RMON2 Traffic Profiling Report Pack

Software Version: 3.0

HP OpenView Performance Insight

User Guide

May 2005

Legal Notices

Warranty

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

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

Restricted Rights Legend

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

Hewlett-Packard Company
United States of America

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

Copyright Notices

© Copyright 2004 - 2005 Hewlett-Packard Development Company, L.P.

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

Trademark Notices

UNIX® is a registered trademark of The Open Group.

Windows® and MS Windows® are US registered trademarks of Microsoft Corporation.

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

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

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

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

Support

Please visit the HP OpenView web site at:

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

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

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

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

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

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

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

To find more information about access levels, go to:

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

To register for an HP Passport ID, go to:

https://passport2.hp.com/hpp/newuser.do

Contents

1 Overview 7
OVPI and RMON2 Probes 7
Ways to Customize Reports 9
Sources for Additional Information 11

2 Package Installation 13
Guidelines for a Smooth Install 13
Installing RMON2 Traffic Profiling 3.0 15
Accessing Deployed Reports 17
Package Removal 17

3 Polling Groups and MIB Values 19
Adding Probes and Setting MIB Values 19
Command Line Options for ConfigAlMatrix.pl 20

4 Setting Up a Distributed System 21
Configuring the Central Server 21
Configuring a Satellite Server 22
System Clocks 22

5 Sample Reports 23

A Editing Tables and Graphs 35
View Options for Tables 35
View Options for Graphs 36

Glossary 43

Index 45

1 Overview

This chapter covers the following topics

- OVPI and RMON2 Probes
- Objects, reports, and groups
- Ways to customize reports
- Sources for additional information

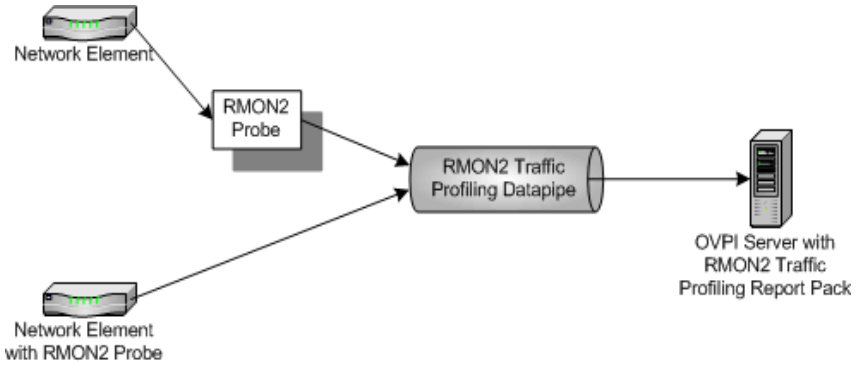
OVPI and RMON2 Probes

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

The RMON2 Traffic Profiling Report Pack installs on OVPI. Using processing directives supplied by the report pack, OVPI generates the following statistics:

- Utilization host-by-host
- Utilization application-by-application
- Percentage of total interface traffic associated with each host and each application
- Bytes
- Average bytes per packet

In the figure below, an RMON2 probe queries network elements for information about network traffic and stores the results in an SNMP MIB. The data in the SNMP MIB indicates where network traffic is going, traffic volume, and which protocols are involved. The RMON2 Traffic Profiling Datapipe collects data from the SNMP MIB and populates database tables maintained by OVPI.



RMON2 Traffic Profiling 2.0 supports the following RMON2 probes:

- Agilent
- Cisco NAM
- NetScout

Version History

The following table outlines recent enhancements to RMON2 Traffic Profiling.

Package Version	Release Date	Features/Enhancements
1.0	May 2003	15 reports RMON2 Traffic Profiling Datapipe 1.0 Sybase support
2.0	October 2003	OVPI Object Manager support *new datapipe:* RMON2 Traffic Profiling Datapipe 2.0
2.0	April 2004	No changes
2.0	August 2004	No changes
3.0	November 2004	Oracle support *new datapipe:* RMON2 Traffic Profiling Datapipe 3.0
3.0	June 2005	*new upgrade package:* UPGRADE_RMON2_Traffic_Profiling_to_3.0

Objects, Reports, and Groups

If you have access to the Management Console, you can display the reports in this package by opening the Object/Property Management window and navigating to the following object:

- RMON2 Probe Interface

Look for a list of reports under **Report Specific Tasks**. If you log in to the OVPI Application Server, you will see three folders:

- ALMATRIX
- HOST
- TOP_TEN

The ALMATRIX folder contains the following reports:

- Daily ALMATRIX Details
- Daily ALMATRIX Summary
- Hourly ALMATRIX Details
- Hourly ALMATRIX Summary
- Monthly ALMATRIX Detail

- Monthly ALMATRIX Summary

The HOST folder contains the following reports

- Daily Host Detail
- Daily Host Summary
- Hourly Host Detail
- Hourly Host Summary
- Monthly Host Detail
- Monthly Host Summary

The TOP_TEN folder contains the following reports:

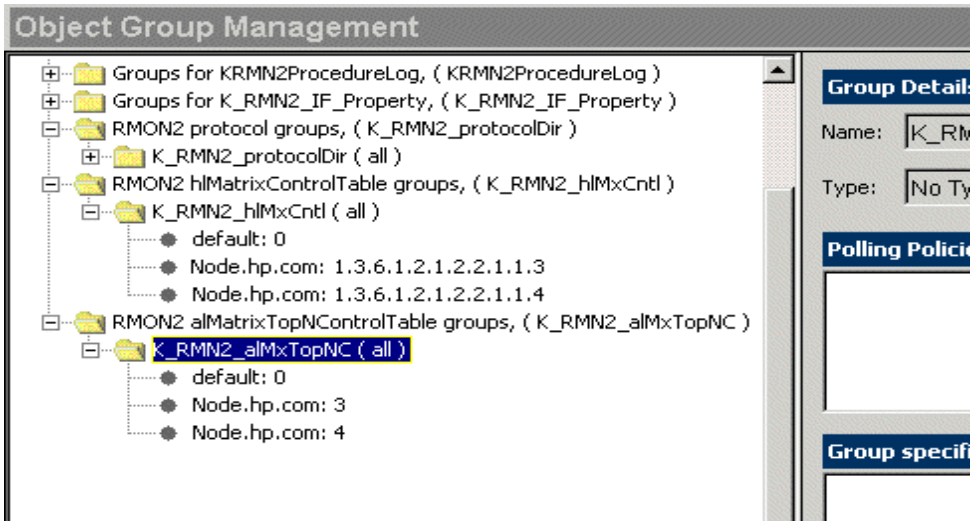
- Daily Top Ten
- Hourly Top Ten
- Monthly Top Ten

Summary reports aggregate data by application and host devices and display hourly, daily, and monthly trending analysis. Use these reports to find out whether recent excess traffic was a short-lived anomaly or a long-standing trend that requires corrective action.

Detail reports drill down on Summary reports, allowing you to see which source/destination combinations and host/protocol combinations are contributing to excess traffic.

Top Ten reports indicate which protocols had the greatest impact on interface utilization, and which hosts had the greatest impact on interface utilization.

RMON2 Traffic Profiling 3.0 adds the following groups to the object tree:



Ways to Customize Reports

The contents of a report can be customized by importing location data, by applying group filters, by editing parameters, and by editing tables and graphs,. While service providers use group filters to produce customer-specific reports, any user can import locations, edit parameters, or change view options for tables and graphs.

Group Filters

If you intend to share your reports with customers, or let divisions within your enterprise see division-specific performance data, you must produce customer-specific reports by filtering the database. Creating customer-specific reports involves the following tasks:

- Importing customer names and device locations using Common Property Tables
- 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 group filters, refer to the *OVPI 5.1 Administration Guide*.

Editing Parameters

When you edit a parameter, you apply a constraint to the report. The constrain eliminates the data you are not interested in seeing. For example, if you edit the RMON2 Probe parameter, the only data that appears in the report is data for the probe you typed in the RMON2 Probe field.

You can apply multiple constraints at the same time. RMON2 Traffic Profiling supports the following parameter edits:

- IF_Customer_Name
- IF_Customer_ID
- Start_Time
- End_Time
- Client_Name (of source)
- Server_Name (of destination)
- Application_Name (of protocol)
- RMON2 Probe Interface
- RMON2 Probe

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

If the client component of OVPI is installed on your system, you have access to Report Viewer. To edit a parameter, select **Edit > Parameter Values** from the menu bar. The Modify Parameter Values window opens. Click the **Current Value** field, enter a new value, and click **OK**.

Importing Locations

Although RMON2 Traffic Profiling operates without importing custom property information, none of the location-oriented reports will contain useful information unless you add locations. To add locations to reports, use the property import utility bundled with Common Property Tables. For details, refer to the *Common Property Tables 3.5 User Guide*.

Sources for Additional Information

This user guide contains samples of some of the reports in the RMON2 package. The demo package that comes with RMON2 is complete, containing a sample of every report in the package. If you have access to the demo package and you want to know what fully-populated reports look like, install the demo package. Like real reports, demo reports are interactive. Unlike real reports, demo reports are static and do not change over time.

The following documents are related to this manual:

- *RMON2 Traffic Profiling Report Pack 3.0 Release Statement*
- *Interface Reporting Report Pack 5.0 User Guide*
- *Common Property Tables 3.5 User Guide*
- *Interface Discovery Datapipe 2.2 User Guide*
- *OVPI Report Packs, Version 8.0: Release Notes, June 2005*

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

http://www.managementsoftware.hp.com

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

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

2 Package Installation

This chapter covers the following topics:

- Guidelines for a Smooth Install
- Installing RMON2 Traffic Profiling 3.0
- Accessing Deployed Reports
- Package Removal

Guidelines for a Smooth Install

Each reporting solution that runs on OVPI consists of a report pack and one datapipe, or sometimes a report pack and multiple datapipes. When you install the datapipe, you configure OVPI to collect a specific type of performance data at a specific polling interval. When you install the report pack, you configure OVPI to summarize and aggregate the performance data collected by the datapipe.

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

Software Prerequisites

RMON2 Traffic Profiling 3.0 has the following prerequisites:

- OVPI 5.0 or higher
- All available service packs for the version of OVPI (5.0 or 5.1) you are running
- Common Property Tables 3.5
- Interface Reporting Report Pack 5.0
- Interface Discovery Datapipe 2.2

If you are not currently running any version of the Interface Discovery Datapipe, or any version of Common Property Tables, you can install these packages when you install RMON2 Traffic Profiling 3.0.

If you are running earlier versions of Common Property Tables, version 2.2 or 3.0, upgrade to version 3.5. Installing the “to_3.5” upgrade package is no different from installing other upgrade packages; however, do not install the “to_3.5” upgrade package and other packages at the same time. Install the upgrade package for Common Property Tables and *only* the upgrade package for Common Property Tables.

Install Procedure for Distributed Systems

Installation is more complex if you intend to run this package as a distributed system across multiple servers. Here is an overview of the installation procedure:

1. Verify that all servers are running the same version of OVPI and all available service packs for that version.
2. Disable trendcopy on the central server.
3. Install RMON2 Traffic Profiling 3.0 on the central server.
4. Install RMON2 Traffic Profiling 3.0 and the RMON2 Traffic Profiling Datapipe on each satellite server.
5. Re-enable trendcopy on the central server.

When the installation is complete, set up connections with satellite server databases, configure trendcopy pull commands, and switch off hourly and daily aggregations at each satellite server. For details, see Chapter 4, Setting Up a Distributed System.

Upgrading from Version 2.0 to Version 3.0

If you are currently running version 2.0 and you are already familiar with Package Manager, you should have no difficulty upgrading to the latest release. Keep in mind that you must delete certain packages that cannot be upgraded. Here is an outline of the upgrade procedure:

1. Stop OVPI Timer and extract OVPI packages from the report pack CD.
2. If necessary, upgrade to Common Property Tables 3.5.
3. If necessary, upgrade to Interface Reporting 5.
4. Install UPGRADE_RMON2_Traffic_Profiling_to_3.
5. Datapipes cannot be upgraded. Uninstall these datapipes:
   - Interface Discovery Datapipe 1.1 / 2.0 / 2.1
   - RMON2 Traffic Profiling Datapipe 2.0
6. Install Interface Discovery Datapipe 2.2.
7. Install RMON2 Traffic Profiling Datapipe 3.0.
8. Restart OVPI Timer.

Datapipes and Remote Pollers

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

- Single polling policy for a emote pollers
- Clone polling policies for multiple remote pollers
- Type and group information associated with a modified polling policy

You can export existing configurations by using the collection_manager and group_manager commands.

Exporting Polling Policy Configurations

If your environment contains polling policy assignments to remote pollers, use the collection_manager command to export polling policies to a file.

UNIX: As user trendadm, run the following command:

```
cd $DPIPE_HOME

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

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

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

Exporting Custom Polling Groups

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

UNIX: As user trendadm, execute the following command:

```
cd $DPIPE_HOME

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

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

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

Custom Table Views

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

Installing RMON2 Traffic Profiling 3.0

Complete the following tasks to install RMON2 Traffic Profiling 3.0:

- Stop OVPI Timer and extract OVPI packages from the report pack CD
- If necessary, upgrade to Common Property Tables 3.5
- Install RMON2 Traffic Profiling

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

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

   On Windows, do the following:

   a. From the Control Panel, select **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 report pack CD in the CD-ROM drive.

Windows: The Main Menu automatically displays.

UNIX:

a Mount the CD (if the CD does not mount automatically)

b Navigate to the top level directory on the CD

c Run **`./setup`**.

4 Type **`1`** in the choice field and press **Enter**. The install script displays a percentage complete bar. When the copy is complete, the install script starts Package Manager. The Package Manager welcome window opens.

Task 2: If necessary, upgrade to Common Property Tables 3.5

If you are not running any version of Common Property Tables, skip this task and let Package Manager install Common Property Tables for you

RMON2 Traffic Profiling 3.0 requires Common Property Tables. If you have not already upgraded to Common Property Tables 3.5, install the "to_3.5" upgrade package now. Do not install other packages at the same time. Install the upgrade package for Common Property Tables and *only* the upgrade package for Common Property Tables. When the upgrade install is complete, click **Done** to return to the Management Console.

Task 3:Install RMON2 Traffic Profiling

1 From the Management Console, select **Tools > Package Manager**. The Package Manager welcome window opens.

2 Click **Next**. The Package Location window opens.

3 Click **Install.** Approve the default installation directory or select a different directory if necessary.

4 Click **Next**. The Report Deployment window opens. Accept the default for Deploy Reports. Type your user name and password for the OVPI Application Server.

5 Click **Next**. The Package Selection window opens.

6 Click the check box next to the following packages:

- *RMON2 Traffic Profiling 3.0*
- *RMON2 Traffic Profiling Demo*

  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.

- *RMON2 Traffic Profiling Datapipe 3.0*
- *Interface Discovery Datapipe 2.2* (if not already installed)
- *Common Property Tables 3.5* (if not already installed)

7 Click **Next**. The Type Discovery window opens. Disable the default.

8 Click **Next**. The Selection Summary window opens.

9 Click **Install**. The Installation Progress window opens. When installation finishes, a package installation complete message appears.

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

11 Restart OVPI Timer.

On Windows, do the following:

a From the Control Panel, select **Administrative Tools > Services**

b Select OVPI Timer from the list of services.

c From the Action menu, select **Start**.

On UNIX, as root, enter one of the following commands:

— HP-UX: **`sh /sbin/ovpi_timer start`**

— Sun: **`sh /etc/init.d/ovpi_timer start`**

Accessing Deployed Reports

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

- OVPI client applications
- Web browser

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

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

Package Removal

Follow these steps to uninstall the RMON2 Traffic Profiling Report Pack and RMON2 Traffic Profiling Datapipe:

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

2 Stop OVPI Timer and wait for processes to stop running.

On Windows, do the following:

a From the Control Panel, select **Administrative Tools > Services**

b Select OVPI Timer from the list of services.

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

On UNIX, as root, enter one of the following commands:

— HP-UX: **`sh /sbin/ovpi_timer stop`**

— Sun: **`sh /etc/init.d/ovpi_timer stop`**

3 From the Management Console, start Package Manager. The Package Manager welcome window opens.

4 Click **Next**. The Package Location window opens.

5 Click **Uninstall.**

6 Click **Next**. The Report Undeployment window opens. Accept the default for Undeploy Reports, application server name, and port.

7 Click **Next**. The Package Selection window opens.

8 Click the check box next to the following packages:

- *RMON2 Traffic Profiling*
- *RMON2 Traffic Profiling Datapip*e
- *RMON2 Traffic Profiling Demo* (if installed)

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

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

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

12 Restart OVPI Timer.

On Windows, do the following:

a From the Control Panel, select **Administrative Tools > Services**

b Select OVPI Timer from the list of services.

c From the Action menu, select **Start**.

On UNIX, as root, enter one of the following commands:

— HP-UX: **`sh /sbin/ovpi_timer start`**

— Sun: **`sh /etc/init.d/ovpi_timer start`**

Uninstalling the RMON2 Traffic Profiling Report Pack automatically uninstalls the datapipe even if you do not select the datapipe for removal.

3 Polling Groups and MIB Values

This chapter covers the following topics:

- How to add RMON2 probes to polling groups
- How to set MIB values
- Command line options for configAlMatrix.pl

Adding Probes and Setting MIB Values

Follow these steps to add probes to Polling Groups:

1. Using Polling Policy Manager, do the following:
   a. Add each RMON2 probe node to the RMON2 polling group.
   b. Specify the Community String Profile for each node added to the RMON2 polling group. Typically, you use the default settings (Read: public; Write: private). However, if you configured an RMON2 probe to use a non-default community string profile, you must configure this non-default community string profile for each node.
2. Using the OVPI SNMP Tool `ConfigAlMatrix.pl` command (click the **Set Table** button), or a tool of your own choice, set the following MIB objects:

Table 1 Variables Under hlMatrixControlTable

MIB Object	OID	Value
hlMatrixControlNIMaxDesiredEntries	.1.3.6.1.2.1.16.15.1.1.6	6,000
hlMatrixControlAIMaxDesiredEntries	.1.3.6.1.2.1.16.15.1.1.10	12,000
hlMatrixControlStatus	.1.3.6.1.2.1.16.15.1.1.12	active

Table 2 Variables under alMatrixTopNControlTable

MIB Object	OID	Value
alMatrixTopNControlRateBase	.1.3.6.1.2.1.16.17.3.1.3	alMatrixTopNTerminalsPkts
alMatrixTopNControlTimeRemaining	.1.3.6.1.2.1.16.17.3.1.4	900
alMatrixTopNControlRequestedSize	.1.3.6.1.2.1.16.17.3.1.7	400
alMatrixTopNControlStatus	.1.3.6.1.2.1.16.17.3.1.11	active

Command Line Options for ConfigAlMatrix.pl

`ConfigAlMatrix.pl` is a tool supplied with the RMON2 Traffic Profiling Datapipe. You can use this tool to create the RMON2 data source to MIB-2 ifIndex and set all the MIB objects to the values listed in Table 2 for a specified RMON2 probe.

If you are using these MIB objects for other purposes, and if you do not want them set to these values, do not run this tool; instead, use the OVPI SNMP Tool or some other tool of your choice.

The following command line options are available:

`ConfigAlMatrix.pl -a ProbeHost [-c CommunityString -f ConfigFile]`

-a *ProbeHost*	Required	The name of the RMON2 probe.
-c *CommunityString*	Optional	Default: private. The write community string profile of the RMON2 probe. If the write community string profile of the RMON2 probe is set to something other than private, then you must use this option to specify the probe's write community string profile.
-f *ConfigFile*	Optional	Default: `\OVPI\packages\RMON2_Traffic_Profiling_Datapipe\RMON2_Traffic_Profiling_Datapipe.ap\alMatrixConfig.xml`. XML configuration file for the RMON2 probe. This file contains the MIB objects that can be modified. By default, MIB objects are set to the values listed in the preceding table. Modifying MIB objects will change the amount of data collected.

4 Setting Up a Distributed System

If you intend to run RMON2 Traffic Profiling in a distributed environment, and if you followed the instructions in the installation chapter, your central server is running the report pack, and each of your satellite servers is running the report pack and the datapipe.

Your next task is to set up connections with satellite server databases, configure trendcopy pull commands for hourly data, and switch off hourly and daily aggregations at each satellite server. In addition, make sure that the system clock on each satellite server is synchronized with the system clock on the central server.

Configuring the Central Server

Follow these steps to configure the central server:

1. Set up the connection with the satellite server databases:
   a. Start the Management Console.
   b. Click the **Systems** icon on the lower left. The System/Network Administration pane opens.
   c. Right-click the **Databases** folder. When prompted, select **Add OVPI Database**. The Add Database Wizard opens.
   d. Click **Next**.
   e. Type the hostname and port number for the database you want to add; click **Next**.
   f. Review the Summary. Repeat steps **d** and **e** for each additional database.
   g. When you are done adding databases, click **Finish**.
2. Edit the file `$DPIPE_HOME/scripts/RMN2_Hourly.pro`:
   a. For each satellite server, configure trendcopy pull commands from the central server by modifying the trendcopyblock:
      – Remove "#" before each line in trendcopyblock, including the begin and end lines.
      – Replace *SATELLITE_SERVER_1_DATABASE* with the satellite server name.
      – Replace *THIS_MACHINE_DATABASE* with the central server name.

      If there is more than one satellite server, copy and modify the trendcopyblock for each satellite server.
   b. Save and close `$DPIPE_HOME/scripts/RMN2_Hourly.pro`.

Configuring a Satellite Server

Switch off hourly and daily aggregations. Follow these steps:

This procedure assumes that the satellite server is not performing local reporting and that the RMON2_Traffic_Profiling module is installed.

1. Navigate to `$DPIPE_HOME/lib/trendtimer.sched`:
2. Comment out the lines referencing *RMN2_Hourly.pro* and *RMN2_Daily.pro*.
3. Save and close `$DPIPE_HOME/lib/trendtimer.sched`.

System Clocks

Verify that the system clock on each satellite server is synchronized with the system clock on the central server.

5 Sample Reports

RMON2 Traffic Profiling includes 15 reports. The following reports are reproduced below:

1. Monthly Top Ten Summary
2. Hourly AlMatrix Summary
3. Hourly AlMatrix Detail
4. Daily Host Summary
5. Daily Host Detail

Top Ten reports serve as a starting point for in-depth analysis of traffic problems. They contain the following information:

- Hourly utilization (in the hourly report only)
- Busy hour utilization (daily and monthly reports)
- A list of applications generating the most traffic, sorted from most to least
- A list of hosts generating the most traffic, sorted from most to least

ALMATRIX reports display traffic information by protocol and by source/destination host. RMON2 Traffic Profiling includes summary reports for ALMATRIX and detail reports for ALMATRIX. The summary reports aggregate data by protocol and by host devices; the detail reports contain information about the traffic between specific source and destination nodes for a selected protocol.

Host reports display traffic information by source. RMON2 Traffic Profiling includes summary reports for hosts and detail reports for hosts. The summary reports display traffic information for source nodes (listed by IP address) that generate the most traffic on the probe; the detail reports display traffic information sent by a protocol/application to a destination node for a selected source node.

RMON2 Traffic Profiling

Monthly Top Ten Summary

The Top Ten Summary report lists the top contributers to the total traffic on an interface. Select an interface and a time period to see the top ten hosts and protocols values with the greatest impact on the interface utilization for the time period selected.

Probe List

Probe	Interface	Busy Hour Utilization
sniffer	3	1.17

Peak Hourly Utilization

Month	Busy Hour Utilization
April, 2003	1.17
March, 2003	0.69

Top Ten Hosts

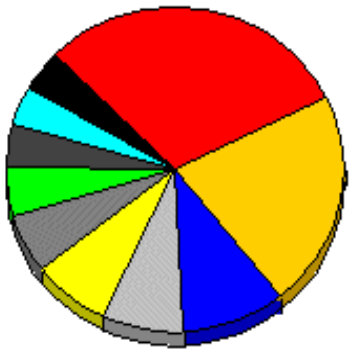
	Host	Busy Hour Utilization	% of Traffic
1	15.0.73.147	0.10	8.81
2	15.0.73.150	0.07	6.24
3	15.0.73.141	0.03	2.88
4	15.0.73.148	0.03	2.30
5	15.244.20.169	0.02	2.22
6	15.244.81.51	0.02	1.72
7	15.244.60.116	0.02	1.48
8	15.0.73.146	0.01	1.02
9	15.244.60.182	0.01	0.99
10	15.244.60.188	0.01	0.99

Top Ten Protocols

	Protocol	Busy Hour Utilization	% of Traffic
1	wildcard.ip.udp.netbios-dgm	0.70	59.21
2	wildcard.ip.icmp	0.14	12.97
3	wildcard.ip.tcp.netbios-ssn	0.10	8.87
4	wildcard.ip.udp.netbios-ns	0.09	7.76
5	wildcard.ip.udp.ntp	0.04	2.96
6	wildcard.ip.udp.sunrpc	0.04	2.95
7	wildcard.ip.udp.dns	0.03	1.99
8	wildcard.ip.udp.bootp-client	0.02	1.32
9	wildcard.ip.tcp.sunrpc	0.01	0.66
10	wildcard.ip.tcp.dns	0.01	0.33

Host Distribution

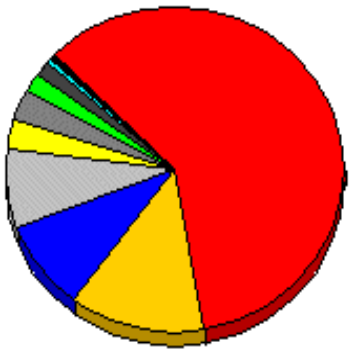
Top Ten Hosts



: 15.0.73.147 :
: 15.0.73.150 :
: 15.0.73.141 :
: 15.0.73.148 :
: 15.244.20.169 :
: 15.244.81.51 :
: 15.244.60.116 :
: 15.244.16.185 :
: 15.8.156.1 :
: 15.0.73.146 :

Protocol Distribution

Top Ten Protocols



3: sniffer : 3 : wildcard.ip.udp.netbios-dgm :
3: sniffer : 3 : wildcard.ip.icmp :
3: sniffer : 3 : wildcard.ip.tcp.netbios-ssn :
3: sniffer : 3 : wildcard.ip.udp.netbios-ns :
3: sniffer : 3 : wildcard.ip.udp.ntp :
3: sniffer : 3 : wildcard.ip.udp.sunrpc :
3: sniffer : 3 : wildcard.ip.udp.dns :
3: sniffer : 3 : wildcard.ip.udp.bootp-client :
3: sniffer : 3 : wildcard.ip.tcp.sunrpc :
3: sniffer : 3 : wildcard.ip.tcp.http :

RMON2 Traffic Profiling

Hourly ALMATRIX Summary

The ALMATRIX Summary Report presents a breakdown of the protocols which contribute to the total traffic on an interface. Select ar interface and a time period to see a list of protocols that had the most impact on the interface utilization for the time period selected. Select a protocol to see graphs of its historical traffic patterns.

Probe List

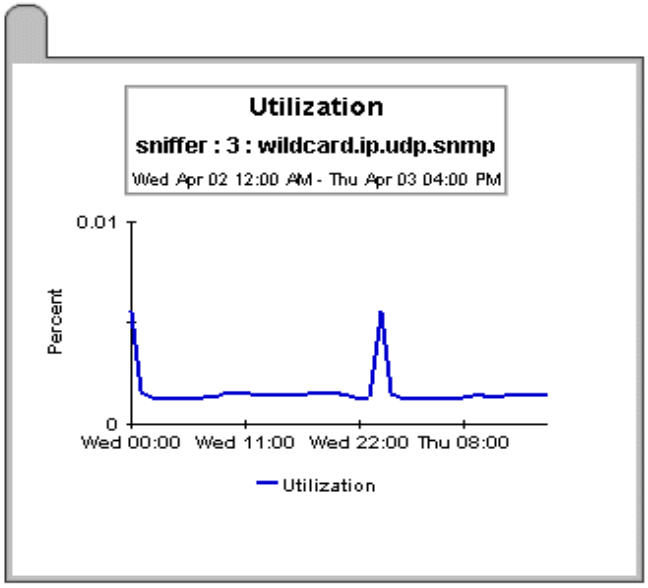
Probe	Interface	Utilization
sniffer	3	0.00

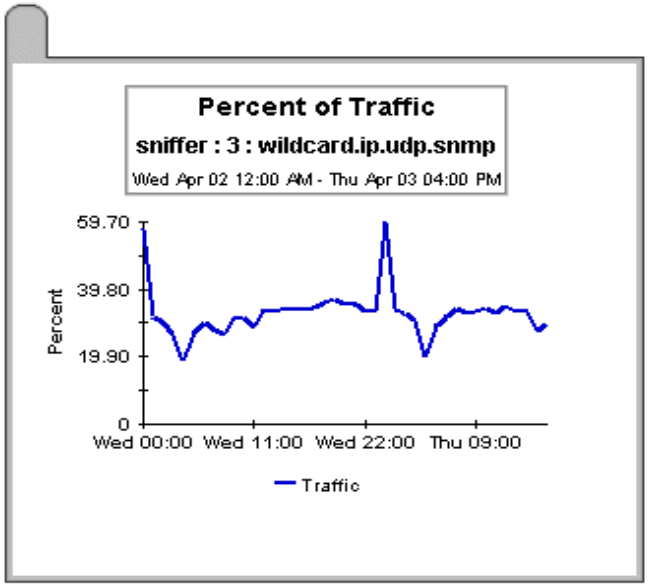
Hourly Utilization

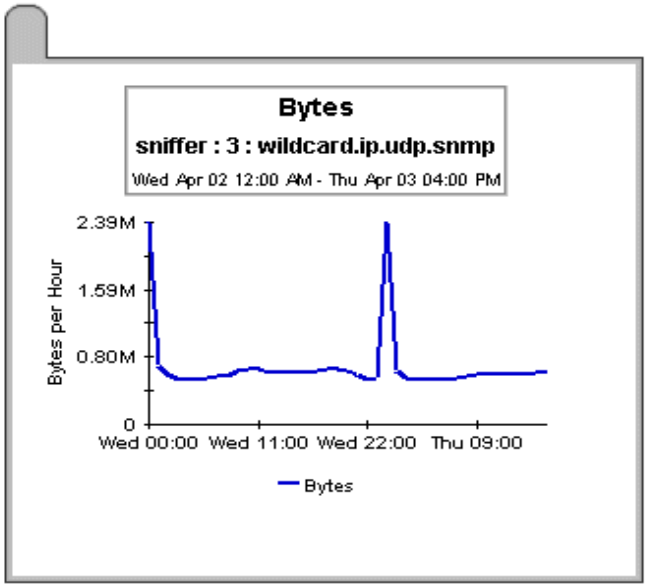
Hour	Utilization
4:00 PM, April 3, 2003	0.00
3:00 PM, April 3, 2003	0.01
2:00 PM, April 3, 2003	0.00
1:00 PM, April 3, 2003	0.00
12:00 PM, April 3, 2003	0.00
11:00 AM, April 3, 2003	0.00
10:00 AM, April 3, 2003	0.00

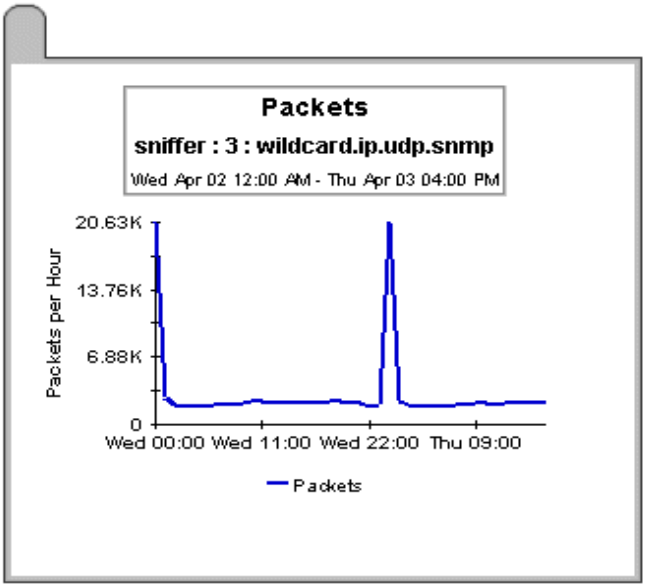
Top Talking Protocols / Applications

Protocol	Utilization	% of Traffic	Bytes	Average Bytes per Packet
wildcard.ip.udp.snmp	0.00	29.73	637.70 k	286.35
wildcard.ip.tcp.netbios-ssn	0.00	19.34	414.95 k	366.56
wildcard.ip.udp.netbios-dgm	0.00	13.56	290.94 k	254.99
wildcard.ip.tcp.telnet	0.00	11.39	244.37 k	87.27
wildcard.ip.udp.netbios-ns	0.00	11.38	244.08 k	103.82
wildcard.ip.icmp	0.00	5.09	109.22 k	218.88
wildcard.ip.udp.dns	0.00	3.76	80.69 k	261.97
wildcard.ip.udp.bootp-client	0.00	2.11	45.23 k	297.55
wildcard.ip.ospfigp	0.00	1.38	29.52 k	82.00


Utilization
sniffer : 3 : wildcard.ip.udp.snmp
Wed Apr 02 12:00 AM - Thu Apr 03 04:00 PM
0.01
Percent
0
Wed 00:00 Wed 11:00 Wed 22:00 Thu 08:00
Utilization


Percent of Traffic
sniffer : 3 : wildcard.ip.udp.snmp
Wed Apr 02 12:00 AM - Thu Apr 03 04:00 PM
59.70
39.80
19.90
Percent
0
Wed 00:00 Wed 11:00 Wed 22:00 Thu 09:00
Traffic


Bytes
sniffer : 3 : wildcard.ip.udp.snmp
Wed Apr 02 12:00 AM - Thu Apr 03 04:00 PM
2.39M
1.59M
0.80M
Bytes per Hour
0
Wed 00:00 Wed 11:00 Wed 22:00 Thu 09:00
Bytes


Packets
sniffer : 3 : wildcard.ip.udp.snmp
Wed Apr 02 12:00 AM - Thu Apr 03 04:00 PM
20.63K
13.76K
6.88K
Packets per Hour
0
Wed 00:00 Wed 11:00 Wed 22:00 Thu 09:00
Packets

Back to top.

RMON2 Traffic Profiling

Hourly ALMATRIX Detail

The ALMATRIX Detail Report presents a breakdown of the protocols, sources and destinations which contribute to the total traffic on an interface(data source). Select an interface and a time period to see a list of protocols that had the most impact on the interface utilization for the time period selected. Select a protocol to see a list of sources / destinations utilizing the protocol source through the selected interface. Select a source / destination combination to see graphs of its historical traffic patterns.

Probe List

Probe	Interface	Utilization
sniffer	3	0.00

Hourly Utilization

Hour	Utilization
4:00 PM, April 3, 2003	0.00
3:00 PM, April 3, 2003	0.01
2:00 PM, April 3, 2003	0.00
1:00 PM, April 3, 2003	0.00
12:00 PM, April 3, 2003	0.00
11:00 AM, April 3, 2003	0.00
10:00 AM, April 3, 2003	0.00

Top Talking Protocols / Applications

Protocol	Utilization	% of Traffic	Bytes	Average Bytes per Packet
wildcard.ip.udp.snmp	0.00	29.73	637.70 k	286.35
wildcard.ip.tcp.netbios-ssn	0.00	19.34	414.95 k	366.56
wildcard.ip.udp.netbios-dgm	0.00	13.56	290.94 k	254.99
wildcard.ip.tcp.telnet	0.00	11.39	244.37 k	87.27
wildcard.ip.udp.netbios-ns	0.00	11.38	244.08 k	103.82
wildcard.ip.icmp	0.00	5.09	109.22 k	218.88
wildcard.ip.udp.dns	0.00	3.76	80.69 k	261.97
wildcard.ip.udp.bootp-client	0.00	2.11	45.23 k	297.55
wildcard.ip.ospfigp	0.00	1.38	29.52 k	82.00

Top Talking Source / Destination Pairs

Source	Destination	Utilization	% of Traffic	Bytes	Average Bytes per Packet
15.1.158.148	15.0.73.150	0.00	14.74	316.08 k	287.35
15.0.73.150	15.1.158.148	0.00	14.72	315.75 k	287.05
15.0.73.150	15.24.115.12	0.00	0.11	2264	283.00
15.24.115.12	15.0.73.150	0.00	0.11	2264	283.00
15.244.16.185	15.244.63.9	0.00	0.05	1098	122.00

Source Owner

Unassigned

Source Location

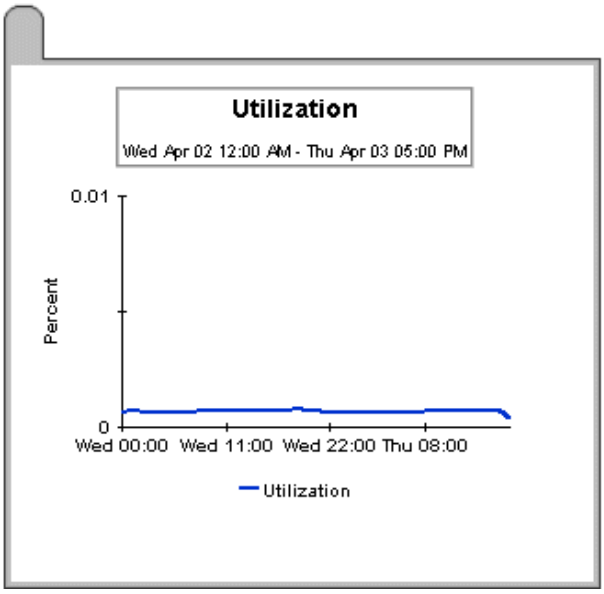
Unassigned

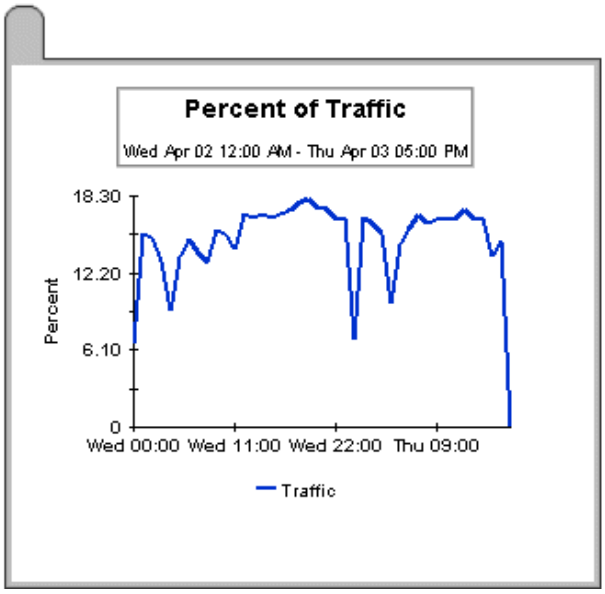
Destination Owner

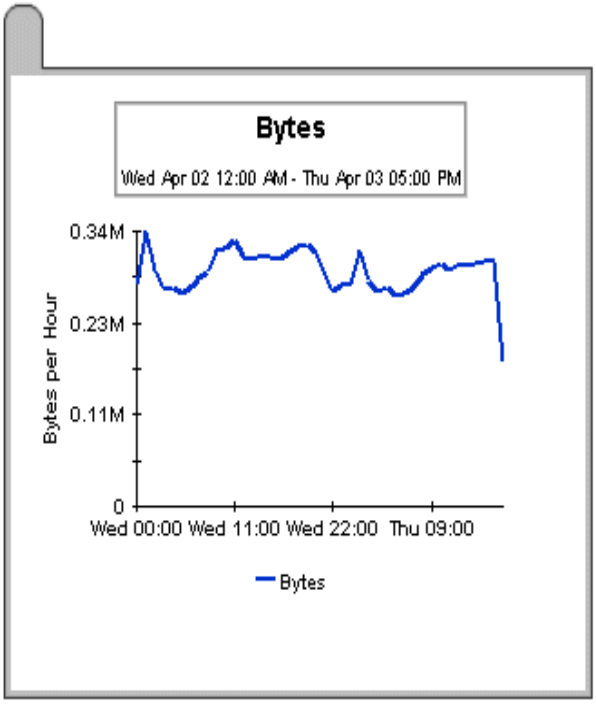
Unassigned

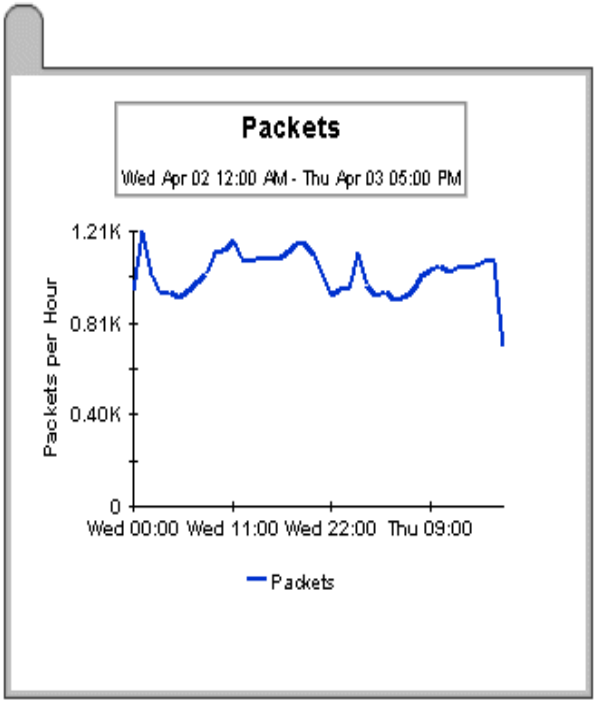
Destination Location

Unassigned









Back to top.

RMON2 Traffic Profiling

Daily Host Summary

The Host Summary Report presents a breakdown of the host devices which contribute to the total traffic on an interface. Select an interface and a time period to see a list of hosts that had the most impact on the interface utilization for the time period selected. Select a host device to see graphs of its historical traffic patterns.

Probe List

Probe	Interface	Busy Hour Utilization
sniffer	3	0.01

Peak Hourly Utilization

Day	Busy Hour Utilization
April 1, 2003	0.01
March 31, 2003	0.01
March 30, 2003	0.01
March 29, 2003	0.01
March 28, 2003	0.01
March 27, 2003	0.01

Top Talking Hosts

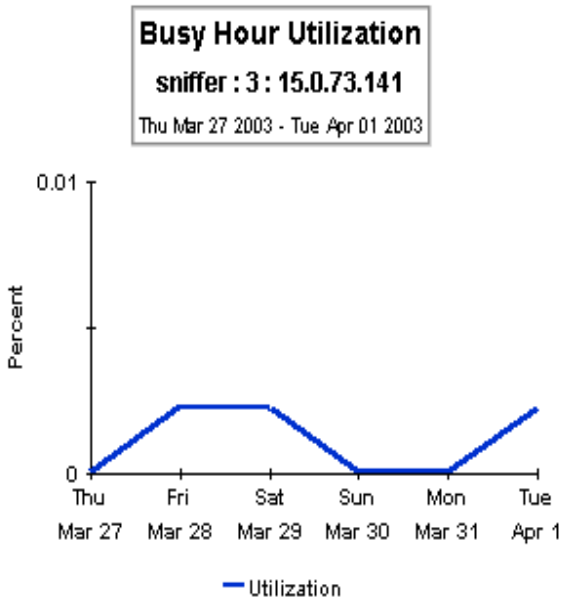
Host	Busy Hour Utilization	% of Daily Traffic	Bytes	Average Bytes per Packet
15.0.73.141	0.00	2.62	1392.39 k	103.06
15.243.128.51	0.00	8.37	4449.27 k	255.90
15.0.73.150	0.00	19.71	10.47 M	195.72
15.8.155.228	0.00	14.26	7574.20 k	731.81
15.1.158.148	0.00	13.96	7416.62 k	288.33
15.244.60.106	0.00	0.55	294.47 k	130.18
15.244.60.239	0.00	0.46	242.46 k	116.62
15.0.73.2	0.00	0.45	236.80 k	115.23
15.0.73.146	0.00	7.43	3945.02 k	106.39

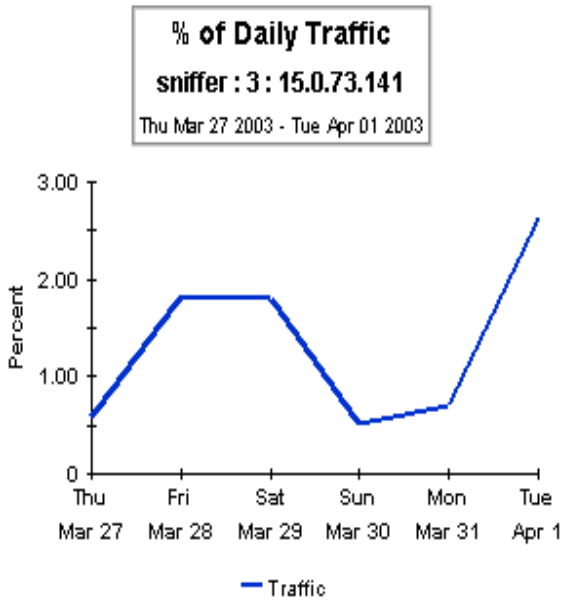
Host Owner

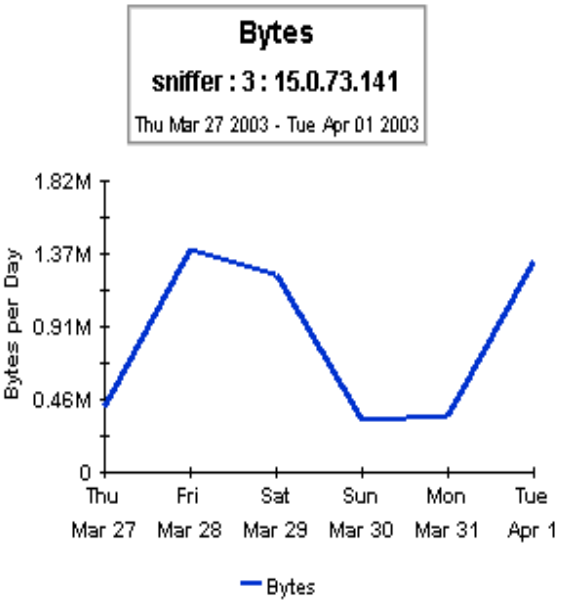
Unassigned

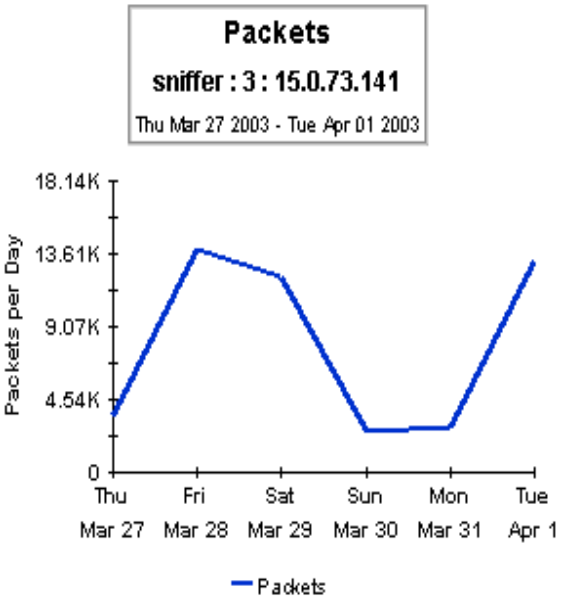
Host Location

Unassigned


Busy Hour Utilization
sniffer : 3 : 15.0.73.141
Thu Mar 27 2003 - Tue Apr 01 2003
0.01
0
Percent
Thu Mar 27
Fri Mar 28
Sat Mar 29
Sun Mar 30
Mon Mar 31
Tue Apr 1
Utilization


% of Daily Traffic
sniffer : 3 : 15.0.73.141
Thu Mar 27 2003 - Tue Apr 01 2003
3.00
2.00
1.00
0
Percent
Thu Mar 27
Fri Mar 28
Sat Mar 29
Sun Mar 30
Mon Mar 31
Tue Apr 1
Traffic


Bytes
sniffer : 3 : 15.0.73.141
Thu Mar 27 2003 - Tue Apr 01 2003
1.82M
1.37M
0.91M
0.46M
0
Bytes per Day
Thu Mar 27
Fri Mar 28
Sat Mar 29
Sun Mar 30
Mon Mar 31
Tue Apr 1
Bytes


Packets
sniffer : 3 : 15.0.73.141
Thu Mar 27 2003 - Tue Apr 01 2003
18.14K
13.61K
9.07K
4.54K
0
Packets per Day
Thu Mar 27
Fri Mar 28
Sat Mar 29
Sun Mar 30
Mon Mar 31
Tue Apr 1
Packets

Back to top.

RMON2 Traffic Profiling

Daily Host Detail

The Host Detail Report presents a breakdown of the hosts and protocols which contribute to the total traffic on an interface. Select an interface and a time period to see a list of hosts that had the most impact on the interface utilization for the time period selected. Select a host device to see a list of hosts / protocols accessed by the host through the selected interface. Select a host / protocol combination to see graphs of its historical traffic patterns.

Probe List

Probe	Interface	Busy Hour Utilization
sniffer	3	0.01

Peak Hourly Utilization

Day	Busy Hour Utilization
April 1, 2003	0.01
March 31, 2003	0.01
March 30, 2003	0.01
March 29, 2003	0.01
March 28, 2003	0.01
March 27, 2003	0.01

Top Talking Hosts

Host	Busy Hour Utilization	% of Daily Traffic	Bytes	Average Bytes per Packet
15.0.73.141	0.00	2.62	1392.39 k	103.06
15.243.128.51	0.00	8.37	4449.27 k	255.90
15.0.73.150	0.00	19.71	10.47 M	195.72
15.8.155.228	0.00	14.26	7574.20 k	731.81
15.1.158.148	0.00	13.96	7416.62 k	288.33
15.244.60.106	0.00	0.55	294.47 k	130.18
15.244.60.239	0.00	0.46	242.46 k	116.62
15.0.73.2	0.00	0.45	236.80 k	115.23
15.0.73.146	0.00	7.43	3945.02 k	106.39

Host Owner

Unassigned

Host Location

Unassigned

Top Talking Host / Protocol Pairs

Destination Host	Protocol	Busy Hour Utilization	% of Daily Traffic	Bytes	Average Bytes per Packet
15.243.128.51	wildcard.ip.udp.dns	0.00	0.13	70.12 k	85.30
15.13.218.121	wildcard.ip.udp.snmp	0.00	0.04	21.53 k	97.00
15.61.226.191	wildcard.ip.udp.snmp	0.00	0.03	15.71 k	97.00
15.244.37.53	wildcard.ip.udp.snmp	0.00	0.02	11.05 k	98.67
15.244.36.67	wildcard.ip.udp.snmp	0.00	0.02	11.05 k	98.67

Destination Host Owner

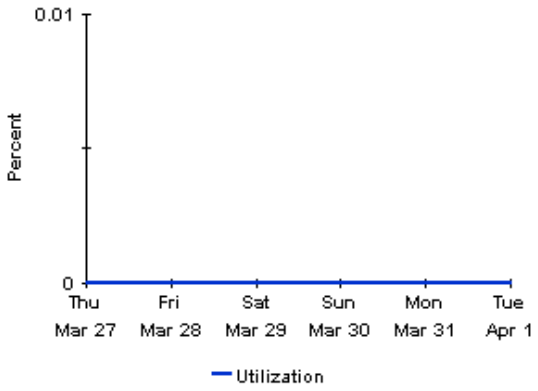
Unassigned

Destination Host Location

Unassigned

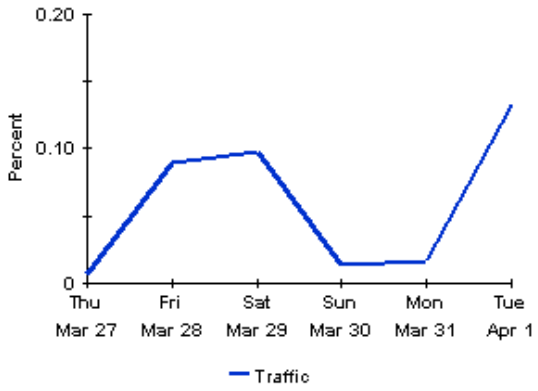
Busy Hour Utilization

Thu Mar 27 2003 - Tue Apr 01 2003



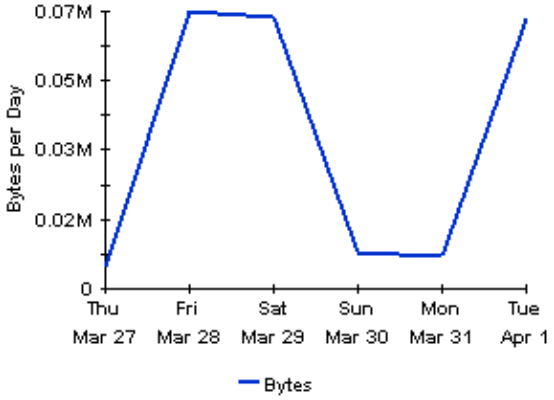
% of Daily Traffic

Thu Mar 27 2003 - Tue Apr 01 2003



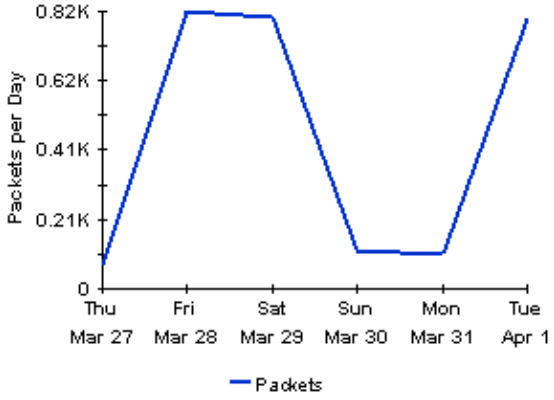
Bytes

Thu Mar 27 2003 - Tue Apr 01 2003



Packets

Thu Mar 27 2003 - Tue Apr 01 2003



Back to top.

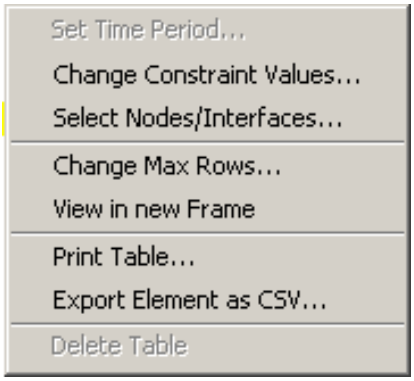
A Editing Tables and Graphs

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

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

View Options for Tables

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



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

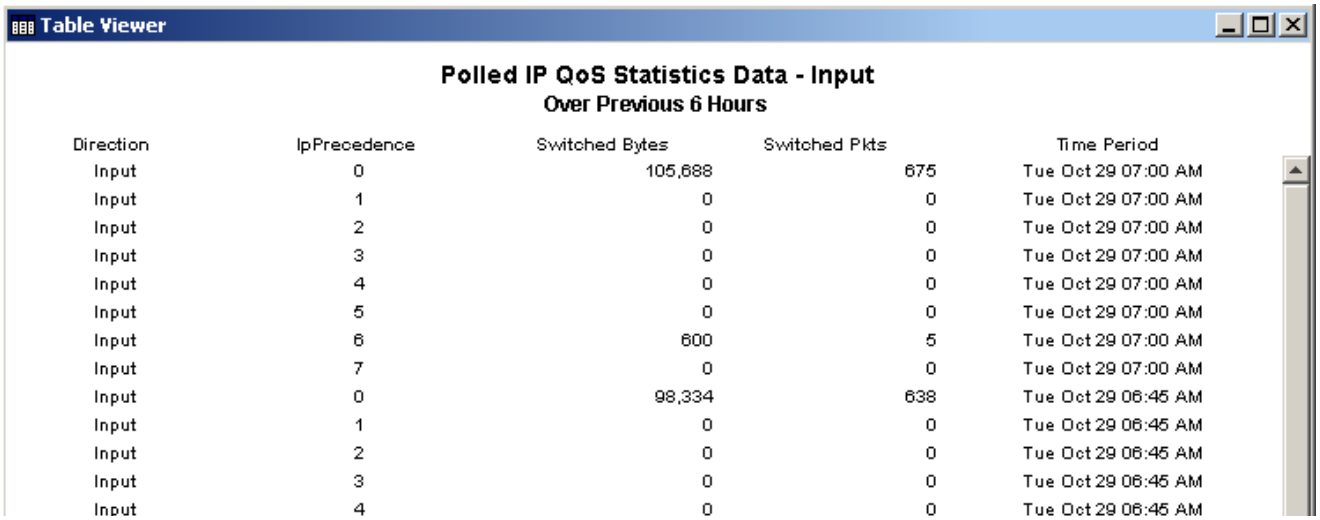
You may shorten the period of time covered by the table from, for example, 42 days to 30 days or to 7 days. If you are interested in a specific period of time that starts in the past and stops *before* yesterday, click **Use Absolute Time** and select a Start Time and an End Time.

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

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

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

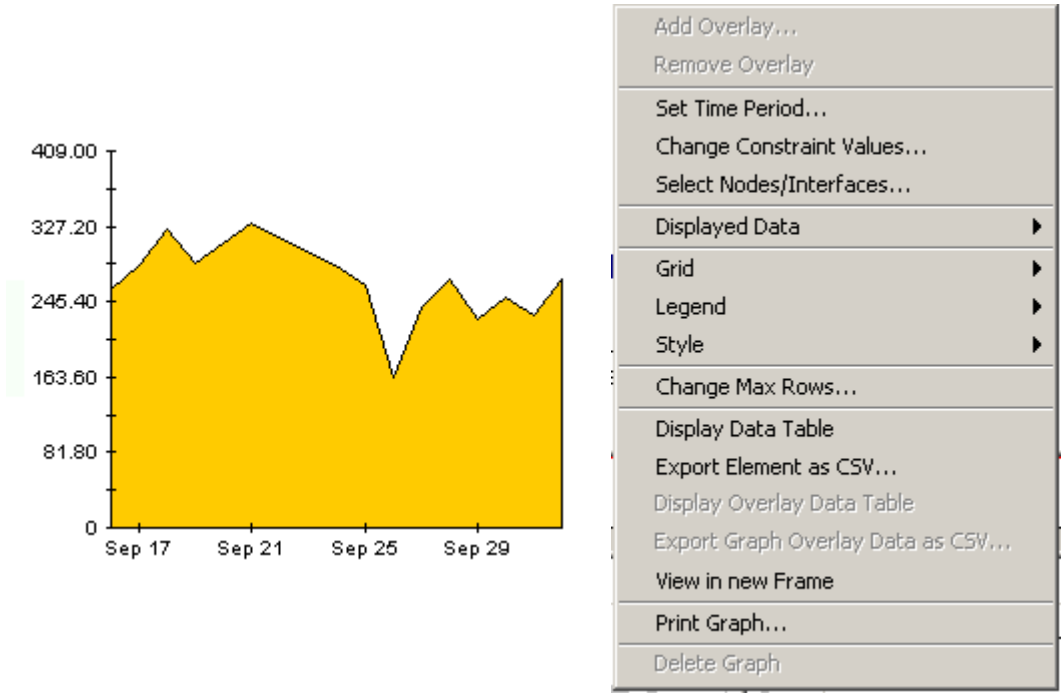
View in new Frame opens the table in a Table Viewer window, shown below. If necessary, make the data in the table more legible by resizing the window.



Direction	IpPrecedence	Switched Bytes	Switched Pkts	Time Period
Input	0	105,688	675	Tue Oct 29 07:00 AM
Input	1	0	0	Tue Oct 29 07:00 AM
Input	2	0	0	Tue Oct 29 07:00 AM
Input	3	0	0	Tue Oct 29 07:00 AM
Input	4	0	0	Tue Oct 29 07:00 AM
Input	5	0	0	Tue Oct 29 07:00 AM
Input	6	600	5	Tue Oct 29 07:00 AM
Input	7	0	0	Tue Oct 29 07:00 AM
Input	0	98,334	638	Tue Oct 29 06:45 AM
Input	1	0	0	Tue Oct 29 06:45 AM
Input	2	0	0	Tue Oct 29 06:45 AM
Input	3	0	0	Tue Oct 29 06:45 AM
Input	4	0	0	Tue Oct 29 06:45 AM

View Options for Graphs

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

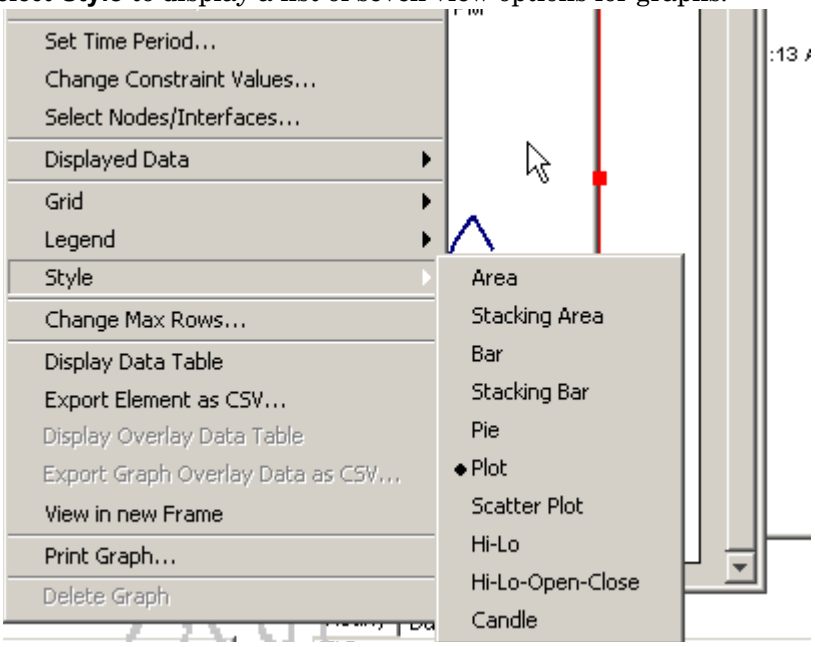


The following table provides details about each option.

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

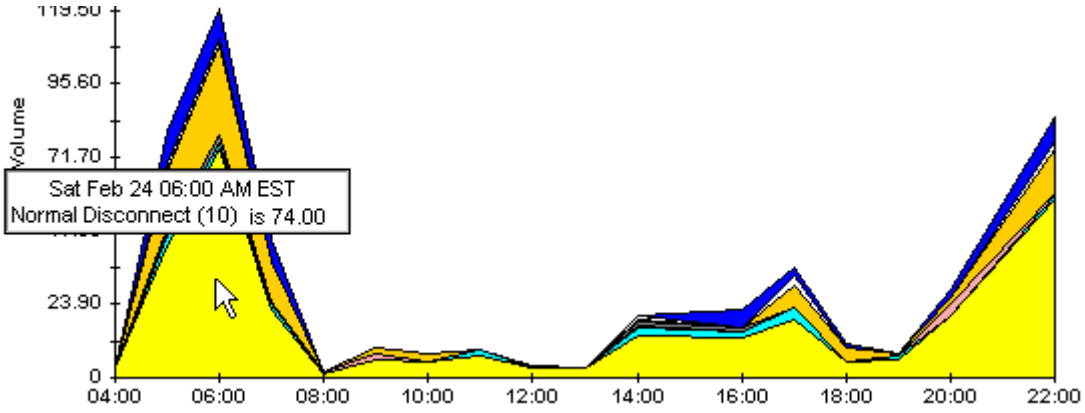
Style Options

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



Style > Area

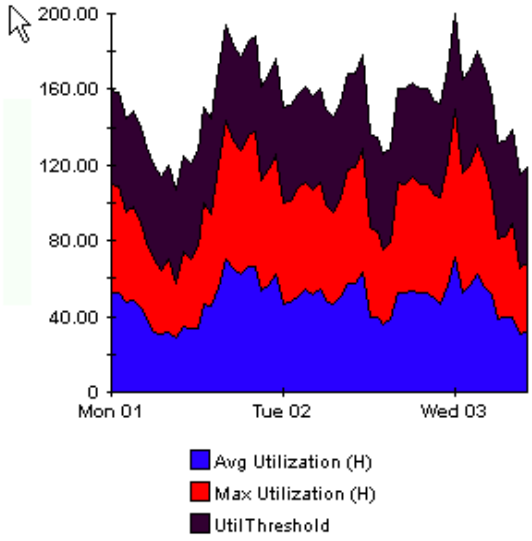
The plot or bar chart changes to an area graph. While relative values and total values are easy to view in this format, absolute values for smaller data types may be hard to see. Click anywhere within a band of color to display the exact value for that location



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

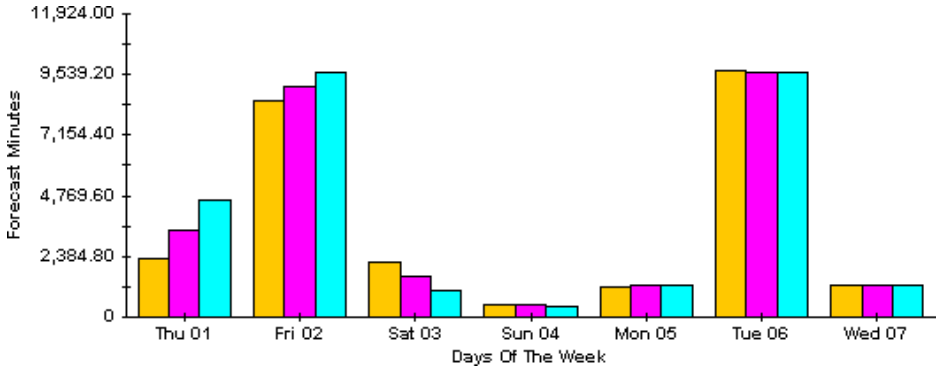
Style > Stacking Area

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



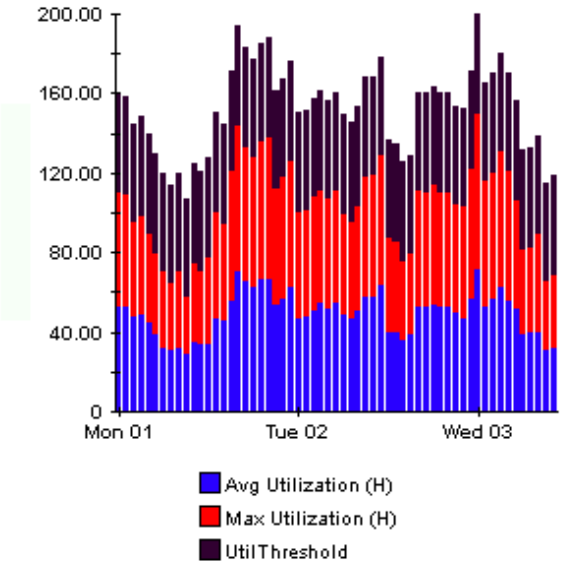
Style > Bar

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



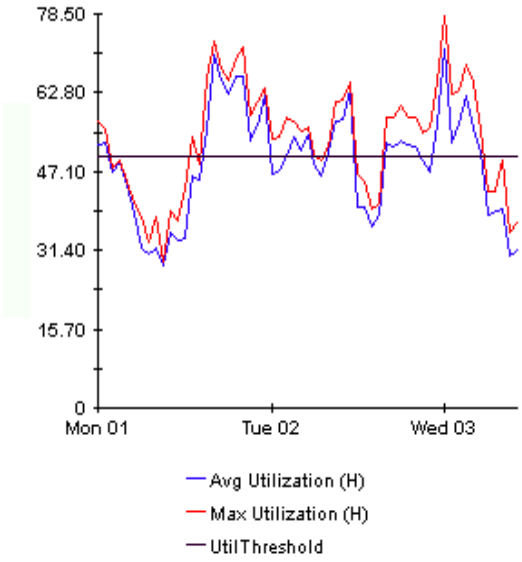
Style > Stacking Bar

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



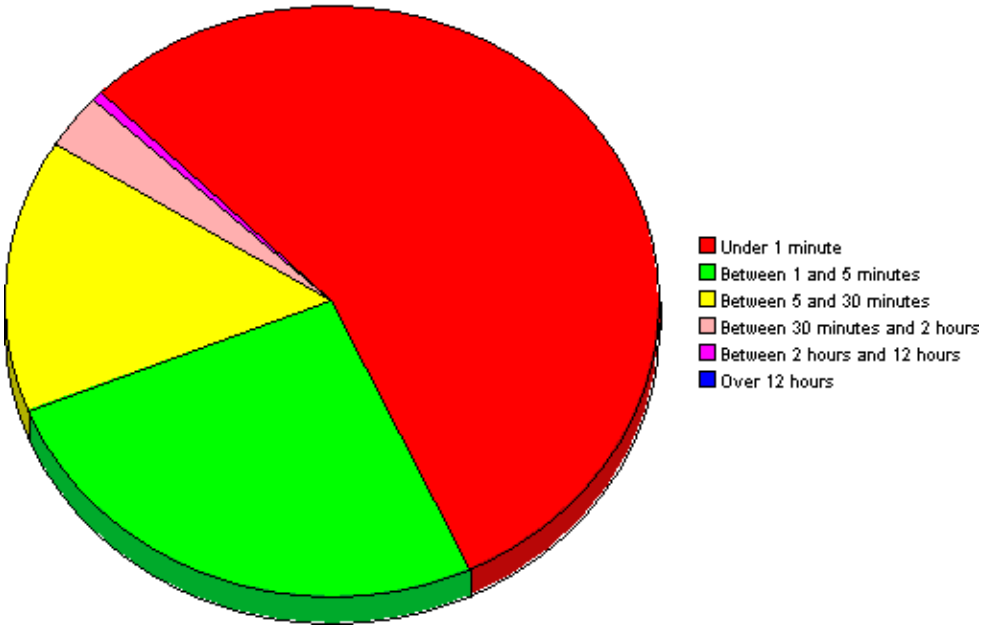
Style > Plot

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



Style > Pie

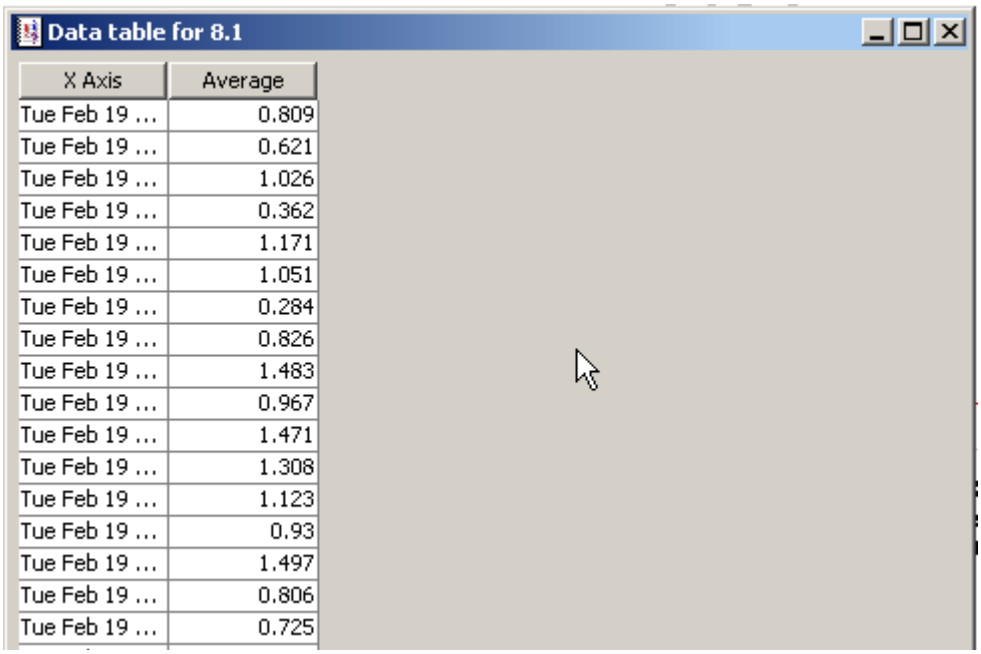
An area graph becomes a pie chart. Bands in an area graph convert to slices of a pie and the pie constitutes a 24-hour period. This view is helpful when a small number of data values are represented and you are looking at data for one day.



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

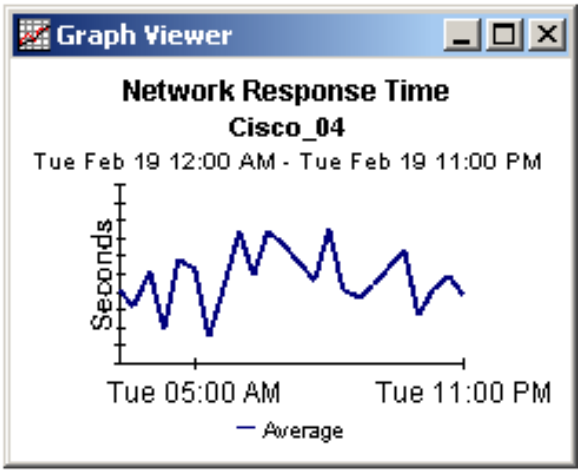
Display Data Table

This option changes a graph into a spreadsheet.



View in New Frame

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



Glossary

average bytes per packet

The average number of bytes per packet passed by the host or application or passed between the source/destination.

busy hour utilization

The maximum hourly average for the day. Unlike the average for the day, this value does not smooth out daily peaks and valleys. Unlike daily maximum, or peak, this value represents a relatively persistent phenomenon, not a momentary condition. Note that since busy hour is an average, actual utilization may have been well above the average for a portion of that hour.

bytes

The number of bytes passed by the host or application or passed between the source/destination.

day

The day of the year for which the information was collected.

destination

Where the application/protocol traffic is going.

host

Where the application/protocol traffic is coming from.

hour

The hour for which the information was collected.

interface

The network interface number of the probe.

month

The month for which the information is collected.

packets

The total number of packets passed by the host or application or passed through the source/destination.

percentage of traffic

The percentage of traffic attributed to the host, application, or source/destination in relation to the total traffic passing through the interface.

probe

The name of an RMON2 probe.

protocol

The name of the protocol through which the network traffic is being routed.

source

See **host**.

utilization

The percentage of system resources used for one hour, beginning at the listed time.

Index

Symbols

% of traffic, 43

A

Agilent, 8

almatrix reports, 8, 23
    hourly detail example, 24
    hourly summary example, 26

average bytes per packet, 43

B

busy hour utilization, 43

bytes, 43

C

central server
    configure, 21
    install report pack, 14
    upgrade report pack, 14

change max rows option, 37

Cisco NAM, 8

collection_manager (command), 14, 15

command line options
    ConfigAlMatrix.pl, 20

Common Property Tables
    upgrade, 16

ConfigAlMatrix.pl, 20
    options, 20

configure
    central server, 21
    polling group, 19
    satellite server, 22
    SNMP variables, 19

custom data table views, 15

customer-specific reports, 10

custom views of data or property tables, 15

D

Datapipe Manager, 15

day, 43

demo package, 11

destination, 43

detail reports, 9

Display Data Table, 37

displayed data option, 37

distributed systems guidelines, 14

E

editing parameters, 10

extract package, 15

G

graph view options, 35

grid options, 37

group_manager (command), 14, 15

group filters, 10

H

host, 43

host reports, 9, 23
    daily summary example, 28

hour, 43

I

install package, 15

interface, 43

L

legend options, 37

M

month, 43

N

NetScout, 8

P

package
- extract, 15
- folders, 16
- remove, 17
- uninstall, 17
- upgrade, 16

packets, 43

percentage of traffic, 43

polling group
- configure, 19

polling policies, 14

Polling Policy Manager, 19

probe, 44

Product Manuals Search (web page), 11

protocol, 44

R

remote pollers, 14

remove package, 17

reports
- almatrix, 8, 23
- daily host summary example, 28
- detail, 9
- host, 9, 23
- hourly almatrix detail example, 24
- hourly almatrix summary example, 26
- summary, 9
- top ten, 9
- top ten example, 23

resources
- RMON, 7

S

satellite server, 22
- configure, 22
- install report pack, 14
- upgrade report pack, 14

source, 43

style options for graphs, 37

summary reports, 9

supported RMON2 probes, 8

T

table view options, 35

top ten reports, 9
- example, 23

trendcopy pull commands, 21

trendtimer.sched, 22

U

uninstall package, 17

upgrade
- central server, 14
- Common Property Tables, 16
- RMON2 Traffic Profiling package, 16
- satellite server, 14

Use Absolute Time, 35

utilization, 44

V

variables
- configure, 19

view in new frame, 36