



Proactive Solutions to the Five Most Critical Networking Problems

Table of Contents

| | |
|---------------------------------------------------------------------------------|----|
| The Challenge of Managing Networks | 2 |
| Proactive Versus Reactive Solutions | 2 |
| This White Paper Can Help | 2 |
| The First Steps | 3 |
| Proactive Solutions to Your Most Important Network Management Problems | 4 |
| Problem #1—New Client/Server Application Deployments | 4 |
| Case Study: Deploying a New Client/Server Application | 5 |
| Case Study: Migration to Client/Server | 6 |
| Problem #2—Migrating to New Technologies | 7 |
| Case Study: Simplifying Migration to New Technologies | 8 |
| Problem #3—Poor Network Performance | 9 |
| Case Study: Improving Network Performance..... | 10 |
| Problem #4—Not Enough Staff..... | 11 |
| Case Study: Maximizing Existing Resources | 12 |
| Problem #5—Network Downtime..... | 13 |
| Case Study: Reducing Downtime..... | 14 |
| What Network Managers Require..... | 16 |
| Network Associates Can Help | 16 |

The information in this guide has been provided by Network Associates, Inc. To the best knowledge of Network Associates, Inc., these companies offer the types of products described. These companies are solely responsible for their software, distribution, and support services. Network Associates, Inc. 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, Inc. endorsement of the products, the companies, or support services. Product information is subject to change without notice.

The Challenge of Managing Networks

As a network management professional, you face increasing challenges from many directions. A new client/server application must be deployed...new networking technologies must be integrated...high network availability is essential. Nevertheless, you're expected to handle the growing requirements of network management with little or no increase in resources. How can you keep pace? What can you do to be more proactive in solving network problems?

Proactive Versus Reactive Solutions

Most network managers feel stuck in a seemingly endless cycle, where users complain about network problems, those problems are fixed, and then users complain about new problems. The result is that morale suffers, productivity is slowed, and users learn to distrust the network. Other network managers use proactive strategies to anticipate problems and minimize their impact ahead of time. These strategies include regular network baselining, proactive testing, and building network testbeds. For more than 10 years, Network Associates has been helping network managers develop and apply these strategies. Using this information, Network Associates has developed specific proactive solutions that help solve the five biggest networking problems.

This White Paper Can Help

The objective of this white paper is to help you become more proactive in the fault and performance management of your network.

We will show you how to develop a plan to detect minor problems before they become major failures. We will provide an introduction to proactive measures that can dramatically improve your efficiency (and lower your stress level). Most importantly, we will outline practical steps you can take to anticipate and resolve the five most common networking problems:

- Difficulty deploying new client/server applications
- Uncertainties surrounding migrating to new network technologies
- Poor network response time and slow overall network performance
- Limited network management resources (such as, not enough staff)
- Excessive network downtime

The First Steps

Before addressing specific problems and solutions, here are six steps to help you create a proactive strategy for solving your most common network management headaches:

- **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" — it 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/or services understand where you are and where you want to be. Partner with companies directly experienced in meeting objectives similar to yours.

Proactive Solutions to Your Most Important Network Management Problems

How can you be more proactive, rather than reactive, in solving your most common network problems? The following sections offer specific suggestions, answers, and solutions to problems that plague networks every day.

Problem #1

New Client/Server Application Deployments

Imagine that you have just spent the last few weeks (or months) fixing network problems and bringing network performance to its peak. Everything is running smoothly and everyone is happy. Suddenly, your CIO tells you about a new finance application that needs to be supported by the network. You put the new client/server application on the network, and all you gain is a bunch of new problems. Does this scenario sound familiar?

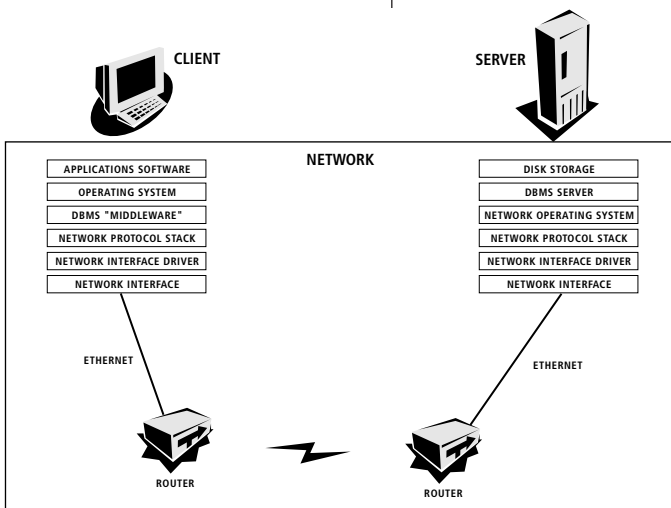


FIGURE 1:
Client/Network/Server model

The term "client/server" can be more accurately described as client/network/server (see Figure 1). The network is in the middle of clients and servers, and, as a network management professional, so are you. No matter how well managed an existing client/server system is, new problems inevitably crop up when a new application is put on the network. The roll-out of new client/server applications often causes problems like sluggish performance, poor response time, and even downtime.

When new applications are deployed in existing networks, they can affect the performance and reliability of other applications in ways that are difficult to predict, understand, isolate, and solve. Problems can range from graceful degradation, to intermittent failure, to disaster. Often,

higher levels of client/server protocols and long transaction sequences must be understood to isolate faults. The costs—both the initial problem solving and the additional maintenance required—are often not anticipated in the original planning.

What can be done to improve the process of new client/server application deployment?

Here are some specific steps:

- Remember that the performance and reliability of client/server applications are directly dependent upon the performance and reliability of the network that carries their communication, not the other way around.
- To minimize problems and optimize application performance, run the new application on a limited testbed before you begin new client/server application deployments.

- To monitor application performance and analyze any problems related to response time in the testbed network, use distributed protocol analysis and troubleshooting tools with visibility into all seven layers of the OSI model.
- Identify and resolve bottlenecks before deployment by evaluating the performance and capacity of the production network to assess the network's ability to support the new application.
- After you optimize the new application's performance, and tune the network, plan a staged application roll-out to the entire enterprise.
- Implement advanced full-time proactive monitoring tools with high-level protocol decodes and expert analysis upfront to help detect problems during testing phases, before the network is affected.
- Maintain seven-layer network visibility. If the application is deployed and problems exist, the better the visibility, the faster you can find a solution and achieve the benefits of the new system.
- Develop a written deployment plan, then follow the plan using the right tools and training. As you upgrade your network to a client/server environment, this can result in fewer problems and smoother transitions.

There are two ways to look at client/server deployment. The first is when a company rolls out a new application in an existing client/server system. The second is when an enterprise initially migrates from a legacy mainframe system to a client/server network.

Case Study: Deploying a New Client/Server Application

The benefits of proactive testing were understood at a major insurance company; management wanted 300 Windows NT clients in Accounting to have direct access to Human Resources information in an Oracle database on a UNIX server (see Figure 2). One option was to upgrade the clients with the necessary TCP/IP stack and Oracle TCP Protocol Adapter software—costly and time-consuming. The alternative was a less expensive \$1,500 Multi-Protocol Interchange (MPI) software upgrade to the NetWare server. MPI software provides a gateway service that allows Oracle clients and servers to communicate using different protocols.

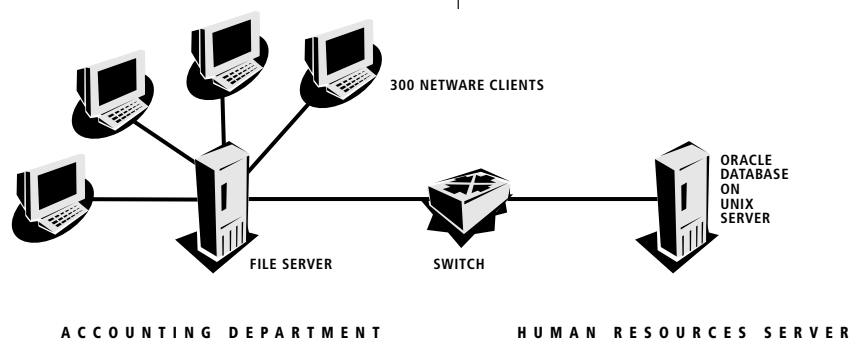


FIGURE 2:
Clients access Oracle database.

Before approving the latter, the IT manager wanted assurance that this solution would not cripple the response time of important and repetitive transactions caused by delays added by MPI software. Using the Sniffer Distributed Analysis Suite with included Oracle, the server upgrade solution theory was tested. At the time, the longest transaction involved 200 packets, with a total response time of 2–3 seconds. Testing showed that users were dissatisfied and less productive when response time approached six seconds.

The Sniffer DAS measured the added latency of the MPI software on the server to be acceptable: only five milliseconds/packet, or a one-second addition in response time. The benefits of this proactive approach were:

- Three hundred tedious desktop software upgrades were avoided.
- A cost-saving solution was deployed, satisfying management and users alike.
- The right decision was made based on hard data, not on conjecture and guesswork.

Case Study: Migration to Client/Server

A major American utility company had an aging token ring network of some 500 nodes communicating with IBM mainframes and UNIX servers. Management wanted to improve uptime, maximize profit, and reduce costs by upgrading to a client/server-based system. The

company implemented a cycle for upgrading legacy networks to a client/server environment (see Figure 3).

First, they deployed a Distributed Sniffer System with RMON and a “SWAT team” to optimize and baseline the network. They also put two Distributed Sniffer System with RMON agents to work: one in the applications development lab to test new applications; another to test new vendor hardware. The benefits of this proactive approach were:

- Response-time expectations were met 98% of the time.
- Key technical resources were leveraged.

- The need for additional personnel during the transition was eliminated.
- Troubleshooting time was reduced.
- New application development time was reduced.
- The roll-out of new client/server applications was smooth and successful.

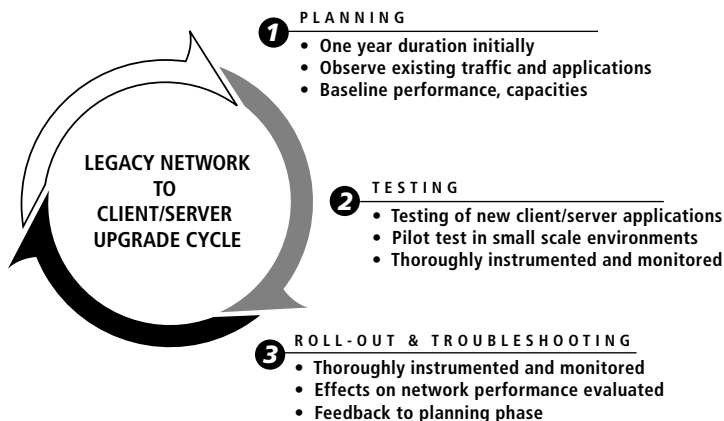


FIGURE 3:

Cycle of upgrading a legacy system to a client/server network

Upon completing the new client/server network deployment, the company would install Network Informant Suite—to proactively monitor and report network status. Able to automatically discover network elements and utilize data sources available on the new network, Network Informant provides the status summaries key to management reporting and troubleshooting. Also, RouterPM provides exception reports that give early warning of changes in device performance before they become critical problems. These products enable customers to:

- Anticipate problems before they affect service levels
- Automate problem identification with 7x24 expert analysis of device performance
- Leverage staff by allowing them to focus on the most critical problems
- Accurately plan for future growth with rolling 52 weeks of historical data

Problem #2

Migrating to New Technologies

Many organizations are installing high-speed and switched network technologies to improve network performance. Surprised at the unexpected problems, delays, and inefficiencies, they quickly learned that adopting new technologies, while essential, can be time consuming and risky.

To reduce deployment time and lower risks, you need a thorough understanding of your network and the new technologies—top-to-bottom, end-to-end information. By combining RMON and other standards-based tools with distributed data collection and expert analysis consoles, you can get a detailed understanding of traffic flow patterns, network utilization, and protocol turn-around times.

Whether you are upgrading to switching or installing a high-speed backbone, you need solid information—not guesswork. Here are some specific steps you can take to get the information you need:

- As you plan your migration strategy, learn as much as you can about your network.
- Employ device analysis tools such as Network Informant to: baseline your network to document trends and utilization patterns; understand where the critical segments, users, and applications are, as well as the impact of downtime or poor performance; identify the segments that are candidates for upgrade. Additionally, trending functionality helps you project when you will need the capacity.

- Use distributed protocol analysis and troubleshooting tools with visibility into all seven layers of the OSI model to gather information on application performance, top network conversations, server bottlenecks, and more.
- Based upon the information obtained about your network, determine which elements of your network to upgrade to improve response time for particular users.
- Pinpoint inefficiencies such as excessive retransmissions, time-outs, unexpected network hogs, and poor frame sizing, so you can make more informed decisions about moving to higher-bandwidth network technologies or tuning your network.
- Remember that what works on a small scale in an isolated network segment can bring the whole enterprise down when deployed in quantity on the production network.
- Design in fault and performance management tools that match the needs of new technologies; for instance, purchasing FDDI and ISDN protocol analyzers if you are installing FDDI backbones and ISDN in remote branch offices.

Case Study: Simplifying Migration to New Technologies

To the medical industry, the term “mission critical” often means life or death. Every network segment becomes mission critical as network communications affect the care of patients. Data accuracy and speed are crucial.

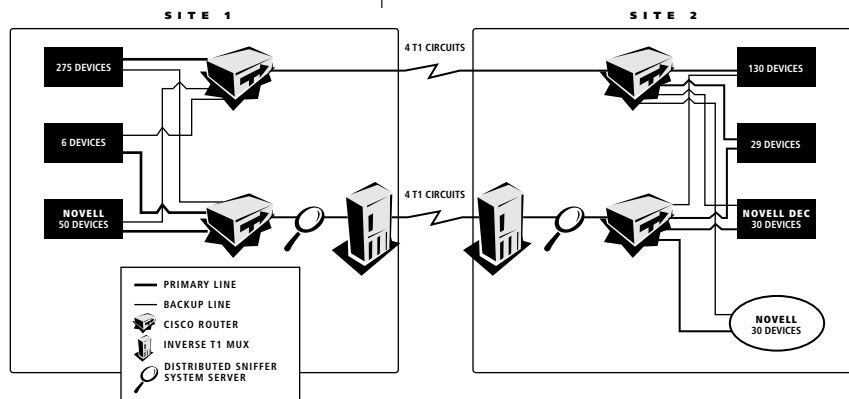


FIGURE 4.

Distributed analysis is used to continuously monitor traffic across networks

To continually improve the quality of care for its 28,000 patients each year, a major hospital in the South is constantly adding new technologies such as bedside terminals, video conferencing, voice recognition for doctor dictation, and optical disk libraries for high-volume data storage and transfer. These patient-care technologies, in turn, place high demands on network and telecommunications technologies. The hospital's token ring and Ethernet

LANs support over 500 user nodes. Campus locations are connected via 17 voice T1 and 8 data T1 lines that transport TCP/IP, IPX, and DECnet protocols.

As a result, fault and performance management has played a big part in helping plan and implement life-saving applications. Before installing a new network technology, such as a high-speed fiber-optic backbone, the hospital uses its Distributed Sniffer System with RMON to study the existing network's performance. Any problems detected are solved before implementing a new technology.

By also deploying Network Informant, network managers would be able to get an early warning of exception conditions on their critical network backbone and WAN segments as they migrate to their new topology, facilitating the transition and helping avoid problems before they occur. Utilization trending also assists to identify future capacity requirements.

After deployment, the hospital uses the same Distributed Sniffer System with RMON to monitor positive and negative impacts of the new technology. With visibility into its distributed network segments (see Figure 4), the hospital can better ensure the reliability and performance of critical segments carrying patient care and charting, surgery scheduling, operations, and administrative applications traffic.

The benefits of this proactive approach were:

- The hospital has positioned itself strategically by implementing advanced technology to respond to patient needs quickly and safely in a cost-conscious environment.
- By pairing Network Informant's proactive management capabilities with the Expert analysis of Sniffer technology, the hospital can better maintain mission-critical networks, enabling it to provide the best care for patients.
- The Distributed Sniffer System with RMON has proactively "tightened up" the network so the hospital can rely on their mission-critical technologies to work as planned.
- With full confidence in their network, the hospital can use labor-saving technologies safely and efficiently.

Problem #3

Poor Network Performance

Isolating and solving poor network response time is one of a network manager's biggest frustrations. If poor network response time becomes chronic, you will be the first to hear about it. And while you search for bandwidth, bottlenecks, or router problems, users call your department "unresponsive."

The complexity of today's network is a factor. A typical network transaction involves multiple vendors, technologies, sites, and potential points of failure. 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 applications software.

Or the problem may be the result of the complex end-to-end interaction of all of these components. This problem, which is becoming more common as the enterprise moves to client/server architectures, requires a significant amount of time and energy, as well as various levels of technical knowledge, to isolate and resolve. Often, the problem is only resolved through a combination of tedious hand-decoding of long transaction trace files, expert knowledge, and time on the phone with several vendors.

What can be done to improve that labored process? Here are some specific steps:

- Obtain total visibility of your network. If you can't see the cause of problems, you can't solve the problems. Put into operation network fault and performance management tools and systems that extend visibility beyond the LAN and into applications, systems, and databases. Partner with a network vendor that offers proven experience and technology to help maximize network visibility.
- Clearly define the problem. A statement such as "the network is slow" describes a symptom, not the root problem. You must narrow the problem down to a statement such as "the file server does not respond fast enough to user requests because it does not have the processing power," so you can then decide if an increase in bandwidth or a shift to microsegmentation will improve performance. Definitive, measurable statements will help you find and fix the problem.
- Employ expert-based analysis systems. They speed problem resolution and can be upgraded over time, letting you take advantage of the growing base of troubleshooting experience of other industry professionals.
- Design into your network powerful distributed monitoring systems as part of a full-time management strategy. The data necessary to detect the source of slowly degrading performance can be captured over time and solutions planned long before users complain.
- Consider building a partnership relationship with a reliable provider of networking services. A full-service partner can provide valuable expertise from planning to troubleshooting.

Case Study: Improving Network Performance

A major international insurer maintains its leadership position by organizing its global resources into a single enterprise working toward common goals. The backbone of this enterprise is the extensive LAN and WAN network connecting offices around the globe.

In less than three months following the installation of the Distributed Sniffer System with RMON, the company improved network response time by identifying where delays took place and making necessary corrections.

In one instance, desktop access to critical information on a VAX server was improved by using the Distributed Sniffer System with RMON. By determining the time a packet took to cross a switch, the distributed solution provided the key information leading to the discovery of a bottleneck.

In another instance, the Distributed Sniffer System with RMON successfully indicated that a problem with a switch was causing a delay. The network administrator was able to fix the problem locally and send a trace of the delay to a switch manufacturer who used the information to correct the problem for users with similar configurations. This proactive measure saved the insurer a tremendous amount of time in troubleshooting other locations with related performance problems.

The benefits of this proactive approach were:

- The root causes of network performance problems were more easily and quickly identified and solved using expert analysis.
- Instead of dealing with vendor finger-pointing, the insurance company was able to promptly identify which vendor's products were the cause of poor performance.
- In many cases, network performance problems were solved before users ever complained about poor response time.
- The insurance company has increased overall productivity, as well as its ability to compete in the marketplace, by proactively maintaining high network performance.

Problem #4

Not Enough Staff

It's a reality of network management. Networks grow in size and complexity, but the resources to manage them usually don't keep pace. Budgets are stretched. Existing staff must be leveraged as effectively as possible. As Figure 5 shows, you're expected to know more and do more with fewer resources and less help.

One way to increase the effectiveness of your network management resources is to improve the quality of your service. Here are some specific steps you can take:

- Make proactive network management your standard operating procedure. The best fault and performance detection and correction tools must be designed into the network and operated full time, rather than on a crisis basis.

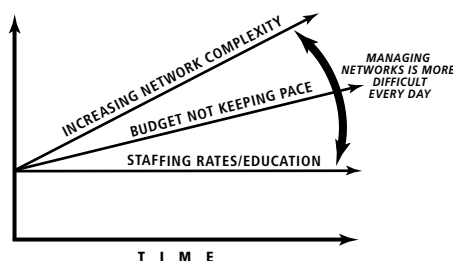


FIGURE 5.

The widening gap between network complexity and network management resources

- Use expert systems, which leverage the experience of others.
- Integrate network analysis tools to stretch your management resources.
- Ask industry vendors to work together more closely to solve problems and communicate solutions to users.
- Deploy advanced tools with distributed data gathering devices and expert-based centralized analysis consoles to help you monitor your entire network with fewer people, solve problems faster, and make better decisions for the future.
- Utilize tools that allow you to automate tasks, such as data gathering and report generation, as much as possible.
- Take advantage of products that provide exception reports and high-level summaries. This information can help you prioritize problems and focus resources on the most critical needs.

Case Study: Maximizing Existing Resources

A large government contractor had a network consisting of 50 Ethernet segments with an FDDI backbone. The contractor's three locations used WAN connections to share a mission-critical project management application. Then a serious problem developed: data was being lost over the WAN connections.

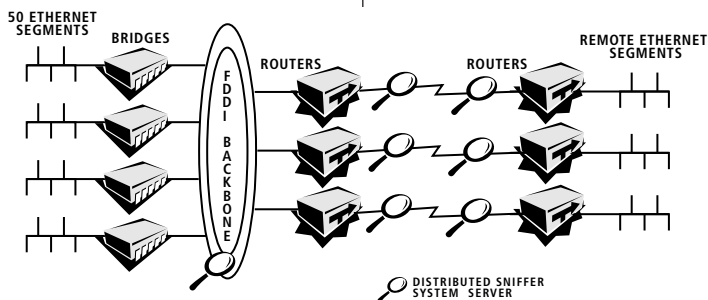


FIGURE 6:
Distributed analysis optimizes mission-critical WAN segments

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 the Distributed Sniffer System with RMON (see Figure 6), the troubleshooters used the Expert analysis capabilities to zero in on the problem—it was the application software itself. The

acknowledgment times preprogrammed in the software were insufficient for use over a WAN connection. The solution was to dedicate a 10 Mbps link for the critical application.

To further maximize network performance, this contractor could implement a rules-based analysis tool, such as Network Informant, to perform round-the-clock monitoring and expert analysis of all router interfaces. Automatic analysis of data and display of a prioritized list of potential problems allows a network manager to take corrective action without having to wait until a failure or critical user problem manifests itself. Additionally, partnering with a reliable provider of networking services can give you the advantage of proven expertise in meeting planning, design, implementation and management requirements.

The benefits of using a centralized problem-solving system were:

- The Distributed Sniffer System with RMON finds the causes of problems in minutes, not days, saving critical time for the entire network management organization.
- The distributed fault and performance management solution realized cost savings in its very first assignment. The Distributed Sniffer System with RMON was able to locate, in a matter of minutes, a problem that had stymied four people for a total of 120 hours (4 people at \$25/hour is \$12,000, which greatly exceeds the investment in the Distributed Sniffer System with RMON).
- 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.

Problem #5

Network Downtime

When your network or a part of it is unavailable, what does it cost your organization?

Today, the performance of the network is closely tied to the performance of the organization as a whole. What would it be worth to your organization to reduce or eliminate network downtime?

Given the complexity and nature of the technology, as well as human factors, some network downtime is virtually unavoidable. However, networks can be designed to recover more quickly from failures. Here are some specific steps you can take to reduce network downtime:

- Identify all mission-critical network segments first. Determine what network segments, routers, servers, or other devices are absolutely essential to the daily operations and health of the organization.
- Provide redundant or backup systems that can be brought on-line quickly or even automatically during failures.
- Consider upgrading to full-time network fault and performance systems. Rather than being reactive to critical failures, it may actually cost the organization less money (and the network manager less unpaid overtime) to be using a proactive, full-time network communications management solution.
- Use advanced tools that help you quickly locate problems and determine their exact causes by providing visibility into every layer of network traffic.

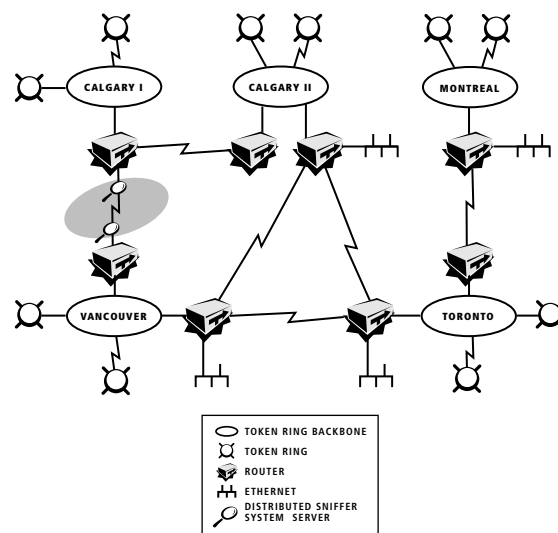


FIGURE 7:

Visibility into both sides of the WAN connection showed that hardware on the internetwork link was causing CRC errors

- Measure and track downtime with automated tools to help proactively identify problems and document availability.
- Stress test the network after making off-hours equipment or configuration (e.g. router table) changes to verify that these changes did not adversely affect network connectivity, performance, or reliability.
- Use integrated expert systems to provide the analysis to determine the root causes (not just the symptoms) of problems and then recommend solutions. Expert systems can detect problems at an overall lower cost than the lost productivity from network downtime.

Case Study: Reducing Downtime

An international airline relied on a network of 60 remote token ring LANs with Cisco and IBM source route bridges connected via high-speed internetwork links. The network was used to process over 300,000 flights annually and provide mission-critical services for over 2,000 end users.

Users of a critical application that ensured proper staffing of revenue-generating routes began to have access problems. Without it, staffing for flights had to be coordinated manually at a very high cost. There was also increased risk that critical revenue-generating flights would go unstaffed and be unable to depart.

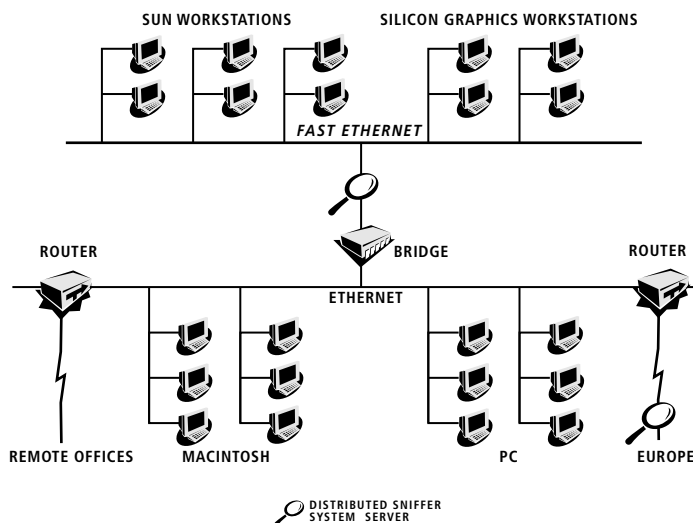


FIGURE 8:

Strategically-placed distributed servers can troubleshoot existing problems as well as anticipate potential problems

The application resided on a remote file server which generated TCP/IP traffic across internetwork links to token ring segments. Isolating the problem in this complex path was elusive. First it was assumed that it was NetBIOS related because many of the company's applications were built on NetBIOS and had a history of excess bandwidth consumption problems in the network configuration.

The Distributed Sniffer System with RMON (see Figure 7) was able to isolate the problem to a particular hardware component on the internetwork link that was causing Cyclic Redundancy Check (CRC) errors on large-sized frames. Once the problem was identified, access to the essential application was quickly restored.

The benefits to this major airline were:

- The cause of the problem was pinpointed immediately, avoiding guesswork and speculation.
- Network downtime was eliminated in a mission-critical revenue-generating application, allowing the company to continue to be competitive and productive.

In another case, a technology company in the Northwest used its troubleshooting success to springboard into proactive network management. Its network supports 500 users on Pentium PCs, 40 Sun Workstations, and a few Apple and Silicon Graphics machines linked by Ethernet and Fast Ethernet segments running NetWare and Solaris 2.4. It also supports a WAN connection to Europe, as well as 25 remote offices (see Figure 8).

The Network Services group put their Distributed Sniffer System with RMON to work on day one. In the first 10 minutes of operation, the Expert analysis capabilities immediately pointed out 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 the network managers would learn about network problems before hearing from angry users. The Distributed Sniffer System with RMON was also used extensively to create a monitored testbed for every stage of their network segmentation and server additions. During the installation of an NT server, Network Services had trouble with the distribution of DHCP IP addresses across network segments. The Distributed Sniffer System with RMON quickly and accurately pinpointed the problem and provided actionable information to solve it. This prevented the problem from spreading to the production network.

The benefits of this proactive approach were:

- The Distributed Sniffer System with RMON provided a very high return on investment (ROI) by replacing speculation about problem causes with real information and analysis.
- All efforts were concentrated on solving the problems rather than searching for their cause.
- The expert symptom and diagnosis system helped proactively look for little problems before they became big problems.
- And finally, both cases could also have benefitted from the use of service level management software to track network downtime and demonstrate improvements in the area of QoS and availability. Because the network is often inaccurately blamed for downtime caused by servers or applications, this sort of reliable reporting is especially helpful.

What Network Managers Require

For more than 10 years, Network Associates has been talking to senior IS managers throughout the world about network fault and performance management. Our goal is to learn about network managers' most important problems and then develop solutions. As the largest company in the world totally dedicated to network security and management, Network Associates has more network fault and performance management experience than virtually anyone else.

A clear consensus emerges when we ask IS managers what they want from a network fault and performance management solution: they want intelligent solutions that provide not just data, but also value-added information to enable their staff to quickly solve network problems and optimize network performance.

This is the future trend in network management—building in greater network visibility on a full-time basis. Instead of “seeing” the network from the limited viewpoint of certain devices, managers need to understand the actual communications that occur between devices. Beyond network management, they need network communications management to troubleshoot problems at higher levels, such as client/server transactions.

Network Associates Can Help

Network communications management solutions like the Distributed Sniffer System with RMON and its supporting tools provide the end-to-end and top-to-bottom visibility essential to achieving real-world gains in network performance and uptime.

The Distributed Sniffer System with RMON, with built-in expert analysis and protocol interpretation capabilities, incorporates the accumulated experience of network experts who may have already identified and solved your current problem.

Network Associates' addition of RMON to the Distributed Sniffer System enable customers to have comprehensive, superior fault and performance management solutions from one supplier. And—through advanced network applications like Network Informant that use the instrumentation already built into your network—Network Associates helps you assess and report quality of service, proactively identify network problems, and predict capacity needs through trend utilization.

For more information, contact your authorized Network Associates sales representative or call 1-800-SNIFFER (1-800-764-3337) or visit our Web site at <http://www.nai.com>.



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

CORPORATE HEADQUARTERS

3965 Freedom Circle
Santa Clara, CA 95054
TEL: (408) 988-3832*
FAX: (408) 970-9727

**Call for additional Worldwide Sales Offices*

Visit our Website



<http://www.nai.com>

Sniffer, Distributed Sniffer System, RouterPM and Network Associates are registered trademarks of Network Associates, Inc. and/or its affiliates in the U.S. 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-VSG-PAS-003 8/99