November 2016

謀
RESEARCH
Influence and insight
through social media

Simplified Programming of a Visibility Layer
Can Have a Big Impact on

APPLICATION PERFORMANCE

WHITE PAPER

Prepared by
Zeus Kerravala

ZK Research
A Division of
Kerravala Consulting

INTRODUCTION: DIGITAL TRANSFORMATION CREATES TOOL SPRAWL

ZK Research defines digital transformation as the application of technology to build new operating models or processes by leveraging the convergence of people, business and things. Digital advancements are creating new product and services opportunities as well as transforming business operations, enabling organizations to generate more revenue, lower costs and achieve higher levels of efficiency to gain an advantage over their competitors.

Historically, sustaining a competitive advantage was based on having the best product, the lowest prices or the best people. However, this is no longer the case. In the digital business era, sustainable market leadership is based on an organization's ability to recognize shifts in the market landscape and adapt quickly. This is why becoming an agile organization is at the top of every business leader's priority list.

Becoming a digital enterprise will require several new technologies. This is similar to the shift that occurred in the IT landscape when the internet business era began. Digital organizations need to be agile, and this requires IT infrastructure that supports a world in which applications, people and content are becoming increasingly dynamic and distributed.

Businesses are now relying on the following technologies to enable a higher level of business agility:

Virtualization: Server virtualization technology has been around for almost two decades and has become the norm for most companies. The technology has evolved past simple server consolidation, with more IT resources being virtualized including storage, the network and security applications. Virtual resources enable IT to be much more dynamic, as resources can be invoked, moved or shut down as the business requires.

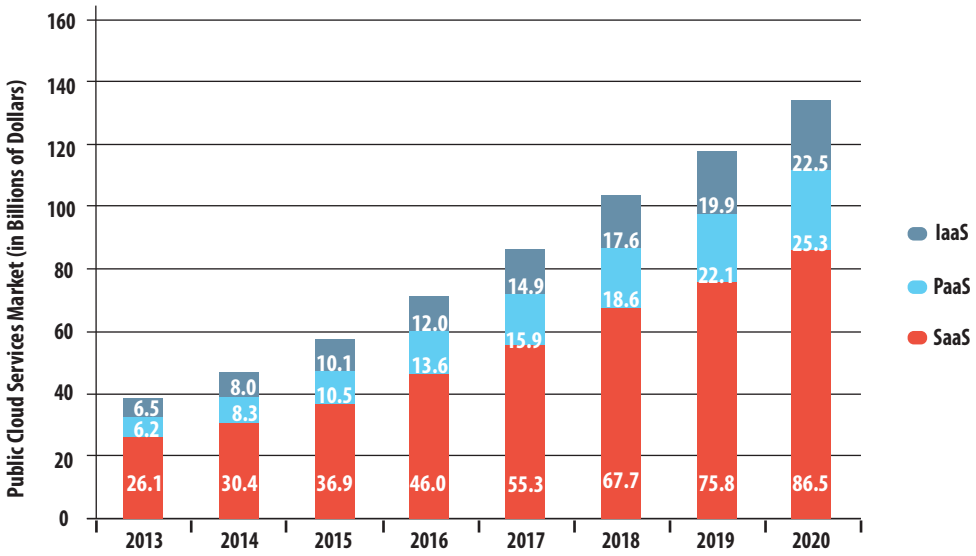
Software-defined infrastructure: Historically, most IT infrastructure was managed one box at a time. The process of making broad changes could often take months to complete. The ZK Research 2016 Network Purchase Intention Study found that four months was the average time it took businesses to implement network changes, far too slow for digital organizations. Software-defined infrastructure extracts the control function from the underlying technology and centralizes it in software so configuration changes can be made much faster. Software-defined infrastructure also lets businesses orchestrate infrastructure changes as the application environment changes.

Cloud computing: Most organizations started down the cloud path years ago but used it as a low-cost alternative to premises-based computing. However, cloud usage has exploded recently (Exhibit 1), as businesses are looking to use the cloud to fundamentally change the way the organization operates. The elastic nature of the cloud enables much higher levels of business agility than traditional computing methods.

ABOUT THE AUTHOR

Zeus Kerravala is the founder and principal analyst with ZK Research. Kerravala provides tactical advice and strategic guidance to help his clients in both the current business climate and the long term. He delivers research and insight to the following constituents: end-user IT and network managers; vendors of IT hardware, software and services; and members of the financial community looking to invest in the companies that he covers.

Exhibit 1: Cloud Services Set to Skyrocket



ZK Research 2016 Global Cloud Survey

Enterprise mobility: Mobile working has rapidly become the norm. Workers now need real-time access to information regardless of where they are and what device they are using. Building a mobile strategy requires more than implementing a "bring your own device" (BYOD) strategy. It also requires a robust wireless network, mobile applications and a scalable cloud platform to deliver secure services.

All of these technologies have come together to enable businesses to do so much more than ever before. Companies that understand how to harness the power of digital transformation have a chance to become market leaders; those that do not will struggle to survive.

However, it's critical that IT leaders understand the implications of heading down the digital path and change their management and security strategies to minimize risk and optimize their return on technology investments. Adding more security and management tools is not sufficient, as "tool sprawl" can make the environment more complex and more difficult to manage and secure.

Rather, organizations require a solution that enables them to have a complete view of the current operating environment and understand the impact of changes. A visibility solution with a robust graphical user interface (GUI) is superior to one that utilizes a command line, as it enables greater agility and faster programming and reduces errors.

SECTION II: DIGITAL TRANSFORMATION INCREASES IT COMPLEXITY

The innovation in IT over the past decade enables companies to do so much more than ever before. Workers have almost unlimited freedom to accomplish any task anywhere with a similar experience to being in the office. However, the complexity of IT is at an all-time high. Legacy IT was

built on a model of tight control in which the entire ecosystem was purchased, secured and controlled by the IT department. Each application had its own infrastructure and management tools and sometimes its own network.

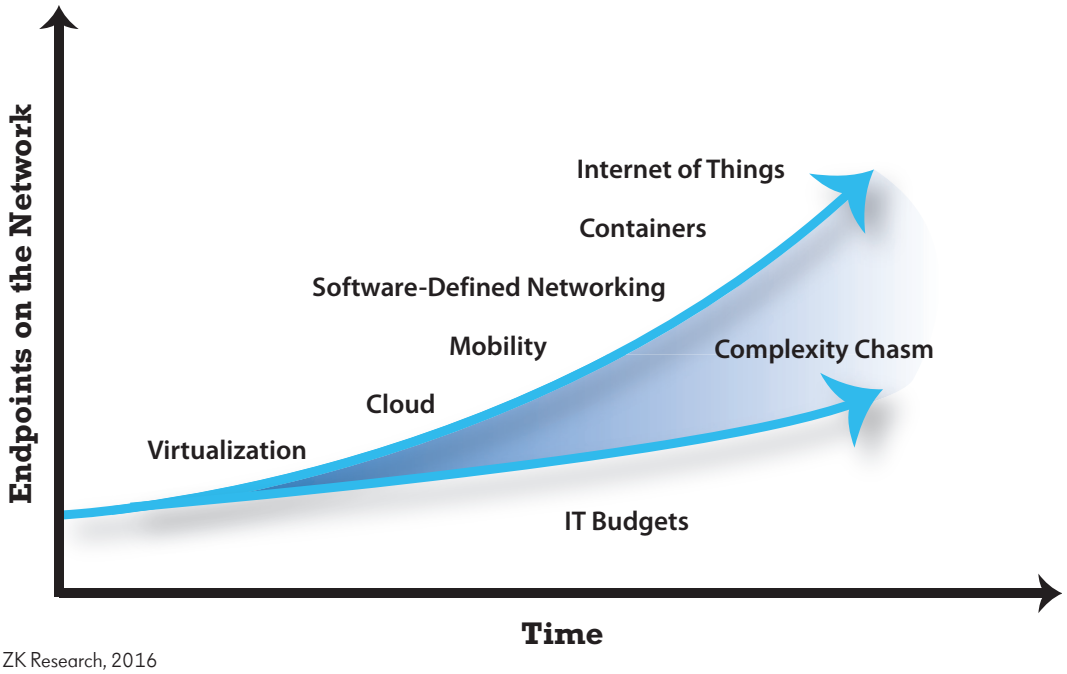
Today's modern applications use components and data from multiple sources; some may be running in virtual machines or containers or even in the cloud. The client can be a wired desktop connected over WiFi or cellular connectivity or be running in a browser. The worker can be located in a headquarters location, in a branch office, at home or literally anywhere in the world. Delivering applications was once a straightforward equation that has become exponentially more complex.

Looking ahead, many other technologies are coming—such as artificial intelligence, augmented reality and the Internet of Things (IoT)—that will widen the complexity chasm (Exhibit 2) even more, causing IT to fall farther behind.

The increased level of IT complexity has made it significantly harder to secure the infrastructure and manage application performance. In response, businesses have started to deploy more tools to solve specific challenges. On paper, the concept of having more tools might make sense, but "tool sprawl" brings numerous unintended consequences that can make managing the environment more difficult instead of easier.

One challenge is that most of these tools need to be connected to the SPAN or mirror port on a network device. Typically, there are only a few of these per network node, meaning that the tool can only be connected part of the time. Therefore, network managers must swap out tools to solve specific problems, which means historical information can't be stored for trending or troubleshooting purposes.

Exhibit 2: The Complexity Chasm Is Widening



ZK Research, 2016

The network is the common element that connects users, applications, devices and infrastructure to each other.

Also, most of the tools operate at different speeds and have a wide range of polling intervals. Some look at every packet, some look every few seconds and some look only periodically. This creates highly inconsistent views in which one system may show that the environment is fine and others might show some kind of problem. The IT department then must resort to several manual processes to determine if an issue exists.

Securing the environment becomes significantly more difficult as well. Legacy environments had a very well-defined perimeter with a single ingress/egress point. Today, every cloud application, mobile device and remote worker creates an additional entry point, which results in an asymmetrical security problem. Security teams must secure hundreds, or even thousands, of entry points, but hackers only need to find a single way in.

Solving these challenges may seem daunting, but it's necessary for businesses to increase the level of visibility of traffic flows in the infrastructure. For most organizations today, the network is the business, and end-to-end visibility can provide insights as to how applications are performing and help businesses quickly spot security breaches. And the best tool to maximize visibility is a network packet broker (NPB).

SECTION III: NETWORK PACKET BROKERS SIMPLIFY NETWORKS AND IMPROVE TOOL PERFORMANCE

All of the building blocks of the digital enterprise are network-centric paradigms. The network is the common element that connects users, applications, devices and infrastructure to each other. Because of this, it is uniquely positioned to provide the visibility necessary to change the way organizations manage and secure applications.

Security and network management tools are important components in the process of understanding network behavior and identifying anomalies that could indicate a breach or an application problem. As enterprises become dynamic and distributed, traffic volumes will explode following an increase in cloud and mobile traffic. Also, the level of encrypted traffic has risen steadily because of the erosion of the perimeter. Combine these factors with the expansion of software-defined networking, and it's easy to see why securing, monitoring and troubleshooting networks has become extremely challenging.

Traditional thinking is that new tools can help simplify things, but they can actually add to the complexity by introducing more infrastructure layers. This can diminish or even eliminate the return on investment companies were hoping to receive from performance and security solutions. Clearly, the digital era requires a new way of gaining complete visibility into the network and distributing traffic to a multitude of tools.

An NPB, also known as a monitoring switch, sits between the network infrastructure layer and the tools layer and can provide an unparalleled level of visibility. NPBs filter traffic from the network layer, aggregate it, perform several other actions and then pass it on to the tools layer. The devices also perform data preparation tasks by removing sensitive content, de-duplicating packets and decrypting traffic so the tools do not have to do so. This can significantly improve the effectiveness of security and monitoring tools.

For example, the ZK Research 2016 Security Survey found that 45% of respondents admitted to turning off security features in devices to improve performance. The need to perform non–security-related tasks, such as decrypting and encrypting traffic, can often overwhelm devices that were never designed to perform those tasks.

Also, without an NPB, every tool must be connected to every network device, creating a highly complicated mesh of connections that make troubleshooting and configuration difficult, if not impossible, to accomplish in large scale. With an NPB, each network element is plugged into it and the tools are then connected to it via a single connection. The NPB then determines the best traffic to send to each tool instead of having all traffic sent to every tool. NPBs provides a superior solution to improve the efficiency and utilization of security and monitoring tools rather than plugging all tools into the network devices directly (Exhibit 3).

An NPB is the best approach to handling and manipulating network traffic that offers end-to-end visibility at line rate. The result is an efficient, simplified network that makes network troubleshooting and threat detection easier. Exhibit 4 presents the key functions found in NPBs.

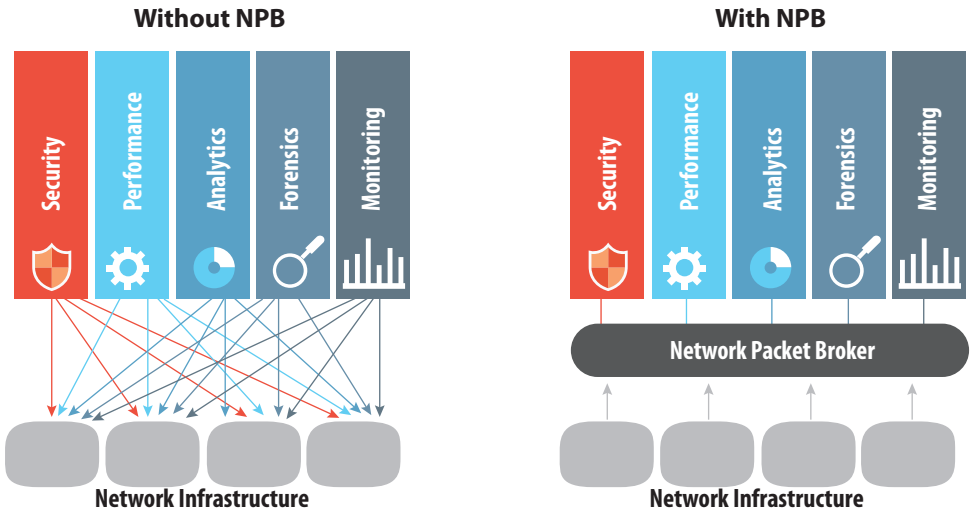
The following is a comprehensive list of functions that NPBs provide:

Aggregation of monitored traffic from multiple links and segments

Deep packet inspection and filtering that grooms traffic to relieve overburdened monitoring tools

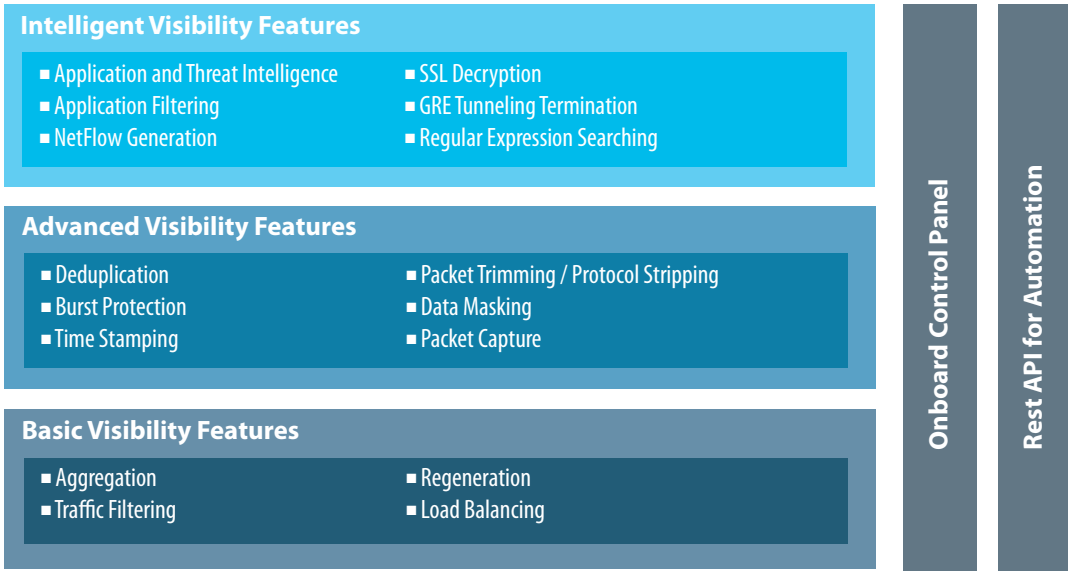
Load balancing of traffic across a variety of tools

Exhibit 3: Tool Access to Data Without NPB and with NPB



ZK Research, 2016

Exhibit 4: Network Packet Brokers Improve Security and Network Management



ZK Research, 2016

Regeneration of traffic to multiple tools

Time stamping and data masking to aid in compliance and working with sensitive data

Extended burst protection, available with the Advanced Feature Module, which offers traffic management and protection to online businesses subject to bursts of activity

SSL decryption for greater insight, including all traffic

Improved threat intelligence

NPBs come in a variety of form factors including modular, virtual and chassis-based systems to distribute and load balance network traffic being sent to expensive network and security tools. Businesses that deploy an NPB will realize a more granular view of how the network is performing, application performance issues and security threats. This technology should be considered a core component of every organization's digital strategy.

SECTION IV: IXIA OFFERS A VISUAL APPROACH TO NETWORK PACKET BROKERS

Ixia is the market leader in network testing and is a trusted supplier by the world's largest companies and service providers. The company has leveraged its expertise in networking to expand into the network packet broker market. Ixia offers a broad line of NPBs that are easy to use

and deliver intelligent filtering and distribution of traffic, including Layer 7 application flows and encrypted Secure Sockets Layer (SSL) at line rate with zero loss of packets.

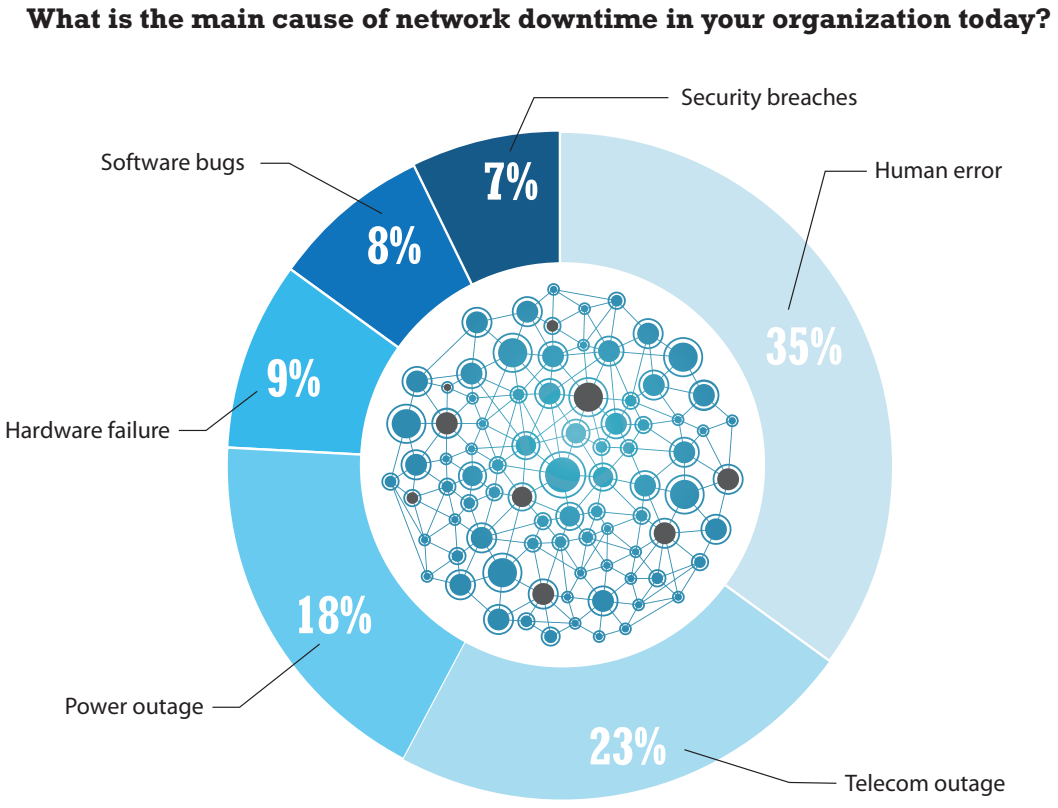
Although many network packet broker vendors compete in the market, Ixia takes a unique approach and is the only vendor to offer a GUI to configure and manage the product.

Other vendors require customers to use a cryptic, command-line interface (CLI) or complicated filter maps to manage their products. CLIs have been proven to be a huge source of downtime, as the largest cause of network downtime is from human error from misconfiguration through a CLI (Exhibit 5).

Ixia's user interface provides the following benefits:

Improved accuracy of monitoring filters: The monitoring filters can be thought of as the rules that create the intelligence in an NPB. Based on interviews with network managers, ZK Research estimates that monitoring filters have been created with errors at least 20% of the time when CLIs are used.

Exhibit 5: Command-Line Configuration Leads to Network Downtime



ZK Research 2016 Network Purchase Intention Study

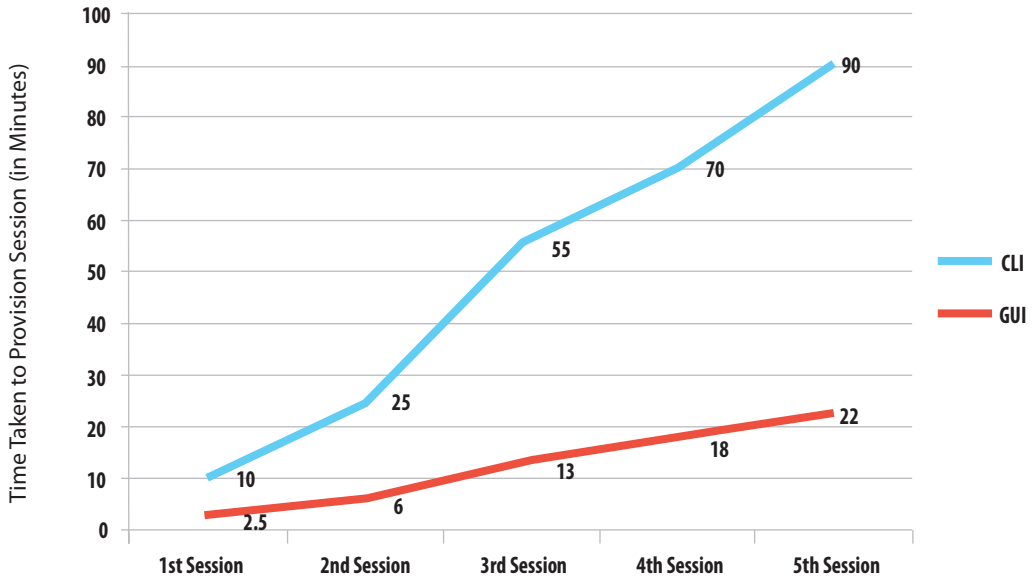
Faster provisioning than SPAN sessions: The process for creating SPAN sessions is long and tedious with CLIs and follows the process below:

1. Enter username and password to log in to the system.
2. Manually remove existing code to prevent coding problems.
3. Write new code.
4. Launch new code.
5. Monitor output data on the SPAN port, which may require a feed from a TAP to increase the accuracy of data and verify that the programming is correct.

The process of creating SPAN sessions is non-linear (the third step takes longer than the second, which takes longer than the first) because the troubleshooting and verification time increases with each monitoring session. Exhibit 6 shows how the time to provision sessions increases as more are configured.

Quicker filter-changing process: According to ZK Research, more than three-quarters of enterprises change connections between tools and NPBs at least twice a month, and each change requires programming modifications. CLI-based configurations and changes take four times longer than when using a GUI. This becomes significant because almost 50% of network managers spend more than half of their time configuring monitoring tools—leaving little time for innovation. Networks are becoming more dynamic and require more frequent updates, so Ixia's GUI can save network managers a significant amount of time, enabling them to spend more time on strategic initiatives and less on day-to-day tasks.

Exhibit 6: SPAN Session Configuration Time Increases per Session



ZK Research, 2016

The digital era has arrived, and it has introduced several new technologies that have increased business agility.

Lower cost of testing and troubleshooting filters: Each time a filter is created, it must be tested to ensure it passes the correct data through. An exhaustive test takes 1.5 to 2 hours to complete when a CLI is used. To streamline this process, network managers often do simple tests, which frequently miss critical information. Ixia's GUI allows exhaustive tests to be done in 15 minutes, the same time it takes to do a quick test with a CLI.

Intelligent filter interaction: With CLI-driven systems, engineers need to understand how filters interact with each other and write rules to accommodate. Ixia automates the process of filter interaction to ensure they work well together.

No troubleshooting requirements: With CLI-based products, extensive trial and error is needed to troubleshoot configuration problems. Ixia has a patented Dynamic Filter Engine (DFE) that removes potential misconfiguration and data-clipping errors. The engine checks every rule for errors. It supports overlapping filters and performs necessary actions in the background so it will not interfere with operations. The DFE saves operational time and money and significantly reduces the amount of time needed to resolve problems.

Faster network problem resolution: The ease of use enables customers to attempt to find network problems more often rather than contacting the vendor directly.

Drag-and-drop benefits – Short learning curve: Ixia's solution has an intuitive interface that makes it easy to use. No special training is needed—everything is as simple as "point and click" and "drag and drop." CLI and filter-mapping systems require long training periods, while Ixia's GUI requires none. Also, highly paid, senior network engineers manage CLI-based products, but Ixia's GUI allows more junior engineers to use the tools.

Many different NPBs are available to customers today, but Ixia's GUI-driven system provides all the benefits of traditional CLI systems without the associated risk and complexity. This can improve security, increase visibility, lower costs and significantly lower the cost of managing the network.

SECTION V: CONCLUSION AND RECOMMENDATIONS

The digital era has arrived, and it has introduced several new technologies that have increased business agility. Organizations can lower costs, respond to competitive pressures faster and boost worker productivity to new levels.

However, the corresponding increase in flexibility and improvement in resource utilization have an impact on IT. The IT complexity chasm is growing wider at an accelerating rate. As the cloud, IoT and data center modernization become mainstream, it's critical that organizations increase their

network visibility to understand who is on the network, identify threats and locate application performance problems. Visibility is critical to the success of a digital enterprise.

Historically, businesses have turned to using more tools to understand network traffic and improve security, but tool sprawl is now overwhelming IT operations. Network packet brokers can simplify the network, provide an unparalleled level of visibility and improve the utilization of management and security tools. IT leaders should make NPB investment a top priority today. With this understanding, ZK Research makes the following recommendations:

Focus on improving network visibility. It's impossible to manage and secure the network without understanding application traffic flows. Companies should set baselines and understand what changes are taking place to help network managers be more predictive and address issues before they affect users.

Understand the user experience. Using packet brokers to understand the user experience will enable IT to more directly measure the value of technology and create measurable ROI. An NPB is necessary to do this in a scalable, cost-effective way.

Lessen the reliance on command-line interfaces. CLIs have been the norm in network operations for decades. Although this was sufficient years ago, CLIs and data/filter maps are too slow and too error prone to be effective in the digital business era. Choose solutions—like Ixia's NPB—that have the rich range of features found in traditional systems but with the speed and ease of configuration of GUIs.

CONTACT

zeus@zkresearch.com

Cell: 301-775-7447

Office: 978-252-5314