This documentation (the "Documentation") and related computer software program (the "Software") (hereinafter collectively referred to as the "Product") is for the end user’s informational purposes only and is subject to change or withdrawal by CA at any time.

This Product may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Product is confidential and proprietary information of CA and protected by the copyright laws of the United States and international treaties.

Notwithstanding the foregoing, licensed users may print a reasonable number of copies of the Documentation for their own internal use, and may make one copy of the Software as reasonably required for back-up and disaster recovery purposes, provided that all CA copyright notices and legends are affixed to each reproduced copy. Only authorized employees, consultants, or agents of the user who are bound by the provisions of the license for the Software are permitted to have access to such copies.

The right to print copies of the Documentation and to make a copy of the Software is limited to the period during which the license for the Product remains in full force and effect. Should the license terminate for any reason, it shall be the user’s responsibility to certify in writing to CA that all copies and partial copies of the Product have been returned to CA or destroyed.

EXCEPT AS OTHERWISE STATED IN THE APPLICABLE LICENSE AGREEMENT, TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS PRODUCT “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO THE END USER OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS PRODUCT, INCLUDING WITHOUT LIMITATION, LOST PROFITS, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED OF SUCH LOSS OR DAMAGE.

The use of this Product and any product referenced in the Documentation is governed by the end user’s applicable license agreement.

The manufacturer of this Product is CA.

This Product is provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7013(c)(1)(ii), as applicable, or their successors.

All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Copyright © 2006 CA. All rights reserved.
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Preface</strong></td>
<td>5</td>
</tr>
<tr>
<td>Audience</td>
<td>5</td>
</tr>
<tr>
<td>About This Guide</td>
<td>5</td>
</tr>
<tr>
<td>Reading Path</td>
<td>5</td>
</tr>
<tr>
<td>Revision Information</td>
<td>6</td>
</tr>
<tr>
<td>Documentation Conventions</td>
<td>6</td>
</tr>
<tr>
<td>Technical Support</td>
<td>6</td>
</tr>
<tr>
<td><strong>Chapter 1</strong></td>
<td>7</td>
</tr>
<tr>
<td>Introduction to eHealth — Response</td>
<td>7</td>
</tr>
<tr>
<td>What is eHealth — Response</td>
<td>7</td>
</tr>
<tr>
<td>Application Response</td>
<td>8</td>
</tr>
<tr>
<td>Service Availability (SA) and Voice Quality Monitor (VQM)</td>
<td>8</td>
</tr>
<tr>
<td>Cisco IOS IP Service Level Agreements (SLAs)</td>
<td>9</td>
</tr>
<tr>
<td>Juniper Real-Time Performance Monitoring (RPM)</td>
<td>9</td>
</tr>
<tr>
<td>How eHealth Monitors Response Time</td>
<td>10</td>
</tr>
<tr>
<td>Creating Response Paths</td>
<td>10</td>
</tr>
<tr>
<td><strong>Chapter 2</strong></td>
<td>11</td>
</tr>
<tr>
<td>Adding Response Elements to the Poller Configuration</td>
<td>11</td>
</tr>
<tr>
<td>Overview of the Discover Process</td>
<td>11</td>
</tr>
<tr>
<td>Discovering Response Elements</td>
<td>12</td>
</tr>
<tr>
<td>Creating Response Destination Elements</td>
<td>14</td>
</tr>
<tr>
<td>Creating Response Paths</td>
<td>16</td>
</tr>
<tr>
<td>Response Element Naming Conventions</td>
<td>19</td>
</tr>
<tr>
<td>Verifying That Your Application Response Paths Appear in eHealth</td>
<td>20</td>
</tr>
<tr>
<td>Interpreting Polling Errors on Response Path Elements</td>
<td>20</td>
</tr>
<tr>
<td><strong>Chapter 3</strong></td>
<td>21</td>
</tr>
<tr>
<td>Managing Response Elements</td>
<td>21</td>
</tr>
<tr>
<td>Managing Response Path Elements</td>
<td>22</td>
</tr>
<tr>
<td>Modifying Response Path Elements</td>
<td>24</td>
</tr>
<tr>
<td>Modifying Source and Destination Elements</td>
<td>28</td>
</tr>
<tr>
<td>Deleting Response Elements</td>
<td>29</td>
</tr>
</tbody>
</table>
Chapter 4 Using eHealth Reports to Manage Response

- Overview of Response Reports ..................................................31
- Preparing to Run Response Reports ........................................33
  - Creating Response Groups and Group Lists .........................33
  - Setting Response Limits ......................................................38
- Running Response Reports ......................................................42
  - Running At-a-Glance Reports ..............................................42
  - Running Trend Reports ......................................................43
  - Running Service Level Reports ...........................................43
  - Running Health Reports .....................................................44

Index 47
This guide describes how to use eHealth — Response to discover response elements, create response paths for those elements, and display response time data in eHealth reports.

This guide supports eHealth Release 5.7 and later.

**NOTE**
This document replaces the “Using eHealth — Response” chapter of the eHealth Response Administration Guide, which is obsolete in eHealth Release 5.7.

**Audience**
This guide is intended for eHealth administrators who need to configure eHealth to collect and report on response data.

**About This Guide**
This section describes the possible reading paths that you should follow, depending on your needs, as well as the changes and enhancements that have been made since the last release of this guide. It also includes the documentation conventions used in this guide.

**Reading Path**
Before you use eHealth — Response, you must install eHealth and become familiar with its features. For information about eHealth, refer to the following documentation.

- *Introduction to eHealth* – Provides an introduction to and overview of eHealth.
- *eHealth Administration Guide*. Describes how to perform the critical eHealth administration tasks such as discovery, polling, database maintenance, and report administration.
- *eHealth Reports Guide*. Provides an overview of the types of reports that you can generate from the eHealth console and from the Web interface.
Revision Information
This is the second release of this guide. It includes the following changes:

- Support for Juniper real-time performance monitoring (RPM) has been added to eHealth.
- The guide has been reorganized to improve usability.

Documentation Conventions
Table 1 lists the conventions used in this document.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File or Directory Name</td>
<td>Text that refers to file or directory names.</td>
</tr>
<tr>
<td><code>code</code></td>
<td>Text that refers to system, code, or operating system command line examples.</td>
</tr>
<tr>
<td><code>emphasis</code></td>
<td>Text that refers to guide titles or text that is emphasized.</td>
</tr>
<tr>
<td><code>enter</code></td>
<td>Text that you must type exactly as shown.</td>
</tr>
<tr>
<td>Name</td>
<td>Text that refers to menus, fields in dialog boxes, or keyboard keys.</td>
</tr>
<tr>
<td>New Term</td>
<td>Text that refers to a new term, that is, one that is being introduced.</td>
</tr>
<tr>
<td><code>Variable</code></td>
<td>Text that refers to variable values that you substitute.</td>
</tr>
<tr>
<td><code>→</code></td>
<td>A sequence of menus or menu options. For example, <code>File → Exit</code> means “Choose <code>Exit</code> from the <code>File</code> menu.”</td>
</tr>
</tbody>
</table>

**NOTE**
Important information, tips, or other noteworthy details.

**CAUTION**
Information that helps you avoid data corruption or system failures.

**WARNING**
Information that helps you avoid personal physical danger.

Technical Support
If you have a Support Contract ID and password, you can access our Support Express knowledgebase at the following URL: http://search.support.concord.com.

If you have a software maintenance contract, you can obtain assistance with eHealth. For online technical assistance and a complete list of primary service hours and telephone numbers, contact Technical Support at http://support.concord.com.
Introduction to eHealth — Response

This chapter provides an overview of eHealth™ — Response, and describes the components from which it collects data. It contains the following sections:

- “What is eHealth — Response”
- “How eHealth Monitors Response Time”

What is eHealth — Response

eHealth—Response is an eHealth technology that collects response time data from a variety of sources for real-time analysis, historical reporting, and service level management. You can use eHealth—Response to monitor and manage the performance and availability of applications and services in your infrastructure. You can also report on network activity between Cisco® or Juniper® routers and other devices.

eHealth—Response offers a comprehensive set of reports that help you manage your critical services and applications. You can also use Live Health™ to detect any performance problems in real time. These features enable you to detect degrading performance or declining availability of your critical services before those problems affect users, and maintain service levels by measuring the actual response times that end users experience.

eHealth collects response data using one or more of the following products:

- eHealth Application Response (AR)
- eHealth Service Availability (SA)
- eHealth Voice Quality Monitor (VQM)
- Cisco IOS IP Service Level Agreements (SLAs)
- Juniper Real-Time Performance Monitoring (RPM)

NOTE
Cisco IOS IP SLAs were previously named the Cisco Service Assurance Agent (SAA)
Application Response

Application Response agents aggregate data and send it to eHealth. You do not discover AR agents and poll them for data. Application Response elements appear in the database automatically when you install AR agents. However, you must ensure that the AR agent data appears in the database to report on it with eHealth — Response. For instructions on using Application Response, refer to the Application Response Web Help.

**NOTE**

When you discover objects, eHealth adds elements for those objects to the poller configuration. This enables eHealth to poll the objects for performance data.

Service Availability (SA) and Voice Quality Monitor (VQM)

Both Service Availability (SA) and Voice Quality Monitor (VQM) are plug-in modules for the eHealth SystemEDGE agent. The procedures to monitor response time with SA and VQM have been enhanced in Release 5.7. After you discover the SystemEDGE agent systems that you want to monitor, you use new features of the eHealth Web interface. For SA, you use new Service Availability features to create tests that measure response time. For VQM, you use AdvantEDGE View to create response paths; then rediscover in response mode.

**To access AdvantEDGE View and Service Availability:**

1. Log in to the eHealth Web interface with administrative privileges.
2. Select the **Systems & Apps** tab.
3. Click **AdvantEDGE View** or **Service Availability**.

**To access the AdvantEDGE View and Service Availability Help contents:**

1. On the Web interface, click the Help icon next to the **Administration** tab.
2. In the eHealth Web Help Contents window, click the **AdvantEDGE View** link. The AdvantEDGE View Web Help Contents window appears.
3. To access the Service Availability Web Help Contents, in the AdvantEDGE View Web Help Contents window, scroll to the **Monitoring Applications** section, and then click the **Monitoring Service Availability** link.
Cisco IOS IP Service Level Agreements (SLAs)

Cisco® IOS IP Service Level Agreements (SLAs) monitor network performance between a Cisco router and a remote device. IP SLAs provide performance information that you use for service level monitoring, troubleshooting, and resource planning. It measures response time for various network protocol devices, performance metrics, and statistics.

When you configure Cisco IP SLA with eHealth — Response, the Cisco router generates traffic to specified network resources, and measures the availability of the resource and response time between the router and that resource. Cisco IP SLA can also measure important metrics such as latency, packet loss, and jitter, which are then stored in the eHealth database.

You can use this information to troubleshoot network problems, identify and analyze potential problems, and design future network topologies. Response data from Cisco IP SLA can appear in the eHealth reports described in Chapter 4, “Using eHealth Reports to Manage Response,” and can be used by Live Health to generate real-time alarms.

eHealth can also obtain data about HTTP or DNS transactions from routers that use Cisco IOS (Release 12.0T [5] or greater) to measure response time of these Internet applications. Response time of these applications includes the total elapsed time to perform a task at a connection level (such as downloading a Web page), including network delay between the router and the HTTP or DNS server. You can display this data in eHealth reports. For more information about Cisco IOS IP SLAs, refer to the Cisco IOS IP SLAs Configuration Guide and the Cisco Web site (http://www.cisco.com).

**NOTE**
Cisco IOS IP SLAs were previously named the Cisco Service Assurance Agent (SAA).

Juniper Real-Time Performance Monitoring (RPM)

The Juniper® real-time performance monitoring (RPM) feature monitors network performance between a Juniper router and a remote device. RPM generates probes between two network endpoints, and measures performance information, allowing you to perform service level monitoring, troubleshooting, and resource planning.

When you use eHealth—Response to configure RPM, the Juniper router generates traffic between specified network resources, and measures performance information for those response paths. eHealth then polls the response paths, allowing you to monitor metrics including availability, packet response time and jitter. If both the source and destination elements use the same Network Time Protocol (NTP) server, RPM records both one-way and round-trip data for the path. This information is then stored in the eHealth database.

You can use this information to track the quality of service a user experiences, troubleshoot network problems, and design future network topologies. Response data from Juniper RPM can appear in the eHealth reports described in Chapter 4, “Using eHealth Reports to Manage Response,” and can be used by Live Health to generate real-time alarms.

**NOTE**
Juniper RPM defines jitter as the difference between the maximum response time and the minimum response time for a group of pings (Jitter = Maximum Response Time – Minimum Response Time). This jitter measurement may differ from that calculated by other devices.

For more information about Juniper routers and the RPM feature, refer to the documentation for your router and the Juniper Web site (http://www.juniper.net).
How eHealth Monitors Response Time
To begin using eHealth—Response, you discover devices in your network on which Juniper RPM, Cisco IP SLA, and SystemEDGE agents reside. eHealth adds these devices to the poller configuration, which enables eHealth to poll them for performance data. The devices that you monitor for response time data are called response elements in eHealth.

**NOTE**
You do not need to discover AR agents, but you must ensure that the data associated with these elements appears in the database before you can report on it with eHealth—Response.

Creating Response Paths
You may need to create response paths to test response time, depending on the product that you are using to collect data:

- With Cisco IP SLAs and Juniper RPM, you create response paths using the eHealth path manager.
- With Application Response, eHealth creates response paths automatically.
- With Service Availability (and the SystemEDGE agent), you create response tests using the Service Availability interface.
- With VQM, you use AdvantEDGE View to create the response paths; then rediscover in response mode.

When you discover devices that Cisco IP SLA, Juniper RPM, and SystemEDGE agents monitor, eHealth adds elements for these devices to the poller configuration. Then, you use these elements to create response paths. You can run various reports on your AR, Cisco IP SLA, Juniper RPM, and SystemEDGE paths to display application activity and response time.

Chapter 2, “Adding Response Elements to the Poller Configuration” describes how to discover these response elements, and how to configure the elements for reporting.
Adding Response Elements to the Poller Configuration

This chapter explains how to use eHealth to discover SA, VQM, Cisco IOS IP SLA, and Juniper RPM devices. It also explains how to create response destination elements and paths that enable eHealth to display response time data in eHealth reports.

• “Overview of the Discover Process”
• “Discovering Response Elements”
• “Creating Response Destination Elements”
• “Creating Response Paths”
• “Verifying That Your Application Response Paths Appear in eHealth”

Overview of the Discover Process

To add response elements to the poller configuration, you run the eHealth discover process to discover SNMP agents (Cisco IP SLA, Juniper RPM, and SystemEDGE agents). When you save the results of this discover process, eHealth creates an entry in the database for each response element that the discover process finds. Then, after each poll, eHealth saves data about these elements in the database.

After you discover Cisco IP SLA and Juniper RPM elements, you must define response destinations and create response paths for them using the eHealth path manager.

**NOTE**

In addition to the SNMP agents it discovers as response elements, eHealth also discovers any pre-existing RFC2925 (Disman) response paths on Cisco or Juniper routers. These response paths are polled as plain data elements by eHealth. They are not managed the same way as the response paths you create using eHealth—Response. If you do not want to discover these pre-existing response paths, edit the poller configuration before saving the results of the discover process.
Discovering Response Elements

When you run the discover process, eHealth looks for SNMP agents at ports 161 and 1691 by default. You can configure eHealth to search for SNMP agents on other agent ports by modifying the NH_DISCOVER_RESPONSE_PORTS environment variable.

For information on specifying other ports, refer to the eHealth Administration Guide. For instructions on modifying environment variables, refer to the eHealth Administration Reference.

To discover response elements:

1. Select Setup → Discover on the console. The Discover dialog box appears.
2. Select Response under Mode.

   **NOTE**
   
   Select Response under Mode for Cisco IP SLA, Juniper RPM, and Service Availability. Select Response and System for VQM.

3. Specify one or more community strings that allow write permission to the response elements in the Community Strings field. This field is case sensitive. For information about community strings, refer to the Console Help.

   **NOTE**
   
   You can limit the community string of a Cisco router to a specific MIB tree.

4. Specify a range of IP addresses in the IP Address Range field. For example: 152.16.10.50-90. For information about range formats that eHealth accepts, refer to the Console Help.

5. Optionally, you can complete the remaining fields in the Discover dialog box. For information about these fields, refer to the Console Help.

6. Click Discover. The Discovering dialog box appears.

When the discover process finishes, the dialog box displays a message that indicates the number of newly discovered elements. You can scroll through the Discovery Results field to view the list of IP addresses and the associated response element type for each, if one was discovered.
7. Optionally, click **View Discover Log** to view the log file for the newly discovered elements before you save it to the database.

   **NOTE**
   You can also edit this information before saving it. For more information, refer to the Console Help.

8. Click **Save** to save the results of the discover process. eHealth creates an entry in the database for each response element, and each time eHealth polls these elements, it saves response time data that the elements collect.

### Scheduling a Discover Job

To ensure that the response element information is current, you can schedule the discover process to run on a regular basis. When you schedule a discover job, eHealth automatically discovers any new SNMP agents installed on devices within the IP address range you are monitoring.

**To schedule a discover job for response elements:**

1. Select **Setup → Schedule Jobs** on the console. The Schedule Jobs dialog box appears.
2. Select **Add Discover** from the drop-down list. The Add Scheduled Discover dialog box appears.
3. Select **Response** under Mode.
4. Specify one or more community strings that allow write permission to the response elements in the Community Strings field.
5. Specify IP addresses and, optionally, a group name and IP exclusion file.
6. Specify the options and schedule for the scheduled discover job; then click **Schedule**. The Scheduled Jobs dialog box displays the information that you configured.
7. Click **Modify** to change the information you entered, or click **OK** to schedule the discover job.
Chapter 2   Adding Response Elements to the Poller Configuration

Creating Response Destination Elements

After you discover Cisco IP SLA or Juniper RPM response elements and save them to the eHealth database, you must create response destination elements using the eHealth path manager. You use these destination elements to define response paths.

**Note**

You do not perform this procedure for eHealth SA and VQM. For SA and VQM, you create response paths using Service Availability and AdvantEDGE View.

Destination elements indicate one endpoint of a response path that eHealth monitors. The other endpoint is an existing response source. eHealth monitors activity between the endpoints you specify, and displays this information in reports.

You can create response destination elements from routers and servers you have previously discovered, or you can specify the IP address of a new element that does not yet exist in the poller configuration.

**To create response destination elements:**

1. Select **Setup → Poller Configuration** on the console. The Poller Configuration dialog box appears.
2. Click **Path/PVC Manager**. The Path/PVC Manager dialog box appears.
3. Select **Response Path** under List Elements by Type.
4. Click **Add Paths**. The Add Paths dialog box appears.
5. Click **Add Destination**. The Add Destination Element dialog box appears.
   - If you want to use existing elements to create response destination elements, refer to Step 6.
   - If you want to add information for a new response element that does not currently reside in the poller configuration, and that you want to designate as a response destination, refer to Step 7.
6. Create response destination elements from existing elements as follows:
   a. Select **Create Response Destinations from existing elements**.
   b. Select one or more elements from the Select Elements list. (To search for a known element, specify the initial characters of the element name in the Search for Name field, then press **Enter**.)
   c. Click **Apply**. The selected elements appear in the list of path destinations in the Add Paths dialog box. (This dialog box appears in the background on your screen.)
   d. Click **OK** to save these elements as destination elements and to close the Add Destination Element dialog box.
   e. Go to “Creating Response Paths” on page 16.

7. Create a new response destination element as follows:
   a. In the Add Destination Element dialog box, select **Add a new Response Destination**. The Add Destination Element dialog box displays new fields.
   b. Specify a name in the Endpoint Name field for the element. You can specify a maximum of 64 single-byte or 32 double-byte characters using the letters A through Z and a through z, the numbers 0 through 9, dashes (-), periods (.), underscores (_), colons (:), and slashes (/).

   **NOTE**

   eHealth reports often truncate the element names, therefore, 30 characters is recommended. If you use a combination of single-byte and double-byte characters, the total length cannot exceed 64 bytes.

   c. Optionally, specify an alias name in the Endpoint Alias field for the element. The alias name has the same length and character restrictions as the element name.
   d. Specify the IP address of the response destination in the IP Address field.
   e. Optionally, specify the unique network name of the destination in the Host Name field. To add the destination element, DNS must be able to resolve this hostname.
   f. Click **Apply**. eHealth adds the new element to the list of path destinations in the Add Paths dialog box.
   g. Click **OK**. The new element is saved as a destination element.
   h. Go to “Creating Response Paths” on page 16.
Creating Response Paths

Once you have discovered source endpoints and created response destinations, you must create response paths for your Cisco IP SLA and Juniper RPM elements. eHealth adds these paths to the poller configuration, and uses them for active response testing and for reporting on the response data collected.

- Application Response paths appear in eHealth automatically when you configure your AR agent information through the Web interface. You should verify that these paths appear. For more information, refer to “Verifying That Your Application Response Paths Appear in eHealth” on page 20.
- You use AdvantEDGE View to create VQM paths. For instructions, refer to the AdvantEDGE Web Help.
- For SA elements, you use Service Availability to create tests. For instructions, refer to the Service Availability Web Help.

When you create response paths with the path manager, you select a protocol, one or more sources, and one or more destinations. Table 2 shows the protocols that eHealth — Response supports and the types of agents that monitor these protocols.

**Note**

When creating response paths for Juniper RPM, ensure that both the source and destination elements use the same Network Time Protocol (NTP) server.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>Cisco RTTMON and Service Availability</td>
</tr>
<tr>
<td>FTP</td>
<td>Service Availability</td>
</tr>
<tr>
<td>HTTP</td>
<td>Cisco RTTMON GET, Cisco RTTMON Advanced, and Service Availability</td>
</tr>
<tr>
<td>Jitter</td>
<td>Cisco RTTMON and Juniper ICMP Echo</td>
</tr>
<tr>
<td>NNTP</td>
<td>Service Availability</td>
</tr>
<tr>
<td>Ping</td>
<td>Cisco Ping, Cisco RTTMON, Disman ICMP Echo, and Juniper ICMP Echo</td>
</tr>
<tr>
<td>POP3</td>
<td>Service Availability</td>
</tr>
<tr>
<td>SMTP</td>
<td>Service Availability</td>
</tr>
<tr>
<td>TCP Connect</td>
<td>Cisco RTTMON</td>
</tr>
<tr>
<td>TCP</td>
<td>Service Availability</td>
</tr>
<tr>
<td>UDP</td>
<td>Cisco RTTMON</td>
</tr>
<tr>
<td>VoIP</td>
<td>eHealth VQM</td>
</tr>
</tbody>
</table>

**Note**

The protocols listed in the Agent column for Service Availability and eHealth VQM are not selections in the path manager.
To create response path elements:

1. From the Add Paths dialog box, select a protocol from the Create paths that support data collection using this protocol list. When you select a protocol, it populates the Select one or more path sources list. This list shows only those sources that support the protocol that you select.

2. Select one or more sources from the Select one or more path sources list.

3. Optionally, modify the values for the path properties by doing the following:
   a. Select the property under Attribute. eHealth displays a brief description of the selected property in the Description field.
   b. Specify a new value in the Value field. The number, type, and default values of the properties differ for each.

4. Select one or more path destinations from the Select one or more path destinations list by using one of the selection methods described in Step 2. If response destinations are not listed, or if the list does not contain the element that you want to use, click Add Destination. For more information, refer to “Creating Response Destination Elements” on page 14.

5. At the bottom of the Add Paths dialog box, refer to the note that shows the number of paths that eHealth will build with your choices. (This number includes any paths that already exist.) eHealth creates path elements between each source and destination that you select. For example, if you select three sources and five destinations, eHealth creates 15 path elements, unless a path already exists. Confirm that this is what you want to do.
The NH_RTTMON_MAX_PATHS_PER_AGENT environment variable specifies the maximum number of paths that eHealth can create on a Cisco router. The default value is 20, but you can increase or decrease it. For instructions, refer to the section on modifying environment variables in the eHealth Administration Reference.

6. Do one of the following:
   - Click **Apply** to save the response path elements and refresh the window so that you can create other response path elements.
   - Click **OK** to save the response path elements and close the Add Paths dialog box. The Path Builder Results dialog box appears.

**NOTE**

If the path needs a hostname for one or more destinations, the Path Builder Results dialog box indicates that eHealth detected invalid destinations and lists the destinations for which you must specify a hostname.

7. Review the following:
   - Number of paths that eHealth created
   - Names of the duplicate paths that it did not create
   - Names of paths that it did not create because they exceed the maximum number of paths for a response source

8. Click **OK** to close the Path Builder Results dialog box; then click **Close** to close the Path/PVC Manager dialog box.

9. You must click **OK** or **Apply** in the Poller Configuration dialog box to save the path sources and destinations that you selected. When you click **OK** or **Apply**, eHealth creates the response paths.

**CAUTION**

If you click **Cancel** in the Poller Configuration dialog box, you lose all of the work that you have performed since you opened this dialog box.
Response Element Naming Conventions

When you discover response source endpoints, create response destinations from existing elements, or create response path elements, eHealth names the response elements according to the format defined in Table 3.

Table 3. Response Element Name Formats

<table>
<thead>
<tr>
<th>Element Type</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response source</td>
<td>systemName-RS</td>
</tr>
<tr>
<td>Response destination</td>
<td>elementName-RD</td>
</tr>
<tr>
<td>Path</td>
<td>sourceElementName-DestinationElementName-protocol-AP</td>
</tr>
</tbody>
</table>

eHealth creates a unique element name for each element. If you create response path elements that are identical except for the value that you assign to a polling variable, eHealth appends a letter to create a unique element name. For example, if you have a path element named router21-webserver1-ciscoPing, you can create an identical element that uses a different packet size. eHealth names the new element router21-webserver1-ciscoPing-A.
Verifying That Your Application Response Paths Appear in eHealth

To verify that your Application Response paths appear in eHealth, you can view them through the Poller Configuration dialog box. Application Response paths consist of a client, application, module, and server name, as shown in Figure 1. eHealth appends an AP to the end of these paths to indicate that they are Application Paths.

When you configure Application Response paths, the path name cannot exceed 64 characters. If a path name does exceed this limit, eHealth generates an error and does not include response time data for this path in reports. When you create names for applications, modules, and servers using AR Agent Management, each name should not exceed 15 characters.

<table>
<thead>
<tr>
<th>Client name</th>
<th>Module name</th>
<th>Application path</th>
</tr>
</thead>
<tbody>
<tr>
<td>yellow-Outlook-Read-Default-Exchange-AP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server name</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 1. Application Response Path

Interpreting Polling Errors on Response Path Elements

Often, after you create a response path, you must perform other steps to properly configure the response source to collect data or validate the information specified for the path such as the IP address. If a path is polled successfully, but it returns all zero data or is unavailable, the path is probably not configured correctly. eHealth can report these conditions to help you troubleshoot improperly configured paths.

For response paths configured on Cisco routers, eHealth displays an error message in the console window when the number of consecutive successful polls that return all zero data exceeds the value of the NH_RTRZERO_DATA_POLLS environment variable. The default value of this variable is 6. After six such polls, eHealth displays the message and resets the counter. You can decrease the value to obtain the error message after fewer polls that meet this criteria, or increase it to obtain the message after more consecutive polls that meet this criteria.

For response paths configured on Juniper routers, eHealth may display one of two error messages:

- **Ping Response Probe juniper-ICMP-AP did not run on remote machine** – Indicates that the test did not run. If this error occurs on every poll cycle, the destination element is not reachable from the router. You should verify the IP address of the destination. If the error occurs only occasionally, it generally indicates the router did not have the resources to run the test (it was too busy routing traffic).

- **Ping Response Probe juniper-ICMP-AP ran on remote machine, but did not receive any responses** – Indicates that the test ran but did not receive a response. If this error occurs consistently, the destination element probably does not exist on the network. You should verify that the destination exists and the path is configured correctly. If the error occurs sporadically, the destination is occasionally not responding to the ping. It may be offline for certain time periods.
Managing Response Elements

This chapter describes how to use the Poller Configuration dialog box to manage the response path elements in your configuration. It includes the following sections:

- “Managing Response Path Elements”
- “Modifying Response Path Elements”
- “Modifying Source and Destination Elements”
- “Deleting Response Elements”
Managing Response Path Elements

Use the Path/PVC Manager dialog box to manage the response path elements in your configuration.

To display the Path/PVC Manager dialog box:

1. Select Setup → Poller Configuration on the console. The Poller Configuration dialog box appears.
2. Click Path/PVC Manager. The Path/PVC Manager dialog box appears.

![Path/PVC Manager Dialog Box]

**NOTE**

The title of the Path/PVC Manager dialog box indicates the **Set Element Filter** setting in the Options dialog box. If you have not set a filter, the dialog box lists all paths.

3. Under **List Elements of Type**, select **Response Path**.
4. Optionally, manage your view of the elements in the list by sorting the list of elements. Specify a sorting method under **Sort List by**:
   - Select **Alias** to display the elements in alphanumeric order according to their aliases. This option only appears if you selected **Show Alias Names** in the Options dialog box.
   - Select **Name** to display the elements in alphanumeric order according to their element names.
   - Select **Source** to list the paths by their response source. The paths appear in alphanumeric order according to their element or alias names.
   - Select **Destination** to list the paths by their response destination. The paths appear in alphanumeric order according to their element or alias names.
   - Select **Protocol** to list the paths by the protocol setting. The paths appear in alphanumeric order according to their element or alias names.
   - Select **Poll Rate** to display the elements according to their poll rate.
   - Select **Agent Type** to display the elements in alphanumeric order according to their agent type.
5. By default, eHealth displays all response path elements that exist in your poller configuration. Optionally, customize the list by selecting one of the following under Show:
   - Select All to display all path elements.
   - If you are building new paths, select Newly Added to display only the newly created paths that have not yet been saved in the Poller Configuration dialog box.
   - If you want to display only the response path elements that Live Exceptions is not monitoring, select LE Unmonitored.

   When Live Exceptions monitors a group or group list, it monitors all elements in the group or group list. However, you can disable monitoring for one or more specific elements, as described in Chapter 3, “Managing Response Elements.”

6. Do one of the following:
   - To save the elements that are currently displayed in the dialog box and to save their information in the paths.cfg.log file in the log directory of your eHealth installation, click Save List To File.
     The paths.cfg.log file is an ASCII file with tab-separated fields, as described in Table 4. If a field does not apply to the element, that field remains empty.

   **Table 4. paths.cfg.log File Fields**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Specifies the order of this element in the file.</td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the element name; or, if you selected Show Alias Names, when you save this file, this field specifies the alias that you assigned to this element.</td>
</tr>
<tr>
<td>Response Source</td>
<td>Specifies the response source element for the path element.</td>
</tr>
<tr>
<td>Response Destination</td>
<td>Specifies the response destination element for the path element.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Specifies the protocol used to test the response of the path.</td>
</tr>
<tr>
<td>Poll</td>
<td>Specifies the polling rate that eHealth uses to poll the element.</td>
</tr>
<tr>
<td>Agent Type</td>
<td>Specifies the type of data collected by the path element.</td>
</tr>
<tr>
<td>Element</td>
<td>Specifies the element name of the path.</td>
</tr>
</tbody>
</table>

   - To save newly added paths, click Close on the Path/PVC Manager dialog box and then click Apply or OK in the Poller Configuration dialog box to save your changes.
Modifying Response Path Elements

You can use the Path/PVC Manager dialog box to modify Cisco IP SLA and Juniper RPM response path elements in the following ways:

- Change its alias name, source, or destination.
- Specify a new protocol (agent type).
- Specify new settings and limits for the protocol.
- Change its response polling variables.

**NOTE**

You can also use the path manager to modify Service Availability elements, but CA recommends that you use the new Service Availability interface.

To modify a single response path element:

1. Select **Setup → Poller Configuration** on the console. The Poller Configuration dialog box appears.
2. Click **Path/PVC Manager** in the Poller Configuration dialog box. The Path/PVC Manager dialog box appears. The title of the dialog box indicates the Set Element Filter setting in the Options dialog box.

**NOTE**

To access the Options dialog box, select **Setup → Options** on the console.

- If you have not set a filter, the title indicates that the Path Manager dialog box lists all paths.
- If you have set a filter, the title indicates the group name.
3. Optionally, select an option on which to sort the elements in the list under **Sort List by**.
4. Optionally, customize the list by selecting **Newly Added** or **LE Unmonitored** under **Show**. By default, eHealth displays all response path elements that exist in your poller configuration.
5. Select an element and click **Modify**. The Modify Path Element dialog box appears.
6. Optionally, do any of the following:
   • Change the name by replacing the text in the **Name** field.
   • Specify an alias name by specifying text in the **Alias** field.
   • Select a protocol from the **Agent Type** list.

**CAUTION**

Ensure that the Agent Type you specify is appropriate for the selected response element. Changing the Agent Type to an unsupported protocol can result in polling errors.

• Specify another source or destination by replacing the text in the **Source** or **Destination** fields, respectively. To select an element from a list, click **Browse** next to either field.
• When Live Exceptions monitors a group or group list, it monitors all elements in the group or group list. Disable Live Exceptions monitoring for this element by deselecting **Monitor** under **Live Exceptions**.
• By default, Live Exceptions monitors elements using the time zone of the eHealth server. Specify a different time zone for the element by selecting a time zone from the **Time Zone** list.

**NOTE**

The **Live Exceptions** fields only appear if you have a Live Health license. For more information, refer to the eHealth Live Health Web Help.

• Under **Response Polling Variables**, turn polling off, or select **Normal**, **Slow**, or **Fast** polling for the element.
• Specify different settings for attributes. Select the attribute in the **Attribute** list and specify another value in the **Value** field.
7. Do one of the following:
   • Click **Apply/Next** to change the path element and display the next element in the list.
   • Click **OK** to change the path element and close the Modify Element Path dialog box.

8. Click **Close** to close the Path/PVC Manager dialog box.

9. Click **OK** or **Apply** in the Poller Configuration dialog box to save the changes.

**To modify multiple response path elements:**

1. In the Poller Configuration dialog box, click **Path/PVC Manager**. The Path/PVC Manager dialog box appears. The title of the dialog box indicates the **Set Element Filter** setting in the Options dialog box.
   • If you did not set a filter, the title indicates that this dialog box lists all paths.
   • If you have set a filter, the title indicates the group name.

2. Optionally, select a column on which to sort the elements in the list under **Sort List by**.

3. By default, eHealth displays all response path elements that exist in your poller configuration. Optionally, customize the list by selecting **All**, **Newly Added**, or **LE Unmonitored** under **Show**.

4. Select multiple elements and click **Modify**. The Modify Path Elements dialog box appears.

5. Optionally, change the polling rate for the elements by selecting **Change Poll To**, then:
   • Select **Off** to turn off polling for the elements.
   • Select **Normal** to poll elements at the Normal rate.
   • For statistics elements, select **Slow** to poll elements at the Slow rate.
   • For statistics elements, select **Fast** to poll elements at the Fast rate.

   If a path element does not support a polling interval setting, eHealth does not make that setting selectable. For more information about polling rates, refer to the section on changing polling rates in the *eHealth Administration Guide*. 

*Using eHealth Response*
6. Specify in the **Retries** field the number of times you eHealth to send requests to an element before giving up on a poll.

7. Specify in the **Timeout** field the amount of time (in microseconds) that you want to wait before timing out a poll for an element. (Specify an integer value.)

8. Optionally, change the names of the selected elements by selecting **Change Element Name**. Specify the part of the name that you want to replace in the **Replace sub-string** field. Specify the new part of the name in the **with** field. The name strings are case sensitive.

9. Optionally, change the alias names of the selected elements by selecting **Change Alias Name** and following the instructions in Step 8.

10. Optionally, change the community string for the elements that you selected by selecting **Change Community**. Specify the old community string in the **from** field; then specify a new community string for which you have **write** permission in the **to** field. Specify the **entire** community string. The community strings are case-sensitive.

11. Optionally, specify a shared response time target by selecting **Set Limit To** and specifying a number in the adjacent field.

12. Optionally, specify another response source by selecting **Change Source**. Specify the element name of the current source element in the **from** field and the element name of another source element in the **to** field. (To find source element names, switch to the Poller Configuration dialog box; then copy and paste between the dialog boxes.)

13. Optionally, specify another response destination by selecting **Change Destination**. Specify the element name of the current destination element in the **from** field and the element name of another destination element in the **to** field. (You can copy element names from the Poller Configuration dialog box.)

14. Optionally, specify another IP address to use for the source element by selecting **Change Source IP**. Specify the current source element’s IP address in the **from** field and the IP address of another source element in the **to** field.

15. Optionally, specify another IP address to use for the destination element by selecting **Change Destination IP**. Specify the IP address of the current destination element in the **from** field and the IP address of another in the **to** field.

16. Optionally, change the Live Exceptions monitoring status by doing one or both of the following:
   - When Live Exceptions monitors a group or group list, it monitors **all** elements in the group or group list. Disable Live Exceptions monitoring for this element by selecting **Monitor and No** under **Live Exceptions**.
   - By default, Live Exceptions monitors elements using the time zone of the eHealth server. Select a different time zone for the elements by selecting **Modify Time Zone** and selecting a time zone from the **Time Zone** list.

**NOTE**

The **Live Exceptions** fields appear only if you have a Live Health license. For more information, refer to the eHealth Live Health Web Help.

17. Click **OK** to modify the response path elements and close the Modify Path Elements dialog box.

18. Click **Close** on the Path/PVC Manager dialog box.

19. Click **OK** or **Apply** in the Poller Configuration dialog box to save the changes.
Modifying Source and Destination Elements

You can modify a response source or destination element by changing its name, alias name, IP address, or community string.

**NOTE**

Since eHealth does not poll response sources and response destinations, the Poll field in the Poller Configuration dialog box is not active. When you view response elements, N/A appears in the Poll field.

**To modify a source or destination element:**

1. Select **Setup → Poller Configuration** on the console. The Poller Configuration dialog box appears.
2. Select an element in the Poller Configuration dialog box.
3. Click **Modify**. The Modify Element dialog box appears.

![Modify Element dialog box](image)

4. Do one or more of the following:
   - Change the element name or alias name.
   - Specify another IP address.
   - Change the community string and read community string for a response source element.
   - Change the poll rate, retries rate, and timeout rate.
   - Change the discovered information (system name and interface).
5. Do one of the following:
   - Click **Apply/Next** to update the element with the changes and display the next element in the poller configuration list.
   - Click **OK** to update the element with the changes and close the Modify Element dialog box.
6. Click **OK** or **Apply** in the Poller Configuration dialog box to save the modifications to the elements.
Deleting Response Elements

You can use the Poller Configuration dialog box to delete Cisco IP SLA and Juniper RPM response source and destination elements. You delete these types of response elements using the Path/PVC Manager dialog box.

**To delete response source or destination elements:**

1. Select **Setup → Poller Configuration** on the console. The Poller Configuration dialog box appears.
2. Select one or more elements in the Poller Configuration dialog box and click **Delete**. If you delete a source or a destination, you also delete all paths associated with that element. For more information about deleting elements, refer to the *eHealth Administration Guide*.
3. You must click **OK** or **Apply** in the Poller Configuration dialog box to save the information that you change.

**CAUTION**

If you click **Cancel** in the Poller Configuration dialog box, you will lose all work you have performed since you opened this dialog box.

**To delete response path elements:**

1. Select **Setup → Poller Configuration** on the console. The Poller Configuration dialog box appears.
2. In the Poller Configuration dialog box, click **Path/PVC Manager**. The Path/PVC Manager dialog box appears.

**NOTE**

The title of the Path Manager dialog box indicates the **Set Element Filter** setting in the Options dialog box. If you have not set a filter, the title indicates that the Path Manager dialog box lists all paths. If you have set a filter, the title indicates the group name.

3. Optionally, select a column on which to sort the elements in the list under **Sort List by**.
4. Select one or more elements, and click **Delete**.
5. Click **Close** on the Path/PVC Manager dialog box.
6. Click **OK** or **Apply** in the Poller Configuration dialog box to save the information that you changed.
Using eHealth Reports to Manage Response

This chapter provides an overview of the types of eHealth reports that you can run to display response data, and describes how to configure and run those reports to manage the response elements in your configuration. It includes the following sections:

- "Overview of Response Reports"
- "Preparing to Run Response Reports"
- "Running Response Reports"

Overview of Response Reports

With eHealth – Response, you can report on response sources, destinations, and paths. You can run the following standard and licensed eHealth reports to display your response element data:

- At-a-Glance
- Top N
- Trend
- Health
- Service Level
- MyHealth
- What-If

Note

When you generate a Trend report for a response element, you can report on the total number of transactions collected by an AR agent that exceed a given time constraint defined in an Application rule for that element.

In addition, you can run the special set of reports described in Table 5 to provide you with the information you need to manage the response time and performance of applications in your infrastructure.
## Table 5. Running Reports to Manage Response Time and Performance

<table>
<thead>
<tr>
<th>Report Type</th>
<th>Report Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Level</td>
<td>CIO Executive</td>
<td>This report shows response time and related metrics for all applications for all groups, or for a selected group list. Use this report to summarize current service levels experienced by user groups.</td>
</tr>
<tr>
<td>Health</td>
<td>Path Summary</td>
<td>This report presents the poorest performing paths in a selected group. It breaks down performance by component—client, network, server—so you can troubleshoot the component that is the major source of the problem.</td>
</tr>
<tr>
<td>At-a-Glance</td>
<td>Application Response Client Set</td>
<td>This report helps the network operations center (NOC) analyst or planner diagnose application performance in detail. It shows response time and related metrics for all applications used by a selected client set.</td>
</tr>
<tr>
<td></td>
<td>Application Response Service</td>
<td>This report provides more detail on application performance for the NOC analyst or planner. This report shows response time and related metrics for all client sets served by a selected application service for a particular application.</td>
</tr>
<tr>
<td>AdvantEDGE View Query</td>
<td>Service Availability</td>
<td>This report monitors the response time and availability of critical network services from any system within the enterprise network. Service Availability performs real test transactions using a specified service to provide a real view of the response times and availability for common network services.</td>
</tr>
<tr>
<td></td>
<td>VQM</td>
<td>This report monitors the mean opinion score (MOS) for response paths between two systems.</td>
</tr>
<tr>
<td>At-a-Glance</td>
<td>VQM</td>
<td>This report provides important performance indicators for a specific VQM response path element during the report period.</td>
</tr>
<tr>
<td>Service Level</td>
<td>Application Response:</td>
<td>These reports determine the relative performance of an application for a specific location or functional group, or for a group of locations or functional groups for selected applications. You can use them to report on the applications, modules, and module sets within your infrastructure.</td>
</tr>
<tr>
<td></td>
<td>• Service Delivery</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Service Summary</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Service Performance</td>
<td></td>
</tr>
<tr>
<td>VoIP:</td>
<td>• Executive</td>
<td>• <strong>VoIP Executive reports</strong> provide information about the availability, usability, usage, and usage trends of the VoIP service. They can also help you to determine which customers are receiving poor service and how you can fix it.</td>
</tr>
<tr>
<td></td>
<td>• IT Manager</td>
<td>• <strong>VoIP IT Manager reports</strong> provide information about long-term trends in voice quality, as well as volume trends within the VoIP infrastructure. They can help you determine whether the current infrastructure is providing adequate service and how it will grow.</td>
</tr>
<tr>
<td></td>
<td>• Service Customer</td>
<td>• <strong>VoIP Service Customer reports</strong> provide information about whether service customers are getting good service, including information about the availability and quality of the VoIP service, the amount of the service that they are using, and their usage trends.</td>
</tr>
<tr>
<td></td>
<td>• Response Executive</td>
<td>These reports provide information about the response times, failed attempts, and health of the response elements in your region, department, or business process. You can run them for response paths, endpoints, and client sets, setting service level ranges to analyze data based on your service goals and agreements.</td>
</tr>
<tr>
<td></td>
<td>• Response Service Customer</td>
<td></td>
</tr>
</tbody>
</table>
Preparing to Run Response Reports

Before you run reports on response elements, you might want to do the following:

- Create response groups and group lists to organize your elements.
- Set response limits to measure the performance of a response path element.
- Create any service profiles that you want to use, as described in the eHealth Administration Guide.

Creating Response Groups and Group Lists

eHealth enables you to organize your elements into groups so that you can associate related elements (such as those for a specific department or customer) and generate reports for those specific element sets. To organize your groups, you can create group lists.

NOTE

To organize Application Response elements, you create agent sets through the Application Response interface. These agent sets appear as groups in eHealth.

For example, you can use group lists to model larger organizations, such as all of the groups for a customer, a company, geographic region, and so on. By focusing on a subset of elements—rather than all elements in your infrastructure—you can create effective reports that address your specific needs. A group can belong to multiple group lists. You can use groups and group lists to control access to reports and elements in the Web interface.

A group of response elements can contain response endpoints (sources and destinations), paths, or both. Group lists can contain response groups.

NOTE

When creating groups of router/switch elements, LAN/WAN elements that correspond to groups of response charts, or response elements, the eHealth administrator must use the same name as the response path group name; otherwise, the user cannot successfully drill down to Top N reports from Service Availability and Application Response Path Summary reports.

You can run Top N, Trend, and Health reports on groups, and you can run Service Level reports on groups or group lists. You can use Live Exceptions to monitor both groups and group lists. To generate Health and Service Level reports, you must obtain the appropriate eHealth licenses.
Creating Groups of Response Elements

To create a new group, you can use the Groups, Run Report, and Schedule Report dialog boxes, which are all accessible from the eHealth console.

You may want to create the following types of groups:

- All VQM paths that originate from the same transmitter/receiver.
- All Cisco IP SLA paths that originate from the same Cisco device.
- All Juniper RPM paths that originate from the same Juniper router.
- All paths that test the same protocol.

To create a group of response elements:

1. Display the Response Groups dialog box by doing one of the following:
   - Select Reports → Edit Groups → Response Groups on the eHealth console.
   - Click Edit next to the Group list in a Run Report or Schedule Report dialog box.

   The Response Groups dialog box appears.

2. Click Add. The Add Response Groups dialog box appears.
3. Specify a name in the **Group Name** field.

   You can specify a maximum of 64 single-byte or 32 double-byte characters using the letters A through Z and a through z, the numbers 0 through 9, periods (.), dashes (-), and underscores (_). The word All, the word FirstSense, and spaces are not permitted.

   **NOTE**

   If you use a combination of single- and double-byte characters, the total length cannot exceed 64 bytes.

4. Select one of the following element types under Available Elements:
   - **Response Client Set**
   - **Response Source**
   - **Response Destination**
   - **Response Path**

   The list shows the available elements for the type that you select.

5. By default, eHealth displays all elements in the Available Elements list. If necessary, specify a string in the **Filter by Name** field to reduce the number of elements shown in this list. You can include a wildcard, such as an asterisk (*) to match zero or more characters, or a question mark (?) to match any single character. If you do not include a wildcard, the filter displays the elements that contain that string anywhere in the name.

6. Select elements from the Available Elements list to add to the group.

7. Move the selected elements to the Group Members list by clicking the top arrow. To move a single element, select the element and either click the top arrow or double-click the element.

8. Optionally, add more elements to the group by repeating Steps 4 through 7. To remove elements from the group, select them in the Group Members list, and either click the bottom arrow or double-click the element.

9. When you have completed the group, click **OK** or **Apply** to save the group. The new group appears in the Groups dialog box.

10. When you finish adding groups, click **Close** in the Groups dialog box.
**Creating Response Group Lists**

A group list is a collection of one or more groups. Group lists allow you to associate related groups. To create a new Response group list, you can use the Group List, Run Report, and Schedule Report dialog boxes, which are all accessible from the eHealth console.

You may want to create the following types of group lists:
- A response group list of all of your VQM groups.
- A multi-tech group list of all of your response path groups.
- A response group list of all of your response groups.

**To create a Response group list:**

1. Display the appropriate Group List dialog box by doing one of the following:
   - Select Reports → Edit Group Lists → Response Group Lists on the console.
   - Click Edit next to the Group list in a Run Report or Schedule Report dialog box.

   The Response Group List dialog box appears.

2. Click Add. The Add Response Group List dialog box appears.
3. Specify a name in the **Group List Name** field. You can specify a maximum of 64 single-byte or 32 double-byte characters using the letters A through Z and a through z, the numbers 0 through 9, periods (.), dashes (-), and underscores (_). The words All and FirstSense, and spaces are not permitted.

**NOTE**

If you use single-byte and double-byte characters, the total length cannot exceed 64 bytes.

4. Optionally, reduce the number of groups shown in the Available Groups list by specifying a string in the **Filter by Name** field.

5. Select the groups to add to the group list.

6. Move the selected groups to the Group List Members list by clicking the top arrow. To move a single group, select the group and click the top arrow or double-click the group.

7. Optionally, remove groups from the group list by selecting the groups in the Group List Members list and clicking the bottom arrow.

8. When you finish creating the group lists, click **OK** or **Apply**. The new group list appears in the Group List dialog box.

9. Optionally, create more group lists by repeating Steps 5 through 8.

10. Click **Close** to save your group lists and close the Group List dialog box.

For more information on creating groups and group lists, refer to the *eHealth Administration Guide*. 
Setting Response Limits

A **response limit** is a time threshold (specified in milliseconds) used to measure the performance of a response path element. When the response time for a path exceeds the limit, the path is not meeting the desired response time performance.

You set the response limit for each path element to measure performance based on its characteristics and the needs of the users or applications. For example, a path that uses long-distance WAN links might have a very high response limit because traffic typically takes a long time to travel over that link. However, paths that use high-speed LAN links to connect your sales department workstations to the sales application server might have very low response limits because delays could impact sales order processing.

You can group related response path elements to monitor and report on them. For example, you can monitor a group of response path elements using Live Health so that you will be notified when a path in the group exceeds its response limit or matches the alarm rule criteria. If you have the optional Health report license, you can run a report for a group of path elements (that could each have different response limits) to locate paths that exceeded their limits during the report period and to determine whether the response time over those paths is improving or degrading.

*e*Health provides a set of commands that evaluate and set response limits for your response path elements. The following sections describe these commands.

Evaluating Response Limits

The `nhGetRespLimit` command evaluates and recommends response limit values for a group of Cisco IP SLA or Juniper RPM response path elements. It uses a Top N report to calculate the average response time for the group over a specified time period. The command also recommends a response time limit value based on the average multiplied by a limit factor.

**To use the `nhGetRespLimit` command:**

1. Log on to the *e*Health system as the *e*Health administrator.
2. Change to the *e*Health directory by entering the following command in any terminal window (such as an `xterm` or shell window), where `ehealth` is the full pathname of that directory:
   ```
   cd /ehealth
   ```
3. Enter the following command:
   ```
   ./bin/nhGetRespLimit
   ```
4. At the following prompt, enter the name of a group of response path elements:
   ```
   Enter a response path group name:
   ```
5. At the following prompt, enter the time range over which you want to evaluate the average response time:
   ```
   Time range:
   1) Custom    7) Last month
   2) Today     8) Previous hour
   3) Yesterday 9) Previous 12 hrs
   4) This week 10) Previous 24 hrs
   5) Last week 11) Previous 7 days
   6) This month 12) Previous 4 hrs
   What is your choice? (1-12)
   ```
6. At the following prompt, enter the factor that eHealth uses to determine the recommended response time limit:

Enter a limit factor [2.0]

You can use the limit factor to tailor the recommended response time limit based on a multiple of the average response time. The default value is 2.0, which causes the script to recommend a limit value that is twice the average response time.

The command then displays the information that you entered and prompts you for the next step. The following is a sample output:

You have specified the following parameters:

Response path group name: PathGrp
Time range: today
Start Date/time: 
End Date/time: 
Limit factor: 2.0

At this point, you can:
1) Continue with retrieval of response limit
2) Change response path group name
3) Change time range
4) Change start date/time
5) Change end date/time
6) Change limit factor
7) View the parameters entered
8) Exit the Script

What is your choice? (1|2|3|4|5|6|7|8)

7. Change the parameters that you specified, or enter 1 to continue. If you enter 1, the command displays the following:

Getting response path limits...
Creating recommendation file: /ehealth/output/topN/nhRecommend.txt

At this point, you can:
1) Exit the script and view/edit the response path limit recommendation in a text editor.
2) View the recommendation

What is your choice? (1|2)

8. Do one of the following:

- Enter 1 to exit the script and review the recommendations file, /ehealth/output/topN/nhRecommend.txt.
- Enter 2 to display the nhRecommend.txt file contents.

The following is a sample nhRecommend.txt file:
Output of the Average Response with Recommended Limit:

Element Avg Response Recommended Limit
"path1-UDP" 25.00 50.00
"path2-ICMP" 25.00 50.00

At this point, you can:
1) Exit the script and view/edit the response path limit recommendation in a text editor.
2) Launch the Set Response Limit script (nhSetRespLimit).

9. Do one of the following:
   • Enter 1 to exit the script.
   • Enter 2 to run the nhSetRespLimit command, which is described in the next section, "Setting Response Limits."
Setting Response Limits

The nhSetRespLimit command sets the response limits based on an input file such as the nhRecommend.txt file that is produced by nhGetRespLimit.

**NOTE**

If you have already run the command through the nhGetRespLimit command (as described in the previous section), proceed to Step 4.

**To run the nhSetRespLimit command:**

1. Log on to the eHealth system as the eHealth administrator; then change to the eHealth directory by entering the following command in any terminal window (such as an xterm or shell window), where *ehealth* is the full pathname of that directory:
   
   ```
   cd /ehealth
   ```

2. Enter the following command:

   ```
   ./bin/nhSetRespLimit
   ```

3. Enter the name of a recommendation file:

   ```
   Enter a recommendation file name: [/ehealth/output/topN/nhRecommend.txt]
   ```

**NOTE**

If you specify a file other than nhRecommend.txt, confirm that it uses the following format for each response path element. The *average* and *recommended* values should be in the format *nn.nn*; for example: 25.00, 35.60, and so on.

   ```
   "elementName" average recommended
   ```

The system displays the following information:

You have specified the following parameter:

   Recommendation file name: nhRecommend.txt

At this point you can:

1) Continue and set the response limits
2) Change the recommendation file
3) Quit

What is your choice? (1|2|3)

4. Do one of the following:

   - Enter 1 to update the response path elements to use the recommended value as the response limit (which you can view using the Modify Path Element dialog box).
   - Enter 2 to specify a different recommendation file.
   - Enter 3 to exit the command without changing the response limits.
Running Response Reports

You can run reports on response elements from the eHealth console or Web interface. Health and Service Level reports require separate licenses and work slightly different from other report types. The following sections describe these report types.

This section describes running the following types of reports:
- At-a-Glance reports
- Trend reports
- Service Level reports
- Health reports
- Response Path Summary reports

Running At-a-Glance Reports

At-a-Glance reports provide an overall look at the critical performance indicators for a response element. Each At-a-Glance report presents several charts on a single page, allowing you to easily compare variables to troubleshoot performance problems. When you identify a problem, you can then drill down directly to a Trend report for more details.

You can run At-a-Glance and Trend reports on performance variables such as round-trip delay, jitter, and jitter variation to obtain an accurate view of the quality of response time or VoIP service that a user experiences.

Figure 2 shows sample charts from an At-a-Glance report for a Juniper RPM response path. These charts show metrics for jitter that you can use to monitor and manage attributes of network traffic that affect the quality of voice service.

![Figure 2. Sample At-a-Glance Report Charts for Juniper RPM](image-url)
Running Trend Reports

Trend reports show a historical view of response performance. Trend reports are useful for troubleshooting response elements by revealing patterns over time, as well as relationships between multiple response elements or multiple variables.

You can use a Trend report to plot one variable for up to ten elements over any time period, or to plot up to ten variables for one element. You can also run a group Trend report that shows either of the following:

- Aggregate data for a group of elements, which allows you to identify trends for the group as a whole
- A separate chart (for each of the chosen variables) for each element in a group, which allows you to compare the performance of elements within a group

Figure 3 shows a sample Cisco IOS IP SLA Trend report. The report shows that, for the specified time period, average response time to ping devices from the router was fairly steady, except for a spike of response time between 2:20 P.M. and 2:50 P.M; this situation may merit further investigation.

Running Service Level Reports

If you have a Service Level Report license, you can run Service Level reports to on response elements to accomplish the following:

- Determine relative performance of applications within your infrastructure.
- Determine the availability, usability, usage, and usage trends of the VoIP service and long-term trends in voice quality.
- Obtain monthly or quarterly summary information about an enterprise, a region, a department, or a business process.

Before you run these reports, create groups and group lists for your response elements, as described in “Creating Response Groups and Group Lists” on page 33. You might prefer to specify the ranges against which to measure service levels. eHealth uses a default service profile that defines values from these ranges, but you might prefer to create your own customized service profiles.

Table 5 on page 32 lists the various types of Service Level reports that you can run on response elements. For more information about running standard eHealth reports for response elements, refer to the Console Help and the Web Help.
Running Health Reports

If you have a Health report license, you can run a Health report on the response paths or response endpoints (sources and destinations), depending on the elements that appear in the Exceptions section and in the Situations to Watch table. That is, a report on paths and a report on endpoints in the same group are identical. However, a Health report on paths contains only paths in the Exceptions section and in the Situations to Watch table, whereas a report on endpoints contains only endpoints in the Exceptions section and in the Situations to Watch table. In either case, the data in the report pertains to the paths in the group.

For a response path Health report, eHealth includes the paths listed in the group. For a response endpoint Health report, it includes all paths whose source or destination is an endpoint in the group. A Health report on endpoints could result in duplicate path data if an endpoint and a destination are in the group.

Health Report Sections

Health reports on response elements contain four sections: Exceptions, Summary and Top Ten, Element Detail, and Supplemental.

NOTE

The standard response Health report is designed for Service Availability, Cisco IP SLA, and Juniper RPM. For Application Response, use the CIO Summary report.

Exceptions Section. The Exceptions section of a daily Health report contains an Exceptions Summary and an Exceptions Detail report. Examine this section to determine if an element experienced high latency, high packet drops, long response times, or low availability during the report period. The Exceptions Summary report lists those elements that experience the highest rate of these conditions. The Exceptions Detail report also provides details about the most frequently occurring of these conditions.

Summary and Top Ten Section. The Summary and Top Ten section contains summary information on the elements in the report and on the response time leaders and change leaders. The charts in this section report on the average normalized response time for all elements by day and by hour, the top ten leaders in response time, and the top ten change leaders in response time. It also contains a Situations to Watch chart that lists either the endpoints or paths that require close monitoring.

Element Detail Section. The Element Detail section compares data for each element in the report. This section provides charts that show the Health Index, response time compared to the baseline, response time compared to limit, and availability of each element.

Supplemental Section. The Supplemental section provides more detail on the group. Some of the charts in this section allow you to view the same information displayed in the Summary and Top Ten sections, but for more elements than the other sections provide.

Other charts in the Supplemental section do the following:

- List the threshold settings for Health Indexes and Situations to Watch.
- List elements that experienced missed polls, bad polls, and reboots.
- Display the availability, response, and reachability of each element in the report.
Running Response Path Summary Reports

You can determine which paths in a selected group have the worst performance by generating response path Daily Summary Reports. For Cisco IP SLA, Juniper RPM, and Service Availability, you can report on path performance by component (specifically, DNS lookup, TCP connect, and transaction time). For Application Response, you can report on path performance by client, server, and network.

The Daily Summary Report charts provide the following information:

- Ranking of the 25 response paths with the worst performance, according to their average response time
- Total response time for each group for each unit in the baseline period compared to the overall trend for the group
- Summary of each component’s contribution to the total response time for the selected report period

Generating the Report

To generate a response path summary report, select the specific report type from the Report list in the Run Health Report dialog box as follows:

- To report on a SystemEDGE agent with the Service Availability module, select ServiceResponse.
- To report on an Application Response agent, select ApplicationResponse.

After specifying the report type, select ResponsePath from the Subject list; then select a group from the Group list. For complete instructions, refer to the procedure on running Health reports in the eHealth Administration Guide.

NOTE

When creating groups of router/switch elements, LAN/WAN elements that correspond to groups of response charts, or response elements, the eHealth administrator must use the same name as the response path group name; otherwise, the user cannot successfully drill down to Top N reports from Service Availability and Application Response Path Summary reports.
Index

A
Agents
AR 8
Cisco IP SLA 9
Juniper RPM 9
SystemEDGE 8
Application Response
overview 8
reports 31
AR 8
At-a-Glance reports 42

C
Cisco
jitter protocols 16
ping protocols 16
Cisco IP SLA
creating response destination elements 14
creating response paths 16
overview 9
Cisco SA Agent, overview 9
Creating
destination elements 14
response paths 16

D
Deleting, response elements 29
Destination elements
creating 14
modifying 28
Destinations, Health report 44
Dialog box
Add Destination Element 14
Add Groups 34
Group List 36
Modify Path Element 24
Modify Path Elements 26
Response Path Manager 22
Discover
overview 11
response elements 12
response sources 12
scheduling 13
Disman
ping protocols 16
pre-existing response paths 11

E
eHealth — Response
element naming conventions 19
elements
adding to poller configuration 11
discovering 12
groups and group lists, creating 33
limits 38
managing for reports 31
nhGetRespLimit utility 38
overview 7
polling errors 20
protocols 16
reports, running 42
response path elements, creating 17
response paths, creating 16
Elements
deleting 29
destination 14, 28
naming conventions 19
source 28
G
Group lists
   creating for response 36
   response 33
Groups
   creating for reports 33
   response 33
   used as filter for console and Web 33

H
Health reports 44

I
IP SLA
   creating response destination elements 14
   creating response paths 16
   discovering 12
   overview 9

J
Jitter
   Cisco measurement 9
   Cisco protocols 16
   Juniper definition 9
   Juniper protocols 16
Juniper RPM
   creating response destination elements 14
   creating response paths 16
   jitter definition 9
   jitter protocols 16
   overview 9
   ping protocols 16

L
Live Exceptions, monitoring elements 23

M
Modifying
   destination elements 28
   response paths 24
   source elements 28

N
Naming conventions, response elements 19
Network resources 9
nhSetRespLimit utility 41

P
Packet loss 9
Path builder 18
Path Summary reports 32
Paths
   AR 20
   deleting 29
   Health report 44
   modifying 24
   pre-existing 11
   response 10, 16
   paths.cfg.log file 23
Ping protocols
   Cisco 16
   Disman 16
   Juniper 16
   RFC2925 16

R
Recommendation file, specifying 41
Reports
   Application Response 31
   At-a-Glance 42
   CIO SLR 32
   Cisco IP SLA reports 9
   Health 44
   health 44
   Juniper RPM reports 9
   Path Summary 32
   preparing to run 33
   response 31
   response sources, destinations, and paths 31
   response summary 45
   running 42
   Service Level, response 43
trend 43
   Trend reports 43
Response
   adding paths 17
   deleting paths 29
   element naming conventions 19
   endpoints 44
Response (continued)
  Health report 44
  modifying paths 24
  reports 31
  saving paths in file 23
  sources, discovering 12
  summary report 45
Response destination
  adding elements to the poller configuration 14
  creating 14
  elements 14
  troubleshooting 20
Response elements
  adding 11
  deleting 29
  discovering 12
  managing 21, 22
  naming 19
Response limit
  definition 38
  evaluating 38
  recommending and setting 38
Response paths
  adding elements to the poller configuration 17
  AR 20
  creating 10, 16
  deleting elements 29
  managing 22
  managing elements 22
  modifying 24
  polling errors 20
  pre-existing 11
Response report types 31
Response source, modifying elements 28
Response summary reports 45
Response time, monitoring with eHealth 10
RFC2925
  ping protocols 16
  pre-existing response paths 11
RPM
  creating response destination elements 14
  creating response paths 16
  discovering 12
  overview 9
RTTMON, Cisco 16
Running reports 42

S
SA
  discovering 12
  overview 8
SAA. See IP SLA.
Scheduling discover 13
Service Availability 8
Service Level reports, response 43
SNMP agents, discovering 12
Source elements, modifying 28
SystemEDGE, plug-in modules 8

T
Trend reports 43

V
Variables
  NH_DISCOVER_RESPONSE_PORTS 12
  NH_RTR_ZERO_DATA_POLLS 20
  NH_RTTMON_MAX_PATHS_PER_AGENT 18
Voice Quality Monitor 8
VQM
  discovering 12
  overview 8