



# **NETWORK MANAGEMENT IN DISTRIBUTED ENVIRONMENTS**

---

Challenges and Opportunities for MSPs

## I. INTRODUCTION

As networks have grown in size and capabilities, they also have grown in terms of their importance to the organization. In many cases, the network – which encompasses the Internet, intranet sites, email, local area networks (LANs), wide area networks (WANs), virtual LANs (VLANs), and wireless networks – is the company. It's where applications and transactions are hosted; where internal and external users access, send, and share information; and where mission-critical customer, product, and business data are stored.

That's why it's so essential to ensure network availability and security. And it's hard enough to effectively manage a single network within a single organization 24/7, with complete transparency and the ability to track, respond to, and report on changes in performance and status over time. Consider, then, how the complexity grows exponentially in distributed customer environments with multiple LANs and WANs – and the same critical need for consistent performance.

This paper describes the challenges and opportunities that managed service providers (MSPs) face in the increasingly important area of network management. We will provide the basic requirements found in single-network environments, and contrast that with the more complex requirements of an MSP delivering network management services to a number of customers.

## II. BASIC NETWORK MANAGEMENT

To best understand the challenges and opportunities of network management in distributed environments, it is useful first to define the requirements and realities of single-site implementations.

In a corporate or institutional setting, the network is a complex, expansive, and dynamic asset. It runs 24/7, and is typically accessed by both internal and external users on a continuous basis. After all, websites never close and there always are users somewhere around the world who are sending emails and working on projects with the expectation that access is available regardless of time zone and location of assets. This means that the network must be monitored at all times, collecting information about performance levels, utilization, and operational status. That information must be stored and made available for analysis so that trends can be tracked and reports can be generated.

What gets managed? Everything. Routers, hubs, and switches. Workstations and other networked devices via Simple Network Management Protocol (SNMP) agents and Management Information Bases (MIBs). Windows applications via Windows Management Instrumentation (WMI) agents. Email. Databases and archives. Firewalls and spam and virus filters. Virtual private networks (VPNs) and virtual LANs (VLANs). If any of these items fail or is compromised in any way, it can lead to serious consequences. 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, frustrated users, and damaged reputation.
- When partners can't collaborate or communicate with the company, it harms the relationship and affects their bottom line.
- Security and privacy regulations make organizations liable for data breaches even when systems – like an email archive server – are down.

That said, networks are so complex and dynamic (in many virtualized and web-service based environments, network configuration changes occur frequently), that something is bound to go wrong. Network management can't prevent all troubles, but it can minimize loss of service and the impact of downtime. For example, when utilization rates increase, performance tends to suffer and the risk of a crash grows. If the network administrator can see that a certain threshold is being reached, corrective action can be taken to add more capacity and prevent a potential problem from becoming an all-out disaster. Or, if an alert indicates that a server has crashed, the administrator can bring a redundant one online quickly while restarting the service on the first.


Therefore, what is required in a single-network environment is a solution that can:

- “observe” the entire network and everything on it or connected to it
- provide the network administrator with a visual representation of the network to easily identify what is happening and where
- utilize rules to understand baseline status and thus be able to discover anomalous behavior
- provide alerts and enable actions to correct issues that arise
- report on all activity

### III. NETWORK MANAGEMENT REQUIREMENTS FOR MSPS

In a distributed environment, the same requirements apply yet they are necessarily more difficult to achieve. The biggest challenges are that it's impossible for one network administrator to be in multiple locations at the same time, and it's difficult to get real-time visibility into what's going on in customer locations whether they're across town or on the other side of the globe.

Real-time visibility is essential because when there are issues – and there inevitably will be issues – network administrators need to be alerted immediately, either through audio alerts, on-screen displays, emails, SMS, or other forms automatically generated by the network monitoring solution. The sooner they know what is going on, the sooner they can take remedial action. While administrators need to be alert themselves, they need tools to help them see in all places at all times.



Additionally, because an MSP's diverse client base will present a wide variety of network types, architectures, and equipment, they require an agnostic solution capable of seeing disparate networks as if they part of the same organization.

Another challenge is one of scale. Despite operating in a distributed environment, most MSPs are small organizations with fewer than five employees responsible for monitoring all client networks. Their clients typically are very small as well, often along the size of doctor's offices or small e-commerce concerns. Though small, their networks are as important to them as the network is to a Fortune 500 company. The point is that each client may have fewer than two dozen network devices to manage, which means that there is an economic ceiling in terms of what MSPs can charge – even though the level of service must always be high.

MSPs have to be able to make sufficient margins on a per-client basis, so they are caught between what they pay for a network management solution and what they can charge for providing network management services. What they can't afford is to have an inferior system, since their ability to attract and retain business is dependent on their ability to provide the critical services their clients need to make sure their networks are operating at acceptable levels. For example, because margins are low MSPs need a system sophisticated enough to distinguish between real emergencies and false alerts so they are not making unnecessary visits.

So the requirements for MSP environments include a cost-effective, technology-agnostic system in which network management applications or agents are installed in each client location, with the centralized network operations center (NOC) outfitted with a dashboard display that clearly maps out the network assets of each and every client, and a range of configurable alert options.

#### IV. WHAT TO LOOK FOR IN A NETWORK MANAGEMENT APPLICATION

If you are an MSP with diverse customers, you have specific network management needs that require a specific set of capabilities.

For example, because all networks are heterogeneous environments, you need a solution that offers a great deal of flexibility, one that can identify and monitor the full breadth of network devices, applications, and equipment. This requires the ability to support both SNMP and WMI.

SNMP lets you manage and monitor network performance, availability, and throughput, as well as troubleshoot problems. SNMP is standard in most network devices and network management solutions. However, only a few such solutions currently include WMI monitoring among their capabilities. WMI is a Microsoft standard for retrieving information from Windows applications. WMI comes installed by default on SQL Server, Exchange, Windows 2000, 2003, Vista, and XP systems, so it is an important tool for monitoring network environments that include Windows servers and applications.



The solution must be able to employ these different types of monitors:

- **ACTIVE** – the solution sends out a “ping” signal and waits to hear a response
- **PASSIVE** – the solution reads information left in syslog event files and SNMP traps
- **PERFORMANCE** – the solution monitors and responds to threshold levels

Furthermore, the solution must look for and report on problems – not cause them. Think of it: the solution monitors multiple networks 24/7, collecting huge amounts of information. If the solution tries to send all that information to the NOC, it would greatly hamper network performance and possibly cause false alerts. Instead, the solution should be able to transmit only changes in state, keeping the rest of the information in its own locally stored databases. Reports can then also be generated locally, yet viewed from the NOC.

Another important point to make about the amount of information the solution collects is that the network administrator must be able to make sense of the data quickly, so that if action is required, it can be done with minimal delay and disruption of service levels. This requires a solution that can display this data visually, via network maps, as an intuitive dashboard.

With multiple locations, the network administrator can receive numerous alerts. It’s important to know when an alert represents an emergency, and when it does not. For example, you don’t want the network management solution to alert you during planned service periods. You want to be able to program maintenance schedules into the system so it can distinguish between planned and unplanned downtime. In other words, no false alarms. This way, when an alert occurs, the network administrator can know that it’s a real emergency.

Networks have to run 24/7 but network administrators usually go home at the end of the day. They need to be able to access the network management solution anywhere, anytime. For that matter, different levels and types of users will need to access the system for different reasons, and not everyone should be able to access the same level of information. You want a solution that affords remote access and role-based views to ensure maximum efficiency and security.

Last but certainly not least, you need a solution that offers full functionality without blowing up your budget or your margins. It is possible to find vendors with proven, cost-effective solutions, such as Ipswitch’s WhatsUp Gold.

## V. WHATSUP GOLD MSP EDITION

Ipswitch WhatsUp® Gold MSP Edition enables service providers and value-added resellers to deliver network management excellence to end-users as a service. Scalable, easy to use, and market-tested, the MSP Edition allows network administrators to deliver powerful and accurate management of critical devices, processes, and applications at a positive price point that delivers the operating margins they need to compete. The new MSP Edition has been specifically designed for use in distributed client environments, where different network structures, device demographics, and geographic distances make it difficult to cost-effectively provide network monitoring services.

WhatsUp Gold offers simple deployment, robust scalability, groundbreaking usability, and fast return on investment. For any number of locations or clients, Ipswitch's solution:

- Discovers and maps all network devices
- Supports both SNMP and WMI
- Alerts administrators when problems arise
- Gathers network information over time and generates reports
- Provides anytime, anywhere network monitoring

The MSP Edition features a full range of extraordinary features, including:

- Coverage for all network infrastructure via SNMP MIB support and usage
- Predefined and customized system performance reports using WMI counters
- Screen Manager that displays summary information for all sites
- Application monitoring templates for SQL Server and Exchange
- Customizable workspaces and workspace reports
- Support for non-persistent SNMP instances for performance monitors
- Customizable interface speed for interface utilization reporting
- A full web application for remote users reliant on web access
- Service level/quarterly availability reports
- Movable device map icons
- 100+ workspace reports
- 50+ full detail reports

Detailed technical information is available from the WhatsUp Support Center at [www.whatsupgold.com/support](http://www.whatsupgold.com/support).

System and hardware requirements are available at [www.ipswitch.com/WUGMSPSysReq](http://www.ipswitch.com/WUGMSPSysReq).

## CONCLUSION

Your clients' networks are your business. Network management helps you to stay in business. The more you know, the more you can maximize performance and availability. Look for a solution that has the features and capabilities you need, and also respects your budgets and need for margins. 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 v1-3 and WMI.

## 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](http://www.dailynetworkmonitor.com).

For product and sales information, visit [www.ipswitch.com](http://www.ipswitch.com).

Ipswitch values community involvement; to find out how to become involved visit [icare.ipswitch.com](http://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](http://www.ipswitch.com)