



Optimize Your Monitoring, Maximize Your ROI

Taking the Challenge Out of Monitoring Enterprise Networks

Monitoring Optimization Benefits

- Extend the range & depth of tool coverage
- Reduce troubleshooting time
- Eliminate shortages of SPANs and Taps
- Monitor 10G links with 1G tools
- Cut network infrastructure & monitoring costs
- Reduce setup and management time for tools by up to 90%

Maximize the Value of All Tools

- IDS & Security
- Application Performance Monitors
- Protocol Analyzers
- Data Recorders
- Compliance Auditors
- VOIP Analyzers
- Network Emulators
- Open Source Tools



Network and application monitoring is a critical piece of the network operations and data center puzzle. IT organizations must guarantee minimum levels of security, compliance, performance, availability, and reliability for both the network and the applications that run on that network. To do so, a wide range of monitoring and analysis devices are required, including application monitors, security (IDS/IPS), sniffers, VOIP, and compliance audit tools.

Monitoring is often seen as a technical problem that should be left to the network operations teams. In reality, monitoring is a solution to business problems and should be considered in a broader light. There is a big difference between plugging in a tool to monitor a problem at a specific location in the data center, and strategically managing the network and the tools that monitor the network. With tight budgets and limited staff to manage the whole process, it is imperative to maximize ROI on tools and to make the whole process very easy to set up and maintain.

To achieve a real solution to these business and technical challenges, all three key ingredients of network monitoring need to be taken into account:

- The Network
- The Monitoring and Analysis Tools
- The IT Staff Responsible for Security and/or the Data Center

Unless all of the issues are identified, resolved and verified, you are only applying a temporary bandage on the problem.

Do You Have Optimal Monitoring Coverage of Your Network?

Companies use a wide range of networking tools to secure their networks, maintain application performance, and minimize risk. However, unless these tools have the network visibility they need, they aren't really monitoring your network. The tools are only as good as the data they receive. Network operations teams frequently suffer from an inability to establish full visibility and network coverage for several reasons.



Shortages of SPANs and Taps

Most data centers suffer from a severe shortage of available SPAN and Tap ports for all the tools that need access to the network. With limited network access points available for so many tools, IT and security teams often find themselves fighting over who can use each SPAN/Tap to deploy tools.

Tools Need to See All of the Right Data to Do Their Jobs

Today's redundant, tiered, and fully meshed networks make it extremely challenging to provide tools with the visibility they require. With traffic passing through any of countless network segments in a data center, it is impractical and expensive to deploy tools at all necessary locations. In short, there are too many tools to deploy, too many network segments to monitor, and too few data access points.

Are You in Complete Command of Your Tool Utilization?

Enterprises are making significant financial investments in monitoring tools, often totaling many millions of dollars of investment for larger enterprises. With such hefty capital outlays involved, these tools should be utilized to the maximum of their abilities. In reality, this is often not the case. There are several challenges to optimizing tool utilization.

Overwhelmed Tools

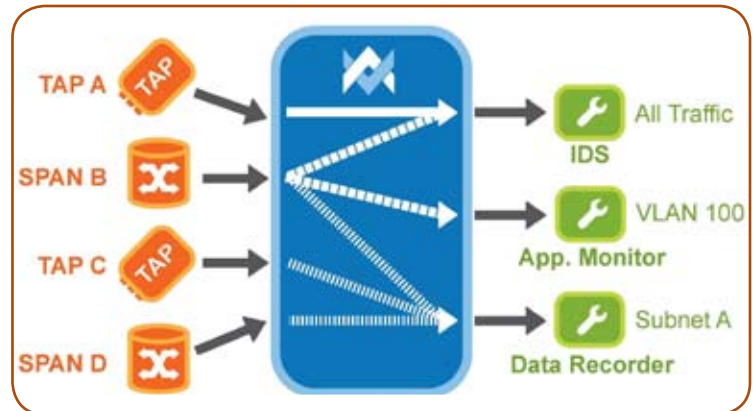
In many cases, tools are used inefficiently, because they are overwhelmed with irrelevant data. Most tools need to see only a small portion of network traffic to do their jobs. Overwhelmed tools spend resources sorting through all the unneeded data, which in turn leads to dropped packets, compromised network coverage, and ineffective tool ROI.

Underutilized Tools

Many tools are underutilized, because they can be deployed at only one access point. If more traffic can be filtered properly and directed to these tools, they can be used to efficiently cover more of the network.

Out of Date Tools

Because networks and applications change constantly (e.g. adding a new VLAN or reconfiguring a switch to address a troubleshooting emergency), it is crucial to ensure persistent, thorough, and continuous management of traffic from the right network access points to the right tools. Overwhelmed tools compromise network visibility, while underutilized tools leave value on the table. The only way to maximize the ROI for all purchased tools is to optimize utilization by precisely managing what traffic is sent to those tools on an ongoing basis.



Unlimited connectivity addresses many problems.

Can Your IT Operations Staff Operate at Peak Efficiency?

While network coverage and tool utilization are important issues, daily productivity for IT staff represents a significant "hidden cost" when monitoring tools are deployed and used in a non-optimal way. With today's complex and constantly changing networks, network operations staffs often find themselves operating in constant "fire-drill" mode. This challenge is even further complicated by the broad IT responsibility for ensuring uptime of not just the network, but also business-critical applications. To meet those objectives, they must employ a wide range of tools. Ideally, all of these tools would be easy-to-use and automated, in order to provide the most thorough and proactive coverage solution. Specifically, the key staff productivity challenges in using tools include:

- Difficulty, complexity, and time to learn complex Command Line Interface (CLI) scripting languages for tool set up
- Time to make and break connections to temporary SPAN ports and to manually adjust filters accordingly while performing daily troubleshooting
- Lack of ability to effectively and efficiently share learnings and filters across different user groups on the data center and security teams

It is clear that your IT and security staff needs relief, and that relief can only come in the form of a dynamic, proactive solution to this monitoring challenge.

The Anue Net Tool Optimizer™ represents a major step forward in enterprise network monitoring. By optimizing all three of the key components of monitoring – the network, the tools, and productivity of the operations and security staff – companies are empowered to finally focus on the business problems that monitoring is meant to address.



The Anue Net Tool Optimizer

The Next Generation in Network Tool Management

The Anue 5200 Series Net Tool Optimizer™ helps companies deploy multiple network tools by conveniently linking test and monitoring tools to any traffic on the network. This improves network visibility and maximizes return on investment for those tools. The Net Tool Optimizer aggregates network data from SPAN ports and Taps in your data center to a convenient centralized or distributed tool farm, where multiple tools can share simultaneous access to that network data. This product offers outstanding filtering capabilities, so each unique tool receives exactly the data it needs and is optimally load balanced.

Proactively See and Manage What Happens on the Network

With the Anue Net Tool Optimizer, enterprises can achieve full and accurate visibility of any or all segments of the network. The product offers unlimited connectivity options and powerful packet-filtering capabilities, enabling maximum coverage of even the most complex, multi-tiered network infrastructures. By maximizing visibility of the network, data centers can finally rest assured that they are minimizing the risks associated with incomplete coverage.

Delivers the Data Tools Need to Succeed

Only the Anue Net Tool Optimizer offers both Dynamic Many-to-Many Connectivity™ (DMMC) and Dynamic Filters™. DMMC is the only solution that can accurately and simultaneously aggregate traffic from multiple ports to one tool while also sharing SPANs and Taps with multiple tools. Specifically, DMMC enables any combination of the following:

- **Any-to-Any** – directs data from any link in your network to any tool
- **Any-to-Many** – eliminates shortages of SPAN ports and Taps by multicasting traffic from one link to multiple tools
- **Many-to-Any** – aggregates traffic from multiple links to provide tools a “big pipe” view

Dynamic Filters self-adjust to ensure continued accuracy of data transmission over time, regardless of other changes to filters, tool configuration, and connectivity. Like a traditional Ingress filter, Dynamic Filters are excellent for aggregation, because traffic is filtered before it is aggregated. However, similar to Egress filtering, Dynamic Filters are also strong at sharing traffic from one network port to multiple tools, because the traffic that is sent to each tool can be filtered on independent, Layer 2-4 criteria.

This can all be done in a small fraction of the time it takes to perform the same task using traditional, Command Line Based Filter coding, and the results are significantly more accurate.

Eliminates SPAN and Tap Shortages

The tool’s customizable connectivity is particularly useful for data centers with a shortage of SPANs and Taps to connect to tools. With full control over the number of ports available to receive packets from network segments and which ports are available for tool connectivity, network operations and security teams are no longer forced to make tradeoffs between coverage and access point availability.

Optimize Monitoring Tool Deployment for Maximum Value Tool Management Features

With the in-depth Anue Tool Management View, operators can view tool utilization and data throughput statistics in real-time. Dropped packets can be avoided through the use of internal alarms that indicate when a tool is oversubscribed with data. Underutilization of tools can be identified and corrected by directing more traffic to those devices, thereby extracting full value from the tools.

Port and Bandwidth Flexibility

Flexibility is another important feature of the Anue 5200. The system can grow and change as your needs do, so you can best leverage your investment in it. You can upgrade the system in one port increments in the field via a simple licensing approach, with no hardware upgrade required. Multiple units can be interconnected as your port needs further expand. The ultimate flexibility is an ability to upgrade 1G ports to 10G, ensuring you have the right number and right bandwidth of ports available to accommodate any infrastructure changes.

Many Sources of Improved ROI

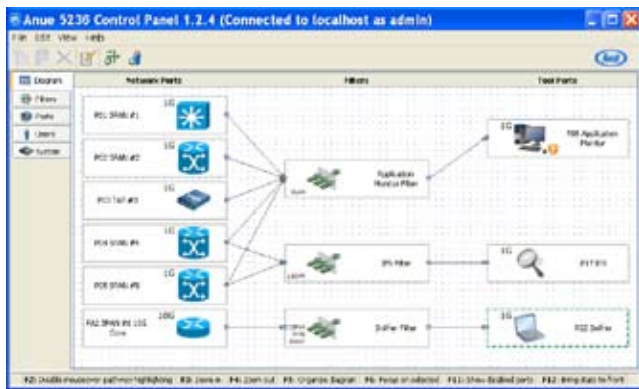
- Lower Tool Costs
- Increase Uptime for Business-Critical Applications
- Monitor 10G Links With 1G Tools
- Increase Staff Productivity



Improve Network Staff Productivity

Fully Integrated Optimization Control Panel GUI

With the Anue Net Tool Optimizer, companies can achieve significantly improved staff productivity related to network monitoring. First, the product's drag & drop GUI is very easy to use for setup, management, and maintenance of connections and filters. All filtering, including complex Boolean logic, is managed right in the GUI with no need to learn complex CLI coding languages or to keep a CLI coding expert on staff to manage the system. You can also manage multiple interconnected or individual systems using system-based tabs within the product's unified GUI.



The Anue solution is the easiest in its class and can be operated by nearly anyone you choose on your IT, network, or security teams. Anyone can claim ease of use, but only the Anue platform was originally designed to be the most user-friendly Monitoring Optimization solution on the market.

Faster MTTR

For troubleshooting, the days of running down to the data center to make & break connections are in the past. When problems on the network arise, simply drag & drop the appropriate connections to troubleshooting tools, set up the filters, and dive into analysis within a matter of minutes, not hours. With so much time and effort currently spent putting out fires, this benefit cannot be underemphasized.

Enterprise Workgroup Features

In today's technical environment, Network Operations and Security personnel are being asked to wear many hats. Matrixed organizations operate with a combination of "official" groups and ever-changing inter-department workgroups.

For this reason, the Anue 5200 Series Net Tool Optimizer provides the following Enterprise Workgroup Features to help enable teams to work together more efficiently:

Security/Access Control: Security has become mission critical. To meet this need, the Anue Net Tool Optimizer™ can manage authentication locally (admin-controlled) or via your existing TACACS+ solution. The 5200 Series also offers advanced Access Control using Groups. The Access Control is managed by creating groups and assigning members to those groups, and then setting permissions for modification and/or connection to ports and filters based on group membership. These features are important in limiting access to the Net Tool Optimizer™ itself, and in ensuring limited access to key filters, network ports, and tools for compliance, confidentiality, or any other important security-related objectives.

Knowledge-Sharing Functions: To help facilitate cross-user learning and reuse of filters, configurations, etc., the 5200 Series includes Filter Libraries, Configuration Import/Export, and Real-time Updates of Changes. Filter Libraries are useful for sharing complex filter settings that can be reused at a later time, shared with other users, or even used to manage time-sensitive and changing monitoring needs over the course of days or weeks. Likewise, system topology can be exported for archiving or backup purposes, or to toggle between various monitoring scenarios (e.g. business as usual, application performance troubleshooting, security remediation). Finally, the system allows for multiple users to work at the same time, and it automatically updates the topology view when changes are made. In order to minimize cross-user errors, the GUI displays an alert when another user changes anything on a port or filter that you are in the act of viewing.

Point Solutions Are Not Enough

Point solutions are simply ineffective. RSPANs provide limited filtering and multicasting, offer no aggregation, and can significantly degrade switch and network performance. Physical layer switches have serious limitations since they cannot filter or aggregate. Tap aggregators and replicating Taps also offer no filtering and provide very limited connectivity options. Products like filtering Taps or Data Access Switches provide some network visibility; however, those devices require complex and time intensive CLI scripting for configuration and filtering. None of these solutions can offer DMMC, Dynamic Filtering, equally flexible system configuration options, a fully integrated GUI, and similar knowledge-sharing functions. If your organization employs any of these simple technologies, you would be better served by moving to the Anue Net Tool Optimizer.