



7 Quick Wins with Network Traffic Analysis

How to Strengthen Your Network
Management Superpowers

ipswitch



Network Traffic Analysis gives you x-ray vision

One of the most useful things to have in your network monitoring toolkit is Network Traffic Analysis (NTA). It collects and processes network flow data (commonly available through features such as Cisco's NetFlow) to give you x-ray vision into your network traffic. This includes:

- Port level analysis of applications consuming bandwidth
- End-points ('talkers') consuming bandwidth by port
- Bandwidth consumption by end-point or application over time

Pretty easy to see how this would be useful, right? But just in case you are way past your last energy drink and lacking in imagination at the moment, let's list seven ways this can make your life easier.

#1: Your bosses think you're pretty smart

Network Traffic Analysis gives you in-depth application monitoring and bandwidth utilization capabilities. This new visibility lets you provide insights to management you just can't get with network device monitoring alone. These insights can positively impact day-to-day operations.

For instance, you can accumulate data for a week and verify bandwidth utilization between your corporate headquarters and branch offices. Let it run for a month and you have a good picture of just how much of the bandwidth you are paying for is actually being used. Management likes to know that IT pros are contributing to the business and this level of visibility just makes you look a lot smarter.

#2: You see who is playing games or watching videos

Some of your peers may see you as "Big Brother" once they realize you can produce reports that show who is playing games, visiting porn sites or streaming movies when they are supposed to be working. But research has shown that when employees know someone is watching, they misbehave a lot less and productivity goes up.

It's only fair to let people know you have this capability before you actually start using it. It won't advance your career to discover that the CEO is the biggest culprit.



#3: You optimize performance

Maybe you already know who is streaming video or playing games. But do you know how that impacts key applications and services? Network Traffic Analysis shows you how much bandwidth is consumed by which users/apps at what times. It is a simple matter to see spikes in video usage stealing bandwidth from a core business application.

If users complain about response times at the same time that someone is streaming videos, you have a simple path to a clear win. And, oh BTW, this also makes you look pretty sharp to your bosses.

#4: You blast through traffic jams

Network Traffic Analysis gives you a ready tool for a quick deep dive into the underlying causes of network slowdowns. Especially if you are continuously collecting and analyzing traffic data.

One IT pro we know set up a new company-wide, anti-Spam software solution with the most up-to-date signature libraries stored on their corporate servers. After the installation was complete, they noticed that the link to the branch office was experiencing high utilization nearly every hour. Their NTA software quickly detected that client machines from the remote sites were all communicating with the anti-Spam server for updates at the same time. Problem solved! They staggered the update requests over the span of a few minutes and eliminated the utilization bottleneck.

#5: You gain move/adds/changes superpowers

How about the user that relocated their finance and accounts staff from one floor to another. The move required a different subnet and they decommissioned an old router in the process. Unfortunately, a few of the workstations were still configured to be part of the old network.

Right after the move they saw an increase in the amount of bounced traffic between these workstations and the default gateway. With Network Traffic Analysis they knew exactly which workstation was part of the routing loops and that made it easy to rectify the configuration and get the new network to settle down smoothly.

#6: You spot cyber attacks as they happen

Imagine arriving at work one morning and seeing there are a large number of failed connections on your main router. You also note that this pattern had persisted for a couple of hours. Network Traffic Analysis shows you that all of the transmissions are from a few IP addresses outside your network. It's a classic case of a portscan -



an external attack looking for vulnerable open ports on your router firewall.

You show up as the hero and quickly block the offending IP addresses. Then you call in the cavalry, your security team, for additional support.

#7: Download it today and solve problems tomorrow

You can do all of this right now, with WhatsUp Gold. Give yourself some big wins with a 30-day trial and you get the Network Traffic Analysis capabilities in the process. WhatsUp Gold installs in minutes and it is pretty straightforward to configure your routers and switches so you can collect the flow records.

That same day you can fine-tune your implementation by spending few hours configuring Flow Monitor to gain automated insight into specific areas of interest. Set up thresholds for the volume of traffic or conversations from each workstation source and key interfaces (on your router and switches). Have VoIP? Set up custom threshold tracking of RTP traffic from/to specific hosts. Set up notifications to track failed connections, which can alert you to intrusion attempts.

Give yourself some quick wins and see what Network Traffic Analysis can do to enhance your superpowers!

[Try WhatsUp Gold free - visit ipswitch.com/free-trials/whatsup-gold](https://www.ipswitch.com/free-trials/whatsup-gold)

About Ipswitch

Ipswitch helps IT teams solve complex problems with low-cost, easy-to-use software. The company's software is trusted by millions of people worldwide to securely transfer files containing mission-critical and sensitive data; and to monitor networks, applications and hybrid infrastructures. Ipswitch was founded in 1991 and is based in Lexington, Massachusetts with offices through the U.S., Europe and Asia.