NetworkVision window
- content pane [2-5](#)
 - links view [2-13](#)
 - list view
 - overview [2-10](#)
 - toolbar [2-12, 2-41](#)
 - map view [2-6](#)
 - icons [2-8](#)
 - right-click options [2-7](#)
 - severity indicators [2-10](#)
 - navigation pane [2-5](#)
 - shortcut menus
 - Aggregated Node [2-33](#)
 - Device [2-30](#)
 - Link [2-34](#)
 - Links view [2-36](#)
 - Map [2-33](#)
 - Ticket [2-37](#)
 - ticket pane [2-15](#)
 - toolbar [2-22](#)
 - layout tools [2-23](#)
 - map options [2-22](#)
 - map zoom tools [2-23](#)
 - navigation tools [2-23](#)
 - overlay tools [2-23](#)
 - viewing options [2-22](#)
- Cisco ANA PathTracer
- comparing paths [11-22](#)
 - content pane [11-16](#)
 - counter values, saving [11-21](#)
 - destinations [11-10](#)
 - endpoints [11-25](#)
 - examples of launching [11-7](#)
 - in MPLS networks [11-24](#)
 - launching from an EFP [11-7](#)
 - launching from an Ethernet port [11-11](#)
 - launching from an IP interface [11-8](#)
 - launching from a pseudowire endpoint [11-11](#)
 - launching from a VLAN bridge [11-10](#)
 - layer tabs [11-19](#)
 - menus [11-14, 11-16, 11-18](#)
 - multipath window [11-12, 11-14](#)
 - opening [11-3](#)
 - overview [1-6, 11-1, 11-2](#)
 - paths pane [11-16](#)
 - path trace
 - from inventory [11-7](#)
 - from map view [11-5](#)
 - starting [11-4](#)
 - properties table [11-19](#)
 - rerunning paths [11-22](#)
 - right-click options [11-4](#)
 - roles required [11-2](#)
 - single-path window [11-16, 11-18](#)
 - starting points [11-25](#)
 - tabs [11-15](#)
 - toolbar [11-14, 11-18](#)
 - topological map [11-19](#)
 - viewing Layer 2 Tunnel Protocol path information [11-23](#)
 - viewing path information [11-20](#)
 - viewing QinQ path information [11-22](#)
- Cisco ANA Report Manager overview [1-6](#)
- Cisco ANA Soft Properties Manager overview [1-6](#)
- Cisco ANA vs. Event Archive Statistics report [10-8](#)
- Cisco Discovery Protocol. See CDP
- clearing and removing tickets [9-17](#)
 - clearing tickets [9-5, 9-16](#)
 - clocking service, properties [18-29](#)
 - clock recovery, pseudowire properties [18-37](#)
 - color coding, severity icons [7-4](#)

Command Builder. See Cisco ANA Command Builder

configuration script, launching [2-7, 2-32, 2-33, 2-36, 4-2](#)

Connectivity Fault Management (CFM), viewing properties [15-2](#)

content pane

in Cisco ANA NetworkVision [2-5](#)

in Cisco ANA PathTracer [11-16](#)

in the Cisco ANA NetworkVision inventory window [3-10](#)

tabs in logical inventory [3-17](#)

conventions, used in this document [xix](#)

Correlation tab (tickets) [9-14](#)

CPU usage graph, opening [4-26](#)

creating

maps [4-6](#)

report folders [10-34](#)

VPNs [17-6](#)

cross-connects

overview [18-4](#)

properties [18-5](#)

viewing [18-4](#)

cross-VRF routing entries [17-34](#)

D

Daily Average and Peak report [10-9](#)

Daily Event Count by device report [10-9](#)

defining report types [10-33](#)

deleting

maps [4-13](#)

report folders [10-35](#)

reports [10-30](#)

destination, for Cisco ANA PathTracer [11-10](#)

Detailed Syslog report [10-9](#)

Detailed Traps report [10-9](#)

Details tab

events [8-15](#)

tickets [8-19, 9-9](#)

device

adding to maps [4-6](#)

aggregated nodes [4-22](#)

CPU usage, checking [4-26](#)

finding in maps [4-19](#)

icons [2-6, A-1](#)

in maps [4-16, 4-22](#)

management state [2-19](#)

pinging [4-27](#)

removing from map [4-9](#)

renaming aggregated nodes [4-23](#)

resizing in maps [4-14](#)

severity indicator [2-18](#)

status indicators [2-17](#)

Telnet to a device [4-27](#)

viewing properties [3-2](#)

Devices with the Most Events report

by severity [10-10](#)

by type [10-10](#)

Devices with the Most Syslogs report [10-10](#)

Devices with the Most Traps report [10-10](#)

Device Unreachable management state [2-19](#)

device view pane

in the Cisco ANA NetworkVision inventory window [3-8](#)

toolbar [3-9](#)

disaggregating nodes [4-23](#)

discovery

EFD [12-33](#)

VLAN [12-33](#)

document

audience [xviii](#)

conventions [xix](#)

terminology [1-1](#)

duplication count, definition [2-17](#)

DWDM properties, roles required for viewing properties [14-1](#)

E

EFD discovery [12-33](#)

EFP

launching a path trace [11-7](#)

overview [12-35](#)

understanding severity and ticket badges [12-22](#)

EFP cross-connects

adding [12-65](#)

viewing properties [12-66](#)

working with [12-64](#)

egress adjacents, VRF [17-21](#)

elements, business

deleting [6-5](#)

renaming [6-5](#)

Ethernet flow domains

renaming [12-30](#)

viewing [12-30](#)

Ethernet flow point (EFP), viewing properties [12-20](#)

Ethernet LAG, viewing properties [12-14](#)

Ethernet Link Aggregation Groups (LAGs),
viewing [12-13](#)

Ethernet LMI, viewing properties [15-8](#)

Ethernet Local Management Interface. See Ethernet LMI

Ethernet OAM

overview [15-2](#)

roles required for viewing properties [15-1](#)

Ethernet Operations, Administration, and Maintenance.
See Ethernet OAM

Ethernet port, launching a path trace [11-11](#)

Ethernet Service report

detailed [10-13](#)

options [10-23](#)

summary [10-13](#)

Ethernet services

adding overlays [12-92](#)

adding to maps [12-91](#)

viewing

properties [12-94](#)

working with [12-90](#)

EVC service, viewing properties [12-23](#)

event properties

Audit tab [8-17](#)

Details tab [8-15](#)

Provisioning tab [8-17](#)

Security tab [8-17](#)

Trap tab [8-18](#)

events

categories [7-4](#)

definition [1-2](#)

filtering [8-21](#)

refreshing list in Cisco ANA EventVision [8-20](#)

removing filters [8-24](#)

viewing in Cisco ANA EventVision [8-2](#)

viewing properties [8-14](#)

events reports [10-8](#)

generating from

Cisco ANA NetworkVision [10-25](#)

Report Manager [10-15](#)

Reports menu [10-25](#)

report options [10-16](#)

Run Report dialog box [10-16](#)

EventVision. See Cisco ANA EventVision

exporting

data from Cisco ANA EventVision [8-24](#)

data from Cisco ANA NetworkVision [2-45](#)

external application, launching [2-7, 2-13, 2-32, 2-33, 2-36, 4-2](#)

F

fault management in MPLS networks [15-1](#)

filtering

events [8-21](#)

links

by type [4-24, 4-26](#)

collection method [5-14](#)

- removing for events and tickets [8-24](#)
- tables [2-43, 2-45](#)
- tickets [8-21](#)
 - by criteria [9-6](#)
 - by device [9-5](#)
- flickering links [5-2](#)

G

- generated ticket [9-4](#)

H

- History tab (tickets) [9-10](#)
- H-VPLS, working with [12-69](#)

I

- icon
 - badges [A-11](#)
 - alarm and ticket [A-13](#)
 - network element [A-12](#)
- Cisco ANA EventVision
 - Auto Refresh [8-20](#)
 - Refresh Now [8-20](#)
 - Ticket Properties dialog box [A-10](#)
 - toolbar [A-10](#)
- Cisco ANA NetworkVision [A-1](#)
 - links [A-6](#)
 - map view [2-8](#)
 - table toolbar [A-6](#)
 - toolbar [A-4](#)
- devices [2-6, A-1](#)
- logical inventory [3-15, A-7](#)
- management states [2-19, A-11](#)
- maps [17-4](#)
- map view, in Cisco ANA NetworkVision [2-8](#)
- physical inventory [3-10, A-8](#)

- reference [A-1](#)
- REP [12-52](#)
- Report Manager toolbar [A-11](#)
- severities [A-9](#)
- severity, color coding [2-18, 7-4](#)
- tickets [2-22](#)
- VLAN domains [12-52](#)
- VLAN overlays [12-52](#)

- IMA, viewing group properties [18-7](#)

- impact analysis
 - accumulating affected parties [9-19](#)
 - affected pair report [9-20](#)
 - affected severities [9-18](#)
 - automatic mode [9-18](#)
 - disabling [9-20](#)
 - links and [5-10](#)
 - proactive mode [9-18](#)

- Initializing management state [2-19](#)

- inventory reports [10-11](#)
 - generating from
 - Cisco ANA NetworkVision [10-25](#)
 - Report Manager [10-19](#)
 - Reports menu [10-25](#)
 - report options [10-20](#)
 - Run Report dialog box [10-20](#)

- inventory window
 - content pane [3-10](#)
 - device view pane [3-8](#)
 - device view pane toolbar [3-9](#)
 - logical inventory [3-13](#)
 - navigation pane [3-8](#)
 - opening [3-6](#)
 - options
 - Disable Sending Alarms button [3-11](#)
 - Open Port Utilization Graph button [3-11](#)
 - Show Cross-Connect Table button [3-11](#)
 - Show DLCI Table button [3-11](#)
 - Show Encapsulation button [3-11](#)
 - Show VC Table button [3-11](#)

overview [3-6, 3-7](#)

physical inventory [3-10, 3-11](#)

ticket pane [3-9](#)

IP interface, launching a path trace [11-8](#)

IP SLA, viewing responder service properties [12-97](#)

IPv6, VPN over MPLS [16-1](#)

IS-IS, viewing properties [12-98](#)

K

keyboard shortcuts, for tables [2-41](#)

L

Layer 2 Cisco ANA PathTracer (VPN) [11-26](#)

Layer 3 Cisco ANA PathTracer (VPN) [11-26](#)

layer tabs, in Cisco ANA PathTracer [11-19](#)

LCA

creating [17-15](#)

deleting [17-16](#)

moving [17-15](#)

LCP

adjacent [17-16](#)

disconnecting in map [17-12](#)

displaying or hiding CE [17-12](#)

linking in map [17-11](#)

moving [17-16](#)

LDP Neighbors tab [17-29](#)

link

adding [5-12](#)

arrowheads [5-3](#)

bidirectional vs. unidirectional [5-3](#)

colors [5-3](#)

creating [17-11](#)

dashed line [5-3](#)

definition [1-2](#)

disconnecting [17-12](#)

dynamic [5-2](#)

filtering [A-6](#)

by type [4-24, 4-26](#)

collection method [5-14](#)

in maps [4-24](#)

finding in maps [4-18](#)

flickering [5-2](#)

impact analysis [5-10](#)

links view in Cisco ANA NetworkVision [5-5](#)

overview [5-1](#)

properties [5-3](#)

selecting in maps [4-18, 5-14](#)

solid line [5-3](#)

static [5-2](#)

tooltips [5-4](#)

user roles required for working with [5-1](#)

viewing

between VLAN elements and devices [12-46](#)

options [5-14](#)

properties [5-3, 5-7](#)

Link Layer Discovery Protocol, viewing properties [12-5](#)

Link OAM

overview [15-12](#)

viewing properties [15-12](#)

Link Properties window

link list pane [5-8](#)

overview [5-7](#)

properties pane [5-9](#)

links view

filtering [2-15, A-6](#)

in Cisco ANA NetworkVision [2-13](#)

information displayed [2-14](#)

list view

in Cisco ANA NetworkVision [2-10](#)

overview [2-10](#)

toolbar [2-12, 2-41, A-6](#)

LLDP, viewing properties [12-5](#)

logical inventory

branches [3-14](#)

content pane [3-17](#)

- content pane tabs [3-17](#)
- icons [3-15](#), [A-7](#)
- navigation pane [3-14](#)
- tabs [3-17](#)
- viewing in Cisco ANA NetworkVision [3-13](#)
- window [3-13](#)
- logical link, definition [1-2](#)
- LSE
 - inventory details [17-27](#)
 - Label Switching Table tab [17-27](#)
 - MPLS Interfaces tab [17-27](#)
 - viewing [17-27](#)

M

- Maintenance management state [2-19](#)
- managed element, definition [1-2](#)
- management state
 - icons [A-11](#)
 - overview [2-19](#)
- managing maps, roles required [4-2](#)
- managing report folders
 - creating [10-34](#)
 - deleting [10-35](#)
 - moving [10-34](#)
 - renaming [10-35](#)
 - viewing properties [10-36](#)
- managing reports
 - deleting [10-30](#)
 - moving reports [10-30](#)
 - renaming [10-28](#)
 - roles required [10-1](#)
 - saving [10-27](#)
 - sharing [10-29](#)
 - viewing [10-27](#)
 - viewing report properties [10-31](#)
- managing tickets [9-15](#)

- managing VPNs [17-6](#)
 - adding to maps [17-7](#)
 - creating [17-6](#)
 - moving virtual routers between [17-8](#)
 - overlays
 - adding [17-9](#)
 - displaying [17-10](#)
 - hiding [17-10](#)
 - removing from maps [17-8](#)
- map
 - adding network elements [4-6](#)
 - adding VLANs [12-38](#)
 - aggregated nodes [4-22](#)
 - CE devices [17-12](#)
 - Cisco ANA PathTracer files [11-20](#)
 - closing [4-5](#)
 - creating [4-6](#)
 - creating links [17-11](#)
 - customizing [2-39](#)
 - deleting [4-13](#)
 - devices in [4-16](#), [4-19](#), [4-22](#)
 - disconnecting links [17-12](#)
 - filtering links [4-24](#)
 - finding
 - affected elements [4-17](#)
 - links in maps [4-18](#)
 - in Cisco ANA NetworkVision [2-6](#)
 - layouts [4-10](#)
 - opening [4-3](#)
 - any map [4-4](#)
 - commonly used [4-3](#)
 - options [4-4](#)
 - overlays
 - callouts [17-10](#)
 - VPN [17-9](#)
 - overview [17-3](#), [17-4](#)
 - previewing before printing [4-27](#)
 - printing [4-27](#)
 - print setup [4-28](#)

- removing
 - devices [4-9](#)
 - VLANs [12-41](#)
 - VPNs [17-8](#)
 - renaming [4-14](#)
 - renaming aggregated nodes [4-23](#)
 - roles required [4-2](#)
 - saving [4-10](#)
 - as an image [4-11](#)
 - as new map [4-11](#)
 - with information [4-10](#)
 - selecting views [4-16](#)
 - viewing
 - network [4-15](#)
 - network overview [4-15](#)
 - thumbnail [4-15](#)
 - VPNs
 - adding [17-7](#)
 - overlays [17-9](#)
 - viewing [17-3](#)
 - map view
 - adding VLAN overlays [12-49](#)
 - in Cisco ANA NetworkVision [2-6](#)
 - menus
 - Cisco ANA EventVision [7-6](#)
 - Cisco ANA NetworkVision [2-24](#)
 - Cisco ANA PathTracer [11-14, 11-16, 11-18](#)
 - Report Manager [10-3](#)
 - monitoring Carrier Ethernet services [12-1, 13-1](#)
 - Most Common Daily Events report [10-10](#)
 - Most Common Syslogs report [10-10](#)
 - moving
 - report folders [10-34](#)
 - reports between folders [10-30](#)
 - MP-BGP. See BGP
 - MPLS
 - ARP table [17-23](#)
 - BGP, viewing [17-30](#)
 - Cisco ANA PathTracer and [11-24](#)
 - LSEs, viewing [17-27](#)
 - monitoring services [17-17](#)
 - NDP table [17-24](#)
 - PWE3s, viewing [17-35](#)
 - rate limit information [17-26](#)
 - roles required for viewing properties [17-1](#)
 - routing entities [17-22](#)
 - TE tunnels, viewing [17-36](#)
 - MPLS pseudowire over GRE, properties [18-26](#)
 - MPLS TE tunnel, inventory details [17-36](#)
 - MTOP, roles required for working with [18-1](#)
-
- ## N
- navigation pane
 - Cisco ANA NetworkVision [2-5](#)
 - logical inventory [3-14](#)
 - physical inventory [3-10](#)
 - NDP table [17-24](#)
 - network
 - finding devices [4-19](#)
 - viewing devices [4-16](#)
 - viewing maps [4-15](#)
 - network clocking service
 - clock service properties [18-29](#)
 - monitoring [18-28](#)
 - monitoring PTP service [18-30](#)
 - overview [18-28](#)
 - PTP interface properties [18-31](#)
 - PTP service [18-30](#)
 - network element
 - adding to maps [4-6](#)
 - aggregating [4-22](#)
 - definition [1-2](#)
 - icon badges [A-12](#)
 - removing from maps [4-9](#)
 - resizing in maps [4-14](#)

network service reports [10-12](#)
 generating from
 Cisco ANA NetworkVision [10-25](#)
 Report Manager [10-22](#)
 Reports menu [10-25](#)
 report options [10-23](#)
 Run Report dialog box [10-22](#)
 NetworkVision. See Cisco ANA NetworkVision
 Notes tab (tickets) [9-15](#)

O

obtaining documentation [xx](#)
 Open Map dialog box options [4-4](#)
 Operational management state [2-19](#)
 options, opening maps [4-4](#)
 OSPF
 supported versions [12-101](#)
 viewing properties [12-101](#)
 overlays
 applying [4-20](#)
 to VLAN [12-49](#)
 applying to
 pseudowire [12-85](#)
 displaying and hiding
 for VLANs [12-51](#)
 for VPNs [17-10](#)
 Ethernet service [12-92](#)
 hiding [4-22](#)
 pseudowire [12-77, 12-85](#)
 removing [4-22, 12-51](#)
 viewing [4-22](#)
 pseudowire tunnel links in VPLS [12-73](#)
 REP information [12-52](#)
 STP
 information [12-54](#)
 VLAN
 adding [12-49](#)
 removing [12-51](#)

 viewing STP link information [12-55](#)
 working with [12-33](#)
 VPLS callouts [12-74](#)
 VPLS instance [12-71](#)
 VPN [17-9](#)
 adding [17-9](#)
 callouts [17-10](#)
 working with [4-19](#)
 overview
 Cisco ANA Command Builder [1-6](#)
 Cisco ANA EventVision [1-7](#)
 Cisco ANA NetworkVision [1-4](#)
 Cisco ANA NetworkVision inventory window [3-6](#)
 Cisco ANA PathTracer [1-6, 11-1](#)
 Cisco ANA Report Manager [1-6](#)
 Cisco ANA Soft Properties Manager [1-6](#)
 cross-connects [18-4](#)
 EFPs [12-35](#)
 network clocking service [18-28](#)
 reports [10-1](#)
 SAToP [18-2](#)
 switching entities [12-34](#)
 unassociated bridges [12-61](#)
 VLANs [12-34](#)

P

Partially Supported management state [2-19](#)
 parties, accumulating affected [9-5](#)
 password, changing [2-38](#)
 paths pane, in Cisco ANA PathTracer [11-16](#)
 path trace
 launching examples [11-7](#)
 launching from
 an EFP [11-7](#)
 an Ethernet port [11-11](#)
 an IP interface [11-8](#)
 a pseudowire endpoint [11-11](#)
 a VLAN bridge [11-10](#)

- starting [11-4](#)
 - from inventory [11-7](#)
 - from map view [11-5](#)
- viewing
 - Layer 2 Tunnel Protocol path information [11-23](#)
 - path information [11-20](#)
 - QinQ path information [11-22](#)
- path trace information, viewing in Cisco ANA PathTracer [11-20](#)
- PathTracer. See Cisco ANA PathTracer
- permissions, security [1-3](#)
- physical inventory
 - branches [3-10](#)
 - buttons
 - Disable Sending Alarms [3-11](#)
 - Open Port Utilization Graph [3-11](#)
 - Show Encapsulation [3-11](#)
 - content pane [3-11](#)
 - icons [3-10](#), [A-8](#)
 - navigation pane [3-10](#)
 - viewing device properties [3-10](#)
 - viewing in Cisco ANA NetworkVision [3-10](#)
 - window [3-9](#)
- physical link, definition [1-2](#)
- pinging
 - devices [4-27](#)
 - pseudowires [12-80](#)
- ports
 - alarms
 - disabling [3-12](#)
 - enabling [3-12](#)
 - viewing configuration [17-33](#)
 - with IPv4 and IPv6 addresses [16-3](#)
- Port Utilization graph, opening [3-11](#)
- printing maps [4-27](#)
- properties
 - CEM interface [18-42](#)
 - clock service [18-29](#)
 - MPLS pseudowire over GRE [18-26](#)
 - pseudowire clock recovery [18-37](#)
 - PTP interface [18-31](#)
 - report folders [10-36](#)
 - report types [10-37](#)
 - SBC [19-3](#)
 - AAA [19-6](#)
 - DBE [19-4](#)
 - H.248 [19-5](#), [19-7](#)
 - media address [19-4](#)
 - policy [19-7](#)
 - SBE [19-5](#)
 - SIP [19-11](#)
 - TDM-specific [18-11](#)
 - properties table, in Cisco ANA PathTracer [11-19](#)
 - properties window in Cisco ANA NetworkVision [3-3](#)
 - provider, definition [1-2](#)
 - Provider Backbone Bridge (PBB), viewing properties [12-19](#)
 - provisioning route targets, roles required [16-1](#)
 - Provisioning tab, in Cisco ANA EventVision [8-4](#)
 - pseudowire
 - viewing
 - tunnel links in VPLS overlays [12-73](#)
 - pseudowire clock recovery
 - overview [18-33](#)
 - properties [18-37](#)
 - viewing properties [18-33](#)
 - pseudowire endpoint, launching a path trace [11-11](#)
 - pseudowires
 - adding to maps [12-77](#)
 - applying overlay [12-85](#)
 - overlays [12-77](#)
 - pinging [12-80](#)
 - viewing
 - endpoint properties [12-27](#)
 - VCCV and CC information [12-83](#)
 - viewing properties [12-86](#)
 - working with [12-77](#)

PTP

- interface properties [18-31](#)
- monitoring service [18-30](#)

PWE3

- inventory details [17-35](#)
- viewing [17-35](#)

R

rate limits, for routing entities [17-26](#)

reduction count, definition [2-17](#)

related documentation [iii-xx](#)

removing

- tickets [9-17](#)
- VLAN overlays [12-51](#)
- VLANs from maps [12-41](#)
- VPNs [17-8](#)

renaming

- Ethernet flow domains [12-30](#)
- maps [4-14](#)
- report folders [10-35](#)
- reports [10-28](#)

REP

- icons and badges [12-52](#)
- viewing
 - for VLAN service link properties [12-53](#)
 - in VLAN domain views [12-52](#)
- viewing in
 - VLAN overlays [12-52](#)

report categories [10-8](#)

report folders

- creating [10-34](#)
- deleting [10-35](#)
- moving [10-34](#)
- renaming [10-35](#)
- viewing properties [10-36](#)
- working with [10-33](#)

Report Manager

- content pane [10-5](#)
- events reports [10-8](#)
- generating reports [10-15](#)
- inventory reports [10-11](#)
- menu options [10-3](#)
- navigation tree [10-4](#)
- network service reports [10-12](#)
- overview [1-6](#)
- report categories [10-8](#)
- right-click options [10-6](#)
- roles required [10-1](#)
- toolbar icons [10-4, A-11](#)
- using [10-2](#)

report properties, viewing [10-31](#)

reports

- creating folders [10-34](#)
- defining types [10-33](#)
- deleting
 - folders [10-35](#)
 - reports [10-30](#)

events

- Cisco ANA vs. Event Archive Statistics [10-8](#)
- Daily Average and Peak [10-9](#)
- Detailed Event Count (by device) [10-9](#)
- Detailed Syslog [10-9](#)
- Detailed Traps [10-9](#)
- Devices with the Most Events by severity [10-10](#)
- Devices with the Most Events by type [10-10](#)
- Devices with the Most Syslogs [10-10](#)
- Devices with the Most Traps [10-10](#)
- Most Common Daily Events [10-10](#)
- Most Common Syslogs [10-10](#)
- Syslog Count by device [10-11](#)
- Syslog Count by type [10-11](#)
- Syslog Trend by severity [10-11](#)

formats [10-27](#)

- generating [10-14](#)
 - events reports [10-15](#)
 - inventory reports [10-19](#)
 - network service reports [10-22](#)
- generating from
 - Cisco ANA NetworkVision [10-25](#)
 - Report Manager [10-15](#)
 - Reports menu [10-25](#)
- inventory
 - Software Version Summary by device [10-11](#)
 - Software Version Summary by version [10-11](#)
- limiting access to [10-30](#)
- managing [10-26](#)
- moving between folders [10-30](#)
- moving folders [10-34](#)
- network service
 - AToM Detailed [10-12](#)
 - AToM Summary [10-12](#)
 - Ethernet Service Detailed [10-13](#)
 - Ethernet Service Summary [10-13](#)
 - VPLS Detailed [10-14](#)
 - VPLS Summary [10-14](#)
- options for
 - events reports [10-16](#)
 - inventory reports [10-20](#)
 - network service reports [10-23](#)
- overview [10-1](#)
- renaming
 - folders [10-35](#)
 - reports [10-28](#)
- Report Properties dialog box [10-32](#)
- roles required [10-1](#)
- saving [10-27](#)
- sharing [10-29](#)
- using Report Manager [10-2](#)
- viewing [10-27](#)
 - report folder properties [10-36](#)
 - report type properties [10-37](#)
- viewing properties [10-31](#)
 - working with folders [10-33](#)
- Reports menu, and generating reports [10-25](#)
- report types, viewing properties [10-37](#)
- Resilient Ethernet Protocol (REP), viewing properties [12-13](#)
- right-click options
 - Cisco ANA EventVision [7-7](#)
 - Cisco ANA NetworkVision [2-7](#)
 - Cisco ANA PathTracer [11-4](#)
 - Report Manager [10-6](#)
- roles
 - managing reports [10-1](#)
 - security [1-3](#)
 - viewing
 - Carrier Ethernet properties [12-2](#)
 - Carrier Grade NAT properties [13-1](#)
 - DWDM properties [14-1](#)
 - Ethernet OAM tool properties [15-1](#)
 - IPv6 properties [16-1](#)
 - working with
 - business tags [6-1](#)
 - Cisco ANA EventVision [7-1, 8-1](#)
 - Cisco ANA NetworkVision [2-1, 3-1](#)
 - Cisco ANA PathTracer [11-2](#)
 - maps [4-2](#)
 - MPLS networks [17-1](#)
 - MToP [18-1](#)
 - tickets [9-1](#)
- routing entities [17-22](#)
 - ARP table [17-23](#)
 - NDP table [17-24](#)
- rate limit information [17-26](#)
- viewing properties [17-22](#)

S

SAToP, overview [18-2](#)

saving

maps [4-10](#)

reports [10-27](#)

SBC

AAA properties [19-6](#)

DBE properties [19-4](#)

H.248 properties [19-5, 19-7](#)

logical inventory properties [19-1](#)

media address properties [19-4](#)

policy properties [19-7](#)

properties [19-3](#)

SBE properties [19-5](#)

SIP properties [19-11](#)

user roles required for viewing properties [19-2](#)

viewing in logical inventory [19-2](#)

scopes, and security [1-3](#)

scripts

launching [2-7, 2-32, 2-33, 2-36](#)

launching (activation and configuration) [4-2](#)

security

permissions [1-3](#)

roles [1-3](#)

scopes [1-3](#)

Security tab, in Cisco ANA EventVision [8-5](#)

selecting links in maps [4-18](#)

Service tab, in Cisco ANA EventVision [8-6](#)

service view

LCAs [17-15, 17-16](#)

LCPs [17-16](#)

overlays [17-10](#)

removing VLANs [12-41](#)

removing VPNs [17-8](#)

tunnels [17-13, 17-14](#)

virtual routers [17-8](#)

VPNs [17-6, 17-17](#)

Session Border Controller. See SBC [19-1](#)

severity

color of device icon [2-19](#)

icons [A-9](#)

propagation [2-18](#)

severity indicators

in Cisco ANA NetworkVision map view [2-10](#)

overview [2-18](#)

sharing reports [10-29](#)

shortcut menus, in Cisco ANA NetworkVision [2-29](#)

sites

disconnecting in map [17-12](#)

displaying or hiding CD [17-12](#)

linking in map [17-11](#)

properties, viewing [17-17](#)

Soft Properties Manager. See Cisco ANA Soft Properties Manager

Software Version Summary report

by device [10-11](#)

by version [10-11](#)

Spanning Tree Protocol (STP), viewing properties [12-7](#)

static link, adding [5-12](#)

STP

viewing

in VLAN domain views [12-54](#)

in VLAN overlays [12-54](#)

link information in VLAN overlay [12-55](#)

VLAN service link properties [12-56](#)

Structure-Agnostic TDM over Packet. See SAToP

submitting a service request [xx](#)

subscriber, definition [1-2](#)

switching entities

containing termination points [12-38](#)

overview [12-34](#)

Syslog Count report

by device [10-11](#)

by type [10-11](#)

Syslog tab, in Cisco ANA EventVision [8-7](#)

Syslog Trend report by severity [10-11](#)

System tab, in Cisco ANA EventVision [8-5](#)

T

- table
 - filtering [2-43](#)
 - finding text in [2-41](#)
 - keyboard shortcuts for [2-41](#)
 - managing in Cisco ANA NetworkVision [2-40](#)
 - sorting [2-42](#)
 - toolbar icons [A-6](#)
- tabs, in Cisco ANA PathTracer window [11-15](#)
- tag manipulations, for associated VLANs [12-43](#)
- TDM-specific properties [18-11](#)
- Telnet to devices [4-27](#)
- termination points, in switching entities [12-38](#)
- terminology in this document [1-1](#)
- TE tunnels and Cisco ANA PathTracer [11-27](#)
- ticket pane
 - Cisco ANA NetworkVision [2-15](#)
 - Cisco ANA NetworkVision inventory window [3-9](#)
 - information displayed [2-16](#)
- ticket properties, Details tab [8-19](#)
- Ticket Properties dialog box
 - Advanced tab [9-15](#)
 - Affected Parties tab [9-11](#)
 - Correlation tab [9-14](#)
 - Details tab [9-9](#)
 - History tab [9-10](#)
 - Notes tab [9-15](#)
 - toolbar [9-9](#)
- tickets
 - acknowledging [9-5, 9-16](#)
 - and EFP severities [12-22](#)
 - badges [A-13](#)
 - clearing [9-5, 9-16](#)
 - clearing and removing [9-17](#)
 - definition [1-3](#)
 - filtering [8-21](#)
 - by criteria [9-6](#)
 - by device [9-5](#)
 - finding affected elements [9-16](#)
 - finding affected elements in map [4-17](#)
 - generated [9-4](#)
 - icons [2-22](#)
 - managing [9-15](#)
 - propagating new [2-18](#)
 - properties [9-7](#)
 - removing [9-17](#)
 - removing filters [8-24](#)
 - roles required [9-1](#)
 - status [9-4](#)
 - viewing in Cisco ANA EventVision [8-2](#)
 - viewing in Cisco ANA NetworkVision [9-2](#)
 - viewing properties [9-9](#)
 - working with in Cisco ANA NetworkVision [9-1](#)
- Ticket tab, in Cisco ANA EventVision [8-8](#)
- toolbar
 - Cisco ANA EventVision [7-5](#)
 - Cisco ANA NetworkVision [2-22](#)
 - Cisco ANA NetworkVision list view [2-12, 2-41, A-6](#)
 - Cisco ANA PathTracer [11-14, 11-18](#)
 - Report Manager [10-4](#)
 - Ticket Properties window [9-9](#)
- toolbar icons
 - Cisco ANA PathTracer multipath window [11-14](#)
 - Cisco ANA PathTracer single-path window [11-18](#)
 - Report Manager [10-4, A-11](#)
 - Ticket Properties window [9-9](#)
- tooltip, links [5-4](#)
- topological map, in Cisco ANA PathTracer [11-19](#)
- Traffic Engineering LSPs tab [17-28](#)
- Trap tab (events) [8-18](#)
- tunnels, adding [17-13, 17-14](#)

U

unassociated bridges

- adding [12-62](#)
- overview [12-61](#)

understanding

- EFP severity and ticket badges [12-22](#)
- Ethernet Connectivity Fault Management [15-2](#)
- static and dynamic links [5-2](#)
- unassociated bridges [12-61](#)

Unknown management state [2-19](#)

unmanaged network, definition [1-3](#)

Unsupported management state [2-19](#)

updating affected severity [9-20](#)

Up ticket [9-5](#)

user roles

- viewing SBC properties [19-2](#)
- working with links [5-1](#)

V

V1 Trap tab, in Cisco ANA EventVision [8-8](#)

V2 Trap tab, in Cisco ANA EventVision [8-9](#)

V3 Trap tab, in Cisco ANA EventVision [8-10](#)

VCCV, viewing information for pseudowire endpoint [12-83](#)

viewing

- BFD properties [17-31](#)
- Carrier Ethernet properties, roles required [12-2](#)
- Carrier Grade NAT properties [13-2, 13-4](#)
- CEM groups [18-41](#)
- CEM interfaces [18-40](#)
- device properties [3-2](#)
- EFP cross-connect properties [12-66](#)
- EFP properties [12-20](#)
- Ethernet flow domains [12-30](#)
- Ethernet LAG properties [12-14](#)

Ethernet LAGs [12-13](#)

Ethernet Link Aggregation Groups [12-13](#)

Ethernet LMI properties [15-8](#)

Ethernet services properties [12-94](#)

EVC service properties [12-23](#)

IMA group properties [18-7](#)

IP SLA responder service properties [12-97](#)

IPv6 properties, roles required [16-1](#)

IS-IS properties [12-98](#)

Layer 2 Tunnel Protocol path trace [11-23](#)

Link Layer Discovery Protocol (LLDP) properties [12-5](#)

Link Layer Discovery Protocol properties [12-5](#)

link properties [5-7](#)

links between VLAN elements and devices [12-46](#)

LLDP properties [12-5](#)

LSE properties [17-27](#)

MPLS TE tunnel information [17-36](#)

OSPF properties [12-101](#)

PBB properties [12-19](#)

port configuration information [17-33](#)

pseudowire

- endpoint properties [12-27](#)
- properties [12-86](#)
- VCCV and CC information [12-83](#)

PWE3 tunnel information [17-35](#)

QinQ path trace [11-22](#)

REP information in

- VLAN domain views [12-52](#)
- VLAN overlays [12-52](#)

report folder properties [10-36](#)

report properties [10-31](#)

reports [10-27](#)

report type properties [10-37](#)

REP properties [12-13](#)

REP properties for VLAN service links [12-53](#)

routing entities [17-22](#)

SBC properties in logical inventory [19-2](#)

- STP
 - information in VLAN domain views [12-54](#)
 - properties [12-7](#)
 - properties for VLAN service links [12-56](#)
- STP information in VLAN overlays [12-54](#)
- ticket properties [8-18](#)
- tickets in Cisco ANA NetworkVision [9-2](#)
- Virtual Switching Instance properties [12-25](#)
- VLAN
 - bridge properties [12-59](#)
 - mapping properties [12-44](#)
 - mappings [12-41](#)
 - service link properties [12-52](#)
 - trunk group properties [12-57](#)
- VNE properties [3-4](#)
- VPLS
 - access Ethernet EFP properties [12-29](#)
 - instance properties [12-75](#)
 - properties [12-75](#)
- VPN
 - properties [17-17](#)
 - site properties [17-17](#)
- VRF properties [17-18](#)
- VSI properties [12-25](#)
- viewing cross-VRF routing entries [17-34](#)
- virtual CEMs, listing [18-41](#)
- virtual cloud, definition [1-3](#)
- Virtual Private Network. See VPN
- virtual routers
 - moving [17-8](#)
 - properties, viewing [17-18](#)
 - VRF tables [17-21](#)
- Virtual Switching Instance (VSI), viewing properties [12-25](#)
- VLAN
 - adding associated VLANs [12-43](#)
 - adding to map view [12-38](#)
 - associations [12-43](#)
 - definition [1-3](#)
 - discovery [12-33](#)
 - elements
 - EFPs [12-35](#)
 - icons in Cisco ANA NetworkVision [12-34](#)
 - network VLAN [12-34](#)
 - overview [12-34](#)
 - switching entities [12-34](#)
 - overlays
 - STP link information [12-55](#)
 - viewing REP information [12-52](#)
 - viewing STP information [12-54](#)
 - overview [12-34](#)
 - removing from map [12-41](#)
 - removing overlay [12-51](#)
 - tag manipulations for associations [12-43](#)
 - viewing
 - associated VLAN mapping properties [12-44](#)
 - associated VLAN service links [12-44](#)
 - bridge properties [12-59](#)
 - links between elements and devices [12-46](#)
 - mappings [12-41](#)
 - REP properties [12-53](#)
 - service link properties [12-52](#)
 - STP properties [12-56](#)
- VLAN bridge
 - launching a path trace [11-10](#)
- VLAN overlays
 - adding to maps [12-49](#)
 - working with [12-33](#)
- VLANs
 - working with [12-33](#)
- VLAN trunk group, viewing properties [12-57](#)
- VNEs, viewing properties [3-4](#)
- VNE Unreachable management state [2-19](#)
- VPLS
 - adding instances to maps [12-70](#)
 - overlays
 - link callout [12-74](#)
 - viewing pseudowire tunnel links [12-73](#)

- viewing
 - access Ethernet EFP properties [12-29](#)
 - instance properties [12-75](#)
 - properties [12-75](#)

- working with [12-69](#)

VPLS core, viewing pseudowire endpoint properties [12-27](#)

VPLS forward, viewing pseudowire endpoint properties [12-27](#)

VPLS instance overlays [12-71](#)

VPLS report

- detailed [10-14](#)
- options [10-24](#)
- summary [10-14](#)

VPNs

- adding to maps [17-7](#)
- and LCAs [17-15](#), [17-16](#)
- and LCPs [17-16](#)
- and tunnels [17-13](#), [17-14](#)
- and virtual routers [17-8](#)
- creating [17-6](#)
- managing [17-6](#)
- moving virtual routers between [17-8](#)
- overlays [17-9](#)
 - callouts [17-10](#)
 - creating [17-9](#)
 - displaying [17-10](#)
 - hiding [17-10](#)
- properties, viewing [17-17](#)
- removing from maps [17-8](#)
- sites [17-17](#)
- viewing in maps [17-3](#)
- virtual routers [17-18](#)

VRFs

- cross-VRF routing entries [17-34](#)
- tables
 - egress [17-21](#)
 - ingress [17-21](#)

- viewing properties [17-18](#)

- VRF tab [17-29](#)

- with IPv4 and IPv6 addresses [16-4](#)

VSI, viewing properties [12-25](#)

W

working with

- associated VLANs [12-43](#)
- business elements [6-1](#)
- business tags [6-1](#)
- EFP cross-connects [12-64](#)
- Ethernet services [12-90](#)
- H-VPLS [12-69](#)
- links, user roles required [5-1](#)
- overlays [4-19](#)
- pseudowire overlays [12-77](#)
- pseudowires [12-77](#)
- tickets in Cisco ANA NetworkVision [9-1](#)
- VLAN overlays [12-33](#)
- VLANs [12-33](#)
- VPLS [12-69](#)

