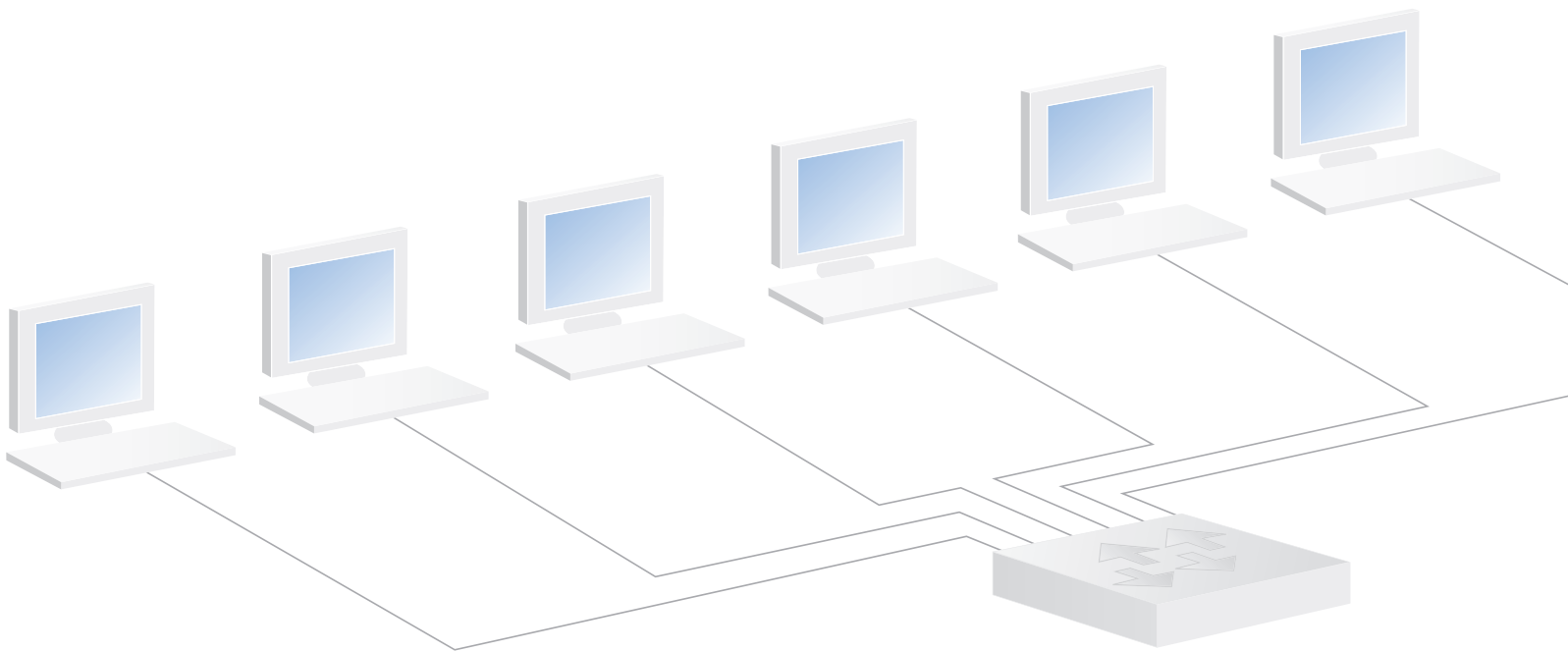


Retrospective Network Analysis

While network complexity and bandwidth demands continue to increase, applications such as VoIP increase performance requirements. Now more than ever, network administrators require 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 a failure or attack can offer distinct advantages over analysis tools that only operate in real time.



Background

Retrospective network analysis (RNA) allows IT professionals to quickly browse backwards through massive amounts of network traffic. RNA allows network engineers to view breaches and anomalies exactly as they happened, within the context of other activity as it occurred on the network, thus sidestepping the often labor intensive step of trying to re-create problems to troubleshoot them. This requires that all network traffic (or some targeted subset) is 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 retrospective analysis functions and why it offers a significant time and cost savings over conventional real-time analysis.

State of the Industry

Paradoxically, improved hardware reliability has made the network engineer's job more complex. Instead of finding and replacing obviously failed hardware, network engineers need to solve more and more intermittent (and subtle) problems. The continuing transformation of enterprise networks into complex webs comprising multiple technologies and topologies, with users from hourly employees to CEOs demanding flawless, department-specific functionality, makes the job of network managers increasingly difficult. Still, IT professionals continue to waste valuable time, energy, and resources gathering information in an attempt to **replicate intermittent problems** or enforce security and compliance regulations.

The Concerns

With these growing demands come new concerns. According to a recent Network Instruments® survey:

- Nearly 70 percent of IT administrators are concerned about the increased complexity of their networks
- Nearly the same number expressed concern about an increasing volume of network traffic
- Over half said their most common problem is a lack of information about network problems and their causes
- 30 percent cited the inability to replicate user problems as a recurring network issue

Case Study: The Way Things Were

A major Midwest healthcare provider, with many hospitals and over 200 clinics and pharmacies across 90 communities, required a powerful network monitoring and analysis solution to ensure its business-critical operations remained up and running. The provider relied on a mix of T1, DS3, Gigabit, and 10 Gigabit Ethernet links to provide access to some 30,000 users. When staff access to patient records can be a life-or-death matter, downtime is not an option, and time-consuming, reactive troubleshooting is unfeasible. This healthcare provider decided to explore retrospective network analysis solutions.

How It Works

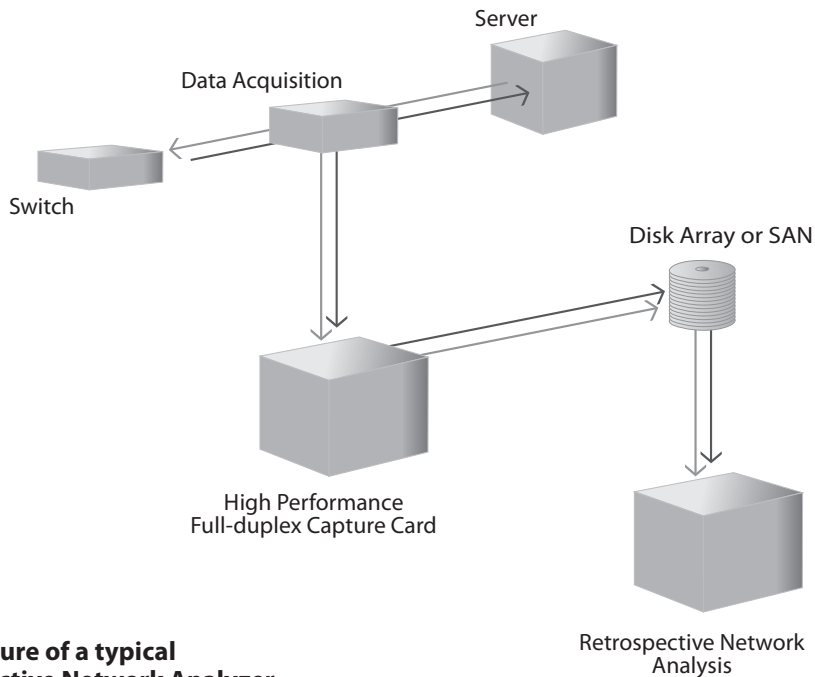
RNA acts like a **TiVo® for the network**, changing the way administrators conduct analysis.

Traditional real-time packet capture and analysis gives network administrators insight into their networks via packet-level protocol decode and analysis. While these tools are certainly useful when managing any mid- to enterprise-level network, using them to provide administrators with 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—it is far easier to find the culprit using a stored video of the crime rather than just a photograph.

Connection	Percent Usage	GigaStor™ Size	Capacity
1 Gig	10	4T 12T	88 hrs 7 days+
1 Gig	25	4T 12T	35 hrs 106 hrs
10 Gig	10	4T 12T	8 hrs 26 hrs
10 Gig	25	4T 12T	3 hrs 10 hrs

Appliances such as GigaStor are capable of storing terabytes of packet-level traffic collected from a variety of full-duplex network topologies, including WAN, LAN, Fibre Channel, wireless, gigabit, and 10 Gigabit (10 GbE). The appliance performs real-time Expert processing at the probe rather than transferring packet captures over the network to the console. The GigaStor has a 64-bit core and can capture up to 12 TB, or offload to a SAN for nearly unlimited storage.

But there is more to RNA than just capturing and storing the traffic. To truly be useful, the tool should make it easy to find the relevant connection or time period as quickly as possible, further improving troubleshooting efficiency. RNA for the enterprise should also provide IT staff with the drill-down detail necessary for isolating problems to particular protocols, applications, servers, and stations. They should be flexible enough to monitor any topology, including LAN, WAN, WLAN, gigabit, 10 GbE, and Fibre Channel. For true network forensic analysis, **the ability to reconstruct files, web pages, images, e-mails, and IMs**; and compare breaches to Snort rules, is indispensable.



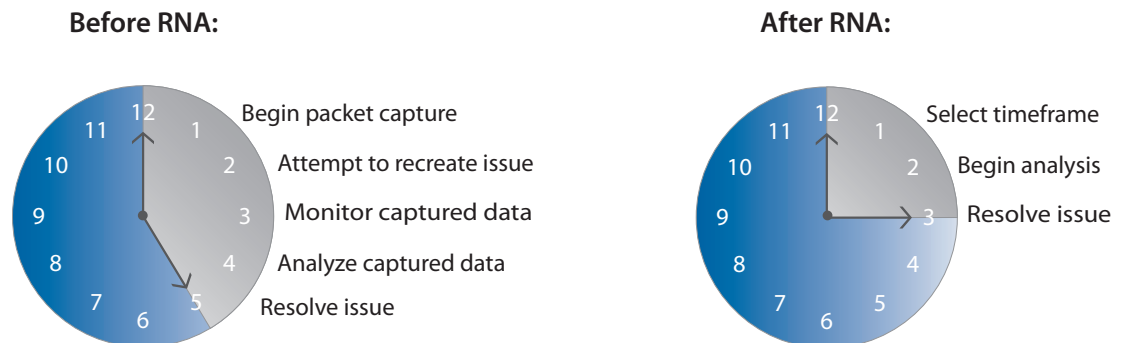
Architecture of a typical Retrospective Network Analyzer

Case Study: Implementation

The Midwest healthcare provider decided to implement a series of multi-terabyte GigaStor appliances across their network, in conjunction with several Observer® Expert consoles, from which they hoped to manage VoIP, a wireless network with over one thousand access points, and other network applications.

Benefits

Troubleshooting Process



The benefits of employing an RNA solution are numerous and tangible:

- Higher network availability
- Improved ability to conduct business efficiently and effectively
- Satisfied customers and employees
- Ability to validate and provide evidence for compliance and security issues streamlines enforcement process

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 (or will 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.

Case Study: After Implementation

The Midwest healthcare provider has seen marked improvements and saved thousands of dollars in costs since implementing RNA solutions on its network. It routinely uses GigaStor to diagnose intermittent problems with its network, application performance, and infrastructure. On multiple occasions, it has been able to diagnose intermittent issues on critical servers, allowing IT staff to take action before problems impacted overall network performance.

Summary

Whereas traditional protocol analyzers have evolved over time, adding features and capabilities in a natural progression, RNA has proved a different type of innovation: it is a true paradigm shift in network monitoring, security, and analysis technology. Many organizations currently use RNA technology to provide better service and improved security to their customers and employees in a way that saves both time and money.

When considering the purchase of an RNA solution, **look for products that provide the following features.** Some vendors charge extra for additional functionality that is included in devices such as the GigaStor.

- Security forensics capability
- Real-time analysis on the probe
- VoIP analysis and call scoring
- Stream or application reconstruction
- Multi-user, multi-session access
- Connection Dynamics
- Nanosecond resolution
- Seamless integration
- Option to offload to SAN

Operative Software Products

7219 Kentwood Avenue • Los Angeles, CA 90045
 telephone US only (866) 204-6289 or (310) 410-9350

www.operativesoft.com/html/observer_gigstor.htm

