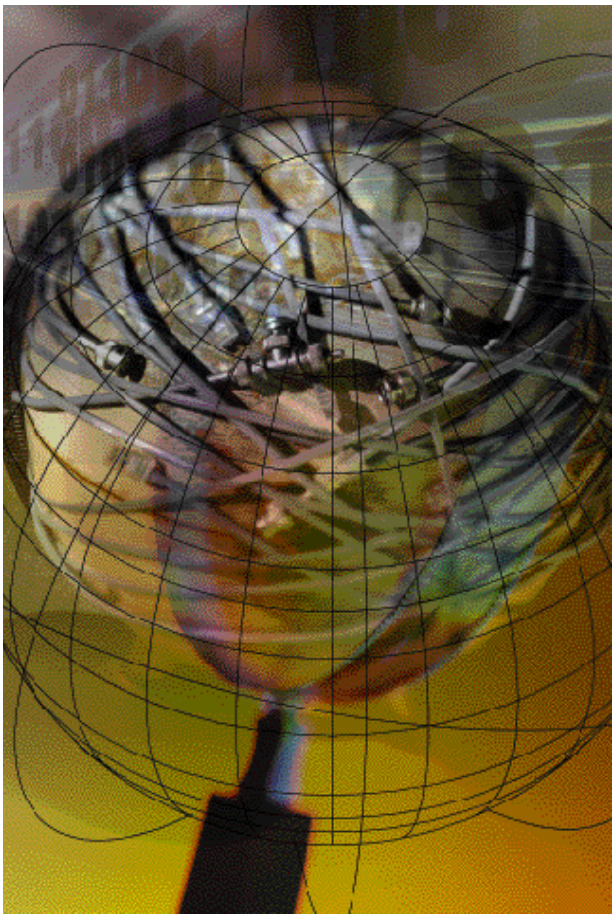


Creating High-Performance Networks and Cutting Downtime With Proactive Management Tools

A Network Visibility Guide

network ASSOCIATES

Who's watching your network

Table of Contents

Overview

Managing a network has never been so challenging. Its primary role in business and customer operations makes network management a high visibility occupation. Today, you might be a hero, yet one major network glitch could trample you tomorrow.

The stakes are high because data networks are the lifeblood of business. When they work well, networks advance a complex web of applications that provide just-in-time products and services. Smooth, efficient network operations keep business humming. Bottlenecks or breaks in the network can bring business down. The results go straight to – or off of – the bottom line.

Network Associates has prepared this Visibility Guide to help network and business managers understand the financial risks of network downtime and poor performance. This Guide explains how network performance tools are used, and how Network Associates products complement and enhance traditional offerings to create a complete solution. This Guide concludes with suggestions for creating a proactive strategy to ensure quality network performance.

The Business Cost of Network Downtime

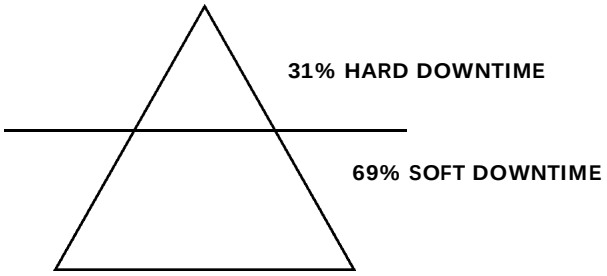
Network performance problems cause two types of productivity losses. The first is "hard downtime," when equipment failures or physical faults leave users stranded. The other is "soft downtime," which is application degradation caused by a slow or malfunctioning network.

Everyone knows when hard downtime occurs. Hard downtime brings transactions to a halt, interrupts customer service, and causes direct revenue loss. A recent Infonetics Research, Inc.,study found that hard downtime translates to an annual loss of $2.5 million on average in mid-sized organizations[1].

Hard downtime is a tangible problem. A network manager's performance is usually measured against network availability, so networking budgets are geared towards minimizing the impact of hard downtime and resolving it as quickly as possible when it happens. However, it is only the tip of the iceberg.

Soft downtime, or service degradation, is less catastrophic in nature but more insidious than hard downtime. Service degradation costs most organizations about twice as much in productivity loss as hard downtime, according to Infonetics. Soft downtime is more pervasive, more constant,more difficult to measure; and causes the most damage.

Productivity Hits from LAN Downtime



Most of the costs are hidden for service degradations or soft downtime but the most damage is done at this level. In fact, service degradations annually costs the average company twice as much in productivity loss as hard downtime. (Based on 100% productivity loss for affected users during hard downtime, and 50% during a service degradation).
Source: Infonetics

Soft downtime comes from poor application performance – many times caused by network congestion. Although it may be chronic,soft downtime doesn't register with senior management as acutely as hard downtime does because service degradation tends to move through different areas of the network over time, and its causes can be elusive.

[1] Infonetics Research, Inc., "Business-Centric Network Management and Downtime Costs," 1997. Infonetics surveyed 100 organizations with networks of at least 1,500 nodes, averaging 14,000 employees and revenue of $3 billion.

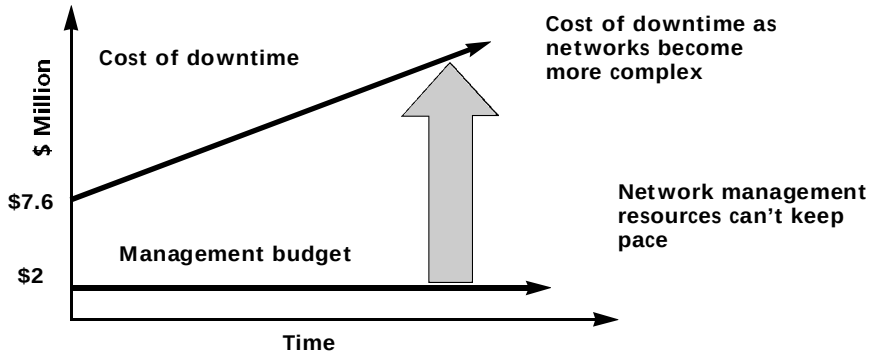
Following are network downtime statistics gathered by Infonetics.

$7.6 Million Annual Average Downtime Cost

Hard Downtime Metrics	
Average outages per month	1.8
Average duration per outage	1.3 hours
Total hard downtime per year	28 hours
Percent of employees affected	33%
Revenue loss per year	$2.5 million
Productivity cost per year (100% productivity loss during outage)	$1.6 million
Soft Downtime Metrics	
Average service degradations per month	3.9
Average duration of service degradation	2.3 hours
Total service degradation per year	107.6 hours
Percent of employees affected	41%
Productivity cost per year (50% productivity loss during soft downtime)	$3.5 million

Source: Infonetics

The risk of more losses grows with bigger, more complex networks hosting critical business applications. Ironically, despite the importance of ensuring network performance and managing an ever-changing array of new communications technology, most corporate information systems groups are scraping by with little or no growth in technical resources and staff.



The Infonetics study reported an average LAN management budget of $2 million – one quarter of what the same organizations lose each year from network performance glitches. The planning required to proactively avoid downtime gets the least attention because network managers spend most of their time fixing urgent problems affecting availability of the network. Because their focus is on keeping the network running, they lack the time and resources to anticipate problems and take proactive measures to avoid them. As a result, most network managers cannot guarantee performance levels for their networks.

Conventional Network Performance Tools: Spotty Payoff

Network planning is often a gut-level exercise conducted with pencil and paper. Proactive tools for network performance planning, design, and optimization are available, but most are difficult to use–they're too complex, expensive, and require too much training. Very often the effort required to install and maintain such tools outweighs the benefits they provide.

Network managers may justifiably use the latter excuse since most are buried by reactive, fire fighting tasks that consume their days. It is an obvious Catch-22: preoccupation with avoiding and fixing hard downtime ensures the likelihood of service degradations. And it's the latter that causes more damage in productivity costs and snow-balling effects rather than hard downtime, according to Infonetics.

Yet proactive management efforts to control soft downtime will actually stop most problems from ever developing into network failures. "Spend a little and save a lot" is the operative mantra.

Network managers should use available network analysis and proactive management tools. Unfortunately, many are inadequate for the task of true proactive management. These products usually focus on status reporting, problem identification and resolution, or reactive fire fighting. They lack substantive performance reporting and trending information, which is critical to proactive management.

Pitfalls of Traditional Management Platforms and Tools

Isolating and solving poor network response time is one of a network manager's biggest frustrations. Poor network response time can be caused by a variety of problems, including inadequate bandwidth, undetected network errors,server bottlenecks, misconfigured routers, PC configuration errors,and inefficient or misbehaving applications software.

Problems often stem from the complex end-to-end interaction of all of these factors. This scenario is becoming more common as organizations move to client-server architectures. Problem resolution requires a significant amount of time and technical know how. Fixes often need a combination of tedious hand-decoding of long transaction trace files, expert knowledge, and time on the phone with several vendors.

LAN Management Platform Roles

	Device Management	Network Availability	Expert Analysis
Products:	• CiscoWorks • Bay Optivity	• HP OpenView •Cabletron Spectrum •Other applications using the RMON MIB	•Sniffer TNV

Traditional SNMP-based network and device management platforms, such as HP OpenView, SunNet Manager, Cabletron Spectrum, CiscoWorks, Bay Optivity, and other solutions that rely on RMON MIB and SNMP data are used to monitor the minute-by-minute availability of network components or provide generic network statistics. In general, the applications running on these platforms tend to focus on identifying network hardware problems or providing statistical information, but not interpreting it or recommending solutions. They are not geared to proactive management or consultative problem resolution techniques.

Network Availability and Device Management platforms are good tools for troubleshooting the hardware faults that cause hard downtime or acting as traffic level counters. However, they do not provide detailed analysis of traffic at all layers of the network, which is how more complicated problems are identified. Proactive management requires being able to analyze, at all network layers, the impact of a particular application, connection, or server system. Management platforms are not designed for such analysis. The consequence is "management by swivel chair," as network operators move from monitor to monitor checking server, hub, router, and firewall; or pour through reams of statistical data to determine why the fault occurred or what they should do to resolve it.

Network Associates Software Automates Problem Resolution

Network managers welcome the idea of automating network performance tasks. But automation is a difficult, complex process. Many automated management tools are not immediately useful, frustrating managers with the amount of minutia and detailed product knowledge they require.

This complexity of automation stems from the roles that network management tools traditionally play: device management and network availability reporting. Device Management applications are typified by products such as CiscoWorks, which allows managers to monitor the status of

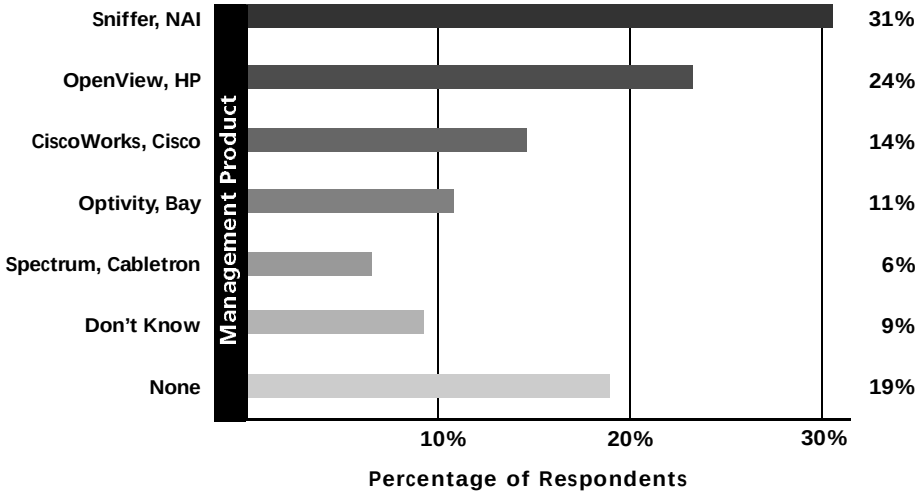
individual network components to ascertain their accessibility. While providing a thorough view of network hardware health, such tools do not help to track down higher-level problems that arise in network traffic flow. The Network Availability tools moniter traffic flows, but configuring the data collection is usually a manual process and the amount of data generated can be overwhelming.

Both tools are required in a network, but simply automating their tasks leaves network managers wading through reams of statistical data. What is needed is automated "expert analysis" that can filter out the most relevant data when troubleshooting specific problems or monitoring the network for particular symptoms of health. Automation alone does not bestow this expert analysis, as many managers have found.

Here is what network managers really need from easy to use, expert-based automated tools:

1. Isolate network problems occurring anywhere in the seven-layers of the OSI networking model. Intelligent troubleshooting technology allows high-speed protocol analyzers to perform the extended analysis required to find and solve upper-layer problems and troubleshoot lower-layer problems. As the industry's most widely-used tool for network fault and performance management, Network Associates' Sniffer® Total Network Visibility® Suite (Sniffer TNV) provides the automated intelligence you need to prevent,pinpoint, and resolve problems – swiftly and efficiently.

LAN MANAGEMENT PRODUCTS THAT SHORTEN DOWNTIME



Source: 1997 Infonetics Research., Business-Centric Network Management and Downtime Costs, 1997

2. Monitor real-time network conditions and application behavior throughout the OSI layers. A centralized console that monitors distributed data gathering devices and provides expert-based analysis can help to proactively manage entire networks with fewer people, solve problems faster and support better planning for the future. Network Associates' Sniffer Service Desk Suite provides high-level reports of problems and recommended solutions before performance problems develop.
3. Speed up problem resolution through automated trouble-ticketing and response management. Network Associates' McAfee* Total Service Desk (TSD) integrates traditional help desk functions with network management tools. It can register potential problems before they develop, automatically notifying management staff to avert downtime before users notice.

Using these tools can save organizations a substantial sum of time and money and improve the service delivered to end users. They allow network managers to cut downtime and ensure more efficient network and application performance. Proactive management is the key to literally millions of dollars in downtime prevention.

The Value of Expert Analysis in the Sniffer Total Network Visibility Suite

It is unlikely that downtime will ever disappear, so the challenge is to minimize and handle it more efficiently through automated expert-analysis of network problems. Network Associates' expert-based Sniffer Total Network Visibility Suite automatically diagnoses and resolves problems spanning all layers of the network.

High-speed networking technologies such as ATM, FDDI, and Fast or Gigabit Ethernet present a whole new set of challenges. Finding and solving the upper-layer problems caused by distributed applications requires that an analyzer "observe" network conversations for several minutes. But faster network speeds make it more difficult for protocol analyzers to handle data capture for the extended periods of time required to "see" a complete conversation between network elements. Analyzers can easily miss critical information if they do not have sufficient time and memory to capture data at the full-line rate.

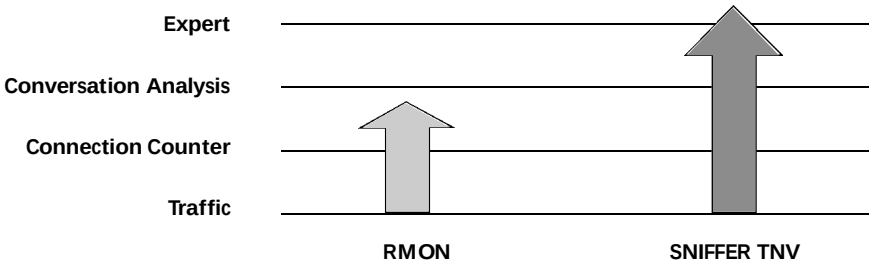
RMON, or remote monitoring, is useful in addressing some of these challenges, but not all. Applications that utilize an RMON MIB to collect information provide very detailed traffic level information and connection counters. However, in order to accurately obtain application performance or client server connection details, you need expert analysis.

GOVERNMENT CONTRACTOR ISOLATES COMPLEX PROBLEM IN MINUTES WITH SNIFFER TNV

A large government contractor was losing critical project-management data on wide-area router links that connected three locations with a total of 50 Ethernet segments on FDDI backbones.

Four troubleshooters spent two weeks trying to diagnose the cause, with no results. At night, they extensively tested network interface cards, routers, and the WAN connection. Finally, it seemed that a router was dropping packets, but the cause could not be determined. After installing Sniffer Pro WAN, the troubleshooters used its expert analysis to zero in on the problem – it was the application software itself. The application's preset acknowledgment times were insufficient for use over a WAN connection. The solution was to dedicate a 10 Mbps link for the critical application.

Sniffer Pro WAN was able to locate, in a matter of minutes, a problem that had stymied four people for a total of 120 hours. Four people at $50/hour is $24,000, which greatly exceeds the investment in the Sniffer TNV tool set. Moreover, from a personnel utilization standpoint, those four people could have been working on other projects, such as proactively optimizing network performance to avoid problems in the future.



Network managers need an intelligent way to determine which data is important, coupled with an analysis methodology that finds problems at all layers of the OSI model. Sniffer TNV is exactly such a tool.

Sniffer TNV Provides Total Network Visibility of Fast Networking Technology

Sniffer TNV employs more than 350 protocol decodes to analyze network traffic and spot problems causing downtime or service degradation on multi-topology, multi-protocol networks automatically and in real-time.

Sniffer TNV products are easy to use. Hitting one key opens the expert-overview screen, which breaks down the network according to the 7-layer Open Systems Interconnection (OSI) model,showing applications, connections, sub-networks and physical devices. The expert engine, in Sniffer TNV, then looks for anomalies, scanning for over 200 different types of problems.

On screen, Sniffer TNV highlights any such problems that it finds. Users select one that troubles them, hit a key, and Sniffer TNV explains the problem in detail, suggesting causes and recommends solutions.

To deal with the high traffic volume and complexity of fast networking technologies, Sniffer TNV uses specialized filtering mechanisms for ATM and frame-based networks.

SmartCapture™ is a filter that sorts through the complexities of ATM traffic for troubleshooting purposes. Most ATM problems are connection oriented problems, involving a series of requests and replies that flow across many layers of ATM signaling protocols. With the patented SmartCapture technique, Sniffer TNV is able to follow the entire setup procedure to sift out key, often hard to find information that really matters in resolving ATM network connection problems.

Focused Expert is a frame-based filter for Ethernet and FDDI backbones. It divides and conquers network traffic in order to scan it more efficiently. By intelligently analyzing the most relevant network conversations, Sniffer TNV provides efficient and automatic seven-layer expert analysis at high speeds.

NATURAL FUEL PRODUCER SAVES $300K AND BOOSTS DATABASE PERFORMANCE WITH SNIFFER TNV

One of the nation's largest natural fuel producers found itself stymied while trying to upgrade an inefficient but critical business application. To eliminate the need for nightly synchronization of three databases across wide-area leased lines, the company chose to re-host its application to a single Oracle database that could be accessed in real-time by its three main LAN sites.

But during the test phase, performance was abysmal. Transactions that used to take 30 seconds on the LANs took up to four minutes over the WAN. Already five months into development, management was concerned that it would have to scrap the project. One alternative would cost $300,000 in additional equipment, and the only other choice was to maintain the status quo.

The source of the problem was puzzling. WAN performance was obviously poor, but performance on the LAN was also bad. The new Oracle database should have vastly outperformed the old PC-based servers. Was it the network or the database? The answer was finally found by using Sniffer TNV to see what was happening between the application and network layers.

The problem was found in two hours: when they re-hosted the application, programmers had retained batch-processing to avoid changing client applications. This method sent each individual data row as a separate network packet, destroying network performance. A transfer of 10,000 rows sent 10,000 packets, plus an acknowledgement for every packet sent.

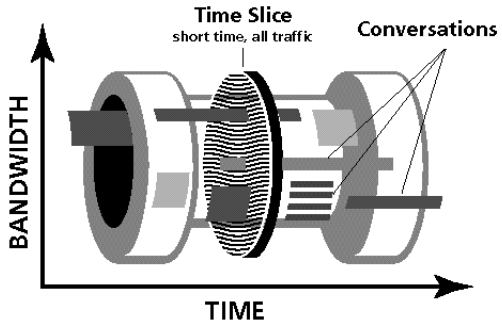
The fix turned out to be easy: simply tuning the application to IP's maximum transmission unit of 1,500 bytes per frame. Performance over the WAN improved three times over what users saw with the original application, nightly synchronization has been eliminated, and the company avoided a potential $300,000 gaffe.

Conventional Analyzers Face Challenges with Fast Network Analysis

The traditional method for troubleshooting networks is to capture data at the full-line rate while simultaneously applying expert analysis to the data streams at all layers of the OSI model. This can be a very useful technique, especially if there is a specific occurrence you are investigating or you are analyzing lower speed links.

However, if the objective is to "see" all the data over an extended period of time, few PCs have enough memory or disk space to accommodate all the data that is collected,particularly at high speeds. As a way around this limitation, data is captured to a buffer at the full-line rate for a short duration, with subsequent analysis of the buffered data at a slower pace. The following diagram illustrates this approach.

Traditional Network Analysis



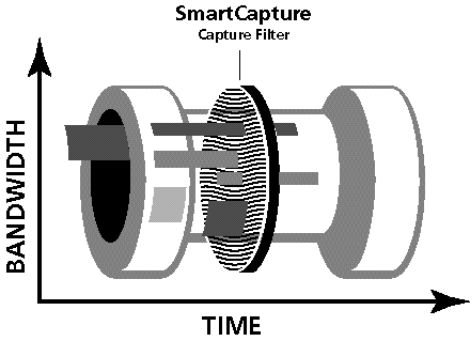
Here we see a very short-duration sample of all of the data. The sample is represented in the diagram by the thin cross-section, which represents a time slice of the data – typically two or three seconds. There are two problems with this approach. The first is that unless you have a specific occurrence in mind there is no easy way to decide which data to capture, so you end up with a random sample. This is adequate if you are simply gathering statistics. But for troubleshooting specific performance problems,especially at the higher layers of the OSI model, this approach is random and inefficient.

The second issue is that short samples usually make it impossible to identify application problems at the upper-layer of the OSI model, which is where the most difficult network problems occur. These problems transpire over a longer time period than the sample can capture. The sampling duration is so short that you never get a chance to see complete conversations between network elements.

Sniffer TNV's Capture and Analysis Filters are Tailored for Fast Network Analysis

Sniffer TNV instead uses two different intelligent troubleshooting technologies for high speed ATM and Ethernet/FDDI networks.

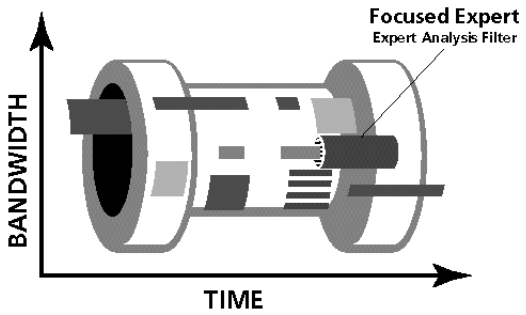
ATM - SmartCapture



SmartCapture performs a function very much like trying to find a needle-in-a-haystack. Taking advantage of the ATM hardware's filtering capability it isolates the critical signaling and control protocol information (the needles) from the other traffic that does not affect ATM network operation (the hay) on the network. The filter determines exactly which data to examine more closely and screens out all other network traffic. Since this data represents only a tiny fraction (much less than 0.1%) of any link's traffic, without SmartCapture, problems at this level would be impossible to identify.

SmartCapture is the cornerstone of Sniffer TNV's ability to provide efficient network troubleshooting of ATM problems.

Focused Expert: Ethernet and FDDI



The Focused Expert filter takes a different approach to Ethernet and FDDI network analysis. Consider the analogy of tuning into a radio station. There are many radio stations which you scan, finally selecting your favorite. You listen to the entire song playing on that station. You then scan the radio stations again selecting your second favorite and listen to the entire song playing on that station.

Similarly, Focused Expert sets network ID filters so that it can study entire network conversations. It selects specific conversations to analyze, one at a time, prioritizing them and applying expert analysis to each in turn. Thus, it can examine conversations for several minutes to find problems at any layer of the OSI model - including the all-important application layer.

During each filtered capture, Focused Expert looks for symptoms and diagnoses problems in real-time. If it sees any problems, it stores the associated trace files for analysis by the user. Pressing a single key starts a capture process. Sniffer TNV even changes filters on its own as it narrows in on the problem. The result of this analysis is that a relatively small amount of data is stored, and all of it is relevant to troubleshooting the problem at hand.

Proactive Network Management with Net Tools Manager

The key to proactive management is monitoring and analysis of network conditions overtime. Most management tools can monitor network statistics and report them when they reach certain thresholds, but staffers must then wade through this data to figure out what it means.

The Proactive Device Analysis tools in Sniffer Service Desk Suite (SSD) leverage Sniffer expert-based analytical capabilities to provide real-time, distributed monitoring of network health across the entire infrastructure. The result is an automatically updated, prioritized list of potential network problems. Network managers will see problems before they develop. The

software presents a detailed analysis of problem causes, allowing network managers to prevent service degradation or potential network failures.

Advanced Capabilities Brings Proactive Device Management

No matter how well managed, new problems inevitably crop up when one installs new network applications or hardware. The roll-out can affect the performance and reliability of other applications in ways that are difficult to predict,understand, isolate, and solve. Problems can range from service degradation, to intermittent failure, to meltdown.

Complex faults require higher levels of analyzing client-server protocols and long transaction sequences. The costs – both the initial problem solving and the additional maintenance required – are usually not included in the original planning.

To ease deployment time and lower the risk of downtime, you need a thorough understanding of your network and how its technologies interact. By combining RMON and other standards-based tools with distributed data collection and expert analysis, you can get a detailed understanding of traffic flow patterns,network utilization, and application response times.

Sniffer Service Desk can be used to:

- Baseline your network to document trends and utilization patterns.
- Understand where the critical segments, users, and applications are and measure their impact on downtime or poor performance.
- Identify the segments that need to be upgraded, or project over time when they will need additional capacity.

Sniffer Service Desk is a suite of distributed analysis and reporting tools with visibility into all seven layers of the OSI network model. It gathers information on specific applications performance, network links, server bottlenecks, and more. Based on this information, Sniffer Service Desk provides reports that show which elements of your network require upgrades to improve response time for particular users.

The software can also pinpoint inefficiencies such as network transmission errors, time-outs,unexpected network hogs, and poor frame sizing, allowing you to make more informed decisions about moving to higher-bandwidth network technologies or tuning your network.

PACIFIC NORTHWEST TECHNOLOGY COMPANY PROACTIVELY GAINS CONTROL OF ITS NETWORK WITH SNIFFER SERVICE DESK

When the Network Services group of a Pacific Northwest technology company put Sniffer Service Desk Suite to work, within 10 minutes its analysis spotted 10 potential problems.

After a week of solving these immediate problems, network managers began the process of proactive performance management. They set bandwidth and error condition alarms, and then tied those alerts to their paging system to provide early warnings of network trouble conditions. This strategy ensured that network staff would learn about problems without hearing from users.

Sniffer Service Desk was also used to create a monitored testbed for every stage of ongoing network segmentation and server additions. During the installation of an NT server, managers had trouble with the distribution of DHCP IP addresses across network segments. Sniffer Service Desk quickly and accurately pinpointed the problem and provided actionable information to solve it before the problem could spread to the production network.

The benefits of this proactive approach were:

- Sniffer Service Desk provided a very high return on investment by replacing speculation with real information and analysis. Efforts were concentrated on solving problems rather than searching for their cause.
- The expert symptom and diagnosis system helped proactively look for little problems before they became big problems.
- Because the network is often inaccurately blamed for downtime that is actually caused by servers or applications, management staff gained not just insight, but also relief.

Sniffer Service Desk Suite: How it works

At a centralized console, Sniffer Service Desk gathers information from SNMP-managed devices in the network. It analyzes MIB statistics and determines which are the most critical, trending them over time to predict when a specific interface will exceed its performance threshold. Sniffer Service Desk pulls network statistics and analyzes them on a real-time basis if desired, whereas other products simply gather scheduled updates and compile them once a day.

Sniffer Service Desk employs an expert-based error system to prioritize problems and generate a list of their probable causes and best solutions. Depending on the type of device raising an alarm, Sniffer Service Desk is indexed to the hardware vendor's own documentation to help managers quickly resolve the problem.

These products are easy to set up and use. Managers simply define the devices they want to manage; Sniffer Service Desk gathers the information and automatically diagnoses it. A simple graphical interface allows managers to easily understand what's going on.

Sniffer Service Desk even shows the performance characteristics of networking equipment's more intricate parts. Routers, for example, contain specialized elements such as memory, an operating system, an input/output bus, and network interfaces. Sniffer Service Desk can report on how a router is tuned or configured,allowing adjustments to better fit a particular environment.

Proactive Problem Resolution with McAfee Total Service Desk

Doing more with less while providing higher service levels is one of the most critical challenges facing technical support and network managers today. These challenges are most keenly felt at the network help desk.

Traditionally, the help desk was responsible for end user support while network management staff were responsible for the network infrastructure. But increasingly, many help desks have to juggle support challenges with management-related tasks such as tracking corporate IT assets or resolving network-related problems on the spot.

The traditional help desk and network management are now being integrated into one entity. What is needed is a suite of thoroughly integrated network management and help desk applications that help to unify these dual roles.

The Integrated Help Desk/Network Management Solution

McAfee Total Service Desk (TSD) provides all the tools necessary to handle the day-to-day tasks of network management, such as inventory, software metering, and software distribution. It includes many functions to improve the help desk's efficiency and enhance its capabilities.

All the TSD tools are tightly integrated to provide one source of network and desktop information, and to automate the process of interpreting and acting on this information. TSD offers a unique combination of proactive management and help desk tools.

Proactive Problem Prevention

Total ServiceDesk allows help desk staffers to be more proactive by identifying potential problems and taking corrective action before they occur. TSD can detect problems before users become aware of them, suggest solutions, and automatically inform IS staff via e-mail or pager.

Immediate help desk awareness of problems affecting multiple users allows consistent management and timely resolution of these problems. This results in less downtime, fewer calls to the help desk and greater user satisfaction. For example, knowing that a server is having problems and may go down enables proactive notification of affected users via e-mail, before they call to add their trouble tickets to the workload.

Automatic notification can also be used to inform personnel immediately when a network component malfunctions. This cuts redundant call volume, enabling help desk operators and network managers to apply more of their time to solving and preventing problems. In many cases, problems can be resolved before any end users are affected.

Total Service Desk applies its advanced messaging capabilities in the opposite direction as well. Users can notify help desk operators of a problem by simply clicking on the "Rescue" icon on their desktops. Rescue immediately collects all of the appropriate desktop configuration information, such as copies of configuration files and a snapshot of the user's desktop, attaches these files to an e-mail message and forwards the message to the help desk. This trouble ticket is automatically processed using a set of predefined rules to locate and notify the appropriate help desk personnel.

Proactive Network Management Problem Resolution

Total ServiceDesk supports open standards such as SNMP. This makes it convenient to have your network management tools deliver their notifications

NETWORK CONSULTING FIRM SPEEDS LARGE NETWORK ANALYSIS WITH SNIFFER SERVICE DESK

A network-consulting firm specializing in enterprise network management systems uses Sniffer Service Desk to help speed diagnostic analysis of its customers' large LAN/WAN routed networks.

The consultants use Sniffer Service Desk to proactively monitor bandwidth utilization for capacity planning and performance reports, taking advantage of Sniffer Service Desk's automatic, real-time evaluation. A manual evaluation using traditional network management tools would require checking each individual circuit – a tedious, virtually impossible exercise.

One customer was rolling out a distributed SAP/R3 installation across more than 300 locations. With Sniffer Service Desk, the consultants tracked bandwidth utilization on hundreds of WAN circuits costing more than $1 million per year in access charges. They performed trend analysis on every circuit and identified overutilized links that were causing poor application performance. This analysis helped to improve application response times while avoiding the purchase of yet more gear or bandwidth.

Sniffer Service Desk also helps solve problems with carrier services. During an audit of a customer's frame relay service, Sniffer Service Desk spotted incidents of high congestion which were resulting in sluggish performance. The carrier, however, had only noticed lower utilization rates and concluded that the line was fine. The customer used Sniffer Service Desk's reports to prove their case to the carrier, who subsequently solved the problem.

to the service desk. By doing so, you leverage TSD's powerful escalation and alerting functions. These functions can be monitored by TSD's Service Level Agreement module, giving you complete control over defining who should receive each type of alert and what the appropriate response time should be. Event Orchestrator, a component of TSD that runs as a Windows NT Service, constantly monitors the network for SNMP alerts that are posted when a network component malfunctions. When an alert is intercepted, a trouble ticket is generated and the help desk and network personnel are automatically notified via e-mail or pager of the component's unavailability – even users who are likely to be affected can be notified.

Total Service Desk provides tools that allow help desk analysts to fix problems without having to rely on network management personnel. Information such as hardware, software, and configuration file data assists the help desk operator in diagnosing problems quickly without passing the problem on to second level support. They can review resource allocations and alter access,upgrade outdated software versions, replace DLLs, control end user menus, reset access, and perform other tasks that would otherwise be handled by network management personnel.

McAfee Total Service Desk Is Easy to Use

Many users who have chosen competitive help desk products are dismayed to find that implementation can take six to nine months due to proprietary development languages and limited database integration. Furthermore, most such point products focus on the help desk only – they are not an integrated suite of help desk and network management tools.

Other network management packages that use proprietary databases cannot provide enterprise help desks with access to the network management information stored in those databases. TSD instead uses non-proprietary database and development standards; therefore, you can be up and running in a production environment in less than 45 days. The key to this integrated ease of use is support for open database standards such as Oracle, SQL, and Sybase database management systems.

The integration of these technologies allows your help desk to do what it increasingly must – help to manage the network and eliminate downtime by fixing trouble calls before they occur. Centralizing alerts at the IT service desk insures that the entire IT organization is constantly informed of the network status and can react in a confident and coordinated fashion when a crisis occurs. The TSD White Board feature lets the entire IT organization know

about critical issues that are being worked on. This assures that consistent status information is given to end users and that IT management is not blind sided when serious problems occur. This targeted messaging system, Beacon, lets you send advisory messages to affected users before they call the Service Desk, reducing call volume and letting you focus on resolving problems quickly.

Since all IT activities are coordinated through ServiceDesk, a much more accurate and consistent record of problems and accomplishments is maintained. This greatly helps long term planning and management review of historical events. It is also invaluable to assist you in preparing change management projections.

Summary

Today's fast-paced business environment cannot tolerate slow networks or networks that break. The cost of faulty performance is enormous, averaging millions of dollars each year for large organizations. Conventional network analysis and management products are unable to help time-strapped information systems staffers keep networks running as smoothly as they should. These professionals must obtain greater in-depth network visibility on a full-time basis. Instead of "seeing" the network from the limited viewpoint of hardware devices, managers need to understand the actual communications that occur throughout the communications stack.

LAN Downtime — Costs, Causes, and Solutions

	Hard Downtime	Service Degradation
Productivity Cost	$1.6 million per year	$3.5 million per year
Revenue Loss	$2.5 million per year	—
Causes	• Hardware failures • Physical layer problems	• Traffic congestion • Poor application design
Broad Solutions	• Move from reactive to proactive planning • Invest in training • Replace old network equipment • Invest in new management tools	• Same as hard downtime
Focused Solutions	• Replace cabling • Modernize patch panels • Buy and install fault-tolerant, redundant hardware	• Invest in new traffic monitoring, RMON, real-time reporting, and trending tools • Invest in planning, design, and optimization tools

Source: Infonetics

A new generation of automated network management diagnostic and expert analysis software from Network Associates allows network managers to proactively prevent network performance problems before they occur. Network Associates provides Total Network Visibility so that your network will work the way users expect it to.

The following suggestions will help you create a proactive network performance management strategy.

- **Build the Team**. Talk to all parties that contribute to network planning and whose support you'll need in implementing changes. This includes end users, applications developers, system managers, network managers, and tool vendors.
- **Set Realistic Goals**. Identify your most important problems and prioritize them. Which will provide the most improvement for your organization? What future upgrades are planned? Don't wait for a perfect solution to every problem. Make improvements where you can using your prioritized list.
- **Get the Facts**. Gather hard data from controlled experiments or actual usage using the best tools you have. Be sure your decisions are based on facts rather than guesswork. As a final measure, always ask "why" – this will ensure that you understand the underlying reasons and have as much information as possible.
- **Review Your Options**. Once you have the data and understand the "why's" of your problems and goals, work with your team to review and discuss the most promising options.
- **Develop a Plan**. Any modification to one component of the network may affect other components. Develop a short-term and long-term testing program with likely variables to avoid as many problems as possible. Have backups and contingency plans so you'll always be prepared.
- **Partner Wisely**. At any step, you may need outside help to solve your problems and achieve your goals. Identify your objectives and "missing pieces." Make sure any outside providers of products and services understand where you are and where you want to be. Partner with companies directly experienced in meeting objectives similar to yours.

Return On Investment (ROI) Analysis

This worksheet will help you to calculate the costs, benefits, and payback period of Network Associates Sniffer Total Network Visibility and Sniffer Service Desk software suites.

	Typical Network	Your Network
I. Calculating your company's productivity gain		
• Number of users	500	
• Number of users X average annual cost of network	$716,500	
downtime ($1,433 per desktop)		
• Downtime saved by Sniffer and Sniffer Service Desk	50%	
software		
• Annual productivity benefit to your company (Line 2 X 3)	**$358,250**	
II. Calculating your company's revenue benefits		
• Increased E-commerce productivity	$50,000	
• Faster time to market for new products and R&D	$200,000	
• Increased production volumes	$50,000	
• Faster and more accurate billing of customers	$50,000	
• Better customer service		
• Other benefits to company		
• Total revenue benefit per year	$350,000	
• Your company's % gross profit margin target	10%	
• Your company's increased profit	**$35,000**	
III. Your company's benefit from lowering support staff expenses through improved troubleshooting		
• Number of support personnel	5	
• Average annual salary + overhead (fully burdened cost)	$75,000	
• % of time spent solving problems	75%	
• % of time saved by using Sniffer suites	50%	
• Annual support budgets that can be used for other activities – planning, product evaluation, solving less urgent problems, proactive management, etc.	**$140,625**	
IV. Payback on investment		
• Total annual benefits	**$533,875**	
• Total daily benefits	**$1,463**	
• Cost of Sniffer TNV and Sniffer Service Desk investment	**$112,875**	
V. Your Bottom Line Summary		
• Payback in how many days...	77	

Network Associates

CORPORATE HEADQUARTERS

3965 Freedom Circle
Santa Clara,CA 95054
TEL:(408) 988-3832
FAX: (408) 970-9727
Sales: (800) SNIFFER, (800) 764-3337

EUROPEAN HEADQUARTERS

Network Associates UK Ltd.
Royal Albert House
Sheet Street
Windsor, Berkshire
SL4 1BE,England
TEL:(44) 1753-827-500
FAX:(44) 1753-827-520

CANADIAN OFFICES

Network Associates Canada,Ltd.
TEL:(905) 479-4189
FAX:(905) 479-4540

ASIA/PACIFIC/LATIN AMERICA

Network Associates Asia
TEL:81-6-615-6370
FAX:81-6-615-6371

Network Associates Australia Pty Ltd.
TEL:2-9437-58-66
FAX: 2-9439-51-66

Network Associates Latin America
TEL:(954) 452-1721
FAX:(954) 236-8031

Network Associates products, support, and services are available from sales offices, authorized resellers, and distributors worldwide.

network ASSOCIATES
Who's watching your network

Forward product questions or sug gestions to Network Associates at: saless@nai.com
Information is available o n World Wide Web at http://www.nai.com