

HP OpenView Performance Insight

RMON2 Traffic Profiling Report Pack User Guide

Software Version: 2.0

Reporting and Network Solutions 6.0



September 2004

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

Legal Notices

Warranty

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

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

Restricted Rights Legend

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

Hewlett-Packard Company
United States of America

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

Copyright Notices

© Copyright 2003–2004 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.

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

- Chapter 1 Overview** 7
 - OVPI and RMON2 Probes 7
 - Objects, Reports, and Groups 8
 - Ways to Customize Reports 9
 - Sources for Additional Information 11

- Chapter 2 Package Installation** 13
 - Guidelines for a Smooth Install 13
 - Installing RMON2 Traffic Profiling 2.0 15
 - Package Removal 17

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

- Chapter 4 Distributed Systems** 21
 - Configuring the Central Server 21
 - Configuring a Satellite Server 22
 - System Clocks 22

- Chapter 5 Five Sample Reports** 23
 - Report Descriptions 23
 - View Options for Tables and Graphs 34

- Glossary** 35

- Index** 37

Overview

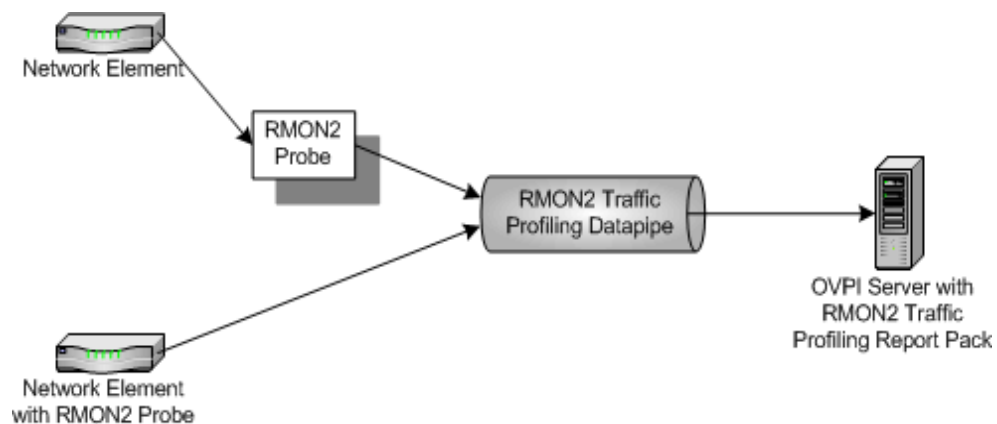
This overview covers the following topics

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

OVPI and RMON2 Probes

An RMON2 probe queries network elements for information about network traffic and stores the results in an SNMP MIB. The information in the MIB indicates where network traffic is going, traffic volume, and which protocols are involved.

The figure below shows the RMON2 Traffic Profiling Datapipe collecting data from the RMON2 MIB and loading the results into OpenView Performance Insight (OVPI).



OVPI processes the data collected by the datapipe, creating trending analysis for:

- Utilization
- Percentage of total interface traffic
- Bytes
- Average bytes per packet

Supported Probes

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	RNS Version and Release Date	Features/Enhancements
1.0	RNS 3.0, May 2003	15 reports; Sybase support
2.0	RNS 4.0, October 2003	OVPI Object Manager support
2.0	RNS 5.0, April 2004	No changes
2.0	RNS 6.0, August 2004	No changes

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 and view RMON2 Traffic Profiling remotely, 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:

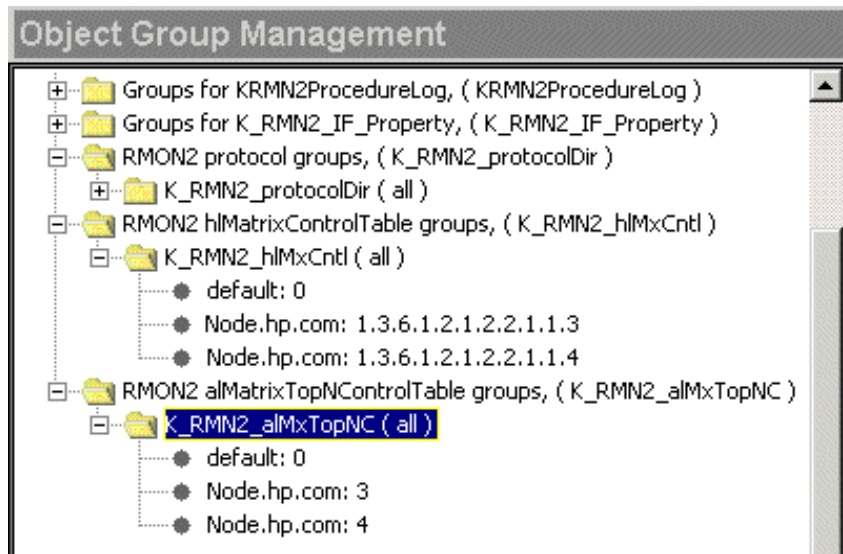
- Daily Top Ten
- Hourly Top Ten
- Monthly Top Ten

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 longer-standing trend that requires corrective action.

Detail reports drill down further on Summary report data, allowing you to see the contribution of source/destination and host/protocol combinations.

Top Ten reports provide two lists, the protocols that had the greatest impact on interface utilization, and the hosts that 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 applying group filters, editing parameters, editing tables and graphs, and importing location data. While group filters are designed for service providers who need 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 will need customer-specific reports containing data limited to one customer. 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 creating filters for group accounts, refer to the *Performance Insight Administration Guide*.

Editing Parameters

When you edit a parameter, you apply a constraint to the report that eliminates the data you are not interested in seeing. For example, if you edit the ProbeName parameter, only data for the probe you typed in the ProbeName field appears in the report, and data for all other probes drops out of the report. You can apply multiple constraints at the same time. RMON2 Traffic Profiling supports the following parameters:

- ProbeName
- Interface_Name
- IF_Customer_Name
- IF_Customer_ID
- Start_Time
- End_Time
- Client_Name (of source)
- Server_Name (of destination)
- Application_Name (of protocol)

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 2.0 Release Statement*
- *RNS 6.0 Release Notes, August 2004*
- *Common Property Tables 3.5 User Guide*
- *Interface Discovery Datapipe 2.0 User Guide*

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

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

Select **Technical Support** > **Product Manuals** to reach the **Product Manuals Search** page. The user guides for the core product are listed under **Performance Insight**. The user guides for report packs, datapipes, and the value-add components for NNM are listed under **Reporting and Network Solutions**.

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

Package Installation

This chapter covers the following topics:

- [Guidelines for a Smooth Install](#)
- [Installing RMON2 Traffic Profiling 2.0](#)
- [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 performance data in a specific way.

The RNS 6.0 CD includes NNM components as well as OVPI components. When you insert the CD, launch the package extraction interface, and select OVPI report packs for extraction, the install script extracts every OVPI package from the CD and copies the results to the Packages directory on your system. When the extraction process finishes, the install script prompts you to launch Performance Insight and 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
- All available service packs for OVPI 5.0
- Common Property Tables 2.2 or higher
- Interface Discovery Datapipe 2.0

If you are not currently running any version of the Interface Discovery Datapipe or any version of Common Property Tables, you may install these packages when you install RMON2 Traffic Profiling 2.0.

If you are running Common Property Tables 2.2, you have the option of upgrading to version 3.0 or version 3.5. Installing the upgrade package is easy; however, you cannot install the 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.

Datapipes cannot be upgraded. If you are currently running an earlier version of the Interface Discovery Datapipe, first remove your earlier version, then install the new version.

Upgrading to RMON2 Traffic Profiling 2.0

If you are already familiar with Package Manager, you should have no difficulty installing the upgrade package. Keep in mind that you will need to 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 RNS 6.0 CD.
- 2 If desired, upgrade to Common Property Tables 3.0 or 3.5.
- 3 Delete these packages:
 - Interface Discovery Datapipe 1.1
 - RMON2 Traffic Profiling Datapipe 2.0
- 4 Install Interface Discovery Datapipe 2.0.
- 5 Install UPGRADE RMON2 Traffic Profiling 1.0-to-2.0.
- 6 Install RMON2 Traffic Profiling Datapipe 2.0.
- 7 Restart OVPI Timer.

Polling Policies for Remote Pollers

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

- Polling policies for remote pollers
- Multi-poller polling policies
- 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 Data Table Views

If you created custom data table views using existing property table views, drop the custom data table views now, before upgrading the report pack. Dropping views will not result in lost data.

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 the central server and every satellite server are running OVPI 5.0 and all available service packs for OVPI 5.0.
- 2 Disable `trendcopy` on the central server.
- 3 Install RMON2 Traffic Profiling 2.0 on the central server.
- 4 Install RMON2 Traffic Profiling 2.0 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 aggregations at each satellite server. For details, see [Chapter 4, Distributed Systems](#).

Installing RMON2 Traffic Profiling 2.0

Complete the following tasks to install RMON2 Traffic Profiling 2.0:

- Stop OVPI Timer and extract OVPI packages from the RNS CD
- Upgrade to Common Property Tables 3.0 or higher (optional)
- Install RMON2 Traffic Profiling

Task 1: Stop OVPI Timer and extract OVPI packages from the RNS 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 RNS 6.0 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.

Task 2: Upgrade to Common Property Tables 3.0 or higher (optional)




If you are not running any version of Common Property Tables, skip this task.

The RMON2 Traffic Profiling Report Pack 2.0 requires Common Property Tables 2.2. You have the option of running version 2.2 or upgrading to version 3.0 or version 3.5. If you install an upgrade package, 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 installation finishes, 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 2.0*
 - *RMON2 Traffic Profiling Demo*

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

 - *RMON2 Traffic Profiling Datapipe 2.0*
 - *Interface Discovery Datapipe 2.0* (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`

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 Datapipe*
 - *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**

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

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
<code>hlMatrixControlNIMaxDesiredEntries</code>	<code>.1.3.6.1.2.1.16.15.1.1.6</code>	6,000
<code>hlMatrixControlAIMaxDesiredEntries</code>	<code>.1.3.6.1.2.1.16.15.1.1.10</code>	12,000
<code>hlMatrixControlStatus</code>	<code>.1.3.6.1.2.1.16.15.1.1.12</code>	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, the MIB objects are set to the values listed in the preceding table. Modifying these MIB objects changes the amount of data collected.

Distributed Systems

This chapter covers the following topics:

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

If you intend to run RMON2 Traffic Profiling 2.0 in a distributed environment, and you followed the advice in the installation chapter, the central server is running the report pack and each satellite server is running the report pack and the datapipe. Your next task is to set up connections with satellite server databases, configure trendcopy pull commands, and switch off hourly and daily aggregations at each satellite 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 e and e for each additional database.
 - g Click **Finish** when you finish adding databases.
- 2 Edit the file `$DPIPE_HOME/scripts/RMN2_Hourly.pro`:
 - a Comment out blocks 1 through 4 by adding the comment sign (“#”) before the word **begin** and the word **end**.
 - b 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.

c Save and close `$DPIPE_HOME/scripts/RMN2_Hourly.pro`.

3 Edit this file: `$DPIPE_HOME/scripts/RMN2_Daily.pro`

a Comment-out blocks 1 and 2 by adding the comment sign (“#”) before the word **begin** and the word **end**.

b For each satellite server, configure trendcopy pull commands 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.

c Save and close `$DPIPE_HOME/scripts/RMN2_Daily.pro`.

Configuring a Satellite Server

Switch off hourly and daily aggregations on the satellite server. 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.

Five Sample Reports

This chapter provides:

- Brief report descriptions
- A screen shot of selected reports
- Information about view options for tables and graphs

Report Descriptions

RMON2 Traffic Profiling includes 15 interactive 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 contributors 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

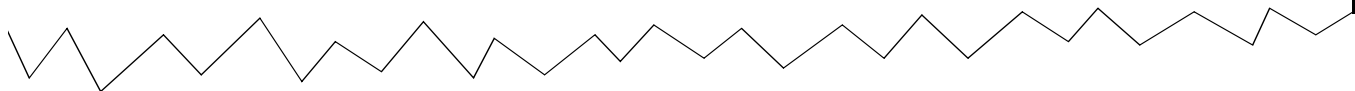
Month	Busy Hour Utilization
April, 2003	1.17
March, 2003	0.69 

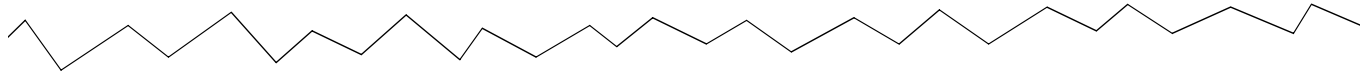
Top Ten Hosts

	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	0.86
10	wildcard.ip.tcp.dns	0.01	0.33



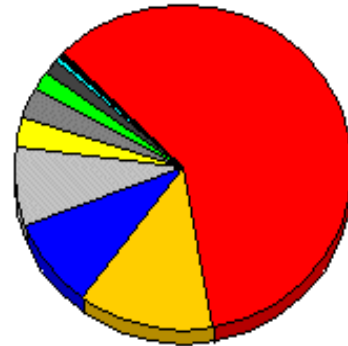


Host Distribution
Top Ten Hosts



■ : 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.top.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.top.sunrpc :
 ■ 3: sniffer : 3 : wildcard.ip.top.http :

RMON2 Traffic Profiling

Hourly ALMATRIX Summary

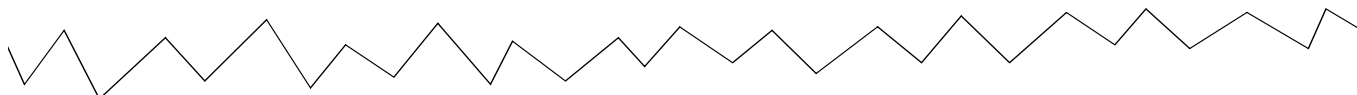


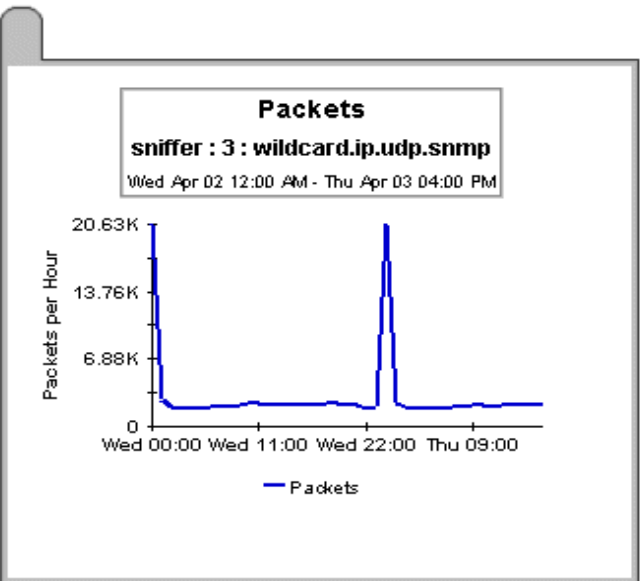
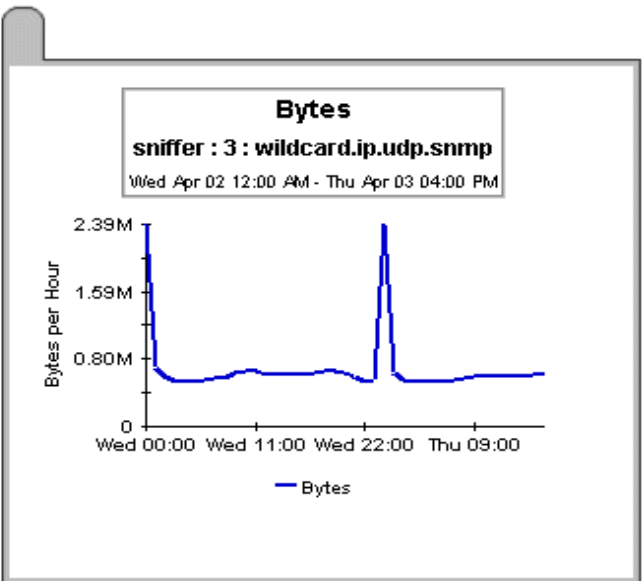
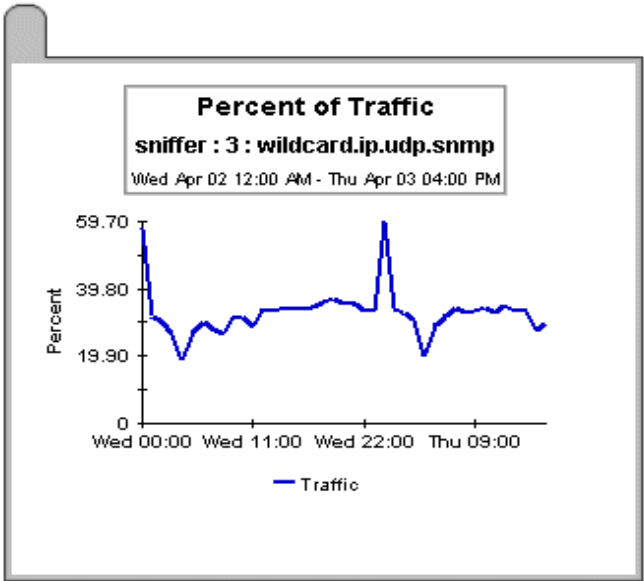
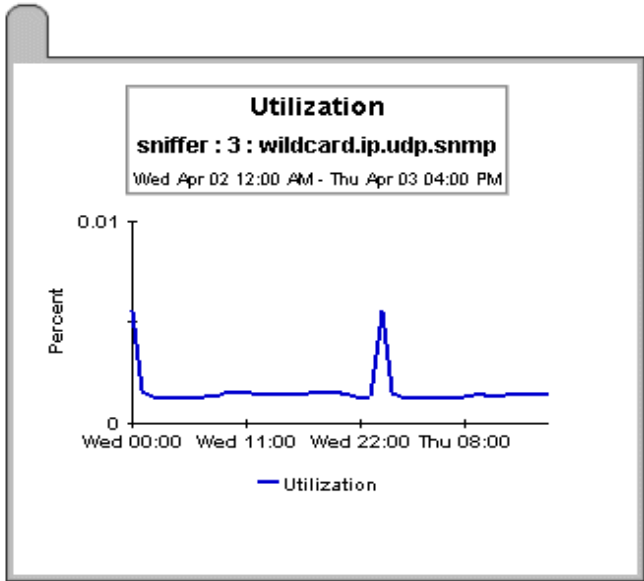
The ALMATRIX Summary Report presents a breakdown of the protocols which contribute to the total traffic on an interface. Select an interface and a time period to see a list of protocols that had the most impact on the interface utilization for the time period selected. Select a protocol to see graphs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

Probe List			Hourly Utilization	
Probe	Interface	Utilization	Hour	Utilization
sniffer	3	0.00	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





[↑ 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

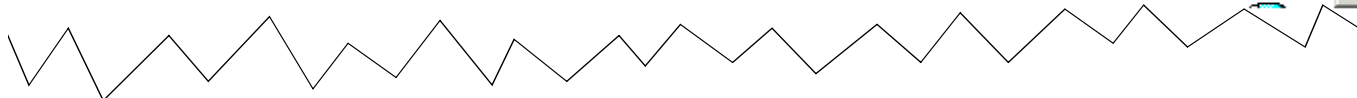
Hour	Utilization
4:00 PM, April 3, 2003	0.00
3:00 PM, April 3, 2003	0.01
2:00 PM, April 3, 2003	0.00
1:00 PM, April 3, 2003	0.00
12:00 PM, April 3, 2003	0.00
11:00 AM, April 3, 2003	0.00
10:00 AM, April 3, 2003	0.00

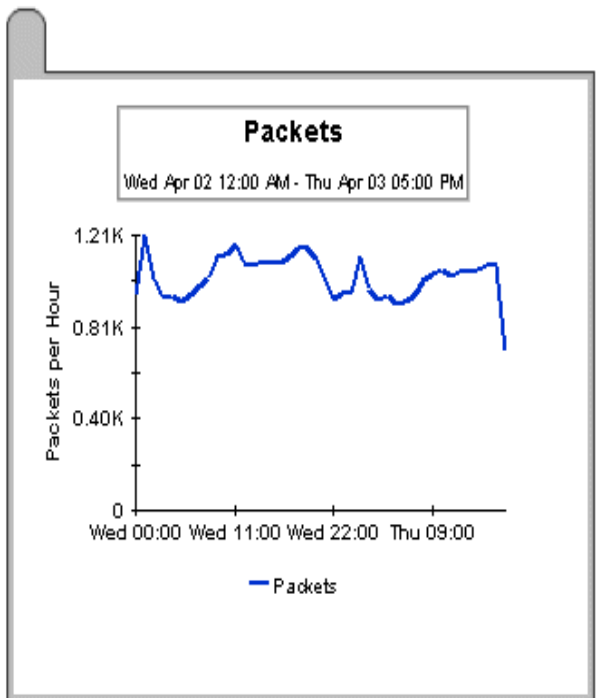
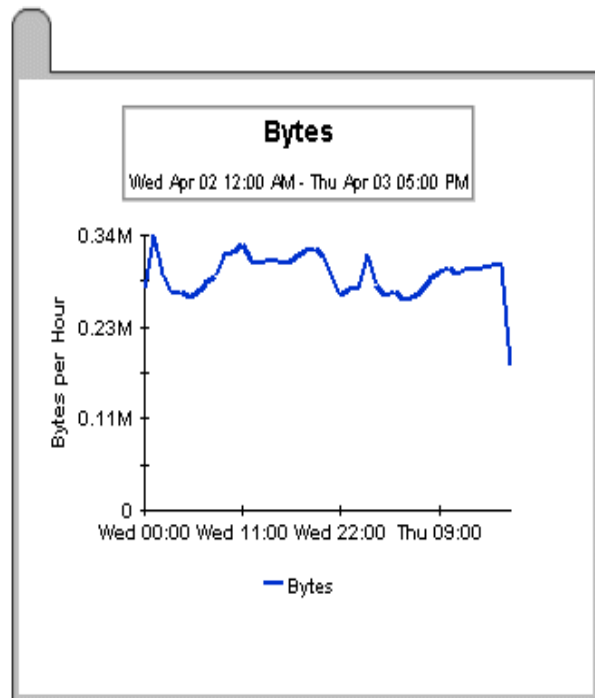
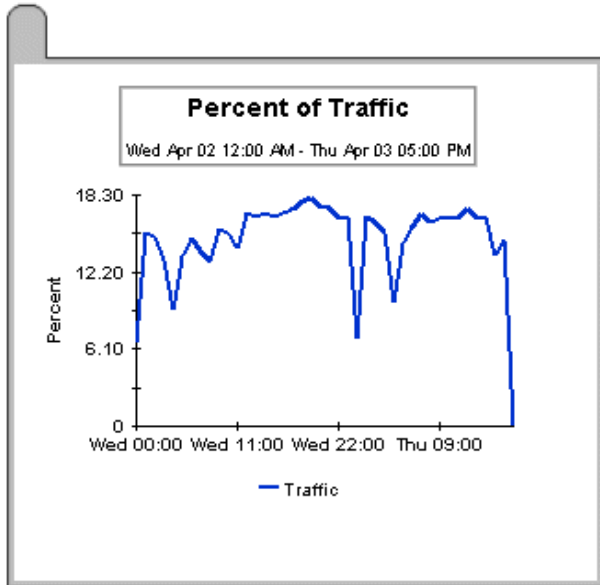
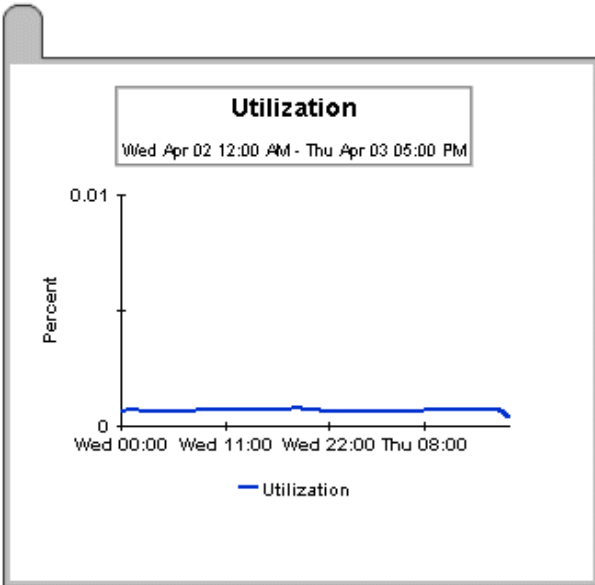
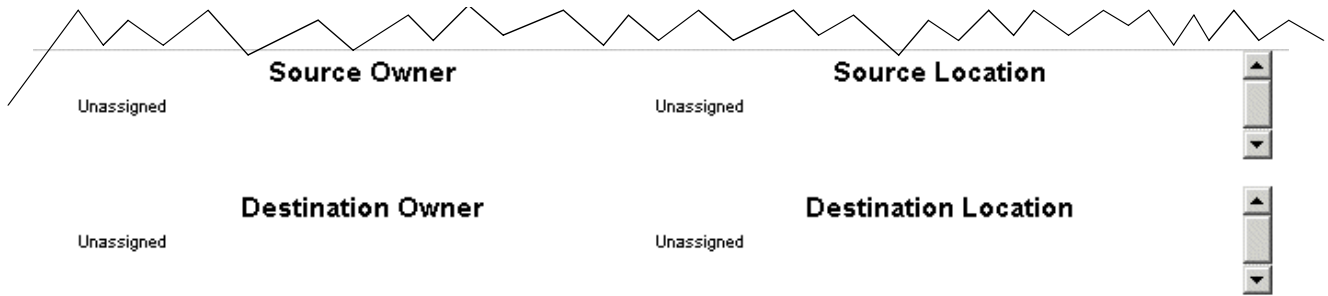
Top Talking Protocols / Applications

Protocol	Utilization	% of Traffic	Bytes	Average Bytes per Packet
wildcard.ip.udp.snmp	0.00	29.73	637.70 k	286.35
wildcard.ip.top.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.top.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





[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

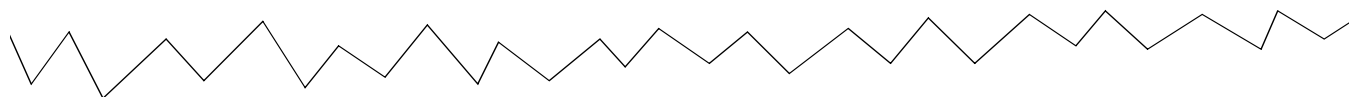
Host Owner

Unassigned

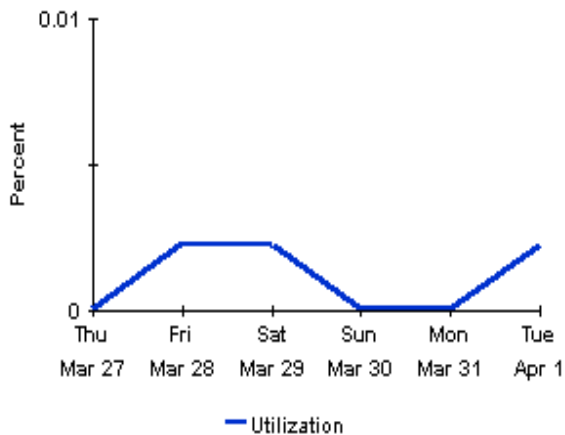
Host Location

Unassigned

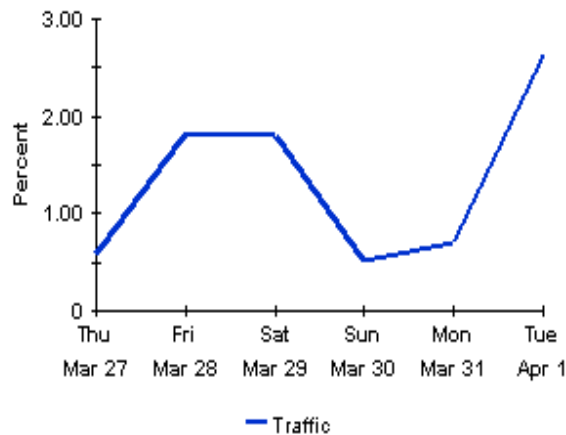




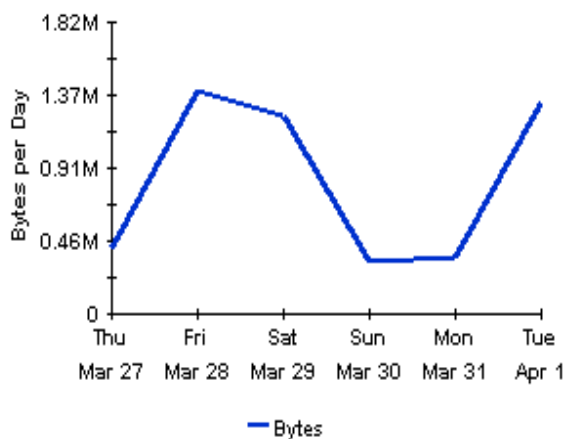
Busy Hour Utilization
sniffer : 3 : 15.0.73.141
Thu Mar 27 2003 - Tue Apr 01 2003



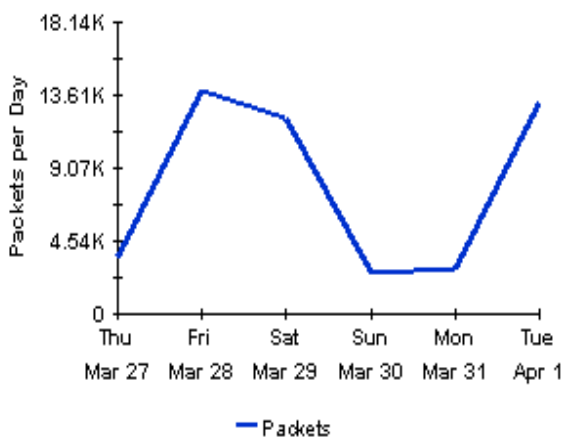
% of Daily Traffic
sniffer : 3 : 15.0.73.141
Thu Mar 27 2003 - Tue Apr 01 2003




Bytes
sniffer : 3 : 15.0.73.141
Thu Mar 27 2003 - Tue Apr 01 2003



Packets
sniffer : 3 : 15.0.73.141
Thu Mar 27 2003 - Tue Apr 01 2003



 [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

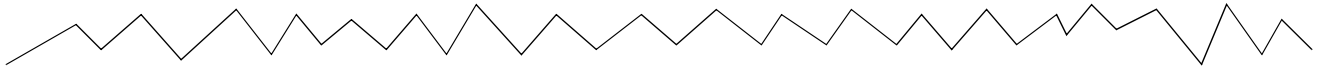
Unassigned

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

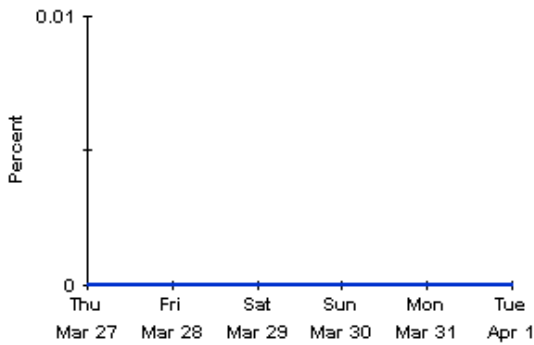
Destination Host Location

Unassigned



Busy Hour Utilization

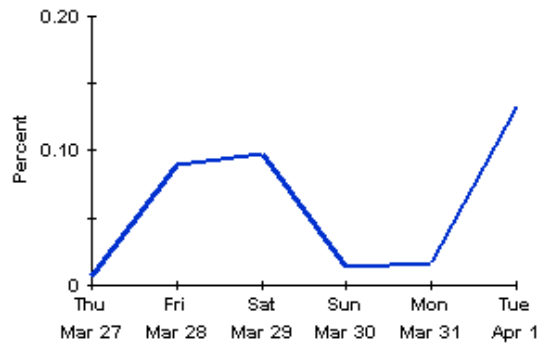
Thu Mar 27 2003 - Tue Apr 01 2003



— Utilization

% of Daily Traffic

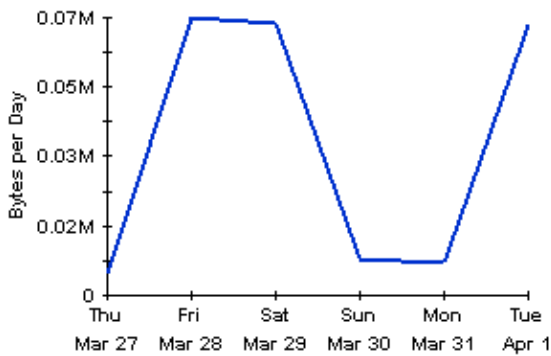
Thu Mar 27 2003 - Tue Apr 01 2003



— Traffic

Bytes

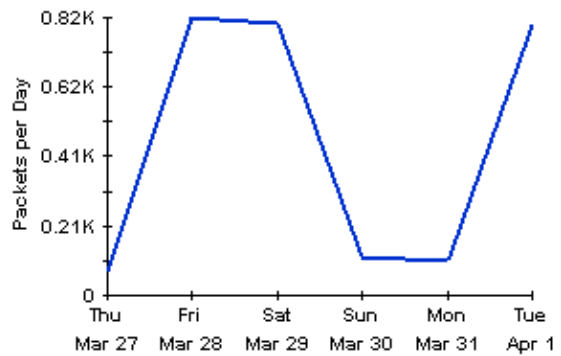
Thu Mar 27 2003 - Tue Apr 01 2003



— Bytes

Packets

Thu Mar 27 2003 - Tue Apr 01 2003



— Packets

[Back to top.](#)



View Options for Tables and Graphs

There are multiple ways to view the tables and graphs in reports. Although the default view may be the view you use most of the time, you can easily change to a different view.

Report Viewer: Right-Click the Object

If you are looking at a report using Report Viewer (part of the OVPI client component), follow these steps to change your default view of a table or graph:


- 1 With your cursor on the table or graph, right-click. The options list opens.
- 2 Select one of the view options.

You can customize the following table and graph view options:

- Set Time Period — alter the relative time or set an absolute time period
- Change Constraint— display or do not display grid lines
- Legend (*graph only*) — reposition a graph's legend
- Style (*graph only*) — change the type of graph displayed
- Change Max Rows — display more rows of data or display fewer rows of data
- Display Data Table/Display Overlay Data Table (*graph only*) — display data for every point on a graph in a spreadsheet

Web Access Server: Click the Edit Icon

If you are looking at a report using the Web Access Server, follow these steps to change your default view of a table or graph:

- 1 Specify element editing as a report reference:
 - a Click **Preferences** on the links bar.
 - b Expand **Reports** in the navigation frame.
 - c Click **Viewing**.
 - d Select the **Allow element editing** box.
 - e Click **Apply**.
- 2 Click on  (the Edit icon) next to the table or graph.

You can customize the following table and graph view options:

- Max Rows — display more rows of data or display fewer rows of data
- Constraints — display more data or display less data
- Time Range — alter the relative time or set an absolute time period
- Graph Style — change the type of graph displayed

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.

Symbols

% of traffic, **36**

A

Agilent, **8**

almatrix reports, **8, 23**

hourly detail example, **24**

hourly summary example, **26**

average bytes per packet, **35**

B

busy hour utilization, **35**

bytes, **35**

C

central server

configure, **21**

install report pack, **15**

upgrade report pack, **15**

Cisco NAM, **8**

collection_manager, **14**

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**

customize tables and graphs, **34**

D

day, **35**

demo package, **11**

destination, **35**

detail reports, **9**

distributed systems, **14**

distributed systems guidelines, **15**

E

editing parameters, **10**

extract package, **15**

G

graphs, customize, **34**

group_manager, **14**

group filters, **10**

H

host, **35**

host reports, **8, 23**

daily summary example, **28**

hour, **35**

I

install package, **15**

interface, **35**

M

month, **35**

N

NetScout, **8**

P

- package
 - extract, **15**
 - folders, **16**
 - remove, **17**
 - uninstall, **17**
 - upgrade, **16**
- packets, **35**
- percentage of traffic, **36**
- polling group
 - configure, **19**
- polling policies, **14**
- Polling Policy Manager, **19**
- probe, **36**
- Product Manuals Search (web page), **11**
- protocol, **36**

R

- remote pollers, **14**
- remove package, **17**
- reports
 - almatrix, **8, 23**
 - customize tables and graphs, **34**
 - daily host summary example, **28**
 - detail, **9**
 - host, **8, 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, **15**
 - upgrade report pack, **15**
- source, **35**
- summary reports, **9**
- supported RMON2 probes, **8**

T

- tables, customize, **34**

- top ten reports, **9**
 - example, **23**
- trendcopy pull commands, **21, 22**
- trendtimer.sched, **22**

U

- uninstall package, **17**
- upgrade
 - central server, **15**
 - Common Property Tables, **16**
 - RMON2 Traffic Profiling package, **16**
 - satellite server, **15**
- utilization, **36**

V

- variables
 - configure, **19**