



# Simplify Network Monitoring



**Table of Contents**

Executive Summary ..... 4

Network Monitoring Shouldn't Be So Difficult ..... 4

A New Era of Simplicity..... 5

Simple Is Supercharged ..... 6

Simple Is Powerful ..... 7

Simple Is Smart..... 8

Simple Is Here: Ixia Network Visibility Solutions ..... 9

Simple Is Brilliant .....10

## Executive Summary

As networks have expanded, network monitoring has become much more difficult. Network monitoring technology hasn't really kept pace. So, if you feel like you're running in place, it's because you are. But network monitoring doesn't have to be this hard. A technology breakthrough, the network monitoring switch, can strategically offload your network monitoring tools and dramatically simplify network monitoring – making it look and feel more like using consumer software.

## Network Monitoring Shouldn't Be So Difficult

With all the technological advances of the last two decades, there is no rational reason why the day-to-day monitoring of networks should still be so difficult. There's no reason why network monitoring professionals should have to spend every day manually de-duplicating packets, writing and using lots of scripts, and making only educated guesses when filtering and re-routing traffic.

For that matter, there's no reason why network monitoring professionals should still be performing routine tasks with generations-old command-line software. By now, network monitoring should be at least approaching the simplicity with which you use Google and consumer applications.

So, why is network monitoring so difficult? You probably know the reasons.

Overall, networks continue to expand, and the applications and services they deliver are increasingly important to the business. The volume of traffic is soaring. Attacks on networks are frequent and often persistent – and they target multiple points inside the network not just the perimeter.

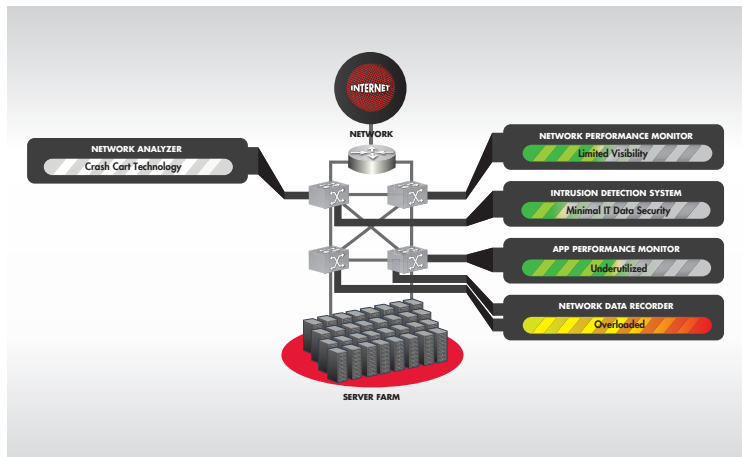
Your network monitoring infrastructure – with its seemingly endless proliferation of monitoring tools – has become more complex, more demanding, and more intrusive of your production network.

There are three major technological problems:

- First, the limitations of SPAN and TAP make it more difficult for your monitoring tools to access and visualize all the traffic they need to see – whether it's for spotting security vulnerabilities or application performance trends.
- Second, without the ability to visualize all your network traffic, you can't get good, actionable insights. You don't have good control – and without control, you're trapped in react-only mode.
- Third, without complete network visibility, you can't optimize the performance of your current monitoring tools, so you're probably under-utilizing some tools even as you're being asked to add new ones.

But cheer up: An innovative network monitoring switch is now solving or alleviating all these problems.

**With all the technological advances of the last two decades, there is no rational reason why the day-to-day monitoring of networks should still be so difficult.**



*Figure 1: Without a Network Monitoring Switch, Monitoring Tools are not effectively utilized and Packets Are Dropped*

## A New Era of Simplicity

This innovative technology – the network monitoring switch – is ushering in a new era of simplicity.

Network monitoring switches strategically offload and control your current monitoring tools, dramatically simplifying your job. They deliver intelligent automation and some even feature advanced graphical user interfaces which give you time back. They also give you more control over your network and deliver better performance from your current tools.

With network monitoring switches, network monitoring begins to look and feel more like using consumer software, but with the robust capability you need from your network monitoring infrastructure.

By offloading the common, low-level, manual tasks from your network monitoring tools, the switches empower network professionals to do their jobs better – much as spreadsheets offloaded the burden of doing calculations from millions of business professionals.

Network monitoring switches bring to network monitoring the kinds of advancements that have revolutionized consumer software:

- Select monitoring switches use intelligent automation technologies to provide simple, visual management: For everyday work, replace the command-line interface with a graphical, point-and-click interface. And view multiple monitoring tools on a “single pane of glass.” (Of course, you can and should retain the command-line technology for use when needed to write special scripts or to solve the occasional arcane problem.)
- Network monitoring switches replace awkward, largely manual and cobbled-together traffic filtering methods with dynamic filtering. It’s simple; almost effortless.
- Network monitoring switches replace manual actions with intelligent, “hands-off” automation of critical management tasks – raising the sophistication of your management without adding skills or staff.

**Network monitoring switches strategically offload and control your current monitoring tools, dramatically simplifying your job.**

- Some vendors, like Ixia, work with your existing tools to automate your time-consuming basic tasks; the automation anticipates and flags problems before you could, and it enables you to be proactive vs. reactive. Similarly to AutoCorrect in Microsoft Office applications.

When you dramatically simplify your network monitoring, you can reach new levels of efficiency, flexibility and scalability. You can avoid common IT headaches and suffer less downtime. You can manage more traffic and more-complex, highly distributed networks with your current tools, staff and skills. You can move faster and smarter, with more confidence.

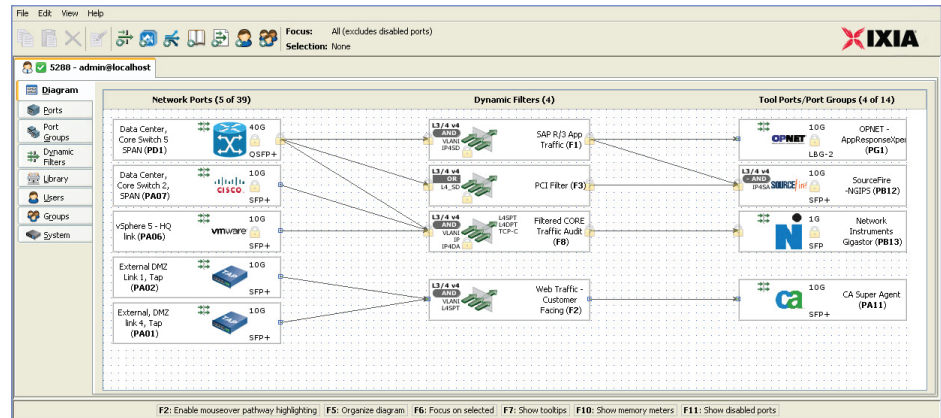


Figure 2: A user friendly, drag-and-drop interface allows users to easily connect monitoring tools to their appropriate SPAN and TAP ports with the click of a mouse.

## Simple Is Supercharged

Network monitoring switches give you complete visibility of your network. This dramatically simplifies how you manage network traffic and tools because you can easily see everything happening across your network. Every part of network monitoring – visibility, control, performance – becomes easier.

**Visibility:** Virtually extend your network monitoring and attain 100-percent network coverage by your critical monitoring tools – overcoming the architectural limitations of SPANs and TAPs. All of your monitoring tools can access all the data from multiple network segments and have a complete view of the network traffic; and each tool can have a copy of the data from one or more segments, so more tools can have access to the same network.

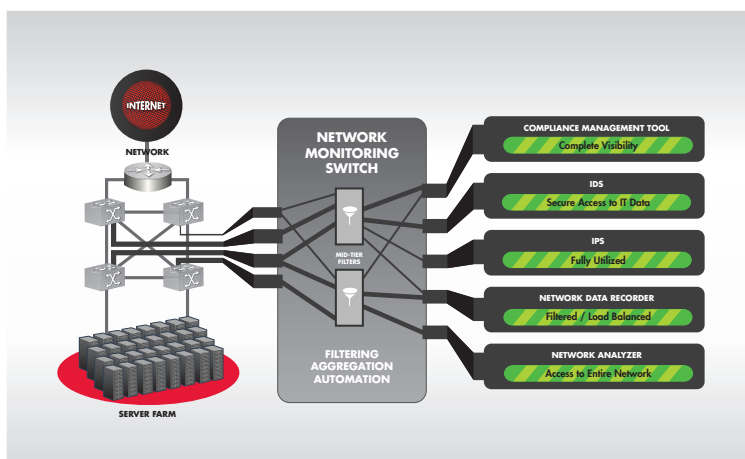
With little or no effort, you get actionable insights. You can easily but precisely see where your traffic goes, whether you're filtering out packets, load-balancing, aggregating packets from the same source, sending packets from the same source to two different places, or replicating or de-duplicating packets.

You can spot problems more easily. You spend your time analyzing network traffic instead of chasing after it.

**Control:** You can keep up with the flow of data, providing the right information to the right tools at the right time. You can act on changes, problems and opportunities faster and with more precision. Intelligently automated management techniques let you do more – and better – with less effort. For example:

Network monitoring switches give you complete visibility of your network. This dramatically simplifies how you manage network traffic and tools because you can easily see everything happening across your network.

- **Intelligent Traffic Distribution:** Packet aggregation for SPAN/TAP shortages, packet routing to the appropriate tools, and “downshifting” of network traffic speeds that lets you use 1G/10G tools to monitor 10G/40G networks.
- **Packet Conditioning:** Filtering, stripping, slicing; de-duplication of replicated packets; load-balancing across multiple tools; buffering of burst-y traffic to tools.
- **Adaptive Response:** Proactive monitoring for changes, bandwidth, incidents and threats, with automatic adjustment of packet delivery to meet needs. You can dynamically update configurations without Change Board approval or manual intervention, and dramatically improve and simplify troubleshooting.



*Figure 3: A network monitoring switch enhances visibility and maximizes tool utilization, reducing time, effort and investment.*

As a result of automatically offloading important but non-mission-critical tasks from individual monitoring tools, you get more performance from your existing equipment and reduce the need for additional equipment.

You can be proactive instead of reactive: quickly head off an incipient hacker attack, or perform rapid forensic analysis to make the proper changes to the network architecture. Network and security professionals can now view the same network data and collaborate more effectively in solving or preventing problems.

**Performance:** As a result of automatically offloading important but non-mission-critical tasks from individual monitoring tools, you get more performance from your existing equipment and reduce the need for additional equipment. For example, offloading packet filtering, load balancing, packet de-duplication, packet trimming, and MPLS stripping from individual tools can generate significant cost savings. You can manage the same (or more) traffic using fewer tools, and avoid the SPAN and TAP shortage problem. You free up your tools to handle what they were designed for, getting better performance from every tool. Intelligent filtering and automation make all of this simple.

## Simple Is Powerful

Network monitoring switches lets you stay ahead of network growth and change.

The switches work with your current infrastructure and your current tools. They aggregate, filter, and replicate traffic so that all tools get the data they need at the right time. The result is simpler, easier, more meaningful insight into network behavior – including user behavior, security vulnerabilities, network capacity, application performance, and IT resiliency.

**Network monitoring  
switches empower  
you to keep up with  
business demand  
and change.**

You actually gain bandwidth, by avoiding under- and over-utilization. This will help you keep up with the growing monitoring demands, including the massive demand created by mobile users.

Network monitoring switches integrate easily; they are designed to integrate with what's already on the market. They are easy to deploy, configure and use. A point-and-click, drag-and-drop control panel simplifies everything you have to do.

The switches are also designed to let you mix and match network monitoring tools easily (1G, 10G, 40G and 100G) for right-sized network monitoring. And, with "smart" instrumentation, you can simply and quickly customize your network monitoring to your needs. No more endless re-instrumentation.

Network monitoring switches also embody open architecture plus open business processes, ensuring your continuing flexibility. For example, you can filter 100G, 40G and 10G links with 1G tools; add IDS units and sniffers; and customize network user permissions – and make these adjustments with a single click. All this improves the performance of your monitoring tools and minimizes the pain and frustration. You can be nimble and keep your network running smoothly.

Do more, simply, with what you already have, by improving data reliability, delivery, security and accuracy.

## **Simple Is Smart**

Network monitoring switches empower you to keep up with business demand and change.

A network monitoring switch gives you network monitoring capability that you won't outgrow as your business grows and changes. It extends the life of your current tools; for example, you can manage 10G, 40G and 100G traffic with 1G, 10G and 40G tools. This breaks the cycle of adding more and more tools, while optimizing those you have today.

Scalability is more than a buzzword. You can purchase only the number of ports and features needed now, so that you can more effectively manage your IT investment. You can use your current networking tools with the filters you need now; as your needs change, you can adjust or add filters with a few simple clicks of a mouse. You can quickly and flexibly redeploy visibility ports as your needs change, in whatever way works best: top-of-rack, end-of-row or single-chassis stack – with no change in UI or management overhead.

You're no longer constrained by architectural limitations such as SPANs and TAPs, or by idiosyncrasies such as redundant network paths. Or by people, skills or tools.

Suddenly, it's simple to be scalable. And simple to be smarter in network monitoring.



# Simple Is Here: Ixia Network Visibility Solutions

Ixia Anue Net Tool Optimizer® (NTO) is the stunningly simple approach to network monitoring.

Ixia is the premier supplier of network monitoring switches. The company is the standard-setter in intelligent automation, having pioneered open architecture, dynamic filtering, a simple-to-use GUI, and support of major platforms.

The Anue NTO delivers all the capabilities as described in this white paper.

The current product line, the Ixia Anue Net Tool Optimizer® 5200 series network monitoring switch, intelligently connects your data center network with monitoring tools to aggregate, filter, load-balance, and de-duplicate network traffic. The Anue NTO 100GbE, 40GbE, 10GbE, and 1GbE interface modules provide patented filtering and de-duplication technology that ensures each monitoring tool gets exactly the right data needed for analysis. The Anue NTO is powered by the easiest-to-use drag-and-drop management in the industry. It simplifies your work: it improves the way you manage your data center, it saves valuable IT time, and it maximizes return on IT investment.

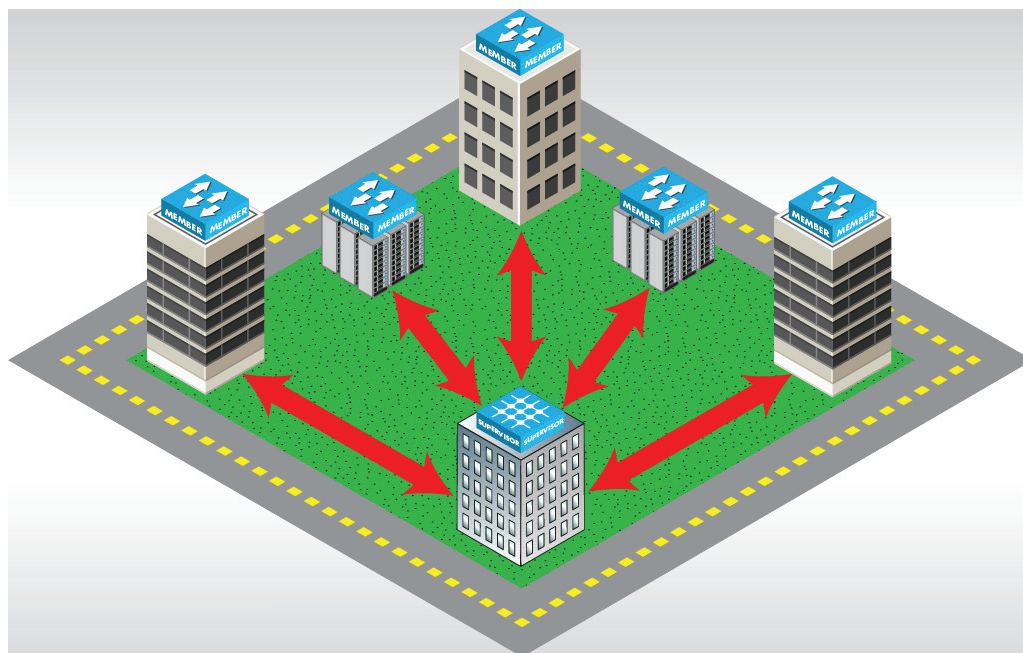
The Anue NTO is easy to own and use. It is particularly distinguished in its provision of these capabilities:

- 10/40/100G Capabilities
- Drag-and-Drop Control Panel
- Software Port Licensing
- Overlapping Filter Engine
- Automated Response Technology
- Packet De-Duplication
- Centralized Filter Templates

Our recently announced Ixia Anue ControlTower™ Network Visibility Architecture builds on the Anue NTO technologies to take monitoring simplicity to a whole new level. The ControlTower provides centralized, intelligent monitoring of highly distributed, complex networks, including cloud hosting facilities, geographically distributed enterprises, and traditional data centers with growing port-density. It presents the entire distributed visibility environment as a single switch – making management of multiple network segments as simple as managing one.

**The current product line, the Ixia Anue Net Tool Optimizer® 5200 series network monitoring switch, intelligently connects your data center network with monitoring tools to aggregate, filter, load-balance, and de-duplicate network traffic.**

Network monitoring  
no longer has to  
be so difficult –  
no matter how  
distributed or  
complex your  
monitoring  
environment.



*Figure 4: Because perimeter defenses are inadequate, the ControlTower network visibility architecture enables network administrators to effectively deploy a central 'tool farm' and cost-effectively monitor segments across the enterprise network for potential information theft and malware transmission.*

## Simple Is Brilliant

Network monitoring no longer has to be so difficult – no matter how distributed or complex your monitoring environment. A network monitoring switch strategically offloads your tools and dramatically simplifies network monitoring. The Ixia Anue Net Tool Optimizer (NTO), the industry-leading network monitoring switch, combines powerful monitoring functionality with an easy-to-use graphical user interface and a scalable network visibility architecture that you'll never outgrow. Your control panel looks and feels more like consumer software - whether you're managing one Anue NTO switch or the Ixia ControlTower™ Network Visibility Architecture. You enjoy more efficiency, flexibility, and scalability than ever before. You can manage more traffic, more complexity and more highly distributed monitoring environments with your current tools, staff and skills. It's simply brilliant.

To learn more, call (512) 600-7171 (Americas), 44 (0) 189 076 204 (EMEA) and 65 84 441 912 (APAC). You may also contact an Anue NTO representative at [visibility@ixiacom.com](mailto:visibility@ixiacom.com).





For more information see <http://www.ixiacom.com/>

This material is for informational purposes only and subject to change without notice. It describes Ixia's present plans to develop and make available to its customers certain products, features, and functionality. Ixia is only obligated to provide those deliverables specifically included in a written agreement between Ixia and the customer.