HP OpenView Performance Insight

MPLS VPN Report Pack User Guide

Software Version: 3.0

Reporting and Network Solutions 6.0

August 2004

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

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® Corp.

Support

Please visit the HP OpenView Web site at:

http://openview.hp.com/

There you will find contact information and details about the products, services, and support that HP OpenView offers.

You can go directly to the HP OpenView Web site at:

http://support.openview.hp.com/

The support Web site includes:

- Downloadable documentation
- Troubleshooting information
- Patches and updates
- Problem reporting
- Training information
- Support program information

contents

1

Overview

This overview covers the following topics:

- OVPI and the MPLS Protocol
- Folders and Reports
- New Objects and a New View
- Ways to Customize Reports
- Sources for Additional Information

OVPI and the MPLS Protocol

IETF document RFC2547 describes a virtual private network (VPN) as follows:

> "Consider a set of sites which are attached to a common network which we may call the backbone. We shall apply some policy to create a number of subsets of that set, and we shall impose the following rule: two sites may have IP interconnectivity over that backbone only if at least one of these subsets contains them both.
>
> The subsets we have created are virtual private networks (VPNs). Two sites have IP connectivity over the common backbone only if there is some VPN which contains them both. Two sites which have no VPN in common have no connectivity over the backbone."

A service provider with an IP backbone may provide VPNs for its customers. The service provider will use two protocols:

- Multi-Protocol Label Switching (MPLS)
- Border Gateway Protocol (BGP)

MPLS forwards packets over the backbone; BGP distributes routes over the backbone.

The MPLS VPN Report Pack focuses on MPLS-enabled networks that support large-scale site-to-site VPNs. The fundamental reporting component is the device-level logical interface. This interface can be MPLS-enabled, or it can be configured as one of many VPN endpoints. When an interface is configured as part of a VPN endpoint, it belongs to a VRF.

The MPLS VPN Report Pack will help you monitor service levels across multiple VPN networks. You may use it to manage small, medium, or large VPN networks. Use the reports in this package to:

- Identify VPN connection endpoints (VRFs) that are generating errors

- Identify VRFs that are not functioning
- Rank VPNs based on historical utilization
- Group multiple VPN-associated interfaces into single entities
- Apply SLA metrics, such as utilization or discard ratios, to VPNs and individual VRFs
- Monitor the generation of events in real time as breaches occur
- Discover VPN network configurations and relationships automatically
- View statistics for label usage and failed label lookups

Dependencies

MPLS VPN 3.0 builds on the capabilities of Interface Reporting 4.5. The following packages and 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	RNS Version and Date	Features/Enhancements
1.0	RNS 3.0, May 2003	27 reports Directed-instance polling support Interface re-indexing support MPLS VPN Datapipe
2.0	RNS 4.0, October 2003	OVPI Object Manager support *Forms:* • Create SLA Config Details • Change SLA Config Details • Change MPLS VPN Name • Change MPLS VPN Customer & SLA • Update VPN & VRF SLA Settings
3.0	RNS 5.0, April 2004	OVPI 5.0 support Oracle support
3.0	RNS 6.0, August 2004	Upgrade package (to_3.0)

Folders and Reports

An outline of folder contents follows.

Admin folder (3 reports). Two inventory reports and one VPN configuration report. These reports give you a sense of how the system is operating.

Devices folder (3 reports). These reports monitor recent MPLS and VPN activity at the device level, including route activity (changes and totals) across a device on an hourly and daily basis.

Interfaces folder (11 reports). These reports relate specifically to VPN-associated interfaces or MPLS-enabled interfaces. Use these reports to monitor performance and troubleshoot problems.

VPNs folder (6 reports). Reports in this folder focus on recent and historical utilization across the VRF and its component interfaces.

VRFs folder (4 reports). These reports cover route activity, volume, interface availability, and general summary information for VPNs as a whole.

The following table, arranged by folder, provides details about each report.

Folder/Reports	Purpose
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	An up to date view of all devices with MPLS enabled interfaces. Provides label count, label lookup and fragment count detail.
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 a device which supports VRFs.
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 point during the previous 6 hours.

Folder/Reports	Purpose
Near Real Time MPLS	Displays configuration data accompanied by exception counts, utilization, discards and errors.
Near Real Time MPLS Snapshot	Same as Near Real Time MPLS but with an interface pre-selection to accommodate selective displays of data.
Near Real Time VPN	Displays configuration data accompanied by exception counts, utilization, discards and errors.
Near Real Time VPN Snapshot	Same as Near Real Time VPN but with an interface pre-selection 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.
VPNs	
Route Activity	Examine historical hourly and daily route activity for a VPN as a whole and also on a per VRF basis.
Top/Bottom Ten — Interface Availability	The top and bottom ten VPNs on the network in terms of their component interface availability.
Top/Bottom Ten Volume	The top and bottom ten VPNs on the network in terms of their 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 VPN problems yesterday. Details include exception counts across all VPN associated interfaces, route counts across all VRFs within the VPN and traffic statistics.

Folder/Reports	Purpose
VPN Executive Summary	A monthly summary for each VPN a range of statistics such as # routes, total volume transferred, interface exceptions, security violations and operational seconds.
VRFs	
Current OperStatus	The operational status of each VRF on the network ordered so that 'Down' and 'Unknown' VRFs appear first in the list for ease of trouble shooting.
Historical Utilization	Select a VRF to see traffic, utilization and exception history, plus utilization 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 plus configuration changes as of the most recent poll.
Recent Utilization	The most recent complete polled hour utilization, traffic and exception details for VRFs and their component interfaces.

New Objects and a New View

Any item that appear 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**, and a list of reports under **Object Specific Reports**.

The object tree changes each time you install a new report pack. For example, 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.

Ways to Customize Reports

You can customize the contents of a report by applying group filters, by adding property data, by modifying property data, by applying constraints, and by changing view options for tables and graphs. While group filters appeal to people who need customer-specific reports, anyone can modify property data, edit a parameter, or change a view option for a table or a graph. For details about view options, see Appendix B, Editing Tables and Graphs.

Group Filters

If you intend to share your reports with customers, or with groups of people within your organization, you will need reports that contain data limited to one customer. 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 a customer or group
- Creating a group filter for the group account

For more information about creating filters for group accounts, refer to the *HP OpenView Performance Insight 5.0 Administration Guide.*

Editing Parameters

Editing a parameter applies a constraint. The constraint filters out the data you do not want to see. 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. If you edit the Location Name, data for all locations except the location you typed in the Location Name field drops from the report.

You can apply multiple constraints at once. MPLS VPN 3.0 supports 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 remotely, 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:

- *Interface Reporting Report Pack 4.5 User Guide*
- *Interface Discovery Datapipe 2.0 User Guide*

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

- *Interface Reporting ifEntry Datapipe 2.0 User Guide*

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

- *Thresholds Module 5.0 User Guide*
- *NNM/Performance Insight Integration Module 2.0 User Guide*
- *RNS 6.0 Release Notes, August 2004*

Manuals for OVPI and manuals for the reporting solutions that run on OVPI are posted to the following website:

http://www.hp.com/managementsoftware

Select **Technical Support > Product Manuals** to open the Product Manual Search page. Manuals for OVPI are listed under **Performance Insight**. Manuals for report packs, datapipes, and preprocessors are listed under **Reporting and Network Solutions**.

Every user guide listed under Reporting and Network Solutions indicates the month and year of publication. If a user guide is revised and reposted, the date of publication will change even if the software version number does not change. Because revised PDFs are posted to this site on a regular basis, you should check this site for updates before using an older PDF that may not be the latest PDF available.

2

Package Installation

This chapter covers the following topics:

- Guidelines for a Smooth Install
- Installing MPLS VPN 3.0
- Post-Installation Steps
- Uninstalling MPLS VPN 3.0

Guidelines for a Smooth Install

Each reporting solution that runs on OVPI consists of a report pack and one 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 performance data in a specific way.

The RNS 6.0 CD includes components for Network Node Manager (NNM) as well as OVPI report packs and datapipes. When you insert the RNS 6.0 CD, launch the package extraction interface, and select OVPI report packs for installation, the install script copies every OVPI package from the CD to the Packages directory on your system. After the copy process finishes, the install script prompts you to start Package Manager. Before running Package Manager, review the following guidelines.

Software Prerequisites

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

- OVPI 5.0
- Any service pack available for OVPI 5.0
- Common Property Tables Report Pack 3.0 or higher
- Interface Reporting Report Pack 4.5

Interface Reporting Report Pack 4.0 requires these datapipes:

- Interface Discovery Datapipe 2.0
- Interface Reporting ifEntry Datapipe 2.0

If you are about to upgrade to Interface Reporting 4.5, you must remove earlier versions of those two datapipes, specifically:

- Interface Discovery Datapipe 1.1
- Interface Reporting ifEntry Datapipe 1.1

For details about upgrading to Interface Reporting 4.5, refer to the *Interface Reporting Report Pack 4.5 User Guide*.

Common Property Tables

MPLS VPN 3.0 requires Common Property Tables version 3.0 or higher. 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, upgrade to version 3.0 by installing the 2.2-to-3.0 upgrade package. If you are running Common Property Tables 3.0, upgrading to version 3.5 is optional. If you install an upgrade package, do not install anything else at the same time. Install the upgrade package for Common Property Tables and *only* the upgrade package for Common Property Tables.

If you need assistance 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 will probably want to install the optional thresholds sub-package. MPLS_VPN_Threshold comes with the report pack. You will see it as an installable option when you run Package Manager. If you install it, the report pack will have a set of customized performance thresholds and OVPI can send thresholds traps to your NNM server, where traps will display as alarms in the NNM alarm browser.

You have the option of setting thresholds for rate data only, rate data and aggregated data, or just aggregated data. If you are setting thresholds for rate data only, and you are installing MPLS VPN 3.0 in a distributed environment, then the satellite servers will need MPLS_VPN_Threshold, not the central server. If you want to set thresholds on aggregated data (for example, daily data, or a forecast), you must install MPLS_VPN_Threshold on the central server as well.

When you install MPLS_VPN_Threshold, Package Manager will install the Thresholds Module for you. You may already have the Thresholds Module installed. The oldest version of the Thresholds Module you can run with MPLS VPN 3.0 is version 3.0. Upgrading to Thresholds Module 5.0 is recommended.

Upgrading from MPLS 2.0 to MPLS 3.0

If you installed MPLS VPN 2.0 a few months ago, you will have no problem upgrading to MPLS VPN 3.0. Look for the following package when you are running 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 this sequence of events:

1. Remove the old MPLS VPN Datapipe.
2. Install UPGRADE_MPLS_VPN_2.0_to_3.0.
3. Install the new MPLS VPN Datapipe.

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, Distributed Systems.

Installing MPLS VPN 3.0

Follow these steps to install MPLS VPN 3.0:

- Stop OVPI Timer and extract packages from the RNS CD
- Upgrade to Common Property Tables 3.0 or higher
- Install MPLS VPN 3.0 and restart OVPI Timer

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

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. Insert the RNS CD.

   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 the copy 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 3.0 or higher

MPLS VPN 3.0 requires Common Property Tables 3.0 or higher. If you are not running any version of Common Property Tables, skip this step. If you are running version 2.2, install the 2.2-to-3.0 upgrade package. If you are running version 3.0, upgrading to version 3.5 is optional. When Package Manager tells you that installation of the upgrade package has finished, 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*
   - *Interface_Reporting_ifEntry_Datapipe_2.0* (if not already marked as installed)
   - *Interface_Discovery_Datapipe_2.0* (if not already marked as installed)

- *Interface_Reporting_4.5* (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 Launch Polling Policy Manager and make sure that the list of nodes includes your MPLS VPN nodes.

2 In approximately 1 hour, check that polling started as expected.

Examine the Configuration and Logging Report in the Interface Reporting Admin folder. Messages from MPLS_VPN procedures will have MPLS or VPN in their name. You should see creation messages for devices, interfaces, VRFs, and VPNs.

3 Provision managed elements that are not automatically provisioned. For details, see Appendix A, Manual Provisioning.

Installation Verification

Calling the MPLS_VPN_Check_Status.sql script from the command line produces useful information about the status of the report pack. If the script detects an unusual configuration, warning messages will be printed and logged.

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.

Options for Viewing Reports

Before reports can be viewed using a web browser, they must be deployed. During the preceding installation step, you enabled the Deploy Reports option. As a result, MPLS VPN reports are deployed and available for remote viewing.

The report viewing methods available to the user depends on how OVPI was installed. If the client component is installed on the user's system, the user has access to Report Viewer, Report Builder, and the Management Console. If the client component is not installed, viewing reports on the web is the only way to view reports.

For more information about the client component, refer to the *Performance Insight Installation Guide*. For more information about deploying, viewing, and undeploying reports, refer to the *Performance Insight Guide to Building and Viewing Reports*.

Uninstalling MPLS VPN 3.0

If you remove a report pack, the associated tables and all the data in those tables will be deleted. If you want to preserve the data in those tables, archive the data before removing the package. 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.
8. Click the check box next to the following packages:
   - *MPLS_VPN*
   - *MPLS_VPN_Datapipe*
   - *MPLS_VPN_Demo* (if installed)
9. Click **Next**. The Selection Summary window opens.

10 Click **Uninstall**. The Progress window opens. When removal is complete, a package removal complete message appears.

11 Click **Done**.

12 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

Distributed Systems

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 *HP OpenView Performance Insight 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. That is, edit the $DPIPE_HOME/scripts/MPLS_Hourly_Process.pro file and modify the trendcopy commands (adding more, if necessary) so that each command includes the correct server name for each satellite server.

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 a satellite server to produce reports, switch off unnecessary processing by disabling MPLS VPN daily and monthly processing. Switch off these processes by removing the entry in $DPIPE_HOME/lib/trendtimer.sched referencing 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

Using 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

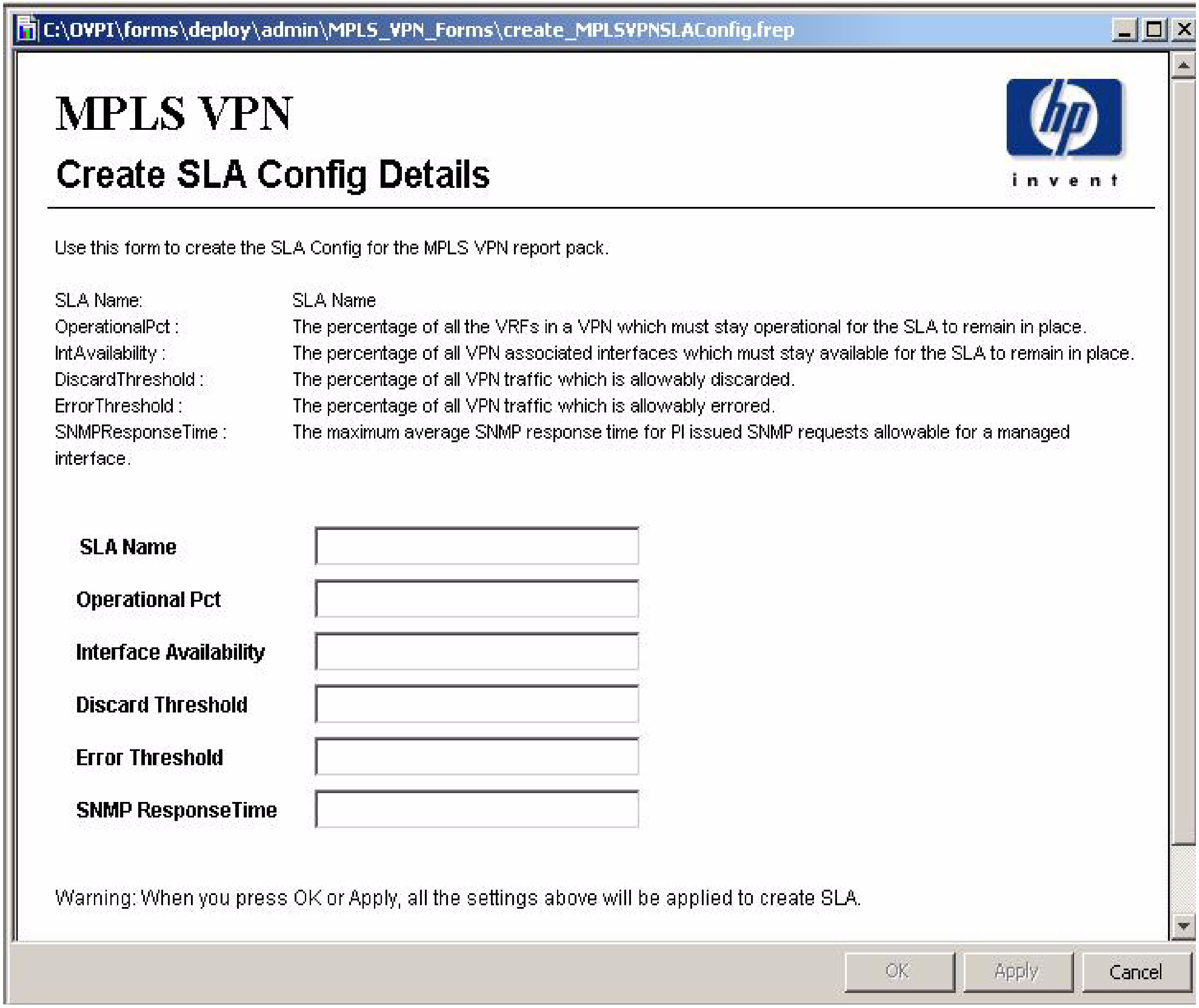
You are free to import property data in batch-mode by using a file. The batch-mode method is more efficient if you have a lot changes to make or if you are working with an automated import mechanism configured from another application. For details about creating property import files, see Appendix A,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



C:\OVPI\forms\deploy\admin\MPLS_VPN_Forms\create_MPLSVPNSLAConfig.frep

MPLS VPN

Create SLA Config Details

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

SLA Name: SLA Name
OperationalPct : The percentage of all the VRFs in a VPN which must stay operational for the SLA to remain in place.
IntAvailability : The percentage of all VPN associated interfaces which must stay available for the SLA to remain in place.
DiscardThreshold : The percentage of all VPN traffic which is allowably discarded.
ErrorThreshold : The percentage of all VPN traffic which is allowably errored.
SNMPResponseTime : The maximum average SNMP response time for PI issued SNMP requests allowable for a managed interface.

SLA Name

Operational Pct

Interface Availability

Discard Threshold

Error Threshold

SNMP ResponseTime

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

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.

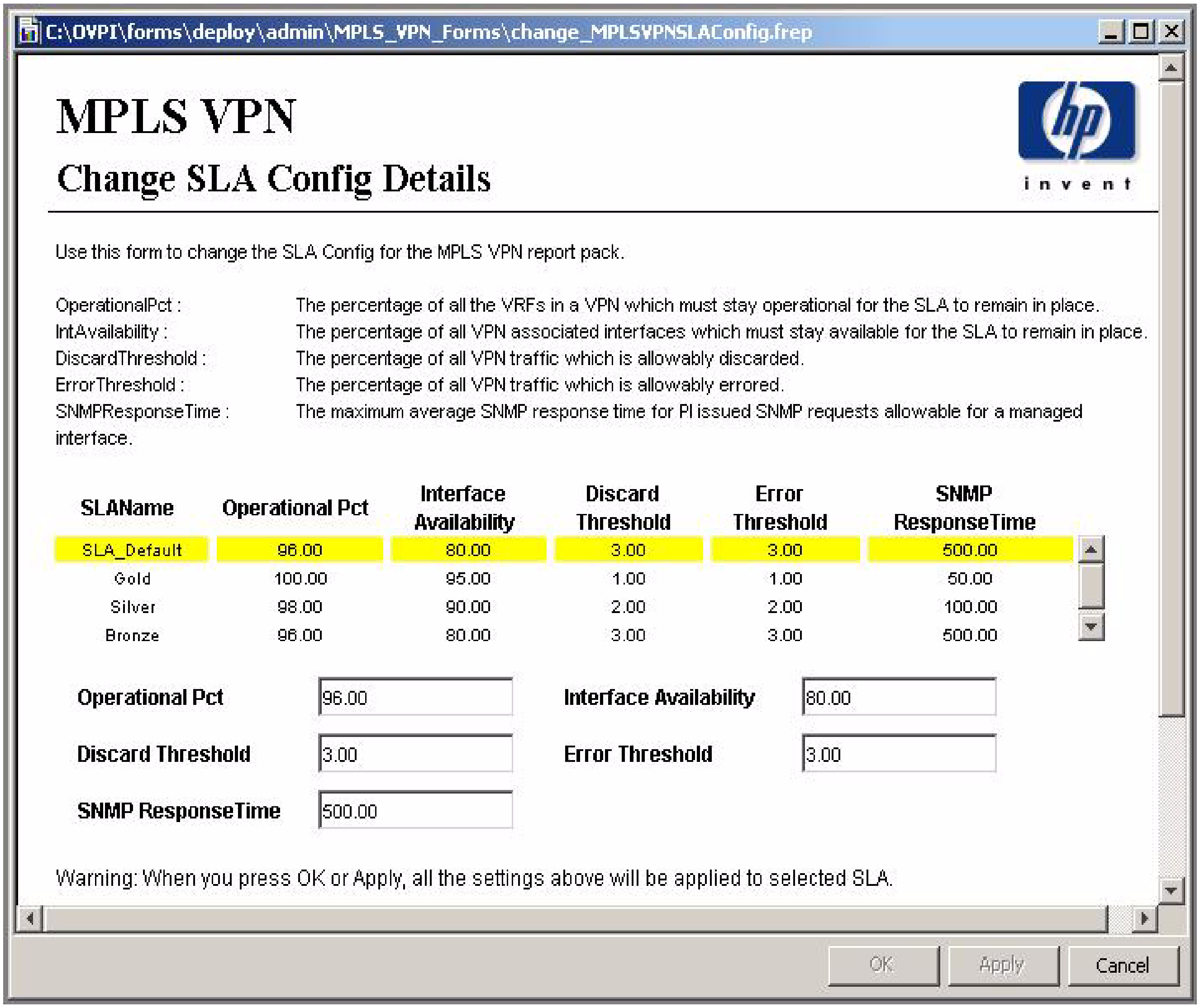
Change SLA Configuration Details

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**.



C:\OVPI\forms\deploy\admin\MPLS_VPN_Forms\change_MPLSVPNSLAConfig.frep

MPLS VPN

Change SLA Config Details

Use this form to change the SLA Config for the MPLS VPN report pack.

OperationalPct : The percentage of all the VRFs in a VPN which must stay operational for the SLA to remain in place.
IntAvailability : The percentage of all VPN associated interfaces which must stay available for the SLA to remain in place.
DiscardThreshold : The percentage of all VPN traffic which is allowably discarded.
ErrorThreshold : The percentage of all VPN traffic which is allowably errored.
SNMPResponseTime : The maximum average SNMP response time 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

Operational Pct	96.00	**Interface Availability**	80.00
Discard Threshold	3.00	**Error Threshold**	3.00
SNMP ResponseTime	500.00		

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

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:

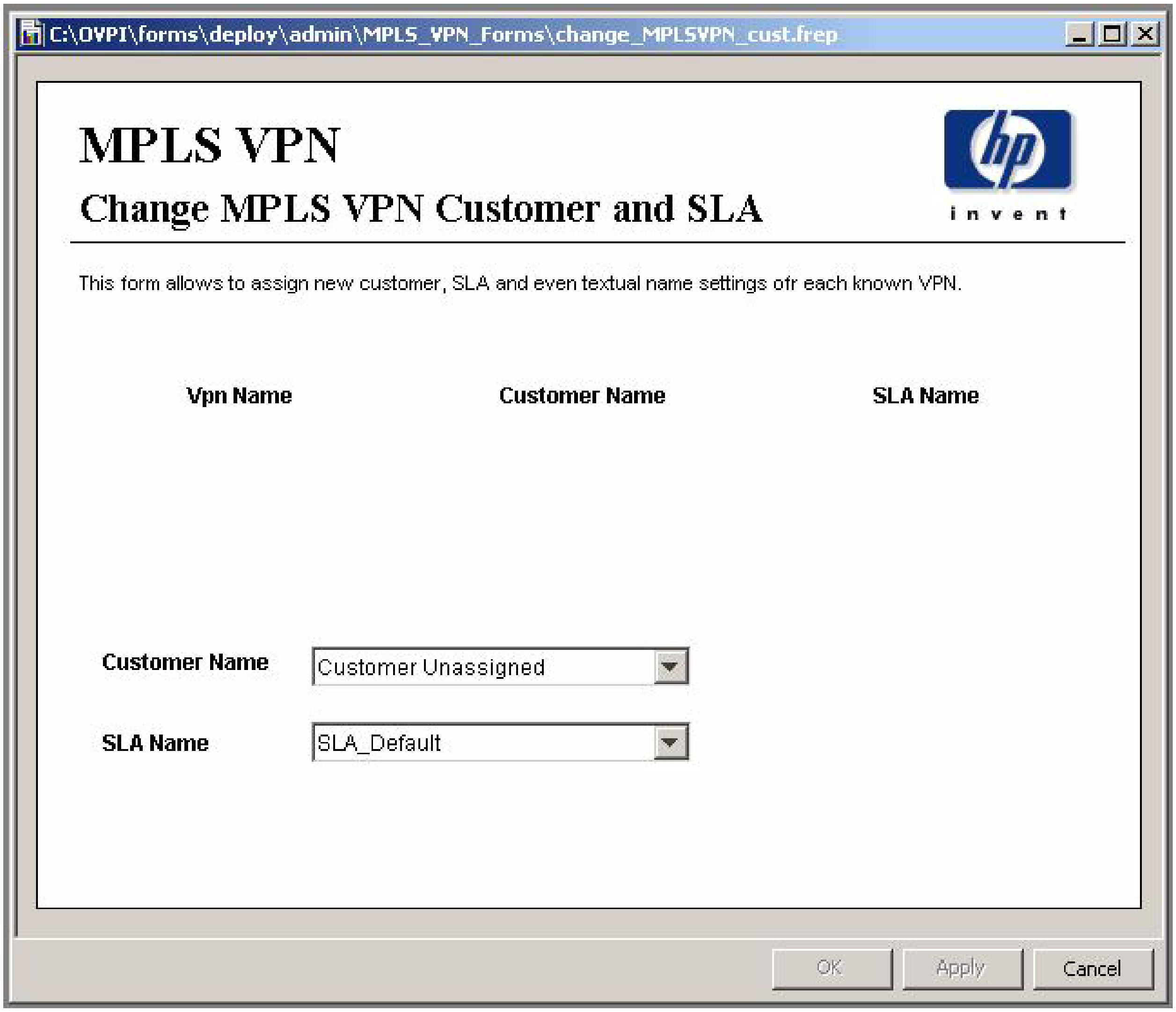
1 In the Management Console, click the **Objects** icon.

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**.



C:\OVPI\forms\deploy\admin\MPLS_VPN_Forms\change_MPLSVPN_cust.frep

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

Customer Name: Customer Unassigned

SLA Name: SLA_Default

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.

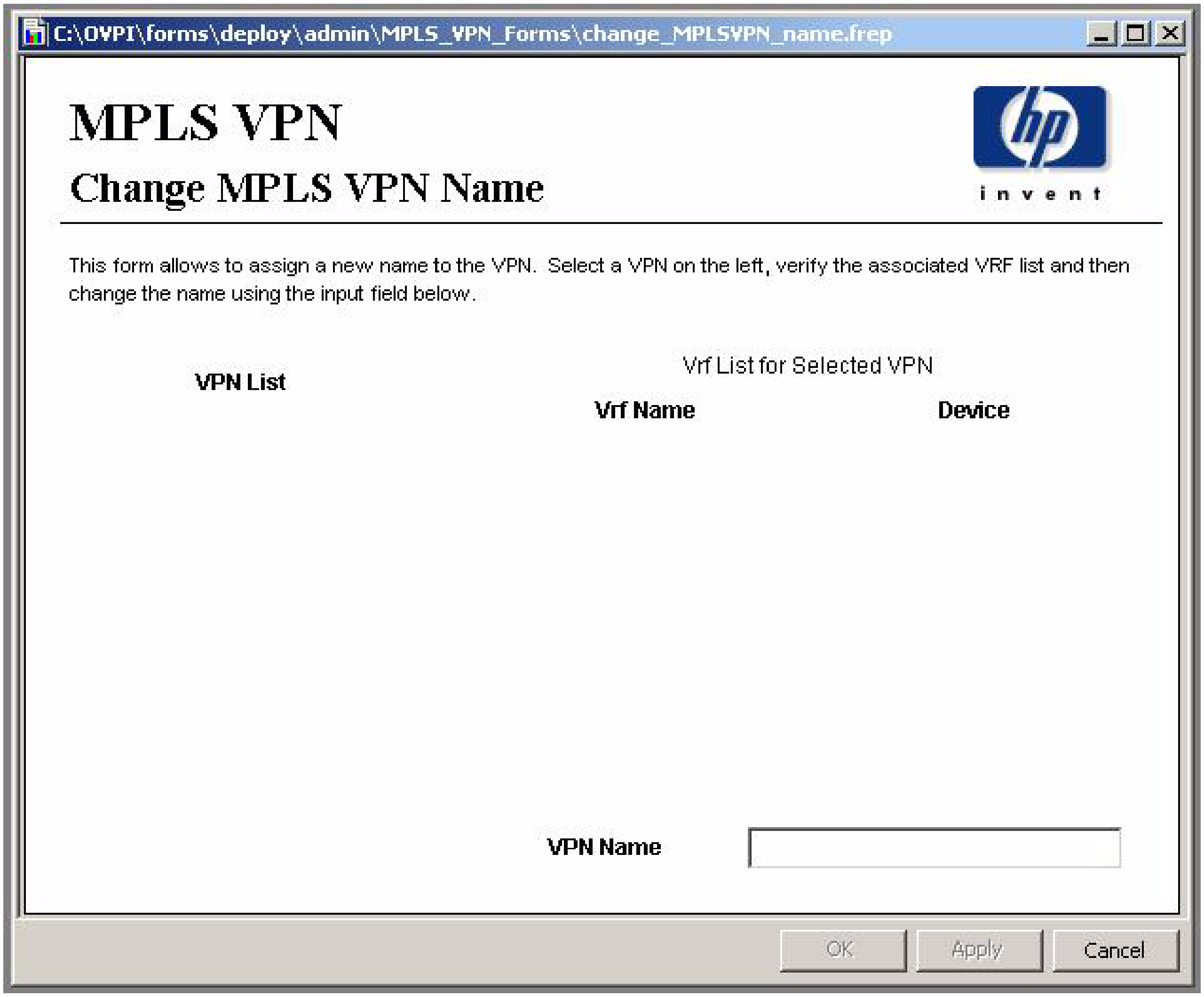
Change a VPN Name

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**.


C:\OVPI\forms\deploy\admin\MPLS_VPN_Forms\change_MPLSVPN_name.frep
invent
OK
Apply
Cancel

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

VPN Name

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.

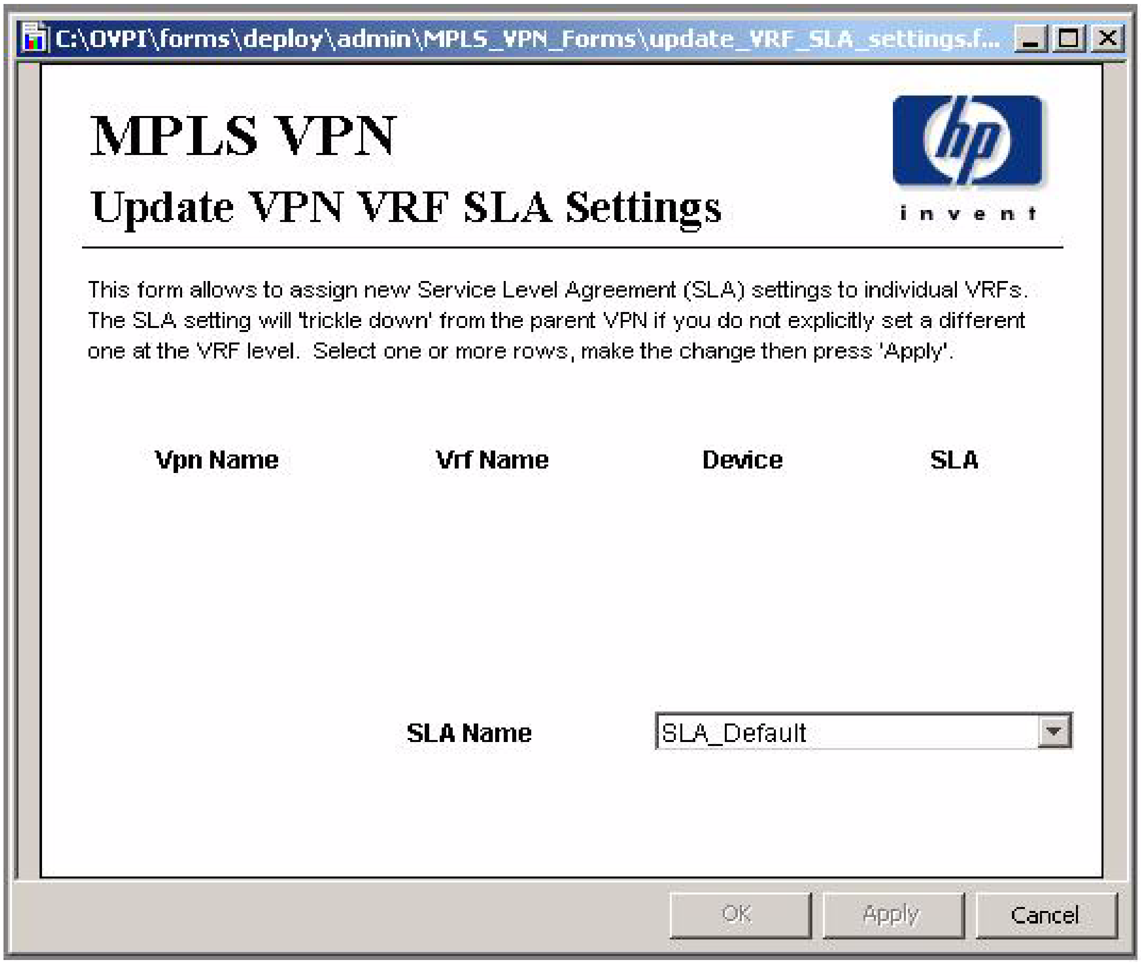
Update VPN VRF SLA Settings

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.**


C:\OVPI\forms\deploy\admin\MPLS_VPN_Forms\update_VRF_SLA_settings.f...
MPLS VPN
Update VPN VRF SLA Settings
invent

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

SLA Name: SLA_Default

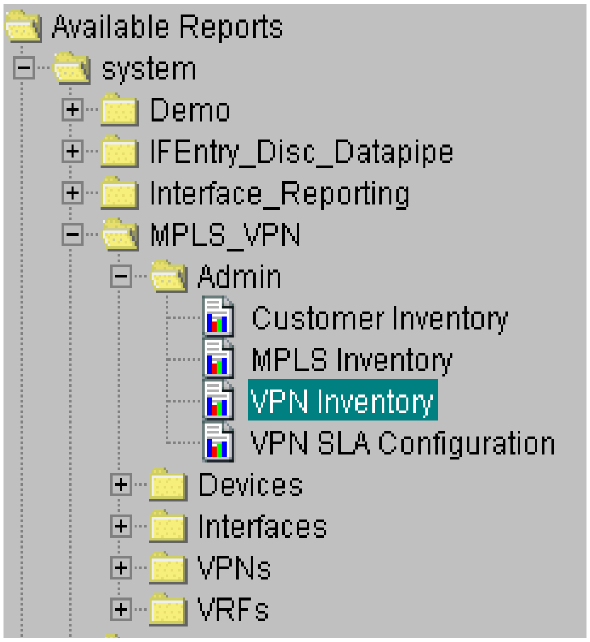
4 Assign a new SLA VPN VRF using the **SLA Name** drop-down selection list.

5 Click **Apply**, then click **OK** to save the changes and close the form.

5

VPN Inventory

The VPN Inventory report illustrates the current VPN configuration as presented by the network devices. Use this report to grasp 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.



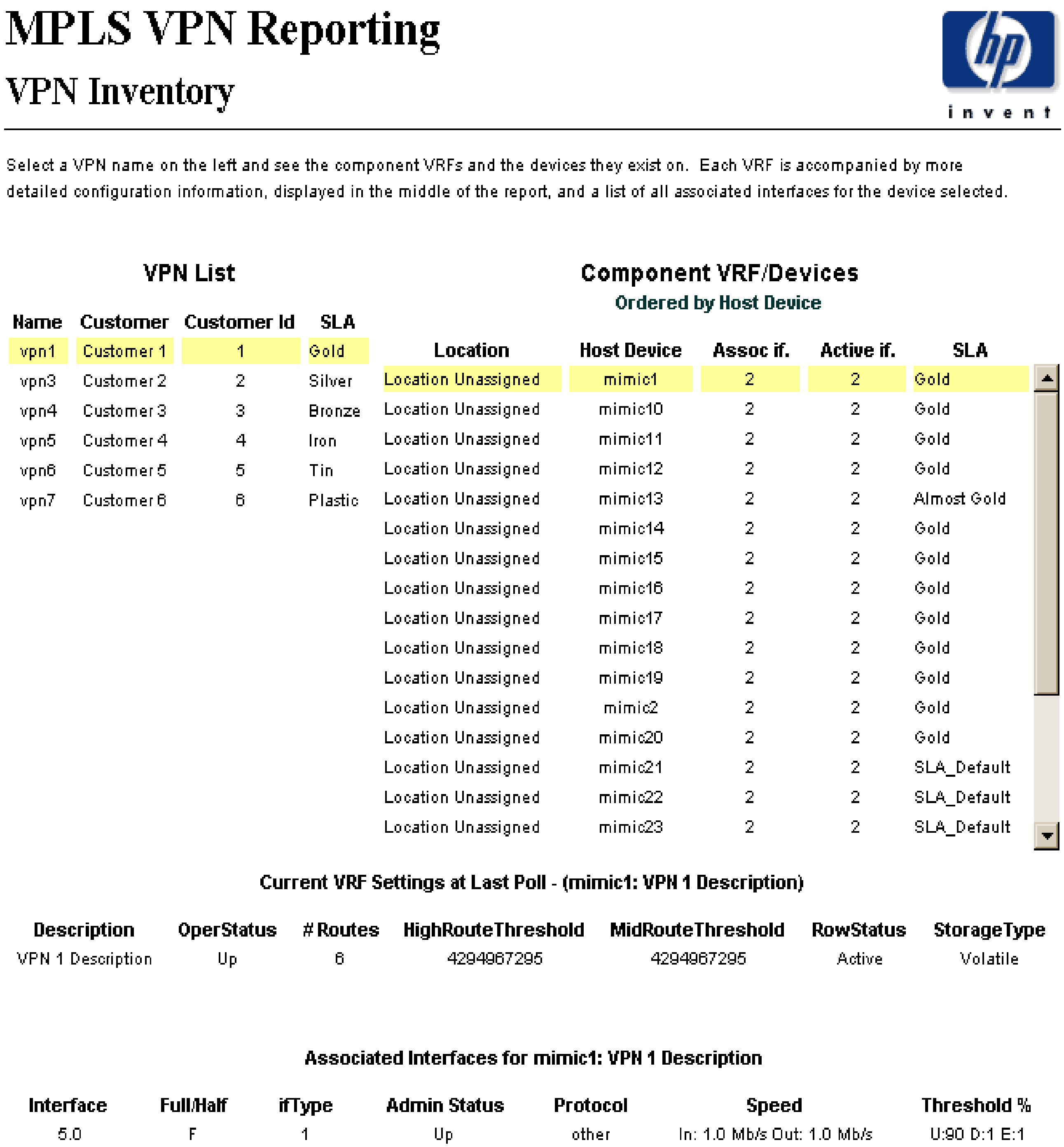
The VPN Inventory report resides in the Admin folder. Other administrative reports in this folder focus on customer oriented inventory lists, MPLS-enabled interfaces, and VPN SLA settings.

After each poll cycle, the system updates its stored view of the network configuration to reflect the latest information. Newly discovered VPNs will be noted and representations created in the MPLS VPN Report Pack database tables.

A selection list at the top of the report includes each known VPN. If customers and service levels have been configured against the VPN, then the table will include those settings. Select a VPN to display a list of VRFs that make up the VPN. You will see the number of associated and active interfaces as well as the Service Level associated with each VRF. Select a VRF to list the associated interfaces on that device and their individual configurations.

You can filter the contents 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 more detailed configuration information, displayed in the middle of the report, and a list of all associated interfaces for the device selected.

VPN List

Name	Customer	Customer Id	SLA
vpn1	Customer 1	1	Gold
vpn3	Customer 2	2	Silver
vpn4	Customer 3	3	Bronze
vpn5	Customer 4	4	Iron
vpn6	Customer 5	5	Tin
vpn7	Customer 6	6	Plastic

Component VRF/Devices

Ordered by Host Device

Location	Host Device	Assoc if.	Active if.	SLA
Location Unassigned	mimic1	2	2	Gold
Location Unassigned	mimic10	2	2	Gold
Location Unassigned	mimic11	2	2	Gold
Location Unassigned	mimic12	2	2	Gold
Location Unassigned	mimic13	2	2	Almost Gold
Location Unassigned	mimic14	2	2	Gold
Location Unassigned	mimic15	2	2	Gold
Location Unassigned	mimic16	2	2	Gold
Location Unassigned	mimic17	2	2	Gold
Location Unassigned	mimic18	2	2	Gold
Location Unassigned	mimic19	2	2	Gold
Location Unassigned	mimic2	2	2	Gold
Location Unassigned	mimic20	2	2	Gold
Location Unassigned	mimic21	2	2	SLA_Default
Location Unassigned	mimic22	2	2	SLA_Default
Location Unassigned	mimic23	2	2	SLA_Default

Current VRF Settings at Last Poll - (mimic1: VPN 1 Description)

Description	OperStatus	# Routes	HighRouteThreshold	MidRouteThreshold	RowStatus	StorageType
VPN 1 Description	Up	6	4294967295	4294967295	Active	Volatile

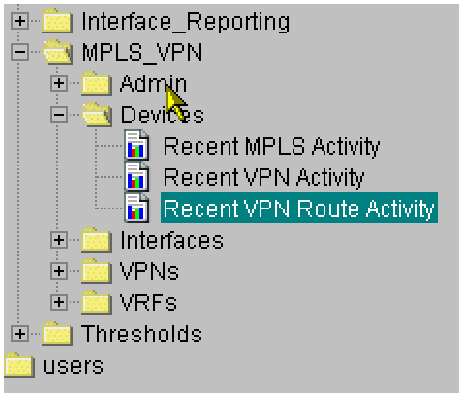
Associated Interfaces for mimic1: VPN 1 Description

Interface	Full/Half	ifType	Admin Status	Protocol	Speed	Threshold %
5.0	F	1	Up	other	In: 1.0 Mb/s Out: 1.0 Mb/s	U:90 D:1 E:1

6

VPN Route Activity

The VPN Route Activity report, residing in the Devices folder, presents current and historical information about devices supporting VPN interfaces. Route change activity, and thus IGP activity, is the focus of this report.



Network operations staff responsible for monitoring route activity and changes across the network will find this report particularly helpful. Tables and charts present a combination of most recent poll configuration information, or hourly and daily aggregated data. The other two reports in the Devices folder, Recent MPLS Activity and Recent VPN Activity, analyze network activity on a per device basis.

At the top of the report you will see a list of known devices, user-provisioned attributes such as Customer and Location, and network-sourced attributes such as Active VRFs and Connected Interfaces.You can filter the contents of this report by applying the following constraints:

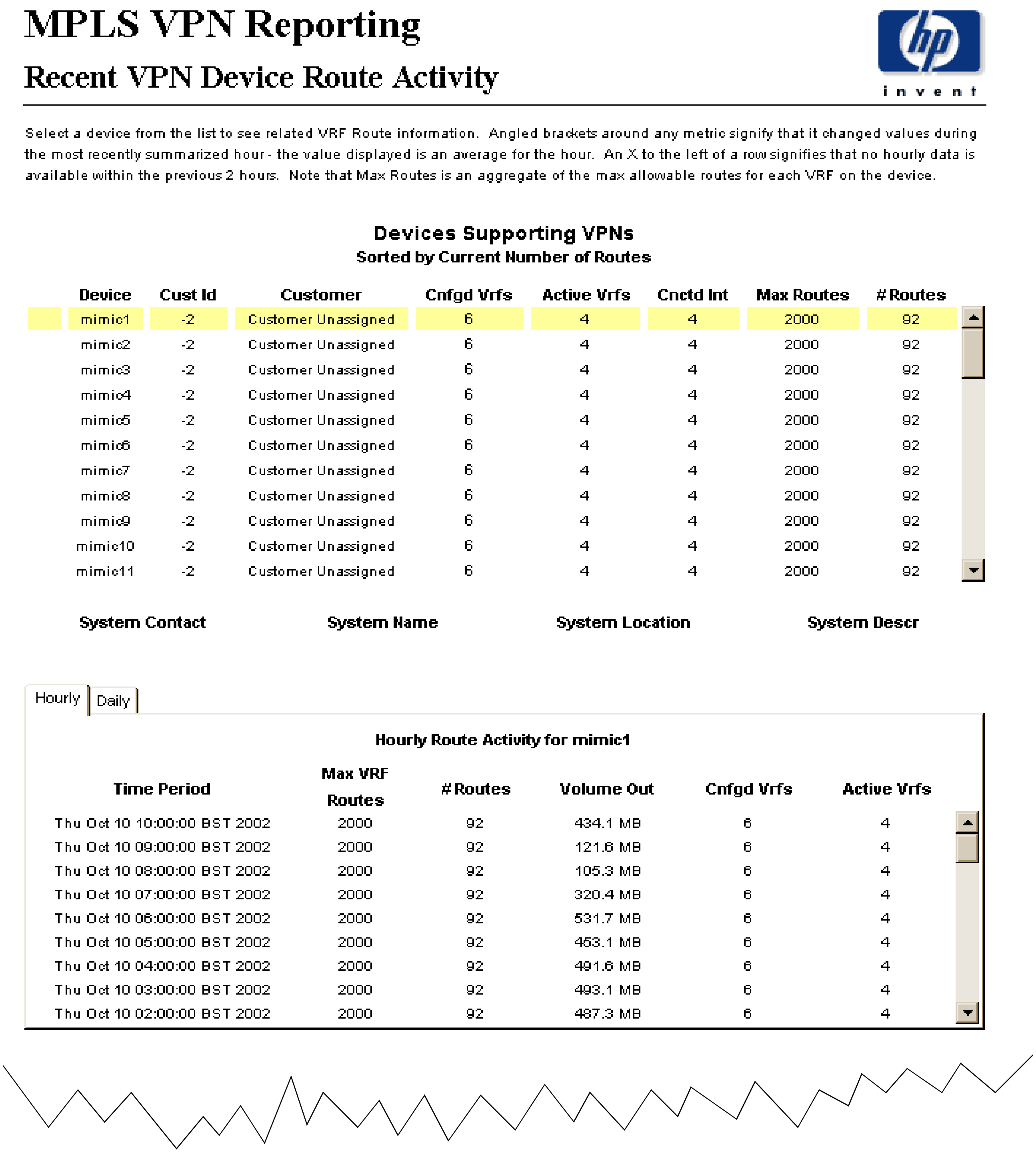
- Customer ID
- Location Name
- Location ID

Devices Supporting VPNs

The selection table presents relevant information for all devices supporting VPN VRFs. The small “x” to the left of two devices tells you that the data in the table is at least two hours out of date. The most likely reason for this is that polling of the device has not been successful, indicating that the device is out of operation or that network connectivity has been lost.

The Max Routes column is an aggregate of the maximum routes for each VRF on the device. This method of calculation is more accurate than simply presenting the single value of maximum routes as presented by the device. Examine the lower portion of the report to see how the routes are spread across the VRFs on the device.

Restrict the devices that display in this table by using the following parameters: Device, Customer Name, Customer ID, Location Name, Location ID.



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

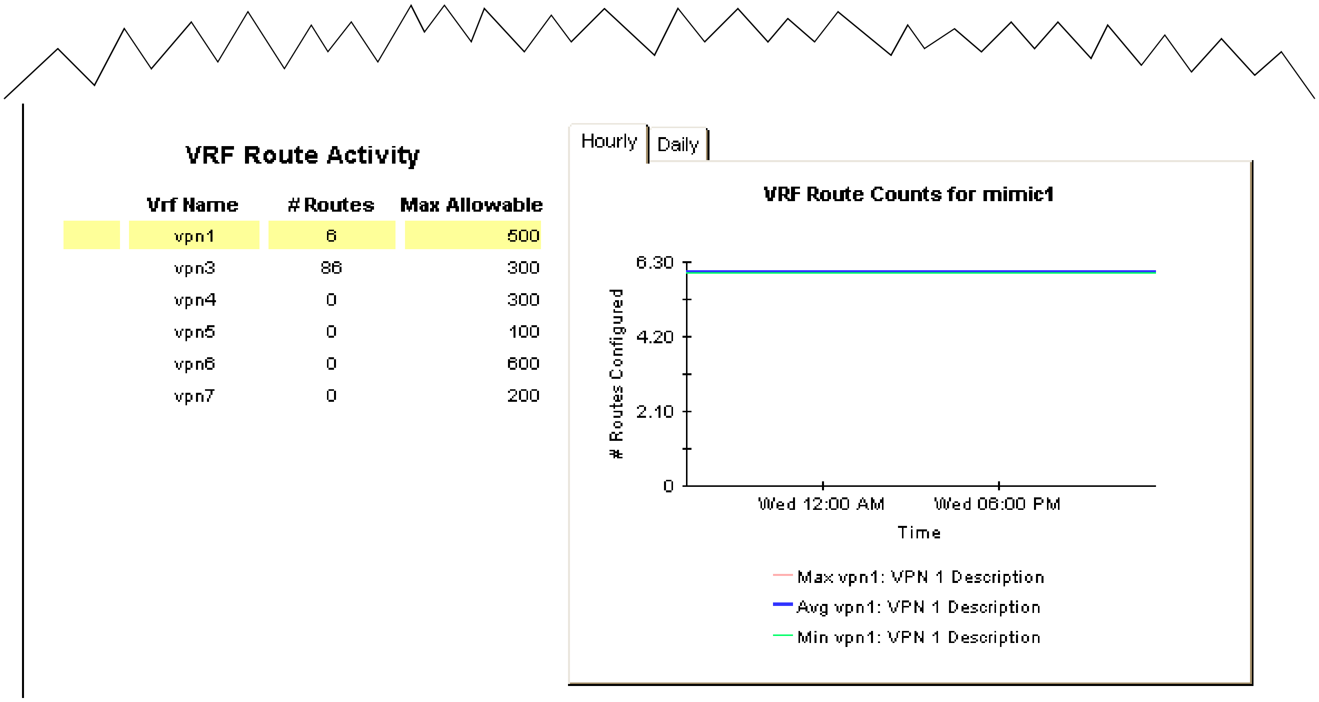
Sorted by Current Number of Routes

Device	Cust Id	Customer	Cnfgd Vrfs	Active Vrfs	Cnctd Int	Max Routes	# Routes
mimic1	-2	Customer Unassigned	6	4	4	2000	92
mimic2	-2	Customer Unassigned	6	4	4	2000	92
mimic3	-2	Customer Unassigned	6	4	4	2000	92
mimic4	-2	Customer Unassigned	6	4	4	2000	92
mimic5	-2	Customer Unassigned	6	4	4	2000	92
mimic6	-2	Customer Unassigned	6	4	4	2000	92
mimic7	-2	Customer Unassigned	6	4	4	2000	92
mimic8	-2	Customer Unassigned	6	4	4	2000	92
mimic9	-2	Customer Unassigned	6	4	4	2000	92
mimic10	-2	Customer Unassigned	6	4	4	2000	92
mimic11	-2	Customer Unassigned	6	4	4	2000	92

System Contact	System Name	System Location	System Descr

Hourly Route Activity for mimic1

Time Period	Max VRF Routes	# Routes	Volume Out	Cnfgd Vrfs	Active Vrfs
Thu Oct 10 10:00:00 BST 2002	2000	92	434.1 MB	6	4
Thu Oct 10 09:00:00 BST 2002	2000	92	121.6 MB	6	4
Thu Oct 10 08:00:00 BST 2002	2000	92	105.3 MB	6	4
Thu Oct 10 07:00:00 BST 2002	2000	92	320.4 MB	6	4
Thu Oct 10 06:00:00 BST 2002	2000	92	531.7 MB	6	4
Thu Oct 10 05:00:00 BST 2002	2000	92	453.1 MB	6	4
Thu Oct 10 04:00:00 BST 2002	2000	92	491.6 MB	6	4
Thu Oct 10 03:00:00 BST 2002	2000	92	493.1 MB	6	4
Thu Oct 10 02:00:00 BST 2002	2000	92	487.3 MB	6	4



VRF Route Activity

Vrf Name	# Routes	Max Allowable
vpn1	6	500
vpn3	86	300
vpn4	0	300
vpn5	0	100
vpn6	0	600
vpn7	0	200

Hourly
Daily
VRF Route Counts for mimic1
6.30
4.20
2.10
0
# Routes Configured
Wed 12:00 AM
Wed 06:00 PM
Time
Max vpn1: VPN 1 Description
Avg vpn1: VPN 1 Description
Min vpn1: VPN 1 Description

Hourly Route Activity

The central tabbed area provides an instant historical record of routing changes on the device and how they compare with total volume placed on the backbone by this VRF, the number of configured and of active VRFs. Time periods available are Hourly and Daily.

“Configured” and “Active” VRF counts represent the maximum value recorded during the time period. “# Routes” is the aggregated number of routes across all VRFs on the device for that time period. A change in route count on a device implies IGP activity and configuration changes.

The Time Period column represents the time the reporting period started. The top row is showing activity between 10:00 and 11:00 a.m.

VRF Route Activity

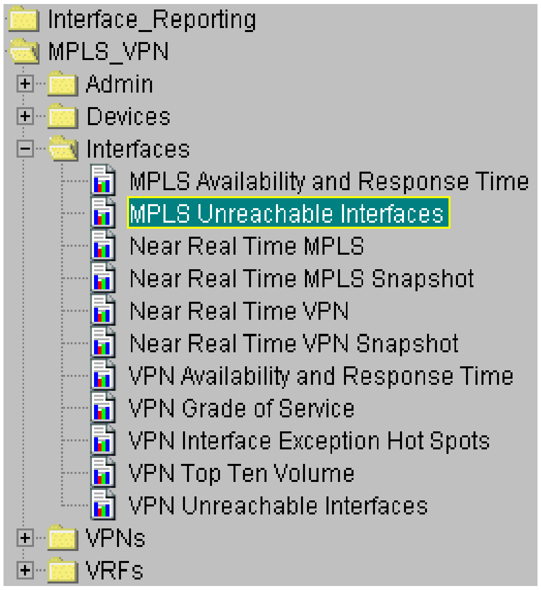
The lowest section of the report depicts information on a per-VRF basis. The selection of VRFs displayed is driven by the device selection table at the top. As with the device selection, if data has not been aggregated for a VRF, for any reason, within the last two hours, then an X will appear to the left of the VRF name. The most likely reasons for a VRF having no aggregated data is that it has been removed from the device, or the device is temporarily unreachable. VRF data will be aged out of this table, and others like it, within two days.

Selecting a VRF from the left selection list results in the route count graph to the right being populated with maximum, minimum, and average route count data. The Hourly tab by default displays the previous 50 hours, while the daily tab displays the previous 50 days.

7

Unreachable MPLS Interfaces

The Unreachable Interfaces report presents a list of interfaces that have not been polled within the previous 35 minutes. This report is intended for operations staff responsible for troubleshooting faulty devices or network connections.



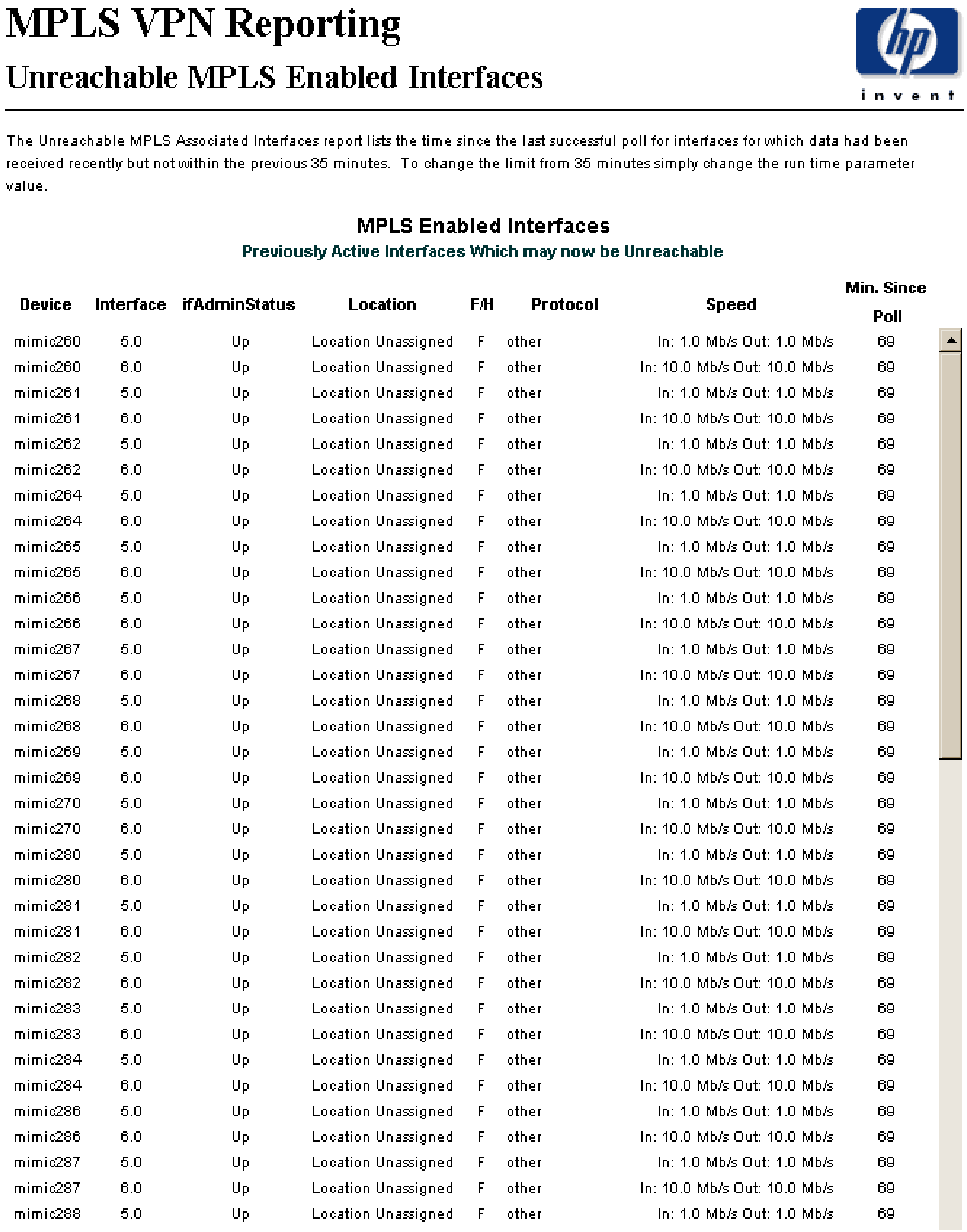
- Interface_Reporting
- MPLS_VPN
  - Admin
  - Devices
  - Interfaces
    - MPLS Availability and Response Time
    - MPLS Unreachable Interfaces
    - Near Real Time MPLS
    - Near Real Time MPLS Snapshot
    - Near Real Time VPN
    - Near Real Time VPN Snapshot
    - VPN Availability and Response Time
    - VPN Grade of Service
    - VPN Interface Exception Hot Spots
    - VPN Top Ten Volume
    - VPN Unreachable Interfaces
  - VPNs
  - VRFs

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.

You can modify the list of unreachable MPLS interfaces using the MinutesSincePoll parameter. By default, the system will poll on a 15 minute cycle. The value of 35 for MinutesSincePoll allows for interfaces that missed one poll cycle. Increasing this value will display interfaces only when they have been out of reach for longer.

You can filter the interfaces in this list 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. Note that an interface will inherit the customer details of the parent device if none are explicitly specified.
- Location - The location name associated with the interface. Note that an interface will inherit the location details of the parent device if none are explicitly specified.
- Full or Half - The duplex configuration of the interface - full duplex (2) or half duplex (1).
- MinutesSincePoll - The number of minutes since the beginning of the last completed poll cycle.



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

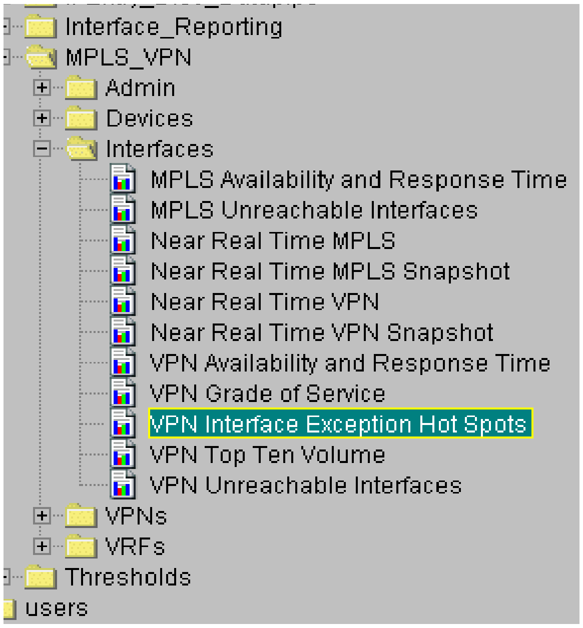
Previously Active Interfaces Which may now be Unreachable

Device	Interface	ifAdminStatus	Location	F/H	Protocol	Speed	Min. Since Poll
mimic260	5.0	Up	Location Unassigned	F	other	In: 1.0 Mb/s Out: 1.0 Mb/s	69
mimic260	6.0	Up	Location Unassigned	F	other	In: 10.0 Mb/s Out: 10.0 Mb/s	69
mimic261	5.0	Up	Location Unassigned	F	other	In: 1.0 Mb/s Out: 1.0 Mb/s	69
mimic261	6.0	Up	Location Unassigned	F	other	In: 10.0 Mb/s Out: 10.0 Mb/s	69
mimic262	5.0	Up	Location Unassigned	F	other	In: 1.0 Mb/s Out: 1.0 Mb/s	69
mimic262	6.0	Up	Location Unassigned	F	other	In: 10.0 Mb/s Out: 10.0 Mb/s	69
mimic264	5.0	Up	Location Unassigned	F	other	In: 1.0 Mb/s Out: 1.0 Mb/s	69
mimic264	6.0	Up	Location Unassigned	F	other	In: 10.0 Mb/s Out: 10.0 Mb/s	69
mimic265	5.0	Up	Location Unassigned	F	other	In: 1.0 Mb/s Out: 1.0 Mb/s	69
mimic265	6.0	Up	Location Unassigned	F	other	In: 10.0 Mb/s Out: 10.0 Mb/s	69
mimic266	5.0	Up	Location Unassigned	F	other	In: 1.0 Mb/s Out: 1.0 Mb/s	69
mimic266	6.0	Up	Location Unassigned	F	other	In: 10.0 Mb/s Out: 10.0 Mb/s	69
mimic267	5.0	Up	Location Unassigned	F	other	In: 1.0 Mb/s Out: 1.0 Mb/s	69
mimic267	6.0	Up	Location Unassigned	F	other	In: 10.0 Mb/s Out: 10.0 Mb/s	69
mimic268	5.0	Up	Location Unassigned	F	other	In: 1.0 Mb/s Out: 1.0 Mb/s	69
mimic268	6.0	Up	Location Unassigned	F	other	In: 10.0 Mb/s Out: 10.0 Mb/s	69
mimic269	5.0	Up	Location Unassigned	F	other	In: 1.0 Mb/s Out: 1.0 Mb/s	69
mimic269	6.0	Up	Location Unassigned	F	other	In: 10.0 Mb/s Out: 10.0 Mb/s	69
mimic270	5.0	Up	Location Unassigned	F	other	In: 1.0 Mb/s Out: 1.0 Mb/s	69
mimic270	6.0	Up	Location Unassigned	F	other	In: 10.0 Mb/s Out: 10.0 Mb/s	69
mimic280	5.0	Up	Location Unassigned	F	other	In: 1.0 Mb/s Out: 1.0 Mb/s	69
mimic280	6.0	Up	Location Unassigned	F	other	In: 10.0 Mb/s Out: 10.0 Mb/s	69
mimic281	5.0	Up	Location Unassigned	F	other	In: 1.0 Mb/s Out: 1.0 Mb/s	69
mimic281	6.0	Up	Location Unassigned	F	other	In: 10.0 Mb/s Out: 10.0 Mb/s	69
mimic282	5.0	Up	Location Unassigned	F	other	In: 1.0 Mb/s Out: 1.0 Mb/s	69
mimic282	6.0	Up	Location Unassigned	F	other	In: 10.0 Mb/s Out: 10.0 Mb/s	69
mimic283	5.0	Up	Location Unassigned	F	other	In: 1.0 Mb/s Out: 1.0 Mb/s	69
mimic283	6.0	Up	Location Unassigned	F	other	In: 10.0 Mb/s Out: 10.0 Mb/s	69
mimic284	5.0	Up	Location Unassigned	F	other	In: 1.0 Mb/s Out: 1.0 Mb/s	69
mimic284	6.0	Up	Location Unassigned	F	other	In: 10.0 Mb/s Out: 10.0 Mb/s	69
mimic286	5.0	Up	Location Unassigned	F	other	In: 1.0 Mb/s Out: 1.0 Mb/s	69
mimic286	6.0	Up	Location Unassigned	F	other	In: 10.0 Mb/s Out: 10.0 Mb/s	69
mimic287	5.0	Up	Location Unassigned	F	other	In: 1.0 Mb/s Out: 1.0 Mb/s	69
mimic287	6.0	Up	Location Unassigned	F	other	In: 10.0 Mb/s Out: 10.0 Mb/s	69
mimic288	5.0	Up	Location Unassigned	F	other	In: 1.0 Mb/s Out: 1.0 Mb/s	69

8

VPN Interface Exception Hot Spots

Use the VPN Interface Exception Hot Spots report to display every VPN-associated interface that experienced at least one exception. Any interface shown here broke a pre-set threshold sometime during the previous day. Use this report to find out whether an exception that occurred yesterday is a normal condition or an abnormal condition.


Interface_Reporting
MPLS_VPN
Admin
Devices
Interfaces
MPLS Availability and Response Time
MPLS Unreachable Interfaces
Near Real Time MPLS
Near Real Time MPLS Snapshot
Near Real Time VPN
Near Real Time VPN Snapshot
VPN Availability and Response Time
VPN Grade of Service
VPN Interface Exception Hot Spots
VPN Top Ten Volume
VPN Unreachable Interfaces
VPNs
VRFs
Thresholds
users

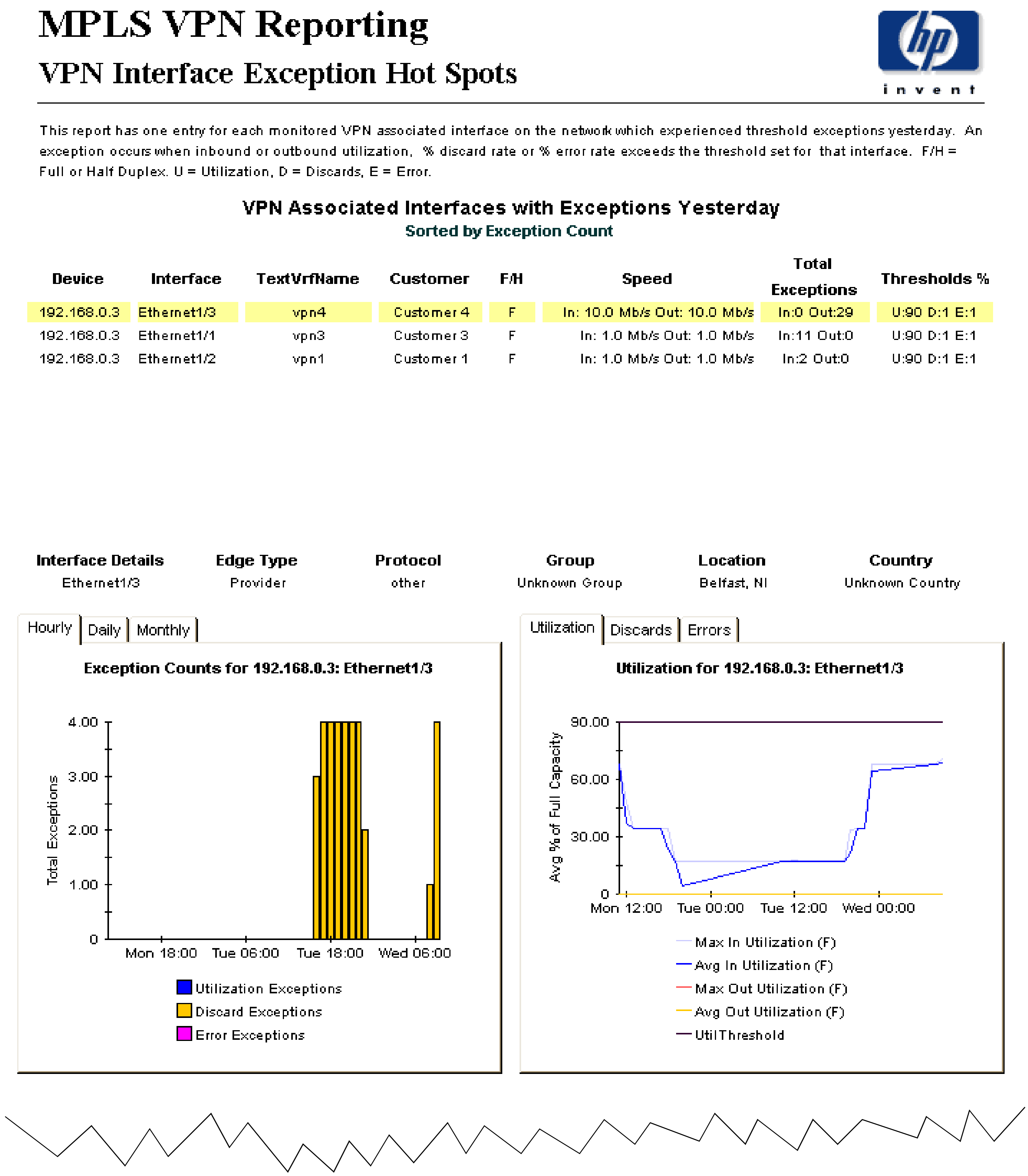
The reports in the Interfaces folder focus on either MPLS-enabled, or VPN-associated interfaces. While similar to the interface-specific reports in the Interface Reporting Report Pack, these reports offer additional MPLS or VPN related attributes on a per-interface basis. In addition, these reports only list interfaces of interest to users in the MPLS/VPN-oriented community.

Selecting an interface populates the exception, utilization, error, and discard ratio graphs. Tabs in the middle right section focus on Utilization, Discard, or Error rates. Tabs on the lowest graph combine all three metrics and split the traffic into either inbound or outbound components where applicable.

The thresholds in this report can be modified using forms that come with the Interface Reporting Report Pack. For details, refer to the *Interface Reporting Report Pack 4.5 User Guide*.

You can filter 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

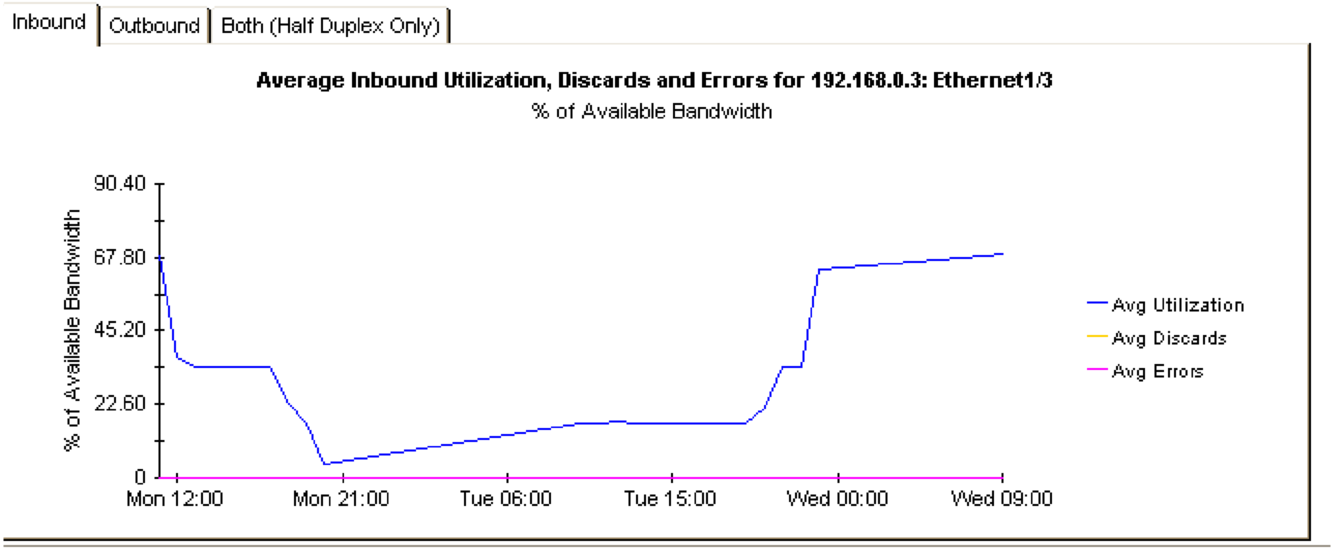
This report has one entry for each monitored VPN associated interface on the network which experienced threshold exceptions yesterday. An exception occurs when inbound or outbound utilization, % discard rate or % error rate exceeds the threshold set for that interface. F/H = Full or Half Duplex. U =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

VPN Associated Interfaces with Exceptions Yesterday

Sorted by Exception Count

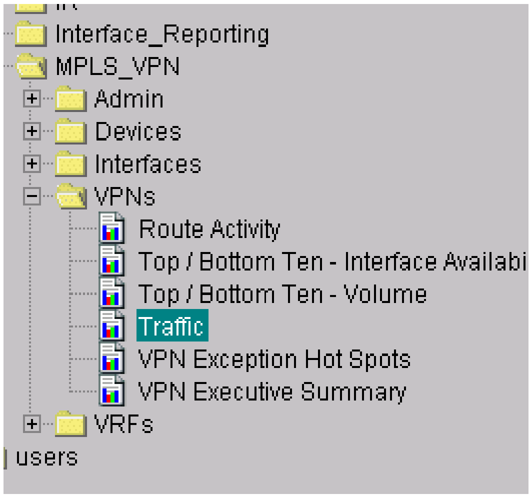
Device	Interface	TextVrfName	Customer	F/H	Speed	Total Exceptions	Thresholds %
192.168.0.3	Ethernet1/3	vpn4	Customer 4	F	In: 10.0 Mb/s Out: 10.0 Mb/s	In:0 Out:29	U:90 D:1 E:1
192.168.0.3	Ethernet1/1	vpn3	Customer 3	F	In: 1.0 Mb/s Out: 1.0 Mb/s	In:11 Out:0	U:90 D:1 E:1
192.168.0.3	Ethernet1/2	vpn1	Customer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

Interface Details	Edge Type	Protocol	Group	Location	Country
Ethernet1/3	Provider	other	Unknown Group	Belfast, NI	Unknown Country


Inbound
Outbound
Both (Half Duplex Only)
Average Inbound Utilization, Discards and Errors for 192.168.0.3: Ethernet1/3
% of Available Bandwidth
% of Available Bandwidth
90.40
67.80
45.20
22.60
0
Mon 12:00
Mon 21:00
Tue 06:00
Tue 15:00
Wed 00:00
Wed 09:00
Avg Utilization
Avg Discards
Avg Errors

9

VPN Traffic Volume



The VPN Traffic Volume report provides customer details and high-level metrics for every VPN you are monitoring. The metrics include the number of interfaces associated with the VPN, the operational% of the component VRFs, and the volume across the VPN.

This is one of six reports in the VPNs folder. The reports in this 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. Due to the high level nature of the reports in this folder, they are more suitable for external customer deployment or management review than operational network monitoring.

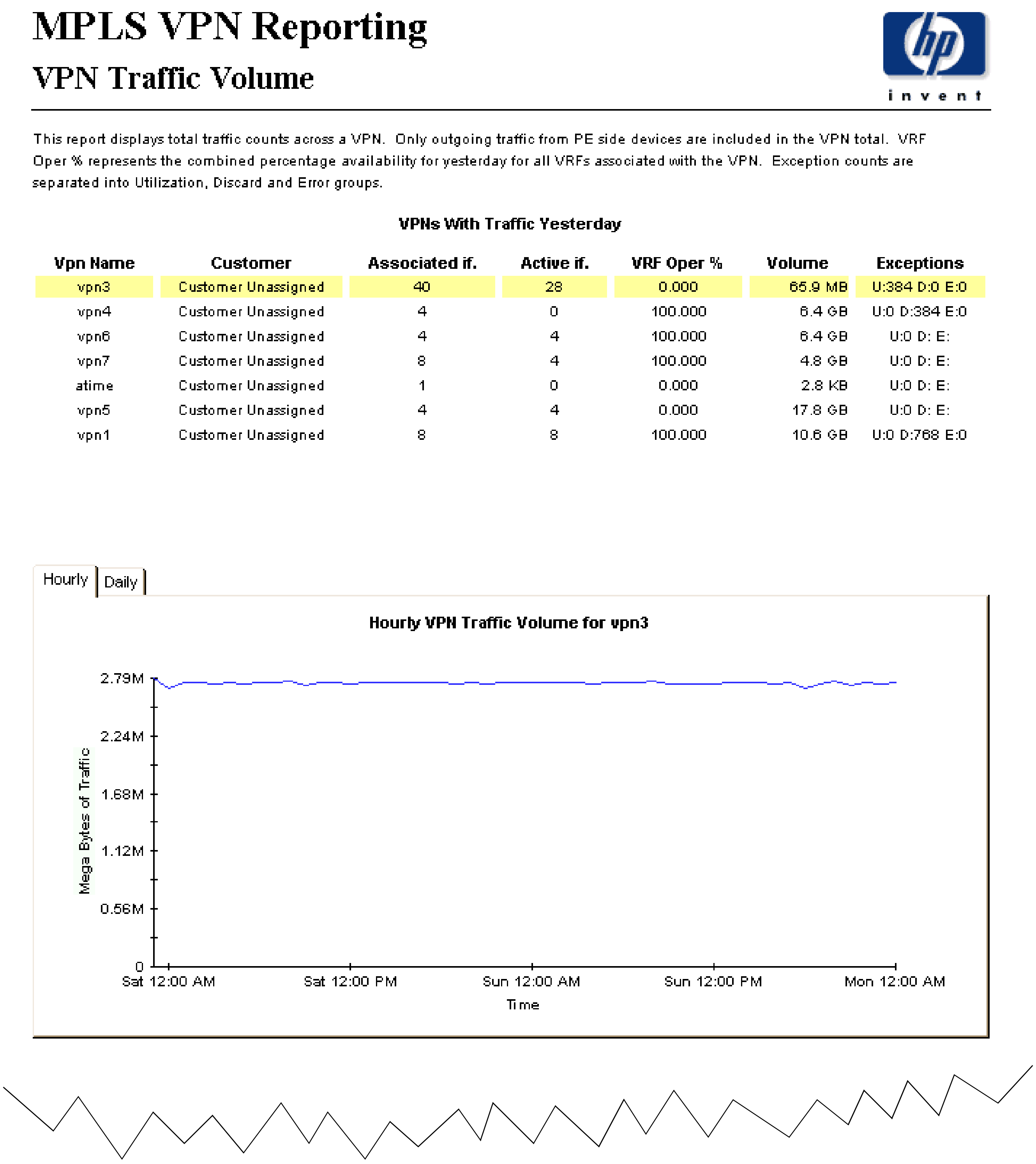
The selection tables display yesterday's aggregated data for the VPN. Select a VPN from the top table and view the component VRF utilization and volume figures.

The VRF Operational Status% is 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.

Utilization, discard, and error exceptions are generated at the interface level, in response to a threshold configured at the interface level. Exceptions in this report refer to an aggregated total for all interfaces in the VPN.

You can filter this report by applying the following constraints:

- Device - The device name or IP address.
- Customer_Name - The customer name associated with the VPN. Note that all interfaces associated with a VPN will inherit the customer details of the parent if it not explicitly specified as something else.
- Cust_ID - The numeric identifier for this customer.
- VPN - The textual name for this VPN.



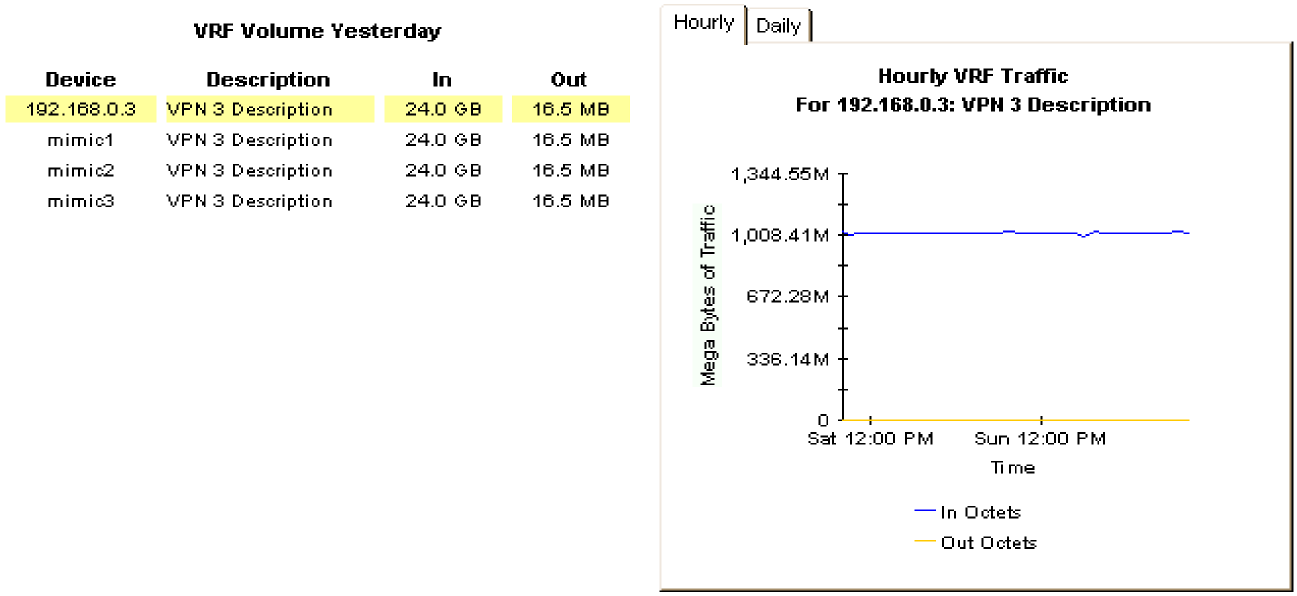
MPLS VPN Reporting

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 if.	Active if.	VRF Oper %	Volume	Exceptions
vpn3	Customer Unassigned	40	28	0.000	65.9 MB	U:384 D:0 E:0
vpn4	Customer Unassigned	4	0	100.000	6.4 GB	U:0 D:384 E:0
vpn6	Customer Unassigned	4	4	100.000	6.4 GB	U:0 D: E:
vpn7	Customer Unassigned	8	4	100.000	4.8 GB	U:0 D: E:
atime	Customer Unassigned	1	0	0.000	2.8 KB	U:0 D: E:
vpn5	Customer Unassigned	4	4	0.000	17.8 GB	U:0 D: E:
vpn1	Customer Unassigned	8	8	100.000	10.6 GB	U:0 D:768 E:0



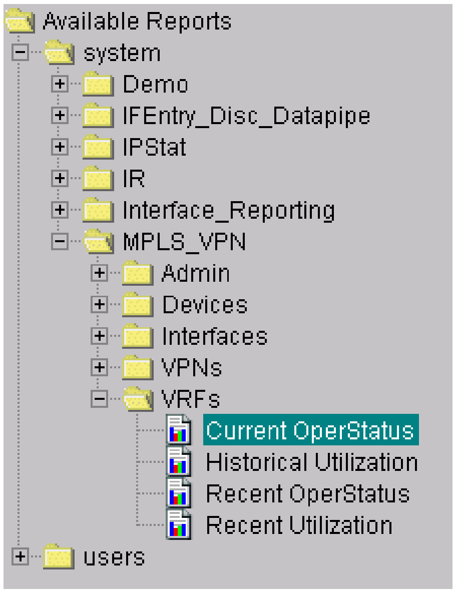
VRF Volume Yesterday

Device	Description	In	Out
192.168.0.3	VPN 3 Description	24.0 GB	16.5 MB
mimic1	VPN 3 Description	24.0 GB	16.5 MB
mimic2	VPN 3 Description	24.0 GB	16.5 MB
mimic3	VPN 3 Description	24.0 GB	16.5 MB

Hourly VRF Traffic
For 192.168.0.3: VPN 3 Description

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 are currently operationally up.

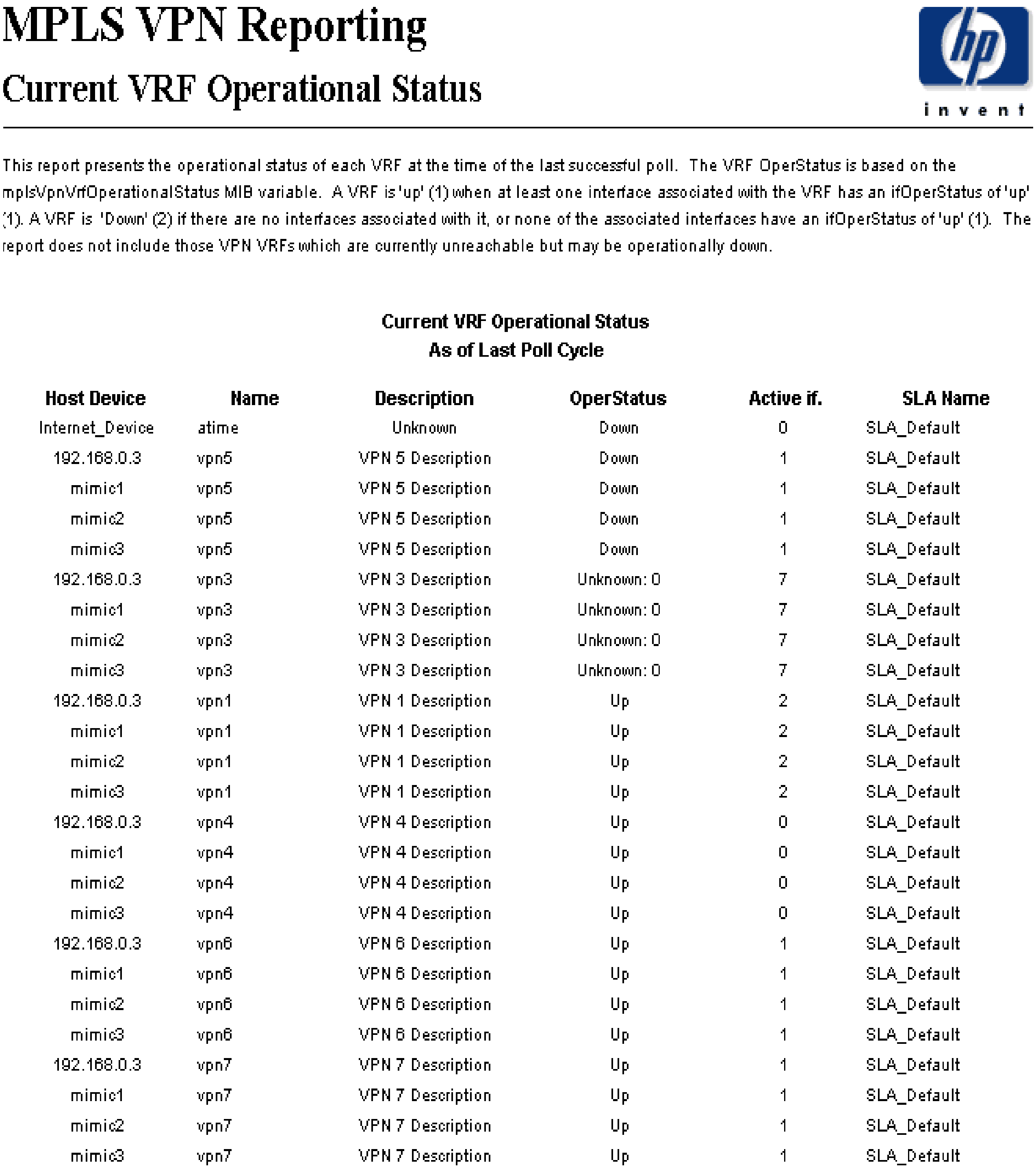
This is one of four reports in the VRFs folder. The reports in this folder focus on individual VRFs. A VRF is an instance of a VPN on a device. All VRFs with the same VPN name are considered part of a single VPN. Due to the real time nature of this report, it is suitable for use by operational network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

To filter this report, apply the following constraints:

- Device - The device name or IP address.

- VPN Name- The textual name for this VPN.

- SLA Name - The 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	vpn5	VPN 5 Description	Down	1	SLA_Default
mimic2	vpn5	VPN 5 Description	Down	1	SLA_Default
mimic3	vpn5	VPN 5 Description	Down	1	SLA_Default
192.168.0.3	vpn3	VPN 3 Description	Unknown: 0	7	SLA_Default
mimic1	vpn3	VPN 3 Description	Unknown: 0	7	SLA_Default
mimic2	vpn3	VPN 3 Description	Unknown: 0	7	SLA_Default
mimic3	vpn3	VPN 3 Description	Unknown: 0	7	SLA_Default
192.168.0.3	vpn1	VPN 1 Description	Up	2	SLA_Default
mimic1	vpn1	VPN 1 Description	Up	2	SLA_Default
mimic2	vpn1	VPN 1 Description	Up	2	SLA_Default
mimic3	vpn1	VPN 1 Description	Up	2	SLA_Default
192.168.0.3	vpn4	VPN 4 Description	Up	0	SLA_Default
mimic1	vpn4	VPN 4 Description	Up	0	SLA_Default
mimic2	vpn4	VPN 4 Description	Up	0	SLA_Default
mimic3	vpn4	VPN 4 Description	Up	0	SLA_Default
192.168.0.3	vpn6	VPN 6 Description	Up	1	SLA_Default
mimic1	vpn6	VPN 6 Description	Up	1	SLA_Default
mimic2	vpn6	VPN 6 Description	Up	1	SLA_Default
mimic3	vpn6	VPN 6 Description	Up	1	SLA_Default
192.168.0.3	vpn7	VPN 7 Description	Up	1	SLA_Default
mimic1	vpn7	VPN 7 Description	Up	1	SLA_Default
mimic2	vpn7	VPN 7 Description	Up	1	SLA_Default
mimic3	vpn7	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:

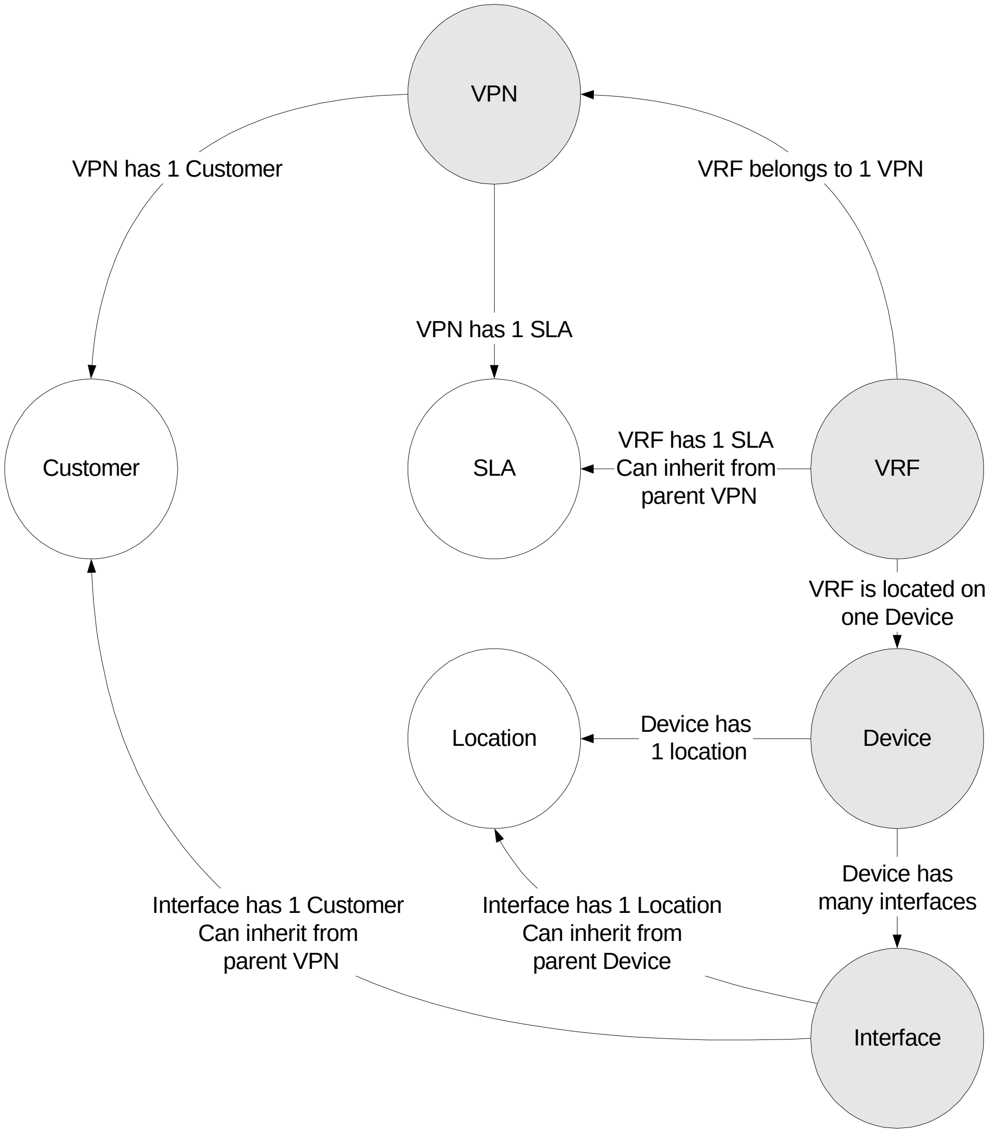
- VPN
- VRF
- SLA
- Interface (MPLS-enabled or VPN-associated)
- Device

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

Managed Element	**Associated Properties**
VPN	Customer Customer ID SLA
VRF	SLA
SLA	Operational% Interface availability Discard threshold

Managed Element	**Associated Properties**
Interface	See *Interface Reporting Report Pack 4.0 User Guide*
Device	See *Common Property Tables 3.5 User Guide*

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 come with the MPLS VPN Report Pack
- Create a property file and import the contents

If you chose 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 you 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

The interface is fundamental to the MPLS VPN Report Pack. The provisioning of interfaces is handled through the Interface Reporting Report Pack. As explained in the *Interface Reporting Report Pack 4.5 User Guide,* 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
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 which 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 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 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
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 in the Admin folder of Interface Reporting.

B

Editing Tables and Graphs

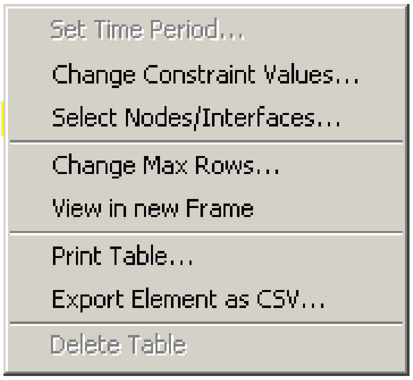
Any table or graph can be viewed in several ways. While the default view is usually adequate, you can easily change to a different view.

If you are using the Report Viewer application, right-click the object to display a list of view options. If you are looking at a report 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 a Table

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.

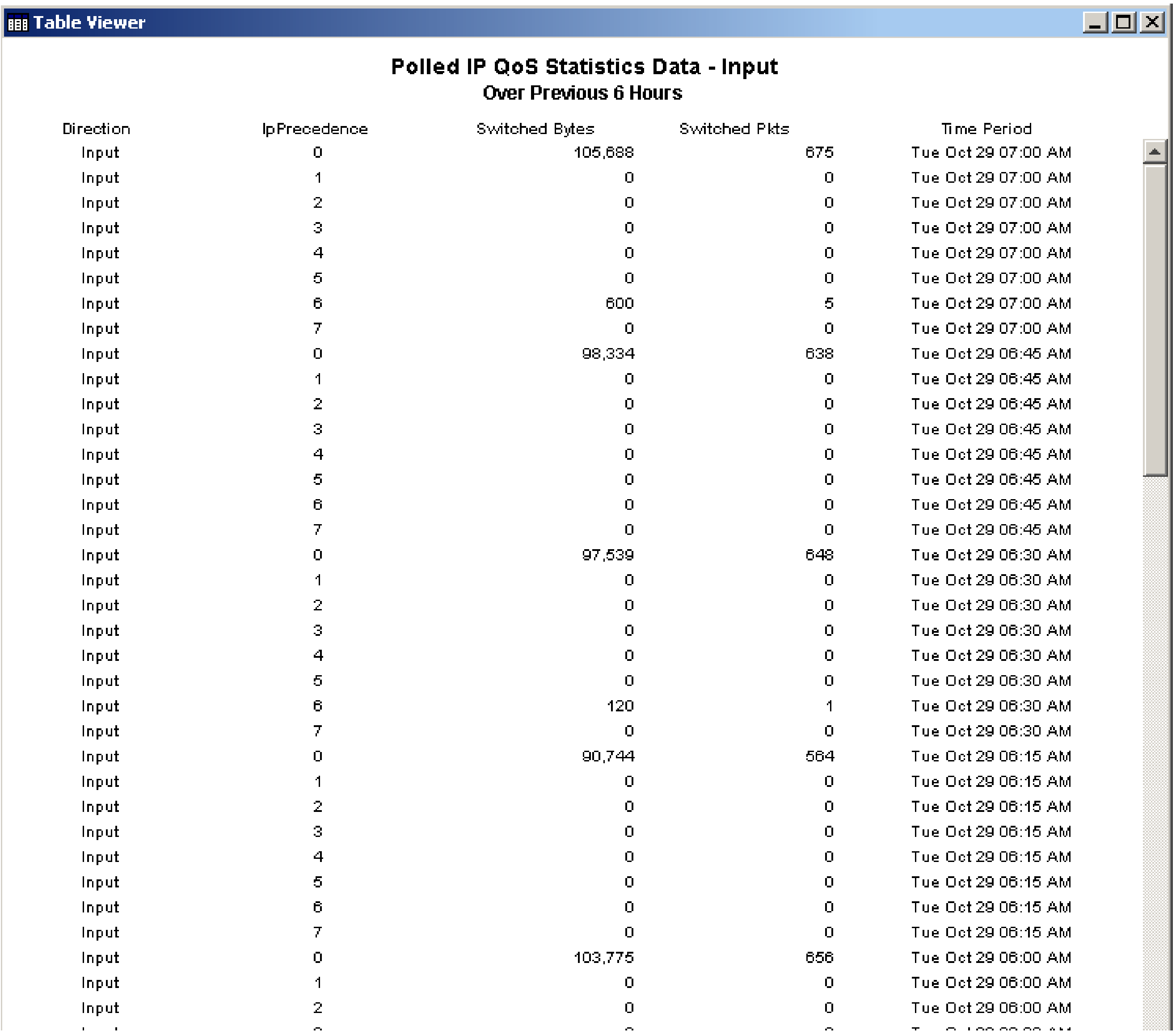
You may shorten the period of time covered by the table from, for example, 42 days to 30 days or to 7 days. If you are interested in a specific period of time that starts in the past and stops *before* yesterday, click **Use Absolute Time** and select a Start Time and an End Time.

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.



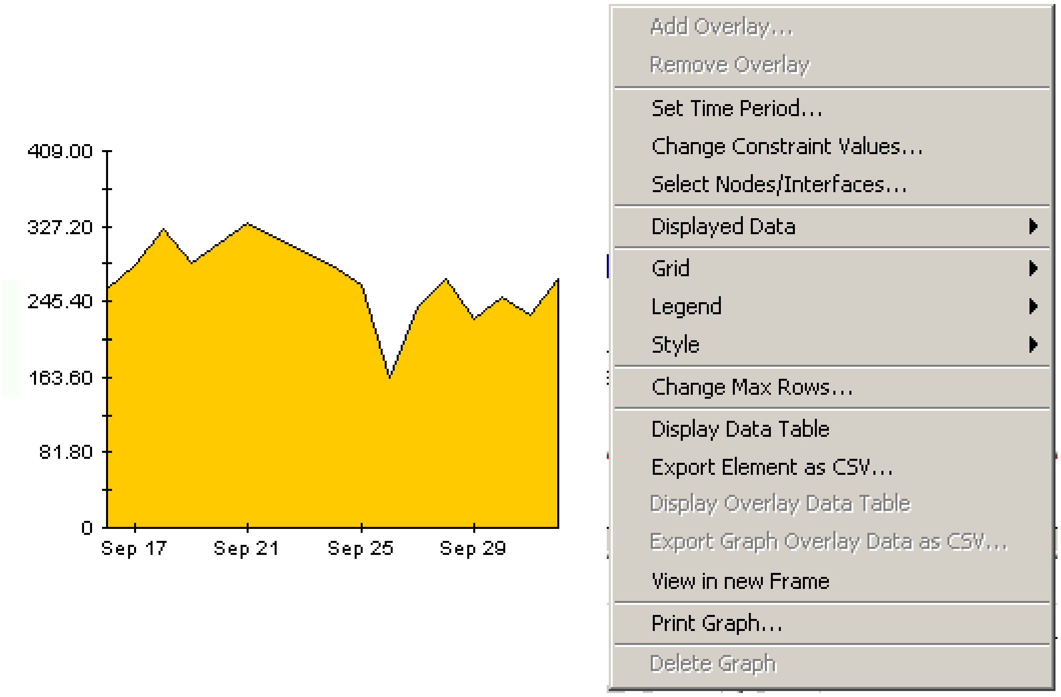
Polled IP QoS Statistics Data - Input

Over Previous 6 Hours

Direction	IpPrecedence	Switched Bytes	Switched Pkts	Time Period
Input	0	105,688	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
Input	5	0	0	Tue Oct 29 06:45 AM
Input	6	0	0	Tue Oct 29 06:45 AM
Input	7	0	0	Tue Oct 29 06:45 AM
Input	0	97,539	648	Tue Oct 29 06:30 AM
Input	1	0	0	Tue Oct 29 06:30 AM
Input	2	0	0	Tue Oct 29 06:30 AM
Input	3	0	0	Tue Oct 29 06:30 AM
Input	4	0	0	Tue Oct 29 06:30 AM
Input	5	0	0	Tue Oct 29 06:30 AM
Input	6	120	1	Tue Oct 29 06:30 AM
Input	7	0	0	Tue Oct 29 06:30 AM
Input	0	90,744	564	Tue Oct 29 06:15 AM
Input	1	0	0	Tue Oct 29 06:15 AM
Input	2	0	0	Tue Oct 29 06:15 AM
Input	3	0	0	Tue Oct 29 06:15 AM
Input	4	0	0	Tue Oct 29 06:15 AM
Input	5	0	0	Tue Oct 29 06:15 AM
Input	6	0	0	Tue Oct 29 06:15 AM
Input	7	0	0	Tue Oct 29 06:15 AM
Input	0	103,775	656	Tue Oct 29 06:00 AM
Input	1	0	0	Tue Oct 29 06:00 AM
Input	2	0	0	Tue Oct 29 06:00 AM

View Options for a Graph

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.



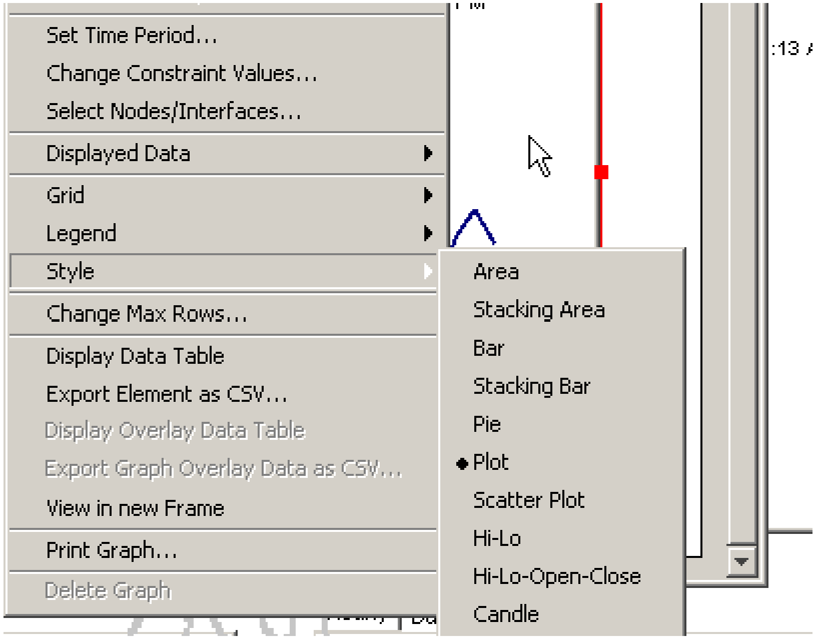
The following table provides details about each option.

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.

Option	Function
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.

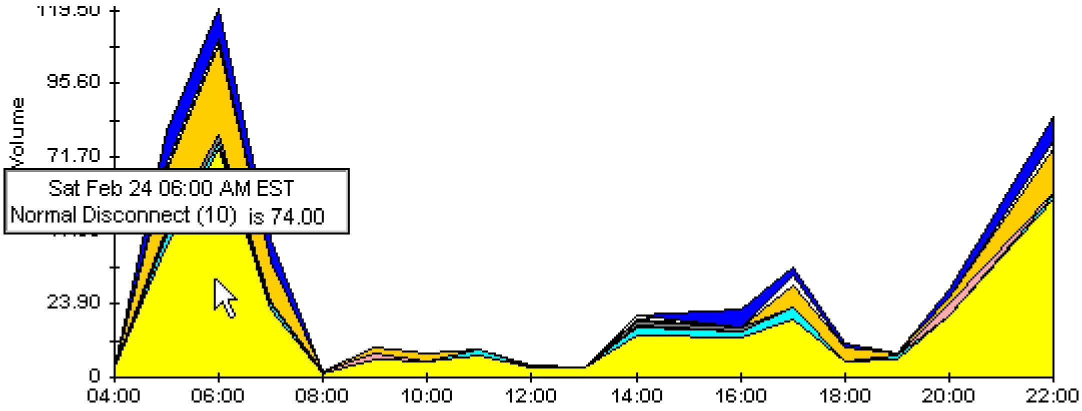
Style Options

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



Style > Area

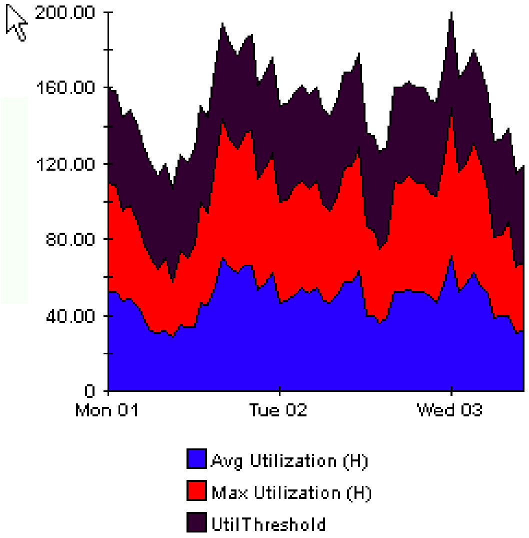
The plot or bar chart changes to an area graph. While relative values and total values are easy to view in this format, absolute values for smaller data types may be hard to see. Click anywhere within a band of color to display the exact value for that location



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.

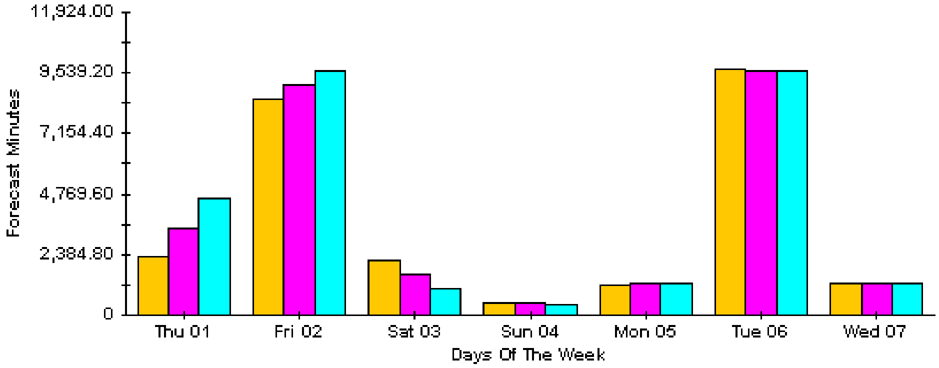
Style > Stacking Area

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



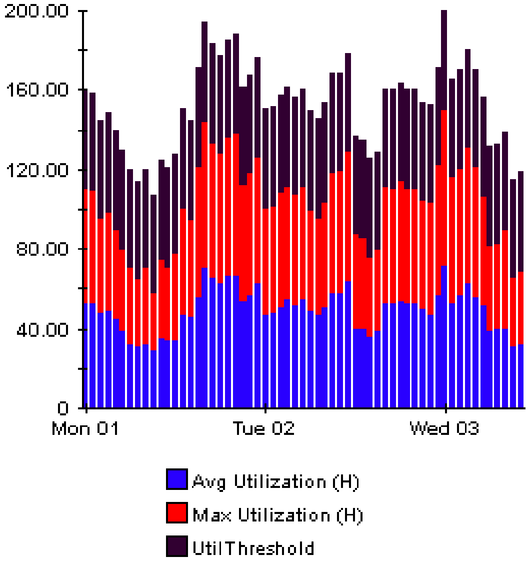
Style > Bar

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.



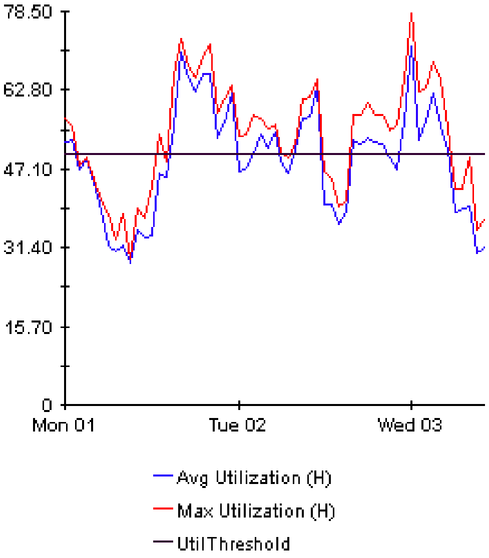
Style > Stacking Bar

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.



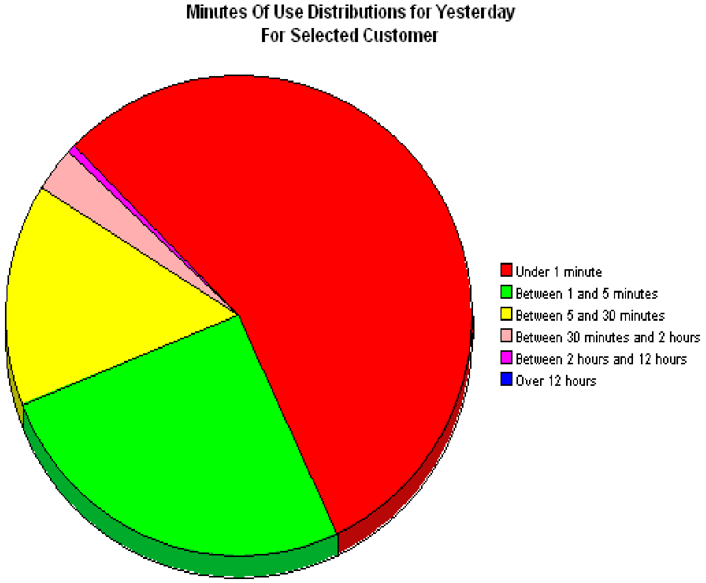
Style > Plot

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

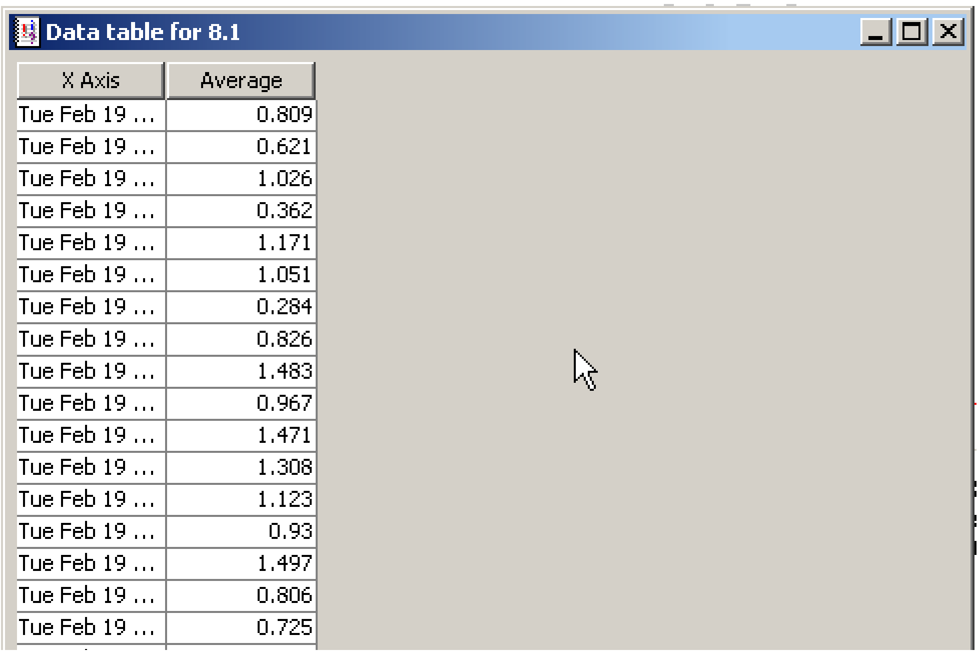
An area graph becomes a pie chart. Bands in an area graph convert to slices of a pie and the pie constitutes a 24-hour period. This view is helpful when a small number of data values are represented and you are looking at data for one day.



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

Display Data Table

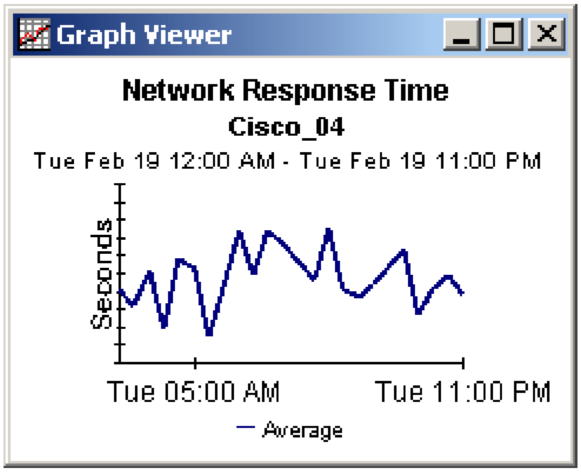
This option changes a graph into a spreadsheet.


Data table for 8.1

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

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