

Realtime
publishers

The Essentials Series

Network

Troubleshooting and
Problem Identification

sponsored by
solarwinds 

by Greg Shields

SUPER-CHARGE YOUR NETWORK WITH *SOLARWINDS ORION POWER PACK!*

The **Orion Power Pack** combines three of our most popular products to take your network management to the next level!

- **Orion NPM** delivers comprehensive fault and performance management across multi-vendor networks of any size.
- **Orion APM** extends Orion NPM's powerful monitoring capabilities to applications and servers.
- **Orion NTA** provides deep visibility into network traffic behavior and trends by leveraging NetFlow, J-Flow and sFlow data.



Article 1: Bandwidth Monitoring and Traffic Analysis.....	1
Different Perspectives for Different Needs.....	1
Flow Analysis Provides a Big Picture View.....	3
Finding Resolutions to Common Problems	4
Focusing on the Right Features.....	5
Looking Forward	5
Article 2: Isolating Network vs. Application Problems.....	6
Common Problems in IT.....	6
Common Ways to “Tell the Difference”	7
Network Device Metrics Collection	7
Server Metrics Collection	8
Application Status and Event Collection	8
Transaction Timing Measurements.....	8
Alerting and Notification	9
Auto-Remediation.....	9
Isolating Problems Requires the Work of All IT Teams	9
Article 3: Automating the Top 5 Network Tasks with Configuration Management	10
Configuration Management’s Top 5 Tasks.....	11
Config Backups.....	11
Change Documentation and Audit Trails	12
Implementing Mass Changes	12
Identifying Inappropriate Configurations	13
Network Problem Notification and Remediation	13
From Highly Manual to Highly Automated.....	13

Copyright Statement

© 2008 Realtime Publishers, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtime Publishers, Inc. (the “Materials”) and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtime Publishers, Inc or its web site sponsors. In no event shall Realtime Publishers, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtime Publishers and the Realtime Publishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtime Publishers, please contact us via e-mail at info@realtimepublishers.com.

Article 1: Bandwidth Monitoring and Traffic Analysis

Your company's network lines and the interstate freeways have a lot in common. Each is a necessary component of an overall system. When well designed, each provides a high-speed connection between two points within that system. And each, when oversubscribed, results in a less-than-desirable experience for its users. You can use this freeway analogy in many comparisons between what is considered good network performance—high speed, low latency, few collisions—and performance that doesn't meet acceptable levels. To put it simply, when there are too many cars on the road, nobody gets to their ultimate destination very quickly.

Taking the analogy a step further, monitoring and measuring both network and vehicular traffic works in much the same way. There are multiple ways in which network traffic can be monitored and measured for performance. Traditional packet-based monitoring tools enable peering into individual packets to determine their contents, the transactions between systems, and the details of communications being passed along that network. Yet the packet-based approach is a lot like attempting to determine the cause of a traffic jam by peeking into each individual vehicle. Knowing what people and cargo are travelling within each vehicle may be helpful in answering some questions, but it's not likely to illuminate the cause of the system-wide slowdown.

Different Perspectives for Different Needs

Bandwidth monitoring and traffic analysis are two key activities for every business environment. Performing each correctly assists the network administrator with identifying areas of bottleneck. It helps the admin identify the network needs and uses of servers and their hosted applications, as well as how the network needs of one IT service impacts another. It also delivers hard data that objectively verifies the ability of the network to meet stated Service Level Agreements (SLAs).

And yet the perspective gained through these two activities is different than what we nominally think of as *packet analysis*. Whereas packet analysis tends to look at network conditions from a very close-in perspective, bandwidth monitoring and traffic analysis step back to see conditions on the system as a whole. To help you understand the differences in perspective here, let's take a look at common ways used to measure traffic on a network:

- *SNMP monitoring of network devices.* Device monitoring using the Simple Network Management Protocol (SNMP) provides a very device-centric view of network conditions. Using SNMP, counters on a device such as a router, switch, or firewall can be measured and forwarded to a network management system for review. This data is useful for understanding performance conditions that are specific to that device such as processor or memory utilization; however, analysis suffers when attempting to see conditions that occur across multiple devices or on the system as a whole.
- *Protocol analyzers.* Protocol analyzers take a look at network conditions from the perspective of the packet. These tools analyze conversations between devices on the network from the location where the analyzer is measuring. This information gives the network administrator an extremely detailed view of individual transactions between two computers and the specific data being transferred between them. But this perspective also suffers when attempting to gather information across the entire environment.
- *Hardware probes and distributed analyzers.* Hardware probes and distributed analyzers are an early attempt to overcome the limitations of an individual protocol analyzer. These tools can be positioned all across the network for the gathering of information. They go far in providing the whole-system perspective that is so difficult to gather through the previous two perspectives. Yet because each individual probe requires separate management, administration, and maintenance, their use suffers from scalability issues as the network grows.
- *Traffic flow analyzers.* These tools overcome the administration headaches of hardware probes and distributed analyzers by leveraging the data flow capture capabilities of the network device itself. Generically referred to as NetFlow or NetFlow data due to the prevalence of Cisco equipment in most IT environments—NetFlow is a Cisco protocol—there are, in fact, multiple manifestations of these protocols: SFlow, JFlow, and IPFIX to name a few. Traffic flow analyzers receive flow data directly from monitored devices and analyze that data to gain the high-level perspective needed for troubleshooting incidents across the network system.

Flow Analysis Provides a Big Picture View

Consider the situation in which you, the network administrator, are notified that there appears to be a problem with the network. When you sit down to troubleshoot the problem and look through your available tools, which of them provides the best picture of the situation? Depending on the problem at hand, flow analysis tools can be superior to the others for a number of reasons:

- *Easy to use and understand.* The big picture perspective of flow analysis tools tends to result in visualizations that are easy to understand. Traffic patterns between devices are regularly gathered, allowing for the visual mapping of network capacity compared to network consumption. With the high-level view of the network map readily available and with drill-down capabilities into problem areas, you can quickly identify system-wide behaviors that might relate to the problem at hand.
- *High-level traffic flows rather than packet-level inspection.* Although packet-level inspection is exceptionally useful for identifying the specific communication between two or more computers, network issues are most often reported at a higher level. Having the ability to see high-level flows helps the troubleshooting administrator quickly isolate the problem before digging deeper into its resolution.
- *Common vendor support.* Flow analysis tools tend to support multiple vendor networks. This is especially critical considering that most networks are not completely homogeneous. With devices from multiple network vendors being positioned around the network, crossover support for the flow analysis tools of each means that a Cisco router can be monitored by the same tool that looks after a Juniper device or an application firewall.
- *Low cost and low administrative overhead.* Unlike the use of probes or distributed analyzers, individual devices typically include native flow capture capabilities. Enabling these capabilities and directing them towards network management systems for data collection involves little additional work, virtually all of which is completed during the device's initial installation.
- *Provides rapid answers to critical questions.* Although deep packet-level inspection capabilities are handy for some network problems, the most often questions usually asked of the network administrator often relate to “What is consuming my bandwidth?” and “Why is the network slow today?” Quickly finding answers to these questions requires a holistic understanding of the network, its connections, and the types and levels of traffic being experienced across network links. Information gathered through high-level tools can usually be later leveraged for a deeper discovery once the larger initial questions have been answered.

Finding Resolutions to Common Problems

To further explain how flow analysis improves a troubleshooting administrator's efficiency, let's take a look at three common issues seen on most business networks today. The first of these relates to resource overuse by a specific application. When an application on the network begins consuming more than its fair share of network bandwidth, its use will impact the capacity available for other network services. The problem with identifying these incidents using other types of network tools is that the reporting of problems tends to focus on the network service being impacted. For example, when the problem occurs, the network administrator usually starts with knowledge that Application B "is slow today." The job is then theirs to determine why the service is slow and what is inhibiting its desired level of performance. Using effective flow analysis tools, the administrator can easily view the traffic and usage patterns across the entire network to identify that Application A is actually the culprit. Conversely, using tools with a closer perspective may incorrectly focus the administrator's troubleshooting on Application B, while ignoring the impact of Application A.

A second and similar issue occurs when a specific protocol overconsumes network resources. Streaming protocols are an excellent example of this type of constant and predictable network flow. When users on a network make use of streaming applications, their consumption typically occurs at a constant level over an extended period of time. Different than transaction-based protocols, streaming protocols have the tendency to saturate available network resources due to the additive effect of multiple streams. One user making use of one stream may not be likely to cause a network problem, but 50 or 100 users employing an equal number of streams quickly begins saturating the network. Unlike packet-based tools that analyze individual pieces as they go by, flow analysis tools enable the identification of the source, destination, and protocol of streams across the network. The end result is the ability to craft effective network policies that enable streaming protocols where necessary while preventing those that negatively impact the functionality of the network.

A final area for which flow analysis tools are particularly well suited is during LAN and WAN optimization activities. In both the case of LANs and WANs, there occasionally comes the need to stand back from the network architecture and look for where improvements can be made. With the constraints of limited time and funding, these activities need to focus on solving the network's biggest problems first. Flow analysis tools, especially those with the ability to see historical traffic and usage patterns, deliver quantitative information to the network architect that allows them to make educated improvement decisions.

Focusing on the Right Features

To this point, this article has attempted to illustrate the differences between the vision gained through the use of flow analysis tools compared with others available to the network administrator. In much the same way that you don't measure the efficiency of interstate highway traffic by looking at the each vehicle's cargo, different network tools illuminate a different view of the network. The right tools include the right set of features for assisting with problem resolution and network management. When looking for products that fulfill your needs for flow analysis, consider those that include


- *Multiple vendor and protocol support.* Although the term *NetFlow monitoring* is often used to describe the kinds of flow analysis activities discussed here, NetFlow is only one of many protocols available on network devices today. An effective flow analysis tool will include the support for all currently available forms of network flow analysis irrespective of vendor (jFlow, sFlow, IPFIX, etc.). This ensures that your environment is not later forced into using network devices of a single manufacturer down the road.
- *Real-time and historical analysis capabilities.* Although most problems in network administration directly relate to how the network operates *right now*, the only effective way to ascertain today's behaviors is to view them in comparison with yesterday's or last week's. Effective flow analysis requires the capability to store and later review statistics over an extended period of time. This ability enables the network administrator to identify long-term traffic patterns and plan for growth.
- *Visualizations accessible from anywhere.* As a network administrator, you're not always sitting in your office. Problems and issues tend to pop up all across the network, some of which require on-site support. In these cases, having visualizations that can be accessed from anywhere—for example, using a standard Web browser—gives you the ability to take your toolset to wherever the problem exists.
- *Drill-down support.* With drill-down support built-in to flow analyzer's visualizations, it is possible to quickly move from the highest-level view down into specific problems as needed. Drill-down support reduces on-screen clutter, enabling a single-glimpse and high-level view of the network during periods of nominal activity.
- *Affordability.* Lastly, any toolset used in troubleshooting and resolving network issues must cost less than the amount of benefit it provides. Expensive solutions take longer to pay for themselves and may be more difficult to obtain in a time of shrinking IT budgets. Finding the tool that meets your needs at an acceptable cost is important to gaining the biggest return on your investment.

Looking Forward

The second article of this series will delve specifically into one difficult topic for many network administrators—namely, isolating the source of problems between the network and its hosted applications. As you'll find, the flow analysis capabilities discussed in this article are one of many tools used by troubleshooting administrators in determining the source of the problem.

Article 2: Isolating Network vs. Application Problems

“The network is slow today” is without a doubt one of the most disliked phrases heard by network administrators. The network has become a dumping ground for problems that originate as often as not from servers and applications as from the network. Thus, one of the biggest jobs of the network administrator is to defend their network from being labeled the cause of today’s problem. Because slow environment performance is often first—and often incorrectly—attributed to the network, rapid triage and problem isolation is critical to the administrator’s workload.

 In the case of this author, the story of the “blame game” between network and applications is no better told than at a previous employer. There, an actual scoreboard was set up in one of the IT offices. On one side was labeled “*It is the network.*” On the other was “*It is the server.*” Over time, assigning points to one or the other column became a regular last step in problem resolution. Examples like this are prevalent in IT environments everywhere. They foster a competitive team spirit amongst members of IT while encouraging everyone to make sure their team wasn’t the culprit.


All things being equal, problems in the IT environment occur just as regularly within its applications as within the network itself. Often, impact from network conditions combines with application behaviors to manifest into the problem of the day. Because of this, it is critical to avoid technology and monitoring silos between IT teams. When the network team can view performance and other information related to servers and applications, they can apply their network-based troubleshooting knowledge to a resolution. Conversely, when server and application teams have the ability to peer into network statistics, they gain the ability to relate what they see and know within their domains.

Common Problems in IT

The best way to illustrate the need for cross-team problem identification is through a series of examples. Tools available to network administrators today have the ability to pierce the long-standing divide between “the network” and “the application,” giving the troubleshooting administrator a more-complete set of data to work with.

As a first example, one common problem occurs when network performance itself is the source of the IT problem. In this case, the tick mark goes into the “*It is the network*” column. For situations like these, the first sign of trouble often arrives when users experience slowdowns in application performance. Here, calls to the service desk fill out a picture that email traffic or working with files is not performing to usual standards. In this case, the server or application team may be the first group to be contacted to resolve the problem. If that team can rely on only performance counters native to the systems and applications themselves, they are not likely to find the problem’s resolution on their own. Instead, should they have access to see easy-to-understand traffic flow analysis data from the network side, they may be able to quickly isolate the problem to the network domain. Resolution may not be within their skill set, but general knowledge combined with heads-up visualizations gives them the information they need to redirect the issue to those that can.

A second example is the case in which the network is performing to specifications but an application or database residing on top of that network is experiencing problems. In this case, either team may be dispatched to isolate and resolve the problem. Either team has their domain-specific set of tools at hand to triage the problem—for example, WMI for Windows systems and applications, SNMP for network devices, and so on. Yet due to the complexity of the problem neither group of tools alone can sufficiently come to a resolution. Only through the combination of network statistics alongside those sourcing from servers and applications can a resolution be found. On the network side, that resolution may start with traffic flow analysis, followed by a deeper packet inspection to identify that perhaps the conversation itself between application client and server is the ultimate source of the problem.

 When the network, server, and application teams all view a common monitoring interface, they gain a greater ability to share information, see the problems and issues that relate to other teams, and work together more effectively. For this reason, today's best-in-class monitoring platforms are not limited to monitoring network components exclusively. Instead, they aggregate the best data from all sources to gain an overall picture of the IT environment.

Common Ways to “Tell the Difference”

Most often, simply identifying the source of the problem takes 80% of the time required to fix it. Thus, leveraging tools that speed the problem identification process greatly improves the efficiency of IT. Narrowing the possible options to one or more problem domains means that the most appropriate IT personnel can be assigned to its resolution.

Considering the previous examples, it can be argued that more data is generally preferred to less when troubleshooting IT problems. When network teams have the ability to pull system-based or application-based information, they gain a better vision of the overall IT environment. Yet the quality of that data is important as well. Not all types of monitoring are useful for troubleshooting all problems. To maximize the information available for troubleshooting administrators, an effective network monitoring tool should include some or all of the classes of monitoring explored in the following sections.

Network Device Metrics Collection

Network device metrics provide information about the system resources on each individual device. These metrics are critical in ascertaining whether a resource overuse problem is a central cause of a reduction in performance. Collecting and reporting on network devices helps the troubleshooting administrator quickly identify whether the device is a source of the problem or the problem lies within the network traffic or application communication itself. Virtually all network monitoring tools include the ability to gather and report on these statistics, most commonly through SNMP.

Server Metrics Collection

Essentially all network monitoring products include the ability to look at network device counters, but not all have the ability to do the same with servers that reside on that network. Although the technology for pulling these metrics has been available for many years, the long-held organizational boundaries between “network” and “server” responsibilities have resulted in these metrics not being gathered by many monitoring products. Yet, as discussed earlier, there is value to IT in aggregating server- and application-based metrics with network device metrics. Network administrators gain the ability to view the impact of network conditions on servers and applications, while server administrators can easily see how their applications are affecting the network.

Application Status and Event Collection

Server metrics illuminate one part of the picture, but their performance-focused information is not complete without the additional detail gained through application status and event collection. Capturing status information—up or down—of applications helps IT teams identify when servers and the network are up but their residing applications are not. Lacking this detailed level of information, it is difficult for troubleshooting teams to quickly isolate the cause of a problem. For example, a server may be operational and responding to a low-level ping request, but its residing application may no longer be functioning. Including this detailed information alongside traditional metrics enables teams to quickly isolate the problem and proceed to a resolution.

Transaction Timing Measurements

Even with the information gathered using the previously mentioned methods, there remains a class of problems that are still difficult to identify. These problems occur when the user’s experience degrades, but does so in ways that are difficult for traditional metrics to capture. Consider the situation in which a user is working with a Web-based application that involves multiple servers. A problem within that multi-server system may manifest as a significant slowdown to the user but not impact system counters, application availability, or even result in the creation of a log event. However, the user is experiencing a legitimate problem with the system.

In this case, the most effective way to measure the user’s experience is through the measurement of network transactions between the elements of that system. Transaction measurements provide a way to determine when and where the user is experiencing delays in their interaction with the system. Analyzing transaction timing over an extended period of time provides a way to determine how the application is responding in comparison with previous measurements. Transaction measurements are sometimes augmented with the ability to submit synthetic or “test” transactions to the application as a way to measure timing against a known result.

Alerting and Notification

A common feature in almost all network monitoring platforms, alerting and notification capabilities are necessary to warn administrators when conditions change in the IT environment. Although alerting features are common, there are major differences between products in the level of detail in alerts as well as granularity in administrator targeting. Effective network monitoring tools enable the ability for rich targeting of administrators based on the type and source of problems. Also important are the mediums supported for alert submission, with better products including support for more and different alerting mediums.

Important also is the data sent to the administrator as part of the alert. Inefficient monitoring solutions alert administrators regarding changes in environmental status. Without the right level of tuning, administrators can be overloaded with alerts as situations occur. The right monitoring solution will alert administrators in real-time with actionable information regarding the situation, while reducing alerts to the minimum necessary.

Auto-Remediation

In mature environments where the configurations are well known, effective documentation and workflows are in place, and the environment is properly baselined, a good monitoring solution can enhance the problem resolution process by solving known problems automatically. Auto-remediation is the process whereby known problems are resolved automatically as they occur. Examples of problems that work well with auto-remediation are network services that require restarting, devices that require resetting, or even the full repopulation of config files in the case of outages. Auto-remediation activities require a network monitoring solution that is aware of environment conditions and has the logic in place to complete an action when a predetermined condition occurs.

Isolating Problems Requires the Work of All IT Teams

The traditional boundaries between what was considered the purview of the “network team” and the “applications team” are steadily blurring. With applications spanning multiple servers in multiple network locations, determining the source of IT problems whether network or application requires the cooperation of both groups of people. As the complexity of the IT environment grows over time, teams must work together to resolve issues as they occur.

A critical assistance to this task is the aggregation of otherwise siloed monitoring needs into a centralized network monitoring solution that is accessible by everyone. Through the process of integrating data from the network and applications halves, both teams gain the necessary information they need to do their jobs effectively.

That process of doing one’s job effectively is important. Article 3 in this series will talk about the five configuration management tasks commonly handed to network administrators. That article will discuss not only the tasks but also tools that make the completion of those tasks much easier.

Article 3: Automating the Top 5 Network Tasks with Configuration Management

In the world of the harried network administrator, there are far too many tasks that involve manual intervention. Updating router configs, changing parameters on switches, and maintaining documentation of the environment all require one or more manual steps to accomplish. With only a few network devices in the environment, the manual steps required to keep them operational might not add up to much. But as your environment grows, so do the sheer number of elements that must be correctly managed.

Exacerbating this problem even more is the knowledge that between 60 and 80% of all network issues relate to device misconfiguration. Using CLI tools might display your prowess with your network device's command-line IOS, but relying solely on that functionality for all forms of management is likely causing you more work all the while adding an operational cost associated with the occasional mistake.

For many network administrators, the next step in automating their responsibilities often starts with the creation of homegrown scripts. These scripts enable the administrator to quickly update running configs or query devices for information. But in the case of a job change, homegrown scripts rarely outlast the administrator. When your environment is bandaged together with scores of homegrown scripts that only you truly understand, your departure from your job is likely to also be the end of your attempts at automation.

Management tools are available today that assist with these problems. These tools automate many of the highly manual activities of the network administrator, significantly reducing or eliminating the possibility of error while ensuring that device configurations remain correct. There are a number of improvements to a network administrator's operational workflow associated with doing configuration changes through a centralized tool:

- *Reduction of error-prone text manipulation.* The tried-and-true method for updating network device configurations has long been manual through the command line. Adding lines to a device's configuration file through the command line appears easy and requires little more than the knowledge of the proper command and a remote access utility. However, text-based configurations tend to be highly error-prone. With dozens or hundreds of lines of code scrolling by and even the smallest error potentially having a major impact on functionality, it is easy to see how a segregated tool with database storage and offline manipulation goes far in preventing errors.
- *Eliminates the idiosyncrasies of Telnet/SSH.* Most remote console applications that connect to network devices are designed specifically for command-line access and online config manipulation. However, Telnet, SSH, or other protocols commonly used suffer from usability limitations. Scrolling down may be interactively possible, while scrolling up may only be possible by reading back through the tool's command buffer. If you need to look at one part of a configuration while editing another, multiple connections are usually required. The idiosyncrasies of these tools as well as the complex language of network device configurations make them a challenging learning curve for new administrators.

-
- *Supportability.* It is likely that your network environment is not entirely homogeneous. Network devices from multiple vendors may have different and completely separated mechanisms for configuration. One device's Web-based configuration may require a completely different set of skills than another's command line-based configuration. Leveraging a centralized network configuration management tool gives you a single place to call when problems occur.

Configuration Management's Top 5 Tasks

There are a lot of administrative challenges that can be overcome by moving away from native interfaces towards a common toolset for network configuration management. In this section, we'll look at five of the top tasks that are commonly assigned to the network administrator and how centralized configuration management toolsets enhance the ability to get the job done. For each, you'll find that the move to centralized configuration management also brings about great levels of automation. With the right toolsets and techniques in place, managing five network devices involves the same processes as managing five hundred.

Config Backups

Network devices are unique in IT in that their configurations are typically stored in a text-based format irrespective of the type of device. Working with and managing change within that format is a large part of the learning curve associated with being a network administrator. With essentially all settings being contained within individual text files, the process to back up a device's configuration is as simple as a file copy. Migrating one device's settings to another involves copying a set of files from the old device to the new.

Although the file format itself is easy to work with, the processes by which files are transferred and ultimately backed up off individual devices is less intuitive. With the majority of file-based storage in an IT environment usually being hosted atop Windows servers, the process of simply getting backups to a storage location can be cumbersome. Even more difficult are the necessary scheduled tasks that back up those devices on a regular schedule.

Needed to resolve this inadequacy with native tools is a segregated, centralized configuration management solution that works across all devices and device classes. Once connected to a centralized configuration management server, virtually every function of a network device can then be managed from the server itself. This includes setting up and managing regular device backups, monitoring their success or failure, and later restoring config files to devices in the case of a failure.

Change Documentation and Audit Trails

In an environment in which security needs and compliance regulations mandate the logging of all user and administrator activity, knowing “who did what” is a critical component of a secure IT environment. Network devices have historically enjoyed fairly limited access by IT personnel. Relatively few IT staff members are usually granted access to view and manipulate device configurations. Because of this, the capabilities associated with administrator activity logging at the individual device level have been relatively undeveloped.

Security and regulatory requirements along with the desire to track which administrator made which change drive the need for a greater level of logging. That logging must include at a minimum the administrator who logged in; the time, date, and location of access; and detailed information about the individual configuration change completed. This data also assists with the troubleshooting process in the case where a misconfiguration causes a problem. By identifying the changes made immediately prior to a failure, it is possible to quickly back out those changes to return the environment to normal. An effective configuration management solution will provide audit trails for every activity made by an individual within the system. Particularly effective ones will provide mechanisms for alerting administrators when changes are made.

Implementing Mass Changes

If an issue or a problem in the IT environment requires the update of a router configuration for resolution, making and testing that change requires only a short amount of time. But if the resolution to that issue or problem requires updating configurations on dozens or hundreds of routers, the manual update process could take hours or days. Repeating that update across hundreds of devices also introduces the potential for error, which exacerbates the problem rather than assists.

Centralized configuration management tools are by definition automation enablers. They provide a way to incorporate a change across multiple devices all at once. Effective centralized configuration management tools usually incorporate a database of device configurations taken from the last round of backups. This database houses the actual configurations of all devices across the enterprise. Making a mass change across each of those devices when their configuration is known and stored in a local format enables a mechanism by which the administrator can update every device at once.

This capability grows even more valuable when integrated with fault or performance management features intrinsic to the configuration management tool. Consider the situation where a device misconfiguration trips an alert based on a fault or performance issue. Within the same tool, the network administrator can quickly identify the location of the fault, drill down into the specific configuration problem to find a solution, and push that update to all affected devices. Each of these activities occurs without the need to directly log in and manipulate a single network device.

Identifying Inappropriate Configurations

With large or even moderate numbers of devices in service within an IT environment, it is likely that each device will have specific customizations that are unique to the device. One device will allow certain traffic while another is configured to prevent it. One set of devices is set to route in a particular direction while another set routes in a completely different way. Defining and managing these configurations is one of the biggest tasks of the network administrator.

But even across dozens or hundreds of unique configurations, there are elements of similarity. Each configuration has portions that correspond to the device's configuration template. Finding deviations in those portions and comparing the configuration of one device to another is challenging using native tools. As discussed previously, trying to line up two configuration files in two remote console windows is a painful process at best.

Good configuration management toolsets provide mechanisms by which config file differences between devices can be highlighted for review by an administrator. These differences provide a visual mechanism for the administrator to seek out and fix problems or incorrect configurations. Best-in-class configuration management solutions integrate fault and performance management capabilities into the same toolset. This integration enables a direct linkage between problem occurrence, administrator notification, and suggested resolution.

Network Problem Notification and Remediation

This integration between configuration management and fault and performance management is key to maintaining the highest levels of network uptime. The monitoring and database storage of real-time performance statistics ensures that today's performance is at least as good as yesterday's. Changes in performance can be traced over periods of time and against known configuration changes to identify the problem's source. Fault identification and alerting immediately alerts administrators when devices, services, or even network applications stop responding. And since the system that alerted on the fault is the same that is used to resolve it, that interface can quickly lead the troubleshooting administrator to a suggested resolution.

From Highly Manual to Highly Automated

The right configuration management tools in the hands of network administrators give them the integrated interface they require to best serve the needs of business. Implementing such a system for use by network administrators eliminates the need for manual update tasks and administrator-specific homegrown scripts. With a database-driven backend, automated actions directly initiated from the tool itself, a rich interface for making and applying configuration changes across the board, and granular notifications and alerts, an effective network configuration management solution is a must-have for the proactive IT environment.