



THE VALUE OF NETWORK MONITORING

Why It's Essential to Know Your Network

Sponsored by Ipswitch

I. INTRODUCTION

All companies are different, but the value of their network to their business varies little. In fact, as a business grows, its network grows not only in size and complexity, but also in significance and value. Very quickly, the network not only supports the company, it *is* the company. This is obvious for e-businesses and other entities that are highly dependent on their website for driving revenues. Yet at its most basic and strategic level, the network is about collaboration, communication, and commerce – everything that keeps a business running and growing. It's where business applications are hosted, and where mission-critical customer, product, and business information are stored.

With a resource this valuable, ensuring its availability is essential. It's also challenging because of threats such as hackers, denial of service attacks, viruses, and information theft, all of which can lead to downtime, loss of data, and overall decreasing credibility and profitability. Additionally, the network is evolving drastically, with new technologies, devices, and strategies, such as virtualization and service-oriented architectures. That's why network management is such an important function and capability for businesses of all sizes. If your business depends on your network, then network management is critical.

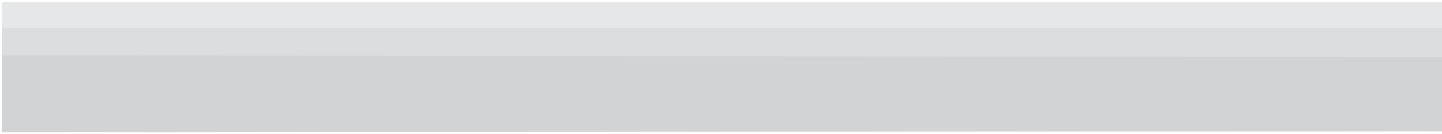
Network management is a broad functional area incorporating device monitoring, application management, security, ongoing maintenance, service levels, troubleshooting, planning, and other tasks – ideally all coordinated and overseen by an experienced and reliable network administrator. Yet even the most knowledgeable and capable network administrator is only as good as the network information that is visible, and that he or she can manage and act on. Administrators need to know what's happening on their networks at all times, including real-time and historical information on usage, performance, and status of every device, application, and all data on the network.

This is the domain of network monitoring, the most critical function of network management. The only way to know if everything on your network is operating as it should is to monitor it continuously. This paper describes the importance of network monitoring in maintaining the availability of an organization's network, with a goal of enabling readers to make informed decisions.

II. KNOW YOUR NETWORK

Today's networks can be astounding in their complexity. Routers, switches, and hubs link the multitude of workstations to critical applications on myriad servers and to the Internet. In addition, there are numerous security and communications utilities and applications installed, including firewalls, virtual private networks (VPNs), and spam and virus filters. These technologies span all verticals and companies of all sizes. Network management, therefore, is not confined to only certain industries or solely to large, public companies.

Understanding the composition and complexity of your network, and having the capacity to be informed of how all the individual elements are performing at any given time, is a key success factor in maintaining the performance and



integrity of the network – and often of the business – as a whole. There are potentially thousands of data points to monitor on a network, and it is critical to be able to access meaningful, accurate, and current information at any given time. Network administrators need to feel confident that they know what’s happening on their network from end to end at any given point in time. It is critical to “know your network” at all times.

A network is no longer a monolithic structure. It includes the Internet, local area networks (LANs), wide area networks (WANs), virtual LANS (VLANS), wireless networks, and all of the devices, servers, and applications that run on them. Whatever enables users to access and share information, utilize applications, and communicate with each other and with the outside world – either through voice, data, or images – is, in essence, your network.

A network typically has both internal and external users, including employees, customers, partners, and other stakeholders. Suboptimal network performance affects companies in different ways, depending on the type of user. For example, if employees can’t access the applications and information they need to do their jobs, it means lost productivity and missed deadlines. When customers can’t complete transactions online, it means lost revenues and damaged reputation. And when strategic partners can’t collaborate or communicate with the company, it harms the relationship and affects their bottom line. Even stakeholders such as investors and analysts who can’t get the information they need when they need it will also look unfavorably at your company, leading to lower stock prices and loss of shareholder value.

The fact is, though, that networks are so complex that something will go wrong. Every component in the network represents a potential point of failure. That’s why it’s essential to implement redundancy and/or a failover strategy in order to minimize downtime. This way, if a server or router fails, another one waiting idly until needed can automatically come online to mitigate the impact of the failed equipment.

Of course, not every problem can be addressed quite so proactively before any warning signs are apparent. However, if you can monitor network performance proactively in real time, you can identify problems before they become emergencies. An overloaded server, for example, can be replaced before it crashes – but only if you know that its utilization rate is increasing to such an extent that a crash is all but imminent. With network monitoring, you should know the status of everything on your network without having to watch it personally, and be able to take the timely action needed to minimize and, when necessary, quickly correct problems.

III. WHAT TO MONITOR AND WHY

For something as mission-critical as your network, it’s important to have the right information at the right time. Of primary importance is to capture status information about current network devices (e.g., routers and switches) and critical network servers. A network administrator also needs to know that essential services (e.g., email, website, and file transfer services) are consistently available.

The following table contains a representative list of some of the key types of network status information you need to know every minute of every day – and why.

| WHAT TO MONITOR | WHY TO MONITOR |
|--|---|
| Availability of network devices (such as switches, routers, servers, etc.). | The “plumbing” of a network keeps the network running. |
| Availability of all critical services on your network. | The whole network doesn’t have to be down to have a negative impact; loss of email, HTTP, or FTP server availability for even just one hour can shut a business down. |
| Amount of disk space in use on your key servers. | Applications require disk capacity. It’s also important to be aware of any anomalous behavior in disk capacity, which can indicate a problem with a specific application or system. |
| Percentage of your routers’ maximum throughput utilized on average. | If you anticipate when you need to upgrade before you feel the pain of needing to upgrade, you’ll minimize disruption to your business. |
| Average memory and processor utilization of your key CPUs/servers. | If you wait until memory is used up, users will never let you forget it. |
| Function of firewalls, antivirus protection, update servers, and spyware/malware defenses. | There’s a difference between having security, and having security that’s working. |
| Amount of traffic coming in and out of routers. | The better you can identify peak periods and maximum throughput, the better you can plan for optimal performance at all times. |
| Availability of all network devices. | Most networks are a combination of heterogeneous devices; you need to be able to monitor Windows, Linux, UNIX, and other types of servers, workstations, and printers. |
| Events written to logs, such as WinEvent or Syslog. | By taking advantage of messages written to event logs, you can gain direct knowledge of events and conditions throughout the network. |
| SNMP traps, such as printer information or temperature probes in server rooms. | You can learn when printers are malfunctioning or need toner even before users notice, and ensure that your servers don’t overheat. It’s important to note that these are just two examples of unique attributes that your network monitoring solution should be able to handle. |
| Windows application and servers. | Most network environments include Windows applications running on Windows servers. While not every network monitoring solution currently supports WMI, Ipswitch’s WhatsUp Gold Premium solution monitors SQL Server and Exchange out of the box, and can be customized to track attributes of other Windows applications through the use of customer-configured WMI monitors. |

When there are issues, you should be alerted immediately, either through audio alerts, on-screen displays, or emails automatically generated by the network monitoring solution. The sooner you know what is going on – and the more complete the information included with the alert – the sooner you can take corrective action. Alerts should announce not only when a problem has occurred (or a threshold is being approached), but also whenever a new application or piece of equipment is brought online. They should contain information about the device, the issue, and the event that triggered the notification.

At the same time, it's important to generate only meaningful alerts and to minimize the number of alerts stemming from the same problem or event on the network. For example, you want the flexibility to configure the monitoring solution so that it doesn't alert when scheduled maintenance downtime is initiated. And if availability to many devices is constrained because of a problem with a router or switch, eliminating dependent alerts enables the administrator to more effectively and efficiently diagnose the actual problem. Suppressing these dependencies decreases the information you have to assimilate and increases overall confidence in the alerts you do receive.

TOP TEN REASONS TO USE NETWORK MONITORING

- 1. Know what is happening.** Network monitoring solutions keep you informed about the operation and connectivity of your devices and resources on your network. Without these features, you have to wait until someone tells you something is down before you can fix it.
- 2. Plan for upgrades or changes.** If a device is constantly down, or the bandwidth to a specific subnet is constantly running near the limit, it may be time to make a change. Network monitoring applications allow you to track this type of data and make appropriate changes with ease.
- 3. Diagnose problems quickly.** One of your servers is unreachable from the intranet. Unfortunately, without network monitoring, you may not be able to tell if the problem is the server, the switch the server is connected to, or the router. Knowing exactly where the problem is saves you time.
- 4. Show others what is going on.** Graphical reports go a long way in explaining the health of and activity on your network. They're great tools in proving an SLA or showing that a troublesome device needs replacing.
- 5. Know when to apply your disaster-recovery solutions.** With enough warning, you can transfer the operation of important servers to a backup system until the primary system can be repaired and brought back online. Without network monitoring, you may not know there is a problem until it is too late.
- 6. Make sure your security systems are operating properly.** Companies spend a lot of money on security software and hardware. Without a network monitoring solution, how can you be sure that your security devices are up and running as configured?
- 7. Keep track of your customer-facing resources.** Many devices on your network are really just applications running on a server (HTTP, FTP, mail, and so on). Network monitoring can watch these applications and make sure your customers can connect to the servers and are seeing what they need to see.
- 8. Be informed of your network status from anywhere.** Many network monitoring applications provide remote viewing and management from anywhere with an Internet connection. That way, if you're on vacation and problem crops up, you can log into your Web interface and see what's wrong.
- 9. Ensure customer uptime.** If you have customers depending on your network for their business, you have to be sure they're up and running at all times. Would you rather know the moment a problem occurs and fix it before your customer finds out, or get that angry phone call?
- 10. Save money!** Above all, network monitoring helps you cut down on the total amount of downtime and time it takes to investigate problems. This translates to fewer man-hours and less money when problems occur.

From Ipswitch Network Monitoring for Dummies, by Robert Armstrong, Wiley Publishing, Inc., 2007.

IV. WHAT TO LOOK FOR IN A NETWORK MONITORING APPLICATION

To really know your network, you need a network monitoring solution that can tell you what you need to know – in real time and from anywhere, anytime.

For businesses of all sizes, you also need a solution that's easy to use, quick to deploy, and offers low total cost of ownership – yet also delivers all the features you need. You need a solution with comprehensive capabilities and the same reliability you expect from your network. If you want your network running at high availability, you need a proven solution that you can depend on as well.

Remember, you're monitoring a lot of network components and you're collecting a lot of information. In order to see things clearly and quickly, you need a solution that displays this data – including a network map, report data, alerts, historical information, problem areas, and other useful information – as a network operating center (NOC) dashboard. Aside from making troubleshooting easier, this will help you to leverage historical network data to understand trends in device usage, network usage, and overall network capacity to enable more accurate and effective network design and planning.

As discussed earlier, alerts are important. However, they are like alarm clocks – you want them to go off when you need them to, not when you don't. For example, just as you don't want your alarm to go off on Saturday morning, you don't want your network monitoring solution to alert you during planned service periods. You want to be able to program your weekly maintenance schedule into the system so it can distinguish between planned and unplanned downtime. In other words, no false alarms.

Networks have to run 24/7 regardless of what hours your employees work. And while your network generally stays in one location, your employees sometimes travel. Regardless, you need to be able to access your network monitoring solution anywhere, anytime. For that matter, different people will need to access the system for different reasons, and not everyone should be able to access the same level of information. You need a solution that affords role-based views, that assigns levels of permissions based on the user's function in the organization. This not only makes the user more productive, it also adds an important layer of security around the information.

Finally, you should look for a solution that supports multiple methods of monitoring devices. SNMP (Simple Network Management Protocol) is a flexible technology that lets you manage and monitor network performance devices, troubleshoot problems, and better prepare for future network growth. Many network devices support SNMP, making it easy to monitor them using a solution that supports SNMP.

WMI (Windows Management Instrumentation) is a Microsoft standard for retrieving information from Windows applications. WMI comes installed by default on SQL Server, Exchange, and Windows 2000, 2003, Vista, and XP systems, so it's an important tool for monitoring network environments running Windows. Unfortunately, only a few network monitoring solutions currently include WMI monitoring among their capabilities.

CONCLUSION

Your network is your business. Network monitoring helps you to stay in business. The more you know your network, the more you can assure internal and external users that your network will be able to achieve performance and availability goals. Look for a solution that is easy to use but also full-featured. In particular, you want a solution that lets you see real-time status on a dashboard; enables secure, role-based, remote access to the system; has configurable alerts; offers full reporting features; and supports both SNMP and WMI.

IPSWITCH WHATSUP GOLD

Ipswitch WhatsUp® Gold delivers comprehensive and easy-to-use application and network monitoring that allows you to turn network data into actionable business information. By proactively monitoring all critical network devices and services, WhatsUp Gold reduces costly and frustrating downtime that can impact your business. With an all-new Web-based interface, WhatsUp Gold lets you take control of your network infrastructure and applications for the important strategic work that drives results. In a marketplace overwhelmed with complexity, WhatsUp Gold provides simple deployment, robust scalability, groundbreaking usability and fast return on investment.

WhatsUp Gold isolates network problems and provides awareness and understanding of network performance and availability. WhatsUp Gold:

- Discovers and maps all your network devices
- Notifies you when problems happen on the network
- Gathers network information over time and generates reports
- Provides anytime, anywhere network monitoring

In addition, WhatsUp Gold delivers all the tools you need to monitor and manage your network, including dynamic network discovery and mapping, fast problem resolution, and comprehensive SNMP and WMI network monitoring and reporting.

To learn more about WhatsUp Gold, please visit www.whatsupgold.com.

ABOUT IPSWITCH, INC.

Ipswitch develops and markets innovative IT software that is easy to learn and use. More than 100 million people worldwide use Ipswitch software to manage their networks with Ipswitch WhatsUp®, transfer files over the Internet using the market leading Ipswitch WS_FTP® Professional client and Ipswitch WS_FTP Server and communicate via Ipswitch IMail Server.

To view the Daily Network Monitor blog, visit www.dailynetworkmonitor.com.

For product and sales information, visit www.ipswitch.com.

Ipswitch values community involvement; to find out how to become involved, visit icare.ipswitch.com.

For more information about network management and how Ipswitch WhatsUp Gold delivers both ease of use and comprehensive capabilities in distributed environments, please contact us at:

IPSWITCH, INC.

10 Maguire Road Suite 220

Lexington, MA 02421

Phone: (781) 676-5700

Fax: (781) 676-5710

www.ipswitch.com