

How to Maximize Monitoring Coverage When You Are Out of SPANs/Taps

Monitoring Is Critical

As security and IT professionals, network and application monitoring has become increasingly important for a variety of reasons, including:

- New Data Security and Lawful Intercept compliance requirements that mandate full monitoring coverage, rather than sampling, the most common monitoring approach before these regulations emerged
- Service-Level Agreements that require a minimum level of performance and availability on important services and applications
- New high-bandwidth applications such as IPTV and VoIP that must not only be monitored, but must also be delivered to the user with the packets in the correct sequence
- Increased dependence on electronics communications mediums and digital business transactions, requiring minimized downtime to support revenue and other financial goals
- Desire to shorten troubleshooting and disaster recovery activities without interrupting business processes or making customers aware that a problem happened in the first place
- Need to increase the network operations team's productivity and to pre-empt upgrade and service needs before problems emerge

Clearly, these issues are relevant to both technical and business stakeholders, so monitoring has become a core requirement for network operations and security purposes.

The Challenge: Too Many Tools and Too Few SPANS or Taps

To achieve all of these new objectives, security and IT strategists have had to turn to a wide variety of monitoring tools, including application monitors, IDS/IPS/IDP, VoIP Analyzers, Data Recorders, Compliance Auditors, and Protocol Analyzers, each tasked with meeting a particular monitoring need.



At the same time, businesses are finding themselves with a lack of available SPAN and Tap ports for mirroring data to these tools, preventing companies from attaching tools to the right access points to get the visibility the business needs. This issue comes up frequently with security and network operations teams, with the teams competing for access points to deploy their various tools.

We also see this problem frequently with troubleshooting tools. Typically, this contention results in troubleshooting tools being kept offline until a problem arises. Then, when a problem does occur, the network administrators are forced to "make & break" connections, isolate and correct the problem, and then re-attach the original tool to the port. Aside from the obvious productivity impact of this situation, it results in a loss in coverage by the tool that is temporarily removed from the network.

Tools such as physical layer switches and Tap replicators can allow sharing of access points by multiple tools. However, this only provides a partial solution, since those devices send all the traffic from each access point to all connected tools. For tools to be used most efficiently, each tool should only see the data that it needs to see to complete its assigned monitoring task.

The Solution: Monitoring Optimization

Imagine a world where you can achieve full monitoring coverage regardless of the number of available SPAN ports and/or Taps. It can be done due to two important enablers:

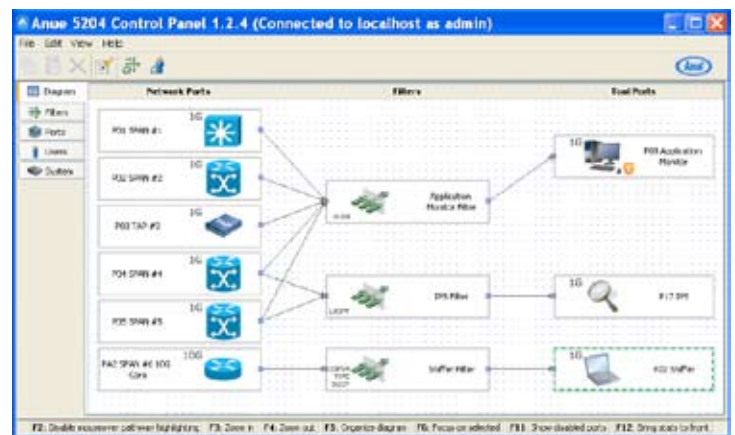
- Most tools only need to see a small fraction of the network traffic to do their jobs, although often this traffic comes from separate network segments. Sending more data than is required actually degrades efficiency, because tools cannot keep up.
- Monitoring Optimization, a new industry trend, enables 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 bandwidths up to 10G and filtered on Layer 2/3/4 criteria. With this technique, security and network operations professionals can use as many tools as needed to monitor the same access points. Then, users can independently and simultaneously filter traffic to each tool, providing each of those tools with the precise information they need to optimize visibility and monitoring coverage.

So exactly how should traffic be filtered? It depends on the tools you are using, the applications you monitor, and your business objectives. For example, let's say you have an application performance monitoring (APM) tool and a VoIP monitor both attached to the same span port. A typical APM 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.

The Essentials of Monitoring Optimization

1. Ease of Use
2. Automatic Accommodation of Packet Overlaps
3. Dynamic, Self-Maintaining Filters



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

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.

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 operation team is already being stretched to do "more with less," so your chosen solutions should be as easy to use as possible.

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 them 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 sharing 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 offer Dynamic Filtering to 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.

“As 10G equipment costs have come down and the need for additional bandwidth has increased due to data center consolidation, virtualization technologies and even convergence with storage networks, many companies have made the switch to 10G.

Those companies have experienced the challenges of attempting to cost effectively monitor these new networks, so they can ensure adequate application performance levels and the required security demanded by the business.

This challenge will be even more important in 2009 as IT budgets tighten. The Anue 5236 provides companies a valuable solution to monitor 10G networks by aggregating and filtering traffic so those networks can be monitored by existing 1G tools.”

Bob Laliberte
Analyst, Enterprise Strategy Group

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

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, via Dynamic Filtering.

Benefits of Monitoring Optimization

- Share SPAN ports and Taps so more tools can monitor different segments of the same traffic
- Maximize coverage across network segments, providing full visibility and control over data flows to network and application monitoring tools
- Filter traffic so each tool gets only the data it needs, enabling it to operate at full efficiency, even in mixed 10G / 1G environments
- Aggregate traffic from many links, enabling tools to cost-effectively monitor more network segments
- Use 1G tools to monitor 10G links
- Reduce costs for deploying, managing, and operating monitoring tools



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 solution 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.

Anue Dynamic Filtering handles overlapping filters. 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 to take advantage of this feature set. Equally important, the product's Dynamic 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.

The Monitoring Optimizer is very easy to use, with an intuitive GUI that provides simple, "drag 'n drop" control over all of these functions, without requiring CLI coding or other cumbersome management techniques.

The Monitoring Optimizer improves network visibility and maximizes return on investment for monitoring tools, even in mixed 10G and 1G environments with a shortage of available SPAN ports and TAPs.

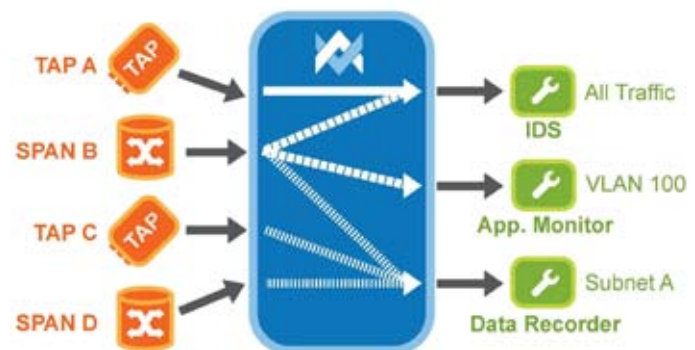
Summary

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.



The Net Tool Optimizer provides multiple tools access to a single data stream, intelligently extending the coverage by aggregating and filtering traffic.



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