

# **A practitioner's guide to more efficient network management**

Business white paper





## Table of contents

---

<b>Executive summary</b> . . . . .	3
<b>A practitioner's guide to more efficient network management</b> . .	3
<b>Just one example of the problems you face</b> . . . . .	3
<b>Four key initiatives for attacking inefficiency</b> . . . . .	3
Optimize fault management . . . . .	4
Unify fault and performance management . . . . .	4
Automate network change, configuration, and compliance. . .	4
Automate common operator tasks . . . . .	6
<b>Just one example of how much more efficient your network management could be</b> . . . . .	6
<b>Steps you can take to achieve efficiency now</b> . . . . .	7
<b>Why HP?</b> . . . . .	7
<b>A complete solution</b> . . . . .	8
Comprehensive training . . . . .	8
HP Financial Services . . . . .	8

## Executive summary

As the networks become ever more essential to business processes, they are also increasing rapidly in size and complexity. Many factors can affect network availability and performance—increasing traffic, configuration problems, failed network elements, changes, and more. Since not all of these problems are hard failures, managing the network to detect and correct business-impacting problems requires new tools, strategies, and initiatives. To deliver the availability and performance business demands, network management teams need to optimize fault management and ensure availability, unify fault and performance management, automate change and configuration management to ensure compliance, and automate IT processes. This integrated approach is called Automated Network Management (ANM).

## A practitioner's guide to more efficient 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.

This important role networks play in business processes and business success increases every day, and so does the size and complexity of the typical network. According to CIO Magazine, “The biggest area for steady cost growth is the ever-expanding network, either as a result of physical expansion or a general thirst for connectivity.”<sup>1</sup>

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.

## Just one example of the problems you 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 network team at the data center in the United States sees a saw-tooth 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 of the United States starts working, and the network slows to a stop.

The probable cause is a spanning tree loop—and this starts a time-consuming investigation with many handoffs. First the network 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.

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 officially a financial disaster, and the CEO wants to see the VP of IT early the 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, and operators are often unable to capture information necessary to proactively detect and solve problems before they impact the network.

---

<sup>1</sup> [www.cio.com](http://www.cio.com)—“Network Management: Tips for Managing Costs,” Karen D. Schwartz, August 25, 2008

---



Existing disparate network management products 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

#### **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 today's operations demand, a network fault management system needs, at a minimum, the ability to:

- Make sense of your network by discovering and understanding your physical network, virtual network services, and the complex relationships between them.
- Effectively understand and update topology in dynamically changing modern networks. The fault management system must have the ability to adapt to changes "on the fly" to guarantee pinpoint Root Cause Analysis (RCA).
- Quickly identify and assess the impact of problems with intelligent diagnostics, automated root-cause analysis, and service-state determination and 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 functionality.
- Scale to meet your needs with a flexible architecture allowing for regional control with consolidation information.

#### **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 to put more power in the hands of first-tier operators, provide more information to specialists when problems are escalated, and improve information sharing across all levels of network support.

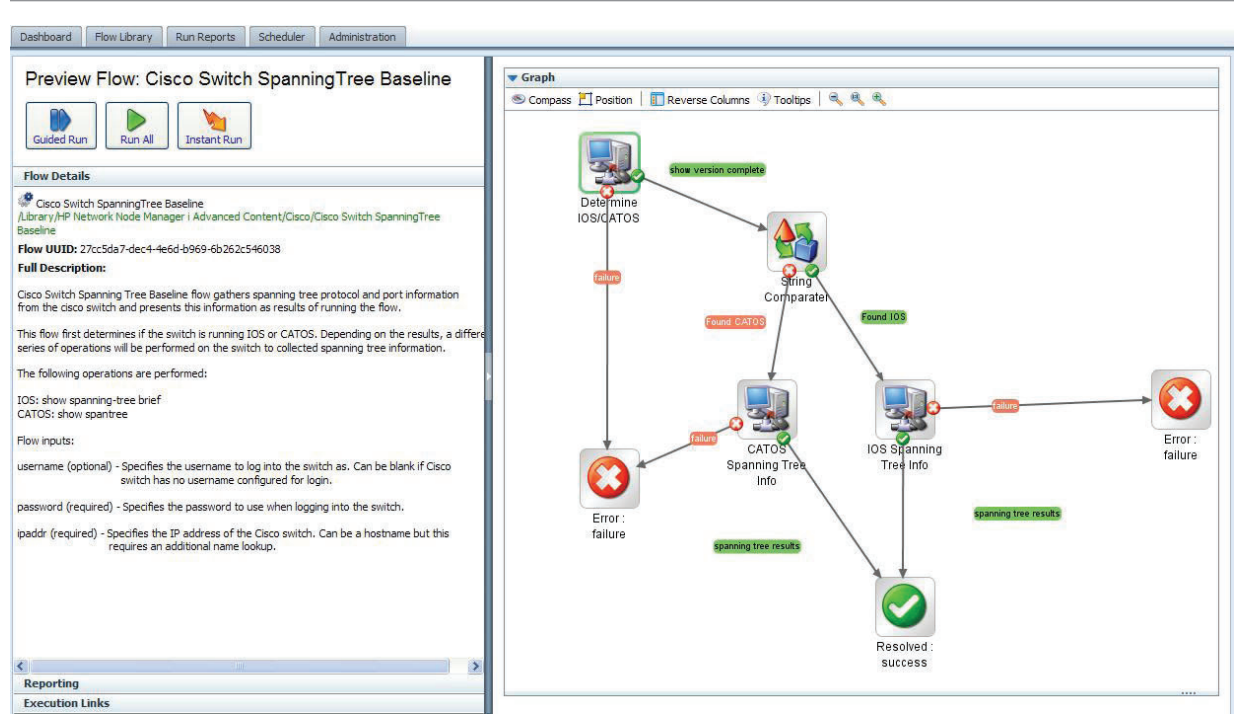
Unifying fault and performance information in a common console streamlines network operations and provides a much richer view of how the network is actually performing than disparate point tools could ever provide. This increases the capabilities of first-tier operators, who can base their investigation processes on both performance issues and hard faults and reduce the number of incidents that need to be escalated to specialists because they are now being handled by first-tier operators. Discovering and monitoring configured path availability tests in the network allows your first-tier operators to be much more proactive than they could have been in the past. 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. With the ability to visualize and report on an application's path through the network and show the fault and performance status of each link and device along the path, network, and other teams avoid finger-pointing, and assign problems to the correct team to solve them faster.

Unifying the tools can also reduce the administration of network management tools overall by having fewer installations and reduced configuration. And additional capabilities, such as being able to watch device CPU, memory, and buffers, can be key to determining what is causing a performance problem. The ability to monitor redundant cards and ports as well as power supplies and fans for failures, and then alert operators before these components fail, makes preventive maintenance possible.

#### **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.

**Figure 1**  
Automated diagnostic flow from HP iSPI Network Engineering Toolset



The first is to avoid the errors caused by manual processes. The second is compliance with and reporting for regulations such as the Sarbanes-Oxley Act (SOX) and the Health Insurance Portability and Accountability Act (HIPAA). Network configuration management tools can automate both policy compliance and reporting.

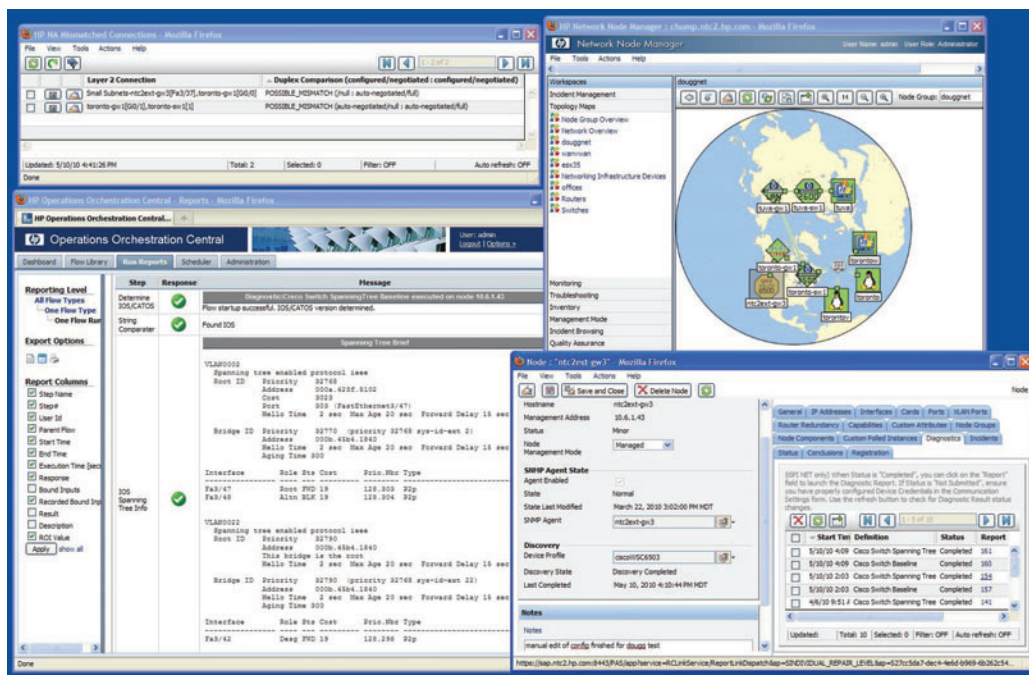
Automation yields a number of improvements:

- With auto-remediation, the system detects unauthorized changes and can be set to automatically restore the last approved configuration. 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.
- 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.
- 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.

- Automated audit trails log changes, note who made them, and provide information for reports.
- If changes do have unanticipated consequences, automatic roll-back can prevent hours of downtime and eliminate error-prone processes.
- Some automated NCCM systems have vendor best practices built in. For example, Cisco security updates recommend specific configuration changes, automatically available for review and implementation through the tool. This not only saves implementation time, but also research time.

Password changes, policy reporting, and audit trails hit one customer we know of during an audit. Staff members had solved the problem of changing device parameters by taking the time to write scripts. However, during an audit they could produce no reports showing what changes were made, when they were made, and who made them because there was no reporting or audit trails in the scripts. The auditor's report of issues that needed to be resolved was approximately one-inch thick.

**Figure 2**  
Spanning tree state investigation



### 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 incidents as 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. Network engineers then often need to manually log in to network devices to capture diagnostic and configuration information about that device when troubleshooting for a trouble ticket. Automating the process of capturing this information for the tier-one network operators at the time that the incident is registered saves the network engineers' time. Furthermore, it provides the ability for 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.

Because things happen very quickly in networks today, automated diagnostics can help technology teams keep pace with events. Once an issue is detected, for example, by a performance monitoring system, automated diagnostics can be activated to collect key information before it becomes unavailable and deliver it to a management system for later operations staff diagnosis.

### Just one example of how much more efficient your network management could be

Now 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, and would have helped network engineering to quickly pinpoint the problem. A well-designed and integrated fault and performance management system discovers and displays topology and status, including device, component, interface, link, and path performance status. Given a source and destination address, the path can be displayed with fault and performance status.
- Automation could have prevented the problem in the first place. The real root cause was a manual change 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.

**Table 1**

Steps you can take to achieve efficiency now

Step	HP building block	Efficiency gain
Implement fault management	HP Network Node Manager i	Reduce downtime by dynamically adapting to changes in the infrastructure
Integrate performance management and fault management	HP NNM iSPI Performance for Metrics HP NNM iSPI Performance for Traffic HP NNM iSPI Performance for Quality Assurance	Detect performance degradations before they become outages and resolve problems before they impact business
Automate change, configuration, and compliance management	HP Network Automation	Significantly reduce costs and improve reliability and compliance
Automate common operator tasks	HP NNM iSPI Network Engineering Toolset	Reduce costs and enable tier-one operators

- Integration of the fault management system would have enabled the network engineer to do an impact analysis from the fault management system that 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 was introduced, new diagnostic data would 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.
- Automation 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 to the device and the network fault system should run a new discovery of associated nodes and interfaces, which 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 perhaps to the VP of IT's career as well.

## Steps you can take to achieve efficiency now

HP supports a building-block approach to progressive efficiency and cost reduction in network management. The first step is to get fault management under control and reduce the number of outages that consume resources and interrupt business processes. The second step is to integrate fault management with performance management, enabling IT teams to be proactive. The third step is to replace manual configuration and change management with more efficient, less error-prone automated management. The final step is to enable network operations through automating time consuming manual tasks.

Table 1 shows the steps in this approach, the HP solutions that enable them, and the efficiency gains.

## Why HP?

HP Software and Solutions has invested heavily in its network management and automation solution. We have completely reengineered HP Network Node Manager i (NNMi) software, and according to an Enterprise Management Associates (EMA) analyst, "HP has seized the opportunity to unify network fault, availability and performance management and is in an excellent position to improve the effectiveness and efficiency of network engineering and operations practitioners."<sup>2</sup>

<sup>2</sup> Enterprise Management Associates, Impact Brief: HP unifies network fault, availability and performance management with NNMi9, 2010

HP received a strong positive in the Gartner MarketScope for Network Configuration and Change Management (March 2010). Strong Positive is the highest possible rating given.

HP has also been recognized for leadership in the area of automation. Gartner rated HP as a strong positive in the MarketScope for Network Configuration and Change Management (2010).

The HP approach to network management efficiency is not theoretical. It is an established methodology, proven in use by numerous enterprises in major industries:

- A major U.S. lender reduced mean time to recovery (MTTR) from 150 minutes to 15 minutes, a time savings of 90 percent.
- The State of Kansas achieved a 15 to 20 percent improvement in uptime and more than 3,500 hours per year of estimated savings.<sup>4</sup>
- A global search-engine company went from 3 percent audit compliance to 100 percent.
- Using automation, a major U.S. grocery store chain reduced the two weeks required to update 10,000 WiFi Protected Access (WPA) keys to two hours.

## A complete solution

### Comprehensive training

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

<sup>4</sup> Scott Steves, Systems Network Software Consultant, Network Analysis Group, Division of Information Systems and Communications, State of Kansas

With more than 30 years of experience in meeting complex education challenges worldwide, HP knows training. This experience, coupled with unique insights into HP Software & Solutions products, positions HP to deliver an outstanding training experience. For more information about these and other educational courses, visit [www.hp.com/learn](http://www.hp.com/learn)

### HP Financial Services

HP Financial Services provides innovative financing and financial asset management programs to help you cost-effectively acquire, manage, and ultimately retire your HP solutions. For more information on these services, contact your HP sales representative or visit [www.hp.com/go/hpfinancialservices](http://www.hp.com/go/hpfinancialservices)

## HP Services

### Get the most from your software investment

HP provides high-quality software services that address all aspects of your software application lifecycle needs. With HP, you have access to standards-based, modular, multi-platform software coupled with global services and support. The wide range of HP 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 HP software services, visit [www.managementsoftware.hp.com/service](http://www.managementsoftware.hp.com/service)

To access technical interactive support, visit Software Support Online at [www.hp.com/managementsoftware/services](http://www.hp.com/managementsoftware/services)

To learn more about HP Software Customer Connection, a one-stop information and learning portal for software products and services, visit [www.hp.com/go/swcustomerconnection](http://www.hp.com/go/swcustomerconnection)

To learn how you can significantly improve your network efficiency, visit [www.hp.com/go/anm](http://www.hp.com/go/anm)

Share with colleagues



Get connected

[www.hp.com/go/getconnected](http://www.hp.com/go/getconnected)

Get the insider view on tech trends, alerts, and HP solutions for better business outcomes

© Copyright 2009, 2010 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The MarketScope is copyrighted 2010 by Gartner, Inc. and is reused with permission. The MarketScope is an evaluation of a marketplace at and for a specific time period. It depicts Gartner's analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor, product or service depicted in the MarketScope, and does not advise technology users to select only those vendors with the highest rating. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

