Service Assurance Report Pack

Software Version 3.1

HP OpenView Performance Insight

User Guide

June 2005

Legal Notices

Warranty

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

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

Restricted Rights Legend

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

Hewlett-Packard Company
United States of America

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

Copyright Notices

© Copyright 2002 - 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

Java™ is a US trademark of Sun Microsystems, Inc.

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

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

UNIX® is a registered trademark of The Open Group.

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

Support

Please visit the HP OpenView web site at:

http://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
SAA and the Service Assurance Report Pack 7
Folders and Reports 9
Integration with Network Node Manager 11
Ways to Customize Reports 12
Sources for Additional Information 13

2 The Upgrade Install 15
Guidelines for a Smooth Upgrade 15
Distributed Environments 17
Installing Upgrade Packages and New Datapipes 17

3 The New Install 21
Guidelines for a Smooth Install 21
Installing Service Assurance 3.1 22
Package Removal 25

4 Router Configuration 27
CiscoSAA_Config 27
Using an XML Block to Define an Operation 28
Configuration Script Syntax 28
Delete Script Syntax 29
Other Approaches to Configuring SAA Tests 29

5 Package Configuration 31
Defaults in Service_Assurance_Thresholds 31
The Thresholds Form 32
Distributed Systems 33

6 Ranking Exception Counts 37

7 Aggregating Performance Data 47

8 Forecasting Future Performance 55

9 Ranking the Worst Performers 61

10 Sample Data in Near Real Time 67

11 Monitoring Jitter 75

A Editing Tables and Graphs 83

View Options for Tables 83
View Options for Graphs 84
Index 91

1 Overview

This chapter covers the following topics:

- SAA and the Service Assurance Report Pack
- Folders and reports
- Integration with Network Node Manager (NNM)
- Ways to customize reports
- Sources for additional information

SAA and the Service Assurance Report Pack

The following text is borrowed from a white paper from Cisco Systems:

> SAA is an embedded, synthetic performance-monitoring tool to measure service performance from the network perspective. Because SAA is embedded in Cisco IOS Software, it is platform independent from all Cisco routers and switches running Cisco IOS Software.
>
> Because SAA is an intelligent agent embedded in the router, it provides only raw statistics. The programmatic interface allows an external application to configure and retrieve performance metrics. The external application can then use the metrics to analyze and present the measurements graphically, as well as to generate service-level monitoring reports.

The raw statistics generated by SAA are stored in the CISCO-RTTMON-MIB. OpenView Performance Insight (OVPI) is an external application that polls this MIB and then processes the data it collects from the MIB in accordance with directives from the Service Assurance Report Pack. Using directives from the report pack, OVPI calculates the following statistics:

- Response time — round-trip time for specific SAA tests
- Exception counts — number of SAA tests that exceeded the threshold for response time
- Availability — the ratio of successful SAA tests to total tests
- Jitter — variation in the packet inter-arrival time
- Throughput — an estimate of the bytes per second transmitted during an SAA test
- Number of transactions — number of SAA tests completed
- Traffic volume — number of bytes sent and received by an SAA source device
- MOS — estimated Mean Opinion Score for VoIP tests

Datapipes and NRT Reports

If you use the Cisco SAA Datapipe and only the Cisco SAA Datapipe, you will have one NRT report, the NRT Summary report in the Source-Destination-Application folder. If you use the Cisco SAA NRT Datapipe and the Cisco SAA Datapipe, you will have three NRT reports.

The Cisco SAA NRT Datapipe polls data from the Latest Test Table. How often the Cisco SAA NRT Datapipe polls the Latest Test Table is configurable. Because the Service Assurance Agent may conduct tests at a frequency that varies from test to test, the frequency of polling should not exceed the frequency of testing. The maximum rate of polling is once every 5 minutes.

Configuring Routers for SAA Operations

The Service Assurance Agent will not operate unless someone configures it. Although the command line interface for IOS provides a way to configure SAA operations, run SAA operations, and view statistics, this approach to SAA configuration is awkward and slow, especially when multiple routers are involved. The Cisco SAA Datapipe includes a configuration utility that makes this task easier. You can use this utility to define which operations are conducted, the frequency of the operation, and the destination. For more information, see Chapter 4, Router Configuration.

Version History

The following table provides details about recent enhancements to Service Assurance.

Version	Release Date	Features/Enhancements
1.0	May 2003	32 reports Sybase support
2.0	October 2003	OVPI Object Manager support MPLS VPN Aware Test Modify SAA Thresholds (form)
3.0	April 2004	Oracle support Minor changes to property tables Minor changes to existing reports Removal of obsolete TEEL directives *new datapipe:* • CiscoSAA_NRT_Datapipe *new sub-package:* • Service Assurance NRT 1.0: — NRT - Latest Test — Jitter NRT
3.0	August 2004	*new upgrade packages:* • UPGRADE_Service_Assurance_to_3 • UPGRADE_Service_Assurance_Location_to_3

Version	Release Date	Features/Enhancements
3.0	November 2004	Service_Assurance_NRT 2.0: • VoIP NRT - Latest Test (new report) • Changes to NRT Latest Test: — Location — ToS — Tag • Changes to Jitter NRT: — Location — ToS — Tag CiscoSAA_Datapipe 5.5: • Improved performance of stored procedures • Support VoIP test (MOS data collection) CiscoSAA_NRT_Datapipe 2.0: • Improved performance of stored procedures • Support VoIP test (MOS data collection)
3.1	June 2005	*defect fixes:* Service_Assurance 3.1 Service_Assurance_Location 3.1 UPGRADE_Service_Assurance_to_31 UPGRADE_Service_Assurance_Location_to_31 CiscoSAA_Datapipe 5.6 CiscoSAA_NRT_Datapipe 2.1

There is no upgrade path for Service_Assurance_NRT. If you are running version 1.0 and you want to install version 2.0, your first step is to delete version 1.0. After deleting version 1.0, restart Package Manager and install version 2.0. Although you will lose data when you delete version 1.0, OVPI will quickly recollect the data that you lost.

Folders and Reports

Service Assurance 3.1 contains the following report folders:

- Application
- Customer
- Destination
- Jitter
- Location
- Source
- Source / Destination / Application
- NearRealTime

The following table provides a list of the reports in each folder.

Folder	Reports
Application	• Application Exceptions by Source/Destination • Application Forecast • Application Forecast by Source/Destination • Application Summary • Application Top Ten
Customer	• Customer Forecast • Customer Summary • Customer Top Ten
Destination	• Destination Exceptions by Source / Application • Destination Forecast • Destination Forecast by Source / Application • Destination Summary • Destination Top Ten
Jitter	• Jitter Destination Summary • Jitter Source/Destination Summary • Jitter Source Summary
Location	• Application Exceptions by Location / Destination • Application Forecast by Location / Destination • Destination Exceptions by Location / Application • Destination Forecast by Location / Application • Location Summary • Location Exceptions by Application / Destination • Location Forecast • Location Forecast by Application / Destination • Location Top Ten
Source	• Source Exceptions by Application / Destination • Source Forecast • Source Forecast by Application / Destination • Source Summary • Source Top Ten
Source/Dest/App	• Near Real Time Summary (collections once an hour) • Source Destination Application Summary
NRT	• Near Real Time - Latest Test • Jitter Near Real - Latest Test • VoIP Near Real Time - Latest Test

Following is a brief description of each generic report.

Exception. Shows elements that exceeded the predefined response time threshold during the previous day. The element can be a source, a destination, an application, or a location. Does not include jitter test results.

Summary. Displays aggregations of performance data for a particular perspective—a source, a destination, an application, a location, or a customer. Helps you identify anomalies and performance trends within the element group. Does not include jitter test results.

Forecast. Presents a summary of response time and throughput forecasts from different perspectives. Identifies the applications, sources, destinations, locations, or customers that are likely to have response time or throughput problems in the near future. Does not include jitter test results. Although some data will appear in forecast reports a few days after you install Service Assurance, reliable forecasting will not be available until the initial baseline is complete, about thirteen weeks after installation.

Top Ten. Identifies ten elements ranked by response time, throughput, and rate of change. Provides data tables for worst response time, projected response time, worst throughput, projected throughput, most transactions, and most traffic. Does not include jitter test results.

Near Real Time. Available in two flavors. The report in the Source/Destination/Application folder is produced from hourly data collected by the Cisco SAA Datapipe. This report provides a list of source/destination/application combinations with high exception counts. Updated hourly, this report also provides hourly and daily data for response time, throughput, transactions, traffic, exceptions, and availability. The three reports in the optional Service Assurance NRT module contain data collected by the Cisco SAA NRT Datapipe. These reports can be updated more frequently, as often as every 5 minutes.

Jitter. Displays total jitter tests and response time exceptions for each customer and deviation statistics for all devices belonging to each customer. Monitors response time, packet error types, deviation, and packet loss. Includes jitter test results only.

Integration with Network Node Manager

If you use NNM as well as OVPI, you have the option of improving your ability to diagnose a problem by integrating OVPI with NNM. To integrate OVPI and NNM, install the Integration Module. The Integration Module contains packages for NNM and packages for OVPI.

If NNM and OVPI are integrated, you should install the optional thresholds sub-package that comes with Service Assurance. Installing the optional thresholds sub-package configures the Thresholds Module to monitor the database for threshold conditions and respond to breach conditions by taking one of several possible actions in accordance with category, severity, and destination parameters. The default response is to send a breach trap to NNM. The breach trap received by NNM becomes an alarm in the NNM alarm browser. The NNM operator responds to the alarm by launching the Near Real Time report in the Source/Destination/Application folder.

Configuring the Thresholds Module is not necessary. You do not need to define an action or specify a destination for breach traps. However, you are free to modify category, severity, and destination parameters at any time. For details about these options, refer to the *Thresholds Module 5.0 User Guide*.

Ways to Customize Reports

Service Assurance reports can be customized by applying group filters, by importing properties (customers and locations), by applying constraints, and by editing tables and graphs. If you intend to share reports with customers, you will use group filters to produce customer-specific reports. Any user can apply constraints to a report, or edit tables and graphs. For more information about view options for tables and graphs, see Chapter A, .

Group Filters

If you intend to share your reports with customers, you will need to produce customer-specific reports. Creating customer-specific reports involves the following tasks:

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

Importing Property Data

The Cisco SAA Datapipe populates Service Assurance reports with SAA tests and IP addresses (or DNS names) for source and destination routers. Tests, addresses, and DNS names appear automatically. If you want to associate a customer and a location with a device, you must import this information yourself. To do that, use the change forms that come with Common Property Tables, or use the property import utility that comes with the Common Property Tables.

Editing Parameters

Editing a parameter applies a constraint. The constraint filters out data you are not interested in seeing. If you edit Customer Name, data for every customer except the customer you typed in the Customer Name field drops from the report. If you edit Destination Location, data for all destination locations except the destination location you typed in the field drops from the report.

You can apply multiple constraints at once. Service Assurance supports the following parameters:

- Customer Name
- Customer ID
- Source Name
- Source Location
- Destination Name
- Destination Location
- Application (SAA test type)
- ToS (Type of Service)
- Tag (Test Tag defined in the source router)

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

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

Sources for Additional Information

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

For information regarding the latest enhancements to Service Assurance, any known issues affecting this package, and any known issues affecting the two datapipes associated with this package, refer to the *Service Assurance Report Pack 3.1 Release Statement*. You may also be interested in the following documents:

- *Common Property Tables 3.5 User Guide*
- *Thresholds Module 5.0 User Guide*
- *NNM / OVPI Integration Module 2.0 User Guide*
- *OVPI Report Packs, Version 8.0: Release Notes, June 2005*

Manuals for OVPI, and manuals for the reporting solutions that run on OVPI, can be downloaded from the following web site:

http://www.managementsoftware.hp.com

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

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 searching this site for updates before using an older manual that might not be the latest version available.

2 The Upgrade Install

This chapter covers the following topics:

- Guidelines for a smooth upgrade to version 3.1
- Datapipes and remote pollers
- Custom table views
- Upgrading in a distributed environment
- Installing upgrade packages and the new datapipes

Guidelines for a Smooth Upgrade

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

Prerequisites for the Upgrade

The following software must already be installed before upgrading to Service Assurance 3.1:

- OVPI 5.0 or higher
- Any available service pack for the version of OVPI (5.0 or 5.1) you are running
- Service Assurance 1.0, 2.0, or 3.0
- Cisco SAA Datapipe (version 5.5 or earlier)
- Cisco SAA NRT Datapipe 1.0

You can find information about OVPI service packs, including installation instructions, in the release notes issued with the service pack.

Upgrading Common Property Tables

If you are running an older version of Service Assurance on any server, you are probably running an older version of Common Property Tables. Service Assurance requires Common Property Tables 3.0 or higher. Upgrading to version 3.5 is recommended. Do not install the "to_3.5" upgrade package for Common Property Tables *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 and Remote Pollers

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

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

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

- collection_manager
- group_manager

Exporting Polling Policy Configurations

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

UNIX: As user trendadm, run the following command:

```
cd $DPIPE_HOME

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

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

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

Exporting Polling Group Configurations

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

UNIX: As user trendadm, execute the following command:

```
cd $DPIPE_HOME

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

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

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

Custom Table Views

If you created one or more custom table views, the views you created may interfere with the report pack upgrade process, causing the process to fail. Whether your custom table 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 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 report pack is upgraded.

Installing Service Assurance NRT 2.0

The Service Assurance NRT 2.0 sub-package includes one new report and modifications to two existing reports. There is no upgrade path. If you want to install version 2.0, first delete version 1.0, then install version 2.0.

Distributed Environments

If you are running Service Assurance as a distributed system, the central server, every satellite server, and every remote poller must be running the same version of OVPI and all available Service Packs. Follow these steps to upgrade a distributed system:

1. Disable trendcopy on the central server.
2. Install the upgrade package for the report pack; deploy reports.
3. Install the upgrade package for locations.
4. Remove Cisco SAA Datapipe (version 5.5 or earlier) and Cisco SAA NRT Datapipe 1.0 from the central server.
5. Install the following datapipes:
   - Cisco SAA Datapipe 5.6
   - Cisco SAA NRT Datapipe 2.1
6. For each satellite server:
   - Install the “to_31” upgrade package for the report pack
   - Install the “to_31” upgrade package for locations.
   - Remove these packages:
     - Cisco SAA Datapipe (version 5.0 or earlier)
     - Cisco SAA NRT Datapipe 1.0
   - Install the following datapipes:
     - Cisco SAA Datapipe 5.6
     - Cisco SAA NRT Datapipe 2.1
7. Re-enable trendcopy on the central server.

Installing Upgrade Packages and New Datapipes

Perform the following tasks to upgrade to Service Assurance 3.1:

- Task 1: Stop OVPI Timer and extract packages from the product CD
- Task 2: Upgrade to the latest release of Common Property Tables
- Task 3: Install the “to_31” upgrade package for the report pack
- Task 4: Install these packages:
  - UPGRADE_Service_Assurance_Location_to_31

- Service Assurance Thresholds (optional)
- Service Assurance NRT (optional)

- Task 5: Uninstall old datapipes:
  - Cisco SAA Datapipe (version 5.5 or earlier)
  - Cisco SAA NRT Datapipe 1.0.
- Task 6: Install new datapipes:
  - Cisco SAA Datapipe 5.6
  - Cisco SAA NRT Datapipe 2.1

Task 1: Extract packages from the product CD to the Packages directory

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

   Windows: Select **Settings > Control Panel** > **Administrative Tools > Services**

   UNIX: As root, type one of the following:

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

   Sun: **`sh /etc/init.d/ovpi_timer stop`**
3. Insert the June 2005 report pack CD in the CD-ROM drive. On Windows, a main menu appears automatically. On UNIX, mount the CD, navigate to the top level directory on the CD, and run the **./setup** command.
4. Type **1** in the choice field and press **Enter**. The install script displays a percentage complete bar. When the copy is complete, the install script starts Package Manager. The Package Manager welcome window opens.

Once the copy to the Packages directory is complete, you have the option of navigating to the Packages directory to see the results. The Packages directory contains separate folders for Service Assurance and each datapipe. The following folders appear under Service Assurance:

- Service_Assurance.ap
- Service_Assurance_Demo.ap
- Service_Assurance_Location.ap
- Service_Assurance_NRT.ap
- Service_Assurance_Thresholds.ap
- UPGRADE_Service_Assurance_to_31.ap
- UPGRADE_Service_Assurance_Location_to_31.ap

The following folder appears under Cisco SAA Datapipe:

- Cisco_SAA_Datapipe.ap

The following folder appears under Cisco SAA NRT Datapipe:

- Cisco_SAA_NRT_Datapipe.ap

Task 2: Upgrade to Common Property Tables 3.5

Service Assurance 2.0 required Common Property Tables 2.2. If you have not already upgraded to Common Property Tables 3.5, do this now. When you upgrade Common Property Tables, do not install other packages at the same time. Install the “to_3.5” upgrade package for Common

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

Task 3: Install the upgrade package for the report pack

1. Start 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; accept the defaults for application server name and port. 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 package:

   UPGRADE_Service_Assurance_to_31
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 and the install begins. When installation finishes, an install complete message appears.
10. Click **Done**.

> Do not be surprised if the upgrade package you just installed seems to have disappeared. The install wizard displays what you just installed as *Service Assurance 3.1*. This is not an error.

Task 4: Install UPGRADE Service Assurance Location and optional packages (thresholds and NRT)

1. Start Package Manager. The Package Manager welcome window opens.
2. Click **Next**. The Package Location window opens.
3. Click **Install.**
4. Click **Next.** The Report Deployment window opens. Accept the default for Deploy Reports; accept the defaults for application server name and port. 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:
   - *UPGRADE_Service_ Assurance_Location_to_31*
   - *Service_Assurance_Thresholds*
   - *Service_Assurance_NRT*
7. Click **Next.** The Type Discovery window opens. Disable the default.
8. Click **Next.** The Selection Summary window opens.
9. Click **Install.** The Install Progress window opens. When installation finishes, an install complete message appears.
10. Click **Done**.

Task 5: Remove old datapipes

1. Start Package Manager. The Package Manager welcome window opens.
2. Click **Next.** The Package Location window opens.
3. Click **Uninstall**.
4. Click **Next.** The Report Undeployment window opens. Accept the default for Undeploy Reports; also accept the defaults for application server name and port. 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 package:

   Cisco_SAA_Datapipe

   Cisco_SAA_NRT_Datapipe
7. Click **Next.** The Type Discovery window opens. Disable the default.
8. Click **Next**. The Selection Summary window opens.
9. Click **Uninstall.** The Progress window opens and the removal process begins. When removal finishes, a package removal complete message appears.
10. Click **Done.**

Task 6: Install new datapipes and restart OVPI Timer

1. Start Package Manager. The Package Manager welcome window opens.
2. Click **Next**. The Package Location window opens.
3. Click **Install**. 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; accept the defaults for application server name and port. 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:
   - *Cisco_SAA_Datapipe 5.6*
   - *Cisco_SAA_NRT_Datapipe 2.1*
7. Click **Next.** The Type Discovery window opens. Disable the default.
8. Click **Next.** The Selection Summary window opens.
9. Click **Install.** The Install Progress window opens. When installation finishes, an install complete message appears.
10. Click **Done**.
11. Restart OVPI Timer.

    Windows: Select **Settings > Control Panel** > **Administrative Tools > Services**

    UNIX: As root, type one of the following:

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

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

3 The New Install

This chapter covers the following topics:

- Guidelines for a smooth install of Service Assurance 3.1
- Installing the report pack
- Accessing deployed reports
- New object categories in the object model
- Package removal

Guidelines for a Smooth Install

When you insert the June 2005 report pack 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 launch OVPI and start Package Manager. Before running Package Manager, review the following guidelines.

Prerequisites for a New Install

The following software must be installed before installing Service Assurance 3.1:

- OVPI 5.0 or OVPI 5.1
- Any service pack available for the version of OVPI (5.0 or 5.1) you are running

You will find information about each service pack, including installation instructions, in the release notes issued with the service pack.

Upgrading Common Property Tables

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

Integration with NNM: Threshold Alarms

If OVPI and NNM are integrated, you have the option of launching Service Assurance reports from NNM in response to threshold breaches detected by OVPI. To take advantage of this feature, install the thresholds sub-package, Service_Assurance_Thresholds.

Service_Assurance_Thresholds provides default threshold settings. The thresholds sub-package cannot operate without the Threshold and Event Generation Module, commonly known as the Thresholds Module. If you select the thresholds sub-package for installation, Package Manager will install the Thresholds Module for you, automatically.

Distributed Environments

If you are running Service Assurance as a distributed system, the central server, every satellite server, and every remote poller must have OVPI 5.0 installed. Following is an overview of the installation procedure for distributed environments:

1. Disable trendcopy on the central server.
2. Install the following packages on the central server:
   - Service Assurance 3.1; deploy reports.
   - Service Assurance Location 3.1
   - Service Assurance Thresholds (optional)
   - Service Assurance NRT (optional)
   - Cisco SAA Datapipe 5.6
   - Cisco SAA NRT Datapipe 2.1
3. Install the following packages on each satellite server:
   - Service Assurance 3.1
   - Service Assurance Location 3.1
   - Service Assurance Thresholds (optional)
   - Service Assurance NRT (optional)
   - Cisco SAA Datapipe 5.6
   - Cisco SAA NRT Datapipe 2.1
4. Re-enable trendcopy on the central server.

After the installation is complete, you must set up connections with satellite server databases, configure trendcopy pull commands, and switch off daily aggregations at each satellite server. These steps are covered in Chapter 5, Package Configuration.

Installing Service Assurance 3.1

Perform the following tasks to install Service Assurance 3.1:

- Task 1: Extract packages from the report pack CD
- Task 2: If necessary, upgrade to Common Property Tables 3.5
- Task 3: Install the following packages:
  - Service_Assurance 3.1
  - Cisco_SAA_Datapipe 5.6
  - Cisco_SAA_NRT_Datapipe 2.1

If desired, install the optional sub-packages when you install the report pack.

Task 1: Extract packages from the report pack CD to the Packages directory

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

   Windows: Select **Settings > Control Panel** > **Administrative Tools > Services**

   UNIX: As root, type 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. On Windows, a Main Menu displays automatically. On UNIX, the CD may or may not mount automatically; if it does not mount automatically, navigate to the top level directory on the CD, and run the **./setup** command.
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 install wizard opens.

When the copy to the Packages directory is complete, you can navigate to the Packages directory to see the results. The Packages directory contains separate folders for Service Assurance and each datapipe. The following folders appear under Service Assurance:

- Service_Assurance.ap
- Service_Assurance_Demo.ap
- Service_Assurance_Location.ap
- Service_Assurance_NRT.ap
- Service_Assurance_Thresholds.ap
- UPGRADE_Service_Assurance_to_31.ap
- UPGRADE_Service_Assurance_Location_to_31.ap

The following folder appears under Cisco SAA Datapipe:

- Cisco_SAA_Datapipe.ap

The following folder appears under Cisco SAA NRT Datapipe:

- Cisco_SAA_NRT_Datapipe.ap

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

Task 2: Upgrade to Common Property Tables 3.5

If you are not running any version of Common Property Tables, let Package Manager install Common Property Tables for you. If you are running an earlier version, 2.2 or 3.0, upgrade Common Property Tables by installing the “to_3.5” upgrade packages. Do not install other packages when you do this; install the upgrade package for Common Property Tables and *only* the upgrade package for Common Property Tables. When Package Manager indicates that installation is complete, click **Done** to return to the Management Console.

Task 3: Install Service Assurance 3.1, the datapipes, and optional sub-packages

1. Start Package Manager. The Package Manager install wizard 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; accept the defaults for application server name and port. Type your user name and password for the OVPI Application Server.
5. Click **Next.** The Package Selection window opens. Click the check box next to the following packages:

   Service_Assurance

   Service_Assurance_Location

   Service_Assurance_NRT

   Service_Assurance_Thresholds

   Cisco_SAA_Datapipe 5.6

   Cisco_SAA_NRT_Datapipe 2.1

   If your system is distributed, the Location and Thresholds sub-packages belong on the central server *only*, not on satellite servers.

6. Click **Next.** The Type Discovery window opens. Keep the default.
7. Click **Next**. The Selection Summary window opens.
8. Click **Install.** The Install Progress window opens and the installation begins. When the installation finishes, an install complete message appears.
9. Click **Done** to return to the Management Console.
10. Restart OVPI Timer.

    Windows: Select **Settings > Control Panel** > **Administrative Tools > Services**

    UNIX: As root, type one of the following:

    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 and forms reside on the OVPI Application Server, you have two ways to view them:

- OVPI client applications
- Web browser

If you have the client applications, you have access to Report Viewer, Report Builder, and the Management Console. If you don't have the client applications, using a web browser to view reports is the only way you can view reports.

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

New Object Categories in the Object Model

An object is any item that has performance data associated with it. Devices, customers, and locations are object categories that belong to OVPI's default object model. When you select an object in the object model, the right side of the Object/Property Management window refreshes, showing a list of forms under **General Tasks**, a list of forms under **Object Specific Tasks**, and a list of reports under **Object Specific Reports**.

The object tree changes each time you install a new report pack. Some report packs will add a new class of objects or services that do not fit within the default model. When this happens, the report pack adds a new view. To open the new view, select **View > Change View**.

Service Assurance adds the following object categories to the OVPI object model:

- SAA_Source
- SAA_Destination
- SAA_Application

Package Removal

Follow these steps to uninstall Service Assurance and the Cisco SAA Datapipe.

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

   Windows: Select **Settings > Control Panel** > **Administrative Tools > Services**

   UNIX: As root, type one of the following:

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

   Sun: **`sh /etc/init.d/ovpi_timer stop`**
3. Launch Performance Insight and start Package Manager. The Package Manager welcome window opens.
4. Click **Next.** The Package Location window opens.
5. Click the **Uninstall** radio button.
6. Click **Next.** The Report Undeployment window opens.
7. Click the check box next to the following packages:

   Service_Assurance

   Service_Assurance_Locations (if installed)

   Service_Assurance_NRT (if installed)

   Service_Assurance_Thresholds (if installed)

   Service_Assurance_Demo (if installed)

   Cisco_SAA_Datapipe

   Cisco_SAA_NRT_Datapipe (if installed)
8. Click **Next.** The Uninstall Packages window opens.
9. Click **Uninstall.** The Progress window opens. When the removal finishes, a removal complete message appears.

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

11 Restart OVPI Timer.

Windows: Select **Settings > Control Panel** > **Administrative Tools > Services**

UNIX: As root, type one of the following:

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

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

4 Router Configuration

The Cisco SAA Datapipe 5.0 supports the following SAA tests:

- Echo
- udpEcho
- tcpConnect
- HTTP
- DNS
- DLSw
- DHCP
- FTP
- Jitter
- MPLS VPN Aware Cisco IOS 12.2(2)T or later
- VoIP UDP (Cisco IOS 12.3(4)T or later

Although you can configure SAA tests using the Cisco IOS Command Line Interface and the SNMPSET command, these techniques are not that easy to use, especially when multiple routers are involved. To make this task easier and faster, use CiscoSAA_Config. This is a Perl module that functions as a batch-mode SAA test configuration utility for source routers.

CiscoSAA_Config

CiscoSAA_Config resides inside the Cisco SAA Datapipe package. The full path is:

```
$DPIPE_HOME/packages/CiscoSAA_Datapipe/CiscoSAA_Config
```

CiscoSAA_Config consists of two perl scripts and one XML file.

CiscoSAAConfig.pl. Perl script that reads an XML configuration file and sets SAA operations in a router.

CiscoSAADelete.pl. Perl script that deletes the SAA operations that were set by the CiscoSAAConfig script.

CiscoSAAConfig.xml. XML file that defines MIB values in the CISCO-RTTMON-MIB; includes some examples of SAA operations with nominal IP address.

The following Perl modules are required to run this utility:

- Getopt::Std
- Cwd
- File::Spec

- Net::SNMP
- XML::Simple

You should have no problem running CiscoSAA_Config on the OVPI server. To verify that no modules are missing and that all modules are correctly installed, run the following command:

```
perl –e “use Getopt::Std;use Cwd; use File::Spec; use Net::SNMP; XML::Simple”
```

Using an XML Block to Define an Operation

Each SAA operation is defined by an XML block. For each operation, only basic arguments are defined. Additional arguments can be defined based on the CISCO-RTTMON-MIB. The value of some arguments (excluding MIBName and ValueType) should be modified to fit your network and SAA target information. These arguments are located in the last few arguments in each operation block.

For example, the following block defines an Echo operation:

```
<Operation Name="ECHO">
<!-- Following arguments cannot be modified -->
<OperationArg MIBName="rttMonCtrlAdminRttType" ValueType="i">1</
OperationArg>
<OperationArg MIBName="rttMonEchoAdminProtocol" ValueType="i">2</
OperationArg>
<!-- Following arguments are required and must be modified -->
<OperationArg MIBName="rttMonEchoAdminTargetAddress"
ValueType="d">192.15.115.22</OperationArg>
<!-- Following arguments are optional and could be modified -->
<OperationArg MIBName="rttMonCtrlAdminTag" ValueType="s">SNMP_ECHO</
OperationArg>
<OperationArg MIBName="rttMonCtrlAdminThreshold" ValueType="i">1000</
OperationArg>
<OperationArg MIBName="rttMonCtrlAdminFrequency" ValueType="i">600</
OperationArg></Operation>
```

When you configure an Echo operation in your router using this example, you have to change the value of the rttMonEchoAdminTargetAddress to the IP address of your target device.

Configuration Script Syntax

Use the main configuration script as follows:

```
Perl CiscoSAAConfig.pl -a router_address [-c community] [-f
   XML_config_file] [-m] [-h]
```

where:

- **-a** Cisco Router IP address, required argument
- **-c** read/write community string, default is *private*
- **-f** name of XML configuration file, default is *CiscoSAAConfig.xml*

- **-m** enable writing the SAA probes into the non-volatile memory, default is *0* (false)

  If this option is set to **1**, you must log in to the source router and enter the command **write** after this script runs.

- **-h** help

Delete Script Syntax

The configuration script will hard-code the lifetime of all operations as *forever*. If you want to delete the SAA operations that have been set in the router, run the CiscoSAADelete.pl script. Use this script as follows:

```
Perl CiscoSAADelete.pl -a <router address> [-c <community>] [-b] [<SAA
Test Index> ...] [-h]
```

Where:

- **-a** Cisco Router IP address, a required argument
- **-c** community string, default is *private*
- **-b** delete all SAA tests
- **<SAA Test Index>** delete one or more SAA tests
- **-h** help

If you do not enter an SAA index or use the **-b** option, the script will return all SAA indexes in the router. This is one way to find out which SAA tests have been configured. Once you know which SAA tests have been configured, you can use the SAA index value (the number after the last “dot” sign) to delete the SAA test you want to stop.

Other Approaches to Configuring SAA Tests

You have three other approaches to SAA test configuration:

- Command Line Interface (CLI)
- Cisco’s VPN Solution Center
- Cisco Works

For more information about using the CLI, go here:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/saaoper.htm

For more information about the VPN Solution Center, go here:

http://www.cisco.com/warp/public/779/servpro/operate/csm/nemnsw/vpn/prodlit/

For more information about Cisco Works, go here:

http://www.cisco.com/warp/public/cc/pd/wr2k/index.shtml

5 Package Configuration

This chapter covers the following topics:

- Default thresholds in the Service_Assurance_Thresholds sub-package
- Using the Modify SAA Thresholds form to change default values
- Distributed Systems

You can modify the exception thresholds for all the devices owned by one customer, for all the devices in one location, for all the test operations initiated from one device, or for a subset of test operations initiated by one device belonging to one customer.

Defaults in Service_Assurance_Thresholds

The Service_Assurance_Thresholds sub-package imposes thresholds for two MIB counters:

- Number of response time exceptions
- Number of test failures

The actual threshold for response time is controlled by Cisco IOS. To configure the threshold, use CiscoSAA_config, the test configuration utility described in the previous chapter. You will probably want to set this parameter on a test-by-test basis. For any one test, the threshold can vary from destination to destination.

The thresholds sub-package monitors the response time exceptions counter and the test failures counter. When either counter breaches the threshold, the thresholds sub-package sends a trap to the network management system. (If OVPI is currently integrated with Network Node Manager, the Thresholds Module will, by default, send threshold traps to your NNM server.) The following table indicates the default for each threshold category and the severity level for each threshold breach.

MIB Counter	OVPI Threshold	Condition for NNM Alarm	Severity
Response Time	Exception Hour	75% of tests exceed the threshold for response time.	Minor
	Exception Day	50% of tests exceed the threshold for response time.	Major
Test Failures	Failed Hour	100% of tests failed.	Warning
	Failed Day	100% of tests failed.	Critical

For details about the Thresholds Module, such as how to enable multiple types of traps or how to set up multiple trap destinations, refer to the *Thresholds Module 5.0 User Guide*.

The Thresholds Form

Service Assurance provides a form for modifying the default thresholds for:

- Exception Hour
- Exception Day

The other two fields in this form, Failed Hour and Failed Day, cannot be modified. Although there is only one form, the contents of the form will change depending on where you are in the object tree. The object tree provides these objects:

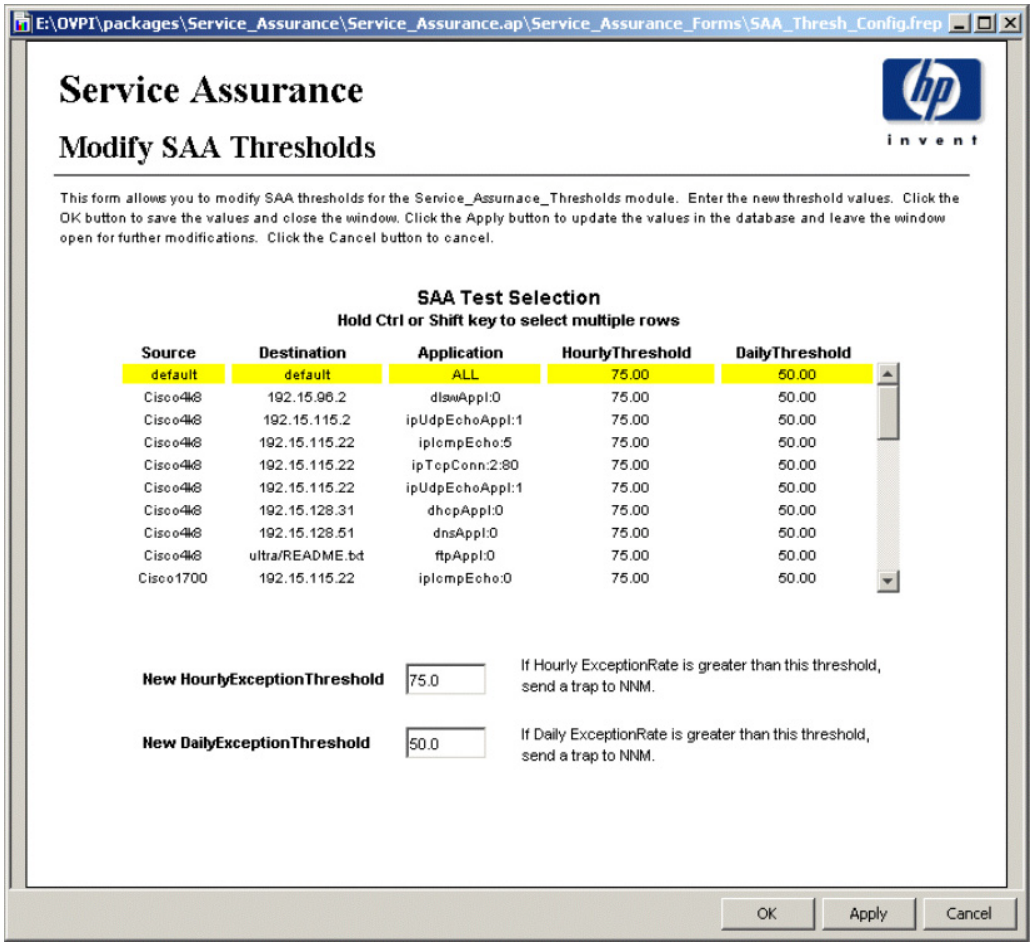
- Default [Device]
- Customer
- Location

You may apply your modification to all the devices belonging to one customer, to selected devices belonging to one customer, or to one device belonging to one customer. If you are modifying the thresholds for one device, you may apply the modification to every application (test operation) or to selected applications.

Follow these steps to open the form:

1. Start the Management Console.
2. Click **Objects**. In the **Object/Property Management** pane, navigate to a customer, a location, or a device. For each customer, your options are:
   - Device
   - SAA_Application
   - SAA_Destination
   - SAA_Source
3. Highlight an object. You will see the Modify SAA Thresholds form listed under **Object Specific Tasks**.

4 Double-click **Modify SAA Thresholds**. The form opens.



5 Modify one or both defaults.

If you want to modify multiple, contiguous test operations, hold down the **SHIFT** key and use the mouse to highlight multiple test operations. If you want to modify individual test operations, hold down the **CTRL** key and use the mouse to select individual test operations.

6 Click **Apply** to save changes, **OK** to save changes and close the form, or **Cancel** to close the form without saving changes.

Distributed Systems

If you intend to run Service Assurance as a distributed system, you need to configure every server in the system. Before doing that, use the following table to verify that datapipes and optional packages are installed where they need to be installed.

Central Server	Satellite Server
Service Assurance	Service Assurance
Common Property Tables	Common Property Tables

Central Server	Satellite Server
Thresholds Module	Thresholds Module
Service_Assurance_Thresholds	Service_Assurance_Thresholds
	Cisco SAA Datapipe
	Cisco NRT SAA Datapipe

Typically, the central server does not poll. If you want the central server in your system to poll, then you must install one or both datapipes on the central server.

If you are only interested in setting thresholds on hourly data or rate data, you do not need to install the thresholds sub-package on the central server. If you are interested in setting thresholds for aggregated data (for example, summary data of any kind, or a forecast) then you need to install Service_Assurance Thresholds on the central server.

Configuring the Central Server

This task involves the following steps:

- Task 1: Set up connections with satellite server databases
- Task 2: Disable the hourly trendsum process
- Task 3: Configure trendcopy pull commands for hourly data
- Task 4: Configure trendcopy pull commands for rate data (optional)

In addition to performing these tasks, it is important to verify that the system clock on the central server is synchronized with system clocks on the satellite servers.

The following steps apply to new installations only. If you just upgraded to Service Assurance 3.1 and your servers were already configured for operation as a distributed system, those settings are still in effect.

Task 1: Set up connections with satellite server databases

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

Task 2: Disable the hourly trendsum process

1. Modify the hourly process file; open the following file:

   ```
   $DPIPE_HOME/scripts/Service_Assurance_Hourly.pro
   ```

2 Comment out block1 by adding the comment sign (“#”) before the word **begin** and the word **end**.

Task 3: Configure trendcopy pull commands for hourly data

1 Configure trendcopy pull commands for each satellite server; open the following file:

```
$DPIPE_HOME/scripts/Service_Assurance_Hourly.pro
```

2 Modify block2 as follows:

- Remove “#” before the word **begin** and before the word **end**
- Replace *SATELLITE_SERVER_1_DATABASE* with the satellite server name
- Replace *THIS_MACHINE_DATABASE* with the central server name

3 If there is more than one satellite server, create a copy of block2 for each satellite server and repeat step 2 for each copy of block2.

Task 4: Configure trendcopy pull commands for rate data (optional)

If you want to view the Near Real Time report from the central server, you must copy rate data from each satellite server to the central server. To do that, configure trendcopy pull commands from the central server for each satellite server.

Pulling rate data from satellite servers has two side-effects. It increases the traffic between satellite servers and the central server, and it increases the processing load on the central server.

1 Open the following file:

```
$DPIPE_HOME/scripts/Service_Assurance_Hourly.pro
```

2 Modify block3 as follows:

- Remove “#” before the word **begin** and before the word **end**
- Replace the *SATELLITE_SERVER_1_DATABASE* with the satellite server name
- Replace *THIS_MACHINE_DATABASE* with the central server name

3 If there is more than one satellite server, create one copy of block3 for each satellite server and repeat step 2 for each copy of block3.

Configuring a Satellite Server

Follow these steps to configure a satellite server:

1 Switch off daily aggregations. Do this by commenting out the lines referencing *Service_Assurance_Daily.pro* in the `$DPIPE_HOME/lib/trendtimer.sched` file.

2 In the same file, modify the start time in the `Service_Assurance_Hourly.pro` file. By default, hourly summarizations start 40 minutes after the hour. Since you want the satellite server to complete hourly summarizations before the central server copies the data, make the start time earlier. Change it from 1:00+40 to 1:00+25.

Configure polling policies for the Cisco SAA Datapipe. Make sure that each SAA router is polled by only one satellite server.

6 Ranking Exception Counts

The exception reports rank elements according to yesterday's exception count. Use the exception reports to drill down from elements with relatively high exception counts to the specific element pairs that are causing the exceptions. There are six exception reports:

- Source Exception Report, by Application/Destination
- Destination Exception Report, by Source/Application
- Destination Exception Report, by Location/Application
- Application Exception Report, by Source/Destination
- Application Exception Report, by Location/Destination
- Location Exception Report, by Source/Destination

The customer selection table ranks customers by number of exceptions. The next table is a list of elements, also ranked by number of exceptions. The third selection table provides a list of element pairs, for example, source and destination pairs, or location and destination pairs, that contributed to the exception total. The history graphs to the right compare yesterday's activity to the previous 30 days.

The bottom table and the graphs below the bottom table focus on one specific element pair, from one perspective, for one customer. The graphs provide hourly data for yesterday and daily data for the previous 90 days. The following table outlines the scope of each graph.

Hourly/Daily Graph	**What it Tracks**
Response time	Minimum, average, and maximum response time.
Throughput	Minimum, average, and the maximum throughput.
HTTP Response Time	DNS lookup time + TCP connection time + HTTP transaction time. Applies to HTTP tests only.
Exception Counts	Total number of response time exceptions.
Number of Transactions	Total number of transactions.
Availability	The end user's perception of destination availability.

Samples of three exception reports follow: (1) Destination by Source/Application, (2) Source by Application/Destination, and (3) Application by Source/Destination.

Service Assurance

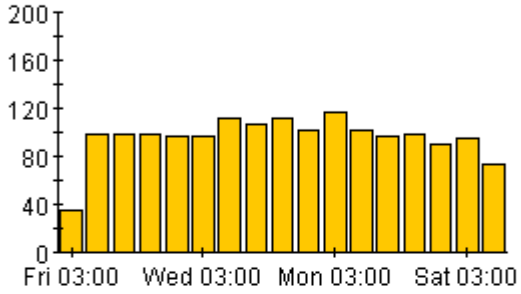
Destination Exception by Source/Application

The Destination Exception by Source / Application Report allows the users to quickly identify the destination devices which are experiencing the worst performance. Once a destination device is selected, the performance of individual source / application pairs can be investigated in detail.

Sun Dec 08 2002

Customer	CustID	# Trans	# Exceptions
Desktalk	3	743	73
HPOV	1	1,133	2

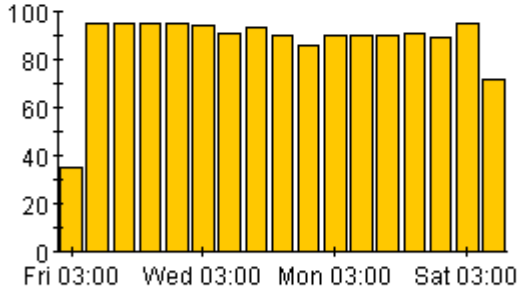
Exception Counts
Desktalk
Fri Nov 22 2002 - Sun Dec 08 2002



Destinations with Most Exceptions
Sun Dec 08 2002

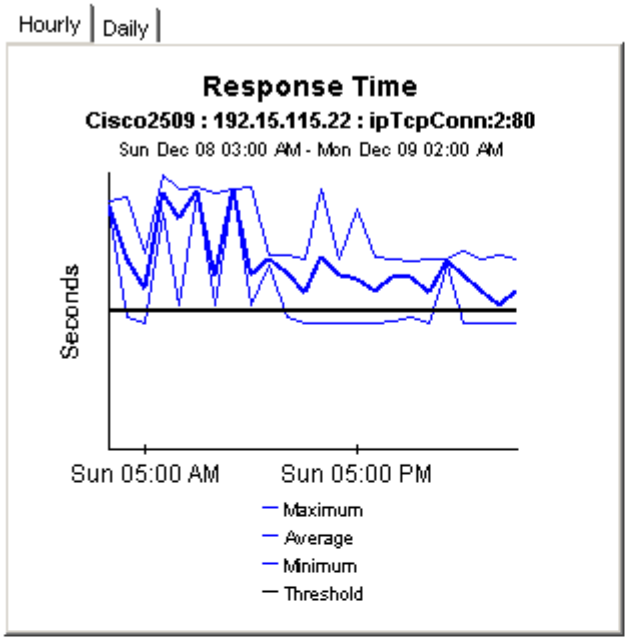
Destination	# Trans	# Exceptions
192.15.115.22	336	72
www.yahoo.com	71	1

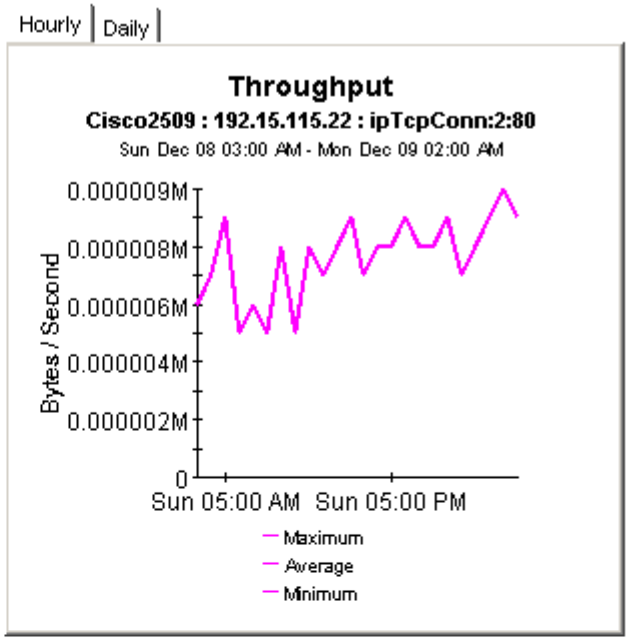
Exception Counts
192.15.115.22
Fri Nov 22 2002 - Sun Dec 08 2002

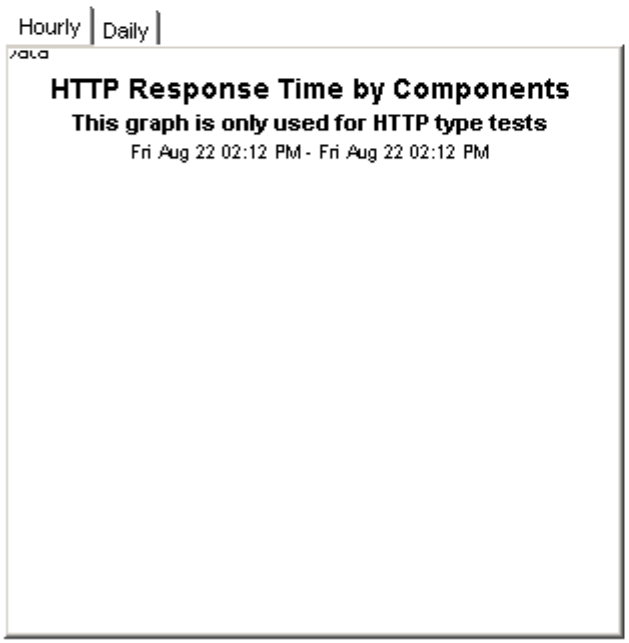


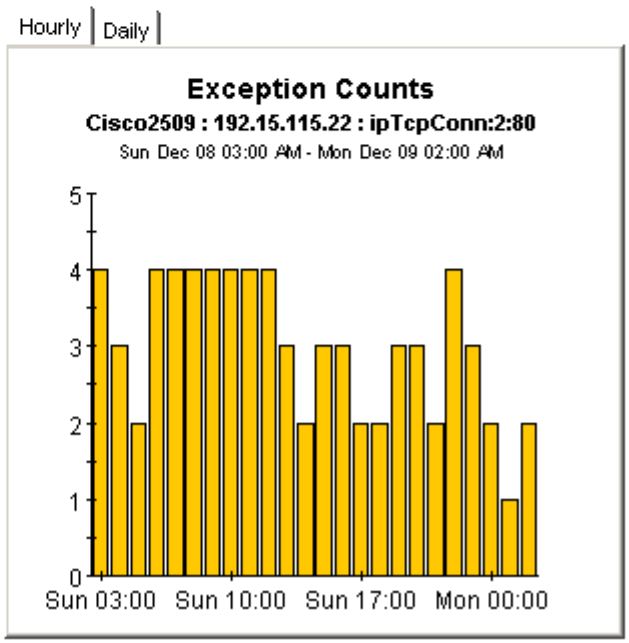
Source / Application Pairs with Most Exceptions
Sun Dec 08 2002

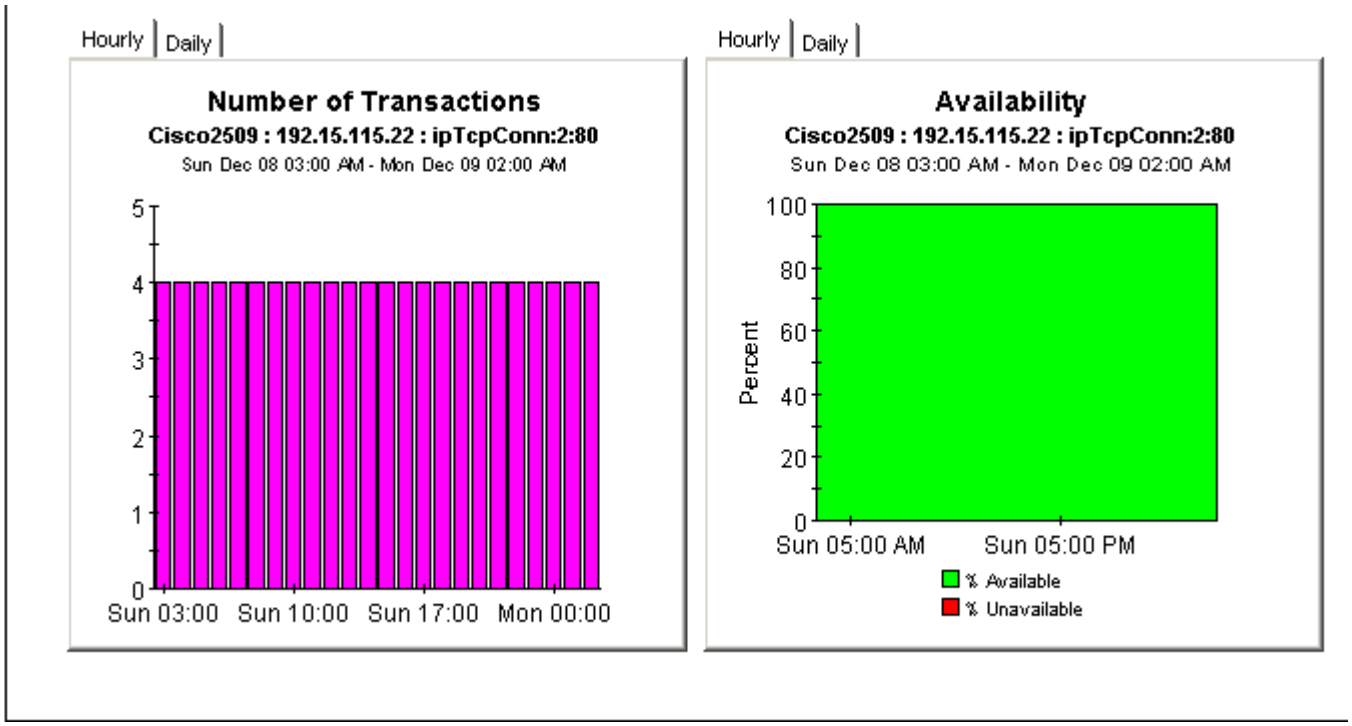
Source	Application	Number of Transactions	Availability	Response Time Exceptions
Cisco2509	ipTcpConn:2:80	96	100.0	72


Hourly
Daily
Response Time
Cisco2509 : 192.15.115.22 : ipTcpConn:2:80
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
Seconds
Sun 05:00 AM
Sun 05:00 PM
Maximum
Average
Minimum
Threshold


Hourly
Daily
Throughput
Cisco2509 : 192.15.115.22 : ipTcpConn:2:80
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
Bytes / Second
0.000009M
0.000008M
0.000006M
0.000004M
0.000002M
0
Sun 05:00 AM
Sun 05:00 PM
Maximum
Average
Minimum


Hourly
Daily
HTTP Response Time by Components
This graph is only used for HTTP type tests
Fri Aug 22 02:12 PM - Fri Aug 22 02:12 PM


Hourly
Daily
Exception Counts
Cisco2509 : 192.15.115.22 : ipTcpConn:2:80
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
5
4
3
2
1
0
Sun 03:00
Sun 10:00
Sun 17:00
Mon 00:00


Hourly
Daily
Number of Transactions
Cisco2509 : 192.15.115.22 : ipTcpConn:2:80
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
5
4
3
2
1
0
Sun 03:00
Sun 10:00
Sun 17:00
Mon 00:00
Hourly
Daily
Availability
Cisco2509 : 192.15.115.22 : ipTcpConn:2:80
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
Percent
100
80
60
40
20
0
Sun 05:00 AM
Sun 05:00 PM
% Available
% Unavailable

Service Assurance

Source Exception by Application/Destination

The Source Exception by Application / Destination Report allows the users to quickly identify the source devices which are experiencing the worst performance. Once a source device is selected, the performance of individual application / destination pairs can be investigated in detail.

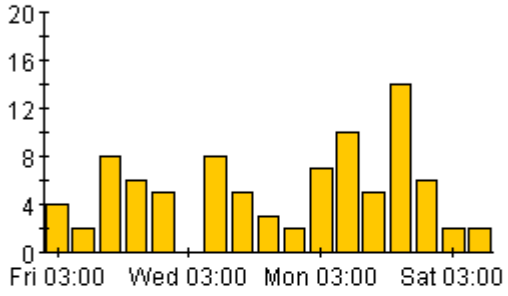
Sun Dec 08 2002

Customer	CustID	# Trans	# Exceptions
Desktalk	3	743	73
HPOV	1	1,133	2

Exception Counts

HPOV

Fri Nov 22 2002 - Sun Dec 08 2002



Sources with Most Exceptions

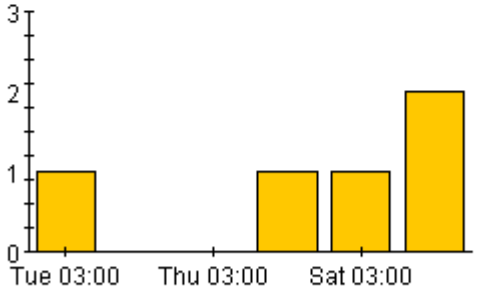
Sun Dec 08 2002

Source	# Trans	# Exceptions
Mcrouter85	96	2

Exception Counts

Mcrouter85

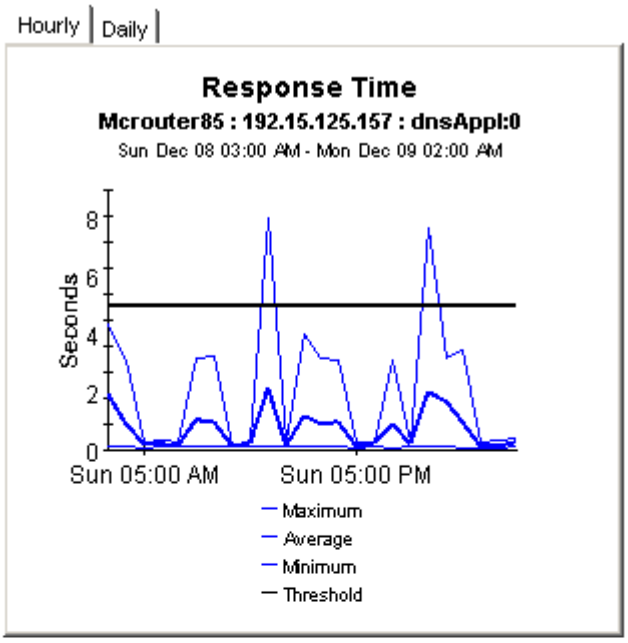
Tue Dec 03 2002 - Sun Dec 08 2002

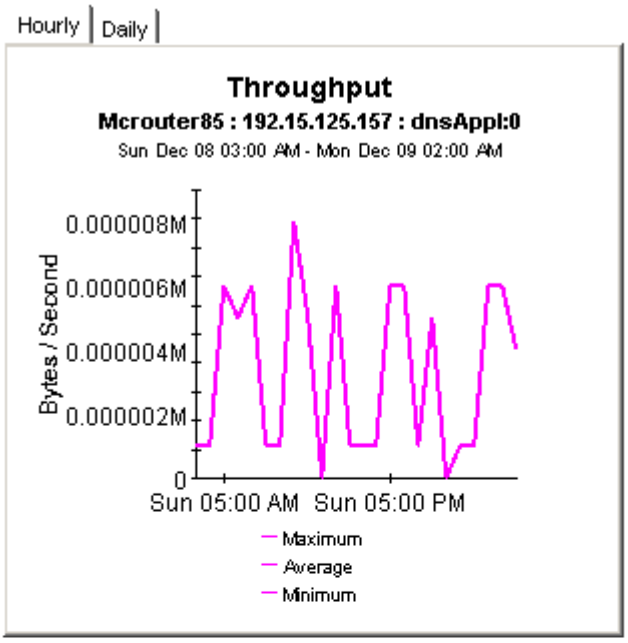


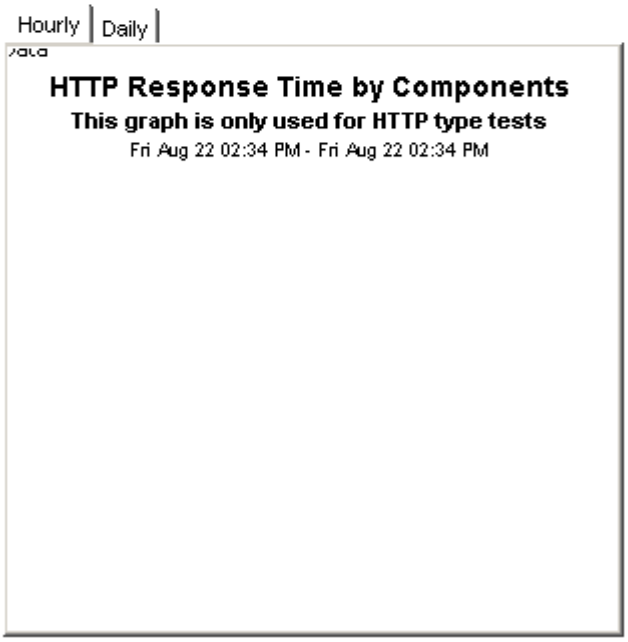
Application / Destination Pairs with Most Exceptions

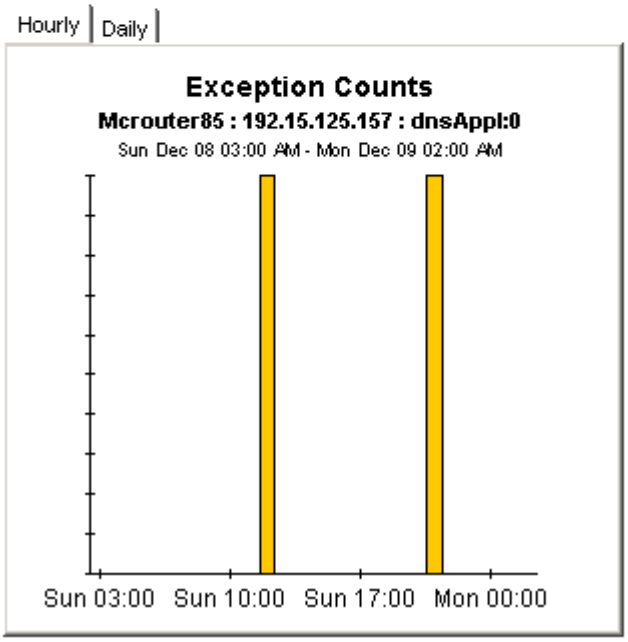
Sun Dec 08 2002

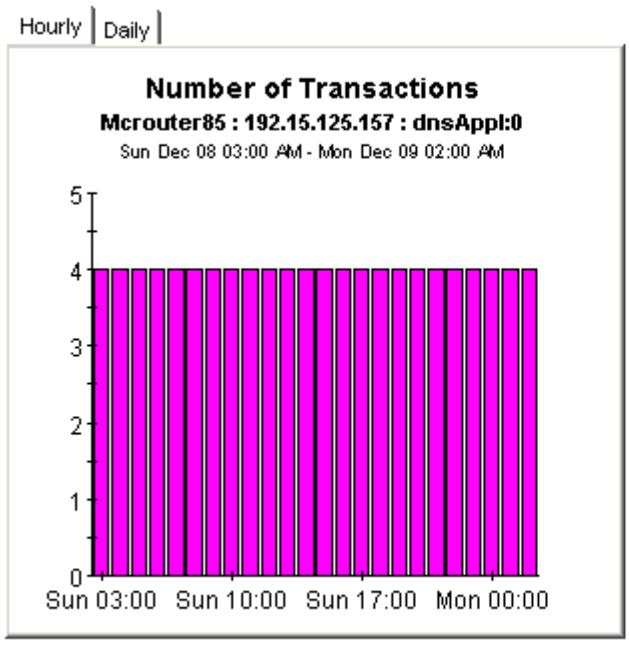
Application	Destination	Number of Transactions	Availability	Response Time Exceptions
dnsAppl:0	192.15.125.157	96	100.0	2

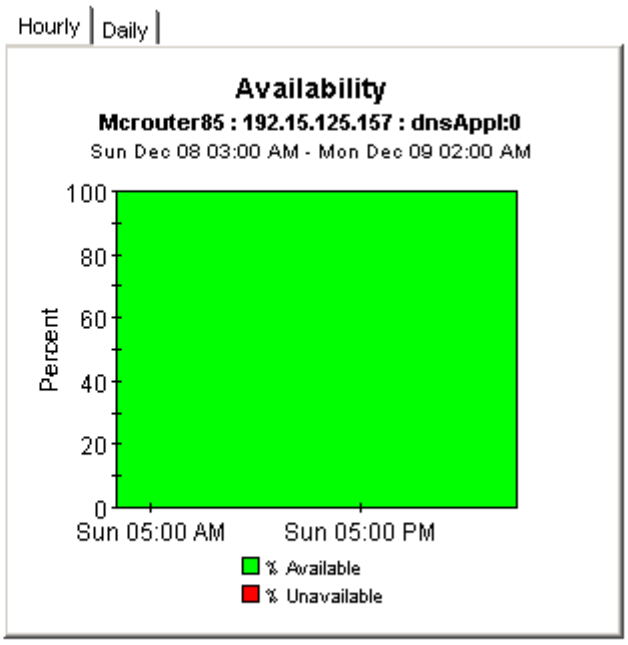

Hourly
Daily
Response Time
Mcrouter85 : 192.15.125.157 : dnsAppl:0
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
Seconds
8
6
4
2
0
Sun 05:00 AM
Sun 05:00 PM
Maximum
Average
Minimum
Threshold


Hourly
Daily
Throughput
Mcrouter85 : 192.15.125.157 : dnsAppl:0
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
Bytes / Second
0.000008M
0.000006M
0.000004M
0.000002M
0
Sun 05:00 AM
Sun 05:00 PM
Maximum
Average
Minimum


Hourly
Daily
HTTP Response Time by Components
This graph is only used for HTTP type tests
Fri Aug 22 02:34 PM - Fri Aug 22 02:34 PM


Hourly
Daily
Exception Counts
Mcrouter85 : 192.15.125.157 : dnsAppl:0
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
Sun 03:00
Sun 10:00
Sun 17:00
Mon 00:00


Hourly
Daily
Number of Transactions
Mcrouter85 : 192.15.125.157 : dnsAppl:0
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
5
4
3
2
1
0
Sun 03:00
Sun 10:00
Sun 17:00
Mon 00:00


Hourly
Daily
Availability
Mcrouter85 : 192.15.125.157 : dnsAppl:0
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
Percent
100
80
60
40
20
0
Sun 05:00 AM
Sun 05:00 PM
% Available
% Unavailable

Service Assurance

Application Exception by Source/Destination

The Application Exception by Source/Destination Report allows the users to quickly identify the applications which are experiencing the worst performance. Once an application is selected, the performance of individual source / destination pairs can be investigated in detail.

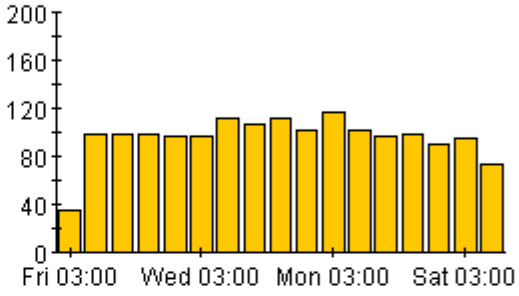
Sun Dec 08 2002

Customer	CustID	# Trans	# Exceptions
Desktalk	3	743	73
HPOV	1	1,133	2
Trinagy	2	432	0

Exception Counts

Desktalk

Fri Nov 22 2002 - Sun Dec 08 2002



Applications with Most Exceptions

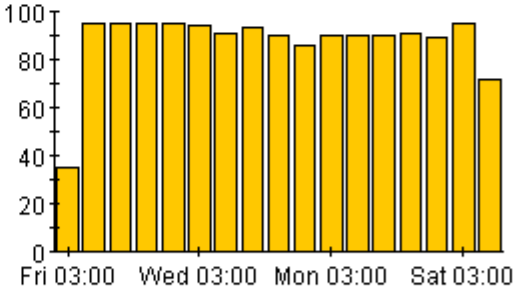
Sun Dec 08 2002

Application	# Trans	# Exceptions
ipTcpConn:2:80	96	72
httpAppl:0	215	1

Exception Counts

ipTcpConn:2:80

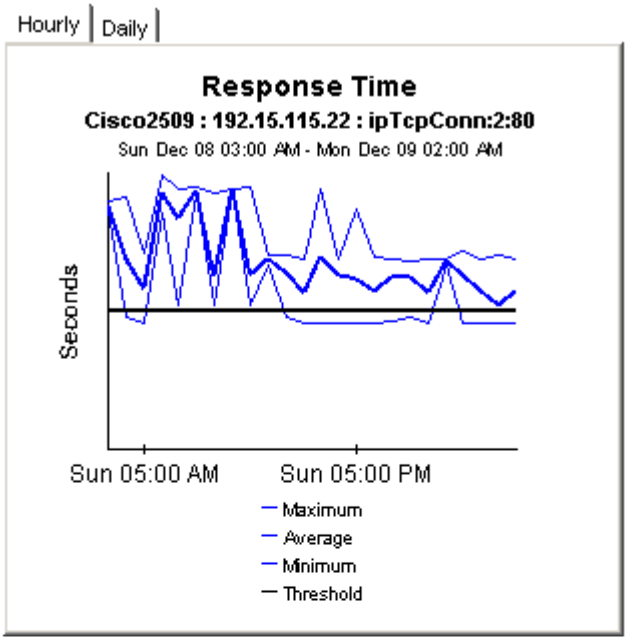
Fri Nov 22 2002 - Sun Dec 08 2002

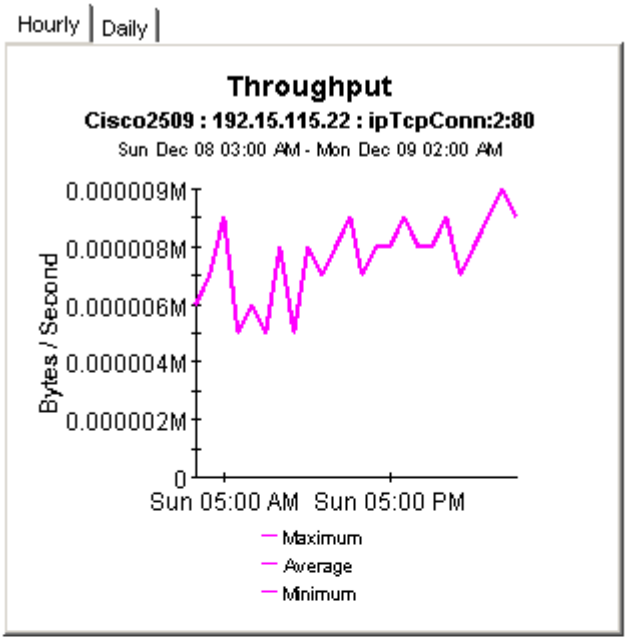


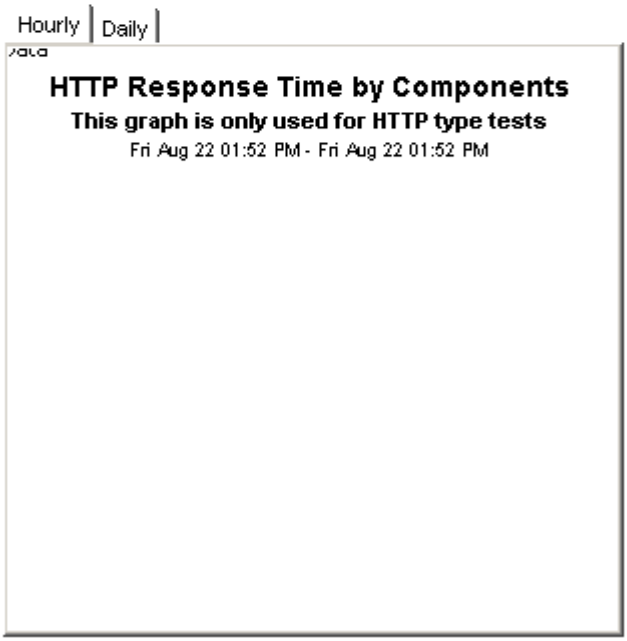
Source / Destination Pairs with Most Exceptions

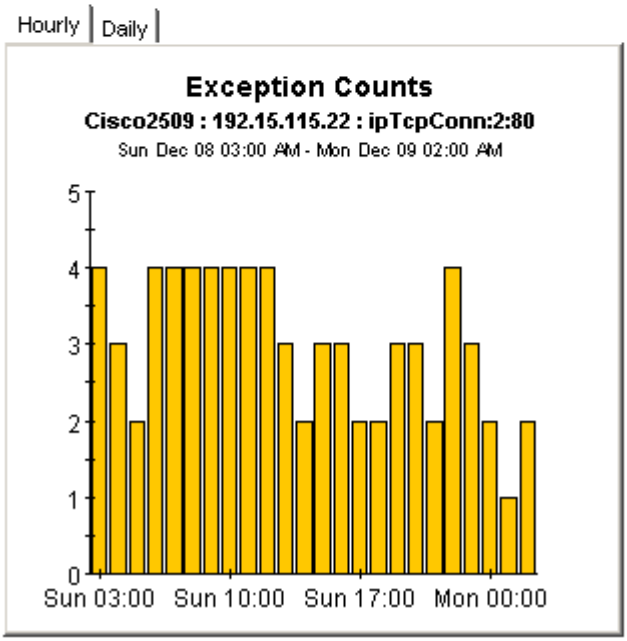
Sun Dec 08 2002

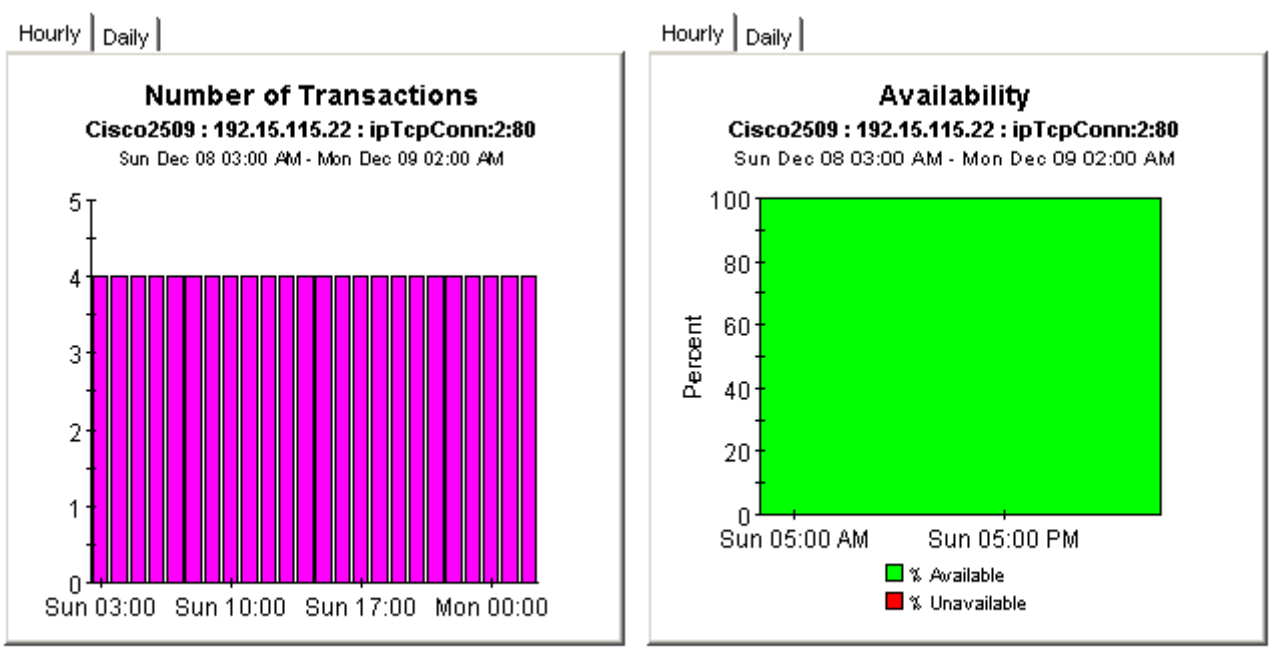
Source	Destination	Number of Transactions	Availability	Response Time Exceptions
Cisco2509	192.15.115.22	96	100.0	72


Hourly
Daily
Response Time
Cisco2509 : 192.15.115.22 : ipTcpConn:2:80
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
Seconds
Sun 05:00 AM
Sun 05:00 PM
Maximum
Average
Minimum
Threshold


Hourly
Daily
Throughput
Cisco2509 : 192.15.115.22 : ipTcpConn:2:80
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
0.000009M
0.000008M
0.000006M
0.000004M
0.000002M
0
Bytes / Second
Sun 05:00 AM
Sun 05:00 PM
Maximum
Average
Minimum


Hourly
Daily
HTTP Response Time by Components
This graph is only used for HTTP type tests
Fri Aug 22 01:52 PM - Fri Aug 22 01:52 PM


Hourly
Daily
Exception Counts
Cisco2509 : 192.15.115.22 : ipTcpConn:2:80
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
5
4
3
2
1
0
Sun 03:00
Sun 10:00
Sun 17:00
Mon 00:00


Hourly
Daily
Number of Transactions
Cisco2509 : 192.15.115.22 : ipTcpConn:2:80
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
5
4
3
2
1
0
Sun 03:00
Sun 10:00
Sun 17:00
Mon 00:00
Hourly
Daily
Availability
Cisco2509 : 192.15.115.22 : ipTcpConn:2:80
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
Percent
100
80
60
40
20
0
Sun 05:00 AM
Sun 05:00 PM
% Available
% Unavailable

7 Aggregating Performance Data

Summary reports look at aggregations of data. For example, if you are looking at the destination summary, the statistics for each destination bring together individual statistics for each source and each SAA test that was initiated by the source. The data that is brought together for the destination is either a total or an average. These are totals compiled from multiple sources:

- Number of transactions
- Number of bytes

These are averages based on results from multiple sources:

- Response time
- Throughput
- Availability

Use summary reports to find out whether recent activity appearing in a Top Ten report is a temporary condition with no history behind it, or a longer term trend that you may need to investigate more closely. The Service Assurance package includes one summary report for each of the following perspectives:

- Source
- Destination
- Application
- Location
- Customer
- Source / Destination / Application

Most summary reports have two selection tables. The Customer Summary has one selection table and the Source Summary by Application/Destination has three selection tables. The third selection table lists all application/destination pairs associated with the selected source. The Source Summary by Application/Destination provides the greatest amount of detail, since it is looking at performance from the source-destination-application perspective.

See below for samples of the following reports:

- Destination Summary
- Application Summary
- Source Summary by Application/Destination

Service Assurance

Destination Summary

The Destination Summary Report presents destination device performance metrics aggregated over all sources and applications for a given customer. This report can be used to view historical destination device performance to identify devices with degrading performance.

Sun Dec 08 2002

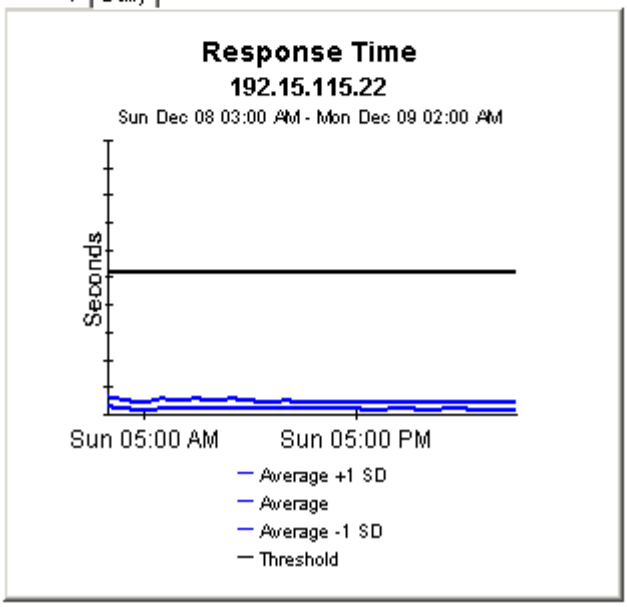
Customer	Customer ID	Number of Transactions	Number of Exceptions
All Customers	-1	2,308	75
Desktalk	3	743	73
[illegible]	[illegible]	[illegible]	[illegible]

Destination Device Selection Table

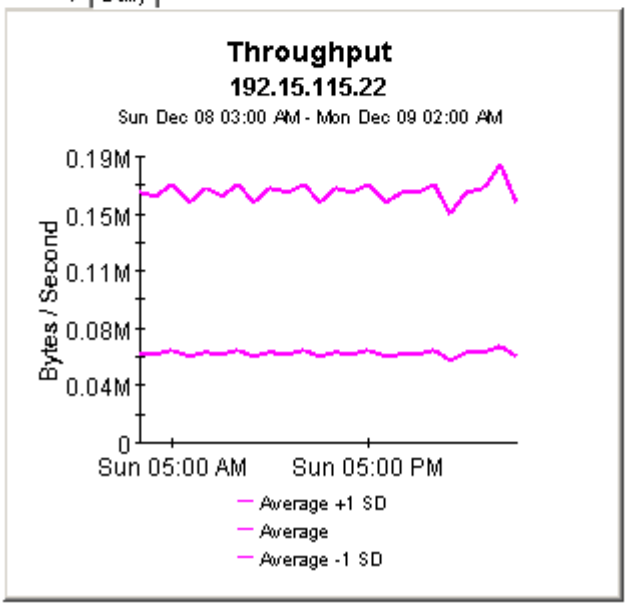
Sun Dec 08 2002

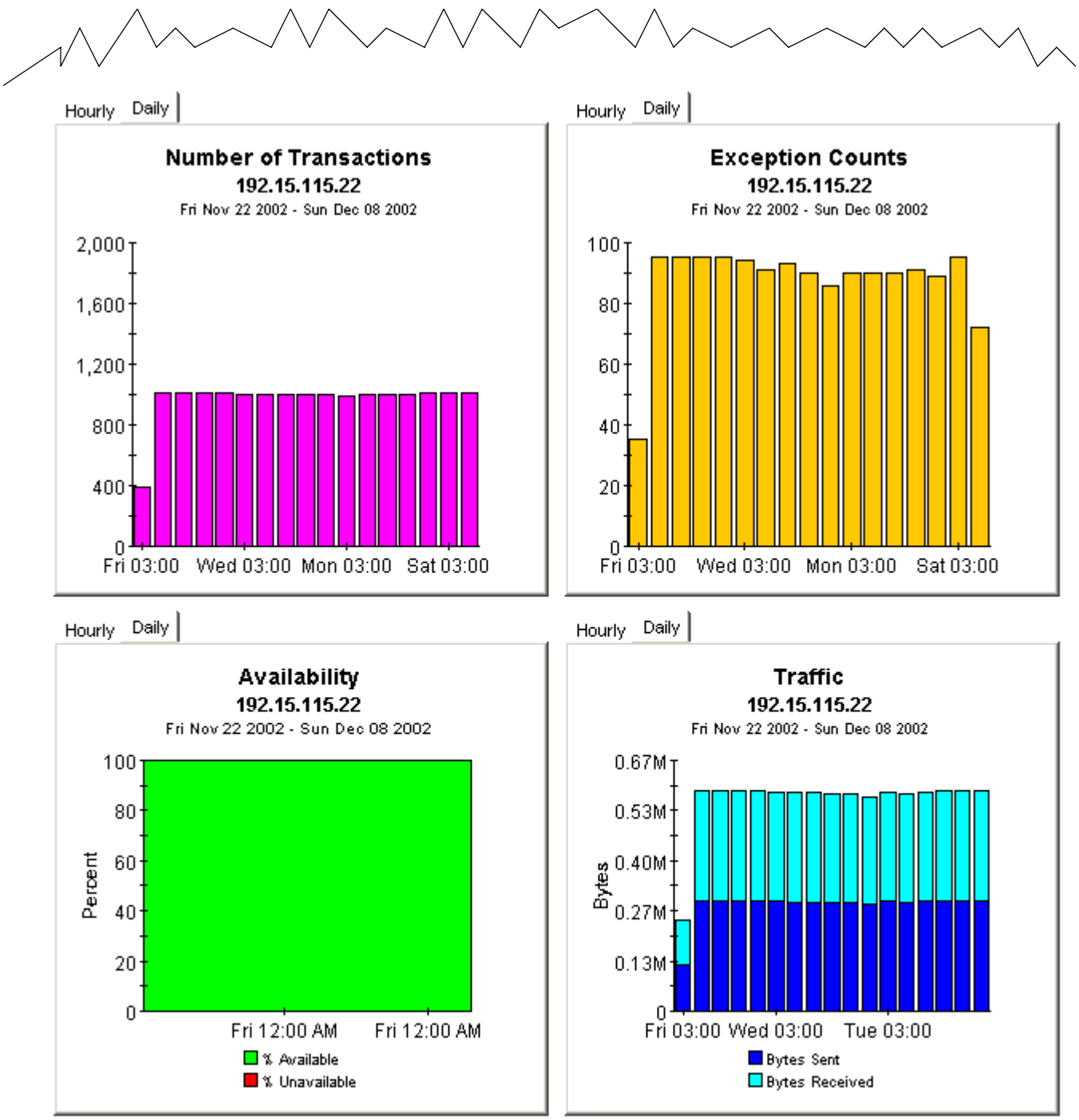
Destination	# Trans	Avg Resp. Time (Seconds)	Avg Throughput (Bps)	Availability (Percent)	Traffic (Bytes)
192.15.115.22	1,008	0.040	62.20 k	100.00	614.59 k
athp.hp.com	480	0.330	1050.9	83.33	81.12 k
www.yahoo.com	148	1.612	21.12 k	77.08	4218.4 k
ultra/README.txt	96	0.841	1.54	100.00	192.00
192.15.125.157	96	0.737	3.29	100.00	192.00
www.aol.com	96	0.435	11.26 k	100.00	229.39 k
192.15.128.51	96	0.152	7.50	100.00	192.00
192.15.96.2	96	0.120	0.00	100.00	0.00
192.15.160.51	96	0.037	29.00	100.00	192.00

Hourly | Daily



Hourly | Daily




Hourly
Daily
Number of Transactions
192.15.115.22
Fri Nov 22 2002 - Sun Dec 08 2002
2,000
1,600
1,200
800
400
0
Fri 03:00
Wed 03:00
Mon 03:00
Sat 03:00
Hourly
Daily
Exception Counts
192.15.115.22
Fri Nov 22 2002 - Sun Dec 08 2002
100
80
60
40
20
0
Fri 03:00
Wed 03:00
Mon 03:00
Sat 03:00
Hourly
Daily
Availability
192.15.115.22
Fri Nov 22 2002 - Sun Dec 08 2002
Percent
100
80
60
40
20
0
Fri 12:00 AM
Fri 12:00 AM
% Available
% Unavailable
Hourly
Daily
Traffic
192.15.115.22
Fri Nov 22 2002 - Sun Dec 08 2002
Bytes
0.67M
0.53M
0.40M
0.27M
0.13M
0
Fri 03:00
Wed 03:00
Tue 03:00
Bytes Sent
Bytes Received

Service Assurance

Application Summary

The Application Summary Report presents application performance metrics aggregated over all sources and destinations for a given customer. This report can be used to view historical application performance and identify applications with degrading performance.

Sun Dec 08 2002

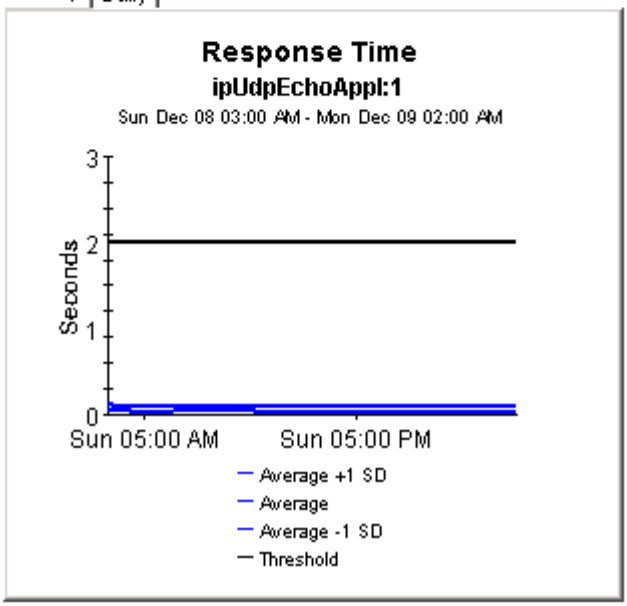
Customer	Customer ID	Number of Transactions	Number of Exceptions
All Customers	-1	2,308	75
Desktalk	3	743	73
HROV	4	1,133	2

Application Selection Table

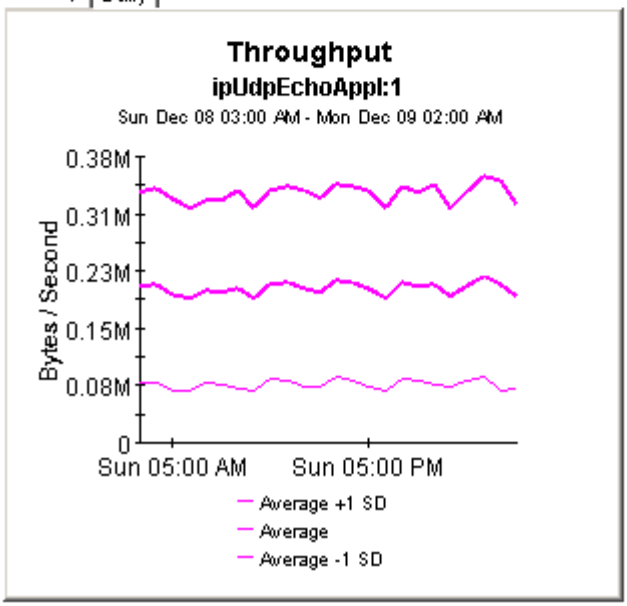
Sun Dec 08 2002

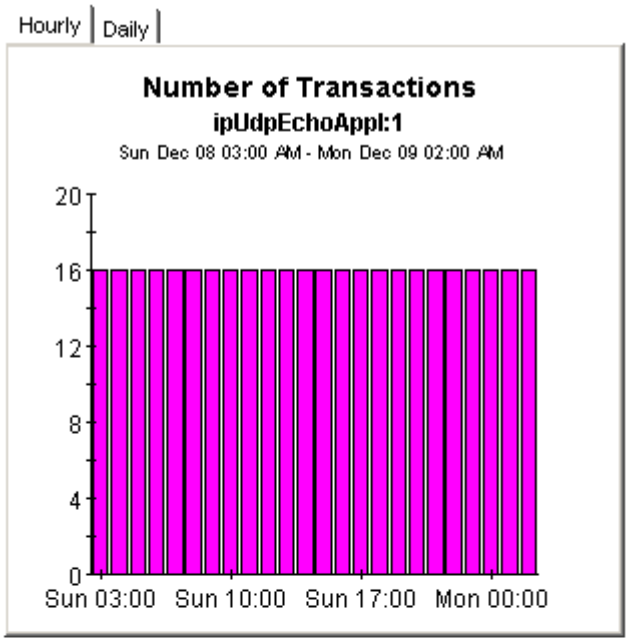
Application	# Transactions	Avg Resp. Time (Seconds)	Avg Throughput (Bps)	Availability (Percent)	Traffic (Bytes)
httpAppl:0	532	0.708	8464.7	92.36	4496.5 k
ipUdpEchoAppl:1	384	0.034	214.59 k	100.00	786.43 k
dnsAppl:0	288	0.309	13.26	100.00	576.00
iplcmpEcho:0	288	0.049	14.15 k	100.00	16.13 k
ipTcpConn:2:80	288	0.047	324.22	100.00	576.00
httpAppl:2	192	0.323	1079.8	66.67	32.45 k
iplcmpEcho:5	144	0.001	24.55 k	100.00	8064.0
ftpAppl:0	96	0.841	1.54	100.00	192.00
dlswAppl:0	96	0.120	0.00	100.00	0.00

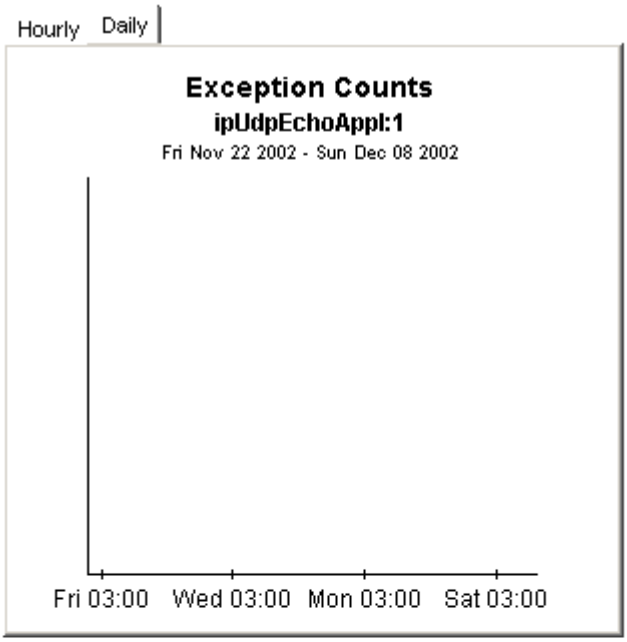
Hourly | Daily

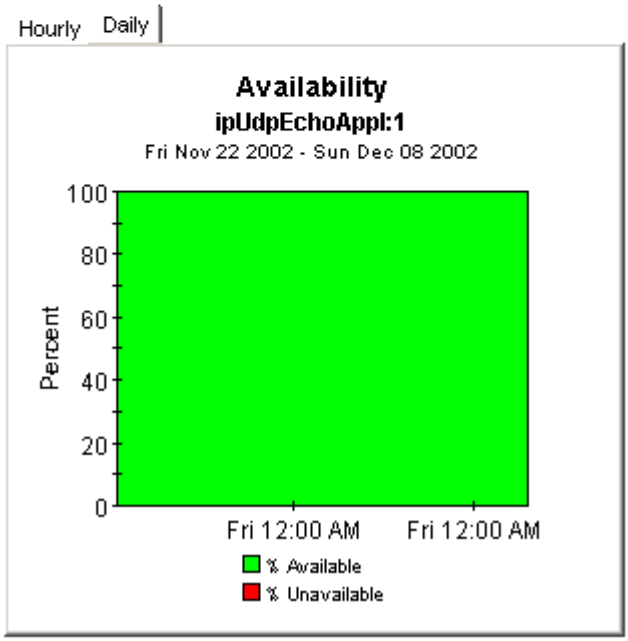


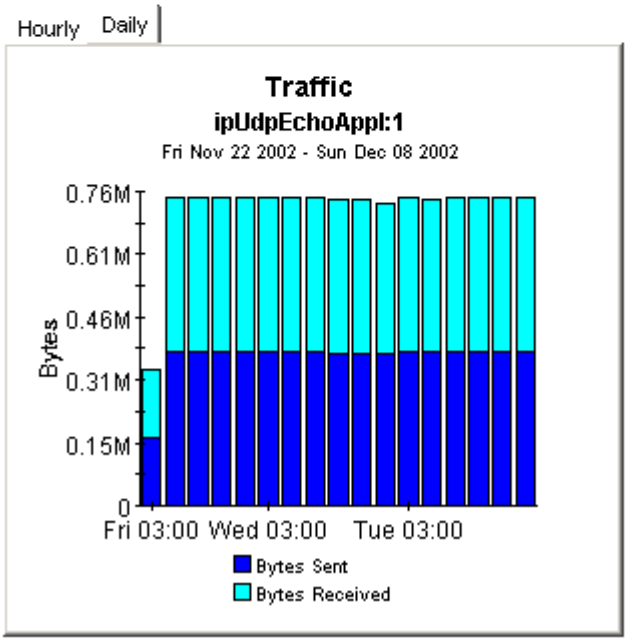
Hourly | Daily




Hourly
Daily
Number of Transactions
ipUdpEchoAppl:1
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
20
16
12
8
4
0
Sun 03:00
Sun 10:00
Sun 17:00
Mon 00:00


Hourly
Daily
Exception Counts
ipUdpEchoAppl:1
Fri Nov 22 2002 - Sun Dec 08 2002
Fri 03:00
Wed 03:00
Mon 03:00
Sat 03:00


Hourly
Daily
Availability
ipUdpEchoAppl:1
Fri Nov 22 2002 - Sun Dec 08 2002
100
80
60
40
20
0
Percent
Fri 12:00 AM
Fri 12:00 AM
% Available
% Unavailable


Hourly
Daily
Traffic
ipUdpEchoAppl:1
Fri Nov 22 2002 - Sun Dec 08 2002
0.76M
0.61M
0.46M
0.31M
0.15M
0
Bytes
Fri 03:00
Wed 03:00
Tue 03:00
Bytes Sent
Bytes Received

Service Assurance

Source Summary by Application/Destination

The Source Summary by Application / Destination Report presents hourly and daily source / application / destination performance metrics. Source devices are listed first, followed by a list of application / destination pairs utilized by the selected source device. Both lists are sorted by number of transactions. The charts below present historical performance metrics for the source / application / destination combination selected in the tables.

Sun Dec 08 2002

Customer	CustID	Number of Transactions	Number of Exceptions
Desktalk	3	743	73
HPOV	1	1,133	2
Trinagy	2	432	0

Source Device Selection Table

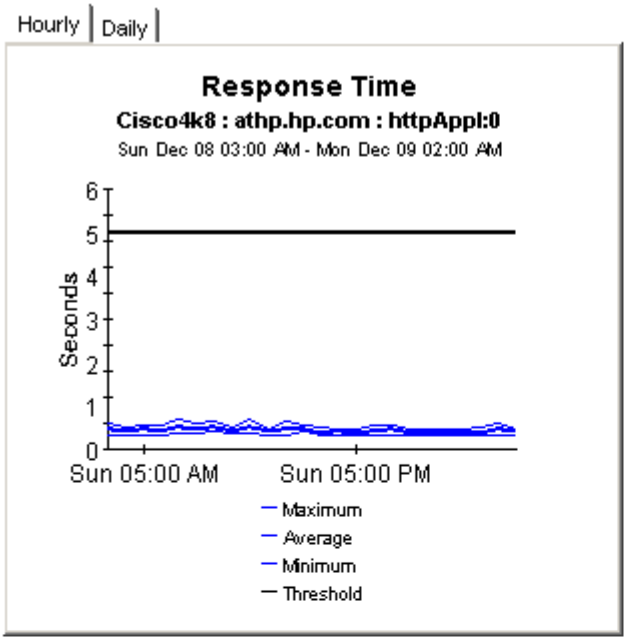
Sun Dec 08 2002

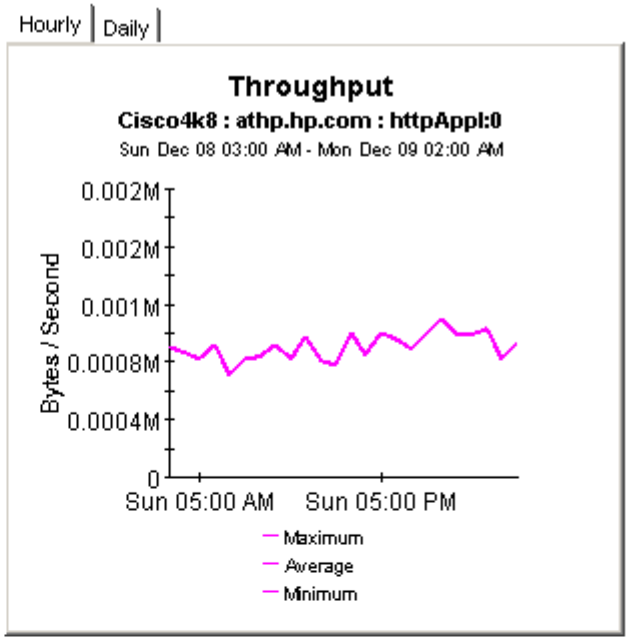
Source	# Transactions	Resp. Time (seconds)	Throughput (Bps)	Availability (Percent)	Traffic (bytes)
Cisco4k8	1,037	0.322	51.63 k	98.20	2637.2 k
Mcrouter85	96	0.737	3.29	100.00	192.00

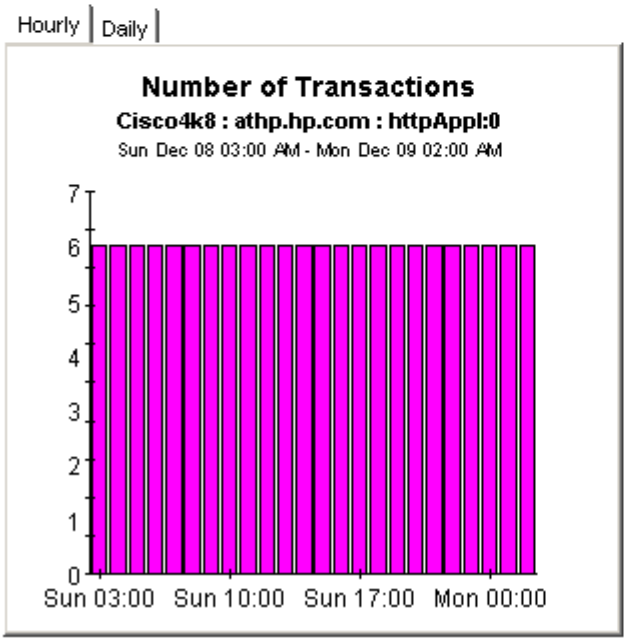
Application / Destination Pair Selection Table

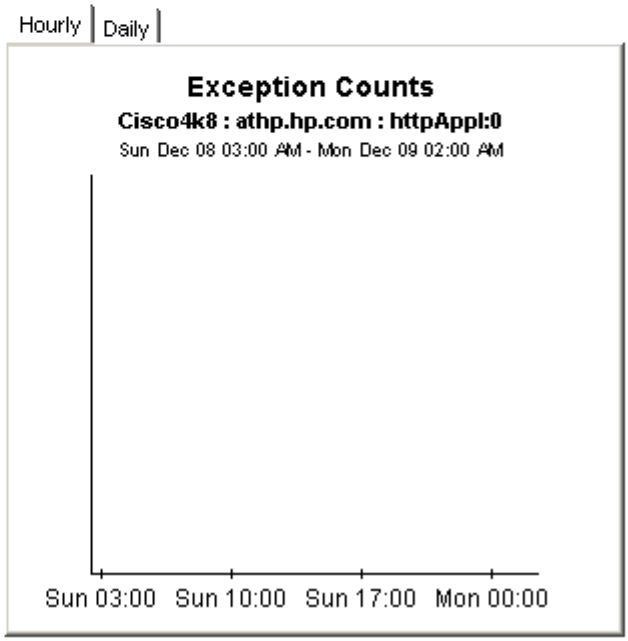
Sun Dec 08 2002

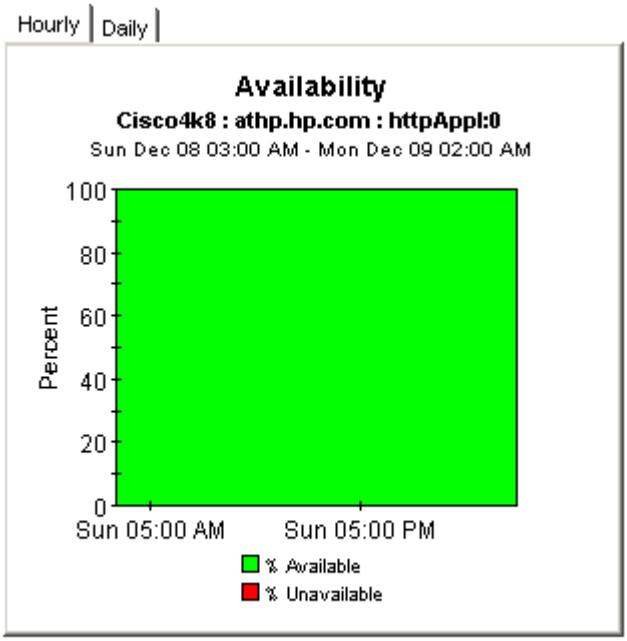
Application	Destination	# Trans	Resp. Time (seconds)	Throughput (Bps)	Availability (Percent)	Traffic (Bytes)
httpAppl:0	athp.hp.com	144	0.428	902.08	100.00	24.34 k
iplcmpEcho:5	192.15.115.22	144	0.001	24.55 k	100.00	8064.0
ftpAppl:0	ultra/README.txt	96	0.841	1.54	100.00	192.00
httpAppl:2	athp.hp.com	96	0.430	910.04	100.00	16.22 k
dnsAppl:0	192.15.128.51	96	0.152	7.50	100.00	192.00
dlswAppl:0	192.15.96.2	96	0.120	0.00	100.00	0.00
ipUdpEchoAppl:1	192.15.115.22	96	0.005	214.97 k	100.00	196.61 k
ipUdpEchoAppl:1	192.15.115.2	96	0.004	285.46 k	100.00	196.61 k
ipTcpConn:2:80	192.15.115.22	96	0.002	436.29	100.00	192.00

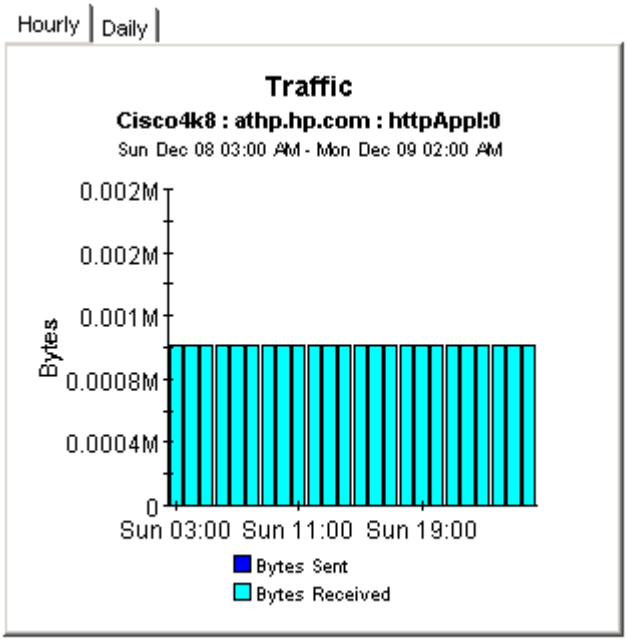

Hourly
Daily
Response Time
Cisco4k8 : athp.hp.com : httpAppl:0
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
Seconds
6
5
4
3
2
1
0
Sun 05:00 AM
Sun 05:00 PM
Maximum
Average
Minimum
Threshold


Hourly
Daily
Throughput
Cisco4k8 : athp.hp.com : httpAppl:0
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
Bytes / Second
0.002M
0.002M
0.001M
0.0008M
0.0004M
0
Sun 05:00 AM
Sun 05:00 PM
Maximum
Average
Minimum


Hourly
Daily
Number of Transactions
Cisco4k8 : athp.hp.com : httpAppl:0
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
7
6
5
4
3
2
1
0
Sun 03:00
Sun 10:00
Sun 17:00
Mon 00:00


Hourly
Daily
Exception Counts
Cisco4k8 : athp.hp.com : httpAppl:0
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
Sun 03:00
Sun 10:00
Sun 17:00
Mon 00:00


Hourly
Daily
Availability
Cisco4k8 : athp.hp.com : httpAppl:0
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
100
80
60
40
20
0
Percent
Sun 05:00 AM
Sun 05:00 PM
% Available
% Unavailable


Hourly
Daily
Traffic
Cisco4k8 : athp.hp.com : httpAppl:0
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
0.002M
0.002M
0.001M
0.0008M
0.0004M
0
Bytes
Sun 03:00
Sun 11:00
Sun 19:00
Bytes Sent
Bytes Received

8 Forecasting Future Performance

Forecast reports alert you to elements (customers, applications, sources, destinations, and locations) that may be headed for response time or throughput problems. This report comes in two styles: short and long. The following short-version reports let you drill down from customers to elements that belong to a particular customer:

- Application Forecast
- Source Forecast
- Destination Forecast
- Location Forecast
- Customer Forecast

The following long-version reports let you drill down to specific element pairs:

- Application Forecast by Source/Destination
- Application Forecast by Location/Destination
- Source Forecast by Application/Destination
- Destination Forecast by Source/Application
- Destination Forecast by Location/Application
- Location Forecast by Application/Destination

The first table sorts customers by F90 Response Time, highest to lowest. The second table sorts elements by the rate at which response time is increasing or the rate at which throughput is decreasing. The graphs provide three views of response time and throughput:

- Bar chart that compares F30 to F60 and F90
- Table showing aggregations by day of week
- Line graph tracking historic trends

See below for samples of the following reports:

- Destination Forecast
- Application Forecast
- Application Forecast by Source/Destination

Service Assurance

Destination Forecast

The Destination Forecast Report enables the user to quickly identify destination devices with the greatest projected degradation in performance. The list of destination devices are sorted by rate of increase in response time or decrease in throughput. Drill down charts present forecasted overall performance metrics for the selected device.

Fri Nov 22 03:00 AM

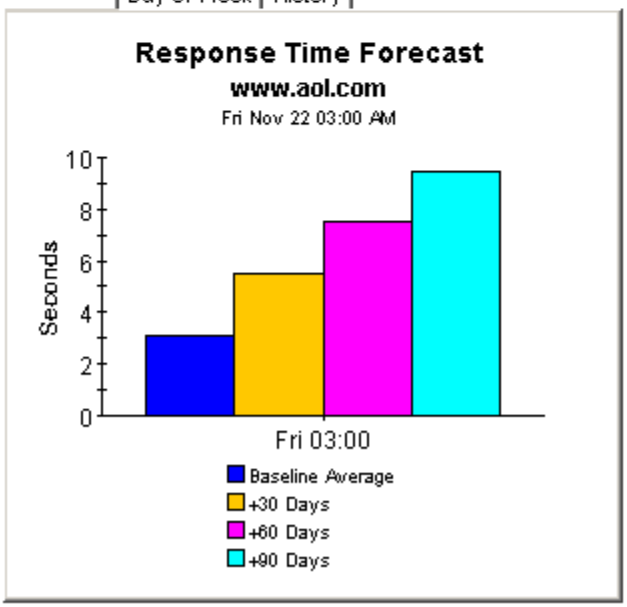
Customer	Response Time Baseline (sec)	F90 Response Time (sec)	Throughput Baseline (Bps)	F90 Throughput (Bps)
Desktalk	0.696	2.058	2984.98	0.00
Trinagy	0.686	2.103	80.67 k	0.00
HPOV	0.706	0.000	47.80 k	0.00

Destination Devices with Greatest Rate of Change in Response Time or Throughput

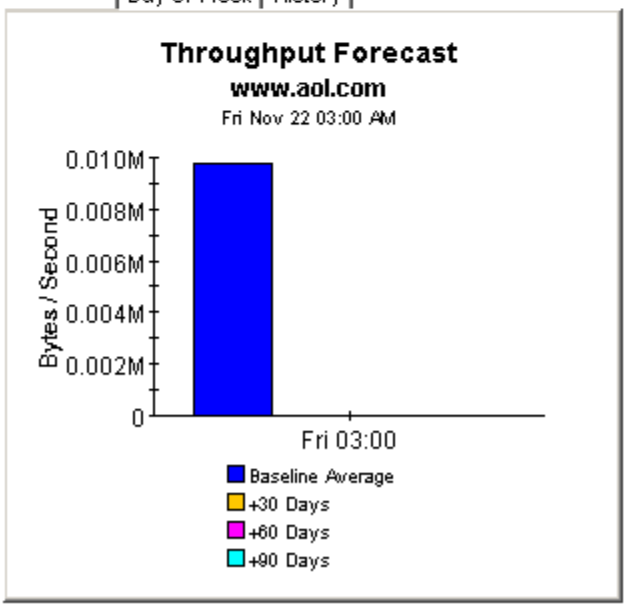
Fri Nov 22 03:00 AM

Destination	Response Time Baseline (sec)	F90 Response Time (sec)	Throughput Baseline (Bps)	F90 Throughput (Bps)
www.aol.com	3.080	9.460	9784.88	0.00
192.15.115.22	0.003	0.006	99.54 k	0.00
athp.hp.com		0.000	0.00	0.00
192.15.128.51		0.000	0.00	0.00

Standard | Day of Week | History



Standard | Day of Week | History



Service Assurance

Application Forecast

The Application Forecast Report enables the user to quickly identify applications with the greatest projected degradation in performance. The list of applications are sorted by rate of increase in response time or decrease in throughput. Drill down charts present forecasted overall performance metrics for the selected application.

Fri Nov 22 03:00 AM

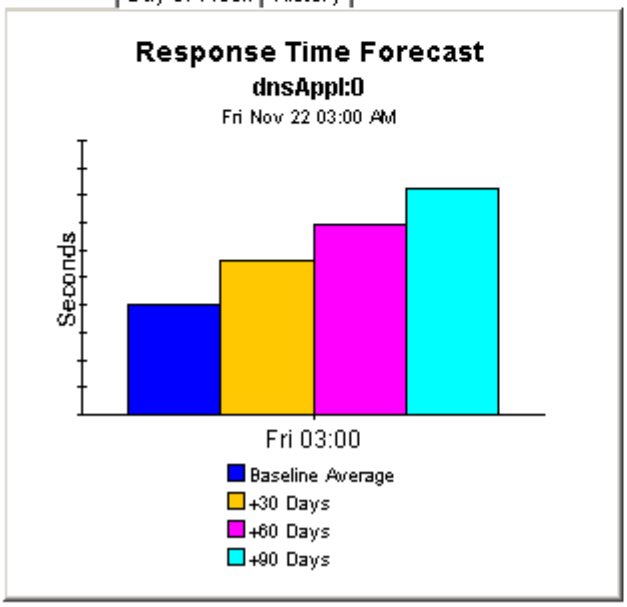
Customer	Response Time Baseline (sec)	F90 Response Time (sec)	Throughput Baseline (Bps)	F90 Throughput (Bps)
Desktalk	0.696	2.058	2984.98	0.00
Trinagy	0.686	2.103	80.67 k	0.00
HPOV	0.706	0.000	47.80 k	0.00

Applications with Greatest Rate of Change in Response Time or Throughput

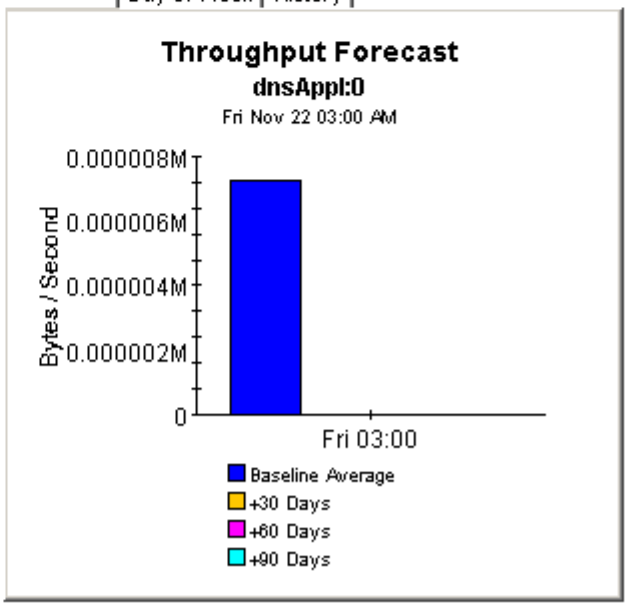
Fri Nov 22 03:00 AM

Application	Response Time Baseline (sec)	F90 Response Time (sec)	Throughput Baseline (Bps)	F90 Throughput (Bps)
dnsAppl:0	0.800	1.653	7.25	0.00
httpAppl:2	1.165	1.723	606.06	0.00
ipTcpConn:2:80	0.874	6.401	2.88	0.00
httpAppl:0	1.453	3.973	5971.08	0.00
ipIcmpEcho:0	0.130	0.410	224.94	0.00
ipUdpEchoAppl:1	0.155	0.331	6765.75	0.00

Standard | Day of Week | History



Standard | Day of Week | History



Service Assurance

Application Forecast by Source/Destination

The Application Forecast by Source / Destination Report enables the user to quickly identify applications with the greatest projected degradation in performance. The list of applications are sorted by rate of increase in response time or decrease in throughput. Source / Destination pairs utilizing the selected application can be selected to retrieve forecasted performance metrics.

Fri Nov 22 03:00 AM

Customer	CustID	Response Time Baseline (sec)	F90 Response Time (sec)	Throughput Baseline (Bps)	F90 Throughput (Bps)
Desktalk	3	0.696	2.058	2984.98	0.00
Trinagy	2	0.686	2.103	80.67 k	0.00
HPOV	1	0.706	0.000	47.80 k	0.00

Applications with Greatest Rate of Change in Response Time or Throughput

Fri Nov 22 03:00 AM

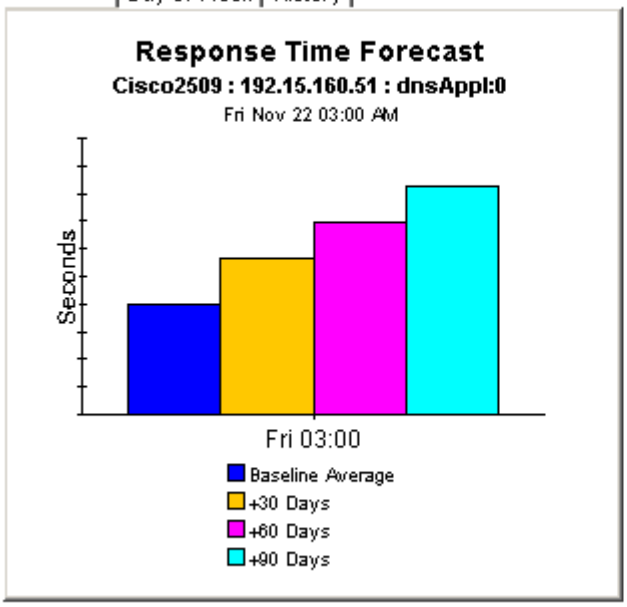
Application	Response Time Baseline (sec)	F90 Response Time (sec)	Throughput Baseline (Bps)	F90 Throughput (Bps)
dnsAppl:0	0.800	1.653	7.25	0.00
httpAppl:2	1.165	1.723	606.06	0.00
ipTcpConn:2:80	0.874	6.401	2.88	0.00
httpAppl:0	1.453	3.973	5971.08	0.00
ipIcmpEcho:0	0.130	0.410	224.94	0.00
ipUdpEchoAppl:1	0.155	0.331	6765.75	0.00

Source / Destination Pairs with Greatest Rate of Change in Response Time or Throughput

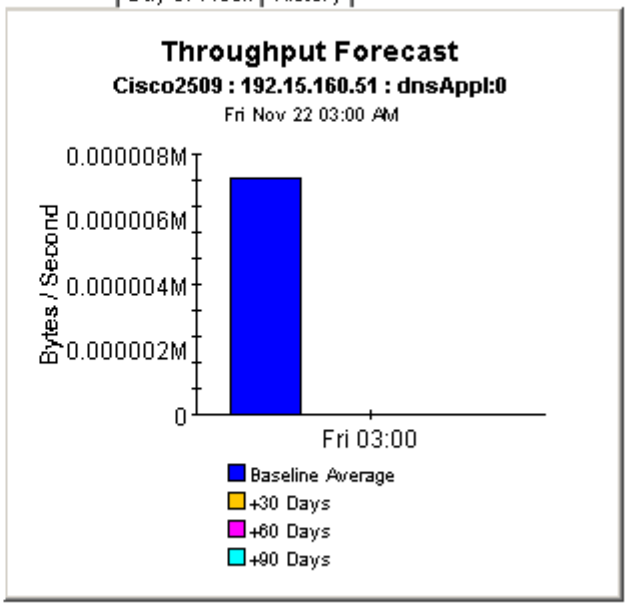
Fri Nov 22 03:00 AM

Source	Destination	Response Time Baseline (sec)	F90 Reponse Time (sec)	Throughput Baseline (Bps)	F90 Throughput (Bps)
Cisco2509	192.15.160.51	0.800	1.653	7.25	0.00

Standard | Day of Week | History



Standard | Day of Week | History



Standard | Day of Week | History

Response Time Forecast

Cisco2509 : 192.15.160.51 : dnsAppl:0

Thu Nov 28 03:00 AM

Day	Baseline (sec)	+ 30 / 60 / 90 Days (sec)
Sun	1.16	0.000 / 0.000 / 0.000
Mon	0.79	8.016 / 14.485 / 20.954
Tue	0.80	7.938 / 14.333 / 20.729
Wed	0.44	3.825 / 6.858 / 9.892
Thu	1.17	0.000 / 0.000 / 0.000
Fri	0.56	0.690 / 0.797 / 0.905
Sat	0.80	0.000 / 0.000 / 0.000

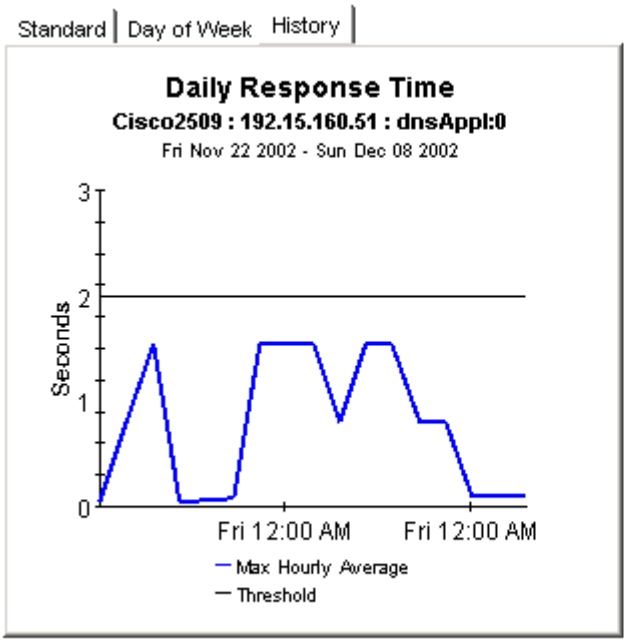
Standard | Day of Week | History

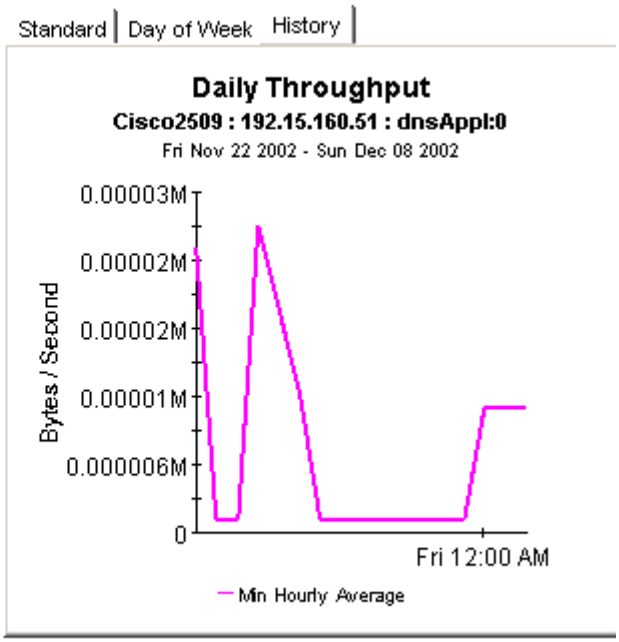
Throughput Forecast (Bytes/Second)

Cisco2509 : 192.15.160.51 : dnsAppl:0

Thu Nov 28 03:00 AM

Day	Baseline	+ 30 / 60 / 90 Days
Sun	1.00	1.00 / 1.00 / 1.00
Mon	14.00	0.00 / 0.00 / 0.00
Tue	10.50	0.00 / 0.00 / 0.00
Wed	6.50	0.00 / 0.00 / 0.00
Thu	1.00	1.00 / 1.00 / 1.00
Fri	12.33	0.00 / 0.00 / 0.00
Sat	4.33	30.76 / 52.19 / 73.62


Standard
Day of Week
History
Daily Response Time
Cisco2509 : 192.15.160.51 : dnsAppl:0
Fri Nov 22 2002 - Sun Dec 08 2002
Seconds
3
2
1
0
Fri 12:00 AM
Fri 12:00 AM
Max Hourly Average
Threshold


Standard
Day of Week
History
Daily Throughput
Cisco2509 : 192.15.160.51 : dnsAppl:0
Fri Nov 22 2002 - Sun Dec 08 2002
Bytes / Second
0.00003M
0.00002M
0.00002M
0.00001M
0.000006M
0
Fri 12:00 AM
Min Hourly Average

9 Ranking the Worst Performers

A top ten report performs a ranking function for yesterday's collection of test results. Use this type of report to identify potential problems related to response time, throughput, transaction counts, or traffic volume. Service Assurance contains five top ten reports:

- Application
- Customer
- Destination
- Location
- Source

Except for the Customer Top Ten, which is slightly different, each reports contains a customer table followed by ten tables with ten entries in each table. The tables are:

- Worst response time
- Response time increase
- Worst throughput
- Throughput increase
- Most transactions
- Most traffic

See below for samples of the following reports:

- Application Top Ten
- Destination Top Ten

Service Assurance

Application Top Ten

The Application Top Ten Report provides lists of applications which had the worst performance (response time and throughput) or highest volume (transactions and total bytes) during the previous day. Applications are also listed by the projected rate of change for each metric.

Customer	Customer Id
All Customers	-1
HPOV	1
Trinagy	2
Desktalk	3

Worst Response Time (Seconds)

Sun Dec 08 03:00 AM

	Application	Average Response Time
1	ftpAppl:0	0.841
2	httpAppl:0	0.708
3	httpAppl:2	0.323
4	dnsAppl:0	0.309
5	dlswAppl:0	0.120
6	iplcmpEcho:0	0.049
7	ipTcpConn:2:80	0.047
8	ipUdpEchoAppl:1	0.034
9	iplcmpEcho:5	0.001
10	dhcpAppl:0	0.000

Response Time Increase (Seconds)

Thu Dec 05 03:00 AM

	Application	Baseline	+ 30 / 60 / 90 Days
1	ipTcpConn:2:80	0.307	1.016 / 1.583 / 2.150
2	dnsAppl:0	0.791	1.607 / 2.259 / 2.911
3	iplcmpEcho:0	0.065	0.119 / 0.162 / 0.205
4	httpAppl:0	1.369	1.994 / 2.495 / 2.995
5	iplcmpEcho:5	0.002	0.002 / 0.003 / 0.003
6	ipUdpEchoAppl:1	0.041	0.049 / 0.056 / 0.063
7	httpAppl:2	0.983	1.086 / 1.167 / 1.249
8	dlswAppl:0	0.127	0.104 / 0.082 / 0.059
9	ftpAppl:0	3.382	0.000 / 0.000 / 0.000
10	dhcpAppl:0		0.000 / 0.000 / 0.000

Worst Throughput (Bytes/Second)

Sun Dec 08 03:00 AM

	Application	Average Throughput
1	dlswAppl:0	0.00
2	ftpAppl:0	1.54
3	dnsAppl:0	13.26
4	ipTcpConn:2:80	324.22
5	httpAppl:2	1079.75
6	httpAppl:0	8464.67
7	iplcmpEcho:0	14.15 k
8	iplcmpEcho:5	24.55 k
9	ipUdpEchoAppl:1	214.59 k
10	dhcpAppl:0	0.00

Throughput Decrease (Bytes/Second)

Thu Dec 05 03:00 AM

	Application	Baseline	+ 30 / 60 / 90 Days
1	dnsAppl:0	6.03	0.00 / 0.00 / 0.00
2	httpAppl:0	8472.06	454.55 / 0.00 / 0.00
3	httpAppl:2	724.53	60.92 / 0.00 / 0.00
4	iplcmpEcho:0	11.67 k	6770.3 / -1068 / 0.0(
5	ipTcpConn:2:80	258.21	199.98 / 106.81 / 106.
6	iplcmpEcho:5	15.12 k	12.46 k / 10.34 k / 8217
7	ipUdpEchoAppl:1	191.57 k	165.33 k / 144.34 k / 123.
8	ftpAppl:0	0.13	0.13 / 0.13 / 0.13
9	dhcpAppl:0	0.00	0.00 / 0.00 / 0.00
10	dlswAppl:0	0.00	0.00 / 0.00 / 0.00

Most Transactions

Sun Dec 08 03:00 AM

Application	Number of Transactions
httpAppl:0	532
ipUdpEchoAppl:1	384
dnsAppl:0	288
ipTcpConn:2:80	288
iplcmpEcho:0	288
httpAppl:2	192
iplcmpEcho:5	144
ftpAppl:0	96
dlswAppl:0	96
dhcpAppl:0	0

Traffic (Bytes)

Sun Dec 08 03:00 AM

	Application	Total Traffic
1	httpAppl:0	4496.51 k
2	ipUdpEchoAppl:1	786.43 k
3	httpAppl:2	32.45 k
4	iplcmpEcho:0	16.13 k
5	iplcmpEcho:5	8064.00
6	dnsAppl:0	576.00
7	ipTcpConn:2:80	576.00
8	ftpAppl:0	192.00
9	dhcpAppl:0	0.00
10	dlswAppl:0	0.00

Service Assurance

Destination Top Ten

The Destination Top Ten Report provides lists of destination devices which had the worst performance (response time and throughput) or highest volume (transactions and total bytes) during the previous day. Destination devices are also listed by the projected rate of change for each metric.

Customer	Customer Id
All Customers	-1
HPOV	1
Trinagy	2
Desktalk	3

Worst Response Time (Seconds)

Sun Dec 08 03:00 AM

	Destination	Average Response Time
1	www.yahoo.com	1.612
2	ultra/README.txt	0.841
3	192.15.125.157	0.737
4	www.aol.com	0.435
5	athp.hp.com	0.330
6	192.15.128.51	0.152
7	192.15.96.2	0.120
8	192.15.115.22	0.040
9	192.15.160.51	0.037
10	192.15.115.2	0.004

Response Time Increase (Seconds)

Thu Dec 05 03:00 AM

	Destination	Baseline	+ 30 / 60 / 90 Days
1	192.15.115.22	0.119	0.326 / 0.491 / 0.657
2	www.aol.com	3.080	5.530 / 7.490 / 9.450
3	192.15.160.51	0.800	1.128 / 1.391 / 1.653
4	www.yahoo.com	2.376	3.219 / 3.894 / 4.569
5	192.15.115.2	0.004	0.006 / 0.006 / 0.007
6	athp.hp.com	0.805	0.998 / 1.153 / 1.307
7	192.15.128.51	1.166	1.129 / 1.100 / 1.071
8	192.15.96.2	0.127	0.104 / 0.082 / 0.059
9	ultra/README.txt	3.382	0.000 / 0.000 / 0.000
10	192.15.125.157	2.137	0.000 / 0.000 / 0.000

Worst Throughput (Bytes/Second)

Sun Dec 08 03:00 AM

	Destination	Average Throughput
1	192.15.96.2	0.00
2	ultra/README.txt	1.54
3	192.15.125.157	3.29
4	192.15.128.51	7.50
5	192.15.160.51	29.00
6	athp.hp.com	1050.92
7	www.aol.com	11.26 k
8	www.yahoo.com	21.12 k
9	192.15.115.22	62.20 k
10	192.15.115.2	285.46 k

Throughput Decrease (Bytes/Second)

Tue Dec 03 03:00 AM

	Destination	Baseline	+ 30 / 60 / 90 Days
1	192.15.160.51	7.25	0.00 / 0.00 / 0.00
2	www.aol.com	9784.88	0.00 / 0.00 / 0.00
3	www.yahoo.com	18.52 k	6344.1 / 0.00 / 0.00
4	athp.hp.com	827.67	418.08 / -237.3 / 0.00
5	192.15.115.2	235.50 k	168.88 k / 115.59 k / 62.29 k
6	192.15.115.22	56.02 k	46.41 k / 38.72 k / 31.03 k
7	ultra/README.txt	0.13	0.13 / 0.13 / 0.13
8	192.15.125.157	0.60	0.60 / 0.60 / 0.60
9	192.15.128.51	1.19	4.66 / 10.22 / 10.22
10	192.15.128.31	0.00	0.00 / 0.00 / 0.00

Most Transactions

Sun Dec 08 03:00 AM

	Destination	Number of Transactions
1	192.15.115.22	1,008
2	athp.hp.com	480
3	www.yahoo.com	148
4	ultra/README.txt	96
5	www.aol.com	96
6	192.15.96.2	96
7	192.15.115.2	96
8	192.15.128.51	96
9	192.15.160.51	96
10	192.15.125.157	96

Traffic (Bytes)

Sun Dec 08 03:00 AM

	Destination	Total Traffic
1	www.yahoo.com	4218.45 k
2	192.15.115.22	614.59 k
3	www.aol.com	229.39 k
4	192.15.115.2	196.61 k
5	athp.hp.com	81.12 k
6	ultra/README.txt	192.00
7	192.15.128.51	192.00
8	192.15.160.51	192.00
9	192.15.125.157	192.00

10 Sample Data in Near Real Time

The reports in previous chapters look backward in time, to what happened yesterday, last week, last month — and forward in time, to what is expected to happen in the future. The Near Real Time (NRT) reports looks at sample data collected over the last six hours.

If you install the Cisco SAA Datapipe only, you have one NRT report, NRT Summary inside the Source/Destination/Application folder. The contents of this report come from data stored by SAA in the MIB History Table. This report changes once an hour. Use this report to identify:

- Source / destination / application combinations with high exception counts
- Availability percentage for each combination

The NRT Summary includes *any* combination that experienced activity during the last six hours, not just combinations that reported exceptions. If an exception count looks unusual, and you want to know how NRT performance compares with past performance, inspect the following graphs, tabbed `Last 24 Hours` and `Last 30 Days`:

- Response time
- Throughput
- Transactions
- Exception Counts
- Availability
- Traffic

If you install the Cisco SAA NRT Datapipe, you will have three additional NRT reports:

- Near Real Time - Latest Test
- Jitter Near Real Time - Latest Test
- VoIP Near Real Time - Latest Test

The contents of these reports are derived from data stored by SAA in the Latest Test Table. How often the contents of these reports are updated depends on how frequently the Cisco SAA NRT Datapipe polls the Latest Test Table. The maximum frequency is once every 5 minutes.

See below for samples of the following reports:

- NRT Summary
- Jitter NRT - Latest Test
- VoIP NRT - Latest Test

Service Assurance

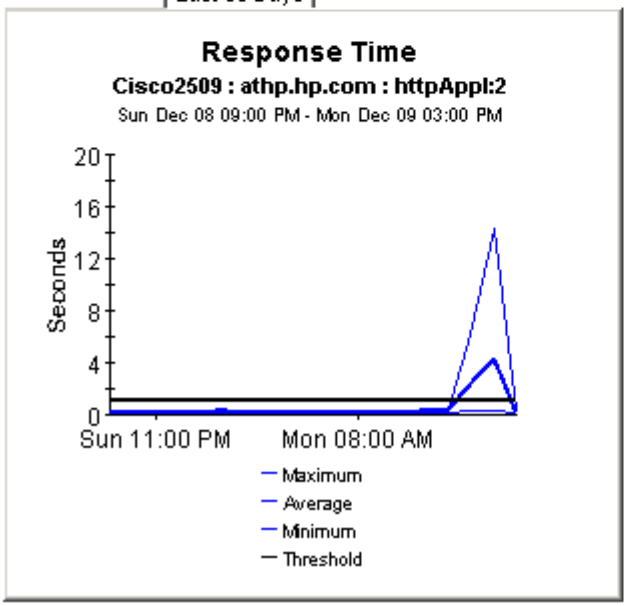
Near Real Time Summary

The Near Real Time Summary Report presents the most recent performance statistics available. Data is presented for each source / destination / application combination that had activity within the last 6 hours. By selecting a source / destination / application combination, performance data for both the last 24 hours and the last 30 days can be analyzed.

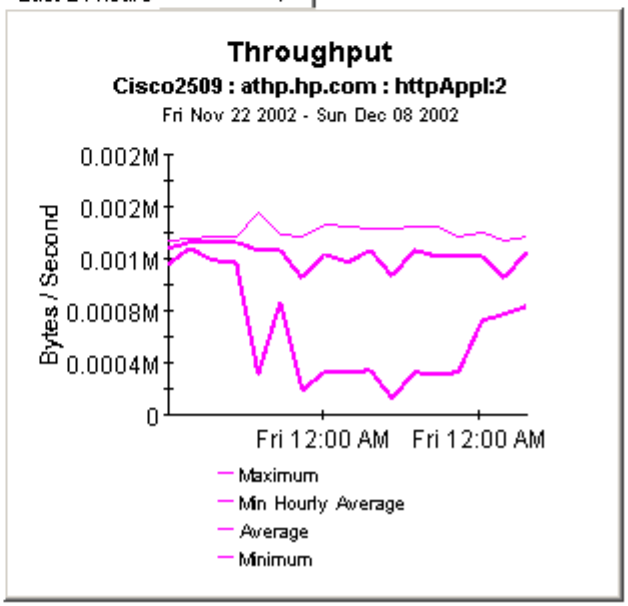
Mon Dec 09 07:00 PM

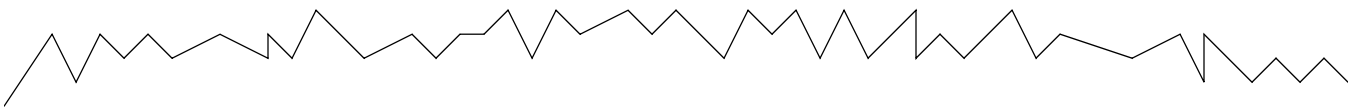
Source / Destination / Application	Exceptions	Availabilty (Percent)
Cisco2509 / 192.15.115.22 / ipTcpConn:2:80	7	100.00
Cisco2509 / athp.hp.com / httpAppl:2	3	91.67
Cisco2509 / www.yahoo.com / httpAppl:0	1	50.00
Cisco4k8 / www.yahoo.com / httpAppl:0	1	58.33
Cisco2509 / athp.hp.com / httpAppl:0	1	94.74
Cisco1700 / athp.hp.com / httpAppl:2	0	0.00
15.24.115.3 / www.yahoo.com / httpAppl:0	0	96.43
15.24.115.3 / 15.6.96.2 / dlswAppl:0	0	100.00
15.24.115.3 / 15.24.115.22 / ipTcpConn:2:80	0	100.00
15.24.115.3 / 15.24.115.22 / ipUdpEchoAppl:1	0	100.00

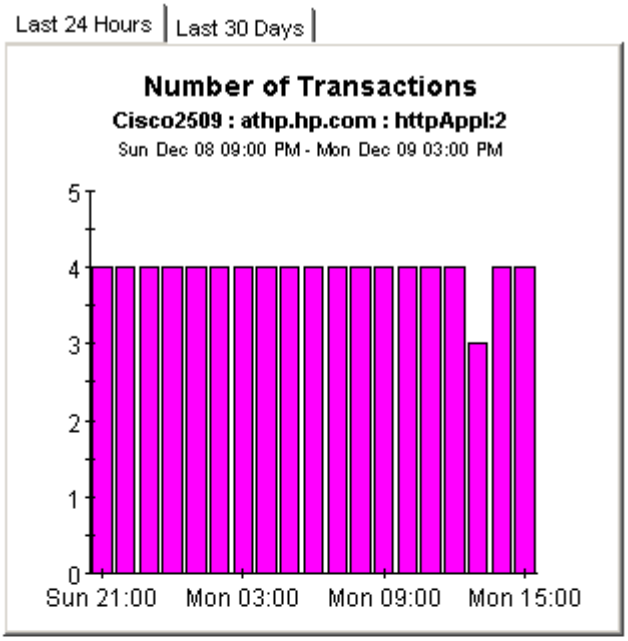
Last 24 Hours | Last 30 Days

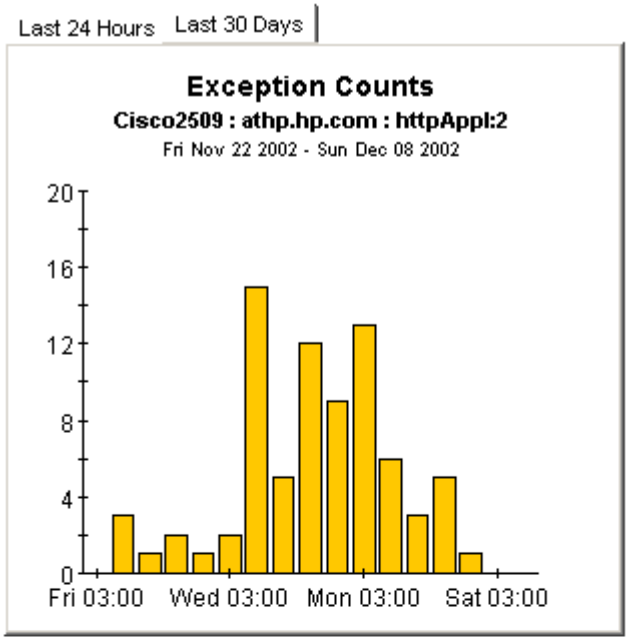


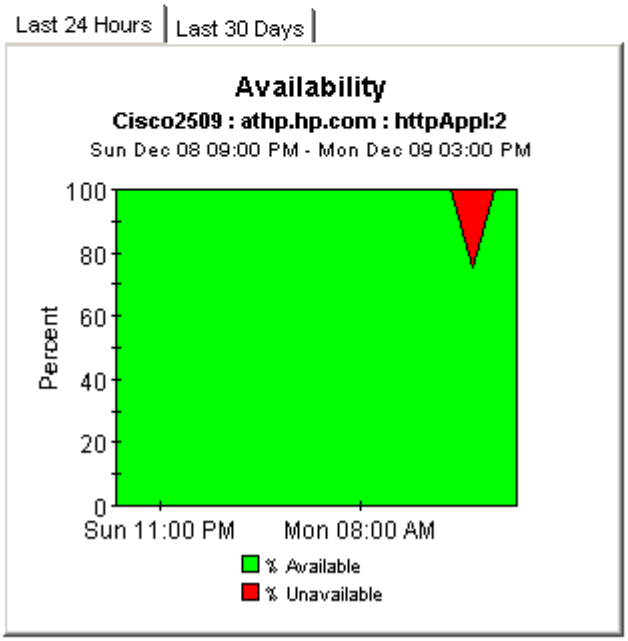
Last 24 hours | Last 30 Days

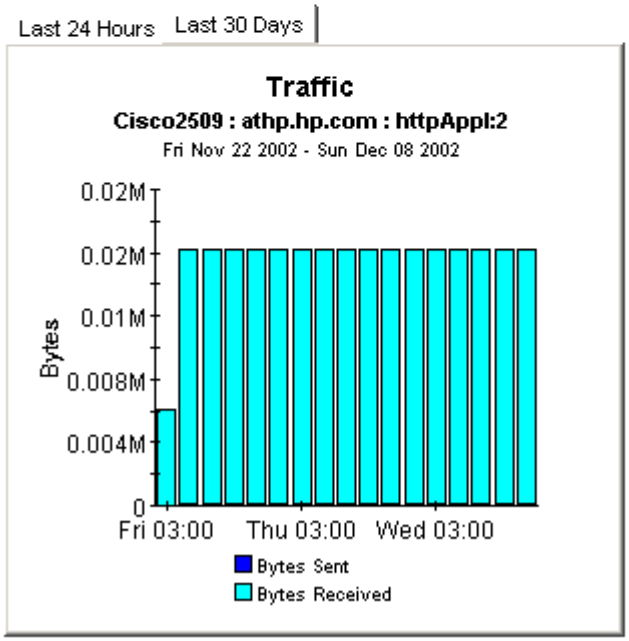





Last 24 Hours
Last 30 Days
Number of Transactions
Cisco2509 : athp.hp.com : httpAppl:2
Sun Dec 08 09:00 PM - Mon Dec 09 03:00 PM
5
4
3
2
1
0
Sun 21:00
Mon 03:00
Mon 09:00
Mon 15:00


Last 24 Hours
Last 30 Days
Exception Counts
Cisco2509 : athp.hp.com : httpAppl:2
Fri Nov 22 2002 - Sun Dec 08 2002
20
16
12
8
4
0
Fri 03:00
Wed 03:00
Mon 03:00
Sat 03:00


Last 24 Hours
Last 30 Days
Availability
Cisco2509 : athp.hp.com : httpAppl:2
Sun Dec 08 09:00 PM - Mon Dec 09 03:00 PM
Percent
100
80
60
40
20
0
Sun 11:00 PM
Mon 08:00 AM
% Available
% Unavailable


Last 24 Hours
Last 30 Days
Traffic
Cisco2509 : athp.hp.com : httpAppl:2
Fri Nov 22 2002 - Sun Dec 08 2002
Bytes
0.02M
0.02M
0.01M
0.008M
0.004M
0
Fri 03:00
Thu 03:00
Wed 03:00
Bytes Sent
Bytes Received

Service Assurance

Jitter Near Real Time - Latest Test

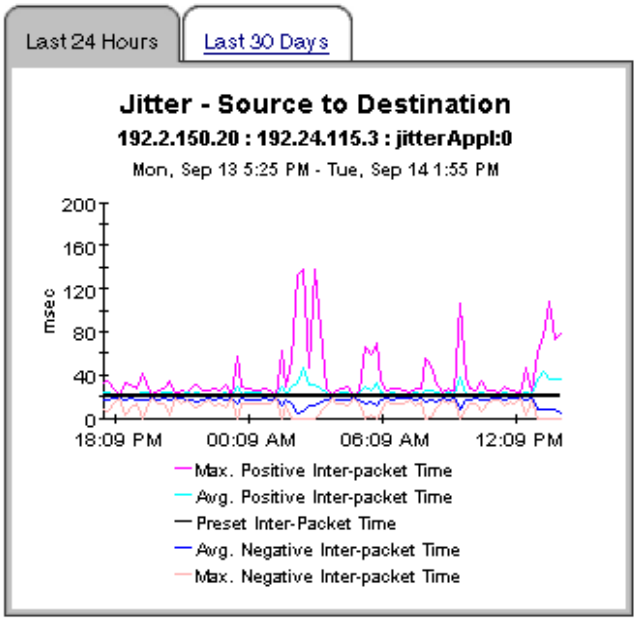
The Jitter Near Real Time - Latest Test Report presents the most recent performance statistics available for Jitter tests. Data is presented for each source / destination combination that had activity within the last 6 hours. By selecting a source / destination combination, performance data for both the last 24 hours and the last 30 days can be analyzed.

Source	Destination	Tag	Avg Response Time (msec)	Avg SD Dev (msec)	Avg DS Dev (msec)	Avg PacketLoss (SD/DS,%)
192.2.150.20	192.24.115.3	SNMP_JITTER	77.1	-8.0 / +8.8	-4.6 / +5.7	1.0 / 0.0
192.24.115.3	192.24.115.7	SNMP_JITTER	1.5	-1.0 / +1.0	-1.0 / +1.0	0.0 / 0.0
192.2.150.20	192.2.150.1	\VoIPG711ulaw	1.0	-2.1 / +2.1	-1.0 / +1.0	0.0 / 0.0
192.2.150.20	192.2.150.1	\VoIPG711alaw	1.0	-1.7 / +1.8	-1.0 / +1.0	0.0 / 0.0
192.2.150.20	192.2.150.1	\VoIPG729a	1.0	-2.0 / +2.1	-1.0 / +1.0	0.0 / 0.0
192.2.150.20	192.2.150.1	\VoIPG729a2	1.0	-1.0 / +1.0	-1.0 / +1.0	0.0 / 0.0
192.2.150.20	192.2.150.1	voiceCalcImpairm	1.0	-1.0 / +1.0	-1.0 / +1.0	0.0 / 0.0
192.24.115.3	192.24.115.2	SNMP_JITTER	1.0	-1.0 / +1.0	-1.0 / +1.0	0.0 / 0.0

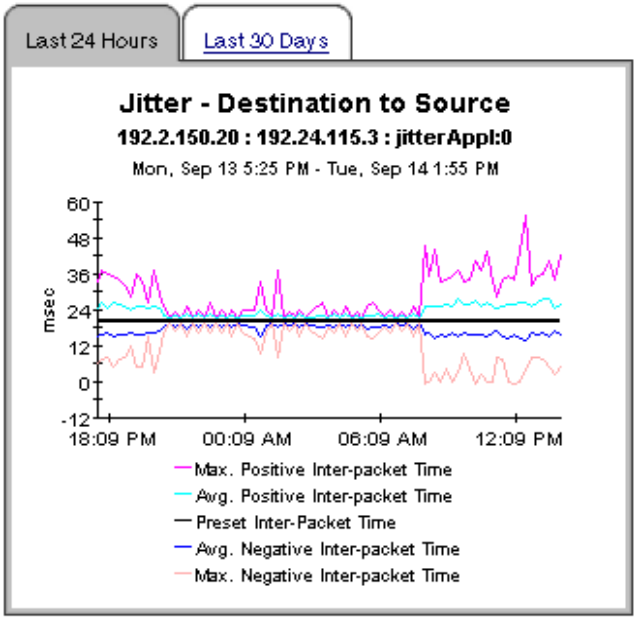
More Information for Selected Test

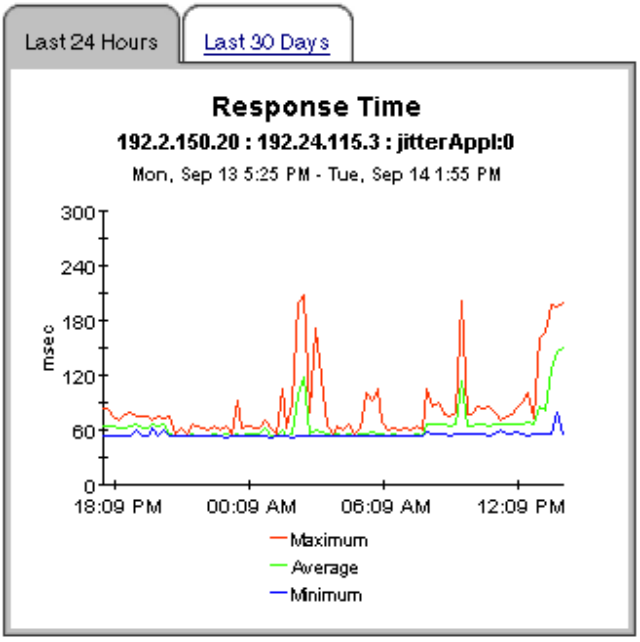
Source Location	Destination Location	TOS	Total RTT
Ft. Collins	Reston	0	2377

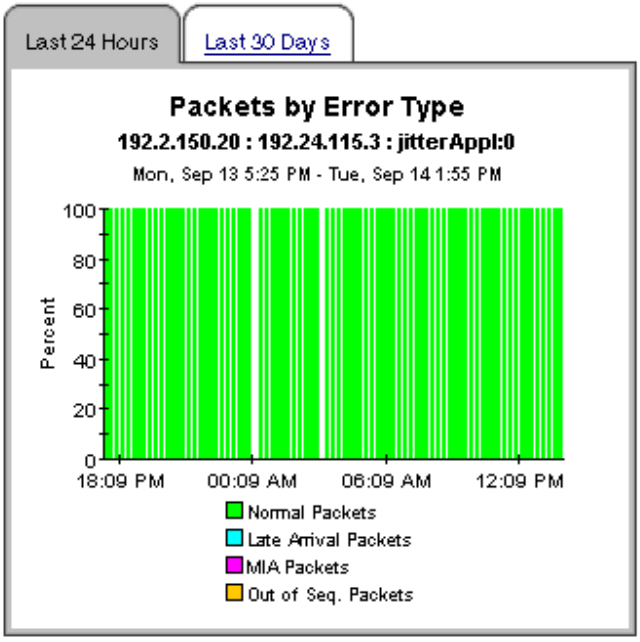
Last 24 Hours | Last 30 Days

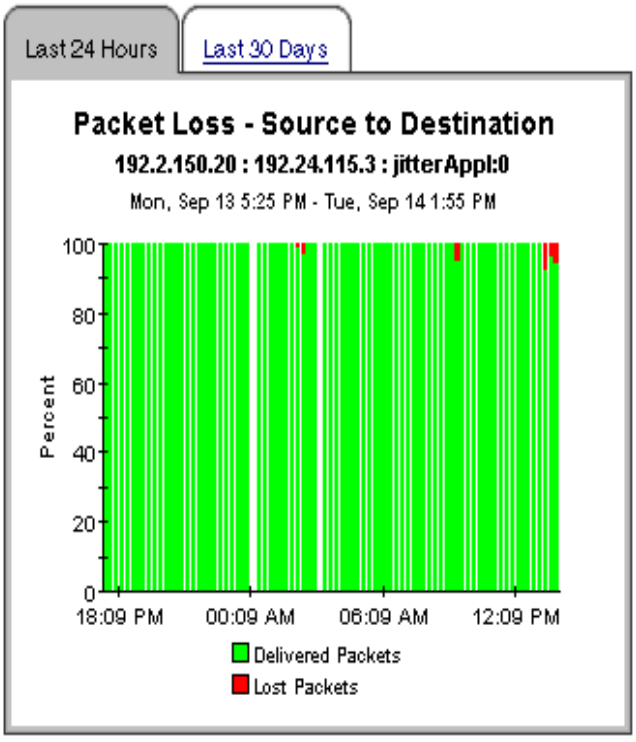


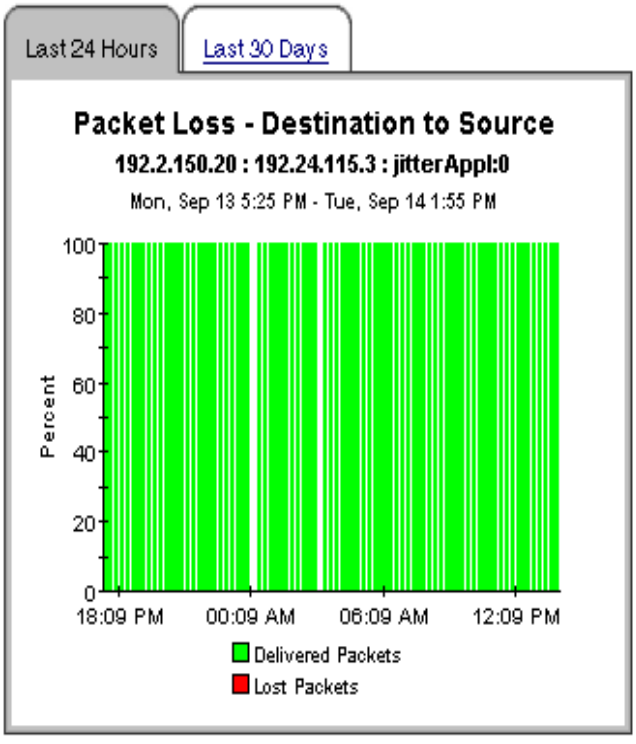
Last 24 Hours | Last 30 Days




Last 24 Hours
Last 30 Days
Response Time
192.2.150.20 : 192.24.115.3 : jitterAppl:0
Mon, Sep 13 5:25 PM - Tue, Sep 14 1:55 PM
msec
300
240
180
120
60
0
18:09 PM
00:09 AM
06:09 AM
12:09 PM
Maximum
Average
Minimum


Last 24 Hours
Last 30 Days
Packets by Error Type
192.2.150.20 : 192.24.115.3 : jitterAppl:0
Mon, Sep 13 5:25 PM - Tue, Sep 14 1:55 PM
Percent
100
80
60
40
20
0
18:09 PM
00:09 AM
06:09 AM
12:09 PM
Normal Packets
Late Arrival Packets
MIA Packets
Out of Seq. Packets


Last 24 Hours
Last 30 Days
Packet Loss - Source to Destination
192.2.150.20 : 192.24.115.3 : jitterAppl:0
Mon, Sep 13 5:25 PM - Tue, Sep 14 1:55 PM
Percent
100
80
60
40
20
0
18:09 PM
00:09 AM
06:09 AM
12:09 PM
Delivered Packets
Lost Packets


Last 24 Hours
Last 30 Days
Packet Loss - Destination to Source
192.2.150.20 : 192.24.115.3 : jitterAppl:0
Mon, Sep 13 5:25 PM - Tue, Sep 14 1:55 PM
Percent
100
80
60
40
20
0
18:09 PM
00:09 AM
06:09 AM
12:09 PM
Delivered Packets
Lost Packets

Back to Top

Service Assurance

VoIP Near Real Time - Latest Test

The VoIP Near Real Time - Latest Test Report presents the most recent MOS values for VoIP tests. The average MOS (Mean Opinion Score) data is presented for each VoIP test between source / destination pair that had activity within the last 6 hours. By selecting a VoIP test between the source / destination pair, MOS data for the last 24 hours are displayed. The corresponding Jitter statistics of VoIP test can be viewed from the Jitter Near Real Time - Latest Test Report.

Near Real Time VoIP Test Performance

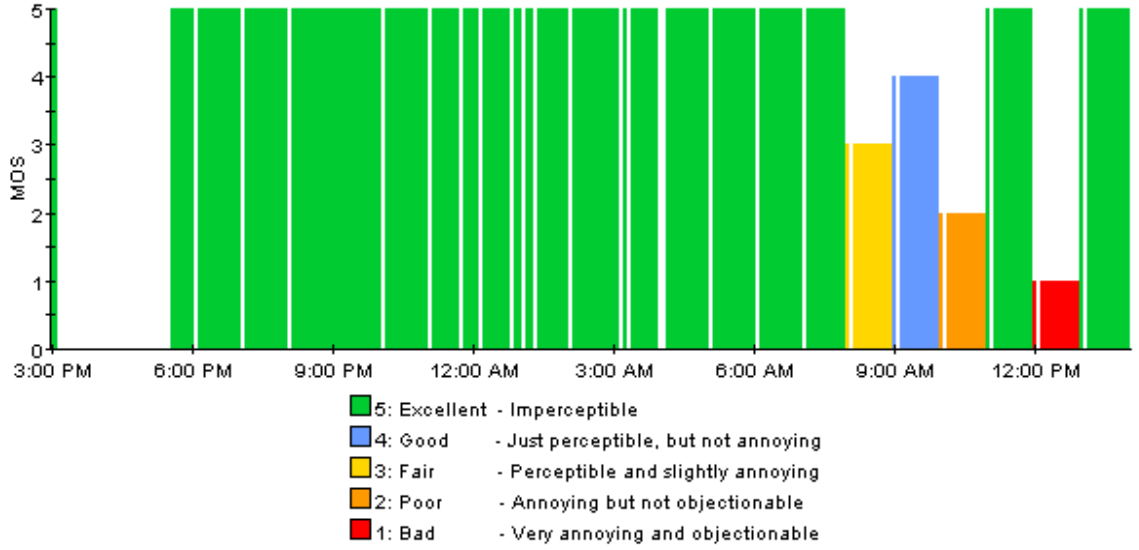
For Last Six Hours

Tue, Sep 14 2:00 PM

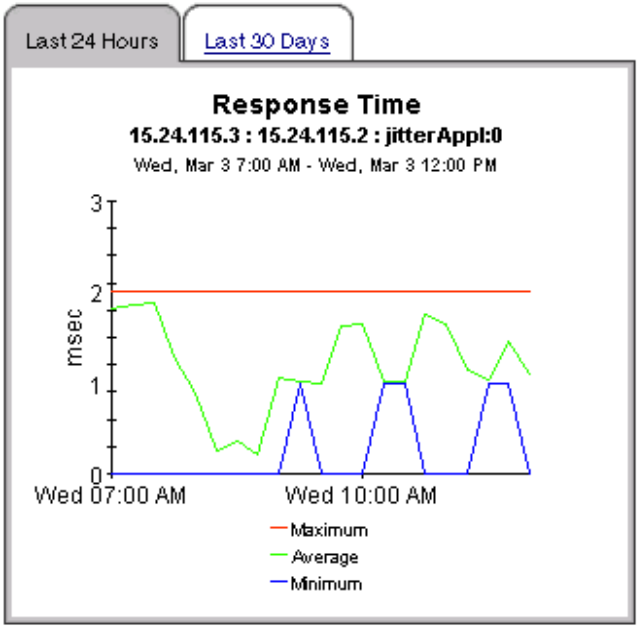
Source	Source Location	Destination	Destination Location	Tag	TOS	Codec	Avg MOS
192.2.150.20	Ft. Collins	192.2.150.1	Cupertino	VoIPG711ulaw	0	g711ulaw	3.36
192.2.150.20	Ft. Collins	192.2.150.1	Cupertino	VoIPG729a	0	g729a	4.00
192.2.150.20	Ft. Collins	192.2.150.1	Cupertino	VoIPG729a2	0	g729a	4.00
192.2.150.20	Ft. Collins	192.2.150.1	Cupertino	VoIPG711alaw	0	g711alaw	5.00
192.2.150.20	Ft. Collins	192.2.150.1	Cupertino	voiceCalcImpairm	0	g711alaw	5.00

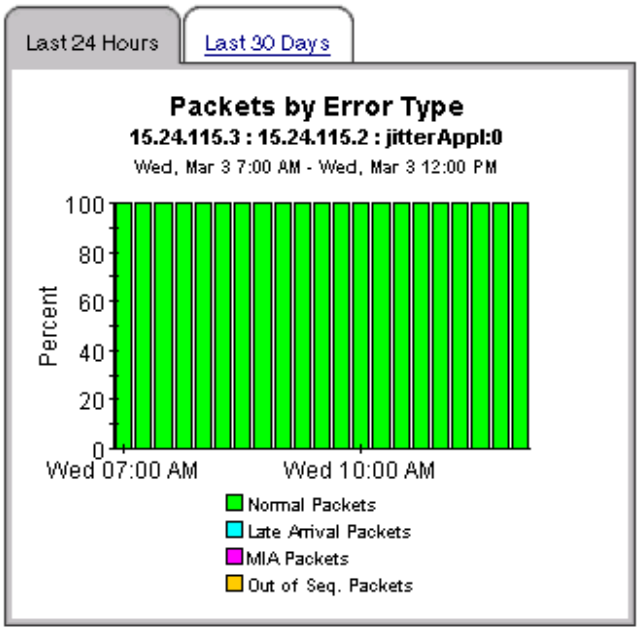
MOS Value for Selected VoIP Test

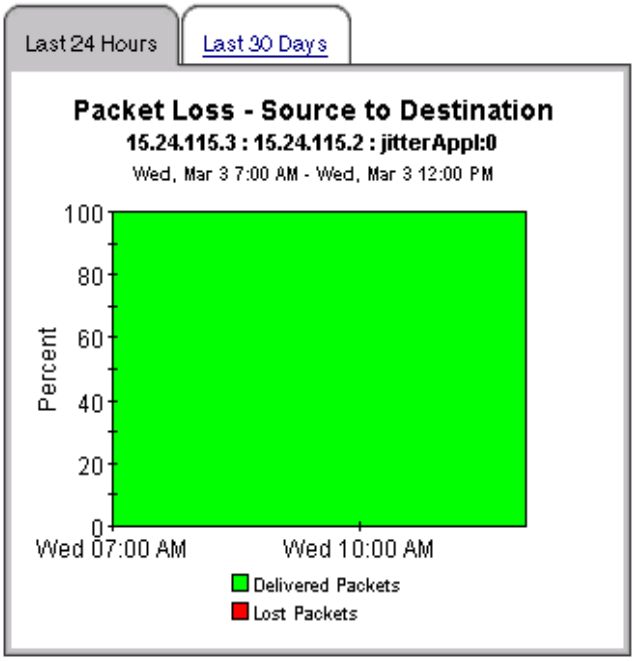
Mon, Sep 13 3:00 PM - Tue, Sep 14 2:00 PM

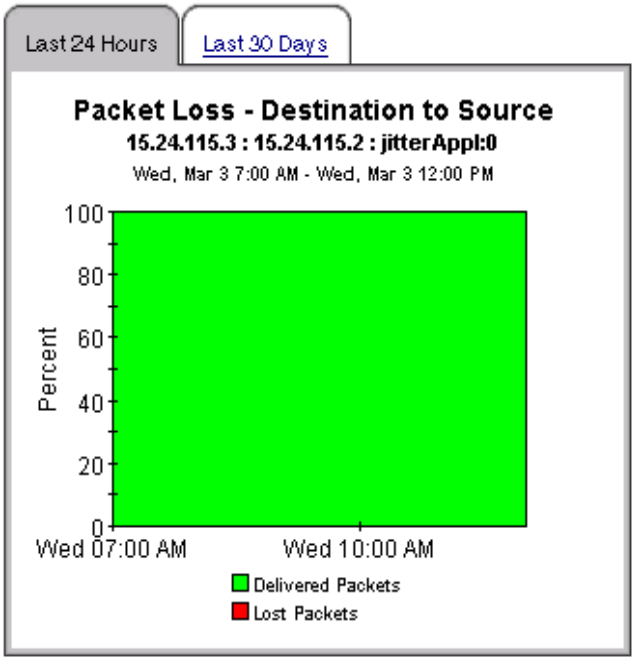


Back to Top


Last 24 Hours
Last 30 Days
Response Time
15.24.115.3 : 15.24.115.2 : jitterAppl:0
Wed, Mar 3 7:00 AM - Wed, Mar 3 12:00 PM
msec
3
2
1
0
Wed 07:00 AM
Wed 10:00 AM
Maximum
Average
Minimum


Last 24 Hours
Last 30 Days
Packets by Error Type
15.24.115.3 : 15.24.115.2 : jitterAppl:0
Wed, Mar 3 7:00 AM - Wed, Mar 3 12:00 PM
Percent
100
80
60
40
20
0
Wed 07:00 AM
Wed 10:00 AM
Normal Packets
Late Arrival Packets
MIA Packets
Out of Seq. Packets


Last 24 Hours
Last 30 Days
Packet Loss - Source to Destination
15.24.115.3 : 15.24.115.2 : jitterAppl:0
Wed, Mar 3 7:00 AM - Wed, Mar 3 12:00 PM
Percent
100
80
60
40
20
0
Wed 07:00 AM
Wed 10:00 AM
Delivered Packets
Lost Packets


Last 24 Hours
Last 30 Days
Packet Loss - Destination to Source
15.24.115.3 : 15.24.115.2 : jitterAppl:0
Wed, Mar 3 7:00 AM - Wed, Mar 3 12:00 PM
Percent
100
80
60
40
20
0
Wed 07:00 AM
Wed 10:00 AM
Delivered Packets
Lost Packets

Back to Top

11 Monitoring Jitter

When a Service Assurance Agent conducts a jitter test, it sends synthetic UDP traffic from the source device to a destination device and back again to the source device. A jitter test produces the following statistics:

- Variation in the inter-packet delay in each direction
- Number of lost packets in each direction
- Number of packet sequence errors in each direction
- Round trip time

Service Assurance contains the following jitter reports:

- Jitter Source Summary
- Jitter Destination Summary
- Jitter Source-Destination Summary

Jitter reports highlight the number of jitter tests that took place yesterday and the number of response time exceptions that were recorded for each customer. From the customer table you can drill down to investigate delay variance and response time on a device-by-device basis. If the deviation or the response time for a device looks suspicious, you can investigate further by viewing hourly and daily data graphs for response time, types of packet errors, deviation, and packet loss.

Samples of all three jitter reports follow.

Cisco Service Assurance

Jitter Destination Summary

The Jitter Destination Summary Report presents hourly and daily jitter performance metrics aggregated by the destination device. A selection list of destination devices is presented which drills down to charts of historical performance metrics aggregated over all jitter tests where the selected device is defined as the destination.

Sun Dec 08 2002

Customer	CustID	# of Transactions	# of Exceptions
All Customers	-1	576	0
HPOV	1	384	0
Trinagy	2	96	0

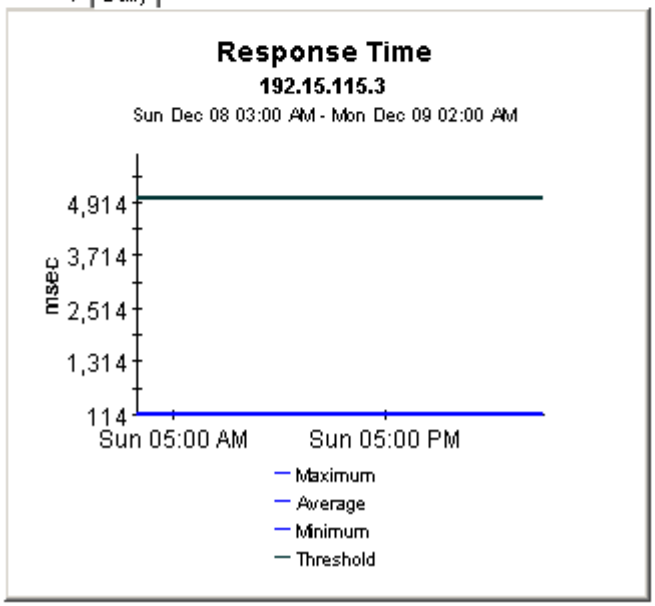
Destination Device Selection Table

S2D: Source to Destination, D2S: Destination to Source

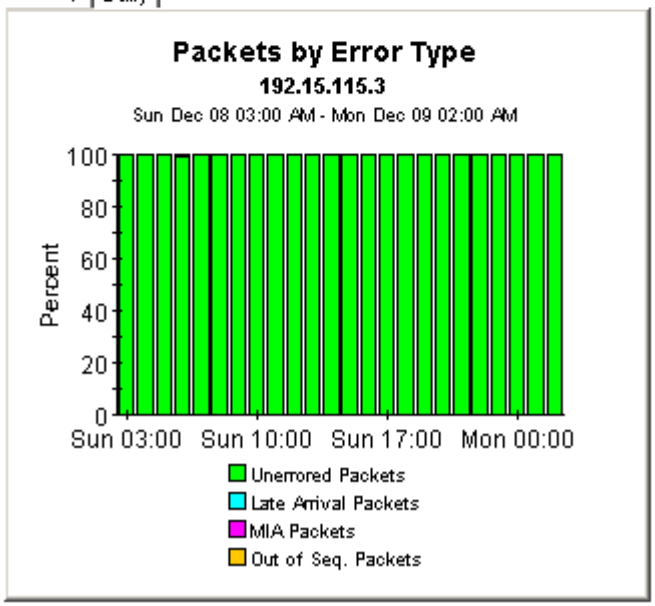
Sun Dec 08 2002

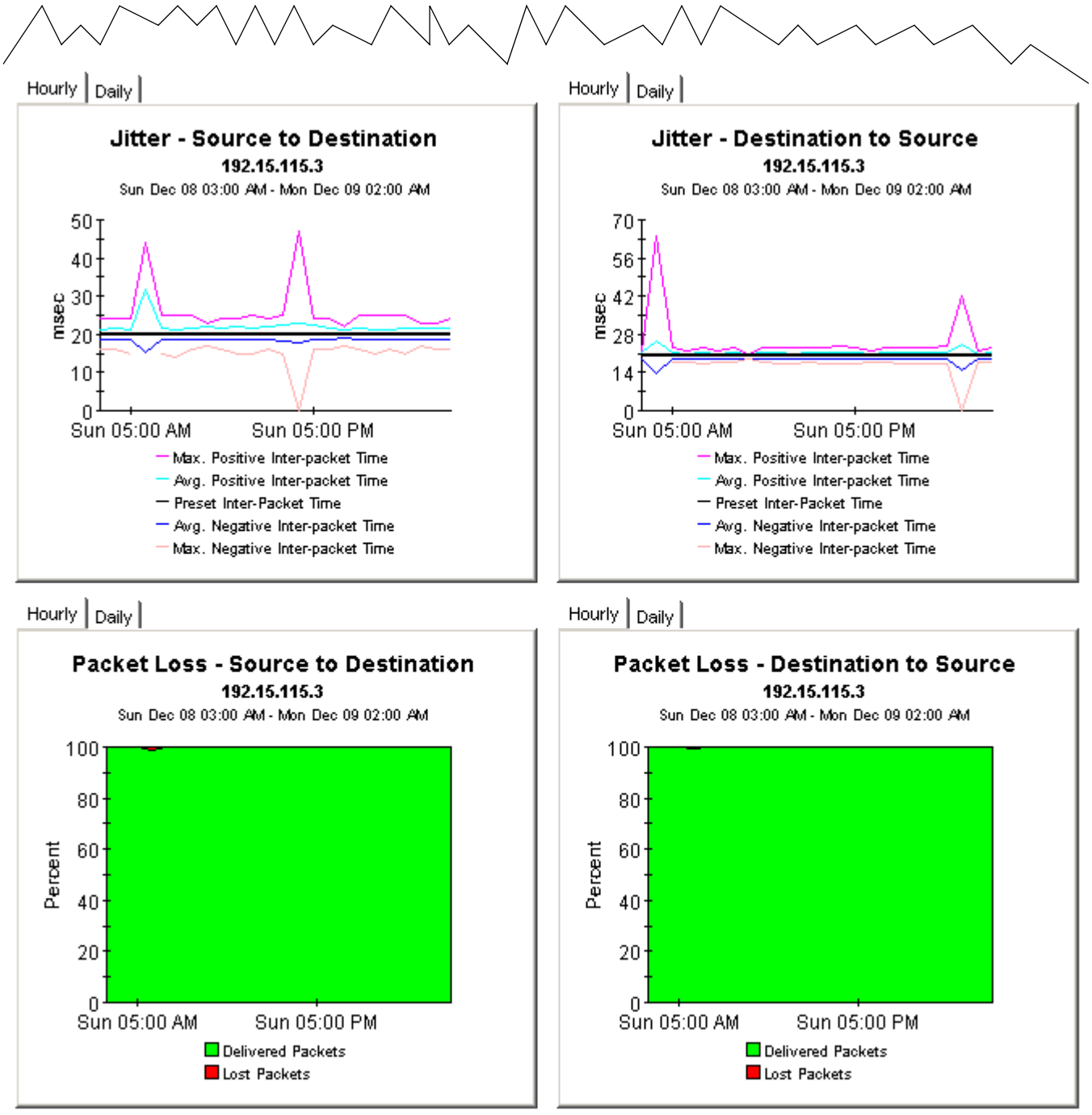
Destination	# of Transactions	Avg Response Time (msec)	S2D Avg Dev (msec)	D2S Avg Dev (msec)	S2D Max Dev (msec)	D2S Max Dev (msec)
192.15.115.3	96	119	-1 / +2	-2 / +2	-21 / +27	-21 / +44
192.15.117.63	96	94	-2 / +2	-2 / +2	-20 / +45	-23 / +33
192.15.115.2	288	79	-2 / +2	-1 / +1	-20 / +37	-16 / +42

Hourly | Daily



Hourly | Daily




Hourly
Daily
Jitter - Source to Destination
192.15.115.3
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
msec
50
40
30
20
10
0
Sun 05:00 AM
Sun 05:00 PM
Max. Positive Inter-packet Time
Avg. Positive Inter-packet Time
Preset Inter-Packet Time
Avg. Negative Inter-packet Time
Max. Negative Inter-packet Time
Hourly
Daily
Jitter - Destination to Source
192.15.115.3
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
msec
70
56
42
28
14
0
Sun 05:00 AM
Sun 05:00 PM
Max. Positive Inter-packet Time
Avg. Positive Inter-packet Time
Preset Inter-Packet Time
Avg. Negative Inter-packet Time
Max. Negative Inter-packet Time
Hourly
Daily
Packet Loss - Source to Destination
192.15.115.3
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
Percent
100
80
60
40
20
0
Sun 05:00 AM
Sun 05:00 PM
Delivered Packets
Lost Packets
Hourly
Daily
Packet Loss - Destination to Source
192.15.115.3
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
Percent
100
80
60
40
20
0
Sun 05:00 AM
Sun 05:00 PM
Delivered Packets
Lost Packets

Service Assurance

Jitter Source Summary

The Jitter Source Summary Report presents hourly and daily jitter performance metrics aggregated by the source device. A selection list of source devices is presented which drills down to charts of historical performance metrics aggregated over all jitter tests where the selected device is defined as the source.

Sun Dec 08 2002

Customer	CustID	# of Transactions	# of Exceptions
HPOV	1	384	0
Trinagy	2	96	0

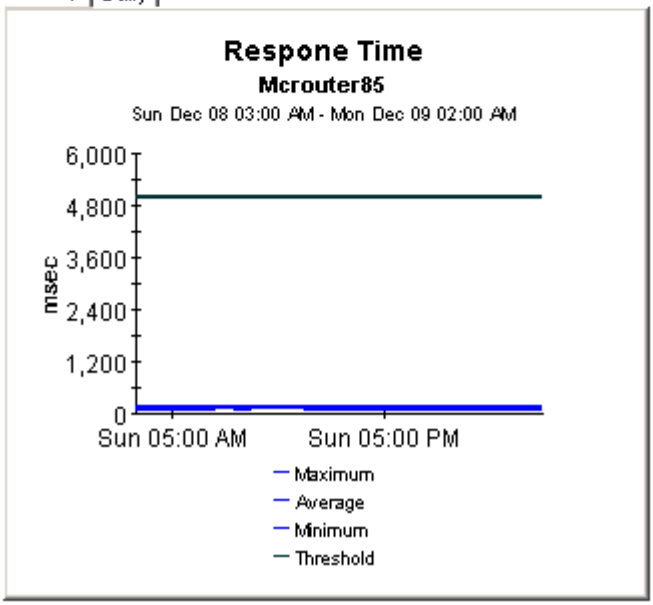
Source Device Selection Table

S2D: Source to Destination, D2S: Destination to Source

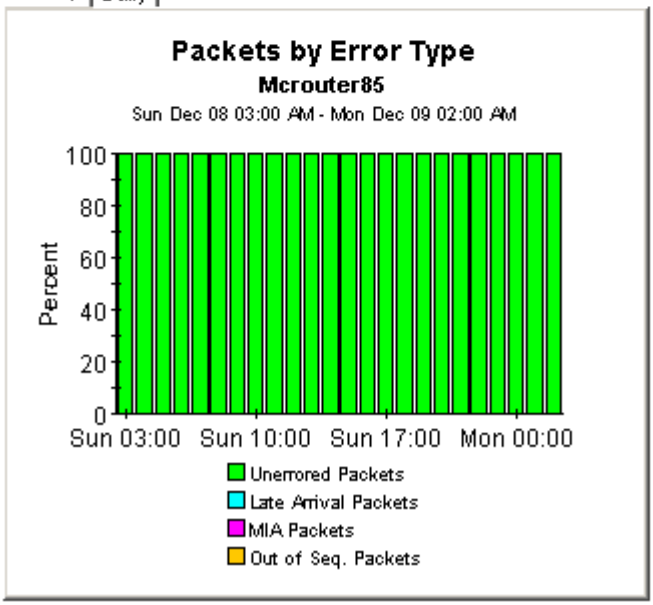
Sun Dec 08 2002

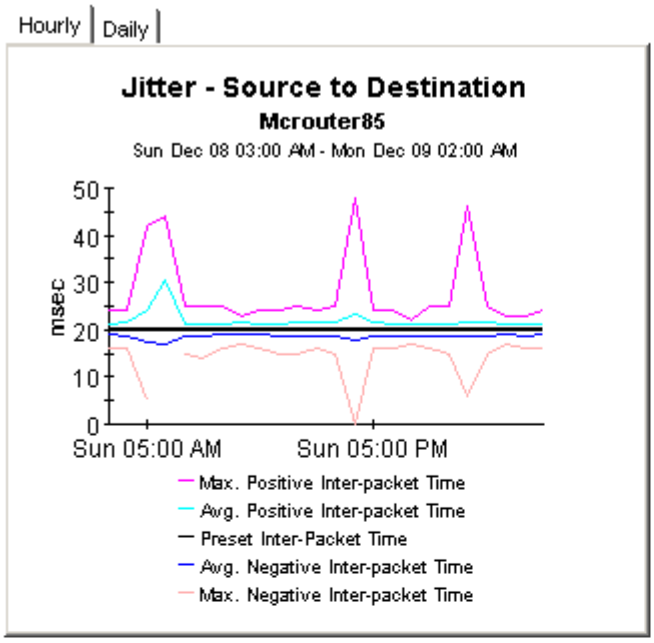
Source	# of Transactions	Avg Response Time (msec)	S2D Avg Dev (msec)	D2S Avg Dev (msec)	S2D Max Dev (msec)	D2S Max Dev (msec)
Mcrouter85	192	130	-1 / +2	-2 / +1	-21 / +28	-21 / +44
Cisco4k8	192	48	-2 / +2	-2 / +2	-20 / +45	-23 / +33

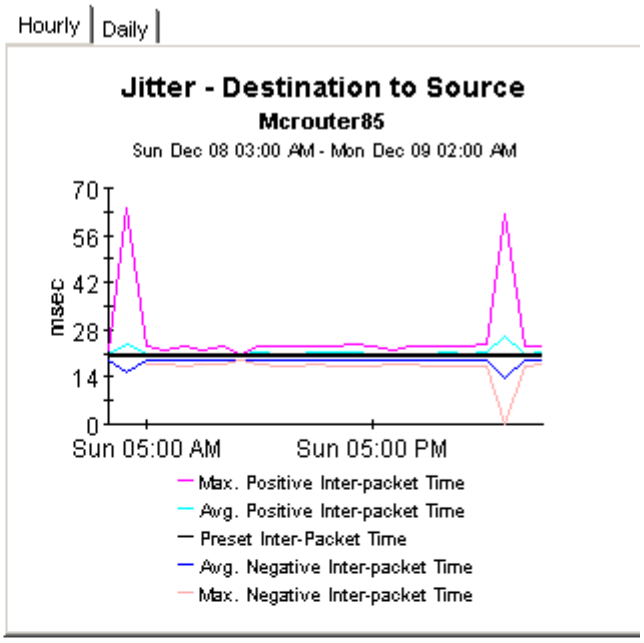
Hourly | Daily

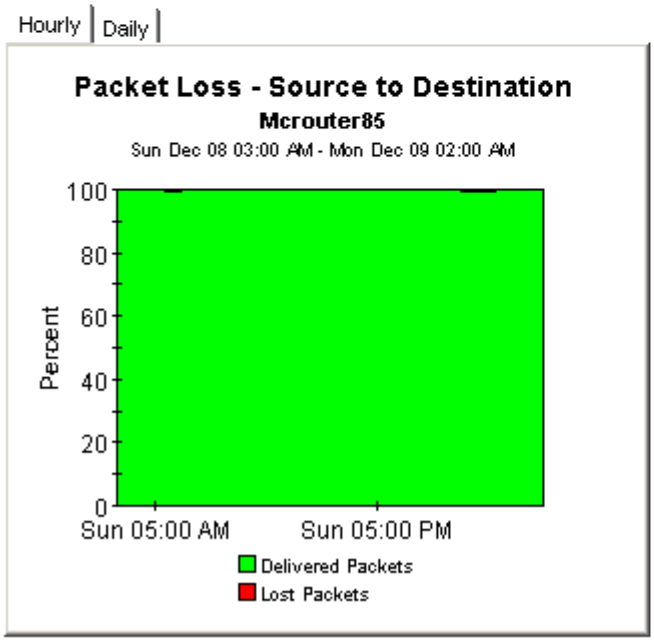


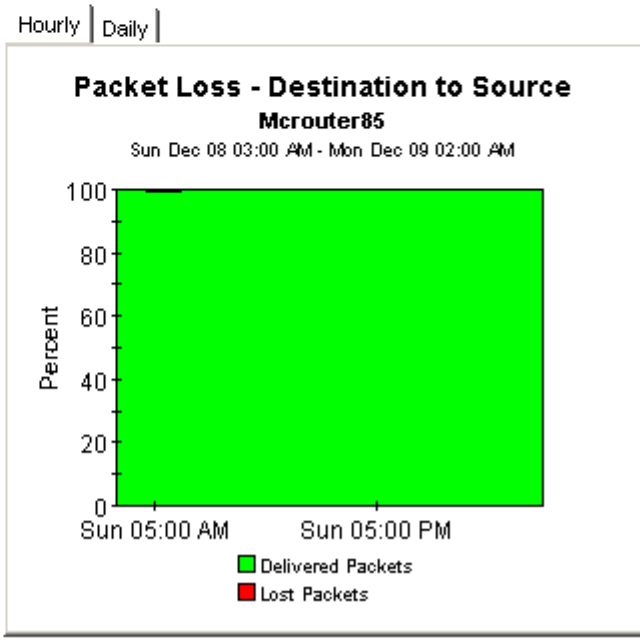
Hourly | Daily




Hourly
Daily
Jitter - Source to Destination
Mcrouter85
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
msec
50
40
30
20
10
0
Sun 05:00 AM
Sun 05:00 PM
Max. Positive Inter-packet Time
Avg. Positive Inter-packet Time
Preset Inter-Packet Time
Avg. Negative Inter-packet Time
Max. Negative Inter-packet Time


Hourly
Daily
Jitter - Destination to Source
Mcrouter85
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
msec
70
56
42
28
14
0
Sun 05:00 AM
Sun 05:00 PM
Max. Positive Inter-packet Time
Avg. Positive Inter-packet Time
Preset Inter-Packet Time
Avg. Negative Inter-packet Time
Max. Negative Inter-packet Time


Hourly
Daily
Packet Loss - Source to Destination
Mcrouter85
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
Percent
100
80
60
40
20
0
Sun 05:00 AM
Sun 05:00 PM
Delivered Packets
Lost Packets


Hourly
Daily
Packet Loss - Destination to Source
Mcrouter85
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
Percent
100
80
60
40
20
0
Sun 05:00 AM
Sun 05:00 PM
Delivered Packets
Lost Packets

Service Assurance

Jitter Source/Destination Summary

The Jitter Source/Destination Summary Report presents hourly and daily jitter performance metrics. A selection list of source devices is presented followed by the destination divices utilized by the selected source device. Both lists are sorted by number of tests. The charts below present historical performance metrics for the jitter tests performed between the selected source and destination.

Sun Dec 08 2002

Customer	CustID	# of Transactions	# of Exceptions
HPOV	1	384	0
Trinagy	2	96	0
Desktalk	3	96	0

Source Device Selection Table

S2D: Source to Destination, D2S: Destination to Source

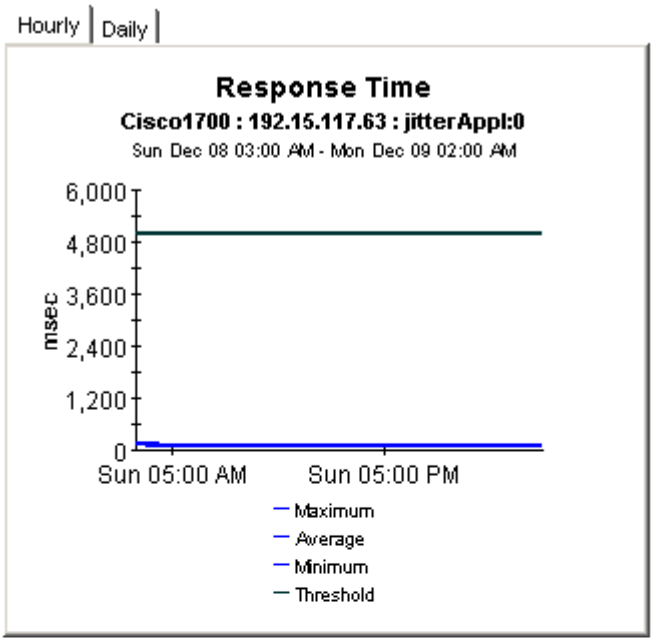
Sun Dec 08 2002

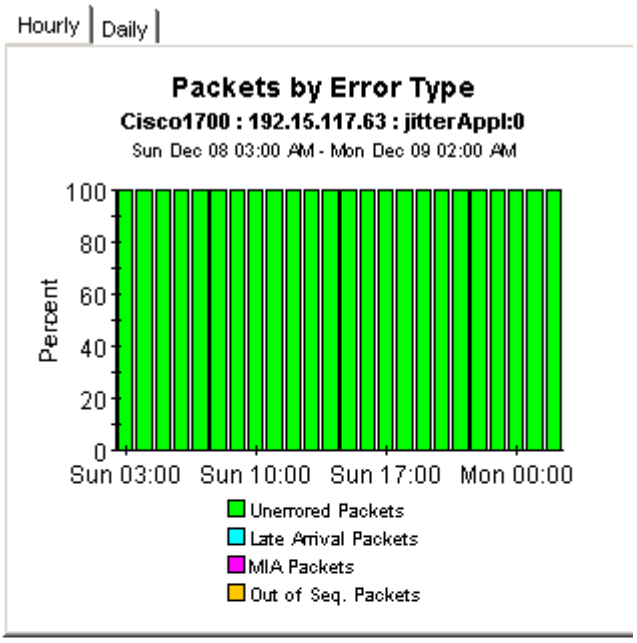
Source	# of Transactions	Avg Response Time (msec)	S2D Avg Dev (msec)	D2S Avg Dev (msec)	S2D Max Dev (msec)	D2S Max Dev (msec)
Cisco1700	96	94	-2 / +2	-3 / +3	-20 / +42	-21 / +39

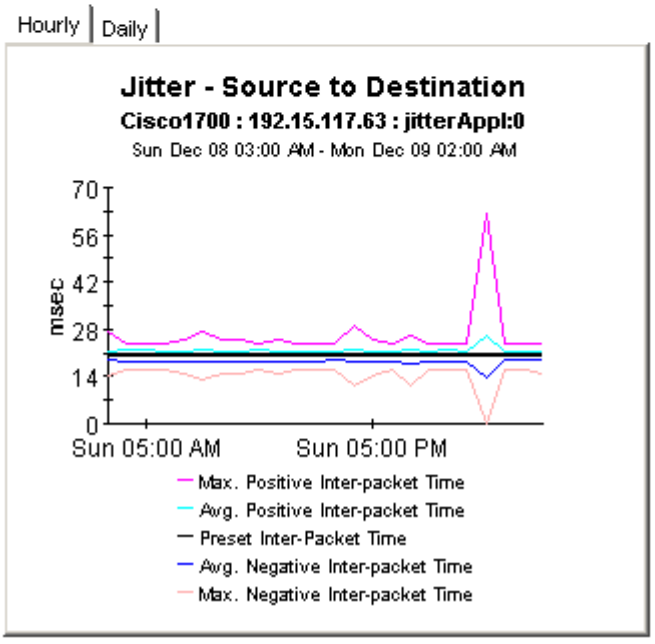
Destination Device Selection Table

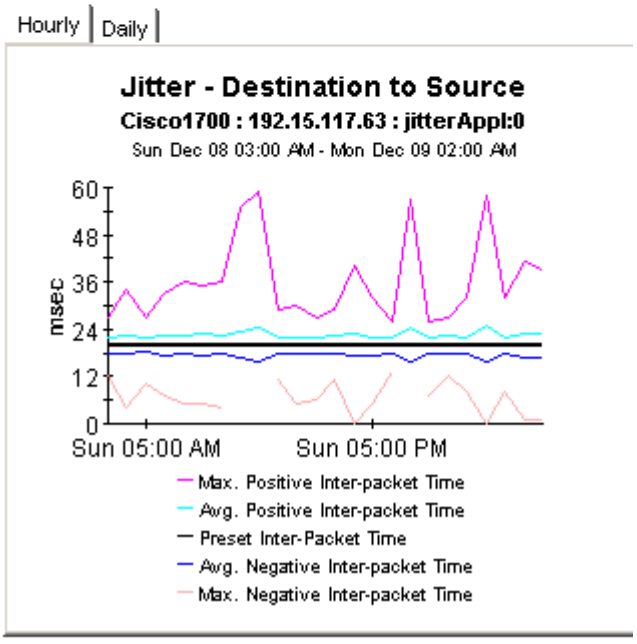
Sun Dec 08 2002

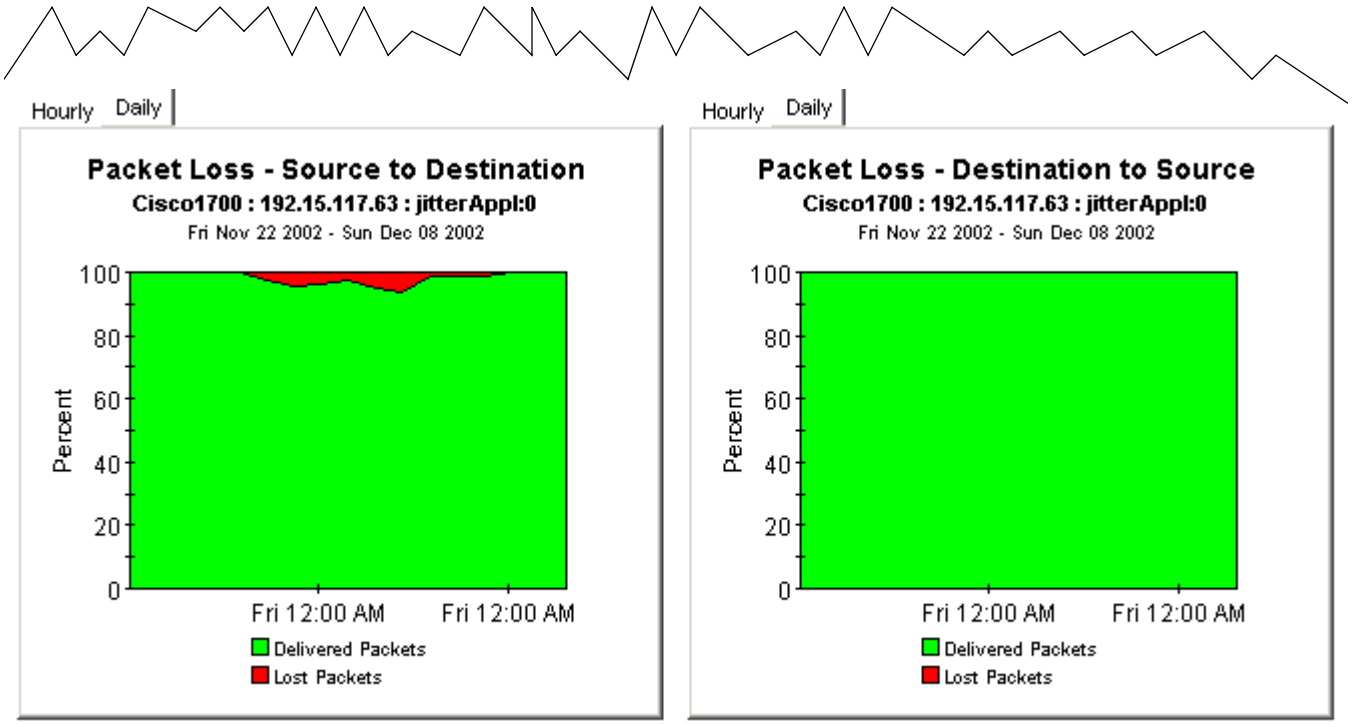
Destination	TOS	# of Transactions	Response Time (msec)	S2D Avg Dev (msec)	D2S Avg Dev (msec)	S2D Max Dev (msec)	D2S Max Dev (msec)
192.15.117.63	0	96	94.487	-2 / +2	-3 / +3	-20 / +42	-21 / +39


Hourly
Daily
Response Time
Cisco1700 : 192.15.117.63 : jitterAppl:0
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
6,000
4,800
3,600
2,400
1,200
0
msec
Sun 05:00 AM
Sun 05:00 PM
Maximum
Average
Minimum
Threshold


Hourly
Daily
Packets by Error Type
Cisco1700 : 192.15.117.63 : jitterAppl:0
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
100
80
60
40
20
0
Percent
Sun 03:00
Sun 10:00
Sun 17:00
Mon 00:00
Unerrored Packets
Late Arrival Packets
MIA Packets
Out of Seq. Packets


Hourly
Daily
Jitter - Source to Destination
Cisco1700 : 192.15.117.63 : jitterAppl:0
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
70
56
42
28
14
0
msec
Sun 05:00 AM
Sun 05:00 PM
Max. Positive Inter-packet Time
Avg. Positive Inter-packet Time
Preset Inter-Packet Time
Avg. Negative Inter-packet Time
Max. Negative Inter-packet Time


Hourly
Daily
Jitter - Destination to Source
Cisco1700 : 192.15.117.63 : jitterAppl:0
Sun Dec 08 03:00 AM - Mon Dec 09 02:00 AM
60
48
36
24
12
0
msec
Sun 05:00 AM
Sun 05:00 PM
Max. Positive Inter-packet Time
Avg. Positive Inter-packet Time
Preset Inter-Packet Time
Avg. Negative Inter-packet Time
Max. Negative Inter-packet Time


Hourly
Daily
Packet Loss - Source to Destination
Cisco1700 : 192.15.117.63 : jitterAppl:0
Fri Nov 22 2002 - Sun Dec 08 2002
100
80
60
40
20
0
Percent
Fri 12:00 AM
Fri 12:00 AM
Delivered Packets
Lost Packets
Hourly
Daily
Packet Loss - Destination to Source
Cisco1700 : 192.15.117.63 : jitterAppl:0
Fri Nov 22 2002 - Sun Dec 08 2002
100
80
60
40
20
0
Percent
Fri 12:00 AM
Fri 12:00 AM
Delivered Packets
Lost Packets

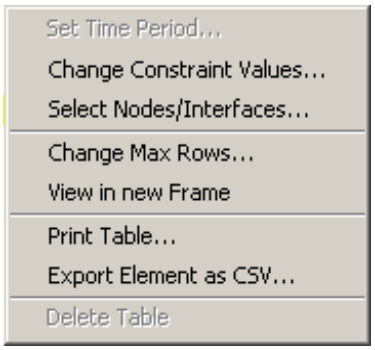
A Editing Tables and Graphs

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.

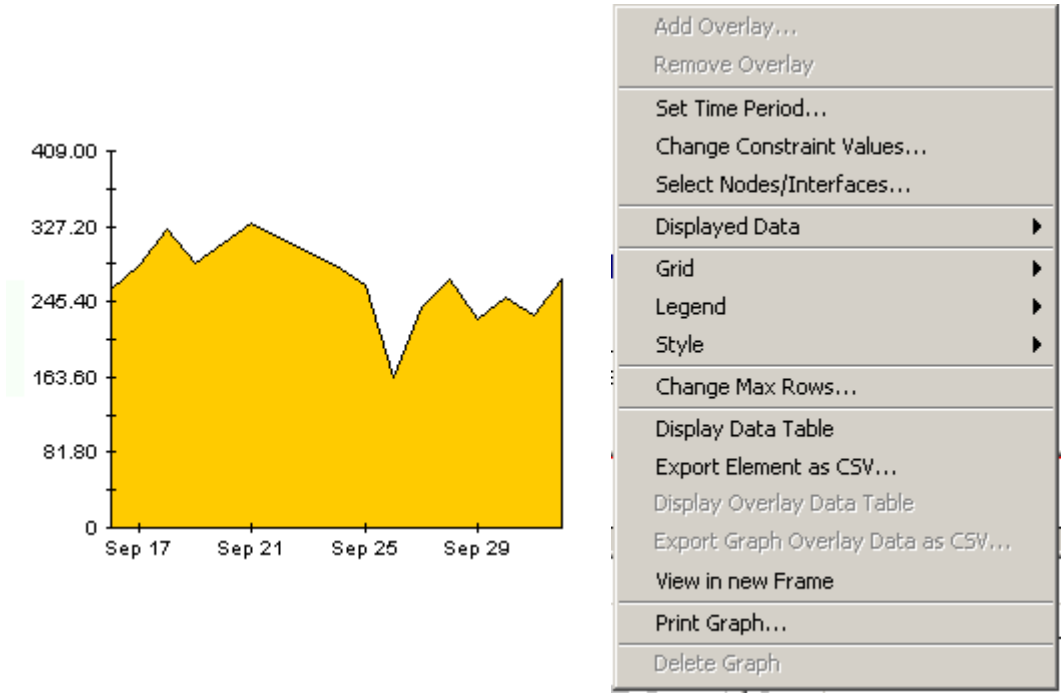
Table Viewer

Polled IP QoS Statistics Data - Input
Over Previous 6 Hours

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

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.

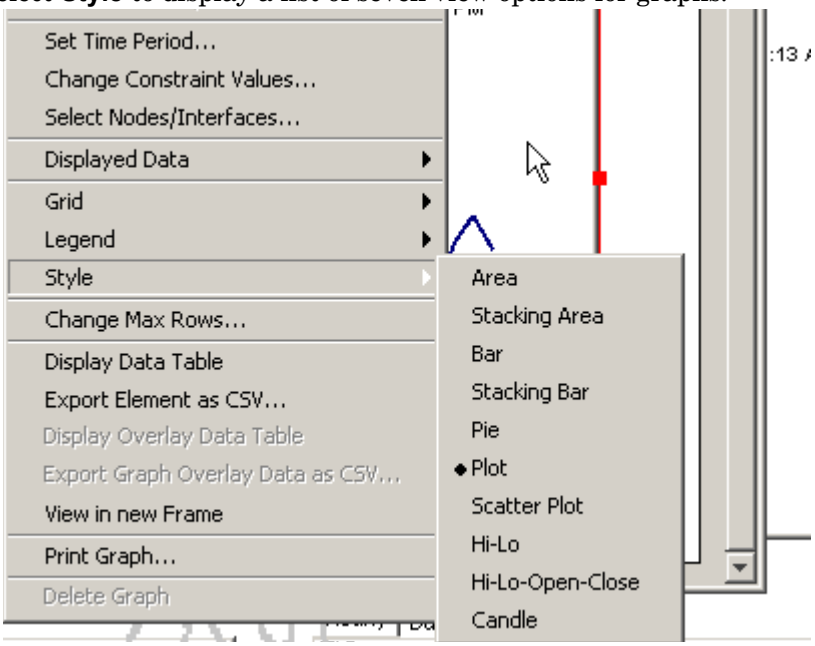


The following table provides details about each option.

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.

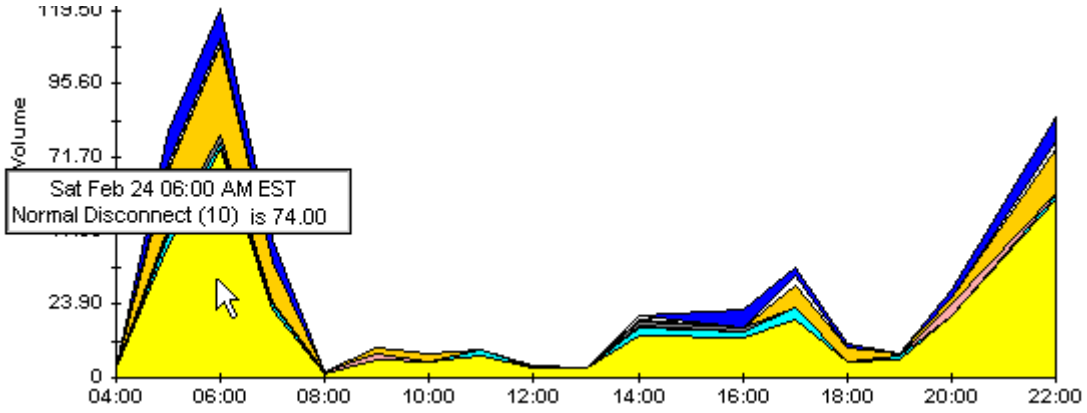
Style Options

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



Style > Area

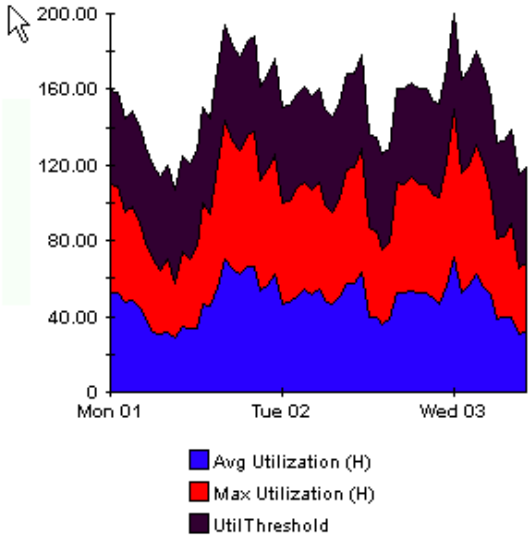
The plot or bar chart changes to an area graph. While relative values and total values are easy to view in this format, absolute values for smaller data types may be hard to see. Click anywhere within a band of color to display the exact value for that location



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.

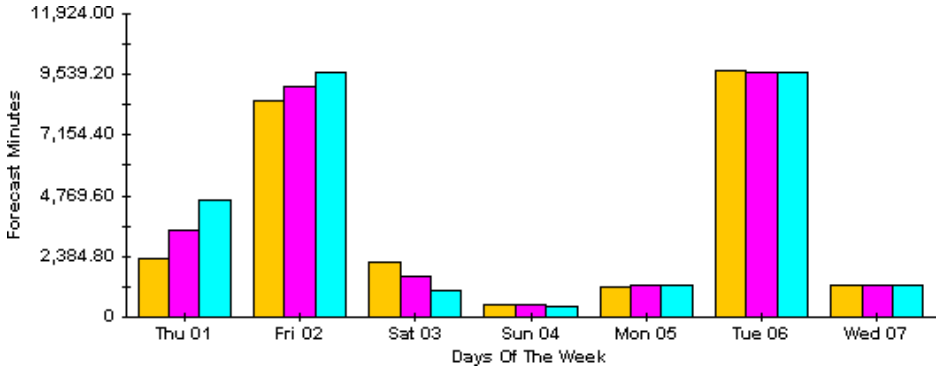
Style > Stacking Area

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



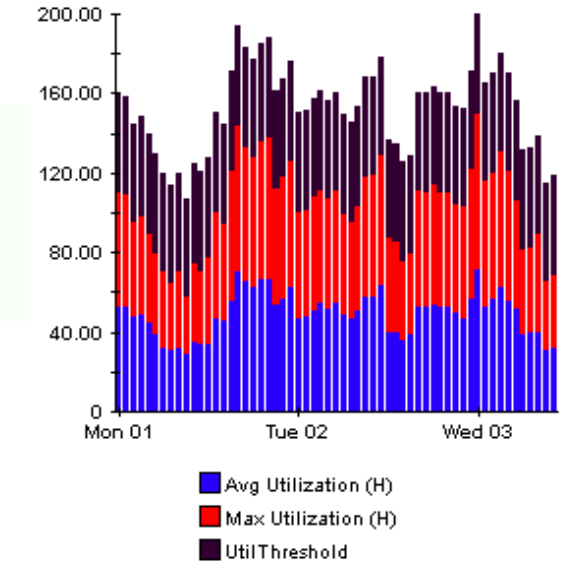
Style > Bar

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.



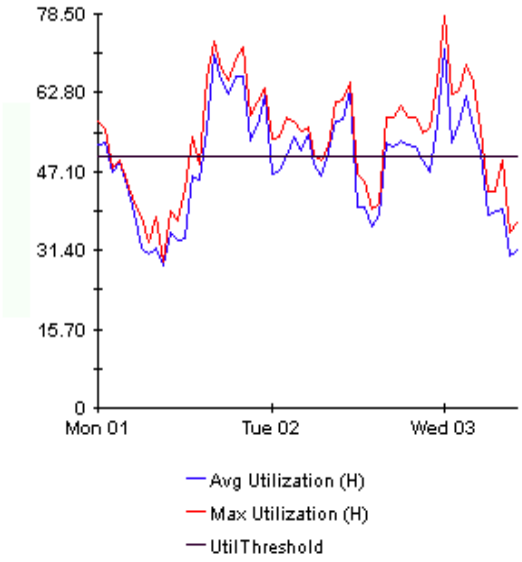
Style > Stacking Bar

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.



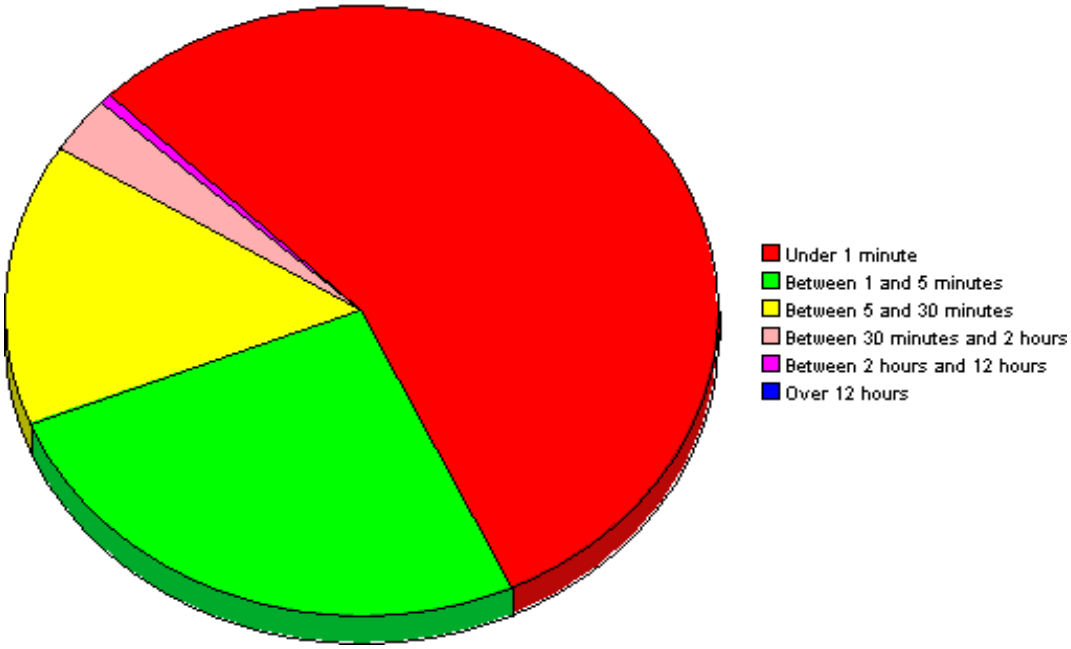
Style > Plot

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

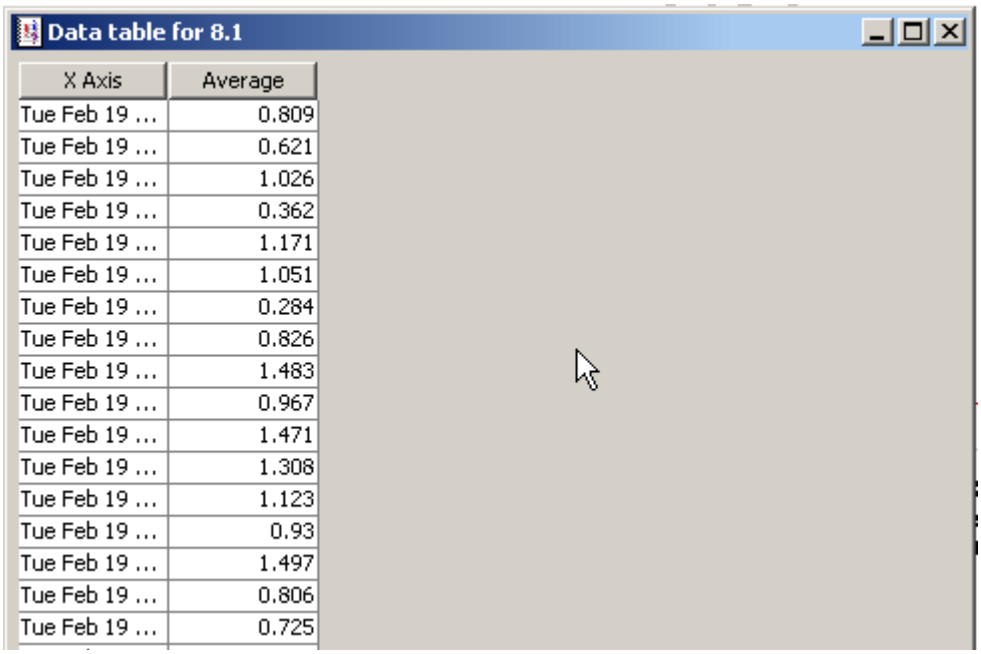
An area graph becomes a pie chart. Bands in an area graph convert to slices of a pie and the pie constitutes a 24-hour period. This view is helpful when a small number of data values are represented and you are looking at data for one day.



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

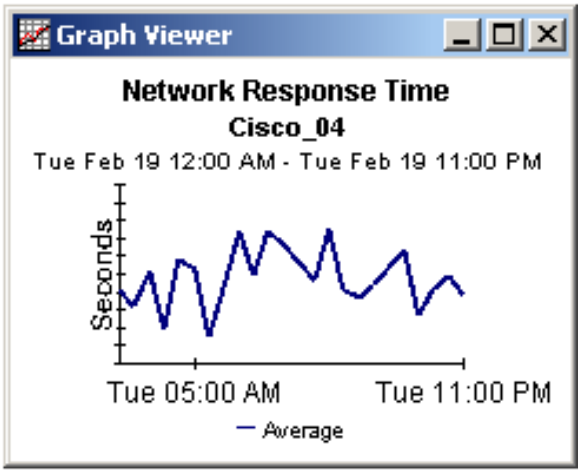
Display Data Table

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.



Index

A

alarm severity, 31

Application Exception Report, by Location/ Destination, 37

Application Exception Report, by Source/ Destination, 37

Application Forecast, 55

Application Forecast by Source/Destination, 55

Application Summary, 47

Application Top Ten, 61

C

change max rows option, 85

Cisco_SAA_Datapipe 5.6, 20

Cisco_SAA_NRT_Datapipe, 24

Cisco_SAA_NRT_Datapipe 2.1, 20

Cisco IOS Command Line Interface, 27

CiscoSAA_Config, 27

CiscoSAAConfig.pl, 27

CiscoSAAConfig.xml, 27

Cisco SAA Datapipe, 8, 24, 27

CiscoSAADelete.pl, 27

Cisco SAA NRT Datapipe, 8

Cisco VPN Solution Center, 29

collection_manager (command), 16

Common Property Tables, 15, 21

configuring SAA operations, 8

configuring source routers, 32

customer-specific reports, 12

Customer Top Ten, 61

custom views of data or property tables, 16

D

Datapipe Manager, 16

defining an SAA operation, 28

demo package, 13, 23

Destination Exception Report, by Location/ Application, 37

Destination Exception Report, by Source/ Application, 37

Destination Forecast, 55

Destination Summary, 47

Destination Top Ten, 61

device aggregations, 35

Display Data Table, 85

displayed data option, 85

distributed systems, 17, 22

E

editing parameters, 12

exception reports, 37

F

forecast reports, 55

G

grid options, 85

group_manager (command), 16

group filters, 12, 31

H

History Table (MIB), 8

J

Jitter Near Real Time - Latest Test, 67

Jitter Summary Report, 75

L

Latest Test Table (MIB), 8

legend options, 85

Location Exception Report, by Source/Destination, 37

N

Near Real Time - Latest Test, 67
Near Real Time Summary, 67
NRT reports
    Jitter NRT - Latest Test, 67
    NRT - Latest Test, 67
    NRT summary, 67

O

object categories, 25

P

polling policies, 16
Product Manuals Search (web page), 13
pulling rate data from satellite servers, 35

R

report parameters, 32

S

SAA_Application (object model), 25
SAA_Destination (object model), 25
SAA_Source (object model), 25
sample data, 67
satellite servers, 35
script syntax for CiscoSAA_Config, 28
Service_Assurance 3.1, 24
Service_Assurance_Daily.pro, 35
Service_Assurance_Hourly.pro, 35
Service_Assurance_Locations 3.1, 24
Service_Assurance_Thresholds (module), 24
Service Assurance NRT 2.0, 17
Source Exception Report, by Application/
    Destination, 37
Source Summary by Application/Destination, 47
style options for graphs, 85
summary reports, 47
system clocks, 31

T

threshold conditions, 31
top ten reports, 61
trendcopy pull commands, 35

U

UPGRADE_Service_ Assurance_Location_to_31, 19
UPGRADE_Service_Assurance_to_31, 19
Use Absolute Time, 83

V

view in new frame, 84