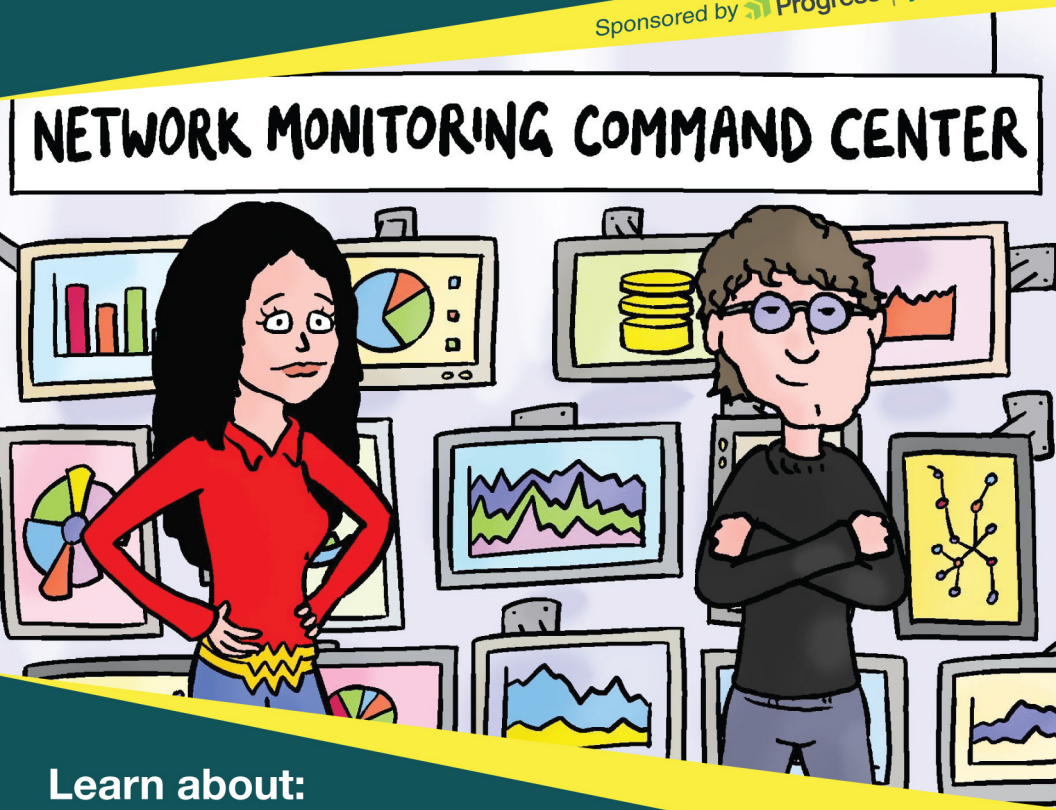
Conversational
Network Monitoring

A ConversationalGeek® Book

Sponsored by Progress® | ipswitch®



Learn about:

- The challenges and benefits of network discovery and monitoring
- Capabilities necessary for successful network monitoring
- The value of Ipswitch's WhatsUp® Gold

3rd Edition

By Brien M. Posey (Microsoft MVP, Commercial Scientist-Astronaut Candidate)

Sponsored by Progress | Ipswitch

Today's hard-working IT teams are relied upon to manage increasing complexity and deliver near-zero downtime. Progress' wide portfolio improves application and network performance, monitors diverse IT environments, and ensures secure exchange of data that meets PCI, HIPAA, GDPR, and other industry and government data security and regulatory requirements.

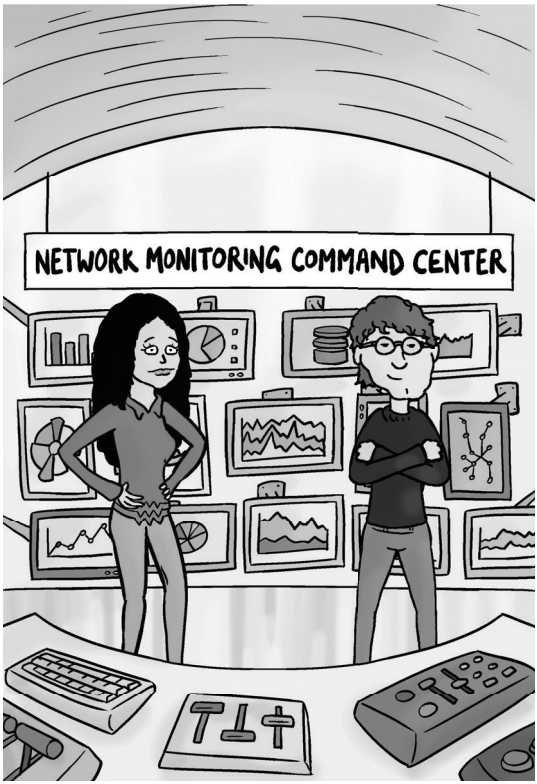
Progress (formerly Ipswitch) produces and sells file transfer and network management software for IT professionals to make the networked world a safer place to share data. Progress' suite of network and security solutions includes WhatsUp® Gold for network monitoring, and MOVEit® and WS_FTP® for secure file transfer. Progress' focus on customer success is supported by an online community with over 115,000 members. To meet the varying needs of its customers, Progress solutions support a range of environments including on-premises, hybrid, and public or private cloud, via perpetual and subscription licensing. Progress solutions meet the highest commercial and government data security requirements and are PCI-, HIPAA-, and GDPR-compliant.

Find out more at

www.ipswitch.com

Conversational Network Monitoring

By Brien Posey



ConversationalGeek®

Conversational Networking Monitoring

Published by Conversational Geek Inc.
www.conversationalgeek.com

Trademarks

Warning and Disclaimer

Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at ConversationalGeek.com

Publisher Acknowledgments

All of the folks responsible for the creation of this book:

Author:	Brien Posey
Project/Copy Editor:	Steven Zimmerman
Content Reviewer(s):	J. Peter Bruzzese

Note from the Author

Greetings, and Welcome to Conversational Network Monitoring. I'm Brien Posey, a long-time tech author and speaker. In this book, I am going to be giving you something of a quick crash course in network monitoring, but I'm going to approach the topic in a somewhat unique way.

If you work in IT, then I'm guessing you probably already know something about network monitoring. Even if you're not a network monitoring expert, I'm sure you at least know what a network monitor is, what it does, and why network monitoring software is useful. But here's the thing… There is little consistency among network monitors. Network monitoring tools have widely varying feature sets, and some IT pros find they actually have to use multiple network monitors in order to accomplish their goals.

My goal in writing this book is to talk about the features, capabilities, and strategies that are most useful for finding and correcting network problems. Along the way, I will even talk about some common vendor scams.

Oh, there is one more thing I want to be sure to mention before I get started. This book is not intended to be a sales pitch. I'm sure this book will eventually have a sponsor (we can't produce these books for free), but my goal is to help you to objectively evaluate your network monitoring capabilities, not to sell you a product.

Brien Posey

The “Conversational” Method

We have two objectives when we create a “Conversational” book: First, to make sure it’s written in a conversational tone so it’s fun and easy to read. Second, to make sure you, the reader, can immediately take what you read and include it in your own conversations (personal or business-focused) with confidence.

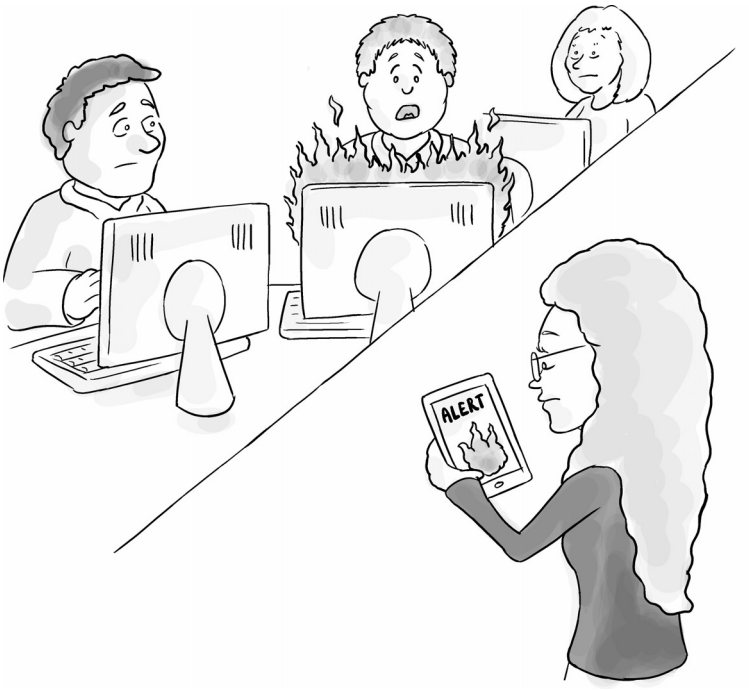
These books are meant to increase your understanding of the subject. Terminology, conceptual ideas, trends in the market, and even fringe subject matter are brought together to ensure you can engage your customer, team, co-worker, friend and even the know-it-all Best Buy geek on a level playing field.

“Geek in the Mirror” Boxes

We infuse humor into our books through both cartoons and light banter from the author. When you see one of these boxes, it’s the author stepping outside the dialog to speak directly to you. It might be an anecdote, it might be a personal experience or gut reaction and analysis, it might just be a sarcastic quip, but these “geek in the mirror” boxes are not to be skipped.

Within these boxes I can share just about anything on the subject at hand. Read ’em!

Network Monitoring



Networkers have a saying; “the network is guilty until proven innocent and it takes a great deal of fact management to prove its innocence.”

Most IT pros seem to understand what network monitoring entails, and why it is so important. And while it’s tempting to think of network monitoring in a really technical way, I think it is equally important to take a step back and look at the big picture. Specifically, this means considering the rationale for using network monitoring in your own organization, and what it is you really want to accomplish by doing so.

The reason it’s so important to stop and think of network monitoring in both a philosophical and objective way is because like any other IT technology, network monitoring has

evolved over the years. In fact, I tend to think of network monitoring as being a lot like Wi-Fi.

On the surface, comparing network monitoring to Wi-Fi is ridiculous; Wi-Fi and network monitoring are two completely different technologies that are used for totally different things. But forget about what these technologies do for a moment and think about them philosophically instead.

When Wi-Fi was first brought to market less than 20 years ago, almost nobody used it. Wi-Fi was crazy expensive, ridiculously complicated to configure, and very insecure. In fact, one of the big stories of the time was that hackers were sniffing Wi-Fi networks from afar by using antennas that were made out of Pringles cans.

So, with that in mind, consider how Wi-Fi has evolved over time. Today, Wi-Fi is a commodity technology and almost every consumer electronic device includes Wi-Fi connectivity. In fact, there are even vendors that Wi-Fi enable non-traditional (to put it mildly) devices that leave tech journalists like myself scratching our collective heads. In the last couple of years, for example, I have heard stories of Wi-Fi-enabled curling irons, spoons, toasters, hairbrushes, and the list goes on. Maybe I'm old fashioned, but I just don't see the practical benefit of connecting a stapler to my wireless network.

OK, so what does any of this have to do with network monitoring? Well, like Wi-Fi, network monitoring has become something of a "me too" technology. Let me explain.

I'll be the first to admit that network monitoring isn't being rampantly used in the consumer space the way Wi-Fi is, but just think about how many enterprise products have network monitoring capabilities built in. Sure, there are dedicated network monitoring applications, but network monitoring capabilities are also sometimes integrated into hardware components such as switches and routers, operating systems,

management tools, and so forth. In fact, I once had an anti-malware product that had a built-in network monitor.

My point is that just as some Wi-Fi-enabled devices are much more useful than others, some network monitoring solutions are better than others. Some of the available network monitoring solutions do a really good job, while others offer minimal capabilities and are simply bolted on to a product so the vendor can list network monitoring capabilities as a product feature.

Given the vast array of network monitors that are available today, IT pros must be able to differentiate between a network monitoring solution that is truly useful, and a solution that might not quite get the job done. That's why it's so important for an organization to consider why it is using network monitoring and what it hopes to accomplish by doing so. Only then does it become possible to find a network monitoring solution that aligns with the organization's goals and requirements.

Of course, every organization's needs are different, but there do tend to be certain requirements that are more or less universal, and I want to take the opportunity to talk about some of the more common requirements. My goal in doing so isn't to create a network monitoring buyer's guide, or to pitch a particular vendor's solution, or anything like that. Instead, my hope is that by presenting some of the more common requirements and objectives related to network monitoring, I can help you to more easily brainstorm the things that are most important to your own organization.

Find and Fix Problems… Fast!

OK, pop quiz! You get a call from the CEO. He has an important video conference coming up in fifteen minutes, but for some reason his network connection has slowed to a crawl. The

connection probably isn't even fast enough to support a voice call, much less a video call. *What do you do?*

Actually, this one is a trick question. The correct answer is that you should ideally be able to detect and correct the issue before the CEO even notices that anything is wrong.

Remember, successful IT careers are built on self-preservation. But just for the sake of argument, let's pretend the CEO's problem was not detected early on, and that the problem has caught everyone by surprise. *How would you go about diagnosing and fixing the problem before the CEO's highly important video call?*

The way an IT pro would go about diagnosing and fixing this sort of problem would vary depending on the network monitoring solution they are using. For the purposes of this discussion though, the actual method isn't important. What is important is that your network monitoring solution, whatever it may be, should allow you to very quickly and confidently diagnose and correct any problems that happen. If you had to stop and think about how you might be able to diagnose and correct a problem like the one described above, then it may be a sign your current network monitoring solution is somewhat lacking.

Although a network monitoring solution should ideally be able to proactively detect and correct adverse conditions before they become problems, such a tool also needs to be able to diagnose problems that have already occurred. Most network monitoring tools can be used to detect problems, but it's worth considering the degree of effort and the depth of knowledge that will be required on the part of the administrator.

Over the last few years, enterprise software vendors seem to be gravitating toward the use of "single pane of glass" business dashboards. Such an interface tends to work relatively well for

assessing the health of a network, especially when the display is combined with an underlying automation engine that can detect the source of the problem. Even so, the software should really take things at least one step further.

Let me give you an example of why a dashboard that identifies the cause of a network problem might be inadequate by itself.

Imagine for a moment that an organization's headquarters span an entire campus as opposed to being confined to a single building.

Let's also pretend that the organization's IT department is using a network monitoring tool that's equipped with an interface that shows the entire network within a dashboard display.

Just for fun, let's also assume the software is capable of automatically detecting network problems.

Now, suppose this fictitious organization has a problem somewhere on their network. The network monitoring software immediately alerts the IT staff to the problem and even identifies the piece of hardware causing the problem. Armed with that information, it should be easy for the IT staff to correct the issue, right? *Maybe, maybe not.*

In reality, a network monitoring solution such as the one from the previous example can point the IT staff in the right direction so they can begin the troubleshooting process, but there are two key pieces of information such a tool may or may not provide.

For starters, the IT staff will need to know what type of network segment they are dealing with. Is the problem occurring on a physical network segment, or is the problem specific to a virtual network segment? If the problem is occurring on a physical network, what kind of link is being impacted? Is the segment based on copper wire or fiber, or is

the segment wireless? If the network segment is virtual, does the segment reside on a virtualization host, on a hardware component, or somewhere else?

Since at least some of the newer network monitors can differentiate between physical and virtual network segments, let's pretend the network monitoring software from the previous example is able to attribute the problem to one specific piece of physical networking hardware. The IT staff must then determine where the hardware is located; remember that this imaginary network spans an entire campus, and there are presumably dozens of wiring closets scattered among the various buildings.

If a network monitoring tool is to help the IT staff fix network problems in as little time as possible, the software must be able to convey the physical location of each networking component. Otherwise, the IT staff may waste a lot of time hunting for hardware.

Most importantly, all of this information has to be put into context, because just looking at each individual area of the network may not help you without a complete contextual view.

Consider this: *What if the problem is intermittent and difficult or impossible to replicate? What if the problem only occurs at certain times based on certain conditions?*

Without a solution that provides a contextual view of interconnected systems, the IT staff will have an uphill battle just diagnosing the issue.

In a real-world example, a regular sales demonstration of an application seemed to fail for no immediately discernable reason. The application checked out, the virtual and physical servers it used were running perfectly and all the relevant links were up every time IT checked. Then someone got the bright idea to look at the performance logs of the network to

determine when this issue was happening. It turned out that the only time this application failed was when it was being demonstrated from a particular conference room between 11:45 AM and 12:30 PM. Otherwise, it worked perfectly.

A quick look at the location determined the wireless access point for that conference room was on the other side of a wall from a small kitchenette – and in close proximity to an elderly microwave oven. Sure enough, when the microwave was turned on, the Wi-Fi at that access point was disrupted just enough to cause the fault – something IT would never have been able to figure out if they hadn't had a detailed, contextual view of not just all the connections in the area, but the proximity of other devices and the time of day.

Keep the Solution Cost Effective

A secondary goal, that's almost as important as the first, is that of keeping network monitoring affordable. After all, nobody has unlimited funds to spend on network monitoring. In fact, organizations usually try to spend as little as possible on network monitoring so the bulk of the IT budget can be spent on other things.

Although the concept of not breaking the bank when shopping for a network monitoring solution would seem to be completely straightforward, there are actually many different ways of thinking about the cost of a solution.

At the beginning of this book, I mentioned that network monitoring solutions were starting to become something of a "me too" technology, and that network monitoring features could be found in a variety of different products. As such, there is a good chance an organization will already have at least some network monitoring capabilities, even if it has not purchased a dedicated network monitoring product.

From a cost standpoint, this would seem to be ideal. After all, the cheapest solution is the one that you already have. However, relying solely on the network monitoring capabilities that are built into existing hardware and software might prove to be somewhat impractical.

Suppose for a moment that a particular vendor decides to include network monitoring capabilities in the network switches it manufactures. Those native capabilities will probably do a great job of monitoring the network switches. But they likely lack the ability to perform any sort of in-depth monitoring of other network resources.

It's conceivable that an organization may be able to cobble together somewhat extensive network monitoring capabilities by relying on those capabilities that exist within the products it already has. For example, an organization might use a combination of network monitoring tools built into switches, routers, operating systems, and applications.

Although such an approach can indeed be cost effective, it probably isn't going to be practical or efficient.

Think back to the previous question of what to do if the CEO were to experience network problems mere moments before an important video conference. If the IT department were to rely on a collection of network monitoring tools rather than a single, integrated solution, it may not be able to diagnose the problem in time for the CEO's video conference. That's because the IT department would have to run each individual tool in hopes that one of the tools would be able to spot the problem.

In essence, any perceived cost savings could be quickly dissolved by the inability to collectively use the tools to diagnose and correct a problem when it really matters.

Another way to think about the cost of network monitoring is to consider the total cost of the required software licenses.

This one can be tricky because of the way some software vendors license their products. The initial licensing costs may cover only basic monitoring, with additional licenses required for monitoring switches, applications, and that sort of thing.

I tend to think of this licensing model as being similar to that of purchasing a new car. No, I'm not talking about dealing with a pushy salesperson who uses high-pressure tactics to try to fatten their own commission checks, although that might be another similarity. I'm talking about the way new cars are priced.

The base model of a vehicle may be modestly priced, but the price increases sharply as you begin to add on options and trim packages. Suppose, for instance, that you want to add a navigation system to the car. Most automotive manufacturers won't just sell you a navigation system. If you want a navigation system, you may be forced to buy a "technology package" which increases the cost of the car by a thousand dollars or more, even though portable navigation systems can be had for about a hundred dollars.

Even though licensing network monitoring software based on the resources that need to be monitored has long been a standard practice, there are two factors that can greatly complicate things. First, perpetual software licenses are quickly becoming a thing of the past. As such, a vendor may require its customers to renew their software licenses on an annual basis.

The most obvious impact to annual license renewals is that of ongoing costs. The organization must include the cost of network monitoring software in its annual budget going forward, because it will never truly own the software.

A less obvious, but equally painful, consequence to annual license renewals is that license management can become far more complex.

To show you what I mean, imagine for a moment that you purchase a network monitoring solution that requires licenses to be renewed annually. Now let's pretend that half way through the first year you decide to expand your network, and therefore need to purchase some licenses to cover the new equipment you have added. Depending on the vendor, you could end up in a situation in which you have licenses that have to be renewed at different times throughout the year, rather than being renewed all at once. Such a renewal model can increase the license management burden substantially.

Another factor you should consider with regard to overall cost is that of vendor upselling. Some software vendors won't just sell you the software by itself. The vendor may also require the purchase of a maintenance contract. In some cases, however, the bulk of the costs may not be incurred until after the purchase is complete.

I have recently heard some stories regarding the unscrupulous sales practices used by some vendors. I have no way of knowing whether or not these stories are true, but regardless, these alleged scams serve as a cautionary tale. Knowing how the scam works can help keep you from falling victim.

The story begins with an IT pro who is in need of a network monitoring solution, although the same basic story line could easily apply to just about any type of enterprise software. The IT pro contacts a number of different vendors, all of whom quote a price way higher than the organization is willing to pay. When the IT pro tells the vendors that their products are too expensive, one of the vendors steps forward and tells the IT pro that they will work with the organization to deliver a solution on budget. *This is where the trouble starts.*

The vendor brings the price down substantially by licensing the software in a way that allows the organization to use the core capabilities they really need, but without paying for any of the extras the organization doesn't really need. It seems like a

good idea, so the organization buys the software. After purchasing the software however, the organization quickly discovers the software's core capabilities are just a little bit too minimalistic, and do not meet its needs. The organization contacts the vendor who is happy to sell it the necessary licenses- at a sharply inflated price. At this point the organization has little choice but to purchase the licenses, because they have already invested a substantial amount of money into a product they cannot use.

Obviously, not every vendor uses unethical sales practices, but if one does quote a price that seems just a little bit too low, then it might be a good idea to go online and see what other customers are saying about the vendor.

Make Sure that the Solution is Easy to Use

Ease of use and cost effectiveness are often at odds with one another. For example, there are some really powerful open source network monitors available, and some of them are free. The problem with at least some of the open source solutions is that they require a very deep understanding, not just of network monitoring, but also of Linux. Although such products might be friendly to the bottom line, they can be anything but intuitive to use.

I will be the first to admit that, if forced to choose between ease of use and functionality, functionality wins every time. After all, if a product doesn't do what it's supposed to do, then it really doesn't matter whether or not it's easy to use. Besides, no one ever said working in IT is easy.

Even so, there is no rule that says a product can't be both powerful and intuitive. One of my major pet peeves with enterprise software is I have always gotten the impression that many vendors will make their software a lot more complex than it needs to be, in an effort to somehow justify the product's huge price tag.

In my opinion, complexity is overrated. Besides, excessive complexity can be counterproductive. Think about the example I presented earlier in which the CEO's network connection was running slowly, and IT had less than fifteen minutes to figure out what was going on and fix the problem. In a high-pressure situation like that, would you rather be using a product with a really tedious interface, or a product with an interface that is simple and intuitive?

Now don't get me wrong… network monitoring is a science, and its very nature means that there is going to be some inherent complexity. Even so, there is no reason why a network monitoring solution's interface has to be so complicated it gets in the way of figuring out what is going on with the network.

Manage Your Network Hardware

It's tempting to think of network monitoring in terms of… well, monitoring. However, there can sometimes be a degree of crossover between network monitoring and network management. Ideally, a network monitoring tool should help you manage the devices on your network.

To show you what I mean, imagine for a moment an organization has based its network around a particular make and model of network switch, and therefore has a number of identical pieces of switch hardware. In such a situation, there is a reasonably good chance the organization has configured each of the switches in the same way.

The problem with this is that manually configuring hardware is tedious, time consuming, and the process is also prone to human error. It would be much better from a management standpoint to be able to create a standard template that can apply a predetermined configuration to devices of a particular make and model. This approach would reduce the administrative burden, while also reducing the potential for human error.

Such an approach to network hardware configuration would also be beneficial to organizations that are subject to regulatory compliance. Regulations such as HIPAA, FISMA, PCI, and SOX each have their own nuances but, generally speaking, regulations typically require IT to put into place (and document) controls that standardize the way data is handled.

The use of an automated template for network hardware configuration could help IT pros more easily prove to compliance auditors that network hardware is running a standardized configuration.

Network Discovery and Monitoring

Back in the 90s, one of the places where I worked adopted a network monitoring solution that required the IT department to manually create a network topology map. Believe me when I say that manually entering information about the various network devices was a tedious process. Thankfully, most – if not all – modern network monitoring solutions perform automated network discovery.

Discovering your network is certainly important; you've got to know WHAT'S connected. But the question is: *can you monitor it?* See, that's where licensing comes in. All solutions can discover what's out there on your network to some degree of granularity, but proceeding to monitor all those devices, applications, configurations, traffic flows, etc. is another matter.

Sure, you might work with a free solution. It should discover the entire network but will typically only allow an extremely limited amount of monitoring because it's free. That's great if all you need is a network map, but not much help for ongoing monitoring unless you have a tiny network.

You need to know and understand what you're buying when you look at a solution. Ideally you want to buy the monitoring capabilities you need and nothing more. This is why you can purchase a bare-bones, basic-level product that only monitors servers, switches and routers. If you need wireless monitoring that's something else you can add on, same for virtual monitoring, configuration management, network traffic analysis, etc. This isn't necessarily a bad thing!

As previously explained, networks can be monitored at many different levels of granularity, and the level of granularity that is required determines the components that must be monitored. If, for example, basic packet monitoring is all that is required then you could probably get away with only using switch level monitoring. If, on the other hand, you need to perform application-specific monitoring, then your monitoring solution will require some degree of application support, such as a plug-in that makes the tool application-aware. Of course, these plug-ins or add-ons typically require a license, and that's where you need to pay close attention to your costs. It makes sense to consider not just your current needs, but also how your network is expected to grow in the future when pricing out a monitoring solution. Often, you'll find yourself paying more over the next few years to expand your monitoring capabilities than you would have if you'd bought a full-featured solution in the first place.

Detect and Manage Configuration Changes

When network problems occur, those problems can often be traced back to configuration changes that have been applied to the network hardware. It stands to reason that one of the most effective ways of coping with potential problems is to not only audit configuration changes, but also to bring configuration changes to the administrator's attention. Alerting an administrator to a configuration change can save the administrator from having to take the time to hunt through log files in search of an elusive entry.

Although there are some devices that can produce administrative alerts in response to a configuration change, it's far more effective to centralize the monitoring and alerting functions rather than dealing with devices on an individual basis. Such centralization accomplishes a few different things.

For starters, it ensures that all network hardware is being monitored in a consistent manner. In doing so, the network monitoring software eliminates the potential for human error. You should never have to worry that a busy administrator has forgotten to enable monitoring on one of the network devices.

The automatic detection of configuration changes is also good from a security standpoint. If, for example, the network monitoring software has detected a configuration change on your organization's router, and the change was not put into place by anyone on the IT team, then it is an indication that the organization has a serious security problem. Without automated detection and alerting of configuration changes, such an event might go unnoticed for an extended period.

And remember, it may be important to maintain and track consistent configurations for regulatory purposes depending on your region or business.

Automatically Provision New Hardware

Although not normally a consideration within the realm of network monitoring software, the provisioning of new network hardware should also be a consideration when you are selecting a network monitoring solution. As we all know, networks are anything but static. Networks tend to grow over time as more and more devices are added to the network. Even if a network is not expected to see any significant growth in the foreseeable future, it still remains a dynamic environment due to the fact that aging hardware may be replaced with new hardware.

Given the dynamic nature of network environments, IT pros should consider their approach to the provisioning of new network hardware. Typically, if a new switch or router is added to a network, then someone from the IT department is going to have to spend some time configuring that device and getting it ready to use. As previously discussed, a manual configuration process leaves the possibility that the person who is configuring the device will make a mistake, resulting in a configuration that does not completely adhere to the organization's established requirements.

Another issue that can sometimes be a factor regarding manual device configurations is that the act of provisioning a new device is not always tied to network expansions or upgrades. Sometimes hardware fails and needs to be replaced. If an organization manually configures its networking hardware, the configuration process will add to the amount of time it takes to replace a failed device with a new one.

Ideally, network hardware provisioning should be tied to the discovery process. Earlier, I talked about the possibility of using a profile or a template to apply a standardized configuration to a piece of hardware. This same basic concept can be extended to the provisioning of new hardware.

Imagine for a moment that an organization has five identical switches on its network. Now let's suppose that, in the interest of security and compliance, the organization creates a standard configuration for these switches and enforces that configuration through their network monitoring software. Now suppose the organization decides to expand its network and acquires another switch that's identical to the ones already in use.

Because a standard configuration for that particular make and model of switch already exists on the network, the network monitoring software should theoretically be able to discover the new switch, determine that the switch is of a known make

and model, and then apply the configuration the organization has established for that make and model of switch. This automated process would not only reduce the administrative workload, it would also ensure the new network hardware is configured quickly and correctly.

Reporting and SLA Compliance

One more consideration that must be taken into account is reporting. Sure, you need the software to be able to let you know when a problem has been detected with your network, but that's not what I'm talking about. I'm talking about basic reporting capabilities.

I have to admit that, on the surface, this particular requirement seems relatively unimportant. However, there are at least two different reasons why having a good reporting engine built into your network monitoring software could prove to be very important.

The first of these reasons is that some organizations are subject to Service Level Agreements (SLA's). SLA's guarantee the IT department will provide a certain guaranteed minimal level of service. These SLA's are often financially backed and provide compensation to customers when service drops below the guaranteed level. Granted, many organizations are not bound by SLA's. But, for those that are, the stakes could not be higher; a single minute of sub-par performance could potentially cost the organization thousands of dollars. As such, it's critically important for a network monitoring tool to be able to accurately report statistical information on an as-needed basis.

A second reason it's important to have a good reporting engine built into your network monitoring software has to do with the IT department's ability to continue using the software. As previously noted, many software companies have abandoned perpetual licensing in favor of annual license

renewals. In most organizations, IT spending is heavily scrutinized, and the IT department must justify all its purchases. This means that there are no guarantees that the finance department will approve funding for renewing your network monitoring software license for the next year. One way of improving your odds of getting to keep your network monitoring capabilities for another year is to be able to justify the software's existence.

A good reporting engine should be able to document the number of problems the network monitoring software was able to help resolve. Similarly, the reporting engine should be able to provide documented proof of improved performance or increased network availability as a result of having the tool. Another key point is that a reporting engine should document that your network monitoring software has reduced the mean time to resolution (MTTR) for any problems detected.

Vendor Sponsored Chapter: Progress | Ipswitch

Monitoring your network can be highly challenging, given you – like most organizations – have a vast range of devices, applications, manufacturers, operating systems, etc. that, in total, make up "your network." Many vendors provide monitoring capabilities to watch the performance of their own products, but taking that route leads to the need for 5, 10, 15, even 20 different products.

A recent study by Enterprise Management Associates (EMA) found that organizations with more than one monitoring tool suffered losses in productivity and (as you would assume) as

the number of monitoring tools reduced to one, productivity went up.

Progress' focus on making powerful – yet practical –monitoring solutions has culminated in WhatsUp® Gold – a highly flexible, robust, and unified network, server, and application monitoring solution. The WhatsUp® Gold monitoring platform has all of the features and capabilities discussed earlier regarding the industry standard FCAPS model (Fault, Configuration, Accounting, Performance, and Security), while providing high levels of visibility and intelligent detail to put the information you need within your reach quickly and intuitively.

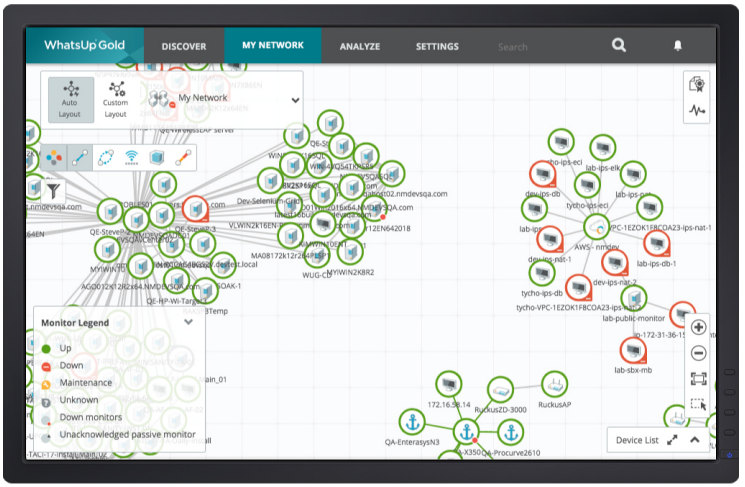
As mentioned previously, all network administrators need a clearly defined Network Monitoring Toolbox and a deep understanding of each tool in that box. WhatsUp® Gold answers this call to action by providing visibility across on-premises, cloud, virtual, or physical – all of the critical pillars for network monitoring and even greater capabilities including;

- ICMP and SNMP Management
- Network Traffic Analysis and Assessment
- Flow Collection, Analysis and Reporting
- Log Collection, Analysis and Reporting
- Application Monitoring
- Wireless Monitoring
- Virtual Machine Monitoring
- Configuration Management
- Storage Monitoring
- Cloud Monitoring
- Distributed Monitoring
- API Integration

WhatsUp® Gold provides multiple options for network device and network discovery by using specific IP addresses, IP address ranges or seed file using SNMP for these discoveries.

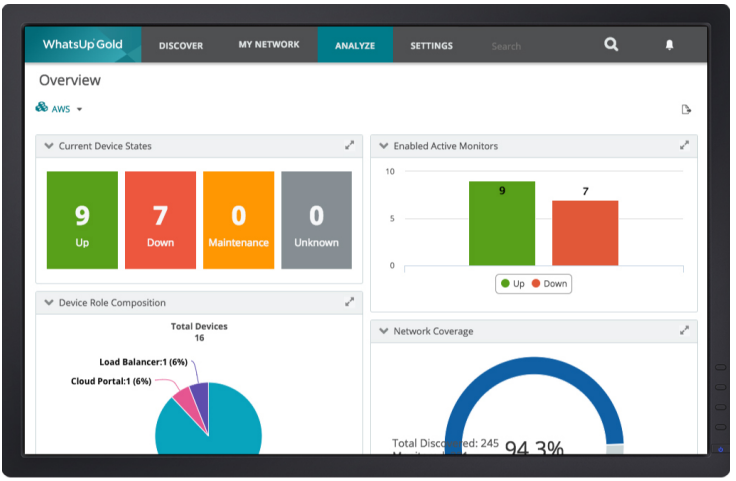
WhatsUp® Gold

Rather than interacting with tables and charts, WhatsUp® Gold uses an interactive, dynamic workspace in which you can view and manage your network. This unique workspace allows you to both visualize and manage your network using the same interface.



Using pre-defined overlays, contextual details around dependencies and link status, your virtual network, or how your network interacts with your wireless infrastructure, you can easily home in on specific details to help elevate basic monitoring information to become actionable intelligence.

WhatsUp® Gold provides you a network traffic analysis module (NTA) to collect network traffic and usage from flow-enabled devices on the network supporting NetFlow, J-Flow, sFlow, IPFIX and NSEL protocols. It also can collect and view data for Cisco CBQoS (Class Based Quality of Service) and NBAR (Network Based Application Recognition).



Clear, Actionable Visibility

WhatsUp® Gold gives you at-a-glance visibility, to more of your IT environment, through a single interface than most monitoring products. Because IT pros wear multiple hats, they can't afford to invest large amounts of time trying to extract the information they need from your management tools. That's why Ipswitch focuses so much attention on making WhatsUp® Gold the perfect balance of visibility and ease of use.

WhatsUp® Gold provides an interactive network map that enables users to see everything that's connected to the network in context. Filter insight by device type or state, or provide overlays showing wireless networks, virtual environments, cloud resources, network dependencies, and interface utilization. WhatsUp® Gold makes troubleshooting and initiating administrative workflows seamless, possible directly from the map to assure the fastest time to answers.

Drag and drop dashboard components, right-click to sort, filter, or change chart types and empower IT pros and their teams with just the information they need when and where they

need it. And any dashboard can be exported as a live link to easily share customized views with any audience.

WhatsUp® Gold's discovery process automatically applies out-of-the-box or custom device roles to accelerate monitoring setup. Users are up and running in less than half an hour with immediate visibility through the interactive network map and notifications through email, SMS or slack of developing problems.

Simply put: WhatsUp® Gold is a network monitoring platform worth evaluation and consideration based on the unified capability it provides for network, application, and server monitoring.

NOTES

Easily “converse” about Network Monitoring in any setting.

Your organization’s productivity rests on the availability and performance of your network. This requires you to discover and monitor every device within the organization, working to maintain the delicate balance of speed, accessibility, and utilization. Learn the how, what, and why of network monitoring, and how a third-party solution can help.

About Brien M. Posey

Brien Posey is an 18 time Microsoft MVP and an internationally published author and conference speaker with over two decades of IT experience. In addition to his technology work, Posey is also a Commercial Scientist-Astronaut Candidate. (http://www.brienposey.com/space) Follow him on Twitter @BrienPosey

ConversationalGeek®

Visit conversationalgeek.com for more books on topics geeks love.