Network Instruments

white paper

RETROSPECTIVE NETWORK ANALYSIS

Unified Communications (UC) and other bandwidth-intensive applications can greatly increase network performance requirements. Network professionals need versatile monitoring and analysis tools to quickly troubleshoot business-critical operations and monitor security and compliance. In this environment, Retrospective Network Analysis (RNA) tools that let you go "back in time" to reconstruct sporadic failures or attacks can offer distinct advantages over analysis tools that only operate in real time.

NETWORK® INSTRUMENTS
JDSU Performance Management

WHAT IS RNA?

Retrospective network analysis (RNA) allows network administrators to quickly browse backward through massive amounts of network traffic. With RNA, admins can view breaches and anomalies exactly as they happened, within the context of other activity as it occurred on the network.

With RNA, it is possible to sidestep the often labor-intensive task of trying to recreate problems in order to troubleshoot them. To do this, all network traffic (or some targeted subset) must be efficiently captured and stored, in much the same way a convenience store might use a video security system.

The purpose of this paper is to explain how RNA functions and why it offers a significant time and cost savings over conventional real time analysis.

A fully loaded 10 Gb network can generate over a terabyte of data every seven minutes.

WHY IS RNA IMPORTANT?

While hardware reliability has improved, it has also made the network administrator's job more complex. Instead of finding and replacing obviously failed hardware, admins must now solve more and more intermittent (and subtle) problems usually found in the application layer. To do so, they must first determine that the network is not at fault.

Additional time, energy, and resources are often spent gathering information in an attempt to replicate intermittent problems or enforce security and compliance regulations. With RNA, the task of replicating network or application problems is no longer necessary.

THE CONCERNS

With these growing demands come new concerns. According to a recent Network Instruments® State of the Network Global Study[1]:

- Nearly 70 percent of respondents identified their top application troubleshooting challenge as determining whether an issue was caused by the network, system, or application
- In managing complex applications, the same number cited a lack of visibility into the user experience as their greatest challenge
- Bandwidth demand for organizations will grow by 28% in 12 months and 51% in two years

This lack of visibility and constant bandwidth pressure translates into unplanned downtime that impacts the bottom line. According to IT analyst firm TRAC Research, nearly half of IT staffs reported that, on average, they spend more than 60 minutes per incident repairing performance issues. Additionally, every hour of downtime costs companies $161,000 on average[2].

[1]Sixth Annual State of the Network Global Study, July 23, 2013

[2]Aberdeen Group Report, February 2012

HOW IT WORKS

RNA acts like a DVR for the network, changing the way engineers conduct analysis. Traditional real-time packet capture and analysis gives network professionals insight into their networks via packet-level protocol decode and analysis. While these tools are useful when managing any midsize to enterprise level network, using them to collect enough information to solve subtle or sporadic problems is an arduous task. What's more, the ability to witness a compliance violation or security breach is limited to those lucky enough to be watching when it happens. RNA acts like a 24/7 surveillance camera—allowing you to rewind and watch the incident happen – rather than recreate it.

The Observer® Performance Management Platform with its powerful Observer GigaStor™ appliance is capable of storing terabytes of packet-level and flow-based traffic collected from a variety of full-duplex network topologies, including gigabit, 10 Gb, 40 Gb, and wireless. The appliance performs real-time processing at the probe rather than transferring large packet captures over the network to the console for analysis. GigaStor utilizes a high-performance architecture to capture packets off the wire and write them to disk, storing up to 5 Pb.

When utilizing long-term packet capture appliances like GigaStor for troubleshooting, it is essential to consider the network connection, bandwidth, current use, future use, and the organization's time requirements. The following graph provides an approximate idea of the necessary GigaStor capacity that would be required based upon the above considerations.

CONNECTION (Gb)	PERCENT USAGE	GIGASTOR CAPACITY (TB)	RECORDING TIME
1	25	4	1 day, 8 hours
		8	2 days, 16 hours
		16	5 days, 8 hours
10	25	16	13 hours
		48	1 day, 14 hours
		96	3 days, 5 hours
10	50	16	6.5 hours
		48	19 hours
		96	1 day, 15 hours
40	25	48	9.5 hours
		96	19 hours
		144	1 day, 5 hours

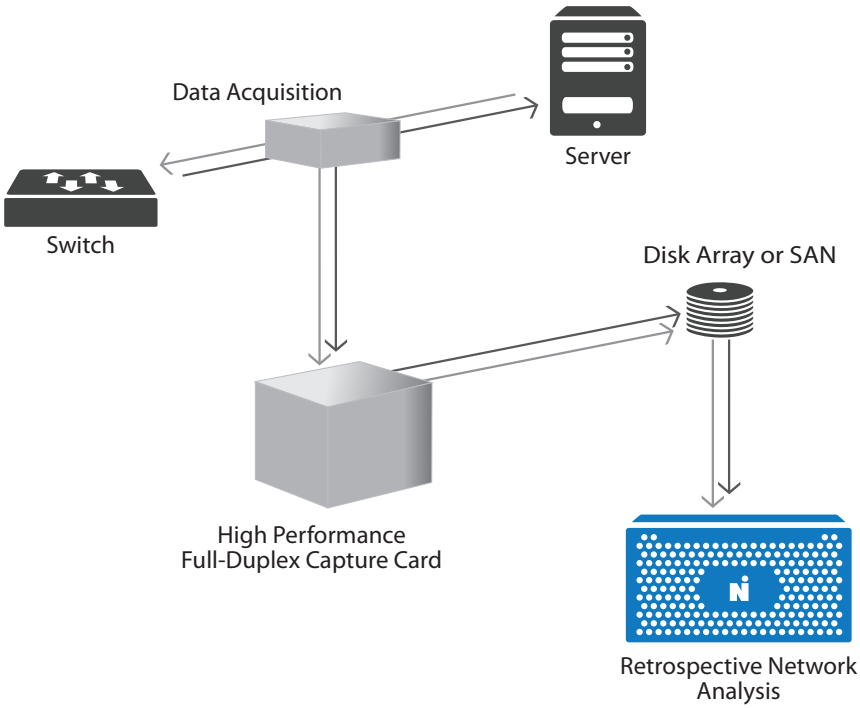
RNA offers numerous benefits including enhanced network availability and faster resolution security breaches.

But there is more to RNA than just capturing and storing traffic. To truly be useful, the tool should make it easy to find the relevant information as quickly as possible and significantly improve troubleshooting efficiency. RNA should provide IT staff with the drill-down detail necessary to isolate problems to particular protocols, applications, servers, and stations. Finally, for true forensic analysis, the ability to reconstruct files, web pages, images, emails, and IMs; and compare breaches to Snort rules, is indispensable.

RNA can also be used for planning, rollout, and performance management stages for new applications such as VoIP, by taking advantage of monitoring and trending data to determine exactly how applications affect the network. Preliminary testing can save an enterprise the cost and headaches associated with a problematic application rollout.

Finally, the comprehensive functionality of RNA lets IT staff spend less time attempting to recreate problems and spend more time on proactive planning. In short, reduced downtime, plus faster problem resolution equals a rapid return on investment.

Architecture of a typical Retrospective Network Analyzer



CASE STUDY: RNA IN THE REAL WORLD

A major Midwest healthcare provider implemented a series of multi-terabyte GigaStor appliances across their network, in conjunction with several Observer® Expert consoles, from which they managed VoIP, a wireless network with over one thousand access points, and other network applications.

After implementing RNA solutions they saw marked improvements and saved thousands of dollars in costs. The IT department routinely uses GigaStor to diagnose intermittent problems with its network, application performance, and infrastructure. On multiple occasions, they have been able to diagnose intermittent issues on critical servers, allowing IT staff to take action before problems impacted overall service performance.

They benefited from an RNA solution with:

- Higher network availability
- Improved ability to conduct business efficiently and effectively
- Satisfied customers and employees
- Ability to investigate and document compliance and security issues to streamline enforcement process

FINDING THE RIGHT RNA SOLUTION

RNA is a true paradigm shift in application and service monitoring, security, and analysis technology. When considering the purchase of an RNA solution, look for products that provide the following features. Keep in mind that some vendors charge extra for additional functionality.

Key RNA Features:

- In-depth application analysis and detail
- VoIP and videoconferencing analysis and call scoring
- Support for 10 Gb and 40 Gb networks
- Stream and application reconstruction
- Multi-user, multi-session access
- Real-time analysis on the probe
- Seamless integration
- Security forensics capability

ABOUT THE NETWORK INSTRUMENTS RNA SOLUTION

GigaStor is a high-speed packet capture and retrospective network analysis appliance. It is available in portable and field-scalable rack mount models that span from 2 TB to 5 PB of storage and support network speeds of up to 40 Gb. Included inside the GigaStor is the custom Observer Gen2™ capture card. Designed for superior functionality, the Gen2 capture card features the fastest independently verified performance in the industry.

GigaStor Upgradeable

Rack Size: 2U Storage: 2 TB - 16 TB

Rack Size: 5U Storage: 8 TB - 48 TB

- Data center/branch facilities/network edge
- Field upgradeable without removal from rack
- 2 to 48 TB capacity
- 1 and 10 Gb networks

GigaStor Portable

- Transportable design
- 2 to 4 TB capacity
- 1, 10, and 40 Gb networks

All appliances use the Network Instruments-designed Gen2™ capture card

GigaStor Expandable

Rack Size: 5U (+) Storage: 48 TB (+)

- Data center/large branch
- Field expandable
- 48 TB to 5 PB capacity
- 1,10, and 40 Gb networks

GigaStor 10 Gb Wire Speed

Rack Size: 5U (+) Storage: 144 TB

- Large data center/enterprise core
- World's fastest 10 Gb write-to-disk appliance
- 144 TB capacity
- 10 Gb line rate

As part of the Observer Platform, GigaStor data is seamlessly aggregated within Observer Apex™ with packet metrics captured in the Observer Analyzer Console. Observer Infrastructure (OI) offers deep insight into the health of underlying internally hosted and cloud devices by leveraging multiple polling technologies including SNMP, WMI, and IP SLA alongside synthetic transactions. Combining this information with packet data, the Observer Platform provides end-to-end application and service awareness with drill-down capabilities and expert analytics for immediate problem resolution.

North American Location
10701 Red Circle Drive · Minnetonka, MN 55343 · USA
Toll Free: 800.526.7919 | Voice: 952.358.3800
www.networkinstruments.com

WP-140929-V17-B1

NETWORK INSTRUMENTS®
JDSU Performance Management