HP OpenView Performance Insight

Report Pack for MPLS VPN
User Guide

Software Version: 3.0

Reporting and Network Solutions

April 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 Company. Windows® is a U.S. registered trademark of Microsoft® Corp. UNIX® is a registered trademark of The Open Group.

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

Support

Please visit the HP OpenView Web site at:

http://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 chapter introduces Multi Protocol Label Switching (MPLS) and covers the following topics:

Introduction to MPLS

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 MPLS to forward packets over the backbone and Border Gateway Protocol (BGP) to distribute routes over the backbone.

Package Dependencies

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 the interface is configured as a VPN endpoint, it is known as a VRF.

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

- 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.

The MPLS VPN Datapipe collects data for the MPLS VPN Report Pack. This datapipe is currently the only means of data collection for the report pack. While the datapipe is not a prerequisite for the report pack, MPLS VPN reports will not contain any data until the datapipe is installed and running.

Features and Benefits

The MPLS VPN Report Pack will help you monitor service levels across multiple VPN networks. This package is easy to scale. 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 for Service Level Agreement (SLA) monitoring purposes
- 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

The MPLS VPN Report Pack supports interface re-indexing and directed-instance polling.

Enhancements in This Version

MPLS VPN version 3.0 provides support for Oracle as well as Sybase database software.

Report Folders and Report Objectives

This package contains 27 reports in the following folders:

- Admin (3)
- Devices (3)
- Interfaces (11)
- VPNs (6)
- VRFs (4)

Admin Contains two inventory reports and one VPN configuration report. These reports give you a sense of how the system is operating.

Devices Reports in this folder monitor recent MPLS and VPN activity at the device level, including route activity (changes and totals) across a device on an hourly and historical basis. If you used Common Property Tables to assign custom attributes to devices, those attributes will be automatically inherited by reports in the MPLS VPN Report Pack.

Interfaces Reports in this folder relate specifically to VPN-associated interfaces or MPLS-enabled interfaces. Use these reports to monitor performance and troubleshoot problems. For reporting on all network interfaces, regardless of use, see the Interface Reporting Report Pack. If you assigned customer and location attributes to the interfaces being monitored by the Interface Reporting Report Pack, those attributes will be inherited automatically.

VRFs Reports in this folder focus on recent and historical utilization across the VRF and its component interfaces. As explained in Appendix A, you may assign custom attributes to a VRF. The custom attributes are customer, location, and Service Level Agreement setting.

VPNs These reports cover route activity, volume, interface availability, and general summary information for VPNs as a whole. As explained in Appendix A, you may assign custom attributes to a VPN. The custom attributes are customer and Service Level Agreement setting.

The objectives of each report are outlined in the following table.

Grouping	Report	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.

Grouping	Report	Purpose
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.
	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.

Grouping	Report	Purpose
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.
	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.

Special Terms

The following table defines terms that appear in MPLS VPN reports.

Term	Definition
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.

Term	Definition
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	The textual name associated with the enumerated ifType of the interface.
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.

Ways to Customize Reports

You can customize the contents of a report by applying group filters, by importing customers and locations, by editing parameters, and by editing tables and graphs. When you apply a group filter, your goal is to change how the entire package appears to a particular group of users. If you edit a report, you are making a temporary change. For more information about editing tables and graphs, also known as selecting a different view option for tables and graphs, see Editing Tables and Graphs on page 67.

Group Filters

If you intend to share your reports with customers, or let divisions within your enterprise see division-specific performance data, you will want these reports to be customer-specific, containing data limited to one customer. Creating customer-specific reports is an administrator task that involves the following steps:

- Importing customers and locations using Common Property Tables 3.0
- Creating a group account for all of the users affiliated with a particular customer
- 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*.

Importing/Modifying Property Data

The reports in MPLS VPN will display property data at VPN-level, VRF-level, device-level, and general interface-level. For information on importing and modifying property data, see "Modifying Object Properties" on page 29 and "Provisioning Custom Attributes" on page 59.

Report Parameters

Editing a parameter applies a constraint. The constraint filters out the data you do not want to see. If you were to edit the Customer Name parameter, data for every customer except the customer you typed in the Customer Name field would drop from the report. Similarly, if you edited the Location Name, data for all locations except the location you typed in the Location Name field would drop from the report.

Filtering the contents of a report by editing parameters is completely optional and you may 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

Some reports support every parameter in this list, while most reports support a subset of this list. To edit parameters, click the **Edit Parameters** icon at the bottom right-hand corner of the report. When the Edit Parameters window opens, type the constraint in the field and then click **Submit**.

Sources for Additional Information

For information regarding the latest enhancements to MPLS VPN 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 4.0 User Guide*
- *Interface Discovery Datapipe 2.0 User Guide*
- *Interface Reporting ifEntry Datapipe 2.0 User Guide*
- *Thresholds Module 5.0 User Guide*
- *Integrating Performance Insight with Network Node Manager*
- *Reporting and Network Solutions 5.0 Release Notes*

The following documents are sources of information about OVPI, the platform that runs HP OpenView reporting solutions:

- *HP OpenView Performance Insight 5.0 Administration Guide*
- *HP OpenView Performance Insight 5.0 Installation Guide*
- *HP OpenView Performance Insight 5.0 Guide to Building and Viewing Reports*

Manuals for the platform are in two places: bundled with the HP OpenView Performance Insight CD, and posted to the following website:

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

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.

Each title under a product indicates the date of publication. The date comes from the manual's title page. Because new and updated user guides are posted to the web on a regular basis, always check for updates on the web before using an older PDF that may have been superceded.

2

Installing and Uninstalling MPLS VPN

This chapter covers the following topics:

Guidelines for a Smooth Installation

MPLS VPN 3.0 is part of Reporting and Network Solutions 5.0. The RNS 5.0 CD includes Network Node Manager (NNM) solution components as well as OVPI solution components. When you select OVPI solution components for installation, the install script copies every package to the Packages directory on your system. After the copy process is complete, the install script will prompt you to launch OVPI and run Package Manager. Before getting to that stage, you may want to be familiar with the following guidelines.

Software Prerequisites

The following software must already be in place before installing MPLS VPN 3.0:

- OVPI 5.0
- Any OVPI 5.0 Service Pack available for installation
- Common Property Tables Report Pack 3.0

You can find information about each Service Pack, including installation instructions, in the release notes distributed with the Service Pack.

Also, MPLS VPN requires the following software, which you can install at the time that you install MPLS VPN.

- Interface Reporting Report Pack 4.0
- Interface Discovery Datapipe 2.0
- Interface Reporting ifEntry Datapipe 2.0

> If you have installed a previous version of either or both of the datapipes listed above, you must remove the old version from your system before installing the latest version. This procedure is described in Task 3: Uninstall Datapipes (if necessary) on page 20.

The Threshold and Event Generation Module (hereafter referred to as the Thresholds Module) is optional. If you use this module, you must have at least version 3.0. The latest version, 5.0, is recommended.

Distributed Environments

If you are planning to install MPLS VPN in a distributed environment, keep these requirements in mind:

- The central server, every satellite server, and every remote poller must be running OVPI 5.0 and all available Service Packs.
- Before installing MPLS VPN and its associated packages on any server, central or satellite, uninstall these packages if they are currently installed:
  - Any Interface Discovery Datapipe version prior to 2.0
  - Any Interface Reporting ifEntry Datapipe version prior to 2.0

Upgrading Common Property Tables

MPLS VPN 3.0 requires Common Property Tables version 3.0.

- If you are not currently running any version of Common Property Tables, simply let Package Manager install the correct version for you.
- If you are running an older version of Common Property Tables, upgrade to the appropriate version by installing the appropriate upgrade package. Do this *before* installing or upgrading the MPLS VPN Report Pack.

Installing the upgrade package(s) for Common Property Tables is easy, but if you need assistance with the installation or if you want to know more about how this package operates, refer to the *Common Property Tables 3.0 User Guide*.

Integration with NNM: Threshold Alarms

If you have already integrated OVPI with NNM, you will probably want to install the optional thresholds sub-package, MPLS_VPN_Threshold, on the OVPI server. If this package is installed, threshold breaches spotted by OVPI will appear in the NNM alarm browser, allowing the NNM operator to launch an MPLS VPN report.

The thresholds sub-package cannot operate unless the Threshold and Event Generation Module, commonly known as the Thresholds Module, is also installed. You may be running the previous version of the Thresholds Module. If you are running the previous version, you have the option of upgrading to the latest release.

For more information about recent enhancements to the Thresholds Module, refer to the *Thresholds Module 5.0 User Guide*.

Prerequisite Tasks for Upgrade or Installation

Complete the following tasks before upgrading or installing the MPLS VPN Report Pack:

Task 1: Extract the Packages

To extract the MPLS VPN Report Pack packages from the RNS CD to the Packages directory on your system, do the following:

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.

5 Do one of the following:

- If you want to upgrade MPLS VPN now, complete tasks 2 and 3, then go to Procedure for Upgrading Packages on page 22.
- If you want to install MPLS VPN for the first time now, go to Procedure for a New Installation on page 23.
- If you do not want to install or upgrade at this time, go to Step 6.

6 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`**

After 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. Reports in the demo package are interactive; tables are linked to graphs, and you may experiment with editing parameters, tables, and graphs.

Task 2: Upgrade to Common Property Tables 3.0

The MPLS VPN Report Pack requires Common Property Tables 3.0. Upgrade to Common Property Tables 3.0 *before* upgrading the MPLS VPN Report Pack. If you need help with the upgrade, refer to the *Common Property Tables 3.0 User Guide*.

If this is a new installation of the MPLS VPN Report Pack, install Common Property Tables 3.0 with the report pack. (This task is described in Procedure for a New Installation on page 23.)

Task 3: Uninstall Datapipes (if necessary)

If you already have an older version of one or more datapipes that you want to upgrade, you must first uninstall the old version. The following procedure explains how to remove an old version of a datapipe. You can install the latest version of any datapipe when you install or upgrade the report pack, as explained later in this chapter.

To remove the old version of a datapipe, do the following:

1. Log in to the system. On UNIX systems, log in as root.
2. If it is not already stopped, stop OVPI Timer and wait for processes to stop running.

   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/opvi_timer stop`**
3. Start Package Manager.

   a. Launch OVPI and select **Management Console**.
   b. Select **Tools > Package Manager**.

      The Package Manager Welcome window opens.
4. Click **Next**.

   The Packages Location window opens.
5. Click the **Uninstall** button and click **Next**.

   The Report Undeployment window opens.
6. Click **Next**.

   The Package Selection window opens.
7. Click the check box next to any of the following datapipes that are currently installed:

   - MPLS_VPN_Datapipe
   - Interface_Discovery_Datapipe
   - IRifEntry_Datapipe
8. Click **Next**.

   The Selection Summary window opens.
9. Click **Uninstall**.

   The Progress window opens. When removal is complete, a message appears.
10. Click **Done** to return to the Management Console.

Now that you have completed the prerequisite tasks, do one of the following:

- To upgrade the MPLS VPN Report Pack, go to Procedure for Upgrading Packages below.
- To install the MPLS VPN Report Pack for the first time, go to Procedure for a New Installation on page 23.

Procedure for Upgrading Packages

You must complete the tasks in Prerequisite Tasks for Upgrade or Installation on page 19 before beginning the following procedure. If Package Manager is already running, begin this procedure at Step 5.

1. Log in to the system. On UNIX systems, log in as root.
2. If your system is distributed, disable trendcopy.
3. Launch OVPI and select **Management Console**.
4. From the Tools menu, select **Package Manager**.

   The Package Manager Welcome window opens.
5. Click **Next**.

   The Packages Location window opens.
6. Click the **Install** button.
7. Approve the default installation directory or select a different directory if necessary. .
8. Click **Next**.

   The Report Deployment window opens.
9. Type your username and password for the OVPI Application Server.
10. Click **Next**.

    The Package Selection window opens.
11. Click the check box next to each of the following packages:
    - UPGRADE_MPLS_VPN_2.0_to_3.0
    - MPLS_VPN_Threshold
    - MPLS_VPN_Datapipe
    - IR_ifEntry_Datapipe_2.0
    - Interface_Discovery_Datapipe_2.0
    - Interface_Reporting_4.0 (if not already installed)
    - MPLS_VPN_Demo (optional)
12. Click **Next**.

    The Type Discover window opens.
13. To run Discover immediately after package installation, accept the default and click **Next**.

    The Selection Summary window opens.
14. Verify that the contents of this window are correct and click **Install** to begin the installation process.

    The Installation Progress window opens. When installation is complete, a message appears.
15. Click **Done** to return to the Management Console.

16 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`**

Procedure for a New Installation

You must complete the tasks in Prerequisite Tasks for Upgrade or Installation on page 19 before beginning the following procedure. If Package Manager is already running, begin this procedure at Step 5.

1 Log in to the system. On UNIX systems, log in as root.

2 If your system is distributed, disable trendcopy.

3 Launch OVPI and select **Management Console**.

4 From the Tools menu, select **Package Manager**.

The Package Manager Welcome window opens.

5 Click **Next**.

The Packages Location window opens.

6 Click the **Install** button.

7 Approve the default installation directory or select a different directory if necessary.

8 Click **Next**.

The Report Deployment window opens.

9 Type your username and password for the OVPI Application Server.

10 Click **Next**.

The Package Selection window opens.

11 Click the check box next to each of the following packages:

- MPLS_VPN
- MPLS_VPN_Threshold
- MPLS_VPN_Datapipe
- Interface_Reporting_ifEntry_Datapipe_2.0
- Interface_Discovery_Datapipe_2.0
- Interface_Reporting_4.0 (if not already installed)
- MPLS_VPN_Demo (optional)

12 Click **Next**.

The Type Discover window opens.

13 To run Discover immediately after package installation, accept the default and click **Next**.

The Selection Summary window opens.

14 Verify that the contents of this window are correct, then click **Install** to begin the installation process.

The Installation Progress window opens. When installation is complete, a message appears.

15 Click **Done** to return to the Management Console.

16 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`

Most report packs include a demo package. The demo package is independent of other packages and can be installed at any time. Demo reports are static; the data does not change from day to day, but the linking works. Tables are linked to graphs, and you can experiment with various options for viewing tables and graphs.

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.

You can check this by examining 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 customer and location information.

For information on importing and modifying property data, see Modifying Object Properties on page 29 and Provisioning Custom Attributes on page 59, which includes information about property attributes, the format of your property import file, and the defaults that control file locations and scheduling.

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 you depend on the way OVPI was installed. If the client component is installed on your system, you have access to Report Viewer, Report Builder, and the Management Console. If the client component was not installed on your system, use the Web Access Server 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*.

Procedure for Uninstalling Packages

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 Report Pack and any datapipe that depends on the report pack:

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.
4. From the Tools menu, select **Package Manager**.

   The Package Manager Welcome window opens.
5. Click **Next**.

   The Packages Location window opens.
6. Select the **Uninstall** button and click **Next**.

   The Report Undeployment window opens.
7. Keep the defaults and click **Next**.

   The Package Selection window opens.

8 Click the check box next to the following packages:

- MPLS_VPN
- MPLS_VPN_Datapipe
- MPLS_VPN_Thresholds (if installed)
- 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 message appears.

11 Click **Done** to return to the Management Console.

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

Configuring MPLS VPN

This chapter covers the following topics:

Configuring Distributed Systems

If you deploy MPLS VPN in a distributed architecture, you must modify the central server and each satellite server. You may also need 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 a 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

Follow these steps to configure a satellite server.

1. If you do not intend for this system to produce reports, switch off unnecessary processing. That is, disable MPLS VPN daily and monthly processing by removing the entry in $DPIPE_HOME/lib/trendtimer.sched referencing MPLS_DMF_Process.pro.
2. Make sure that the system clock is synchronized with the system clock on the central server and the system clock on all other satellite servers. This is extremely important when linked processes are executing in exact sequences across independent machines.

Administrative Utilities

The MPLS VPN Report Pack includes two additional utilities that an administrator or technical support person may find helpful:

- Installation verification
- Table backup

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.

4

Modifying Object Properties

This chapter covers the following topics:

Objects and Object Models

OVPI includes functionality that enhances your ability to visualize the objects on your network. The term "object" refers to any item that can appear on a report with accompanying performance or property information.

Examples of object categories are Devices, Customers, and Locations. These three object categories are included in the system by default. Click on **Objects** in the Management Console to see the managed object tree structure of the objects currently monitored by your OVPI system.

Each report pack will include the ability to monitor and report on new objects. How these objects relate to those already understood by the OVPI system is included within the configuration of the report pack. For this reason, you may see the default object model change when you load new report packs. An example of this is the inclusion of Interfaces as a branch under Devices in the object tree after you load the Interface Reporting Report Pack. Selecting an object in the tree will cause the windows to the right of the application to refresh with tasks and reports specific to the selected managed object.

In some cases, the report pack includes whole new classes of objects or services that do not fit within the default model. In this case the report pack will include a new view (tree hierarchy), which will be available from the **View > Change View** menu drop-downs.

In the case of the MPLS VPN Report Pack, there is a new view tailored to VPNs and their VRFs called **Mpls Vpn model**. The object tree hierarchy for this view is as follows:

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

Property information configured at any level of the tree will "trickle down" to the lower levels. For example, setting a Customer against an MPLS VPN will apply the Customer to all interfaces in that VPN that have not already had their Customer set differently.

Updating Property Data

The reports in MPLS VPN will display property data at device-level, generic interface-level, VPN-level, and VRF-level.

- Device-level property data is inherited from Common Property Tables. To update device-level property data, use the update forms that come with Common Property Tables.
- Generic interface-level property data is inherited from Interface Reporting. To update interface-level property data, you can either import a file that contains your updates or use the property update forms that are included with the MPLS VPN Report Pack.
- To update VRF/VPN-level property data, you can either import a file that contains your updates or use the property update forms that are included with the MPLS VPN Report Pack.

The import file method is described in Provisioning Custom Attributes on page 59. The property update forms are described below.

Using Forms to Add Property Information to Reports

MPLS VPN provides several forms that make it easy to update properties. (Note: You may still wish to import property data in a batch file if you have large sets of changes or have an automated import mechanism configured from another application.) Use these forms to:

- Create MPLS VPN Service Level Agreement (SLA) configuration details
- Change MPLS VPN SLA configuration settings
- Change the customer and SLA name of each known VPN
- Assign a new name to the VPN
- Assign new SLA settings to individual VRFs

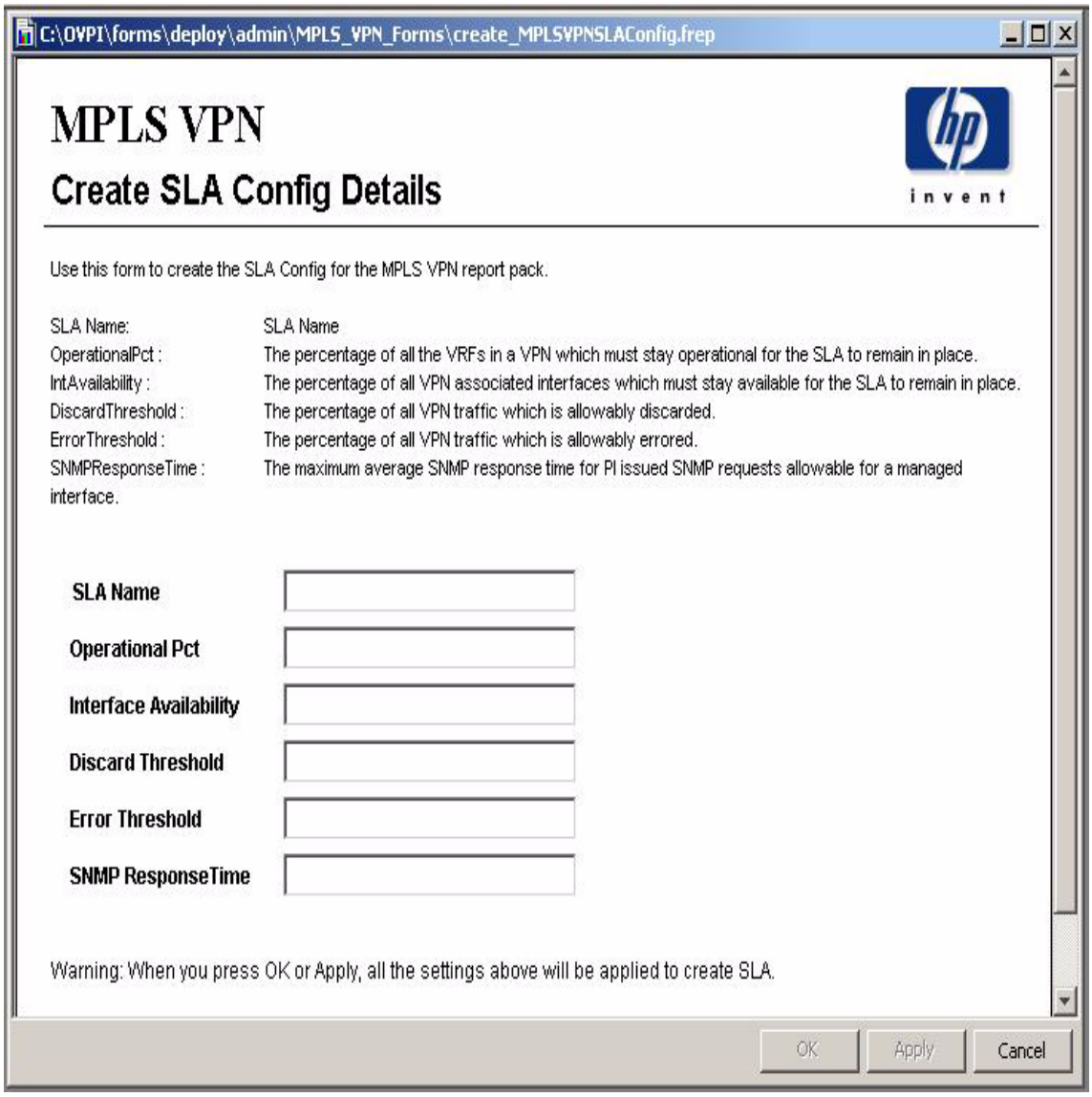
Creating MPLS VPN SLA Configurations

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. These metrics can be combined into a single Service Level Agreement (SLA) and applied to the entire VPN or to individual VRFs.

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

1. In the Management Console, click the **Objects** icon.
2. Select **File > New**.
3. Select **Create MPLS VPN SLA** and click **Create**.

The form opens.



4 Enter the appropriate data in each field in the form. Details about the field are given in the form text.

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

Changing MPLS VPN SLA Configuration Settings

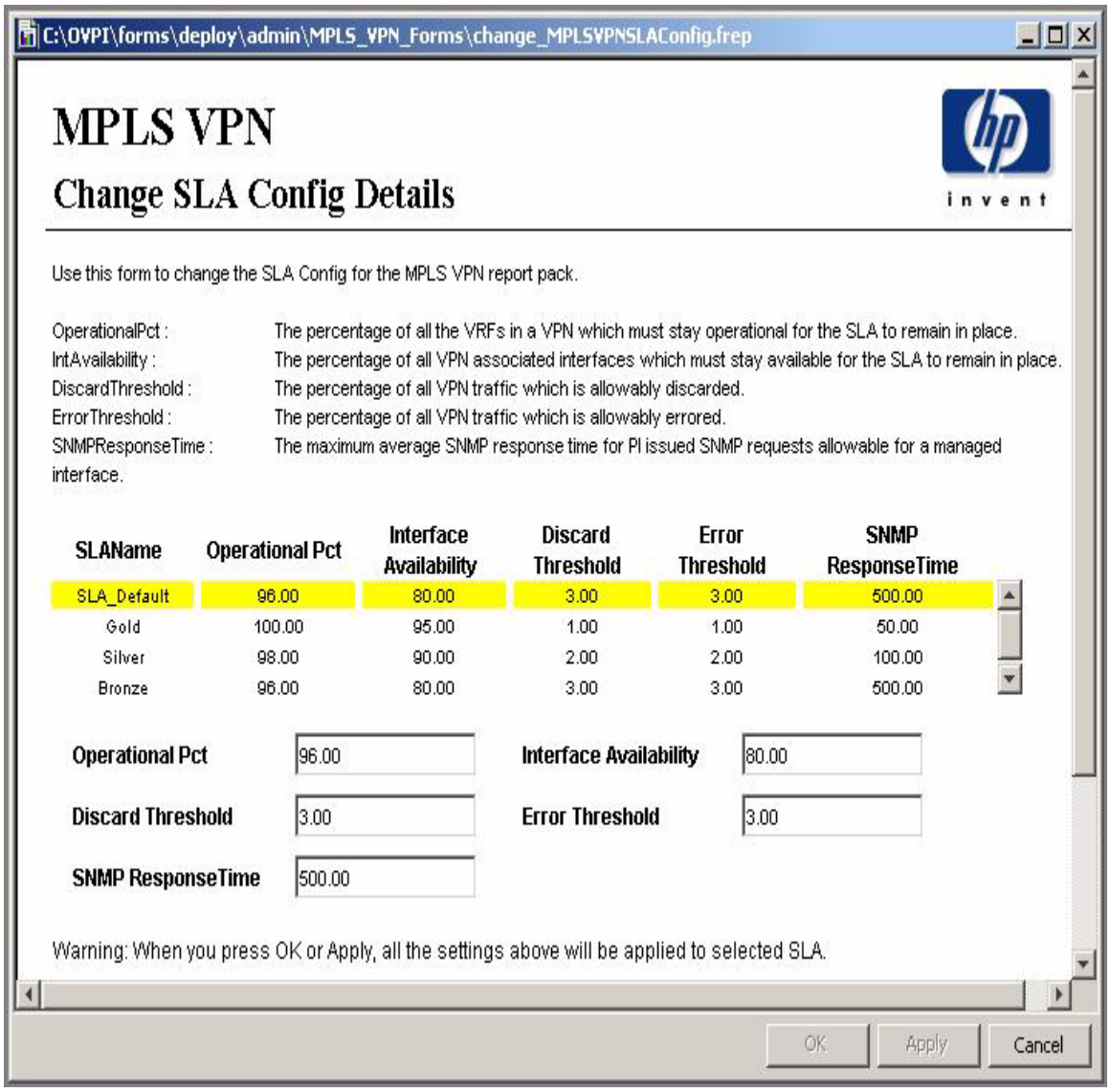
SLA details do not relate to a managed object directly; they are applied to a managed object. For this reason the Change MPLS VPN SLA Configuration form always appears in the General Tasks window when any object is selected. Follow these steps to open the form and change the SLA Configuration details:

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

2 Select any object in the model.

3 In the list of General Tasks, double-click **Change SLA Config**.

The form opens.



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.

Changing MPLS VPN Customer and SLA Name

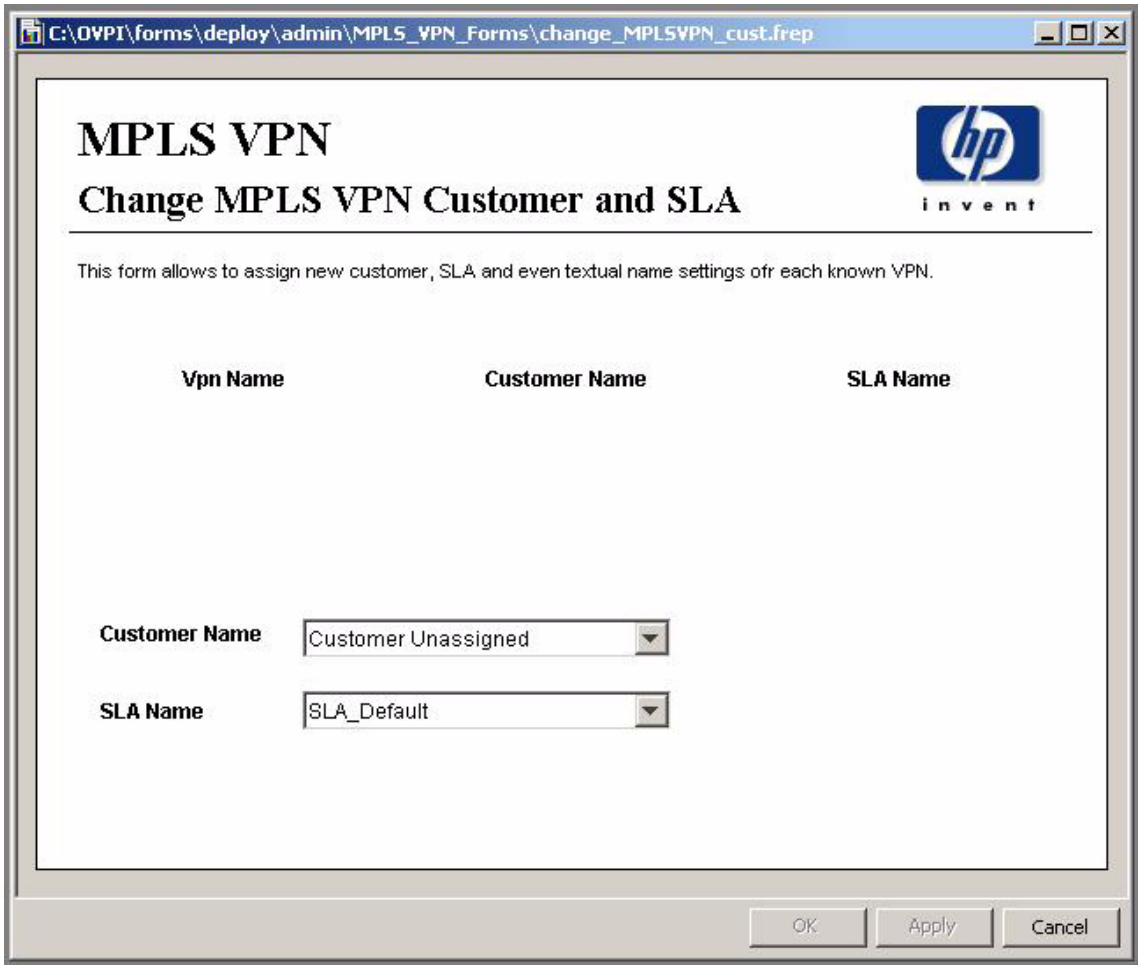
The form described in this section allows you to modify the customer and SLA name assigned to a VPN. Before using this form to modify customer information, you must create customer entries by using the import file mechanism that comes with the Common Property Tables package or the “create new” forms that are also included with that package. For details, refer to the *Common Property Tables User Guide*.

SLAs must be created for the first time by using the “create new” form that comes with this package or by using the import file mechanism. For details, refer to Creating MPLS VPN SLA Configurations on page 30 or Provisioning Custom Attributes on page 59.

Follow these steps to open the form and update the customer and SLA name assigned to the MPLS VPN:

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**.

   The form opens.



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

Changing a VPN Name

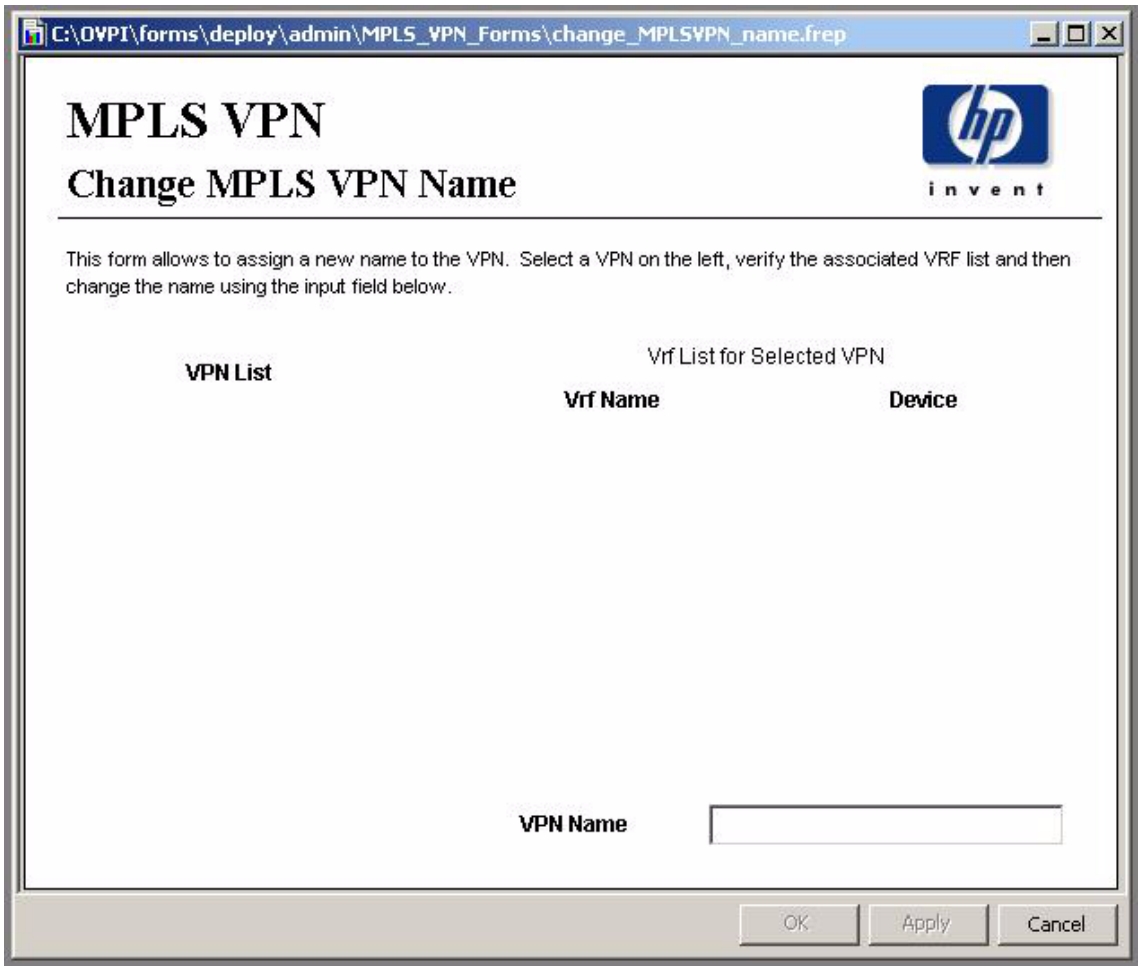
The system attempts to assign a meaningful name to each discovered group of VRFs, using the following rules:

- If this 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 if one or more VRFs are seen to 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, as explained in the following steps:

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**.

The form opens.



6 Follow the instructions on the form to 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.

Updating VPN VRF SLA Settings

SLAs must be created for the first time by using the “create new” form that comes with this package or by using the import file mechanism. For details, refer to the Creating MPLS VPN SLA Configurations on page 30 or to Provisioning Custom Attributes on page 59.

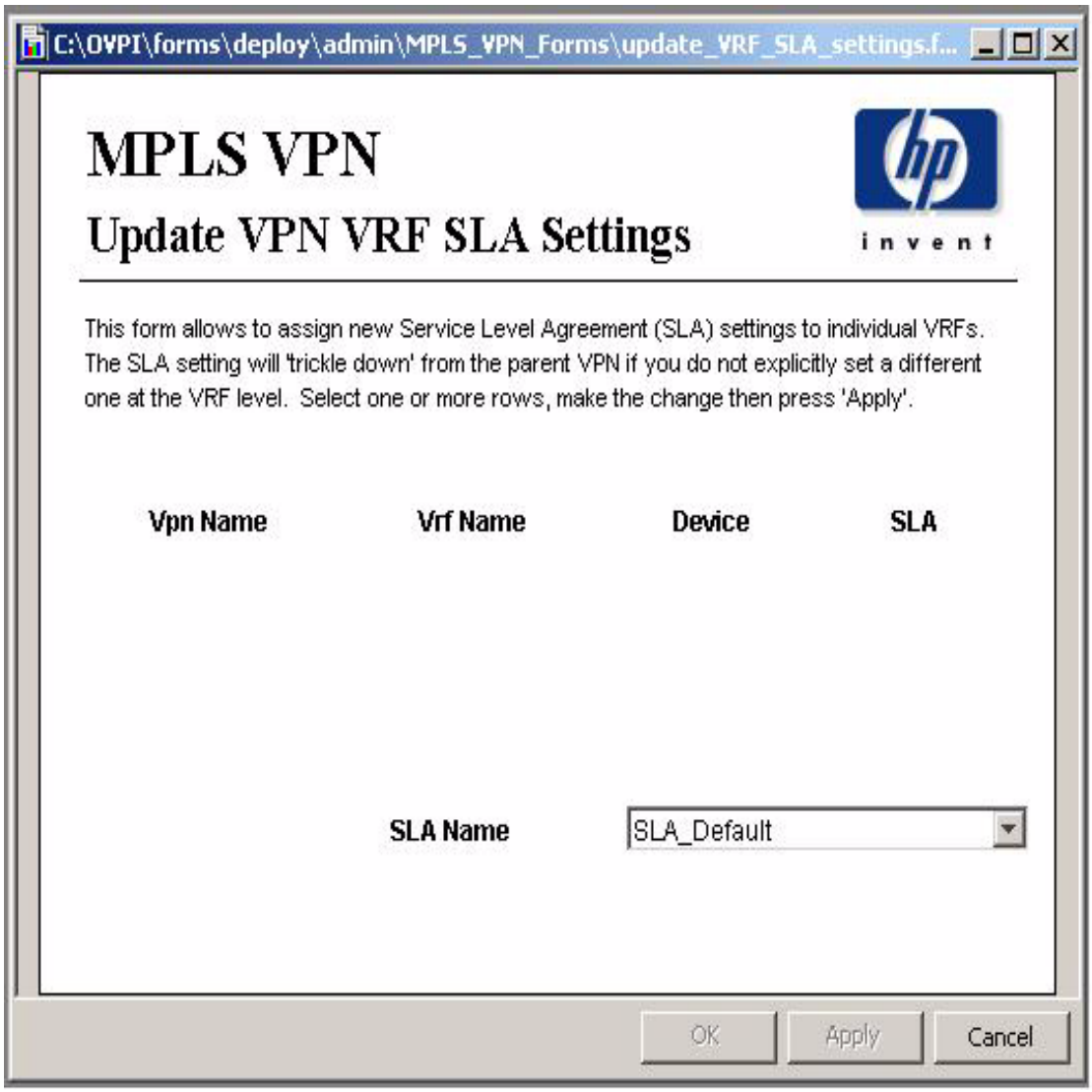
Follow these steps to open the form and assign new SLA settings to the VPN VRF:

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.**

The form opens.



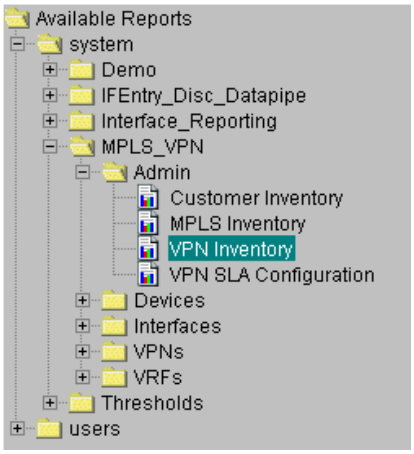
4 Assign a new SLA VPN VRF using the **SLA Name** drop-down selection list.

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 administrative report to quickly 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 parameters:

- 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

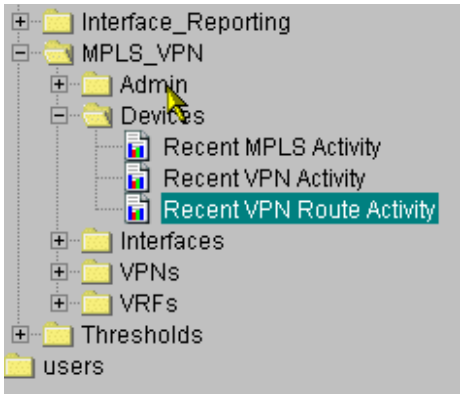
Associated Interfaces for mimic1: VPN 1 Description

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 parameters:

- 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 | Daily

Hourly Route Activity for mimic1

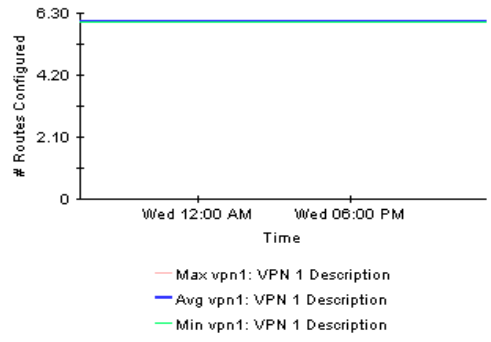
Time Period	Max VRF Routes	# Routes	Volume Out	Cnfgd Vrfs	Active Vrfs
Thu Oct 10 10:00:00 BST 2002	2000	92	434.1 MB	6	4
Thu Oct 10 09:00:00 BST 2002	2000	92	121.6 MB	6	4
Thu Oct 10 08:00:00 BST 2002	2000	92	105.3 MB	6	4
Thu Oct 10 07:00:00 BST 2002	2000	92	320.4 MB	6	4
Thu Oct 10 06:00:00 BST 2002	2000	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



Devices Supporting VPNs
Sorted by Current Number of Routes

	Device	Cust Id	Customer	Cnfgd Vrfs	Active Vrfs	Cnctd Int	Max Routes	# Routes
X	mimic2	2	Customer 2	6	4	4	2000	92
X	mimic25	-2	Customer Unassigned	6	4	4	2000	92
	mimic1	-2	Customer Unassigned	6	4	4	2000	92
	mimic3	3	Customer 3	6	4	4	2000	92
	mimic4	4	Customer 4	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

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.

Hourly | Daily

Hourly Route Activity for mimic2

Time Period	Max VRF Routes	# Routes	Volume Out	Cnfgd Vrfs	Active Vrfs
Thu Oct 10 10:00:00 BST 2002	2000	92	434.4 MB	6	4
Thu Oct 10 09:00:00 BST 2002	2000	92	121.7 MB	6	4
Thu Oct 10 08:00:00 BST 2002	2000	92	105.2 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	493.2 MB	6	4
Thu Oct 10 02:00:00 BST 2002	2000	92	487.2 MB	6	4

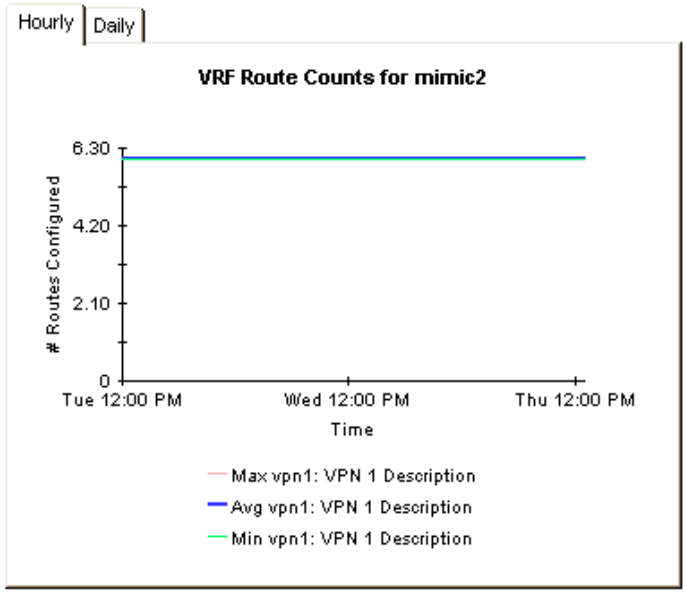
The central tabbed area provides an instant historical record of routing changes on the device and how they compare with total volume placed on the backbone by this VRF, the number of configured and of active VRFs. Time periods available are Hourly and Daily.

"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

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



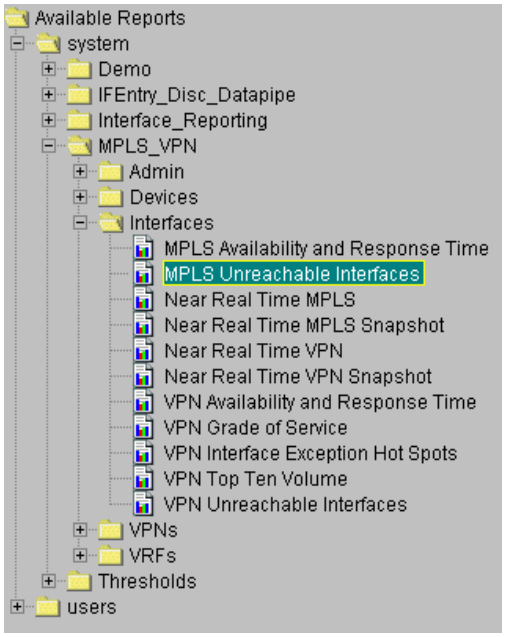
The lowest section of the report depicts information on a per-VRF basis. The selection of VRFs displayed is driven by the device selection table at the top. As with the device selection, if data has not been aggregated for a VRF, for any reason, within the last two hours then an X will appear to the 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.



There are eleven reports in the interfaces folder. All of them 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.

The list of unreachable MPLS interfaces can be modified 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.

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
mimic288	6.0	Up	Location Unassigned	F	other	In: 10.0 Mb/s Out: 10.0 Mb/s	69
mimic289	5.0	Up	Location Unassigned	F	other	In: 1.0 Mb/s Out: 1.0 Mb/s	69
mimic289	6.0	Up	Location Unassigned	F	other	In: 10.0 Mb/s Out: 10.0 Mb/s	69
mimic290	5.0	Up	Location Unassigned	F	other	In: 1.0 Mb/s Out: 1.0 Mb/s	69
mimic290	6.0	Up	Location Unassigned	F	other	In: 10.0 Mb/s Out: 10.0 Mb/s	69
mimic291	5.0	Up	Location Unassigned	F	other	In: 1.0 Mb/s Out: 1.0 Mb/s	69
mimic291	6.0	Up	Location Unassigned	F	other	In: 10.0 Mb/s Out: 10.0 Mb/s	69
mimic292	5.0	Up	Location Unassigned	F	other	In: 1.0 Mb/s Out: 1.0 Mb/s	69
mimic292	6.0	Up	Location Unassigned	F	other	In: 10.0 Mb/s Out: 10.0 Mb/s	69
mimic293	5.0	Up	Location Unassigned	F	other	In: 1.0 Mb/s Out: 1.0 Mb/s	69
mimic293	6.0	Up	Location Unassigned	F	other	In: 10.0 Mb/s Out: 10.0 Mb/s	69
mimic294	5.0	Up	Location Unassigned	F	other	In: 1.0 Mb/s Out: 1.0 Mb/s	69
mimic294	6.0	Up	Location Unassigned	F	other	In: 10.0 Mb/s Out: 10.0 Mb/s	69
mimic295	5.0	Up	Location Unassigned	F	other	In: 1.0 Mb/s Out: 1.0 Mb/s	69
mimic295	6.0	Up	Location Unassigned	F	other	In: 10.0 Mb/s Out: 10.0 Mb/s	69

This list of interfaces can be filtered by applying the following parameters:

- 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.

8

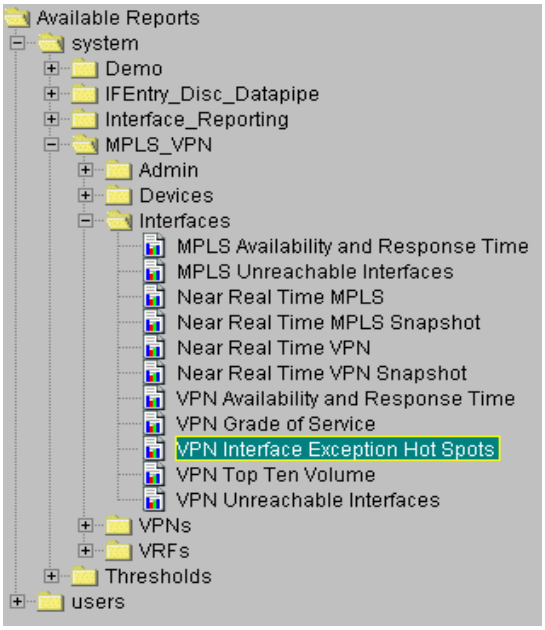
VPN Interface Exception Hot Spots

Use the VPN Interface Exception Hot Spots report to display every VPN-associated interface that experienced at least one exception yesterday. Any interface shown here broke a pre-set threshold sometime during the previous day.

The historical analysis contained in this report is intended to help you find out whether an exception occurring yesterday is a normal or abnormal condition.

This report is one of eleven in the Interfaces folder. All reports in this 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 those interfaces which are of interest to users in the MPLS/ VPN-oriented community.

Selecting an interface from the list at the top populates the exception, utilization, error and discard ratio graphs. Note how the tabs in the middle right section of the report focus on Utilization, Discard, or Error rates.



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

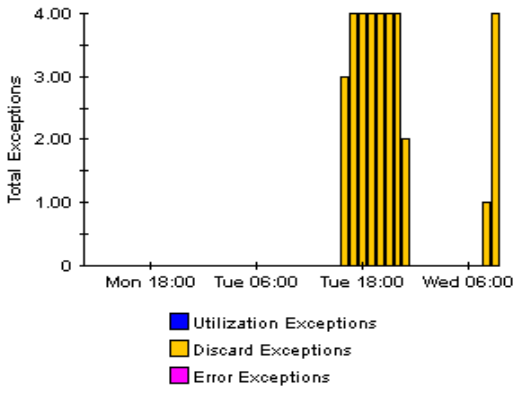
Sorted by Exception Count

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

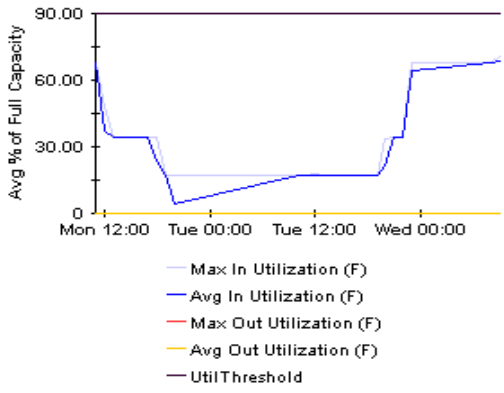
Hourly | Daily | Monthly

Exception Counts for 192.168.0.3: Ethernet1/3



Utilization | Discards | Errors

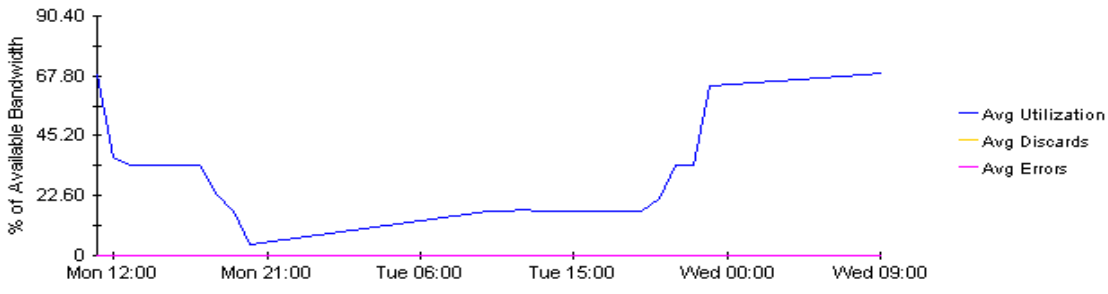
Utilization for 192.168.0.3: Ethernet1/3



Inbound | Outbound | Both (Half Duplex Only)

Average Inbound Utilization, Discards and Errors for 192.168.0.3: Ethernet1/3

% of Available Bandwidth



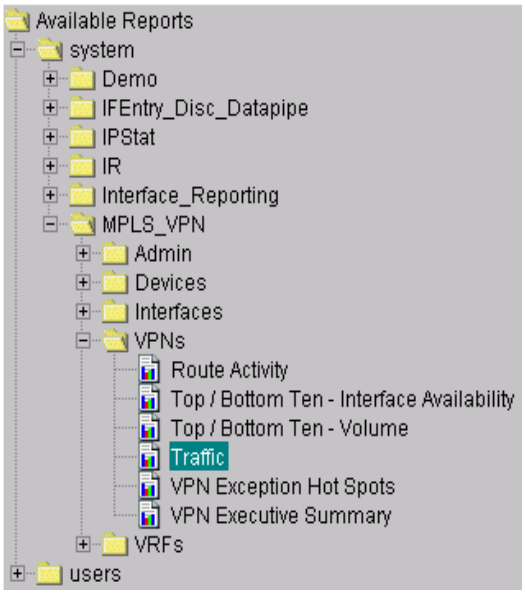
The tabs on the lowest graph combine all three metrics and split the traffic into either inbound or outbound components where applicable. The thresholds displayed in this report are stored on a per-interface basis and are used to generate exceptions and, potentially, to external events using the Thresholds Module. See the Interface Reporting User Guide for more details on how to populate or modify these values.

You can filter this report by applying the following parameters:

- 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).

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. All 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.

Select a VPN from the top table and view the component VRF utilization and volume figures.

Note that the selection tables are displaying yesterday's aggregated data for the VPN.

MPLS VPN Reporting

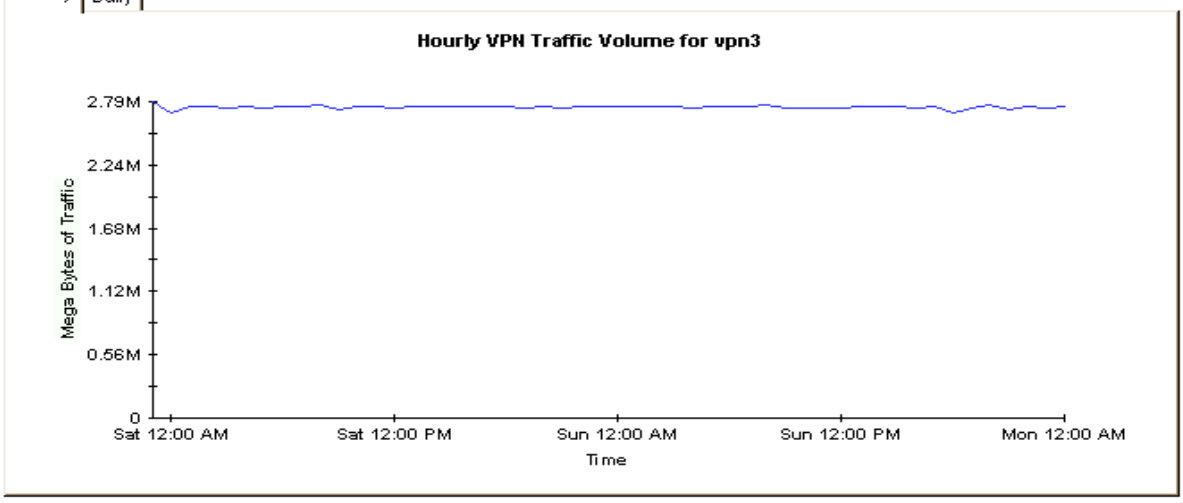
VPN Traffic Volume

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

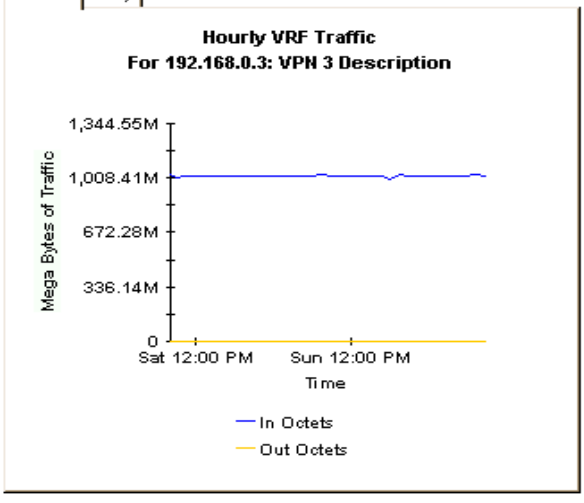
Hourly | Daily



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 | Daily



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.

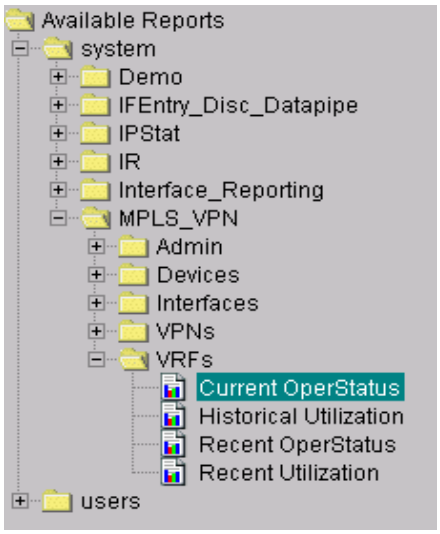
Exceptions are generated at the interface level and are dependent upon the individual thresholds configured. They are categorized as Utilization, Discard or Error exceptions and the numbers in this report refer to the aggregated total exceptions for all interfaces in the VPN.

You can filter this report by applying the following parameters:

- 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.

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. All 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.

You can filter this report by applying the following parameters:

- 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

Provisioning Custom Attributes

This appendix covers the following topics:

For information about the frequency of collections and the specific SNMP MIBs and OIDs used in reports, refer to the user guides for the Interface Discovery Datapipe and the Interface Reporting ifEntry Datapipe.

Sources for Custom Attributes

Any managed element can be provisioned with custom attributes, also known as property information. Provisioning can be automatic or manual. When attributes are sourced from the network, or inherited from an existing report pack, provisioning is automatic. When attributes cannot be sourced or inherited, a manual process is necessary. There are two ways to perform the manual process:

- Use the forms that are described in Modifying Object Properties on page 29.
- Create a properly formatted property file and import the contents. This appendix describes this method.

Since various attributes are sourced from the network and inherited from the Interface Reporting Report Pack, the MPLS VPN Report Pack can operate without manual provisioning. However, if you choose, you may manually provision various attributes associated with the following elements:

- VRFs
- VPNs

Property Import Files

The custom attributes you are able to assign vary from report pack to report pack. The MPLS VPN Report Pack accommodates user-friendly names for devices, SLA settings for VRFs, and customer and location assignments for VPNs.

If you need to provision a managed element using the manual method, the property data for that element will be loaded in bulk format from a text file. Known as a property import file, the text file is imported and processed by OVPI. Your task is to create the file and put it 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 the file from OVPI after OVPI has had sufficient time to collect property information on its own

We recommend the third approach. Regardless of the method you use, the file must adhere to the format shown here. The sequence of attributes in your file must follow the sequence shown here, and you must use a tab to separate columns. Your file will not have column headings, only rows of data.

Importing Property Information

The MPLS VPN Report Pack represents the network as a collection of managed elements with custom attributes associated with each managed element. The managed elements are:

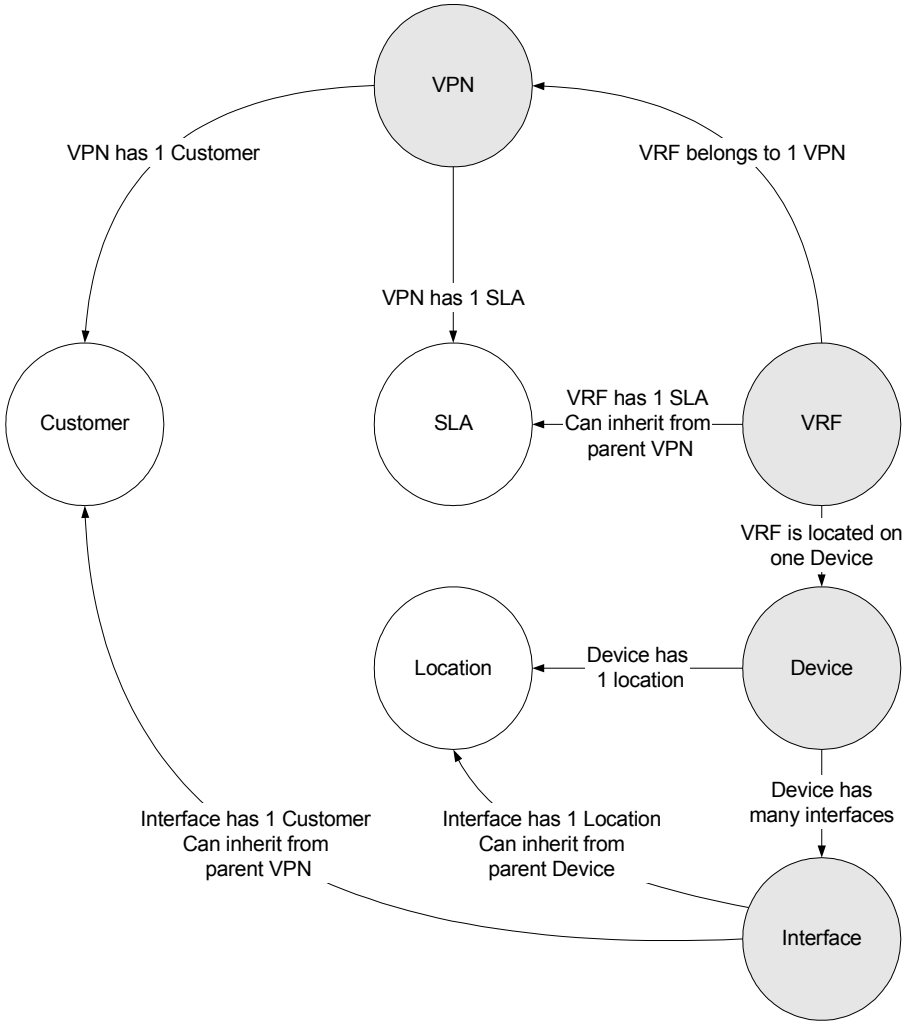
- VPN
- VRF
- SLA
- Interface (MPLS-enabled or VPN-associated)
- Device

The following table indicates which property attributes can be associated with each managed element.

Table 1 Managed Elements and Property Attributes

Element	Properties
VPN	Customer, Customer ID, SLA
VRF	SLA
SLA	Operational%, Interface Availability, Discard Threshold, Error Threshold, SNMP Response Time
Interface	See the Interface Reporting ReportPack User Guide
Device	See the Common Property Tables User Guide

The relationships between the managed elements and the associated properties are shown in the following diagram.



As shown in the preceding diagram, manual provisioning will be necessary for those managed elements introduced by the MPLS VPN Report Pack, while automatic provisioning will handle attributes that can be sourced from the network or inherited from an existing report pack.

Interfaces

The most fundamental element in the MPL VPN Report Pack is the interface. The provisioning of interfaces is handled through the Interface Reporting Report Pack. For more information about importing custom attributes for interfaces, refer to the *Interface Reporting Report Pack User Guide.* As explained there, 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.

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 User Guide*.

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.

The second option requires that you create a property file and call the import mechanism for VRFs. The format of the VRF property file (VRF_Property.dat) is as follows:

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

There are two ways to import this file:

- Type **`trend_proc -f VRF_importdata.pro`** from within the MPLS_VPN.ap directory.
- Execute the perl script by the same name in the same directory.

There are two ways to export this file:

- Type **`trend_proc -f VRF_exportdata.pro`** from within the MPLS_VPN.ap directory.
- Execute the perl script by the same name in the same directory.

If you are importing data, your import file will be archived to this directory:

```
MPLS_VPN.ap/PropertyData/Archive
```

If you are exporting data, the results will be deposited to this directory:

```
MPLS_VPN.ap/PropertyData
```

Reference to an SLA which does not yet exist will result in the creation of 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.

Importing the VRF property file logs messages to the Configuration and Logging Report in the Admin folder of Interface Reporting.

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. To assign a customer and/or SLA to a VPN, or provision new, not yet monitored VPNs, you must provide a property import file and call the import mechanism for VPNs.

The format of the VPN Property file (VPN_Property.dat) is as follows:

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

There are two ways to import this file:

- Type **`trend_proc -f VPN_importdata.pro`** from within the MPLS_VPN.ap directory.
- Execute the perl script by the same name in the same directory.

There are two ways to export this file:

- Type **`trend_proc -f VPN_exportdata.pro`** from within the MPLS_VPN.ap directory.
- Execute the perl script by the same name in the same directory.

If you are importing data, your import file will be archived to this directory:

```
MPLS_VPN.ap/PropertyData/Archive
```

If you are exporting data, the results will be deposited to this directory:

```
MPLS_VPN.ap/PropertyData
```

Although the *customer* attribute is stored and managed by Common Property Tables, references to a *customer ID* or *customer name* in this file will be 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 supplied in the customer tables, then a new customer with the basic properties of customer name and ID will be created. Other customer properties will be defaulted. This implies that you may create—but not modify—customer entries using this import mechanism.

Although not essential, you should create any required customer entries using the Common Property Table import utility, with correct properties, ahead of time to avoid this situation.

Reference to an SLA that does not yet exist will result in the creation of 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 procedures described in this chapter.

Importing the VPN property file logs messages to the Configuration and Logging Report in the Admin folder of Interface Reporting.

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. To modify an existing SLA, or create a new one using the import procedure, you must provide a property import file and call the import mechanism for SLAs. The format of the SLA property file (SLAConfig_Property.dat) is as follows:

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

There are two ways to import this file:

- Type **`trend_proc -f SLAConfig_importdata.pro`** from within the MPLS_VPN.ap directory.
- Execute the perl script by the same name in the same directory.

There are two ways to export this file:

- Type **`trend_proc -f SLAConfig_exportdata.pro`** from within the MPLS_VPN.ap directory.
- Execute the perl script by the same name in the same directory.

If you are importing data, your import file will be archived to this directory:

```
MPLS_VPN.ap/PropertyData/Archive
```

If you are exporting data, the results will be deposited to this directory:

```
MPLS_VPN.ap/PropertyData
```

Importing the SLA property file logs messages to the Configuration and Logging Report in the Admin folder of Interface Reporting.

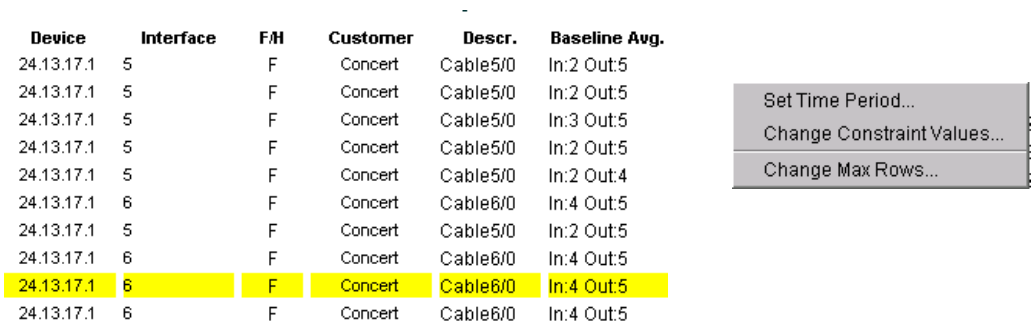
B

Editing Tables and Graphs

Every table and graph in a report displays in a default view. To change the default view, simply right-click the object and choose one of the optional views in the view options menu. The view options for tables are different from the view options for graphs.

View Options for Tables

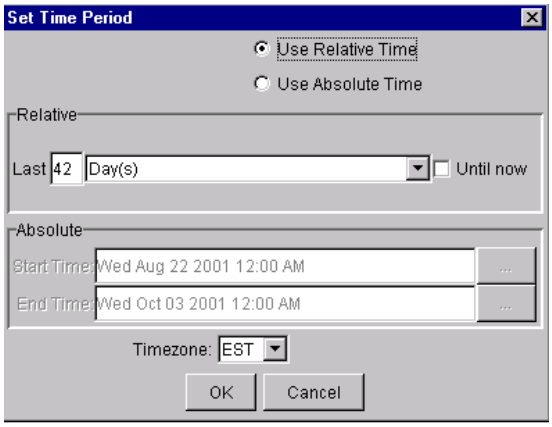
Right-clicking a table opens the view options menu to the right.



Device	Interface	F/H	Customer	Descr.	Baseline Avg.
24.13.17.1	5	F	Concert	Cable5/0	In:2 Out:5
24.13.17.1	5	F	Concert	Cable5/0	In:2 Out:5
24.13.17.1	5	F	Concert	Cable5/0	In:3 Out:5
24.13.17.1	5	F	Concert	Cable5/0	In:2 Out:5
24.13.17.1	5	F	Concert	Cable5/0	In:2 Out:4
24.13.17.1	6	F	Concert	Cable6/0	In:4 Out:5
24.13.17.1	5	F	Concert	Cable5/0	In:2 Out:5
24.13.17.1	6	F	Concert	Cable6/0	In:4 Out:5
24.13.17.1	6	F	Concert	Cable6/0	In:4 Out:5
24.13.17.1	6	F	Concert	Cable6/0	In:4 Out:5

Set Time Period

Select this option to alter the scope of relative time period (relative to now) or set an absolute time period. The following window opens.



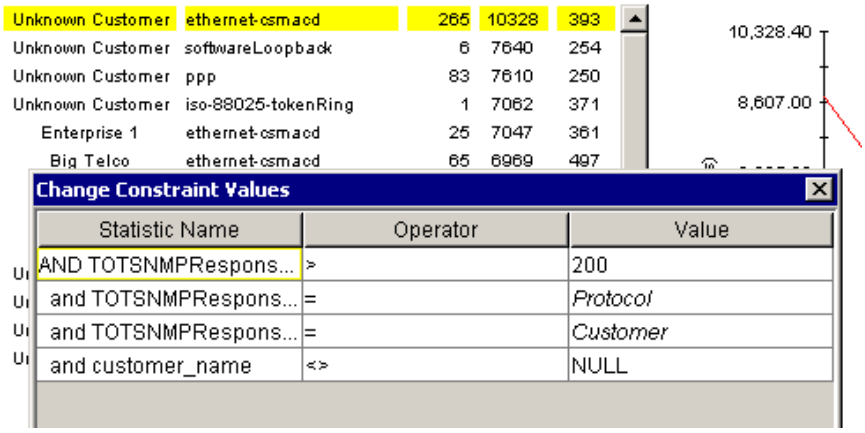
Alter the relative time range or specify an absolute time range. The defaults for a table containing data for 42 days are:

- Use Relative Time
- Last 42 Days

You may shorten the period of time covered by the table. To do that, change 42 days to 30, 14, or 7 days. If you are interested in a range of time that starts well in the past and stops before yesterday, click Use Absolute Time and select a start and end time.

Change Constraint Values

Select this option to tighten or loosen a constraint in order to display less data or more data. The Change Constraint Value window opens.



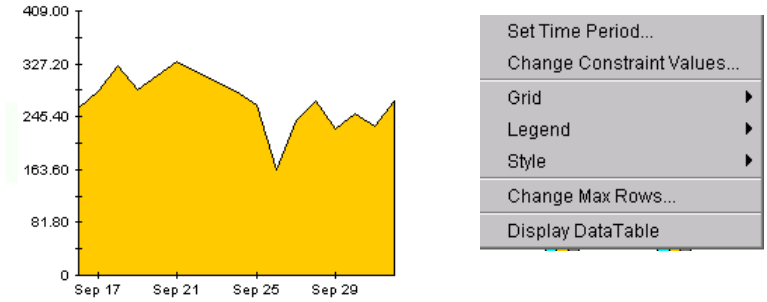
The table columns are Statistic Name, Operator, and Value. The operator in this sample is greater than (>). Other operators include less than (<) and equal to (=). To loosen the constraint and thereby include more data in the table, lower the default to a value below 200. To tighten the constraint and thereby reduce the amount of data in the table, increase the default to a value above 200.

Change Max Rows

Select this option to increase or decrease the default. The default is 50 rows. If you are monitoring a large network with hundreds of managed elements, using the default will ensure that this table displays as quickly as possible. If you increase max rows to a high number, be prepared to wait a moment or two while the table populates completely.

View Options for Graphs

Right-click a graph to display the view options menu.



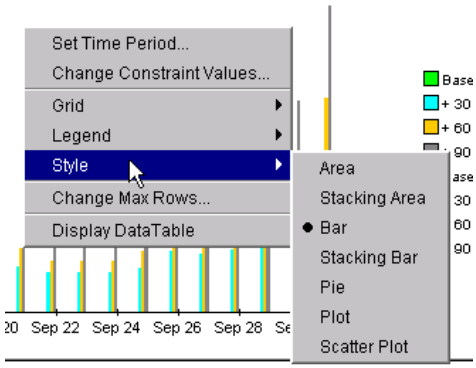
The following table describes each view option.

Table 2 View Options for Graphs

Option	Function
Set Time Period	Same as the table view option. See Set Time Period on page 68.
Change Constraint Values	Same as the table view option. See Change Constraint Values on page 68.
Grid	Allows you add these to the graph: • X axis grid lines • Y axis grid lines • X and Y axis grid lines
Legend	Alter placement of the legend or eliminate the legend. The options are below, to the right, to the left, and none.
Style	See Style Options on page 70.
Change Max Rows	Same as table view option. See Change Max Rows on page 69.
Display Data Table	See Display Data Table on page 74.

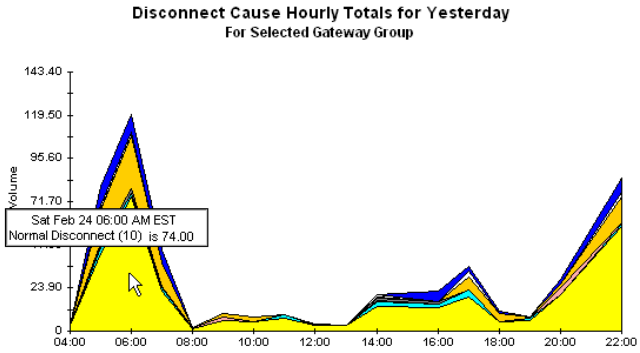
Style Options

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



Style > Area

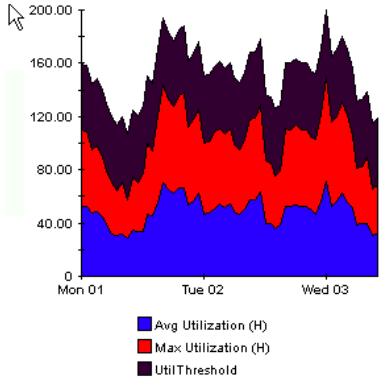
The plot or bar chart changes to an area graph. While relative values and total values are easy to view in this format, absolute values for smaller data types may be hard to see. However, if you click anywhere within a band of color, the exact value for that location in the graph appears in a box.



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 and only the selected time span displays.

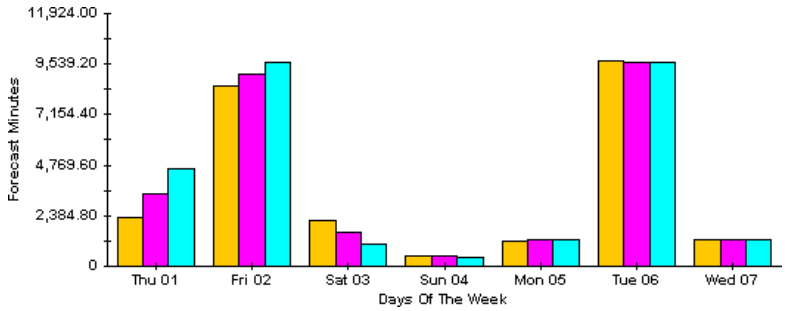
Style > Stacking Area

The area or plot graph changes to a stacking area graph. This view is suitable for showing relatively equal values for a limited number of variables.



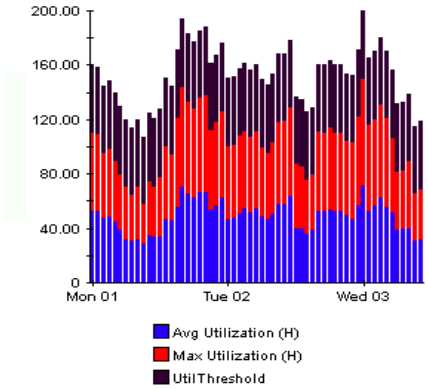
Style > Bar

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



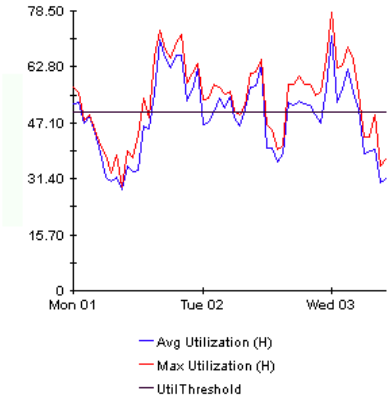
Style > Stacking Bar

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.



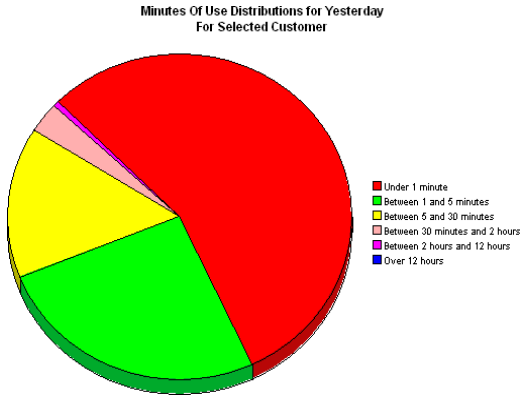
Style > Plot

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.

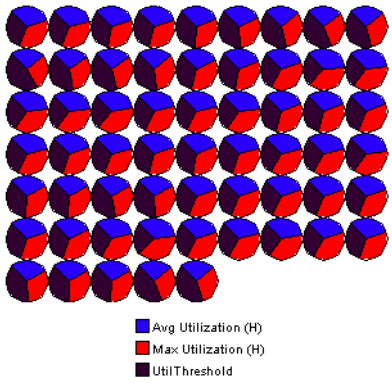


Style > Pie

An area graph becomes a 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 limited 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.



Display Data Table

This option changes a graph into a spreadsheet. Once in this format, there are four ways to manipulate the spreadsheet. Each method is highlighted below.

1. Double-click a column header to sort the column in descending order.

2. Click and hold a column header to drag and drop it anywhere in the table.

3. Hold down the SHIFT key and double-click a column header to sort the column in ascending order.

	Normal Disconnect (10)	User Busy (11)	No User Response (12)	No User Answer (13)	No Circuit (22)	No Resource (2F)	Unassigned Number (01)	No Route To Destination (03)	Invalid Number (1C)	Call Id In Use (54)	Recovery On Timer Expires (66)	Unknown Disconnect Code (?)
1	58.00	1.00	0.00	0.00	1.00	0.00	0.00	14.00	0.00	0.00	3.00	8.00
2	20.00	0.00	0.00	0.00	4.00	0.00	0.00	2.00	0.00	0.00	0.00	3.00
3	6.00	1.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00
4	5.00	0.00	0.00	0.00	0.00	0.00	0.00	5.00	0.00	0.00	0.00	1.00
5	19.00	4.00	0.00	0.00	0.00	0.00	0.00	7.00	0.00	0.00	3.00	3.00
6	13.00	2.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	6.00
7	14.00	2.00	0.00	0.00	1.00	0.00	1.00	1.00	0.00	0.00	1.00	0.00
8	3.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
9	3.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00
10	7.00	2.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
11	5.00	0.00	0.00	0.00	0.00	0.00	0.00	3.00	0.00	0.00	0.00	0.00
12	6.00	0.00	0.00	0.00	2.00	0.00	0.00	2.00	0.00	0.00	0.00	0.00
13	1.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
14	22.00	2.00	0.00	0.00	1.00	0.00	0.00	13.00	0.00	0.00	0.00	7.00
15	74.00	2.00	0.00	0.00	0.00	0.00	3.00	29.00	0.00	0.00	2.00	10.00
16	43.00	3.00	0.00	0.00	1.00	0.00	2.00	18.00	1.00	0.00	2.00	10.00
17	3.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

4. Click and hold a row number to drag it up or down in the table.

index

G

I

L

M

N

O

P

R

S

T

U

V

W