

---

White Paper

# Proactive Analysis is the Key to Optimizing Networks

An Executive Guide to Addressing Network Challenges

**Netcordia**

---

# Copyright

Copyright © 2006 Nectordia, Inc. All Rights Reserved.

March, 2006

## **Restricted Rights Legend**

This document may not, in whole or in part, be photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form without prior consent, in writing, from Nectordia, Inc.

Information in this document is subject to change without notice and does not represent a commitment on the part of Nectordia, Inc.

## **Trademarks**

Nectordia and NetMRI are registered trademarks of Nectordia, Inc.

All other company and product names are trademarks of their respective owners.

## **Nectordia, Inc.**

2431 Solomons Island Road, Suite 302  
Annapolis, MD 21401  
Phone: 410.266.6161  
Fax: 410.573.5777  
[www.netcordia.com](http://www.netcordia.com)

---

# Contents

Executive Summary.....	1
What You Don't Know Can Hurt You.....	2
Delivering Actionable Information to Improve Management.....	3
Managing Risk and Ensuring Business Continuity.....	3
Optimizing Network Performance.....	5
Identifying and Correcting Security Vulnerabilities.....	5
Demonstrating Compliance with Federal & State Mandates.....	6
Improving the Productivity of Network Staff.....	6
Summary.....	8

# Executive Summary

IT executives today are under pressure to ensure high performing, highly available, secure networking environments at the lowest possible cost. At the same time, compliance with state and federal regulations is another vital priority impacting network management, as CIOs share accountability with CEOs and CFOs for lapses in consistent processes and reporting.

With today's complex, heterogeneous, and far-flung networks, the information and functionality the network staff needs to address these challenges requires a new type of solution to complement traditional, reactive network management tools. What's needed is a proactive analysis tool that continually evaluates and improves the health of the network, while helping ensure compliance and security of the network.

NetMRI delivers the proactive analysis needed by network engineers to maximize network performance and uptime and be more productive. With NetMRI, difficult to find problems, intermittent outages and unpredictable operational errors are brought to light quickly, saving considerable troubleshooting resources and maximizing network reliability and response time.

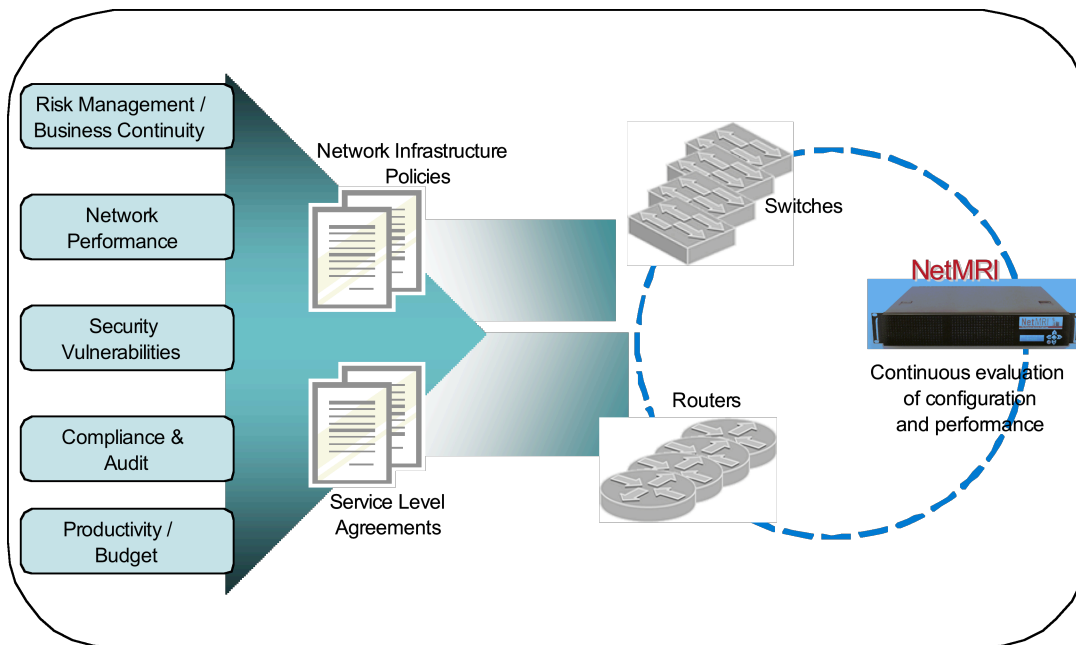


Figure 1. NetMRI Addresses Key Network Challenges

NetMRI enables engineers to address network management challenges to:

- Mitigate risk of a network outage
- Reduce network security vulnerabilities
- Optimize network performance
- Demonstrate compliance with mandates such as Sarbanes-Oxley, HIPAA, and others
- Be more productive and efficient

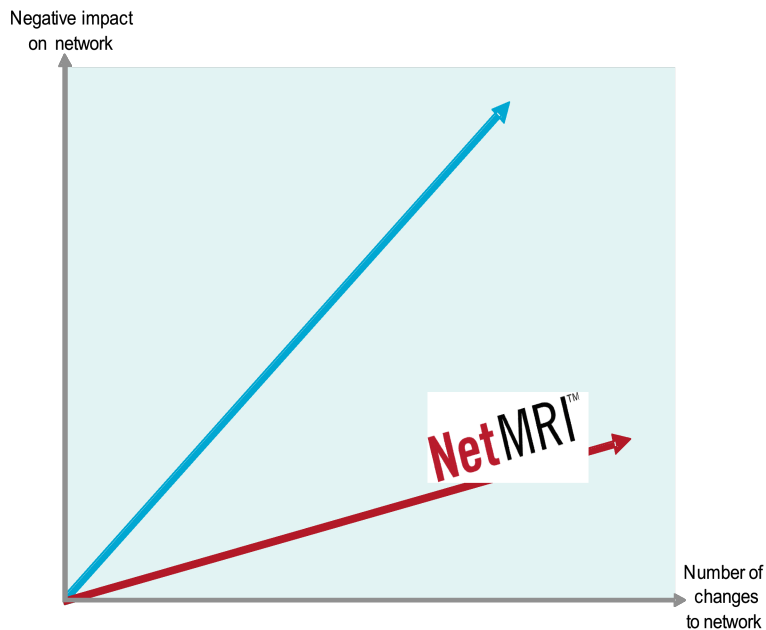
This paper describes how NetMRI helps organizations address the issues of performance, security, reliability and compliance. It also shows how NetMRI can rapidly pay for itself by helping network staff respond to potential problems before they happen in a more productive, efficient manner.

---

## What You Don't Know Can Hurt You

In most situations today, network availability and reliability are critical dependencies for an organization's success and ongoing viability. The problem is that today's networks are complicated beasts -- with the challenge being the sheer breadth of topologies that must be managed. Add to that the increase in converged networks that carry data, voice, wireless and video traffic. One mistake or failure in these complex environments can set a domino effect of major problems into motion.

Research from Enterprise Management Associates (EMA) shows that numerous changes are made every day to the typical enterprise network, and 80 percent of changes made to any one IT resource will change the behavior of other infrastructure components. EMA also estimates that 60 to 80 percent of all network problems are due to



Analysts attribute 60 -80% of network problems to configuration mistakes – NetMRI works to pre-empt these

configuration mistakes.

---

Figure 2. NetMRI Reduces Network Problems Due to Configuration Mistakes

Yet, it's nearly impossible for network engineers to constantly monitor every aspect of every device configuration. Nor can they be expected to analyze millions of data points to identify potential future performance issues. If anything, network engineers are faced with too much data from traditional systems management tools -- with little analysis or prioritization.

Executives today are searching for solutions that help them squeeze the most out of their network investment, while delaying capital expenditures and improving the productivity of the network staff. For this, network engineers need a tool that can methodically and continually evaluate network/device configurations as well as performance and report back on potential issues. Ideally, they need:

- A better view into network hot spots, for both performance and errors
- Daily operational configuration checks
- Identification of configuration changes and configuration policy exceptions
- Complete audit of network inventory
- A prioritized actionable list to help them target the most serious problems first

## **Delivering Actionable Information to Improve Management**

Unlike traditional systems management tools which generate alerts and error messages when something happens, a proactive network analysis tool methodically evaluates the entire network on a daily basis to detect potential issues before they become more serious in nature. NetMRI from Nectordia provides what network engineers need to assess and improve the health of the network, preventing major problems down the road and optimizing performance.

NetMRI provides in-depth network analysis on an ongoing basis, including: a constant audit of network inventory, compliance and vulnerability assessments, Layer 2 & 3 path diagnostic charts, and benchmarks with root cause analysis.

By providing end-to-end visibility, NetMRI identifies difficult-to-find problems such as suboptimal configurations or intermittent problems that steal bandwidth, slow response time and reduce reliability. The NetMRI correlation engine analyzes data and focuses in on the real issues affecting the network, presenting the results as a scorecard with a prioritized, actionable list of tasks.

As it gathers and correlates statistics from network devices and identifies issues that could threaten availability, security, or performance, NetMRI is not only helping your staff do more with less, it's bringing the benefit of hundreds of best practices and expert techniques recommended by Cisco and other leading manufacturers to the management of your company's network.

## **Managing Risk and Ensuring Business Continuity**

Regardless of the industry, outages are serious and costly impacts to the business or organization. Often, many small, seemingly insignificant errors or problems can combine to produce a major performance degradation or outage. According to EMA, the more complex the network, the more likely that a single change can have potentially serious downstream effects. The risk increases well out of proportion to the number of

network points, as both the number of points and the complexity of their configuration increases.

NetMRI enables network engineers to prevent significant problems by addressing potential issues proactively. NetMRI gathers information on a continuous basis and compares this to best practices to notify network managers of potential trouble spots prior to these issues becoming failures in the network that impact business operations. It provides proactive network analysis on routers, switches, firewalls, VPN concentrators, and wireless access points, including:

- Configuration correctness & stability
- Interface performance characteristics and statistics
- Memory & CPU Utilization
- HSRP configuration correctness and stability VLAN configuration correctness and stability

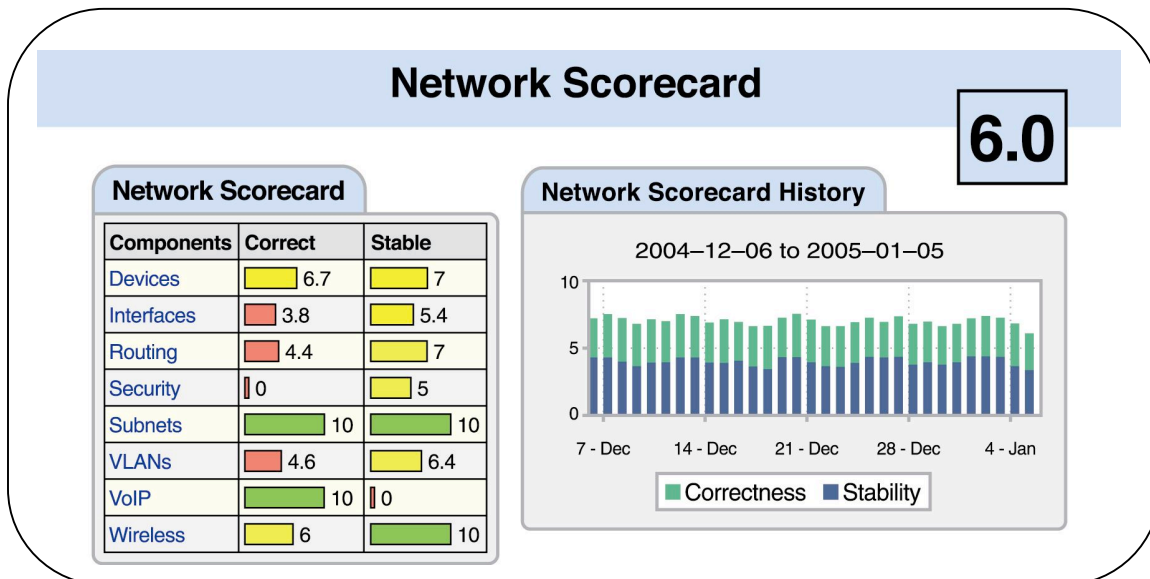


Figure 3. NetMRI Network Analysis Results

A prime example of how NetMRI helps ensure business continuity is its checking of network redundancy configurations, providing network staff time to correct deficiencies before they affect business operations. Using traditional methods, network analysts establish the redundancy on initial installation, but have no automated way to continuously monitor the state of the redundancy. They are only notified by traditional systems management tools that a redundancy has failed once it has begun to affect business operations, meaning that they only know of the failure at the point the redundancy is really needed.

---

NetMRI continuously monitors the health of the established redundancy, to make sure it's there when the organization needs it, i.e. when the primary component fails. If the state of redundancy changes, the network manager is proactively notified and can immediately access all the information about the operating behavior of the network to determine the source of the problem and correct it before it affects business operations.

## Optimizing Network Performance

With increasing demand for network services and expanding networks, executives are under constant pressure to ensure delivery of a consistently high level of performance, wringing the most out of the existing infrastructure investment. Maximizing the efficiency of the network not only enables companies to provide that high level of service, it can also help delay the acquisition of new equipment or expansion of the network.

NetMRI identifies, analyzes, and prioritizes issues that may impact performance, such as switch port duplex mismatches that cause the network to operate more slowly, or tracking utilization changes that could reflect a topology change affecting the routing of traffic on the network. Unlike reactive tools, NetMRI helps network engineers address many problems before they impede the performance of the network -- keeping your staff out of fire fighting mode and allowing them to spend more time proactively servicing the network.

One area particularly sensitive to performance is voice over IP (VoIP), which has become a core application for many companies. For those organizations with a converged data/voice network, the network managers' challenge is to provide mission-critical, reliable and well-performing VoIP service.

NetMRI's VoIP module identifies issues affecting performance and call quality. It analyzes call detail records (CDRs) and call management records (CMRs), along with SNMP data from routers, switches, gateways, etc., and compares configuration and QoS status across the call path. It also tests for jitter, latency and packet loss, so it can be used to both assess network readiness for VoIP and monitor production VoIP environments.

## Identifying and Correcting Security Vulnerabilities

While other areas of IT security may receive more attention, potential security vulnerabilities can occur or be introduced relatively easily into an organization's core network infrastructure devices through innocent mistakes or oversights. These vulnerabilities could then go undetected until a potential attacker exploits them and gains the "keys to the kingdom."

Mitigating the risk of a network breach therefore requires constant vigilance of network devices and configurations to ensure they continue to conform to your organization's established configuration policy as well as best practice rules for securing the enterprise.

As reported by the press and analysts, lapses in network configuration management have in fact played a substantial role in recent security exploits, such as the "success" of the many high-profile worms, denial-of-service attacks, and "zero-day" attacks.

NetMRI identifies and assesses vulnerabilities related to network devices and provides an actionable list to address them. It leverages security-related configuration checks based on published best practices from leading network equipment manufacturers as well as expertise and experience gleaned from hundreds of major networks. And because IT security is a vital component of regulatory compliance, NetMRI vulnerability analysis helps organizations comply with a variety of regulatory mandates, including Sarbanes-Oxley, HIPAA, and the Graham-Leach-Bliley Act.



---

In addition to configuration checks, NetMRI also locates other vulnerabilities that could potentially allow an attacker to gain control of a network device from a remote location. NetMRI helps network managers identify and close the “holes”-- such as an open Web browser interface on a router or switch -- that could enable access to unauthorized persons.

## Demonstrating Compliance with Federal & State Mandates

Network security is a critical component of regulatory compliance, with controls and measures mandated to prevent manipulation of sensitive data and inappropriate access to information resources. With mandates such as the Sarbanes-Oxley Act and HIPAA, it’s more important than ever for executives to demonstrate compliance by proving that the appropriate processes and oversight are in place.

The ability to automatically audit network configurations on a regular or daily basis across the entire corporate network is crucial to complying with these mandates as well as providing documentation to prove compliance.

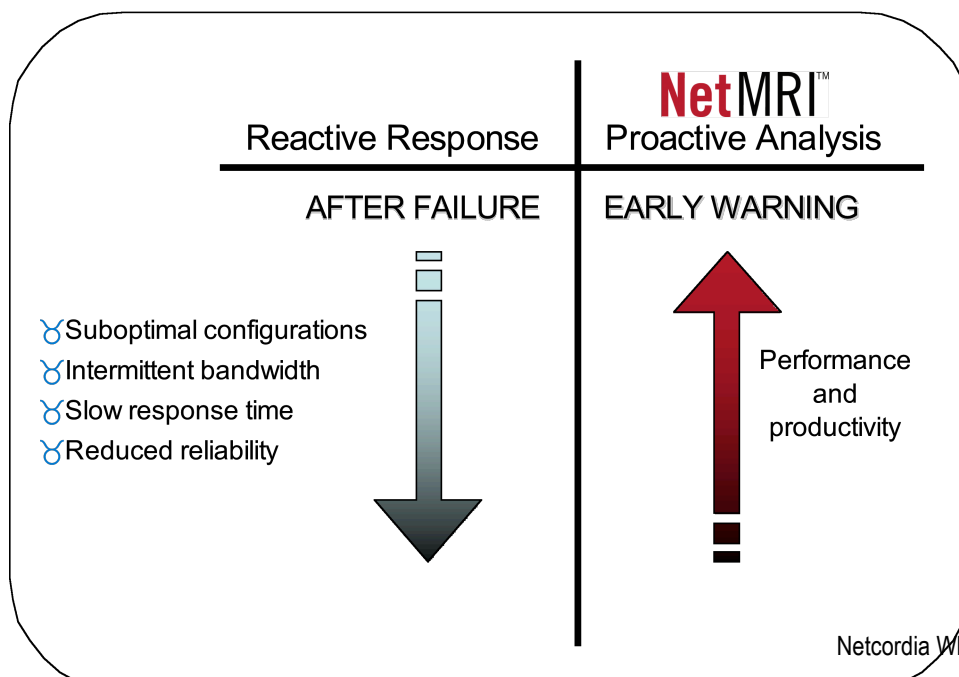
NetMRI supports continuous auditing of network device configurations against established company standards and processes. It helps companies comply with mandates by vigilantly ensuring that network policies and procedures are followed. Network device configurations are automatically audited every day and network managers are notified about devices that do not meet these guidelines.

Using NetMRI reports, companies can demonstrate compliance with mandates by showing consistent application of processes across all network devices and enforcement of those processes through daily monitoring of all network configurations.

## Improving the Productivity of Network Staff

As the network grows, so does the number of devices within the network -- making it more difficult to monitor and manage with traditional, reactive tools. At the same time, network budgets remain flat, so companies are forced to do more with less.

NetMRI saves significant time and resources by automating data gathering, performing analysis and providing a prioritized list of actionable issues. It’s an easy-to-install and use appliance with minimal maintenance requirements, freeing network management staff to more efficiently support the business.



---

Figure 4. NetMRI Improves Productivity Through Proactive Warnings

Network staff transition from fighting fires to more effectively improving the health of the network. If problems develop, NetMRI also reduces the amount of time spent troubleshooting by providing in-depth diagnoses to prevent trouble-shooting dead-ends.

To achieve similar results manually would require a significant increase in staff. Instead, NetMRI allows you to make the most of your current resources, even supplementing their network expertise with best practices rules. Conservatively calculated based on a 100-device network, with 70 switches, 20 routers, and 10 wireless access points, NetMRI would perform the equivalent of 80 person-hours of work. For more information on the rapid time-to-benefit and return on investment of NetMRI, see the “ROI of NetMRI” white paper.

---

## Summary

Traditionally, companies have purchased reactive management tools such as HP OpenView, CiscoWorks, and Tivoli for managing their network infrastructure. In an era where the network is more mission critical than ever, IT organizations need to add proactive management tools that better address the challenges today's IT executives face: high availability, high performance, reduced vulnerability, and regulatory compliance.

NetMRI from Netcordia complements traditional reactive network management products, with proactive analysis of the ongoing health of the network. It methodically evaluates the network and reports on issues that could impact performance and availability before they become major problems. It enables IT executives to do more with less and maximize their investment in network infrastructure.