CRANNOGSOFTWARE
making networks assets, not overheads

ResponseWatch User's Guide

Version 1.5.1

www.crannog-software.com

Contents

Introduction

This document is intended as a User Manual for the Crannog Software ResponseWatch product, a software product designed to collect IP SLA information from Cisco equipment and provide meaningful and useful graphical and textual based reporting.

Please consult your Cisco documentation for any queries you have relating to the equipment itself. For more information on IP SLA from the Cisco website, go to Cisco IPSLA .

This manual is regularly updated. Visit ResponseWatch to download the latest version.

What is Cisco IP SLA?

Cisco IP SLA is a network performance monitoring agent that is embedded in the Cisco IOS. It measures response times, network resource availability, application performance, jitter, connect time, throughput and packet loss. Performances can be measured between Cisco device and any remote IP host.

What is ResponseWatch?

ResponseWatch is a standalone software product that collects IP SLA information from Cisco devices. This information is then presented to users on a web front-end. ResponseWatch provides the user with a powerful but easy to understand view of network performance.

Features and Benefits

- IP SLA is embedded in Cisco IOS (No additional Hardware Costs)
- Unique GUI giving Real-time Views of your networks performance.
- Monitoring of your networks SLAs.
- Ease of configuration and use.
- Configurable time-based performance reporting in HTML, PDF or CSV formats with SLA compliance and breach information.
- Executive Reports detailing in textual and graphical format
- Configurable SLA Alerting allowing you to receive SysLog alerts whenever a breach or sustained breaches occur.

Installation

Minimum System Requirements

The specification of your ResponseWatch system depends on the number of tests ResponseWatch is collecting statistics from. These requirements are the absolute minimum needed for the system to run:

- 256 MB RAM
- 2 GB free hard disk space on the volume to which the database is installed, 100 MB free hard disk space on the volume to which the program is installed.
- Pentium III, 1 GHz or greater
- Windows NT4 or greater.

Cisco Device: The Cisco Device and its IOS version must support IP SLA. For more information consult the Cisco IP SLA IOS support Matrix in Appendix 2 of this manual.

Installation on Microsoft Windows™

Installation is straightforward and should take no more than a few minutes. If you received ResponseWatch on CD the setup program should start automatically. If not, simply open the CD drive in My Computer and double-click "setup.exe". If you downloaded the software simply double-click the file you downloaded. Installation involves several steps. At each step, you can click the "Next >" button to accept the default choices and continue.

Ready to Install

Click "Install" to start. Installation should take no more than a few minutes. If it appears to have stopped for a long time you should contact Crannog Software. When installation is complete you can click "Finish" to close the install program. The following steps are required for installation of ResponseWatch:

Welcome & Licence Agreement

Once the Java Runtime Environment is installed, you can press the "Next >" button to view Crannog Software's licence agreement, which you must agree to before pressing "Next >" again.

Customer Information

You will be asked to provide your name and company name, and whether to install the software just for yourself or for every user that logs in to the system. If you choose to install the software just for yourself, only you will see the shortcut to the web front-end and only you will be able to uninstall the software.

Setup Type

If you choose "Complete" ResponseWatch will be installed to the folder "responsewatch" on your system drive, MySQL to the folder "MySQL" on the same drive, and the internal web server will run on port 80 if available. If port 80 is unavailable you will be prompted to choose another. If you want to change the install folders or choose a different port even if 80 is available you must choose "Custom".

Custom Setup

You will only see this dialog if you chose custom setup above. You should see options for ResponseWatch and MySQL, unless an unsupported version of MySQL was detected. To change the install folder for either ResponseWatch or MySQL, click on the feature and then on "Change…"

Select HTTP Port

You will only see this dialog if you chose custom setup or if port 80 is in use. You can choose a port and press "Test" to check if it is available, or simply press "Next >" this will not allow you to proceed if the port is unavailable.

Installation Issues

The following are some solutions to potential installation issues that you many encounter:

Unsupported MySQL detection

If MySQL is installed on the server already, you will see a message informing you of this and asking if you wish to continue. While it is not recommended that you do continue, it is possible. Note however that ResponseWatch was tested with the version of MySQL it ships with and may not function correctly with a different version. The installation program will fail if the installed version of MySQL uses a root password.

Java Runtime Environment installation

If the server does not have the required version of the Java Runtime Environment installed, you will be prompted to press Ok to install it. It will take several seconds to launch the Java installer, after which you must accept Sun's licence agreement. You will then be given the choice of Typical or Custom installation: if you wish not to have your web browser configured to use Sun's Java Plug-in you must choose Custom installation.

Quick Start

Once you have successfully completed the installation of ResponseWatch there are a few essential steps required to collect and display the IP SLA information from your network. More detail for each step is available in subsequent sections of this manual.

- Set up IP SLA on your router(s) or switch(es).
  - Appendix 1 gives a quick guide on setting up IP SLA on Cisco devices. For more information on this, refer to your router documentation, or go to Cisco IPSLA .
- Install ResponseWatch on the workstation as shown in the previous section.
- You can access the web-based interface of ResponseWatch using a web browser.
  - The interface can be shown by opening a web browser and going to: http://<IP_of_the_Responsewatch_Machine>: <port number>.
  - The port number is selected during installation. This can be omitted from the above URL if it is the default value of 80. Make sure there is no other web server running on this port, as only one web server application can use each port.
- Click on the Configuration Button.
- Click "All Devices" this section allows you to add a device to ResponseWatch. Simply enter a Device Name, Device IP and the devices Community String then click 'add'. This is the minimum required for monitor a device.
  - **Licensing:** If you have received a licence with ResponseWatch, it should be loaded here. If you have received the licence in a binary file, upload the file using the **browse** and **load** buttons. If you have it in text-based hex code, paste it into the window provided and click **decode**. ResponseWatch will run without a licence in evaluation mode for 24 hours.
  - For more configuration information, read the Configuration Guide.
- Graphs will be available to view almost immediately. Click on **home** at the top of the page and go to **Reporting -> View Devices** to access the graphs.

Once you have added a device to ResponseWatch and configured IP SLA on that device you can view information relating to the overall performance of that device.

Configuration Guide

System Settings

Responsewatch comes with pre configured system wide default settings for alerting and SLA Threshold values. The alerting defaults are the alerting settings used for all newly created groups in Responsewatch. The default SLA Threshold values are the values given to all newly discovered IP SLA tests.

Adding a device

To add new device to ResponseWatch you need the IP address and 'read only 'community string of the device you wish to add. Once the device is added ResponseWatch discovers all the IP SLA tests configured on that device. If the status indicator is not 'up' there may have been a problem discovering the device. The usual causes of this are a wrong community string or access restrictions to device.

Grouping

ResponseWatch includes the concept of "IP SLA Groups". IP SLA Groups lets you assign individual IP SLA tests to logical or physical groups. These groups can then be used into the creation of Real-Time Views (See Below) and reporting.

From this page you may create, change or remove IP SLA groups from the system. You can also configure alerting settings for the group.

You must press **OK** on this page to commit changes to the groups. Click **Add** to add an IP SLA group to the system or on a groups name to change or remove it.

Real-Time Views

Real-time views are the main GUI interface with Responsewatch and they are created in this section. Every Real-Time view consists of a number of segments which correspond to a specific group. You can add as many segments to a Real-Time view as you like however if there is too many segments the Real-Time view may become less readable. From this page you may create, change or remove Real-Time views from the system. You must press **OK** on this page to commit changes to the Real-Time views. Click **Add** to add new Real-Time view to the system or on a views name to change or remove it.

Alerting

Alerting within Responsewatch is purely group based. Therefore if you wish to alert on a specific test you must add it to a group and then configure alerting for that group. The alerting is based on a standard Rising\Falling model. Alerts are sent when a test goes over a certain threshold and are not sent again until the test goes below that threshold. Alerting can also be configured so tests do not alert until they exceed their threshold for a certain period of time. E.g. alert when a test exceeds its SLA for 15 minutes or more. All alerts are currently sent as syslog messages. Groups can be configured to send alerts to different syslog servers if required. Viewing and general alert handling should be done using a 3rd party event management system.

IP Application Names

Responsewatch performs 'TCPConnect' and 'UDPconnect' tests based on port number. These correspond directly to specific network applications. Many are predefined (well-known ports) while others (registered ports) are defined by the software manufacturer. ResponseWatch comes configured with the well-known ports as well as many others. You can edit this list yourself with this page. By default, ports below 1024 are not shown on this page as they normally don't need to be changed but, if required, these can be shown by clicking (more…) in the title of the Port column. A comprehensive list of all the well-known and registered ports is available at ***http://www.iana.org/assignments/port-numbers***.

Licensing

If you have received a licence with ResponseWatch, it should be loaded here. If you have received the licence in a binary file, upload the file using the **Browse** and **Load** buttons. If you have a long string of letters and numbers, paste it into the window provided and click **Decode**. ResponseWatch will run without a licence in evaluation mode for 24 hours. After loading the licence, click **Ok** to activate it or **Cancel** to abort. You can also check the status of an existing licence on this page.

Security Settings

You can set up password protection of the web front end to ResponseWatch by adding user accounts here. To add an account, type a login and the same password twice, and tick the administrator box if you wish the user to be able to configure the system. Click **Add** to add the user. To delete an existing user, tick the box above the **Delete** button corresponding to them and click **Delete**. You can also make a user an administrator or not and change there password. You must also choose what level of protection you desire. You can choose not to protect access at all; to protect only configuration access or to protect both configuration and normal access.

User Guide

Real-Time Views

This section represents the main ResponseWatch Graphical User Interface. The Real-Time view places IP SLA tests in various locations on the 'Target' view based on how they are performing. The user can see at a glance how its network is performing. The dropdown box allows users to switch between various Real-Time views. The 'Detach' button allows user to display multiple "Mini Real-Time Views" on one screen.

IP SLA tests in the green area are complaint with their SLA and are not in need of immediate attention. Tests within the red area have exceeded their SLA and are in need of attention. Tests gradually become closer to the red area as they near their SLA. When a test requires attention the user can click on that test and get a detailed graph as to how it is performing.

IP SLA Performance Graphs

In the reporting section you can view all the devices that ResponseWatch is currently monitoring. By clicking on a device you can view some high level information on that device and performance graphs on all the IP SLA tests configured for that device. The performance graphs available depend on the 'Type' of the IP SLA test.

The Latency Graph represents minimum, average and maximum response times for that test over a specific time period. The default display is the previous 25 hours however weekly, monthly and quarterly views are also available.

The Availability Graph represents connectivity availability of the IP SLA test. The single red line represents connection from the ResponseWatch server machine and the Cisco device running the IP SLA test. The green blocked represents the availability of the service the IP SLA test is monitoring. To get a correct availability representation for the IP SLA test the red line should always be at 100%.

The Packet Loss Graph shows minimum, average and maximum packet loss figures for that test over a specific time period. The default display is the previous 25 hours however weekly, monthly and quarterly views are also available. This graph is only available for jitter IP SLA tests.

The VoIP Scores Graph shows minimum, average and maximum VoIP scores results for that test over a specific time period. The default display is the previous 25 hours however weekly, monthly and quarterly views are also available. This graph is only available for jitter IP SLA tests. For more information on VoIP scores see here.

IP/SLA Performance Reports

This section allows you to view reports of IP/SLA tests and is available though the 'Reporting' button on the ResponseWatch splash screen. It also provides you with SLA compliance and breach count information per test displayed.

You can generate a report based by selecting the following:

- All Devices, All groups or an individual device or group.
- A Time period of daily, weekly, monthly, quarterly or yearly.
- You can filter by showing all IP/SLA tests or select from Echo, APM, Jitter, Http, VoIP jitter, IP Connect, Udp Echo, Dns or Dhcp tests.
- You can choose to show one or multiple of the following resport types on the same page:
    - Response Times
    - Availability
    - Jitter Source-Destination and Jitter Destination-Source
    - Packet Loss Source-Destination and Packet Loss Destination-Source
    - Mos Score

Each report can viewed in HTML, PDF or CSV format and a summary of information in the report is provided at the end of each report. The data per test based on the type of report generated provides links into the respective IP/SLA Performance Graphs.

SLA Executive Summaries

This section allows you to view SLA Executive summaries and is available though the 'Reporting' button on the ResponseWatch splash screen. It provides you with a detailed SLA compliance and breach count information for Network Quality, Application Performance and VoIP Network Quality which are further explained in the Report Glossary at the end of the report.

You can generate an SLA Executive summary by selecting the following:

- A report format, either textual or graphical.
- All groups or an individual group.
- A Time period of daily, weekly, monthly, quarterly or yearly.

On the graphical report each pie chart gives an overall SLA Compliance Percentage and Breach Count for each section and is linked to the IP/SLA Performance reports as are the individual colour coded bars to the right of the pies.

The textual report provides the same data in the HTML, PDF or CSV format.

Alerting

SLA Alerting can be set per group, by selecting a group and in the group details change the following:

- Enabled or disable alerting for the group.
- Provide a SysLog server IP address where the alerts will be sent.
- Provide a period in minutes that indicates whether an alert should be sent due to a sustained breach.

In the 'home > configuration > system settings' section you can also set the default values for the above, which are used when a group is created.

Appendix 1: Configuring Cisco IP SLA

IP SLA operations are configured using the Cisco CLI.

The main command used is' RTR' in older IOS versions and 'IP SLA Monitor' in newer IOS versions

To configure a new IP SLA test perform the following steps starting in global configuration mode: -

Configuration Steps

1. Firstly enter Configuration mode by typing 'RTR' or 'IP SLA monitor' and an ID number for the test.
2. Choose the type of test you which to configure using the TYPE command.
3. Configure test characteristics (Optional).
4. Type exit to return to global configuration.
5. Schedule the test.

Setting Test Characteristics

IP SLA Command	Purpose
Router (config-rtr)# **tag** *text*	Textual Description for the test.
Router (config-rtr)**#frequency** *seconds*	Sets how often the test performs the test.
Router (config-rtr) **#lsr-path** *{name | ip}...*	Defines the path the IP echo tests take.
Router (config-rtr)**#owner** *text*	The owner of the test.
Router (config-rtr)**#timeout** *milli*	The amount of time the test waits for a response.
Router (config-rtr)**#tos** *number*	Defines the IP tos Byte.

Scheduling the Test

After you have configured the test you now have to start the test collecting statistics. You can schedule a test to start immediately or sometime in the future. You can also set how long you wish the test to collect statistics.

To schedule the test use the following command in global config mode:

ip sla monitor schedule id **start-time** now **life** forever

or

Rtr schedule *id* **start-time** *now* **life** *forever*

Detailed IP SLA Configuration Guide

For a detailed discussion on configuring each individual IP SLA test and for configuring IP SLA Alerting see the **Cisco IP SLA Configuration Guide**

Appendix 2: Frequently Asked Questions

Installation

I can't access the web interface for Responsewatch

The front-end of Responsewatch is completely implemented in a web-based interface. This is accessed from the browser with a URL of the form ***http://<server>:<port>***, where ***<server>*** is the name or IP address of the Responsewatch workstation and ***<port>*** is the port number specified during installation, e.g. ***http://responsewatch:8000*** (If you are using the default port of **80**, the port number can be omitted). To access ResponseWatch from the workstation on which it is installed, you can use the shortcut inserted in the Start Menu by the installer. You can also use this shortcut to ascertain which port the web server uses.

When I try to access the web interface, I see another web server. How does this happen?

During installation, ResponseWatch checks that your selected port is not in use by another web server but, if that other server is not running, it will not be detected. Either disable the other web server, (if it is not required) change its server port or re-install ResponseWatch using another server port.

Cisco IP SLA

What impact does IP SLA tests have on router CPU and Memory?

The table below show the results of tests carried out by Cisco on Cisco 2600 Router with a 40MHZ Motorola 860 RISC CPU.

Test Type	Operations per min	Avg Mem	Avg CPU (ms)
UDP Echo	2000	13k	8.65
UDP Jitter	1440	17k	22.63
ICMP Echo	2000	11k	1.90
Responder	3900	58k	7.60

What Cisco IOS Supports IP SLA?

Feature	11.2	12.0(3)T	12.0.(5)T	12.1(1)T	12.2(2)T
ICMP Echo	X	X	X	X	X
ICMP Pathecho	X	X	X	X	X
SNA	X	X	X	X	X
UDP Echo		X	X	X	X
TCP Connect		X	X	X	X
UDP Jitter			X	X	X
HTTP			X	X	X
DNS			X	X	X
DCHP			X	X	X
DLSw+			X	X	X
One-way latency				X	X
FTP Get				X	X
SNMP Support				X	X
MPLS VPN					X
Frame Relay					X
ICMP Path Jitter					X
APM					X

How Secure is IP SLA?

If necessary IP SLA can be configured to be MD5 encrypted.

Appendix 3: Third Party Software Components

ResponseWatch makes use of several third party libraries, distributed under various licences.

MM.MySQL

ResponseWatch includes MM.MySQL v2.0.13, available at http://sourceforge.net/projects/mmmysql/. This is distributed under the Lesser GNU Public License, a copy of which is available at http://www.gnu.org/licenses/lgpl.html.

Jakarta Log4j

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).
ResponseWatch includes Jakarta Log4j v1.1.3, available at http://jakarta.apache.org/log4j/. This is distributed under the Apache Software License, a copy of which is available at http://www.apache.org/LICENSE.

Jakarta Tomcat

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).
ResponseWatch includes Jakarta Tomcat v3.3.1, available at http://jakarta.apache.org/tomcat/. This is distributed under the Apache Software License, a copy of which is available at http://apache.org/LICENSE.

joeSNMP

ResponseWatch includes joeSNMP v0.2.6, available at http://www.opennms.org/files/releases/joeSNMP/. This is distributed under the Lesser GNU Public License, a copy of which is available at http://www.gnu.org/licenses/lgpl.html.

jspSmartUpload

This product includes software developed by Advantys (http://advantys.com).
ResponseWatch includes jspSmartUpload v2.1, available at http://jspsmart.com. This is distributed under the Advantys Freeware license contract, a copy of which is available at http://jspsmart.com/liblocal/docs/legal.htm#free.

Jasper Reports

ResponseWatch includes Jasper Reports, available at http://sourceforge.net/projects/jasperreports/.

This is distributed under the Lesser GNU Public License, a copy of which is available at http://www.gnu.org/licenses/lgpl.html.

JFree Charts

ResponseWatch includes JFree Charts, available at http://www.jfree.org/lgpl.php. This is distributed under the Lesser GNU Public License, a copy of which is available at http://www.gnu.org/licenses/lgpl.html.