

# MPLS VPN Report Pack

Software Version 3.0

HP OpenView Performance Insight

---

## User Guide

June 2005



## Legal Notices

### Warranty

*Hewlett-Packard makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.*

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

### Restricted Rights Legend

Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company  
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

### Copyright Notices

© Copyright 2003 - 2005 Hewlett-Packard Development Company, L.P.

No part of this document may be copied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard Company. The information contained in this material is subject to change without notice.

### Trademark Notices

OpenView is a U.S. registered trademark of Hewlett-Packard Development Company, L.P.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

Oracle® is a registered U.S. trademark of Oracle Corporation, Redwood City, California.

UNIX® is a registered trademark of The Open Group.

Windows® and Windows NT® are U.S. registered trademarks of Microsoft Corporation.

All other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

## Support

Please visit the HP OpenView web site at:

**<http://www.managementsoftware.hp.com/>**

This web site provides contact information and details about the products, services, and support that HP OpenView offers.

You can also go directly to the support web site at:

**<http://support.openview.hp.com/>**

HP OpenView online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valuable support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and log in. Many also require a support contract.

To find more information about access levels, go to:

**[http://support.openview.hp.com/access\\_level.jsp](http://support.openview.hp.com/access_level.jsp)**

To register for an HP Passport ID, go to:

**<https://passport2.hp.com/hpp/newuser.do>**



# Contents

<b>1</b>	<b>Overview</b> .....	7
	Label-Switched Paths in a VPN .....	7
	OVPI and SLA Monitoring for Label-Switched VPNs .....	7
	Folders and Reports .....	9
	Ways to Customize Reports .....	11
	Sources for Additional Information .....	13
<b>2</b>	<b>Installing Packages</b> .....	15
	Guidelines for a Smooth Install .....	15
	Guidelines for a Smooth Upgrade .....	17
	Installing MPLS VPN 3.0 .....	18
	Post-Installation Steps .....	20
	Uninstalling MPLS VPN 3.0 .....	21
<b>3</b>	<b>Setting Up a Distributed System</b> .....	23
	Configuring the Central Server .....	23
	Configuring a Satellite Server .....	24
	System Clocks .....	24
<b>4</b>	<b>Change Forms</b> .....	25
	Create SLA Configuration Details .....	25
	Change SLA Configuration Details .....	27
	Change MPLS VPN Customer and SLA .....	28
	Change a VPN Name .....	29
	Update VPN VRF SLA Settings .....	30
<b>5</b>	<b>VPN Inventory</b> .....	33
<b>6</b>	<b>Route Activity</b> .....	35
<b>7</b>	<b>Unreachable VPN Interfaces</b> .....	39
<b>8</b>	<b>VPN Interface Exception Hot Spots</b> .....	41
<b>9</b>	<b>VPN Traffic Volume</b> .....	45
<b>10</b>	<b>Current VRF Operational Status</b> .....	49
<b>A</b>	<b>Manual Provisioning</b> .....	51
	Elements and Properties .....	51
	Provisioning Interfaces .....	53

Provisioning Devices .....	53
Provisioning VRFs .....	53
Provisioning VPNs .....	55
Provisioning SLAs .....	56
<b>B Editing Tables and Graphs .....</b>	<b>59</b>
View Options for Tables .....	59
View Options for Graphs .....	60
<b>Glossary .....</b>	<b>67</b>
<b>Index .....</b>	<b>71</b>

# 1 Overview

This chapter covers the following topics:

- [Label-Switched Paths in a VPN](#)
- [OVPI and SLA Monitoring for Label-Switched VPNs](#)
- [Folders and Reports](#)
- [Ways to Customize Reports](#)
- [Sources for Additional Information](#)

## Label-Switched Paths in a VPN

An internet service provider can create virtual private networks (VPNs) for its customers. Each VPN shares a common backbone that connects all the sites belonging to a customer. Each VPN contains backbone routers, provider edge routers, and customer edge routers. If the service provider implements Multi-Protocol Label Switching (MPLS), the provider edge routers communicate with each other using label-switched paths.

Each provider edge router maintains a virtual routing and forwarding table, or VRF. The purpose of the VRF is to point traffic toward the correct customer edge router. The provider edge router receives routing updates from customer edge routers and distributes routing updates to other provider edge routers. The interfaces on a provider edge router can be MPLS-enabled or they can function as VPN endpoints. When an interface is MPLS-enabled, it faces the common backbone. When an interface functions as a VPN endpoint, it belongs to a VRF and faces the customer.

## OVPI and SLA Monitoring for Label-Switched VPNs

HP OpenView Performance Insight (OVPI) is a performance management and reporting application. Long-term data collection, in-depth analysis, and automated web-based reporting are this application's primary strengths. If desired, OVPI can be integrated with network management and system management applications, including NNM and OVO. Integration enhances fault isolation, problem diagnosis, and capacity planning.

The MPLS VPN Report Pack installs on OVPI. The reports in this package monitor the status of large-scale enterprise VPNs running over MPLS-enabled networks. The basic reporting component is the device-level logical interface, as presented by the ifTable in MIB-II. The MPLS VPN Report Pack collects data from the ifTable and automates the following chores:

- Finding VRFs that are generating errors
- Finding VRFs that are not functioning

- Ranking VPNs according to utilization
- Grouping multiple VPN-associated interfaces into single entities
- Applying SLA metrics, such as utilization or discard ratios, to VPNs and individual VRFs
- Discovering VPN network configurations and relationships
- Calculating statistics for label usage and failed label lookups

## Dependencies

MPLS VPN 3.0 builds on the capabilities of the Interface Reporting Report Pack. The following packages are prerequisites for MPLS VPN 3.0:

- Interface Discovery Datapipe — discovers MIB-II interfaces and tracks them for re-indexing events
- Interface Reporting ifEntry Datapipe — polls devices for MIB-II data
- Common Property Tables — maintains a single set of customer, location, and device tables shared by multiple report packs
- Threshold and Event Generation Module — generates SNMP traps based on service level metrics and sends traps to the network management system

## Version History

The following table outlines recent enhancements to the MPLS VPN Report Pack.

Package Version	Release Date	Features/Enhancements
1.0	May 2003	27 reports Directed-instance polling support Interface re-indexing support MPLS VPN Datapipe 1.0
2.0	October 2003	OVPI Object Manager support MPLS VPN Datapipe 2.0 <i>new forms:</i> <ul style="list-style-type: none"> <li>• Create SLA Config Details</li> <li>• Change SLA Config Details</li> <li>• Change MPLS VPN Name</li> <li>• Change MPLS VPN Customer &amp; SLA</li> <li>• Update VPN &amp; VRF SLA Settings</li> </ul>
3.0	April 2004	OVPI 5.0 support Oracle support MPLS VPN Datapipe 3.0
3.0	August 2004	Upgrade package (to_3.0)



Package Version	Release Date	Features/Enhancements
3.0	November 2004	Juniper MPLS VPN Datapipe 1.0 MPLS VPN Datapipe 3.1
3.0	June 2005	No changes

## Folders and Reports

If you are viewing reports using the Web Access Server, you will see the following report folders:

- Admin
- Devices
- Interface
- VPNs
- VRFs

The following table provides details about the reports in each folder.

Folder	Reports	
Admin	MPLS Inventory	A list of all MPLS enabled interfaces with MPLS specific configuration data.
	VPN Inventory	Select a VPN to see component VRFs. Select a VRF to display a list of all associated interfaces.
	VPN SLA Configuration	Displays VPNs and their component VRFs, with the current SLA settings for each.
Devices	Recent MPLS Activity	A current view of all devices with MPLS enabled interfaces. Provides details for label count, label lookup, and fragment count.
	Recent VPN Activity	Historical analysis of configured interfaces, configured and active VRF counts, interface exception counts (by utilization, error and discard ratio) and route counts.
	Recent VPN Route Activity	Historical route change activity across devices that support VRFs.

<b>Folder</b>	<b>Reports</b>	
Interfaces	MPLS Availability and Response Time	Availability (based on ifOperStatus) and SNMP response time (for management traffic) for MPLS-enabled interfaces.
	MPLS Unreachable Interfaces	MPLS-enabled interfaces that have not responded to poll requests within the previous 35 minutes, but have responded at some time during the previous 6 hours.
	Near Real Time MPLS	Displays configuration data accompanied by exception counts, utilization, discards and errors.
	NRT MPLS Snapshot	Same as Near Real Time MPLS, but with an interface pre-selection window to accommodate selective displays of data.
	Near Real Time VPN	Displays configuration data accompanied by exception counts, utilization, discards and errors.
	NRT VPN Snapshot	Same as Near Real Time VPN, but with an interface pre-selection window to accommodate selective displays of data.
	VPN Availability and Response Time	Availability (based on ifOperStatus) and SNMP response time (for management traffic) for VPN-associated interfaces.
	VPN Grade of Service	VPN-associated interfaces with their exception counts, presented in a GOS type report showing hours with and without exceptions.
	VPN Interface Exception Hot Spots	VPN configuration data accompanied by interface exception counts, utilization, discards and errors.
	VPN Top Ten Volume	A list of the top and bottom ten VPN-associated interfaces based on transferred volume. Provides many configuration details.
VPN Unreachable Interfaces	VPN-associated interfaces that have not responded to poll requests within the previous 35 minutes, but have responded at some point during the previous 6 hours.	

Folder	Reports	
VPNs	Route Activity	Lets you examine hourly and daily route activity for a VPN as a whole, and also on a per-VRF basis.
	Top 10/Bottom 10 — Interface Availability	The top and bottom ten VPNs on the network in terms of component interface availability.
	Top 10/Bottom 10 — Volume	The top and bottom ten VPNs on the network in terms of volume. Only ifOutOctets are counted in order to avoid double-counting each packet.
	Traffic	Historical traffic counts for a VPN as a whole. Includes exception counts across all interfaces in the VPN and links to the VRF traffic graphs.
	VPN Exception Hot Spots	A historical report focusing on yesterday's problems. Includes details for exception counts across all VPN-associated interfaces, route counts across all VRFs within the VPN, and traffic statistics.
	VPN Executive Summary	A monthly summary for each VPN; includes number of routes, total volume transferred, interface exceptions, security violations, and operational seconds.
VRFs	Current OperStatus	The operational status of each VRF on the network, arranged so that <i>Down</i> and <i>Unknown</i> VRFs appear first in the list for ease of trouble shooting.
	Historical Utilization	Traffic, utilization, and exception history for each component interface of the VRF on a daily basis.
	Recent OperStatus	Operational status changes for each VRF over the previous 24 hours, including active and associated interface counts, as well as configuration changes.
	Recent Utilization	Utilization, traffic, and exception details for VRFs and their component interfaces during the most recent complete polled hour.

## Ways to Customize Reports

You can customize the contents of MPLS VPN reports by applying group filters, by adding property data, by modifying property data, by applying constraints, and by changing view options for tables and graphs. For details about view options for tables and graphs, see [Appendix B, Editing Tables and Graphs](#).

## Group Filters

Group filters allow service providers (or any organization interested in sharing reports with customers) to produce customer-specific reports. Creating customer-specific reports involves the following tasks:

- Importing customers and locations using Common Property Tables
- Creating a group account for all of the users affiliated with each customer or group
- Creating a group filter for each group account

For more information about group filters, refer to the *OVPI 5.1 Administration Guide*.

## Applying Constraints

You apply constraints by editing parameters. Editing a parameter filters out the data you are not interested in seeing. For example, if you edit the Customer Name parameter, data for every customer except the customer you typed in the Customer Name field drops from the report. You can apply multiple constraints at once. The reports in MPLS VPN 3.0 support the following parameters:

- VPN Name
- SLA Name
- VRF Name
- Device
- Interface
- Protocol
- Customer Name
- Customer ID
- Location
- MinutesSincePoll
- Full or Half

If you are using the Web Access Server to view reports, edit parameters by clicking the Edit Parameters icon at the bottom right-hand corner of the report. When the Edit Parameters window opens, enter the constraint in the field and click **Submit**.

If you are using Report Viewer, select **Edit > Parameter Values** from the menu bar. When the Modify Parameter Values window opens, click the **Current Value** field. Type a new value and click **OK**.

## Adding and Modifying Property Data

The reports in MPLS VPN 3.0 accommodate custom property information for:

- Devices
- Interfaces
- VPNs
- VRFs

If you used Common Property Tables to assign custom attributes to devices, the reports in MPLS VPN 3.0 will inherit those attributes automatically. To update device-level property data, use the change forms that come with Common Property Tables.

If you assigned customer and location attributes to the interfaces monitored by Interface Reporting, the reports in MPLS VPN 3.0 will inherit those attributes automatically. To update interface-level property data, you can import a file that contains your updates, or you can use the change forms that come with Interface Reporting.

Property data for VPNs is not inherited. The following attributes can be assigned to a VPN:

- Customer
- Location
- SLA settings

Property data for VRFs is not inherited. The following attributes can be assigned to a VRF:


- Customer
- SLA settings

## Sources for Additional Information


This user guide contains samples of some of the reports in MPLS VPN 3.0. The demo package that comes with MPLS VPN 3.0 contains a sample of every report in the package. If you have access to the demo package and you want to know what fully-populated reports look like, install the demo package. Like real reports, demo reports are interactive. Unlike real reports, demo reports are static.

For information regarding the latest enhancements to MPLS VPN 3.0 and any known issues affecting this package, refer to the *MPLS VPN Report Pack 3.0 Release Statement*. You may also be interested in the following documents:

- *MPLS VPN Juniper Datapipe 1.0 Release Statement*
- *MPLS VPN Datapipe 3.1 Release Statement*
- *Interface Reporting Report Pack 5.0 User Guide*
- *Interface Discovery Datapipe 2.2 User Guide*

 Includes information about the frequency of collections, specific SNMP MIBs, and specific SNMP OIDs.

- *Interface Reporting ifEntry Datapipe 2.2 User Guide*

 Includes information about the frequency of collections, specific SNMP MIBs, and specific SNMP OIDs.

- *Thresholds Module 5.0 User Guide*
- *NNM/OVPI Integration Module 2.0 User Guide*
- *OVPI Report Packs, Version 8.0: Release Notes, June 2005*

Manuals for the core product, OVPI, and manuals for the reporting solutions and shared packages that run on OVPI, can be downloaded from this site:

<http://www.managementsoftware.hp.com>

Select **Support > Product Manuals** to reach the **Product Manuals Search** page. The user guides for OVPI are listed under **Performance Insight**. The user guides for report packs and datapipes are listed under **Performance Insight Reporting Solutions**.

The manuals listed under **Performance Insight Reporting Solutions** indicate the month and year of publication. If a manual is revised and reposted, the date of publication will change even if the software version number does not change. Since we post revised manuals on a regular basis, we recommend that you search this site for updates before using an older manual that might not be the latest version available.

## 2 Installing Packages

This chapter covers the following topics:

- [Guidelines for a Smooth Install](#)
- [Guidelines for a Smooth Upgrade](#)
- [Installing MPLS VPN 3.0](#)
- [Post-Installation Steps](#)
- [Accessing Deployed Reports](#)
- [New Objects and a New View](#)
- [Uninstalling MPLS VPN 3.0](#)

### Guidelines for a Smooth Install

The reporting solutions designed for OVPI consist of a report pack and a datapipe, or sometimes a report pack and multiple datapipes. When you install a datapipe, you configure OVPI to collect a specific type of performance data at a specific polling interval. When you install the report pack, you configure OVPI to summarize and aggregate the performance data collected by the datapipe.

The June 2005 report pack CD includes the latest report packs and datapipes. When you insert the CD in the CD\_ROM drive and launch the package extraction program, the install script copies every package from the CD to the Packages directory on your system. After the extract finishes, the install script prompts you to launch OVPI and start Package Manager. Before using Package Manager, review the following guidelines.

### Software Prerequisites

The following software must be installed before installing MPLS VPN 3.0:

- OVPI 5.0 or higher
- All service packs available for the version of OVPI (5.0 or 5.1) you are running
- Common Property Tables 3.5
- Interface Reporting 5.0

Interface Reporting requires two datapipes:

- Interface Discovery Datapipe 2.2
- Interface Reporting ifEntry Datapipe 2.2

If you are upgrading Interface Reporting, you may need to remove earlier versions of those datapipes, specifically:

- Interface Discovery Datapipe 1.1 / 2.0 / 2.1
- Interface Reporting ifEntry Datapipe 1.1 / 2.0 / 2.1

For details about upgrading Interface Reporting, refer to the *Interface Reporting Report Pack 5.0 User Guide*.

## Common Property Tables

MPLS VPN 3.0 requires Common Property Tables. If you are not currently running any version of Common Property Tables, Package Manager will select and install Common Property Tables for you, automatically.

If you are running Common Property Tables 2.2 or 3.0, upgrade to version 3.5 by installing the “to\_3.5” upgrade package. When you install the upgrade package for Common Property Tables, do not install anything else. Install the upgrade package and *only* the upgrade package. If you need help with the upgrade, or if you want to know more about how this package operates, refer to the *Common Property Tables 3.5 User Guide*.

## MPLS\_VPN\_Threshold

If NNM and OVPI are integrated, you should install the optional thresholds sub-package, MPLS\_VPN\_Threshold. Installing the thresholds sub-package enables a set of customized performance thresholds and configures OVPI to send thresholds traps to NNM. Threshold traps sent to NNM display as alarms in the NNM alarm browser.

You have the following options for setting thresholds:

- Set thresholds for rate data only
- Set thresholds for rate data and aggregated data
- Set thresholds for aggregated data only

The option you want determines where you need to install the thresholds sub-package. If you want to set thresholds for rate data only, then you must install the thresholds sub-package on satellite servers only. If you want to set thresholds for rate data and aggregated data (daily data, or a forecast), then you must install the thresholds sub-package on the central server as well as on each satellite server.

If you install MPLS\_VPN\_Threshold, Package Manager will install a prerequisite package, the Thresholds Module, for you. You may already have the Thresholds Module installed. Although MPLS VPN 3.0 is compatible with Thresholds Module 3.0, we recommend upgrading to Thresholds Module 5.0.

## Distributed Environments

Package installation in a distributed environment is more complicated than package installation on a stand-alone system. If you are planning to install MPLS VPN in a distributed environment, the central server, every satellite server, and every remote poller must be running OVPI 5.0 and all available service packs for OVPI 5.0. Here is a high-level overview of the installation procedure for a distributed environment:

- 1 Disable trendcopy on the central server.
- 2 Install MPLS VPN 3.0 (along with any prerequisite packages that are not already installed) on the central server; deploy reports.



- 3 Install MPLS VPN 3.0 (along with any prerequisite packages that are not already installed) and the MPLS VPN Datapipe on each satellite server; do not deploy reports
- 4 Re-enable trendcopy on the central server.

When installation is complete, you must set up connections between the central server and satellite server databases, configure trendcopy pull commands, and switch-off daily and monthly aggregations on satellite servers. For details, see [Chapter 3, Setting Up a Distributed System](#).

## Guidelines for a Smooth Upgrade

If you are currently using MPLS VPN 2.0, you should have no problem upgrading to MPLS VPN 3.0. Look for the following package when you run Package Manager:

```
UPGRADE_MPLS_VPN_2.0_to_3.0
```

The datapipe that collected data for MPLS VPN 2.0 cannot be upgraded. Before installing the upgrade package for the report pack, remove the previous datapipe.

Follow these steps to upgrade from version 2.0 to version 3.0:

- 1 Start Package Manager; remove MPLS VPN Datapipe 2.0.
- 2 Exit Package Manager.
- 3 Start Package Manager; install UPGRADE\_MPLS\_VPN\_2.0\_to\_3.0.
- 4 Exit Package Manager.
- 5 Start Package Manager; install MPLS VPN Datapipe 3.1.
- 6 Exit Package Manager.

There are two preliminary tasks that may or may not apply to your situation. The first task pertains to remote pollers and the need to save configuration data related to polling policies and polling groups. The second task pertains to custom table views.

## Datapipes and Remote Pollers

When you uninstall an existing datapipe, the following information is lost:

- Single polling policy for a remote poller
- Cloned polling policies for multiple remote pollers
- Customized polling groups

To prevent this information from being lost, you can export existing polling policy configurations and customized polling groups by using the following commands:

- `collection_manager`
- `group_manager`

## Exporting Polling Policy Configurations

If your environment contains polling policies for remote pollers, use the `collection_manager` command to export existing policy configurations to a file.

*UNIX:* As user `trendadm`, run the following command:

```
cd $DPIPE_HOME
```

```
./bin/collection_manager -export -file /tmp/savePollingPolicy.lst
```

*Windows:* As Administrator, launch a command window. Navigate to the OVPI install directory and execute the following command:

```
bin\collection_manager -export -file \temp\savePollingPolicy.lst
```

## Exporting Polling Group Configurations

If your environment contains customized polling groups, use the `group_manager` command to export groups to individual `.xml` files.

*UNIX:* As user `trendadm`, execute the following command:

```
cd $DPIPE_HOME
```

```
./bin/group_manager -export_all -outfile /tmp/savePollingGroups
```

*Windows:* As Administrator, launch a command window, then navigate to the OVPI install directory and execute the following command:

```
bin\group_manager -export_all -outfile \temp\savePollingGroups
```

## Custom Table Views

If you created custom views for data or property tables, the views you created may interfere with the report pack upgrade process, causing the process to fail. Whether or not your views interfere with the upgrade process depends on how you created them. If you created them using SQL, the upgrade will succeed but your views will not be available once the upgrade is complete. If you created them using Datapipe Manager, the upgrade is likely to fail. To prevent the upgrade from failing, delete your custom views before upgrading the report pack, then recreate them after the upgrade is complete.

## Installing MPLS VPN 3.0

Follow these steps to install MPLS VPN 3.0 on a stand-alone system:

- Stop OVPI Timer and extract packages from the report pack CD
- Upgrade to Common Property Tables 3.5
- Install MPLS VPN 3.0 and restart OVPI Timer

Task 1: Stop OVPI Timer and extract packages from the report pack CD

- 1 Log in to the system. On UNIX<sup>®</sup> systems, log in as root.
- 2 Stop OVPI Timer and wait for processes to terminate.

On Windows, do the following:

- a Select **Control Panel > Administrative Tools > Services**
- b Select OVPI Timer from the list of services.
- c From the Action menu, select **Stop**

On UNIX, as root, do one of the following:

- HP-UX: **sh /sbin/ovpi\_timer stop**
  - Sun: **sh /etc/init.d/ovpi\_timer stop**
- 3 Insert the June 2005 report pack CD in the CD-ROM drive.  
Windows: The Main Menu automatically displays.  
UNIX:
    - a Mount the CD (if the CD does not mount automatically).
    - b Navigate to the top level directory on the CD.
    - c Run **./setup**
  - 4 Type **1** in the choice field and press **Enter**. The install script displays a percentage complete bar. When the copy is complete, the install script starts Package Manager. The Package Manager welcome window opens.

Once extraction to the Packages directory is complete, you can navigate to that directory to see the results. Under the MPLS VPN report pack you will see the following folders:

- MPLS\_VPN.ap
- MPLS\_VPN\_Demo.ap
- MPLS\_VPN\_Thresholds.ap

Installing the demo package is optional. You may install the demo package by itself, with no other packages, or you may install the demo package along with everything else.

#### Task 2: Upgrade to Common Property Tables 3.5

MPLS VPN 3.0 requires Common Property Tables 3.5. If you are not running any version of Common Property Tables, skip this step. If you are running version 2.2 or version 3.0, install the “to\_3.5” upgrade package. When Package Manager indicates that the upgrade is complete, click **Done** to return to the Management Console.



If you need help with the upgrade, refer to the *Common Property Tables 3.5 User Guide*.

#### Task 3: Install MPLS VPN 3.0 and restart OVPI Timer

- 1 Start Package Manager. The Package Manager welcome window opens.
- 2 Click **Next**. The Package Location window opens.
- 3 Click **Install**.
- 4 Click **Next**. The Report Deployment window opens. Accept the default for Deploy Reports; type your username and password for the OVPI Application Server.
- 5 Click **Next**. The Package Selection window opens.
- 6 Click the check box next to the following packages:
  - *MPLS\_VPN*
  - *MPLS\_VPN\_Threshold*
  - *MPLS\_VPN\_Datapipe*
  - *Juniper\_MPLS\_VPN\_Datapipe*
  - *Interface\_Reporting\_ifEntry\_Datapipe\_2.2* (if not already marked as installed)

- *IFEntry\_Discovery\_Datapipe\_2.2* (if not already marked as installed)
  - *Interface\_Reporting\_5.0* (if not already marked as installed)
  - *MPLS\_VPN\_Demo* (optional)
- 7 Click **Next**. The Type Discovery window opens. Accept the default and click **Next**. The Selection Summary window opens.
  - 8 Click **Install**. The Installation Progress window opens. When installation is complete, a package installation complete message appears.
  - 9 Click **Done** to return to the Management Console.
  - 10 Restart OVPI Timer.

On Windows, do the following:

- a Select **Control Panel > Administrative Tools > Services**
- b Select OVPI Timer from the list of services.
- c From the Action menu, select **Start**

On UNIX, as root, do one of the following:

- HP-UX: **sh /sbin/ovpi\_timer start**
- Sun: **sh /etc/init.d/ovpi\_timer start**

## Post-Installation Steps


After you install the report pack, do the following:

- 1 Verify correct installation by calling the `MPLS_VPN_Check_Status.sql` script from the command line. If the script detects an unusual configuration, it will log warning messages.

To run this script, type the following command from one of these directories:

- For Oracle: `OVPI/packages/MPLS_VPN/MPLS_VPN.ap/Oracle`
- For Sybase: `OVPI/packages/MPLS_VPN/MPLS_VPN.ap/Sybase`

**ovpi\_run\_sql -sqlscript MPLS\_VPN\_Check\_Status.sql**

-  Running this script does not guarantee that the report pack was properly configured.

- 2 Launch Polling Policy Manager and make sure that the list of nodes includes your MPLS VPN nodes.
- 3 In approximately 1 hour, check that polling started as expected. Examine the Configuration and Logging Report (Admin folder, Interface Reporting). Messages from MPLS\_VPN procedures will have MPLS or VPN in their name. You should see creation messages for devices, interfaces, VRFs, and VPNs.
- 4 Provision managed elements that are not automatically provisioned. For details, see [Appendix A, Manual Provisioning](#).

## Accessing Deployed Reports

When you installed the MPLS VPN Report Pack, you enabled the Deploy Reports option. As a result, the reports in this package (as well as any change forms that come with the reports) were deployed to the OVPI Application Server. Once reports reside on the OVPI Application Server, you have two ways to view them:

- OVPI client applications
- Web browser

If the client applications are installed on your system, you have access to Report Viewer, Report Builder, and the Management Console. If the client applications are not installed on your system, using a web browser to view reports is the only way you can view reports.

For more information about the clients, refer to the *OVPI 5.1 Installation Guide*. For details about the Management Console, including how to use the Object/Property Management view to launch reports specific to a selected object, refer to the *OVPI 5.1 Administration Guide*.

## New Objects and a New View

Any item that appears in a report accompanied by performance data or property information is an object. Devices, customers, and locations are objects, and all three of these object categories belong to OVPI's default object model. When you select an object in the object model, the right side of the Object/Property Management window refreshes, showing:

- A list of forms under **General Tasks**
- A list of forms under **Object Specific Tasks**
- A list of reports under **Object Specific Reports**

The object tree changes each time you install a new report pack. Installing Interface Reporting adds interfaces as objects under devices. In addition to adding new objects, some report packs add an entirely new class of objects or services. When this happens, the report pack provides a new view. To open the new view, select **View > Change View**.

The MPLS VPN Report Pack provides a new view tailored to VPNs and their VRFs. The new view is called **Mpls Vpn**. The object tree hierarchy for this view is as follows:

**Mpls Vpn > Device > Vpn Vrf > Interface Type > Interface**

Lower levels of the object tree inherit property information assigned to the upper levels. For example, setting a customer against an MPLS VPN will apply this customer to every interface in that VPN that does not already have the customer attribute set to a different value.

## Uninstalling MPLS VPN 3.0

Follow these steps to uninstall the MPLS VPN 3.0 and any dependent datapipe:

- 1 Log in to the system. On UNIX systems, log in as root.
- 2 Stop OVPI Timer and wait for processes to terminate.

On Windows, do the following:

- a Select **Control Panel > Administrative Tools > Services**
- b Select OVPI Timer from the list of services.

- c From the Action menu, select **Stop**.

On UNIX, as root, do one of the following:

- HP-UX: **sh /sbin/ovpi\_timer stop**
- Sun: **sh /etc/init.d/ovpi\_timer stop**

- 3 Open the Management Console and start Package Manager. The Package Manager welcome window opens.
- 4 Click **Next**. The Package Location window opens.
- 5 Click **Uninstall**.
- 6 Click **Next**. The Report Undeployment window opens. Keep the defaults.
- 7 Click **Next**. The Package Selection window opens. Click the check box next to:
  - *MPLS\_VPN*
  - *MPLS\_VPN\_Datapipe*
  - *Juniper\_MPLS\_VPN\_Datapipe*
  - *MPLS\_VPN\_Demo* (if installed)
- 8 Click **Next**. The Selection Summary window opens.
- 9 Click **Uninstall**. The Progress window opens. When removal is complete, a package removal complete message appears.
- 10 Click **Done**.
- 11 Restart OVPI Timer.

On Windows, do the following:

- a Select **Control Panel > Administrative Tools > Services**
- b Select OVPI Timer from the list of services.
- c From the Action menu, select **Start**

On UNIX, as root, do one of the following:

- HP-UX: **sh /sbin/ovpi\_timer start**
- Sun: **sh /etc/init.d/ovpi\_timer start**

# 3 Setting Up a Distributed System

If you deploy MPLS VPN 3.0 in a distributed environment, you must configure the central server and each satellite server. This chapter covers:

- Configuring the central server
- Configuring a satellite server
- System clocks

You may also want to install and configure remote pollers. If you need help installing and configuring a remote poller, refer to the *OVPI 5.1 Installation Guide*.

## Configuring the Central Server

To configure the central server, perform the following tasks:

- Task 1: Set up connections with satellite server databases
- Task 2: Configure trendcopy pull commands and modify the trendtimer entry

### Task 1: Set up connections with satellite server databases

- 1 Select **HP OpenView > Performance Insight > Management Console**.
- 2 Click the **Systems** icon on the lower left. The **System/Network Administration** pane opens.
- 3 Right-click the Databases folder. When prompted, select **Add OVPI Database**. The Add Database Wizard opens.
- 4 Click **Next**.
- 5 Type the hostname and port number for the database you want to add; click **Next**.
- 6 Review the Summary. Repeat Steps 4 and 5 for each additional database.
- 7 Click **Finish** when you finish adding databases.

### Task 2: Configure trendcopy pull commands and modify the trendtimer entry

- 1 Configure trendcopy pull commands from the central server to each remote satellite. Do that by opening `$DPIPE_HOME/scripts/MPLS_Hourly_Process.pro` and modifying the trendcopy commands. Add to each command the name of the central server and the same of the satellite server. If necessary, add more commands.
- 2 Modify the hourly MPLS\_VPN trendtimer entry.

This process currently starts at 30 minutes after the hour. If you make the start time 10 minutes later, the central server will not attempt to copy data from the satellites at the same instant the satellites begin their summarizations.

## Configuring a Satellite Server

If you do not want local reporting, switch off unnecessary processing by disabling MPLS VPN daily and monthly processing. Switch off these processes by commenting out the entry in `$DPIPE_HOME/lib/trendtimer.sched` that references `MPLS_DMF_Process.pro`.

## System Clocks

Make sure that the system clock on each satellite server is synchronized with the system clock on the central server. Synchronization is extremely important when linked processes are executing in exact sequences across independent machines.



## 4 Change Forms

Change forms make it easy to update properties. Use change forms to:

- Create SLA configuration details
- Change SLA configuration details
- Change the name of the customer assigned to a VPN
- Change the name of the SLA assigned to a VPN
- Assign a new name to a VPN
- Update the SLA settings assigned to a VRF

You are free to import property data in batch-mode by using a file. The batch-mode method is more efficient if you have a lot changes to make or if you are working with an automated import mechanism configured from another application. For details about creating property import files, see [Appendix A, Manual Provisioning](#).

### Create SLA Configuration Details

With the MPLS VPN Report Pack, the user can configure thresholds for metrics such as the operational percentage of the VPN, the overall interface availability, and the error percentage of traffic traversing the VPN. If you want to combine these metrics into a single Service Level Agreement (SLA), you have the option of applying the SLA to the entire VPN or to individual VRFs.

Follow these steps to open the form and create MPLS VPN SLA configurations:

- 1 In the Management Console, click the **Objects** icon.
- 2 Select **File > New**.

- 3 Select **Create MPLS VPN SLA** and click **Create**. The form opens.

C:\OVPI\forms\deploy\admin\MPLS\_VPN\_Forms\create\_MPLSVPNSLAConfig.frep

## MPLS VPN

### Create SLA Configuration Details

Use this form to create the SLA Configuration for the MPLS VPN report pack.

SLA Name:	SLA Name
Operational % :	The percentage of all the VRFs in a VPN which must stay operational for the SLA to remain in place
Int Availability % :	The percentage of all VPN associated interfaces which must stay available for the SLA to remain in
Discard Threshold % :	The percentage of all VPN traffic which is allowably discarded.
Error Threshold % :	The percentage of all VPN traffic which is allowably errored.
SNMP Response Time :	The maximum average SNMP response time (in milliseconds) for PI issued SNMP requests allowable managed interface.

<b>SLA Name</b>	<input type="text"/>
<b>Operational Pct</b>	<input type="text"/>
<b>Interface Availability</b>	<input type="text"/>
<b>Discard Threshold</b>	<input type="text"/>
<b>Error Threshold</b>	<input type="text"/>
<b>SNMP ResponseTime</b>	<input type="text"/>

Warning: When you press OK or Apply, all the settings above will be applied to create a new SLA.

OK Apply

- 4 Create details about the SLA by adding data to each field.
- 5 Click **Apply**, then click **OK** to save the changes and close the form.

# Change SLA Configuration Details

SLA details do not relate to a managed object directly; they are applied to a managed object. For this reason the Change SLA Configuration Details form always appears in the General Tasks window when any object is selected. Follow these steps to open the form and change SLA Configuration details:

- 1 In the Management Console, click the **Objects** icon.
- 2 Select any object in the model.
- 3 Under General Tasks, double-click **Change SLA Config**.

## MPLS VPN Change SLA Config Details



Use this form to create the SLA Configuration for the MPLS VPN report pack.

SLA Name:	SLA Name
Operational % :	The percentage of all the VRFs in a VPN which must stay operational for the SLA to remain in place.
Int Availability % :	The percentage of all VPN associated interfaces which must stay available for the SLA to remain in place.
Discard Threshold % :	The percentage of all VPN traffic which is allowably discarded.
Error Threshold % :	The percentage of all VPN traffic which is allowably errored.
SNMP Response Time :	The maximum average SNMP response time (in milliseconds) for PI issued SNMP requests allowable for a managed interface.

SLAName	Operational Pct	Interface Availability	Discard Threshold	Error Threshold	SNMP ResponseTime
SLA_Default	96.00	80.00	3.00	3.00	500.00
Gold	100.00	95.00	1.00	1.00	50.00
Silver	98.00	90.00	2.00	2.00	100.00
Bronze	96.00	80.00	3.00	3.00	500.00

<b>Operational Pct</b>	<input type="text" value="96.00"/>	<b>Interface Availability</b>	<input type="text" value="80.00"/>
<b>Discard Threshold</b>	<input type="text" value="3.00"/>	<b>Error Threshold</b>	<input type="text" value="3.00"/>
<b>SNMP ResponseTime</b>	<input type="text" value="500.00"/>		

- 4 Select an existing SLA that you want to change.
- 5 Modify the values in the editable boxes below.
- 6 Click **Apply** to save changes, then click **OK** to save the changes and close the form.

# Change MPLS VPN Customer and SLA

This change form allows you to modify the customer and SLA assigned to a VPN. Before using this form, you must create customer entries. Create customer entries by using the batch-mode property import that comes with Common Property Tables or the “create new” forms that come with Common Property Tables.

SLAs are created by using the batch-mode property import that comes with the MPLS VPN Report Pack or by using the Create SLA Configuration Details form. Follow these steps to open the form and update the assigned customer and SLA name:

- 1 In the Management Console, click the **Objects** icon.
- 2 Select **View > Change View**.
- 3 Select **Mpls Vpn** model from the list.
- 4 Navigate to the MPLS VPN and select a VPN you want to update.
- 5 In the list of Object Specific Tasks, double-click **Update VPN Customer and SLA**.

## MPLS VPN

### Change MPLS VPN Customer and SLA



This form allows to assign new customer, SLA and even textual name settings ofr each known VPN.

Vpn Name	Customer Name	SLA Name
Blue	Customer Unassigned	SLA_Default
Dash-Blue	Customer Unassigned	SLA_Default
Gold	Customer Unassigned	SLA_Default
Red_	Customer Unassigned	SLA_Default
brown-	Customer Unassigned	SLA_Default

Customer Name

SLA Name

OK

Apply

- 6 Select the VPN you want to change.
- 7 Change the customer name or the SLA name using the drop-down selection boxes.
- 8 Click **Apply**, then click **OK** to save the changes and close the form.

## Change a VPN Name

Every time a group of VRFs is discovered, a meaningful name is assigned to the group. Name assignment take place according to these rules:

- If the VRF group matches a group stored in the database and a non-default name is already available, continue to use that name. A discovered VRF group matches a stored VRF group when it appears that one or more VRFs exist in both sets.
- If the VRF group has a default name, examine the individual VRF names for each VRF in the group:
  - If each VRF in the list has the same name AND that name IS NOT in use already as a VPN name, assign that text string as the VPN name of this VRF group.
  - If each VRF in the list has the same name AND that name IS in use already as a VPN name, assign that text string as the VPN name and append the VPN Internal ID number to the end of the string, separated by an underscore ( \_ ).
- Examine each VRF name in the VRF group. If the first characters of each name match, use the maximum number of initial matching characters as the VPN name, provided that the length of this subset is greater than 3 characters and this name is not in use already.

If you decide to change a system-assigned VPN name, use the Change MPLS VPN Name form. Follow these steps to open the form:

- 1 In the Management Console, click the **Objects** icon.
- 2 Select **View > Change View**.
- 3 Select **Mpls Vpn** model from the list.
- 4 Navigate to the MPLS VPN and select a VPN you want to update.
- 5 In the list of Object Specific Tasks, double-click **Change MPLS VPN Name**.

# MPLS VPN

## Change MPLS VPN Name



This form allows to assign a new name to the VPN. Select a VPN on the left, verify the associated VRF list and then change the name using the input field below.

VPN List	Vrf List for Selected VPN	
	Vrf Name	Device
Blue	Blue	mplspe01.cnd.hp.com
Dash-Blue		
Gold	Blue	mplspe04.cnd.hp.com
Red_	Blue	mplspe03.cnd.hp.com
brown-		

VPN Name

OK

Apply

- 6 Select a VPN, then type the new VPN name in the editable box.
- 7 Click **Apply**, then click **OK** to save the changes and close the form.

## Update VPN VRF SLA Settings

SLAs must be created for the first time by using the property import file described in Appendix A or by using the Create SLA Configuration Details form. Follow these steps to open the update form and assign new SLA settings to the VRF:

- 1 In the Management Console, click the **Objects** icon.
- 2 Navigate to the device you want to update and select a specific VRF. (If you want to view all of the VRFs on a device, navigate to the device and select it.)

- 3 In the list of Object Specific Tasks, double-click **Update VPN VRF SLA Settings**.

**MPLS VPN**

**Update VPN VRF SLA Settings**

This form allows to assign new Service Level Agreement (SLA) settings to individual VRFs. The SLA setting will 'trickle down' from the parent VPN if you do not explicitly set a different one at the VRF level. Select one or more rows, make the change then press 'Apply'.

Vpn Name	Vrf Name	Device	SLA
Blue	Blue	mplspe01.cnd.hp.com	SLA_Default
Blue	Blue	mplspe04.cnd.hp.com	SLA_Default
Blue	Blue	mplspe03.cnd.hp.com	SLA_Default
Gold	Gold	mplspe01.cnd.hp.com	SLA_Default
Gold	Gold	mplspe03.cnd.hp.com	SLA_Default

SLA Name:

OK Apply Cancel

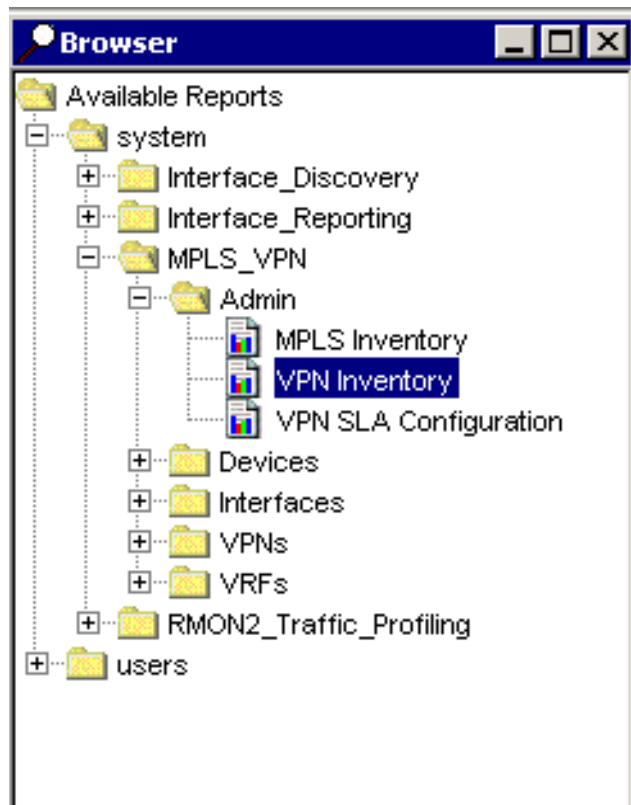
- 4 Assign a new SLA VPN VRF using the **SLA Name** drop-down selection list.
- 5 Click **Apply**, then click **OK** to save the changes and close the form.





## 5 VPN Inventory

The VPN Inventory report functions as a catalog of VPNs as reported by network devices. Use this report to find out which devices and interfaces are being used within a VPN and to see the VPN-specific configuration settings deployed at that time. This report does not contain graphs or analysis of historical performance.



The VPN Inventory report is inside the Admin folder. The other reports in this folder focus on customer-oriented inventory lists, MPLS-enabled interfaces, and VPN SLA settings.

Since the VPN Inventory report is updated once per poll cycle, you can go to this report to find the latest information. Newly discovered VPNs will be noted and representations created in the MPLS VPN Report Pack database tables.

The selection table on the left provides a list of every known VPN. If the VPN has been provisioned with a customer and an SLA setting, that information will show as well. Select a VPN to display a list of VRFs that make up the VPN. In the table on the right you will see the number of associated interfaces, the number of active interfaces, and the SLA setting for each VRF. Select a VRF to display the settings for that VRF and a list of interfaces associated with that VRF.

You can reduce the scope of this report by applying the following constraints:

- VPN
- Customer Name
- Customer ID

# MPLS VPN Reporting

## VPN Inventory

Select a VPN name on the left and see the component VRFs and the devices they exist on. Each VRF is accompanied by detailed configuration information, displayed in the middle of the report, and a list of all associated interfaces for the

VPN List				Component VRF/Devices Ordered by Host Device			
Name	Customer	Customer Id	SLA	Location	Host Device	Assoc if.	Active if.
vpn1	Customer 1	1	Gold				
vpn3	Customer 2	2	Silver	Location Unassigned	mimic1	2	2
vpn4	Customer 3	3	Bronze	Location Unassigned	mimic10	2	2
vpn5	Customer 4	4	Iron	Location Unassigned	mimic11	2	2
vpn6	Customer 5	5	Tin	Location Unassigned	mimic12	2	2
vpn7	Customer 6	6	Plastic	Location Unassigned	mimic13	2	2
				Location Unassigned	mimic14	2	2
				Location Unassigned	mimic15	2	2
				Location Unassigned	mimic16	2	2
				Location Unassigned	mimic17	2	2
				Location Unassigned	mimic18	2	2
				Location Unassigned	mimic19	2	2
				Location Unassigned	mimic2	2	2
				Location Unassigned	mimic20	2	2
				Location Unassigned	mimic3	2	2
				Location Unassigned	mimic4	2	2
				Location Unassigned	mimic5	2	2
				Location Unassigned	mimic6	2	2

### Current VRF Settings at Last Poll - (mimic1: 0)

Description	OperStatus	# Routes	HighRouteThreshold	MidRouteThreshold	Ro
VPN 1 Description	Up	6	4,294,967,295	4,294,967,295	

### Associated Interfaces for mimic1: 0

Interface	Full/Half	ifType	Admin Status	Protocol	Speed
5.0	F	1	Up	other	In: 1.0 Mb/s Out: 1.0 Mb/s

## 6 Route Activity

The VPN Route Activity Report is in the Devices folder. This report is designed for network operations staff responsible for monitoring route change activity.

This report includes a selection table, a route activity table, a VRF route activity table, and a VRF route activity graph. Tables and graphs are described below.

Table or Graph	Function
Selection table	<ul style="list-style-type: none"><li>• Every device that supports a VPN</li><li>• Customer and location (attributes provisioned by the user)</li><li>• Active VRFs and Connected Interfaces (attributes sourced from the network)</li><li>• <b>Max Routes</b> = aggregate of the maximum routes for all VRFs on the device</li><li>• <b># Routes</b> = aggregate of actual routes for all VRFs on the device</li></ul>
Route activity table	<ul style="list-style-type: none"><li>• Configured VRFs (maximum # during the time period)</li><li>• Active VRFs (maximum # during the time period)</li><li>• Shows changes in number of routes</li><li>• Allow you to compare routing changes to total volume placed on the backbone by this VRF</li></ul>
VRF route activity table	<ul style="list-style-type: none"><li>• Actual number of routes per VRF</li><li>• Maximum number of routes allowed per VRF</li></ul>
VRF route activity graph	<ul style="list-style-type: none"><li>• Tracks maximum route count over time</li><li>• Tracks minimum route count over time</li><li>• Tracks average route count</li><li>• <b>Hourly</b> = previous 50 hours</li><li>• <b>Daily</b> = previous 50 days</li></ul>

# MPLS VPN Reporting

## Recent VPN Device Route Activity



Select a device from the list to see related VRF Route information. Angled brackets around any metric signify that it changed values during the most recently summarized hour - the value displayed is an average for the hour. An X to the left of a row signifies that no hourly data is available within the previous 2 hours. Note that Max Routes is an aggregate of the max allowable routes for each VRF on the device.

### Devices Supporting VPNs Sorted by Current Number of Routes

Device	Cust Id	Customer	Cnfgd Vrfs	Active Vrfs	Cnctd Int	Max Routes	# Routes
192.168.0.3	8	Backbone	< 6 >	< 5 >	< 6 >		92

System Contact

System Name

System Location

System Descr

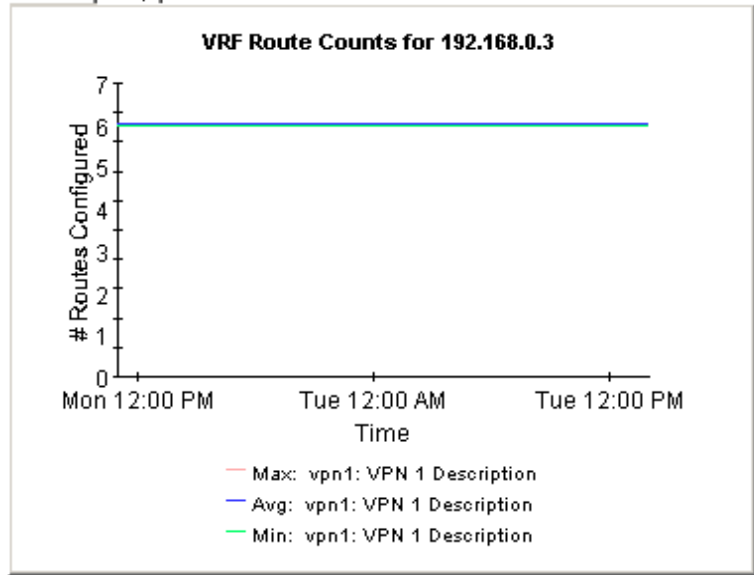
Hourly | Daily

Time Period	Max VRF Routes	# Routes	Volume Out	Cnfgd Vrfs	Active Vrfs
Tue Sep 17 02:00 PM		92	0 bytes	6	5
Tue Sep 17 01:00 PM		92	0 bytes	5	5
Tue Sep 17 12:00 PM		92	0 bytes	5	5
Tue Sep 17 11:00 AM		92	0 bytes	5	5
Tue Sep 17 10:00 AM		92	0 bytes	5	5
Mon Sep 16 08:00 PM		92	0 bytes	5	5
Mon Sep 16 07:00 PM		92	0 bytes	5	5
Mon Sep 16 06:00 PM		92	0 bytes	5	5
Mon Sep 16 05:00 PM		92	0 bytes	5	5
Mon Sep 16 04:00 PM		92	0 bytes	5	5

### VRF Route Activity

Vrf Name	# Routes	Max Allowable
vpn1	6	
vpn3	86	
vpn4	0	
vpn5	0	
vpn6	0	
vpn7	0	

Hourly | Daily

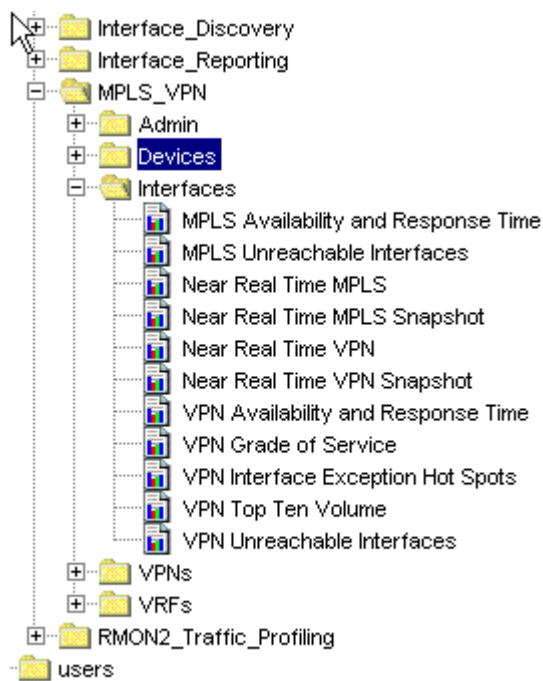




# 7 Unreachable VPN Interfaces

The reports in the Interfaces folder focus on MPLS-enabled and VPN-associated interfaces. While similar to the interface-specific reports in the Interface Reporting Report Pack, these reports offer additional MPLS or VPN related attributes on a per-interface basis.

The MPLS Unreachable Interfaces report contains a list of interfaces that have not been polled within the previous 35 minutes. Use this report to troubleshoot faulty devices and network connections.



You can reduce the scope of this report by applying the following constraints:

- Device: device name or IP address
- Interface: unique identifier for the interface
- Protocol: name of protocol (enumeration of ifType)
- Customer: name of customer associated with the interface. An interface will inherit the customer details of the parent device if none are explicitly specified.
- Location: name of the location associated with the interface. An interface will inherit the location details of the parent device if none are explicitly specified.
- Full or Half: duplex configuration of the interface - full duplex (2) or half duplex (1).
- MinutesSincePoll: number of minutes since the beginning of the last completed poll cycle.

By default, the system will poll on a 15 minute cycle. The default value for *MinutesSincePoll* is 35 minutes. This value for the default accommodates interfaces that missed one poll cycle. If you increase the value for *MinutesSincePoll*, only the interfaces that have been out of reach for the duration you indicate will display in the report.

# MPLS VPN Reporting

## Unreachable MPLS Enabled Interfaces



The Unreachable MPLS Associated Interfaces report lists the time since the last successful poll for interfaces for which data had been received recently but not within the previous 35 minutes. To change the limit from 35 minutes simply change the run time parameter value.

### MPLS Enabled Interfaces Previously Active Interfaces Which may now be Unreachable

Device	Interface	ifAdminStatus	location_name	F/H	Protocol	Speed	Min. Sinc Poll
12.168.0.3	Ethernet1/2	Up	Location Unassigned	F	other	In: 1.0 Mb/s Out: 1.0 Mb/s	22
12.168.0.3	Ethernet1/3	Up	Location Unassigned	F	other	In: 10.0 Mb/s Out: 10.0 Mb/s	22



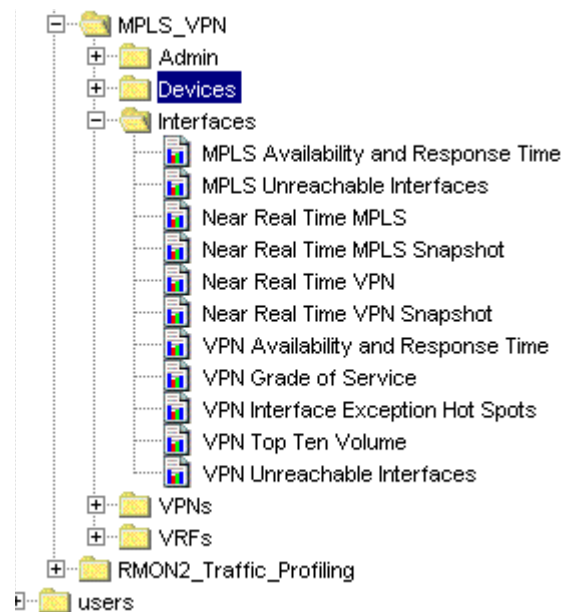
## 8 VPN Interface Exception Hot Spots

The VPN Interface Exception Hot Spots lets you spot interfaces with high exception counts. The report provides a list of all the VPN-associated interfaces that breached one or more of the following thresholds:

- Threshold for percent of packets discarded
- Threshold for percent of packets with errors
- Threshold for excessive utilization

The selection table shows data from yesterday and ranks interfaces by number of exceptions, highest to lowest. The graphs below the selection table allow you to investigate discards, errors, and utilization in much more details. Selecting an interface populates the following graphs:

- Hourly exception count
- Daily exception count
- Monthly exception count
- Utilization (throughout yesterday)
- Errors (throughout yesterday)
- Discards (throughout yesterday)
- Utilization (inbound/outbound/both)
- Errors (inbound/outbound/both)
- Discards (inbound/outbound/both)



You can reduce the scope of this report by applying the following constraints:

- Device - The device name or IP address
- Interface - The unique identifier for the interface
- Protocol - The protocol name (enumeration of ifType)
- Customer - The customer name associated with the interface.
- Location - The location name associated with the interface.
- Full or Half - The duplex configuration of the interface - full duplex (2) or half duplex (1).

# MPLS VPN Reporting

## VPN Interface Exception Hot Spots



This report has one entry for each monitored VPN associated interface on the network which experienced threshold exceptions yesterday. An exception occurs when inbound or outbound utilization, % discard rate or % error rate exceeds the threshold set for that interface. F/H = Full or Half Duplex. U = Utilization, D = Discards, E = Error.

### VPN Associated Interfaces with Exceptions Yesterday Sorted by Exception Count

Device	Interface	TextVrfName	Customer	F/H	Speed	Total Exceptions	Thresholds %
192.168.0.3	Ethernet1/3	vpn4	Customer 4	F	In: 10.0 Mb/s Out: 10.0 Mb/s	In:0 Out:29	U:90 D:1 E:1
192.168.0.3	Ethernet1/1	vpn3	Customer 3	F	In: 1.0 Mb/s Out: 1.0 Mb/s	In:11 Out:0	U:90 D:1 E:1
192.168.0.3	Ethernet1/2	vpn1	Customer 1	F	In: 1.0 Mb/s Out: 1.0 Mb/s	In:2 Out:0	U:90 D:1 E:1

#### Interface Details

Ethernet1/3

#### Edge Type

Provider

#### Protocol

other

#### Group

Unknown Group

#### Location

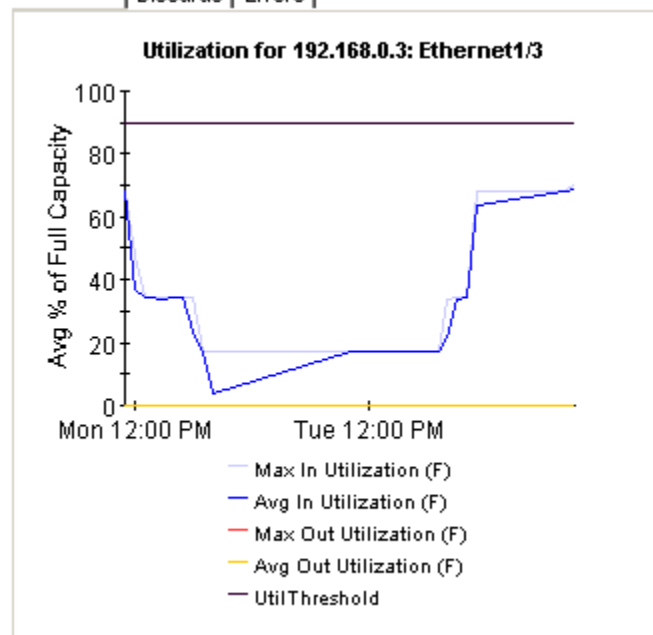
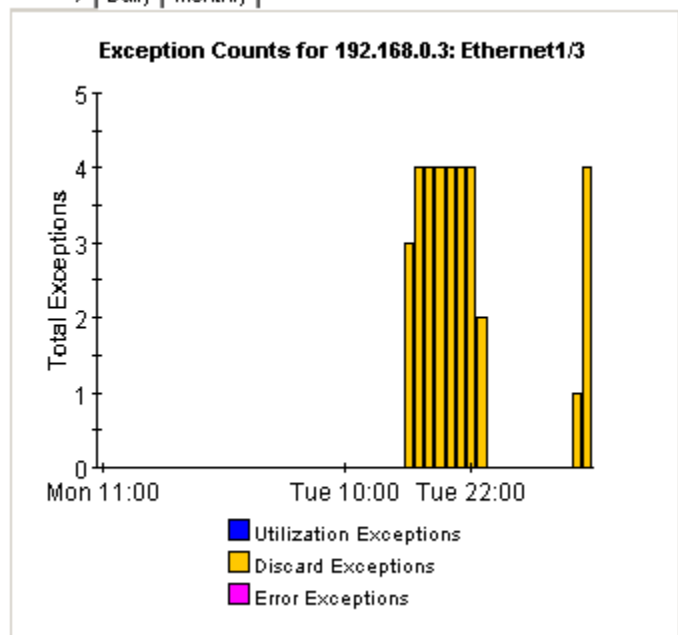
Belfast, NI

#### Country

Unknown Country

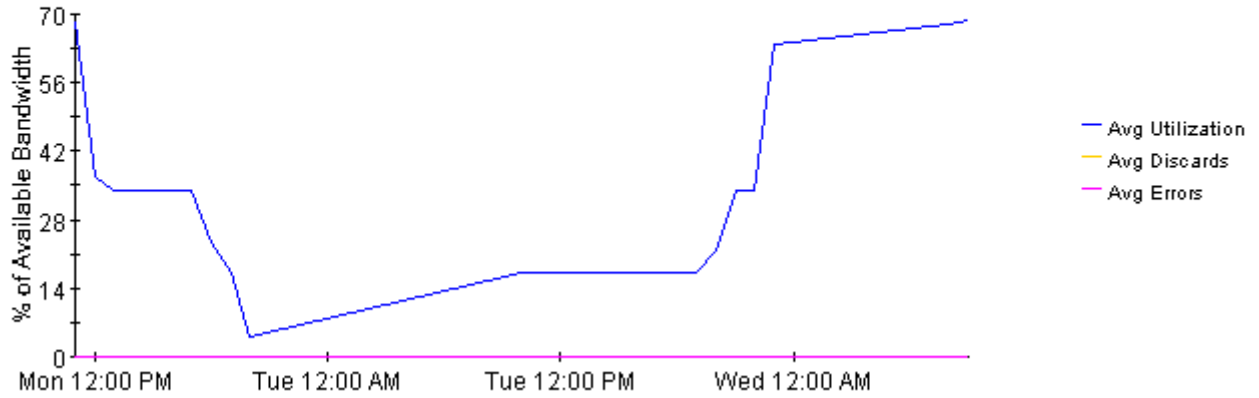
Hourly | Daily | Monthly

Utilization | Discards | Errors



Inbound | Outbound | Both (Half Duplex Only)

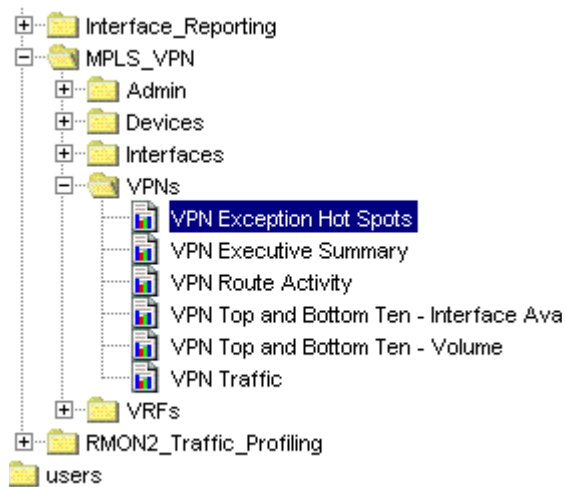
**Average Inbound Utilization, Discards and Errors for 192.168.0.3: Ethernet1/3**  
% of Available Bandwidth





## 9 VPN Traffic Volume

The reports in the VPNs folder focus on the entire VPN. All VRFs with the same VPN name are considered part of a single VPN, and it is their *aggregated* statistics that are presented here. Since all data in each report is aggregated data, the reports in this folder may be more suitable for managers than staff responsible for network operations.



The VPN Traffic Volume report ranks VPNS by traffic volume. If you select a VPN, you can see statistics for hourly traffic volume and daily traffic volume, and you can also inspect traffic volume on a per-VRF basis. At the VRF level, you can see how the traffic volume has changed on an hourly and daily basis.

The **VRF Oper%** column in the selection table shows the average operational percentage of all the component VRFs within the VPN. A VRF is considered operational if one or more of the interfaces associated with it are operationally up. This is regardless of the total number of interfaces associated with it.

The selection table also shows the number of utilization, discard, and error exceptions generated at the interface level, in response to thresholds configured at the interface level. The exception count in this table is an aggregate figure representing all the interfaces associated with the VPN.

You can reduce the scope of this report by applying the following constraints:

- Device - device name or IP address.
- Customer\_Name - customer name associated with the VPN.

▶ All interfaces associated with a VPN will inherit the customer details of the parent, if not explicitly specified as something else.

- Cust\_ID - numeric identifier for this customer.
- VPN - textual name for this VPN.

# MPLS VPN Reporting

## VPN Traffic Volume

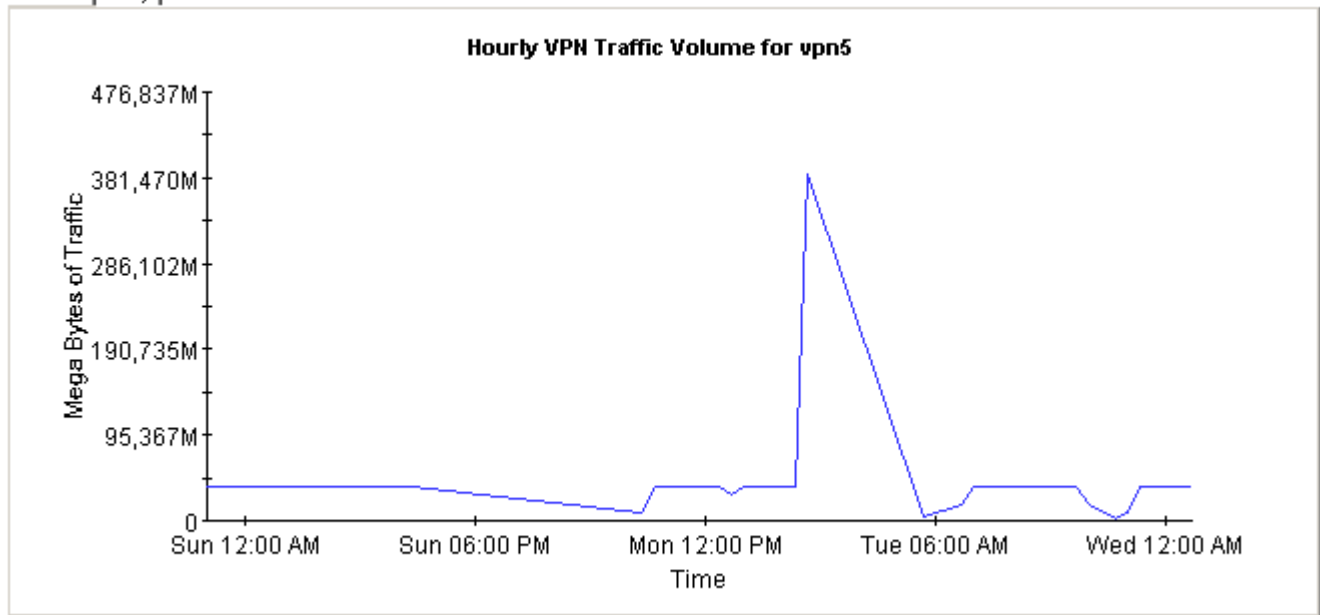


This report displays total traffic counts across a VPN. Only outgoing traffic from PE side devices are included in the VPN total. VRF Oper % represents the combined percentage availability for yesterday for all VRFs associated with the VPN. Exception counts are separated into Utilization, Discard and Error groups.

### VPNs With Traffic Yesterday

Vpn Name	Customer	Associated Int	Active if.	VRF Oper %	Volume	Exceptions
vpn5	Customer Unassigned	199	199	0.000	814.2 GB	U:0 D: E:
vpn1	Customer Unassigned	398	398	100.000	485.5 GB	U:9256 D:35342 E:0
vpn4	Customer Unassigned	199	0	100.000	294.2 GB	U:9256 D:17671 E:0
vpn6	Customer Unassigned	199	199	100.000	294.2 GB	U:0 D: E:
vpn7	Customer Unassigned	398	199	100.000	220.7 GB	U:0 D: E:
vpn3	Customer Unassigned	1,990	1,393	0.000	2.9 GB	U:17671 D:0 E:0

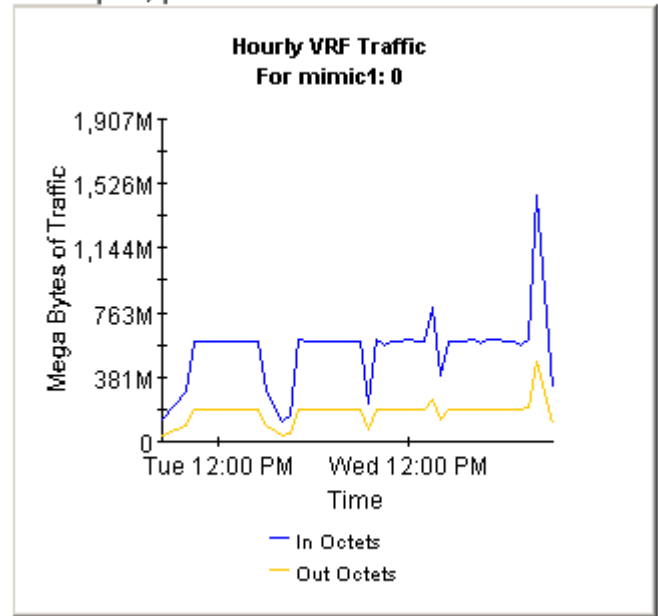
Hourly | Daily



**VRF Volume**

Device	Description	In	Out
mimic1	VPN 5 Description	13.1 GB	4.2 GB
mimic2	VPN 5 Description	13.1 GB	4.2 GB
mimic3	VPN 5 Description	13.1 GB	4.2 GB
mimic4	VPN 5 Description	13.1 GB	4.2 GB
mimic5	VPN 5 Description	13.1 GB	4.2 GB
mimic6	VPN 5 Description	13.1 GB	4.2 GB
mimic7	VPN 5 Description	13.1 GB	4.2 GB
mimic8	VPN 5 Description	13.1 GB	4.2 GB
mimic9	VPN 5 Description	13.1 GB	4.2 GB
mimic10	VPN 5 Description	13.1 GB	4.2 GB
mimic11	VPN 5 Description	13.1 GB	4.2 GB
mimic12	VPN 5 Description	13.1 GB	4.2 GB
mimic13	VPN 5 Description	13.1 GB	4.2 GB
mimic14	VPN 5 Description	13.1 GB	4.2 GB
mimic15	VPN 5 Description	13.1 GB	4.2 GB
mimic16	VPN 5 Description	13.1 GB	4.2 GB
mimic17	VPN 5 Description	13.1 GB	4.2 GB
mimic18	VPN 5 Description	13.1 GB	4.2 GB

Hourly | Daily







---

# 10 Current VRF Operational Status

The Current VRF Operational Status report displays the operational status of all known VRFs. Each metric is updated after every poll cycle. A VRF is considered operational if one or more of the interfaces associated with it is currently operationally up.

The Current OperStatus report is one of four reports in the VRFs folder. The reports in this folder focus on individual VRFs. A VRF is an instance of a VPN on a device. All VRFs with the same VPN name are considered part of a single VPN. Due to the real time nature of this report, it is suitable for use by network operations staff.

You can reduce the scope of this report by applying the following constraints:

- Device - device name or IP address.
- VPN Name - textual name for this VPN.
- SLA Name - textual Service Level Agreement name for this VRF.

# MPLS VPN Reporting

## Current VRF Operational Status



This report presents the operational status of each VRF at the time of the last successful poll. The VRF OperStatus is based on the mplsVpnVrfOperationalStatus MIB variable. A VRF is 'up' (1) when at least one interface associated with the VRF has an ifOperStatus of 'up' (1). A VRF is 'Down' (2) if there are no interfaces associated with it, or none of the associated interfaces have an ifOperStatus of 'up' (1). The report does not include those VPN VRFs which are currently unreachable but may be operationally down.

### Current VRF Operational Status As of Last Poll Cycle

Host Device	Name	Description	OperStatus	Active if.	SLA Name
Internet_Device	atime	Unknown	Down	0	SLA_Default
192.168.0.3	vpn5	VPN 5 Description	Down	1	SLA_Default
	mimic1	VPN 5 Description	Down	1	SLA_Default
	mimic2	VPN 5 Description	Down	1	SLA_Default
	mimic3	VPN 5 Description	Down	1	SLA_Default
192.168.0.3	vpn3	VPN 3 Description	Unknown: 0	7	SLA_Default
	mimic1	VPN 3 Description	Unknown: 0	7	SLA_Default
	mimic2	VPN 3 Description	Unknown: 0	7	SLA_Default
	mimic3	VPN 3 Description	Unknown: 0	7	SLA_Default
192.168.0.3	vpn1	VPN 1 Description	Up	2	SLA_Default
	mimic1	VPN 1 Description	Up	2	SLA_Default
	mimic2	VPN 1 Description	Up	2	SLA_Default
	mimic3	VPN 1 Description	Up	2	SLA_Default
192.168.0.3	vpn4	VPN 4 Description	Up	0	SLA_Default
	mimic1	VPN 4 Description	Up	0	SLA_Default
	mimic2	VPN 4 Description	Up	0	SLA_Default
	mimic3	VPN 4 Description	Up	0	SLA_Default
192.168.0.3	vpn6	VPN 6 Description	Up	1	SLA_Default
	mimic1	VPN 6 Description	Up	1	SLA_Default
	mimic2	VPN 6 Description	Up	1	SLA_Default
	mimic3	VPN 6 Description	Up	1	SLA_Default
192.168.0.3	vpn7	VPN 7 Description	Up	1	SLA_Default
	mimic1	VPN 7 Description	Up	1	SLA_Default
	mimic2	VPN 7 Description	Up	1	SLA_Default
	mimic3	VPN 7 Description	Up	1	SLA_Default

# A Manual Provisioning

This appendix covers the following topics:

- Managed elements and their associated properties
- Provisioning interfaces
- Provisioning devices
- Provisioning VRFs
- Provisioning VPNs
- Provisioning SLAs

## Elements and Properties

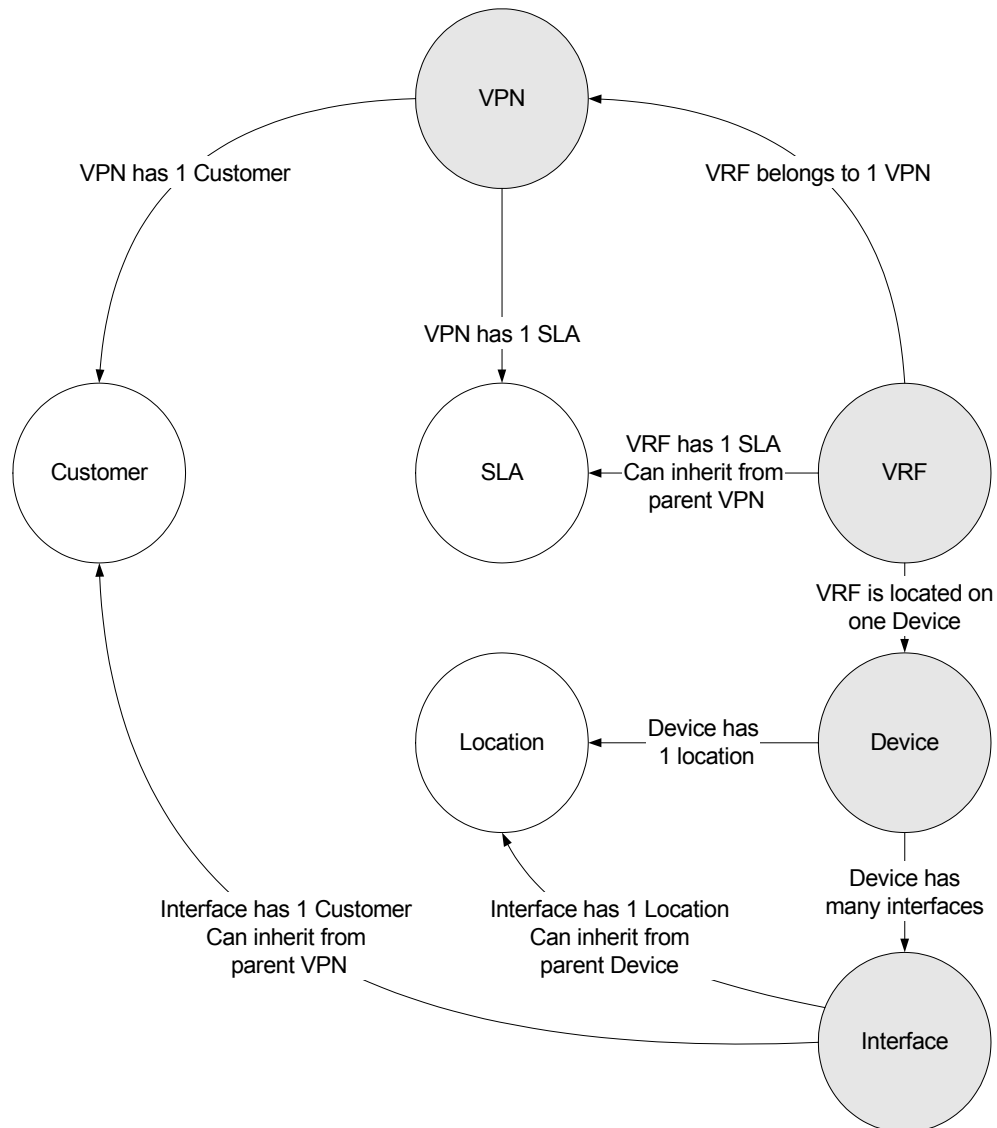
The MPLS VPN Report Pack represents the network as a collection of managed elements. The managed elements are:

- VPN
- VRF
- SLA
- Interface (MPLS-enabled or VPN-associated)
- Device

The following table shows the properties associated with each managed element.

<b>Managed Element</b>	<b>Associated Properties</b>
VPN	Customer Customer ID SLA
VRF	SLA
SLA	Operational% Interface availability Discard threshold
Interface	See <i>Interface Reporting Report Pack 4.6 User Guide</i>
Device	See <i>Common Property Tables 3.5 User Guide</i>

The following diagram shows the relationship between managed elements and their associated properties.



When an attribute can be sourced from the network, or inherited from an existing report pack, OVPI will provision the managed element automatically. When the attribute cannot be provisioned automatically, it must be provisioned manually. Managed elements introduced by the MPLS VPN Report Pack must be provisioned manually.

There are two ways to manually provision a managed element:

- Use one of the change forms that comes with the MPLS VPN Report Pack
- Create a property file and import the contents

If you choose to provision a managed element using a property import file, you have to create the property import file and store the file where OVPI expects to find it. There are several ways to create a property file:

- Create it yourself from scratch using a spreadsheet application
- Export the contents of the file from your own provisioning database
- Export existing property data from OVPI

Since exporting existing property data from OVPI produces a file with the proper format, we recommend using the third approach. If you create your own file, the sequence of attributes in your file must be correct and columns must be separated by tabs.

## Provisioning Interfaces

Interfaces are fundamental to the MPLS VPN Report Pack. Provisioning interfaces is handled through the Interface Reporting Report Pack. As explained in the user guide for Interface Reporting, you may import many attributes, including customer and location, on a per-interface basis.

Keep these guidelines in mind when provisioning interfaces:

- Unless you are concerned that the network will misrepresent certain interface metrics, such as ifSpeed, importing custom attributes on a per-interface basis is not necessary.
- If the device has customer and location assigned to it, the interfaces on this device will inherit customer and location from the device. You may change these attributes later.
- Information indicating whether an interface is MPLS-enabled or VPN-associated is sourced from the network; these attributes cannot be manually provisioned.
- When provisioning a VPN, which has associated VRFs which in turn have associated interfaces, each interface will inherit the customer assigned to the VPN.

## Provisioning Devices

Each interface in the network is physically attached to a device. The device can be referenced by name or by IP address. Since each VRF exists only on a single device, there is a relationship between VRF properties and device properties.

Property data for devices is created and maintained using the import/export utility that comes with Common Property Tables. For more information about assigning property information to devices, refer to the *Common Property Tables 3.5 User Guide*.

## Provisioning VRFs

Every VRF has a relationship with:

- The VPN to which it belongs
- The device on which it exists
- The SLA setting to which it should adhere

Since the relationship with the VPN and the relationship with the device are maintained using data sourced from the network, there is no need to create or modify these custom attributes. The SLA setting, however, is configurable by the user.

SLA values can be associated with a VRF in one of two ways:

- The parent VPN is assigned an SLA setting, in which case all related VRFs will be allocated the same SLA.

- The user explicitly imports a specific SLA for one or more VRFs.

If the parent VPN is assigned an SLA setting, then all related VRFs will be allocated the same SLA. Follow these steps to import a specific SLA for one or more VRFs:

- Create a property file
- Name the file VRF\_Property.dat
- Call the import mechanism for VRFs

The following table describes the format of the file.

Attribute	Type	Default	Comments
VPN Name	char_string,64	required field	The textual name of the VPN to which the VRF belongs.
Device Name	char_string,64	required field	The unique reference for this device, either IP address or host name.
VRF Name	char_string,64	required field	The name of the VRF to which other property values have to be updated.
SLA Name	char_string,64	required field	The unique reference for the SLA associated with the VRF.

## File Import and Export

There are two ways to import the file:

- Navigate to OVPI/data/PropertyData/MPLS\_VPN and type:  
**trend\_proc -f VRF\_importdata.pro**
- Execute the perl script by the same name in the same directory.

There are two ways to export the file from OVPI:

- Navigate to OVPI/data/PropertyData/MPLS\_VPN and type:  
**trend\_proc -f VRF\_exportdata.pro**
- Execute the perl script by the same name in the same directory.

After your file is imported, OVPI will store the file in this directory:

OVPI/data/PropertyData/Archive

## Notes

- 1 Reference to an SLA that does not yet exist will create a new SLA with defaulted values. To avoid this situation, you should create any required SLAs, with correct threshold values, ahead of time using the SLA import/export procedure.
- 2 Importing the VRF property file logs messages to the Configuration and Logging Report. This report is located in the Admin folder of Interface Reporting.

# Provisioning VPNs

Every VPN has an external relationship with:

- The customer to which it belongs
- The SLA configuration to which it should adhere

VPN names will always be created using network sourced values, however in this case the customer and SLA settings will be defaulted. Follow these steps to assign a customer and/or SLA to a VPN, or provision new, not yet monitored VPNs:

- Create a property import file
- Name the file VPN\_Property.dat
- Call the import mechanism for VPNs

The following table describes the format of the file.

Attribute	Type	Default	Comments
VPN Name	char_string,64	required field	The textual name of the VPN to which the VRF belongs.
Customer ID	integer	-2	The unique reference for the customer associated with this VPN.
Customer Name	char_string,64	“customer unassigned”	The textual name for the customer associated with this VPN.
SLA Name	char_string,64	required field	The unique reference for the SLA associated with the VRF.

## File Import and Export

There are two ways to import the file:

- Navigate to OVPI/data/PropertyData/MPLS\_VPN and type:  
**trend\_proc -f VPN\_importdata.pro**
- Execute the perl script by the same name in the same directory.

There are two ways to export the file from OVPI:

- Navigate to OVPI/data/PropertyData/MPLS\_VPN and type:  
**trend\_proc -f VPN\_exportdata.pro**
- Execute the perl script by the same name in the same directory.

After your file is imported, OVPI will store the file in this directory:

OVPI/data/PropertyData/Archive

## Notes

- 1 Although the customer attribute is stored and managed by Common Property Tables, references to a customer ID or customer name in this file are handled as follows:

- If the customer ID matches an existing customer ID, then the reference will be honoured and the customer name supplied in the file will be ignored.
  - If the customer ID does not match any customer ID in the customer tables, then a new customer with the basic properties of name and ID will be created.
- 2 If a new customer is created, other customer properties will be defaulted. Although this approach to creating new customers is valid, we recommend that you create customer entries ahead of time, using the import utility that comes with Common Property Tables.
  - 3 Reference to an SLA that does not exist yet will create a new SLA with defaulted values. To avoid this situation, create any required SLAs, with correct threshold values, ahead of time using the SLA import/export procedure.
  - 4 Importing the VPN property file logs messages to the Configuration and Logging Report. This report is located in the Admin folder of Interface Reporting.

## Provisioning SLAs

Each Service Level Agreement (SLA) has a name and five associated properties:

- Operational percentage
- Interface availability
- Discard threshold
- Error threshold
- SNMP response time

All VPNs and VRFs will be created with an SLA setting of *SLA\_Default* until you modify it to your own preferences. To create a new SLA you can:

- Reference a new SLA name in the VPN or VRF import file
- Import a set of SLAs using the SLA import procedure

If you reference a non-existing SLA in another import file, then a new SLA will be created with the specified name but with defaulted column values. Follow these steps to modify an existing SLA, or create a new SLA, using the import procedure:

- Create a property import file.
- Name the file: `SLAConfig_Property.dat`
- Call the import mechanism for SLAs.

The following table describes the format of the file.

Attribute	Type	Default	Comments
SLA Name	char_string,64	required field	The textual name of the SLA.
Operational%	integer	99	The percentage of time that, combined and averaged over the time period, the VRFs of the VPN must be operational.



Attribute	Type	Default	Comments
Interface Availability	integer	99	The percentage of time that, combined and averaged over the time period, the interfaces of the VPN or VRF must be available.
Discard Threshold	integer	1	The maximum percentage of traffic, when averaged over the time period, that may be discarded.
Error Threshold	integer	1	The maximum percentage of packets, when averaged over the time period, that may be errored.
SNMP Response Time	integer	200	The maximum SNMP response time allowed across all interfaces.

## File Import and Export

There are two ways to import the file:

- Navigate to `OVPI/data/PropertyData/MPLS_VPN` and type:  
**`trend_proc -f SLAConfig_mportdata.pro`**
- Execute the perl script by the same name in the same directory.

There are two ways to export the file from OVPI:

- Navigate to `OVPI/data/PropertyData/MPLS_VPN` and type:  
**`trend_proc -f SLAConfig_exportdata.pro`**
- Execute the perl script by the same name in the same directory.

After your file is imported, OVPI will store the file in this directory:

`OVPI/data/PropertyData/Archive`

## Notes

- 1 Importing the SLA property file logs messages to the Configuration and Logging Report. This report is located in the Admin folder of Interface Reporting.



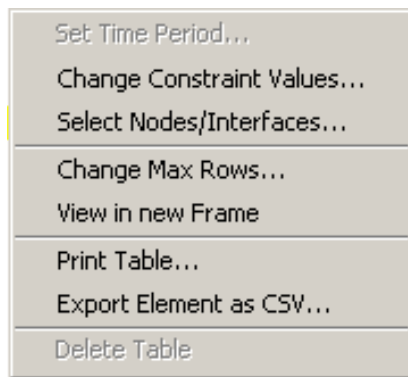
## B Editing Tables and Graphs

Any table or graph can be viewed in several ways. While the default view is usually adequate, you can easily change to a different view. If you are using Report Viewer, right-click the object to open a list of view options. If you are using the Web Access Server, follow these steps to change the default view of a table or graph:

- 1 Click **Preferences** on the links bar.
- 2 Expand **Reports** in the navigation frame.
- 3 Click **Viewing**.
- 4 Select the **Allow element editing** box.
- 5 Click **Apply**.
- 6 Click the Edit icon next to the table or graph.

### View Options for Tables

Right-clicking a table, or selecting the Edit Table icon if you are using the Web Access Server, opens a list of table view options.



Select **Set Time Period** to alter the relative time period (relative to now) or set an absolute time period. The Set Time Period window opens.

You may shorten the period of time covered by the table from, for example, 42 days to 30 days or to 7 days. If you are interested in a specific period of time that starts in the past and stops *before* yesterday, click **Use Absolute Time** and select a Start Time and an End Time.

Select **Change Constraint Values** to loosen or tighten a constraint, thereby raising or lowering the number of elements that conform to the constraint. The Change Constraint Values window opens. To loosen a constraint, set the value lower; to tighten a constraint, set the value higher.

The **Select Nodes/Interfaces** allows you to change the scope of the table by limiting the table to specific nodes, specific interfaces, or a specific group of nodes or interfaces. The Select Node Selection Type window opens.

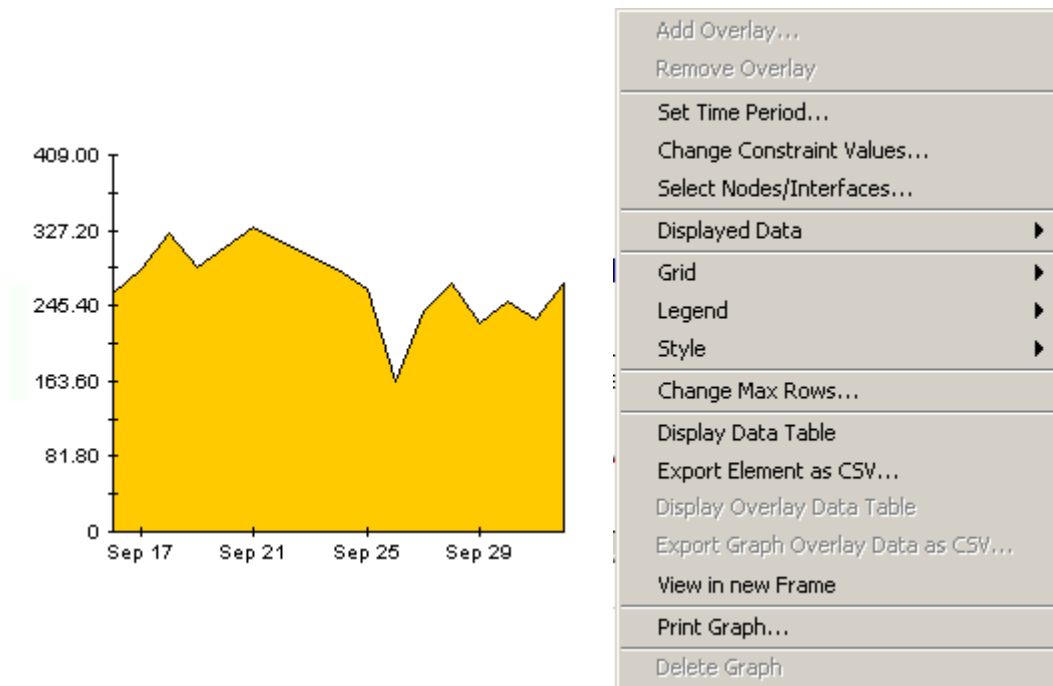
**Change Max Rows** increases or decreases the number of rows in a table. The default is 50. If you expand the default, the table may take more time to open. If you are trending a large network, using the default ensures that the table opens as quickly as possible.

**View in new Frame** opens the table in a Table Viewer window, shown below. If necessary, make the data in the table more legible by resizing the window.

Polled IP QoS Statistics Data - Input Over Previous 6 Hours					
Direction	IpPrecedence	Switched Bytes	Switched Pkts	Time Period	
Input	0	105,888	675	Tue Oct 29 07:00 AM	
Input	1	0	0	Tue Oct 29 07:00 AM	
Input	2	0	0	Tue Oct 29 07:00 AM	
Input	3	0	0	Tue Oct 29 07:00 AM	
Input	4	0	0	Tue Oct 29 07:00 AM	
Input	5	0	0	Tue Oct 29 07:00 AM	
Input	6	600	5	Tue Oct 29 07:00 AM	
Input	7	0	0	Tue Oct 29 07:00 AM	
Input	0	98,334	638	Tue Oct 29 06:45 AM	
Input	1	0	0	Tue Oct 29 06:45 AM	
Input	2	0	0	Tue Oct 29 06:45 AM	
Input	3	0	0	Tue Oct 29 06:45 AM	
Input	4	0	0	Tue Oct 29 06:45 AM	

## View Options for Graphs

Right-clicking a graph, or clicking the Edit Graph icon if you are using the Web Access Server, opens the following list of view options.

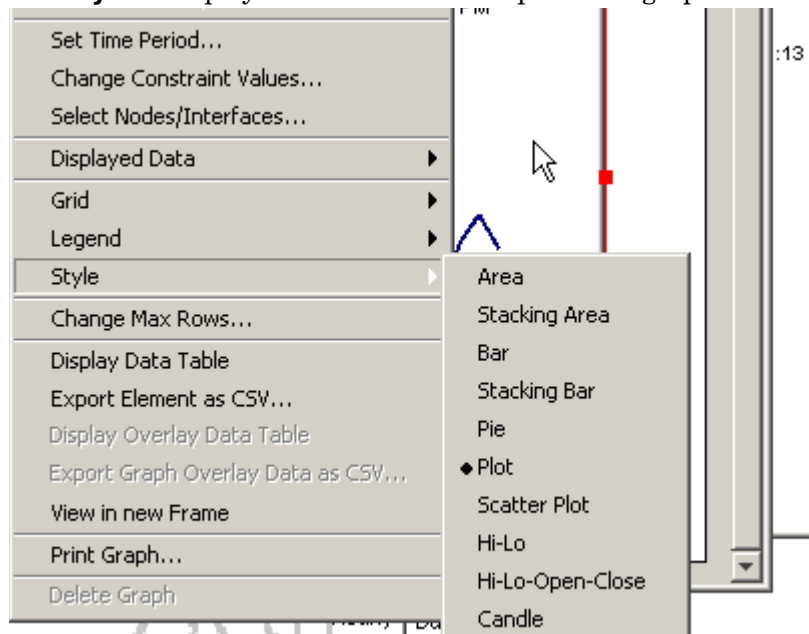


The following table provides details about each option.

Option	Function
Set Time Period	Same as the table option shown above.
Change Constraint Values	Same as the table option shown above.
Select Nodes/Interfaces	Same as the table option shown above.
Displayed Data	For every point on a graph, display data in a spreadsheet.
Grid	Add these to the graph: X axis grid lines Y axis grid lines X and Y axis grid lines
Legend	Delete or reposition the legend.
Style	See the illustrations below.
Change Max Rows...	Same as the table option shown above.
Display Data Table	See below.
Export Element as CSV...	Same as the table option shown above.
View in New Frame	Opens graph in a Graph Viewer window.
Print Graph	Same as the table option shown above.

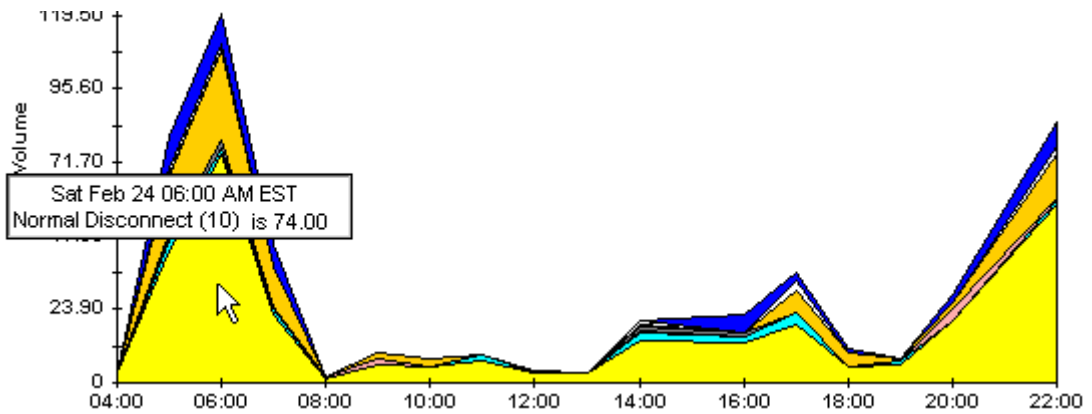
## Style Options

Select **Style** to display a list of seven view options for graphs.



## Style > Area

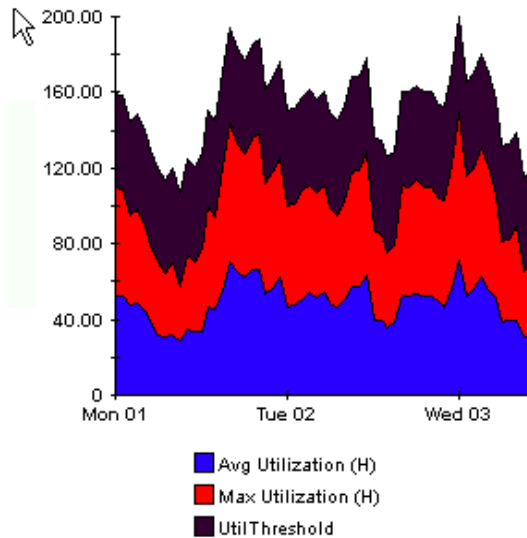
The plot or bar chart changes to an area graph. While relative values and total values are easy to view in this format, absolute values for smaller data types may be hard to see. Click anywhere within a band of color to display the exact value for that location



To shorten the time span of a graph, press SHIFT+ALT and use the left mouse button to highlight the time span you want to focus on. Release the mouse button to display the selected time span.

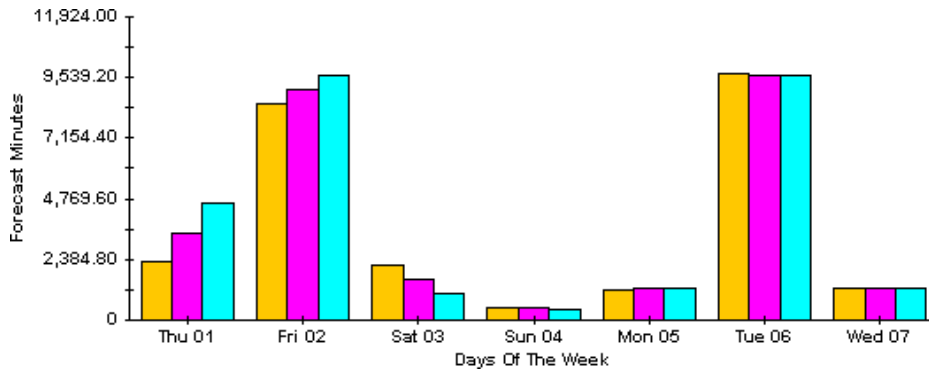
## Style > Stacking Area

The area or plot graph changes to a stacking area graph. This view is suitable for displaying a small number of variables.



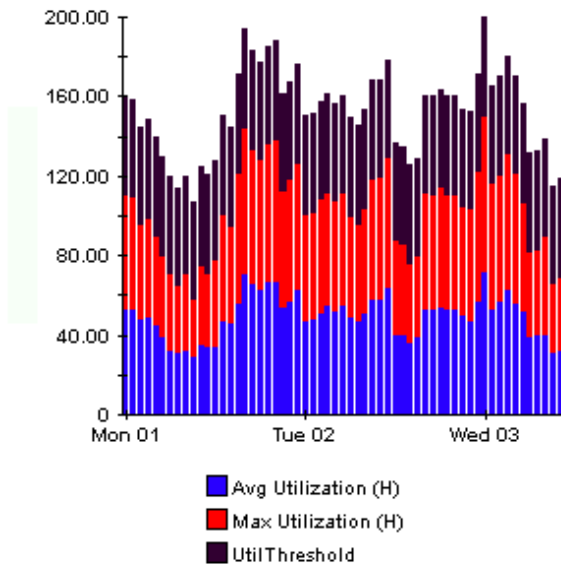
## Style > Bar

The graph changes to a bar chart. This view is suitable for displaying relatively equal values for a small number of variables. There are three variables in the graph below.



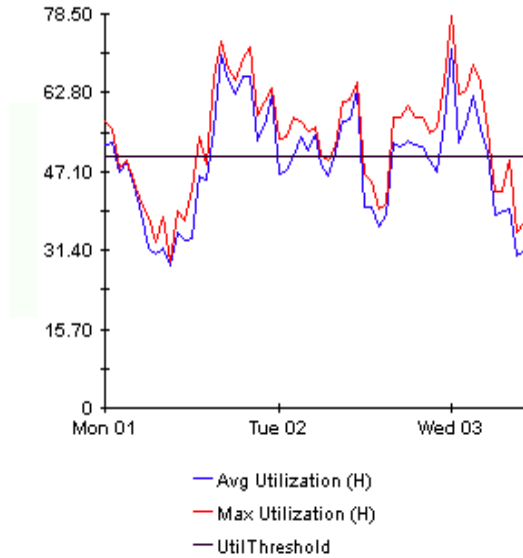
## Style > Stacking Bar

The plot or area graph changes to a stacking bar chart. If you increase the width of the frame, the time scale becomes hourly. If you increase the height of the frame, the call volume shows in units of ten.



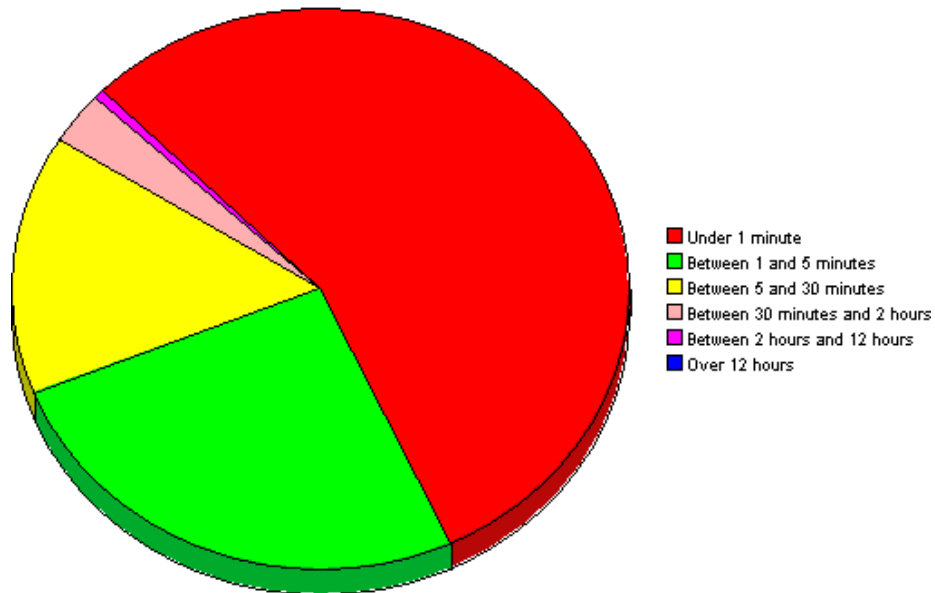
## Style > Plot

Bands of color in an area graph change to lines. If you adjust the frame width, you can make the data points align with hour; if you adjust the frame height, you can turn call volume into whole numbers.



## Style > Pie

An area graph becomes a pie chart. Bands in an area graph convert to slices of a pie and the pie constitutes a 24-hour period. This view is helpful when a small number of data values are represented and you are looking at data for one day.

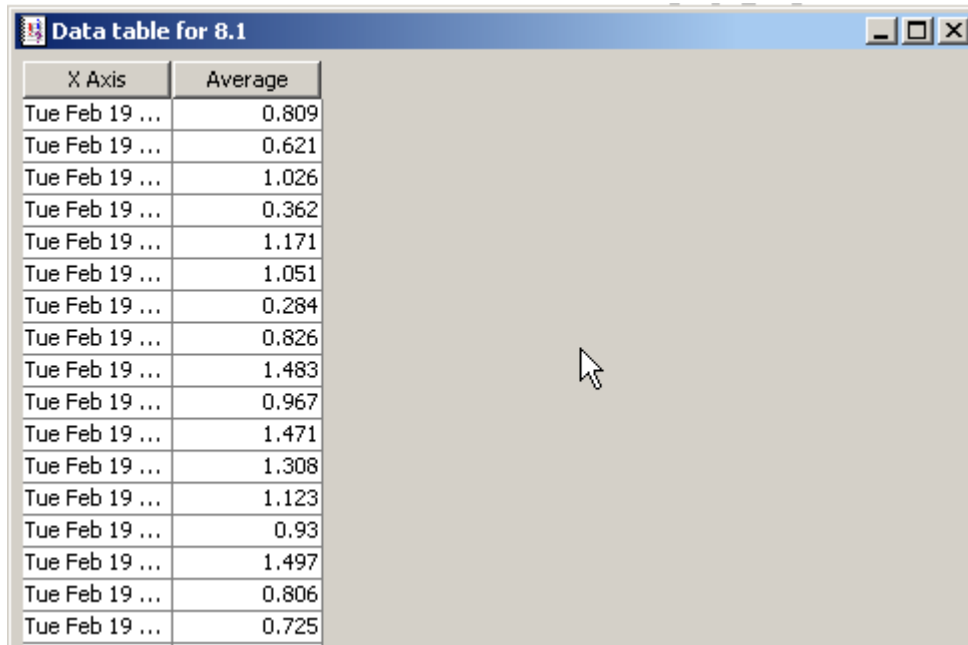


If you are looking at data for more than one day, you will see multiple pie graphs, one for each day.



## Display Data Table

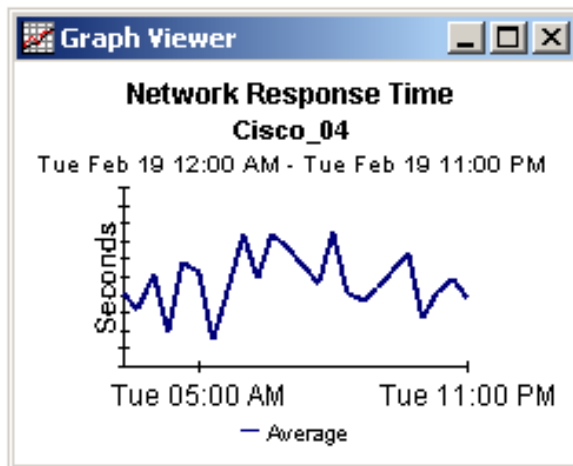
This option changes a graph into a spreadsheet.



X Axis	Average
Tue Feb 19 ...	0.809
Tue Feb 19 ...	0.621
Tue Feb 19 ...	1.026
Tue Feb 19 ...	0.362
Tue Feb 19 ...	1.171
Tue Feb 19 ...	1.051
Tue Feb 19 ...	0.284
Tue Feb 19 ...	0.826
Tue Feb 19 ...	1.483
Tue Feb 19 ...	0.967
Tue Feb 19 ...	1.471
Tue Feb 19 ...	1.308
Tue Feb 19 ...	1.123
Tue Feb 19 ...	0.93
Tue Feb 19 ...	1.497
Tue Feb 19 ...	0.806
Tue Feb 19 ...	0.725

## View in New Frame

The graph opens in a Graph Viewer window. Improve legibility by resizing the window.





---

# Glossary

## **active interfaces**

The number of interfaces associated with a VRF with an ifOperStatus of 'Up'.

## **associated interfaces**

The number of interfaces associated with a VRF irrespective of ifOperStatus.

## **availability**

The percentage of time an interface, or group of related interfaces, has been operational. Identifies outages as reported through the sysUpTime variable, the ifLastChange and ifOperStatus variables. Calculated by combining device sysUpTime with interface ifOperStatus and interface ifLastChange.

## **customer**

A textual name representing an external customer. It can be associated with Interfaces or VPNs and must be imported using the supplied provisioning tools.

## **customer ID**

A numerical identifier that is uniquely associated with a customer name.

## **device**

Any SNMP manageable device.

## **discard rate**

The percentage of packets discarded by the interface. Data about discards is sampled during each poll cycle (by default this is four times an hour); based on those samples, OVPI calculates an average and a maximum discard rate.

## **discard threshold**

The point at which an acceptable percentage of discarded traffic becomes an abnormal percentage and possibly impacts the user experience. If the interface is full duplex, the same threshold value is applied to both in and out packets separately.

## **error rate**

The percentage of packets with errors as reported by the interface. Data about errors is sampled during each poll cycle (by default this is four times an hour); based on those samples, OVPI calculates an average and a maximum error rate.

### **error threshold**

The point at which an acceptable percentage of errored traffic becomes an abnormal percentage and possibly impacts the user experience. If the interface is full duplex, the same threshold value is applied to both in and out packets separately.

### **exceptions**

The number of times a threshold has been broken for the selected object. For an interface, thresholds apply to Utilization, Errors and Discards. For aggregated groups of interfaces such as a VRF, the exception count refers to the total number of exceptions across all component interfaces.

### **interface**

An entry in the SNMP ifTable for of the Device. Can represent a physical or logical interface.

### **location**

A textual name representing a location. It can be associated with Interfaces or devices and must be imported using the supplied provisioning tools.

### **location ID**

A numerical identifier that is uniquely associated with a Location name.

### **MPLS**

Multi Protocol Label Switching protocol

### **response time**

Delay within the network management structure, specifically, delay between the poller and the target device. If the delay is being caused by the device, then this value may point to device resource issues.

### **# routes**

Indicates the number of routes associated with a VRF or device.

### **security violations**

The number of illegally received labels on this VPN/VRF.

### **SLA**

Service Level Agreement. The report package allows you to configure several metrics which can govern an SLA. These include the percentage of time the VPN components were operational and the SNMP response time to VPN components.

### **threshold**

The line between normal and abnormal performance. When this line is crossed, an exception is recorded. Every threshold has a default value that is easily changed to reflect individual needs. Thresholds are used extensively in this package for Utilization, Discard and Error ratios at the interface level and across the VRF or VPN.

### **utilization**

The total number of octets traversing the interface as a percentage of the total *possible* number of octets, using the ifSpeed property. If an interface is full duplex, utilization is calculated and displayed separately in each direction. Groups of interfaces have their utilization calculated by taking the total traffic on all administratively up interfaces in the group and dividing that by the total possible bandwidth for those interfaces. Utilization for a group of interfaces is more meaningful when all the interfaces in the group use the same protocol.

### **utilization threshold**

The point at which the number of octets traversing the interface is considered detrimental to the service level required by network users. In the case of full duplex interfaces, the same threshold value is applied to both in and out packets separately.

### **VPN**

Virtual private network.

### **VRF**

VPN route forwarding. A VRF represents an instance of a VPN supported by one or more PE routers. The collection of matching VRFs from all network devices compose the actual VPN.



# Index

## A

- active interfaces, defined, 67
- associated interfaces, defined, 67
- attributes, custom
  - See importing property data
- availability, 67

## C

- central servers, configuring, 23
- change max rows option, 61
- changing a VPN name, 29
- collection\_manager (command), 17
- Common Property Tables, 8
  - prerequisite, 15
  - upgrading, 16, 19
- configuring
  - central servers, 23
  - satellite servers, 24
- constraints, applying, 12
- Current VRF Operational Status report, 49
- customer, defined, 67
- customer ID, 67
- customer-specific reports, 12
- custom table views, 18

## D

- Datapipe Manager, 18
- demo package, 13
- demo package, installing, 19
- device
  - defined, 67
  - properties associated with, 51
  - provisioning, 53
- discard rate, 67
- discard threshold, 67
- Display Data Table, 61
- displayed data option, 61

- distributed systems, 16
  - configuring, 23

## E

- error rate, 67
- error threshold, 68
- exceptions, defined, 68
- exporting a polling group, 18
- exporting a polling policy, 17
- extracting packages from the report pack CD, 18

## F

- filters, group, 12
- forms
  - changing a VPN name, 29
  - changing MPLS VPN customer and SLA name, 28
  - changing MPLS VPN SLA configuration settings, 27
  - creating MPLS VPN SLA configurations, 25
  - updating property data, 25
  - updating VPN VRF SLA settings, 30
  - using, 12

## G

- grid options, 61
- group\_manager (command), 17
- group accounts, 12
- group filters, 12

## I

- importing property data, 12
- installing
  - demo package, 19
  - MPLS VPN, 19
  - post-installation steps, 20
  - prerequisite software, 15
  - prerequisite tasks, 18
  - verification utility, 20

- interface
  - defined, 68
  - properties associated with, 51
  - provisioning, 53
- Interface Discovery Datapipe, 8
- Interface Reporting ifEntry Datapipe, 8
- Interface Reporting Report Pack
  - prerequisite, 15
- IR\_Check\_Status.sql script, 20

## J

- Juniper MPLS VPN Datapipe 1.0, 9

## L

- legend options, 61
- location, defined, 68
- location ID, 68

## M

- managed elements, properties associated with, 51
- monitoring threshold breaches, 16
- MPLS\_DMF\_Process.pro file, 24
- MPLS\_Hourly\_Process.pro file, 23
- MPLS\_VPN\_Threshold, 16
- MPLS VPN and customer SLA name, changing, 28
- MPLS VPN SLA configurations
  - changing, 27
  - creating, 25

## N

- Near Real Time MPLS report, 10
- Network Node Manager, integration with, 16

## O

- OVPI Timer
  - starting, 20, 22
  - stopping, 18, 21

## P

- packages
  - extracting from RNS CD, 18
- parameters, editing, 12
- polling policies, 17
- post-installation steps, 20
- prerequisites for installation, 8, 15

- Product Manuals Search (web page), 14
- property data, updating, 12
- property data for VPNs, 13
- property data for VRFs, 13
- protocol, 68
- provisioning
  - devices, 53
  - interfaces, 53
  - SLAs, 56
  - VPNs, 55

## R

- Recent VPN Activity report, 9
- remote pollers, 17, 23
- reports
  - Current VRF Operational Status, 49
  - customizing, 11
  - described, 9
  - Near Real Time, 10
  - parameters, 12
  - property data displayed in, 12
  - Recent Activity, 9
  - Unreachable Interfaces, 39
  - view options, 21
  - VPN Interface Exception Hot Spots, 41
  - VPN Inventory, 33
  - VPN Route Activity, 35
  - VPN Traffic Volume, 45
- response time, 68
- routes, number of, 68

## S

- satellite servers, configuring, 24
- security violations, 68
- servers, configuring, 23, 24
- SLAs
  - defined, 68
  - properties associated with, 51
  - provisioning, 56
- software prerequisites, 15
- style options for graphs, 61
- system clocks, synchronizing, 24

## T

- threshold, defined, 68
- threshold breaches, 16
- Thresholds Module, 8



trendcopy, 23  
trendtimer, 23

## U

Unreachable Interfaces report, 39  
updating SLA settings for a VPN VRF, 30  
upgrading  
    Common Property Tables, 16, 19  
Use Absolute Time, 59  
utilization, defined, 69  
utilization threshold, 69

## V

verification utility, 20  
viewing reports, 21  
view in new frame, 60  
VPN Interface Exception Hot Spots report, 41  
VPN Inventory report, 9, 33  
VPN Route Activity report, 35  
VPNs  
    name change, 29  
    properties associated with, 51  
    provisioning, 55  
VPN SLA Configuration report, 9  
VPN Top Ten Volume report, 10  
VPN Traffic Volume report, 45  
VRFs  
    defined, 69  
    properties associated with, 51

