HP OpenView Performance Insight

Report Pack for Cisco Ping
User Guide

Software Version: 4.0

Reporting and Network Solutions

April 2004

Legal Notices

Warranty

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

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

Restricted Rights Legend

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

Hewlett-Packard Company
United States of America

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

Copyright Notices

Trademark Notices

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

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

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

UNIX® is a registered trademark of The Open Group.

Windows® and Windows NT® are U.S. registered trademarks of Microsoft® Corp.

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:

- Troubleshooting information
- Patches and updates
- Problem reporting
- Training information
- Support program information
- Product manuals

contents

Overview

This chapter covers the following topics:

*   OVPI and Ping Tests: Adding Context to Test Results
*   The Action Poller — a special collection mechanism
*   Error messages in trend.log
*   Ways to customize Cisco Ping reports
*   Sources for additional information

> ➤ Version 4.0 of the Cisco Ping Report Pack requires OVPI 5.0. Version 4.0 of the Cisco Ping Report Pack has not been ported to Oracle. Version 4.0 supports Sybase database software only.

OVPI and Ping Tests: Adding Context to Test Results

If you measure latency and reliability, you should be able to measure how well a network is performing. If latency is high, packets are not moving from source devices to destination devices as quickly as possible. If reliability is low, packets are not reaching their intended destination. The conventional approach to measuring latency and reliability is to conduct ping tests and watch for poor results. However, since the surrounding network is hidden from view, the results you get from ping tests tend to be inconclusive.

The Cisco Ping Report Pack overcomes this problem by showing latency and reliability in context. The surrounding network is in view, providing a clear picture of the conditions behind high latency and low reliability. Furthermore, the load on an interface is no longer guesswork. Cisco Ping reports will tell whether the load on the source router interface is about the same as the load on the destination router interface, or whether the load on the source router interface is completely different from the load on the destination router interface.

Cisco Ping reports will also enhance your SLA monitoring capability. If latency breaches a threshold while utilization is high, our reports will qualify that event as a non-SLA breach. If latency or reliability crosses a threshold while utilization is low, our report will qualify these events as SLA breaches.

An Overview of Reports

Following is a brief description of the reports in Cisco Ping 4.0.

Executive Summary. Daily and hourly performance across all pairs. Displays aggregates for the 95th percentile Round Trip Time and the Packet Delivery Ratio.

Forecast. Ranks the worst performing pairs by daily 95th percentile Round Trip Time or by total daily Packet Delivery Ratio. Drill down to baseline values, a daily summary, and projections for F30, F60, and F90.

Worst Performing Pairs. Ranks pairs by daily 95th percentile Round Trip Time and by Packet Delivery Ratio. Drill down to see interface utilization and CPU utilization for the previous day.

Daily QuickView/Daily Snapshot. Ranks node pairs by RTT and delivery and provides analysis of recent RTT and recent delivery; shows rolling baseline and rolling F30 forecast. Drill down to hourly interface and CPU utilization.

Threshold Near Real Time QuickView/Threshold Near Real Time Snapshot. A rolling summary of the previous six hours showing 95th percentile Round Trip Time and Packet Delivery Ratio. Drill down to interface and CPU utilization.

Threshold Daily QuickView. Ranks node pairs by threshold breaches, shows recent Packet Delivery Ratio, recent Round Trip Time, and compares rolling baseline to rolling F30 calculations. Drill down from summary information to hourly utilization data.

Threshold Summary Daily/Threshold Summary Monthly. Provides daily and monthly totals for threshold breaches for every node pair. Shows threshold settings, exception details, SLA qualifications in effect at the time of the exception; tracks changes in the daily SLA threshold count and daily non-SLA threshold count for the last 30 days.

Version History: 3.0 and 4.0

Version 3.0 of the Cisco Ping Report Pack was released October 2003. Version 3.0 installed on OVPI 4.6 and took advantage of object management and forms support capability introduced in OVPI 4.6. Version 3.0 included the following forms.

*   Configure Collection Group

    Create a collection group containing a list of related Cisco Ping device pairs.

*   Configure Device Pairs

    Add new Cisco ping source and destination device pairs to a collection group.

*   Create Device Pair Parameters

    Create new parameters for a device pair. Parameters pertain to parameter count, package size, package timeout, and delay.

*   Update Device Pair Parameters

    Modify the parameters created using the create parameters form.

*   Update Thresholds

    Modify the following threshold values:

    —   *RTT*

    —   *Discard*

— *CPU utilization*

— *Interface utilization*

Version 4.0 was released in April 2004. Version 4.0 does not contains new forms or new reports. The enhancements in version 4.0 pertain to compatibility with OVPI 5.0. The user will not have any direct interaction with these enhancements.

Integration with Network Node Manager

If the preliminary work of integrating OVPI with Network Node Manager has already taken place, the Cisco Ping package will integrate smoothly with the fault management capabilities of Network Node Manager. There are two ways that the NNM operator will come into contact with the reports in the Cisco Ping package:

Scenario 1. Cisco Ping sends a threshold trap to NNM. The NNM operator sees an alarm in the NMM alarm browser. The NNM operator can respond to that alarm by launching the Cisco Ping Near Real Time report.

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

• NNM ovw

• Home Base Dynamic Views

• NNM alarm browser

The Action Poller — A Special Collection Mechanism

Most OVPI report packs use a collection mechanism that collects data from single nodes, is built into OVPI, and operates transparently. The Cisco Ping Report package is different. It has its own collection mechanism—the Action Poller—that collects data from pairs of nodes as opposed to single nodes. Before collection can take place, you need to define node pairs using the Action Poller User Interface.

Guidelines for a Successful Collection

Action Poller collections are governed by the following rules and restrictions:

• A node pair consists of a source node and a destination node. Source and destination nodes must be discovered. Source and destination nodes that have been discovered will be filtered by the Action Poller User Interface into lists for selection.

• The source node is required to be a Cisco router that supports the Cisco Ping MIB or is currently running the Cisco Ping agent, IOS 10.2 or later.

• The write community string for the source node must be correct.

• The Action Poller will perform an SNMP set on the source node. If the SNMP set fails, the node pair collection will fail.

• The destination node must be an SNMP device.

- Any node that is unreachable, unavailable, or not properly configured will generate an error message in the {DPIPE_HOME}\OVPI\log\trend.log file.

> ► Re-indexing events that affect the interfaces on a device should be tracked through the datapipe that is being used to inherit node instance information. Analyze and track these events as necessary.

MIBs and Metrics

Every polling cycle, the Action Poller collects ping statistics once and interface and CPU statistics twice. The sequence is:

1 Collect interface and CPU utilization data.

2 Collect ping test data.

3 Collect interface and CPU utilization data.

The Action Poller collects data from the following MIBs:

- Cisco Ping MIB
- Cisco System MIBlet
- Interface Reporting Basic Info MIBlet

The Action Poller returns the following metrics:

- Average round trip time
- Minimum round trip time
- Maximum round trip time
- Packet delivery ratio
- Interface utilization
- CPU utilization

The following factors influence the metrics returned by the Action Poller:

- CPU load on the source node
- CPU load on the destination node
- Competing user traffic on node interfaces
- Packet size
- Network configuration
- Network load

By configuring Cisco Ping MIB parameters and the frequency of polling, you can collect metrics that simulate the delay experienced by user traffic between node pairs. By correlating delay samples with other metrics, you can determine which factors are contributing to delay.

> ► You cannot set various Ping MIB parameters on the source node or initiate pings unless the write community string is correctly specified. Use Polling Policy Manager to modify the write community string on specific nodes.

Packet Delivery Ratios

A source node that supports a ping MIB can be instructed (by means of SNMP SET requests) to send a defined series of ping messages to a destination node. The source node logs the following metrics:

- Number of attempted pings

- Number of successful pings

- Round trip delay (min, max, and average) for successful pings

If the number of successful pings is less than the number of attempted pings in the ping sequence, one of the nodes in the node pair, or possibly the network in between, discarded the ping request or the returning ping response. Several factors can cause a ping to be unsuccessful:

- Network delay that exceeds the configured ping timeout on the source node

- High CPU load on either the source or destination node

- High traffic loads on the interfaces and/or sub-interfaces of either the source or destination node competing with the ping traffic

- Packet size—larger packets are more susceptible to discard

- The network configuration—including traffic management, buffer sizes, or line speeds among other factors

- Network load—congested links, congested switching, and routing resources

Factors that influence network delay can also influence the network discard rate. In general, depending on how the network is configured to handle queuing and traffic management, overutilization of bandwidth or processing resources can cause delay and discards.

By configuring the Cisco Ping MIB parameters and sampling frequency, you can collect metrics that represent the general delivery/discard characteristics of the traffic between node pairs. You can also correlate packet delivery ratios with other metrics, such as CPU load or buffer size, and determine why packets are being discarded.

Route Availability

If no ping in a given sample is successful, then either connectivity between the source and destination node was unavailable, or the destination node was unavailable when the test took place. An unavailable route can be caused by any of the following:

- Network configuration error—routing, firewalls, proxies, and so on

- Chronic network congestion—packet discard ratio at 100%

- Network/PVC failure

- Remote node is down

By configuring Cisco Ping MIB parameters and the frequency of sampling, you can collect data to compute representative availability on the routes between node pairs. You can also routinely poll the source and destination nodes at the time of the ping sampling. This will tell you whether nodes, or the network between the nodes, is causing an availability problem.

Error Messages in trend.log

Not all of the errors that appear in the trend.log are in fact errors. Several messages are in the log for informational purposes only and can be ignored. Here are the various categories of messages than can be ignored:

- Messages produced during package installation that refer to tables that are dropped and then recreated. If a table does not exist, and there is an attempt to drop the table, a message will be generated.

- Messages produced when the object SQL script attempts to load certain database objects that have already been loaded by the Common Property Tables package.

- Messages produced during each polling cycle. Here are a few examples of messages written during each polling cycle:

```
2004-03-15 14:30:59:000,Eastern Standard Time,-
5:00,bcpfile,,ERROR,2572,2668,0,"DB_ERR 0, OS_ERR 0, SEVERITY 0, SPID 0,
dbErrStr [DataDirect][ODBC Sybase Wire Protocol driver]No upload tables exist,
using original table Risco_ping_rtd_, osErrStr 01000"
```

```
2004-03-15 14:30:59:000,Eastern Standard Time,-
5:00,bcpfile,,ERROR,2572,2668,0,"Failing command"
```

```
2004-03-15 14:30:59:000,Eastern Standard Time,-
5:00,bcpfile,,ERROR,2572,2668,0,"{call dsi_lock_upload_table_p(?, ?, ?, ?, ?)}"
```

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 group of users, whereas when you edit a table, graph, or parameter you are making a temporary change to individual reports. For more information about view options for tables and graphs, see Chapter 15, 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 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.*

Report Parameters

Editing a parameter applies a constraint to the report. The constraint filters out data you do not want to see. If you edit the Customer Name parameter, data for every customer except the customer you typed in the Customer Name field will drop from the report. Similarly, if you edit the Location Name, data for all locations except the location you typed in the Location Name field will drop from the report. Cisco Ping 4.0 supports the following parameters:

- Customer_Name
- Customer_Id
- Location_Name
- Location_Id
- Source
- Destination

Not all reports support every parameter. 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 the Cisco Ping package and any known issues, refer to the *Cisco Ping Report Pack 4.0 Release Statement*. You may also be interested in the following documents:

- *Interface Discovery Datapipe 2.0 User Guide*
- *Thresholds Module 5.0 User Guide*
- *Performance Insight / Network Node Manager Integration Module User Guide*
- *Performance Insight / Network Node Manager Integration Module Release Notes*
- *RNS 5.0 Release Notes, March 2004*

Manuals for the core product (OVPI) and manuals for the reporting solutions that run on the core product can be downloaded from the following web site:

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

Select **Technical Support** > **Product Manuals** to reach the **Product Manuals Search** page. User guides for the core product are listed under **Performance Insight**. User guides for report packs, datapipes, and preprocessors are listed under **Reporting and Network Solutions**.

The manuals listed under **Reporting and Network Solutions 5.0** indicate 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 an older PDF that may no longer be current.

2

The Upgrade Install

This chapter covers the following topics:

- Guidelines for a smooth upgrade

- Using Package Manager to install the upgrade package

- Package removal

If you installed Cisco Ping 3.0 on OVPI 4.6 and then upgraded to OVPI 5.0, you have the option of upgrading to Cisco Ping 4.0. If you are installing Cisco Ping for the first time, see Chapter 3, The New Install.

Guidelines for a Smooth Upgrade to Version 4.0

The RNS 5.0 distribution includes NNM solution components as well as OVPI solution components, and when you select OVPI components for installation, the install script copies every OVPI package to the Packages directory on your system. Once the extract process is complete, you will be prompted to start the Package Manager install wizard. Before getting to that step, review the following guidelines.

Prerequisites for the Upgrade

The following software must already be installed before upgrading from Cisco Ping 3.0 to Cisco Ping 4.0:

- OVPI 5.0

- Any OVPI 5.0 Service Pack available for installation

- Cisco Ping Report Pack 3.0

- Interface Discovery Datapipe 2.0

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

Distributed Environments

If you are running Cisco Ping in a distributed environment, the central server, every satellite server, and every remote poller must be running OVPI 5.0. Following is an overview of the upgrade procedure for a distributed environment:

1   Disable trendcopy on the central server.

2   Remove the previous release of the Interface Discovery Datapipe.

3   Install the upgrade package for the report pack; deploy reports.

4   Install these package simultaneously:

   •   Thresholds sub-package (optional)

   •   The latest release of the Interface Discovery Datapipe

5   For each satellite server:

   a   Remove the previous release of the Interface Discovery Datapipe.

   b   Install the upgrade package for the report pack; do **not** deploy reports.

   c   Install these packages simultaneously:

      –   Thresholds sub-package (optional)

      –   The latest release of the Interface Discovery Datapipe

6   Enable trendcopy on the central server.

Integration with NNM: Threshold Alarms

If you have already integrated OVPI with NNM, you will probably want to install the optional thresholds sub-package, Ping_MIB_Threshold, on the OVPI server. If this package is installed, threshold breaches spotted by OVPI will show up in the NNM Alarms Browser, allowing the NNM operator to launch the Near Real Time report.

The thresholds sub-package cannot operate unless the Threshold and Event Generation Module, commonly known as the Thresholds Module, is also installed. If you are not running any version of the Thresholds Module, let Package Manager install the latest version for you, automatically. If you are running version 4.0, you must upgrade to version 5.0.

Upgrading Cisco Ping 3.0 to Cisco Ping 4.0

Perform the following tasks to upgrade Cisco Ping 3.0 to Cisco Ping 4.0:

•   Task 1: Extract packages from the RNS 5.0 CD

•   Task 2: Uninstall Interface Discovery Datapipe 1.1

•   Task 3: Install Interface Discovery Datapipe 2.0

•   Task 4: Install UPGRADE_Cisco_Ping_3_to_4

•   Task 5: Install the thresholds sub-package (optional)

Task 1:   Extract Packages from the RNS 5.0 CD

Follow these steps to copy OVPI packages from the RNS 5.0 CD to the Packages directory on your system:

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 distribution CD. On Windows, a Main Menu displays automatically; on UNIX, mount the CD if the CD 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 extract is complete, the install script starts Package Manager. The Package Manager welcome window opens.

Once the copy to the Package directory is complete, you have the option of navigating to the Packages directory to see the results. Under the Ping MIB folder, you will see the following folders:

* Ping_MIB.ap
* Ping_MIB_Demo.ap
* Ping_MIB_Thresholds.ap
* UPGRADE_Ping_MIB_3_to_4.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; selection tables are linked to graphs, and you may experiment with view options for individual tables and graphs.

Task 2:   Uninstall the Interface Discovery Datapipe 1.1

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

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

3   Click the **Uninstall** radio button.

4   Click **Next**. The Report Undeploy window opens.

5   Click the check box next to the following packages:

   IFEntry_Disc_Datapipe 1.1

   IR_ifEntry_Datapipe 1.1

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

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

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

Task 3: **Install the Cisco Ping 3.0 to 4.0 Upgrade Package**

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

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

3 Click 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_Ping_MIB_3_to_4

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 the install finishes, a package 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 from Package Manager. Package Manager displays what you just installed as *Cisco Ping 4.0*. This is not an error.

Task 4: **Install the Thresholds Sub-Package and restart OVPI Timer**

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

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

3 Click 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 Disable the option to Deploy Reports.

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

8 Click the check box next to the following packages:

Cisco_Ping_Thresholds

9 Click **Next**. The Type Discovery window opens. Disable the default and click **Next**. The Selection Summary window opens.

10 Click **Install**. The Installation Progress window opens and the install begins. When the install finishes, a package install complete message appears.

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

12 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 remove the Cisco Ping Report Pack.

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

2   Stop OVPI Timer and wait for processes to terminate.

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

> *UNIX*: As root, do 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 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:

> *Ping_MIB*

> *Ping_MIB_Thresholds* (if installed)

> *Ping_MIB_Demo* (if installed)

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

9   Click **Uninstall.** The Progress window opens and the removal begins. When the removal finishes, a package 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, do one of the following:

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

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

3

The New Install

This chapter covers the following topics:

- Guidelines for a smooth installation
- Using Package Manager to install Cisco Ping 4.0
- Options for viewing reports
- Package removal

> Cisco Ping 4.0 does not support Oracle. Version 4.0 supports Sybase only.

Guidelines for a Smooth Installation

The RNS 5.0 CD includes NNM solution components as well as OVPI report packs. When you select OVPI report packs for extraction, the install script extracts every OVPI package to the Packages directory on your system. Once the extract process is complete, the install script will prompt you to start the Package Manager install wizard. Before you get to that step, review the following guidelines.

Prerequisites for Installing Cisco Ping 4.0

The following software must already be in place before installing Cisco Ping 3.0:

- OVPI 5.0, with any available Service Packs for OVPI 5.0
- Interface Discovery Datapipe 2.0

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

> The Interface Discovery Datapipe is a prerequisite for the IRifEntry Datapipe. If you are running IRifEntry Datapipe 1.1, remove it and install IRifEntry_Datapipe 2.0.

Distributed Environments

If you are running Cisco Ping in a distributed environment, the central server, every satellite server, and every remote poller must be running OVPI 5.0. Following is an overview of the installation procedure for distributed environments:

Central Server

1   Uninstall the previous release of the Interface Discovery Datapipe.

2   Install the following packages simultaneously:

   •   Cisco Ping; deploy reports

   •   Thresholds sub-package (optional)

   •   The latest release of the Interface Discovery Datapipe

Each Satellite Server

1   Remove the previous release of the Interface Discovery Datapipe

2   Install the following packages simultaneously:

   •   Cisco Ping; do not deploy reports

   •   Thresholds sub-package (optional)

   •   The latest release of the Interface Discovery Datapipe

Integration with NNM: Threshold Alarms

If you have already integrated OVPI with NNM, you will probably want to install the optional thresholds sub-package, Cisco_Ping_Thresholds, on the OVPI server. If this package is installed, threshold breaches spotted by OVPI will show up in the NNM Alarms Browser.

The thresholds sub-package cannot operate unless the Threshold and Event Generation Module, commonly known as the Thresholds Module, is also installed. You may be running the previous version of the Thresholds Module. If you are running the previous version, you must upgrade to the latest release. For more information about recent enhancements to this package, refer to the *Thresholds Module 5.0 User Guide*.

Installing Cisco Ping 4.0

Perform the following tasks to install Cisco Ping 4.0:

•   Task 1: Extract packages from the RNS product distribution CD

•   Task 2: If you are running the Interface Discover Datapipe 1.1, remove it.

•   Task 3: Install these packages simultaneously:

   —   Cisco_Ping

   —   Cisco_Ping_Thresholds

   —   Cisco_Ping_Demo (optional)

—　IFEntry_Disc_Datapipe 2.0

—　IRifEntry_Datapipe 2.0

Task 1:　Extract Packages from the RNS CD to the Packages directory on your system

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, do 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 if the CD 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 welcome window opens.

Once the copy to the Package directory is complete, you can navigate to the Packages directory to see the results. Under the Ping_MIB folder you will see the following folders:

•　Ping_MIB

•　Ping_MIB_Thresholds

•　Ping_MIB_Demo

•　UPGRADE_Ping_MIB_3_to_4

The UPGRADE package does not apply to you. 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; selection tables are linked to graphs, and you may experiment with view options for individual tables and graphs.

Task 2:　Uninstall the Interface Discovery Datapipe 1.1

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

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

3　Click the **Uninstall** radio button.

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

5　Click **Next**. The Package Selection window opens. Click the check box next to the following packages:

IR_ifEntry_Datapipe 1.1

Interface_Discovery_Datapipe 1.1

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

7　Click **Uninstall.** The Progress window opens and the removal begins. When the removal finishes, a package removal complete message appears.

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

Task 3:   Install Cisco Ping 4.0, associated datapipes, and restart OVPI Timer

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

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

3   Select 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. Click the check box next to the following packages:

> *Cisco_Ping 4.0*
>
> *Cisco_Ping_Thresholds*
>
> *Cisco_Ping_Demo*
>
> *IRifEntry_Datapipe 2.0*
>
> *IFEntry_Disc_Datapipe 2.0*

9   Click **Next**. The Type Discovery window opens. Accept the default and click **Next**. The Selection Summary window opens.

10   Click **Install** to begin the installation process. The Installation Progress window opens and the install begins. When the install completes, a package install complete message appears.

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

12   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, Cisco Ping 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 components are installed on your system, you have access to Report Viewer, Report Builder, and the Management Console. If the client component was not installed on your system, you are restricted to viewing reports on the web.

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

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 remove Cisco Ping 4.0.

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, do 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   Select **Uninstall** and click **Next**. The Report Undeployment window opens.

6   Click **Next**. The Package Selection window opens. Click the check box next to the following packages:

  Cisco_Ping

  Cisco_Ping_Thresholds (if installed)

  Cisco_Ping_Demo (if installed)

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

8   Click **Uninstall.** The Progress window opens and removal begins. When removal finishes, a package removal complete message appears.

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

10 Restart OVPI Timer.

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

 UNIX: As root, type one of the following:

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

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

Action Poller User Interface

This chapter covers the following topics:

- Launching the interface
- Defining node pairs
- MIBlet groups
- Assigning instances to nodes
- Modifying parameter sets
- Terminating the interface

Launching the Interface

The Action Poller User Interface resides in the $DPIPE_HOME/bin directory. To invoke the interface, type the following command at the command prompt:

Windows: `action_config`

UNIX: `action_config.sh`

The Configure Action Poller window opens. If any collection group, including the default Cisco Collection, has already been defined, it will appear in this window.

To add a new collection group, click **New**. To modify an existing collection group definition, highlight the collection you want to modify and click **Modify**. The New Action Collection Group window opens. Follow these steps to define a collection group:

1 Enter the collection group name in the Collection Group field. If you are modifying an existing collection group definition, the name is displayed in the Collection Group field and the field is grayed out.

2 After the configuration is complete, enter the name of the host on which the Action Poller is to run in the Poller Name field.

3 After the new or modified collection is finished, click **Save** and then click **Node Pairs** to open the Node Pair Properties window.

The Action Poller can be configured for distributed polling. For example, you can define collection group_1 to run on poller A, collection group_2 to run on poller B, and so on. During the initial configuration, you can leave the Poller Name set to the value of hostname.

Defining Node Pairs

Highlight any node pair on the Node Pair Properties screen and click the **Remove** button to modify the list of current node pairs assigned to the collection. You may also remove all node pairs. Clicking **Add** opens the Add Node Pairs window.

All nodes that are known to OVPI appear in the Available Nodes list box. If the nodes you want to select are not listed, use Polling Policy Manager to add them and perform a type discovery from the command prompt using the command: **trend_discover -t**

Follow these steps to add a new node pair to the collection group:

1   From the Add Node Pairs window, highlight one node that is to be a source node in the Source Nodes list box. The source node must be a Cisco Router capable of performing an SNMP set.

2   Click **Make Source** to assign the node to the Source Node text box.

3   Select one node that is to be a destination node from the Destination Nodes list box.

4   Click **Make Destination** to assign the node to the Destination Node list box. You can select several destination nodes for a single Source Node to quickly make node pairs using the same Source Node.

5   Click **Make Pairs** to pair the selected source node with each node that is listed in the Destination Nodes list box.

   The node pairs you define are added to the New Node Pairs list box at the bottom of the window. The same node can be the source node of one or more pairs and the destination node of one or more pairs. Each distinct pair of nodes can only be added once per collection. If you want to collect data from different interfaces on the nodes, set up a new collection with the same pair of nodes.

   If you want to remove a node pair from the new node pairs list box, highlight the node pair and click **Remove Node Pair**. The selected pair is removed from the Source-Destination list.

6   Continue to create as many node pairs as you want to assign to this particular collection group. When you are done, click **Add Node Pairs**. To exit, click **Close**.

MIBlet Groups

A *MIBlet group* is a named set of MIBlets that you want to collect as a group at a source or destination node. The Cisco Ping Report Pack always uses the Cisco collection MIBlet and cannot be modified. This group comprises the following two MIBlets:

•   interface_rtd_png_

•   xcpu_util_rtd_png_

These MIBlets correspond to the following standard OVPI MIBlets:

•   interface-reporting_basic_interface_info

•   cisco_system

Assigning Instances to Nodes

Use the Node Pair Properties window to assign the appropriate instance to the source and destination nodes of each node pair you defined. Multiple instances of MIBlet objects can be collected from a node depending on the nature of the MIBlet. An instance corresponds to a unique interface on the node. For example, a separate instance of the interface-reporting_basic_interface_info MIBlet is collected for each interface on a node.

Other MIBlets, such as the cisco_system MIBlet, are collected at the node (rather than interface) level, and return a single set of values for the node. Data that is interface-specific will not be collected if an instance has not been assigned.

Follow these steps to assign source and destination collection instances for each node pair:

1   Highlight a node pair in the list box.

2   The MIB-2 Interface Source and Destination instances are initially set to NULL, indicating that the MIBlet instances to be collected for the source and destination nodes have not been assigned yet.

3   The instances of the selected MIBlet that can be collected for the source and destination nodes of the selected pair appear in the Source MIBlet Instances and Destination MIBlet Instances list boxes, respectively.

> Instance data is inherited from the GENMIB2IF Datapipe or the Interface Discovery Datapipe. Unless one of these datapipes has collected at least two poll cycles of data, the list boxes will contain no instances. You may also import property information, in batch fashion, to add and modify node pair information.

4   Select the source instance to be collected by clicking the instance listed in the Source Node Instances list box.

5   Click **Assign Source**. Note that the selected instance is displayed in the *Src Inst* column of the Source and Destination Instance Info list box.

6   Select the destination instance to be collected by clicking the instance listed in the Destination Node Instances list box.

7   Click **Assign Destination Instance**.

8   Repeat this procedure to assign the appropriate source and destination instance of each MIBlet associated with each node pair you have assigned to this collection group.

9   Click **Save** when finished.

Modifying Parameter Sets

To modify parameter sets, click the **Parameter Sets** button on the Node Pair Properties window and perform any of these tasks:

•   Modify an existing parameter set

•   Create a new parameter set

•   Remove a parameter set

You may assign the parameter set to an individual node pair or all node pairs. Close the window when finished by clicking **Close**.

The following table defines each parameter and indicates what you can specify.

Parameter	Description
Packet Count	Number of packets to send during each ping action. Specify from 1 to 2147483647 (2 GB).
Packet Size	Number of bytes in each packet. Specify from 1 to 2147483647 (2 GB).
Packet Timeout	Milliseconds to wait for a reply from the destination node. Specify from 0 to 3600000.
Delay	Milliseconds to wait between ping actions. Specify from 0 to 3600000.

Terminating the Interface

There are two ways to terminate the interface:

- Click the **Close** button on the initial collection window, or
- Select **File > Exit**

Any specifications you have made up to that point will be saved as part of the current collection group.

Configuration Options

This chapter provides information about the following configuration options:

- Configuring servers in a distributed system
- Provisioning the property table
- Action Poller command line options
- Changing the collection interval

Configuring Servers in a Distributed System

If you are about to run Cisco Ping in a distributed system, you have already installed the report pack on the central server and on each satellite server. You also deployed reports once, from the central server. Now that installation is complete, you need to perform the following tasks:

- Set up connections between the central server and each satellite server database
- At the central server, configure trendcopy pull commands for hourly data
- At each satellite server, disable daily summaries

In addition to performing these tasks, verify that the system clock on the central server is synchronized with all other system clocks, and make sure that you do not have two servers polling the same device.

> The following steps apply to new installations only. If you just upgraded to Cisco Ping 4.0, and your servers were already configured for operation as a distributed system, those settings are still in effect.

Configuring the Central Server

Follow these steps to configure the central server:

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.

8 Configure trendcopy pull commands from the central server to each remote satellite. Do this by editing the {DPIPE_HOME}/scripts/Ping_MIB_Sum.pro file. Make sure that you add all the trendcopy commands you need, and make sure that each command includes the correct name for the satellite server.

9 Comment out the hourly summary. This function belongs to satellite servers.

10 Modify the Ping_MIB_Sum.pro trendtimer entry as shown in the {DPIPE_HOME}/scripts/ Ping_MIB_Sum.pro file. Changing the start time will prevent the central server from pulling data from satellite servers when they are busy summarizing data.

Configuring a Satellite Server

Follow these steps to configure a satellite server.

1 Install Sybase, OVPI 5.0, the Interface Discovery Datapipe and the Cisco Ping Report Pack.

2 Switch off summaries above the hourly level by editing the $DPIPE_HOME/lib/ trendtimer.sched file; comment out the line referencing Ping_MIB_Daily.pro.

3 Comment out the trendcopy pull commands in the {DPIPE_HOME}/scripts/ Ping_MIB_Sum.pro file. Uncomment the hourly summary.

4 Make sure that the system clock on each satellite server is synchronized with the system clock on the central server.

Provisioning the Property Table

Provisioning the property table is optional. If you want to aggregate data by customer or by region, or change default threshold settings, provisioning is mandatory. If you are a service provider and you want to share your reports with customers, provisioning is mandatory. Threshold values are already defaulted, so provisioning those values is necessary only if you want to modify the default.

If you do not want to use the Action Poller User Interface to enter node pairs, consider using the property provisioning mechanism. As the property table is provisioned, any node pairs that already exist will have customer and threshold information updated. If the node pair does not exist, it will be created. You should use the interface to delete node pairs.

> If you do not provision the property table, the term *unassigned* will appear in any list of customers or regions.

This section covers the following topics:

• K_IFEntry_Disc table

• action_property_table file

- Format of the import file
- Changing defaults
- Initializing property tables

K_IFEntry_Disc Table

The Cisco Ping Report Pack looks for the K_IFEntry_Disc property table. This table is created by the Interface Discovery Datapipe. *However, you are not required to use this particular property table or the Interface Discovery Datapipe.* If desired, a different property table from another report pack or datapipe can be used instead.

The Cisco Ping Report Pack can inherit interface information from the GENMIB2IF_ifentry Datapipe. If that is what you want to happen, the correct name of the property table to place in the action_property_table file is K_GENMIB2IF_ifentry. Once the Action Poller user interface has launched, interfaces that have not been discovered, and interfaces that have no collected interface data, will not display node instance information.

action_property_table

The Cisco Ping Report Pack will look for the action_property_table file in the {DPIPE_HOME}\OVPI\lib directory. The contents of the action_property_table file must contain the exact name of the correct property table. Make sure the name for the action_property_table file does not include a file extension such as .txt.

Format of the Import File

While interface instance information can be inherited from the Interface Discovery Datapipe, the following properties must be imported manually using the provisioning interface:

- Customer
- Region
- Round Trip Time Threshold Values
- Packet Delivery Ratio Threshold Values
- Interface Utilization Threshold Values
- Interface CPU Utilization Values

To import this information, create a flat file that contains property information and then import the file. Follow these steps:

1 Create a property import file using the format described below.

2 Give the file this name: Ping_MIB_Property.dat

3 Place the file in the following directory:

```
{DPIPE_HOME}/Packages/PING_MIB/Ping_MIB.ap/PropertyData
```

> This file, which will not be deleted or moved, may also serve as a record of "node ping pairs" currently associated with property data. If you wish to add "node ping pairs" modify this file and save it to the same directory specified above. The process runs daily and will not affect existing property values. Be aware that duplicate "node ping pairs" may cause undesirable results in the assignment of property data values.

Your property import file is a tab-delimited file. There are no column headings. When you create it, be sure to include all the columns listed in the table below and be sure the sequence of your columns left to right follows the sequence in the table top to bottom.

Seq	Column Name	Description
1	src_rtr_name	Source node name
2	src_cpu_instance	CPU instance for the source node
3	src_if_instance	Source node interface instance
4	dst_rtr_name	Destination node name
5	dst_cpu_instance	CPU instance for the destination node
6	dst_if_instance	Destination node interface instance
7	cust_id	Unique integer value for each customer
8	customer_name	Customer name associated with cust_id
9	region_id	Unique integer value for each region
10	region_name	Region name associated with region_id
11	rtt_threshold	Round trip time threshold in milliseconds
12	discard_threshold	Packet discard percentage (0-100) threshold
13	interface_threshold	Interface utilization threshold
14	cpu_threshold	CPU threshold

If you are unsure of the format or the import is failing, consider exporting existing property information from OVPI. Edit the file exported by OVPI, then re-import the new file.

Changing Defaults Related to Property Import

The default directory for property data files, the location where the import utility will look for your edited files, is specified by the SourceDirectory path. This path appears in the following TEEL file:

```
Ping_MIB_Property.teel
```

If you are changing the default directory *before* you install the Cisco Ping Report Pack, you can locate the TEEL files in the Ping_MIB.ap directory. If you want to change the default directory *after* running Package Manager, you must change the path information in two directories:

- Ping_MIB.ap
- {DPIPE_HOME}/lib

SourceDisposition

The default for SourceDisposition is *keep*. Keeping the existing file in place allows the administrator to identify existing ping pairs that are already provisioned. The disposition of this file is determined by a directive in the Ping_MIB_Property.teel configuration file. If desired, you may elect to have the file moved or deleted.

SourceDirectory

To change the SourceDirectory, do the following:

1 Create the new source directory.

2 Navigate to the appropriate directory (see the discussion in the preceding section about which directories are involved) and open the directory.

3 Double-click the Ping_MIB_Property.teel file.

4 Locate the SourceDirectory default path. (The line beginning with `SourceDirectory =`)

5 Change the path, replacing the existing path with the complete path name to the new directory; begin the new path name just after the equal sign (=).

> Leave the file filter as specified in the original SourceDirectory.

Export Directory

To change the default export directory, modify the export data process file. If you are making this change before you install the package, you have to make this modification once, in the Ping_MIB.ap directory. If you are making this change after you run Package Manager, you must make this modification in two places:

- Ping_MIB.ap
- {DPIPE_HOME}/scripts

Follow these steps to change the default export directory:

1 In the Ping_MIB.ap directory double-click the Ping_MIB_exportdata.pro file.

2 Locate the three trend_export statements; beginning at the bracket after the **-o**, replace the existing path with the complete path to the new directory.

3 Only if necessary, that is, only if you have already installed this package, navigate to the {DPIPE_HOME}/scripts directory and make the same changes you made to Ping_MIB_exportdata.pro.

Initializing Property Tables

You must initialize the property tables only if you are not already collecting data from the Interface Reporting Basic Info MIBlet and the Cisco System MIBlet. The Action Poller UI will show instance information only if the property table has been initialized. To initialize the property information, create a dummy poll that collects an instance of the designated MIBlets from each interface on the nodes that you want to participate in Action Poller collections. The easiest way to do this is to perform the following steps:

> ➤ Unless you are adding new nodes to a collection group, you must initialize the property tables with the appropriate MIBlet instances for each new node that you add.

1 Using the OVPI Polling Policy Manager, set up a view that contains all nodes that are to participate in Action Poller collections.

2 Set up a dummy polling policy for that view.

3 Invoke the mw_collect utility from the command prompt with the following command:

```
mw_collect -i 15
```

> ➤ Replace "15" with the polling interval you chose when you created the collection policy.

4 Deactivate the dummy polling policy after the mw_collect utility has completed the poll.

Action Poller Command Line Options

You can invoke the Action Poller from the command line or have OVPI Timer invoke it through an entry in the trendtimer.sched file. The command has the following syntax:

action   [**-c** *child_processes*]

[**-d** *debug_level*]

[**-h**]

-i *polling_interval*

[**-p** *port*]

[**-r** *retries*]

[**-s** *round_factor*]

[**-t** *timeout*]

[**-V**]

The action command has the following options:

-c   Specifies the number of concurrent child action poller processes to run. The Action poller starts one child process for each node pair. The processing power of the host determines the value you specify for this option. The default is 20.

-d   Debug level. Valid values are 0, 1, 2, or 3. The higher the number, the more detailed the debug output. The default is 0, which means no debug output. Debug output is written to the standard out. Keep in mind this option will cause additional overhead.

-h   Displays the command line options (help).

-i   Polling interval. Each collection group that has the specified polling interval will be collected during this invocation of the Action poller.

-p   Port number for SNMP sessions. The default is 161.

-r   The number of collection retries to attempt for each SNMP session. The default is -1, which means the default number of tries configured for SNMP.

-s   This option rounds off the collection time (ta_period). If the Action poller kicks off a collection at 3:07, and if you are using the default collection option of 300 seconds (5 minutes), the actual ta_period value for the collection will be recorded as 3:05.

-t   The collection timeout, in seconds, for SNMP sessions. The default is -1, which means the default timeout configured for SNMP.

-V   Displays the version stamp for action.

         This option is in UPPERCASE.

Changing the Collection Interval

When you install the Cisco Ping Report Pack, the following entry is placed in the trendtimer.sched file:

```
15 - - {DPIPE_HOME}/trend_proc -f {DPIPE_HOME}/scripts/Ping_MIB_poll.pro
```

This statement will execute all Cisco Ping collections every 15 minutes. To alter the interval for the collections from the default of 15 minutes, simply change 15 to the desired interval. In the following example, the new interval is 60:

```
60 - - {DPIPE_HOME}/trend_proc -f {DPIPE_HOME}/scripts/Ping_MIB_poll.pro
```

This will leave all the node pairs in the same group, but change the interval that the collection is performed. Do not make any changes through the Polling Policy Manager. Currently, all collections will be executed using the same time interval.

Forms: Configure, Create, Update

This chapter provides samples of the following forms:

- Configure Collection Group
- Configure Device Pairs
- Create Device Pair Parameters
- Update Device Pair Parameters
- Update Threshold Values

Only two forms in this group, the Update Device Pair Thresholds form and the Update Threshold Values form are accessible from the Management Console. Both of these forms are context sensitive, which means that the only nodes you will be modifying are the nodes you selected before launching the form. The other forms must be loaded using the Builder or Viewer applications.

To reach the Update Device Pair Parameters form, or the Update Threshold Values form, click the **Objects** icon on the left side of the Management Console. The Object Management window opens, showing nodes along the left side of the window, and various types of tasks listed down the right side of the window.

- The Update Device Pair Parameter form is listed under **General Tasks**
- The Update Threshold Values is listed under **Object Specific Tasks**

See below for illustrations of all five forms.

Cisco Ping
Configure Collection Groups

A collection group contains a list of related Cisco Ping device pairs. This form can be used to create or update Cisco Ping collection groups. To add or remove node pairs into a collection group use the "Cisco Ping Configure Device Pairs" form.

Available Collection Groups

Group Name	Poller Name	Polling Interval
Cisco collection	ovpihpt2	15
Cisco collection1	ovpihpt2	15

Collection Group Name	Cisco collection
Poller Name	ovpihpt2
Polling Interval	15

OK   Apply   Cancel

C:\ovpi\packages\Ping_MIB\Ping_MIB.ap\Cisco_Ping_forms\config_dev_pairs.frep

Cisco Ping
Configure Device Pairs

Use this form to add new Cisco Ping device pairs to a Cisco Ping collection group. The new device pair should be assigned interface and CPU instances and a parameter set. The "Cisco Ping Collection Groups" form can be used to define new collection groups. For creating or updating the device pair parameters, use the "Create Device Pair Parameters" and "Update Device Pair Parameters" forms, respectively.

Choose Collection Group

Cisco collection ▼

Available Device Pairs for the selected Collection Group

Source Node	Destination Node
15.6.96.2	15.6.96.7

Cisco Ping Source	15.6.96.2 ▼	**Cisco Ping Destination**	default ▼
Src IF Instance	FastEthernet0 ▼	**Dst IF Instance**	0 ▼
Src CPU Instance	1	**Dst CPU Instance**	1

		Pkt Cnt	Pkt Size	Pkt Timeout	Delay
Src Parameters	1 ▼	5	100	2000	0

		Pkt Cnt	Pkt Size	Pkt Timeout	Delay
Dst Parameters	1 ▼	5	100	2000	0

OK   Apply   Cancel

C:\ovpi\packages\Ping_MIB\Ping_MIB.ap\Cisco_Ping_forms\create_dev_pair_params.frep

Cisco Ping
Create Device Pair Parameters

Use this form to create new device pair parameters. New parameter_id is automatically assigned for the newly created row.

parameter_id	packet_count	packet_size	packet_timeout	delay
1	5	100	2000	0
2	10	500	3000	50

Packet Count	5	Packet Size	100
Packet Timeout	2000	Packet Delay	0

OK   Apply   Cancel

Cisco Ping

Update Device Pair Parameters

Use this form to update the device pair parameters. Please note that changing the an existing device pair paramtere would affect all the existing device pair that use the updated device pair parameters.

parameter_id	packet_count	packet_size	packet_timeout	delay
1	5	100	2000	0
2	10	500	3000	50

Packet Count `5`   **Packet Size** `100`

Packet Timeout `2000`   **Packet Delay** `0`

OK   Apply   Cancel

C:\ovpi\packages\Ping_MIB\Ping_MIB.ap\Cisco_Ping_forms\update_thresholds.frep

Cisco Ping

Update Threshold Values

Use this form to update various threshold values like Round Trip Time, Discard, Interface and CPU Threshold.

Threshold Values

Source	Destination	Sample ID	RTT Threshold	Discard Threshold	Interface Threshold	CPU Threshold
default		0	1,000.00	5.00	50.00	70.00
15.6.96.2	15.6.96.7	1	1,000.00	5.00	50.00	70.00
15.6.96.2	15.6.96.41	2	1,000.00	5.00	50.00	70.00
15.6.96.7	15.0.152.2	3	1,000.00	5.00	50.00	70.00

Source	default
Destination	
Sample ID	0
RTT Threshold	1,000.00
Discard Threshold	5.00
CPU Threshold	50.00
Interface Threshold	70.00

OK   Apply   Cancel

7

Worst Performing Node Pairs

The Worst Performing Pairs report looks at yesterday's activity and provides two views of "worst":

- Node pairs ranked by worst round trip time

- Node pairs ranked by worst packet delivery ratio

You may investigate any node pair in more detail by drilling down to yesterday's hourly data in the tabbed graphs and finding out exactly when RTT went up, or when the delivery ratio went down, and whether or not these events took place when utilization was high or when utilization was low.

The tabbed graphs track these metrics:

- Average hourly round trip time

- Hourly packet delivery ratio

- Source CPU utilization and destination CPU utilization

- Source interface utilization and destination interface utilization

RTT is measured in milliseconds; the delivery ratio is a percentage. A sample report follows.

Cisco Ping
Worst Performing Node Pairs

The Worst Performing Node Pairs Report provides separate charts ranking the worst performing node pairs by round trip time (RTT) and by packet delivery ratio respectively. Drilling down to either chart shows the detailed metrics for the node pair collected over the previous day. Select a customer (left) and a node pair (right) to get the drill down information.

Worst Performing Node Pairs, Ranked by Round Trip Time

Customers	Node Pair	RTT	Delivery Ratio
All			
Unassigned Customer	amsterdam.desktalk.com -> atlanta.desktalk.com	127.00	92.34
	sanjose.desktalk.com -> sydney.desktalk.com	19.00	92.55
	sanjose.desktalk.com -> london.desktalk.com	18.00	92.81
	sanjose.desktalk.com -> chicago.desktalk.com	18.00	92.71
	sanjose.desktalk.com -> newyork.desktalk.com	17.00	92.95
	sanjose.desktalk.com -> lasvegas.desktalk.com	15.00	92.19

RTT | Delivery | CPU Utilization | Interface Util.

Average Round Trip Time
amsterdam.desktalk.com -> atlanta.desktalk.com
Mon Sep 30 12:00 AM

— Avg. RTT
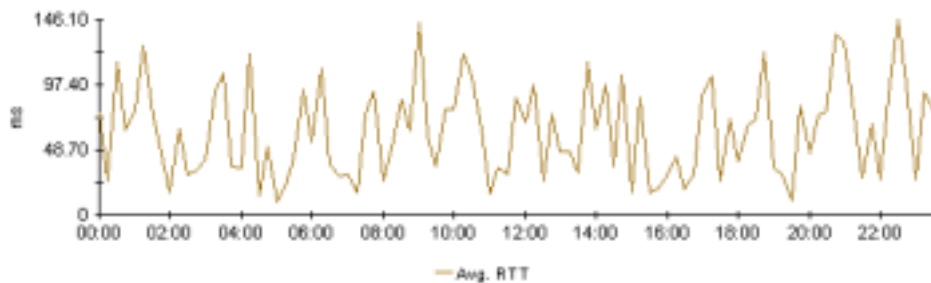
Worst Performing Node Pairs, Ranked by Packet Delivery Ratio
Mon Sep 30 2002

Node Pair	RTT	Delivery Ratio
sanjose.desktalk.com -> newyork.desktalk.com	17.00	92.95
sanjose.desktalk.com -> london.desktalk.com	18.00	92.81
sanjose.desktalk.com -> chicago.desktalk.com	18.00	92.71
sanjose.desktalk.com -> sydney.desktalk.com	19.00	92.55
amsterdam.desktalk.com -> atlanta.desktalk.com	127.00	92.34
sanjose.desktalk.com -> lasvegas.desktalk.com	15.00	92.19

8

Daily QuickView/Daily Snapshot

The Daily QuickView provides a rolling daily summary. Constrained by customer, this report highlights the node pairs with the highest round trip times for any given customer. This is a rolling summary because it shows you how the baseline average and the F30 forecast are changing from day to day.

The Daily Snapshot (not illustrated) is a subset of the Daily QuickView, but otherwise the reports are identical. Open the Daily Snapshot and you will be able to select the node pairs you want included in the report.

The list of node pairs at the top of the report indicates the average RTT and the delivery ratio. Select a node pair to display the following graphs:

• Daily RTT and daily delivery ratio

• Baseline to F30 comparison for RTT and delivery ratio

• Hourly metrics for RTT, delivery, CPU utilization, and interface utilization

The QuickView shows latency and reliability metrics side by side. It also provides the context you need to understand what the latency and reliability data points to. You can see whether the packet delivery ratio is also affected, and you have the surrounding network in view. As a result you now know whether poor ping test results are taking place when CPU and interfaces utilization is higher than usual, lower than usual, or average.

A sample of the Daily QuickView follows.

Cisco Ping

QuickView

The QuickView Report provides a rolling daily summary of 95th percentile round trip time values, or daily packet delivery ratio for the selected customer (left) and the node pair (right). The Top 10 daily samples for the selected node pair are displayed for the chosen timespan, allowing the RTT/Delivery metrics to be visually correlated with the corresponding CPU and interface utilizations.

Customers

All

Unassigned Customer

Node Pairs

sanjose.desktalk.com -> lasvegas.desktalk.com

sanjose.desktalk.com -> sydney.desktalk.com

sanjose.desktalk.com -> london.desktalk.com

sanjose.desktalk.com -> chicago.desktalk.com

amsterdam.desktalk.com -> atlanta.desktalk.com

sanjose.desktalk.com -> newyork.desktalk.com

RTT | Delivery |

Round Trip Time - Daily 95th Percentile
sanjose.desktalk.com -> lasvegas.desktalk.com
Fri Sep 13 2002 - Mon Sep 30 2002
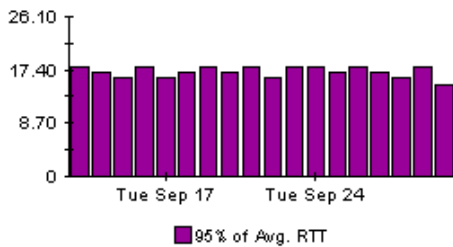
■ 95% of Avg. RTT

RTT: BL & F30 | Delivery: BL & F30 |

Baseline & 30-Day Forecast RTT (P95)
sanjose.desktalk.com -> lasvegas.desktalk.com
Fri Sep 13 2002 - Thu Sep 19 2002

■ Baseline Delay
■ 30-Day Forecast Delay
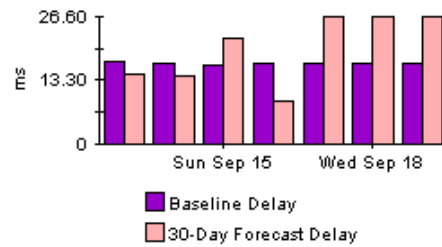
RTT | Delivery | CPU Utilization | Interface Util. |

Top 10 Round Trip Time Samples for Selected Node Pair
sanjose.desktalk.com -> lasvegas.desktalk.com
Mon Sep 30 12:00 AM

■ Avg. RTT

9
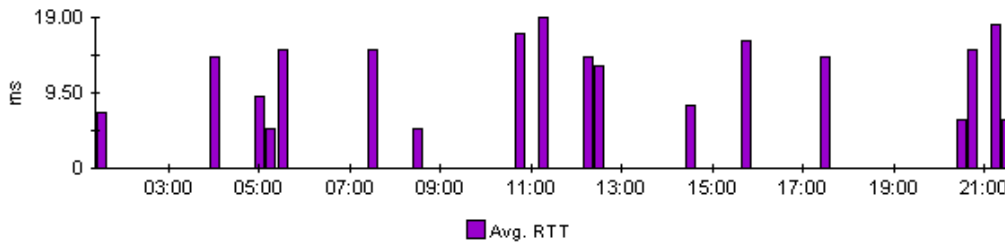
Sample Data in Near Real Time

Near Real Time provides access to sample data collected over the last six hours. This report is available in two flavors, QuickView and Snapshot. Use the QuickView when specific node pairs are not of interest; use the Snapshot when you want to zero in on specific node pairs.

The NRT QuickView tells you which node pairs are reporting the highest number of threshold breaches. The selection table lists node pairs, sorted highest count to lowest count, and also lets you do a quick comparison of SLA breaches to non-SLA breaches. If you see a total that causes concern, you can drill down on the node pair and take a closer look at:

• RTT over the last six hours

• Delivery ratio over the last six hours

• CPU utilization

• Interface utilization

This closer look will let you see actual breaches as well as near breaches. If the SLA breaches are low, then you should see utilization above the SLA Qualification Threshold; if the SLA breaches are high, you should see utilization below the SLA Qualification Threshold.

A sample of the Thresholds NRT QuickView follows.

Cisco Ping

QuickView -- Near Real Time

The QuickView Near Real Time Report displays the 95th percentile round trip time and packet delivery ratio for the selected customer (left) and node pair (right) over the over the last six hours period and provides a visual correlation with the corresponding CPU and interface utilizations.

Customers	Node Pairs
All	sanjose.desktalk.com -> lasvegas.desktalk.com
Unassigned Customer	sanjose.desktalk.com -> sydney.desktalk.com
	sanjose.desktalk.com -> london.desktalk.com
	sanjose.desktalk.com -> chicago.desktalk.com
	amsterdam.desktalk.com -> atlanta.desktalk.com
	sanjose.desktalk.com -> newyork.desktalk.com

RTT │ Delivery │

Round Trip Time for Selected Node Pair
sanjose.desktalk.com -> lasvegas.desktalk.com
Tue Oct 01 06:52 PM

— Avg. RTT
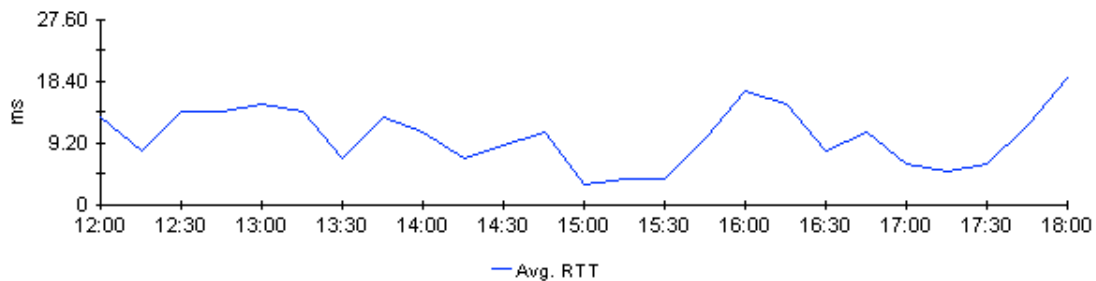
CPU Utilization │ Interface Util. │

CPU Utilization for Selected Node Pair
Tue Oct 01 06:52 PM

— CPU Utilization : sanjose.desktalk.com

10
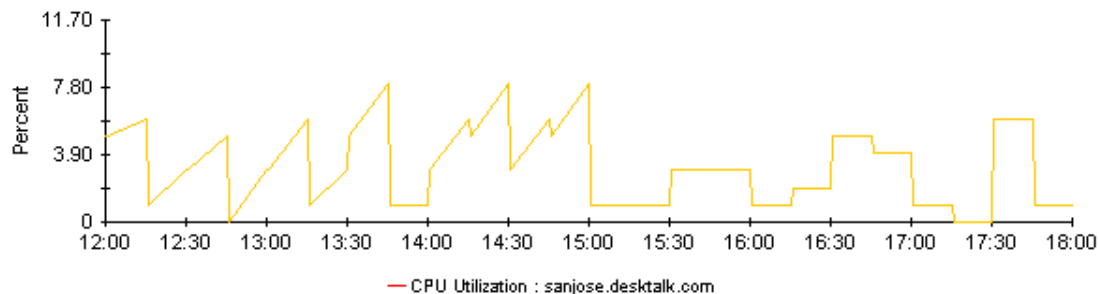
Threshold Daily QuickView

The Threshold Daily QuickView provides a close-up view of yesterday's performance, showing which node pairs had the highest number of response time and discard breaches. Like the two reports discussed in Chapter 8, this is a rolling summary because it calculates the baseline average and the F30 forecast every day and shows how the baseline average and F30 forecast are changing from day to day.

If you want to see how yesterday's activity compares to recent activity, look at the RTT and Delivery graphs. These graphs will tell you whether yesterday's breach count was an isolated incident or part of a trend that has been building over time. You will also see how the average and P95 values compare to the threshold.

The baseline and F30 graphs show whether conditions are getting better or worse. You may see a steady increase in the F30, a steady decrease, or little change. If you see a decrease in the F30, then yesterday's breach activity may be an isolated incident.

The tabbed graph at the bottom provides an hourly analysis of yesterday's activity and tells you exactly when performance crossed the threshold, causing a threshold breach to occur. If these graphs indicate low utilization when the RTT or delivery breach took place, it's likely that SLA breaches took place.

A sample of the Threshold Daily QuickView follows.

Cisco Ping

Performance Threshold Breaches -- Daily Quickview

The Performance Thresholds Quickview Report provides a rolling daily summary of round trip time values, or daily packet delivery ratio for the selected customer (left) and the node pair (right). The Top 10 daily samples for the selected node pair are displayed for the chosen timespan, allowing the RTT/Delivery metrics to be visually correlated with the corresponding CPU and interface utilizations. RTT and Delivery metrics are plotted against the provisioned thresholds allowing breaches or near-breaches to be easily visualized. For a RTT or Delivery threshold breach to be considered a 'SLA' breach, the correlated CPU and interface metrics must fall below the provisioned SLA Qualification Thresholds.
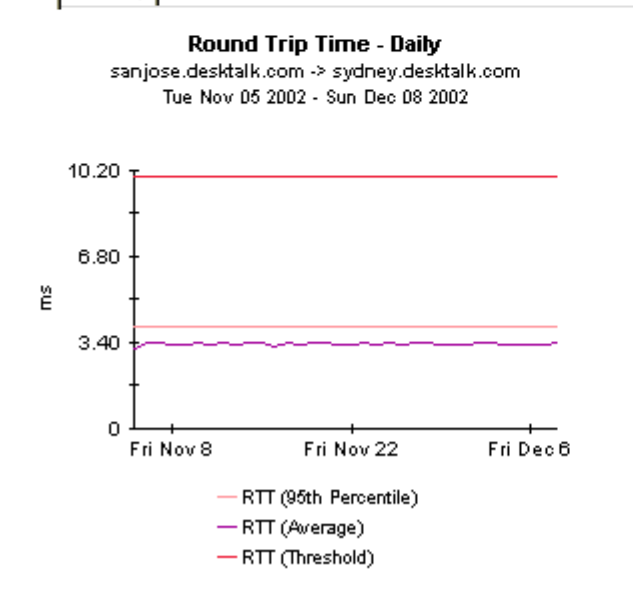
Node Pairs with the Highest Number of Breaches
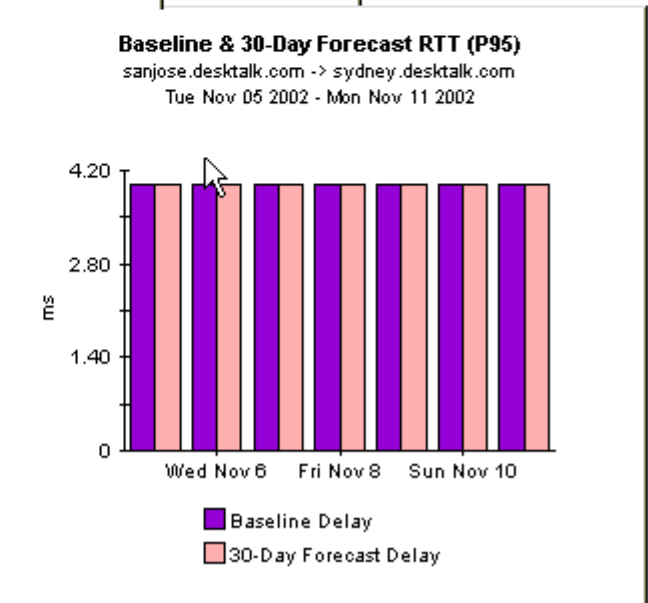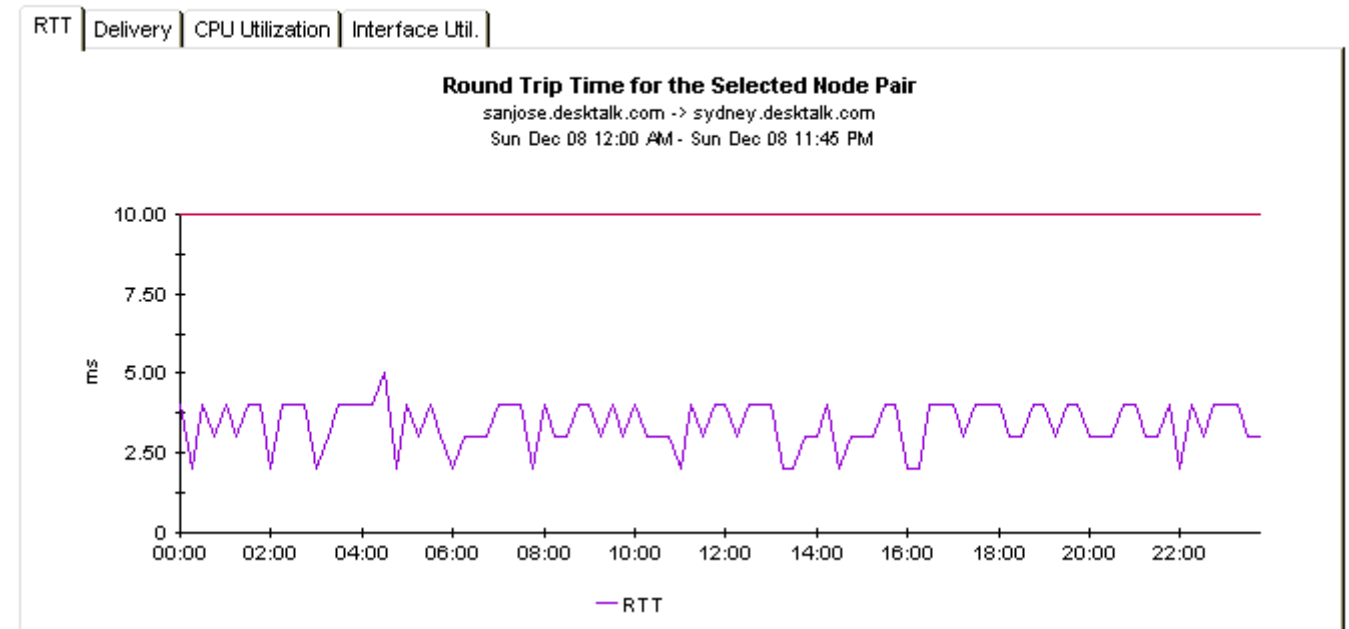Mon Jan 20 2003

Customers

Acme

Trinagy

Node Pairs	Tot RTT Breach	Tot Discard Breach
sanjose.desktalk.com -> sydney.desktalk.com	0	0
sanjose.desktalk.com -> london.desktalk.com	0	0
sanjose.desktalk.com -> chicago.desktalk.com	0	0
sanjose.desktalk.com -> newyork.desktalk.com	0	0
sanjose.desktalk.com -> lasvegas.desktalk.com	0	0

RTT | Delivery

Round Trip Time - Daily
sanjose.desktalk.com -> sydney.desktalk.com
Tue Nov 05 2002 - Sun Dec 08 2002

RTT (95th Percentile)
RTT (Average)
RTT (Threshold)

RTT: BL & F30 | Delivery: BL & F30

Baseline & 30-Day Forecast RTT (P95)
sanjose.desktalk.com -> sydney.desktalk.com
Tue Nov 05 2002 - Mon Nov 11 2002

Baseline Delay
30-Day Forecast Delay

RTT | Delivery | CPU Utilization | Interface Util.

Round Trip Time for the Selected Node Pair
sanjose.desktalk.com -> sydney.desktalk.com
Sun Dec 08 12:00 AM - Sun Dec 08 11:45 PM

RTT
RTT Threshold

Threshold Summaries

If you want to look more closely at breach counts on a customer by customer basis, and see how SLA breaches compare to non-SLA breaches, use the two threshold summary reports. These reports rank node pairs by breach count and indicate what your threshold settings are. The daily version of the report is cumulative for yesterday's activity and the monthly version is cumulative for the last 30 days. Both reports sort node pairs by threshold count, highest to lowest.

The daily version has an Exception Details table that indicates when each breach took place. If the node pair recorded 10 breaches yesterday, the Exception Details table will include 10 entries. Each entry in this table will tell you:

- What type of breach occurred
- Average RTT in effect at that time
- Packet loss ratio in effect at that time

If the Exception Details table includes one or more SLA breaches, you can see what utilization levels were in effect when that breach took place by looking at SLA Qualification Details. The levels you see here will be low compared to the thresholds for CPU and interface utilization.

The monthly version of the report does not provide exception details or the data that justified triggering an SLA breach. Instead you have graphs that track increases and decreases in the total SLA breach count and the total non-SLA breach count for RTT and delivery ratio.

Samples of the Threshold Breaches Summary report (Daily and Monthly) follow.

Cisco Ping

Performance Threshold Breaches -- Daily Quickview

The Performance Thresholds Quickview Report provides a rolling daily summary of round trip time values, or daily packet delivery ratio for the selected customer (left) and the node pair (right). The Top 10 daily samples for the selected node pair are displayed for the chosen timespan, allowing the RTT/Delivery metrics to be visually correlated with the corresponding CPU and interface utilizations. RTT and Delivery metrics are plotted against the provisioned thresholds allowing breaches or near-breaches to be easily visualized. For a RTT or Delivery threshold breach to be considered a 'SLA' breach, the correlated CPU and Interface metrics must fall below the provisioned SLA Qualification Thresholds.

Customers

Customers
Acme
Trinagy

Node Pairs with the Highest Number of Breaches
Thu Dec 19 2002

Node Pairs	Tot RTT Breach	Tot Discard Breach
sanjose.desktalk.com -> sydney.desktalk.com	0	0
sanjose.desktalk.com -> london.desktalk.com	0	0
sanjose.desktalk.com -> chicago.desktalk.com	0	0
sanjose.desktalk.com -> newyork.desktalk.com	0	0
sanjose.desktalk.com -> lasvegas.desktalk.com	0	0

RTT | Delivery

Round Trip Time - Daily
sanjose.desktalk.com -> sydney.desktalk.com
Tue Nov 05 2002 - Sun Dec 08 2002

- RTT (95th Percentile)
- RTT (Average)
- RTT (Threshold)

RTT: BL & F30 | Delivery: BL & F30

Baseline & 30-Day Forecast RTT (P95)
sanjose.desktalk.com -> sydney.desktalk.com
Tue Nov 05 2002 - Mon Nov 11 2002

- Baseline Delay
- 30-Day Forecast Delay

RTT | Delivery | CPU Utilization | Interface Util.

Round Trip Time for the Selected Node Pair
sanjose.desktalk.com -> sydney.desktalk.com
Sun Dec 08 12:00 AM - Sun Dec 08 11:45 PM

— RTT

Cisco Ping

Performance Threshold Breaches -- Monthly Summary

The Performance Threshold Breaches Monthly Summary provides a monthly total of threshold breaches for every node pair. Thresholds on the packet delivery ratio and round trip time can be configured for each pair. In addition, the packet delivery ratio and round trip time are compared against the configurable minimum interface and CPU utilization thresholds to show a service level agreement or SLA style breach. Drilling down from the monthly summary shows daily packet delivery ratio and round trip time breaches for a selected node pair (middle table). Node pairs are constrained by a selectable customer list (top table).

Customers

Acme

Trinagy

SLA Breach Counts for Last Month

Nov 2002

Node Pair	Tot RTT SLA-Breach	Tot RTT Breach	Tot Delivery SLA-Breach	Tot Delivery Breach
sanjose.desktalk.com -> lasvegas.desktalk.com	0	0	10	10
sanjose.desktalk.com -> sydney.desktalk.com	0	0	0	0
sanjose.desktalk.com -> london.desktalk.com	0	0	0	0
sanjose.desktalk.com -> chicago.desktalk.com	0	0	0	0
sanjose.desktalk.com -> newyork.desktalk.com	0	0	0	0

RTT Breach | Packet Delivery

Round Trip Time Breaches
sanjose.desktalk.com -> lasvegas.desktalk.com
For Sat Nov 30 2002

0.01

Total

0

Fri Nov 8   Tue Nov 12   Sat Nov 16   Wed Nov 20   Sun Nov 24   Thu Nov 28

■ Total RTT Non-SLA-Breaches
▦ Total RTT SLA-Breaches
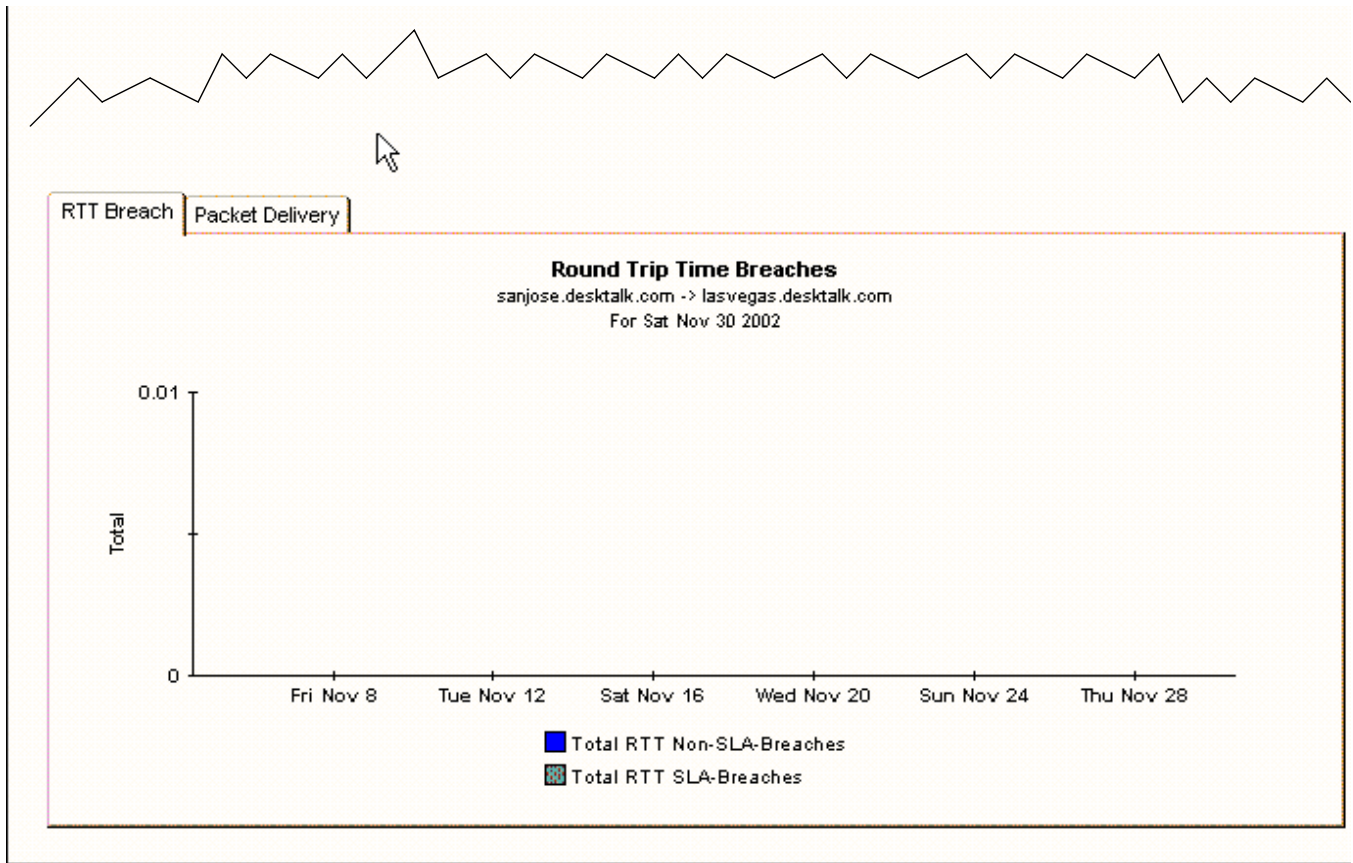
Executive Summary

If your network has users in various regions or users affiliated with various divisions of the company, or if you are a service provider with customers, you are likely to be interested in seeing performance aggregated by region, location, or customer. The Executive Summary meets this need, allowing you to view a "rolled-up" version of performance data.

Instead of looking at performance for a particular node pair, the Executive Summary rolls up performance for an entire region or an entire customer. Quick comparisons are now easy. The division with high response time is easy to spot, and the customer with a low packet delivery ratio is easy to spot.

The Executive Summary gives you an hourly view of the aggregation and a daily view of the aggregation. The hourly view gives you an hour-by-hour analysis of response time and packet delivery, while the daily view gives you a day-by-day view. If the hourly graph for yesterday looks unusual, compare it to the daily. The comparison should provide the evidence you need to determine whether or not yesterday's activity was a temporary condition.

The two graphs for RTT, Hourly Aggregate and Daily Aggregate, show the divergence between average RTT and P95 RTT. As mentioned earlier, the value for P95 is equal to or greater than 95% of the samples for a given day and reflects near-peak usage.

A sample of the Executive Summary follows.

Cisco Ping

Executive Summary

The Executive Summary Report provides hourly and daily aggregate performance of the network across all node pairs over the last month, and over the last day. Select a customer from the table below to view the aggregates of the 95th percentile round trip time and the packet delivery ratio.

Customers

All

Unassigned Customer

Daily Aggregate RTT (95th percentile)
Fri Sep 13 2002 - Mon Sep 30 2002

Avg RTT (95th Percentile)
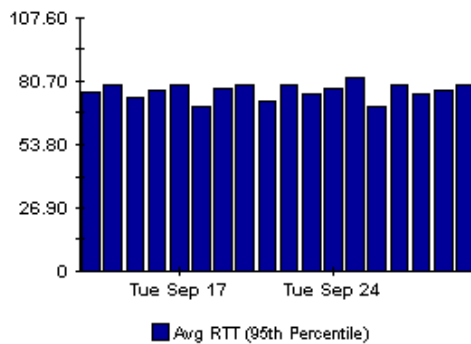
Daily Aggregate Packet Delivery Ratio
Fri Sep 13 2002 - Mon Sep 30 2002
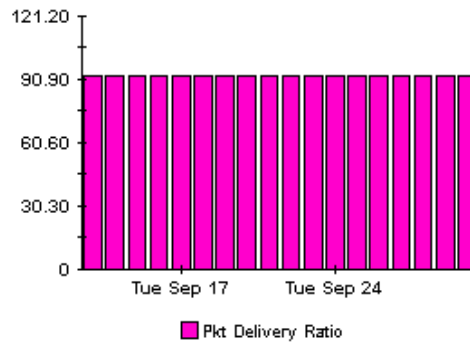
Pkt Delivery Ratio

Hourly Aggregate RTT (95th percentile)
Mon Sep 30 2002

Avg RTT (95th Percentile)
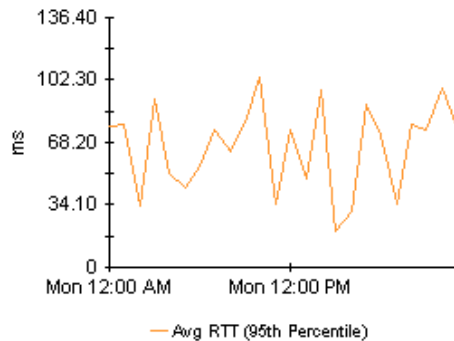
Hourly Aggregate Packet Delivery Ratio
Mon Sep 30 2002

Pkt Delivery Ratio

13
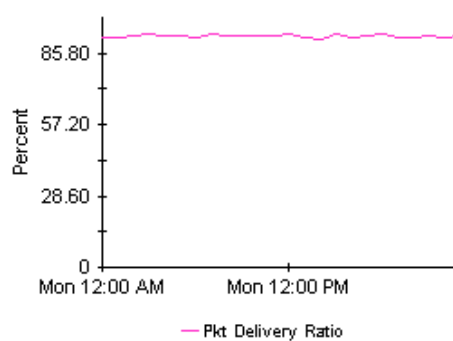
Forecasting Future Performance

The forecast report alerts you to node pairs that may be headed for performance problems. It tells you which node pairs amongst all node pairs are expected to have the worst performance 30 days from now. Worst can refer to highest round trip time or lowest packet delivery ratio.

The forecast table beneath the customer list provides a list of node pairs and values for the following metrics:

- 30 day forecast RTT
- Baseline RTT
- 30 day forecast delivery
- Baseline delivery

The 30 day forecast is a projection. Baseline RTT and baseline delivery are averages. If performance has worsened over the baseline period, the 30 day forecast will be worse than the baseline average; if performance has improved, the 30 day forecast will be better than the baseline average.

The graphs below the forecast table do two things. They let you track daily increases and decreases in P95 values (these are the values responsible for the projection) and they let you see how the P95 value is diverging from the baseline average on a daily basis.

The value for P95 is equal to or greater than 95% of the samples for a given day. The value for P95 reflects near-peak usage and functions as a reliable reflection of the conditions the network is currently accommodating.

A sample forecast report follows.

Cisco Ping
Forecast

The Forecast Report provides a chart ranking the worst performing pairs by daily round trip time or by total daily packet delivery ratio, based on a 4 week projection extrapolated from 6 weeks of data.. Drilling down shows the data on which the forecast was based, at a daily level, with the day-of-week baseline and 30-day forecast values. Select a customer (top table) and a node pair (middle table), for the drill down information. (NOTE: The RTT calculations are based on daily 95th percentile, providing a better basis for planning than either the average or the peak)

Customers

Acme

Trinagy

Forecast -- Worst Performing Node Pairs

Node Pair	30-Day-Forecast RTT	Baseline RTT	30-Day-Forecast Delivery	Baseline Delivery	DOW
amsterdam.desktalk.com -> atlanta.desktalk.com	99.71	64.96	96.29	96.99	Sun

RTT | Delivery

Daily 95th Percentile Round Trip Time
amsterdam.desktalk.com -> atlanta.desktalk.com
Tue Nov 05 2002 - Sun Dec 08 2002

— 95th Percentile : RTT

RTT: BL vs F30 | Delivery: BL vs F30

Round Trip Time -- Baseline vs 30-Day Forecast
amsterdam.desktalk.com -> atlanta.desktalk.com
Tue Nov 05 2002 - Mon Nov 11 2002

■ Baseline Delay
■ 30-Day Forecast Delay

14
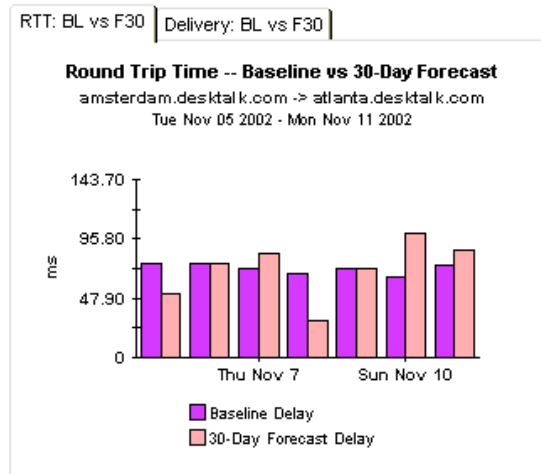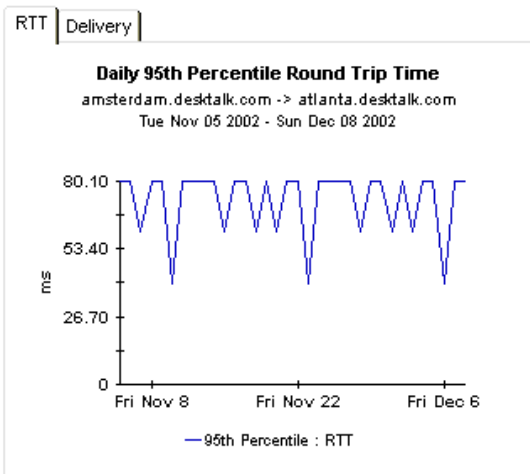
MIB Variables and Summaries

This chapter provides a list of the variables that are polled from the following MIBs:

- Cisco Ping MIB
- Cisco System MIBlet
- Interface Reporting Basic Info MIBlet

The Cisco Ping MIB contains performance data for pings, the Cisco System MIBlet contains CPU utilization data, and the Interface Reporting Basic Info MIBlet contains interface utilization data.

Cisco Ping MIB

The source MIB is the Cisco-Ping-MIB. The source table is Risco_ping_rtd. The following table provides a list of variables, with descriptions.

Variable	OID String	Description
avg_rtt	1.3.6.1.4.1.9.9.16.1.1.1.12	Average round trip for all the packets that have been sent in this sequence. This object will not be created until the first ping response in a sequence is received.
max_rtt	1.3.6.1.4.1.9.9.16.1.1.1.13	Maximum round trip for all the packets that have been sent in this sequence. This object will not be created until the first ping response in a sequence is received.
min_rtt	1.3.6.1.4.1.9.9.16.1.1.1.11	Minimum round trip for all the packets that have been sent in this sequence. This object will not be created until the first ping response in a sequence is received.
packets_received	1.3.6.1.4.1.9.9.16.1.1.1.10	Number of ping packets that were received from the target in this sequence.
packets_sent	1.3.6.1.4.1.9.9.16.1.1.1.9	Number of ping packets that were sent to the target in this sequence.
packet_size	1.3.6.1.4.1.9.9.16.1.1.1.5	Size of ping packets to send to the target in this sequence. The lower and upper boundaries of this object depend on the protocol. An instance of this object cannot be modified unless the associated instance of ciscoPingProtocol has been created (so as to allow protocol-specific range checking on the new value).

cisco_system MIBlet

The source MIBlet is cisco_system. The source table is xcpu_util_rtd_png_.

Variable	OID String	Description
avg_busy1	1.3.6.1.4.1.9.2.1.57	1 minute exponentially-decayed moving average of the CPU busy percentage. Changed from INTEGER to Gauge by HP OpenView.

interface-reporting_basic_interface_info MIBlet

The source MIBlet, basic_interface_info, is a miblet of the MIB-II ifEntry table. The source table is interface_rtd_png_.

Variable	OID String	Description
ifSpeed	1.3.6.1.2.1.2.2.1.5	Estimate of current bandwidth in bits per second. If the interface does not vary in bandwidth, or if an accurate estimate is not possible, this object should contain the nominal bandwidth.
ifInOctets	1.3.6.1.2.1.2.2.1.10	Total number of octets received on the interface, including framing characters.
ifOutOctets	1.3.6.1.2.1.2.2.1.16	Total number of octets transmitted out of the interface, including framing characters.

Summaries

Collected data is summarized on an hourly, daily, and monthly basis.

Summary	What It Aggregates
PingDaily_bykey.sum	Hourly data for all device pairs by day and by key.
PingHourly_bykey.sum	Rate data for all device pairs by day and by key.
PingDaily_allpairs.sum	Hourly data for all device pairs by day.
PingHourly_allpairs.sum	Rate data for all device pairs by hour.
PingHourly_allpairs_by_cust_id.sum	Rate data for all device pairs by hour and by cust_id.
PingDOW_BL_and_FC_bykey.sum	Rate data for all device pairs by day of week and by key.

Baseline and Forecast Data

The source table is SD425Dcisco_ping_rtd_SBF_cisco. Trendsum calculates the values for the variables and stores them in this table.

Variable	OID String	Description
day_of_week	6	This string value notes the day of the week for the collected data.
F30avg_rtt	5	30-day forecast average for round trip delay times.
F30packets_received	3	30-day forecast for packets received.
F30packets_sent	1	30-day forecast for packets sent.
WAVavg_rtt	4	Weighted average for round trip delay times.
WAVpackets_received	2	Weighted average for packets received.
WAVpackets_sent	0	Weighted average for packets sent.

Editing Tables and Graphs

Any table or graph can be viewed in several ways. While the default view is often the view you will use the most, you can easily change to a different view. If you are using the Report Viewer application, change the default view by right-clicking the object and selecting a different view. If you are looking at a report on the Web, click the **Edit Table** or **Edit Graph** icons.

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	
24.13.17.1	5	F	Concert	Cable5/0	
24.13.17.1	6	F	Concert	Cable6/0	
24.13.17.1	6	F	Concert	Cable6/0	
24.13.17.1	6	F	Concert	Cable6/0	

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.

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.

| | | Polled IP QoS Statistics Data - Input | | |
| | | Over Previous 6 Hours | | |
Direction	IpPrecedence	Switched Bytes	Switched Pkts	Time Period
Input	0	105,688	675	Tue Oct 29 07:00 AM
Input	1	0	0	Tue Oct 29 07:00 AM
Input	2	0	0	Tue Oct 29 07:00 AM
Input	3	0	0	Tue Oct 29 07:00 AM
Input	4	0	0	Tue Oct 29 07:00 AM
Input	5	0	0	Tue Oct 29 07:00 AM
Input	6	600	5	Tue Oct 29 07:00 AM
Input	7	0	0	Tue Oct 29 07:00 AM
Input	0	98,334	638	Tue Oct 29 06:45 AM
Input	1	0	0	Tue Oct 29 06:45 AM
Input	2	0	0	Tue Oct 29 06:45 AM
Input	3	0	0	Tue Oct 29 06:45 AM
Input	4	0	0	Tue Oct 29 06:45 AM
Input	5	0	0	Tue Oct 29 06:45 AM
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	650	Tue Oct 29 06:00 AM

View Options for Graphs

Right-click any graph to open a list of view options.
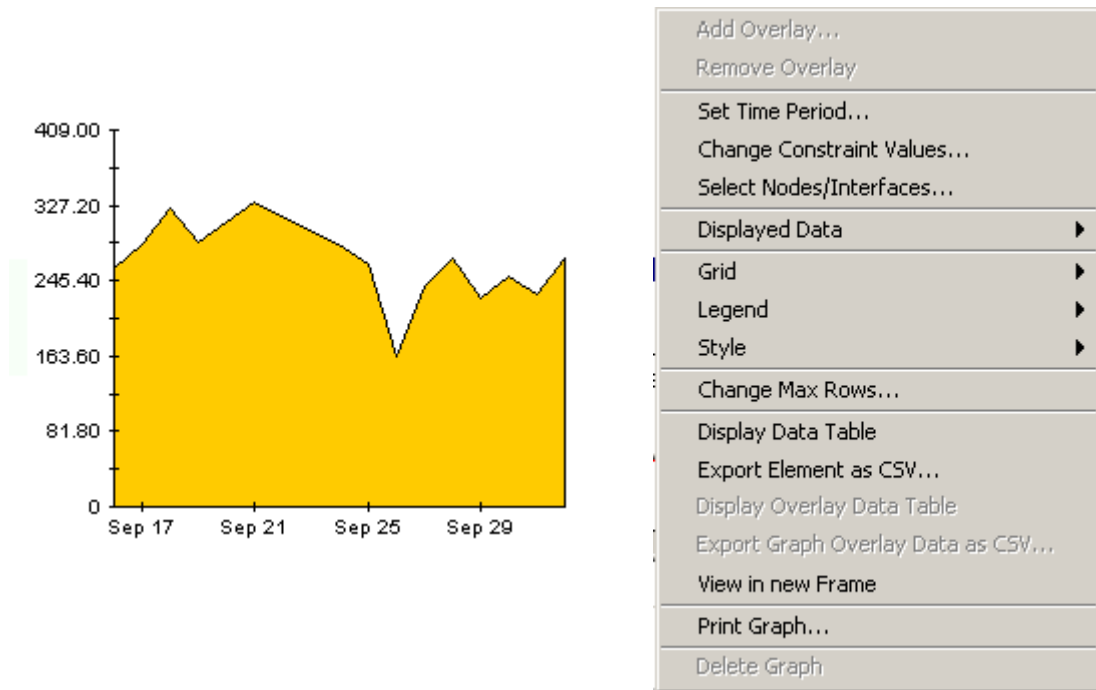
The following table provides a few details about each option.

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 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 ten view options for graphs.
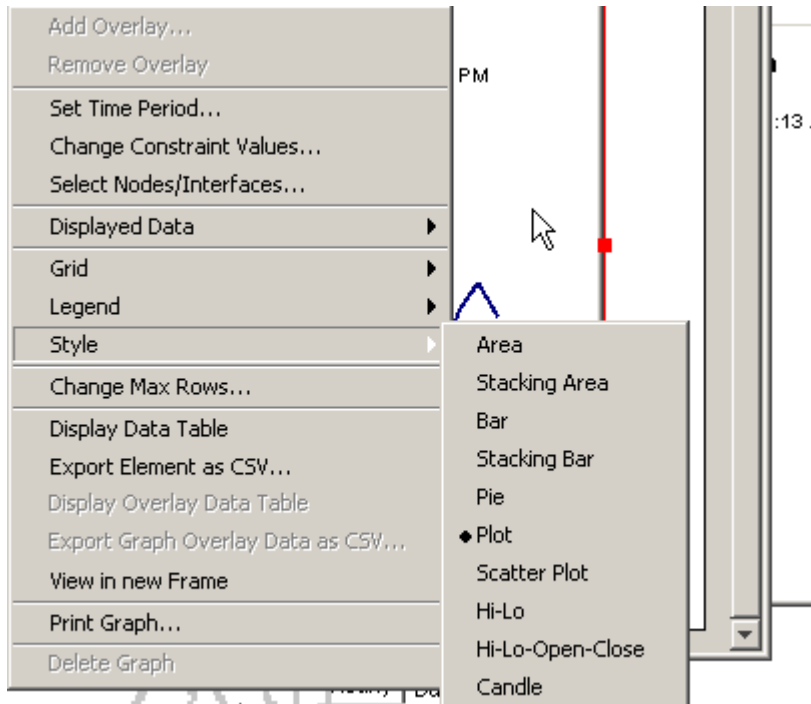
Style > Area

The plot or bar chart changes to an area graph. While relative values and total values are easy to view in this format, absolute values for smaller data types may be hard to see. Click anywhere within a band of color to display the exact value for that location
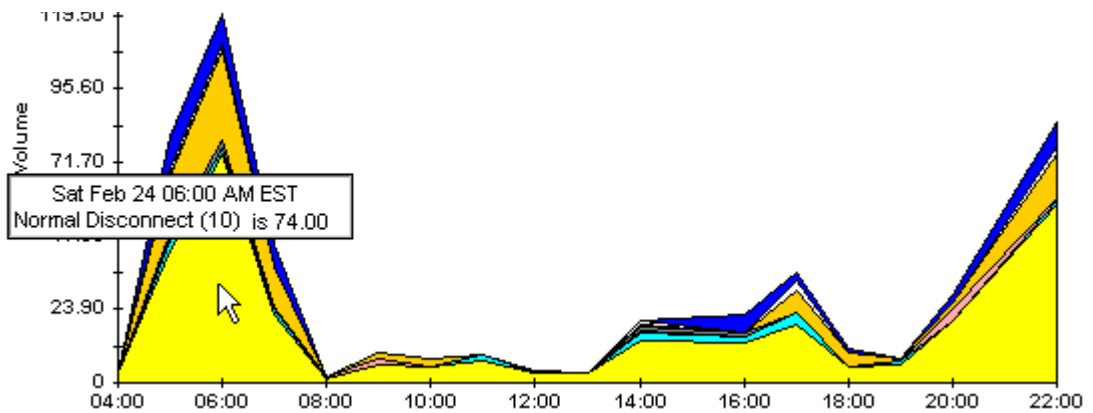
To shorten the time span of a graph, press SHIFT+ALT and use the left mouse button to highlight the time span you want to focus on. Release the mouse button to display the selected time span.

Style > Stacking Area

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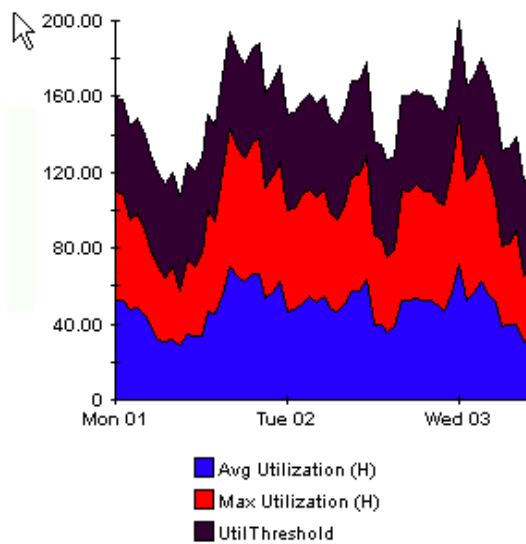
Style > Bar

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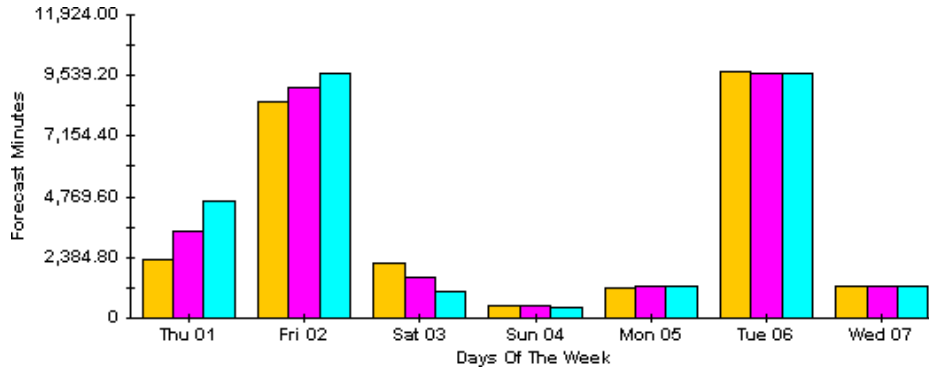
Style > Stacking Bar

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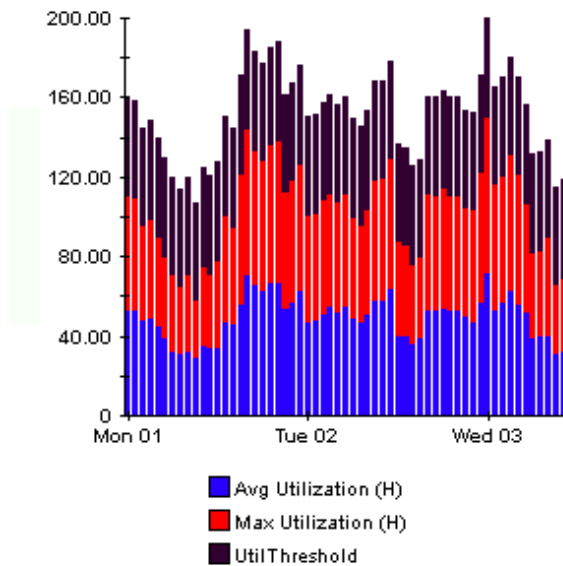
Style > Plot

Bands of color in an area graph change to lines. If you adjust the frame width, you can make the data points align with hour; if you adjust the frame height, you can turn call volume into whole numbers.
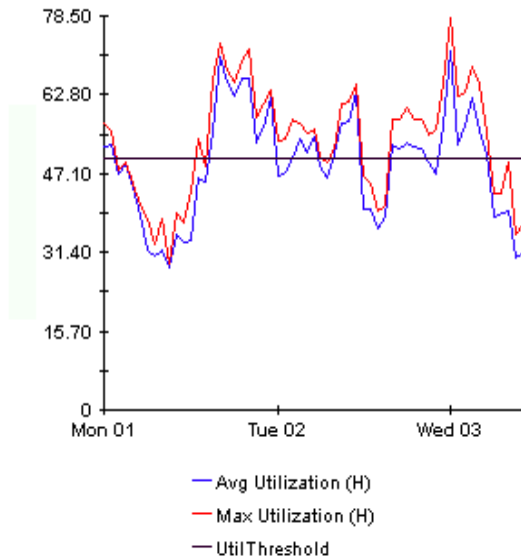
Style > Pie
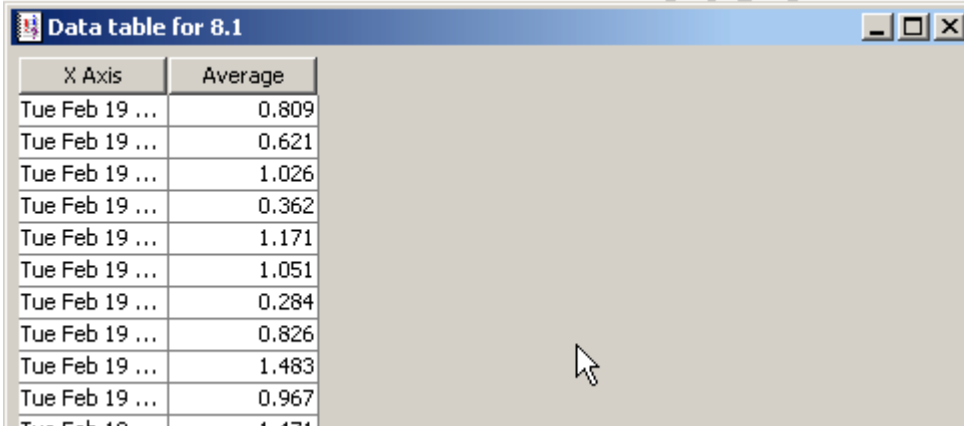
An area graph becomes a pie chart. Bands in an area graph convert to slices of a pie and the pie constitutes a 24-hour period. This view is helpful when a small number of data values are represented and you are looking at data for one day.
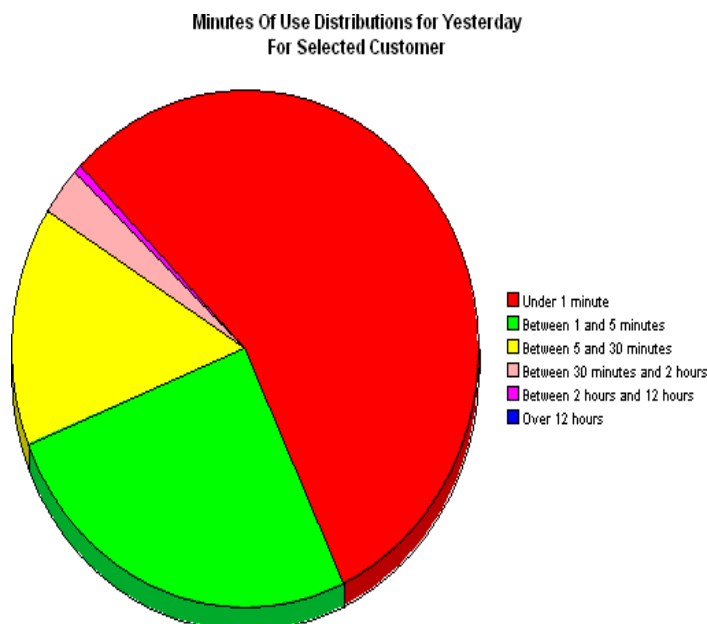
If you are looking at data for more than one day, you will see multiple pie graphs, one for each day.

Display Data Table

This option changes a graph into a spreadsheet.

View in New Frame

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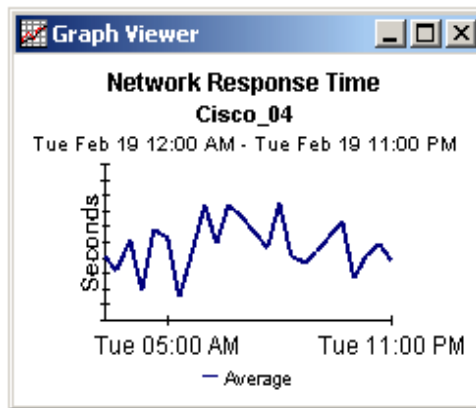
availability

The percentage of time a device has been operational. Identifies device outages as reported through the sysUpTime variable. Calculated by combining device sysUpTime with interface ifOperStatus and interface ifLastChange.

avg volume

This metric is found in capacity planning reports. It refers to average daily volume during the baseline period. F30 Volume is the 30 day forecast for daily volume.

baseline busy hour

The average of 42 busy hour values recorded during the rolling baseline period. This value appears in the Capacity Planning report as Avg BH Util, or Average Busy Hour Utilization.

busy hour

The one hour of the day when utilization was higher than the other 23 hours in the day. Do not confuse busy with peak. Busy hour is an average, an average of four samples. Any sample within that collection of four samples may have been well above or well below the average. The busy hour average is treated as a persistent event suitable for use in calculations that project future performance levels.

daily

A view showing daily performance for the previous 30 days, The most recent day in this view shows performance for yesterday.

day of week

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

device

Any SNMP manageable device.

discard rate

The percentage of packets discarded by the interface. Data about discards is sampled during each poll cycle (by default this is four times an hour); based on those samples, OVPI calculates an average and a maximum discard rate.

discard threshold

The point at which an acceptable percentage of discarded traffic becomes an abnormal percentage and possibly impacts the user experience. If the interface is full duplex, the same threshold value is applied to both in and out packets separately.

error rate

The percentage of packets with errors as reported by the interface. Data about errors is sampled during each poll cycle (by default this is four times an hour); based on those samples, OVPI calculates an average and a maximum error rate.

error threshold

The point at which an acceptable percentage of errored traffic becomes an abnormal percentage and possibly impacts the user experience. If the interface is full duplex, the same threshold value is applied to both in and out packets separately.

F30 / F60 / F90

The level where utilization (or volume) is expected to be 30, 60, and 90 days from now. Calculated by applying linear regression to busy hour levels over the baseline period.

group

This value is imported by the provisioning interface. If this value is not provisioned, the report shows *unknown* in this field.

growth rate

F30 utilization 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.

interface

An entry in the SNMP ifTable for of the device. Can represent a physical or logical interface.

monthly

A view showing performance for each month over the last two years. Blank until data collection has been functioning for at least one month.

region

This value is imported by the provisioning interface. If this value is not provisioned, the report shows *unknown* in this field.

response time

Delay within the network management structure, specifically, delay between the datapipe and the device. If the delay is being caused by the device, then this value may point to device resource issues.

threshold breach

The line between normal and abnormal performance. When this line is crossed, an exception is recorded. Every threshold has a default value that is easily changed to reflect individual needs.

utilization

The total number of octets traversing the interface as a percentage of the total *possible* number of octets, using the ifSpeed property. If an interface is full duplex, utilization is calculated and displayed separately in each direction. Groups of interfaces have their utilization calculated by taking the total traffic on all administratively up interfaces in the group and dividing that by the total possible bandwidth for those interfaces. Utilization for a group of interfaces is more meaningful when all the interfaces in the group use the same protocol.

utilization threshold

The point at which the number of octets traversing the interface is considered detrimental to the service level required by network users. In the case of full duplex interfaces, the same threshold value is applied to both in and out packets separately.

index

trendtimer, *34*

U

unavailable route, *13*

unknown, *34*

unsuccessful pings, *13*

Update Device Pair Parameters form, *41*

Update Threshold Values form, *41*

UPGRADE_Ping_MIB_3_to_4, *20*

Use Absolute Time, *73*

utilization, *83*

utilization threshold, *83*

V

view in new frame, *74*

X

xcpu_util_rtd_png_ (MIBlet), *30*, *71*