



■ **MONITORING IS CRITICAL**

The shift to 10G networks is under way. According to the Network Observations blog, over half of enterprises (2500+ users) should have made the shift to 10G networks by the end of 2008. The trend is not just limited to the United States, as it is also reported that close to 25% of global businesses joined the race to 10G last year.

While these numbers are relevant to larger businesses and corporations, smaller companies will also soon require such extensive bandwidth to manage daily IT and network operations. In preparation, vendors have begun to drive demand through the use of aggressive marketing and price reductions.

With reduced prices on 10G equipment, many organizations are choosing to upgrade their bandwidth immediately for new technology purchases. After all, why purchase older, slower technology at comparable prices, when your organization can simply begin to prepare for the future now?

■ **LEVERAGE MONITORING TOOLS ACROSS THE NETWORK**

- Application Performance Management (APM)
- Intrusion Detection Systems (IDS)
- Intrusion Detection/Prevention (IDP)
- Network Behavior Anomaly Detection (NBAD)
- Compliance Auditors
- Sniffers/Protocol Analyzers
- Data Recorders
- VoIP Analyzers
- Open Source Tools



How to Monitor 10G Links Using 1G Tools

■ **THE CHALLENGE: MONITORING 10G**

Given the current state of the economy, network operations teams are being challenged to do “more with less,” a phrase that has become pervasive enough to take on the look of an industry theme of late. This trend is showing up in 2009 budget estimates, which are expected to fall by an average of 2.5% from 2008 levels, according to Gartner Research. In response, decision makers are forced to more thoroughly evaluate all capital purchases and make hard decisions about canceling/delaying some transactions.

10G projects are not immune to the budget crunch. Although the cost of 10G equipment has come down recently, it is still selling at a premium to 1G tools. At the same time, enterprises are faced with the daunting task of monitoring 10G networks to ensure that their business critical applications are secure and performing at acceptable levels.

With the move to 10G, many IT and security strategists are concerned about whether they will need to upgrade the many different types of network and application monitoring tools that they have already purchased. These business critical tools include: application monitors, intrusion detection systems, compliance tools, data recorders, VOIP monitors, and protocol analyzers. Few organizations have the budget to upgrade some, let alone all of these tools.

■ **THE SOLUTION: MONITORING OPTIMIZATION**

Imagine a world where you can use your 1G tools to monitor a 10G network. It can be done due to two important enablers:

First, most tools only need to see a small fraction of the network traffic to do their jobs. In fact, sending more data than is required actually degrades efficiency, because tools cannot keep up.

Second, Monitoring Optimization, a new industry trend, enables traffic to be filtered and dynamically directed to the correct tools. With this technique, you can increase monitoring coverage and save money.

Monitoring Optimization enables traffic to be received at 10G bandwidths and filtered on Layer 2/3/4 criteria.

In most cases, traffic from a 10G link can be reduced to 1G or less by filtering out data that a tool does not need to see, so your existing 1G tools can still be used. If the filtered traffic is over 1G, then operators can still use their 1G tools by load balancing the traffic to two 1G tools using Monitoring Optimization. With proper filtering, multiple 10G links can be monitored with a single 1G tool in many cases.

So exactly how should traffic be filtered? It depends on the tools you are using, the applications you are monitoring, and your business objectives. For example, a typical application performance monitoring tool only needs to see TCP traffic from the specific application ports that it is monitoring. Likewise most VOIP monitors only need to see certain protocols such as SIP, SCCP, and MGCP. Tools work most efficiently when they are sent only the specific traffic that each tool needs. Only then can 1G tools can be used to monitor 10G links.

■ FILTERING: THE KEY INGREDIENT

Filtering may seem like a straightforward concept, but in reality, there is more to it. If not done correctly, incomplete filtering can compromise network coverage.

There are three key areas where Monitoring Optimization and similar products differ: ease of use, accuracy, and self-maintenance.

1. Ease of use: Does the system offer an intuitive interface / GUI?

Some available systems require the user to enter many lines of complex and cryptic filtering rules via a command line interface (CLI). Other systems offer drag and drop GUIs that cut the required management time for the system from hours to minutes. Your network operations team is already being stretched to do “more with less,” so your chosen solutions should be as easy to use as possible.

2. Accuracy: Does the system automatically handle overlapping packets?

Overlapping packets meet the filter criteria of more than one tool and therefore need to be sent to multiple tools so each tool can do its job. This case can be easily overlooked, but in reality, overlapping packets occur widely in most data centers. If overlapping packets are handled incorrectly, your tools will not see all the right packets, and your monitoring coverage will be severely compromised. Why invest in purchasing and deploying powerful and expensive tools if you cannot send all the packets that those tools need to monitor?

Typical filters run in sequence. Sequential filtering processes the required filter for the first tool, and then sends the remaining data along for subsequent tools. The problem with this approach is that downstream tools fail to get the full set of data that they need to monitor. For systems that use a CLI to manage filters, correcting this problem is excessively difficult and taxing on the operator—it is not uncommon for overlapping packet filters to require coding of over one hundred of lines of complex rules. In a down economy, who has the budget to add headcount so you can have an expert in the filter-coding language on staff?

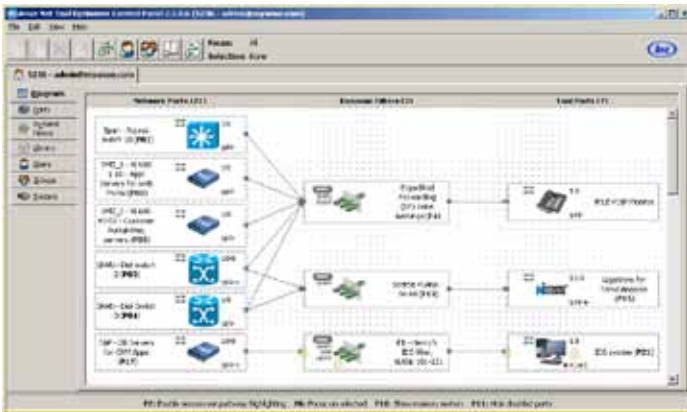
The bottom line is that, when you are share SPAN ports or TAPS with multiple tools, you are almost certain to face the problem of overlapping packets when filtering to those tools.

Insist on solutions that automatically and accurately handle the filtering of overlapping packets. The user simply specifies the data you want each tool to receive, and the system takes care of the complexity.

3. Self-Maintenance: Does the system automatically adjust your filters when changes occur in your network configuration?

Overlapping packet filter rules are not just difficult to set up initially with a sequential CLI-based filtering system. They also have to be continually maintained each time a change is made in the network, the tool itself, or the filter settings. And let’s face it...your network is continuously changing. Failure to keep up with manual maintenance of filters via a CLI results in significant compromises in coverage when tools do not get the data they require to do their jobs. Yet, IT departments do not have the resources to keep a dedicated filtering expert on staff. If you seek to maximize monitoring coverage accuracy as well as operational practicality, do yourself a favor and look for a solution which will automatically maintain filters as your network changes.





The Optimization Control Panel optimizes tool usage and reduces troubleshooting time.

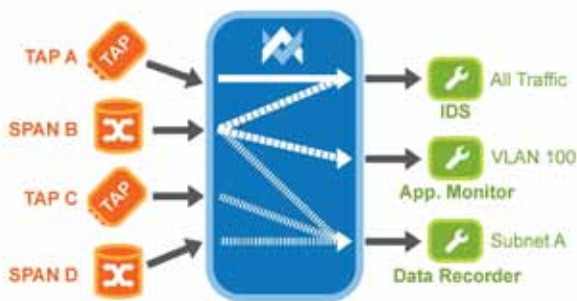
■ BENEFITS OF MONITORING OPTIMIZATION

10G Benefits

- Use 1G tools to monitor 10G links
- Filter traffic so each tool gets only the data it needs, enabling it to operate at full efficiency, even in mixed 10G / 1G environments
- Reduce costs for deploying, managing, and operating monitoring tools

Other Key Benefits

- Share SPAN ports and TAPs so more tools can monitor different segments of the same traffic
- Aggregate traffic from many links, enabling tools to cost-effectively monitor more network segments
- Maximize coverage across network segments, providing full visibility and control over data flows to network and application monitoring tools



The Anue Net Tool Optimizer multicasts data so tools can share relevant data.

■ THE ANUE NET TOOL OPTIMIZER

The Anue 5200 Series Net Tool Optimizer™ was designed to address all of these issues. By aggregating SPAN ports and TAPs to a centralized tool farm, all tools have access to the network traffic that each tool needs to perform its assigned task.

The Anue 5200 Net Tool Optimizer enables you to aggregate and multicast network traffic to the right tools at full line rates. It provides the ability to filter on a variety of Layer 2/3/4 parameters and protocols, offering significant control over load balancing and tool coverage, even with a mix of 10G ports and 1G tools.

The product's Dynamic Filtering approach accurately and automatically handles overlapping packets in situations where port-sharing must send the same traffic to multiple tools. The user simply specifies which traffic to send to each tool, and all overlaps are automatically and accurately handled. Users do not have to write cryptic filter rules. Equally important, the 5200 Net Tool Optimizer's advanced filtering rules are self-maintaining. When network or tool configurations change, each tool automatically continues to get all of the data which that tool is specified to receive.

In addition, the Anue 5200 Net Tool Optimizer is very easy to use, with an intuitive GUI that provides simple, "drag 'n drop" control over all of these functions, without requiring command line coding or other cumbersome management techniques.

The Anue Net Tool Optimizer improves network visibility and maximizes return on investment for monitoring tools, even in mixed 10G and 1G environments.

■ SUMMARY

Monitoring is no longer optional, but a lack of available SPAN ports and TAPs is making it very difficult to achieve full network coverage. Fortunately, monitoring optimization can provide the abilities required to preserve existing investments in monitoring tools using advanced filtering techniques and intuitive GUI-driven operation.

Get the most out of your network, security, and application monitoring tools with the Anue 5200 Series Net Tool Optimizer.



Anue, Anue Systems, and the Anue logo are trademarks or registered trademarks of Anue Systems and/or its affiliates in the U.S. and other countries. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Anue Systems and any other company.