Is your Network Management System giving you the complete picture?

6 key considerations to avoid inherent shortcomings and potential risk

Our thanks for Fluke Networks for allowing us to reprint the following article.

IT professionals today are overwhelmed and understaffed. Although network engineers rely heavily on Network Management Systems (NMS), these systems fail to deliver a complete picture of network and application performance…and that puts the organization at risk. Being aware of the potential shortcomings of an incomplete NMS is essential. Knowing how to counter those shortcomings is the next step. This whitepaper will spell out three common shortcomings, the possible consequences, and six key capabilities to be aware of when evaluating your network management tools and processes in order to avoid these shortcomings and associated risks.

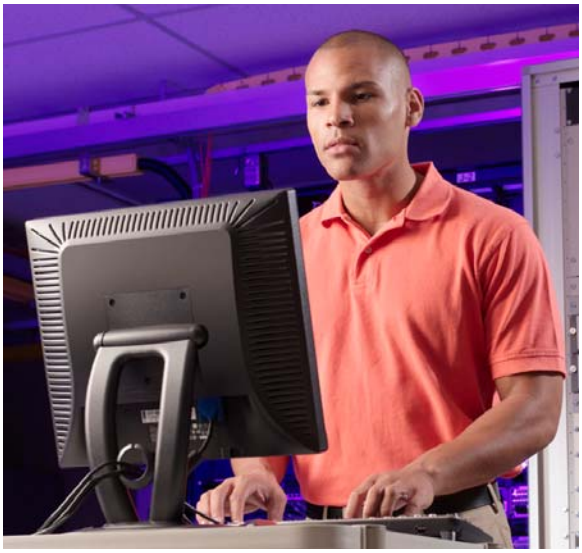
Introduction: Trying to Be Proactive in a Reactive World

The hectic world of network engineers is one of constant struggles. They're routinely dealing with information overload, application performance and bandwidth issues, and the policing of networks and usage. Their days are crowded with alerts sounding around the clock. They face ever more end users, devices and applications to service but with fewer coworkers to share the load.

Ideally, network engineers would have sufficient time and the proper tools to effectively manage daily operations – manage changes, ensure the network and applications are performing optimally and quickly resolve problems when they occur. But because of staffing or workload issues, and shortcomings in their tools, they are stuck in reactive mode and cannot get ahead of the jobs at hand enough to proactively manage the network.

Many IT professionals rely heavily on a Network Management System (NMS) to be proactive on their behalf by monitoring devices for availability and performance, and notify them when issues arise. Information from the system is then used to investigate and solve problems.

In theory, this should work. In reality, Network Management Systems perform well for monitoring availability and some performance metrics, but have limitations caused by their architecture and technologies used. These limitations result in insufficient monitoring of true network and application performance, and in a failure to provide the visibility needed to identify and analyze many network and application performance problems.



Common NMS Shortcomings

Network Management Systems are well-suited for certain aspects of network management, such as fault and configuration management, asset management, and monitoring of certain metrics to gauge the overall health of the network. NMS come in many flavors, from simple ping tools offering limited views to complex, enterprise-wide systems that offer more visibility but also require dedicated staff to maintain. Regardless of the size or complexity of the NMS, when it comes to managing performance or solving problems, there are three critical shortcomings to be aware of:

Lack of proper perspective – the user's point of view

Typical Network Management Systems are based on centralized monitoring. But when an organization only monitors from a central location, no one sees performance from the users' perspective. Performance needs to be analyzed across a broader view, one that measures from multiple points in the network including remote sites as well as the users' point of view. For example, if a user reports performance problems with a web application, the engineer can use the NMS to triage the

problem by testing from the NMS to the user and from the NMS to the server, but a key link is missing: testing from the user or remote site to the server – a shortcoming of centralized monitoring. Measuring end user experience means measuring performance from the user point of view. Without this perspective, network managers get an incomplete view of the state of the network.

A false sense of security – availability is not performance
A ping/port test will indicate what devices are "up" but not whether they are performing optimally. These "red light/green light" indicators give a false sense of network performance. Network Management Systems often fail to monitor and analyze true network and application performance because they rely on measuring the performance of substitute protocols (such as ping) as proxies for actual application traffic. Proxies are not sufficient indicators of how applications are really performing for users across a distributed network.

Lack of troubleshooting and in-depth analysis - "on-the-wire" visibility
With an NMS, network engineers do not have enough visibility to solve performance problems. They do not see the actual traffic on the network, just statistics and symptoms. They lack the depth of visibility and detail required to find the root cause of performance problems. They cannot see actual traffic on-the-wire, (or "in-the-air" in the case of WLANs) to see how an application is responding and behaving…or not. Without on-the-wire visibility, an engineer will never see how an application is behaving. And that means more reactive behavior, responding when a user reports a problem rather than proactively finding the problem before the users even notices it.

The risks inherent with network management systems

With these three shortcomings, a Network Management System shows only part of the performance picture. Having an incomplete view of performance issues puts an organization at risk in several ways, all of them costly.

When problems aren't identified and dealt with promptly, **productivity is impacted**. The workforce gets bogged down when the network or applications are either slow or unavailable. This has a direct impact on the bottom line. The cost of downtime is different for every organization, but there is one commonality: downtime always costs money.

Lack of troubleshooting ability means it takes that **much longer to resolve network problems.** Network engineers are hindered when they can't quickly identify and isolate the problem domain—server or client, application or network—again, negatively impacting the bottom line with downtime. Network engineers also must be able to identify the severity of any problems, and the impact on users and resources, so they can prioritize their heavy workloads, dealing with the most critical issues first.

Lack of insight into the true health of the network can also lead to **ill-informed investment decisions.** Organizations are prone to spend money on unnecessary infrastructure improvements, blaming "bandwidth issues", when the IT staff is unable to truly understand network usage and needs.

Six key capabilities to consider when evaluating your network and application performance tools and processes

Network Management Systems tend to focus on availability and uptime, not efficiency and performance. To get and stay proactive, network engineers require the ability to conduct in-depth daily performance monitoring and root cause analysis of key network devices, links and applications anywhere on the network. Unless it enables a shift in focus from tactical (reacting) to strategic (proactive), over-reliance on a Network Management System could very well turn into a liability for an organization based on the inherent risks.

Below are six key capabilities to consider when evaluating whether your Network Management System tools and processes are providing a complete picture:

1. **Complete network visibility**
   Network managers require complete network visibility, meaning the right information at the right level of detail about every aspect of the network, particularly its true performance. It is important to employ solutions that provide visibility from multiple points in the network, including remote sites and critical points in the network that give the perspective of the end user, combined with "on the wire" and "in the air" diagnostics to see actual traffic on both wired and wireless networks.

2. **Sustained monitoring for early warning on true performance metrics**
   Transforming an organization from reactive to proactive requires monitoring on a constant, sustained basis for fault and failure situations, but also for true performance monitoring, especially at the service and application layers, not just monitoring of proxy protocols. Consistent monitoring of critical network paths and actual application transactions, provides valuable insight into "normal" network and application behaviors. Long term comparative trending allows network engineers to rapidly

identify actual issues, rather than anomalous events.

3. **Intelligence and automation**
   Using tools with built-in knowledge bases is one of the best ways to improve efficiency and effectiveness. These tools typically take the form of "expert" or "advisory" features that can look at patterns of information, present network engineers with likely source scenarios, and recommended courses of action. For example, packet analysis experts look at traces of network packets then apply rules and heuristics to find potential protocol mismatches or application design issues.

4. **Means and methods for easy collaboration**
   Data is more useful when shared. Sharing happens when tools facilitate reporting and collaboration across multiple groups within an organization via web-based reporting. A web-based portal enables multiple people to have visibility into the network, and is useful for defending the network when necessary, and for collaboration between IT staff when dealing with an issue.

5. **Ease of deployment, quick time to value and minimal maintenance**
   Some systems take days or even weeks to configure, some an hour, and some a few minutes. When evaluating an NMS, consider the time to deploy and maintain it. The more time it takes to configure and maintain a system, the less time staff has for monitoring and troubleshooting the network, keeping applications performing and users productive. Also consider the costs of customization or additional services, as well as the learning curves of both the operator and management teams. If an NMS takes a long time to install, configure and learn, then requires dedicated staff to maintain the system, the slower the ROI.

6. **Consolidation to "cut the clutter"**
   When using many different management tools, the licensing, maintenance, training and interoperability (or lack thereof) can add up to major resource and efficiency drains. Tools should cover multiple functions wherever possible.

Conclusion

If an organization relies solely on a typical Network Management System, it will not get the complete picture, no matter how much staff and resources are committed to network management. The only way to overcome a lack of proper perspective, the false sense of security, and insufficient troubleshooting and in-depth analysis capability is to equip staff with a network and application monitoring and analysis solution that provides the right views and measurements to ensure performance. This enables engineers and managers to be proactive and strategic.

Being mindful of the shortcomings and risks, and evaluating your solution in light of the six key capabilities outlined above, will enable an organization to make investments that increase the dependability and performance of their networks and applications, while decreasing the risk of downtime and inefficiency.

OptiView Management Suite (OMS): The complete picture for monitoring, analysis and troubleshooting

OMS provides the breadth of visibility and depth of analysis for a complete picture of network and application performance. It's the only solution that combines proactive monitoring with in-depth "on-the-wire" analysis and portability to see problems up close - anywhere on the network.

Unlike other Network Management Systems, OMS shows you:

- Overall network health: key devices and applications for performance, not just availability
- End-user perspective: measure performance to and from users, critical links, virtual environments and remote sites
- Problems up close: portability allows you to see problems anywhere in the network -- whether wired or wireless
- On-the-wire packet analysis: visibility of packet-level details to quickly troubleshoot application behavior and response time issues

OMS can be used as a holistic management suite or part of your IT organization's toolset, to help reduce complexity and improve productivity in your team's daily workflow of monitoring, analysis and troubleshooting.

For more information, visit www.flukenetworks.com/oms

FLUKE networks

1547 N. Trooper Road • P. O. Box 1117 • Worcester, PA 19490-1117 USA
Corporate Phone: 610-825-4990 • Sales: 800-832-4866 or 610-941-2400
Fax: 800-854-8665 or 610-828-5623 • Web: www.techni-tool.com