



Cisco Active Network Abstraction Managing MPLS User's Guide, 3.5

Corporate 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: 408 526-4100

Text Part Number: OL-8845-01



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

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

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

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

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

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0601R)

Important Notice

Cisco ANA 3.5 is a carrier-class, multi-vendor network and service management platform which builds a real-time virtual model of the network, serving as a live information base for value-added tools and applications for integration into an existing OSS environment.

Cisco ANA 3.5 is a limited release by Cisco Systems of the existing features and functions of the Sheer DNA 4.0.1 software.

As this is a limited release, the naming of the product in the software and the user documentation remains as Sheer DNA.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

Emergencies — security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

Nonemergencies — psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

1 877 228-7302

1 408 525-6532

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the Tools & Resources link under Documentation & Tools. Choose Cisco Product Identification Tool from the Alphabetical Index drop-down list, or click the Cisco Product Identification Tool link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting show command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

- Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
- EMEA: +32 2 704 55 55
- USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

- Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.
- Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.
- Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

Cisco Press publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

Packet magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

iQ Magazine is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqumagazine>

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

About This Guide

This User's Guide describes the tools included in Sheer NetworkVision used in monitoring network-based environments, specifically in MPLS networks and MPLS-based VPN services. In addition, it describes logical inventory information specific to VPNs, fault management, service impact analysis, MPLS-TE, and Sheer DNA's Multi-path tracing capability using the Sheer PathTracer tool. Network administrators and anyone else, responsible for the assurance, fulfillment, planning, and management of the integrity of network resources should use this user's guide.

The current release supports Layer 3 VPN Services (based on the BGP/MPLS VPN as defined in RFC2547); Layer 2 VPN Services (as defined by the Martini draft); and MPLS-TE (Traffic Engineering) support (based on RFC 2702 with RSVP for signaling as described in RFC 3209).

It includes the following chapters:

Chapter 1: Introducing MPLS VPN Maps, provides an introduction to the NetworkVision Service View, Sheer Business elements, and multi-path maps.

Chapter 2: Creating and Manipulating VPN MPLS Maps, describes how to change *Service View* maps by adding and removing VPNs, connecting CE devices and creating aggregations.

Chapter 3: Creating and Manipulating Sheer Business Configuration, describes how to change the business configuration using the functionality provided in the Service View map.

Chapter 4: Viewing VPN Properties in Service View, describes viewing the properties of the various business elements, including overlays and callouts on top of the devices displayed in physical Network maps.

Chapter 5: Viewing MPLS Related Inventory Properties, describes how to view general logical inventory information in the Service View, and describes the VPN specific items that are displayed in the *Inventory* window, including tunnel information.

Chapter 6: Fault Management in MPLS Networks, describes the alarms that Sheer DNA detects and reports for BGP, MPLS TE (using RSVP TE), MPLS Black Holes, as well as alarm reports for Layer 2 and Layer 3 VPNs.

Chapter 7: Calculating Impact Analysis, provides an overview of the impact analysis solution and supported scenarios. In addition, it describes calculating and viewing the VPN affected and potentially affected parties in the network.

Chapter 8:

Working with PathTracer in VPN Service View, describes using the Sheer PathTracer for viewing Layer 2 and Layer 3 VPN information, and working with multi-path routes.

Appendix A: Running a VPN Leak Report Command, describes running a VPN Leak report command.

Appendix B: Additional Alarms, briefly describes the additional alarms that can be supported by Sheer DNA.

Note: Changes to the Registry should only be carried out with the support of Cisco Professional Services.

List of Supported Technologies

The following technologies are supported:

- **MPLS:** Supports MPLS networks.
- **BGP:** Supports BGP technology, including, route reflector scenarios.
- **L3 VPN (2547):** Supports Layer 3 VPN Services (based on the BGP/MPLS VPN as defined in RFC2547).
- **Pseudo Wire End-to-End Emulation Tunnels (PWE3 and Martini tunnels):** Supports PWE3 as defined in RFC3985, the implementation was done for Cisco AToM (Any Transport over MPLS). PWE3 is based on the Luca Martini drafts (draft-martini-l2circuit-encap-mpls-03.txt, draft-martini-l2circuit-trans-mpls-07.txt). Note that currently we only support the payload types “packet” and “cell”. For more information, refer to RFC3985 *Section 3.3*.
- **MPLS Traffic Engineering:** Support is based on RFC 2702 with RSVP for signaling as described in RFC 3209.

Related Documentation

For more detailed information, refer to the following publication:

- *Cisco Active Network Abstraction NetworkVision User's Guide*
- *Cisco Active Network Abstraction Administrator's Guide*
- *Cisco Active Network Abstraction Fault Management Guide*

Table of Contents

1	Introducing MPLS VPN Maps.....	1
1.1	Introducing VPN MPLS Maps	1
1.2	Introducing the Sheer Business Configuration	2
1.2.1	Layer 3 VPN Business Configuration	3
1.2.2	Layer 2 VPN Business Configuration and Tunnels	4
1.3	VPN Topology Connections	4
1.4	VPN Service View Map.....	6
1.4.1	Tree Pane	8
1.4.2	Map Pane	10
1.4.3	Ticket Pane.....	10
2	Creating and Manipulating VPN MPLS Maps	11
2.1	Adding a VPN.....	11
2.2	Removing a VPN from the Map.....	13
2.3	Connecting a CE Device	14
2.4	Disconnecting a CE Device.....	15
2.5	Displaying and Hiding a CE Device.....	15
2.6	Creating an Aggregation	16
2.7	Disaggregating a Node	17
3	Creating and Manipulating Sheer Business Configuration	19
3.1	Creating a VPN.....	20
3.2	Moving a Virtual Router	21
3.3	Adding a Tunnel	21
3.4	Creating a LCA.....	23
3.5	Deleting a LCA	24
3.6	Moving a LCP	25
3.7	Moving a LCA.....	25
3.8	Jumping to the Adjacent LCP	25
3.9	Renaming a Business Element	26
3.10	Deleting a Business Element	26

4	Viewing VPN Properties in Service View	29
4.1	Viewing VPN Properties.....	29
4.2	Viewing Site Properties	30
4.3	Viewing a Virtual Router's Properties	31
4.3.1	Opening the VRF Table.....	34
4.3.2	Displaying the VRF Egress/Ingress Adjacents.....	34
4.4	Viewing VRF Properties in the Inventory Window	35
4.4.1	Viewing Cross VRF Routing Entries.....	37
4.5	Working with the VPN Service Overlay	38
4.5.1	Selecting an Overlay.....	39
4.5.2	Displaying or Hiding Overlays	39
4.5.3	Displaying or Hiding Callouts.....	40
5	Viewing MPLS Related Inventory Properties	43
5.1	Introduction.....	43
5.2	Opening the Inventory Window	44
5.3	Viewing Routing Entities	46
5.3.1	Viewing the ARP Table.....	48
5.4	Viewing Port Configuration	49
5.5	Viewing LSEs	50
5.6	Viewing MP BGP Information.....	52
5.6.1	Viewing BGP Neighbors	53
5.7	Viewing VRF Information.....	54
5.7.1	Opening the VRF Table.....	57
5.7.2	Viewing Cross VRF Routing Entries.....	58
5.8	Viewing Pseudo Wire End-to End Emulation (PWE3) Tunnels.....	60
5.9	Viewing MPLS TE Tunnel Information.....	61
5.9.1	Traffic Engineering LSPs.....	63

6	Fault Management in MPLS Networks	65
6.1	MPLS Related Faults	66
6.1.1	MPLS Black Hole Found Alarm	66
6.1.2	Broken LSP Discovered Alarm	67
6.1.3	Black Hole to Link Down	68
6.2	BGP Related Faults	68
6.2.1	BGP Neighbor Down	69
6.3	Traffic Engineering Faults	69
6.3.1	MPLS TE Tunnel Down and TE Tunnel Flapping	69
6.3.2	Tunnel Reoptimized	70
6.4	Layer 2 VPN Faults	70
6.4.1	Pseudo Wire (L2 VPN) MPLS Tunnel Down	70
6.5	Alarms Summary	71
7	Calculating Impact Analysis	73
7.1	About Service Impact Analysis	73
7.1.1	Automatic Impact Analysis	73
7.1.2	Proactive Impact Analysis	74
7.2	Service Impact Analysis for MPLS Based VPN Services	75
7.2.1	L3 VPN Report (VRFs as Affected)	75
7.2.2	Pseudo Wire (L2 VPN) Report (PWE3 Tunnels as Affected)	76
7.3	Supported Fault Scenarios	76
7.3.1	Link Down	77
7.3.2	Link Over Utilized / Data Loss	77
7.3.3	BGP Neighbor Down	78
7.3.4	Broken LSP Discovered	81
7.3.5	MPLS TE Tunnel Down	81
7.3.6	Pseudo Wire (L2 VPN) MPLS Tunnel Down	81

8	Working with PathTracer in VPN Service View	83
8.1	Sheer PathTracer Tracing Capability	84
8.2	Opening Sheer PathTracer Over MPLS Networks	85
8.3	Sheer PathTracer Windows.....	86
8.4	Using PathTracer for Layer 3 VPN.....	89
8.4.1	Viewing Layer 3 Path Information.....	89
8.5	Using PathTracer for Layer 2 VPN.....	91
8.5.1	Viewing Layer 2 Path Information.....	91
8.6	Using PathTracer for MPLS Traffic Engineering Tunnels.....	92
8.6.1	Viewing MPLS TE Tunnel Information.....	93
A	Running a VPN Leak Report Command.....	97
A.1	Syntax.....	97
A.2	Output.....	97
A.3	Examples.....	97
A.3.1	Get the VPN Leak Report.....	97
A.4	VPN Leak Report Results	98
A.4.1	IVPNLeakReport.....	98
A.4.2	IVpnLeak	98
B	Additional Alarms	99

1 Introducing MPLS VPN Maps

About this chapter:

This chapter provides an introduction to the Service View, business configuration and Service View maps.

Introducing VPN MPLS Maps, page 1, describes Service View maps, including the concepts of VPN topology.

Introducing the Sheer Business Configuration, page 2, provides an introduction to the Layer 2 and Layer 3 VPN business configuration, including, the business elements available.

VPN Topology Connections, page 4, describes viewing the Layer 2 and Layer 3 VPN topology in maps.

VPN Service View Map, page 6, briefly describes the Service View map that is displayed in the *Sheer NetworkVision* window.

For a more detailed description of the *Sheer NetworkVision* window, menus, and toolbars, and working with tables, refer to the *Cisco Active Network Abstraction NetworkVision User's Guide*.

1.1 Introducing VPN MPLS Maps

Sheer DNA automatically discovers VPN services and provides a view of their configuration and topology (*Service View* map), in addition to discovering the physical and logical inventory of the devices (Network maps). Multiple maps may exist in the Sheer DNA system.

The VPNs that are discovered and displayed in Service View maps enable the user to drill down into specific VPNs and view information about the business elements contained in each VPN. For more information, refer to *Section 1.2*.

Note: Network maps are used to display devices. Service View maps are used to display VPNs; in addition devices can now also be displayed in Service View maps and vice-versa. For more information about Network maps, refer to the *Cisco Active Network Abstraction NetworkVision User's Guide*.

Sheer DNA has the capability to automatically determine the different Layer 3 VPNs in the network and their associated Virtual Routers. For more information, refer to *Section 1.2.1*.

After creating a *Service View* map the user can, for example:

- Add and/or remove VPNs that have been automatically discovered by the system based on the automatically discovered information from the network.
- View *business element* properties.
- Select and move LCPs and LCAs

The *Service View* also enables the user to:

- View VPN logical topology, namely, understanding the connectivity between sites.
- View VPN topology.
- Select and display an *overlay* of a specific VPN on top of the devices in the map.
- View logical inventory.
- Add tunnels to a *Service View* map and view **PWE3** and MPLS TE (Traffic Engineering) tunnel information in the *Inventory* window properties tabs.
- View the active faults and tickets that are generated by Sheer DNA for the devices present in the map. For more information, refer to *Chapter 6, Fault Management in MPLS Networks*.
- Identify extranets.

1.2 Introducing the Sheer Business Configuration

Sheer DNA supports the mapping of service-related information to the network resources. This mapping is achieved using a *business element* that is a *wrapper* to a Network Element or service.

The *VPN* is a business element, which represents a set of interconnected Sites forming a single virtual private network over a public network. Sites can be inter-connected either over VRF or through a collection of PWE3 tunnels that relate to one customer.

Sheer organizes the business elements in a way that creates a containment hierarchy that reflects the VPN structure. For more information about the Layer 3 VPN hierarchy, refer to *Section 1.2.1* and for more information about the Layer 2 VPN hierarchy, refer to *Section 1.2.2*.

Business elements are available via the Northbound interface as well as in Sheer NetworkVision.

Any changes that are made to the business configuration are reflected in all maps. For example, if a link is removed this change will be reflected in all of the maps.

1.2.1 Layer 3 VPN Business Configuration

The following business elements are used to represent the Layer 3 VPN configuration:

- **Site (IP Interface):** Represents the VPN access point on the provider edge.
- **Virtual Router:** Represents a VRF in the provider edge.

The Layer 3 VPN configuration hierarchy is composed of VPN business elements that in turn contain multiple *Virtual Routers* and *Sites*. The relationship between the contents of VPNs and Virtual Routers can be changed, for example, by moving a Virtual Router between VPNs, which causes each Site connected to the moved Virtual Router to move as well. The relationship between Virtual Routers and Sites cannot be changed; as Sites are automatically attached to Virtual Routers (Sites cannot be moved on their own).

In the Layer 3 VPN configuration the VPNs are created and named automatically and new Virtual Routers are automatically detected. The Virtual Router is then automatically related or matched to the VPN based on the VRF name. If there is no related or matching VPN, then a new VPN is automatically created and a VRF is assigned to it. The user can then add these VPNs to a map. The user can manually change the auto-discovered service information, for example, by manually creating new VPNs, by deleting empty VPNs, or by renaming VPNs and so on.

Sheer DNA can use different criteria in order to determine the different Layer 3 VPNs in the network and their associated Virtual Routers. By default, Sheer DNA uses the most intuitive criterion – the VRF name in order to deduce the VPNs on the network.

It is possible to change this criterion to fit specific environments through Sheer's professional services, and it can be modified to reflect virtually any criteria. A common change is to identify VPNs by specific Route Distinguisher (RD) bits.

1.2.2 Layer 2 VPN Business Configuration and Tunnels

In Layer 2 VPN there is no automatic creation of VPNs. You can create the VPNs and then add the tunnels. The following business elements are used to represent the Layer 2 VPN configuration:

- **Logical Circuit Peer (LCP):** Represents a Layer 2 tunnel edge that resides on a single device. A pair of LCPs represents both sides of the tunnel edge.

Note: A tunnel can only be associated with one VPN.

- **Logical Circuit Aggregator (LCA):** Represents an aggregation of LCPs on the same device.

LCAs can be manually or automatically created:

- **Automatically:** When a LCP is added to the VPN system, the system automatically creates the LCA by taking all of the LCPs that belong to the same device and aggregating them into a LCA (the LCPs are automatically added under the LCA).
- **Manually:** A LCA that is manually created by the user on a specific VPN has no rules, and is the preparatory step for adding tunnels and/or stranded peers.

For more information about creating LCAs, refer to page 23.



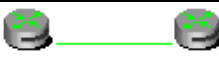
1.3 VPN Topology Connections

Sheer uses route targets (based on the router configuration) to determine the topology between VRFs. Layer 3 VPN topology information is continuously updated to reflect the actual state of the network connections.

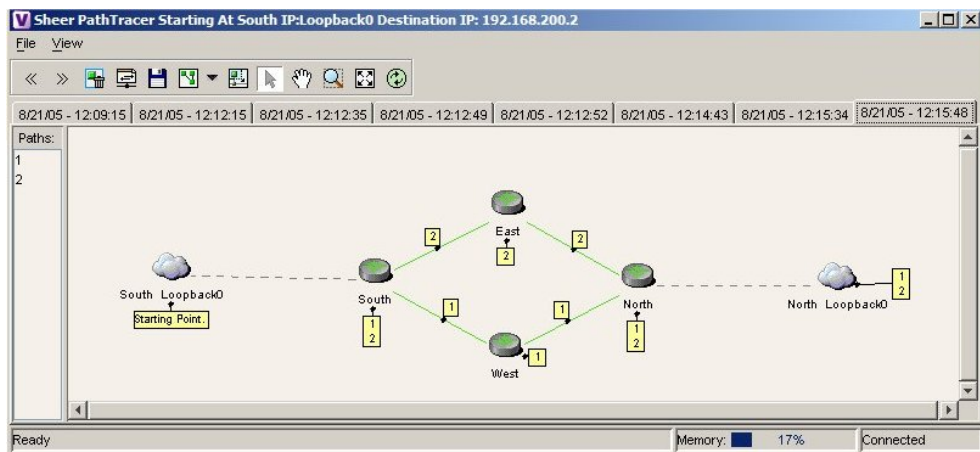
Sheer uses the VC ID and the Router IP address (based on the router configuration) to determine the connectivity between the Layer 2 tunnel edges forming the **PWE3** tunnels.

The current version reflects the actual state of the tunnel (up/down) for the logical link in Layer 2 topology (if it has already been discovered). The link is displayed with a minor severity (yellow) on the map when the tunnel is down.

The different kinds of topology that may be displayed on the *Service View* map are described in the following tables:


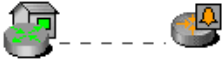

Topology Example	Description
	<ul style="list-style-type: none"> • Topology between VPNs (extranet). • Displayed by means of a solid line with arrows at either end.
	<ul style="list-style-type: none"> • VPN topology between Virtual Routers. • Displayed by means of a solid line with arrows at either end.
	<ul style="list-style-type: none"> • Tunnel between LCPs. • Displayed by means of a solid line. • The link does not reflect a status.

The example below displays several devices that are connected in a multi-path VPN MPLS map in the *Sheer PathTracer Multi-Path* window:



For more information about the icons displayed in the maps of the *Sheer NetworkVision* window, refer to page 8.

In addition to the topology described previously, the associations described in the table below may also be displayed on the *Service View* map:

Association Example	Description
	<ul style="list-style-type: none"> • Symbolizes the association between the customer Site (IP interface) and the access point on the Provider Edge (PE). • Displayed by means of a broken dark gray line.
	<ul style="list-style-type: none"> • Symbolizes the overall connection between the CE device and the Site (IP interface), which may cross different technologies and layers. • Displayed by means of a broken dark gray line.
	<ul style="list-style-type: none"> • Symbolizes the overall connection between the CE device and the LCP. • Displayed by means of a broken dark gray line.

1.4 VPN Service View Map

Sheer DNA automatically discovers VPN services and provides a view of their configuration and topology (*VPN Service View* map), in addition to discovering the physical and logical inventory of the devices (Network maps).

Layer 3 VPN Service View Map

The Service View map presents existing Layer 3 VPNs in the network. At the top-level, the user can see inter-VPN (Extranet) connections. Drilling down into each VPN presents the Service View map, with the following:

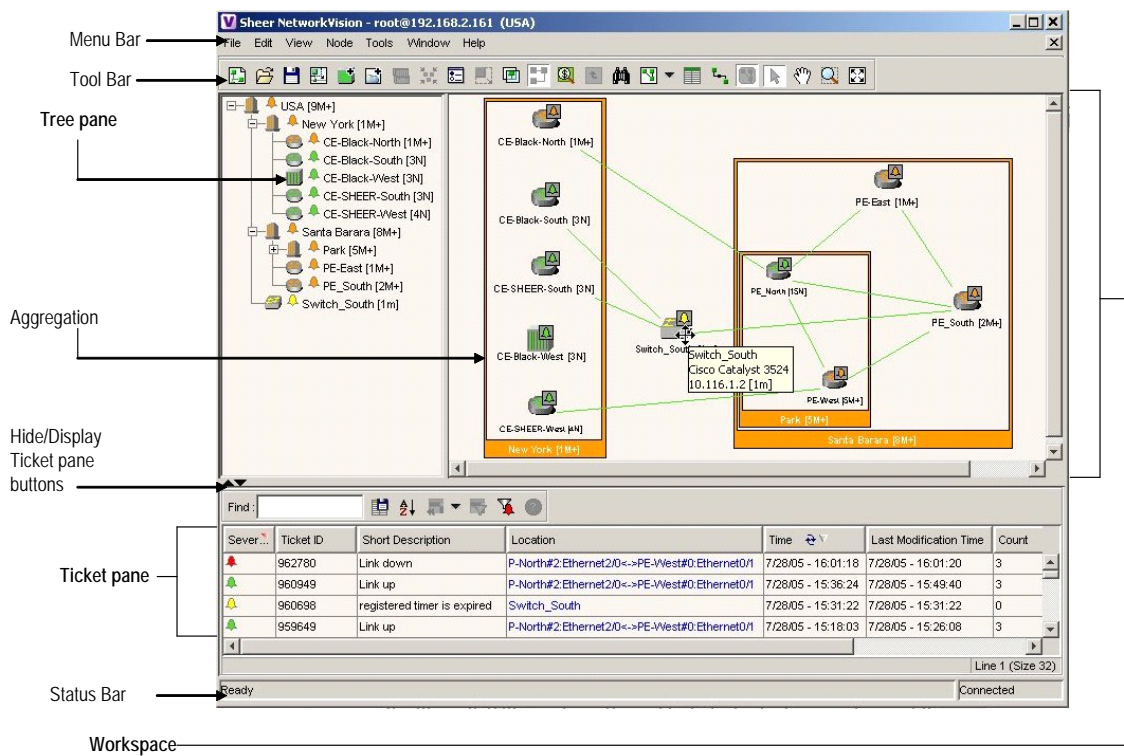
- Participating Virtual Routers and their association with Site entities.
- Site entities and their association Customer Edge (CE) devices.
- Connections between Virtual Routers and their topology (for example, Mesh, Hub, Spoke and so on).

Layer 2 VPN Service View Map

For Layer 2 VPNs the Service View map presents existing Layer 2 VPNs in the network. At the top-level, the user can see inter-VPN (Extranet) associations. Drilling down into each VPN presents the Service View map, with the following:

- Connections between LCPs.
- Connections between LCPs and CEs.
- LCAs containing LCPs.

An example of the *Sheer NetworkVision* window with an open Service View map is displayed below.



The *Sheer NetworkVision* window is divided into three areas or panes, as follows:

- The *Tree* pane, as described on page 8.
- The *Workspace*, which includes the *Map* pane (as described on page 10), *Device View* and *Links View*. For more information about the *Device View* and *Links View*, refer to the *Cisco Active Network Abstraction User's Guide*.
- The *Ticket* pane, as described on page 10.

For a general description of the *Sheer NetworkVision* window, menus and toolbar, refer to the *Cisco Active Network Abstraction NetworkVision User's Guide*.

















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

1.4.1 Tree Pane

The *Tree* pane displays the business configuration for the VPN business elements, as described previously, in a tree-and-branch representation.





Each business element is displayed using an icon that has a color that reflects its severity and may have a management state icon or alarm. For more information, refer to the *Cisco Active Network Abstraction NetworkVision User's Guide*.

The following icons are used in the *Tree* and *Map* panes:

Tree pane	Map pane	Represents
		Root (map name) or aggregation
		VPN business element
		Virtual Router business element
		Site business element
		Site business element with an actively associated CE device and where the device is hidden
		Logical Circuit Aggregator (LCA) business element
		Logical Circuit Peer (LCP) business element
		LCP business element with an actively assigned tunnel edge for the CE device and where the device is hidden

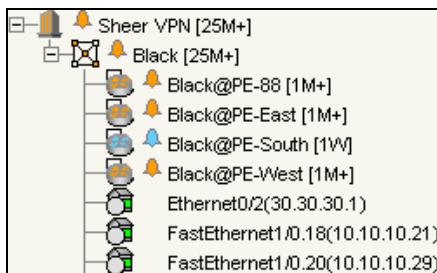
Note: Network Element icons can also be displayed in the *Tree* pane and *Map* pane. For more information about network element icons, refer to the *Cisco Active Network Abstraction NetworkVision User's Guide*.

In addition, the following management state icons are also used in *Service View* maps:

Tree Pane	Map Pane	Description
		The reconciliation icon. The network element wrapped by this business element does not exist, for example, the device configuration has changed. Network problem.
		The neighboring LCP does not exist or was not discovered. Stranded.

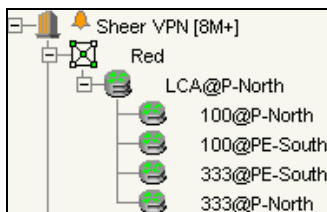
The highest level of the *Tree* pane displays the root or map name. The branches display the VPN and aggregated business elements as well as their names.

The Layer 3 VPN sub-branches display the Virtual Routers and Sites contained in the VPN along with the names of the business elements as displayed in the example below:



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 as displayed in the example below:



In addition, CE devices can also be displayed in the Layer 2 VPN sub-branches.

When an aggregated business element is selected in the *Tree* pane, the *Map* pane displays the business elements contained within the aggregated business element.

1.4.2 Map Pane

The *Map* pane displays the VPN business elements and aggregated business elements loaded in the Service View map along with the names of the business elements. In addition, the *Map* pane displays the VPN topology (between the Virtual Routers in the VPNs) and the topology and associations between other business elements, as described on page 4.

When the root is selected in the *Tree* pane the Service View map displays all of the VPNs.

1.4.3 Ticket Pane

When Sheer DNA presents tickets related to the map, these tickets are displayed in the *Ticket* pane enabling the user to view and manage the VPN tickets that have been generated by Sheer DNA. For more information about the alarms that Sheer DNA detects and reports for Layer 2 and Layer 3 VPNs, refer to *Chapter 6, Fault Management in MPLS Networks*.

For more information about the *Ticket* pane, refer to the *Cisco Active Network Abstraction NetworkVision User's Guide*.

In addition, the user can calculate the affected parties. For more information, refer to the *Cisco Active Network Abstraction NetworkVision User's Guide*

Note: Only when a device or logical part of the device is added to the Service View map are the tickets of that device displayed in the *Ticket* pane, for example, the link or port down ticket.

2 Creating and Manipulating VPN MPLS Maps

About this chapter:

This chapter describes how to change Service View maps by adding and removing VPNs, connecting CE devices and creating aggregations.

Adding a VPN, page 11, describes how to add a VPN to the currently displayed Service View map.

Removing a VPN from the Map, page 13, describes how to change the Service View map by removing a VPN from the currently active map.

Connecting a CE Device, page 14, describes how to connect a CE device to its respective Sites or LCPs.

Disconnecting a CE Device, page 15, describes how to disconnect a CE device.

Displaying and Hiding a CE Device, page 15, describes how to display and hide the CE device on the Service View map.

Creating an Aggregation, page 16, describes how to aggregate business elements according to a logical hierarchy.

Disaggregating a Node, page 17, describes how to disaggregate an aggregated node.


2.1 Adding a VPN


The user can change the Service View map by adding VPNs that have not yet been loaded to the currently displayed map.

Note: Adding VPNs will affect other users if they are working with the same Service View map.

To add an existing VPN

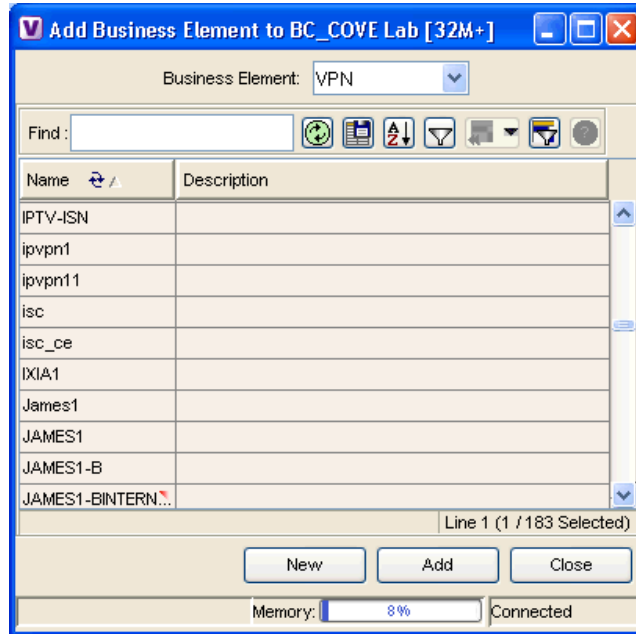
1. Select the root of the map in the *Sheer NetworkVision* window's *Tree* pane.

Note: The **Add VPN** option is only enabled when the root  icon is selected in the *Tree* pane of the Service View map.

2. In the toolbar, click  **Add VPN**.

or

Select **Add VPN** from the *File* menu. The *Add Business Element to <Root>* dialog box is displayed.





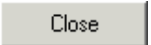
The *Add Business Element to <Root>* dialog box displays a list of:

- The VPNs that have been automatically discovered by Sheer DNA and/or
- The VPNs manually created by the user and not yet loaded in the map

The *Add Business Element to <Root>* dialog box displays the following columns:

- **Name:** The name of the VPN business element.
- **Description:** An additional description of the VPN business element.

The *Add Business Element to <Root>* dialog box displays the following buttons:

Button	Function
	Opens the <i>Create Business Element</i> dialog box, which enables the user to create a new VPN business element. The newly created VPN is displayed in the <i>Add Business Element to <Root></i> dialog box. For more information, refer to <i>Section 3.1</i> .
	Loads the selected VPN in the currently displayed Service View map. The VPN is displayed in the <i>Tree</i> pane and <i>Map</i> pane.
	Closes the <i>Add Business Element to <Root></i> dialog box.

3. Select the required VPN in the table.
4. Click **Add**. The VPN is loaded in the Service View map displayed in the *Sheer NetworkVision* window's *Map* pane in the *Workspace*.
5. Click **Close** to close the *Add Business Element to <Root>* dialog box.

2.2 Removing a VPN from the Map

The user can change the Service View map by removing a VPN from the currently active map (this change does not affect other maps). When a VPN is removed from the map, it still exists in the database. The VPN is displayed in the *Add Business Element to <Root>* dialog box table again so that it may be added back to the map at any time.

Note: This option does not change the business configuration or database.

In addition, the user can select and remove multiple VPNs from the map.

Note: Virtual routers, Sites, LCAs and LCPs cannot be removed from the map without removing the VPN.

To remove a VPN

1. Right-click on the required VPN in the *Sheer NetworkVision* window's *Tree* pane or *Map* pane to display the shortcut menu.
2. Select **Remove from Map**. The selected VPN is removed from the Service View map and displayed again in the *Add Business Element to <Root>* dialog box.

Note: Removing a VPN will affect other users if they are working with the same Service View map.

Note: When the **Remove from Map** option is selected for a VPN, this removes all of the VPN elements from the map, including connected CE devices within the VPN, but excluding remote VPNs (extranets).

2.3 Connecting a CE Device


The connect CE functionality enables the user to create a symbolic link to the overall connection between the CE device and the Site (IP interface) or LCPs. The CE device belongs to the currently displayed map only.

To connect a CE device

1. To add a CE device to a Site, select the required VPN in the *Sheer NetworkVision* window's *Tree* pane or *Map* pane,

or

To add a CE device to a LCP, select the required LCA.

2. In the toolbar, click  **Add Device**,

or

Select **Add Device** from the *File* menu. The *Device List* dialog box is displayed.

For more information, refer to the *Cisco Active Network Abstraction NetworkVision User's Guide*.

3. From the Device List, select the device that you want to add.
4. Click **Add Device**. The device is displayed in the *Tree* pane and the selected map or sub-network in the *Sheer NetworkVision* window's *Workspace*.

Note: The tickets of the device will only be displayed in the *Ticket* pane of the *Sheer NetworkVision* window's *Workspace* when the device is added to the VPN Service View map, for example, the ticket for link or port down.

5. Click **Close** to close the *Device List* dialog box.
6. Right-click on the required Site or LCP in the *Tree* pane or *Map* pane to display the shortcut menu and select **Topology | Connect CE Device**.
7. Right-click on the device in the *Tree* pane or *Map* pane to display the shortcut menu and select **Topology | Connect to Site/LCP** (where Site or LCP displays the details of the Site or LCP to be connected).

8. The Site or LCP is connected to the CE device and the CE device is displayed in the *Tree* pane and *Map* pane. A broken dark gray line is used to indicate the association in the *Map* pane of the *Sheer NetworkVision* window's *Workspace*.

Note: The menu option **Topology | Connect to Site/LCP** is only available after **Topology | Connect CE Device** has been selected from the menu.

2.4 Disconnecting a CE Device

A CE device can be disconnected from its respective Sites or LCPs.

To disconnect a CE device

- Right-click on the required CE device or link in the *Map* pane of the *Sheer NetworkVision* window's *Workspace* to display the shortcut menu and select **Topology | Disconnect CE Device**.



The association with the CE device is no longer displayed in the *Map* pane.

For more information about displaying and/or hiding the CE device, refer to *Section 2.5*.

2.5 Displaying and Hiding a CE Device

The user can display the CE device for a Site and/or LCP in the *Sheer NetworkVision* window's *Tree* pane and *Map* pane, as well as their associations on the Service View map, at any time after the CE has been connected.

To display a connected device

1. Select a Site in the *Map* pane displaying the icon .
or
Select a LCP in the *Map* pane displaying the icon .
2. Right-click on the Site or LCP to display the shortcut menu and select **Show CE Devices**. The connected devices are displayed in the *Tree* pane and *Map* pane including the associations.



The user can also manually add connected devices (some or all of them) in order to view them along with the links to Sites and/or LCPs.

The user can hide the CE device for a Site and/or LCP in the *Tree* pane and *Map* pane as well as their associations, so that they are no longer displayed on the Service View map.

To hide a connected device

1. Select the Site or LCP in the *Sheer NetworkVision* window's *Tree* pane or *Map* pane connected to the CE device.
2. Right-click on the Site or LCP to display the shortcut menu and select **Hide Connected Devices**. The connected CE devices are hidden in the *Tree* pane and *Map* pane.

The following icons are displayed:

	Site where there is at least one hidden connected device
	LCP where there is at least one hidden connected device

The user can also manually remove the connected devices (some or all of them) in order to hide them along with the links to Sites and/or LCPs.


2.6 Creating an Aggregation

The user can aggregate elements, for example, aggregate Sites or aggregate Sites and Virtual Routers.

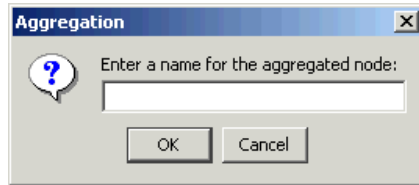
To create an aggregation

1. Select the required business elements in the *Sheer NetworkVision* window's *Tree* pane or *Map* pane using <Ctrl> and/or the selection tool.

Note: The **Aggregate** option is only enabled when the business elements have been selected.

2. In the *Sheer NetworkVision* window's toolbar, click  **Aggregate**,
or
Select **Aggregate** from the *Node* menu.
or
Right-click on the required business elements in the *Tree* pane or *Map* pane to display the shortcut menu and select **Aggregate**.

The *Aggregation* dialog box is displayed prompting you to type a name for the aggregated node.



3. Type a unique name for the aggregated node and click **OK**. The aggregated node is displayed in the *Sheer NetworkVision* window's *Tree* pane and *Map* pane. Aggregated nodes are displayed as a single entity with the following icon:



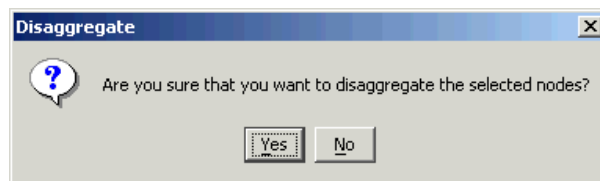
2.7 Disaggregating a Node

The aggregated node selected in the *Sheer NetworkVision* window's *Tree* pane or *Map* pane can be disaggregated.

To disaggregate a node

1. Select the required branch in the *Tree* pane,
or
Select the required aggregated node in the *Map* pane.
2. Select **Disaggregate** from the *Node* menu,
or
Right-click on the aggregated node to display the shortcut menu and select **Disaggregate**.

The following message is displayed:



3. Click **Yes**. The node is disaggregated.

3 Creating and Manipulating Sheer Business Configuration

About this chapter:

This chapter describes how to change the business element configuration using the functionality provided in the *Service View* map. For more information about the business configuration, refer to page 2.

Note: All of the operations described in this chapter have the affect of rearranging the map and do not affect other maps.

Creating a VPN, page 20, describes how to manually create VPNs.

Moving a Virtual Router, page 21, describes how to move a Virtual Router (including its Sites) from one VPN to another.

Adding a Tunnel, page 21, describes how to add tunnels to a VPN.

Creating a LCA, page 23, describes how manually create a LCA.

Deleting a LCA, page 24, describes how to delete a LCA.

Moving a LCP, page 25, describes how to move a LCP to another VPN or LCA.

Moving a LCA, page 25, describes how to move the LCA to another VPN.

Jumping to the Adjacent LCP, page 25, describes how to jump from one peer to the adjacent peer.

Renaming a Business Element, page 26, describes how to rename business elements from the business model.

Deleting a Business Element, page 26, describes how to delete business elements from the business model.

Note: The LCA/LCP operations, like moving is an operation that logically moves the business element from one VPN to another (so all maps that contain the same VPN are automatically affected). A move operation that is performed inside the same VPN has the affect of rearranging the map and does not affect other maps. This also applies to the LCA/LCP operations adding and deleting.

3.1 Creating a VPN

The user can change the business configuration by manually creating VPNs. The VPNs that are manually created do not contain Virtual Routers and Sites.

To create a VPN

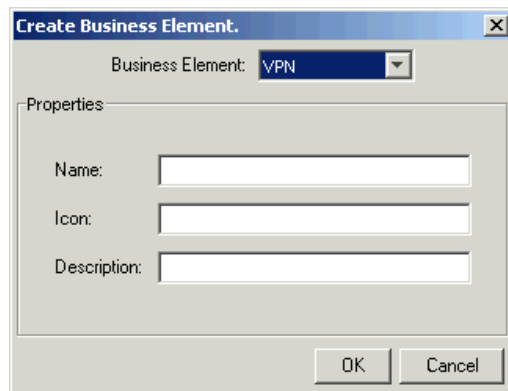
1. Select the root of the map in the *Sheer NetworkVision* window's *Tree* pane.

2. In the toolbar, click  **Add VPN**.

or

Select **Add VPN** from the *File* menu. The *Add Business Element to <Root>* dialog box is displayed.

3. Click **New**. The *Create Business Element* dialog box is displayed.



The following fields are displayed in the *Create Business Element* dialog box:


- **Name:** The unique name of the new VPN business element.
- **Icon:** The path to the icon on the Server.
- **Description:** An additional description of the VPN business element (optional).

4. Type a unique name for the new VPN business element in the **Name** field.

Important Note: VPN business element names are case-sensitive.

Note: For information about renaming a VPN, refer to the section *Renaming an Aggregated Node* in the *Cisco Active Network Abstraction NetworkVision User's Guide*.

5. Specify the path to the required icon (optional).

Note: If a path is not specified to an icon the default VPN icon  is used.

6. Type a description for the new VPN business element (optional).
7. Click **OK**. The new VPN business element is added to the list in the *Add Business Element to <Root>* dialog box.

For more information about loading the newly created VPN business element in the Service View map, refer to *Section 2.1*.

3.2 Moving a Virtual Router

The user can move a Virtual Router (including its Sites) from one VPN to another after a VPN has been created and added to the Service View map.

Note: Moving a Virtual Router moves all of the Virtual Router's Sites as well.


To move a Virtual Router

1. Select the required Virtual Router that you want to move in the *Sheer NetworkVision* window's *Tree* pane or the *Map* pane.
2. Right-click to display the shortcut menu and select **Edit | Move selected**.
3. Select the required VPN in the *Tree* pane or the *Map* pane to where you want to move the Virtual Router.

Warning! When a Virtual Router is moved from one VPN to another it affects all users that have the Virtual Router loaded in their Service View map.

4. Right-click to display the shortcut menu and select **Edit | Move here**. The Virtual Router (including its Sites) is now displayed under the selected VPN in the *Tree* pane and in the *Map* pane.

3.3 Adding a Tunnel

The user can add tunnels and/or partially configured tunnels to a VPN. LCPs with a missing peer are marked with the icon . Each tunnel can only be associated with one VPN.

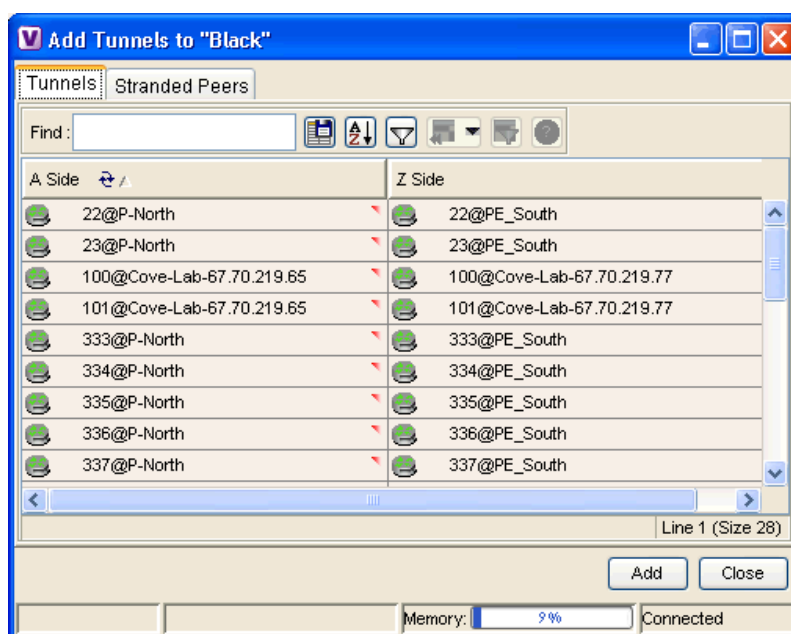
Note: The state of the topology between LCPs does not reflect the actual state of the network; it is only a logical link.

The user can either:

- Add a tunnel (LCP) to a LCA that has been manually created (for more information about manually creating a LCA, refer to page 23),
or
- Add a tunnel (LCP) directly to a VPN in which case the LCA is automatically created beneath the VPN.

To add a tunnel

1. Right-click on the required LCA or VPN in then *Sheer NetworkVision* window's *Tree* pane or *Map* pane to display the shortcut menu.
2. Select **Topology | Add Tunnel**. The *Add Tunnels* dialog box is displayed.



The *Add Tunnels* dialog box displays only those tunnels that are not currently attached to a VPN. It is divided into the **Tunnels** and **Stranded Peers** tabs. The **Tunnels** tab displays the list of **PWE3** tunnels (including both tunnel edges).

The **Stranded Peers** tab displays the list of partially configured tunnel edges. The *Add Tunnels* dialog box enables the user to add a LCP without its peer, for example, when there is a half-managed tunnel or an Agent that fails to load or a device that has been incorrectly configured.

3. Select the required tunnel or stranded peer and click **Add**.
 - If the tunnel or stranded peer is added beneath a LCA, the link between the peers is displayed in the *Map* pane.
 - If the tunnel or stranded peer is added beneath a VPN, Sheer DNA detects the starting point of the **PWE3** tunnel edges and groups all of the LCPs that start at the same device automatically together into a LCA (aggregation) beneath the VPN.

Note: If a tunnel exists between VPNs (namely, an extranet tunnel) add a tunnel to one VPN and then move one LCP (peer) to the VPN with which you want to create the extranet tunnel.

The user can remove a tunnel that was added to a LCA or VPN.

To remove a tunnel

1. Right-click on the required LCP in the in the *Sheer NetworkVision* window's *Tree* pane or *Map* to display the shortcut menu.
2. Select **Topology | Remove Tunnel**. Both sides of the tunnel are removed from the Service View map and are displayed in the *Add Tunnels* dialog box again.

If the deleted tunnel formed part of a LCA that was created manually, the LCA is still displayed in the *Tree* pane or *Map* pane.

If the deleted tunnel formed part of a LCA that was created automatically the LCA is removed from the *Tree* pane or *Map* pane, provided that there are no other LCPs in the LCA.

Note: MPLS TE Tunnels cannot be viewed in VPN Service View maps however; you can view device and topology information. For more information, page 61.

3.4 Creating a LCA

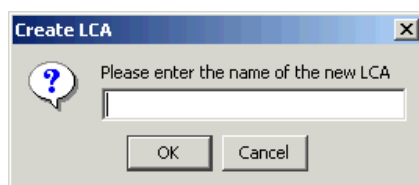
The user can manually create a LCA and populate it by:

- Moving selected LCPs to the LCA. For more information, refer to page 25.
- Adding tunnels (LCPs) to the LCA. For more information, refer to page 21.

For more information about LCAs that are created automatically, refer to page 21.


To create a LCA

1. Select the required VPN in the *Sheer NetworkVision* window's *Tree* pane or *Map* pane.
2. Right-click to display the shortcut menu and select **Create LCA**. The *Create LCA* dialog box is displayed.



3. Type a unique name for the new LCA.
4. Click **OK**. The new LCA is created and displayed in the *Tree* pane the *Sheer NetworkVision* window beneath the selected VPN, and in the *Map* pane.

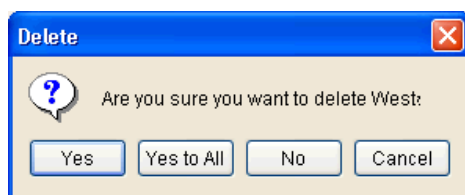
3.5 Deleting a LCA

Sheer DNA enables the user to delete a LCA that was manually created if it has no LCPs or if all of the LCPs have the reconciliation icon .

Note: The user also has the option to move the LCA to another VPN. For more information, refer to page 25.

To delete the LCA

1. Select the required LCA in the *Sheer NetworkVision* window's *Tree* pane or *Map* pane.
2. Right-click to display the shortcut menu and select **Delete**. The following message is displayed:



3. Click **Yes** to delete the LCA. The selected LCA is deleted from the database and Service View maps of all users.

Note: When the user deletes an LCA, the LCA information is deleted from the database.

3.6 Moving a LCP

The user can move a LCP to another VPN or LCA in the Service View map.

To move a LCP

1. Right-click on the required LCP in the *Sheer NetworkVision* window's *Tree* pane or *Map* pane to display the shortcut menu.
2. Select **Edit | Move selected**.
3. Right-click on the required VPN or LCA in the *Tree* pane or *Map* pane to where you want to move the LCP to display the shortcut menu.
4. Select **Edit | Move here**. The single selected LCP moves to the required VPN or LCA, and is displayed in the *Tree* pane and *Map* pane of the selected VPN or LCA.

Note: If a LCP is moved to a VPN then a LCA is automatically created for it.

3.7 Moving a LCA

The user can move the LCA to another VPN in the Service View map. When the LCA is moved all of the LCPs beneath the LCA also move.

To move a LCA

1. Right-click on the required LCA in the *Sheer NetworkVision* window's *Tree* pane or *Map* pane to display the shortcut menu.
2. Select **Edit | Move selected**.
3. Right-click on the required VPN in the *Tree* pane or *Map* pane where you want to move the LCA to display the shortcut menu.
4. Select **Edit | Move here**. The LCA moves to the selected VPN and is displayed in the *Tree* pane and *Map* pane for the selected VPN.

Note: All of the LCPs move along with the LCA.

3.8 Jumping to the Adjacent LCP

The Service View map displays multiple tunnels. The user can quickly and easily access the selected LCP's peer appearing in the same map.

Note: You can only jump from one LCP to a peer LCP, provided the other peer is displayed in the same map.

To jump to the adjacent LCP

1. Select the required LCP in the *Sheer NetworkVision* window's *Tree* pane or *Map* pane.
2. Right-click on the LCP to display the shortcut menu, and select **Jump to Adjacent**. The adjacent LCP is highlighted in the *Tree* pane and *Map* pane.

3.9 Renaming a Business Element

You can rename a business element in Service View maps using the shortcut menu.

To rename a business element

1. Right-click on the required business element in the *Sheer NetworkVision* window's *Tree* pane or *Map* pane to display the shortcut menu.
2. Select **Rename**. The *Rename Node* dialog box is displayed.



3. Type a new name and click **OK**. The changed business element name appears in the *Sheer NetworkVision* window's *Tree* pane and *Map* pane.






Note: When a business element is renamed it affects all users that have the business element loaded in their Service View map.

3.10 Deleting a Business Element

The user can delete business elements from the business model (database). When a business element is deleted it is deleted from the database (irreversible) and is no longer displayed in the *Add Business Element to <Root>* dialog box. A business element is generally deleted when the physical element no longer exists.

Warning! When a business element is deleted it affects all users that have the business element loaded in their Service View map.

The table below describes the checks performed by Sheer DNA before the user can delete the required business element.

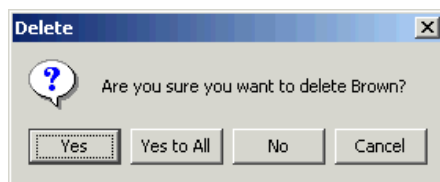
Business Element	Requirements
Layer 3 VPN	<ul style="list-style-type: none"> There are no Virtual Routers. The Virtual Routers, and Sites display the reconciliation icon .
Virtual Router	<ul style="list-style-type: none"> There are no network elements (VRFs and interfaces) contained in the Virtual Router. The Virtual Routers, VRFs, Sites and interfaces display the reconciliation icon .
Site	<ul style="list-style-type: none"> There are no interfaces connected/bound to the VRF. The Sites and interfaces display the reconciliation icon .
Layer 2 VPN	<ul style="list-style-type: none"> There are no LCPs beneath the LCA. The LCPs display the reconciliation icon .
LCA	<ul style="list-style-type: none"> There are no LCPs. All the nested LCPs display the reconciliation icon .

To delete a business element

- Right-click on the required business element in the *Sheer NetworkVision* window's *Tree* pane or *Map* pane to display the shortcut menu.

Note: Make sure that the VPN business element meets the requirements set out in the table. If the requirements are not met, you will be unable to delete the business element.

- Select **Delete**. The following warning message is displayed.



- 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.

4 Viewing VPN Properties in Service View

About this chapter:

This chapter describes viewing the properties of the various business elements.

Viewing VPN Properties, page 29, describes how to view VPN properties.

Viewing Site Properties, page 30, describes how to view Site properties.

Viewing a Virtual Router's Properties, page 31, describes how to view a Virtual Router's properties. In addition, it describes the VRF table and displaying the VRF egress and ingress adjacents.

Viewing VRF Properties in the Inventory Window, page 35, describes viewing VRF and **PWE3** Tunnels VPN specific logical inventory items.

Working with the VPN Service Overlay, page 38, describes how to select and display an overlay, how to display or hide a previously defined overlay, and how to display or hide the callouts for every link in the *Map* pane.

4.1 Viewing VPN Properties

Sheer DNA enables the user to view the properties of the VPN business element.


To view VPN properties

1. Right-click on the VPN in then *Sheer NetworkVision* window's *Tree* pane or *Map* pane to display the shortcut menu. Select **Properties**. The *VPN Properties* dialog box for the selected VPN is displayed.

The following field is displayed in the *VPN Properties* dialog box:

- **Name:** The name of the VPN.

Note: The name of the VPN can be changed using the **Rename** shortcut menu option.

- **ID:** The unique key automatically assigned to the VPN.
2. Click  to close the *VPN Properties* dialog box.

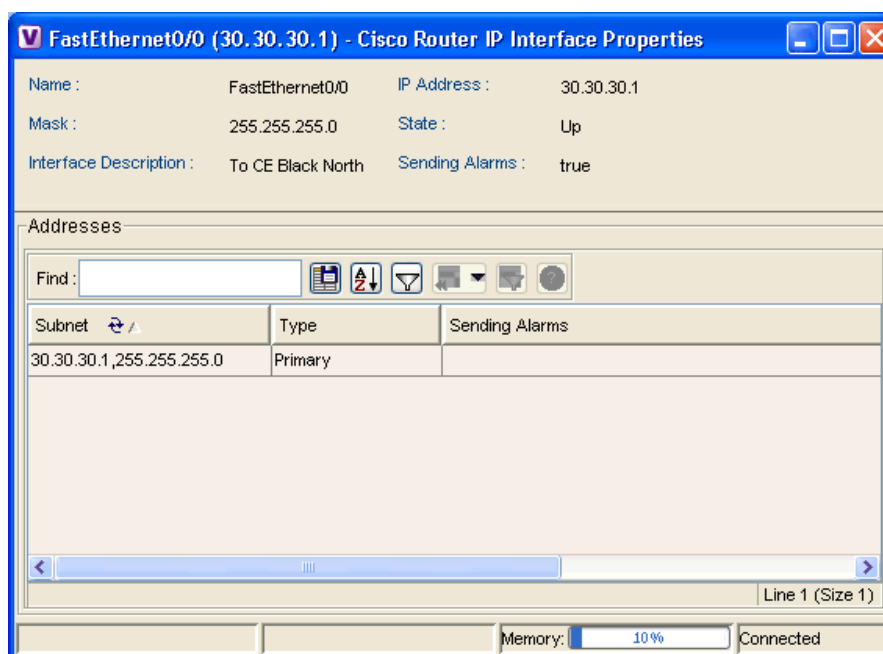
4.2 Viewing Site Properties

Sheer DNA enables the user to view the properties of a Site, including the interfaces that are configured on the PE. The properties that are displayed reflect the configuration that is automatically discovered from the device.

Note: The user can also add a business tag to the interface. For more information about business tags, refer to the *Cisco Active Network Abstraction NetworkVision User's Guide*.

To view Site properties

1. Right-click on a Site in the *Sheer NetworkVision* window's *Tree* pane or *Map* pane to display the shortcut menu. Select **Properties**. The *Router IP Interface Properties* dialog box for the selected Site is displayed.



The following fields are displayed in the *Router IP Interface Properties* dialog box:

- **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, namely, Up or Down.

The **Addresses** table displays the details of the IP interfaces on the PE-side. The **Subnet** column is a combination of the IP address and the subnet mask.

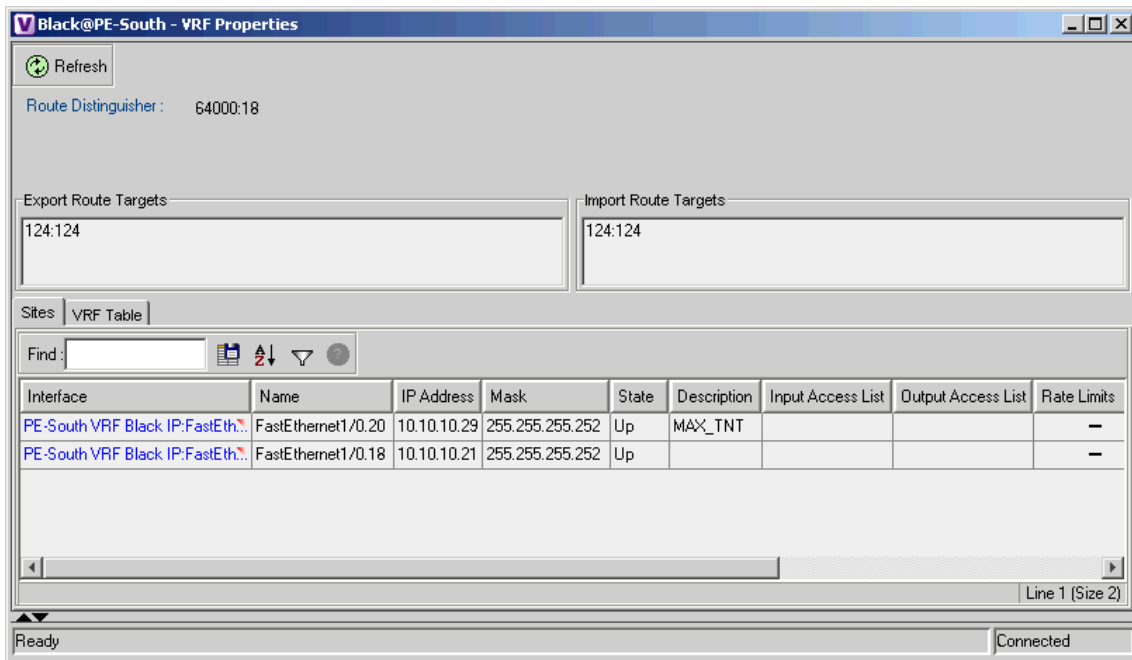
- Click  to close the *Router IP Interface Properties* dialog box.

4.3 Viewing a Virtual Router's Properties

Sheer NetworkVision enables the user to view the route distinguisher, and the import and export policies for each VRF.

To view a Virtual Router's properties

- Right-click on a Virtual Router in the *Sheer NetworkVision* window's *Tree* pane or *Map* pane to display the shortcut menu. Select **Properties**. The *VRF Properties* dialog box for the Virtual Router is displayed.



The following field is displayed at the top of the *VRF Properties* dialog box:

- **Route Distinguisher:** The route distinguisher configured in the VRF.

The **Export/Import Route Targets** areas displayed in the *VRF Properties* dialog box specify separately the export and import policies for each VRF.

The *VRF Properties* dialog box is divided into two tabs, namely, the **Sites** and **VRF Table** tabs. The **Sites** tab displays the interfaces connected to the VRF and the configuration of the interfaces. The following columns are displayed in the **Sites** tab:

- **Interface:** A hyperlink that displays the *Inventory* window for the IP interface linked to the Site on the PE side.
- **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 details of the dotted decimal mask.
- **State:** The state of the sub-interface, namely, Up or Down.
- **Description:** A description of the interface.
- **Input Access List:** The access list applied to the inbound traffic of the interface.

Note: This parameter is only relevant for Cisco IOS devices.

- **Output Access List:** The access list applied to the outbound traffic of the interface.

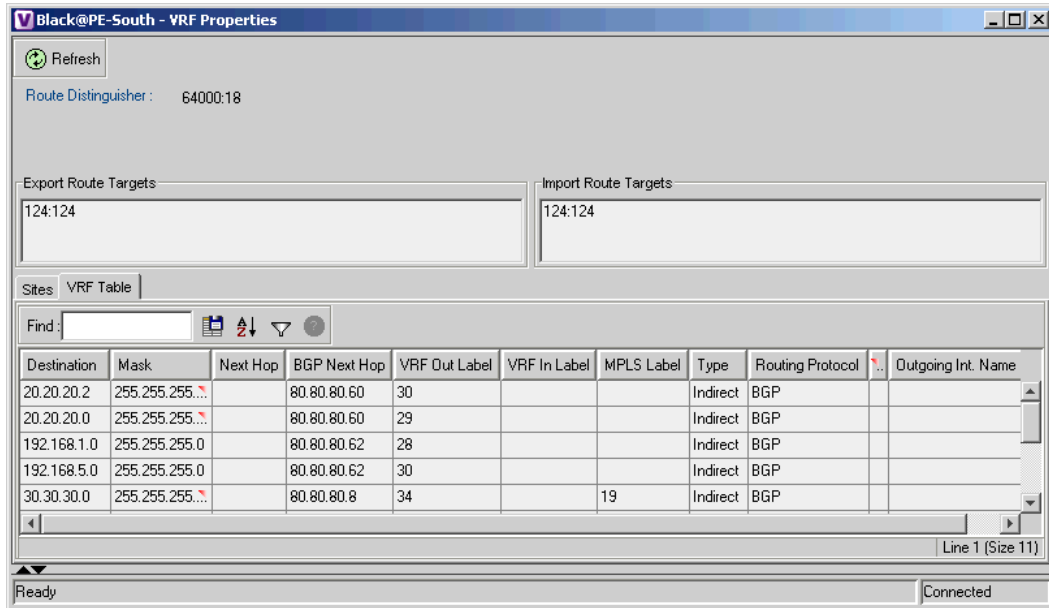
Note: This parameter is only relevant for Cisco IOS devices.

- **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: This parameter is only relevant for Cisco IOS devices.


- **Site Name:** The name of the business element to which the interface is attached.

The **VRF Table** tab is displayed below.



VRF Table tab contains the VRF routing table for the device, namely, a collection of routes that are available or reachable to all the destinations or networks in this VRF. In addition, the forwarding table also contains MPLS encapsulation information.

The following columns are displayed in the **VRF Table** tab:

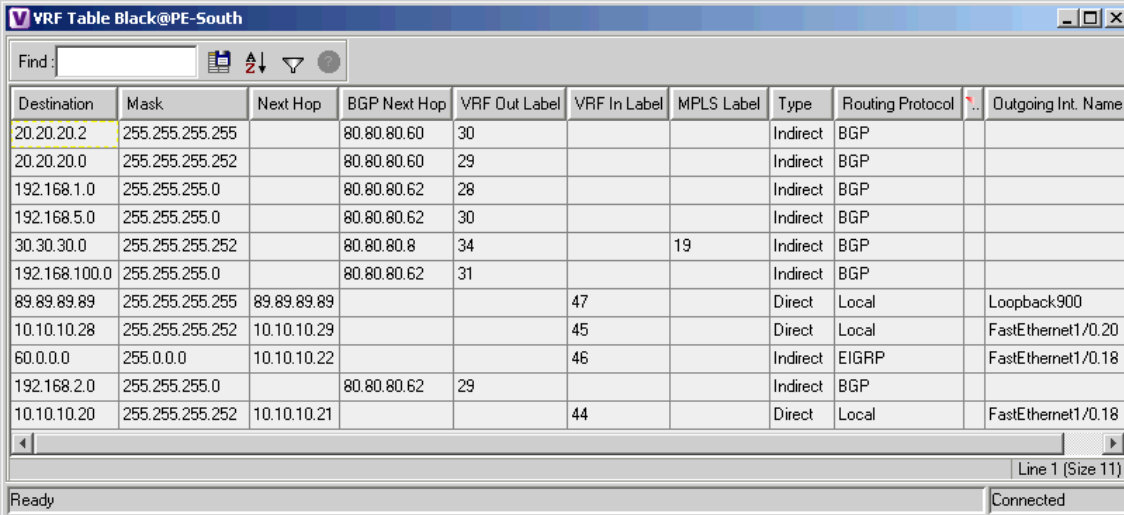
- **Destination:** The destination of the specific network.
 - **Mask:** The mask of the specific network.
 - **Next Hop:** The CE address from where to continue to get to a specific address. This field is empty when the routing entry goes to the PE.
 - **BGP Next Hop:** The PE address from where to continue to get to a specific address. This field is empty when the routing entry goes to the CE.
 - **VRF Out Label:** The label sent with MPLS traffic.
 - **VRF In Label:** The label that is expected when MPLS traffic is received.
 - **MPLS Label:** The MPLS label.
 - **Type:** The type can be direct (local) or indirect
 - **Routing Protocol:** The routing protocol used to communicate with the other Sites/VRFs, namely, BGP or local.
 - **Outgoing Int. Name:** The name of the outgoing interface is displayed if the Routing Protocol type is local.
2. Click  to close the *VRF Properties* dialog box.

4.3.1 Opening the VRF Table

The user can view the VRF table for a Virtual Router.

To open the VRF Table

1. Right-click on the Virtual Router in the *Sheer NetworkVision* window's *Tree* pane or *Map* pane to display the shortcut menu. Select **Open VRF Table**. The *VRF Table* dialog box is displayed.



The screenshot shows a window titled "VRF Table Black@PE-South" with a search bar and a table of routing entries. The table has the following columns: Destination, Mask, Next Hop, BGP Next Hop, VRF Out Label, VRF In Label, MPLS Label, Type, Routing Protocol, and Outgoing Int. Name. The data rows are as follows:

Destination	Mask	Next Hop	BGP Next Hop	VRF Out Label	VRF In Label	MPLS Label	Type	Routing Protocol	Outgoing Int. Name
20.20.20.2	255.255.255.255		80.80.80.60	30			Indirect	BGP	
20.20.20.0	255.255.255.252		80.80.80.60	29			Indirect	BGP	
192.168.1.0	255.255.255.0		80.80.80.62	28			Indirect	BGP	
192.168.5.0	255.255.255.0		80.80.80.62	30			Indirect	BGP	
30.30.30.0	255.255.255.252		80.80.80.8	34		19	Indirect	BGP	
192.168.100.0	255.255.255.0		80.80.80.62	31			Indirect	BGP	
89.89.89.89	255.255.255.255	89.89.89.89					Direct	Local	Loopback900
10.10.10.28	255.255.255.252	10.10.10.29					Direct	Local	FastEthernet1/0.20
60.0.0.0	255.0.0.0	10.10.10.22					Indirect	EIGRP	FastEthernet1/0.18
192.168.2.0	255.255.255.0		80.80.80.62	29			Indirect	BGP	
10.10.10.20	255.255.255.252	10.10.10.21					Direct	Local	FastEthernet1/0.18

For more information about the columns displayed in the *VRF Table* dialog box, refer to *Section 4.3*.

2. Click  to close the *VRF Table* dialog box.

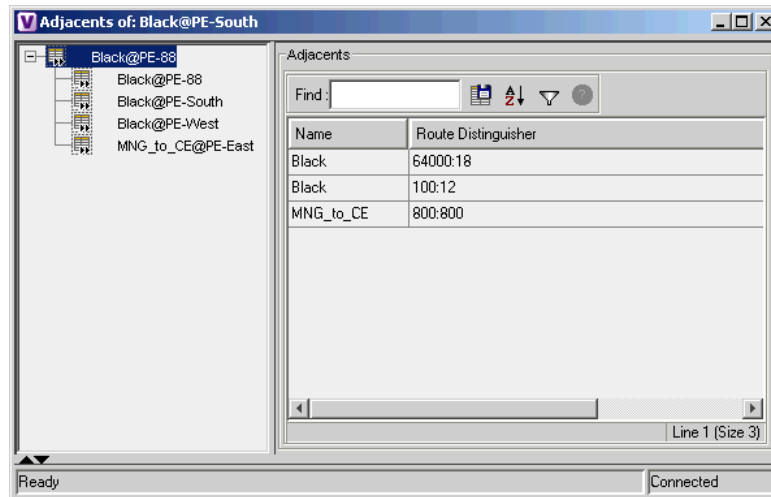
4.3.2 Displaying the VRF Egress/Ingress Adjacents

Sheer DNA enables the user to view the exporting and importing neighbors by displaying the VRF egress and ingress adjacents. In addition, the user can view the connectivity between the VRFs regarding the route targets and view all of their properties.

For example, if VRF A retrieved route target import X then the user will be able to view all of the VRFs in the system that are exporting X as a route target whether its in the same VPN or in another VPN.

To display the VRF egress/ingress adjacents


1. Right-click on the Virtual Router in the *Sheer NetworkVision* window's *Tree* pane or *Map* pane to display the shortcut menu. Select **Show VRF Egress Adjacents/Show VRF Ingress Adjacents**. The *Adjacents* dialog box is displayed.



The adjacents displayed are according to the route targets. The following columns are displayed in the table on the right side of the dialog box (*Properties* pane) when the top branch is selected in the *Tree* pane:

- **Name:** The name of the VRF as it appears in the device.
- **Route Distinguisher:** The route distinguisher configured in the VRF.

Selecting a specific VRF in the *Sheer NetworkVision* window's *Tree* pane displays the properties of the VRF. For more information, refer to *Section 4.3*.

2. Click  to close the *Adjacents* dialog box.

4.4 Viewing VRF Properties in the Inventory Window

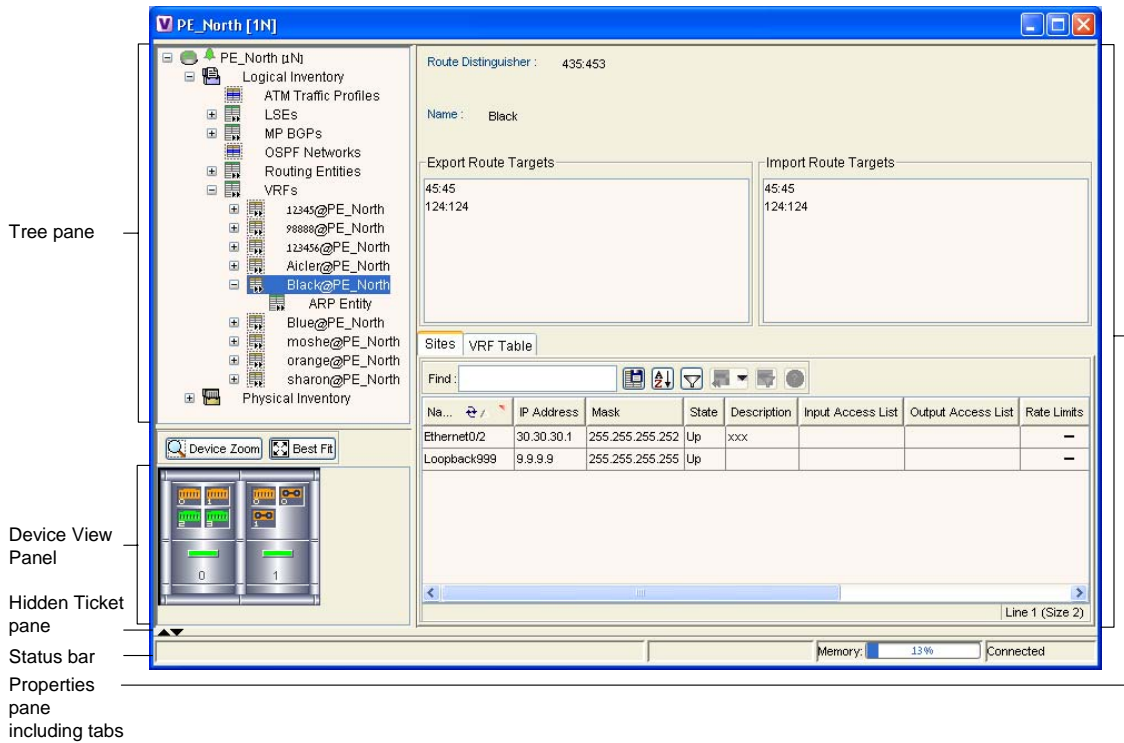
This section describes viewing only the following VPN specific logical inventory items, namely, VRF and **PWE3** Tunnels.

Note: In addition to opening the *Inventory* window from a device, you can also open and view logical inventory information for a specific Virtual Router directly by right clicking on the Virtual Router to display the shortcut menu and selecting **Inventory**.

For details on viewing the following VPN MPLS specific logical inventory items, namely, BGP Neighbor, MP BGP information, LSEs, and MPLS TE tunnels, and MPLS Black Holes, refer to *Chapter 5, Viewing MPLS Related Inventory Properties*.

To open the Inventory window


1. Right-click on a device in the *Sheer NetworkVision* window's *Tree* pane or *Map* pane to display the shortcut menu.
2. Select **Inventory**. The *Inventory* window for the selected device is displayed.



The *Tree* pane displays a tree-and-branch representation of the logical and physical inventory. The heading of the window and the root of the *Tree* pane display the name of the selected router.

The *Properties* pane displays physical and logical inventory information relating to the properties of the item selected in the *Tree* pane.

Note: The properties of the item selected in the *Tree* pane or the row selected in the *Properties* pane can be displayed by double-clicking it or by right-clicking the line and selecting **Properties** from the shortcut menu.

3. Click  to close the *Inventory* window.

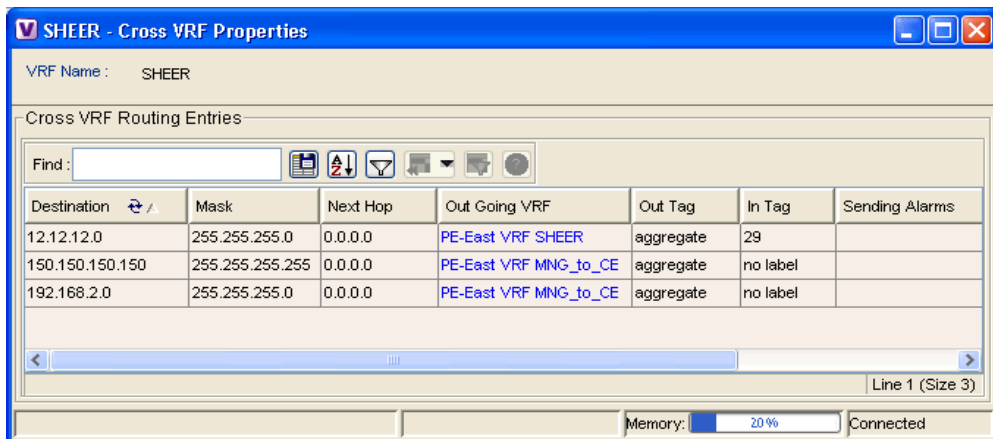
You can view *Inventory* properties in the *Properties* pane and/or properties pane tab tables, or view selected properties in separate window (*Properties* window).

Clicking on a sub-branch *Tree* pane option in the *Inventory* window, displays the properties in the *Properties* pane of the *Inventory* window:

Double-clicking a sub-branch *Tree* pane option in the *Inventory* window, displays properties in a window.

4.4.1 Viewing Cross VRF Routing Entries

Cross VRF Routing entries are displayed by double-clicking on an entry in the *MP BGP Properties* pane. The **Cross VRF Routing Entries** table displays routing information learned from the BGP neighbors (BGP knowledge base). The parameters of the cross VRF routing entries are displayed in the *Cross VRF MP BGP Properties* window tab, an example of which is displayed below.



The screenshot shows a window titled "SHEER - Cross VRF Properties" with a "VRF Name : SHEER" label. Below is a table titled "Cross VRF Routing Entries" with a search bar and several icons. The table has the following data:

Destination	Mask	Next Hop	Out Going VRF	Out Tag	In Tag	Sending Alarms
12.12.12.0	255.255.255.0	0.0.0.0	PE-East VRF SHEER	aggregate	29	
150.150.150.150	255.255.255.255	0.0.0.0	PE-East VRF MNG_to_CE	aggregate	no label	
192.168.2.0	255.255.255.0	0.0.0.0	PE-East VRF MNG_to_CE	aggregate	no label	

At the bottom of the window, there is a "Memory: 20%" indicator and a "Connected" status.

The following information is displayed in the Cross VRF Routing Entries table:

- **Destination:** The destination of the specific network.
- **Mask:** The mask of the specific network.
- **Next Hop:** The PE address from where 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 Out Going 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 in order to reach the destination address that is connected to the other VRF.

- **In Tag:** The MPLS label used by this router in order 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 where the traffic originated.

4.5 Working with the VPN Service Overlay

In addition to Network and *Service View* maps the user can select and display an overlay of a specific VPN on top of the devices displayed on the Network map in the *Map* pane. The overlay is a snapshot of the network which visualizes the flows between the Sites and tunnel peers. When one of the VPNs in the network is selected (in the Network map), the provider edge routers, MPLS routers and physical links that carry the LSP that is being used by the VPN are highlighted in the Network map and all the devices and links that are not part of the VPN are grayed out.

This enables the user to isolate the parts of a network that are being used by a particular service and this information can then be used for troubleshooting. For example, the overlay can highlight configuration or design problems when a bottleneck exists and all the Site interconnections using the same link.

Note: If the routing information changes after the overlay is run, then the current view will not reflect this change.

Sheer NetworkVision enables you to view overlays of specific VPNs on top of the devices displayed in physical Network maps. In addition, it enables you to view selected callouts for the links displayed on the Network map when the overlay is applied.


This section describes the following overlay functionality information:

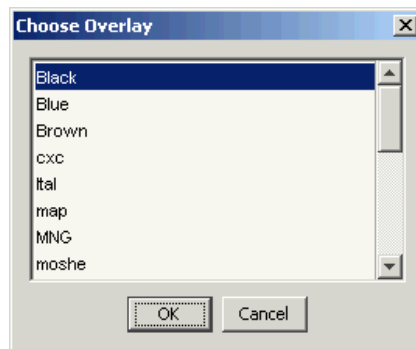
- **Selecting an Overlay** describes how to select and display an overlay of a specific VPN on top of the devices displayed on the physical Network map.
- **Displaying or Hiding an Overlay**, page 39, describes how to display or hide a previously defined overlay of a specific VPN on top of the physical devices displayed on the physical Network map.
- **Displaying or Hiding Callouts**, page 40, describes how to display or hide the callouts for every link in the *Map* pane in order to display related information.

4.5.1 Selecting an Overlay

The user may select and display an overlay of a specific VPN on top of the devices displayed on the physical Network map displayed in the *Map* pane.

To select an overlay

1. Select and display the required Network map in the *Sheer NetworkVision* window.
2. In the toolbar, click  **Choose Overlay**. The *Choose Overlay* dialog box is displayed.



The *Choose Overlay* dialog box displays a list of the available VPNs in the network.

3. Select the required VPN from the list.
4. Click **OK**. The provider edge routers, MPLS routers and physical links that are being used by the selected VPN are highlighted in the Network map and the VPN name is displayed in the title of the window.


Note: The overlay is a snapshot taken at a specific point in time and in order to update the overlay the user must select and run it again.

You can choose to hide previously defined VPN network information in the *Map* pane using the appropriate toolbar buttons:



- Overlay information, such as link and layer details
- Callouts for the VPN network

4.5.2 Displaying or Hiding Overlays

The user can quickly and easily display or hide a previously defined overlay of a specific VPN on top of the physical devices displayed on the Network map in the *Map* pane.

Note: The  **Show Overlay** button in the toolbar toggles when selected (displays the overlay) or deselected (hides the overlay).

To show or hide the overlay

1. Select and display the required Network map in the *Sheer NetworkVision* window.
2. In the toolbar, click  **Show Overlay**. The overlay is displayed in the Network map,
or
In the toolbar, click  **Show Overlay**. The overlay is hidden from view in the Network map.

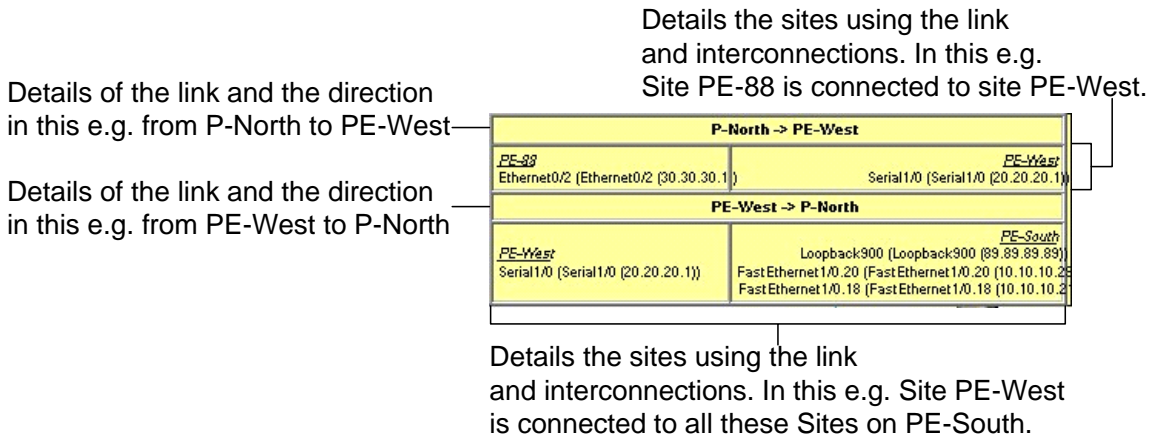
4.5.3 Displaying or Hiding Callouts

The user can display or hide the callouts for the links displayed in the *Map* pane in order to show the details of the sites that are interconnected through the selected links.

Note: Multiple callouts can be opened at the same time.

The *Callouts* dialog box enables the user to view the VPN traffic connections for a specific link (either bi-directional or uni-directional).

In the example below, P-North - > PE-West, the table displays the traffic connections from one Site/LCP to another.

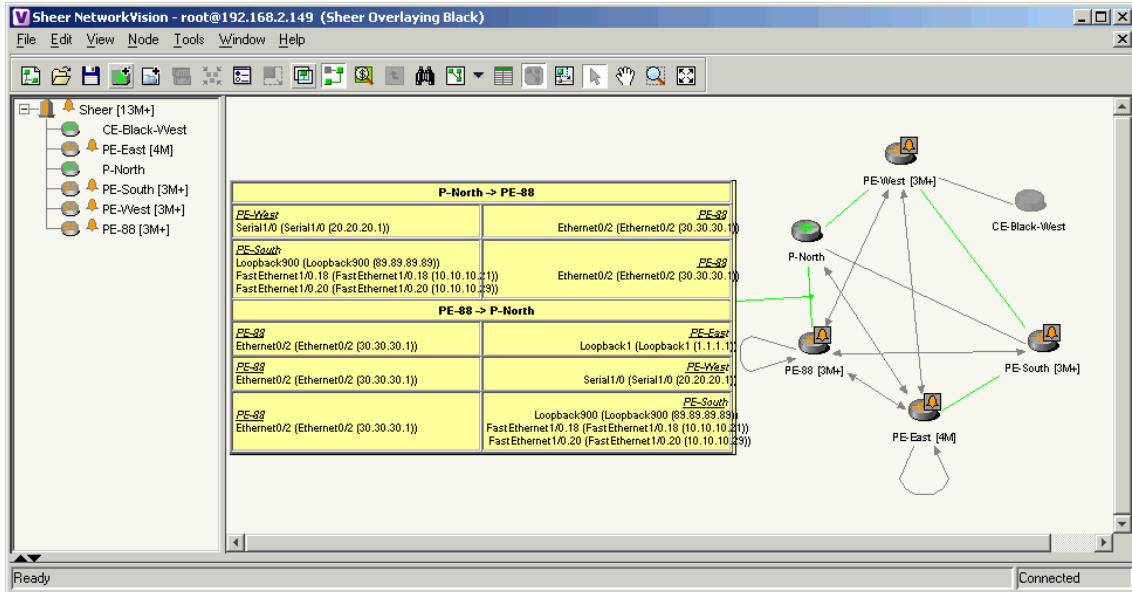


The user can hide the callouts displayed in the *Map* pane.

To view the callouts

1. Select and display the required Network map with an overlay of the specific VPN in the *Map* pane of the *Sheer NetworkVision* window.

- Right-click on the required link in the *Map* pane to display the shortcut menu and select **Show Callouts**. The *Callouts* label is displayed, as shown in the example below.



To hide the callouts

- Right-click on the link in the *Map* pane that has the attached callout. The right-click shortcut menu is displayed.
- Select **Hide Callouts**. The callouts are no longer displayed in the *Map* pane of the *Sheer NetworkVision* window.

5 Viewing MPLS Related Inventory Properties

About this chapter:

This chapter describes how to view general logical inventory information and describes the VPN specific items that are displayed in the *Inventory* window. For a general description of logical inventory and the *Inventory* window, refer to the *Cisco Active Network Abstraction NetworkVision User's Guide*.

Introduction, page 43, introduces the concepts of physical and logical inventory.

Opening the Inventory Window, page 44, describes how to open the *Inventory* window in order to view the logical inventory.

Viewing Routing Entities, page 46, provides a brief description of the Routing Entities item. In addition, it briefly describes the ARP table.

Viewing Port Configuration, page 49, provides a brief description of elements appearing in physical inventory branch that enable user determine what services, for example, are being used on a selected port.

Viewing LSEs, page 50, describes the LSEs item and its properties.

Viewing MP BGP Information, page 52, describes the MP BGPs item and its properties. In addition, it describes the BGP Neighbors item and properties

Viewing VRF Information, page 54, describes the VRF item and its properties. In addition, it describes the import and export policies for each VRF.

Viewing Pseudo Wire End-to End Emulation (PWE3) Tunnels, page 60, describes viewing the Layer 2 tunnel edge properties (per edge).

Viewing MPLS TE Tunnel Information, page 61, describes the Traffic Engineering tunnel item and its properties.

5.1 Introduction

Every node that is managed by Sheer DNA is assigned to an autonomous VNE that manages it. The VNE continuously investigates the Network Element status and configuration in order to reflect it accurately and generate an accurate virtual model of the network.

The physical device inventory contains all the physical components (and their various properties) of the managed Network Element, such as chassis, shelves, cards and ports. The physical inventory is continuously updated for both status and configuration. Any change of status or addition or removal of a component (such as a card), is detected by the VNE and reflected in the network model instantly.

In addition to the physical network inventory, the Sheer DNA VNEs also investigate the logical inventory of each device. The logical inventory reflects dynamic data such as configuration data, forwarding and service-related components, which affects traffic handling in the device, such as traffic profiles, VC and cross-connect tables, routing, bridging, and LSE tables, and so on.

These logical device assets are also updated in the model of the Network Element in order to accurately reflect how the device handles its incoming and outgoing traffic.

Sheer NetworkVision displays the device inventory and allows drill-down to detailed internal physical and logical inventory.

5.2 Opening the Inventory Window

The Sheer solution continuously maintains a real-time, auto-discovered, physical and logical inventory of the network entities, and the relationships between them. Using Sheer's distributed data model, the system automatically reflects every addition, deletion and modification that occurs in the network. The general logical inventory information displayed in the *Inventory* window changes according to the item selected in the *Tree* pane.

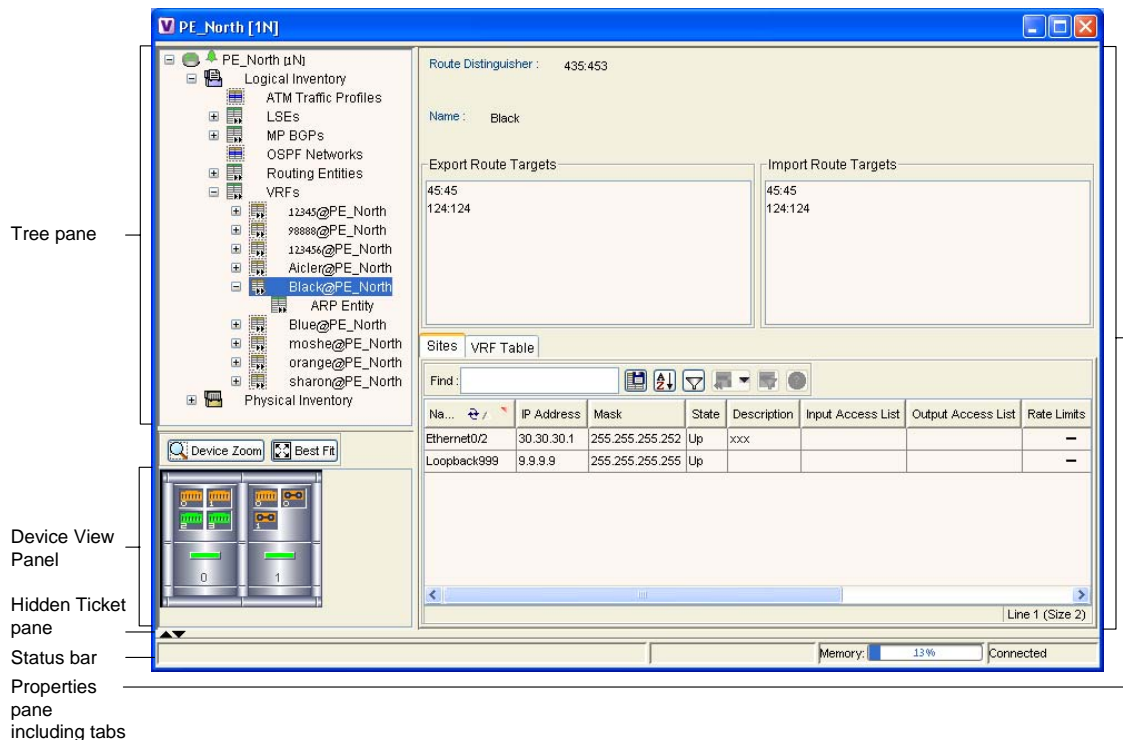
This guide describes viewing only the following VPN MPLS specific logical inventory items, namely, Routing Entities, LSEs, BGP Neighbors, MP BGPs, VRFs, **PWE3** tunnels, and TE tunnels.

Note: In addition to opening the *Inventory* window from a device, the user can also open and view logical inventory information for a specific Virtual Router directly by right clicking on the Virtual Router to display the shortcut menu and selecting *Inventory*.

To open the Inventory window

1. Right-click on a device in the *Sheer NetworkVision* window's *Tree* pane or *Map* pane to display the shortcut menu.


2. Select **Inventory**. The *Inventory* window for the selected device is displayed.



The *Tree* pane displays a tree-and-branch representation of the logical and physical inventory. The heading of the window and the root of the *Tree* pane display the name of the selected router.

The *Properties* pane displays physical and logical inventory information relating to the properties of the item selected in the *Tree* pane.

Note: The properties of the item selected in the *Tree* pane or the row selected in the **Properties** pane can be displayed by double-clicking it or by right-clicking the line and selecting **Properties** from the shortcut menu.

3. Click  to close the *Inventory* window.

Physical and logical inventory properties can be viewed in the *Properties* pane (tabs or tables) or in a separate window (*Properties* dialog box).

- **Properties pane:** Selecting a sub-branch in the *Tree* pane of the *Inventory* window, displays the properties of the selected sub-branch in the *Properties* pane of the *Inventory* window.

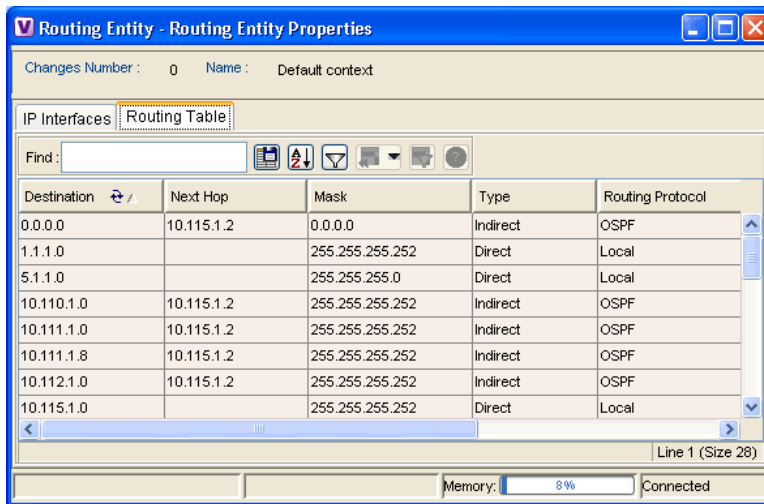
- **Properties dialog box:** Double-clicking on a sub-branch in the *Tree* pane of the *Inventory* window, displays the properties of the selected sub-branch in a separate *Properties* dialog box.

Note: The examples used in this chapter are presented in the *Properties* dialog box, as described above.

5.3 Viewing Routing Entities

The **Routing Entity** sub-branch of the **Routing Entities** branch displays the IP interfaces and routing information.

An example of the *Routing Entity – Routing Entity Properties* dialog box (IP Interfaces) is displayed below.



The following information is displayed at the top of the dialog box:

- **Changes Number:** The number of changes to the currently displayed routing entity.
- **Name:** The name of the routing entity.

The *Routing Entity Properties* dialog box is divided into two tabs, namely, **IP Interfaces** and **Routing Table** tabs. The **IP Interfaces** tab lists the device IP interfaces and the **Routing Table** tab contains routing information.

The following information is displayed in the **IP Interfaces** 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 details of the dotted decimal mask.
- **State:** The state of the sub-interface, namely, Up or Down.

- **Description:** A description of the interface.
- **Input Access List:** The access list applied to the inbound traffic of the interface.

Note: This parameter is only relevant for Cisco IOS devices.

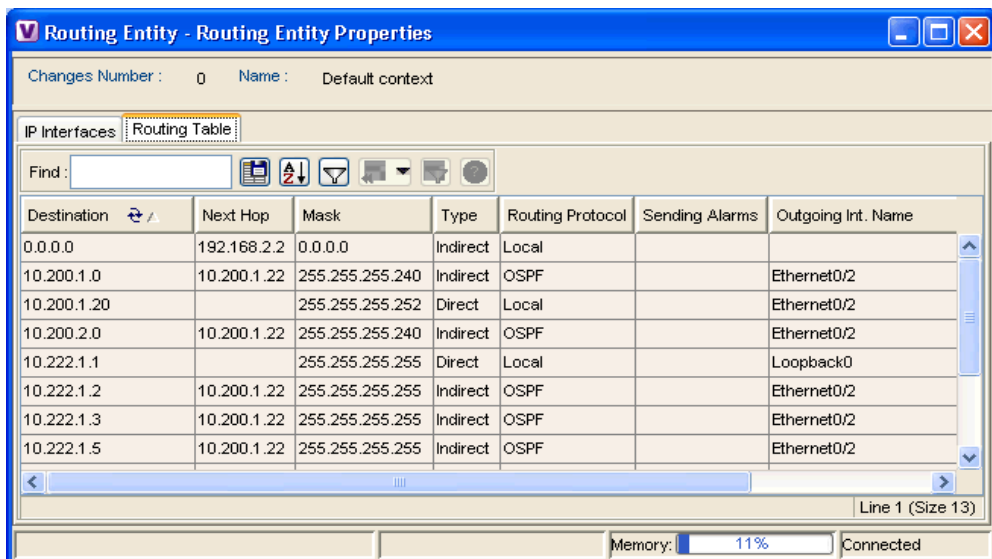
- **Output Access List:** The access list applied to the outbound traffic of the interface.

Note: This parameter is only relevant for Cisco IOS devices.

- **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.
- **Site Name:** The name of the business element to which the interface is attached.
- **Sending Alarms:** This option is currently unavailable.

For more information about the **IP Interfaces** tab, refer to page 31, *Viewing a Virtual Router's Properties*.

The **Routing Table** tab is displayed below.



Routing Entity - Routing Entity Properties
Changes Number : 0 Name : Default context

IP Interfaces: Routing Table

Find: []

Destination	Next Hop	Mask	Type	Routing Protocol	Sending Alarms	Outgoing Int. Name
0.0.0.0	192.168.2.2	0.0.0.0	Indirect	Local		
10.200.1.0	10.200.1.22	255.255.255.240	Indirect	OSPF		Ethernet0/2
10.200.1.20		255.255.255.252	Direct	Local		Ethernet0/2
10.200.2.0	10.200.1.22	255.255.255.240	Indirect	OSPF		Ethernet0/2
10.222.1.1		255.255.255.255	Direct	Local		Loopback0
10.222.1.2	10.200.1.22	255.255.255.255	Indirect	OSPF		Ethernet0/2
10.222.1.3	10.200.1.22	255.255.255.255	Indirect	OSPF		Ethernet0/2
10.222.1.5	10.200.1.22	255.255.255.255	Indirect	OSPF		Ethernet0/2

Line 1 (Size 13)

Memory: 11% Connected

The following information is displayed in the **Routing Table** tab:

- **Destination:** The destination of the specific network.
- **Next Hop:** The CE address from where to continue to get to a specific address. This field is empty when the routing entry goes to the PE.
- **Mask:** The mask of the specific network.

- **Type:** The type can be direct (local) or indirect.
- **Routing Protocol:** The routing protocol used to communicate with other routers.
- **Sending Alarms:** This option is currently unavailable.
- **Outgoing Interface Name:** The name of the outgoing interface is displayed if the Routing Protocol type is local.

5.3.1 Viewing the ARP Table

The **ARP Entity** sub-branch of the **Routing Entity** branch displays ARP information.

An example of the *ARP Entity – ARP Entity Properties* dialog box is displayed below.

MAC	Interface	IP Address	Type	Sending Alarms
00 30 80 B1 8E 41	Ethernet2/0	10.112.1.2	Dynamic	
00 03 E4 11 80 38	Ethernet2/0	10.112.1.1	Static	
00 03 E4 11 80 38	Ethernet2/0.336	1.1.1.1	Static	
00 03 E4 11 80 38	Ethernet2/0.337	1.2.3.5	Static	
00 02 B9 BD FE 63	Ethernet2/1	10.111.1.2	Dynamic	
00 03 E4 11 80 39	Ethernet2/1	10.111.1.1	Static	
00 10 79 37 98 08	Ethernet2/2	192.168.2.212	Dynamic	
00 10 79 37 98 08	Ethernet2/2	192.168.2.31	Dynamic	

The *Properties* pane enables you to view MAC, interface, and IP address information. In addition, you can view the ARP type, namely:

- **Dynamic:** An entry that has been learned by the device according to traffic in the network.
- **Static:** An entry that has been learned by a local interface or by configuring a static ARP, like a static route.
- **Other:** An entry that has been learned by another method which is not explicitly defined.
- **Invalid:** In SNMP this is used to remove an ARP entry from the table.

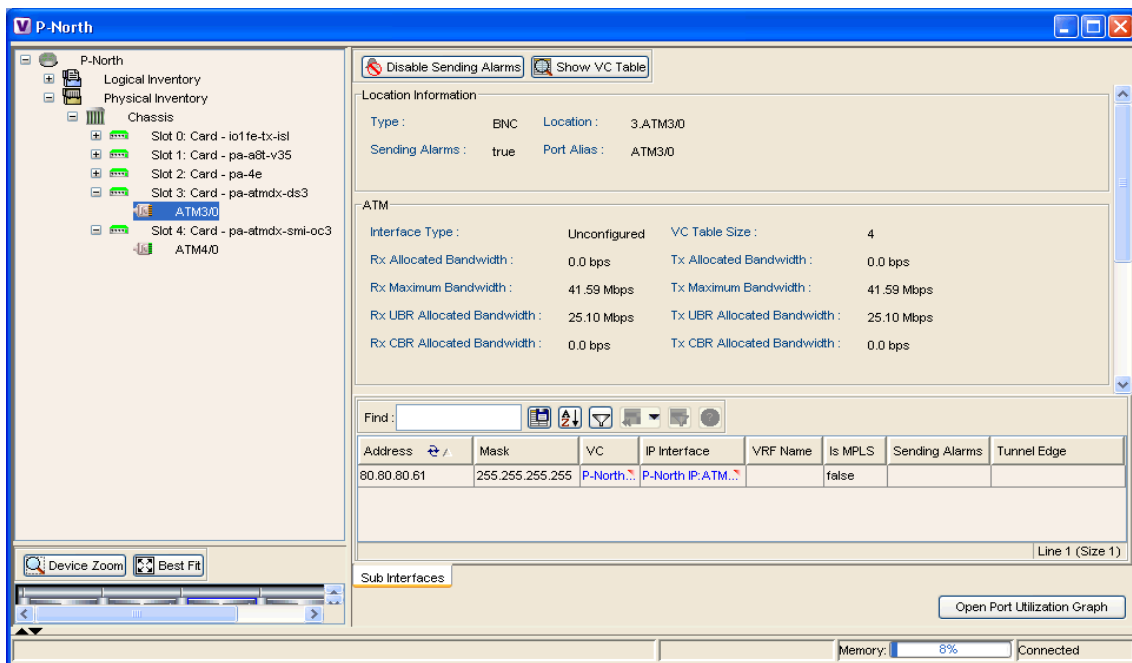
5.4 Viewing Port Configuration

In addition to viewing logical inventory information in the *Inventory* window, when the user selects the physical source (port) in the physical inventory branch the user can determine what services are using the selected port. The user can view:

- Physical layer information
- Layer 2 information, for example, ATM and Ethernet
- The sub-interfaces that the VRF is using.

For detailed information on viewing physical inventory information, refer to the *Cisco Active Network Abstraction NetworkVision User's Guide*.

In the example below, port information (including the sub-interfaces), is displayed when a port is selected in the physical inventory branch of the *Inventory* window.



The sub-interface is the logical interface defined in the device; all of its parameters can be part of its configuration. The following information is displayed in the sub-interface table for the selected port:

- **Address:** The IP address defined in the sub-interface.
- **Mask:** The details of the dotted decimal mask.
- **VC:** If the sub-interface is defined above an ATM or Frame-Relay physical interface and it uses a VC based encapsulation, it is the VC used in this encapsulation.

- **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 a MPLS interface, namely, enabled (**true**) or disabled (**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, namely, enabled (**true**) or disabled (**false**).

5.5 Viewing LSEs

The **LSEs** (Label Switch Entity) branch displays incoming and outgoing label information. An example of the *Label Switching – LSE Properties* dialog box is displayed below.

Incomin...	Action	Outgoing Label	Out Interface	IP Destination	Destination Mask	Next Hop	Sending Alarms
16	Untagged		PE-West IP:Ethernet0/1	10.110.1.0	255.255.255.248	10.112.1.1	
17	Untagged		PE-West IP:Ethernet0/1	10.111.1.0	255.255.255.252	10.112.1.1	
18	Untagged		PE-West IP:FastEthernet1/0	10.114.1.0	255.255.255.252	10.115.1.1	
19	Untagged		PE-West IP:FastEthernet1/0	10.116.1.0	255.255.255.240	10.115.1.1	
20	Swap	29	PE-West IP:Ethernet0/1	80.80.80.8	255.255.255.255	10.112.1.1	
21	Swap	0	PE-West IP:Ethernet0/1	80.80.80.61	255.255.255.255	10.112.1.1	
22	Swap	31	PE-West IP:Ethernet0/1	80.80.80.62	255.255.255.255	10.112.1.1	
23	Untagged		PE-West IP:FastEthernet1/0	80.80.80.63	255.255.255.255	10.115.1.1	
24	Untagged		PE-West IP:FastEthernet1/0	192.168.1.0	255.255.255.0	10.115.1.1	
24	Untagged		PE-West IP:Ethernet0/1	192.168.1.0	255.255.255.0	10.112.1.1	
25	Untagged		PE-West IP:FastEthernet1/0	192.168.2.0	255.255.255.0	10.115.1.1	
25	Untagged		PE-West IP:Ethernet0/1	192.168.2.0	255.255.255.0	10.112.1.1	
26	Untagged		PE-West IP:Ethernet0/1	192.168.100.0	255.255.255.0	10.112.1.1	
26	Untagged		PE-West IP:FastEthernet1/0	192.168.100.0	255.255.255.0	10.115.1.1	
40	Untagged		PE-West IP:Ethernet0/3	80.80.80.64	255.255.255.255	10.111.1.1	

The *Label Switching Properties* dialog box is divided into two tabs, namely, the **Label Switching Table** and **VRF Table** tabs. The **Label Switching Table** tab describes the MPLS label switching entries used for traversing the MPLS core networks.

The following information is displayed in the **Label Switching Table** tab:

- **Incoming Label:** The details of the incoming MPLS label.

- **Action:** The type of action, namely, POP, Swap, Aggregate, and untagged. When the action is defined as POP an outgoing label is not required.
- **Outgoing Label:** The details of the outgoing MPLS label.
- **Out Interface:** The name of the outgoing interface as a hyperlink that displays the physical inventory of the device, specifically the sub-interfaces of the port.
- **IP Destination:** The IP address of the destination network.
- **Destination Mask:** The 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 we want to reach.
- **Sending Alarms:** This option is currently unavailable.

The **VRF Table** tab describes all the MPLS paths that terminate locally at a VRF. The **VRF Table** tab is displayed below.

Incomin...	Sending Alarms	VRF
27		PE-West VRF Black
28		PE-West VRF Black
29		PE-West VRF Black
30		PE-West VRF Black
31		PE-West VRF Blue
32		PE-West VRF SHEER
33		PE-West VRF SHEER
34		PE-West VRF SHEER
35		PE-West VRF TestSpoke
36		PE-West VRF TestSpoke
39		PE-West VRF SHEER

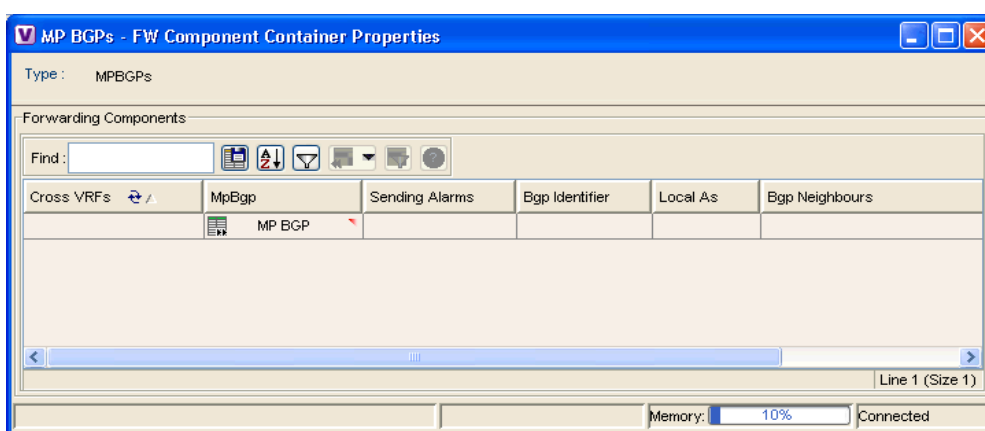
The following information is displayed in the **VRF Table** tab:

- **Incoming Label:** The details of the incoming VRF label.
- **Sending Alarms:** This option is currently unavailable.
- **VRF:** The VRF name as a hyperlink that displays the VRFs properties.

When a **TE Tunnel** starts, the initial TE tunnel information can be viewed by selecting the **LSEs/Label Switching** sub-branch and viewing the information displayed in the **Traffic Engineering LSPs** tab. Later additional information, like bandwidth allocation can be viewed. For more information, refer to page 63.

5.6 Viewing MP BGP Information

The **MP BGPs** branch displays the VRF name and cross VRF routing entries. An example of the *MP BGPs – FW Component Container Properties* dialog box is displayed below.



The following information is displayed in the *MP BGPs – FW Component Container Properties* dialog box:

- **Cross VRFs:** The cross VRF routing entries are displayed when double-clicking on a row. For a description of the table displayed, refer to page 31.
- **MpBgp:** The Multi Protocol BGP peer running on the local router.
- **Sending Alarms:** This option is currently unavailable.
- **Bgp Identifier:** The local BGP router (ID of the local system) IP address used by the local BGP peer when advertising routing information.
- **Local As:** The Autonomous System (AS) to which the BGP neighbor belongs.
- **Bgp Neighbors:** The table contains information on BGP entities that are known to the local BGP entity and exchange information with it.

5.6.1 Viewing BGP Neighbors

The **MP BGP** sub-branch, **Bgp Neighbors** tab displays a list of the routers used in the BGP network (autonomous system), including, the configuration and status of the connections between the routers in the inventory and all the other BGP members (routers displayed in the table).

The *MP BGP – MP BGP Properties* dialog box is divided into two tabs, namely, **Cross VRFs** and **Bgp Neighbors** tabs. The **Cross VRFs** tab is currently unavailable.

The **Bgp Neighbors** tab displays a list of the routers used in the BGP network (autonomous system), including the configuration and status of the connections between the router displayed in the inventory, and all the other BGP members (routers displayed in the table). An example of the **Bgp Neighbors** tab is displayed below.

Peer Kee...	Peer Remote Addr	Peer State	Sending Alarms	Bgp Neighbour Type	Peer Hold Time	Peer Remote As
30	80.80.80.64	Established		Client	90	100
40	80.80.80.65	Established		Client	120	100
40	80.80.80.61	Established		Client	120	100
40	80.80.80.63	Established		Client	120	100
40	102.0.0.2	Established		Client	120	112
40	80.80.80.60	Established		Client	120	100
40	80.80.80.62	Established		Client	120	100
60	80.80.80.1	Open Sent		Client	120	100

The following information is displayed in the **Bgp Neighbors** tab:

- **Peer Keep Alive:** The time interval in seconds between successive KEEPALIVE messages. The BGP process negotiates the KEEPALIVE time with its neighbor upon establishment of the connection.
- **Peer Remote Address:** The BGP peer remote IP address used by the BGP peer to exchange routing information with the local BGP peer.

Note: If the BGP peer is "Client" or "Non Client", the advertising policy is different for the different types of peers.

- **Peer State:** The state of the connection between the local BGP peer to the remote BGP peer. Valid values are: Idle, Connect, Active, Open Set, Open Confirm, and Established.

- **Sending Alarms:** This option is currently unavailable.
- **Bgp Neighbor Type:** Each and every BGP router is uniquely identified by a router ID. A route reflector is not a configuration of a specific router. A router may act as a route reflector if it has a BGP neighbor configured as a BGP client. A router may act as both a route reflector to some of its BGP neighbors (those that are configured as BGP clients) as well as a non-client BGP neighbor to those BGP neighbors that are configured as non-client BGP neighbors.

A route reflector performs the following logic when distributing routes to its BGP neighbors:

- A router will advertise to its client peers all routes learned from both other client and non-client peers.
- A router will advertise to its non-client peers only routes received from client peers.

For more information about route reflectors, refer to page 78.

- **Peer Hold Time:** The BGP Hold Time value (in seconds) that is used when negotiating with peers. According to BGP specifications, if the router does not receive successive KEEPALIVE and/or UPDATE and/or NOTIFICATION messages within the period specified in the Hold Time field of the OPEN message, then the BGP connection to the peer will be closed.
- **Peer Remote As:** The autonomous system ID of the BGP neighbor.
- **Distribute through Interface:** The local interface through which BGP information is distributed to BGP neighbors.
- **Peer Identifier:** The IP address by which the BGP recognizes and converses with its neighbor.

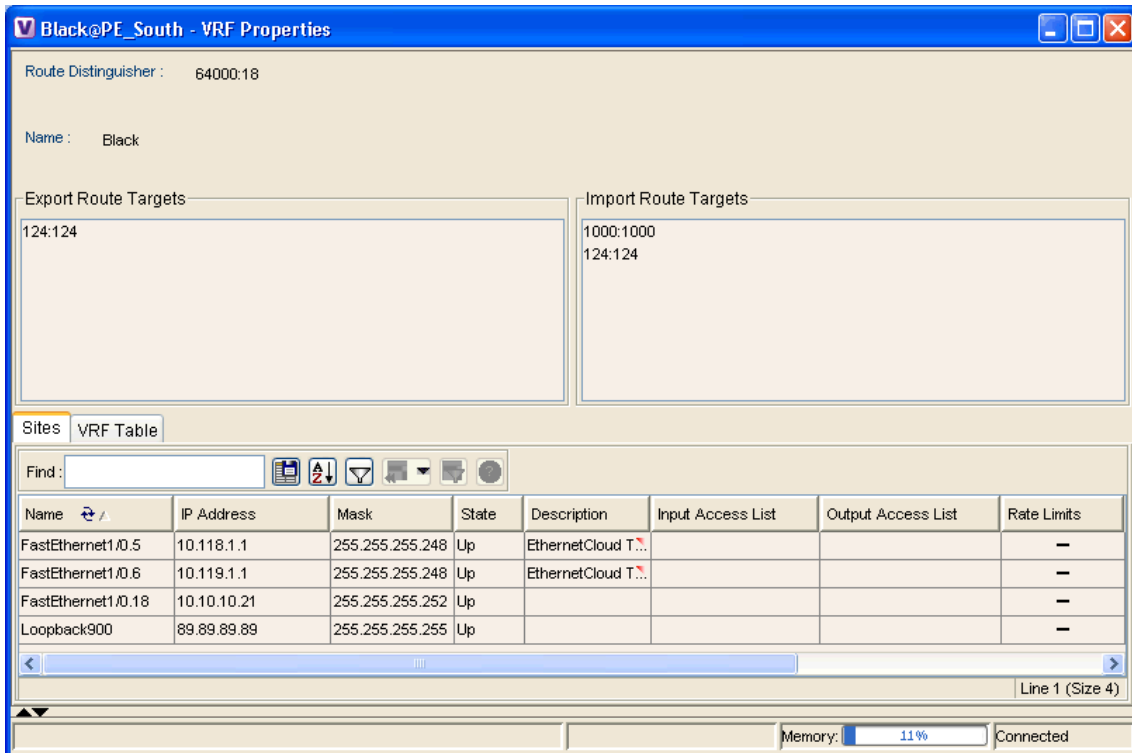
5.7 Viewing VRF Information

Sheer NetworkVision enables the user to view the VRF, and the import and export policies for each VRF.

To view a VRF's properties

1. Right-click on a VRF in the *Tree* pane or *Map* pane of the *Sheer NetworkVision* window to display the shortcut menu.

2. Select **Properties**. The *VRF Properties* dialog box for the VRF is displayed.



The following fields are displayed at the top of the *VRF Properties* dialog box:

- **Route Distinguisher:** The route distinguisher configured in the VRF.
- **Name:** The name of the VRF.

The **Export/Import Route Targets** areas displayed in the *VRF Properties* dialog box specify separately the export and import policies for each VRF.

The *VRF Properties* dialog box is divided into two tabs, namely, the **Sites** and **VRF Table** tabs. The **Sites** tab displays the interfaces connected to the VRF and the configuration of the interfaces. The following columns are displayed in the **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 details of the dotted decimal mask.
- **State:** The state of the sub-interface, namely, Up or Down.

- **Description:** A description of the interface.
- **Input Access List:** The access list applied to the inbound traffic of the interface.

Note: This parameter is only relevant for Cisco IOS devices.

- **Output Access List:** The access list applied to the outbound traffic of the interface.

Note: This parameter is only relevant for Cisco IOS devices.

- **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.
- **Site Name:** The name of the business element to which the interface is attached.
- **Sending Alarms:** This option is currently unavailable.


The **VRF Table** tab contains the VRF routing table for the device, namely, a collection of routes that are available or reachable to all the destinations or networks in this VRF. In addition, the forwarding table also contains MPLS encapsulation information.

The **VRF Table** tab is displayed below.

Dest...	Mask	Next Hop	BGP Next Hop	VRF Out Label	VRF In Label	MPLS Label	Type	Routing Protocol	Sending Alarms	Outgoing Int. Name
0.0.0.0	0.0.0.0	80.80.80.62					Indirect	BGP		
1.1.1.1	255.255...		80.80.80.64	102048		39	Indirect	BGP		
9.9.9.9	255.255...		80.80.80.8	33		16	Indirect	BGP		
10.10.10.0	255.255...		80.80.80.64	1025		39	Indirect	BGP		
10.10.10.20	255.255...	10.10.10.21			50		Direct	Local		FastEthernet1/0.18
10.56.0.0	255.255...		80.80.80.62	47			Indirect	BGP		

The following columns are displayed in the **VRF Table** tab:

- **Destination:** The destination of the specific network.

- **Mask:** The mask of the specific network.
 - **Next Hop:** The CE address from where to continue to get to a specific address. This field is empty when the routing entry goes to the PE.
 - **BGP Next Hop:** The PE address from where to continue to get to a specific address. This field is empty when the routing entry goes to the CE.
 - **VRF Out Label:** The label sent with MPLS traffic.
 - **VRF In Label:** The label that is expected when MPLS traffic is received.
 - **MPLS Label:** The MPLS label.
 - **Type:** The type can be direct (local) or indirect
 - **Routing Protocol:** The routing protocol used to communicate with the other Sites/VRFs, namely, BGP or local.
 - **Sending Alarms:** This option is currently unavailable.
 - **Outgoing Int. Name:** The name of the outgoing interface is displayed if the Routing Protocol type is local.
3. Click  to close the *VRF Properties* dialog box.

5.7.1 Opening the VRF Table

Sheer NetworkVision enables you to view the VRF table for a VRF.

To open the VRF Table

1. Right-click on the required VRF in the *Tree* pane or *Map* pane of the *Sheer NetworkVision* window to display the shortcut menu.

2. Select **Open VRF Table**. The *VRF Table* dialog box is displayed.

Dest...	Mask	Next Hop	BGP Next Hop	VRF Out Label	VRF In Label	MPLS Label	Type	Routing Protocol	Sending Alarms	Outgoing Int. Name
0.0.0.0	0.0.0.0	80.80.80.62					Indirect	BGP		
1.1.1.1	255.255....		80.80.80.64	102048		39	Indirect	BGP		
9.9.9.9	255.255....		80.80.80.8	33		16	Indirect	BGP		
10.10.10.0	255.255....		80.80.80.64	1025		39	Indirect	BGP		
10.10.10.20	255.255....	10.10.10.21			50		Direct	Local		FastEthernet1/0.18
10.56.0.0	255.255....		80.80.80.62	47			Indirect	BGP		
10.118.1.0	255.255....	10.118.1.1			51		Direct	Local		FastEthernet1/0.5
10.119.1.0	255.255....	10.119.1.1			52		Direct	Local		FastEthernet1/0.6
20.20.20.0	255.255....		80.80.80.60	32		37	Indirect	BGP		
20.20.20.2	255.255....		80.80.80.60	33		37	Indirect	BGP		
20.20.20.16	255.255....		80.80.80.64	1025		39	Indirect	BGP		
30.0.0.0	255.255....		80.80.80.64	1025		39	Indirect	BGP		
30.30.30.0	255.255....		80.80.80.8	34		16	Indirect	BGP		
50.50.50.50	255.255....		80.80.80.64	1025		39	Indirect	BGP		

For more information about the columns displayed in the *VRF Table* dialog box, refer to *Section 4.3*.

3. Click to close the *VRF Table* dialog box.

5.7.2 Viewing Cross VRF Routing Entries

The Cross VRF routing entries display routing information learned from the BGP neighbors (BGP knowledge base). The parameters of the cross VRF routing entries are displayed in the *Cross VRF Properties* dialog box.

The Cross VRF Routing entries are displayed by double-clicking on an entry (row) in the **Cross VRFs** tab of the *MP BGP Properties* pane. An example of the *Cross VRF Properties* dialog box is displayed below.

Destination	Mask	Next Hop	Out Going VRF	Out Tag	In Tag	Sending Alarms
9.9.9.9	255.255....	0.0.0.0	PE_North VRF Black	aggregate	33	
30.30.30.0	255.255....	0.0.0.0	PE_North VRF Black	aggregate	34	

The following information is displayed in the *Cross VRF Properties* dialog box:

- **Destination:** The destination of the specific network.
- **Mask:** The mask of the specific network.
- **Next Hop:** The PE address from where 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 Out Going 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 in order to reach the destination address that is connected to the other VRF.
- **In Tag:** The MPLS label used by this router in order 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 where the traffic originated.
- **Sending Alarms:** This option is currently unavailable.

5.8 Viewing Pseudo Wire End-to-End Emulation (PWE3) Tunnels

The **Pseudo Wire Tunnels (PWE3)** branch displays a list of the Layer 2 tunnel edge properties (per edge), including, tunnel status and VC labels. An example of the *Pseudo Wire Tunnels (Martini) – Tunnel Container Properties* dialog box is displayed below.

Port	Peer	Peer VC Label	Tunnel Status	Local VC Label	Local Router IP	Tunnel ID	Peer Router IP	Signaling Protocol
Channel Groups DLCI 600	22@PE_South	31	down	26	80.80.80.61	22	80.80.80.63	LDP
Channel Groups VC 0/123			down	39	80.80.80.61	123	10.111.3.2	LDP
Channel Groups VC 0/444	12@PE_South	25	up	23	80.80.80.61	12	80.80.80.63	LDP
Channel Groups VC 0/446	23@PE_South	62	down	25	80.80.80.61	23	80.80.80.63	LDP
Channel Groups VC 0/500	500@PE_South	27	up	38	80.80.80.61	500	80.80.80.63	LDP
Channel Groups VC 0/501	501@PE_South	28	up	40	80.80.80.61	501	80.80.80.63	LDP
Channel Groups VC 0/510	510@PE_South	29	up	46	80.80.80.61	510	80.80.80.63	LDP
Channel Groups VC 0/700		33	up	47	80.80.80.61	700	80.80.80.65	LDP
Channel Groups VC 0/5445	13@PE_South	26	up	24	80.80.80.61	13	80.80.80.63	LDP
P-North#0:FastEthernet0/0:200			down	53	80.80.80.61	200	10.111.3.2	LDP
P-North#0:FastEthernet0/0:333	333@PE_South	36	up	21	80.80.80.61	333	80.80.80.63	LDP
P-North#0:FastEthernet0/0:334	334@PE_South	57	up	45	80.80.80.61	334	80.80.80.63	LDP
P-North#0:FastEthernet0/0:335	335@PE_South	58	up	49	80.80.80.61	335	80.80.80.63	LDP
P-North#0:FastEthernet0/0:336	336@PE_South	59	up	50	80.80.80.61	336	80.80.80.63	LDP
P-North#0:FastEthernet0/0:337	337@PE_South	60	up	51	80.80.80.61	337	80.80.80.63	LDP
P-North#0:FastEthernet0/0:400			down	16	80.80.80.61	336	80.80.80.62	LDP
P-North#0:FastEthernet0/0:888	999@PE_South	64	up	52	80.80.80.61	999	80.80.80.63	LDP

The following information is displayed in the **Tunnel Edges** table:

- **Port:** The name of the sub-interface or port.
- **Peer:** The details of the selected LCP's peer (edge peer).
- **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.
- **Tunnel Status:** The operational state of the tunnel, namely, **up** or **down**.
- **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.
- **Local Router IP:** The IP of this tunnel edge, which is used as the MPLS router ID.
- **Tunnel ID:** The identifier that along with the router IPs of the two tunnel edges identifies the **PWE3** tunnel.

- **Peer Router IP:** The IP of the peer tunnel edge, which is used as the MPLS router ID.
- **Signaling Protocol:** The protocol used by MPLS to build the tunnel, for example, LDP or TDP.
- **Sending Alarms:** This option is currently unavailable.

For information on viewing **Links** in MPLS-TE (Traffic Engineering) tunnels, refer to the respective sections in *Chapter 7, Calculating Impact Analysis* and *Chapter 8,*

Working with PathTracer in VPN Service View in this user's guide.

5.9 Viewing MPLS TE Tunnel Information

The **Traffic Engineering Tunnels** branch displays specific TE tunnel information on TE tunnels. An example of the *Traffic Engineering Tunnels – Tunnel Container Properties* dialog box is displayed below.

Name	Tunnel destination	Administrative status	Operational status	Outgoing label	Description	Outgoing interface	Bandwidth	Setup priority
Tunnel10	192.168.200.3	Up	Up	21	East via North	West IP:Ethernet0/0	100	4
Tunnel11	192.168.200.3	Up	Up	24	East via South	West IP:Ethernet0/3	100	4
Tunnel120	192.168.200.4	Down	Down		West_t120		100	4

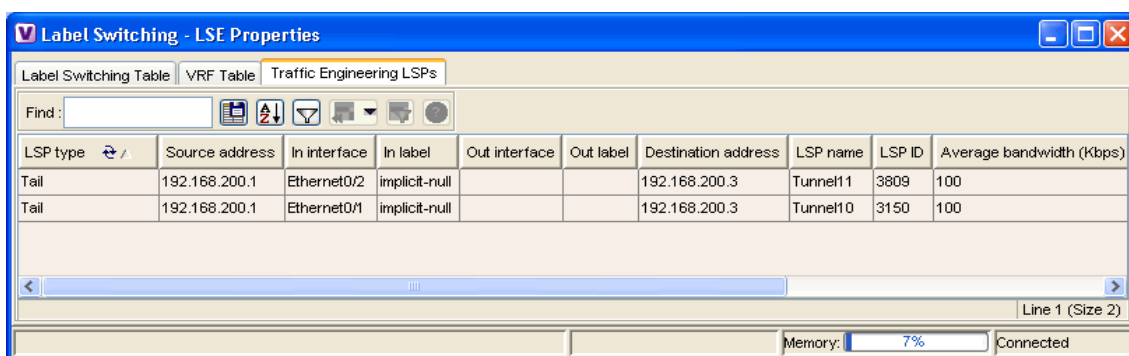
The name of the table is displayed at the top of the *Properties* window in the title bar. The following information is displayed in the **Tunnel Edges** table:

- **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, namely, up or down.
- **Operational Status:** The operational state of the tunnel, namely, up or down.

- **Outgoing Label:** The TE tunnel's MPLS label distinguishing the LSP selection in the next device.
- **Description:** A textual description of the tunnel.
- **Outgoing Interface:** The interface through which the tunnel exits the device.
- **Bandwidth (Kbps):** Bandwidth specification for this tunnel.
- **Setup Priority:** The tunnel's priority upon path setup.
- **Hold Priority:** The tunnel's priority after path setup, when other tunnels try to remove it and claim its resources.
- **Affinity:** The tunnel's preferential bits for specific links.
- **Affinity Mask:** Dictates which bits from the tunnel's affinity should be compared to which bits of the link's attribute bits.
- **Auto Route:** If enabled, destinations behind the tunnel are routed through the tunnel.
- **Lockdown:** If enabled, the tunnel cannot be rerouted.
- **Path Type:** The tunnel's path can be either dynamic, in which case, the tunnels is routed along the ordinary routing decisions after taking into account the constraints the tunnel imposes (attributes, priority, bandwidth) or explicit, in which case the route is explicitly plotted with included and excluded links.
- **Average Rate, Burst and Peak:** Flow specification measured for this tunnel (in Kbps).
- **LSP ID:** LSP identification number.
- **Sending Alarms:** This option is currently unavailable.

5.9.1 Traffic Engineering LSPs

The **Label Switching** sub-branch, **Traffic Engineering LSPs** tab displays TE tunnel LSPs information. Devices which have LSPs running TE tunnels (either as head-ends, mid-point or tail-ends), display tunnel information in the **Traffic Engineering LSPs** tab. An example of the *Label Switching – LSE Properties* dialog box is displayed below:



LSP type	Source address	In interface	In label	Out interface	Out label	Destination address	LSP name	LSP ID	Average bandwidth (Kbps)
Tail	192.168.200.1	Ethernet0/2	implicit-null			192.168.200.3	Tunnel11	3809	100
Tail	192.168.200.1	Ethernet0/1	implicit-null			192.168.200.3	Tunnel10	3150	100

The following information is displayed in the **Traffic Engineering LSPs** tab:

- **LSP Type:** The type of LSP:
 - **Head:** a tunnel starting in this device
 - **Midpoint:** a tunnel passing through this device
 - **Tail:** a tunnel terminating in this device
- **Source Address:** IP address of the device in which the tunnel starts (where the tunnel's "head" is).
- **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 will be appended to tunnel packets going out via 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.
- **LSP ID:** LSP identification number.
- **Average Bandwidth:** Flow specification measured for this tunnel (in Kbps).
- **Burst:** Flow specification measured for this tunnel (in Kbps).
- **Peak:** Flow specification measured for this tunnel (in Kbps).
- **Sending Alarms:** This option is currently unavailable.

6 Fault Management in MPLS Networks

About this chapter:

This chapter describes the alarms that Sheer DNA detects and reports for BGP, MPLS TE (using RSVP TE), MPLS Black Holes, as well as alarm reports for Layer 2 and Layer 3 VPNs.

MPLS Related Faults, page 66, describes the “MPLS black hole found” and “Broken LSP discovered” alarms.

BGP Related Faults, page 68, describes the “BGP neighbor down” alarm.

Traffic Engineering Faults, page 69, describes the “MPLS TE tunnel down”, “MPLS TE tunnel flapping” and “Tunnel reoptimized” alarms.

Layer 2 VPN Faults, page 70, describes the “Pseudo Wire (L2 VPN) MPLS tunnel down” alarm.

Alarms Summary, page 71, provides a brief description of the alarms for VPNs, including their severity and the up alarm (clearing alarm) for each.

Sheer DNA supports the following alarms:

- **MPLS Related Faults:**
 - MPLS black hole found
 - Broken LSP discovered
- **BGP Related Faults:**
 - BGP neighbor down
- **Traffic Engineering Faults:**
 - MPLS TE tunnel down
 - MPLS TE tunnel flapping
 - Tunnel reoptimized
- **Layer 2 VPN Faults:**
 - Pseudo Wire (L2 VPN) MPLS tunnel down

The alarms are displayed in the *Ticket* pane of the *Sheer NetworkVision* window. For more information about the *Ticket* pane, refer to the *Cisco Active Network Abstraction NetworkVision User's Guide*.

6.1 MPLS Related Faults

This section includes descriptions of the following MPLS related faults:

- MPLS black hole found
- Broken LSP discovered

6.1.1 MPLS Black Hole Found Alarm

A MPLS “black hole” is defined as an abnormal termination of a MPLS path (LSP) inside a MPLS network. A MPLS “black hole” exists when on a specific interface there are untagged entries destined for a known PE router. It is assumed that a router functions as a PE router if there are services using the MPLS network, such as L3 VPNs or Pseudo Wire (L2 VPN) MPLS Tunnels. Note that the untagged interfaces may exist in the network in normal situations. For example, where the boundary of the MPLS cloud has untagged interfaces this is still considered normal.

The existence of a MPLS “black hole” results in a loss of all of the MPLS labels on a packet including the VPN information which lies in the inner MPLS label. So if a packet goes through an untagged interface, the VPN information is lost. The VPN information loss translates directly to VPN sites losing connectivity.

A “MPLS Black Hole Found” alarm is detected actively by the system, namely, service alarms are generated whenever Sheer DNA discovers a MPLS interface that has at least one untagged LSP leading to a known PE router.

Black hole alarms are detected either:

- When the system is loaded for the first time and performs the initial discovery of the network.
- Through the ongoing discovery process, which identifies changes in the network.

6.1.2 Broken LSP Discovered Alarm

The “MPLS Black Hole Found” alarm activates a backward flow on the specific untagged entry in order to traverse the full path of the LSPs passing through it. If Sheer DNA locates services (VRFs, Pseudo Wire L2 tunnels) along this path that are using these LSPs a “Broken LSP Discovered” alarm is issued. Such services can only be found on PE routers and they can be found on more than one PE router. The source of the “Broken LSP Discovered” alarm is the PE router on which the service was discovered and in many cases this router is different from the router that issued the “MPLS Black Hole Found” alarm.

“Broken LSP Discovered” alarms are correlated to the “MPLS Black Hole Found” alarm (except in the case of a Black hole alarm due to a link down as described on page 68).

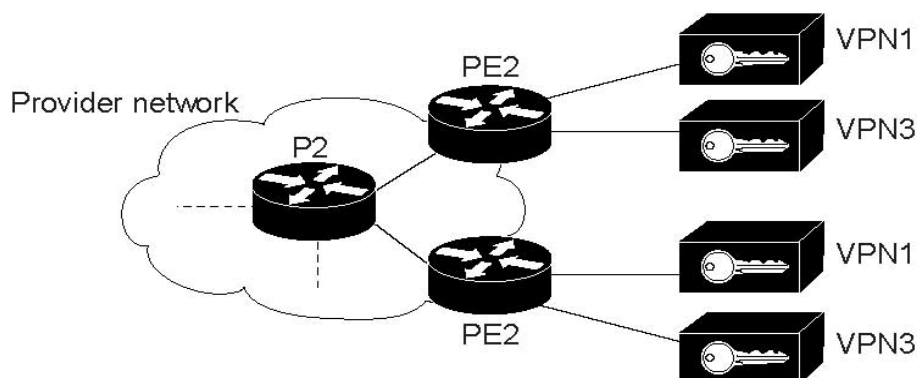
The “Broken LSP Discovered” alarm is detected actively by the system, namely, service alarms are generated.

An example of a MPLS black hole scenario is provided below.

In the network described in this example, the shortest path from PE2 to PE3 is PE2->P2->PE3. The link between P2 and PE3 is a MPLS link, meaning interfaces on both side of the link are configured as MPLS interfaces. Also assume that for some reason the MPLS configuration is incomplete or incorrect, namely:

- Only one interface is configured as a MPLS interface.
- The label distribution protocol is configured differently on both interfaces (protocol mismatch).

In this case the label switching table on P2 and PE3 will have untagged entries for the LSPs between PE2 and PE3. If PE2 and PE3 have VPN services (VRFs, Pseudo Wire tunnels) the outcome will be that the data flow between PE2 and PE3 will be affected.



In this case Sheer DNA does the following:

- Identifies untagged label switching entries on P2 and PE3.
- Issues “MPLS Black Hole Found” alarms on the interfaces on both sides of the link (since the LSP is unidirectional).
- Initiates a backward flow starting from the link on the specific untagged entries and identifies the 2 LSPs traversing the link, namely:
 - LSP from PE2 to PE3.
 - LSP from PE3 to PE2.
- Issues “Broken LSP Discovered” alarms on both LSPs in PE2 and PE3, which are correlated to the corresponding “MPLS Black Hole Found” alarm.

Note: The clearing alarm does not activate flows to locate the LSPs that were passing through it in order to issue a clearing alarm for Broken LSPs, but rather uses the auto clear functionality. Using this functionality, once the “MPLS Black hole found” alarm is cleared, then after a specific (configured) time interval, all of the alarms correlated to the “MPLS Black hole found” alarm are automatically cleared. The auto clear mechanism is performed in the Gateway and the relevant interval is configured as part of the alarm configuration in the Registry.

6.1.3 Black Hole to Link Down

In a case where a link down event in a MPLS network has caused an IP reroute and therefore LDP redistribution, a case may arise where new LSPs are now redirected through a non-MPLS segment thereby creating a black hole.

In this case the “Broken LSP Discovered” alarms are issued as described in *Section 6.1.2*, but all of the broken LSPs that are found are correlated to the “Link Down” alarm and not to the “MPLS Black Hole Found” alarm.

6.2 BGP Related Faults

Sheer DNA monitors BGP neighbor information and makes correlation and impact analysis information available to users.

This section includes a description of the following BGP related faults:

- BGP neighbor down

6.2.1 BGP Neighbor Down

In IP/MPLS VPN networks, when BGP connectivity is lost to a specific device, the resulting BGP connection loss translates directly to VPN sites losing connectivity.

The VNE models the BGP connection between routers and actively monitors its state. A BGP neighbor loss alarm is generated from both sides of the connection in the case of a connectivity loss, resulting in alarms and tickets being issued and users viewing impact analysis information.

The correlation engine identifies various faults that affect the BGP connection and reports them as the root cause for the BGP neighbor loss alarm. For example, Link down, CPU over utilized, and Link data loss.

Note: “BGP Neighbor Down” alarms are not correlated to each other but are correlated to the root cause of the connectivity loss.

The “BGP Neighbor Down” alarm is detected actively by the system, namely, service alarms are generated.

The system also supports “BGP neighbor down” syslogs.

6.3 Traffic Engineering Faults

This section includes a description of the following Traffic Engineering related faults:

- MPLS TE tunnel down
- MPLS TE tunnel flapping
- Tunnel reoptimized

6.3.1 MPLS TE Tunnel Down and TE Tunnel Flapping

When a TE tunnel’s operational status changes to down and the tunnel is not flapping, the system generates a “Tunnel Down” alarm.

The correlation engine identifies various faults that affect the TE tunnel’s status and reports on them as the root cause for the TE “Tunnel Down” alarm, for example, Link down.

Multiple up and down alarms that are generated during a short time interval are suppressed and displayed as a “Tunnel Flapping” alarm (according to the specific flapping configuration).

The “MPLS TE Tunnel Down” and the “TE Tunnel flapping” alarms are detected actively by the system, namely, service alarms are generated.

The system also supports “MPLS TE Tunnel Down” syslog, which are correlated to the service alarm.

6.3.2 Tunnel Reoptimized

Tunnel reoptimization occurs when a tunnel is up and its route changes but the tunnel continues to remain up. When a TE tunnel is reoptimized to take a different path, the system parses the tunnel reoptimized syslog, if such a syslog is available, and displays this syslog as a ticket.

The “Tunnel Reoptimized” alarm is generated from a syslog message sent by the router.

6.4 Layer 2 VPN Faults

This section includes a description of the Layer 2 VPN fault, Pseudo Wire (L2 VPN) MPLS tunnel down.

6.4.1 Pseudo Wire (L2 VPN) MPLS Tunnel Down

A “Pseudo Wire MPLS Tunnel Down” alarm is issued when the pseudo wire link goes down, namely, the pseudo wire tunnel is reported as down from both the devices (based on the status of the tunnel), and the tunnel is not flapping.

The correlation engine identifies various faults that affect the Pseudo Wire tunnel status and reports on them as the root cause for the “Pseudo Wire MPLS Tunnel Down” alarm, for example, Link down.

Sheer DNA traces the LSE path to the edge of the **PWE3** tunnel and marks the edges of the tunnel as affected.

The “Pseudo Wire MPLS Tunnel Down” alarm is detected actively by the system, namely, service alarms are generated.

6.5 Alarms Summary

The following section describes the alarms that may be displayed in the *Ticket* pane of the *Sheer NetworkVision* window for VPNs, including their severity and the up alarm for each:

Alarm	Default Severity	Description	Up Alarm
BGP Neighbor Down	Red (critical)	The “BGP Neighbor Down” alarm is generated whenever BGP connectivity is lost to a specific device.	BGP Neighbor Found
MPLS Black Hole Found	Orange (major)	A “MPLS Black Hole Found” alarm is generated whenever Sheer DNA discovers a MPLS interface that has at least one untagged LSP leading to a known PE router.	MPLS Black Hole Cleared
Broken LSP Discovered	Orange (major)	The “MPLS Black Hole Found” alarm activates a backward flow on the specific untagged entry in order to traverse the full path of the LSPs passing through it. The “Broken LSP Discovered” alarm is generated whenever Sheer DNA locates services (VRFs, Pseudo Wire L2 tunnels) along this path that are using these LSPs.	N/A
MPLS TE Tunnel Down	Orange (major)	The “MPLS TE Tunnel Down” alarm is generated whenever a TE tunnel’s operational status changes to down and the tunnel is not flapping.	MPLS TE Tunnel Up
MPLS TE Tunnel Flapping	Orange (major)	The “TE Tunnel flapping” alarm is generated whenever multiple up and down alarms are generated during a short time interval and they are suppressed.	Is the last state of the tunnel after it has stopped flapping

Alarm	Default Severity	Description	Up Alarm
Pseudo Wire (L2 VPN) MPLS Tunnel Down	Yellow (minor)	The “Pseudo Wire MPLS Tunnel Down” alarm is generated whenever the pseudo wire link goes down, namely, the pseudo wire tunnel is reported as down from both the devices (based on the status of the tunnel).	Layer 2 Tunnel Up
Tunnel Reoptimized	Dark Blue (information)	The “Tunnel Reoptimized” alarm is generated from a syslog message sent by the router whenever a tunnel is up and its route changes but the tunnel continues to remain up.	N/A

For more information about the *Ticket* pane, refer to the *Cisco Active Network Abstraction NetworkVision User's Guide*.

7 Calculating Impact Analysis

About this chapter:

This chapter provides an overview of the service impact analysis solution and supported scenarios, which are used in VPN networks that are based on MPLS, including Layer 3 and Layer 2 VPNs. In addition, it briefly describes proactive and automatic impact analysis.

About Service Impact Analysis, below, describes the service impact analysis solution.

Service Impact Analysis for MPLS Based VPN Services, page 75, describes the impact analysis process for Layer 3 VPN and Pseudo Wire (Layer 2 VPN) scenarios.

Supported Fault Scenarios, page 76, describes the scenarios supported by the service impact analysis solution.

7.1 About Service Impact Analysis

Sheer DNA analyzes network faults in order to determine which network elements involved in the VPN services (such as interfaces on the PE) are affected or potentially affected by the fault.

7.1.1 Automatic Impact Analysis

When a fault occurs Sheer DNA automatically (this behavior can be configured by the user) generates the list of potential and actual service resources that were affected by a fault and embeds this information in the ticket along with all of the correlated faults.

Affected Severity

When the impact analysis solution is **automatic** the affected parties can be marked with one of the following severities:

- **Potentially Affected:** The service may be affected but it's real state is unknown.
- **Real Affected:** The service is affected.
- **Recovered:** The service is recovered. This state only relates to entries that were previously marked as potentially affected. It only indicates that there is an alternate route to the service, regardless of the service quality (level).

The initial impact report may mark the services as either **Potentially Affected** or **Real Affected**. As time progresses and more information is accumulated from the network the system may issue an additional report to indicate which of the potentially affected parties are **Real Affected** or **Recovered**.

The indications for these states are available both through the API and in the GUI.

Note: The reported impact severities vary between fault scenarios. For more information about specific support for each fault scenario, refer to page 76.

Note: When the alarm is cleared there is no **Clear** state for the affected services but the user can identify that the alarm was cleared by checking the **Alarm Clear State** column in the **Affected Parties** tab of the *Ticket Properties* window. For more information about the **Affected Parties** tab of the *Ticket Properties* window, refer to *Chapter 8, Working with Tickets* in the *Cisco Active Network Abstraction NetworkVision User's Guide*.

For more information about automatic impact analysis, refer to *Chapter 8, Working with Tickets* in the *Cisco Active Network Abstraction NetworkVision User's Guide*.

7.1.2 Proactive Impact Analysis

Sheer DNA provides 'what-if' scenarios for determining the *possible* affect of network failures. This enables on-demand calculation of affected VPN Sites 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, the Sheer DNA fabric initiates an end-to-end flow, which determines all the potentially affected edges in the affected VPNs.

The proactive impact analysis solution is available in the:

- *Link Properties* dialog box when selecting a physical link
- *Topological Link Properties* window when selecting a physical link in the *Links View*.

For more information about proactive impact analysis, refer to *Chapter 7, Working with Links* in the *Cisco Active Network Abstraction NetworkVision User's Guide*.

7.2 Service Impact Analysis for MPLS Based VPN Services

A MPLS network with Provider Edge (PE) routers is supported, where the PE routers implement either:

- L3 VPN (RFC2547) and/or
- Pseudo Wire - L2 VPN

Each scenario is described separately.

Note: The description provided in this chapter refers only to faults in the MPLS core and not to faults in access networks.

7.2.1 L3 VPN Report (VRFs as Affected)

When affected parties are generated using the impact solution the real VRFs are displayed as the affected parties on the PE routers that lost connectivity between them in the *Ticket Properties* window.

Note: There is an option available in the Registry to report on the IP interfaces which are attached to the VRFs as the affected parties as well. Changes to the Registry should only be carried out with the support of Cisco Professional Services.

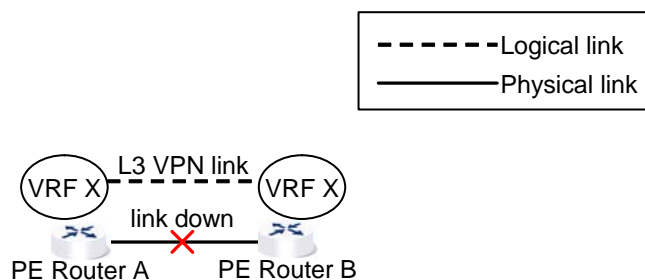
The number of affected parties that are reported are calculated from the pairs of VRFs and are reported in the *Ticket Properties* window.

The structure of the edge points ID is as follows:

Device ID \ VRF ID \ Sub interface (or interface) ID.

Note: In the structure described above “Sub interface (or interface) ID” is optional.

In the example below, there are two PEs A and B with the VRF X in the same VPN:



The Layer 3 VPN faults that are reported in this example are AX – BX.

7.2.2 Pseudo Wire (L2 VPN) Report (PWE3 Tunnels as Affected)

When a **PWE3** tunnel goes down and an alarm occurs, the affected service resources are calculated by tracing the LSP to the edge of the **PWE3** tunnel and collecting the affected pairs from both sides of the **PWE3** tunnel. The edges of the tunnel are marked as affected.

The affected pairs are displayed in the *Ticket Properties* window. For more information about the *Ticket Properties* window, refer to *Chapter 8, Working with Tickets* in the *Cisco Active Network Abstraction NetworkVision User's Guide*.

7.3 Supported Fault Scenarios

The following fault scenarios trigger automatic impact analysis calculation:

- Link Down, page 77.
- Link Over Utilized / Data Loss, page 77.
- BGP Neighbor Down, page 78.
- Broken LSP Discovered, page 81.
- MPLS TE Tunnel Down, page 81.
- Pseudo Wire (L2 VPN) MPLS Tunnel Down, page 81.

The following criteria are used in the tables that are described in the sections that follow:

- **Impact Calculation:** Describes the way in which the affected parties are calculated by system flows.
- **Reported Affected Severity:** Describes the kind of severity generated by the alarm.

Note: Proactive impact analysis is only supported for links.

7.3.1 Link Down

Impact calculation	<ul style="list-style-type: none"> Initiates an affected flow in order to determine the affected parties using the LSPs traversing the link.
Reported affected severity	<ul style="list-style-type: none"> The “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: <ul style="list-style-type: none"> 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 <i>Ticket Properties</i> dialog box displays the latest severity, namely, Real affected. The <i>Affected Parties Destination Properties</i> dialog box displays both reported severities. <p>This functionality is currently only supported for “Link Down”.</p>

7.3.2 Link Over Utilized / Data Loss

Impact calculation	Initiates an affected flow in order to determine the affected parties using the LSPs traversing the link.
Reported affected severity	Only reports on potentially affected.

7.3.3 BGP Neighbor Down

Impact calculation	<ul style="list-style-type: none"> Initiates a local affected flow to all VRFs that are present on the issuing device. Each local VRF which has route entries with a next hop IP that was learned from the BGP neighbor that was lost, collects VRFs from both sides and pairs them together as affected. Supports a Route Reflector configuration, whereby during the affected search, affected parties are located on all BGP neighbors learned via the Route Reflector.
Reported affected severity	Only reports on real affected on the IBGP domain.

Note: The affected only relate to L3 VPN services.

Supporting Route Reflector

Background: The Challenge of the Route Reflector

BGP rules require that all routers within an autonomous system be fully meshed. For large networks, this requirement represents a severe scaling problem. Route reflectors enable a BGP entity to establish a single BGP connection with a peer, where through that single peer, routing information is learned from other peers. As a result the number of BGP sessions and connections is greatly reduced.

As a side effect of decreasing the amount of BGP connections, the presence of route reflectors also separates the data path and the control path. For example, data packets going from A to B do not go through the route reflector while the routing updates between A and B do.

Route Reflector Support

Each and every BGP router is uniquely identified by a router ID. A route reflector is not a configuration of a specific router. A router may act as a route reflector if it has a BGP neighbor configured as a BGP client. A router may act as both a route reflector to some of its BGP neighbors (those that are configured as BGP clients) as well as a non-client BGP neighbor to those BGP neighbors that are configured as non-client BGP neighbors.

A route reflector performs the following logic when distributing routes to its BGP neighbors:

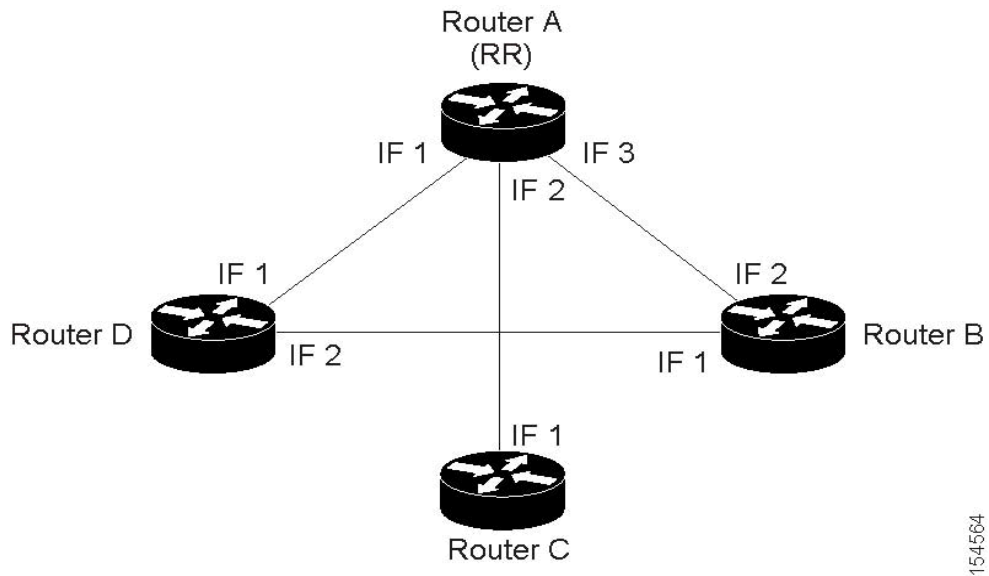
- A router will advertise to its client peers all routes learned from both other client and non-client peers.
- A router will advertise to its non-client peers only routes received from client peers.

Router ID distribution follows the same logic described above.

Sheer DNA modeling provides for each interface, a list of one or more router IDs. This reflects the network behavior of receiving BGP updates from a BGP router (possessing that ID) through that interface.

The VNE also maintains the nature of the relationship (client and non-client) between the various VNEs representing the BGP routers.

An example is displayed below.



154564

For example, in the setup above the following configuration is applied:

- Router A (router ID A) has clients configured B, C and D. Therefore it serves as the route reflector for these BGP routers.
- Routers B, C, and D all have Router A as a BGP non-client neighbor.
- Router D and Router B also have each other configured as BGP non-client neighbors.

In this case in Sheer DNA the following information is maintained by a VNE:

- Router B learns router ID D from interface 1.
- Router B learns router IDs (A, C, and D) from interface 2.
- Router C learns router IDs (A, B, and D) from interface 1.
- Router D learns router ID B from interface 2.
- Router D learns router IDs (A, B, and C) from interface 1.
- Router A learns router ID D from interface 1.
- Router A learns router ID C from interface 2.
- Router A learns router ID B from interface 3.

BGP Neighbor Down Scenario 1

- A BGP connection has been lost from Router A to Router B.
- Router A notifies both Routers C and D of a loss of router ID B.

- Router C removes Router B's ID from its tables and completely loses connectivity to it, resulting in real affected impact analysis.
- Router D loses Router B's ID learned from interface 1 but it still has Router B's ID that was learned through interface 2 therefore no impact analysis is performed.

BGP Neighbor Down Scenario 2

- A BGP connection is lost from Router B to Router D.
- Router B does not notify Router A of its router ID loss because Router A is configured in Router B's tables as a non-client peer.
- Router D does not notify Router A of its router ID loss because Router A is configured in Router D's tables as a non-client peer.
- Router B notes that Router D's ID is no longer learned through interface 1.
- Router D notes that Router B's ID is no longer learned through interface 2.
- No impact analysis is performed.

7.3.4 Broken LSP Discovered

Impact calculation	Initiates an affected flow in order to determine all the affected parties using the LSP.
Reported affected severity	Only reports on real affected. When the link down is cleared, all of the correlated broken LSP alarms are auto-cleared.

7.3.5 MPLS TE Tunnel Down

Impact calculation	Initiates a flow to look for affected parties.
Reported affected severity	Only reports on real affected.

Note: The MPLS TE Tunnel Flapping fault scenario is a transitory state of flapping.

7.3.6 Pseudo Wire (L2 VPN) MPLS Tunnel Down

Impact calculation	Initiates a flow to look for the affected parties.
Reported affected severity	Only reports on real affected on the MPLS domain.

8 Working with PathTracer in VPN Service View

About this chapter:

This chapter describes the Sheer PathTracer for Layer 2 and Layer 3 VPNs, and for MPLS Traffic Engineering tunnels, including opening the Sheer PathTracer and viewing VPN and TE tunnel information in the PathTracer.

Sheer PathTracer Tracing Capability, page 84, provides a brief description of Sheer PathTracer.

Opening Sheer PathTracer Over MPLS Networks, page 85, describes opening the Sheer PathTracer.

Sheer PathTracer Windows, page 86, briefly describes the *Sheer PathTracer Multi-Path* and *Single-Path* windows working environment and the information that can be viewed.

Using PathTracer for Layer 3 VPN, page 89, describes using the Sheer PathTracer for Layer 3 VPNs, including opening the Sheer PathTracer and viewing path information.

Using PathTracer for Layer 2 VPN, page 91, describes using the Sheer PathTracer for Layer 2 VPNs, including opening the Sheer PathTracer and viewing path information.

Using PathTracer for MPLS Traffic Engineering Tunnels, page 92, describes using the Sheer PathTracer for MPLS TE tunnels, including opening the Sheer PathTracer and viewing path information.

For more information about the Sheer PathTracer, refer to the *Cisco Active Network Abstraction NetworkVision User's Guide, Chapter 9*.

8.1 Sheer PathTracer Tracing Capability

Based on its extensive, up-to-date knowledge of the network, Sheer PathTracer traces service routes or network connectivity between two points in the network (or from a single starting point to an IP) providing performance information simultaneously for multiple networking layers along single as well as multiple routes. As it relies on the network model, end-to-end paths are provided across technologies and at different layers of the stack. It also displays various traffic and error statistics for each link and for each hop helping to pinpoint problems that may affect the service or cause service degradation.

Sheer PathTracer immediately pinpoints and highlights exactly where the service affecting problems lie (namely, devices, slots, ports, protocol stacks, including comprehensive multi-layer status information with relevant configuration and traffic parameters). Sheer DNA understands and is able to display the various services on the network due to the up-to-date knowledge of the network.

Sheer PathTracer enables the user to view multiple paths between the source and the destination (or from a source to number of destinations) in the *Sheer PathTracer Multi-Path* window, or to view a selected single-path in the *Sheer PathTracer Single-Path* window:

- *Sheer PathTracer Multi-Path* window: Displays all the discovered paths available between the selected source and destination(s), including devices, and links. For more information, refer to the *Chapter 9* of the *Cisco Active Network Abstraction NetworkVision User's Guide*.
- *Sheer PathTracer Single-Path* window: Displays a single path available between the selected source and destination, as well as, the subscribers and properties. For more information, refer to *Chapter 9* of the *Cisco Active Network Abstraction NetworkVision User's Guide*.

8.2 Opening Sheer PathTracer Over MPLS Networks

You can open and view PathTracer information between service end-points (for example, the IP interface which is attached to the VRF) over a MPLS network. The Label Switch Path (LSP) in the MPLS network is found according to the Cross Connect table of each router.

Note that the LSP can be traced and displayed by PathTracer as part of an end-to-end tracing of a service as well. For example, when viewing a path between one customer edge to another. The PathTracer traces the path which goes over circuits or VLANs in the access networks and LSP between the VRFs going through all the intermediate devices, namely, CEs, aggregation switches, PEs and core routers.

In order to view a specific path you must specify an initial point like an IP interface and a destination IP address (optional). If the traced circuit (for example, VC, VLAN) ends in a router, Sheer PathTracer finds the next hop according to the “destination IP address”. When the user selects an end point the system extracts the relevant IP address from this point and uses it as the destination.

PathTracer Starting Points

The user can also enter the required destination IP address after opening the Sheer PathTracer from the right-click shortcut menu. The table below describes the starting points available in the shortcut menu in order to open the PathTracer:

Element	Location	Start PathTracer Options
IP Interface	<ul style="list-style-type: none"> • <i>Inventory</i> window • Affected entry (this is only enabled if the affected has an IP interface) 	<ul style="list-style-type: none"> • to IP Destination • to Subnet Destination • Start Here
Site	<i>Service View</i> map	<ul style="list-style-type: none"> • to IP 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, and it can then be opened from the <i>Find Business Tag</i> window.	<ul style="list-style-type: none"> • to IP Destination

Element	Location	Start PathTracer Options
Layer 2 MPLS Tunnel	<i>Inventory</i> window	<ul style="list-style-type: none"> to IP Destination
LCP	<i>Service View</i> map	<ul style="list-style-type: none"> to IP Destination Start Here

For information on opening Sheer PathTracer from the *Inventory* window as starting point, refer to *Chapter 9* of the *Cisco Active Network Abstraction NetworkVision User's Guide*.

PathTracer End Points

If you selected the “**Start Here**” option the following end points can be selected as a path destination to open the PathTracer:

Element	Location	End PathTracer Options
IP Interface	<ul style="list-style-type: none"> <i>Inventory</i> window Affected entry (this is only enabled if the affected has an IP interface) 	End Here
Site	<i>Service View</i> map	End Here
LCP	<i>Service View</i> map	End Here

The *Sheer PathTracer Multi-Path* window is displayed. From this window you can open the *Sheer 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, then all of the available paths will be opened automatically, and each one will be displayed in a separate *Sheer PathTracer Single-Path* window.

8.3 Sheer PathTracer Windows

The *Sheer PathTracer Multi-Path* window displays all of the discovered paths for the selected context, including devices, links, and paths. For more information about opening Sheer PathTracer, refer to page 85.

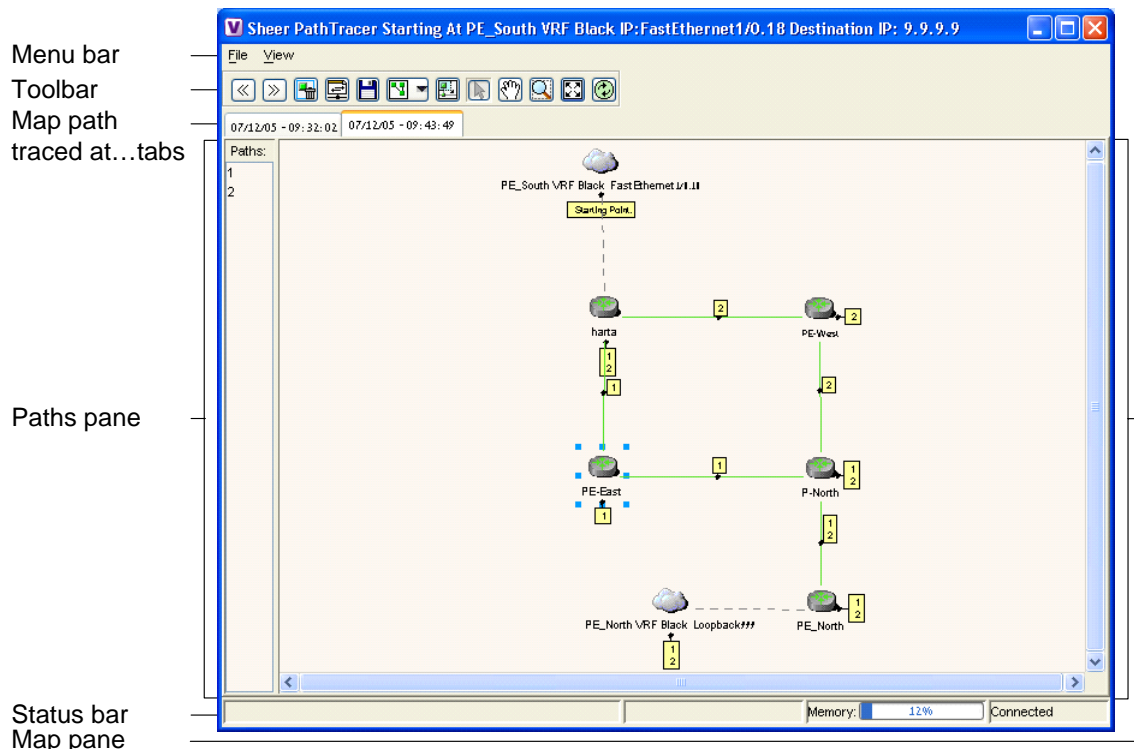
The *Sheer PathTracer Multi-Path* window enables you to perform the following functions:

- View a previous path or view the next path

- Open the *Sheer PathTracer Single-Path* window in order to view a single selected path
- Save the multi-path map to a file
- Run the Sheer PathTracer again

Multi-path is the ability to display all the paths available between the selected source and destination.

An example of the *Sheer PathTracer Multi-Path* window is displayed below.



For a detailed description of the *Sheer PathTracer Multi-Path* window, refer to *Chapter 9* of the *Cisco Active Network Abstraction NetworkVision User's Guide*.

Sheer PathTracer Single-Path window

The *Sheer PathTracer Single-Path* window displays the devices and links of the discovered path, as well as path layer *Properties* information in tables and subscribers.

The *Sheer 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.
 - View traffic statistics along the path.
- Monitor the status and traffic of all of the links along the path.
- View In and Out port properties.

In addition, right-clicking on an item in Sheer PathTracer, enables you to perform certain functions. For example, you can view device information, namely, device properties and attach business tags.

An example of the *Sheer PathTracer Single-Path* window is displayed below:

The screenshot shows the Sheer PathTracer Single-Path window. The top part is a map pane displaying a network diagram with nodes: Edge Point, PE_North, P-North, PE-West, harta, and Edge Point. The bottom part is a properties table for Layer 2.

Layer 2 Properties	IP: PE_North Slot: 0 Port: Ethernet0/3	IP: P-North Slot: 2 Port: Ethernet2/1	IP: P-North Slot: 2 Port: Ethernet2/0	IP: PE-West Slot: 0 Port: Ethernet0/1	IP: PE-Ves Slot: 1 Por
Outer Label			18	18	19
Inner Label	30	30	30	30	30
Auto Negotiate					
MAC Address	00 02 B9 BD FE 63	00 03 E4 11 80 39	00 03 E4 11 80 38	00 30 80 B1 8E 41	00 30 80 B1
Mpls TE Properties	com.sheer.imo.technolo...	com.sheer.imo.technolo...	com.sheer.imo.technolo...	com.sheer.imo.technolo...	com.sheer.imo.technolo...
Type					
Output Flow Control					

At the bottom, there are layer tabs (Layer 1, Layer 2, Layer 3, Business) and a status bar showing Memory: 12% and Connected.

The *Sheer PathTracer Single-Path* window displays information regarding each device. The information is either plain data that was extracted from the device or calculated data such as rates or statistics. The information is displayed in the Layer 1, Layer 2 and Layer 3 tabs.

In addition, the Sheer PathTracer tabs display information regarding VPNs. The information is displayed in the Layer 2 and Layer 3 tabs.

For a detailed description of the Sheer PathTracer Single-Path window, refer to *Chapter 9* of the *Cisco Active Network Abstraction NetworkVision User's Guide*.

8.4 Using PathTracer for Layer 3 VPN

Sheer Path Tracer uses VRF routing and label switching information in order to trace the path from one VRF interface to another.

By selecting a start and end point from the shortcut menu as described in the *Section Opening Sheer PathTracer Over MPLS Networks* on page 85, you can open the Sheer PathTracer for Layer 3 VPNs.

The *Sheer PathTracer Multi-Path* window is displayed showing the VPN topology map. From this window you can open the *Sheer PathTracer Single-Path* window with the appropriate VPN information displayed in the **Layer 2** and **Layer 3** tabs.

8.4.1 Viewing Layer 3 Path Information

For Layer 3 path information Sheer DNA uses VRF routing and label switching information to trace the path from one VRF interface to another. Layer 3 PathTracer information is displayed in the *Sheer PathTracer* window when the path goes over connections and ends in VRFs.

To view Layer 3 path information

- Select the **Layer 3** tab and select **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 *Sheer PathTracer Single-Path* window with the **Layer 3** tab is displayed.

The screenshot shows a network diagram with four nodes: Edge Point (cloud), PE-West (router), P-North (router), and PE_North (router). Connections are shown between Edge Point and PE-West (IP: 20.20.20.1, Black), PE-West and P-North, P-North and PE_North (IP: 30.30.30.1, Black), and PE_North and Edge Point. Below the diagram is a table of Layer 3 properties for the selected device.

Layer 3 Properties	20.20.20.1, Black	30.30.30.1, Black
Name	Serial1/0	Ethernet0/2
IP Address	20.20.20.1	30.30.30.1
Mask	255.255.255.252	255.255.255.252
State	Up	Up
VRF Name	Black	Black
Sending Alarms	true	true

At the bottom of the window, there are tabs for Layer 1, Layer 2, Layer 3 (selected), and Business. A status bar shows Memory usage at 16% and a Connected status.

In the example above, 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, namely, **Up** or **Down**.
- **VRF Name:** The name of the VRF.
- **Sending Alarms:** Whether the alarm for the required port has been enabled (**true**) or disabled (**false**).

8.5 Using PathTracer for Layer 2 VPN

Sheer DNA uses VC ID and label switching information to trace the path from one tunnel interface to another over the MPLS network.

The Sheer PathTracer also covers end-to-end Layer 2 VPN service paths from one customer edge (routers) to another, as part of Sheer DNA's capability of tracing service routes or network connectivity between two points in the network. The path goes over circuits (for example, a VC) or VLANs in the access networks and LSP between the Layer 2 tunnel edge.

For more information about Layer 2, refer to the *Viewing Layer 2 Path Information* section on page 91.

By selecting a start and end point from the shortcut menu as described in the *Section Opening Sheer PathTracer Over MPLS Networks* on page 85, you can open the Sheer PathTracer for Layer 2 VPNs.

The *Sheer PathTracer Multi-Path* window is displayed showing the VPN topology map for the relevant devices and links. From this window you can open the *Sheer PathTracer Single-Path* window with the appropriate VPN information displayed in the **Layer 2** and **Layer 3** tabs.

8.5.1 Viewing Layer 2 Path Information

For Layer 2 path information Sheer DNA uses VC ID and label switching information to trace the path from one tunnel interface to another. Layer 2 PathTracer information is displayed in the *Sheer PathTracer* window when the path goes over **PWE3** tunnels.

To view Layer 2 path information

- Select the **Layer 2** tab and select **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 *Sheer PathTracer Single-Path* window with the **Layer 2** tab is displayed.

The following Layer 2 properties that may be displayed in the **Layer 2** tab relate specifically to VPNs:

- **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 identifier that along with the router IPs of the two tunnel edges identifies the **PWE3** tunnel.
- **Tunnel Type:** The tunnel type, namely, **0=Unknown**, **1= PWE3** and **2=Traffic Engineering**.
- **Tunnel Status:** The operational state of the tunnel, namely, **up** or **down**.
- **Tunnel 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.
- **Tunnel 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.
- **Tunnel Local Router IP:** The IP of this tunnel edge, which is used as the MPLS router ID.
- **Tunnel Peer Router IP:** The IP of the peer tunnel edge, which is used as the MPLS router ID.
- **Distribution Protocol Type:** The protocol used by MPLS to build the tunnel, for example, LDP or TDP.
- **Peer Oid:** The tunnel ID and device name.

8.6 Using PathTracer for MPLS Traffic Engineering Tunnels

Sheer 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 (Traffic Engineering) technology, Sheer DNA's *PathTracer* tool 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.
- Trace the path for the defined MPLS TE-LSP across the network.

By selecting an IP destination from the shortcut menu as described in the *Section Opening Sheer PathTracer Over MPLS Networks* on page 85, you can open the Sheer PathTracer for MPLS TE Tunnels.

The *Sheer PathTracer Multi-Path* window is displayed showing the MPLS TE tunnel topology map. From this window you can open the *Sheer PathTracer Single-Path* window with the appropriate MPLS TE tunnel information displayed in the **Layer 2** tab.

8.6.1 Viewing MPLS TE Tunnel Information

Layer 2 and Layer 3 PathTracer information is displayed in the *Sheer PathTracer* windows when a path is traced over MPLS TE tunnels. This section specifically details Layer 2 TE tunnel properties.

To view Layer 2 path information

- Select the **Layer 2** tab and select **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 *Sheer PathTracer Single-Path* window with the **Layer 2** tab is displayed.

The screenshot shows the Sheer PathTracer Single-Path window. The top part displays a network diagram with four nodes: Edge Point, North, West, and South. A green line represents a path connecting these nodes. The North node has IP address 00 04 9A 24 1E E0, the West node has 00 02 B9 AA 96 80, and the South node has label: 23. The Edge Point nodes are represented by cloud icons.

The bottom part of the window shows a table of Layer 2 properties for the tunnel. The table has columns for IP: North, IP: West, IP: West, and IP: South. The properties listed include Mpls TE Properties, Distribution Protocol Type, Tunnel Lockdown, Tunnel Oper Status, Tunnel Affinity, Tunnel Lsp ID, Tunnel Destination Address, Tunnel Bandwidth Kbps, Tunnel Peak Rate Kbps, Tunnel Auto Route, Tunnel Description, Tunnel Out Interface, Tunnel Hold Priority, Type, Tunnel Admin Status, Tunnel Setup Priority, Tunnel Path Option, Tunnel Burst Kbps, Tunnel Out Label, Tunnel Name, Tunnel Average Rate Kbps, and Tunnel Affinity Mask.

Layer 2 Properties	IP: North Slot: 0 Port: Ethernet0/0	IP: West Slot: 0 Port: Ethernet0/0	IP: West Slot: 0 Port: Ethernet0/3	IP: South Slot: 0 Port: Ethernet0/3	
Mpls TE Properties			com.sheer.imo.technolo...	com.sheer.imo.technolo...	
Distribution Protocol Type			LDP	LDP	
Tunnel Lockdown					disabled
Tunnel Oper Status					Up
Tunnel Affinity					0x00000000
Tunnel Lsp ID					2
Tunnel Destination Address					192.168.200.2
Tunnel Bandwidth Kbps					100
Tunnel Peak Rate Kbps					100
Tunnel Auto Route					enabled
Tunnel Description					North via West
Tunnel Out Interface					South IP:Ether...
Tunnel Hold Priority					2
Type					
Tunnel Admin Status					Up
Tunnel Setup Priority					3
Tunnel Path Option					explicit LSP_to...
Tunnel Burst Kbps					8
Tunnel Out Label					23
Tunnel Name					Tunnel1000
Tunnel Average Rate Kbps					100
Tunnel Affinity Mask					0x0000FFFF

The following Layer 2 properties that may be displayed in the **Layer 2** tab relate specifically to MPLS TE tunnels:

- **Tunnel Operational Status:** The operational state of the tunnel, namely, up or down, however: If the **Tunnel Oper** status is up, the Tunnel Admin Status must also be up (see the Tunnel Admin Status properties for additional information).
- **Tunnel Affinity:** The tunnel's preferential bits for specific links.
- **Tunnel LSP ID:** LSP identification number.
- **Tunnel Destination Address:** The IP address of the device in which the tunnel ends.
- **Average Rate, Burst and Peak:** Flow specification measured for this tunnel.

- **Tunnel Auto Route:** If enabled, destinations behind the tunnel are routed through the tunnel.
- **Tunnel Description:** A textual description of the tunnel.
- **Tunnel Out Label:** The TE tunnel's MPLS label distinguishing the LSP selection in the adjacent (next) device.
- **Tunnel Out Interface:** The interface through which the tunnel exits the device.
- **Tunnel Admin Status:** The operational state of the tunnel, namely, **up** or **down**, however:
 - If the Tunnel Oper status is **up**, the Tunnel Admin Status must also be **UP**;
 - If the Tunnel Admin status is **down**, the Tunnel Oper Status must also be **Down**.
- **Setup Priority:** The tunnel's priority upon path setup.
- **Hold Priority:** The tunnel's priority after path setup, when other tunnels try to remove it and claim its resources.
- **Tunnel Affinity Mask:** Dictates which bits from the tunnel's affinity should be compared to the link's attribute bits.
- **Lockdown:** If enabled, the tunnel cannot be rerouted.
- **Path Option:** The tunnel's path can be either dynamic, in which case, the tunnel is routed along the ordinary routing decisions after taking into account the constraints the tunnel imposes (attributes, priority, bandwidth) or explicit, in which case the route is explicitly plotted with included and excluded links.

A Running a VPN Leak Report Command

About this appendix:

This appendix describes running a VPN Leak report command.

Note: It is required that you read the *Cisco Active Network Abstraction BQL User's Guide* as a prerequisite to understanding this appendix.

A VPN leak report provides a list of all of the links that exist between VPNs.

A.1 Syntax

Item	Code and Explanation
General Syntax	<pre><command name="CreateVpnLeakReport"> <param name="oid"> <value>{[VpnLeakReport]}</value> </param> </command></pre>

A.2 Output

The output of a script is the IMO object: "IVpnLeakReport". For a description of this object, refer to *Section A.4.1*.

A.3 Examples

A.3.1 Get the VPN Leak Report

The example below describes running the command.

```
<command name="CreateVpnLeakReport">
<param name="oid">
<value>{[VpnLeakReport]}</value>
</param>
</command>
```

A.4 VPN Leak Report Results

A.4.1 IVPNLeakReport

The IVPNLeakReport is the IMO object that contains the result of a VPN leak report execution. Each IMO object has a property array of IVpnLeak.

The object property is:

- **Results:** Contains an array of IVpnLeak and each IVpnLeak in turn contains each leak that was detected.

A.4.2 IVpnLeak

The IVpnLeak is the IMO object that describes a single VPN leak. Each IMO object has a property array of IVpn.

The object property is:

- **VPNs:** Contains an array of IVpn and each IVpn in turn contains each VPN that was part of the leak (usually two).

B Additional Alarms

About this appendix:

This appendix briefly describes the additional alarms that can be supported by Sheer DNA.

For further information about enabling the alarms described here, contact Cisco Professional Services.

The alarms described below can be supported by Sheer DNA as well:

Alarm	Severity	Description	Up Alarm
VPN Leak	Dark blue (information)	Upon <i>detection of a link</i> between VPNs the system issues a VPN Leak alarm to alert the user of a possible security breach.	VPN Leak Cleared
Duplicate Route Entry Found	Sky blue (warning)	Upon detection of a duplicate route entry in the same VPN (in two different VRFs), the system issues an alarm indicating the VPN has a duplicate route entry. Note: It is recommended that this is used in variables which do not use multi-homing.	Duplicate Route Entry Fixed

