Cisco Active Network Abstraction MPLS User Guide Version 3.6

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

Text Part Number: OL-12513-01

Cisco Active Network Abstraction MPLS User Guide Version 3.6

CONTENTS

Preface

This User Guide describes the tools included in Cisco ANA 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 Cisco ANA's multi-path tracing capability using the Cisco ANA 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 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 Cisco ANA NetworkVision Service View, Cisco ANA 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 Cisco ANA 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 Cisco ANA 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 Cisco ANA 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 Cisco ANA.

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

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 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.

Supported Routing Protocols

The following routing protocols are supported:

- BGP
- EIGRP
- Cisco IGRP
- OSPF

Related Documentation

For more detailed information, refer to the following publication:

- Cisco Active Network Abstraction NetworkVision User Guide
- Cisco Active Network Abstraction Administrator Guide
- Cisco Active Network Abstraction Fault Management Guide

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

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

CHAPTER 1

Introducing MPLS VPN Maps

This chapter provides an introduction to the Service View, business configuration and Service View maps, as follows:

- Introducing VPN MPLS Maps, page 1-1—Describes Service View maps, including the concepts of VPN topology.
- Introducing the Cisco ANA Business Configuration, page 1-2—Provides an introduction to the Layer 2 and Layer 3 VPN business configuration, including, the business elements available.
- VPN Topology Connections, page 1-3—Describes viewing the Layer 2 and Layer 3 VPN topology in maps.
- VPN Service View Map, page 1-5—Describes the Service View map that is displayed in the Cisco ANA NetworkVision window.

For a more detailed description of the Cisco ANA NetworkVision window, menus, and toolbars, and working with tables, see the *Cisco Active Network Abstraction NetworkVision User Guide*.

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

Introducing VPN MPLS Maps

Cisco ANA 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 Cisco ANA 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, see Introducing the Cisco ANA Business Configuration, page 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, see the *Cisco Active Network Abstraction NetworkVision User Guide*.

Cisco ANA has the capability to automatically determine the different Layer 3 VPNs in the network and their associated Virtual Routers. For more information, see Layer 3 VPN Business Configuration, page 1-2.

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 Cisco ANA for the devices present in the map. For more information, see Chapter 6, "Fault Management In MPLS Networks".
- Identify extranets.

Introducing the Cisco ANA Business Configuration

Cisco ANA 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.

Cisco 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, see Layer 3 VPN Business Configuration, page 1-2 and for more information about the Layer 2 VPN hierarchy, see Layer 2 VPN Business Configuration and Tunnels, page 1-3.

Business elements are available via the Northbound interface as well as in Cisco ANA 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 the maps.

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.

Cisco ANA can use different criteria in order to determine the different Layer 3 VPNs in the network and their associated Virtual Routers. By default, Cisco ANA 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 Cisco'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.

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 adds 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 an LCP is added to the VPN system, the system automatically creates the LCA by taking all 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, see Creating an LCA, page 3-5.

VPN Topology Connections

Cisco 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.

Cisco 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:

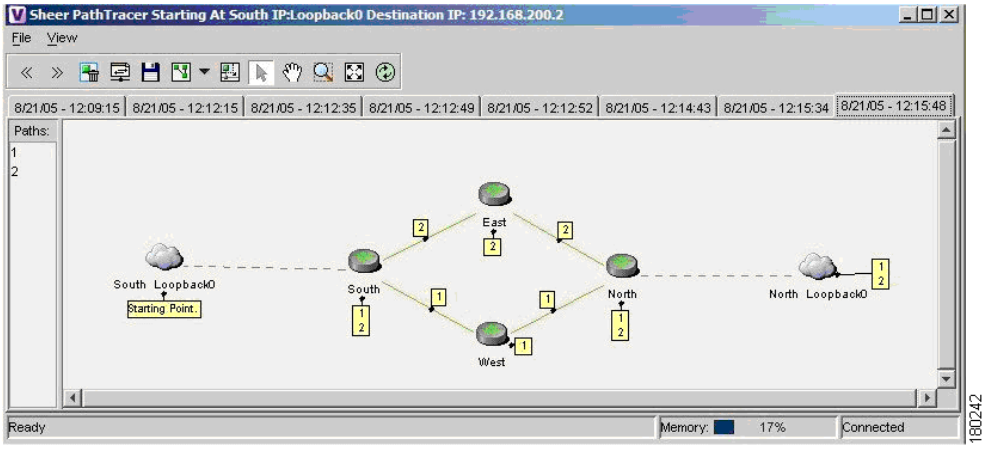
Table 1-1 Topology

Topology Example	Description
	• Topology between VPNs (extranet). • Displayed by means of a solid line with arrows at either end.
	• VPN topology between Virtual Routers. • Displayed by means of a solid line with arrows at either end.
	• Tunnel between LCPs. • Displayed by means of a solid line. • The link does not reflect a status.

Note BGP topology between a PE and CE is not currently supported.

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

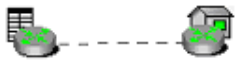
Figure 1-1 Cisco ANA PathTracer Multi-Path Window



For more information about the icons displayed in the maps of the Cisco ANA NetworkVision window, see Table 1-3 on page 1-7.

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

Table 1-2 Associations

Association Example	Description
	• 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.
	• 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.
	• Symbolizes the overall connection between the CE device and the LCP. • Displayed by means of a broken dark gray line.

VPN Service View Map

Cisco ANA 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).

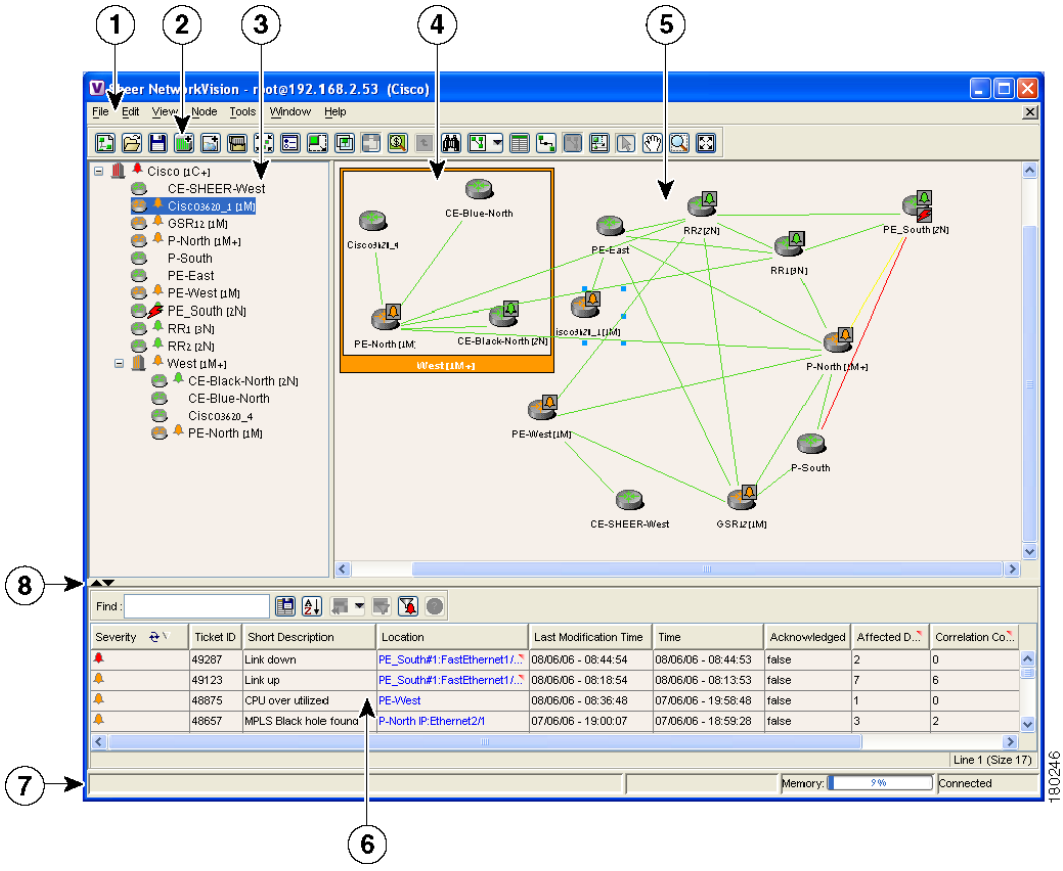
Layer 2 VPN Service View Map

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 Cisco ANA NetworkVision window with an open Service View map is displayed below.

Figure 1-2 Cisco ANA NetworkVision Window



1	Menu bar
2	Toolbar
3	Tree pane
4	Aggregation
5	Workspace
6	Ticket pane
7	Status bar
8	Hide/display ticket pane buttons

The Cisco ANA NetworkVision window is divided into three areas or panes, as follows:

- Tree Pane, page 1-7
- The workspace, which includes the Map Pane, page 1-8, Device View and Links View. For more information about the Device View and Links View, see the *Cisco Active Network Abstraction User Guide*.
- Ticket Pane, page 1-8

For a general description of the Cisco ANA NetworkVision window, menus and toolbar, see the *Cisco Active Network Abstraction NetworkVision User Guide*.

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

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, see the *Cisco Active Network Abstraction NetworkVision User Guide*.

The following icons are used in the tree and map panes:

Table 1-3 Tree and Map Pane Icons

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, see the *Cisco Active Network Abstraction NetworkVision User Guide*.

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

Table 1-4 Management State Icons

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. In addition, CE devices can also be displayed in the Layer 3 VPN sub-branches.

The Layer 2 VPN sub-branches display the LCAs and LCPs contained in the VPN along with the names of the business elements. In addition, CE devices can also be displayed in the Layer 2 VPN sub-branches.

When an aggregated business element is selected in the tree pane, the map pane displays the business elements contained within the aggregated business element.

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 1-3.

When the root is selected in the tree pane the Service View map displays all the VPNs.

Ticket Pane

When Cisco ANA 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 Cisco ANA. For more information about the alarms that Cisco ANA detects and reports for Layer 2 and Layer 3 VPNs, see Chapter 6, “Fault Management In MPLS Networks”.

For more information about the ticket pane, see the *Cisco Active Network Abstraction NetworkVision User Guide*.

In addition, the user can calculate the affected parties. For more information, see the *Cisco Active Network Abstraction NetworkVision User 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.

CHAPTER 2

Creating and Manipulating VPN MPLS Maps

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

- Adding a VPN, page 2-1—Describes how to add a VPN to the currently displayed Service View map.
- Removing a VPN from the Map, page 2-2—Describes how to change the Service View map by removing a VPN from the currently active map.
- Connecting a CE Device, page 2-3—Describes how to connect a CE device to its respective Sites or LCPs.
- Disconnecting a CE Device, page 2-4—Describes how to disconnect a CE device.
- Displaying and Hiding a CE Device, page 2-4—Describes how to display and hide the CE device on the Service View map.
- Creating an Aggregation, page 2-5—Describes how to aggregate business elements according to a logical hierarchy.
- Disaggregating a Node, page 2-6—Describes how to disaggregate an aggregated node.

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:

Step 1 Select the root of the map in the Cisco ANA 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.

Step 2 On 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 Cisco ANA

  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
New	Opens the Create Business Element dialog box, which enables the user to create a new VPN business element. The newly created VPN is displayed in the Add Business Element to <Root> dialog box. For more information, see Disaggregating a Node, page 2-6
Add	Loads the selected VPN in the currently displayed Service View map. The VPN is displayed in the tree pane and map pane.
Close	Closes the Add Business Element to <Root> dialog box.

Step 3 Select the required VPN in the table.

Step 4 Click **Add**. The VPN is loaded in the Service View map displayed in the Cisco ANA NetworkVision window's map pane in the workspace.

Step 5 Click **Close** to close the Add Business Element to <Root> dialog box.

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:

Step 1 Right-click on the required VPN in the Cisco ANA NetworkVision window's tree pane or map pane to display the shortcut menu.

Step 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 the VPN elements from the map, including connected CE devices within the VPN, but excluding remote VPNs (extranets).

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:

Step 1 To add a CE device to a Site, select the required VPN in the Cisco ANA NetworkVision window's tree pane or map pane,

or

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

Step 2 On the toolbar, click **Add Device**,

or

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

For more information see the *Cisco Active Network Abstraction NetworkVision User Guide*.

Step 3 From the Device List, select the device that you want to add.

Step 4 Click **Add Device**. The device is displayed in the tree pane and the selected map or sub-network in the Cisco ANA NetworkVision window's workspace.

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

Step 5 Click **Close** to close the Device List dialog box.

Step 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**.

Step 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).

Step 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 Cisco ANA 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.

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 Cisco ANA 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, see Displaying and Hiding a CE Device, page 2-4.

Displaying and Hiding a CE Device

The user can display the CE device for a Site and/or LCP in the Cisco ANA 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:

Step 1 Select a Site in the map pane displaying the Site business element with an actively associated CE device icon (for more information about icons see Table 1-3 on page 1-7).

or

Select an LCP in the map pane displaying the LCP business element with an actively assigned tunnel edge for the CE device icon.

Step 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 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

Step 1 Select the Site or LCP in the Cisco ANA NetworkVision window's tree pane or map pane connected to the CE device.

Step 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 them) in order to hide them along with the links to Sites and/or LCPs.

Creating an Aggregation

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

To create an aggregation:

Step 1 Select the required business elements in the Cisco ANA 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.

Step 2 In the Cisco ANA 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.

Step 3 Type a unique name for the aggregated node and click **OK**. The aggregated node is displayed in the Cisco ANA NetworkVision window's tree pane and map pane. Aggregated nodes are displayed as a single entity using the aggregation icon (for more information about icons see Table 1-3 on page 1-7).

Disaggregating a Node

The aggregated node selected in the Cisco ANA NetworkVision window's tree pane or map pane can be disaggregated.

To disaggregate a node:

Step 1 Select the required branch in the tree pane,

or

Select the required aggregated node in the map pane.

Step 2 Select **Disaggregate** from the Node menu,

or

Right-click on the aggregated node to display the shortcut menu and select **Disaggregate**.

A confirmation message is displayed.

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

CHAPTER 3

Creating and Manipulating Cisco ANA Business Configuration

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, see Introducing the Cisco ANA Business Configuration, page 1-2.

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

- Creating a VPN, page 3-2—Describes how to manually create VPNs.
- Moving a Virtual Router, page 3-3—Describes how to move a Virtual Router (including its Sites) from one VPN to another.
- Adding a Tunnel, page 3-3—Describes how to add tunnels to a VPN.
- Creating an LCA, page 3-5—Describes how manually create an LCA.
- Deleting an LCA, page 3-5—Describes how to delete an LCA.
- Moving an LCP, page 3-6—Describes how to move an LCP to another VPN or LCA.
- Moving an LCA, page 3-6—Describes how to move the LCA to another VPN.
- Jumping to the Adjacent LCP, page 3-7—Describes how to jump from one peer to the adjacent peer.
- Renaming a Business Element, page 3-7—Describes how to rename business elements from the business model.
- Deleting a Business Element, page 3-7—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.

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

Step 1 Select the root of the map in the Cisco ANA NetworkVision window's tree pane.

Step 2 On the toolbar, click **Add VPN**.

or

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

Step 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).

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

Note VPN business element names are case sensitive.

Note For information about renaming a VPN, see the *Cisco Active Network Abstraction NetworkVision User Guide*.

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

Note If a path is not specified to an icon the default VPN business element icon is used (for more information about icons see 1-7).

Step 6 Type a description for the new VPN business element (optional).

Step 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, see Adding a VPN, page 2-1.

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 the Virtual Router's Sites as well.

To move a Virtual Router

Step 1 Select the required Virtual Router that you want to move in the Cisco ANA NetworkVision window's tree pane or the map pane.

Step 2 Right-click to display the shortcut menu and select **Edit | Move selected**.

Step 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.**

Step 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.

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 stranded icon (for more information about icons see 1-7). 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 an Logical link.

The user can either:

- Add a tunnel (LCP) to an LCA that has been manually created (for more information about manually creating an LCA, see Creating an LCA, page 3-5),

or

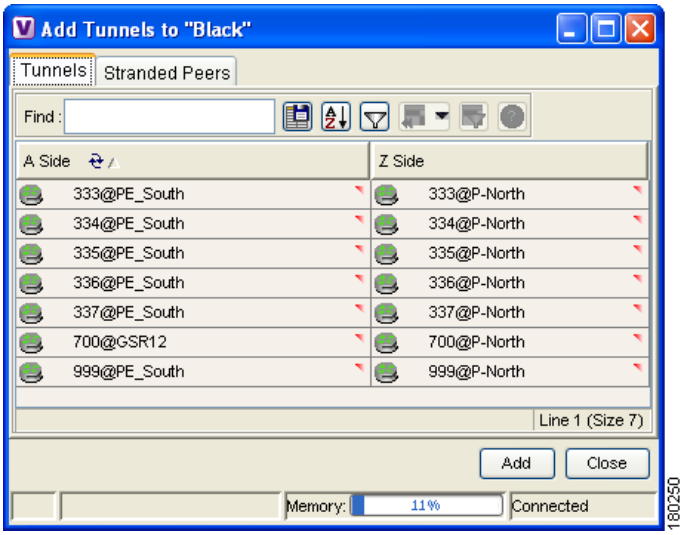
- Add a tunnel (LCP) directly to a VPN in which case the LCA is automatically created beneath the VPN.

To add a tunnel

Step 1 Right-click on the required LCA or VPN in then Cisco ANA NetworkVision window's tree pane or map pane to display the shortcut menu.

Step 2 Select **Topology | Add Tunnel**. The Add Tunnels dialog box is displayed.

Figure 3-1 Add Tunnels dialog box



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 an 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.

Step 3 Select the required tunnel or stranded peer and click **Add**.

- If the tunnel or stranded peer is added beneath an LCA, the link between the peers is displayed in the map pane.
- If the tunnel or stranded peer is added beneath a VPN, Cisco ANA detects the starting point of the **PWE3** tunnel edges and groups all the LCPs that start at the same device automatically together into an 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 an LCA or VPN.

To remove a tunnel

Step 1 Right-click on the required LCP in the in the Cisco ANA NetworkVision window's tree pane or map pane to display the shortcut menu.

Step 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 an LCA that was created manually, the LCA is still displayed in the tree pane or map pane.

If the deleted tunnel formed part of an 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 5-13.

Creating an LCA

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

- Moving selected LCPs to the LCA. For more information, see Moving an LCP, page 3-6.
- Adding tunnels (LCPs) to the LCA. For more information, see Adding a Tunnel, page 3-3.

For more information about LCAs that are created automatically, see Adding a Tunnel, page 3-3.

To create an LCA

Step 1 Select the required VPN in the Cisco ANA NetworkVision window's tree pane or map pane.

Step 2 Right-click to display the shortcut menu and select **Create LCA**. The Create LCA dialog box is displayed.

Step 3 Type a unique name for the new LCA.

Step 4 Click **OK**. The new LCA is created and displayed in the tree pane the Cisco ANA NetworkVision window beneath the selected VPN, and in the map pane.

Deleting an LCA

Cisco ANA enables the user to delete an LCA that was manually created if it has no LCPs or if all the LCPs have the reconciliation icon.

Note The user also has the option to move the LCA to another VPN. For more information, see Moving an LCA, page 3-6.

To delete the LCA

Step 1 Select the required LCA in the Cisco ANA NetworkVision window's tree pane or map pane.

Step 2 Right-click to display the shortcut menu and select **Delete**. A confirmation message is displayed.

Step 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.

Moving an LCP

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

To move an LCP:

Step 1 Right-click on the required LCP in the Cisco ANA NetworkVision window's tree pane or map pane to display the shortcut menu.

Step 2 Select **Edit | Move selected**.

Step 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.

Step 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 an LCP is moved to a VPN then an LCA is automatically created for it.

Moving an LCA

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

To move an LCA:

Step 1 Right-click on the required LCA in the Cisco ANA NetworkVision window's tree pane or map pane to display the shortcut menu.

Step 2 Select **Edit | Move selected**.

Step 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.

Step 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 the LCPs move along with the LCA.

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:

Step 1 Select the required LCP in the Cisco ANA NetworkVision window's tree pane or map pane.

Step 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.

Renaming a Business Element

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

To rename a business element:

Step 1 Right-click on the required business element in the Cisco ANA NetworkVision window's tree pane or map pane to display the shortcut menu.

Step 2 Select **Rename**. The Rename Node dialog box is displayed.

Step 3 Type a new name and click **OK**. The changed business element name appears in the Cisco ANA 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.

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.

Caution 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 Cisco ANA before the user can delete the required business element.

Business Element	Requirements
Layer 3 VPN	• There are no Virtual Routers. • The Virtual Routers, and Sites display the reconciliation icon.
Virtual Router	• 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	• There are no interfaces connected/bound to the VRF. • The Sites and interfaces display the reconciliation icon.
Layer 2 VPN	• There are no LCPs beneath the LCA. • The LCPs display the reconciliation icon.
LCA	• There are no LCPs. • All the nested LCPs display the reconciliation icon.

To delete a business element:

Step 1 Right-click on the required business element in the Cisco ANA 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.

Step 2 Select **Delete**. A confirmation message is displayed.

Step 3 Click **Yes** to delete the currently selected element or click **Yes to All** to delete multiple selected elements. The selected business element is deleted from the business configuration of all users.

CHAPTER 4

Viewing VPN Properties In Service View

This chapter describes viewing the properties of the various business elements, as follows:

- Viewing VPN Properties, page 4-1—Describes how to view VPN properties.
- Viewing Site Properties, page 4-2—Describes how to view Site properties.
- Viewing a Virtual Router's Properties, page 4-2—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 4-6—Describes viewing VRF and **PWE3** Tunnels VPN specific logical inventory items.
- Working With the VPN Service Overlay, page 4-8—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.

Viewing VPN Properties

Cisco ANA enables the user to view the properties of the VPN business element.

To view VPN properties:

Step 1 Right-click on the VPN in the Cisco ANA 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.

Step 2 Click to close the VPN Properties dialog box.

Viewing Site Properties

Cisco ANA 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 see the *Cisco Active Network Abstraction NetworkVision User Guide*.

To view Site properties:

Step 1 Right-click on a Site in the Cisco ANA 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.

Step 2 Click to close the Router IP Interface Properties dialog box.

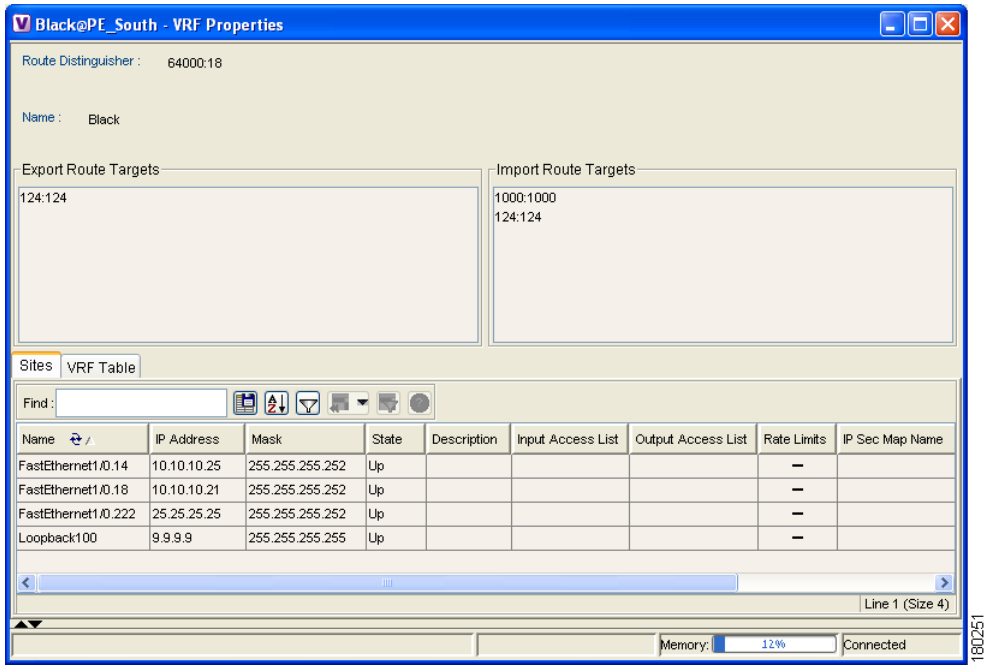
Viewing a Virtual Router's Properties

Cisco ANA 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:

Step 1 Right-click on a Virtual Router in the Cisco ANA 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.

Figure 4-1 VRF Properties Dialog Box



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.

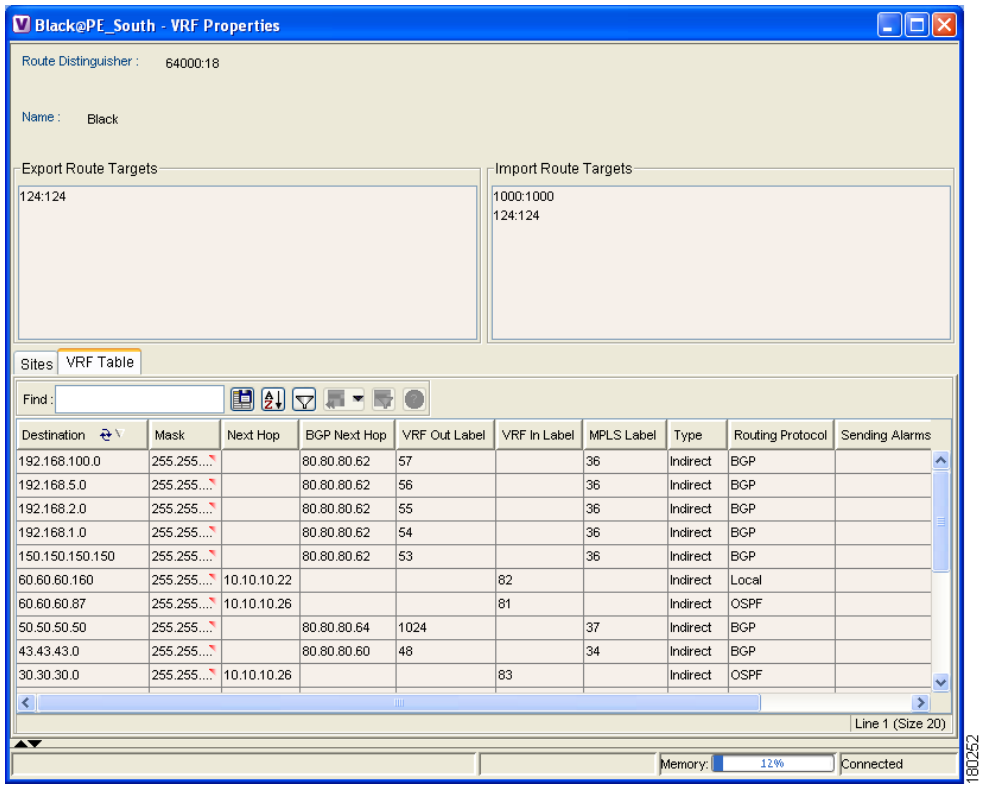
- **Rate Limits—**Measures traffic for the IP interfaces on Cisco devices, including the average rate, normal burst size, excess burst size, conform-action and exceed action.

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.

Figure 4-2 VRF Table Tab



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.

Step 2 Click to close the VRF Properties dialog box.

Opening the VRF Table

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

To open the VRF Table:

Step 1 Right-click on the Virtual Router in the Cisco ANA NetworkVision window's tree pane or map pane to display the shortcut menu. Select **Open VRF Table**. The VRF Table dialog box is displayed.

For more information about the columns displayed in the VRF Table dialog box, see Viewing a Virtual Router's Properties, page 4-2.

Step 2 Click to close the VRF Table dialog box.

Displaying the VRF Egress/Ingress Adjacents

Cisco ANA 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 their properties.

For example, if VRF A retrieved route target import X then the user will be able to view all 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:

Step 1 Right-click on the Virtual Routefr in the Cisco ANA 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 Cisco ANA NetworkVision window's tree pane the displays the properties of the VRF. For more information, see Viewing a Virtual Router's Properties, page 4-2.

Step 2 Click to close the Adjacents dialog box.

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**.

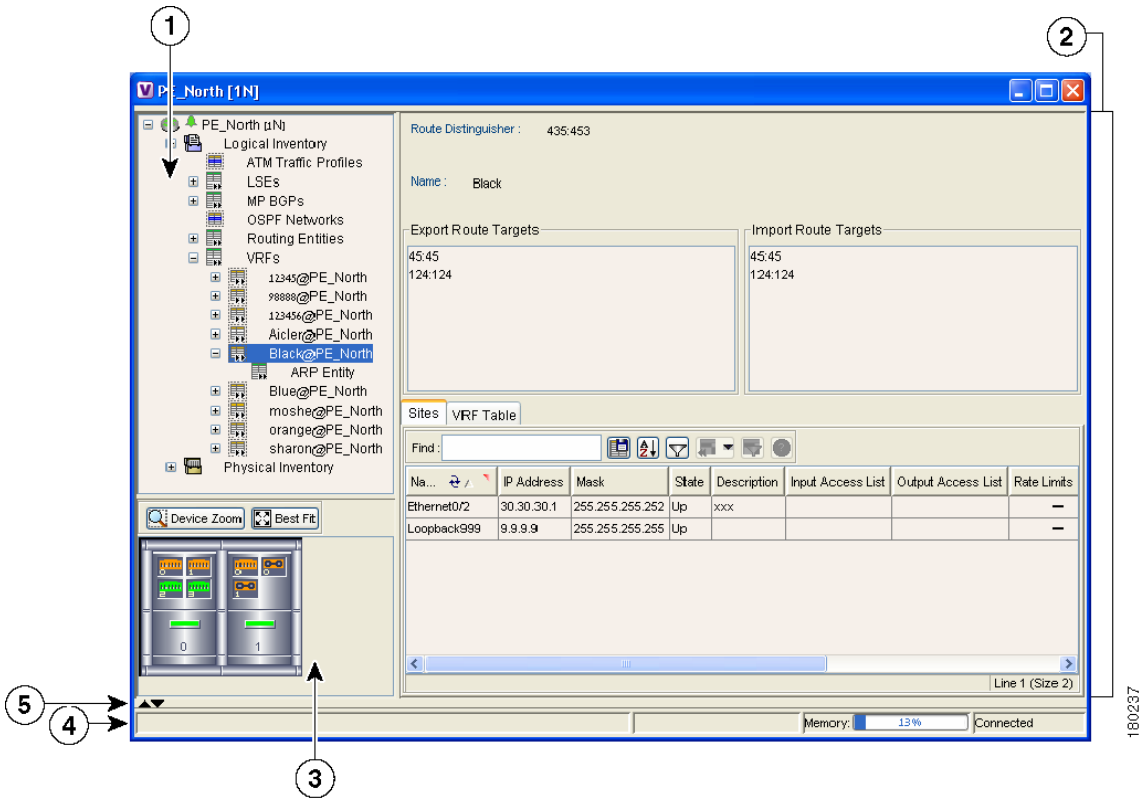
For details on viewing the following VPN MPLS specific logical inventory items, namely, BGP Neighbor, MP BGP information, LSEs, and MPLS TE tunnels, and MPLS Black Holes, see Chapter 4, "Viewing VPN Properties In Service View".

To open the Inventory window:

Step 1 Right-click on a device in the Cisco ANA NetworkVision window's tree pane or map pane to display the shortcut menu.

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

Figure 4-3 Inventory Window



1	Tree pane
2	Properties pane including tabs

3	Device view panel
4	Status bar
5	Hidden ticket pane

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.

Step 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.

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.

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.

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.

Cisco ANA 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, page 4-8—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 Overlays, page 4-9—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 4-9—Describes how to display or hide the callouts for every link in the map pane in order to display related information.

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:

Step 1 Select and display the required Network map in the Cisco ANA NetworkVision window.

Step 2 On 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.

Step 3 Select the required VPN from the list.

Step 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

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 on the toolbar toggles when selected (displays the overlay) or deselected (hides the overlay).

To show or hide the overlay:

Step 1 Select and display the required Network map in the Cisco ANA NetworkVision window.

Step 2 On the toolbar, click **Show Overlay**. The overlay is displayed in the Network map,

or

On the toolbar, click **Show Overlay**. The overlay is hidden from view in the Network map.

Displaying or Hiding Callouts

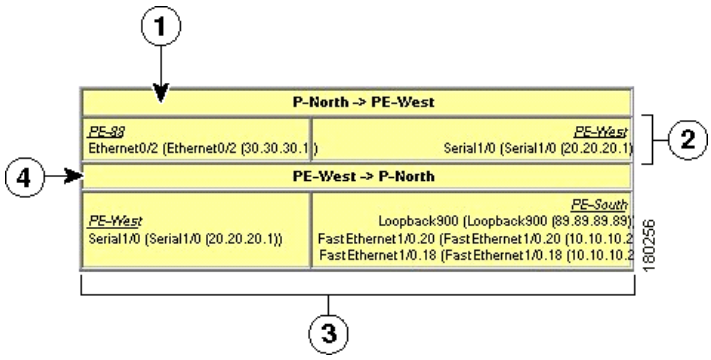
The user can display or hide the callouts for the links displayed in the map pane in order to show the details of the sites that are interconnected through the selected links.

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.

Figure 4-4 Callouts Dialog Box



1	Details of the link and the direction. In this example from P-North to PE-West
2	Details of the sites using the link and interconnections. In this example Site PE-88 is connected to Site PE-West
3	Details of the sites using the link and interconnections. In this example Site PE-West is connected to all these Sites on PE-South
4	Details of the link and the direction. In this example from PE-West to P-North

The user can hide the callouts displayed in the map pane.

To view the callouts:

Step 1 Select and display the required Network map with an overlay of the specific VPN in the map pane of the Cisco ANA NetworkVision window.

Step 2 Right-click on the required link in the map pane to display the shortcut menu and select **Show Callouts**. The Callouts label is displayed.

To hide the callouts:

Step 1 Right-click on the link in the map pane that has the attached callout. The right-click shortcut menu is displayed.

Step 2 Select **Hide Callouts**. The callouts are no longer displayed in the map pane of the Cisco ANA NetworkVision window.

CHAPTER 5

Viewing MPLS Related Inventory Properties

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, see the *Cisco Active Network Abstraction NetworkVision User Guide*.

Introduction

Every node that is managed by Cisco ANA 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 Cisco ANA 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.

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

Opening the Inventory Window

The Cisco ANA solution continuously maintains a real-time, auto-discovered, physical and logical inventory of the network entities, and the relationships between them. Using Cisco ANA'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, LSE, BGP Neighbors, MP BGPs, VRFs, PWE3 tunnels, and TE tunnels.

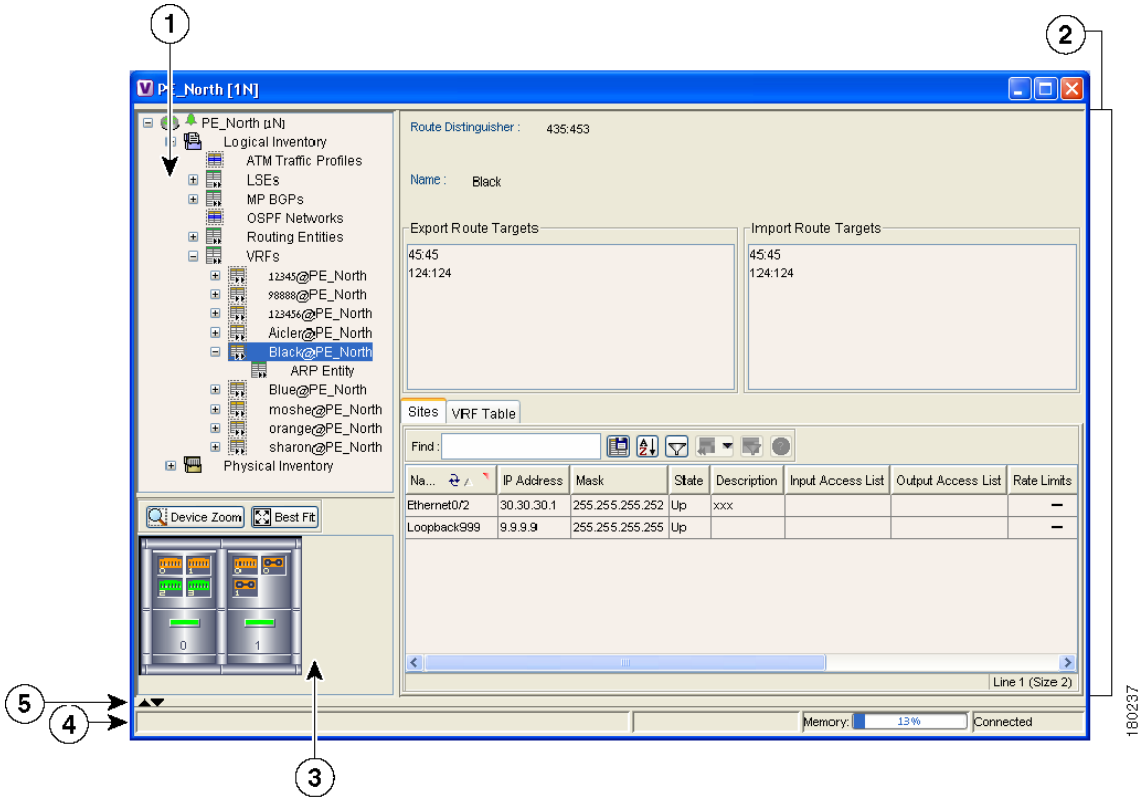
Note In addition to opening the Inventory window from a device, the user can also open and view logical inventory information for a specific Virtual Router directly by right clicking on the Virtual Router to display the shortcut menu and selecting **Inventory**.

To open the Inventory window:

Step 1 Right-click on a device in the Cisco ANA NetworkVision window's tree pane or map pane to display the shortcut menu.

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

Figure 5-1 Inventory Window



1	Tree pane
2	Properties pane including tabs
3	Device View panel
4	Hidden ticket pane
5	Status bar

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.

Step 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.

Viewing Routing Entities

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

The following information is displayed at the top of the Routing Entity – Routing Entity Properties dialog box (IP Interfaces):

- **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—**If an access list is assigned to an IP interface it is available as a property of the IP interface, and a hyperlink highlights the related access list in the **Access List** table. When an access list is assigned to the inbound traffic on an IP interface, the actions assigned to the packet are performed. For information about actions see Viewing Access List Information, page 5-14.

  Note This parameter is only relevant for Cisco IOS devices.

- **Output Access List—**If an access list is assigned to an IP interface it is available as a property of the IP interface, and a hyperlink highlights the related access list in the **Access List** table. When an access list is assigned to the outbound traffic on an IP interface, the actions assigned to the packet are performed. For information about actions see Viewing Access List Information, page 5-14.

  Note This parameter is only relevant for Cisco IOS devices.

- **Rate Limits—**If a rate limit is configured on an IP interface it is available as a property of the IP interface. This option is checked when a rate limit has been defined on a specific IP interface of a device, meaning that the access list is defined as a rate limit access list. It 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 Double-clicking on a specific row displays the properties of the IP interface. When a rate limit has been configured on the IP interface the **Rate Limits** tab is displayed. For more information about rate limits see Viewing Rate Limit Information, page 5-6.

Note This parameter is only relevant for Cisco IOS devices.

- **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, see Viewing a Virtual Router's Properties, page 4-2.

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.

Viewing the ARP Table

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

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.

Viewing Rate Limit Information

Select the **Routing Entities** branch | **Routing Entity** sub-branch | **IP Interfaces** tab and double-click on a specific row to display the properties of the IP interface. When a rate limit has been configured on the IP interface the **Rate Limits** tab is displayed.

Note Rate limit information is only relevant for Cisco IOS devices.

The following information is displayed in the **Rate Limits** tab of the IP Interface Properties dialog box:

- **Type—**The rate limit direction, namely, **Input** or **Output**.
- **Max Burst—**Excess burst size in bytes.
- **Normal Burst—**Normal burst size in bytes.
- **Bit Per Second—**Average rate in bits per second.
- **Conform Action—**The action that can be performed on the packet if it conforms to the specified rate limit (rule), for example, continue, drop, change a bit or transmit.
- **Exceed Action—**The action that can be performed on the packet if it exceeds the specified rate limit (rule), for example, continue, drop, change a bit or transmit.
- **Access List—**A hyperlink that highlights the related access list in the **Access List** table.
- **Sending Alarms—**This option is currently unavailable.

Viewing Port Configuration

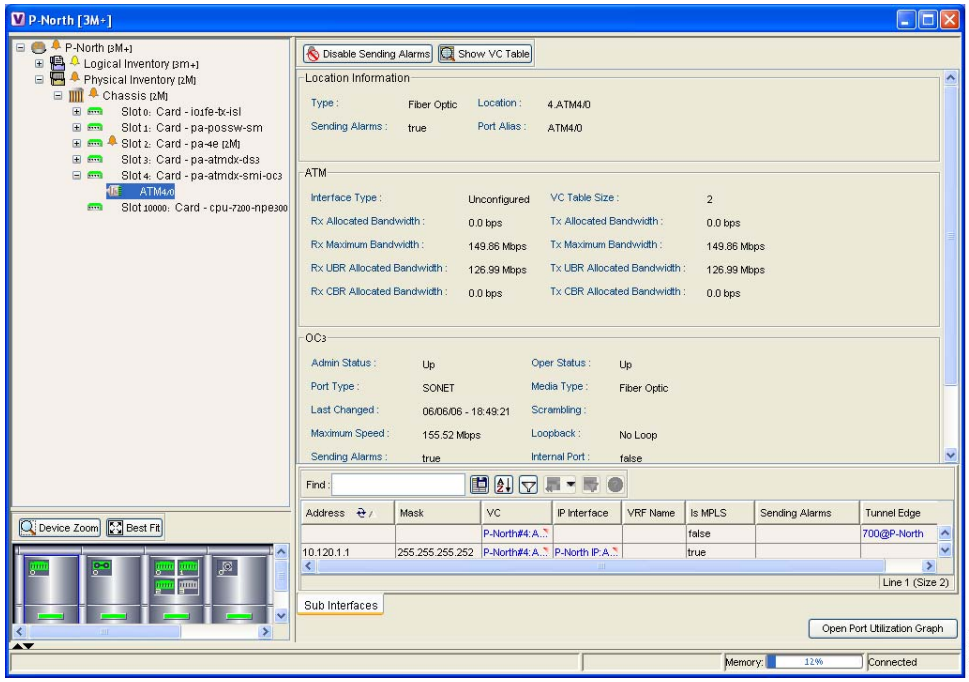
In addition to viewing logical inventory information in the Inventory window, when the user selects the physical source (port) in the physical inventory branch the user can determine what services are using the selected port. The user can view:

- 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 see the *Cisco Active Network Abstraction NetworkVision User Guide*.

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

Figure 5-2 Port Information In the Inventory Window



The sub-interface is the logical interface defined in the device; all 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**).

Viewing a LSE

The **LSEs** (Label Switch Entity) branch displays incoming and outgoing label information.

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. When the action is defined as untagged an outgoing label is not present.
- **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 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 see Traffic Engineering LSPs, page 5-13.

Viewing MP BGP Information

The **MP BGPs** branch displays the VRF name and cross VRF routing entries.

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, see Viewing a Virtual Router's Properties, page 4-2.
- **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.

Viewing BGP Neighbors

The **MP BGP** sub-branch, **BGP Neighbors** tab displays a list of the routers used in the BGP network, 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, 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).

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—**Every BGP neighbor that is configured locally on a BGP router is either defined as a client or non-client type. Route reflector functionality is not specific behavior that is assigned to the device, but rather is defined according to the way that the BGP nieghbor types are defined.

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 see Supporting Route Reflector, page 7-5.

- **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.

Viewing VRF Information

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

Note The Inventory window only displays VRF associations if they exist.

To view a VRF's properties:

Step 1 Right-click on a VRF in the tree pane or map pane of the Cisco ANA NetworkVision window to display the shortcut menu.

Step 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 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.

Step 3 Click to close the VRF Properties dialog box.

Opening the VRF Table

Cisco ANA NetworkVision enables you to view the VRF table for a VRF.

To open the VRF Table:

Step 1 Right-click on the required VRF in the tree pane or map pane of the Cisco ANA NetworkVision window to display the shortcut menu.

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

For more information about the columns displayed in the VRF Table dialog box see Viewing a Virtual Router's Properties, page 4-2.

Step 3 Click to close the VRF Table dialog box.

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.

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.

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.

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 see Chapter 7, "Calculating Impact Analysis" and Chapter 8, "Working with PathTracer in VPN Service View".

Viewing MPLS TE Tunnel Information

The **Traffic Engineering Tunnels** branch displays specific TE tunnel information on TE tunnels.

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.

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.

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.

Viewing Access List Information

The **Access List** branch enables users to classify and filter IP packets on inbound and outbound interfaces in the system. The Access List consists of a set of entries that define what traffic is permitted or denied access according to several parameters, such as IP subnet, protocol or port and so on. The Access List is defined by defining the access list on the device, and then adding the rules.

Note Access limit information is only relevant for Cisco IOS devices.

Each row in the **Access List** table represents an access list. The following information is displayed in the **Access List** table:

- **Name—**The name of the access list.
- **Type—**The type of access list:
  - **Standard—**tests the source address (does not check for protocols)
  - **Extended—**tests the source and destination addresses as well as the TCP/IP protocols and source or destination ports
  - **Named—**the same as the standard and extended types described above, but has a string identifier
- **Access List Entries—**Whether the access list has entries (checked) or not (unchecked).
- **Sending Alarms—**This option is currently unavailable.

Double-clicking on a row in the **Access List** table displays the entries of the list. The entries define what happens (permit or deny the action) when the rules are met. The following information is displayed in the Access List Properties dialog box:

- **Id—**The identifier (name) of the access list entry.
- **Action—**The type of action that will occur when the rules are met:
  - **Permit—**If the rules match, proceeds to the next rule. If all the rules are met then the packet is a match for the access list.
  - **Deny—**If the rules match, does not proceed to the next rule. The packet is not a match for the access list.

- **Protocol—**The type of protocol that is checked, for example, IP, TCP, ICMP and so on.
- **Source—**The IP source of the packet.
- **Source Wildcard—**Defines the source range that will be included in the match using wildcard masking to identify whether to check (0) or ignore (1) corresponding IP address bits.
- **Source Port Action—**Defines the action to be performed at the source port level. Examples of actions that can be performed are, the port number is equal to, or lower than or greater than *x*, where *x* is defined in the **Source Port Range** field.
- **Source Port Range—**Defines the single source port or range of source ports to be checked according to the **Source Port Action** field.
- **Destination—**The IP destination of the packet.
- **Destination Wildcard—**Defines the destination range that will be included in the match using wildcard masking to identify whether to check (0) or ignore (1) corresponding IP address bits.
- **Destination Port Action—**Defines the action to be performed at the destination port level. Examples of actions that can be performed are, the port number is equal to, or lower than or greater than *x*, where *x* is defined in the **Destination Port Range** field.
- Destination Port Range—Defines the single destination port or range of destination ports to be checked according to the **Destination Port Action** field.
- **Precedence—**The QoS of the IP packet for packet classification purposes, namely, TOS (Type of Service) or DSCP (Differentiated Services Code Point).
- **Protocol Specific—**Whether this entry has additional specific protocol defintions (checked) or not (unchecked). The details of any additional protocol definitions can be viewed by double-clicking on the required row (entry) in the **Access List Properties** dialog box. The Access List Entry Properties dialog box is displayed with the details, for example, if the protocol is ICMP, the Access List Entry Properties dialog box defines the exact message in ICMP, for example, echo (which is the ping request).
- **Matches—**The number of packets matching the specific rule.
- **Sending Alarms—**This option is currently unavailable.

CHAPTER 6

Fault Management In MPLS Networks

This chapter describes the alarms that Cisco ANA 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 6-2—Describes the “MPLS black hole found” and “Broken LSP discovered” alarms.
- BGP Related Faults, page 6-4—Describes the “BGP neighbor loss” alarm.
- Traffic Engineering Faults, page 6-5—Describes the “MPLS TE tunnel down”, “MPLS TE tunnel flapping” and “Tunnel reoptimized” alarms.
- Layer 2 VPN Faults, page 6-5—Describes the “Pseudo Wire (L2 VPN) MPLS tunnel down” alarm.
- Alarms Summary, page 6-6—Provides a brief description of the alarms for VPNs, including their severity and the up alarm (clearing alarm) for each.

Cisco ANA supports the following alarms:

- MPLS Related Faults:
  - MPLS black hole found
  - Broken LSP discovered
- BGP Related Faults:
  - BGP neighbor loss
- 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 Cisco ANA NetworkVision window. For more information about the ticket pane, see the *Cisco Active Network Abstraction NetworkVision User Guide*.

MPLS Related Faults

This section includes descriptions of the following MPLS related faults:

- MPLS black hole found
- Broken LSP discovered

Note The MPLS black hole feature is only supported when the PEs are managed by the system.

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 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 Cisco ANA 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.

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 Cisco ANA 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 6-4).

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

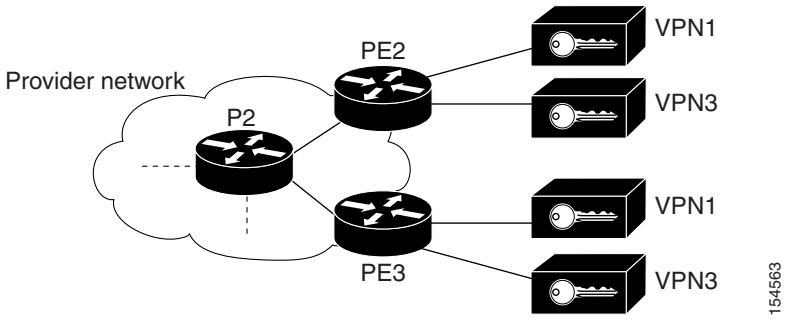
An example of a MPLS black hole scenario is provided below.

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.

Figure 6-1 Example of a MPLS Black Hole Scenario



In this case Cisco ANA 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. The Gateway periodically reviews the tickets and checks if all the alarms under each ticket are cleared or configured as auto cleared alarms, and whether the Gateway correlation timeout has passed, and in this case the Gateway closes the ticket.

Using this functionality, once the "MPLS Black hole" alarm is cleared, then after a specific time interval (configured Gateway correlation timeout) has passed, the Gateway will be able to close the ticket since all the alarms correlated to "MPLS Black hole" are "Broken LSP" which are configured as auto cleared.

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 Broken LSP Discovered Alarm, page 6-2, but all the broken LSPs that are found are correlated to the "Link Down" alarm and not to the "MPLS Black Hole Found" alarm.

BGP Related Faults

Cisco ANA monitors BGP neighbor information and makes correlation and impact analysis information available to users.

This section includes a description of the BGP related faults.

BGP Neighbor Loss

When the VNE's BGP component is polling the status of BGP neighbors (expedite or normal polling), and an entry for a neighbor does not exist any more or its state changed from Established state to any other state, the BGP component will issue an alarm for "BGP Neighbor Loss". This alarm causes the BGP component to issue a Root Cause Analysis (RCA) correlation flow to find its root cause.

If RCA does not find any alarm to correlate to, the VNE will send this alarm to the gateway as a ticket.

If this alarm is configured in the registry to issue "Look For Affected" flow, the following process will be issued:

- For each BGP link, the BGP component holds a list of PE routers (routers with VRFs) that it can reach.
- If there is a BGP neighbor loss and the BGP component has no other BGP link to a PE, all VRFs on this device with route entries with that PE as BGP next hop will be true affected.
- This information will be sent as an update for the previous "BGP Neighbor Loss" alarm.

BGP Process Down

A query checks the status of the BGP process when the VNE's BGP component is polling for the status and configuration of its BGP neighbors (expedite or normal polling).

If the BGP process is not running, the VNE's BGP component will issue an alarm "BGP Process Down".

This alarm will always be a ticket and will not try to correlate to other alarms.

All the "BGP Neighbors Down" alarms issued due to the "BGP Process Down" should correlate to this "BGP Process Down" ticket.

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

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" syslogs, which are correlated to the service alarm.

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.

Layer 2 VPN Faults

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

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.

Cisco ANA 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.

Alarms Summary

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

Table 6-1 Alarms Displayed In the Ticket Pane

Alarm	Default Severity	Description	Up Alarm
BGP Neighbor Loss	Red (critical)	The "BGP Neighbor Loss" alarm is generated whenever BGP connectivity is lost to a specific device.	BGP Neighbor Found
MPLS Black Hole Found	Dark blue (information)	A "MPLS Black Hole Found" alarm is generated whenever Cisco ANA 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 Cisco ANA 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
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, see the *Cisco Active Network Abstraction NetworkVision User Guide*.

CHAPTER 7

Calculating Impact Analysis

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, page 7-1—Describes the service impact analysis solution.
- Service Impact Analysis For MPLS Based VPN Services, page 7-2—Describes the impact analysis process for Layer 3 VPN and Pseudo Wire (Layer 2 VPN) scenarios.
- Supported Fault Scenarios, page 7-4—Describes the scenarios supported by the service impact analysis solution.

About Service Impact Analysis

Cisco ANA 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.

Automatic Impact Analysis

When a fault occurs Cisco ANA 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 the correlated faults.

Note Automatic impact analysis is not performed for every service alarm, but rather for small group of selected alarms, for example, BGP neighbor loss, broken LSP, link down, Layer 2 tunnel down and so on.

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, see Supported Fault Scenarios, page 7-4.

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, see the Cisco Active Network Abstraction NetworkVision User Guide.

For more information about automatic impact analysis, see the Cisco Active Network Abstraction NetworkVision User Guide.

Proactive Impact Analysis

Cisco ANA provides ‘what-if’ scenarios for determining the possible affect of network failures. This enables on-demand calculation of affected VPN Sites for physical links 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 Cisco ANA 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, see the Cisco Active Network Abstraction NetworkVision User Guide.

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.

L3 VPN Report (VRFs As Affected)

When affected parties are generated using the impact solution the 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.

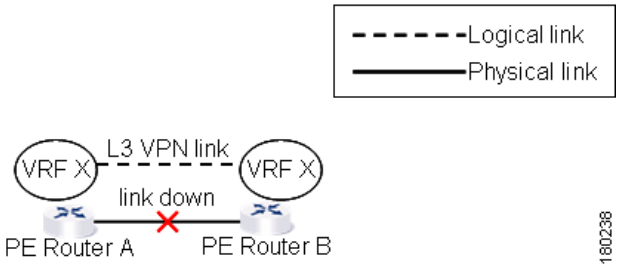
The structure of the edge points ID is Device ID \ VRF ID\ Subinterface (or interface) ID.

Note In the structure described above "**Subinterface (or interface) ID"** is optional.

Note VRF sites are not reported as affected pairs.

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

Figure 7-1 Layer 3 VPN Example



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

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, see the Cisco Active Network Abstraction NetworkVision User Guide.

Supported Fault Scenarios

The following fault scenarios trigger automatic impact analysis calculation:

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.

Link Down

Impact calculation	• Initiates an affected flow in order to determine the affected parties using the LSPs traversing the link.
Reported affected severity	• 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: – 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 (this only applies to cross-MPLS networks). – The **Affected Parties** tab of the Ticket Properties dialog box displays the latest severity, namely, **Real** affected. – The Affected Parties Destination Properties dialog box displays both reported severities. This functionality is currently only supported for “Link Down”.

Note There is an option available in the registry to configure the real and recovered functionality. Changes to the registry should only be carried out with the support of Cisco Professional Services.

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.

BGP Neighbor Loss

Impact calculation	• 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 "BGP Neighbor Loss" alarm represents a scenario where there is a BGP neigbor down.

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.

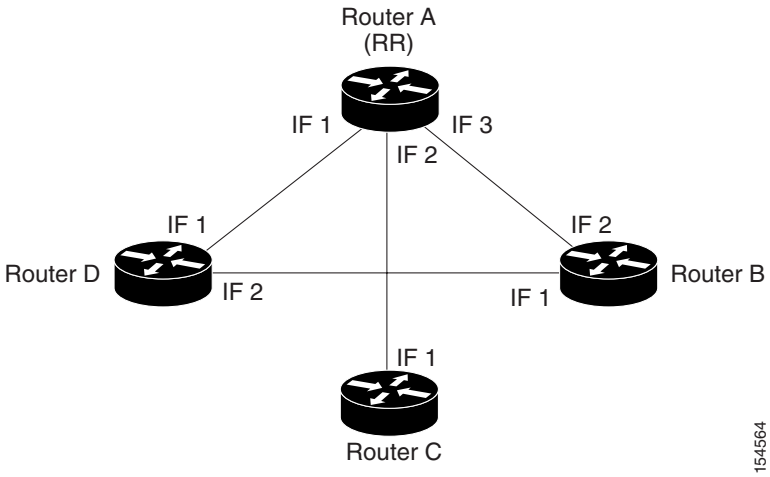
Router ID distribution follows the same logic described above.

Cisco ANA 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.

Figure 7-2 Route Reflector Example



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 Cisco ANA 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 Loss 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 Loss 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.

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 the correlated broken LSP alarms are auto-cleared.

Note There is an option available in the registry to configure broken LSP functionality. Changes to the registry should only be carried out with the support of Cisco Professional Services.

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.

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.

CHAPTER 8

Working with PathTracer in VPN Service View

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

- Cisco ANA PathTracer Tracing Capability, page 8-1—Provides a brief description of Cisco ANA PathTracer.
- Opening Cisco ANA PathTracer Over MPLS Networks, page 8-2—Describes opening the Cisco ANA PathTracer.
- Cisco ANA PathTracer Windows, page 8-3 —Describes the Cisco ANA PathTracer Multi-Path and Single-Path windows working environment and the information that can be viewed.
- Using PathTracer For Layer 3 VPN, page 8-6—Describes using the Cisco ANA PathTracer for Layer 3 VPNs, including opening the Cisco ANA PathTracer and viewing path information.
- Using PathTracer For Layer 2 VPN, page 8-7—Describes using the Cisco ANA PathTracer for Layer 2 VPNs, including opening the Cisco ANA PathTracer and viewing path information.
- Using PathTracer For MPLS Traffic Engineering Tunnels, page 8-8—Describes using the Cisco ANA PathTracer for MPLS TE tunnels, including opening the Cisco ANA PathTracer and viewing path information.

For more information about the Cisco ANA PathTracer, see the *Cisco Active Network Abstraction NetworkVision User Guide*.

Cisco ANA PathTracer Tracing Capability

Based on its extensive, up-to-date knowledge of the network, Cisco ANA 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.

Cisco ANA 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). Cisco ANA understands and is able to display the various services on the network due to the up-to-date knowledge of the network.

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

- Cisco ANA PathTracer Multi-Path window—Displays all the discovered paths available between the selected source and destination(s), including devices, and links. For more information, see the *Cisco Active Network Abstraction NetworkVision User Guide*.
- Cisco ANA 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, see the *Cisco Active Network Abstraction NetworkVision User Guide*.

Opening Cisco ANA PathTracer Over MPLS Networks

You can open and view PathTracer information between service endpoints (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 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, Cisco ANA PathTracer finds the next hop according to the “destination IP address”. When the user selects an endpoint 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 Cisco ANA 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:

Table 8-1 PathTracer Starting Points

Element	Location	Start PathTracer Options
IP Interface	• Inventory window • Affected entry (this is only enabled if the affected has an IP interface)	• to IP Destination • to Subnet Destination • Start Here
Site	Service View map	• 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 Find Business Tag window.	• to IP Destination

Table 8-1 PathTracer Starting Points (continued)

Element	Location	Start PathTracer Options
Layer 2 MPLS Tunnel	Inventory window	• to IP Destination
LCP	Service View map	• to IP Destination • Start Here

For information on opening Cisco ANA PathTracer from the Inventory window as starting point, see the *Cisco Active Network Abstraction NetworkVision User Guide*.

PathTracer Endpoints

If you selected the "**Start Here**" option the following endpoints can be selected as a path destination to open the PathTracer:

Table 8-2 PathTracer Endpoints

Element	Location	End PathTracer Options
IP Interface	• Inventory window • Affected entry (this is only enabled if the affected has an IP interface)	End Here
Site	Service View map	End Here
LCP	Service View map	End Here

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

Note If multiple paths are selected in the paths pane or if nothing is selected in the paths pane, then all the available paths will be opened automatically, and each one will be displayed in a separate Cisco ANA PathTracer Single-Path window.

Cisco ANA PathTracer Windows

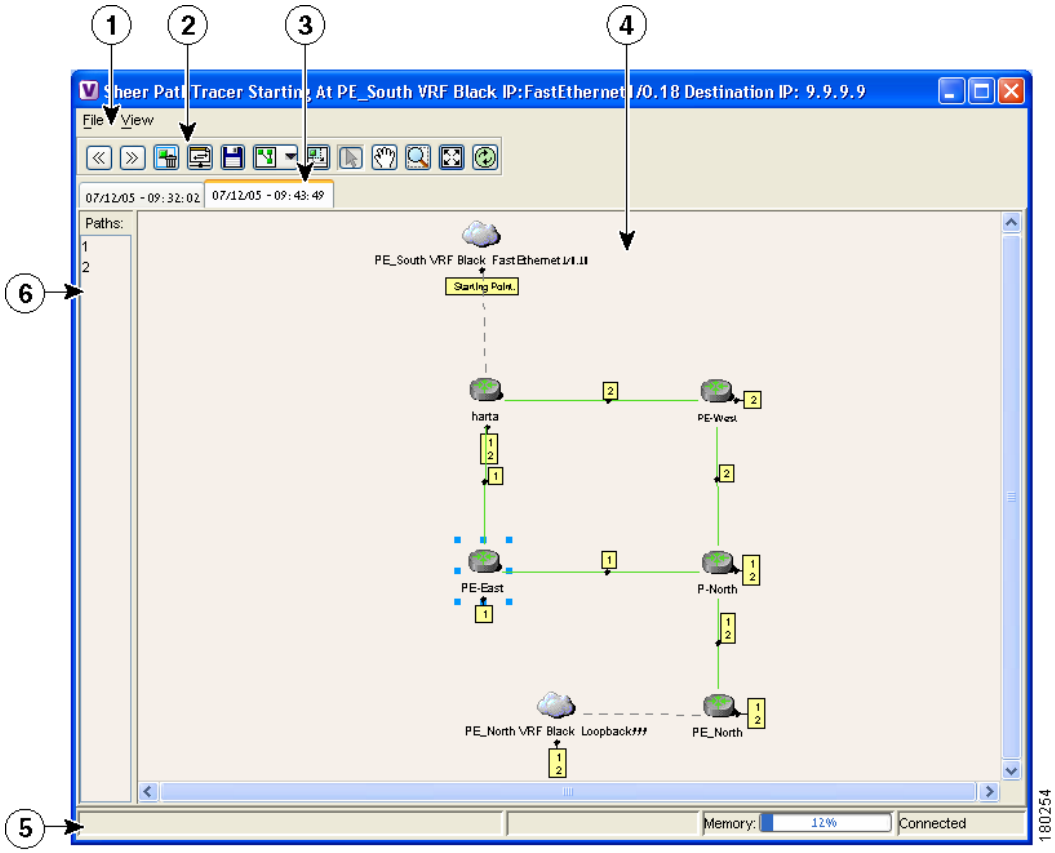
The Cisco ANA PathTracer Multi-Path window displays all the discovered paths for the selected context, including devices, links, and paths. For more information about opening Cisco ANA PathTracer, see Opening Cisco ANA PathTracer Over MPLS Networks, page 8-2.

The Cisco ANA PathTracer Multi-Path window enables you to perform the following functions:

- View a previous path or view the next path
- Open the Cisco ANA PathTracer Single-Path window in order to view a single selected path
- Save the multi-path map to a file
- Run the Cisco ANA PathTracer again

Multi-path is the ability to display all the paths available between the selected source and destination. An example of the Cisco ANA PathTracer Multi-Path window is displayed below.

Figure 8-1 Cisco ANA PathTracer Multi-Path Window



1	Menu bar
2	Toolbar
3	Map path traced at... tabs
4	Map pane
5	Status bar
6	Paths pane

For a detailed description of the Cisco ANA PathTracer Multi-Path window, see the *Cisco Active Network Abstraction NetworkVision User Guide*.

Cisco ANA PathTracer Single-Path Window

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

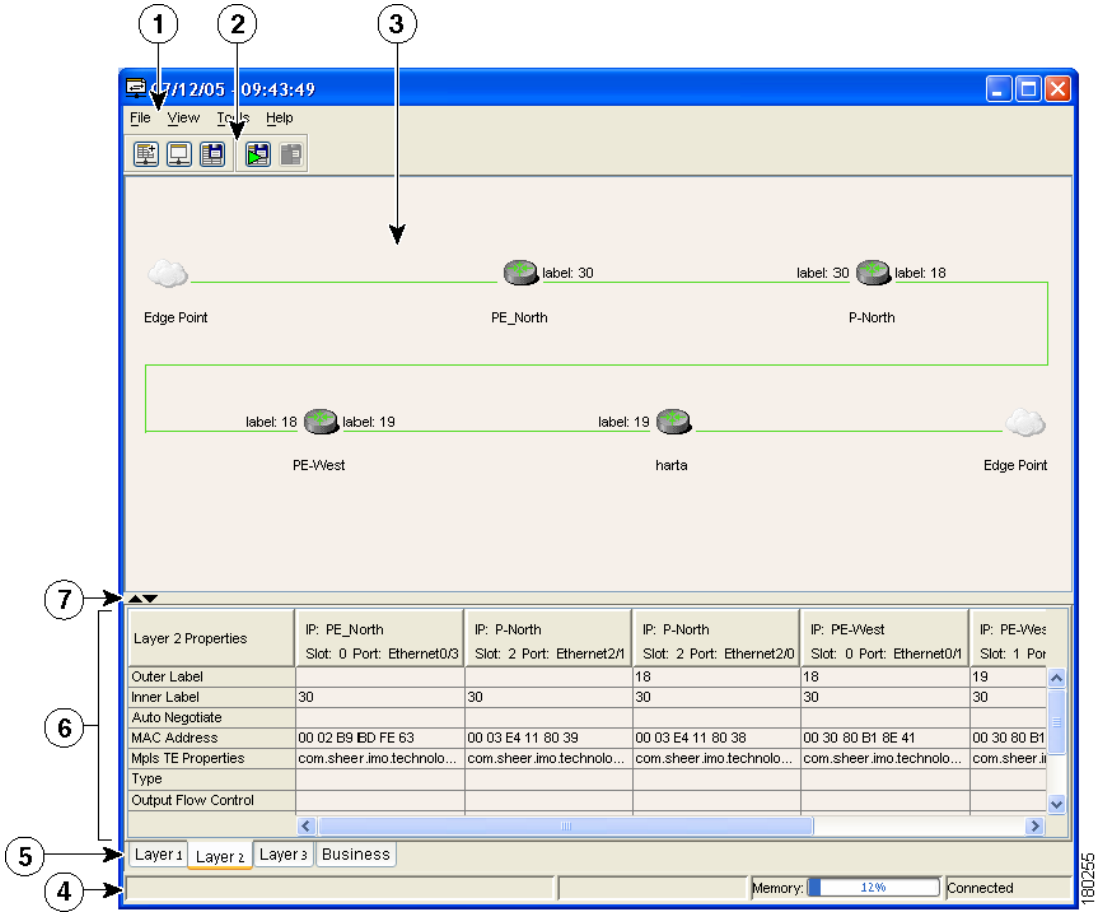
The Cisco ANA PathTracer Single-Path window enables you to:

- View a map of the intermediate network elements.
- View the following information for each network element:
  - The relevant parameters for each interface on all layers along the path.
  - For each layer an indication of a mismatch between the parameters of the interfaces on both sides of a link.
  - View traffic statistics along the path.
- Monitor the status and traffic of all the links along the path.
- View In and Out port properties.

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

An example of the Cisco ANA PathTracer Single-Path window is displayed below:

Figure 8-2 Cisco ANA PathTracer Single-Path Window



1	Menu bar
2	Toolbar

3	Map pane
4	Status bar
5	Layer tabs
6	Properties table
7	Hide/display Properties table

The Cisco ANA 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 Cisco ANA PathTracer tabs display information regarding VPNs. The information is displayed in the Layer 2 and Layer 3 tabs.

For a detailed description of the Cisco ANA PathTracer Single-Path window, see the *Cisco Active Network Abstraction NetworkVision User Guide*.

Using PathTracer For Layer 3 VPN

Cisco ANA 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 endpoint from the shortcut menu as described in Opening Cisco ANA PathTracer Over MPLS Networks, page 8-2, you can open the Cisco ANA PathTracer for Layer 3 VPNs.

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

Viewing Layer 3 Path Information

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

To view Layer 3 path information:

Step 1 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 Cisco ANA PathTracer Single-Path window with the **Layer 3** tab is displayed.

The table displays the Layer 3 VPN information on the device that has a VRF. The following Layer 3 properties displayed in the **Layer 3** tab relate specifically to VPNs:

- **Name—**The name of the Site, for example, ATM4/0.100(10.0.0.1) is a combination of the interface name and IP address used to reach the Site. Each Site belongs to a particular VPN, so the address must be unique within the VPN.
- **IP Address—**The IP address of the interface.
- **Mask—**The mask of the specific network.
- **State—**The state of the interface, 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**).

Using PathTracer For Layer 2 VPN

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

The Cisco ANA PathTracer also covers end-to-end Layer 2 VPN service paths from one customer edge (routers) to another, as part of Cisco ANA'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, see Viewing Layer 2 Path Information, page 8-7.

By selecting a start and endpoint from the shortcut menu, as described in Opening Cisco ANA PathTracer Over MPLS Networks, page 8-2, you can open the Cisco ANA PathTracer for Layer 2 VPNs.

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

Viewing Layer 2 Path Information

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

To view Layer 2 path information:

Step 1 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 Cisco ANA 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.

Using PathTracer For MPLS Traffic Engineering Tunnels

Cisco ANA Path Tracer uses label switching information to trace the end-to-end path of a TE tunnel path from one PE router to another.

Using MPLS TE (Traffic Engineering) technology, Cisco ANA'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 Opening Cisco ANA PathTracer Over MPLS Networks, page 8-2, you can open the Cisco ANA PathTracer for MPLS TE Tunnels.

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

Viewing MPLS TE Tunnel Information

Layer 2 and Layer 3 PathTracer information is displayed in the Cisco ANA 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:

Step 1 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 Cisco ANA 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 MPLS TE tunnels:

- MPLS TE Properties—The MPLS TE data set in an MPLS interface, mainly bandwidth allocation levels and signaling protocol.
- Tunnel Operational Status—The operational state of the tunnel, namely, up or down, if the Tunnel Oper status is up, the Tunne Admin Status must also be up (see the Tunnel Admin Status properties for additional information).
- Tunnel Bandwidth Kbps—Tunnel configured bandwidth in Kbps.
- Tunnel Description—A textual description of the tunnel.
- Tunnel Name—The interface name.
- 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.
- Tunnel Lockdown—If enabled, the tunnel cannot be rerouted.
- Tunnel LSP ID—LSP identification number.
- Tunnel Auto Route—If enabled, destinations behind the tunnel are routed through the tunnel.
- Tunnel Hold Priority—The tunnel's priority after path setup, when other tunnels try to remove it and claim its resources.
- Tunnel Setup Priority—The tunnel's priority upon path setup.
- Tunnel 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.
- Tunnel Out Label—The TE tunnel's MPLS label distinguishing the LSP selection in the adjacent (next) device.
- Tunnel Affinity—The tunnel's preferential bits for specific links.
- Tunnel Destination Address—The IP address of the device in which the tunnel ends.
- Tunnel Peak Rate Kbps—Flow specification measured for this tunnel (in Kbps).

- Tunnel Out Interface—The interface through which the tunnel exits the device.
- Tunnel Burst Kbps—Flow specification measured for this tunnel (in Kbps).
- Tunnel Average Rate Kbps—Flow specification measured for this tunnel (in Kbps).
- Tunnel Affinity Mask—Dictates which bits from the tunnel's affinity should be compared to the link's attribute bits.

APPENDIX A

Running a VPN Leak Report Command

This appendix describes running a VPN Leak report command.

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

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

Syntax

Item	Code and Explanation

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

Output

The output of a script is the IMO object: `"IVpnLeakReport"`. For a description of this object, see IVPNLeakReport.

Examples

Get the VPN Leak Report

The example below describes running the command.

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

VPN Leak Report Results

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.

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).

APPENDIX B

Additional Alarms

This appendix briefly describes the additional alarms that can be supported by Cisco ANA.

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

The alarms described below can be supported by Cisco ANA as well:

Alarm	Severity	Description	Up Alarm
VPN Leak	Dark blue (information)	Upon *detection of a link* 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