NETWORK GENERAL

WHITE PAPER

Your Network Truth. Revealed.

February 2007

INTRODUCTION

That was then, this is now

Yesterday's IT organizations were focused on managing discrete systems. They utilized various niche tools that only trained specialists understood. Today's IT, and the IT organization of tomorrow, demand a performance management solution with intelligence that supports a holistic view of the network, servers and applications. A key focal point in the solution is a feature that easily communicates to business managers, in business terms, the status of critical IT services.

Unlike the networks of yesterday, today's networks are more complex and more frequently subject to change. Using multiple tools to managing individual devices becomes more challenging than ever. Managing virtualized environments and supporting multi-tiered applications are just a few examples of the increasingly complex IT infrastructure.

The IT performance management playing field has changed. Say goodbye to those siloed, niched tool approaches. Today, it's all about accountability and survival. If IT organizations have not evaluated new technologies that tout a more unified, integrated approach to IT performance management, most notably IT service assurance, they are part of a dying breed.

Aligning IT with Business

After the technology wreck at the turn of this century, the demand for IT to show more accountability reached resounding levels. Today, business confidence has improved along with the willingness to make technology investments. However, the drive toward accountability hasn't and isn't going away. IT organizations are evolving into a more integrated set of competencies. By adopting a better way to support business value, IT organizations are quantifying their contributions to business goals.

Today, all businesses demand quality, cost and relevance to guide and assess their effectiveness. However, for a modern IT organization this is a new set of principles, especially for the network and applications departments. No longer protected by a brick wall of outdated acronyms and stuffy attitudes that insulated from the outside world, they are subject to the same business demands for accountability.

It is clear that new management approaches and solutions for network and application analysis are required. A new approach that enables IT professionals to manage to business goals and proactively address the inevitable performance problems. It may not always be possible to catch problems as they happen, or setup the precise network monitoring filters to catch the problem upon recurrence. As a result, many providers of network analysis tools are evolving ther products to provide historical analytic capabilities. The time-consuming nature of the usual manual approaches to solving elusive problems is unacceptable in today's resource constrained IT environment.

RETROSPECTIVE ANALYSIS: THE NEXT GENERATION SOLUTION POWERED BY SNIFFER

The power to look back with total clarity

Retrospective Analysis is an offering delivered through Network General's Sniffer InfiniStream™ network performance analysis product line. It is the next generation network and application analysis product that combines three critical performance analysis and problem resolution functions, into a single holistic solution:

- Real-time, point-in-time analysis: This traditional approach to network management and troubleshooting captures data within a short window – typically 15 seconds or less – and allows network engineers to perform packet-level analysis using protocol decodes, diagnostic tools, and short- and long-term reporting. Point-in-time analysis allows IT professionals to identify and resolve the root causes of network problems as they happen.

- Back-in-time analysis: The back-in-time analysis provided by InfiniStream allows packet level, bit-by-bit specificity to be applied to small or vast amounts of data captured over hours, weeks or months. This breakthrough extension to real-time analysis is a radical improvement, freeing IT professionals from the constraints of limited quantities of captured data. To allow users to understand the impact and implications of network events, the InfiniStream solution can quickly process in-depth, back-in-time data into post-event summary reports on demand.

- Historical analysis: To further complement InfiniStream's own post-event reporting, Network General also offers summary-level analysis in conjunction with its Visualizer reporting product. By importing InfiniStream data into Visualizer, users can receive long-term trend analysis of application and network behavior over an extended period of time. This, in turn, can provide invaluable intelligence to network managers in the areas of capacity planning and trend analysis.

Sniffer InfiniStream also provides a comprehensive set of LAN to WAN instrumentation to gain total visibility into any given point in the network. WAN topologies and protocols supported include DS-3, HSSI, and ATM.

Together, these retrospective analysis capabilities represent the foundation for the next generation of network and application performance analysis solutions being deployed across the distributed enterprise.

The Sniffer InfiniStream contains all of the capabilities required to deliver retrospective analysis. First and foremost, its streaming data capture allows uninterrupted data capture over hours or weeks, eliminating the attempted re-creation of problem scenarios after they occur. To successfully address complex application and network performance

problems in today's networks, streaming data capture is available across multiple links simultaneously, with aggregation capability. Sniffer InfiniStream also offers large storage capacity, up to 15 terabytes. When users are permitted to store large quantities of data, they are empowered to look back further in time and investigate network activity that may take place over a period of time, versus a single incident.

Statistical "drill-down" is an essential part of investigation activity prior to analyzing granular network traffic decodes. Deep statistical analysis capabilities are a strong suit of the Sniffer InfiniStream, whether viewed from the console while watching real-time updates or when researching a post-event network problem. To navigate through the large quantities of captured data, InfiniStream effectively narrows down the timeframe of selectable data, along with limiting the critical business objects viewed, helping to ensure that only pertinent data transactions are examined. Innovative data mining features let users analyze capture files that are opened as streams, so they can examine granularity down to one-second intervals.

Protocol decodes and expert packs available in Sniffer InfiniStream further support advanced analytic capabilities that provide in-depth knowledge of flows and comprehensive detection of network communications abnormalities. It is capable of examining all seven layers of the OSI model in order to identify bottlenecks and protocol violations — even problems such as slow server response times and mis-configured routers.

By combining comprehensive data capture, large storage capacity and statistical drill-down capabilities with best-in-class protocol decodes and expert analysis, Sniffer InfiniStream can analyze and pinpoint even the most challenging network problems. It provides constant updates for real time monitoring information, and can point out key metrics for protocols that are in use, including multicast protocols such as PIM and IGMP. InfiniStream also analyzes the widest breadth of active network and application protocols in the industry, such as VoIP, Citrix ICA, Microsoft Exchange, Oracle database traffic and more than 400 other industry-standard decodes.

Pinpointing Network Inefficiencies

One of the largest health care providers in the Midwest relies on the Retrospective Analysis capabilities of Sniffer InfiniStream to keep its complex network up and running smoothly. It is used primarily to troubleshoot high-traffic servers that are relied on by large numbers of users, as well as mission-critical applications such as PACS (picture archiving and communications system) and VISICU, an electronic monitoring system used in intensive care.

The hospital's network team performed Retrospective Analysis with the InfiniStream solution to identify the source of an intermittent outage that was occurring with VISICU, causing offsite clinicians and physicians to lose momentary contact with the system.

"In the past, we had to catch a problem as it was happening, which any network manager knows can be next to impossible. Sniffer InfiniStream's high-capacity data capture capabilities allow us to capture extreme quantities of data over time, and slice it and dice it in numerous ways in order to catch the problem."

Properly implemented with powerful tools that can aggregate data from multiple network links, this comprehensive, distributed approach to network performance monitoring helps to accelerate resolution of brownouts or other application or network performance problems, regardless of when they occur.

Enhancing Application Performance Visibility

As a technology leader in the highly competitive retail banking business, a Midwestern Bank has a strong track record of using innovative technologies to simplify processes for its customers. Its Web-based solutions put the Bank at the forefront of the e-mortgage business, and the company continually invests in new technologies to maintain its position.

The IT department received numerous complaints that a flagship in-branch application, used to check account balances, was running very slowly. Prior to deploying Sniffer InfinStream, the IT department's troubleshooting process would be to first check the user's PC, testing everything from drivers to application configuration.

After deploying Sniffer InfiniStream along with Sniffer Portable and MultiSegment Intelligence, the IT department discovered a whole new world of troubleshooting.

"With Sniffer InfiniStream, we decided to approach the problem more efficiently, deploying the devices to capture data. We were able to capture the packets, and correlate the client/server and network conversations with the application performance issues."

The extremely slow performance was noticed in the balance checking application. The IT department used the Sniffer InfiniStream to capture conversations between PCs and the Novell server on which the balance application ran, to see the difference between the fast and slow transactions. The IT department also used the expert tool to verify that transactions were identical. However, one took seven times longer to execute. The issue ended up being that the Novell server was the culprit – it could be extremely slow or fast with any given conversation.

With the Analysis report in hand, the networking team communicated their findings to the application server team. From the results of the Sniffer Analysis, the Novell applications server team discovered that the hyper-threading function for use with multiprocessors had been turned on. "This was not recommended by Novell and, sure enough, it came back to haunt us." After the hyper-threading was turned off, the problem disappeared.

Sniffer InfiniStream Network Management is the industry's premier Retrospective Analysis solution, enabling users to capture large amounts of data in their drive to isolate, pinpoint, analyze and solve the performance issues that plague today's high-speed Gigabit and Fast Ethernet networks. The Sniffer InfiniStream overcomes typical limitations of time-based capture devices by offering the largest available data store (up to fifteen terabytes), continuous capture on 10/100 and Gigabit Ethernet topologies, and a precise method for extracting important event-related details that leads to quick isolation and resolution of any network problem.

NETWORK INTELLIGENCE SUITE POWERED BY SNIFFER

Sniffer InfiniStream integrates with the Network Intelligence Suite providing the tools and features required to access, manage and share network and application data.

The Network Intelligence Suite integrates application monitoring with traditional packet-level network and application traffic analysis, yielding an unparalleled view of IT services. Multiple technology layers are managed across IT domains by powerful web-based Business Container™ consoles, delivering management and performance information through a real-time view of the overall business instead of siloed technology performance metrics. The need for support staff to have a deep understanding of the cross-domain infrastructure supporting business services is reduced; IT service and business performance issues are quickly identified, isolated and corrected. By transforming IT data into detailed knowledge about the status of IT and business services, the Network Intelligence Suite provides self-service capability for business users and strengthens the relationships between IT and the business.

SUMMARY

Sniffer InfiniStream contains all of the capabilities required to deliver Retrospective Analysis. First and foremost, its streaming data capture allows uninterrupted data capture over hours or weeks, eliminating the attempted re-creation of problem scenarios after they occur. To successfully address complex application and network performance problems in today's networks, streaming data capture is available across multiple links simultaneously, with aggregation capability.

Sniffer InfiniStream also offers large storage capacity, up to fifteen terabytes. When users are permitted to store large quantities of data, they are empowered to look back further in time and investigate network activity that may take place over a period of time, versus of a single incident. The large storage capacity of Sniffer InfiniStream allows all the data of a complete packet-level traffic history to be saved – a necessity for effective problem resolution and to reduce the need for complex filtering.

Deep statistical analysis capabilities are InfiniStream's third strong suit. Whether sitting in front of the console and watching real-time updates or researching a post-event network problem, statistical "drill-down" is an essential part of investigation activity prior to analyzing granular network traffic decodes. To navigate through the large quantities of captured data, InfiniStream Network Management effectively narrows down the timeframe of selectable data, along with limiting the critical business objects viewed, helping to ensure that only pertinent data transactions are examined. Further data mining features let users analyze capture files that are opened as streams, so they can examine granularity down to one-second intervals.

Finally, the InfiniStream solution's advanced capabilities enable users to easily filter on multiple combinations of data properties, and see a preview of the data selected to quickly determine trends within the dataset. This ensures the user has isolated the packets of interest before drilling down to detailed protocol decode analysis. This function is at the heart of application and network troubleshooting; the InfiniStream solution provides a rich set of decodes to allow users to decipher the latest application and routing protocols.

For more information on the Sniffer InfiniStream product visit: www.networkgeneral.com/infinistream.

ABOUT NETWORK GENERAL CORPORATION

Network General™ is a leading provider of IT management solutions designed to integrate and simplify IT management and troubleshooting across IT domains, assuring the delivery of IT services. The Network General portfolio consists of innovative software solutions and intelligent appliances that monitor and manage all elements of the IT infrastructure including network devices, applications, and servers, while simultaneously delivering a correlated view of the health of the business service. Network General's solutions provide IT professionals with an end-to-end correlated view of the performance and availability of critical business services and the underlying network infrastructure.

NETWORK GENERAL
The Source of Network Truth

REV: 02.07