

HP OpenView Performance Insight

Report Pack for Service Assurance User Guide

Software Version: 3.0

Reporting and Network Solutions



April 2004

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

Legal Notices

Warranty

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

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

Restricted Rights Legend

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

Hewlett-Packard Company
United States of America

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

Copyright Notices

© Copyright 2002-2004 Hewlett-Packard Development Company, L.P., all rights reserved.

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® Corp.

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

UNIX® is a registered trademark of The Open Group.

Support

Please visit the HP OpenView web site at:

<http://openview.hp.com/>

There you will find contact information and details about the products, services, and support that HP OpenView offers. You can go directly to the HP OpenView support site at:

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

The support site provides access to:

- Product manuals
- Troubleshooting information
- Patches and updates
- Problem reporting
- Information about training
- Information about support programs

contents

- Chapter 1 Overview** 7
 - Metrics Tracked by Service Assurance 7
 - Ways to Customize Reports 12
 - Sources for Additional Information 13

- Chapter 2 The Upgrade Install** 15
 - Guidelines for a Smooth Upgrade to Version 3.0 15
 - Upgrading Version 2.0 to Version 3.0 17
 - Package Removal 20

- Chapter 3 The New Install** 21
 - Guidelines for a Smooth Installation 21
 - Installing Service Assurance 3.0 22
 - Options for Viewing Reports 25
 - Package Removal 25

- Chapter 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

- Chapter 5 Package Configuration** 31
 - Configuring Distributed Systems 31
 - Defaults in Service_Assurance_Thresholds 33
 - Using the Thresholds Form 34

- Chapter 6 Ranking Exception Counts** 37

- Chapter 7 Aggregating Performance Data** 47

- Chapter 8 Forecasting Future Performance** 55

- Chapter 9 Focusing on the Worst Performers** 61

- Chapter 10 Sample Data in Near Real Time** 67

Chapter 11 Monitoring Jitter	75
Chapter 12 Editing Tables and Graphs	83
View Options for Tables	83
View Options for Graphs	85
Glossary	91
Index	95

Overview

The following text is borrowed from a white paper prepared by 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 Service Assurance Report Pack is an “external application” that installs on HP OpenView Performance Insight (OVPI). Like other reporting solutions created for OVPI, the Service Assurance Report Pack contains templates for reports, a data model, and processing instructions for OVPI.

The raw statistics generated by SAA are stored in the CISCO-RTTMON-MIB. These statistics are polled in accordance with instructions contained in two datapipe, the Cisco SAA Datapipe and the Cisco SAA NRT Datapipe. OVPI collects data in accordance instructions from both datapipe, manipulates data in accordance with instructions from the report pack, and displays the results in report templates.

Metrics Tracked by Service Assurance

The Service Assurance Report Pack provides trending analysis for the following variables:

- 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

The trending analysis that appears in Service Assurance reports takes the following forms:

- Hourly trends for yesterday
- Daily trends for the previous 30 days
- Near Real Time (MIB History Table)
- Near Real Time (MIB Latest Test Table)
- 30 day forecasts
- 60 day forecasts
- 90 day forecasts

Hourly values are based on multiple tests, and they are calculated by the Service Assurance Agent. Daily values are calculated by OVPI. Near Real Time data is actual sample data. If you are using the Cisco SAA Datapipe only, your only NRT report is the NRT Summary report in the Source-Destination-Application folder. The Cisco SAA Datapipe reads the History Table once an hour. If you are using the Cisco SAA NRT Datapipe in addition to the Cisco SAA Datapipe, you have two additional NRT reports. The Cisco SAA NRT Datapipe reads the Latest Test Table.



You can configure how often the Cisco SAA NRT Datapipe polls the Latest Test Table. The Service Assurance Agent may conduct tests at a frequency that varies from test to test. Therefore, you want the frequency of polling to match the highest frequency of testing. The maximum rate of polling is once every 5 minutes.

Forecasts are estimates that show what performance will be 30, 60, and 90 days in the future. Although some data will appear in forecast reports a few days after you install Service Assurance, forecast reports will not be reliable until you have a complete baseline, about six weeks of data.

Version History: SA 2.0 and SA 3.0

Service Assurance 2.0 was released October 2003. Designed to run on OVPI 4.6, version 2.0 provided the following enhancements:

- Support for OVPI 4.6 Object Manager
- Addition of a form for modifying Exception Hour and Exception Day thresholds
- Support for MPLS VPN Aware testing by the SAA

The MPLS VPN Aware test was introduced in IOS 12.2.(2)T. Collecting results from this test operation required a minor change to the Cisco SAA Datapipe; the report pack itself did not change.

Service Assurance 3.0, released April 2004, includes the following enhancements:

- Support for Oracle as well as Sybase
- Minor changes to property tables
- Minor changes to existing reports
- Removal of obsolete TEEL directives
- CiscoSAA_NRT_Datapipe, a new datapipe
- Service_Assurance_NRT, a new module, containing two new reports:

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

Folders and Reports

Service Assurance 3.0 contains the following report folders:

- Application
- Customer
- Destination
- Jitter
- Location
- Source
- Source / Destination / Application
- Service Assurance NRT

Contents of the Application Folder

- 1 Application Exceptions by Source/Destination
- 2 Application Forecast
- 3 Application Forecast by Source/Destination
- 4 Application Summary
- 5 Application Top Ten

Contents of the Customer Folder

- 1 Customer Forecast
- 2 Customer Summary
- 3 Customer Top Ten

Contents of the Destination Folder

- 1 Destination Exceptions by Source / Application
- 2 Destination Forecast
- 3 Destination Forecast by Source / Application
- 4 Destination Summary
- 5 Destination Top Ten

Contents of the Jitter Folder

- 1 Jitter Destination Summary
- 2 Jitter Source/Destination Summary
- 3 Jitter Source Summary

Contents of the Location Folder

- 1 Application Exceptions by Location / Destination
- 2 Application Forecast by Location / Destination
- 3 Destination Exceptions by Location / Application
- 4 Location Summary
- 5 Location Exceptions by Application / Destination
- 6 Location Forecast
- 7 Location Forecast by Application / Destination
- 8 Location Top Ten

Contents of the Source Folder

- 1 Source Exceptions by Application / Destination
- 2 Source Forecast
- 3 Source Forecast by Application / Destination
- 4 Source Summary
- 5 Source Top Ten

Contents of the Source / Destination / Application Folder

- 1 Near Real Time Summary (collections once an hour)
- 2 Source Destination Application Summary

Contents of the Service Assurance NRT Folder

- 1 Near Real Time - Latest Test
- 2 Jitter Near Real - Latest Test

Report Types

Following is a brief description of each report type.

Exception. Shows elements that exceeded the pre-defined 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.

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 exceptions counts. Updated hourly, this report also provides hourly and daily data for response time, throughput, transactions, traffic, exceptions, and availability. The NRT reports in the optional Service Assurance NRT module contain data collected by the Cisco SAA NRT Datapipe. These reports are 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 Performance Insight is already integrated with Network Node Manager 7.01, the Service Assurance package will integrate smoothly with the fault management capabilities of Network Node Manager 7.01. There are two situations that will bring the NNM operator into contact with reports in the Service Assurance package:

Scenario 1. The Service Assurance Thresholds sub-package has sent a threshold trap to NNM. The NNM operator will see an alarm in the NMM alarms browser. The NNM operator can respond to the alarm by launching any of these reports:

- Source/Destination/Application NRT
- NRT Summary
- Jitter NRT Summary

Scenario 2. The NNM operator is not seeing alarms; however, the operator wants to investigate more closely a device that Service Assurance is monitoring. The operator will find Service Assurance reports listed among other OVPI reports in the Report Launchpad window. The NNM operator can open the Report Launchpad window from:

- NNM oww
- Home Base Dynamic Views
- NNM alarm browser

Configuring Routers for SAA Operations

The Service Assurance Agent will not operate unless it is configured. Although the command line interface for IOS provides a method for configuring SAA operations, running SAA operations, and viewing statistics, this approach to SAA configuration is awkward and slow, especially when multiple routers are involved.

The Cisco SAA Datapipe provides 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.

Ways to Customize Reports

Reports can be customized by applying group filters, by importing customers and locations, by editing parameters, and by editing tables and graphs. When you apply a group filter, you are changing how the entire package appears to a particular group of users, whereas editing tables, graphs, and parameters makes a temporary change to one report. For more information view options for tables and graphs, see Chapter 12, *Editing Tables and Graphs*.

Group Filters

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

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

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

Importing Property Data

The Cisco SAA Datapipe will populate reports with SAA tests and IP addresses or DNS names for source and destination routers. Tests, addresses, and names appear automatically. If you want to associate a customer and a location with a device, you must import this information using the property import utility that comes with the *Common Property Tables* package. For more information about this utility, including details about the format of the property import file and using forms to add new property information and update existing property information, see the *Common Property Tables 3.0 User Guide*.

Report Parameters

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

Filtering the contents of a report by editing parameters is completely optional and you may apply multiple constraints at once. Service Assurance 3.0 supports the following parameters:

- Customer Name
- Customer ID
- Source Name
- Source Location
- Destination Name

- Destination Location
- Application (SAA test type)
- ToS (Type of Service)

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

Sources for Additional Information

For information regarding the latest enhancements to Service Assurance and any known issues affecting this package, refer to the *Service Assurance Report Pack 3.0 Release Statement*. You may also be interested in the following documents:

- *Cisco SAA Datapipe 5.0 Release Statement*
- *Cisco SAA NRT Datapipe 1.0 Release Statement*
- *Common Property Tables 3.0 User Guide*
- *Thresholds Module 5.0 User Guide*
- *Performance Insight /NNM Integration Module 2.0 User Guide*
- *RNS 5.0 Release Notes, April 2004*

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

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

Select **Technical Support** > **Product Manuals** to reach the **Product Manuals Search** page. The user guides for OVPI are listed under **Performance Insight**, while the user guides for reporting solutions are listed under **Reporting and Network Solutions**.

Each title under **Reporting and Network Solutions** indicates the month and year of publication. Because updated user guides are posted to this site on a regular basis, you should check this site for updates before using on older PDF that may no longer be current.

The Upgrade Install

This chapter covers the following topics:

- Guidelines for a smooth upgrade to Version 3.0
- Using the Package Manager wizard to install upgrade packages
- Package removal

Guidelines for a Smooth Upgrade to Version 3.0

If you are running Service Assurance 2.0, you can upgrade your existing version of Service Assurance to the new version by following the procedures in this chapter. If you are installing Service Assurance for the first time, see Chapter 3, The New Install.

If you extracted packages from the RNS 4.0 CD, the technique for extracting packages from the RNS 5.0 CD will seem familiar. Just as before, extraction is automatic once you indicate which components you want to install. If you select OVPI components for installation, the install script will copy every OVPI package to the Packages directory on your system. When the extract and copy is done, the install script will prompt you to run Package Manager. Before getting to that step, become familiar with the following guidelines.

Prerequisites for the Upgrade

The following software must already be installed before upgrading from Service Assurance 2.0 to Service Assurance 3.0:

- OVPI 5.0
- Any available Service Pack for OVPI 5.0
- Service Assurance 2.0
- Cisco SAA Datapipe 4.0

You can find information about a Service Pack, including installation instructions, in the release notes for the Service Pack.

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 OVPI 5.0. Note also that you must disable trendcopy on the central server before installing packages on the central server; and you must re-enable trendcopy after the central server installation is complete. Here is an overview of how to install the upgrade on a distributed system:

- 1 Disable trendcopy on the central server.
- 2 Remove Cisco SAA Datapipe 4.0 from the central server.
- 3 Install the upgrade package for the report pack; deploy reports.
- 4 Install optional sub-packages and the following datapipes:
 - Cisco SAA Datapipe 5.0
 - Cisco SAA NRT Datapipe 1.0
- 5 For each satellite server:
 - Remove Cisco SAA Datapipe 4.0
 - Install the upgrade package for the report pack; do **not** deploy reports
 - Install the following datapipes:
 - Cisco SAA Datapipe 5.0
 - Cisco SAA NRT Datapipe 1.0
- 6 Re-enable trendcopy on the central server.

Upgrading Common Property Tables

If you are running an older version of Service Assurance on any server, you are also running an older version of Common Property Tables. You must upgrade your older version of Common Property Tables. Do this by installing the version 2.2 to 3.0 upgrade package.

Installing this particular upgrade package is no different from installing any upgrade package. However, do not try to install this upgrade *and* other packages at the same time. Install the upgrade package for Common Property Tables and nothing but the upgrade package for Common Property Tables.

Upgrading the Datapipe

Your Cisco SAA Datapipe cannot be upgraded. Since there is no upgrade package for the previous release of the Cisco SAA Datapipe, you need to uninstall the previous version of the datapipe. It does not matter when you do this. Just be sure the previous version of the datapipe has been removed before you attempt to install the new version.

Integration with NNM: Threshold Alarms

If OVPI is integrated with NNM, you will probably want to install the optional thresholds sub-package, `Service_Assurance_Thresholds`. The optional thresholds sub-package contains default thresholds. For more information about default thresholds, see Chapter 5, *Package Configuration*.

The thresholds sub-package cannot operate unless the Threshold and Event Generation Module, also known as the Thresholds Module, is installed. You are probably running version 4.0 of the Thresholds Module. For a description of recent enhancements to this package, refer to the *Thresholds Module 5.0 User Guide*.

Upgrading Version 2.0 to Version 3.0

Perform the following tasks to upgrade Service Assurance 2.0 to Service Assurance 3.0:

- Task 1: Extract packages from the RNS 5.0 product CD
- Task 2: Upgrade to the latest release of Common Property Tables
- Task 3: Uninstall the old datapipe, Cisco SAA Datapipe 4.0
- Task 4: Install the upgrade package for the report pack
- Task 5: Install these packages:
 - Upgrade package for the locations sub-package
 - Cisco SAA Datapipe 5.0
 - Cisco SAA NRT Datapipe 1.0
 - Latest release of the thresholds sub-package (optional)

Task 1: Extract packages from the RNS 5.0 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 RNS 5.0 CD. On Windows, a Main Menu displays 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_Locations.ap
- Service_Assurance_Thresholds.ap
- UPGRADE_Service_Assurance_2_to_3.ap
- UPGRADE_Service_Assurance_Locations_2_to_3.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 3.0

Service Assurance 2.0 required Common Property Tables 2.2. If you have not already upgraded to Common Property Tables 3.0, do this now, *before* moving on to Task 3. If you need help with the upgrade, refer to the *Common Property Tables 3.0 User Guide*.

Task 3: Uninstall the Cisco SAA Datapipe 4.0

- 1 Select **HP OpenView > Performance Insight > Package Manager**. The Package Manager welcome window opens.
- 2 Click **Next**. The Package Location window opens.
- 3 Select the **Uninstall** radio button.
- 4 Click **Next**. The Report Undeployment window opens. Keep the defaults.
- 5 Click the check box next to the following package:
Cisco_SAA_Datapipe 4.0
- 6 Click **Next**. The Selection Summary window opens.
- 7 Click **Uninstall**. The Progress window opens. When the removal finishes, a removal complete message appears.
- 8 Click **Done** to return to the Management Console.

Task 4: Install the Service Assurance 2.0 to 3.0 Upgrade Package

- 1 Select **Tools > Package Manager**. The Package Manager welcome window opens.
- 2 Click **Next**. The Package Location window opens.
- 3 Click the **Install** radio button.
- 4 Approve the default installation directory or select a different directory if necessary.
- 5 Click **Next**. The Report Deployment window opens.
- 6 Accept the default for Deploy Reports; also accept the defaults for application server name and port.
- 7 Type your user name and password for the OVPI Application Server.
- 8 Click **Next**. The Package Selection window opens.
- 9 Click the check box next to the following package:

UPGRADE_Service_Assurance_2_to_3

- 10 Click **Next**. The Type Discovery window opens. Disable the default and click **Next**. The Selection Summary window opens.
- 11 Click **Install**. The Installation Progress window opens and the install begins. When installation finishes, an install complete message appears.
- 12 Click **Done** to return to the Management Console.



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 3.0*. This is not an error.

Task 5: Install the Locations Sub-Package, the Thresholds Sub-Package, and the New Datapipes

- 1 Select **Tools > Package Manager**. The Package Manager welcome window opens.
- 2 Click **Next**. The Package Location window opens.
- 3 Click the **Install** radio button.
- 4 Approve the default installation directory or select a different directory if necessary.
- 5 Click **Next**. The Report Deployment window opens.
- 6 Accept the default for Deploy Reports; also accept the defaults for application server name and port.
- 7 Type your user name and password for the OVPI Application Server.
- 8 Click **Next**. The Package Selection window opens.
- 9 Click the check box next to the following packages:
 - Service_Assurance_Thresholds*
 - UPGRADE_Service_Assurance_Locations_2_to_3*
 - Cisco_SAA_Datapipe 5.0*
 - Cisco_SAA_NRT_Datapipe 1.0*
- 10 Click **Next**. The Type Discovery window opens. Disable the default and click **Next**. The Selection Summary window opens.
- 11 Click **Install**. The Install Progress window opens. When installation finishes, an install complete message appears.
- 12 Click **Done** to return to the Management Console.
- 13 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`

Package Removal

If you remove a report pack, the associated tables and all the data in those tables will be deleted. If you want to preserve the data in those tables, archive the data before removing the package.

Follow these steps to uninstall Service Assurance and the datapipes associates with Service Assurance.

- 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 Start **Package Manager**. The Package Manager welcome window opens.
- 4 Click **Next**. The Package Location window opens.
- 5 Select the **Uninstall** radio button.
- 6 Click **Next**. The Report Undeployment window opens. Keep the defaults.
- 7 Click **Next**. The Package Selection window opens. Click the check box next to the following packages:
 - Service_Assurance*
 - Service_Assurance_Locations* (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 Selection Summary window opens.
- 9 Click **Uninstall**. The Progress window opens. When removal completes, 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`

The New Install

This chapter covers the following topics:

- Guidelines for a smooth installation of Service Assurance 3.0
- Using the Package Manager wizard to install the report pack and the datapipe
- Options for viewing reports
- Package removal

Guidelines for a Smooth Installation

The RNS 5.0 CD contains components for NNM and OVPI. When you select OVPI report packs for installation, the install script on the CD automatically extracts every OVPI package from the CD and copies them to the Packages directory on your system. When the extract finishes, the install script will prompt you to run Package Manager. Before getting to that step, review the following guidelines.

Prerequisites for a New Installation

The following software must be installed before installing Service Assurance 3.0:

- OVPI 5.0
- Any available OVPI 5.0 Service Pack

You will find information about each Service Pack, including installation instructions, in the release notes for the Service Pack.

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 OVPI 5.0. Deploy reports once, from the central server only. When you install the report pack on a satellite server, do not deploy reports. Here is an overview of the entire procedure:

- 1 Disable trendcopy on the central server.
- 2 Install the following packages on the central server:

- Service Assurance 3.0; deploy reports.
 - Optional sub-packages
 - Cisco SAA Datapipe 5.0
 - Cisco SAA NRT Datapipe 1.0
- 3 Install the following packages on each satellite server:
- Service Assurance 3.0; do **not** deploy reports
 - Optional sub-packages
 - Cisco SAA Datapipe 5.0
 - Cisco SAA NRT Datapipe 1.0
- 4 Re-enable trendcopy on the central server.

Upgrading Common Property Tables

If you are running an older version of Common Property Tables, you must upgrade your older version of Common Property Tables. Installing this particular upgrade package is no different from installing other upgrade package, however, keep in mind that you cannot install the upgrade for Common Property Tables *and* other packages at the same time. Finish the upgrade for Common Property Tables first, then run the install wizard a second time to install the other packages.

Integration with NNM: Threshold Alarms

If you have already integrated OVPI with NNM, 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 (also known as the Thresholds Module). If you select the thresholds sub-package for installation, the install wizard will install the Thresholds Module for you, automatically.

If you are running the previous version of the Thresholds Module, you must upgrade to the current version. For more information about the latest enhancements to the Thresholds Module, refer to the *Thresholds Module 5.0 User Guide*.

Installing Service Assurance 3.0

Perform the following tasks to install Service Assurance 3.0:

- Task 1: Extract packages from the distribution CD
- Task 2: If necessary, upgrade to Common Property Tables 3.0
- Task 3: Install the following packages:
 - `Service_Assurance 3.0`
 - `Cisco_SAA_Datapipe 5.0`

— Cisco_SAA_NRT_Datapipe 1.0

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

Task 1: Extract Packages from the RNS 5.0 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 RNS 5.0 CD. 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 have the option of navigating to the Packages directory to see the results. The Packages directory contains separate folders for Service Assurance and the Cisco SAA Datapipe. The following folders appear under Service Assurance:

- Service_Assurance.ap
- Service_Assurance_Demo.ap
- Service_Assurance_Locations.ap
- Service_Assurance_Thresholds.ap
- UPGRADE_Service_Assurance_2_to_3.ap
- UPGRADE_Service_Assurance_Locations_2_to_3.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

Installing the demo package is optional. You may install the demo package by itself, with no other packages, or you may install the demo package along with everything else. Reports in the demo package are interactive, rows in tables are linked to graphs, and you may experiment with view options for individual tables and graphs.

Task 2: Upgrade to Common Property Tables 3.0

Service Assurance 3.0 requires Common Property Tables 3.0. If you have not already upgraded to Common Property Tables 3.0, do this now, *before* moving on to Task 3. (If you need help with the upgrade, refer to the *Common Property Tables 3.0 User Guide*.) When the install of the upgrade package finishes, a package install complete message appears. Click **Done** to return to the Management Console.

Task 3: Install Service Assurance 3.0, the datapipes, and optional sub-packages

- 1 Select **Tools > 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.
- 5 Accept the default for Deploy Reports; also accept the defaults for application server name and port.
- 6 Type your user name and password for the OVPI Application Server.
- 7 Click **Next**. The Package Selection window opens. Click the check box next to the following packages:

Service_Assurance

Service_Assurance_Locations

Service_Assurance_Thresholds

Cisco_SAA_Datapipe

Cisco_SAA_NRT_Datapipe



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

If your system is distributed, the datapipes belong on any server that polls; typically, the central server in a distributed system does not poll.

- 8 Click **Next**. The Type Discovery window opens. Keep the default and click **Next**. The Selection Summary window opens.
- 9 Click **Install**. The Install Progress window opens and the installation begins. When the installation finishes, an install 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`

Options for Viewing Reports

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

The method of report viewing available to you depends on how OVPI was installed. If the client component is installed on your system, you have access to the Report Viewer, Report Builder, and the Management Console. If the client component was not installed on your system, use the Web Access Server to view reports.

For more information about the client components, refer to the *Performance Insight Installation Guide*. For more information about Object Manager and viewing reports specific to a selected object, refer to the *Performance Insight Administration Guide*. For more information about deploying, viewing, and undeploying reports, refer to the *Performance Insight Guide to Building and Viewing Reports*.

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 Select **HP OpenView > Performance Insight > 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_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`

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

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 need to 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>

Package Configuration

This chapter covers the following topics:

- Setting up a distributed system across multiple servers
- Default thresholds in the Service_Assurance_Thresholds sub-package
- Using the Modify SAA Thresholds form to change default values

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.

Configuring Distributed Systems

If you intend to run the Service Assurance package in a distributed system, you need to configure every server in the system. Before doing that, let's verify that you have the right packages on the central server and the right packages on each satellite server. The following table makes clear the difference.

Central Server	Satellite Server
Service Assurance	Service Assurance
Thresholds Module	Cisco SAA Datapipe
Common Property Tables	Common Property Tables
Optional sub-packages	

Typically, the central server does not poll. If you want the central server in your system to poll, then you should install the Cisco SAA Datapipe on every server, the central server as well as each satellite server.

Configuring the Central Server

This task involves the following steps:

- Task 1: Set up connections with satellite server databases

- Task 2: Disable hourly processing on the central server
- 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 3.0, 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** when you are done.

Task 2: Disable hourly processing on the central server

- 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 need to 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.

- 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.



Pulling rate data from satellite servers increases traffic between satellite servers and the central server and increases the processing load on the central server.

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. To make sure the satellite server completes hourly summarizations before the central server begins hourly summarizations, change the start time from `1:00+40` to `1:00+25`.
- 3 Configure polling policies for the Cisco SAA Datapipe, making sure that each SAA router is polled by only one satellite server.

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 text failed.	Critical



If you are interested in knowing more about options for configuring the Thresholds Module, such as enabling multiple types of traps, or setting up multiple trap destinations, refer to the *Thresholds Module 5.0 User Guide*.

Using the Thresholds Form

Service Assurance 3.0 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 **Tasks Specific to the Selected Objects**.

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

Service Assurance
Modify SAA Thresholds

This form allows you to modify SAA thresholds for the Service_Assurance_Thresholds module. Enter the new threshold values. Click the OK button to save the values and close the window. Click the Apply button to update the values in the database and leave the window open for further modifications. Click the Cancel button to cancel.

SAA Test Selection
 Hold Ctrl or Shift key to select multiple rows

Source	Destination	Application	HourlyThreshold	DailyThreshold
default	default	ALL	75.00	50.00
Cisco460	192.15.90.2	dswApp10	75.00	50.00
Cisco460	192.15.115.2	ipVdpEchoApp1-1	75.00	50.00
Cisco460	192.15.115.22	ipVdpEcho5	75.00	50.00
Cisco460	192.15.115.22	ipTopConn2.00	75.00	50.00
Cisco460	192.15.115.22	ipVdpEchoApp1-1	75.00	50.00
Cisco460	192.15.120.31	dswApp10	75.00	50.00
Cisco460	192.15.120.51	dswApp10	75.00	50.00
Cisco460	ultraFEADME14	ipApp10	75.00	50.00
Cisco1700	192.15.115.22	ipVdpEcho0	75.00	50.00

New HourlyExceptionThreshold If Hourly ExceptionRate is greater than this threshold, send a trap to NNM.

New DailyExceptionThreshold If Daily ExceptionRate is greater than this threshold, send a trap to NNM.

OK Apply Cancel

- 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.

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.

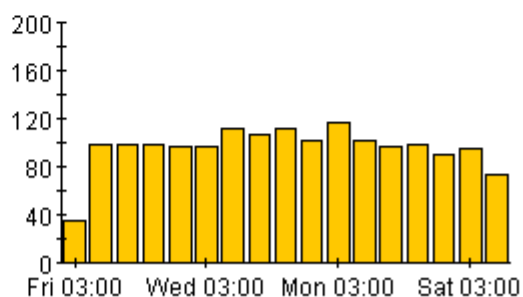
Sun Dec 08 2002

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

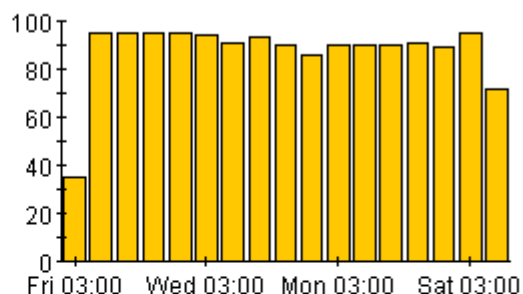
Sun Dec 08 2002

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

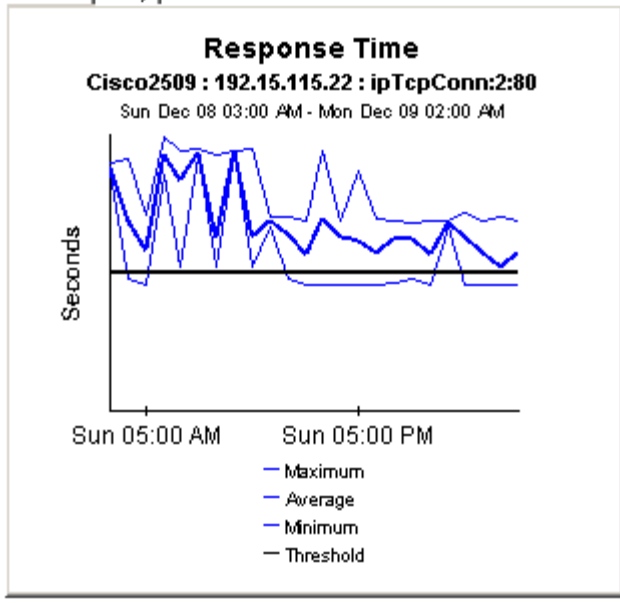
Sun Dec 08 2002

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

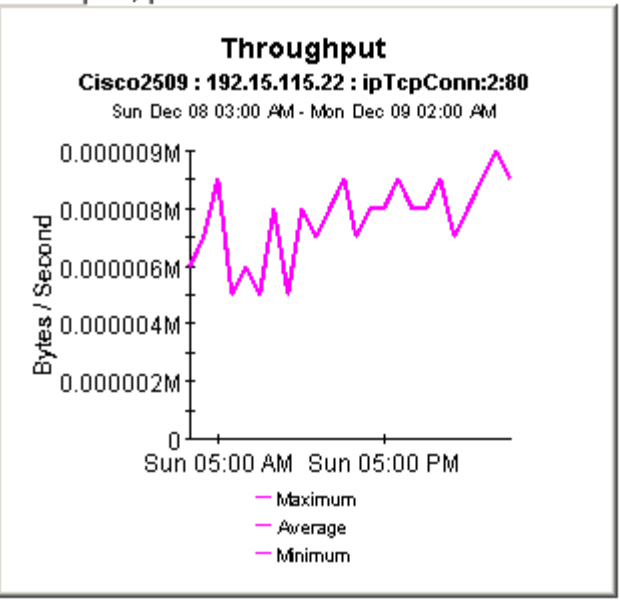




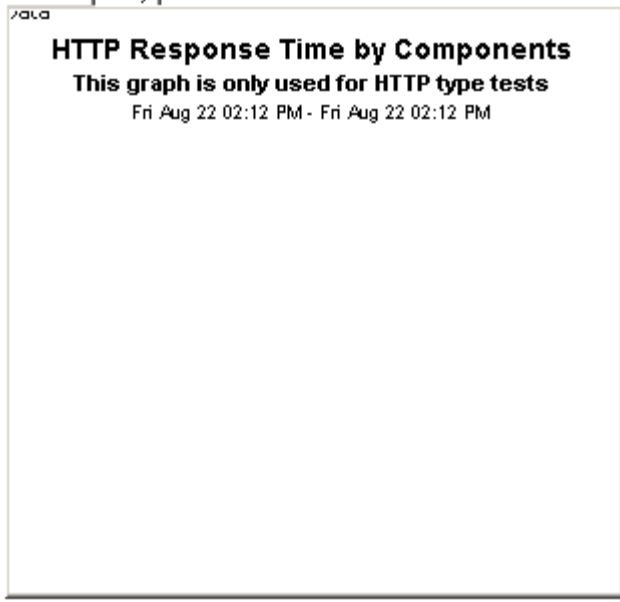
Hourly | Daily



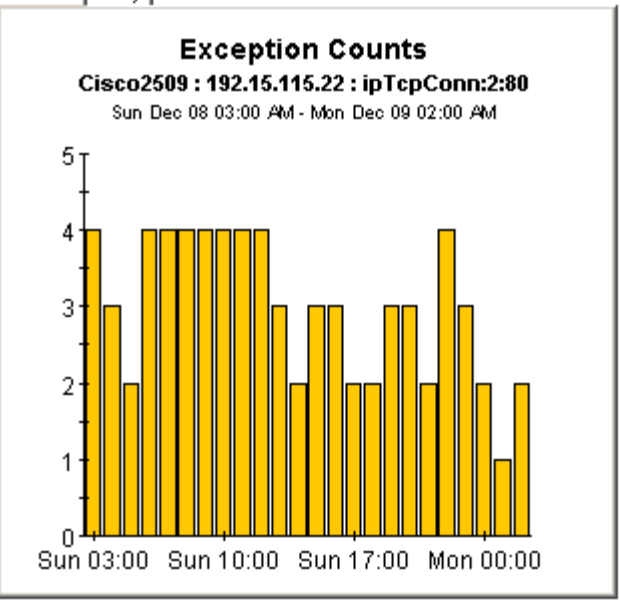
Hourly | Daily



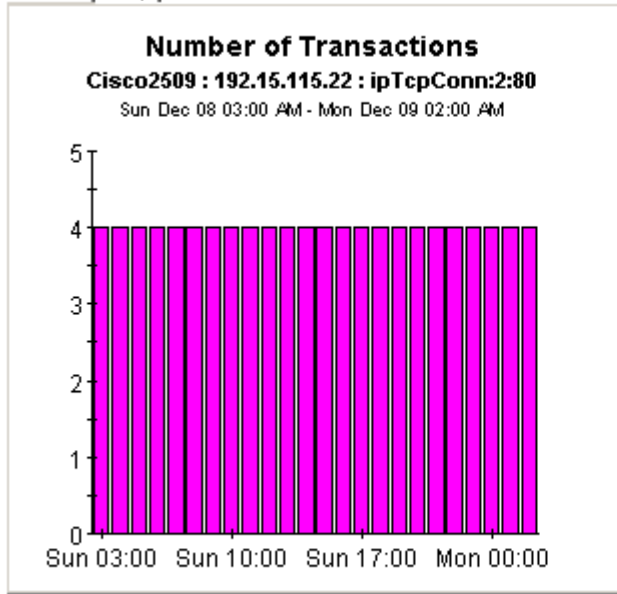
Hourly | Daily



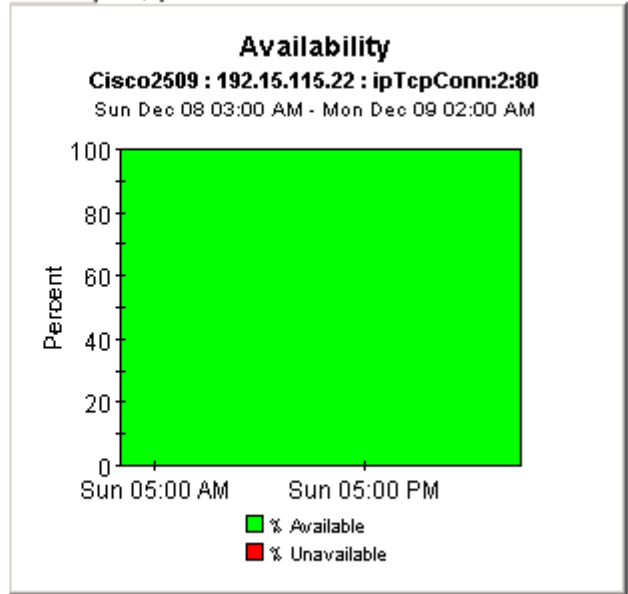
Hourly | Daily



Hourly | Daily



Hourly | Daily



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.

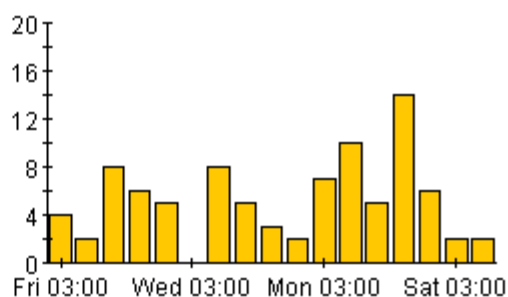
Sun Dec 08 2002

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

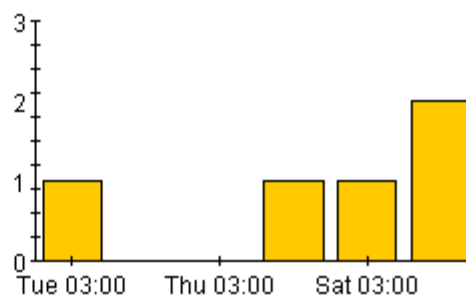
Sun Dec 08 2002

Source	# Trans	# Exceptions
Mcrouter85	96	2

Exception Counts

Mcrouter85

Tue Dec 03 2002 - Sun Dec 08 2002



Application / Destination Pairs with Most Exceptions

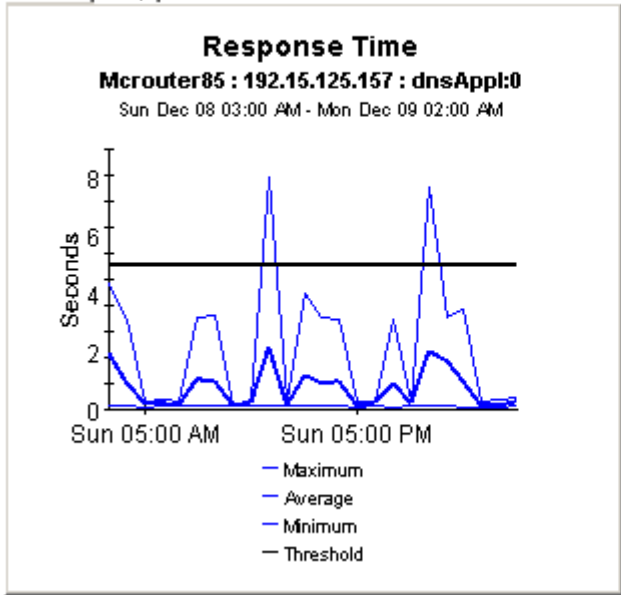
Sun Dec 08 2002

Application	Destination	Number of Transactions	Availability	Response Time Exceptions
dnsApp1:0	192.15.125.157	96	100.0	2

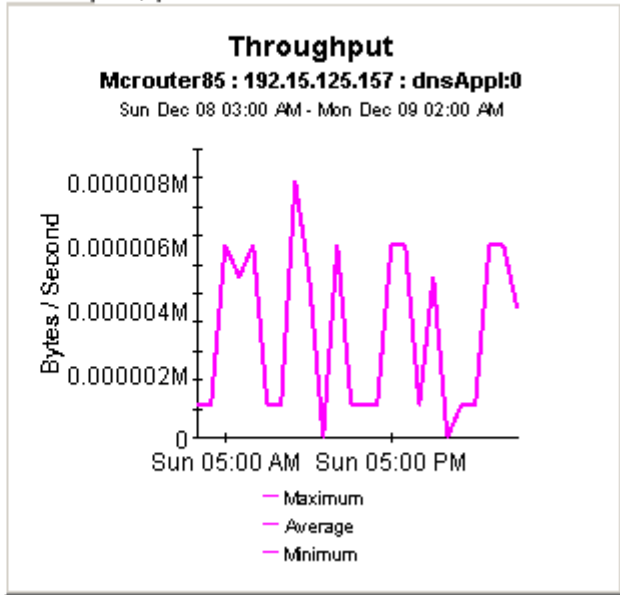




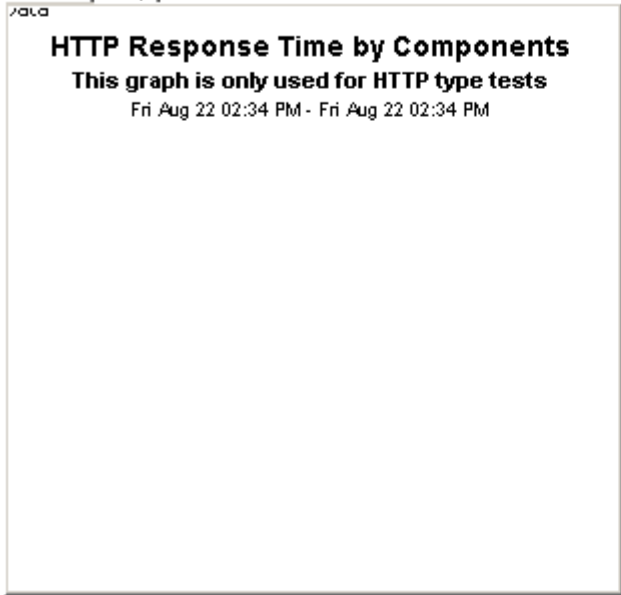
Hourly | Daily



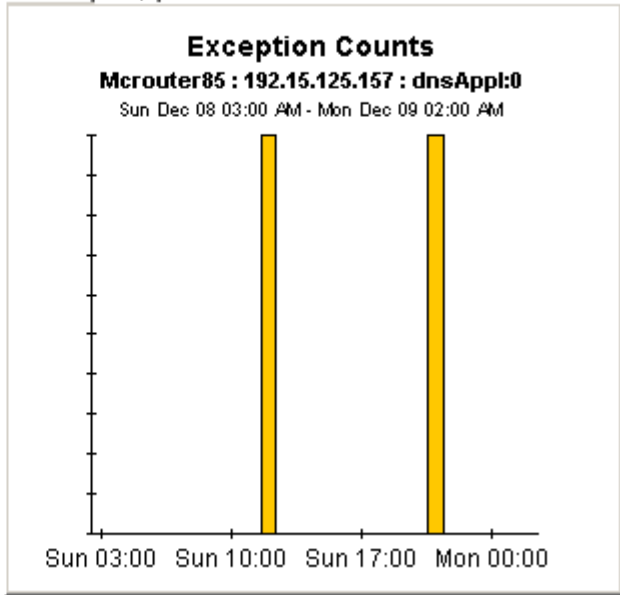
Hourly | Daily



Hourly | Daily

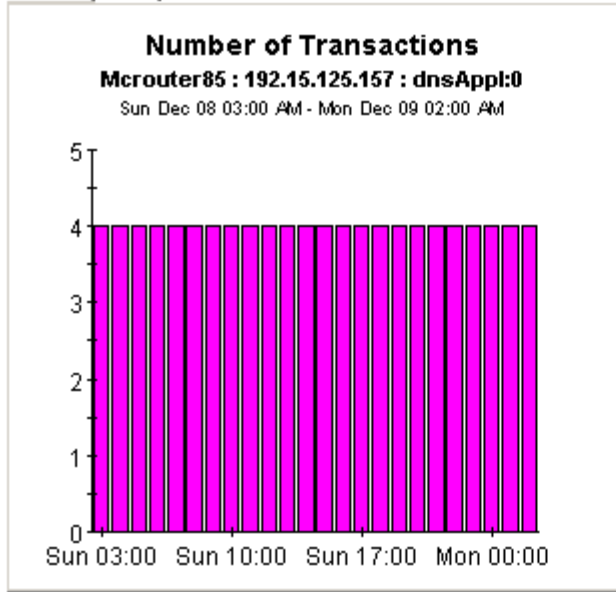


Hourly | Daily

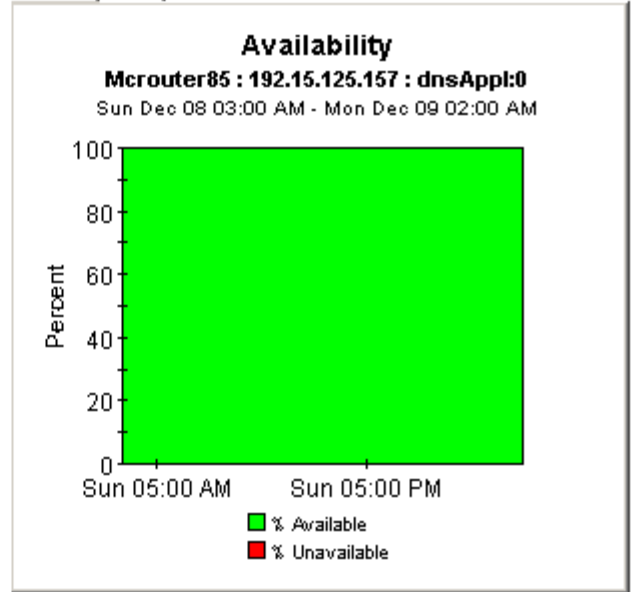




Hourly | Daily



Hourly | Daily



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.

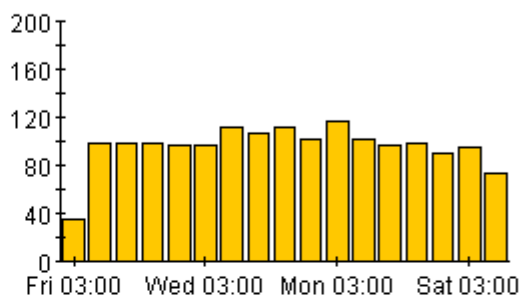
Sun Dec 08 2002

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

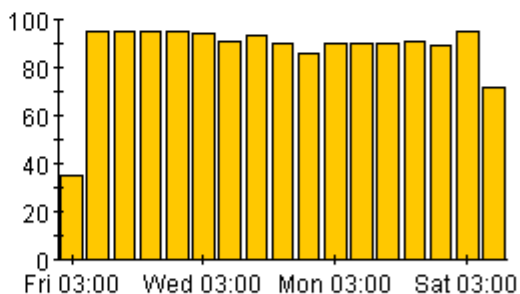
Sun Dec 08 2002

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

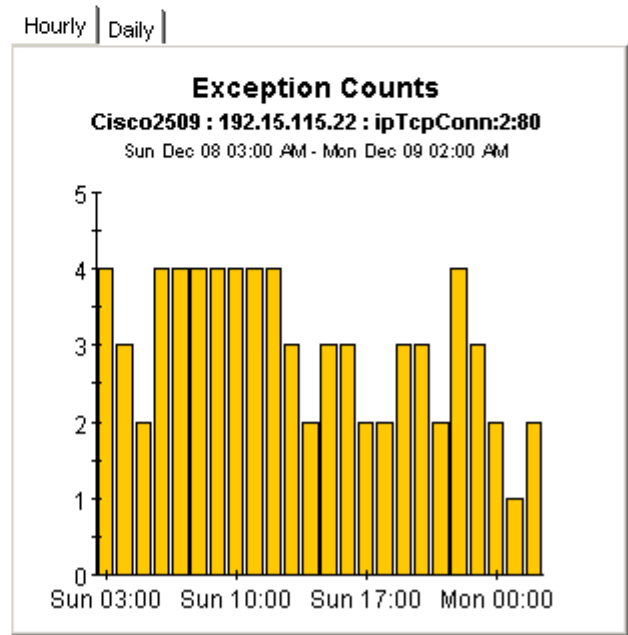
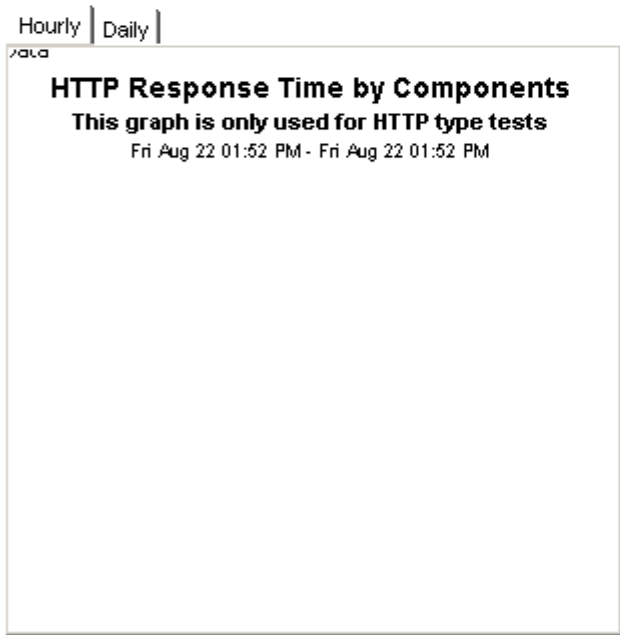
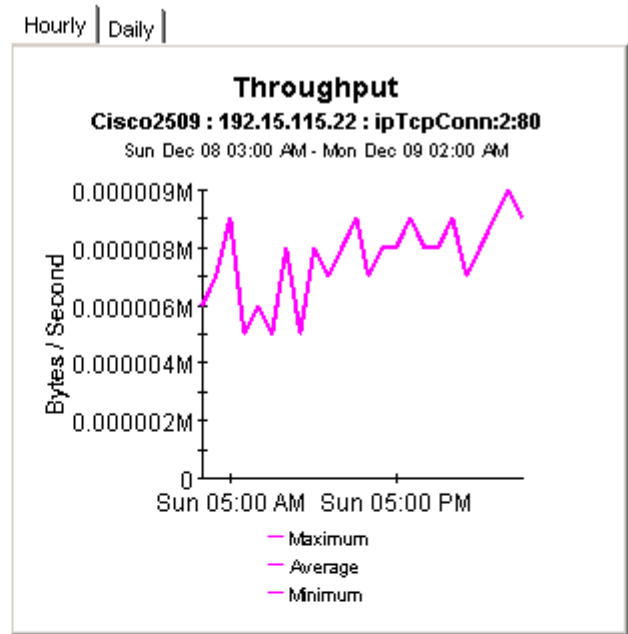
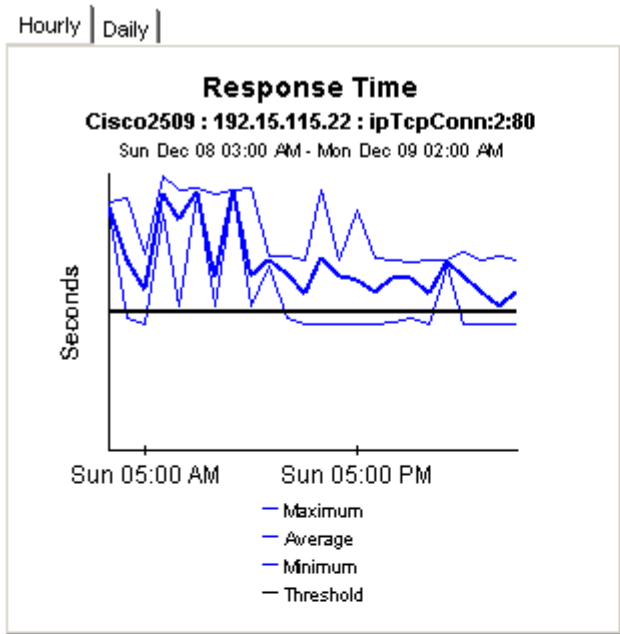


Source / Destination Pairs with Most Exceptions

Sun Dec 08 2002

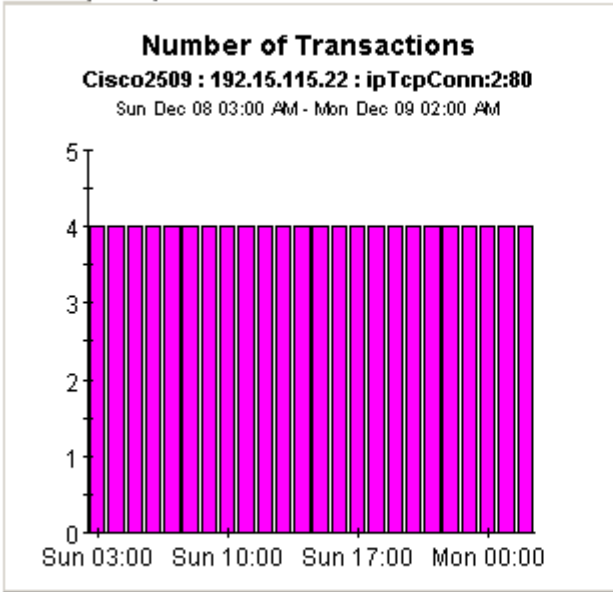
Source	Destination	Number of Transactions	Availability	Response Time Exceptions
Cisco2509	192.15.115.22	96	100.0	72



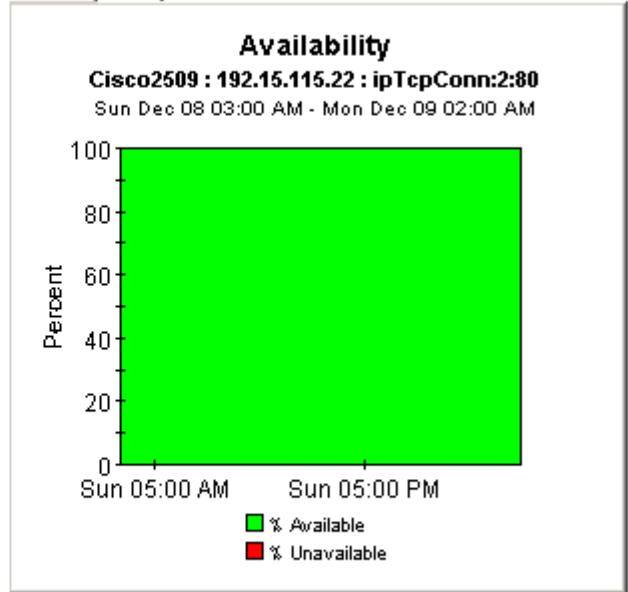




Hourly | Daily



Hourly | Daily



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

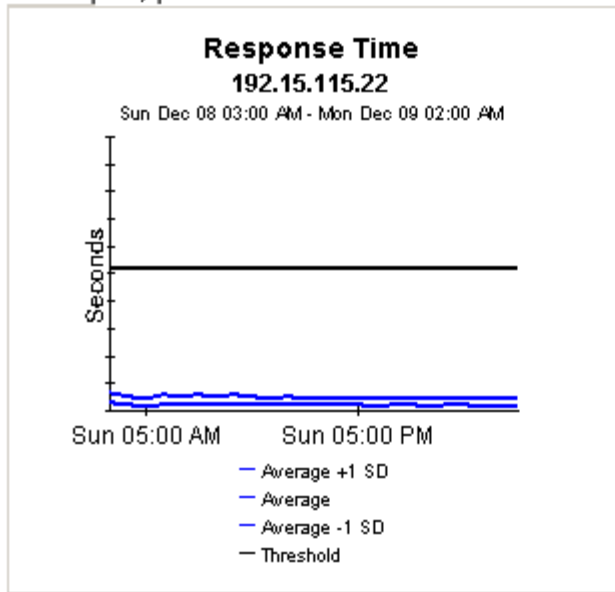
Customer	Customer ID	Number of Transactions	Number of Exceptions
All Customers	-1	2,308	75
DeskTalk	3	743	73
ucom	4	1,432	2

Destination Device Selection Table

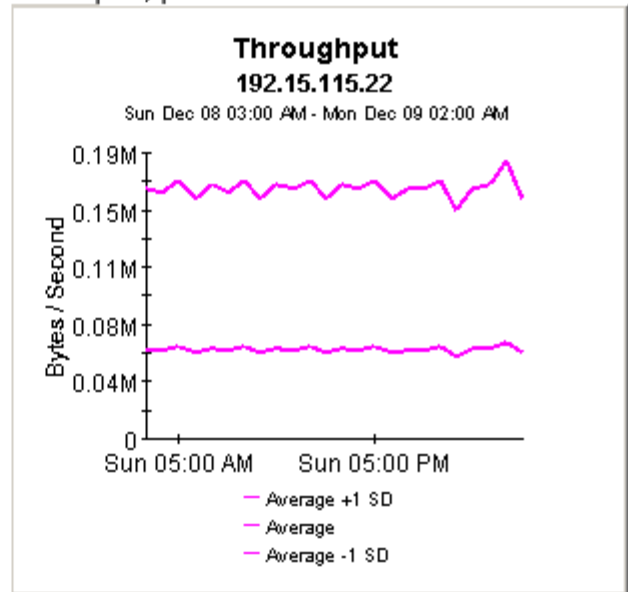
Sun Dec 08 2002

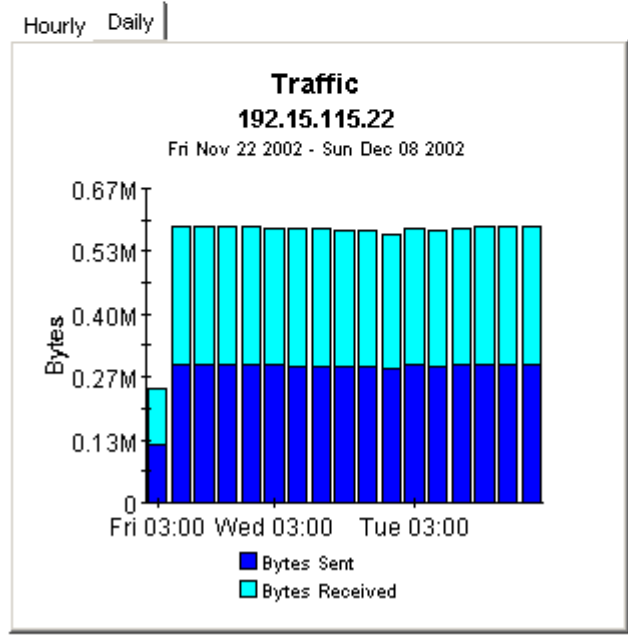
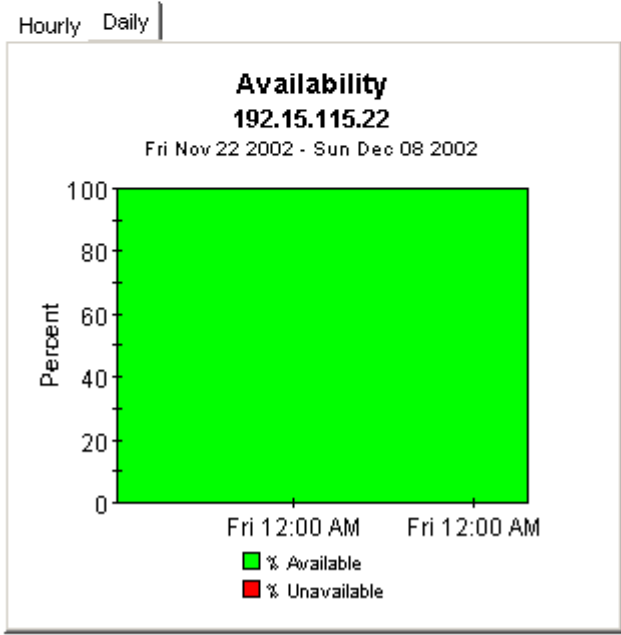
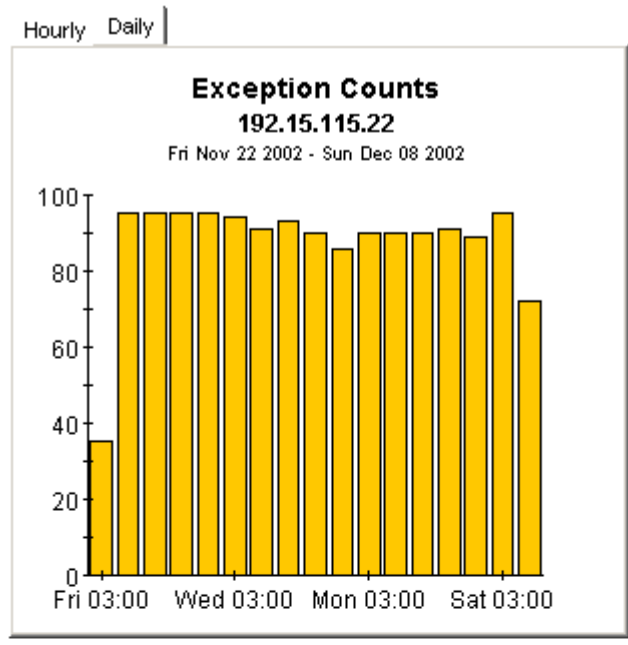
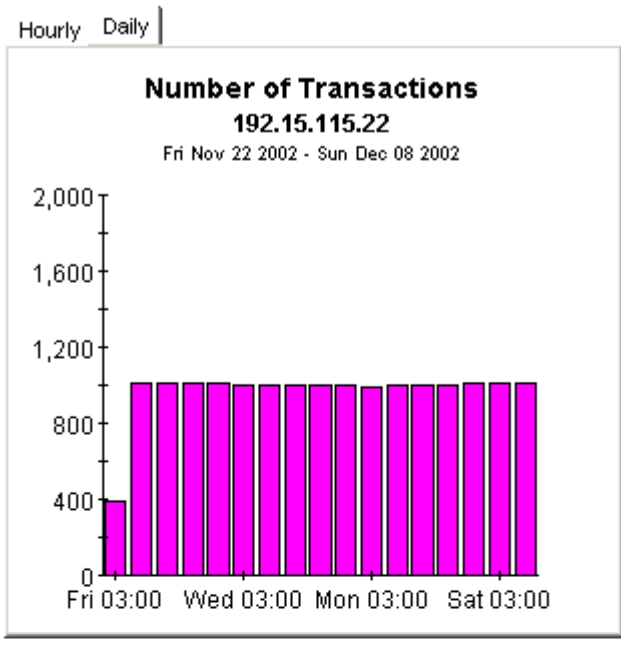
Destination	# Trans	Avg Resp. Time (Seconds)	Avg Throughput (Bps)	Availability (Percent)	Traffic (Bytes)
192.15.115.22	1,008	0.040	62.20 k	100.00	614.59 k
athp.hp.com	480	0.330	1050.9	83.33	81.12 k
www.yahoo.com	148	1.612	21.12 k	77.08	4218.4 k
ultra/README.bt	96	0.841	1.54	100.00	192.00
192.15.125.157	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





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

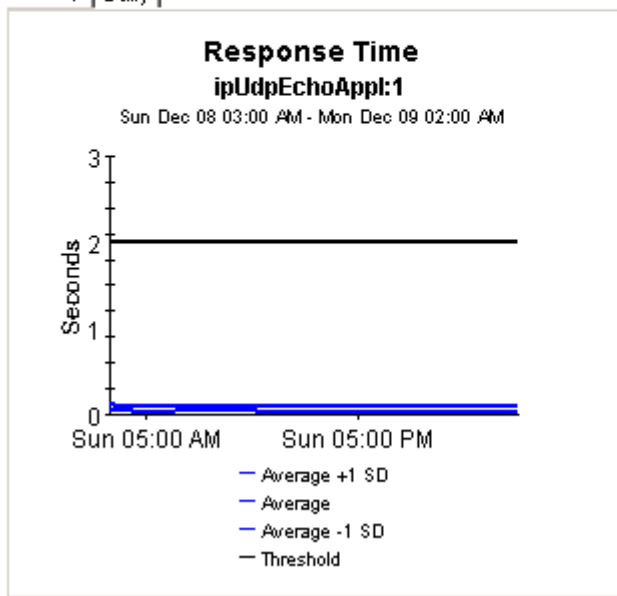
Customer	Customer ID	Number of Transactions	Number of Exceptions
All Customers	-1	2,308	75
Desktalk	3	743	73
ubnir	4	4,122	2

Application Selection Table

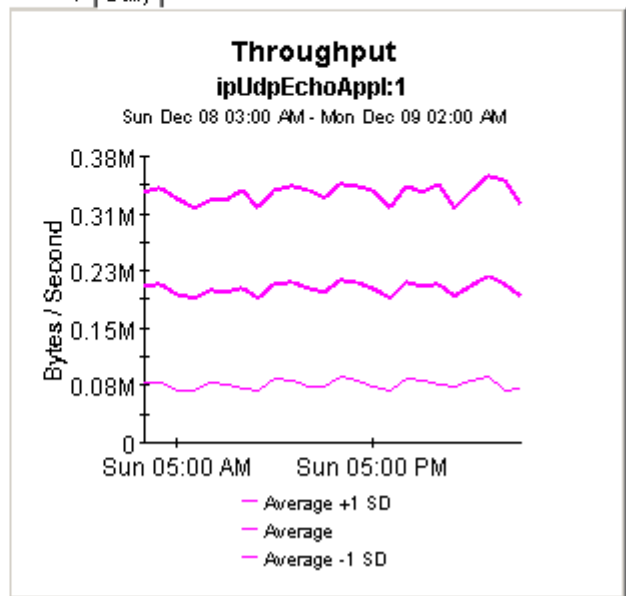
Sun Dec 08 2002

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
iplompEcho: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	32.46 k
iplompEcho:5	144	0.001	24.55 k	100.00	8064.0
ftpAppl:0	96	0.841	1.54	100.00	192.00
rtmAppl:0	96	0.120	0.00	100.00	0.00

Hourly | Daily

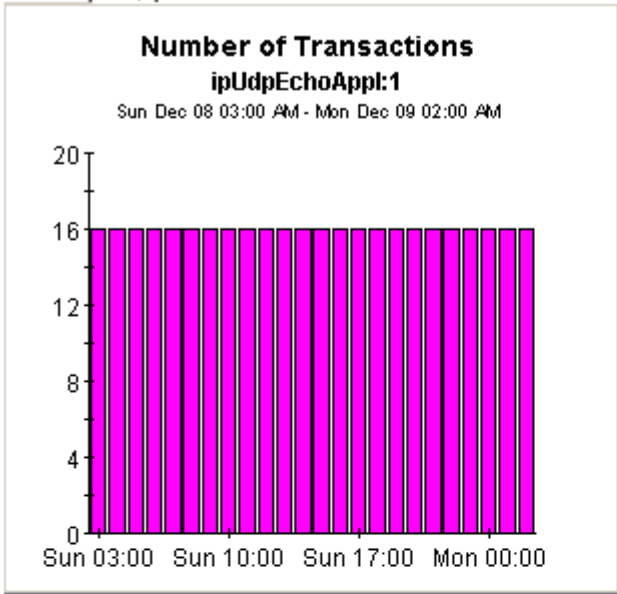


Hourly | Daily

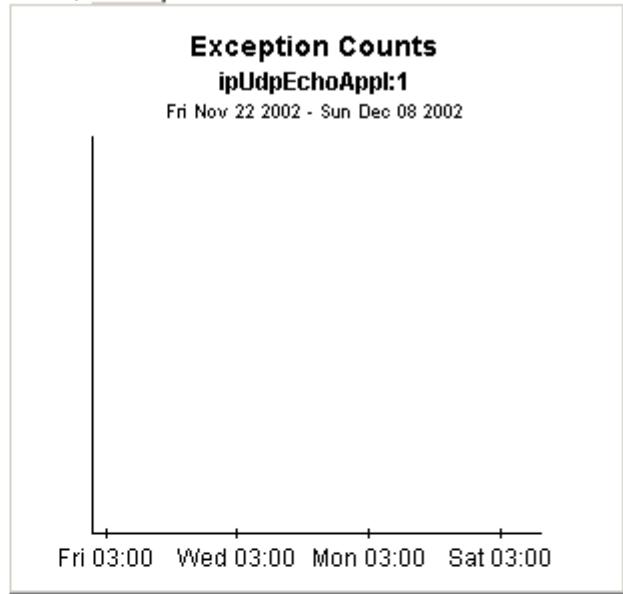




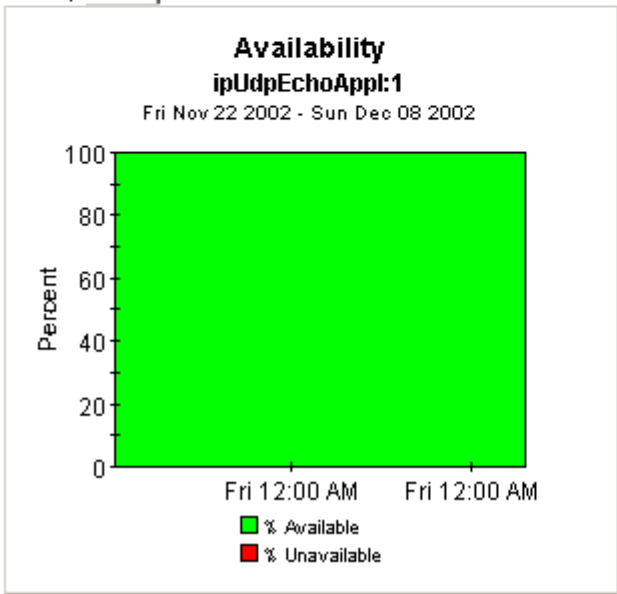
Hourly | Daily



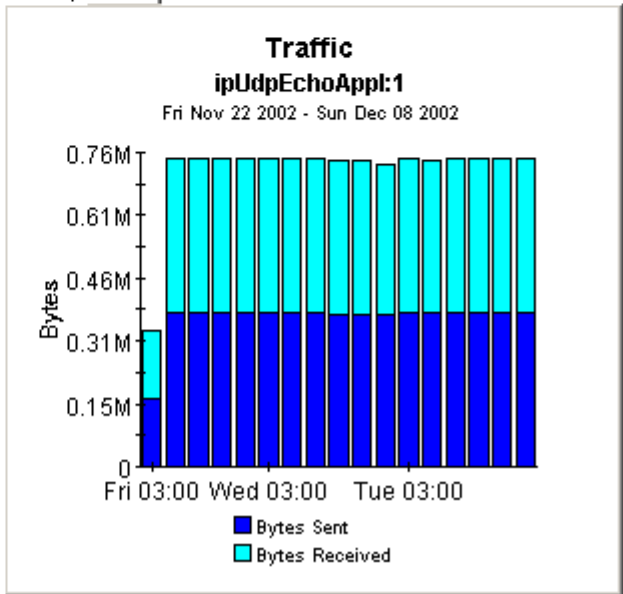
Hourly | Daily



Hourly | Daily



Hourly | Daily



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

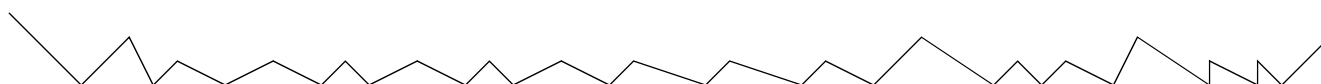
Sun Dec 08 2002

Source	# Transactions	Resp. Time (seconds)	Throughput (Bps)	Availability (Percent)	Traffic (bytes)
Cisco418	1,037	0.322	51.63 k	98.20	2637.2 k
Mcroute85	96	0.737	3.29	100.00	192.00

Application / Destination Pair Selection Table

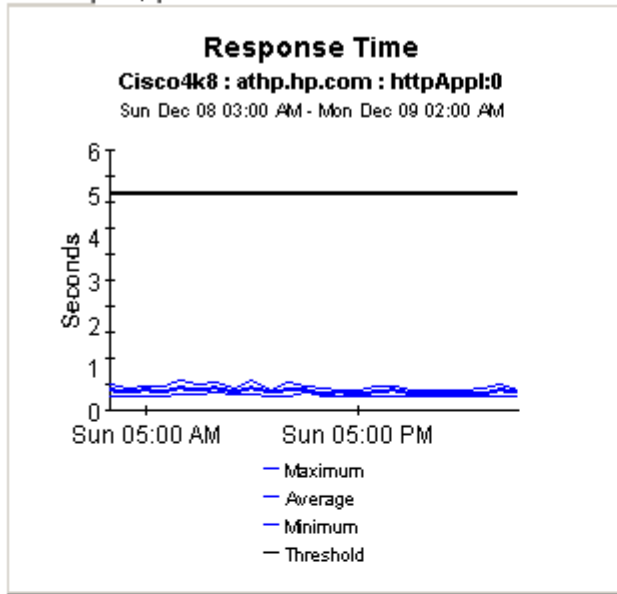
Sun Dec 08 2002

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
ipIcmpEcho: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

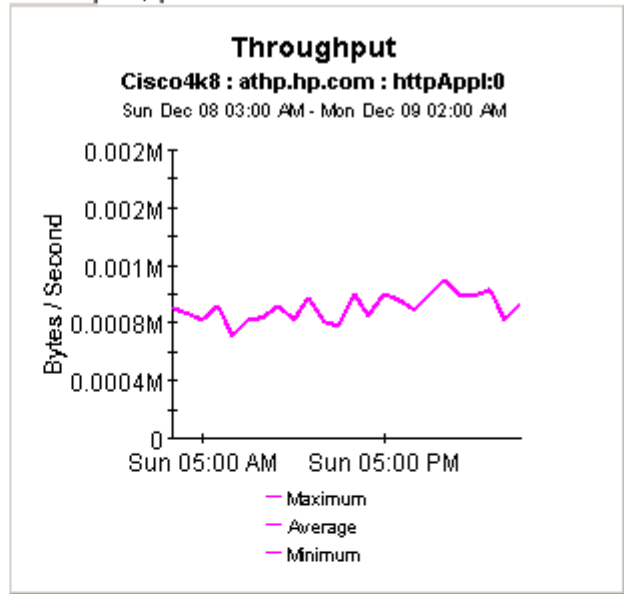




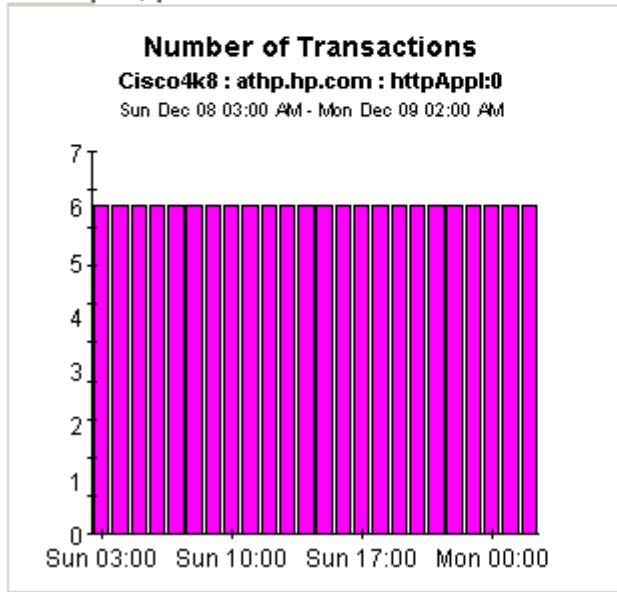
Hourly | Daily



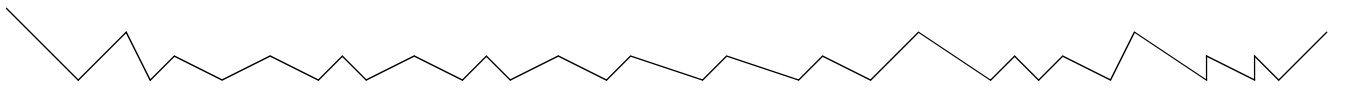
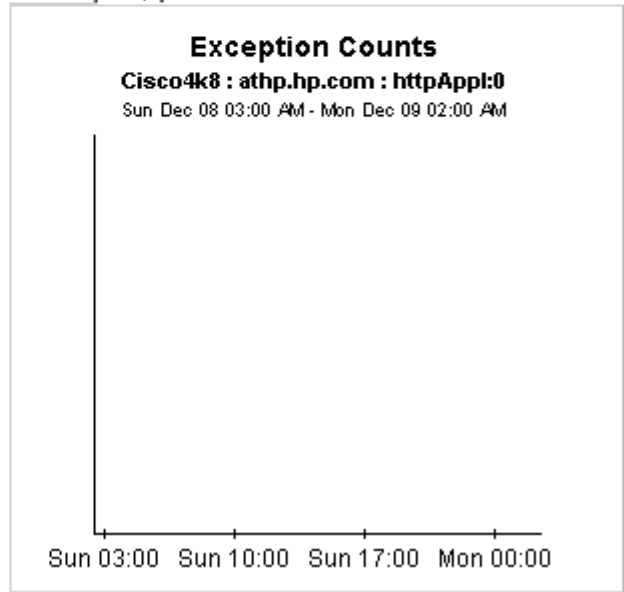
Hourly | Daily



Hourly | Daily

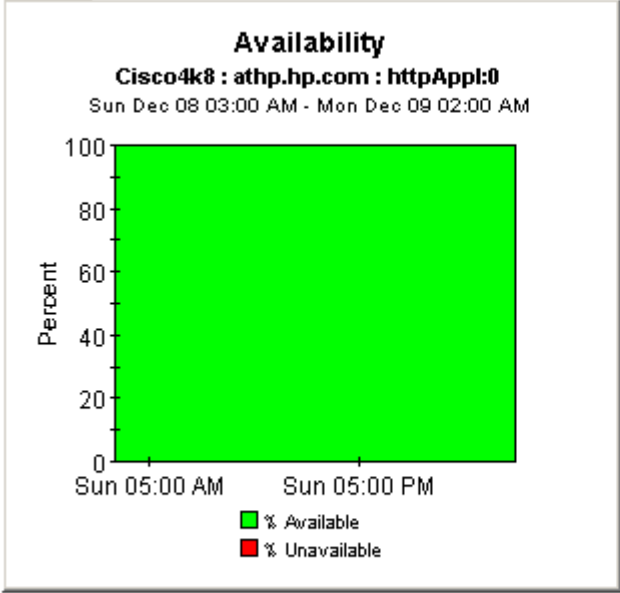


Hourly | Daily

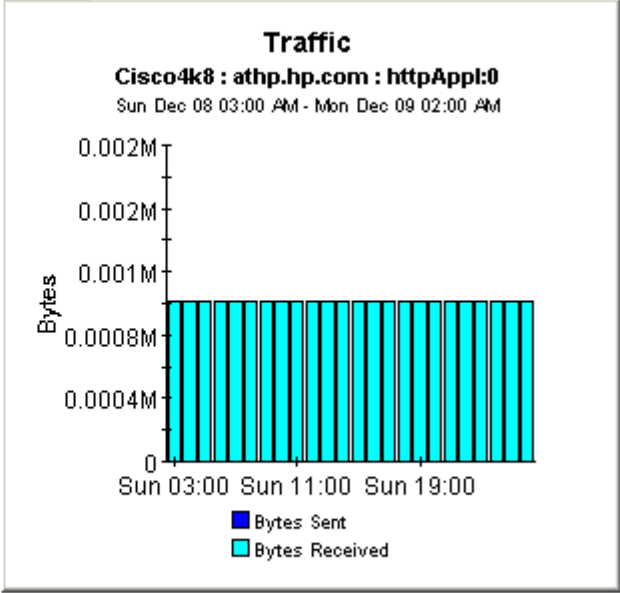




Hourly | Daily



Hourly | Daily



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

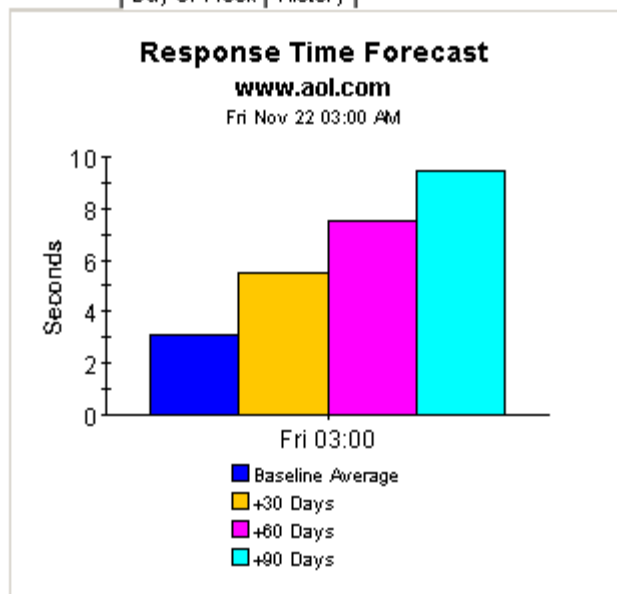
Customer	Response Time Baseline (sec)	F90 Response Time (sec)	Throughput Baseline (Bps)	F90 Throughput (Bps)
Desktalk	0.696	2.058	2984.98	0.00
Trinagy	0.686	2.103	80.67 k	0.00
HPOV	0.706	0.000	47.80 k	0.00
All Customers	0.555	0.550	20.05 k	40.07 k

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

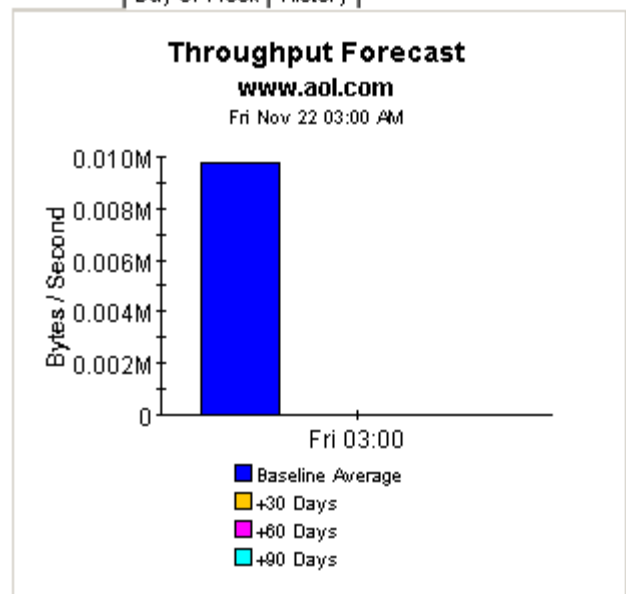
Fri Nov 22 03:00 AM

Destination	Response Time Baseline (sec)	F90 Response Time (sec)	Throughput Baseline (Bps)	F90 Throughput (Bps)
www.aol.com	3.080	9.450	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

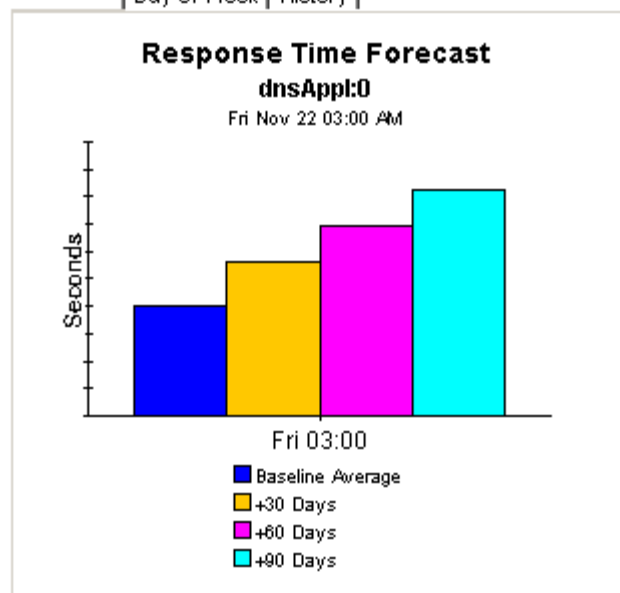
Customer	Response Time Baseline (sec)	F90 Response Time (sec)	Throughput Baseline (Bps)	F90 Throughput (Bps)
DeskTalk	0.896	2.058	2984.98	0.00
Trinagy	0.886	2.103	80.67 k	0.00
HPOV	0.706	0.000	47.80 k	0.00
All Customers	0.886	2.058	2984.98	0.00

Applications with Greatest Rate of Change in Response Time or Throughput

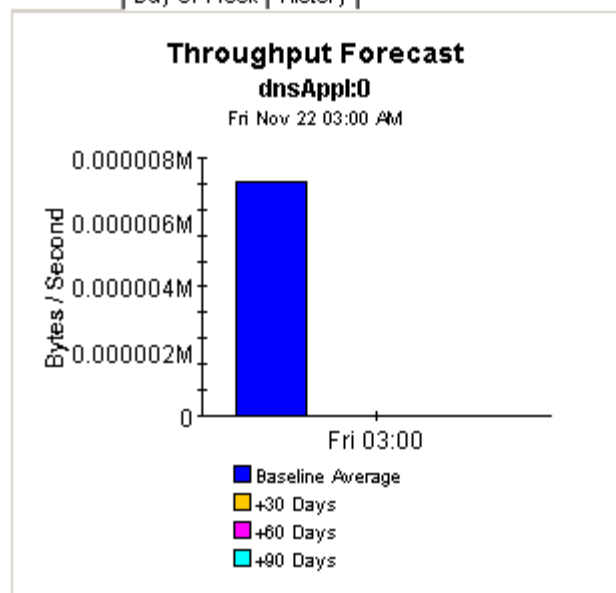
Fri Nov 22 03:00 AM

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
iplcmpEcho:0	0.130	0.410	224.94	0.00
ipUdpEchoAppl:1	0.155	0.331	6765.75	0.00

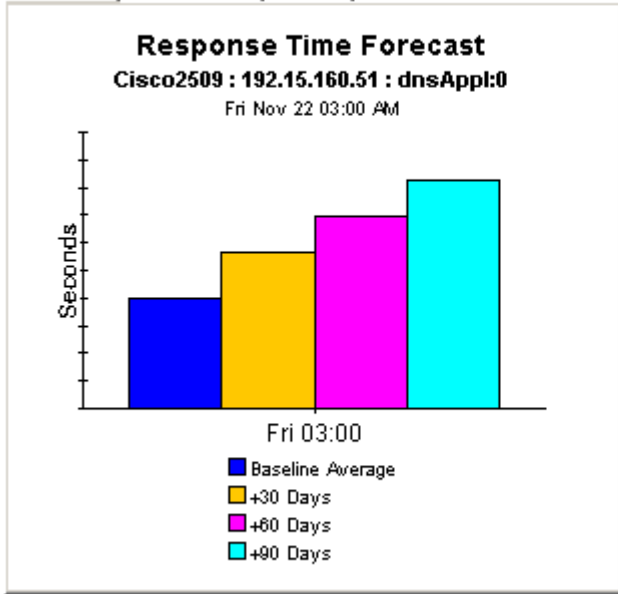
Source / Destination Pairs with Greatest Rate of Change in Response Time or Throughput

Fri Nov 22 03:00 AM

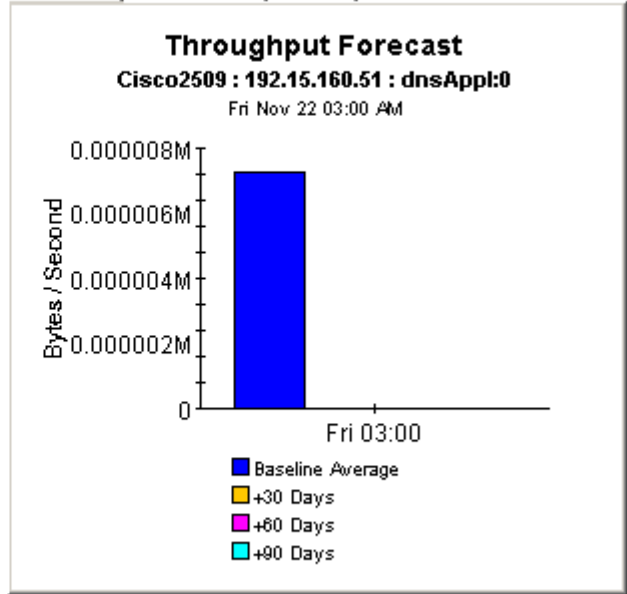
Source	Destination	Response Time Baseline (sec)	F90 Reponse Time (sec)	Throughput Baseline (Bps)	F90 Throughput (Bps)
Ciscoe2509	192.15.160.51	0.800	1.653	7.25	0.00



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

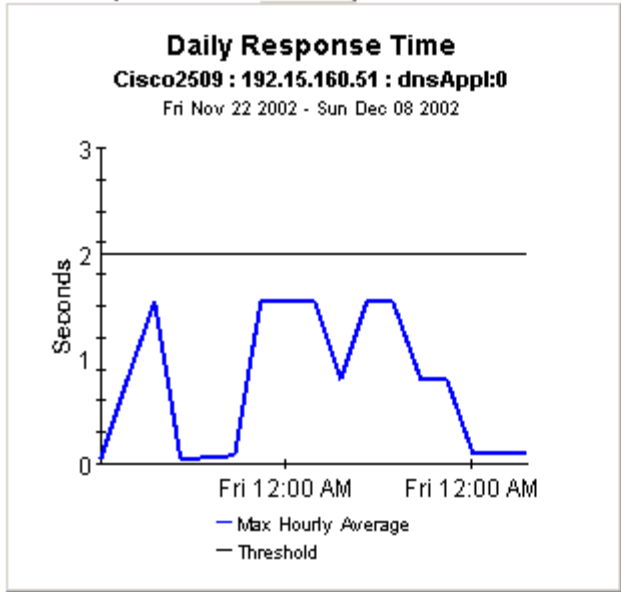
Throughput Forecast (Bytes/Second)

Cisco2509 : 192.15.160.51 : dnsAppl:0
Thu Nov 28 03:00 AM

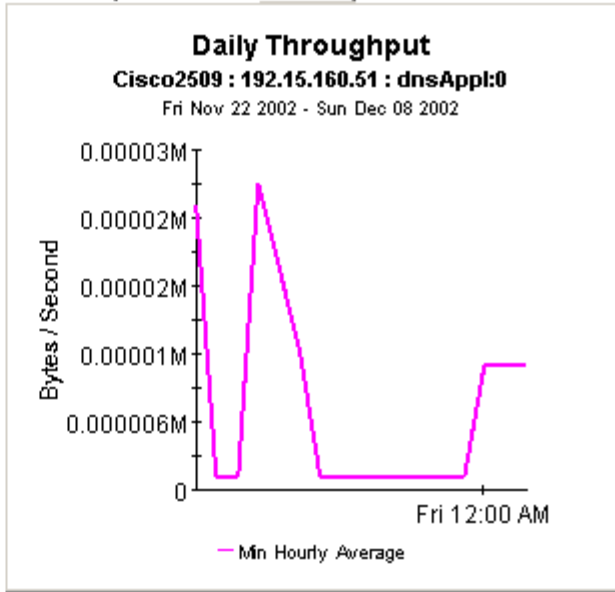
Day	Baseline	+ 30 / 60 / 90 Days
Sun	1.00	1.00 / 1.00 / 1.00
Mon	14.00	0.00 / 0.00 / 0.00
Tue	10.50	0.00 / 0.00 / 0.00
Wed	6.50	0.00 / 0.00 / 0.00
Thu	1.00	1.00 / 1.00 / 1.00
Fri	12.33	0.00 / 0.00 / 0.00
Sat	4.33	30.76 / 52.19 / 73.62



Standard | Day of Week | History



Standard | Day of Week | History



Focusing on 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	ipTopConn: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	ipTopConn: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

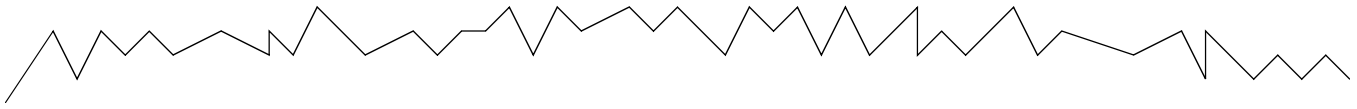
	Application	Average Throughput
1	dlswAppl:0	0.00
2	ftpAppl:0	1.54
3	dnsAppl:0	13.26
4	ipTopConn:2:80	324.22
5	httpAppl:2	1079.75
6	httpAppl:0	8464.67
7	iplcmpEcho:0	14.15 k
8	iplcmpEcho:5	24.55 k
9	ipUdpEchoAppl:1	214.59 k
10	dhcpAppl:0	0.00

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 / 0.00
5	ipTopConn:2:80	258.21	199.98 / 106.81 / 106.81
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 / 123.33 k
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	1
ipUdpEchoAppl:1	384	2
dnsAppl:0	288	3
ipTcpConn:2:80	288	4
ipIcmpEcho:0	288	5
httpAppl:2	192	6
ipIcmpEcho:5	144	7
ftpAppl:0	96	8
dlsWAppl:0	96	9
dhcpAppl:0	0	10

Traffic (Bytes)

Sun Dec 08 03:00 AM

Application	Total Traffic
httpAppl:0	4496.51 k
ipUdpEchoAppl:1	786.43 k
httpAppl:2	32.45 k
ipIcmpEcho:0	16.13 k
ipIcmpEcho:5	8064.00
dnsAppl:0	576.00
ipTcpConn:2:80	576.00
ftpAppl:0	192.00
dhcpAppl:0	0.00
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

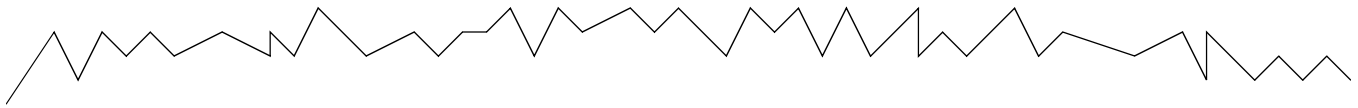
	Destination	Average Throughput
1	192.15.96.2	0.00
2	ultra/README.txt	1.54
3	192.15.125.157	3.29
4	192.15.128.51	7.50
5	192.15.160.51	29.00
6	athp.hp.com	1050.92
7	www.aol.com	11.26 k
8	www.yahoo.com	21.12 k
9	192.15.115.22	62.20 k
10	192.15.115.2	285.46 k

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

Sample Data in Near Real Time

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

If you install the Cisco SAA Datapipe only, you have one NRT report, derived from data stored by SAA in the MIB History Table. The NRT report in the Source/Destination/Application folder is produced from data collected by the Cisco SAA Datapipe. The contents of this report change once an hour. This report identifies:

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

This report 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 two additional reports:

- Near Real Time - Latest Test
- Jitter 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
- NRT - Latest Test
- Jitter NRT - Latest Test

Service Assurance



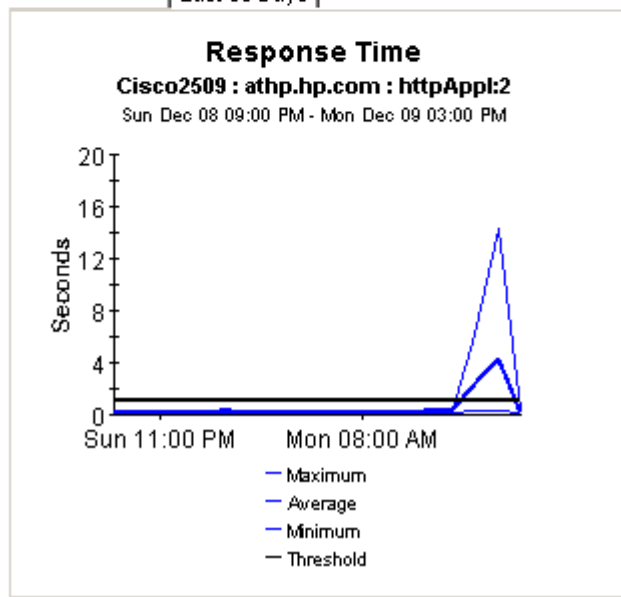
Near Real Time Summary

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.

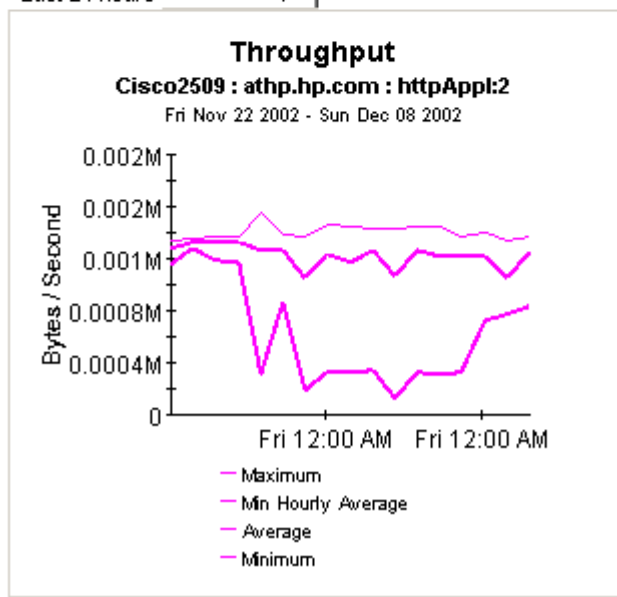
Mon Dec 09 07:00 PM

Source / Destination / Application	Exceptions	Availability (Percent)
Cisco2509 / 192.15.115.22 / ipTopConn: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 / dswAppl:0	0	100.00
15.24.115.3 / 15.24.115.22 / ipTopConn:2:80	0	100.00
15.24.115.3 / 15.24.115.22 / ipUdpEchoAppl:1	0	100.00

Last 24 Hours | Last 30 Days

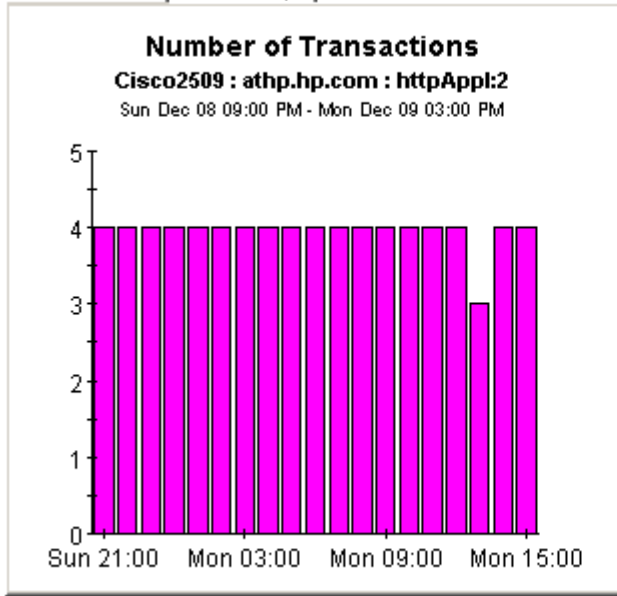


Last 24 hours | Last 30 Days

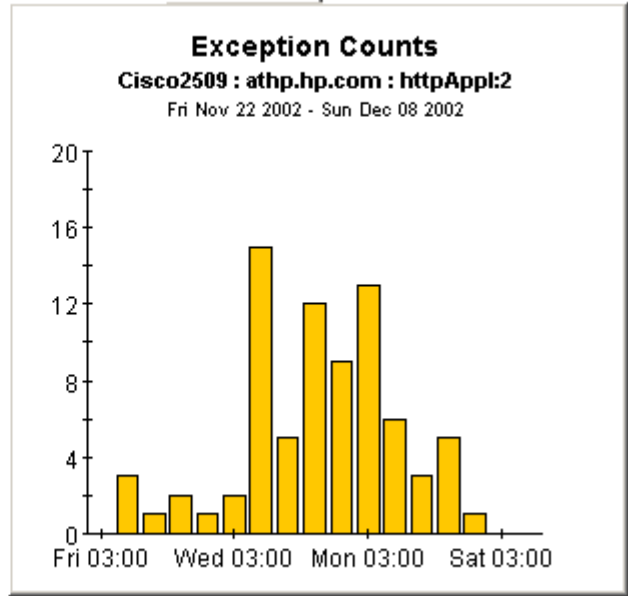




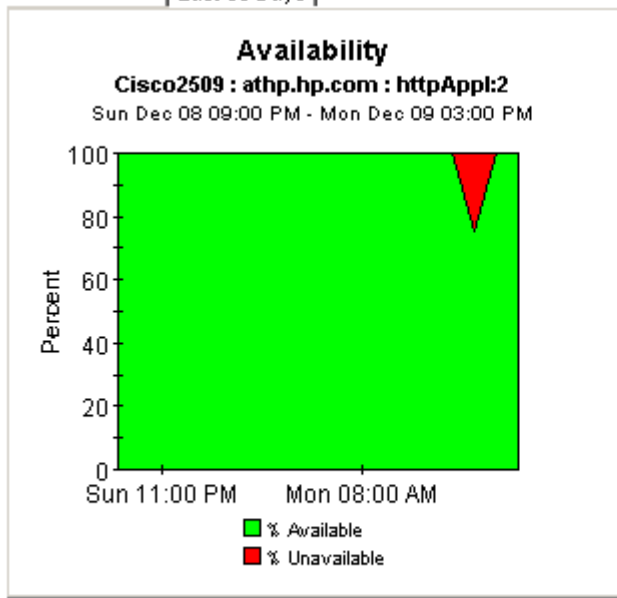
Last 24 Hours | Last 30 Days



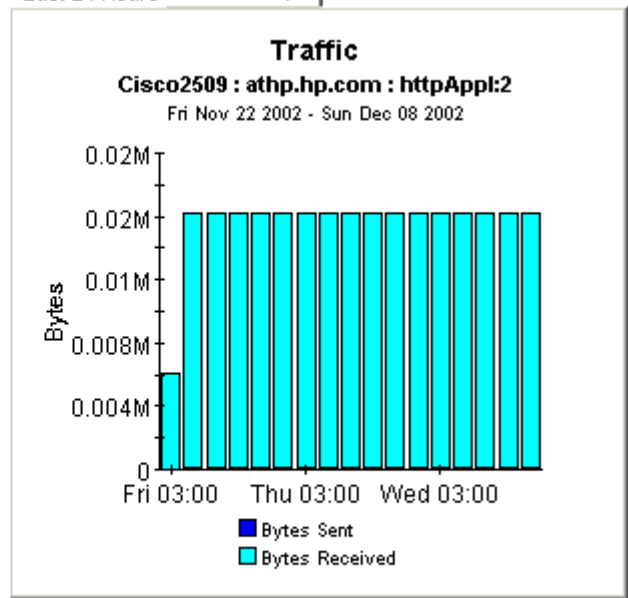
Last 24 Hours | Last 30 Days



Last 24 Hours | Last 30 Days



Last 24 Hours | Last 30 Days



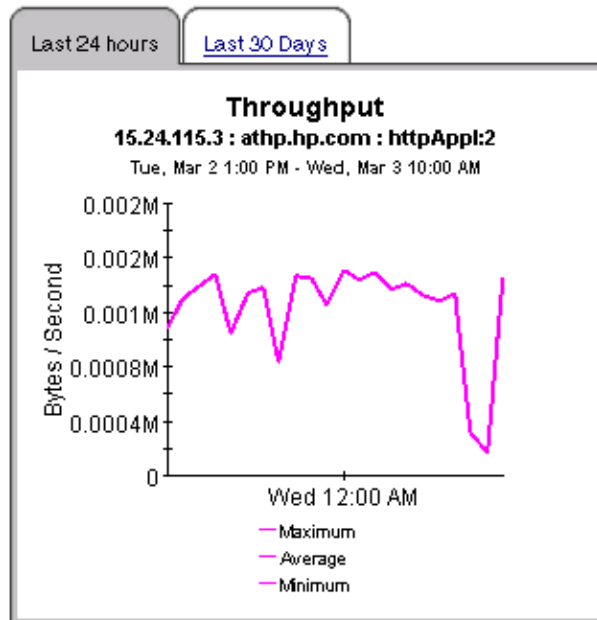
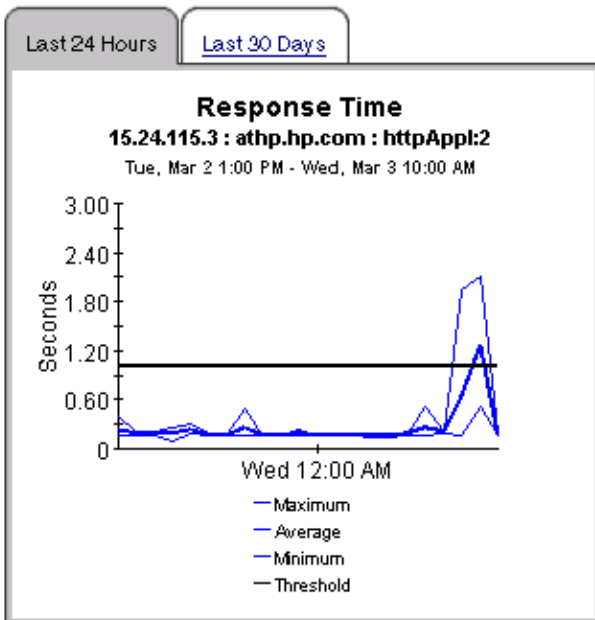
Service Assurance

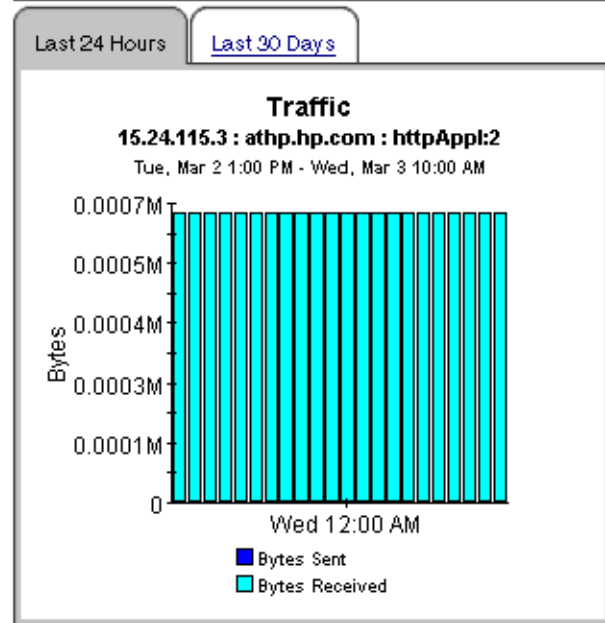
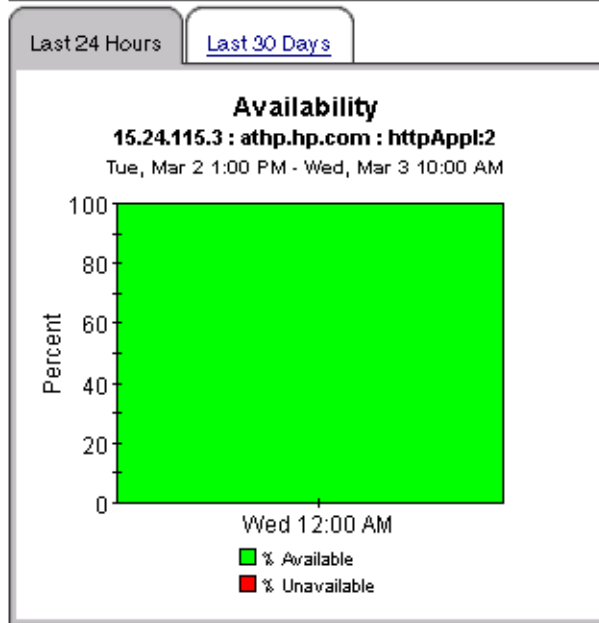
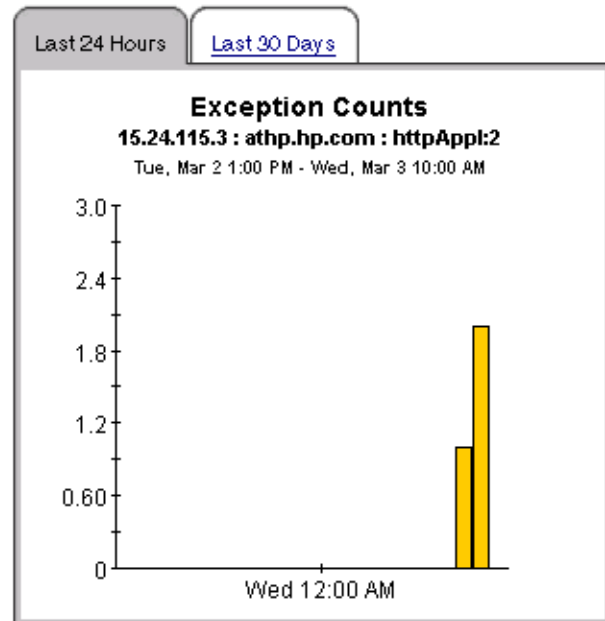
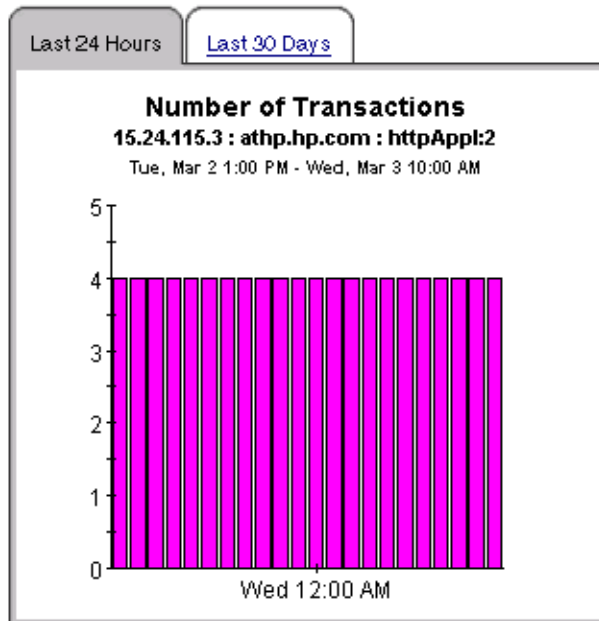
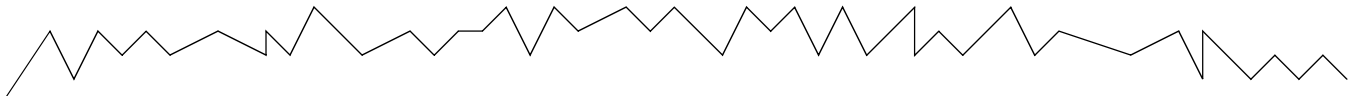


Near Real Time Summary

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.

Source / Destination / Application	Exceptions	Availability (Percent)
15.24.115.3 / athp.hp.com / httpAppl:2	3	100.00
15.24.115.3 / www.yahoo.com / httpAppl:0	3	100.00
15.24.115.3 / 15.227.128.51 / dnsAppl:0	1	100.00
15.24.115.3 / ultra/README.txt / ftpAppl:0	0	0.00
15.24.115.3 / athp.hp.com / httpAppl:0	0	0.00
15.24.115.3 / 15.24.115.22 / iplcmpEcho:0	0	100.00
15.24.115.3 / 15.24.115.22 / ipTopConn:2:80	0	100.00
15.24.115.3 / 15.24.115.22 / ipUdpEchoAppl:1	0	100.00
15.24.115.3 / 15.227.128.51 / dnsAppl:0	0	100.00





[Back to Top](#)



Service Assurance



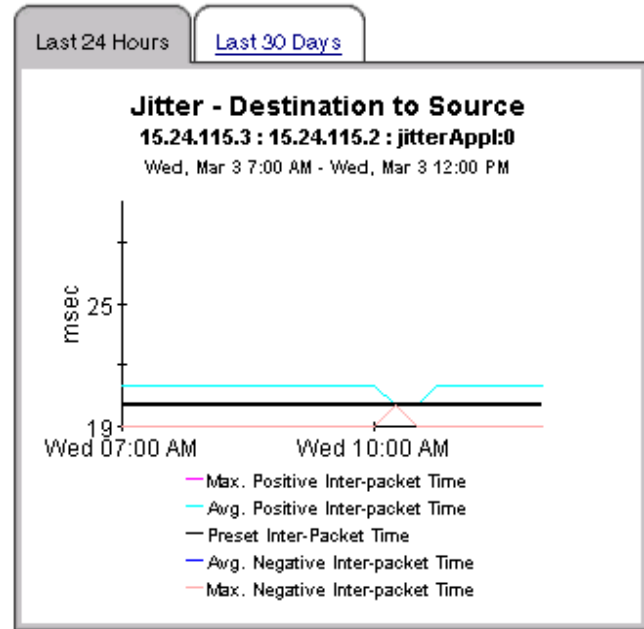
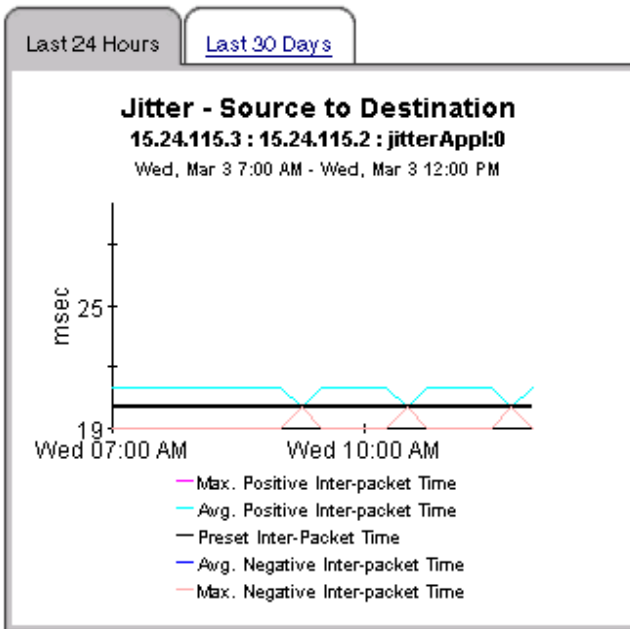
Jitter Near Real Time Summary

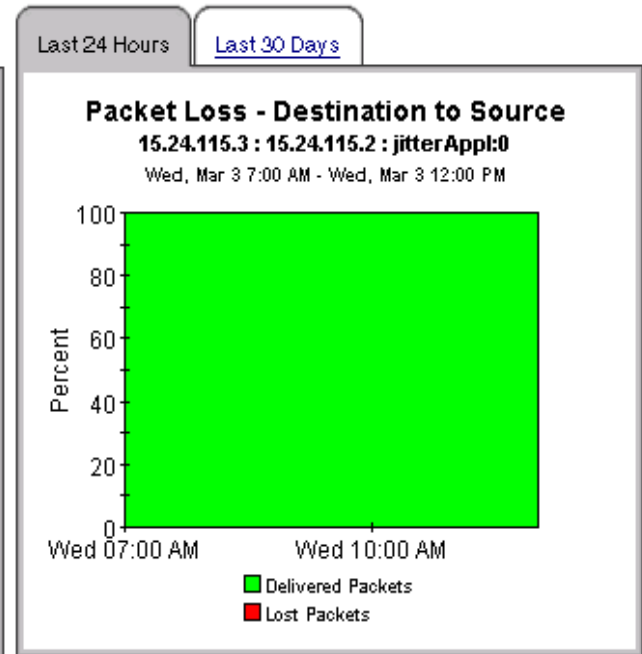
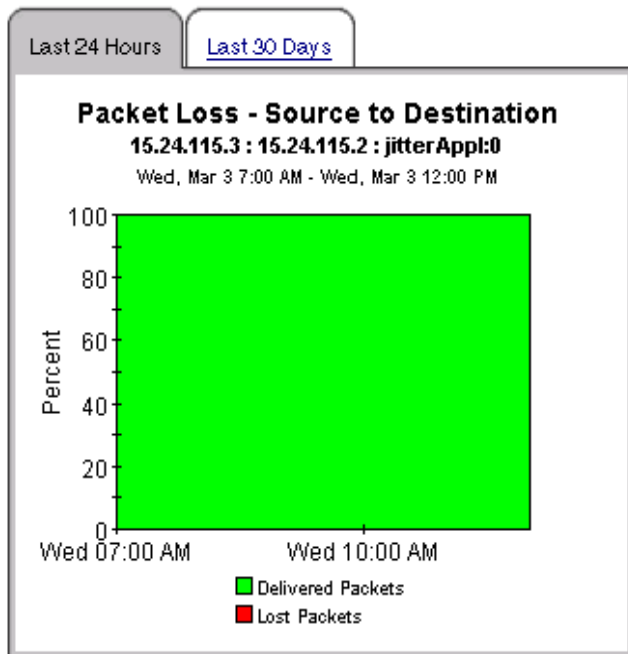
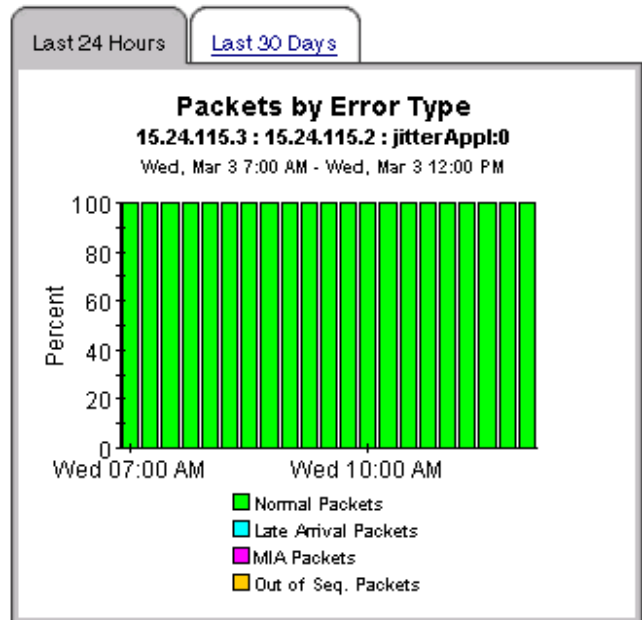
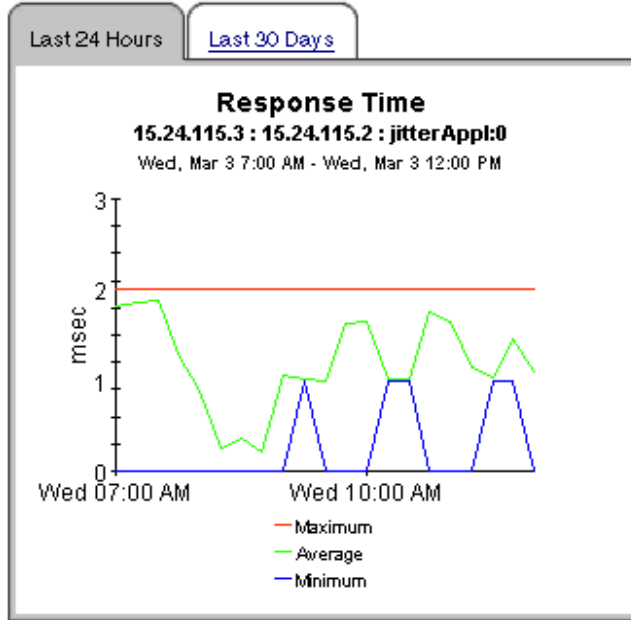
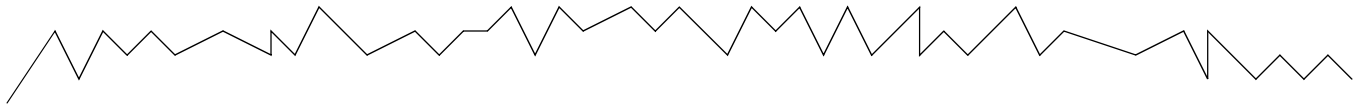
The Jitter Near Real Time Summary Report presents the most recent performance statistics available for Jitter tests. Data is presented for each source / destination combination that had activity within the last 6 hours. By selecting a source / destination combination, performance data for both the last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

Near Real Time Jitter Test Performance For Last Six Hours

Wed, Mar 3 1:00 PM

Source/Destination	# of Tests	Avg Response Time (msec)	Avg SD Dev (msec)	Avg DS Dev (msec)	Avg PacketLoss (SD/DS,%)
15.24.115.3 / 15.24.115.2	25	1.2	-1.0 / +1.0	-1.0 / +1.0	0.0 / 0.0





[↑ Back to Top](#)



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.

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

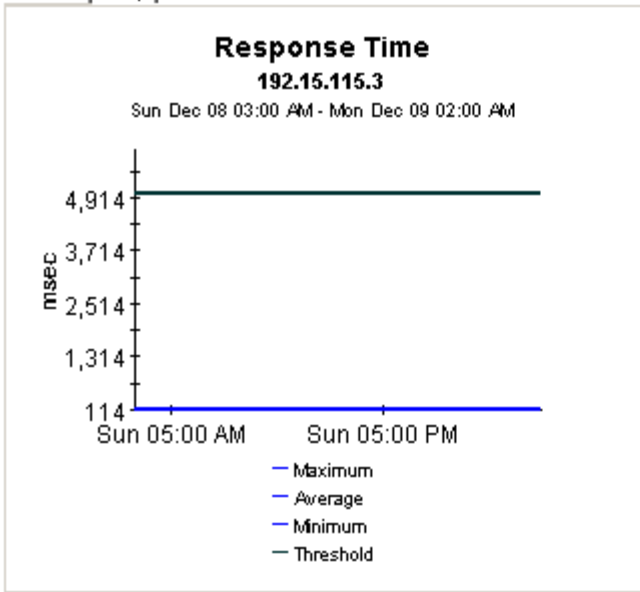
Customer	CustID	# of Transactions	# of Exceptions
All Customers	-1	576	0
HPOV	1	384	0
Trinagy	2	96	0

Destination Device Selection Table
S2D: Source to Destination, D2S: Destination to Source

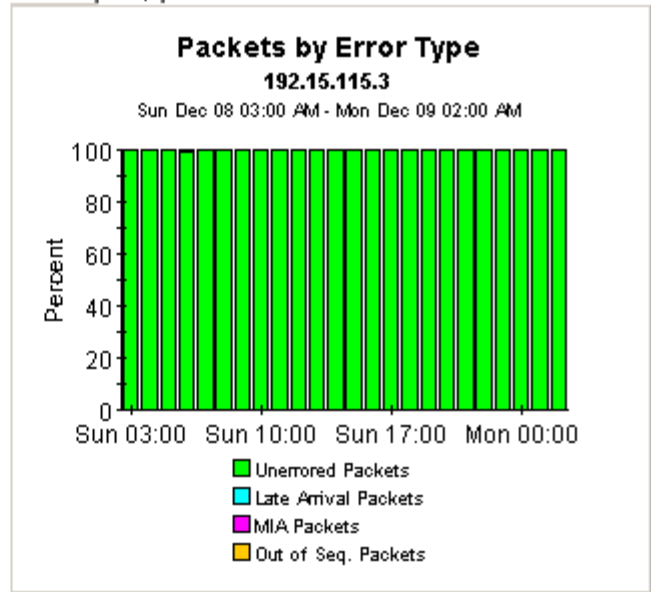
Sun Dec 08 2002

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

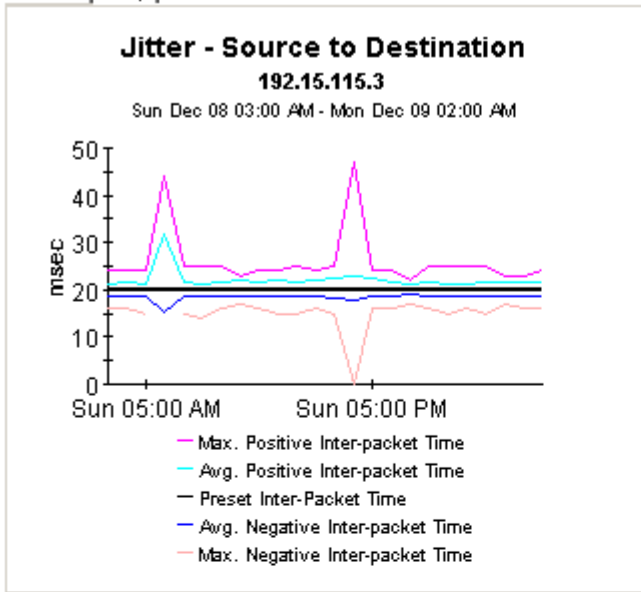


Hourly | Daily

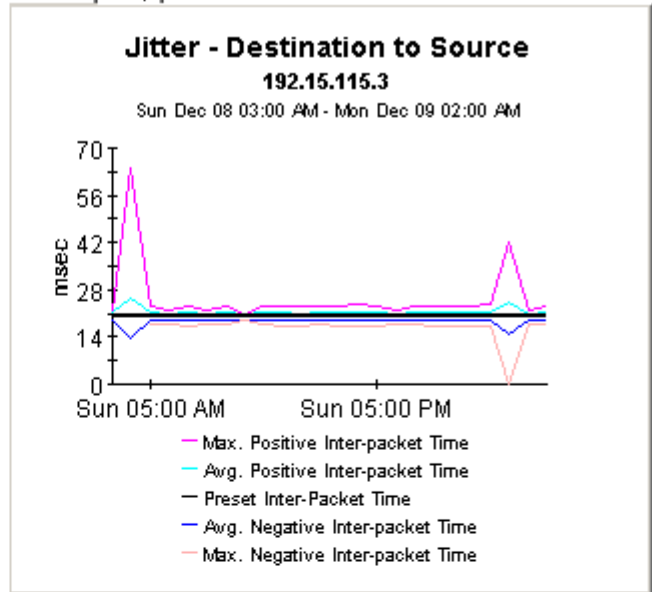




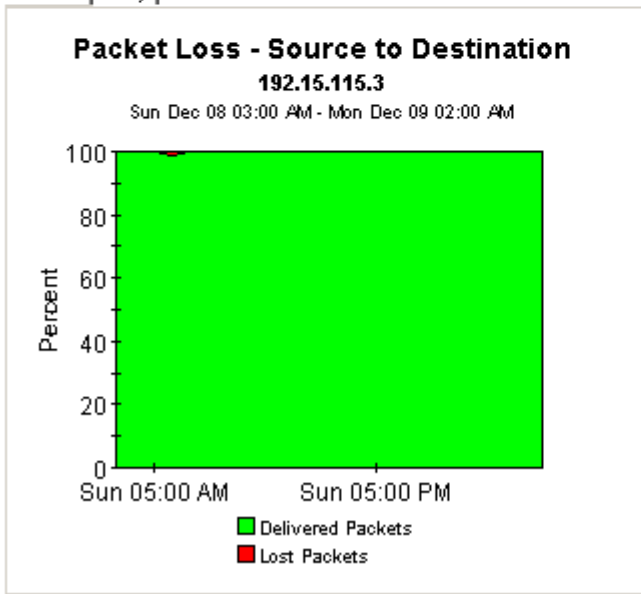
Hourly | Daily



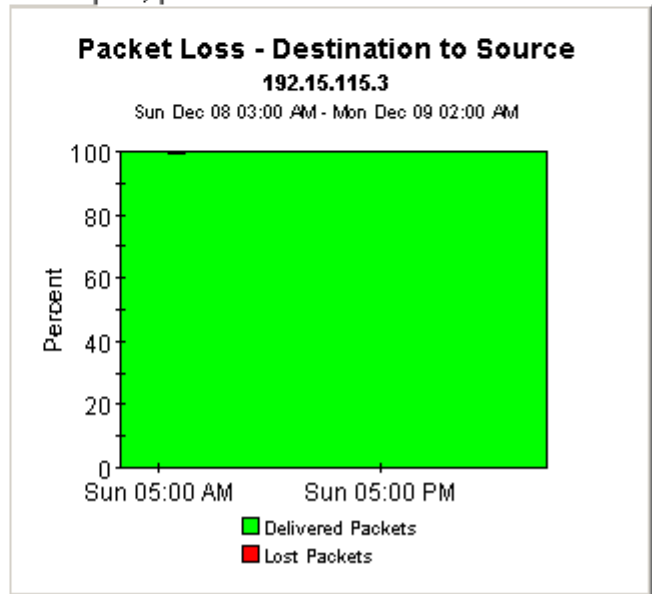
Hourly | Daily



Hourly | Daily



Hourly | Daily



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

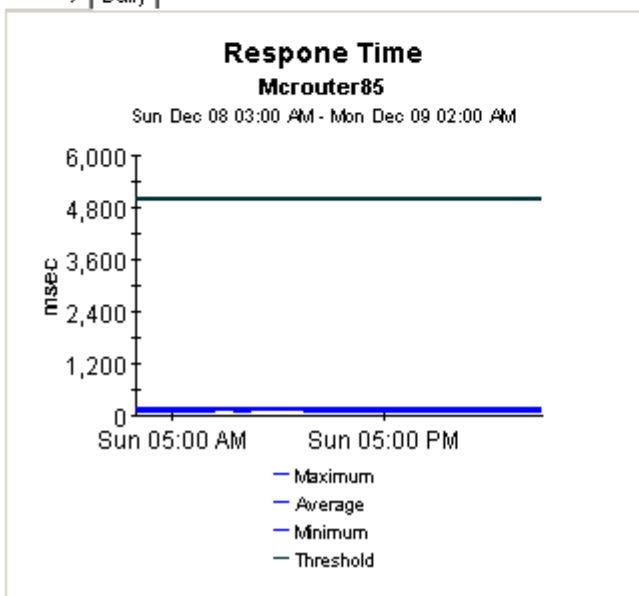
Source Device Selection Table

S2D: Source to Destination, D2S: Destination to Source

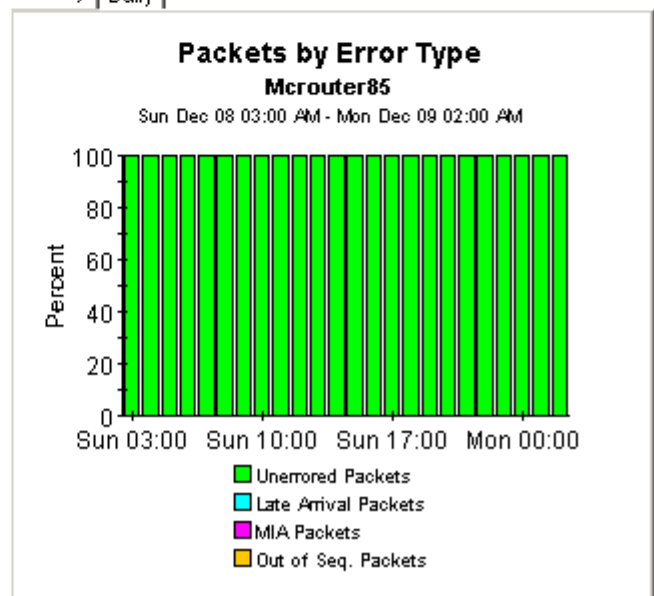
Sun Dec 08 2002

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

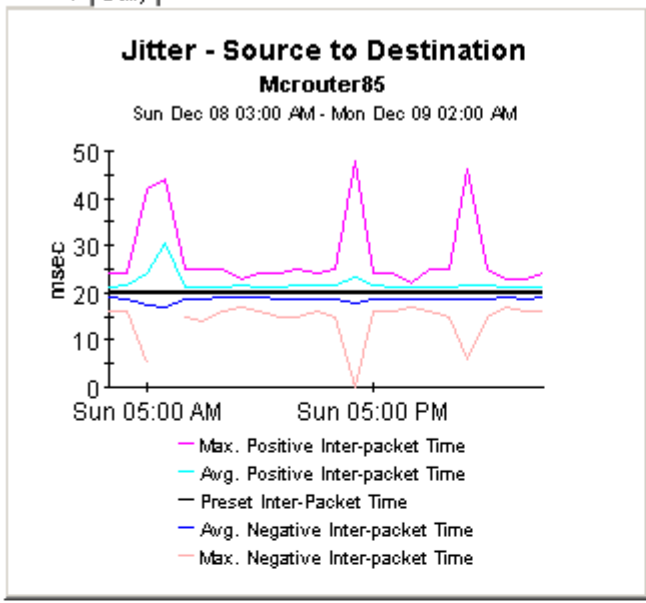


Hourly | Daily

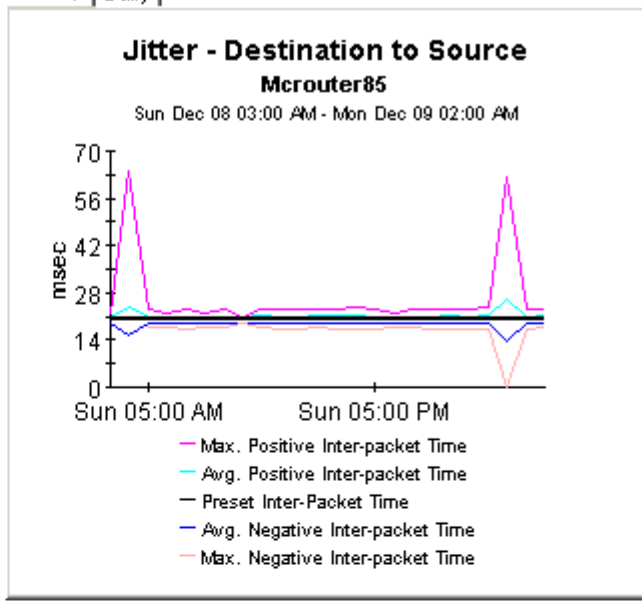




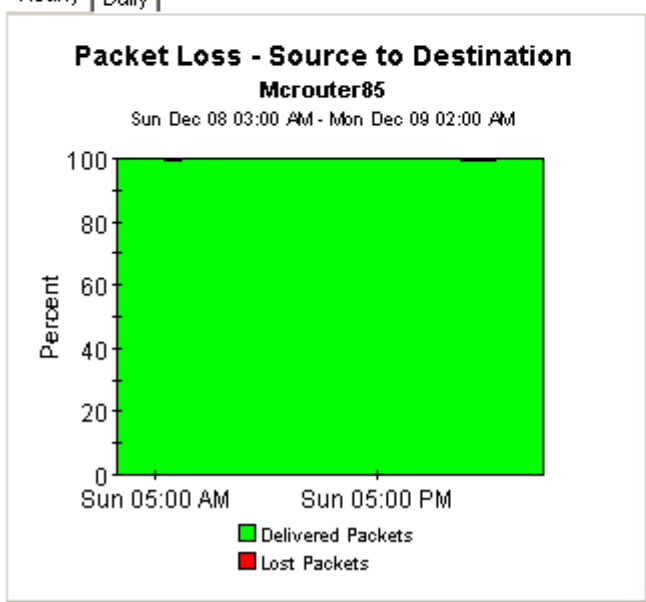
Hourly | Daily



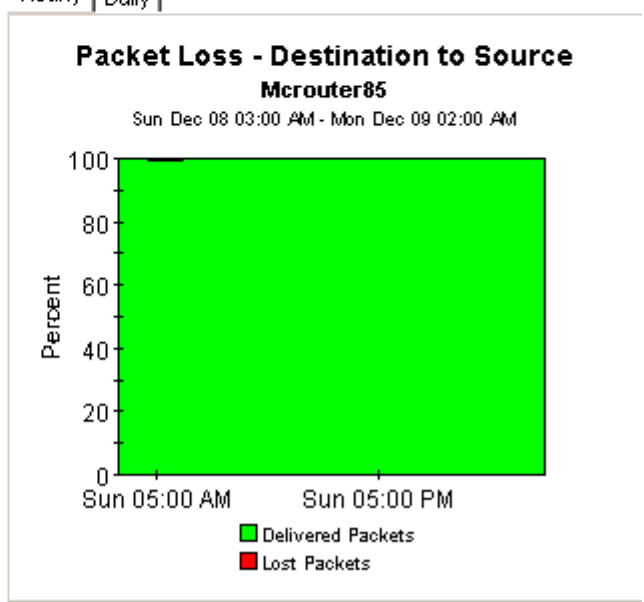
Hourly | Daily



Hourly | Daily



Hourly | Daily



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 devices 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

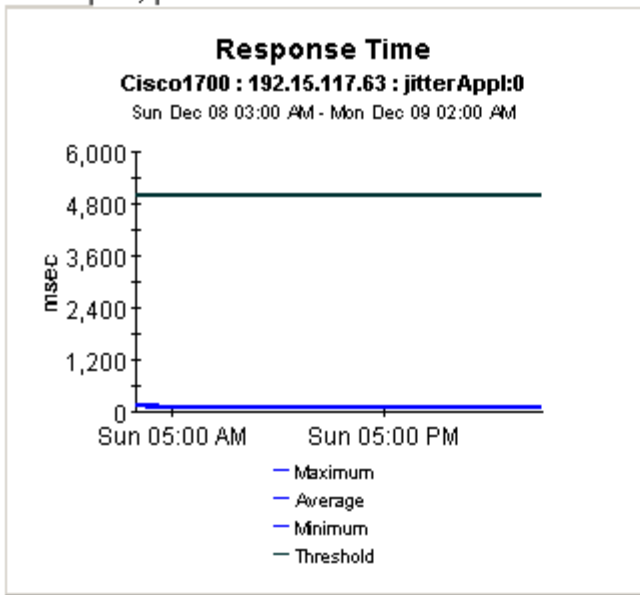
Destination Device Selection Table

Sun Dec 08 2002

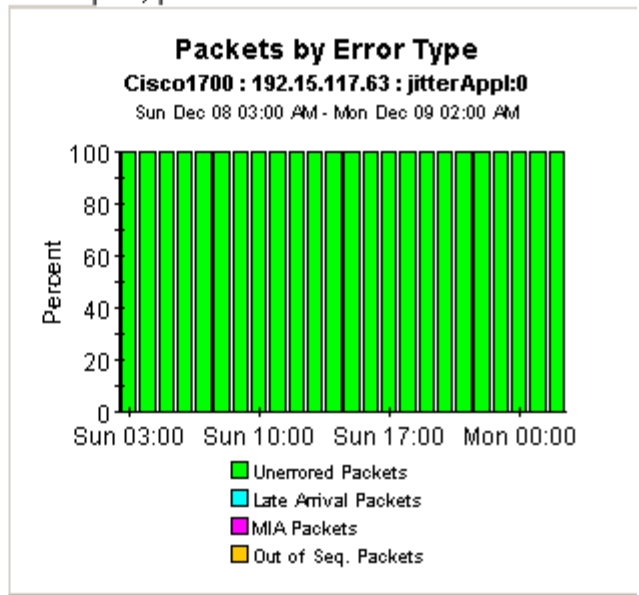
Destination	TOS	# of Transactions	Response Time (msec)	S2D Avg Dev (msec)	D2S Avg Dev (msec)	S2D Max Dev (msec)	D2S Max Dev (msec)
192.15.117.63	0	96	94.487	-2 / +2	-3 / +3	-20 / +42	-21 / +39



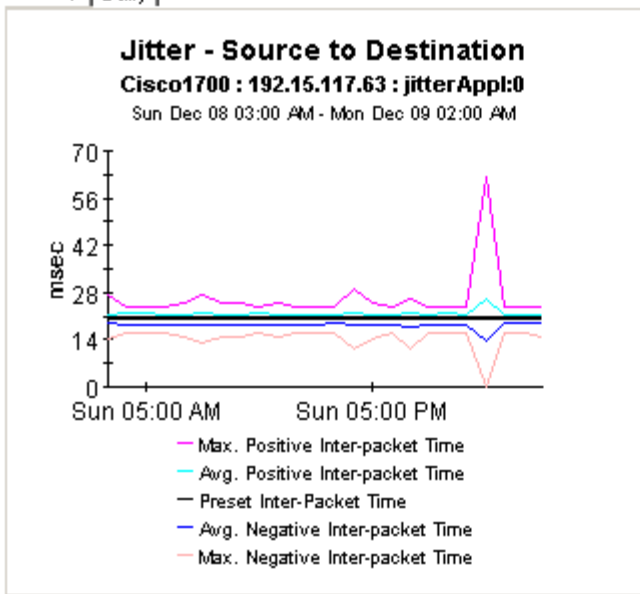
Hourly | Daily



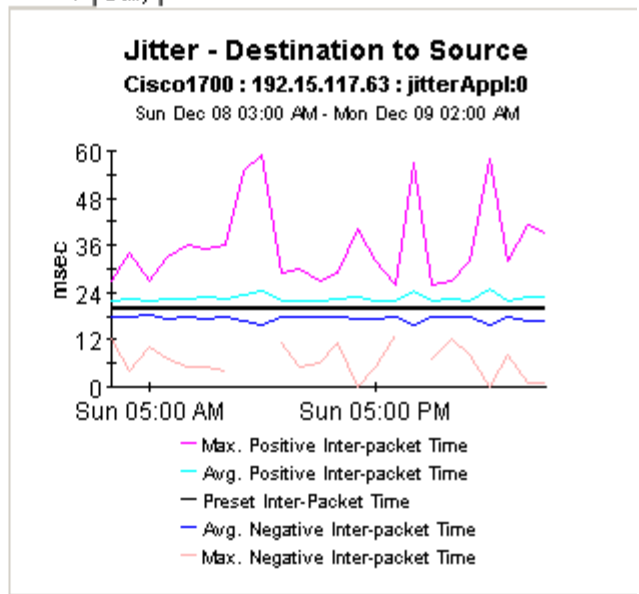
Hourly | Daily



Hourly | Daily

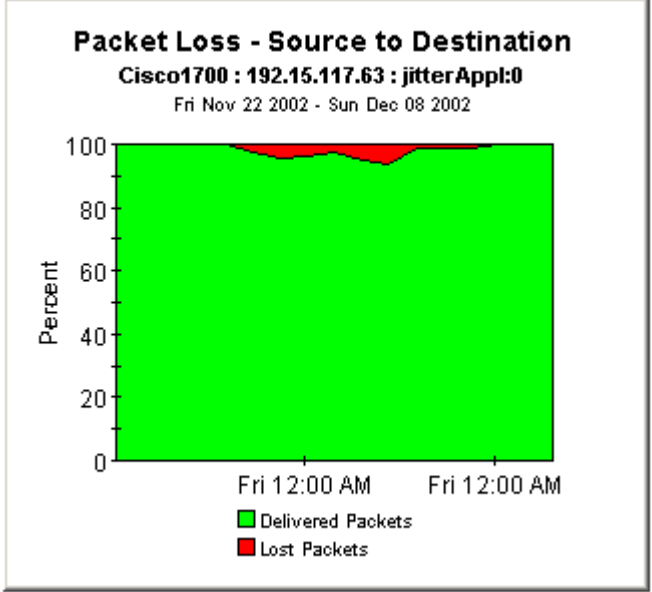


Hourly | Daily

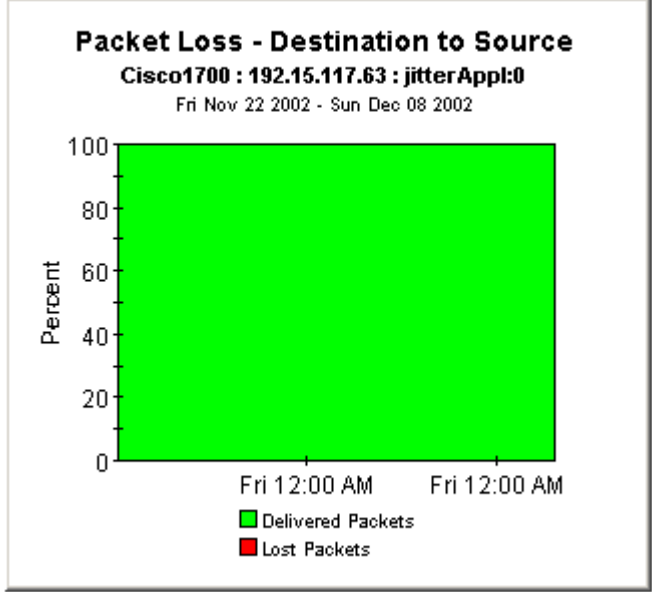




Hourly Daily



Hourly Daily



Editing Tables and Graphs

Tables and graphs can be viewed in several ways. Although the default view may be adequate most of the time, you can easily modify tables and alter the style of graphs by selecting a different view option. If you are using the Report Viewer application, right-click the object and select a different view. If you are looking at a report using the Web Access Server, click the **Edit Table** icon or the **Edit Graph** icon.

View Options for Tables

Right-clicking a table, or selecting **Edit Table**, opens a list of table view options.

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

- Set Time Period...
- Change Constraint Values...
- Select Nodes/Interfaces...
- Change Max Rows...
- View in new Frame
- Print Table...
- Export Element as CSV...
- Delete Table

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

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

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

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

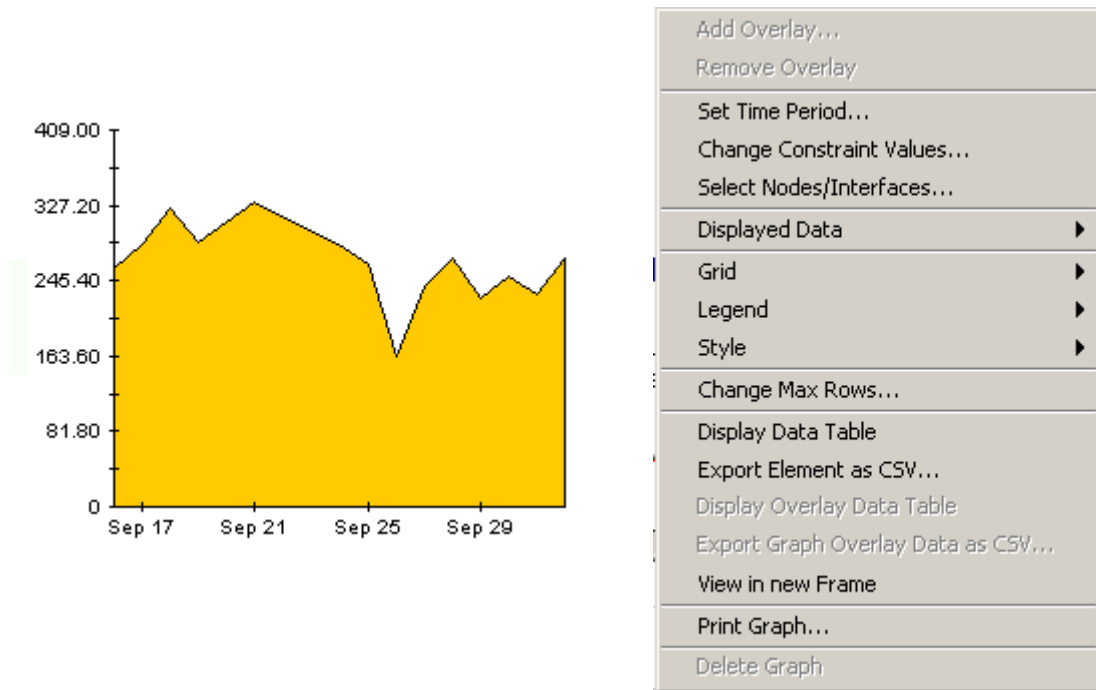
Change Max Rows increases or decreases the number of rows in a table. The default is 50. If you expand the default, the table may take more time to open. If you are trending a large network, using the default ensures that the table opens as quickly as possible.

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

Direction	IpPrecedence	Switched Bytes	Switched Pkts	Time Period
Input	0	105,668	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	800	5	Tue Oct 29 07:00 AM
Input	7	0	0	Tue Oct 29 07:00 AM
Input	0	98,334	638	Tue Oct 29 06:45 AM
Input	1	0	0	Tue Oct 29 06:45 AM
Input	2	0	0	Tue Oct 29 06:45 AM
Input	3	0	0	Tue Oct 29 06:45 AM
Input	4	0	0	Tue Oct 29 06:45 AM
Input	5	0	0	Tue Oct 29 06:45 AM
Input	6	0	0	Tue Oct 29 06:45 AM
Input	7	0	0	Tue Oct 29 06:45 AM
Input	0	97,539	648	Tue Oct 29 06:30 AM
Input	1	0	0	Tue Oct 29 06:30 AM
Input	2	0	0	Tue Oct 29 06:30 AM
Input	3	0	0	Tue Oct 29 06:30 AM
Input	4	0	0	Tue Oct 29 06:30 AM
Input	5	0	0	Tue Oct 29 06:30 AM
Input	6	120	1	Tue Oct 29 06:30 AM
Input	7	0	0	Tue Oct 29 06:30 AM
Input	0	90,744	564	Tue Oct 29 06:15 AM
Input	1	0	0	Tue Oct 29 06:15 AM
Input	2	0	0	Tue Oct 29 06:15 AM
Input	3	0	0	Tue Oct 29 06:15 AM
Input	4	0	0	Tue Oct 29 06:15 AM
Input	5	0	0	Tue Oct 29 06:15 AM
Input	6	0	0	Tue Oct 29 06:15 AM
Input	7	0	0	Tue Oct 29 06:15 AM
Input	0	103,775	658	Tue Oct 29 06:00 AM
Input	1	0	0	Tue Oct 29 06:00 AM
Input	2	0	0	Tue Oct 29 06:00 AM
Input	3	0	0	Tue Oct 29 06:00 AM
Input	4	0	0	Tue Oct 29 06:00 AM
Input	5	0	0	Tue Oct 29 06:00 AM

View Options for Graphs

Right-click any graph to open a list of view options.



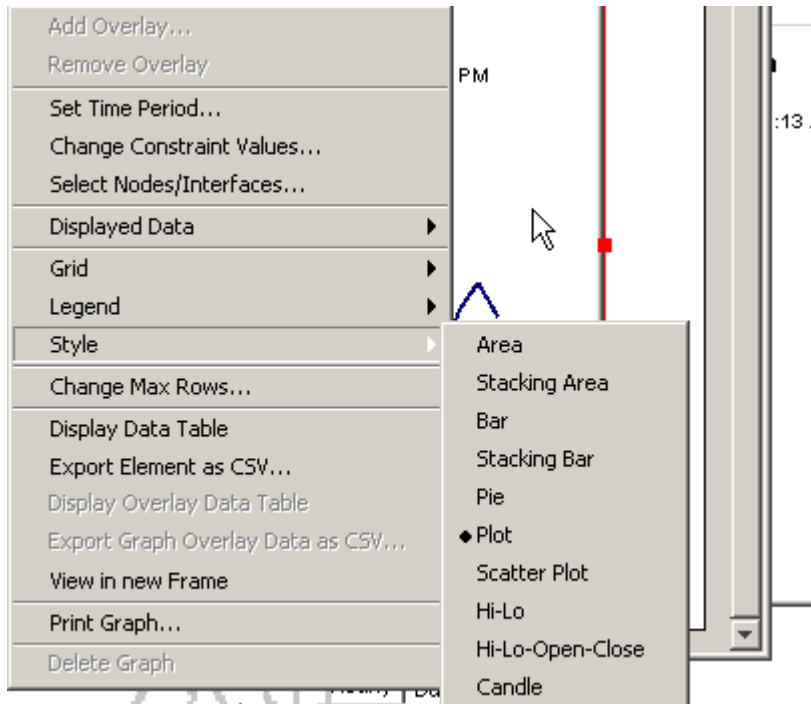
The following table provides details about each option.

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

Option	Function
Export Element as CSV...	Same as the table option shown above.
View in New Frame	Opens graph in a Graph Viewer window.
Print Graph	Same as the table option shown above.

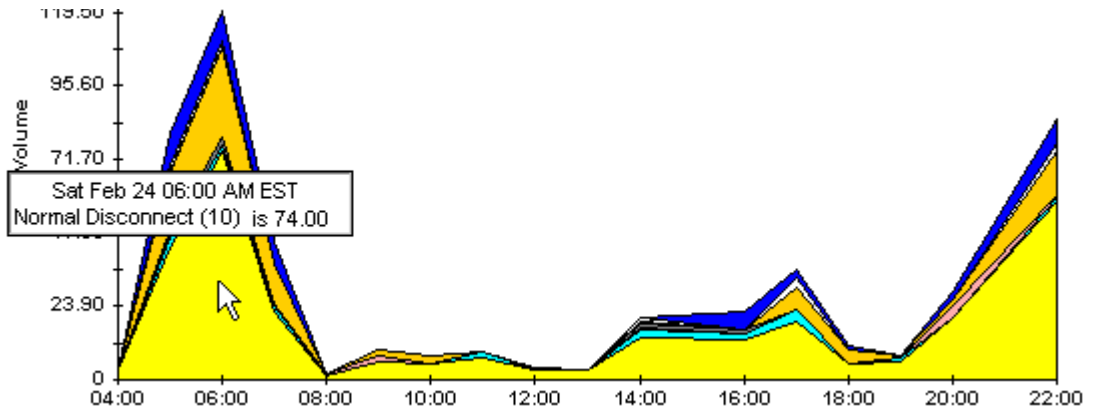
Style Options

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



Style > Area

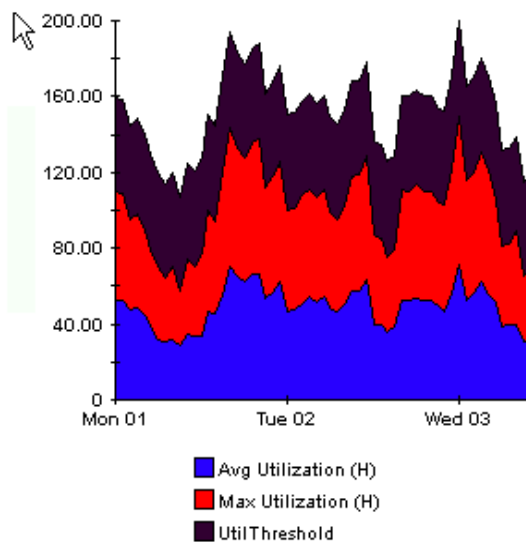
The plot or bar chart changes to an area graph. While relative values and total values are easy to view in this format, absolute values for smaller data types may be hard to see. Click anywhere within a band of color to display the exact value for that location



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

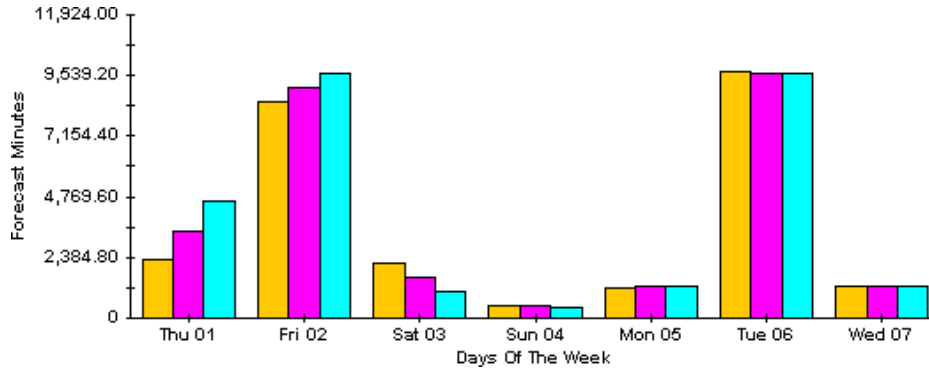
Style > Stacking Area

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



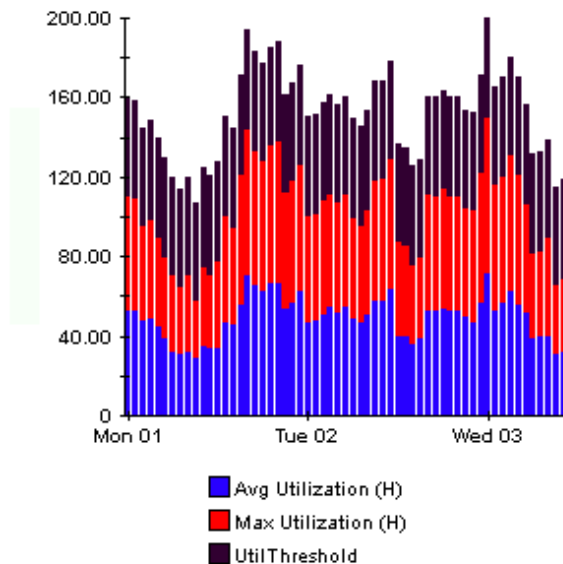
Style > Bar

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



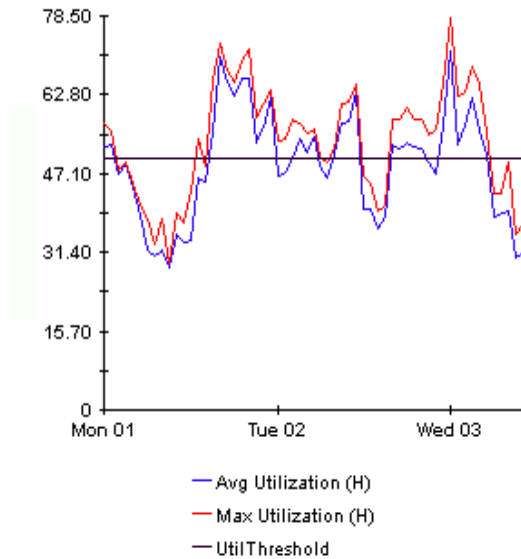
Style > Stacking Bar

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



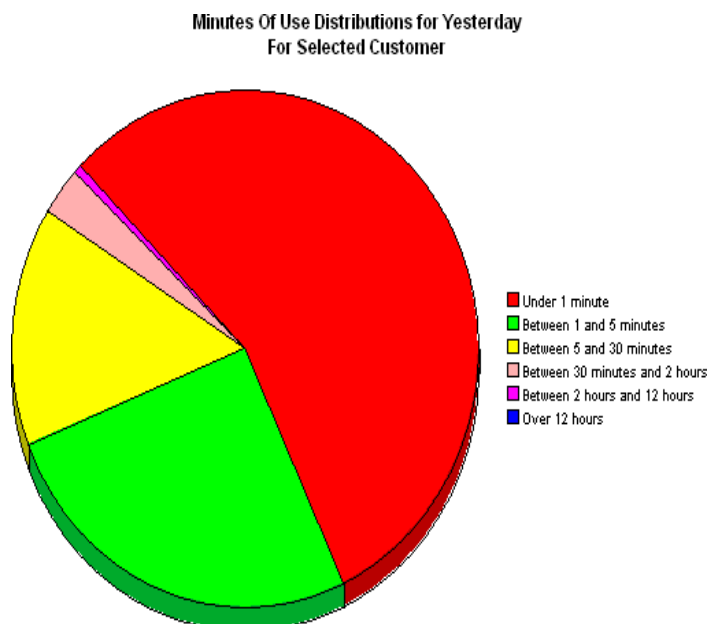
Style > Plot

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



Style > Pie

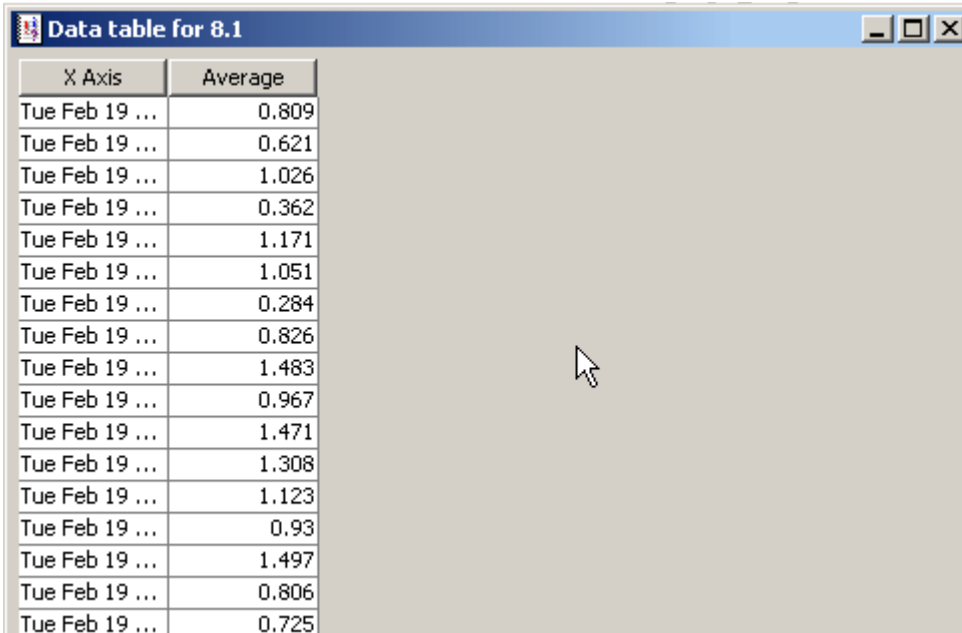
An area graph becomes a pie chart. Bands in an area graph convert to slices of a pie and the pie constitutes a 24-hour period. This view is helpful when a small number of data values are represented and you are looking at data for one day.



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

Display Data Table

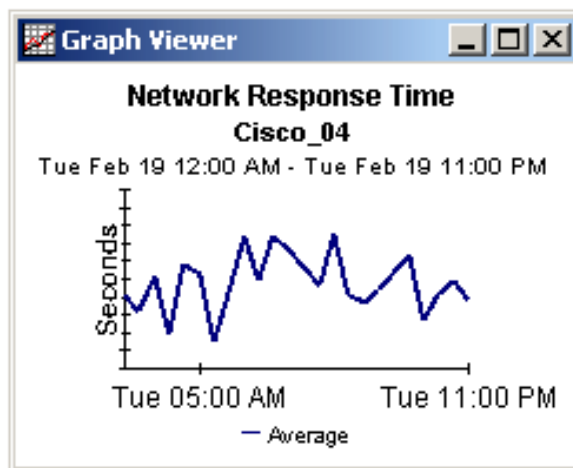
This option changes a graph into a spreadsheet.



X Axis	Average
Tue Feb 19 ...	0.809
Tue Feb 19 ...	0.621
Tue Feb 19 ...	1.026
Tue Feb 19 ...	0.362
Tue Feb 19 ...	1.171
Tue Feb 19 ...	1.051
Tue Feb 19 ...	0.284
Tue Feb 19 ...	0.826
Tue Feb 19 ...	1.483
Tue Feb 19 ...	0.967
Tue Feb 19 ...	1.471
Tue Feb 19 ...	1.308
Tue Feb 19 ...	1.123
Tue Feb 19 ...	0.93
Tue Feb 19 ...	1.497
Tue Feb 19 ...	0.806
Tue Feb 19 ...	0.725

View in New Frame

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



application

In the Service Assurance Report Pack “application” refers to any of the following SAA operations:

- UDP Echo
- UDP Jitter
- TCP Connect
- DNS
- DHCP
- HTTP
- FTP
- DLSw+

availability

Measures the percentage of successful SAA tests. Calculated by dividing the total number of successful tests by the total number of attempted tests.

baseline average

The average of all samples during the baseline period. The baseline period rolls forward daily and comprises the previous 91 days

daily

Performance for the previous 30 days. The most recent day in this view is yesterday.

destination

The destination device for an SAA test. Varies depending on the type of test. The destination is a Target Address for these tests: Echo, udpEcho, DHCP, DLSw, tcpConnect, and Jitter. The destination is a URL for FTP and HTTP tests. The destination is a Name Server for the DNS test.

day of week

A forecast, derived from baseline data, that assigns a growth rate to each day of the week.

deviation

Variation in the inter-packet delay. A positive number indicates more delay; a negative number indicates less delay.

device

Any SNMP-manageable device.

F30 / F60 / F90

Performance 30, 60, and 90 days from today. Calculated by applying linear regression to busy-hour levels over the 90-day baseline period.

growth rate

The projection for F30 divided by average busy-hour.

hourly

A view showing performance for the last two days and whatever portion of today has elapsed. The minimum time range is 48 hours; the maximum is 72 hours.

jitter

A measure of inter-packet delay variance, the difference between the expected and actual inter-packet arrival time. Jitter is an important QoS metric for voice and video applications.

location

The place where the device is located. Locations are imported using the property import interface that comes with Common Property Tables. If no locations are imported, the location field reads *unassigned*.

maximum hourly average / minimum hourly average

The maximum hourly average is determined by comparing all the hourly averages across a day and finding the hour with the highest average. The maximum hourly average is synonymous with busy hour. The minimum hourly average is determined by comparing all the hourly averages across a day and finding the hour with the lowest average. The maximum average and the minimum average are used to project future performance. Both values reflect a relatively persistent phenomenon. Because they are averages of multiple values, the value for maximum is not necessarily close to the daily peak, and the value for minimum is not necessarily close to the daily trough.

QoS

Quality of Service.

response time

The round trip time measured by the SAA test.

source

The device that initiates SAA tests. The SAA test data is polled from the source device.

throughput

The total bytes transmitted during an SAA test divided by the corresponding time. The Service Assurance Agent measures response time primarily. Throughput is a derived statistic, and should be used as an estimate, as opposed to an explicit measure of actual throughput.

threshold

The line between normal and abnormal performance. When this line is crossed, an exception is recorded. In the Service Assurance Report Pack, all exceptions are response time exceptions.

ToS

Type of Service

traffic

The total number of bytes sent and received by the source device.

transaction

An instance of an SAA test.

A

alarm severity, **34**
 application, **91**
 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**
 availability, **91**

B

baseline average, **91**

C

change max rows option, **85**
 Cisco IOS Command Line Interface, **27**
 CiscoSAA_Config, **27**
 CiscoSAAConfig.pl, **27**
 CiscoSAAConfig.xml, **27**
 Cisco SAA Datapipe, **11, 24, 27**
 CiscoSAADelete.pl, **27**
 Cisco SAA NRT Datapipe, **8**
 Cisco VPN Solution Center, **29**
 Common Property Tables, **16, 22**
 configuring SAA operations, **11**
 configuring source routers, **34**
 customer-specific reports, **12**
 Customer Top Ten, **61**

D

daily, **91**

day of week, **91**
 defining an SAA operation, **28**
 demo package, **23**
 destination, **91**
 Destination Exception Report, by Location/
 Application, **37**
 Destination Exception Report, by Source/
 Application, **37**
 Destination Forecast, **55**
 Destination Summary, **47**
 Destination Top Ten, **61**
 deviation, **91**
 device aggregations, **33**
 DHCP, **91**
 Display Data Table, **85**
 displayed data option, **85**
 distributed systems, **16, 21**
 DLSw, **91**
 DNS, **91**

E

Echo, **91**
 exception reports, **37**

F

F30, **92**
 F60, **92**
 F90, **92**
 forecast reports, **55**
 FTP, **91**

G

graph view options, **83**
 grid options, **85**

group filters, **12, 33**

growth rate, **92**

H

History Table (MIB), **8**

hourly view, **92**

HTTP, **91**

J

jitter, **92**

Jitter Near Real Time - Latest Test, **67**

Jitter Summary Report, **75**

L

Latest Test Table (MIB), **8**

legend options, **85**

location, **92**

Location Exception Report, by Source/Destination,
37

M

maximum hourly average, **92**

MPLS VPN Aware, **8**

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**

P

Product Manuals Search, **13**

pulling rate data from satellite servers, **32**

R

report parameters, **12, 34**

response time, **92**

S

sample data, **67**

satellite servers, **33**

script syntax for CiscoSAA_Config, **28**

Service_Assurance, **24**

Service_Assurance_Daily.pro, **33**

Service_Assurance_Hourly.pro, **32**

Service_Assurance_Locations (module), **24**

Service_Assurance_Thresholds (module), **24**

Source Exception Report, by Application/
Destination, **37**

Source Summary by Application/Destination, **47**

style options for graphs, **85**

summary reports, **47**

system clocks, **33**

T

table view options, **83**

tcpConnect, **91**

threshold, **92**

threshold conditions, **34**

throughput, **92**

top ten reports, **61**

traffic, **93**

transaction, **93**

trendcopy pull commands, **32**

U

udpEcho, **91**

UPGRADE_Service_Assurance_2_to_3, **19**

Use Absolute Time, **83**

V

view in new frame, **84**