Optimizing Visibility, Control and Performance of Network Traffic
# Table of Contents

- Executive Summary ................................................................. 4
- Network Monitoring Challenges Intensify .................................... 4
- Attain Complete Network Visibility ........................................... 5
- Take Action with a Network Monitoring Switch .......................... 6
- Act to Control Your Network Traffic ......................................... 7
- Deliver Performance ............................................................... 8
- The Ixia/Anue Net Tool Optimizer ............................................ 9
- Maximize Your ROI – and Your Career ..................................... 11
Executive Summary

Monitoring and protecting your data center is becoming more challenging every day. Unfortunately, you can’t solve this problem with people – or by adding more monitoring tools or trying creative workarounds. These approaches just don’t scale. A new approach - using a modern network monitoring switch to strategically offload and control your current monitoring tools - does. By taking this approach, you can see all your network traffic, control it, and deliver better performance from your current tools. Businesses that have implemented this approach have dramatically improved both the ROI of their monitoring tools and productivity of their IT staff.

Network Monitoring Challenges Intensify

In the space of a few weeks, The Wall Street Journal, The New York Times, Twitter, Facebook, Apple and the U.S. Department of Energy report that their computers and servers have been breached by hackers.\(^1\)

The US mulls broader universal data protection laws, similar to those in Europe, to protect consumer data.\(^2\)

IDC reports that the amount of data in the world will grow 50-fold from the beginning of 2010 to the end of 2020 - to more than 40,000 exabytes. Further, by 2020, nearly 40% of the information in the digital universe will be “touched” by a cloud computing provider, and more than 40% of all data will require protection (up from less than a third in 2010).\(^3\)

In a recent survey, 94% of data center managers report some type of security attack, and 43% report partial or total infrastructure outages from Distributed Denial of Service (DDoS) attacks.\(^4\)

Welcome to the world of data center network and operations management, where the only sure things are more data, more network traffic, and more challenges in protecting the business.

If you’re responsible for managing network operations in your data center, you’re likely dealing on a daily basis with:

- Multiple monitoring tools that rely on network traffic data - and regular requests to add more. Many of these tools are overwhelmed with network traffic, while others are underutilized.
- Demands to meet service-level agreements (SLAs).
- More access control and compliance requirements for sensitive data, creating pressure to have 100% visibility of network traffic.

---

\(^1\) Energy Department is the Latest Victim of Online Attack," New York Times, February 4, 2013
\(^3\) THE DIGITAL UNIVERSE IN 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East, International Data Corporation, December 12, 2012
\(^4\) As cloud use grows, so will rate of DDoS attacks," InfoWorld, February 5, 2013
All of your monitoring tools require network data to perform their analyses. But there aren’t enough data access points (network SPAN and TAP ports) for all the monitoring tools and IT teams that need them - leaving them unable to see 100% of your network segments. While there are other problems inherent in modern networks that impede visibility, 43% of companies in a survey by Enterprise Management Associates cited limited SPAN and TAP ports as the main reason they lacked network visibility.

Because you can’t monitor what you can’t see, you may have potentially dangerous gaps in your insight, your control and your ability to maximize monitoring-infrastructure performance.

What’s needed is a strategy for optimizing the visibility, control and performance of your network traffic - and a fast and efficient way to implement it.

**Attain Complete Network Visibility**

Effective data center monitoring and management start with complete network visibility: 100% network coverage by your critical monitoring tools.

Many tool providers talk about complete network visibility, but no one ever defines it. Here’s our definition:

*Complete network visibility is a state of operation in which: (1) all of your monitoring tools can access all the data from multiple network segments and have a complete view of the network traffic; and (2) each tool can have a copy of the data from one or more segments, so more tools can have access to the same network.*
This state of network-traffic nirvana is not impossible to achieve. An established technology - the network monitoring switch - can efficiently extend visibility to all your monitoring tools. Network monitoring switches reside in data centers between SPANs or TAPs and monitoring tools. They provide complete network visibility by aggregating, filtering and replicating traffic so all tools get the data they need at the right time. The result is easier, more meaningful insight into network behavior, including user behavior, security vulnerabilities, network capacity, application performance and IT resiliency.

**Take Action with a Network Monitoring Switch**

With the complete network visibility afforded by a modern network monitoring switch, you can take action on where your traffic goes with a high degree of precision - 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.

*Figure 2: A Network Monitoring Switch Enhances Visibility and Maximizes Tool Utilization --- Reducing Time, Effort and Investment.*

**With complete network visibility as your foundation:**

- Your current monitoring tools work better and harder for you
- You can spot problems more easily - often before they happen
- You can make better-informed and faster decisions
- You spend your time analyzing network traffic instead of chasing it around with crash carts and cables
- You save time and money
Modern network monitoring switches also easily integrate into network security systems (such as TACACS+) and allow you to provide role-based access to network data by users and groups.

Act to Control Your Network Traffic

When you have complete visibility of your network, you can control it better. You can act on changes, problems and opportunities faster and with more precision.

A modern network monitoring switch dramatically raises your level of control, via intelligently automated management techniques such as:

- **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.

Modern network monitoring switches also easily integrate into network security systems (such as TACACS+) and allow you to provide role-based access to network data by users and groups. You can further increase control by letting monitoring tools, network management systems and IT automation systems directly manage the switch - just use simple scripts to build automated connections.

Figure 3: Modern Network Monitoring Switches use Graphical User Interfaces to be Flexible — Quickly Resolve Problems, and Reduce Errors.
With this action-oriented approach, you can be proactive instead of reactive, which is particularly important in security monitoring. For example, you can identify and head off an incipient hacker attack, or perform rapid forensic analysis to make the proper changes to the network architecture.

Because network and security professionals can now view the same network data, they can collaborate more effectively in solving or preventing problems.

**Deliver Performance**

When properly automated, a network traffic optimization strategy will increase the performance of all your monitoring tools - and the productivity of your IT staff.

A modern network monitoring switch offloads compute-intensive tasks from monitoring tools, so that each tool runs better and produces more of the work it was designed for. Therefore, you can achieve better results with fewer monitoring tools. The switch relieves your tools of several burdens:

**Packet Filtering:** It’s a huge waste to use a monitoring tool to find the required packets and discard the remaining packets it does not need to do its job. However, before modern network monitoring switches, this step - one of three required for effective packet filtering - was necessary to avoid dropping traffic. Today, the switch performs three-stage filtering: at the network port, inter-port filtering (traffic between the network port and the tool port), and filtering at the tool port.

**Load Balancing:** Performing load balancing at the switch level prevents network traffic growth from overwhelming monitoring tools. This keeps session data together for better analysis, while balancing the total network load across multiple monitoring tools. Fewer tools are overwhelmed, fewer tools are under-utilized.

**Packet De-duplication:** Duplicate packets are commonly caused by the use of SPAN/mirror ports. Offloading duplicate packet removal from those monitoring tools that have this capability can (1) cut the CPU load of a tool in half and (2) conserve bandwidth at the Ethernet port of the tool, so more data can be provided to the tool.

**Packet Trimming:** By removing payload data from packets - not required by many tools - and leaving only the header information, the switch can send more data across its link to the tool. The tool gets more network data for analysis. And a bonus: for compliance purposes, you can strip sensitive payload data from packets before they go to monitoring tools.

**MPLS Stripping:** Switches can actually increase the capacity of monitoring tools by stripping the headers from MPLS packets and only forwarding the original packets. Most monitoring tools aren't capable of understanding MPLS-tagged packets, so they can't monitor MPLS networks. With MPLS stripping, now they can.

With the most advanced network monitoring switches, all of the complex work behind configuring the switch, connections and filter definitions is fully automated - and performed via a graphical user interface. No need for IT staff to learn a special command language: they can just drag and drop. This means you can manage bigger environments without adding staff or special skills.
The state of the art in modern network traffic visualization technology is the Ixia Anue Net Tool Optimizer® (NTO). The Anue NTO delivers all of the capabilities mentioned above, in a solution that you and your data center will never outgrow. Only the Anue NTO offers unprecedented levels of:

Ease of Use and Ownership: The Anue NTO is easy to own and operate, intuitive to use, and understandable without training. It integrates easily into your existing IT systems and processes, and makes configuration changes fast and simple while controlling access via powerful role-based rules. You’ll see productivity benefits immediately. Things that used to take hours now take minutes, planned or unplanned outages are reduced, and Change Board management headaches go away. You can spend less time managing your tools, and more time optimizing your traffic.

Dynamic Filtering: Anue pioneered three-stage dynamic filters, and they continue to be the easiest to use and most accurate filters on the market. Dynamic filtering can instantaneously change filters and redirect traffic, reducing errors. Accurate package selection maximizes tool performance, eliminates missing packets, and enables tool heterogeneity. You save money and improve ROI.

Automation: The Anue NTO automates time-consuming manual tasks, proactive vs. reactive responses, and near-real-time, event-triggered responses. MTTR is reduced from days to minutes, forensics and analytics are vastly improved, and IT staff can resolve problems faster and get back to more productive, satisfying work.

Anue NTO customers have achieved significant CAPEX and OPEX savings over the status quo of adding more and more security and network monitoring tools. (See table on page 7)

- The University of Texas at Austin has projected a 120% payback on its investment in the Anue NTO over five years.
- A managed security services provider projects 1.6X payback on its investment.
- A national retail chain dramatically reduced its costs of instrumentation (through better port utilization by aggregating and live switching of packet streams) and reduced MTTR (no missed outages and no need to be gated by change management before starting incident analysis).
Table 1: The Anue Net Tool Optimizer Provides a Competitive Edge to Customers in All Industries

<table>
<thead>
<tr>
<th>Customer</th>
<th>Savings +</th>
<th>Big Win</th>
</tr>
</thead>
<tbody>
<tr>
<td>Higher Education (university)</td>
<td>$320K: 50% reduction in IDS and analysis tool cost</td>
<td>Monitor 40G network with 1G tools</td>
</tr>
<tr>
<td></td>
<td>$216K: Elimination of redundant sensors</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$300K: less rack space needed at each PoP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eliminated monitoring packet drops</td>
<td></td>
</tr>
<tr>
<td>Telco (managed security services)</td>
<td>$200K: 4:1 reduction in performance-monitoring appliances</td>
<td>Faster troubleshooting</td>
</tr>
<tr>
<td></td>
<td>$50K: reduced SLA penalties</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Improved incident response</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ready for new business: expanded monitoring and troubleshooting for E911 services</td>
<td></td>
</tr>
<tr>
<td>Retail (large retailer with 8,000+ retail outlets)</td>
<td>Faster MTTR and reduced outages</td>
<td>Improved MTTR and reduced costs</td>
</tr>
<tr>
<td></td>
<td>Not gated by Change Board</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reduced cost of appliances and better port utilization</td>
<td></td>
</tr>
<tr>
<td>Transportation (airline)</td>
<td>Saved money by eliminating unnecessary TAPs and tools</td>
<td>Increased productivity and reduced MTTR</td>
</tr>
<tr>
<td></td>
<td>Easier access to packet flows</td>
<td></td>
</tr>
<tr>
<td></td>
<td>No more driving to remote data centers to re-cable</td>
<td></td>
</tr>
</tbody>
</table>
Maximize Your ROI – and Your Career

With a properly automated approach to optimizing the visibility, control and performance of your network traffic, you can protect your data center while reducing costs and improving the ROI of monitoring tools. You can scale to accommodate network-traffic and business growth without adding new tools. With the help of a modern network monitoring switch, you can implement a sensible, scalable monitoring infrastructure that’s based on automation instead of endless re-instrumentation. Best of all: you become a master of your network, instead of its slave.
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.