Make Network Management More Efficient

Four key initiatives for addressing under-performing networks
Table of Contents

Executive Summary ................................................. 1
As Networks Become Business-Critical, So Does Network Management .......... 1
Here’s Just One Example of the Problems You May Face .......................... 1
Four Key Initiatives for Attacking Inefficiency .................................. 2
1. Optimize Fault Management ........................................... 3
2. Unify Fault and Performance Management .................................. 3
3. Automate Network Change, Configuration, and Compliance .................. 4
4. Automate Common Operator Tasks ...................................... 6
How Much More Efficient Can Your Network Management Be? ............... 7
Here are Steps You Can Take to Achieve Efficiency Now ....................... 8
Why Micro Focus? .................................................................. 8
A Complete Solution ......................................................... 9
Executive Summary

As your network gets complex, managing it must get simple. Network management teams are very often faced with deploying multiple tools to obtain the visibility and control they need to manage today’s complex networks. See how an integrated approach to managing networks can make it simple by using automation.

As Networks Become Business-Critical, So Does Network Management

The networks you manage are the foundation of the enterprise. Internal communications and collaboration, essential business processes, contact with customers, and revenue-generating transactions all depend on the performance and reliability of the network. The important role networks play in business processes and business success increases every day and so does the size, as well as the complexity of the typical network. According to a CIO article, “the more complex (networks) become, the more they cost to operate and maintain.”

To add to the pressure, network operations teams are expected to run their expanding mission-critical networks with fewer staff members and with disparate management tools.

Here’s Just One Example of the Problems You May Face

To illustrate how important the network is to the business—and how disastrous inadequate network management tools and procedures can be—let’s consider the case of a business that sells technology devices online.

It is the last day of the quarter—the day when most of the company’s business takes place—and orders are rushing in. Around noon, personnel in the Asia-Pacific order-entry department notice a slight performance problem. When Europe comes online, personnel there notice a similar delay.

While this is happening, the enterprise network management team at the data center in the US sees an uneven network performance graph on links between the data center with the order-entry system and the users. They are not sure whether the fluctuation indicates a network problem or an issue with the order-entry system, so they have the ticket routed to the system team. The system team finds nothing on its end and routes the ticket back to the network team. Time has been wasted—and now the problem gets worse. The east coast in the US starts working and the network slows to a stop.

---

1. 20 Ways to Reduce the Operational Costs of Your Network Before it’s too Late, CIO.com, June 2014
The probable cause is a spanning tree loop and this starts a time-consuming investigation with many handoffs. First, the network management team shuts down half the forwarding ports on the switches. When this doesn’t eliminate the problem, they return those ports to service and shut down the other half. They locate the source of the loop in this second half and repeat the process with quarter segments, eighth segments, sixteenth segments, and so forth until they identify the looped port and disable it.

Once informed that the problem is solved, the order-entry department starts furiously entering orders—and the network outage mysteriously starts all over again. The network engineers check each switch and each port looking for errors, finally uncovering a duplex mismatch. The network engineers fix the configuration and network operation returns to normal.

Unfortunately, the day is over and most of the orders have not been booked. The quarter is off to a financial disaster and the CEO wants to see the VP of IT early next morning.

### Four Key Initiatives for Attacking Inefficiency

The root cause was a duplex mismatch, but the real problem was the lack of a unified view and a consolidated management system. And that’s just one potential cause of costly debacles. Network performance issues can be caused by unanticipated traffic growth, configuration problems, link overloads due to traffic rerouted around failed network elements, and more—and such problems are usually hard to detect because they are not hard failures. Changes may lead to unwanted side effects and the monotonous work of making simple changes to hundreds or thousands of devices or objects is error prone. In addition, operators are often unable to capture the information that proactively detects and solves problems before they impact the network.

Existing disparate network management solutions stop short of providing a solution to help solve these types of challenges. What’s needed is an intelligent and integrated approach to managing networks. Four key steps can help you significantly improve network and operator efficiency:

- Optimize fault management
- Unify fault and performance management
- Automate network change, configuration, and compliance
- Automate common operator tasks

Changes may lead to unwanted side effects and the monotonous work of making simple changes to hundreds or thousands of devices or objects is error prone. In addition, operators are often unable to capture the information that proactively detects and solves problems before they impact the network.
1. Optimize Fault Management

In too many enterprises, network growth and complexity have outrun the capabilities of outmoded network management toolsets. To deliver the levels of reliability and availability that today’s operations demand, a system for network fault management needs the ability to:

■ Make sense of your network by discovering and understanding your physical network, virtual network services, and the complex relationships between them.

■ Update topology in real time, which is especially important in dynamically changing modern networks. The fault management system should quickly respond to these changes to help pinpoint the root cause.

■ Identify and assess the impact of issues with intelligent diagnostics, automated root cause analysis (RCA), and service state determination. The management system should then align key incidents with your environment.

■ Increase staff efficiency through built-in intelligence, targeted polling, automated actions, and a user interface that you can tailor to the needs of your IT staff.

■ Organize and restrict views, roles, and users around your customers and your key geographies.

■ Increase network service levels through shorter mean time to repair.

■ Manage new services and technology by expanding your network management software functionality.

■ Scale to meet your needs with a flexible architecture allowing for regional control with consolidation information.

2. Unify Fault and Performance Management

When the network is slow, the business is slow. And although users usually assume the network is at fault, many reports of poor performance are not network problems at all, but the result of overloaded servers.

In order to resolve all types of problems quickly, your team needs tools that unify network fault and performance management. This puts more power in the hands of first-tier operators, provides more information to specialists when problems are escalated, and improves information sharing across all levels of network support.

Unifying fault and performance information monitoring in a common console streamlines network operations and provides a much richer view of how the network is actually performing than disparate point tools could ever provide. This increases the capabilities of first-tier operators, who can base their investigation processes on both performance issues and hard faults, which then reduce the number of incidents that need to be escalated to specialists.
Discovering and monitoring the availability of configured paths in the network allows your first-tier operators to be proactive. Notification that a configured path test is performing outside of defined thresholds directs network operations to investigate whether this is due to a hard fault or network congestion. Operators now have the ability to visualize and report on an application path through the network. This provides them the key insight around the fault and performance of each link along the path, speeding RCA and resolution.

Unifying the tools can also reduce the overall administration of network management software by having fewer installations and reduced configuration. And additional capabilities, such as monitoring device CPU, memory, and buffers can be key to determining what is causing a performance problem. In addition to monitoring power supplies and fans for faults, the ability to monitor and alert for failures on redundant cards and ports allows for preventative maintenance to ensure network uptime.

3. Automate Network Change, Configuration, and Compliance

Network change and configuration management (NCCM) is a long-established discipline that involves establishing, recording, and verifying configuration settings for network devices to avoid downtime caused by configuration errors. Unfortunately, in many IT organizations, it is still a largely manual process. But forward-thinking organizations have begun to automate NCCM processes for two reasons.

The first is to avoid the errors caused by manual processes. The second is compliance with and reporting for internal standards or regulations such as the Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA). The network configuration management tools can automate both policy compliance and reporting.
Examples of Common Automation Flows

- **Compliance Enforcement**—With auto-remediation, the system detects unauthorized changes and can be set to restore the last approved configuration—manually or automatically. For organizations that require Customer Advisory Board (CAB) approval for changes, IT process automation can be used to forward the information to the CAB. When the approval comes back, the system can automatically implement the configuration change.

- **Operations Tasks**—Common changes such as password changes, access-control lists, and quality-of-service settings can be automated, freeing IT staff to focus on strategic activities.

- **Audit support**—Automated policy reporting can give auditors the information they need on multiple devices, quickly and accurately, without fire drills taking staff away from other responsibilities.

- **Configuration Tracking**—Automated audit trails log changes—note who made them and provide information for reports.

- **Automated Rollback**—If changes do have unanticipated consequences, automatic rollback can prevent hours of downtime and eliminate error-prone processes.
4. Automate Common Operator Tasks

With the size and complexity of network infrastructures growing continually, network operations teams need to enable tier-one operators to handle as many incidents as possible when they come in, without escalating to tier-two or tier-three level engineering teams. And, network operations needs to add detailed information to incidents before they are escalated, so that engineering will be more efficient.

Commonly, tier-one operators escalate incidents to network engineering teams with little or no additional triage or troubleshooting data available. Then, network engineers often need to log in to network devices manually to capture diagnostic and configuration information about that device when troubleshooting for a trouble ticket. Automating this information captured by the tier-one network operators speeds analysis by the network engineer, especially when the capture is registered at the time of the incident.

Furthermore, it helps the engineer to compare that diagnostic information against baseline history so that anomalies can be quickly identified. Network engineers can also use this data to verify the device information is normal after a fix has been implemented and thus have the new reference baseline for that device.

With rapid changes occurring in the status of networks, automated diagnostics can help network teams keep pace with events. For example, once an issue is detected by a performance monitoring system, automated diagnostics can be activated to collect key information before device failures render the information unavailable. This captured diagnostic information can be automatically delivered to a management system for review and resolution.
A well-designed and integrated fault and performance management system discovers as well as displays topology and status. It also includes device, component, interface, link, and path performance status.

Any one of these capabilities could have prevented a serious blow to the company’s financial performance—and could have avoided an unpleasant morning for the IT executive in the CEO’s office.

How Much More Efficient Can Your Network Management Be?

Let’s go back to the example we used at the beginning of this white paper—our online device vendor with order-entry problems. Here’s how the tools and initiatives we have discussed could have helped:

- Integration between the fault management system and the performance management system could have notified network operations that a critical network path was performing poorly based on defined availability tests. This would have helped network engineering to pinpoint the problem quickly. A well-designed and integrated fault and performance management system discovers as well as displays topology and status. It also includes device, component, interface, link, and path performance status. Given a source and destination address, the path can be displayed with fault and performance status.

- An integrated network management solution could have prevented the problem in the first place. The root cause was a manual change of the duplex setting made by a network engineer the night before—when traffic was low and the disastrous effect on network performance at peak load was not apparent.

- The optimization of the fault management system would have enabled the network engineer to do an impact analysis of the fault management system. The system would have queried the federated data repository and revealed that the switch the engineer was about to work on was in the path of the order-entry system. The engineer could have alerted the order-entry team, which would have recognized the potential for disrupting end-of-quarter peak traffic, and would have asked for the change to be delayed.

- If none of these factors had managed to prevent the problem, automated diagnostic information gathered at the time of the incident could have helped solve it quickly. Diagnostic data gathered in the past on the switch in question would have recorded the spanning tree ports under normal conditions. Then, when the spanning tree loop is introduced, new diagnostic data could have quickly shown that the spanning tree ports configuration had changed. The time spent searching manually for the problem would have been saved. Diagnostics can also detect common misconfigurations such as duplex or speed mismatches between connected ports.

- A comprehensive enterprise network management solutions could also have enabled network equipment to notify the system of the configuration change made by the network engineer. The system could have remediated the change automatically or could have notified the network fault console. If the change was unauthorized, the NCCM system could trigger a rollback to revert the device to the last approved configuration. The NCCM system would then notify the fault management system that a configuration change had taken place for the device and the network fault system should run a new discovery of associated nodes and interfaces. This process would have discovered the duplex mismatch at the other end of the link and could have executed the appropriate action.

Any one of these capabilities could have prevented a serious blow to the company’s financial performance—and could have avoided an unpleasant morning for the IT executive in the CEO’s office.
Here are Steps You Can Take to Achieve Efficiency Now

What Network Teams Need to Drive Efficiency

Network teams require a broad solution that addresses the management problem differently, cutting across traditional organizational structures and functional siloes of fault, performance, configuration, and compliance. A better way to look at this is to group capabilities into three categories, representing visibility, optimization, and action, and then enable use-cases that work across them—ultimately using automation wherever possible to maximize efficiency and save time.

Network Operations Management

A better way to look at this is to group capabilities into three categories, representing visibility, optimization, and action, and then enable use-cases that work across them—ultimately using automation wherever possible to maximize efficiency and save time.

Why Micro Focus?

Micro Focus is designed from the ground up to build, sell and support software. With more than 5,800 employees in R&D, the combined company helps solve the most complex technology problems for customers, delivering world-class, enterprise-scale solutions in key areas including:

- **DevOps**: enabling the rapid delivery of quality, secure applications with end-to-end visibility across a toolchain of commercial and open source offerings—leveraging the largest portfolio in the industry.
Hybrid IT: simplifying the management of a complex mix of platforms, delivery methods and consumption models to help organizations address business needs, control costs, and ensure availability and performance at global scale.

Security & Risk Management: Securing data, applications and access; powering security operations and governance to mitigate risk and maintain compliance; and harnessing the power of secure DevOps practices to ensure end-to-end risk management.

Predictive Analytics: Helping customers translate siloed data into real-time proactive analytics at scale, anchored on supporting open and cloud-based stacks to create new insights across applications, operations, security and the business.

A Complete Solution

Comprehensive Training
Micro Focus provides a comprehensive curriculum for the Software and IT Service Management courses. These offerings provide the training you need to realize the full potential of your solutions, increase your network optimization and responsiveness, and achieve a better return on your IT investments.

With more than 30 years of experience in meeting complex education challenges worldwide, Micro Focus knows training. This experience, coupled with unique insights into Micro Focus Software and Solutions products, positions us to deliver an outstanding training experience. For more information about these and other educational courses, visit software.microfocus.com/software/enterprise-software-education-services.

Services
Get the most from your software investment. Micro Focus provides high-quality software services that address all aspects of your software application lifecycle needs. With Micro Focus, you have access to standards-based, modular, multi-platform software coupled with global services and support. The wide range of service offerings—from online self-solve support to proactive mission-critical services—enables you to choose the services that best match your business needs.

For an overview of Micro Focus Software Services, visit www.microfocus.com/softwareservices.

Learn More At
www.microfocus.com/networkmgt