WHITE PAPER

ixia

Creating a Visibility Architecture

A New Perspective on Network Visibility

915-6581-01 Rev. A, February 2014

Table of Contents

Introduction

Networking is a rapidly evolving and changing landscape. We've quickly moved from merely moving bits and bytes from workstation to workstation to providing powerful applications and services to millions of consumers. Speed and bandwidth requirements have grown exponentially, new traffic types appear daily, and now a functioning network is a crucial and necessary part of running a successful large or small business in any market.

Executive Summary

Ixia's Visibility Architecture is a holistic approach to network visibility that controls costs and administrative burdens, while optimizing the investment value of monitoring and security tools. Ixia's Visibility Architecture helps speed application delivery and enables effective troubleshooting and monitoring for network security, application performance, and service level agreement (SLA) fulfillment—and allows IT to meet compliance mandates. Ixia's Visibility Architecture enables IT to:

- Deliver better end-customer experience
- Gain visibility into both physical and virtual network traffic
- Ensure tools always get ALL the data they need for true end-to-end visibility and insight
- Simplify management of their visibility solutions by easily integrating with existing Network Management Systems
- Programmatically control the visibility framework to automatically adjust to dynamic issues and security threats
- Secure their data and networks with reliability
- Better leverage existing monitoring and security tools even while migrating the network to higher speeds

IT organizations are tasked with providing their customers with connectivity for communication and for their business critical applications. Customer expectations are now higher and more service-focused – infrastructure and simply creating a functioning network are mere "table stakes" in the network management game. IT is expected to provide the highest possible customer experience in a secure and always-up network environment.

In order to meet these new demands for impeccable service, IT organizations must deal with a myriad of dynamic forces that challenge their ability to meet expectations:

- Growth – Growth is a new constant. It encompasses all aspects of networking, from new users, new applications and services, new use cases, faster processing, migrating networks from 1GE to 10GE to 40GE and 100GE. In each case, change must be executed without a dip in "normal" service. The network must always be in a "stable and reliable" state.
- Workforce Mobilization – Users are on the move. People no longer expect to access the network from only one location. They expect to interact with data wherever they are.
- Infrastructure and technology changes – Change is the only permanent thing. With every new demand, new technology is created to meet the demand. Such advancements as virtualization, cloud services, and software defined networking (SDNs) must be seamlessly integrated into the existing network. At the same time, service level agreements (SLAs) must be maintained.
- Security – Change creates threat. Bring your own device (BYOD), social networking, a mobile workforce, and new services open up weaknesses in network defenses. With our ever-increasing use of networking, intrusions and exploits promise to compromise network security. These incursions can directly impact a businesses' competitiveness, compliance, and bottom line.

Network operators must continually monitor all these network areas for signs of trouble. Excuses – no matter how valid – won't help after the fact. Even with these challenges, IT organizations are expected to support multiple groups with a growing diversity of business critical applications. If there are outage, security, or connectivity issues, IT is expected to deal with these in real time as quickly as possible.

In order for IT to troubleshoot, isolate, and diagnose potential problems with the network or network functions, they need visibility into to the packets traversing the network. Access points to the network traffic (e.g., shortage of SPAN ports) are often limited.

Sometimes multiple tools from multiple groups covering different needs, all require access to the same points in the network. Limited access points create blind spots and complications – limiting the effectiveness of IT to quickly resolve issues. Making matters worse, the one area of growth IT organizations don't have is budget to purchase enough tools to provide complete visibility across their network. They often don't have budget to upgrade or replace their existing tools to higher speeds as networks upgrade from 1GE to 10GE or 40/100GE to match the growing demand for communication bandwidth.

Another critical issue is that monitoring tools have limited processing power and are designed with the assumption they will only receive the packets they need for analysis. This means it is crucial not to overload a tool with unnecessary data or the accuracy of their results degrades or worse simply stop working all together. In other cases, tools cannot provide the promised visibility insight unless they have a more end-to-end view of the network (packets from multiple locations within the network). Bottom line: it is crucial for IT to control what data is sent to each tool.

In general, IT organizations have embraced virtualization as it has many cost and scale benefits. Traffic between virtual machines (east-to-west traffic) has soared to more than 50% of all traffic on the network. This traffic increase creates a new kind of blind spot with new security and compliance challenges – how do you monitor data that does not physically exit the server? IT not only needs access to traffic on the physical network, but they urgently need access to traffic between virtual machines on the same server.

Additionally, security is a primary initiative for IT organizations. There is a growing need to protect against ever-evolving and more sophisticated threats. When it comes to monitoring traffic for security intrusions, an in-band approach is preferred to an out-of-band approach as it allows you to prevent a security threat rather than react to it. The issue with an inline approach is that placing the tool inline creates network reliability concerns. In many cases, it is not acceptable for the network to go down if the inline security tool fails. In other cases however, it may be crucial that all traffic is blocked if the inline security tool stops functioning.

Network and application security and visibility is not a luxury, but a necessity. What operators need is a "visibility architecture" – a smarter, more innovative approach to true end-to-end visibility that is simple to use, easy to scale, and provides immediate ROI on monitoring investments.

Traffic between virtual machines (east-to-west traffic) has soared to more than 50% of all traffic on the network. This traffic increase creates a new kind of blind spot with new security and compliance challenges – how do you monitor data that does not physically exit the server?

Key Attributes of a Visibility Architecture

Implementing a visibility architecture should address the people, processes, and technology issues facing IT organizations today. A successful visibility architecture must be manageable, scalable, automatable, and flexible – all while remaining simple and cost effective.

Manageable

First and foremost, a visibility architecture must be easily manageable. If the effort in controlling the visibility system only adds complexity and cost requirements of running the overall network, then it isn't cost effective. The visibility architecture must be designed foremost to help people with their problems while fitting into their existing processes. Integration into business processes must be seamless and easy, and for example must work with current network management system (NMS) and orchestration systems (i.e., SIEM). User authentication and access control features should be supported to meet compliance and security needs.

With a single pane of glass it is possible to manage local or distributed deployments and SNMP and RESTful APIs enable integrating reporting and alerting functionality into the IT organization's existing systems.

Implementing a visibility architecture should address the people, processes, and technology issues facing IT organizations today.

Scalable

As the network grows, the need to monitor and secure the network will also grow. A visibility architecture must easily scale to match network growth; but cost effectively! Managing the VA should not grow in complexity as new applications and technologies are added. The visibility architecture should be able to accommodate this growth in both the physical and virtual network realms.

Automatable

As the network grows more complicated and technologically diverse, automation becomes essential for enabling IT to manage security, ensure application performance and end-user experience in real-time. Automation is a key in a visibility architecture, as it helps reduce risk by automatically reacting to application issues and security threats in real-time. A visibility architecture must be able to automate these processes or alerts, and be able to dynamically control the data sent to tools as well as reduce risk by enabling security tools to enforce security policies in a dynamic environment.

IT Network Challenges:

- **Growing number of devices, application and monitoring tools**
- **Limited budgets**
- **Increasing customer expectations**
- **Mobilization of the workforce**
- **Virtualization of applications**
- **Virtualization of network devices and functions (SDN, NFV)**
- **Cloud Services (private and public)**
- **Growing and evolving security threats**
- **Compliance and regulatory demands**

Flexible

Networks are always evolving and changing by adding new processes, new services and applications, more users, new technology, etc. This change is constant, and will never abate. Any visibility architecture must adapt to this change without complications while supporting a path to future needs.

For example, a new application may come online that generates a new type of traffic. A new VLAN may be added to carry this new application. A new monitoring tool may be added to the network that needs to look specifically at this new application. It is important that as these changes occur, the visibility products do not require manual reconfigurations to account for broken traffic filters. A good visibility architecture should account for this and reconfigure filters automatically. Another example is when migrating the network from 1GE to 10GE, 40GE, or beyond, your existing tools should continue to be leveragable. This extends tool ROI reducing CAPEX while also reducing churn since IT engineers are already familiar with these existing tools.

Your visibility architecture must easily adapt so you don't have to constantly manually update – and it must be done so that the change is transparent and hitless to ensure the monitoring and security tools have all the data they need to provide accurate analysis.

Your visibility architecture must easily adapt so you don't have to constantly manually update – and it must be done so that the change is transparent and hitless to ensure the monitoring and security tools have all the data they need to provide accurate analysis.

Simple

Keeping up with the changes and new technologies in your network is complicated enough.

A visibility architecture must fit within your organization's processes, have an intuitive visual/graphical interface anyone can use, and provide timely feedback confirming proper operation – otherwise it is just another liability to be dealt with. A proper visibility architecture must be recognized by the users as the easiest solution to fixing network problems when they arise.

Ixia's Visibility Architecture

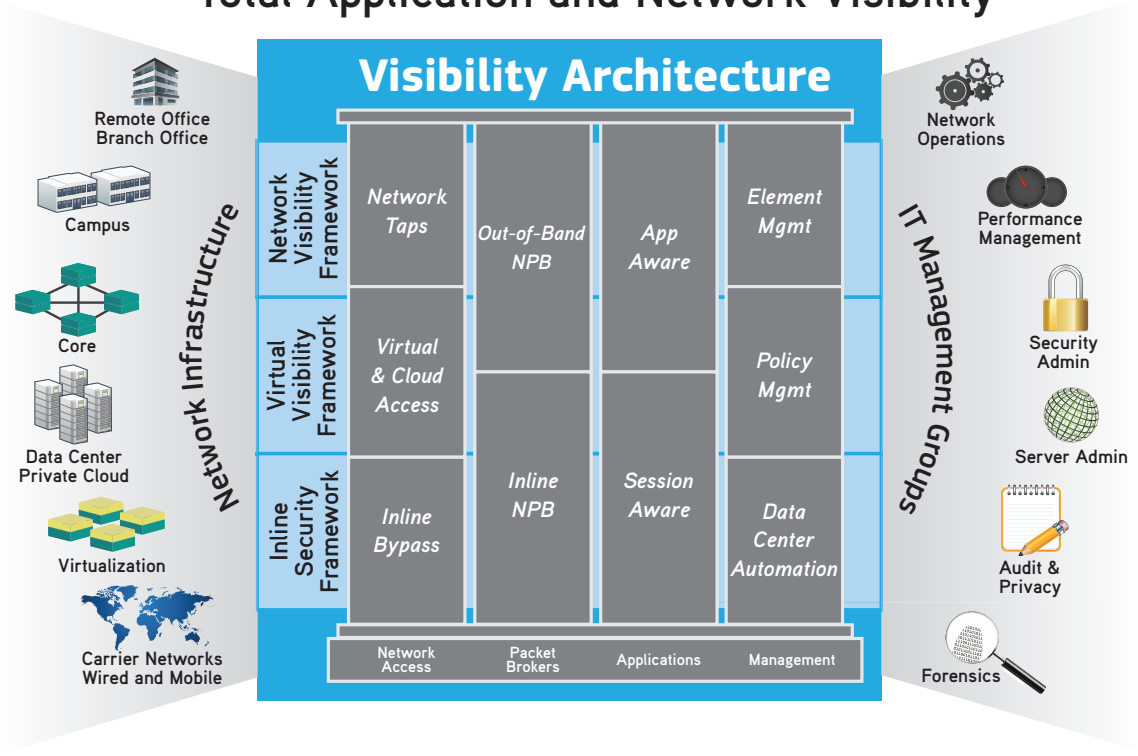
As we just discussed, the only way to achieve scalable, reliable, and sustained visibility is with a holistic and strategic approach to visibility. IT operators must be able to, at a glance, get insight into the totality of the network traffic and security picture. What is happening, where is it happening, is it secure, and – most importantly – why is it happening? Building this type of insight requires not just single solutions at various points in the network, but an end-to-end architecture for monitoring and security that scales along with network growth, that can adapt to new types of applications, and evolves to meet new demands. An easy-to-use and easily-adaptable intelligent visibility architecture is needed to make sure that you have a new perspective on the blind spots in the network.

Ixia's Visibility Architecture allows network, application, and security teams to ensure the network is operating efficiently and securely today – and is ready for any changes coming tomorrow. Network teams can confirm their tools are receiving the right information at the right time and react quickly to new security threats or network requirements. Ixia's Visibility Architecture helps IT achieve end-to-end physical and virtual network and security visibility by giving these tools access to data at any point in the network without compromising network performance or reliability.

Ixia's Visibility Architecture eliminates the compromises that are often made regarding network application and security visibility by integrating easily into existing data center environments and delivering the control necessary to improve the usefulness of and insight gained from existing tools. This provides IT with solid ROI for other management systems, as well as providing an adaptable environment than can fit to your needs. Ultimately, Ixia helps IT professionals deliver on their service level agreements (SLA), meet their key performance indicators (KPI), and provide best-in-class customer service.

Ixia's Visibility Architecture is built on the foundation of a broad and innovative visibility product portfolio. This portfolio starts with a comprehensive offering of access products that include both network and virtual Taps as well as specialized Inline Bypass switches. Then inline and out-of-band capable Network Packet Brokers provide the advanced functionality needed to improve tool performance as well as scale existing tools for higher network speeds. Application and Session aware capabilities bring more intelligence to the VA. And finally there if policy and element management of these products with capabilities to automate processes and integrate into existing management systems.

Total Application and Network Visibility



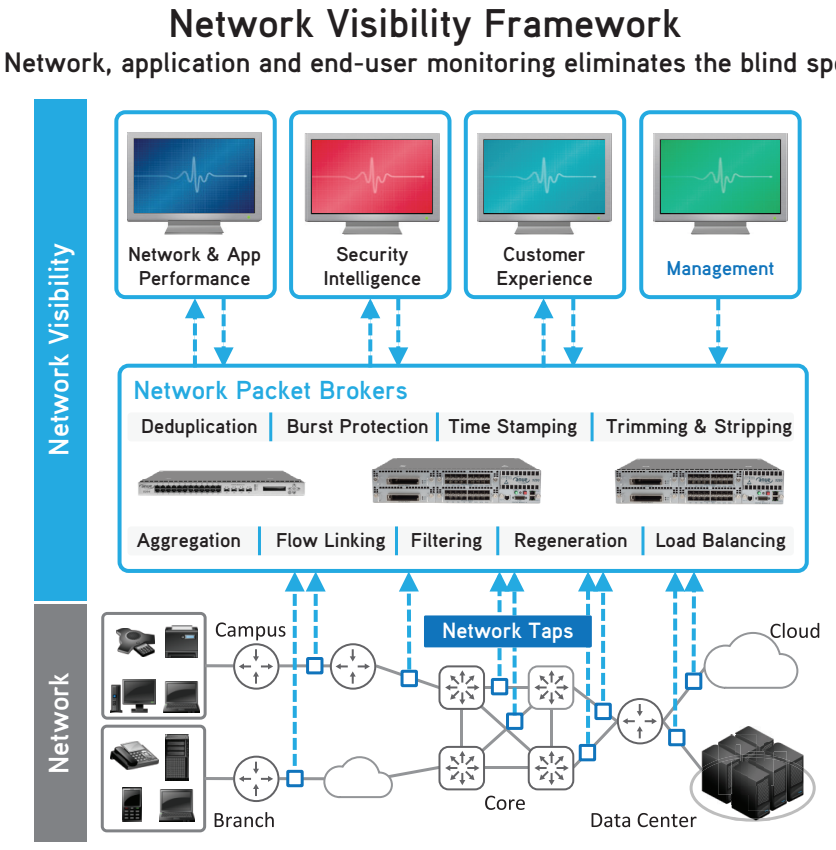
The Ixia Visibility Architecture Framework

There are three solution sets, or frameworks, that make up the Visibility Architecture – which together address key areas of visibility in the physical and virtual networks, as well as the unique reliability requirements needed for in-line security devices. They are highlighted below :

- Network Visibility Framework
- Virtual Visibility Framework
- In-line Security Framework

Network Visibility Framework

The Network Visibility Framework enables true end-to-end monitoring of the network, applications, and end-users – greatly reducing mean time to repair (MTTR). This greater visibility also opens up the opportunity for IT organizations to provide guaranteed services to end-users, with service assurance metrics to manage and prove service level agreements (SLAs).



The Network Visibility Framework provides a simple, scalable approach using management features that can integrate into existing work-flow processes and global network management systems (NMS).

To achieve these goals, the Network Visibility Framework resolves the classic problem of monitoring and security tools not having enough access to the network. Lack of access is what leads to poor visibility into network and application issues. The Netowrk Visibility Framework provides a simple, scalable approach using management features that can integrate into existing work-flow processes and global network management systems (NMS). Network taps provide the reliable access points, while network packet brokers (NPBs) provide the advanced filtering and aggregation to ensure the tools have access to all the data they need.

NPBs also provide other advanced functions, such as aggregation, deduplication, trimming, stripping, and load balancing (to name a few). For example, de-duplication along with filtering and other features ensures the tools are not overwhelmed with unnecessary data that degrades the accuracy and reliability of their analysis. NBPs also allow organizations to leverage existing tools even as they migrate their networks to higher speeds (i.e., 10GE, 40GE, or even 100GE). This saves a tremendous amount of CAPEX by using existing tools, as well as OPEX since the team is already trained and familiar with the tools they have today.

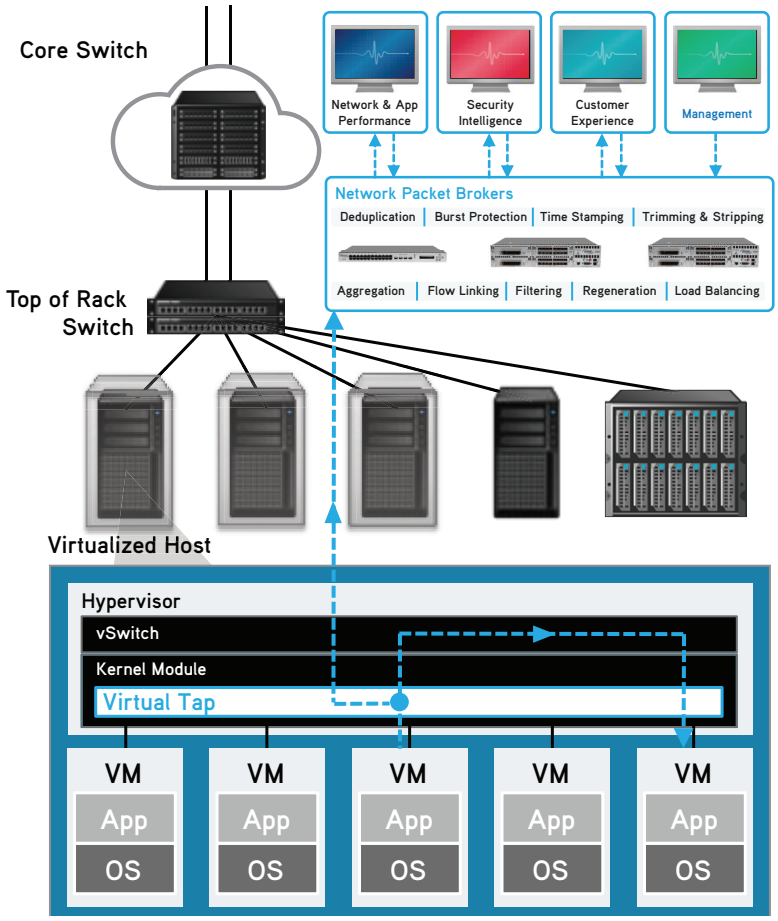
With Ixia's APIs it is possible to program the visibility framework to intelligently adjust in real-time to changing issues and emerging security threats. For example, monitoring tools can dynamically control the NPBs to request data from a specific application or IP address(es) as they detect anomalies in the network. This intelligent and automatic response greatly speeds security and network event diagnosis.

Ixia's Network Visibility Framework brings a scalable, more intelligent approach to network visibility with integrated management capability.

Virtual Visibility Framework

Ixia's Virtual Visibility Framework enables traffic interception between virtual machines within a single host machine (otherwise known as east-west traffic, which never physically leaves the host) for monitoring purposes. This is accomplished with a "virtual tap" installed on the Hypervisor Kernel itself in order to operate with little impact to the server's performance. A single solution supports all the major Hypervisor vendors such as vSphere, KVM, Hyper-V and Xen. This simplifies installation and deployment.

Ixia's Virtual Visibility Framework enables traffic interception between virtual machines within a single host machine (otherwise known as east-west traffic, which never physically leaves the host) for monitoring purposes.



It has been estimated that up to 80% of traffic is between virtual servers. The recent widely-publicized security incidents involving the theft of millions of credit card details at major retailers has shown us that virtual traffic is simply too risky to ignore.

Using the Virtual Visibility Framework, traffic in the virtual network can be monitored with virtual tools or sent to the physical network. In the physical network, we can leverage all

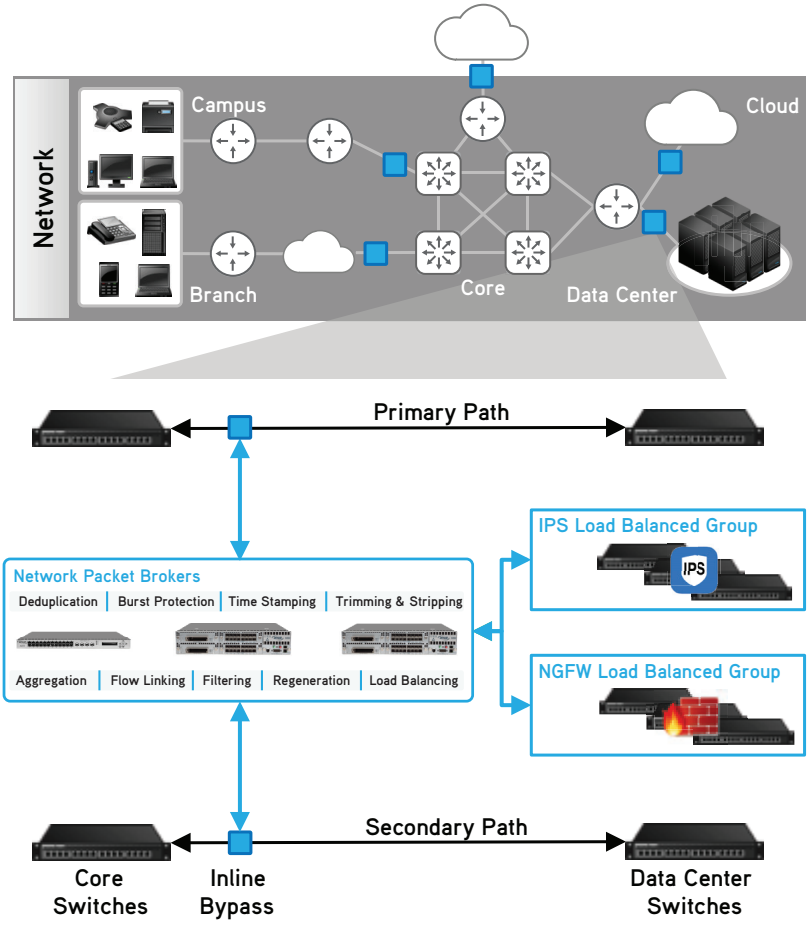
the capabilities and benefits of NPBs in order to efficiently distribute this traffic to existing physical tools.

If an issue occurs with an application, virtual visibility allows you dive in to the problem from a true end-to-end perspective using from a single management pane. It provides visibility coverage from the end-user to the core to the data center, whether in the physical or virtual domain. More rapid and efficient troubleshooting reduces effort and time to resolve critical application and security issues.

Inline Security Framework

Ixia's Inline Security Framework enables enacting network security measures and tools inline in a fail-safe and reliable way (especially where network reliability is paramount). Inline Bypass switches allow you to place tools such as IPS and Next Generation Firewalls logically inline, without compromising the integrity of the network. Enabling inline security monitoring allows for prevention rather than reaction to security threats. The Inline Bypass switches are designed with a cut-through architecture for low latency operation, and use simple bidirectional heartbeat protocols to automatically detect if a tool has gone offline. This means that crucial security tools can fail open or close to maintain network connection and security posture as needed.

Ixia's Inline Security Framework enables enacting network security measures and tools inline in a fail-safe and reliable way (especially where network reliability is paramount).



Even better, employing Ixia's Inline Security Framework gives you the ability to load balance traffic between multiple security tools. If one security tool fails, it is possible to automatically rebalance traffic among the remaining tools to maintain security operation.

The Inline Security Framework allows the IT organization to leverage multiple low-speed tools to monitor higher-speed links. This allows you to scale investment in tools as needs and requirements grow – without breaking the budget and only paying for the capacity needed today.

Conclusion

Change is coming to networks faster than ever before. While growth is a new constant in most networks, it is being compounded by new regulations, virtualization of workloads and services, changing security needs, and migration of applications between data centers and the cloud.

Today, we see a tremendous change in user expectations driven by the "consumerization of IT." In the networking game, infrastructure and application management are quickly becoming "table stakes." Enterprise organizations and service providers are spending more time focused on delivering customer service.

Companies no longer have to make compromises when it comes to network, application and security visibility.

Network and IT organizations are caught in a constant cycle of deploying new services, supporting new use cases, and managing growth – which results in networks that are always trying to get back to a reliable state before the next rounds of change hits.

One of the results of these changes over the last 15-20 years is there are more monitoring, visibility, and security tools in use today than ever before. In fact, these tools are typically required today for all enterprise data center and campus networks, as well as service provider IT, data, and LTE production networks.

But all of these tools need access to data on the production network. In fact, most of the tools function better when they get data from across the entire network, including the data center, security DMZs, the network core, and the different campus and remote office locations. However, the problem is many of these tools aren't getting the data access they need.

IT needs end-to-end visibility, meaning tool access to any point in the physical and virtual network, and it has to be scalable and easy to manage. But more than that, IT needs control. These tools often can't handle all the traffic from across the network, so IT needs the ability to control what information is directed to each tool – and they need to do all this within existing budget constraints.

Ixia's Visibility Architecture helps companies achieve end-to-end visibility and security in their physical and virtual networks by giving their IT tools access to data from any point in the network. Regardless of network scale or management needs, Ixia's Visibility Architecture easily integrates into data center environments and delivers the control and simplicity necessary to improve the usefulness of existing tool investments. Companies no longer have to make compromises when it comes to network, application and security visibility. Ultimately, Ixia helps IT personnel deliver on their service level agreements, meet their key performance indicators, and provide best-in-class customer service.

ixia

Ixia Worldwide Headquarters
26601 Agoura Rd.
Calabasas, CA 91302

(Toll Free North America)
1.877.367.4942

(Outside North America)
+1.818.871.1800
(Fax) 818.871.1805
www.ixiacom.com

Ixia European Headquarters
Ixia Technologies Europe Ltd
Clarion House, Norreys Drive
Maidenhead SL6 4FL
United Kingdom

Sales +44 1628 408750
(Fax) +44 1628 639916

Ixia Asia Pacific Headquarters
21 Serangoon North Avenue 5
#04-01
Singapore 554864

Sales +65.6332.0125
Fax +65.6332.0127

915-6581-01 Rev. A, February 2014