

# Cisco Ping Report Pack

Software Version: 4.2

HP Performance Insight

---

## User Guide

October 2007



## Legal Notices

### Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

### Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

### Copyright Notices

© Copyright 2004 - 2007 Hewlett-Packard Development Company, L.P.

### Trademark Notices

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 Corporation.

## Documentation Updates

The title page contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.

To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

**[http://ovweb.external.hp.com/lpe/doc\\_serv/](http://ovweb.external.hp.com/lpe/doc_serv/)**

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

The following table indicates changes made to this document since the last released edition.

<b>Chapter</b>	<b>Changes</b>
Chapter 1	Enhancements in Version 4.2 (new)
Chapter 2	Minor updates to version numbers
Chapter 3	Minor updates to version numbers
Chapter 5	Minor edits

## Support

You can visit the HP software support web site at:

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

HP Software online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

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

To find more information about access levels and HP Passport, go to:

**[http://support.openview.hp.com/new\\_access\\_levels.jsp](http://support.openview.hp.com/new_access_levels.jsp)**

# Contents

<b>1 Overview</b> .....	3
OVPI and Ping Tests: Putting Results in Context .....	3
Enhancements in Version 4.2 .....	3
Brief Description of Reports .....	4
Action Poller: A Unique Collection Mechanism .....	4
Error Messages in trend.log .....	7
Integration with Network Node Manager .....	7
Options for Customizing Reports .....	8
Sources for Additional Information .....	9
<b>2 The Upgrade Install</b> .....	11
Guidelines for a Smooth Upgrade .....	11
Upgrading to Cisco Ping 4.2 .....	12
Package Removal .....	15
<b>3 The New Install</b> .....	17
Guidelines for a Smooth Installation .....	17
Installing Cisco Ping .....	19
Accessing Deployed Reports .....	21
Package Removal .....	21
<b>4 Action Poller User Interface</b> .....	23
Launching the Interface .....	23
Defining Node Pairs .....	24
MIBlet Groups .....	24
Assigning Instances to Nodes .....	25
Modifying Parameter Sets .....	25
Exiting the Interface .....	26
<b>5 Configuration Options</b> .....	27
Configuring Servers in a Distributed System .....	27
Provisioning the Property Table .....	30
Action Poller Command Line Options .....	34
Changing the Collection Interval .....	35

6	Forms—Configure/Create/Update	37
7	Worst Performing Node Pairs	43
8	Daily QuickView/Daily Snapshot	45
9	Sample Data in Near Real Time	49
10	Threshold Daily QuickView	53
11	Threshold Summaries	55
12	Executive Summary	61
13	Forecasting Future Performance	65
14	MIB Variables and Summaries	67
	Cisco Ping MIB	68
	cisco_system MIBlet	68
	interface-reporting_basic_interface_info MIBlet	69
	Summaries	69
	Baseline and Forecast Data	70
	Glossary	71
A	Version History	75
B	Editing Tables and Graphs	77
	View Options for Tables	77
	View Options for Graphs	78
	Index	85

# 1 Overview

This chapter covers the following topics:

- Performance Insight and ping tests in context
- Enhancements in version 4.2
- Brief description of reports
- Action Poller — a unique collection mechanism
- Error messages in trend.log
- Integration with Network Node Manager
- Options for customizing Cisco Ping reports
- Sources for additional information

## Performance Insight and Ping Tests in Context

Latency and reliability are common ways to measure network performance. If latency is low, packets are moving from source devices to destination devices as quickly as possible. If reliability is high, packets are reaching their intended destination. The conventional approach to measuring latency and reliability is to conduct ping tests and watch for poor results. The problem with this approach is that the surrounding network is hidden from view. You may have test results, but are your test results conclusive?

The purpose of the Cisco Ping Report Pack is to add context to latency and reliability measurements by revealing the surrounding network. With the surrounding network in view, you have a much better picture of the conditions behind high latency and low reliability. In addition, you will no longer have to guess what the load on an interface is. You will know whether the load on the source router interface and the load on the destination router interface are about the same or completely different.

The Cisco Ping Report Pack will also enhance SLA monitoring capability. If latency breaches a threshold while utilization is high, the report pack qualifies this event as a non-SLA breach. If latency or reliability crosses a threshold while utilization is low, the report pack qualifies this event as an SLA breach.

## Enhancements in Version 4.2

Version 4.2 includes a defect fix and a new upgrade package. For details about the enhancements that were made to previous releases, see [Appendix A, Version History](#).

## New Upgrade Package

- UPGRADE\_Ping\_MIB\_to\_42.ap

## Defect Fix

- QXCR1000456570: Arithmetic overflow error

# Brief Description of Reports

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

**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.

# Action Poller: A Unique Collection Mechanism

Most report packs use a collection mechanism that collects data from single nodes. This collection mechanism is built into OVPI and it 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 must 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 must 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—traffic management, buffer sizes, and 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 (1) connectivity between the source and destination node was unavailable or (2) 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 `trend.log` are error messages. The following messages contain supplemental information only and 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(?, ?, ?, ?,
?)}"
```

## Integration with Network Node Manager

You can improve your ability to isolate faults and diagnose problems by integrating OVPI with NNM. Integrating NNM and PI entails running a script on NNM and launching the Integration Wizard on PI. (Until recently, it was necessary to install integration software on NNM and PI. Those software packages are now built into each product.)

If NNM and OVPI are integrated, you should install the optional thresholds sub-package that comes with Cisco Ping. Installing the optional thresholds sub-package supplies default thresholds for Round Trip Time, Discards, CPU, and Interface to the Thresholds Module. The Thresholds Module monitors the database for threshold conditions and responds to a breach by taking an action in accordance with category, severity, and destination parameters. The default response is to send a breach trap to NNM. The breach trap received by NNM becomes an alarm in the NNM alarm browser, and you can respond to that alarm by launching a Cisco Ping Near Real Time report.



Even if you are using the alarms browser, and not seeing alarms from a device that Cisco Ping is monitoring, you can investigate a device that Cisco Ping is monitoring by opening the Report Launchpad window and selecting a Cisco Ping report.

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

## Options for Customizing Reports

Reports can be customized by importing customers and locations, applying group filters, editing parameters, and editing tables and graphs. While group filters allow service providers to share reports with customers, any user can apply constraints to a report or edit tables and graphs. For details about view options for tables and graphs, see [Appendix B, Editing Tables and Graphs](#).

### Group Filters

If you want to share reports with customers, you must produce customer-specific reports. Producing customer-specific reports involves the following steps:

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

For more information about group filters, refer to the *PI Administration Guide*.

### Editing Parameters

Editing a parameter applies a constraint to the report. The constraint filters out data you do not want to see. For example, 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. Cisco Ping supports the following parameters:

- Customer\_Name
- Customer\_Id
- Location\_Name
- Location\_Id
- Source
- Destination

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

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

## Sources for Additional Information

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

For information regarding the latest enhancements to the Cisco Ping package and any known issues, refer to the *Cisco Ping Report Pack Release Notes*. You may also be interested in the following documents:

- *Interface Discovery Datapipe User Guide*
- *Thresholds Module User Guide*
- *NNM/PI Integration User Guide*

Manuals for the core product, and manuals for the reporting solutions that run on PI, can be downloaded from this site:

**[http://ovweb.external.hp.com/lpe/doc\\_serv/](http://ovweb.external.hp.com/lpe/doc_serv/)**

The user guides for OVPI are listed under **Performance Insight**. The user guides for report packs and datapipes are listed under **Performance Insight Report Packs**. Each entry includes a date. If a manual is revised, the date will change. Since revised manuals are posted on a regular basis, you should compare the date on your PDF against the date of the PDF on the web and download the web edition if it is newer.



## 2 The Upgrade Install

This chapter covers the following topics:

- Guidelines for a smooth upgrade
- Using Package Manager to install the upgrade package
- Uninstalling Cisco Ping

### Guidelines for a Smooth Upgrade

The report pack CD contains report packs, datapipes, and shared packages. When you insert the CD and launch the package extraction program, the install script extracts every package from the CD and copies the results to the Packages directory on your system. After the extract process finishes, you will be prompted to start Package Manager. Before using Package Manager, review the following guidelines.

#### Prerequisites for the Upgrade

The following software must already be installed before upgrading to Cisco Ping 4.2:

- OVPI 5.3
- Any and all service packs available for version 5.3
- Cisco Ping Report Pack 4.1
- Interface Discovery Datapipe 2.5
- Interface Reporting ifEntry Datapipe 2.5

You can find information about each service pack for OVPI, including installation instructions, in 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 PI 5.3. Following is an overview of the procedure for upgrading Cisco Ping in a distributed environment:

- 1 Disable trendcopy on the central server.
- 2 If you are running version 2.2 or earlier of the Interface Reporting datapipes, remove them.
- 3 Install UPGRADE\_Ping\_MIB\_to\_42; deploy reports.
- 4 Install these packages simultaneously:

- Cisco Ping Thresholds sub-package (optional)
  - Interface Reporting ifEntry Datapipe 2.5 (if removed version 2.2 or earlier)  
OR  
UPGRADE\_IRifEntry\_Datapipe\_to\_25 (if version 2.3 is installed)
  - Interface Discovery Datapipe 2.5 (if removed version 2.2 or earlier)  
OR  
UPGRADE\_IFEntry\_Disc\_Datapipe\_to\_25 (if version 2.3 is installed)
- 5 For each satellite server:
    - a Remove version 2.2 or earlier of the Interface Discovery Datapipe.
    - b Install UPGRADE\_Ping\_MIB\_to\_42.
    - c Install these packages simultaneously:
      - Cisco Ping Thresholds sub-package (optional)
      - Interface Reporting ifEntry Datapipe 2.5 (if removed version 2.2 or earlier)  
OR  
UPGRADE\_IRifEntry\_Datapipe\_to\_25 (if version 2.3 is installed)
      - Interface Discovery Datapipe 2.5 (if removed version 2.2 or earlier)  
OR  
UPGRADE\_IFEntry\_Disc\_Datapipe\_to\_25 (if version 2.3 is installed)
  - 6 Enable trendcopy on the central server.
  - 7 You must reconfigure your central and satellite servers. See [Configuring Servers in a Distributed System](#) on page 27 for more information.

## Converting Threshold Breaches into Alarms

If OVPI and NNM are integrated, you should install the optional thresholds sub-package, `Ping_MIB_Threshold`, on the OVPI server. If you install the thresholds sub-package, OVPI will respond to a threshold breach by sending a breach trap to NNM, where the trap displays as an alarm in the NNM alarm browser.

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, Package Manager will install the latest version for you, automatically.

## Upgrading to Cisco Ping 4.2

Perform the following tasks to upgrade Cisco Ping:

- Task 1: [Stop OVPI Timer and extract packages from the report pack CD](#)
- Task 2: [Uninstall any old version \(2.2 or earlier\) of the Interface Reporting datapipes](#)
- Task 3: [Install the Upgrade Package](#)
- Task 4: [Install the Thresholds Sub-Package and restart OVPI Timer](#)



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

- 1 Log in to the system. On UNIX systems, log in as root.
- 2 Stop OVPI Timer and wait for processes to terminate.  
On Windows, do the following:
  - a Select **Control Panel > Administrative Tools > Services**.
  - b Select OVPI Timer from the list of services.
  - c From the Action menu, select **Stop**.On UNIX, as root, do one of the following:  
HP-UX: **sh /sbin/init.d/ovpi\_timer stop**  
Sun: **sh /etc/init.d/ovpi\_timer stop**
- 3 Insert the report pack CD in the CD-ROM drive. On Windows, a Main Menu displays automatically; on UNIX, 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.

After 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:

- Cisco\_Ping.ap
- Cisco\_Ping\_Demo.ap
- Cisco\_Ping\_Thresholds.ap
- UPGRADE\_Ping\_MIB\_to\_42.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.

### Task 2: Uninstall any old version (2.2 or earlier) of the Interface Reporting datapipes

- 1 Click **Next**. The Package Location window opens.
- 2 Click **Uninstall**.
- 3 Click **Next**. The Report Undeploy window opens.
- 4 Click the check box next to the following packages:  
*IFEntry\_Disc\_Datapipe*  
*IR\_ifEntry\_Datapipe*
- 5 Click **Next**. The Selection Summary window opens.
- 6 Click **Uninstall**. The Progress window opens and the removal begins. When the uninstall process is complete, a package removal complete message appears.
- 7 Click **Done** to return to the Management Console.

### Task 3: Install the 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 **Install**. Approve the default installation directory or select a different directory if necessary.
- 4 Click **Next**. The Report Deployment window opens. Accept the default for Deploy Reports; accept the defaults for application server name and port. Type your user name and password for the OVPI Application Server.
- 5 Click **Next**. The Package Selection window opens.
- 6 Click the check box next to the following package:
  - UPGRADE\_Ping\_MIB\_to\_42*
  - IR\_ifEntry\_Datapipe 25*
  - or
  - UPGRADE\_IRifEntry\_Datapipe\_to\_25*
  - IFEntry\_Disc\_Datapipe 2.5*
  - or
  - UPGRADE\_IFEntry\_Disc\_Datapipe\_to\_25*
- 7 Click **Next**. The Type Discovery window opens. Disable the default.
- 8 Click **Next**. The Selection Summary window opens.
- 9 Click **Install**. The Installation Progress window opens and the install begins. When the install finishes, a package install complete message appears.
- 10 Click **Done**.



Do not be surprised if the UPGRADE package you just installed has disappeared from view. Package Manager will display what you just installed as *Cisco Ping 4.2*.

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

- 1 Start Package Manager. The Package Manager welcome window opens.
- 2 Click **Next**. The Package Location window opens.
- 3 Click **Install**.
- 4 Click **Next**. The Report Deployment window opens; disable the option to Deploy Reports.
- 5 Click **Next**. The Package Selection window opens.
- 6 Click the check box next to the following packages:
  - Cisco\_Ping\_Thresholds*
- 7 Click **Next**. The Type Discovery window opens.
- 8 Disable the default and click **Next**. The Selection Summary window opens.
- 9 Click **Install**. The Installation Progress window opens and the install begins. When the install finishes, a package install complete message appears.
- 10 Click **Done** to return to the Management Console.

- 11 Restart OVPI Timer.

On Windows, do the following:

- a Select **Control Panel > Administrative Tools > Services**.
- b Select OVPI Timer from the list of services.
- c From the Action menu, select **Start**.

On UNIX, as root, do one of the following:

```
HP-UX: sh /sbin/init.d/ovpi_timer start
```

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

## Package Removal

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.

On Windows, do the following:

- a Select **Control Panel > Administrative Tools > Services**.
- b Select OVPI Timer from the list of services.
- c From the Action menu, select **Stop**.

On UNIX, as root, do one of the following:

```
HP-UX: sh /sbin/init.d/ovpi_timer stop
```

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

- 3 Start Package Manager. The Package Manager welcome window opens.
- 4 Click **Next**. The Package Location window opens.
- 5 Click **Uninstall**.
- 6 Click **Next**. The Report Undeployment window opens.
- 7 Click the check box next to the following packages:
  - Cisco\_Ping*
  - Cisco\_Ping\_Thresholds* (if installed)
  - Cisco\_Ping\_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**.
- 11 Restart OVPI Timer.

On Windows, do the following:

- a Select **Control Panel > Administrative Tools > Services**.
- b Select OVPI Timer from the list of services.

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

On UNIX, as root, do one of the following:

```
HP-UX: sh /sbin/init.d/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
- Installing Cisco Ping
- Accessing deployed reports
- Uninstalling Cisco Ping

## Guidelines for a Smooth Installation

An OVPI reporting solution has at least two ingredients, a report pack and a datapipe. Some reporting solutions offer multiple datapipes. When you install a datapipe, you configure OVPI to collect a specific type of performance data at a specific interval. When you install a report pack, you configure OVPI to summarize and aggregate the data collected by the datapipe.

When you insert the report pack CD and launch the package extraction program, the install script extracts every package from the CD and copies the results to the Packages directory on your system. After the extract process finishes, you are prompted to start the Package Manager install wizard. Before using Package Manager, review the following guidelines.

### Prerequisites for Package Installation

The following software must be installed before installing Cisco Ping:

- Performance Insight 5.3
- Any and all service packs available PI 5.3
- Interface Discovery Datapipe 2.5

You can find information about each service pack, including installation instructions, in the release notes issued with the service pack. The Interface Discovery Datapipe is a prerequisite for the IR ifEntry Datapipe. If you are running version 2.2 or earlier of the IR ifEntry Datapipe, uninstall the old version and install the latest version. If you are running version 2.3, or later, of the IR ifEntry Datapipe, install the upgrade package.

### 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 PI 5.3. Following is an overview of the procedure for installing Cisco Ping in a distributed environment.

## Central Server

- 1 If you are running version 2.2 or earlier of the Interface Discovery Datapipe, remove it.
- 2 Install the following packages simultaneously:
  - Cisco Ping; deploy reports
  - Cisco Ping thresholds sub-package (optional)
  - Interface Reporting ifEntry Datapipe 2.5 *or* UPGRADE\_IRifEntry\_Datapipe\_to\_25
  - Interface Discovery Datapipe 2.5 *or* UPGRADE\_IFEntry\_Disc\_Datapipe\_to\_25

## Each Satellite Server

- 1 If you are running version 2.2 or earlier of the Interface Discovery Datapipe, remove it.
- 2 Install the following packages simultaneously:
  - Cisco Ping
  - Cisco Ping thresholds sub-package (optional)
  - Interface Reporting ifEntry Datapipe 2.5 *or* UPGRADE\_IRifEntry\_Datapipe\_to\_25
  - Interface Discovery Datapipe 2.5 *or* UPGRADE\_IFEntry\_Disc\_Datapipe\_to\_25

## Seeing Threshold Breaches as NNM Alarms

If PI and NNM are integrated, you should install the optional thresholds sub-package, `Cisco_Ping_Threshold`. If you install the optional thresholds sub-package, PI will respond to a threshold breach by sending a breach trap to NNM, where the trap will display as an alarm in the NNM alarm browser. The optional thresholds sub-package cannot operate unless the Thresholds Module is installed. If you are not running any version of the Thresholds Module, Package Manager will install the latest version for you, automatically.

## Multiple Entries in `dsi_server`

Cisco Ping has problems when `dsi_server` contains multiple entries. This can occur on stand-alone systems as well as distributed systems. If multiple entries are present, you will see error messages when you load collection policy data. To avoid this problem, make sure there is one distinct `host_name` in `dsi_server`. Follow these steps:

- 1 Determine whether `dsi_server` contains one or multiple entries:

```
isql -Usa -P
use dpipe_db
go
select distinct host_name from dsi_server
go
```

- 2 If one host name is returned, everything is fine. If multiple entries are returned, set all of them to the same value:

```
update dsi_server set host_name = 'host_name'
go
```

If your system is distributed, substitute the central server `host_name` from `dsi_server` for `host_name`.

- 3 After installation, check `dsi_ping_collection_policy`:

```
isql -Usa -P
use dpipe_db
go
select * from dsi_ping_collection_policy
```

If one record is returned, everything is fine.

## Installing Cisco Ping

Perform the following tasks to install Cisco Ping:

- Task 1: Stop OVPI Timer and extract packages from the report pack CD
- Task 2: If you are running version 2.2 or earlier of the Interface Discover Datapipe, remove it
- Task 3: Install these packages simultaneously:
  - Cisco\_Ping
  - Cisco\_Ping\_Thresholds
  - Cisco\_Ping\_Demo (optional)
  - Interface Discovery Datapipe 2.5
  - or*
  - UPGRADE\_IFEntry\_Disc\_Datapipe\_to\_25
  - Interface Reporting ifEntry Datapipe 2.5
  - or*
  - UPGRADE\_IRifEntry\_Datapipe\_to\_25

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

- 1 Log in to the system. On UNIX systems, log in as root.
- 2 Stop OVPI Timer and wait for processes to terminate.  
On Windows, do the following:
  - a Select **Control Panel > Administrative Tools > Services**.
  - b Select OVPI Timer from the list of services.
  - c From the Action menu, select **Stop**.On UNIX, as root, do one of the following:

```
HP-UX: sh /sbin/init.d/ovpi_timer stop
Sun: sh /etc/init.d/ovpi_timer stop
```
- 3 Insert the report pack 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.

After 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:

- Cisco Ping
- Cisco Ping Thresholds
- Cisco Ping Demo
- UPGRADE\_Ping\_MIB\_to\_42

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

### **Task 2: Uninstall the Interface Discovery Datapipe**

If you are running version 2.2 or earlier of the Interface Discover Datapipe, remove it.

- 1 Click **Next**. The Package Location window opens.
- 2 Click **Uninstall**.
- 3 Click **Next**. The Report Undeployment window opens.
- 4 Click **Next**. The Package Selection window opens.
- 5 Click the check box next to the following packages:  
*IR\_ifEntry\_Datapipe*  
*IFEntry\_Disc\_Datapipe*
- 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 and associated datapipes; restart OVPI Timer**

- 1 Start Package Manager, if it is not already started. The Package Manager welcome window opens.
- 2 Click **Next**. The Package Location window opens.
- 3 Click **Install**.
- 4 Click **Next**. The Report Deployment window opens. Accept the default for Deploy Reports; accept the defaults for application server name and port. Type your user name and password for the OVPI Application Server.
- 5 Click **Next**. The Package Selection window opens.
- 6 Click the check box next to the following packages:  
*Cisco\_Ping 4.2*  
*Cisco\_Ping\_Thresholds*  
*Cisco\_Ping\_Demo*  
*IRifEntry\_Datapipe 2.5* or  
*UPGRADE\_IRifEntry\_Datapipe\_to\_25*  
*IFEntry\_Disc\_Datapipe 2.5* or  
*UPGRADE\_IFEntry\_Disc\_Datapipe\_to\_25*



- 7 Click **Next**. The Type Discovery window opens; accept the default.
- 8 Click **Next**. The Selection Summary window opens.
- 9 Click **Install**. The Installation Progress window opens and the install begins. When the install completes, a package install complete message appears.
- 10 Click **Done**.
- 11 Restart OVPI Timer.

On Windows, do the following:

- a Select **Control Panel > Administrative Tools > Services**.
- b Select OVPI Timer from the list of services.
- c From the Action menu, select **Start**.

On UNIX, as root, do one of the following:

```
HP-UX: sh /sbin/init.d/ovpi_timer start
Sun: sh /etc/init.d/ovpi_timer start
```

## Accessing Deployed Reports

Before reports can be viewed, they must be deployed. When you installed the Cisco Ping Report Pack, you enabled the Deploy Reports option. As a result, the reports in this package were deployed to the OVPI Application Server. Once reports reside on the OVPI Application Server, you have two ways to view them:

- OVPI client applications
- Web browser

If the OVPI client applications are installed on the user's system, the user has access to Report Viewer, Report Builder, and the Management Console. If the client components are not installed on the user's system, the user will need a web browser to view reports.

For more information about the client applications refer to the *PI Installation Guide*. For more information about the Management Console, including how to use the Object/Property Management view to launch reports specific to a selected object, see the *PI 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.

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

On Windows, do the following:

- a Select **Control Panel > Administrative Tools > Services**.
- b Select OVPI Timer from the list of services.
- c From the Action menu, select **Stop**.

On UNIX, as root, do one of the following:

```
HP-UX: sh /sbin/init.d/ovpi_timer stop
```

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

- 3 Start Package Manager. The Package Manager welcome window opens.
- 4 Click **Next**. The Package Location window opens.
- 5 Click **Uninstall**.
- 6 Click **Next**. The Report Undeployment window opens.
- 7 Click **Next**. The Package Selection window opens.
- 8 Click the check box next to the following packages:
  - Cisco\_Ping*
  - Cisco\_Ping\_Thresholds* (if installed)
  - Cisco\_Ping\_Demo* (if installed)
- 9 Click **Next**. The Selection Summary window opens.
- 10 Click **Uninstall**. The Progress window opens and removal begins. When removal finishes, a package removal complete message appears.
- 11 Click **Done**.
- 12 Restart OVPI Timer.

On Windows, do the following:

- a Select **Control Panel > Administrative Tools > Services**.
- b Select OVPI Timer from the list of services.
- c From the Action menu, select **Start**.

On UNIX, as root, do one of the following:

```
HP-UX: sh /sbin/init.d/ovpi_timer start
```

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

## 4 Action Poller User Interface

This chapter covers the following topics:

- Launching the Action Poller User Interface
- Defining node pairs
- MIBlet groups
- Assigning instances to nodes
- Modifying parameter sets
- Exiting 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 **Remove** 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 be added only 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 finish, 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 level, 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 **Parameter Sets** 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.

<b>Parameter</b>	<b>Description</b>
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.

## Exiting the Interface

You can terminate the interface in either of these ways:

- Click **Close** on the initial collection window.
- Select **File > Exit**.

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

# 5 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 intend to run Cisco Ping in a distributed system, you had to install the report pack on the central server and on each satellite server. Now that installation is complete, perform the following tasks:

- Configure the central server.
- Configure the satellite server(s).

### Configuring the Central Server

To configure the central server, perform the following tasks:

- Task 1: Register the satellite server by setting the database role
- Task 2: If you are not copying rate data from satellite servers to the central, enable LIR
- Task 3: If you enable LIR, add LIR mappings
- Task 4: Verify the automatically generated copy policies
- Task 5: Delete LIR mappings for rate tables
- Task 6: Modify the `trendtimer.sched` file

#### Task 1: Register the satellite server by setting the database role

- 1 Start the Management Console (log on with Administrator privileges).
- 2 Click the **Systems** icon in the navigation pane.
- 3 Navigate to the OVPI Databases folder and select the database system.
- 4 Click **Database Properties**.
- 5 From the Database Role list, select the Satellite Server role.

6 Enter any information necessary to configure the Satellite Server role.



To add a new database reference, you can use the Add Database Reference Wizard in the System and Network Administration application.

#### Task 2: Enable LIR

- 1 Start the Management Console (log on with Administrator privileges).
- 2 Click the **Systems** icon in the navigation pane.
- 3 Navigate to the OVPI Databases folder and select the central server.
- 4 Click **LIR Configuration**.
- 5 Select the **LIR enabled** check box.

#### Task 3: Add LIR mappings

- 1 Start the Management Console (log on with Administrator privileges).
- 2 Click the **Systems** icon in the navigation pane.
- 3 Navigate to the OVPI Databases folder and select the central server.
- 4 Click **LIR Configuration**.
- 5 Click **Add Mapping**.
- 6 From the Select Satellite Server list, select a satellite server to which to add a mapping.
- 7 Select the **Category** data table option.
- 8 Select **Cisco Ping** from the drop down list.
- 9 Select the **rate** data type.
- 10 Click **Add to List**.
- 11 If you want to add additional LIR mappings, click **Add to list** and repeat [step 6](#) through [step 10](#).
- 12 Click **OK**.
- 13 Click **Apply**.

A copy policy is automatically generated for the hourly data and for each LIR mapping that you add. The data type selected when adding an LIR mapping (in step 9 above) determines the type of data copied (defined in the generated copy policy). The type of data copied (defined in the generated copy policy) is one greater than the data type selected in the LIR mapping. For example, if you select an hourly data type, you will generate a daily data copy policy.

#### Task 4: Verify the automatically generated copy policies

Verify that a copy policy has been generated for the following tables and that the copy type is set correctly (to Property and Data):

- 1 Start the Management Console (log on with Administrator privileges).
- 2 Click the **Copy Policy** icon in the navigation pane to start the Copy Policy Manager.



3 Find the following tables and verify the copy type is set to Property and Data for each table:

- RPinG\_MIB\_base
- SHcisco\_ping\_rtd\_

If a copy policy has not been generated for a table, do the following:

- 1 Click the **New Copy Policy** icon or select **File > New Copy Policy** from the Copy Policy Manager. The Copy Policy Wizard displays.
- 2 Click **Next**. The Satellite Server and Copy Policy Selection Page displays.
- 3 Select a satellite server from the pull down list. This is the satellite server from which data is copied to the central server.
- 4 Select **Single Table** and select the table from the pull down list.
- 5 Click **Next**. The Copy Type Selection Page displays.
- 6 Select **Property and Data**.
- 7 Click **Next**. The Summary page displays.
- 8 Verify the information in the summary window. If the information is not correct, you can modify it by clicking Back.
- 9 Click **Finish**.
- 10 Repeat [step 4](#) - [step 9](#) for all missing tables.

If the copy type is not set to Property and Data, do the following:

- 1 Double-click the copy policy.
- 2 Select the **Property and Data** copy type.
- 3 Click **OK**.

#### Task 5: [Delete LIR Mappings for the RPinG\\_MIB\\_base rate table](#)

Delete the LIR mappings for RPinG\_MIB\_base (the data is being copied to the central server).

- 1 Start the Management Console (log on with Administrator privileges).
- 2 Click the **Systems** icon in the navigation pane.
- 3 Navigate to the OVPI Databases folder and select the central server.
- 4 Click **LIR Configuration**.
- 5 Unselect the Rate check box for Kisco\_ping\_rtd\_.
- 6 Click **Apply**.

#### Task 6: [Modify the trendtimer.sched file](#)

The `trendtimer.sched` file is found in the `{DPIPE_HOME}/lib/` directory where `{DPIPE_HOME}` is the directory in which OVPI is installed.

Make the following change to this file:

- Find and comment out the following line:

```
1:00+40 - - {DPIPE_HOME}/bin/trend_proc -f {DPIPE_HOME}/scripts/Ping_MIB_Sum.pro
```

## Configuring a Satellite Server

Follow these steps to configure each satellite server.

- 1 Modify the `{DPIPE_HOME}/lib/trendtimer.sched` file (where `{DPIPE_HOME}` is the directory in which OVPI is installed) by switching off interface aggregations above the hourly level.
  - Find and comment out the following line:

```
24:00+3:00 - - {DPIPE_HOME}/bin/trend_proc -f
{DPIPE_HOME}/scripts/Ping_MIB_Daily.pro
```
- 2 Modify the `{DPIPE_HOME}/scripts/Ping_MIB_Sum.pro` file (where `{DPIPE_HOME}` is the directory in which OVPI is installed) by enabling the trendcopy commands to push data to the central server. Uncomment all trendcopy commands.
- 3 Make sure that the system clock on each satellite server is synchronized with the system clock on the central server.
- 4 Verify that you do not have servers polling the same device.

## 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. After the Action Poller user interface has launched, only interfaces that have been discovered, and interfaces that have collected interface data, will 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

The Ping\_MIB\_Property.dat file serves 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

Seq	Column Name	Description
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 if the import fails, consider exporting existing property information from OVPI. Edit the file exported by OVPI, then re-import the updated 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 equals 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 trendtimer 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, and 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 that any value other than 0 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 change the interval for the collections from the default, simply change 15 to the desired interval. Here is what a 60-minute interval would look like:

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

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





---

## 6 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 and the Update Threshold Values are accessible from the Management Console. Both of these forms are context sensitive, which means that the only nodes you will modify are the nodes you selected before you launched the form. The other forms must be loaded using Report Builder or Report Viewer.

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.

C:\ovpi\packages\Ping\_MIB\Ping\_MIB.ap\Cisco\_Ping\_forms\config\_...

# 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**   
**Poller Name**   
**Polling Interval**

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


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

Dst Parameters	Pkt Cnt	Pkt Size	Pkt Timeout	Delay
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

Packet Size


Packet Timeout

Packet Delay

OK Apply Cancel

C:\ovpi\packages\Ping\_MIB\Ping\_MIB.ap\Cisco\_Ping\_forms\update\_dev\_pair\_params.frep

# 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

Packet Size


Packet Timeout

Packet Delay

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**

**Destination**

**Sample ID**

**RTT Threshold**

**Discard Threshold**

**CPU Threshold**

**Interface Threshold**

---

## 7 Worst Performing Node Pairs

The Worst Performing Pairs report looks at yesterday's activity and ranks node pairs in two ways:

- 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 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 and packet delivery ratio respectively. Drilling down to either chart shows the detailed metrics for the node pair collected over a day. Select a customer (left) and a node pair (right) to get the drill down information.

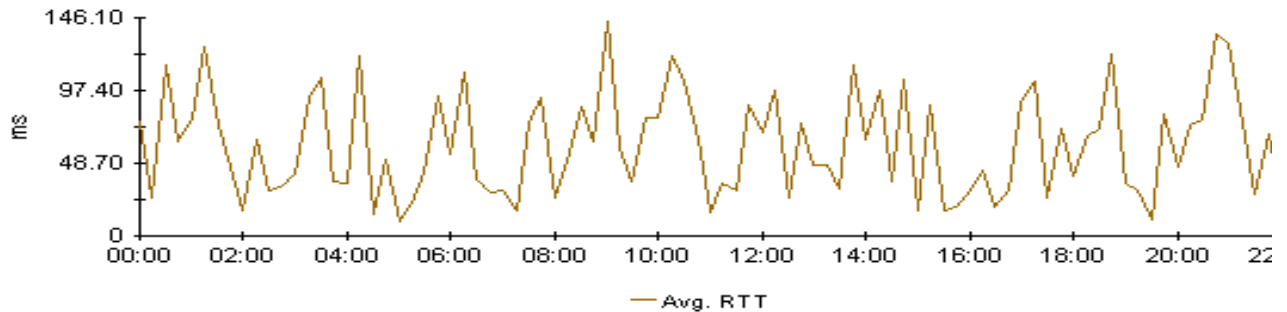
### Worst Performing Node Pairs, Ranked by Round Trip Time

Customers	Node Pair	RTT	De
All			
Unassigned Customer	amsterdam.desktalk.com -> atlanta.desktalk.com	127.00	
	sanjose.desktalk.com -> sydney.desktalk.com	19.00	
	sanjose.desktalk.com -> london.desktalk.com	18.00	
	sanjose.desktalk.com -> chicago.desktalk.com	18.00	
	sanjose.desktalk.com -> newyork.desktalk.com	17.00	
	sanjose.desktalk.com -> lasvegas.desktalk.com	15.00	

RTT | Delivery | CPU Utilization | Interface Util.

### Average Round Trip Time

amsterdam.desktalk.com -> atlanta.desktalk.com  
Mon Sep 30 12:00 AM



### 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 interface utilization are 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

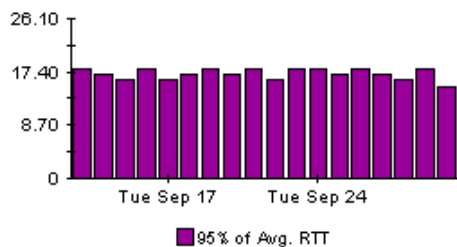
### Node Pairs

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

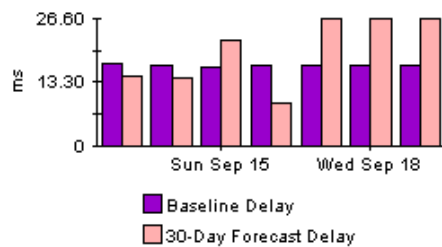
sanjose.desktalk.com -> lasvegas.desktalk.com  
 Fri Sep 13 2002 - Mon Sep 30 2002



RTT: BL & F30 | Delivery: BL & F30

#### Baseline & 30-Day Forecast RTT (P95)

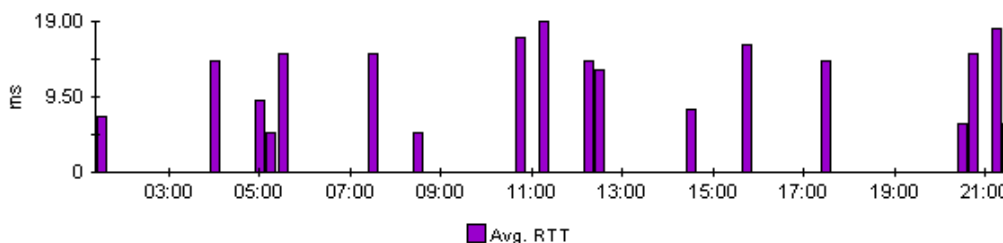
sanjose.desktalk.com -> lasvegas.desktalk.com  
 Fri Sep 13 2002 - Thu Sep 19 2002



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







---

## 9 Sample Data in Near Real Time

The Near Real Time report provides access to sample data collected over the last six hours. This report is available in two formats, 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. Use this table to 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, 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

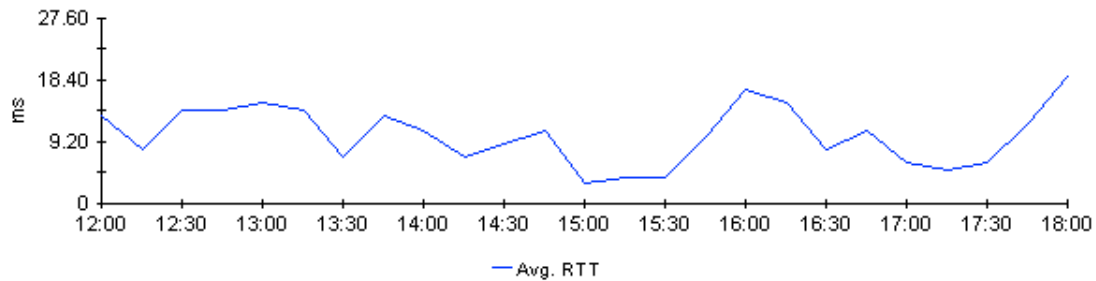


The QuickView Near Real Time Report displays the 95th percentile round trip time and packet delivery ratio for the selected customer (left) and node pair (right) over the over the last six hours period and provides a visual correlation with the corresponding CPU and interface utilizations.

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

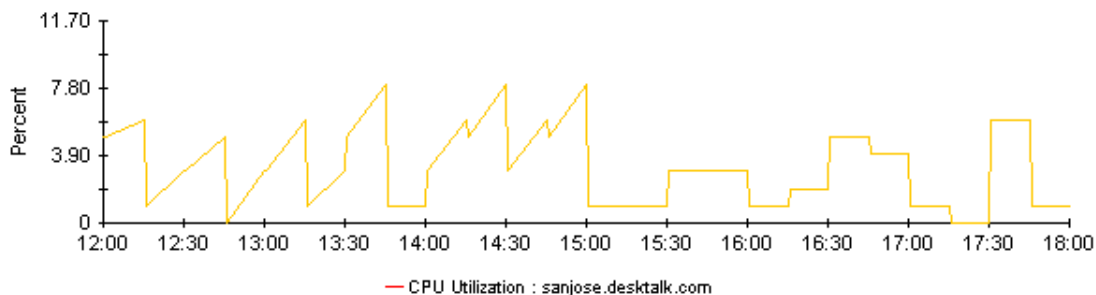
RTT | Delivery |

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



CPU Utilization | Interface Util. |

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









---

## 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, Daily QuickView/Daily Snapshot](#), 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.

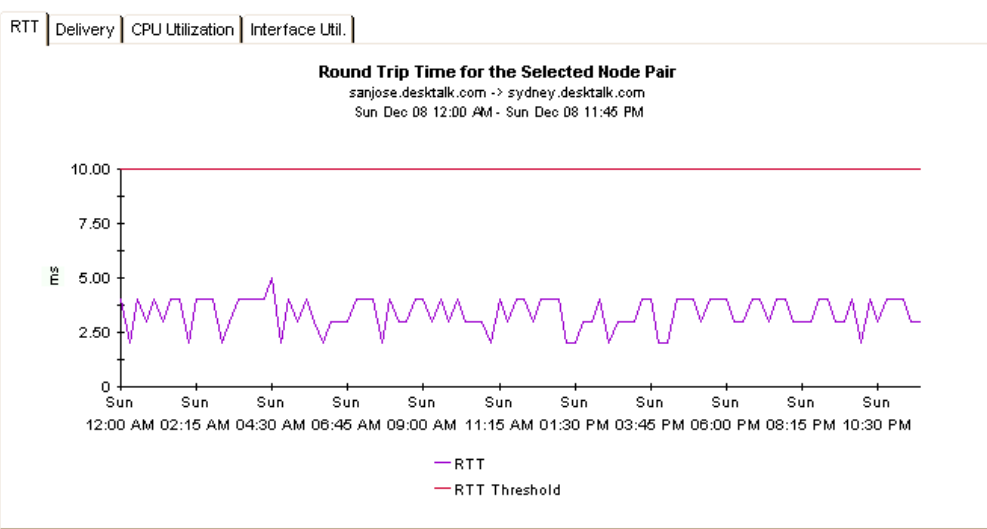
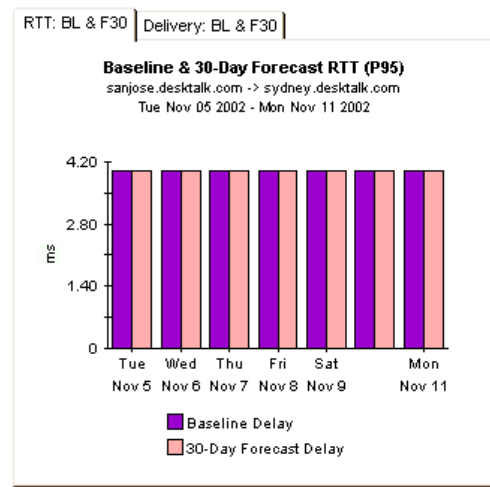
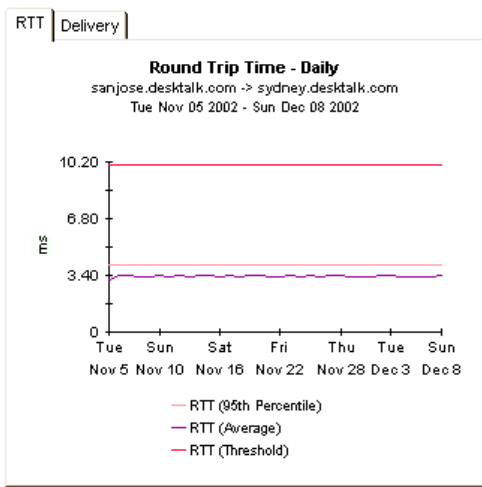
# Cisco Ping

## 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.

Customers	Node Pairs with the Highest Number of Breaches		
Acme	Mon Jan 20 2003		
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



---

# 11 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:

- The type of breach that occurred
- The average RTT in effect at that time
- The 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.

## 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.

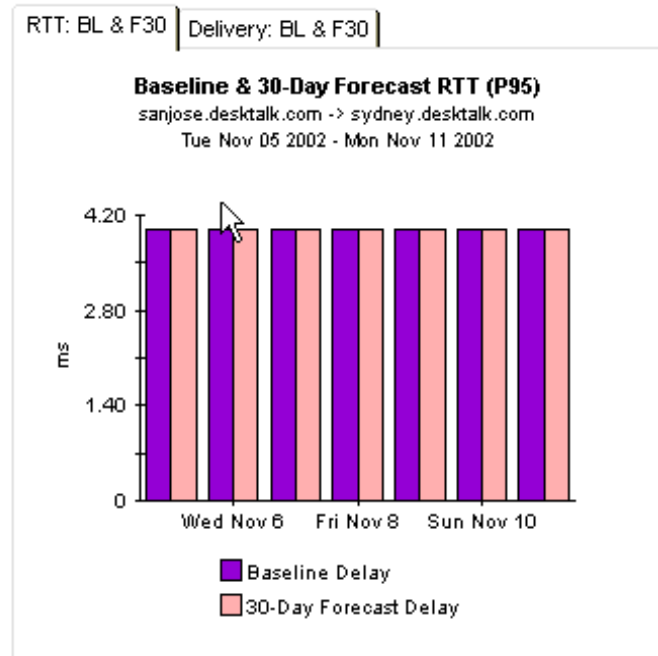
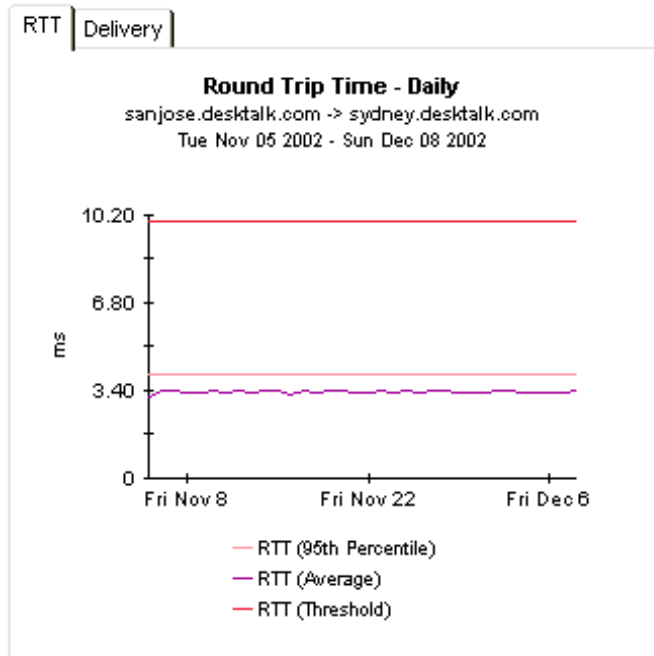
### Customers

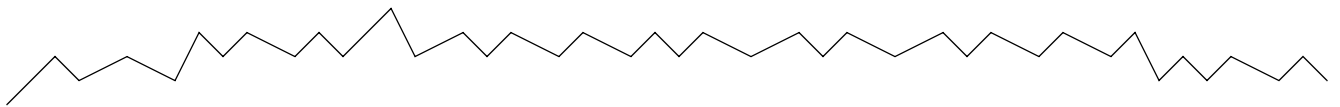
Acme
Trinagy

### 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



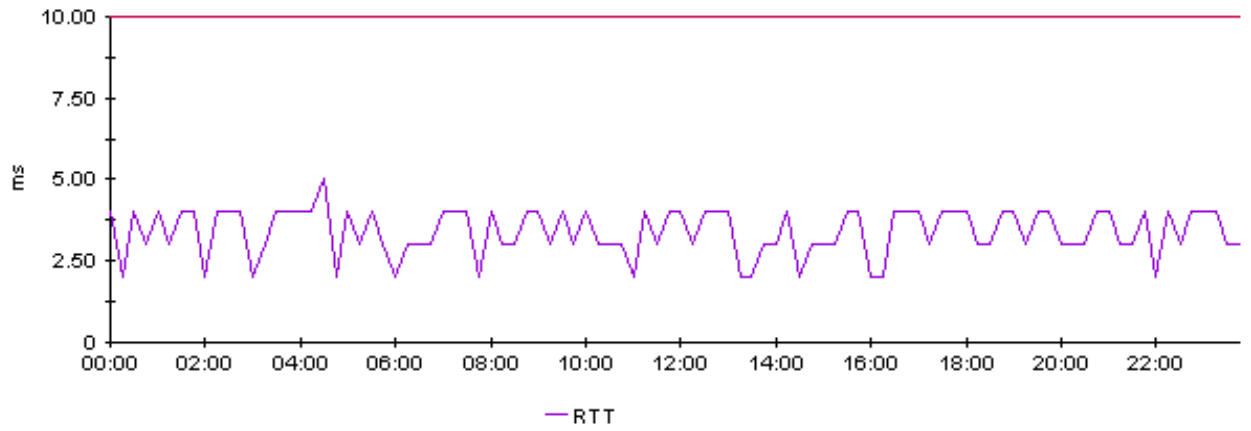


RTT | Delivery | CPU Utilization | Interface Util.

### 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



---

# Cisco Ping

## Performance Threshold Breaches -- Monthly Summary

---

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

### Customers

Acme

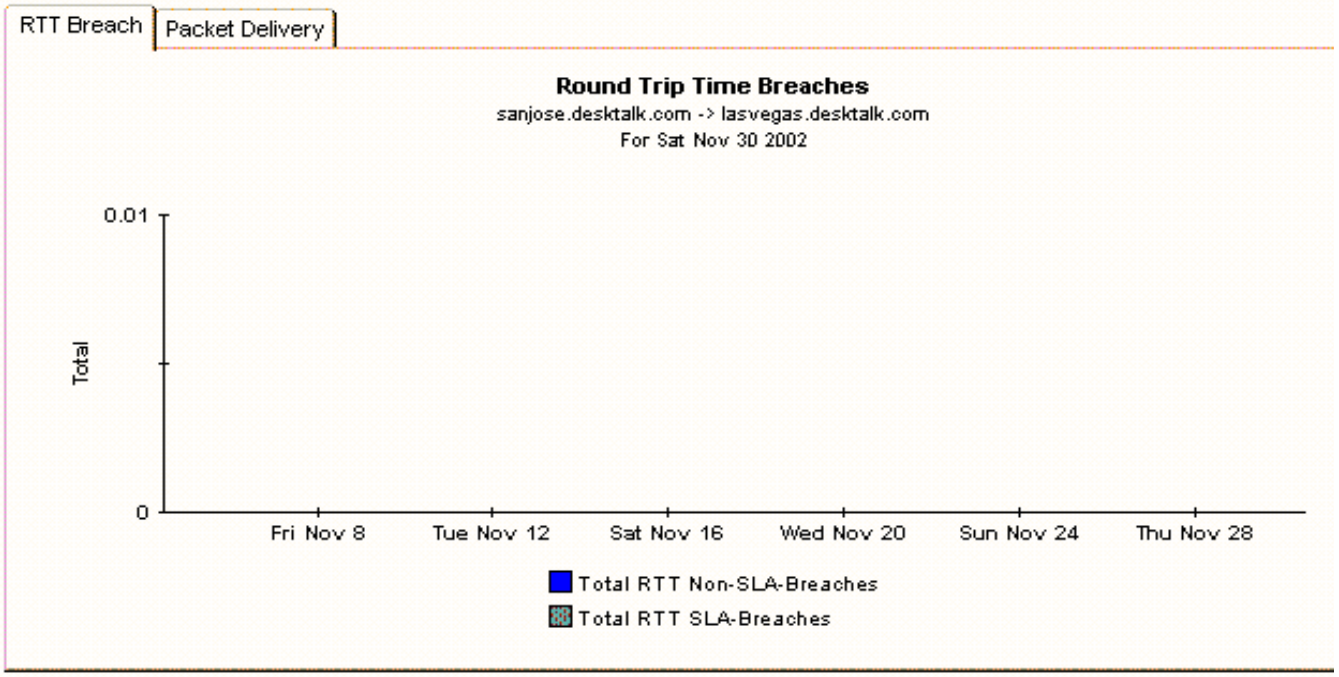
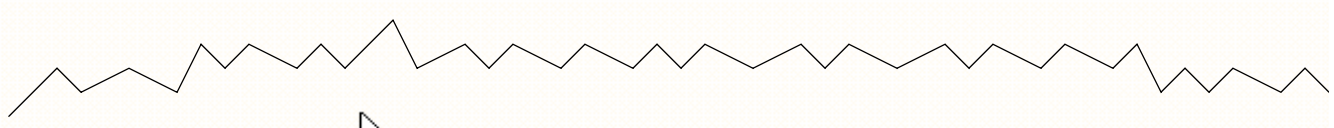
Trinagy

### SLA Breach Counts for Last Month

Nov 2002

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









---

## 12 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



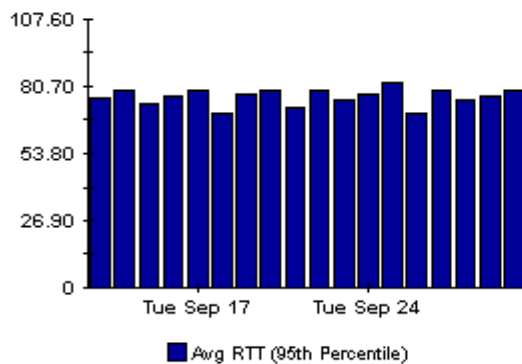
The Executive Summary Report provides hourly and daily aggregate performance of the network across all node pairs over the last month, and over the last day. Select a customer from the table below to view the aggregates of the 95th percentile round trip time and the packet delivery ratio.

### Customers

All
Unassigned Customer

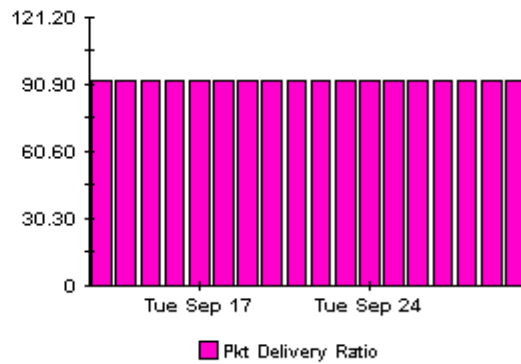
**Daily Aggregate RTT (95th percentile)**

Fri Sep 13 2002 - Mon Sep 30 2002



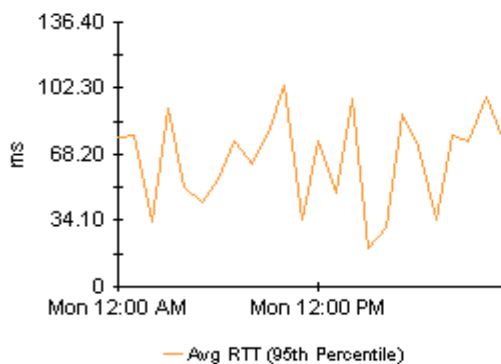
**Daily Aggregate Packet Delivery Ratio**

Fri Sep 13 2002 - Mon Sep 30 2002



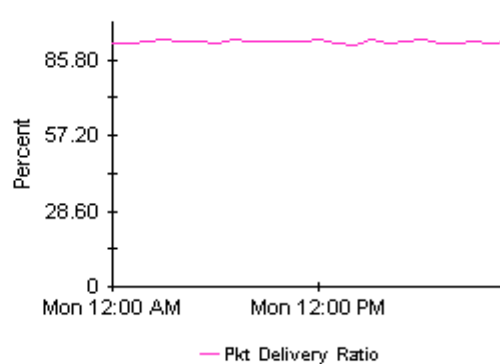
**Hourly Aggregate RTT (95th percentile)**

Mon Sep 30 2002



**Hourly Aggregate Packet Delivery Ratio**

Mon Sep 30 2002







---

# 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 among 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

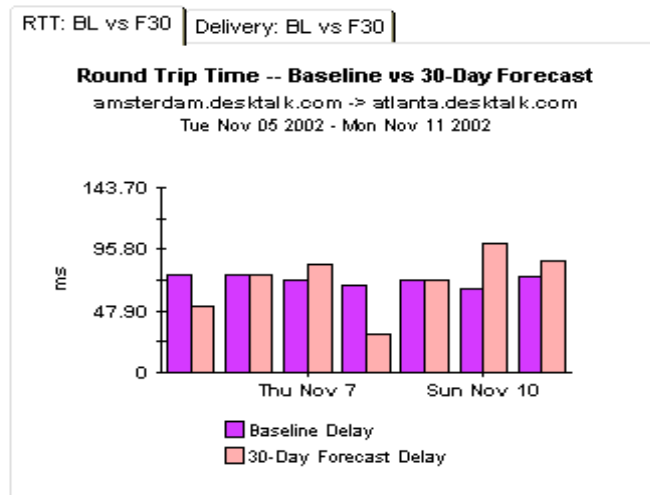
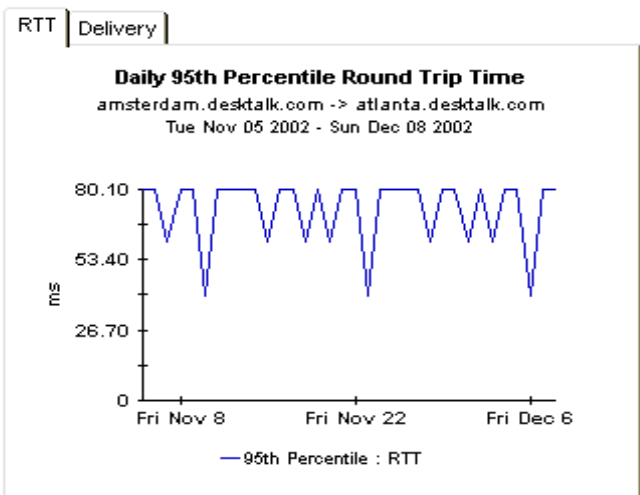
Acme

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



---

# 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 (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\_ping\_.

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 Software.



## 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
<code>ifSpeed</code>	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.
<code>ifInOctets</code>	1.3.6.1.2.1.2.2.1.10	Total number of octets received on the interface, including framing characters.
<code>ifOutOctets</code>	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
<code>PingDaily_bykey.sum</code>	Hourly data for all device pairs by day and by key.
<code>PingHourly_bykey.sum</code>	Rate data for all device pairs by day and by key.
<code>PingDaily_allpairs.sum</code>	Hourly data for all device pairs by day.
<code>PingHourly_allpairs.sum</code>	Rate data for all device pairs by hour.
<code>PingHourly_allpairs_by_cust_id.sum</code>	Rate data for all device pairs by hour and by <code>cust_id</code> .
<code>PingDOW_BL_and_FC_bykey.sum</code>	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.

<b>Variable</b>	<b>OID String</b>	<b>Description</b>
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.

---

# Glossary

## **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.



# A Version History

<b>Version</b>	<b>Release Date</b>	<b>Enhancements</b>
1.0	July 2001	Action Poller User Interface 10 reports: <ul style="list-style-type: none"><li>• Executive Summary</li><li>• Forecast</li><li>• Worst Performing Pairs</li><li>• Daily QuickView</li><li>• Daily Snapshot</li><li>• Threshold Near Real Time QuickView</li><li>• Threshold Near Real Time Snapshot</li><li>• Threshold Daily QuickView</li><li>• Threshold Summary Daily</li><li>• Threshold Summary Monthly</li></ul>
2.0	October 2002	<i>new upgrade package:</i> UPGRADE_Cisco_Ping_10_to_20
3.0	October 2003	<i>new features:</i> <ul style="list-style-type: none"><li>• OVPI 4.6 support</li><li>• OVPI Object Manager support</li></ul> <i>new forms:</i> <ul style="list-style-type: none"><li>• Configure Collection Group</li><li>• Configure Device Pairs</li><li>• Create Device Pair Parameters</li><li>• Update Device Pair Parameters</li><li>• Update Thresholds</li></ul> <i>new upgrade package:</i> <ul style="list-style-type: none"><li>• UPGRADE_Cisco_Ping 20_to_30.ap</li></ul>
4.0	April 2004	<i>new feature:</i> <ul style="list-style-type: none"><li>• OVPI 5.0 support</li></ul>
4.0	June 2005	<i>new feature:</i> OVPI 5.1 support <i>new upgrade package:</i> <ul style="list-style-type: none"><li>• UPGRADE_Cisco_Ping_to_40.ap</li></ul>

Version	Release Date	Enhancements
4.1	April 2007	<p><i>new features:</i></p> <ul style="list-style-type: none"> <li>• LIR Configuration (in OVPI 5.2)</li> <li>• Copy Policy Manager (in OVPI 5.2)</li> <li>• Rate data removed from top level table in NRT reports</li> </ul> <p><i>new upgrade package:</i></p> <ul style="list-style-type: none"> <li>• UPGRADE_Ping_MIB_to_41.ap</li> </ul> <p><i>defect fixes:</i></p> <ul style="list-style-type: none"> <li>• QXCR1000221971</li> <li>• QXCR1000412603</li> </ul>



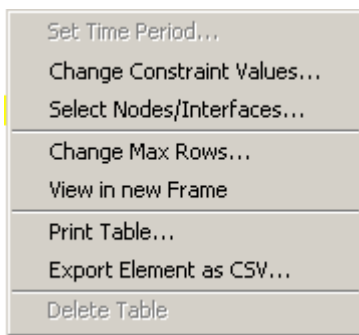
## B Editing Tables and Graphs

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

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

### View Options for Tables

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



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

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

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

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

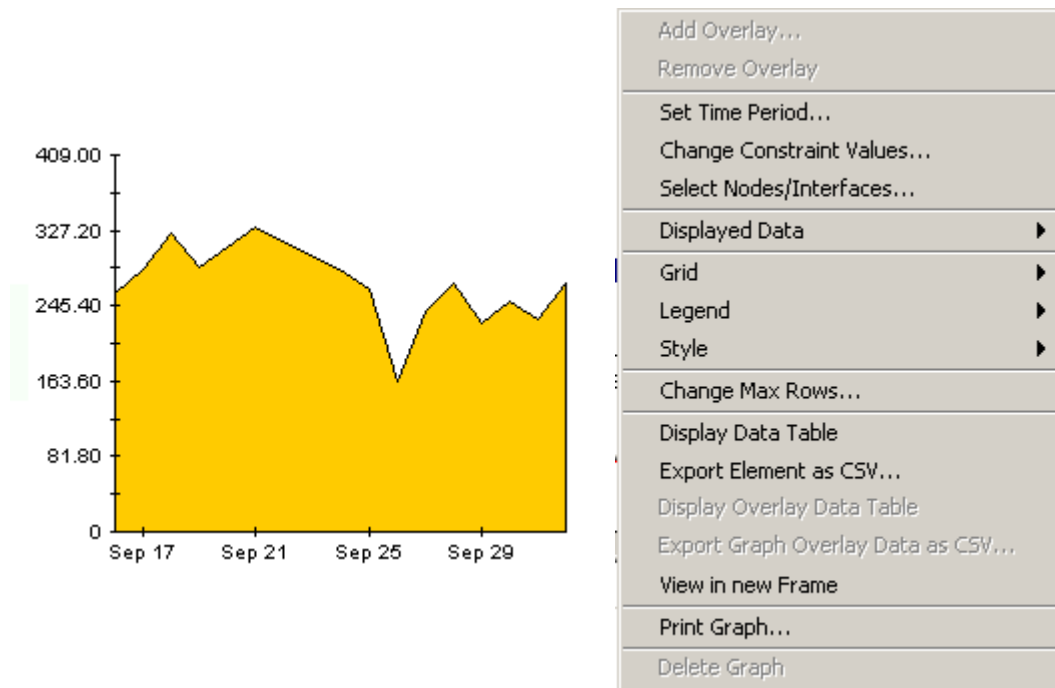
**Change Max Rows** increases or decreases the number of rows in a table. The default is 50. If you expand the default, the table may take more time to open. If you are trending a large network, using the default ensures that the table opens as quickly as possible.

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

Polled IP QoS Statistics Data - Input Over Previous 6 Hours					
Direction	IpPrecedence	Switched Bytes	Switched Pkts	Time Period	
Input	0	105,888	675	Tue Oct 29 07:00 AM	
Input	1	0	0	Tue Oct 29 07:00 AM	
Input	2	0	0	Tue Oct 29 07:00 AM	
Input	3	0	0	Tue Oct 29 07:00 AM	
Input	4	0	0	Tue Oct 29 07:00 AM	
Input	5	0	0	Tue Oct 29 07:00 AM	
Input	6	600	5	Tue Oct 29 07:00 AM	
Input	7	0	0	Tue Oct 29 07:00 AM	
Input	0	98,334	638	Tue Oct 29 06:45 AM	
Input	1	0	0	Tue Oct 29 06:45 AM	
Input	2	0	0	Tue Oct 29 06:45 AM	
Input	3	0	0	Tue Oct 29 06:45 AM	
Input	4	0	0	Tue Oct 29 06:45 AM	

## View Options for Graphs

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

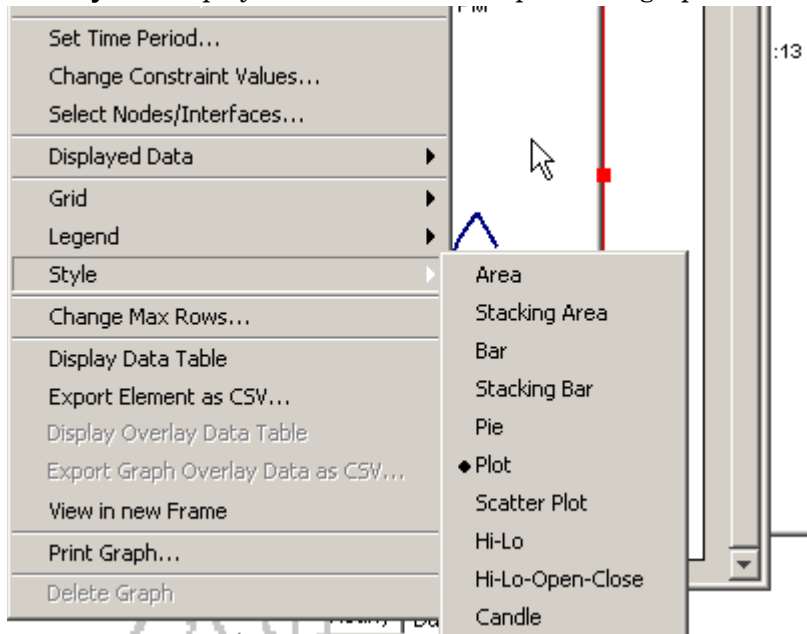


The following table provides details about each option.

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

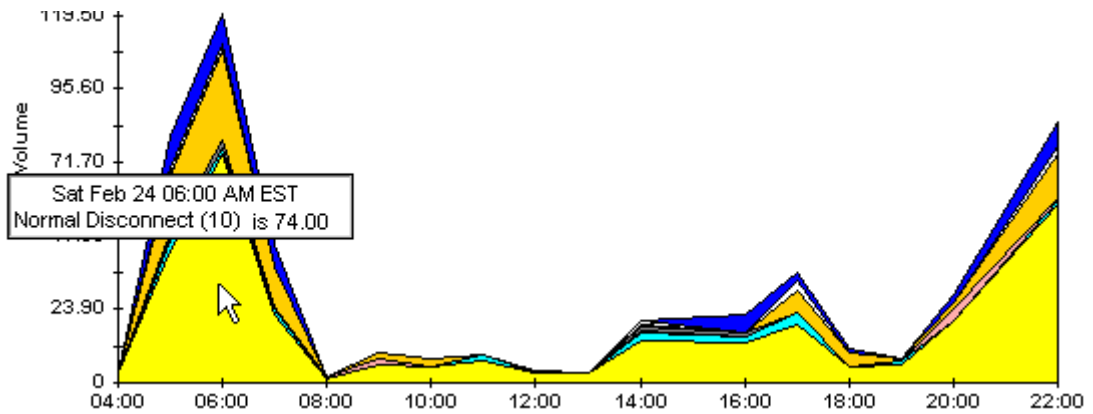
## Style Options

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



## Style > Area

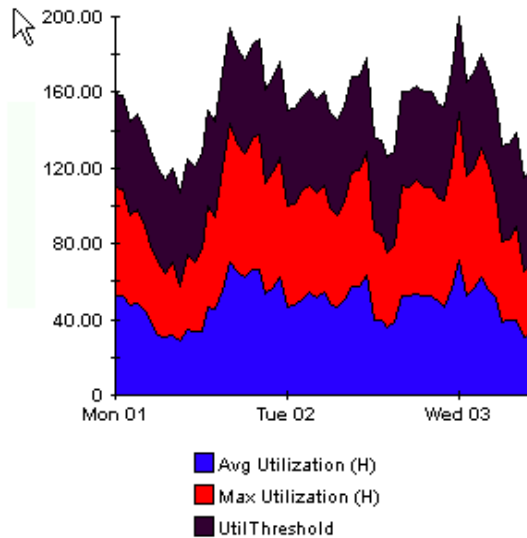
The plot or bar chart changes to an area graph. While relative values and total values are easy to view in this format, absolute values for smaller data types may be hard to see. Click anywhere within a band of color to display the exact value for that location.



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

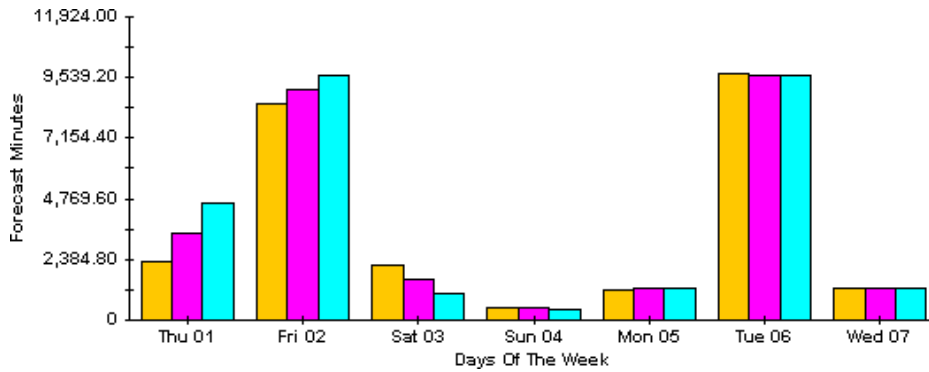
## Style > Stacking Area

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



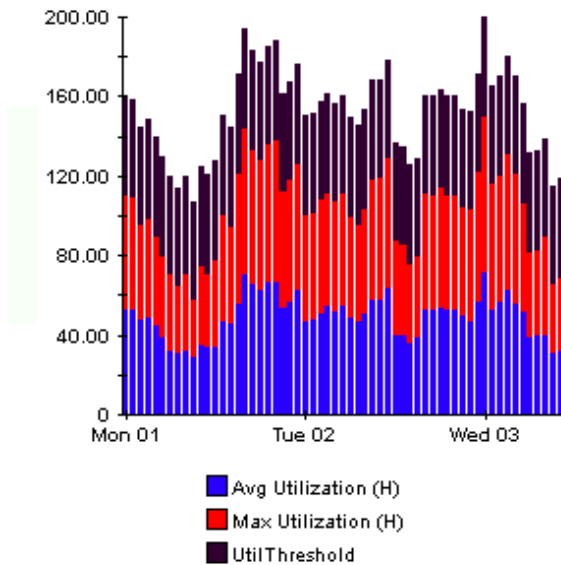
## Style > Bar

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



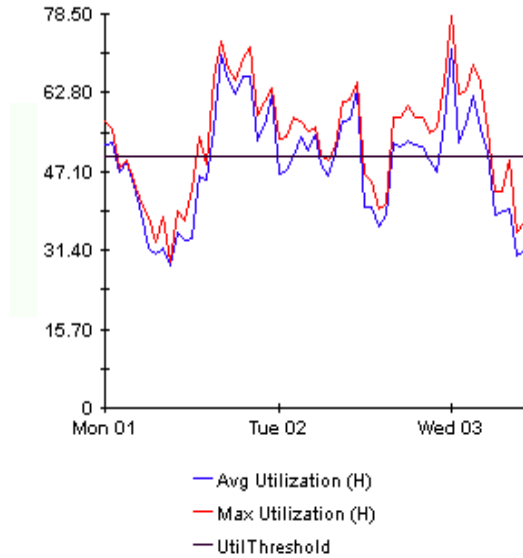
## Style > Stacking Bar

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



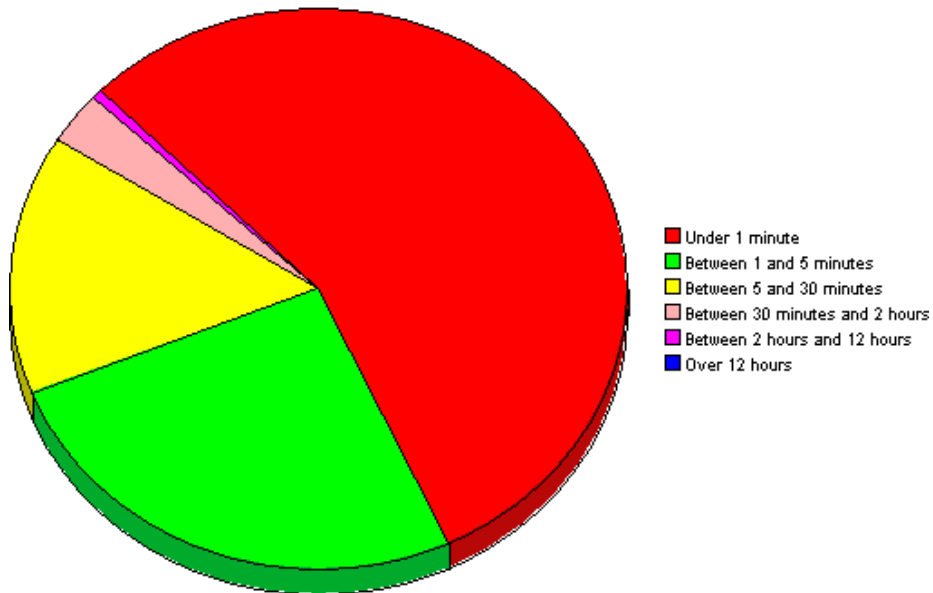
## Style > Plot

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



## Style > Pie

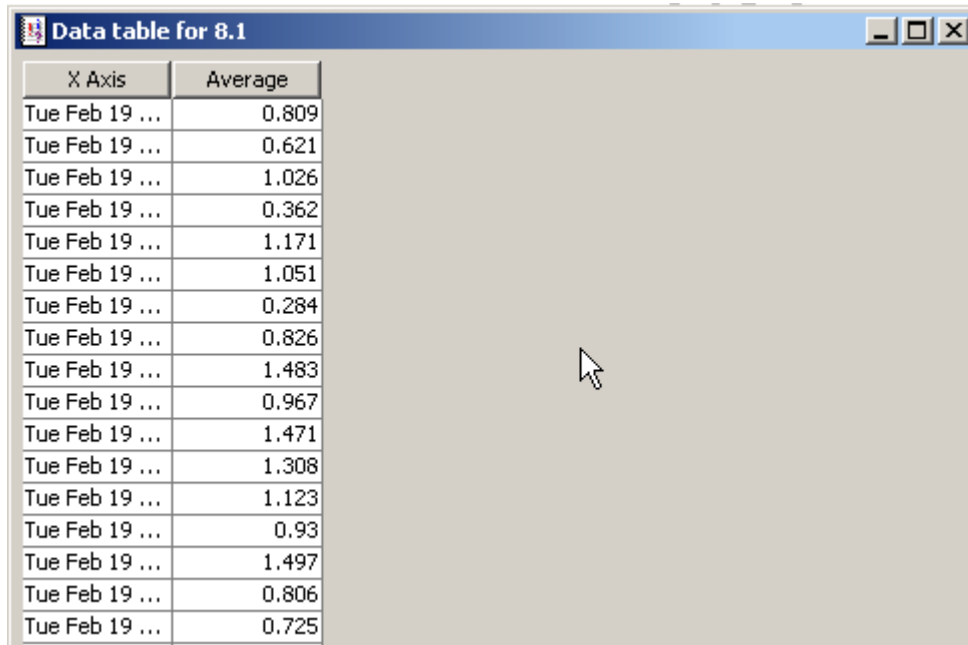
An area graph becomes a pie chart. Bands in an area graph convert to slices of a pie and the pie constitutes a 24-hour period. This view is helpful when a small number of data values are represented and you are looking at data for one day.



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

## Display Data Table

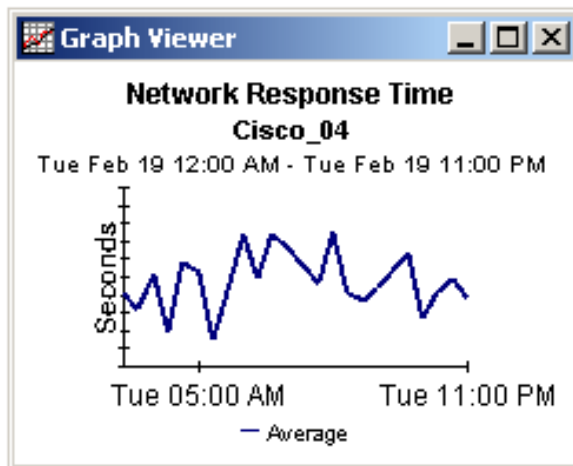
This option changes a graph into a spreadsheet.



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

## View in New Frame

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







# Index

## A

ActionDatapipe, 35

Action Poller

- adding a new collection group, 23
- changing an existing parameter set, 25
- changing the collection interval, 35
- command line option, 34
- defining node pairs, 24
- invoking, 23
- node pair properties, 24
- removing node pairs, 24

adding a collection group definition, 23

avg volume, 71

## B

baseline busy hour, 71

basic\_interface\_info (MIBlet), 69

busy hour, 71

## C

capacity planning, 4, 9

change max rows option, 79

cisco\_system MIBlet, 25

Cisco Ping MIB, 5, 9

Cisco System MIBlet, 5, 9

collection group, 25

Configure Collection Group form, 37

Configure Device Pairs form, 37

Copy Policy Manager, 28, 29

Create Device Pair Parameters form, 37

customer-specific reports, 8, 9

## D

daily, 71

day of week, 71

demo package, 9, 13, 20

deploying reports, 21

destination MIBlet instance, 25

destination node, 26

device, 71

discard exceptions, 4, 9

discard rate, 71

discard threshold, 71

Display Data Table, 79

displayed data option, 79

distributed systems, 11, 17

dummy polls, 33

## E

error messages, 7, 9

error rate, 72

error threshold, 72

## F

F30, 72

F60, 72

F90, 72

forms

Configure Collection Group, 37

Configure Device Pairs, 37

Create Device Pair Parameters, 37

Update Device Pair Parameters, 37

Update Threshold Values, 37

## G

grid options, 79

group, 72

group filters, 8, 9

growth rate, 72

## H

hourly, 72

## I

- ifInOctets (variable), 69
- ifOutOctets (variable), 69
- ifSpeed (variable), 69
- initializing property tables, 33
- interface, 72
- interface\_rtd\_png\_, 24
- Interface Discovery Datapipe, 17, 20
- Interface Reporting Basic Info MIBlet, 5, 9
- IR ifEntry Datapipe, 17

## L

- legend options, 79
- LIR Configuration, 28

## M

- MIBs
  - Cisco Ping MIB, 5, 9
  - Cisco System MIBlet, 5, 9
  - Interface Reporting Basic Info MIBlet, 5, 9
- MIB variables
  - cisco\_system MIBlet, 68
  - Cisco Ping MIB, 68
  - interface-reporting\_basic\_interface\_info MIBlet, 69
- monthly, 72
- multiple entries in dsi\_server, 18
- mw\_collect, 33

## O

- OVPI Timer
  - starting, 15

## P

- packet delivery ratios, 6, 9
- packets\_received, 68
- packets\_sent, 68
- parameters
  - delay, 26
  - packet count, 26
  - packet size, 26
  - packet timeout, 26
- Ping\_MIB\_Property.dat, 31
- Ping\_MIB\_Thresholds, 14
- polling interval, 34

- polling policy, 33
- port number, 34
- Product Manuals Search (web page), 9

## R

- remove node pair, 24
- report parameters, 8, 9
- response time, 72
- round trip time, 68
- route availability, 6, 9

## S

- satellite servers, 30
- SNMP SET request, 6, 9
- source
  - MIB, 68
  - table, 70
- SourceDirectory path, 33
- source instance of each MIBlet, 25
- source MIBlet instance, 25
- style options for graphs, 79
- summaries
  - PingDaily\_allpairs.sum, 69
  - PingDaily\_bykey.sum, 69
  - PingDOW\_BL\_and\_FC\_bykey.sum, 69
  - PingHourly\_allpairs.sum, 69
  - PingHourly\_allpairs\_by\_cust\_id.sum, 69
  - PingHourly\_bykey.sum, 69
- system clocks, 30

## T

- TEEL files, 32
- threshold, 72
- Threshold Breaches Summary, 55
- Threshold Daily QuickView, 53
- thresholds
  - discard, 71
  - error, 72
  - Threshold Breaches Summary, 55
  - Threshold Daily QuickView, 53
  - Thresholds NRT QuickView, 49
  - utilization, 73
- Thresholds NRT QuickView, 49
- trend.log, 7, 9

## U

unavailable route, 6, 9

unknown, 30

unsuccessful pings, 6, 9

Update Device Pair Parameters form, 37

Update Threshold Values form, 37

UPGRADE\_Ping\_MIB\_to\_41, 14

Use Absolute Time, 77

utilization, 73

utilization threshold, 73

## V

view in new frame, 78

## X

xcpu\_util\_rtd\_png\_ (MIBlet), 24, 68

