



Network Monitoring 2.0 – for Enterprise

White Paper

Introduction

As enterprises adapt to new technologies ranging from virtualization to cloud computing, the focus is on making networks faster, flatter and more efficient. The network must support ever increasing traffic volumes as well as increased requirements for security, analytics and compliance. Enterprises have made significant investments in management systems, but there is a limit to what these systems can do. Security, analytics and compliance all require the enterprise to monitor, capture and examine the actual network traffic in depth. As networks get flatter, there will be more traffic at each monitoring point. Operations will need to get that traffic to an increasing number of platforms and monitoring tools. The challenge is how to perform network monitoring cost effectively while keeping up with the loads coming from these denser and faster networks.

Forward thinking IT executives must consider how to integrate network monitoring to best address these challenges. Traffic capture has long since moved past simple packet capture with a portable analyzer. Today, large volumes of packets must be distributed to platforms from Intrusion Prevention Systems for security to analytics tools for troubleshooting. The growth in these platforms and tools represents a significant investment that must be protected even as network interface speeds increase. The enterprise needs to capture the right traffic at the right points in the network, transport this large volume of traffic without compromising network performance, and distribute the traffic to the right platforms. The best way to ensure that a network monitoring solution can do this cost effectively is to make it an integral part of the network architecture.

Nevertheless, with this much transformation taking place in the network, the migration itself does not take place over night. In the foreseeable future, enterprises still need to support a hybrid network that interconnects various types of existing platforms with next-generation systems and devices. The network may have become “flatter”, but it became more complex at the same time. Therefore, the journey toward a converged all-IP network comes with a whole new set of network performance and management philosophies toward which IT organizations must adopt and evolve. Real-time monitoring, troubleshooting and provisioning of the network must be implemented strategically and methodically, as they are driven by the need to maintain and manage the experience of the end user. In particular, real-time monitoring of network traffic has proven to be essential in diagnosing and analyzing the performance of the network and the services, and consequently the quality of experience (QoE) of the user.

It is the purpose of this paper to address the complex challenges associated with the existing network monitoring approach, which can be termed broadly as the “Network Monitoring 1.0” environment.

As the enterprise needs have evolved, the monitoring solution also has to evolve toward a “Network Monitoring 2.0” model – in which a single distributed traffic capture layer creates a simplified and elegant architecture that many large enterprises have begun to adopt today. A number of key issues and differentiations between the two generations are described and compared. The 2.0 model will also shed some light into what lies ahead as the network monitoring solution continues to evolve with the needs of the enterprise.

Defining “Network Monitoring”

“Network monitoring” can be broadly defined as software and hardware solutions that manage the network components of enterprise and Enterprise infrastructures:

Software

The most common software-centric tools are SNMP-based software that uses periodic polling to identify and describe the configurations, conditions and basic statistics of the network elements. Other software-centric tools include flow-based analysis software which provides specific statistical data on each IP flow that passes through a network element. Common standards for flow records include NetFlow, IPFIX, Sflow and Jflow.

Hardware

Hardware-centric tools are probe-based appliances that intercept packet traffic passing through an IP network. These appliances contain a standard NIC to capture packets, which are then often groomed, processed and inspected for various types of analyses and dashboard displays. These appliances include protocol analyzers, forensics recorders, IDSs, performance/fault analyzers, predictive behavior analyzers, and others. While these appliances are hardware based, their primary tasks are analytical in nature, and still require intensive software and CPU times.

Hardware/Traffic Capture

Often used in parallel with these appliances are network taps. These taps range from the traditional taps that provide basic network access, 1-to-1 traffic capture, media conversion, regeneration or aggregation for the aforementioned appliances, to the advanced higher density Distributed Traffic Capture Systems™ with packet level grooming and optimization prior to passing the traffic of interest to the appliance.

While implementing a combination of all of the above components would provide a holistic view of the network, this paper focuses on the hardware solution (probe-based appliance and network traffic capture), an area which has experienced significant development

over the past few years that is creating a paradigm shift in the network monitoring architecture. As the Network Monitoring 1.0 and 2.0 frameworks will clearly demonstrate, probe-based appliances are necessary monitoring tools for their analytical purposes, but the secondary effect of the increasing number of vertical tools is a simultaneous increase in management overhead. Therefore, a well-thought out intelligent traffic capture platform is critical to the simplicity, scalability, sustainability, and cost-effectiveness of the network monitoring solution.

Network Monitoring 1.0

In this initial phase of the network monitoring evolution, enterprises are busy with rolling out applications and services. Network management tools are typically bound to an IT vendor's portfolio of equipment only. For each new IP service deployed, a separate software tool is also introduced. There are also tools that are so-called "managers of managers" deployed in order to provide a consolidated view of the network status. Combined, these tools produce some basic statistics and data on all the active elements in the network. However, in order to gain better visibility of network performance, additional probe-based systems are placed into the network for real-time fault monitoring, isolation, protocol analysis, or capacity planning purposes. Examples of these tools include IDSs, forensics recorders, protocol analyzers, media and signaling analyzers, and traffic (predictive) behavior analyzers. All in all, the network monitoring solutions have come to be an ancillary thought. The layout of the network tools are depicted in Figure 1 below. Several major challenges arise from this monitoring approach:

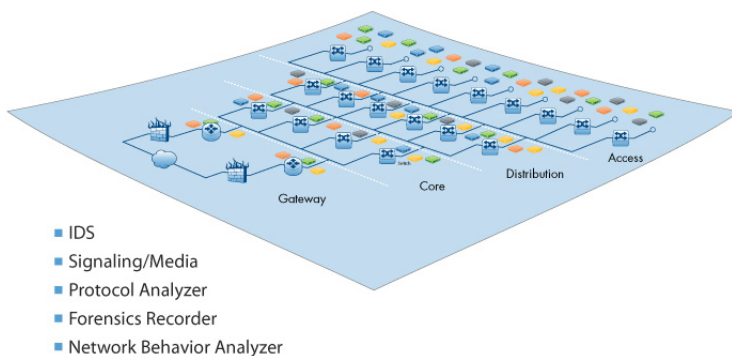


Figure 1. NETWORK MONITORING 1.0 – Fragmented monitoring approaches create further performance and complexity problems

Network & Physical Access

The most obvious problem to the network engineer is the inability to access a particular point in the network for multiple tools. These tools typically collect network traffic through port mirroring (i.e. SPAN) of a network switch. But it is easy to see that there may not be enough SPAN ports to go around, or there is simply no SPAN port available. SPAN ports can also have functional and prioritization issues. The alternative is to use an in-line network tap that effectively copies all traffic from both directions to the tool.

However, in the case of a network engineer troubleshooting with a portable tool, gaining physical access to the premise may be prohibitive. For other reasons, such as network speed, footprint, power supply or other mission critical requirements, a traditional in-line tap may simply be not viable. Either option results in network "blind spots."

Management Overhead

As shown in Figure 1, the different sets of tools are scattered across the network in different physical locations. Each vendor's tools have their own suite of management software, which is often not interoperable with that of other vendors. Therefore the network engineer has to deal with multiple sources of data. If a network configuration change were to take place, the management, reconfiguration and updating of this large number of devices would be overwhelming, potentially still leaving out many blind spots. And even if the in-line taps are available to provide access and minimize the number of blind spots, the taps are isolated devices with little to no awareness of other network devices and events. Should there be a tap failure, all the probes collecting traffic from it would go blind. Depending on the failsafe mechanism available, the failed tap may also trigger a network link failure.

Monitoring Costs

With the configuration and layout of the tools such as those in Figure 1, the CAPEX of the total solution would be substantial, and the OPEX of the monitoring solution could easily become out of control given the management overhead described previously. In a mission-critical environment, not only does this approach increase cost and reduce ROI, it also impacts revenues due to the inability to timely and properly troubleshoot problems. The results include not meeting the stated SLAs for the service organization and ultimately unproductive users.

Tools Utilization

With the in-line taps' aid, the various tools attached are able to collect network traffic at the points of interest. However, the data captured are not necessarily of high quality. If a particular tool is located in a low-volume part of the network it may be undersubscribed. Meanwhile, in a high-volume link, the tool may be oversubscribed due to a mismatch of the line rate or traffic volume and the tool's processing speed. This challenge is not uncommon as the tools need to filter and groom traffic of interest prior to analysis and may not be able to perform at full line rate. The problem is further magnified in very high speed environments (e.g. 10 GigE and beyond) where the tools have to aggregate and synchronize traffic collection across different points of capture.

The monitoring approach in the Network Monitoring 1.0 framework is fragmented at best. The network itself consists of multi-vendor equipment, each with its own view and method of generating network performance data. The total solution is not scalable because it requires multiple expensive devices deployed across network boundaries, creating further complexity, performance issues and management overheads. Traditional network taps find

their places in this world, and address primarily tactical issues with relatively basic functionality. Provided that the tools are given quality traffic data, they are powerful engines that offer deep insights to network performance and subsequently business intelligence. This is by and large the monitoring challenge that large networks inherited over the years.

Network Monitoring 2.0

As communication infrastructure continues to evolve from legacy platforms toward an all-IP network, its architecture becomes “flatter,” thereby substantially increasing the number of complex and heterogeneous IP devices. This translates into a growing number of IP interfaces to monitor, and consequently a much more challenging traffic capture problem. Additionally, tools also require visibility to network traffic in the user plane as well as in the control plane. Responding to these challenges by simply deploying more vertical tools at more network points is not a forward-looking approach. The solution must be future-proof, efficient and adhere to a tight operating budget. In the Network Monitoring 2.0 framework, the overarching vision for network monitoring is simplicity, visibility and efficiency. The Network Monitoring 2.0 vision identifies network taps not as a single device (on a per box basis) but as a network-wide platform of distributed intelligent devices, acting as a single system for traffic capture. As shown in Figure 2, the 2.0 framework decouples the monitoring tools from the communication infrastructure, and creates a single traffic capture layer that is universal to all tools. With careful planning of this layer, this is the only way to achieve the goals of network simplicity, visibility and efficiency. The intelligent taps are expected

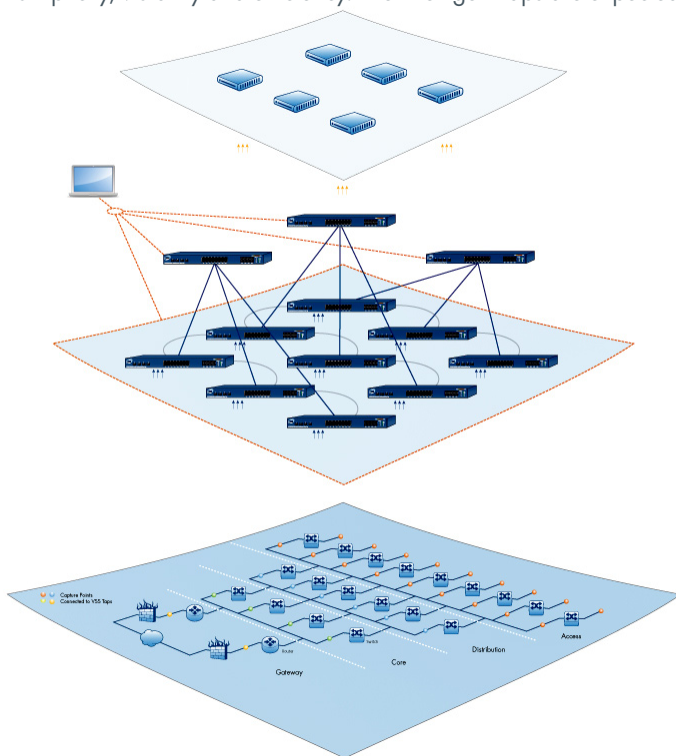


Figure 2. NETWORK MONITORING 2.0 – Traffic capture layer central to simplifying and optimizing network monitoring solution

to play a central role in realizing this vision. The key valuation propositions of the 2.0 framework are described below.

Single Traffic Capture Layer

By decoupling the monitoring infrastructure from the core network, the traffic capture system acts as a universal access layer for all the monitoring tools. The benefit of this decoupling is such that the monitoring architecture can be defined and inserted in a more systematic way. This traffic capture layer is agnostic to the type of tools in the monitoring layer as long as they are interested in IP traffic. This capture layer is possible only because the network taps are distributed and intelligent (described below), and have the capability to interact together as a self-acting system. The system is fitted and scaled to the attributes of each individual network (size, speed, media type, physical environment, number of network interfaces, types of traffic, number/type of tools supported, etc.). With ultra-fast, automatic failover, these network taps are completely non-intrusive and can be safely deployed from end to end.

Distributed Intelligence

As the monitoring tools are centralized and focused on processing and analyzing the traffic data, the Distributed Traffic Capture System in Figure 2 possesses a number of unique features to groom the captured traffic prior to transporting them to the tools. Many tools are application-specific, which means they may be interested in seeing only certain types of IP traffic coming from certain parts of the network. Therefore, various features such as hardware filtering, selective aggregation and port or time stamping of packets allow the tools to view only traffic that they want to see. It is also common that multiple tools are interested in subsets of the same traffic type. Here, session awareness in the traffic capture system is critical in order to load balance this traffic to multiple tools, so that each tool can analyze the entire session or conversation accordingly.

Network-Wide Intelligence

Perhaps most essential to the evolution of the traffic capture layer in the Network Monitoring 2.0 framework is the ability for the intelligent taps to interconnect with and auto-discover one another to form a larger Network Monitoring system. As a kind of intelligent stacking, it is essential to the capture layer because the components (the taps) in a mesh configuration provide self healing – traffic routing is optimized from any port to any port within the system depending on the component level utilization. The performance and capacity of the network traffic capture system can be as much as an order of magnitude larger than that of the standalone approach of isolated taps.

Centralization of Monitoring Tools

By leveraging the traffic capture layer, all tools can now be consolidated to a single location for management and control without compromising the visibility to the points of interest in the network. In fact, network blind spots can be eliminated because there is no more contention for network access as the tools access traffic from the traffic capture platform. The immediate impact of

this centralization is simplification of the network architecture, and a significant reduction in number of tools and consequently the management overhead.

Improved Visibility

The distributed and network-wide intelligence in the traffic capture layer was practically non-existent in the 1.0 framework. Centralization of the tools combined with the traffic capture layer brings unparalleled network level visibility. The session-aware load balancing of high-speed traffic to lower-speed tools (e.g. from 10 GigE to 1Gbps) provides better quality data to the tools. Captured and groomed traffic can also cross WAN borders to maintain a centralized view across a WAN, thereby eliminating further network blind spots and overhead. Additionally, with better-quality traffic data and more pervasive capturing schemes, the traffic capture layer is also essential to the tools in deriving reliable and accurate key performance indicators (KPI) of business operations.

Improved Efficiency

Through centralizing the tools and applying intelligence at the traffic capture layer (i.e. load balancing, filtering and selective aggregation, etc.), the utilization of the tools is much more likely to be at optimal levels. True end-to-end troubleshooting is now possible, resulting in greatly reduced response times to outages and repair (e.g. MTTR). Network level KPIs can also be used in network optimization and planning.

Lowest Cost of Ownership

The Network Monitoring 2.0 framework calls for using the traffic capture systems to scale with evolving network needs. The overall solution cost of the traffic capture layer with a centralized monitoring layer is substantially lower than a non-strategic, non-systematic approach to deploying large number of tools. Lower management overhead and shorter time to troubleshoot and repair mean further reduction in operating costs, faster ROI, reduced customer churn and fastertime to revenue.

Conclusion – Anticipating the Future

Where does the roadmap of the Network Monitoring 2.0 vision lead to? How will the network architecture evolve? This paper offers a perspective on a layered approach to viewing the network infrastructure, by decoupling the network monitoring tools and creating a Distributed Traffic Capture System layer that is much more elegant, cost effective and flexible to scale with the core network. From traditional taps to distributed intelligent taps, traffic capture is used to aid the definition of network monitoring. The hardware solution (probes and taps) is the focus of this paper. In particular, the distributed traffic capture layer is central to a paradigm shift in the network monitoring framework that is already taking place.

While there is no one correct answer to the earlier questions, the key for enterprises (large scale enterprises, small scale enterprises or government) is to develop a holistic and forward-looking strategy for network monitoring and network management. More importantly, they must consider carefully the price-performance, diversity, agility and intelligent capabilities of a traffic capture solution. By adopting the 2.0 framework, network monitoring is no longer an ancillary thought. Depending on future requirements, there are a number of macro trends that enterprises should be mindful of when planning their network monitoring needs:

- **Flattening of Network:** The continued explosion of IP will simply accelerate the pace at which legacy systems are displaced by an all-IP network. The “flattening” effect will create more distributed IP components in the network, and effectively creating more potential points of failure. There will be a broader range of IP services to roll out than anyone can imagine, as a result multiplying the complexity of the network. This creates opportunities for more points of monitoring. The monitoring infrastructure should also be “flat” and flexible across any and all parts of the network.
- **Technology Development:** The Network Monitoring 2.0 framework is laying the groundwork for a smart network monitoring infrastructure. There will be continued needs to monitor user plane and control plane traffic, which can be vastly different in behaviors (e.g. bandwidth requirements). The network elements are expected to increase their per port speed toward 40 GigE or 100 GigE in the not-too-distant future. The monitoring system tools may still lag behind in speed, therefore relying on offloading the front end traffic grooming and bandwidth management tasks to the traffic capture layer. In order to sustain the increase in speed, the traffic capture layer must continue to be performed in hardware, where deeper awareness of packets and applications, as well as more dynamic handling of them, are necessary.
- **Economics – From Cost Center to Profit Center:** Network managers must do more with less – tighter budget control while improving service delivery. Traditionally those are conflicting objectives in the IT organization. The 2.0 framework allows an organization to migrate from a high initial CAPEX business model to a lower and variable CAPEX model in the network monitoring component of the budget. With less, the network managers can now do more in other areas such as network forensics, lawful intercepts, behavioral analysis, centralizing applications for compliance, etc. The layered-approach to network monitoring is fundamental to enabling the business model and differentiation in such network environments.

About VSS Monitoring

VSS Monitoring is the leading innovator of network traffic capture technology and the inventor of Distributed Traffic Capture Systems™, offering the most sophisticated, capability-rich product set with the only fault-tolerant architecture available.

Since its founding in 2003, VSS Monitoring’s mission has been to solve the pervasive efficiency, visibility and performance challenges inherent in monitoring large-scale distributed networks.

Its highly scalable portfolio offers not only basic network taps and SPAN tools but Distributed Traffic Capture Systems that fundamentally improve price-performance and processing efficiency of network analyzers, as well as increase network visibility and reduce mean time to repair.

VSS is headquartered in Burlingame, California USA with regional offices in Japan, China, the UK, and Singapore. All design, manufacture and testing is based at VSS headquarters, with components sourced in and around Silicon Valley, California.

Acronyms

- CAPEX – Capital Expenditure
- CPU – Central Processing Unit
- IDS – Intrusion Detection System
- KPI – Key Performance Indicator
- M2M – Machine-To-Machine
- MSP – Managed Enterprise
- MTR – Mean Time To Repair
- NIC – Network Interface Card
- OPEX – Operating Expenditure
- QOS – Quality of Service
- QOE – Quality of Experience
- SLA – Service Level Agreement
- SNMP – Simple Network Management Protocol

CASE STUDY: VSS SPAN Switches Enable Central Monitoring of Large Enterprise Over Long-Distance Fiber

SEB Group is a Northern European financial group for corporate customers, institutions and private individuals with ten home markets in the Nordic and Baltic countries, Germany, and Poland.

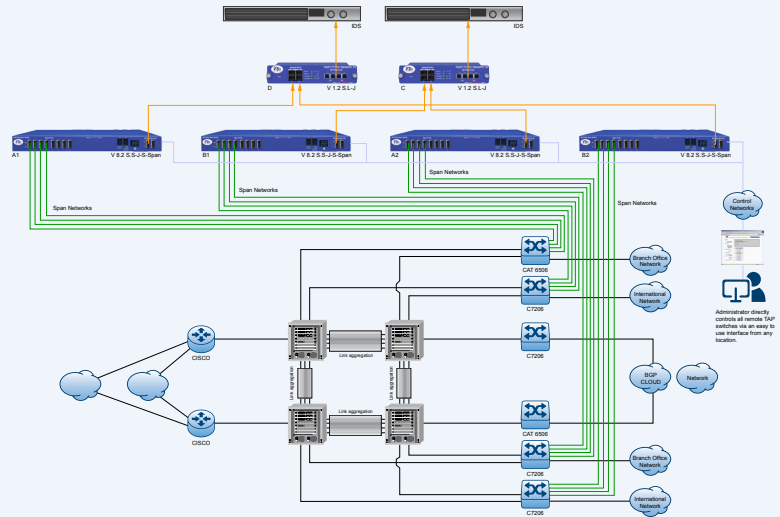
VSS Monitoring’s solution provided remote management, tap switching, data re-clocking, SX to LX media conversion and aggregation of outputs to a single location. This prevented SEB from having to buy expensive additional hardware as well as multiple monitoring devices. The ease and transparency of the installation was also a significant benefit.

Problem:

- Security (Intrusion Detection)
- In the last few years SEB web services grew rapidly, demanding more robust and flexible monitoring solutions.

Solution:

- Monitoring output from the SPAN Switches is regenerated, re-clocked and converted to LX singlemode fiber and forwarded to one central location up to 40km away for aggregation.
- Remotely manageable browser interface allows the operator to choose SPAN sessions to capture at the click of a mouse defined for each connected monitor tool



Benefits:

- Easy management from single location
- Data re-clocking for long distance monitoring
- Immediate and complete network visibility with existing analyzer hardware



Network Visibility. Optimized.

USA
 (Corporate HQ)
 + 1 650 697 8770 phone
 + 1 650 697 8779 fax
 1850 Gateway Drive - Suite 500
 San Mateo, CA 94404
 USA
www.vssmonitoring.com

Japan
 + 81 422 26-8831 phone
 + 81 422 26-8832 fax
 T's Loft 3F, 1-1-9,
 Nishikubo, Musashino,
 Tokyo, 180-0013
 Japan
www.vssmonitoring.co.jp

China
 + 86 10 6563-7771 phone
 + 86 10 6563-7775 fax
 C519, 5 Floor,
 CBD International Tower
 16 Yong'An Dong Li,
 Beijing, China 100022
www.vssmonitoring.com.cn

VSS Monitoring, Inc. is the world’s leading innovator of Distributed Traffic Capture Systems and network taps, focused on meeting the rapidly evolving requirements of security and performance conscious network professionals. Distributed Traffic Capture Systems herald a new architecture of network monitoring, one which fundamentally improves its capability and price-performance.

VSS and Distributed Traffic Capture System are trademarks or registered trademarks of VSS Monitoring, Inc. in the United States and other countries. Any other trademarks contained herein are the property of their respective owners.