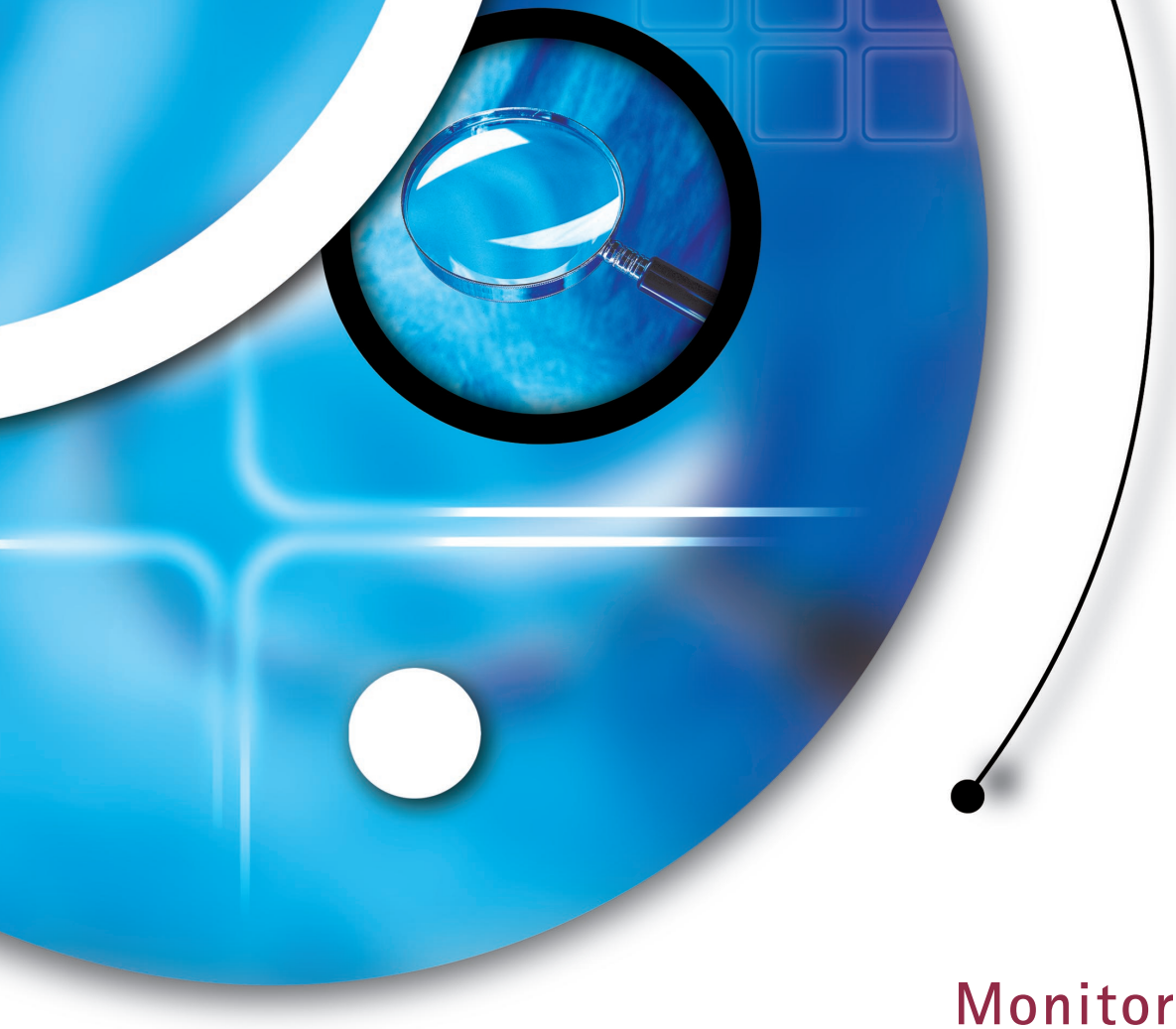


Monitoring the Switched Network

SNIFFER TNV COMBINES EXPERT ANALYSIS WITH RMON MONITORING FOR END-TO-END VISIBILITY AND CONTROL

EXECUTIVE WHITE PAPER

network ASSOCIATES

Who's watching your network

Table of Contents

The information in this white paper has been provided by Networks Associates Technology, Inc. To the best knowledge of Network Associates, these companies offer the types of products described. These companies are solely responsible for their software, distribution, and support services. Network Associates disclaims any and all liabilities for and makes no warranties, expressed or implied, with respect to these products, including, without limitation, the implied warranties of merchantability and fitness for a particular purpose. Distribution of these products, or information concerning these products, does not constitute Network Associates' endorsement of the products, the companies, or support services. Product information is subject to change without notice.

Introduction

In today's economy, business success increasingly depends upon network availability. Mission-critical business operations-from financial operations to supply chain management to product sales and customer service-are moving onto the network, and the cost of network downtime is skyrocketing accordingly. In this environment, no IT organization can afford to be without intelligent, proactive, and distributed network monitoring and management capabilities.

Today's enterprise networks are more often than not switched networks. Only a few years ago most networks were based on shared workgroups connected by multiprotocol routers. But emerging multimedia applications, nearly universal Web access, and the rise of corporate intranets are driving unprecedented demand for bandwidth at the desktop. In response to the growing demand for bandwidth and the rapidly dropping cost of workgroup switching, many organizations are implementing dedicated 10 or 100 Mbps Ethernet to every desktop.

Unfortunately, LAN switches have a downside from a network management perspective: it's hard to "see" inside them. It's difficult to get the same level of visibility into switched LAN traffic that was always available on shared media LANs. Without total network visibility, it is not possible to identify, diagnose, and resolve mission-critical network faults and costly performance problems.

Network Associates' Sniffer Total Network Visibility (TNV) suite is optimized for switched networks. It provides innovative, next-generation Sniffer network analysis solutions for Expert analysis of switched network problems—including VLAN configuration problems—along with proactive, distributed RMON-2 monitoring across the enterprise network. The Sniffer TNV suite delivers a comprehensive, end-to-end monitoring solution for control of your switched network.

Networking Management Takes Center Stage

The business impact of networking is growing every day. More core business processes than ever before are now network-based, and more corporate workers depend on the network to do their jobs. This means that even a network slowdown or "brownout" can be extremely costly in terms of lost productivity and revenue. According to a 1999 Infonetics survey downtime and degraded performance cost an average company $3.9 million a year and affect 41% of the employees for each instance of downtime or slowtime. The primary cause of service degradation is network traffic problems: congestion, delay, and the effects of packet loss.

The explosive adoption of a Web-based model of enterprise information flow has resulted in the growing use of both intranets and extranets in many businesses. The Web-based model lets companies improve business efficiency and enhance communications with customers, suppliers, and partners. For network managers, however, this trend brings new and unpredictable traffic flows, and IT organizations are struggling to respond to dynamically changing network utilization patterns and traffic flows.

In the past, many large enterprises under-invested in instrumentation for monitoring network traffic, expecting that historical network usage information would allow them to manage current and future utilization effectively. But in an age when multimedia, video, and intranet/extranet traffic streams are crowding onto the corporate enterprise, the old rules no longer apply. To manage the network as a high-value business service rather than as a collection of devices requires comprehensive network instrumentation and proactive, distributed, continuous network monitoring and management.

A properly monitored and proactively managed network not only helps avoid disastrous failures and costly downtime. It can also improve the efficiency and reliability of ongoing business operations and dramatically lower network operating costs. By identifying and eliminating potential network congestion, delay, or failure, proactive monitoring and traffic analysis helps leverage limited network management resources to their fullest extent and reduces the need for network specialists to travel to problem locations for costly on-site diagnosis and repair.

Management Challenges in a Switched Network

Traditional LAN technologies used shared media hubs to allow devices to communicate. Shared media hubs regenerate incoming signals on all ports. The available bandwidth is shared by all active stations, with each device "listening" to the network to determine which messages are intended for it, and when it is legal to send a message.

In a flat, shared network, it was possible to connect a network analyzer or Remote Monitoring (RMON) probe at a single location and see all the traffic on a segment (Figure A). The network monitoring strategy centered on instrumenting critical segments of the network with distributed network analyzers or RMON probes. In addition, traffic patterns were fairly constant and predictable over time, so a relatively static monitoring plan was often sufficient to achieve the required levels of network management visibility.

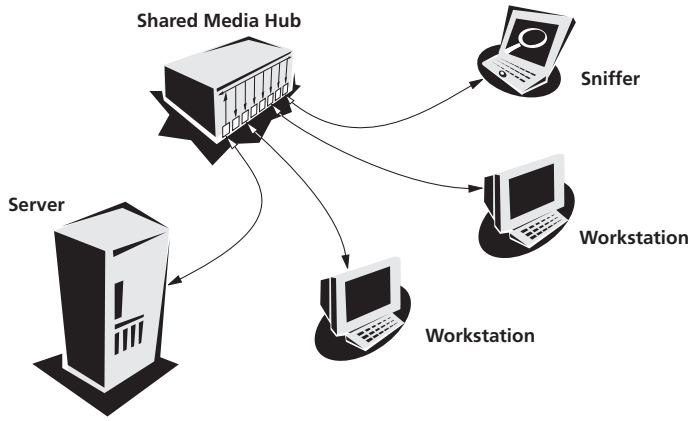


FIGURE A

All stations are visible in a shared network, so analysis can be done from any open port on the segment.

In a switched networking environment, by contrast, multiple conversations occur simultaneously across the switch on different segments (Figure B). There are many more segments to monitor because each switch port can be set as an independent LAN segment. And because the switch replicates only those packets destined for the devices connected to that port (along with broadcast and multicast packets destined for all devices), there is no single connection point from which to see all the traffic traversing the switch.

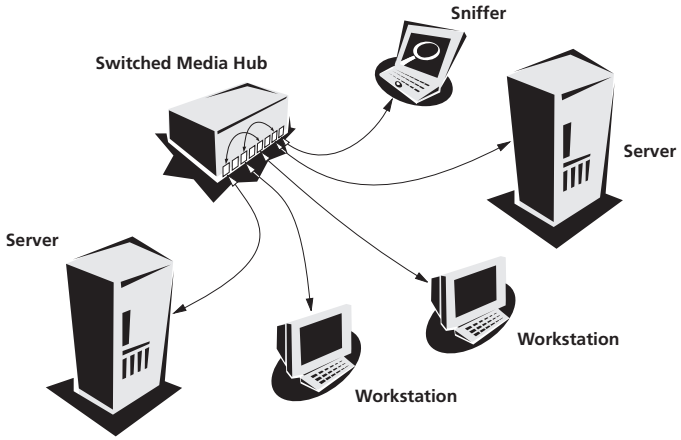


FIGURE B

When networks become switched visibility is lost, traffic is sent to only to specific ports. An analyzer can only see the traffic directed to the port on which it is attached.

Visibility into the switch often consists of little more than access to Simple Network Management Protocol (SNMP) management information base (MIB) statistics. More sophisticated switches have four RMON groups embedded within the switch (mini-RMON), or a means of using an external RMON probe to view the traffic on selected ports.

Visibility into client-server transactions have also become more difficult, servers no longer share a segment with end nodes or clients. More often connection is via full-duplex, point-to-point links, which would normally demand higher performance probes in the management deployment. But while a large increase in probes is not economically feasible, insufficient probe coverage is also unacceptable.

VLAN Management Challenges

The widespread use of virtual LANs (VLANs) in switched networks presents additional management challenges. Organizing a network into VLANs offers benefits in administration, security, and broadcast management. VLANs let you create workgroups based on the actual working relationships among the users rather than physical location, by creating a virtual broadcast domain from any set of ports or Layer 2 hardware Media Access Control (MAC) addresses. VLANs reduce support costs by simplifying address administration and making it easy to move workstations to a different virtual workgroup without address reconfiguration.

Many of today's Layer 3 switches include VLAN support implemented in hardware-based switching. This increases the need for monitoring and traffic analysis of switches and switch ports. Network managers need to be able to monitor traffic by VLAN. For example, VLAN host lists and utilization statistics are important tools for understanding, configuring, and maintaining networks. To provide useful management data in a VLAN environment, statistics should be aggregated, filtered, and reported on a per-VLAN basis. VLAN traffic patterns need to be monitored; ideally, inter-VLAN traffic should be only 10 to 20 percent of the total LAN traffic.

But VLAN monitoring has traditionally been done manually from a separate console. All traffic to or from a single switch port is sent to a designated monitoring port on the switch. Then all the ports involved in a VLAN are combined offline using manually defined VLAN filters in order to aggregate the data needed to view the VLAN and analyze its configuration and performance. Concern about the difficulty of monitoring VLANs has been a significant factor in slowing their adoption, with the result that IT has not realized the full potential that VLANs offer for cost savings in moves, adds, and changes.

Instrumenting Switched Networks

The traditional solution for detailed troubleshooting has been to dispatch a technician with a protocol analyzer to the problem site. And this approach can still be effective, especially for low-priority areas of the network. But for key devices, workgroups, and segments, today's mission-critical networks demand a higher level of ongoing management, one that lets you proactively monitor for potential faults and apply Expert analysis to the source of a problem remotely, from the network operations center. The savings in time and travel alone can often justify the cost of instrumentation. And in today's employment market, where skilled IT personnel are extremely difficult to find and retain, a network monitoring system that is integrated into the centralized enterprise network operations can help maximize the productivity of IT specialists.

To meet the changing needs for network monitoring and management in switched networks, Network Associates has expanded the functionality of its industry-leading Sniffer network analyzer family. Switched Network Expert Analysis and VLAN Expert analysis, combined with full distributed RMON-2 monitoring capabilities, provide powerful end-to-end visibility into the status and health of the switched network, as well as proactive troubleshooting capabilities to resolve problems before they become costly network failures.

RMON Alone is Not Enough

Because it is not usually cost effective to dedicate an analyzer or probe to each port on the switch, some switch vendors are embedding selected groups of RMON into their switches. But RMON alone is not enough to meet the network management challenges of today's networks. RMON provides plenty of raw data, but it doesn't necessarily translate that data into usable intelligence about the causes and solutions for exceptional conditions on the network.

As we have seen, effective network management requires more than just monitoring trouble alerts. IT management must be able to proactively detect and eliminate potential faults before they cause network slowdowns or outages. Ultimately, the goal is to generate the type of networking intelligence that can show how to redirect and optimize traffic flows based on up-to-the-minute traffic management data.

With these needs in mind, Network Associates latest generation of Sniffer network analyzers leverage both protocol analysis and RMON data collection, applying sophisticated Expert analysis to both protocol analysis data and RMON data to provide proactive diagnosis and recommend steps to resolve problems and optimize network operations.

Applying the Right Tools

To develop a monitoring plan for your switched network, first classify network resources according to how critical they are to the operations of the enterprise. Network Associates suggests three categories:

- **"Business-critical" or "mission-critical" resources** such as server clusters, backbones, and WAN links. If one of these resources goes down for even a few minutes, it poses a serious problem for the business. These key resources need dedicated monitoring and troubleshooting resources attached and operating at all times.
- **Important resources** such as an e-mail or intranet server, or a workstation used to perform time-sensitive tasks. These resources, if down for more than a short time, will impair productivity. These important resources should be instrumented with continuous monitoring, and alarms should notify you of current or potential problems. More powerful troubleshooting tools can be deployed to those resources as necessary to solve the problems.
- **Non-critical resources** such as low-priority workstations, or users or groups that can go down for a day or more without causing serious problems to the business. These types of resources don't need continuous monitoring. Embedded RMON can be used to identify problems, and troubleshooting resources, such as a portable Sniffer network analyzer, can be moved to the local network segment as needed.

The Total Network Visibility Solution

Three elements of the Sniffer TNV suite combine to provide the full instrumentation you need for total visibility into your network:

- Sniffer Distributed Analysis suite
- Sniffer Portable Analysis suite
- Network Informant suite

Properly deployed in the network, the Sniffer TNV suite provides a complete, proactive, end-to-end network monitoring and management system to optimize network performance while controlling management costs and meeting service agreements. For the first time a common, comprehensive solution that supports all of the network management team's operational needs-monitoring, planning, troubleshooting, and reporting-can be deployed enterprise-wide.

Sniffer Distributed Analysis Suite

The Sniffer DAS combines Expert analysis with distributed Sniffer system with distributed RMON support to give you the industry's leading network fault isolation and performance management solution. The combination of unique Sniffer Expert technology, the high-speed intelligence of the full-powered Distributed Sniffer System, and the broadest and deepest knowledge and experience base lets you anticipate and diagnose faults and performance problems, even in the most highly segmented switched networks.

Distributed Sniffer System/RMON's charter is simple: keep the network up and running at peak performance. Distributed Sniffer System/RMON analyzes all seven layers of the OSI model (Figure C). It observes network traffic to learn its unique patterns and characteristics in order to better identify and solve network problems. This depth of visibility lets the Expert systems in Distributed Sniffer System/RMON accurately pinpoint a problem's origin and provide the fastest time to resolution, avoiding network slowdowns and outages.

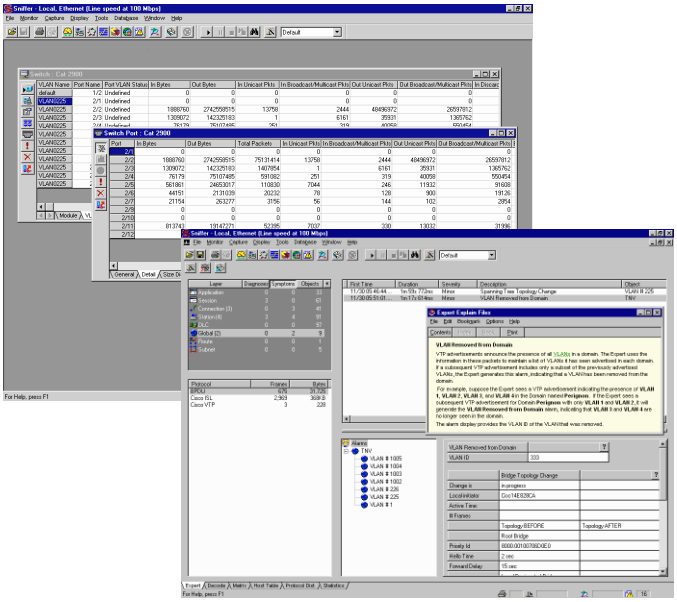


FIGURE C

Sniffer network analyzer can pull the configuration of a switch and monitor traffic in real-time. If a problem is suspected a capture can be done on a port or VLAN from the Sniffer and real-time Expert analysis can be performed based on a standard model of networking.

With the DSS/RMON agent connected to the monitor port of a switch, a network manager at the DSS/RMON console machine can be located anywhere in the network. And they can view the status of all the ports or VLANs on the switch.

If RMON monitoring detects a device utilization problem, a saturated port, or excessive physical layer problems, the Sniffer DAS can automatically instruct the switch to copy the problem traffic to the Sniffer agent for immediate expert analysis. The Sniffer DAS is fully integrated into Magic Total Service Desk's Event Orchestrator, so if needed it can automatically create a Magic TSD trouble ticket to dispatch a technician to the problem site, all without human intervention.

The Distributed Sniffer System/RMON provides automatic RMON-compliant segment monitoring and problem identification from a single management console. But unlike simple RMON-2-only data collection probes which are based on static counters, the Distributed Sniffer System/RMON lets you distribute Roving Expert intelligence to proactively monitor key segments or ports. If your data center switch has 10 server ports, for example, you can schedule the Roving Expert to automatically and continuously monitor those ports for any indication of trouble, identifying potential problems that RMON-2 alone might miss. This unique capability lets you apply extra instrumentation to critical resources for truly effective, proactive network monitoring without overloading critical LAN and WAN segments with unnecessary management traffic.

The Distributed Sniffer System/RMON maintains separate monitoring and communications ports. Because communications with the management console use a different network connection than the monitoring uses, the Sniffer analyzer can be attached transparently to the switch without creating traffic on the link, or breaking the network connection to the critical shared resource.

Modules for analyzing popular database applications make the Distributed Sniffer System even more powerful for determining whether problems originate in the network or the database (Figure D). Priority thresholds let you predefine how various application-level problems should be handled, from simple logging to automatically forwarding an alert to Event Orchestrator to generate a Magic Total Service Desk trouble ticket.

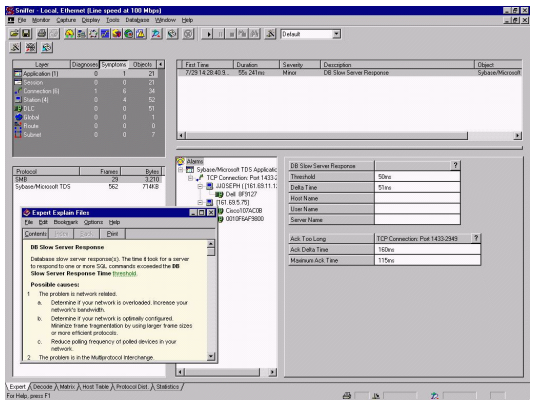


FIGURE D

Sniffer can analyze network traffic from the wire to the application, including databases and web-based applications.

Sniffer Portable Analysis Suite

In the past, the Sniffer analyzer was connected to the switch's passive span or monitor port, and commands were then issued from a separate console instructing the switch to send all traffic to or from a specified port to the monitor port for analysis. VLAN problems could only be diagnosed by manually setting filters to collect and combine data from the various VLAN ports for an offline analysis.

The next-generation Sniffer Portable Analysis suite provides the intelligence you need to prevent, pinpoint, and resolve problems swiftly and efficiently. The Sniffer analyzer runs on desktop, portable, and notebook PCs. It uses an unused switch port to issue commands directly from the analyzer to the switch. With this second connection, the Sniffer analyzer can

FIGURE E

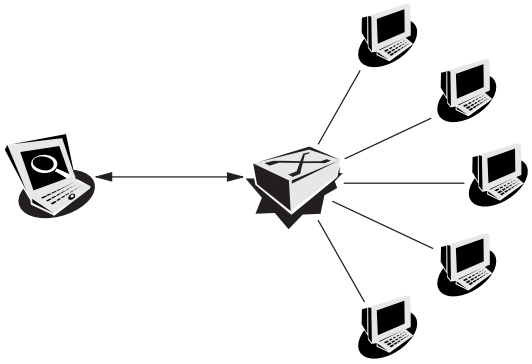
Sniffer with Switch and VLAN Experts

1. Sniffer automatically learns Switch and VLAN configuration
2. Sniffer extracts RMON information from switch and displays on Sniffer Screen
3. Sniffer can monitor activity and error levels across hundreds of ports simultaneously
4. With a single mouse click, Sniffer can "Span & Sniff" ports or VLANs
5. VLAN Expert detects VLAN configuration errors and faults AUTOMATICALLY

autodiscover the switch configuration in real time and automatically mirror specific ports back to the monitor port. Sniffer uses Expert analysis to spot problems causing downtime or slow response and recommend solutions—all in real time.

The Sniffer Portable Analysis suite also helps eliminate VLAN configuration worries by picking up any configuration problems encountered by end users (Figure E). VLAN connection or configuration problems used to be virtually invisible to the IT manager until the end user called in with a trouble report. But the Sniffer Portable Analysis suite's VLAN Expert picks up these kinds of problems and reports them automatically, along with recommendations for resolving them.

Sniffer Switch & VLAN Expert



With this automatic monitoring and expert analysis capability, The Sniffer Portable Analysis is appropriate for a variety of network monitoring instrumentation needs, from less critical segment coverage to high-speed, mission-critical or backbone networks.

Network Informant Suite

The industry-standard RMON in the Sniffer DAS provides long term statistics to support an enterprise view of changing application traffic patterns and network utilization. Network Informant, Network Associates' enterprise reporting and analysis solution, helps you use this information as the basis for strategic network and business investment decisions.

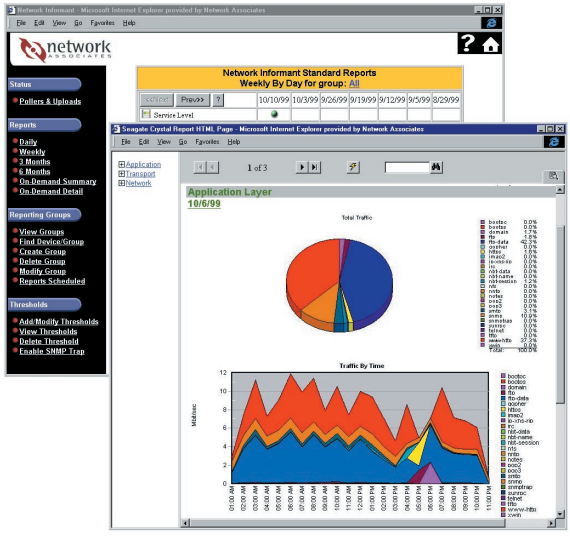


FIGURE F

Comprehensive network performance can be seen in Network Informant, pulling information from a variety of instrumentation devices on the network.

Network Informant collects data from a variety of network resources and compiles a comprehensive view of your network's performance (Figure F).

Web-based reports provide an overall summary and a detailed exception analysis of the network to help prove service levels delivered, control cost of WAN lines, and reduce network downtime. The highly flexible, three-tiered architecture of Network Informant makes it easy to define new network resources and new reports as corporate networking needs grow.

Scenario: Real Benefits for Switched Networks

Sniffer offers visibility at all points across the switched network. Suppose you have recently moved from a flat, shared network to a scalable, switched network in order to take advantage of the increased flexibility and manageability of VLANs. Fourteen tech support specialists are configured as one group, but after one week of high performance, the entire group experiences serious network degradation and poor application performance. The challenge is to discover what part of the switched network is causing this troubling slowdown.

Network Informant reports show no significant changes in overall utilization or type of traffic being transmitted on the network. By connecting a Sniffer unit to the switch span port and utilizing Expert analysis, you learn that a VLAN has been removed from the domain, causing the loss of communication.

In order to prevent problems like this in the future, you install a Distributed Sniffer System/RMON probe on the switch, making all port configuration information available at a central DSS/RMON console. (Figure G). DSS/RMON can respond to threshold violations from the mini-RMON in the switch and will automatically cause the problem VLAN or port to be mirrored to the span port where the full power of Expert analysis can diagnose critical problems and suggest corrective action.

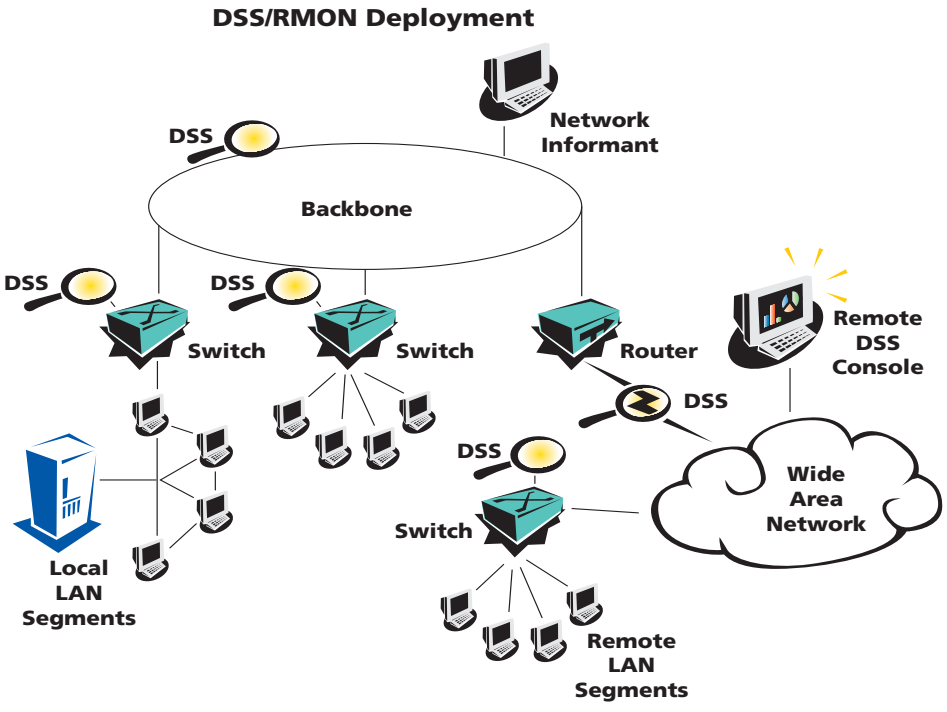


FIGURE G

Distributed Sniffer System/RMON agents can be deployed throughout the enterprise for complete coverage for monitoring, planning, troubleshooting and reporting.

Conclusion

The networking world is moving from shared to switched media. While this shift brings some important changes in monitoring methodology, the familiar fundamentals of network instrumentation still hold. As the enterprise network takes its place at the center of business operations, the need to monitor critical, devices, segments, and links is greater than ever.

Network Associates, the worldwide leader in network analysis and performance management, offers a full array of monitoring tools optimized for the switched network environment. Combining Expert analysis with RMON-2 monitoring, the Sniffer TNV suite for proactive, distributed monitoring, portable analysis and troubleshooting, and trending and reporting deliver the industry's most powerful solution for optimizing the performance of switched networks.

Who's watching your network

For more information on products, services, and support,
contact your authorized Network Associates sales representative.

CORPORATE HEADQUARTERS

3965 Freedom Circle
Santa Clara, CA 95054-1203
Tel (408) 988-3832*
Fax (408) 970-9727

**Call for additional Worldwide Sales Offices*

Visit our Website

www.nai.com

Sniffer, Total Network Visibility, Total Service Desk, SmartCapture, Net Tools, and Network Associates are registered trademarks of Network Associates, Inc. and/or its affiliates in the US and/or other countries. All other registered and unregistered trademarks in this document are the sole property of their respective owners. © 1999 Networks Associates Technology, Inc. All rights reserved.

6-TNV-ISN-001 10/99