



**CRANNOG**SOFTWARE  
making networks assets, not overheads

# ResponseWatch



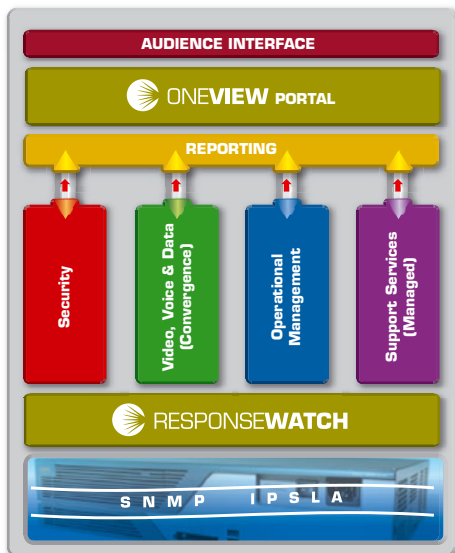
RESPONSE**WATCH**

# ResponseWatch - A sound business decision

It's often said that knowledge is power. In our experience it's true: if you know just what's happening on your network, you have the power to optimise its performance. Response times are arguably the most important performance information relating to the network infrastructure - including applications. So ResponseWatch gives network managers and others with responsibility for administration, support, convergence and security, the insight into network responsiveness they need, to make informed decisions.

Most users are unaware and indeed uninterested in the status of the network and the individual devices on it. They are only interested in the effect it has on their daily jobs. If half the network is down, but users can still send email and access files, then they are happy. What affects the user, and in turn makes or breaks the IT manager's day, is service availability, not network availability.

We have identified four key areas where the improved insight into network activity that ResponseWatch and other Crannog Software applications provide, can have a major impact on organisational effectiveness.



## IP SLA - Network & Application Performance and Availability Management



### Security

Monitoring network activity can play a major part in establishing and maintaining network security. Our monitoring software is based on these fundamentals:

### Coverage

ResponseWatch provides a complete picture of response times across the network, highlighting bottlenecks and potential faults.

### Visibility

Network monitoring can play a significant, albeit passive, part in an overall security strategy. Typical external attacks, such as a major virus (e.g. SQL Slammer) or DoS attack, will negatively affect response times across the

network. ResponseWatch is ideal for highlighting the areas where these negative effects are being felt.

### Operational Management

In order to keep carrier costs under control, Wide Area Networks must run to fine tolerances. As key links are optimised to match available bandwidth to demands, our monitoring software provides the information needed to make informed decisions.

### Proactive Management

ResponseWatch gives management the tools to be proactive. Armed with real-time information on network performance and availability, the support team can warn users of potential problems in advance, thus reducing

# ResponseWatch - Quick and easy install

costly, time-consuming and potentially unnecessary calls to the helpdesk.

## Real-time Information

The Bullseye function in ResponseWatch gives network managers real-time insight into responsiveness across the entire network.

## SLA Management & Compliance

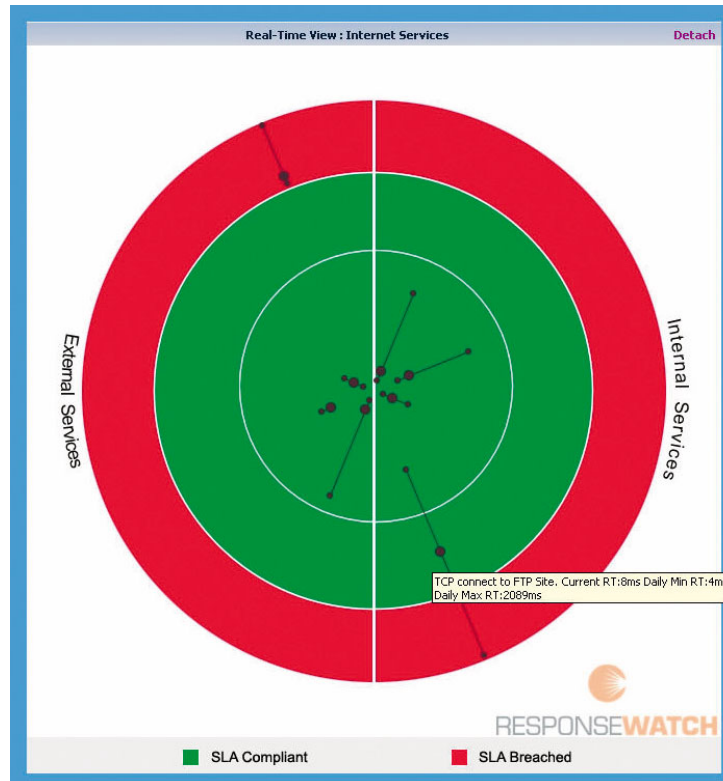
ResponseWatch allows network administrators simultaneously to specify SLA thresholds based on external agreements and also internal expectations of the network's responsiveness. Multiple SLAs can be set per test by applying different thresholds per test group. ResponseWatch integrates with network management systems so that the alerts it generates can be acted on immediately.

## Usability Metrics

By graphing and reporting on MOS and ICPIF voice quality scores, as well as packet loss, jitter and latency, ResponseWatch provides an excellent overview of user experiences.

## Scenarios of use

Scenario	Attributes	Outcome
<b>Security</b>	Ability to monitor link attributes such as availability, packet loss and response time.	Changes in these attributes could indicate tampering of the link or packet interception/redirection.
<b>Video, Voice &amp; Data</b>	Ability to simulate VOIP packets to test end to end network attributes (jitter, response time and packet loss).	Provides the ability to monitor the effects of changes in QOS configuration on VOIP and other network application packets.
<b>Operational Management</b>	Ability to monitor link attributes such as availability, packet loss and response time.	Allows management to monitor link SLAs for suitable service levels and network provider compliance.
<b>Support Services</b>	Ability to monitor link attributes such as availability, packet loss and response time. Ability to monitor web (http) servers for availability and response.	Allows support and services team to identify source of network problems.
<b>Capacity Planning &amp; Traffic Engineering</b>	Ability to monitor the effects of changes in QOS configuration on VOIP packets. Ability to monitor link attributes, such as availability, packet loss and response time.	Changes in attributes will identify network segments of interest (for upgrades, QOS re-engineering etc.)



## The Real-time View

The real-time view gives a snapshot of grouped response time tests. Each item on the bullseye shows the current response time, as well as the range of minimum and maximum values recorded in the past 24 hours.

An item in the red region is outside its SLA value. Hover the mouse over an item to see the actual response time values; click on it to see the response-time graph for this test

## Video, Voice & Data Convergence

As more applications depend on IP networks for their functionality, it is vital that network management has a clear picture of what is happening.

## Coverage

Providing a complete view of what is happening on IP networks handling data, voice and performance-critical applications such as video and voice over IP and thin client implementations.

## Planning for convergence

Can the network cope with a planned or actual voice/video over IP implementation? Using ResponseWatch to baseline network performance before, during and after rollout increases the probability of a successful project and minimises unnecessary expenditure.

## Support Services

Keeping networks running smoothly is very demanding on managers and administrators. The insight and information we provide can greatly ease that burden.

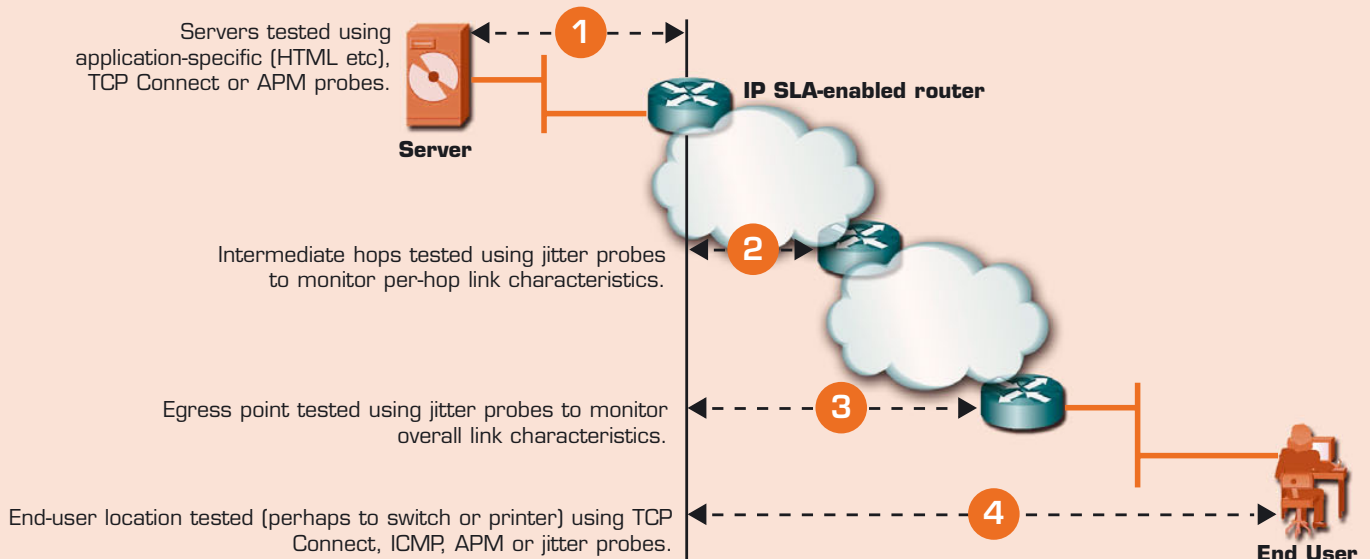
## Reduced Fix time

ResponseWatch allows instant identification of bottlenecks and faults and reduces the time to fix those faults by highlighting the location of the 'real' issue. The email system is not necessarily down, simply because a user

# ResponseWatch - Easy to understand

## Using ResponseWatch for End-to-end Performance and Availability Monitoring

Proper probe selection and positioning can provide an end-to-end view of key network health indicators



complains of losing access to it, for instance - it could potentially be either a LAN or WAN issue. Network availability does not always match network usability, but ResponseWatch allows you to gauge response times across each hop on a packet's journey and so zero in on the underlying cause of such problems. In addition, ResponseWatch monitors the end-user experience, so that management and support can see and confirm that particular applications are working satisfactorily at the client end, identify any that aren't and even identify where on the network an application is or is not working.

### QoS & Continuity

Where network capacity becomes an issue, network engineers need to choose which quality-of-service parameters must be selected, to ensure that network-critical and sensitive applications, such as Video and Voice-over-IP, deliver the required level of service.

### Product Summary

ResponseWatch uses an embedded agent in the Cisco IOS called IP SLA to gather network performance monitoring statistics. IP SLA measures response times, network resource availability, application performance, and jitter, connect time, throughput and packet loss.

Once any performance drops below a certain level, availability drops or latency increases. ResponseWatch alerts use Syslog messages direct to the management workstation, rather than email alerts, making it an ideal adjunct to an event management system.

Finally, many critical management questions about the network become easy to answer:

- How do we know our infrastructure is providing an appropriate service?
- How do we measure performance against SLA thresholds?
- How do we report on our performance?

- How can we measure response times across the network for different types of traffic?
- How can we ensure these response times are within agreed-upon SLAs?
- How can we report on network availability in an easily-understandable format?
- How can we be aware of long-term trends in network availability and response times?
- How can we integrate this information in a single business view?

ResponseWatch integrates with other Crannog applications through the OneView portal, enabling multiple installations to be managed from a single interface. Please see the OneView PDF for more details.

# ResponseWatch - Rich in features

main menu > reporting > sla executive summary

**Summary Filter**

Report Format: Graphical | Timeperiod: Daily | Group: All Tests | All Tests | Generate

**SLA Executive Summary**

Report Coverage: From 11:40 on 20/4/2006 to 11:40 on 21/4/2006 (Day) | Group: All Tests

**Network Quality**

Network Quality - Breaches 21

95.8% Compliant | 4.2% Non Compliant

Response	SLA Breaches	Compliance	Availability	Outages	Compliance
SLA Breaches 13	94.327%	5.673%	Outages 0	100%	0%
Packet Loss	99.231%	0.769%	Jitter	97.692%	2.308%
SLA Breaches 2			SLA Breaches 6		

Network Quality is an overall value of the performance from all network performance tests for the selected group.

**Application Performance**

Application Performance - Breaches 26

95.8% Compliant | 4.1% Non Compliant

HTTP Response	SLA Breaches	Compliance	HTTP Availability	Outages	Compliance
SLA Breaches 0	100%	0%	Outages 26	100%	0%
DNS Response	100%	0%	DNS Availability	100%	0%
SLA Breaches 0			Outages 0	100%	0%
DHCP Response	100%	0%	DHCP Availability	100%	0%
SLA Breaches 0			Outages 0	100%	0%
IP Connect Response	100%	0%	IP Connect Availability	100%	0%
SLA Breaches 0			Outages 0	100%	0%

Application Performance measures the network performance based on key applications on the network or network group.

**VoIP Network Quality**

VoIP Network Quality - Breaches 21

95.5% Compliant | 4.5% Non Compliant

Response	SLA Breaches	Compliance	Availability	Outages	Compliance
SLA Breaches 13	88.654%	11.346%	Outages 0	100%	0%
Jitter	97.692%	2.308%	Packet Loss	99.231%	0.769%
SLA Breaches 6			SLA Breaches 2		
MOS Score	100%	0%			
SLA Breaches 0					

VoIP Network Quality shows the performance of your voice network using all the key metrics that affect voice quality.

## SLA Executive Summary

The SLA executive summary is a simple-to-read overview of the performance of your network. Select a group and a time period and the report will show you the response and availability results for those tests over that period of time.

The number of SLA breaches and outages is shown, with a percentage that indicates a test's compliancy.

Click on a value to see a detailed performance report with more IP SLA test statistics.

## Group Configuration

IPSLA tests are arranged into groups for a number of purposes:

- The real-time views are built from groups: one group per segment on the display.
- SLA values are assigned to tests per group. As a test can be a member of multiple groups, different SLA values can be set for each group, to correspond to different audiences. e.g. one SLA value for a service provider and another for internal use.
- Alerting is configured per group. Set alerting to 'enabled' for a group and specify a syslog destination address that should receive an alert every time an SLA is breached.
- Groups are required for executive summaries.

home > configuration > groups > group settings

**Group Settings**

When new IP SLA tests are added to this group their initial SLA will be the SLA value for this test outside of this group. These SLA values can be changed within this group. Alerting can also be enabled/disabled at the group level.

**Group Details**

Group Name: Local VOIP tests  
 Group Description: all remote college jitter tests  
 SLA Alerting: Disabled  
 Syslog Server: 127.0.0.1  
 Alert when SLA is exceeded for more than 0 minute(s)

**Available IP SLA Tests**

IT Dundalk---->HTTP---->Local Dundalk IT website response  
 IT Dundalk---->TCP Connect---->TCP connect to FTP Site  
 IT Dundalk---->Echo---->Ping test from Dundalk to Tallaght 7200  
 IT Blanchardstown---->HTTP---->Local Blanchardstown IT website response time  
 IT Blanchardstown---->TCP Connect---->TCP connect to FTP Site  
 IT Blanchardstown---->Echo---->ping test from Blanchardstown to Tallaght 7200  
 IT Tallaght---->HTTP---->Tallaght IT website response time

Group 'Local VOIP tests' contains 12 IP SLA Tests

>Description	Response	Availability	Loss SD	Loss DS	(+) Jitter SD	(-) Jitter SD	(+) Jitter DS	(-) Jitter DS	>MOS Score
IT Waterford---->Jitter---->Jitter Test From Remote 3640 to Tallaght Core 7200	80	100.0	0	0	60	60	60	60	0
IAD Dun Laoghaire---->Jitter---->Jitter Test From Remote 3640 to Tallaght Core 7200	80	100.0	0	0	60	60	60	60	0
IT Tallaght---->Jitter---->Jitter Test From Remote 3640 to Tallaght Core 7200	80	100.0	0	0	60	60	60	60	0
IT Blanchardstown---->Jitter---->Jitter Test From Remote 3640 to Tallaght Core 7200	80	100.0	0	0	60	60	60	60	0
IT Dundalk---->Jitter---->Jitter Test From Remote 3640 to Tallaght Core 7200	80	100.0	0	0	60	60	60	60	0
IT Athlone---->Jitter---->Jitter Test From Remote 3640 to Tallaght Core 7200	80	100.0	0	0	60	60	60	60	0
IT Sligo---->Jitter---->Jitter Test From Remote 3640 to Tallaght Core 7200	80	100.0	0	0	60	60	60	60	0
IT Galway---->Jitter---->Jitter Test From Remote 3640 to Tallaght Core 7200	80	100.0	0	0	60	60	60	60	0
IT Limerick---->Jitter---->Jitter Test From Remote 3640 to Tallaght Core 7200	80	100.0	0	0	60	60	60	60	0
IT Tralee---->Jitter---->Latency packet loss to tallaght 7200	80	100.0	0	0	60	60	60	60	0
IT Tralee---->Jitter---->Jitter Test From Remote 3640 to Tallaght Core 7200	80	100.0	0	0	60	60	60	60	0
IT Letterkenny---->Jitter---->Jitter Test From Remote 3640 to Tallaght Core 7200	80	100.0	0	0	60	60	60	60	0

Remove | Delete | Ok

"The network can be a bit of a black box, where you don't really know what the response times are, either in and out of the network, or for intra-network traffic.

ResponseWatch allows us to measure and report on that effectively. So much of what thePlatform does is tied to SLAs, where our customers have certain expectations and ResponseWatch also allows us to be pro-active instead of reactive, where we can start trending."

**Rob Sherrard - Senior Network Architect, thePlatform.com**

# ResponseWatch - A sound business decision

## Primary Features

Feature	Function	Benefit
<b>Group based SLA configuration</b>	Powerful, easy-to-use, Service Level Agreement structure supports the ability to assign multiple SLA values to each IP SLA metric.	Facilitates internal or external SLA tracking, by allowing the network manager to assign network performance metrics to multiple SLA groups, each with their own SLA.
<b>Executive Summaries</b>	Executive summaries provide a high level view of the network on a single screen. Network performance is displayed as a percentage score over different categories, such as Overall Network Quality, Application Performance, VoIP Network Quality and SLA Conformance. Group filters will be available to run these reports over specific logical or physical areas of the network.	ResponseWatch insight is brought to a wider audience in an easily-digested format. Non-technical management gains a better understanding and appreciation of network management issues.
<b>SLA Alerting</b>	Alerts from ResponseWatch can be accepted by any alert management system that can receive Syslog messages. Each SLA Group configured on the system has an option to trigger a Syslog alert a) if an SLA is breached, b) if an SLA is breached continuously for X minutes or c) not at all. Each group can also be configured to send to a different alert management station so that alerts can be directed to the correct administrator.	Alerts are triggered if an SLA has been broken, making immediate action possible and providing an audit trail.
<b>Enhanced report usability</b>	Reports have enhanced usability and all reports are now available in the following formats: HTML, CSV - Comma Separated Variable, PDF.	ResponseWatch reports are easily accessed by popular office applications.
<b>Real-time 'Bullseye'</b>	The ResponseWatch 'Bullseye' has been made clearer and more informative.	At-a-glance response time SLA monitoring.
<b>Portal integration features.</b>	Close integration with Crannog OneView management portal. See OneView PDF.	All network monitoring applications managed and viewed from a single, configurable, interface.

"With ResponseWatch, I can actually see in near-real-time what is the impact on overall performance and throughput, in terms of packet loss, latency and jitter on the wire. Ideally I would deploy ResponseWatch with predefined thresholds and once those are exceeded I could then use NetFlow Tracker to identify the potential causes."

**Rob Sherrard - Senior Network Architect, thePlatform.com**

### Architecture

ResponseWatch's architecture presents the user with complete performance and availability graphs and reports via a web interface - either directly or via the Crannog OneView portal.

### Platform

Minimum server spec:

Intel P4 - 512 MB RAM

20 GB free hard disk space

Pentium 4 2.6 GHz or better

Windows 2000 or later

Recommended server spec:

Dell SC 1425 (1 u rack mount)

or similar

3.2 GHz Xeon processor - 2 GB RAM

2 x 80 GB SATA 7200rpm+ disks

(raid 1) provides mirroring.

Windows 2003 Server

The amount of hard disk required by ResponseWatch will also increase depending on the amount of tests being monitored, and the amount of data being stored for each test.

Linux version optional for some installs - please contact us to discuss your requirements.



**CRANNOGSOFTWARE**  
making networks assets, not overheads

34 Greenmount Office Park  
Harold's Cross, Dublin 6W, Ireland  
Tel: +353 1 454-9196  
Fax: +353 1 454-9312

[info@crannog-software.com](mailto:info@crannog-software.com)

[www.crannog-software.com](http://www.crannog-software.com)

Visit the Crannog Software website for your local office's contact details.