Official Partner

AVIZENT
Network Solutions

Solutions
OVERVIEW

ixia

915-0117-01 Rev C

CONTENTS

IXIA SOLUTIONS OVERVIEW

An always-on, always-available Internet experience has fundamentally changed the way we do business. Networks are no longer simply connected machines providing bits and bytes of uncomplicated data. They are now vast multi-technological powerhouses with global reach that provide media of all types. We rely on these networks to reach other people, other places, and other businesses.

Ixia provides testing, visibility, and security solutions, strengthening applications across physical and virtual networks. Ixia's solutions emulate realistic media-rich traffic and network conditions so that customers can optimize and validate the design, performance, and security of their pre-deployment and production networks. Ixia's solutions flow across all network types and designs: from enterprises and government agencies to service providers and network equipment manufacturers (NEMs).

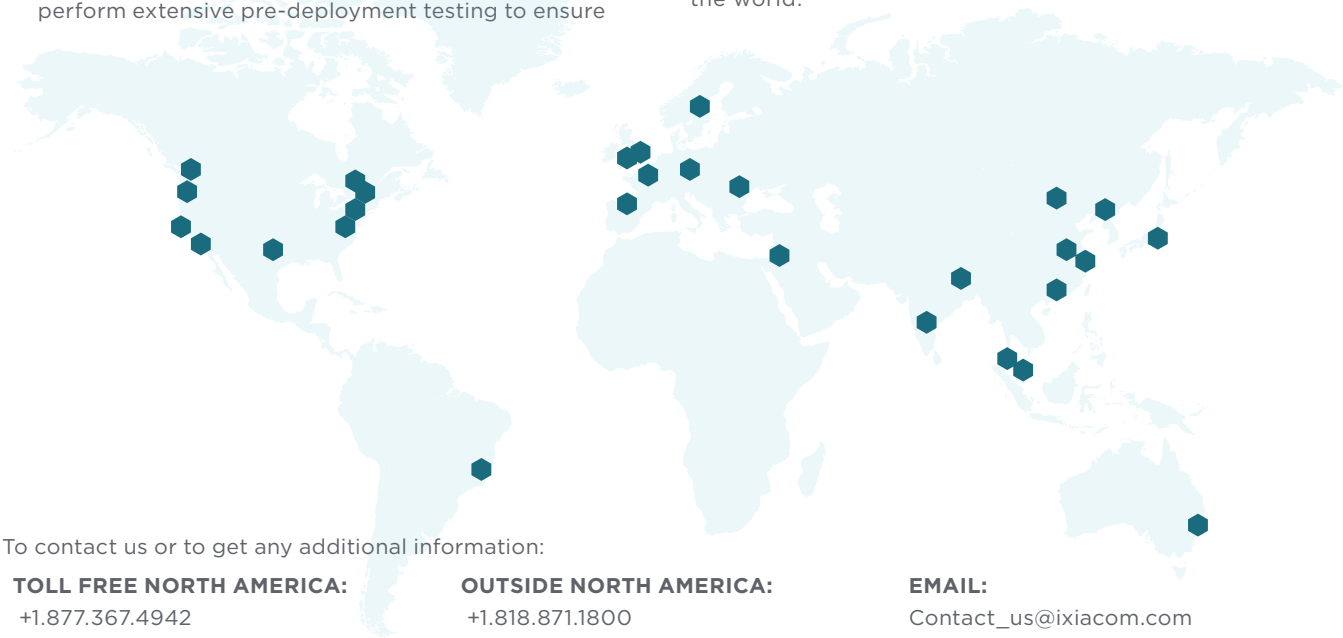
Applications provide many benefits, but they all have bugs and blind spots. Making them stronger requires better testing, security resilience, and monitoring. Ixia takes a three-pronged approach to making applications stronger with IxTest™, IxSecure™, and IxVision™ architecture capabilities.

Ixia's customers benefit from faster time-to-market, optimized application performance, and higher-quality deployments, ensuring that their applications run stronger.

Founded in 1997, Ixia is an international, public company with more than 1,700 employees. Operating worldwide, Ixia has vast expertise in working with our customers to help meet their networking goals:

- Ixia test solutions with IxTest provide an end-to-end approach for organizations to test devices and systems prior to deployment and assess the performance of networks and data centers after upgrades or changes. To verify new service implementation, new device insertion, or network expansion, IxTest helps organizations perform extensive pre-deployment testing to ensure current network functions are not compromised. This testing must be high capacity and simulate networks and applications over-subscription in order to stress network upgrades to their limits.
- Ixia security solutions with IxSecure allow organizations to assess network security and resiliency by testing and validating network and security devices with real-world application traffic and attacks. Using IxSecure, organizations can perform assessments before production deployment and establish ongoing best practices that harden security by assessing individual devices, networks, and data centers. In operation, Ixia solutions monitor traffic—clear and encrypted—to keep malware out, enable security tools to be more efficient by filtering out known bad traffic, and ensure security is resilient and highly available.
- Ixia visibility solutions with IxVision are uniquely positioned to help organizations manage and monitor change in their networks. IxVision provides 100% access without dropping packets, visibility intelligence, load balancing at line rates, and context knowledge to serve the right data to the right tool. Ixia has the most complete visibility portfolio on the market, allowing our customers to build a visibility architecture that best fits the need of their network today—and in the future.
- Ixia's wireless and Internet of Things (IoT) test solutions address the complex challenges mobile operators face in rolling out high-quality, differentiated services. Mobile operators can use Ixia's award-winning Long-Term Evolution (LTE) and Wi-Fi test systems and services to subject devices and configurations to high-stress, high-scale conditions, and a wide mix of voice, video, and data applications. Operators can evaluate the subscriber experience in the face of mobility, system overload, and even device failure on a large-city scale. And with IoT test solutions, they can ensure that their Wi-Fi implementations are robust, cause no interference, and operate as specified.

Join our ever-growing customer base of successful service providers, enterprises, network equipment manufacturers (NEMs), government agencies, data center operators, and cloud providers. We have offices to serve you all over the world.



To contact us or to get any additional information:

TOLL FREE NORTH AMERICA:
+1.877.367.4942

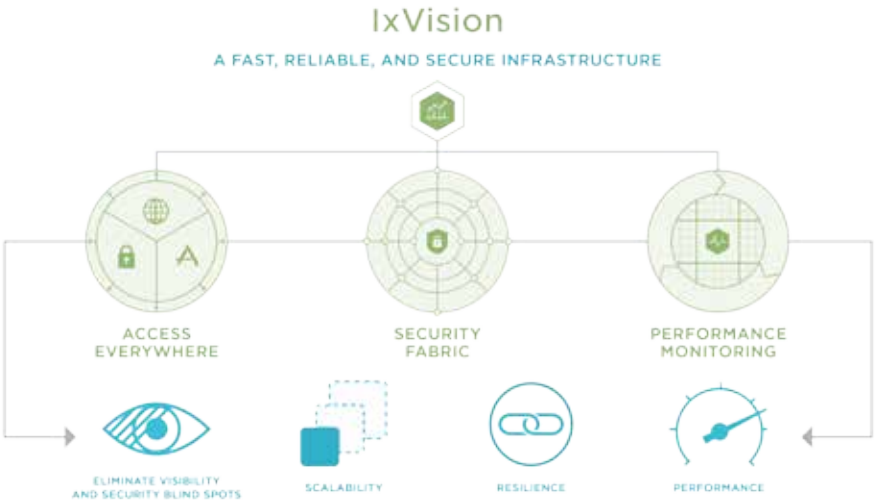
OUTSIDE NORTH AMERICA:
+1.818.871.1800

EMAIL:
Contact_us@ixiacom.com

Visibility
SOLUTIONS

ixia

NETWORK VISIBILITY ARCHITECTURE



SCENARIO

Today's networks are growing in both size and complexity, presenting new challenges for IT and network administrators. More mobile devices are connecting to more data from more sources—and much of that is due to virtualization. IT challenges are further complicated by increasingly high customer expectations for always-on access and immediate application response. This complexity creates network "blind spots" where latent errors germinate and pre-attack activity lurks.

Blind spots are commonly caused by the following issues: poor use of Switch Port Analyzer (SPAN) ports and lack of tap ports, limiting tool access to data; dropped and duplicated packets, which suppress or delay actionable information; SSL encrypted traffic that may be hiding malware; and monitoring plans that are behind migration cycles. Stressed out monitoring systems make it hard, if not impossible, to keep up with traffic and filter data "noise" at a rate that they were not designed to handle.

Network blind spots have become a costly and risk-filled challenge for network operators. Further, unseen inter-VM and cross-blade data center traffic leaves the network vulnerable to threats, noncompliance, loss of availability, and impaired performance. Today, up to 80% of data center traffic can travel between servers, making end-to-end visibility a real challenge.

The answer to these challenges is a highly scalable visibility architecture that helps eliminate blind spots, while providing resilience and control without complexity. Ixia's IxVision Architecture delivers intelligent, resilient, and proactive network visibility.

IXIA'S VISIBILITY SOLUTIONS

The IxVision architecture is founded on a comprehensive product portfolio of high-performance taps, virtual taps, bypass switches, and NPBs, all easily deployed and managed. IxVision helps speed application delivery and enables effective troubleshooting and monitoring for network security, application performance, and SLA fulfillment—and allows IT to meet compliance mandates.

IxVision provides a solution to support both out-of-band and inline monitoring in the physical and virtual network. The Security Fabric, a key pillar of IxVision, enables fail-safe deployment of multiple inline and out-of-band security enforcement and performance tools, such as Intrusion Prevention Systems (IPSs), next-generation firewalls (NGFWs), Application Performance Monitor (APMs), Network Performance Monitor (NPMs), etc.

IMPROVED PERFORMANCE WITH IXVISION

Ixia's Visibility Architecture improves performance by providing:

- **Full network visibility** – Consistently send all the right data to the right tools by matching multiple filter criteria, eliminating dropped packets due to overlapping filter conflicts
- **Automated response technology** – Instantly re-route traffic to monitoring tools based on suspicious activity so that you can reduce the time and cost of human intervention to remediate network problems
- **Load balancing** – Distribute monitoring traffic to several analysis tools so that you can fully use network bandwidth and boost the efficiency of your monitoring tools, even if they are lagging the network in bandwidth
- **Sophisticated filtering and de-duplication** – Increase monitoring tool performance by eliminating unnecessary data before it reaches the tool so that you can more easily adhere to compliance standards and generate more accurate tool statistics
- **Zero packet loss** – Deliver 100% of packets without dropping or losing them due to load
- **Easy-to-use** – Ixia's NPBs are powered by a user-friendly drag-and-drop interface that allows you to easily connect monitoring tools to appropriate SPAN and tap ports with the simple click of a mouse

SIMPLIFIED MANAGEMENT

- Create network connections and filters by using the intuitive GUI so that you can aggregate, filter, and distribute network traffic to monitoring tools with a few clicks of the mouse and virtually eliminate the need to rewire equipment.

- Restrict access to specific filters, ports, or monitoring tools by delivering improved access control management to meet compliance and regulatory requirements.
- From within Vision ONE, NTO, or xStream, monitor key SNMP statistics from any network management system so that you can view and report on key information, such as the amount of traffic each tool receives and instant notification of oversubscribed tools.
- Accommodate your organization's increasing need for more IP addresses by easily accessing Vision ONE, NTO, or xStream using IPv4 or IPv6 addresses.

CAM BEASLEY
Chief Information Security Officer, University of Texas

Ixia's solutions outperformed the competitors we reviewed, offering an industry-leading GUI, dynamic filtering, and improved network responsiveness.

SUGGESTED PLATFORMS	
Vision One	• All-in-one tool for lossless visibility for both inline and out-of-band tools • Intuitive GUI • ATIP, AFM, SSL Decryption • 48 10GE/1GE SFP+ ports and 4 40GE QSFP+ or 16 port 10GE
NTO 7300 (and NEBS 3 compliant 7303) Chassis	• Highest density NPB with up to 384 ports of 10GE in 7U, including up to 192 ports of 10GE or 48 ports of 40GE AFM (Advanced Functionality) • Wire-speed performance • ATIP, AFM, Packet Capture Module
NTO 5288 High-Density 40G	• Up to 64 10GE ports • Offers an efficient and scalable solution to monitor 1, 10, and 40GE
NTO 5236 Enterprise Class	• 10GE visibility for fiber network monitoring tools • Up to 24 SFP/SFP+ Ethernet ports
AFM	Enhance Vision ONE and NTO's capability to aggregate, replicate, and filter network monitoring traffic
ATIP	Gather real-time application data for actionable insight into network activities
Packet Capture Module (PCM)	Capture packet anomalies for quick analysis and solutions at 40GE line rate
xStream 40	Fail-safe inline security network packet broker with aggregation, filtering, and load balancing for 10GE/40GE Networks
Bypass Switches	Fail-safe devices to ensure uptime and high availability of monitoring and security deployments
Taps, Link Aggregators, Tap Aggregators	Copies and sends traffic of interest to the tools that are monitoring your physical network
Phantom™ vTap	Get visibility into the traffic between virtual machines in virtualized environments
CloudLens vPB	Virtual appliance offering packet broker services such as aggregation, filtering, deduplication, and distribution of virtual traffic



Vision ONE


NTO 7300


NTO 5288


NTO 5236


AFM


PCM


xStream 40


Bypass Switches


Taps, Link Aggregators, Tap Aggregators


Phantom vTap

SCENARIO

Proper network access starts with a tap. Taps provide non-intrusive access to data flowing across the network and enable monitoring of network links. Taps are primarily used to optimize passive monitoring of a network link. They are normally placed between any two network devices, including switches, routers, and firewalls to provide network and security personnel a connection for monitoring devices. Taps are used for troubleshooting and offer continuous, non-disruptive network access.

Protocol analyzers, Remote Network Monitoring (RMON) probes, intrusion detection systems (IDSs) and IPSs, and other monitoring tools can now be easily connected to and removed from the network when needed. By using a tap, you also eliminate the need to schedule downtime to run cabling directly to the monitoring device from network devices, thus saving time and eliminating possible cabling issues.

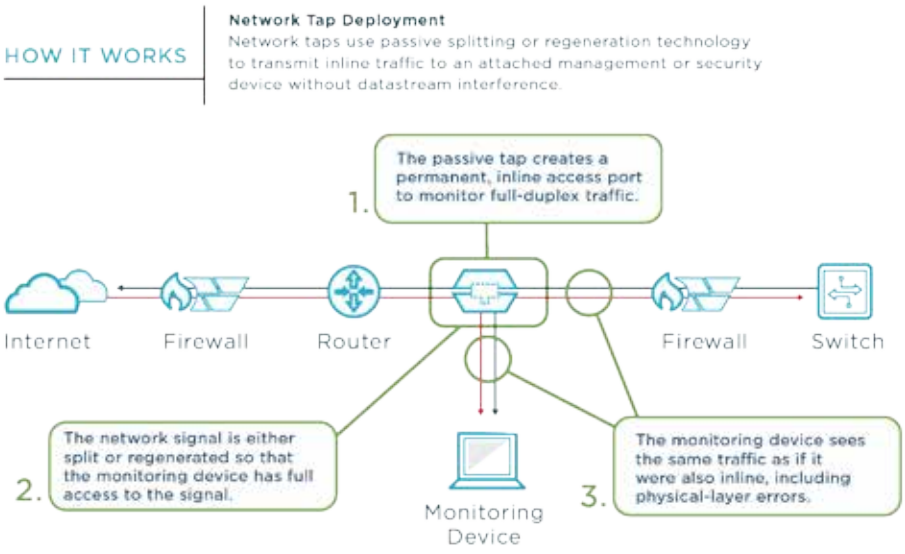
Any monitoring device connected to a network device receives the same traffic as if it were inline, including all errors. This is achieved as the tap duplicates all traffic on the link and forwards it to the monitoring ports. Taps do not introduce delay nor alter the content or structure of the data. Fiber taps are usually passive and do not require power. Copper taps and other powered fiber taps are designed to allow traffic to continue to flow even when power is removed.

IXIA SOLUTIONS

The Ixia family of taps provides 100% visibility and permanent passive access points into your network. When a monitoring tool is needed, simply connect the device to the tap instead of taking down the link and interrupting traffic. Taps pass all network traffic—including Layer 1 and 2 errors—without introducing bottlenecks or points of failure.

Regardless of interface or location in the network, we provide a tap solution, supporting copper and multimode and single-mode fiber at speeds up to 100Gbps with media conversion models available.

SUGGESTED PLATFORMS	
Flex Tap	1/10/40/100G fiber interfaces and highly modular
Slim Tap	Measure traffic loads on networks that carry VoIP, videoconferencing, and security applications
Gig Zero Delay Tap	Industry's only 10/100/1000BaseT tap with true zero-delay operation to prevent network disruptions for maximum network reliability
10/100/1Gb Copper Tap	Visibility for 10/100/1Gb network monitoring and security devices
BiDi Tap	Fiber Flex Tap module designed for use in Cisco 40G BiDi networks, specifically ACI
Phantom vTap	Visibility into traffic between VMs; support VMware ESXi and NSX, Openstack KVM and Microsoft Hyper-V
Regeneration Tap	Enables multiple tools to monitor the same network traffic while adding the flexibility of modular SFP-based monitor ports
Link Aggregation Tap	Provide the reverse service of the regeneration tap; depending on the model, a link aggregation tap aggregates network traffic copies from multiple links onto a single monitoring port
Port Aggregation Tap	Provide access to a single network segment; enables you to view full duplex traffic with a single NIC per device, instead of two
Bypass Switches	Fail-safe devices to ensure uptime and high availability of monitoring and security deployments



INLINE NETWORK VISIBILITY SOLUTIONS

SCENARIO

Along with increased security threats and tighter regulatory compliance requirements, today's networks are delivering more services and carrying greater amounts of multi-protocol traffic at higher data rates. Monitoring and security tools need to be deployed inline to inspect every packet and block incoming threats before they affect the network and potentially disrupt business.

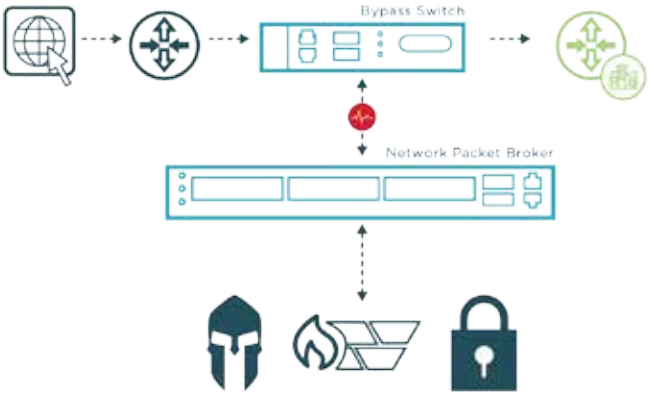
Deployment of any inline tool in the network carries the risk of the tool becoming a point of failure. Should the inline tool become unavailable, it can bring the network link down, making a critical segment of the network unavailable and affecting uptime. To avoid this risk, customers need a fail-safe solution that can protect the network from tool failures while allowing inline tools to protect the network from incoming threats.

A bypass switch is a specialized network device that provides fail-safe inline tool protection for security and monitoring devices. It uses a heartbeat packet to protect the network link from application, link, or power failure on the attached monitoring device.

Specialized packet brokers can then take this inline traffic and filter it at line rate to groom the data quickly and efficiently for the specific inline tools being deployed (IDS, IPS, threat prevention, etc.).

Key benefits of packets brokers used in this scenario include:

- Tool-sharing reduces costs by allowing multiple departments in an organization to use the same monitoring tool to monitor multiple links throughout the organization
- Filtering increases efficiency and maximizes tool use by sending each tool only the traffic it needs
- Tool load balancing protects the investment in existing monitoring tools by splitting the load from 10G and 40G links to 1G and 10G tools
- Relieves oversubscribed tools through load balancing and packet slicing



IXIA SOLUTIONS

Ixia offers many solutions for inline security as part of the inline Security Fabric, including both bypass switches and packet brokers. For bypass switches, this includes a combination of copper or optical interfaces and a range of different network speeds.

The Ixia iBypass 40-10 is an intelligent bypass switch that provides inline tool protection for inline network link deployments. The iBypass 40-10 augments network-monitoring capability through the use of microsecond resolution heartbeat packets, Simple Network Management Protocol (SNMP) traps, field-upgradeable software, and an easy-to-use web-based user interface.

The iBypass switch continuously checks the responsiveness of the inline tool by sending it heartbeat packets, expecting to receive those packets back. If the iBypass switch detects that the tool is not responding, it will bypass the inline tool, allowing network traffic to flow without interruption. Should that happen, the iBypass switch issues an alert to indicate that the tool became unavailable, allowing network or security personnel to take appropriate actions.

The iBypass switch continues to send heartbeat packets to the inline tool even after the tool stopped responding. As soon as the tool becomes operational again, the iBypass re-routes traffic back through the tool to ensure that the tool is continuing to monitor and/or protect the network.

Vision ONE and xStream 40 are NPBs for monitoring high-speed network traffic, letting you share the network's rapidly increasing traffic load among multiple tools. The need to record and inspect all traffic on high-volume 10G and 40G networks puts pressure on organizations to invest heavily in new 10G and 40G tools or risk oversubscribing their current tools.

Now, Vision ONE or xStream 40 enables deployment of multiple tools in parallel, with traffic balanced between them. This approach allows you to use IPSs, firewalls, web accelerators, and other inline tools more efficiently. It also offers a comprehensive set of high availability features that are critical for fail-safe inline security tool deployment.

SUGGESTED PLATFORMS	
xStream 40	40GE visibility for fiber network monitoring tools
Vision ONE	40GE all-in-one tool for lossless visibility for both inline and out-of-band tools with an intuitive GUI and support for ATIP, AFM, PCM, SSL decryption
iBypass 40-10	Fiber, 40GE, SR, 50µm, QSFP+ cages; protects 4-10GE links
10/100/1Gb Copper Bypass Switch	Copper Ethernet interfaces up to 1GE

OUT-OF-BAND NETWORK VISIBILITY SOLUTIONS

SCENARIO

Taps serve as a starting point for creating a visibility architecture. However, a problem arises if you try to connect monitoring tools directly to a tap. Those tools become flooded with too much data, which overloads them, causing packet loss and CPU overload.

This is where an NPB is useful. These devices filter the data to send only the right data to the right tool. Packets are filtered at the Layer 2 through Layer 4 levels. Duplicate packets can also be removed and sensitive content stripped before the data is sent to the monitoring tools, if that is required as well. This provides a better solution to improve the efficiency and utility of your monitoring tools.

Packet brokers provide the following typical benefits:

- Filtering of monitoring data that sends multiple streams of data to the different tools on your network
- Aggregating data from multiple sources
- Load balancing filtered data to multiple tools
- Deduplicating packet data
- Manipulating packets (header slicing, protocol stripping, data masking, etc.)

IXIA SOLUTIONS

Ixia's Security Fabric as part of the IxVision Architecture helps speed application delivery and enables effective troubleshooting and monitoring for network security, application performance, and SLA fulfillment—and allows IT to meet compliance mandates. Ixia's out-of-band network visibility solutions are comprised of a comprehensive product portfolio of high-performance taps, virtual taps, and NPBs, all easily deployed and managed.

The Ixia Vision series of NPBs (including Vision ONE and Net Tool Optimizer) are powered by a user-friendly, drag-and-drop interface that allows you to easily connect monitoring tools to appropriate SPAN and tap ports with the simple click of a mouse.

Ixia NPBs offer simplified, intuitive management that is key to keeping total cost of ownership low. They enable you to:

- Create network connections and filters by using the intuitive GUI to aggregate, filter, and distribute network traffic to monitoring tools with a few clicks of the mouse and virtually eliminate the need to rewire equipment
- Restrict access to specific filters, ports, or monitoring tools by delivering improved access control management to meet compliance and regulatory requirements
- From within Vision ONE and NTO NPBs, monitor key SNMP statistics from any network management system so that you can view and report on key information, such as the amount of traffic each tool receives and get instant notification of oversubscribed tools
- Accommodate your organization's increasing need for more IP addresses by easily accessing the NPB using IPv4 or IPv6 addresses

SUGGESTED APPLICATIONS AND PLATFORMS	
Vision ONE	• All-in-one tool for lossless visibility for both inline and out-of-band tools • Intuitive GUI • ATIP, AFM, SSL Decryption • 48 10GE/1GE SFP+ ports and four 40GE QSFP+ or 16 port 10GE
NTO 7300 (and NEBS 3 compliant 7303) Chassis	• Highest density NPB with up to 384 ports of 10GE in 7U, including up to 192 ports of 10GE or 48 ports of 40GE AFM (Advanced Functionality) • Wire-speed performance • ATIP, AFM, Packet Capture Module
NTO 5293 Carrier-Grade	• NEBS Level 1 certified • 16 40GE ports or up to 64 10GE ports
NTO 5288 High-Density 40G	• Up to 64 10GE ports • Offers an efficient and scalable solution to monitor 1, 10, and 40GE
NTO 5273 High Availability, Carrier Class	• Designed for telecommunication and cable service providers • NEBS Level 3 certified
NTO 5236 Enterprise Class	• 10GE visibility for fiber network monitoring tools • Up to 24 SFP/SFP+ Ethernet ports
NTO 5204 Small Enterprise	Ideal in the lower-speed portions of the network
NTO 2112/2113	Extend core enterprise-class network monitoring feature sets to branch offices
ControlTower NTO 5260/5268	A network visibility architecture for centralized, intelligent monitoring
AFM	Enhance Vision ONE and NTO's capability to aggregate, replicate, and filter network monitoring traffic
ATIP	Gather real-time application data for actionable insight into network activities
Packet Capture Module (PCM)	Capture packet anomalies for quick analysis and solutions at 40 GE line rate
Taps, link aggregators, tap aggregators	Capture and send traffic of interest to the tools that are monitoring your physical network
Phantom vTap	Get visibility into the traffic between virtual machines in virtualized environments

CLOUD VISIBILITY SOLUTIONS

SCENARIO

While the benefits of cloud deployments are many, accessing and monitoring virtual traffic is a challenge. Without granular access to virtual traffic, you may suffer from blind spots in your network that compromise application performance or security.

For public clouds, hyperscale deployments are characterized by continuous configuration changes based on demand. While resource pooling and elastic scale are part of the cloud value proposition, the ability to monitor virtual traffic flows at the same scale has been limited.

Private clouds, on the other hand, use a variety of hypervisors in their build-out. As a result, access to private cloud data means that each hypervisor needs to be taken into account in order to access inter- and intra-VM traffic.

Most modern enterprises do not live solely in public or private cloud environments but use a hybrid approach. You want to monitor data in your public cloud resources as much as you do in your private cloud and, ideally, with a centralized set of tools.

IXIA CLOUD VISIBILITY SOLUTIONS

CloudLens™ is Ixia's platform providing unprecedented visibility across all your cloud environments—public, private, and hybrid. The platform will provide the framework to scale virtual taps and data filtering to meet the elastic demands cloud customers expect in a multi-tenant self-serve model. With the CloudLens platform, deploying monitoring taps occurs in a matter of minutes, not hours or days.

The powerful embedded automation capabilities of the CloudLens platform will enable virtual taps and analysis tools to automatically shift to changes in demand or failures without the need for operator in-the-loop actions. Virtualizing the analysis tools directly in the customer's cloud provides a significant bandwidth-saving option to customers who do not want to tunnel all their virtual data back to centralized physical analysis tools.

The CloudLens platform will enable you to dynamically scale your cloud network visibility as you scale your public cloud resources without creating an extra automation and infrastructure management burden.

For private clouds, the CloudLens platform supports intelligent monitoring of virtual traffic in these environments: OpenStack KVM, VMWare ESXi and NSX, and Microsoft Hyper-V. It combines the power of its virtual network taps, packet and application flow filtering, Netflow with advanced application identification and geographic location, SSL decryption, and deduplication to provide unprecedented insight into network traffic in both physical and virtualized environments. It also offers multiple tapping options, and its tunneling options include Generic Routing Encapsulation (GRE), VLAN, and Encapsulated Remote SPAN (ERSPAN) for maximum coverage across private cloud deployments.

Hybrid clouds give the maximum flexibility, and Ixia provides complete flexibility in monitoring options for hybrid clouds, giving your business a transition path from private cloud to public cloud.

SUGGESTED PLATFORMS	
Phantom vTap	Get visibility into the traffic between VMs in virtualized environments
Vision ONE	All-in-one tool for lossless visibility for both inline and out-of-band tools supporting ATIP, AFM, PCM, SSL decryption
NTO 7300 (and NEBS 3 compliant 7303) Chassis	Highest density NPB with wirespeed performance with support for ATIP, AFM, PCM, and SSL decryption
xStream 40	Fail-safe inline security network packet broker with aggregation filtering, and load balancing for 40/10GE networks
NTO 5236	10GE visibility for fiber network monitoring tools
CloudLens vPB	Virtual appliance offering packet broker services such as aggregation, filtering, deduplication, and distribution of virtual traffic

Phantom vTap

Vision ONE

NTO 7300

xStream 40

NTO 5236

APPLICATION VISIBILITY SOLUTIONS

SCENARIO

One of the biggest challenges facing network administrators today is complete network visibility that extends past Layer 4 information. Many applications run over Hypertext Transfer Protocol (HTTP) within your network or cloud infrastructure, and thus, can be obscured. SSL encryption can also hide data needed for monitoring, as well as security threats like malware.

Access to real-time application data for monitoring tools empowers IT professionals with better data to make better decisions. Application intelligence provides rich data on the behavior and location of users and applications. This allows IT teams to identify unknown network applications, mitigate network security threats from suspicious applications and locations, and spot trends in application usage to predict and forestall congestion.

IXIA'S APPLICATION VISIBILITY SOLUTIONS

The Ixia Application and Threat Intelligence Processor (ATIP) is the answer to these problems with the following core features:

- Dynamic and signature-based application detection, filtering, and monitoring
- SSL decryption capability with stateful decrypted output
- Combines traditional NTO and Vision ONE capabilities with application awareness and context
- Enables application tracking by bandwidth, session, and geography
- Supports generation of NetFlow v9 and v10 and IPFIX data, and supports up to 10 NetFlow collectors
- Delivers frequent updates via ATIP subscription
- Hitless upgrades

One of the features to note is stateful SSL decryption. Stateful decryption means that the integrity (checksum) of the payload is validated and then retransmitted once the data is decrypted. This capability makes this an excellent solution to get the necessary data and forward it on to high-performance monitoring tools for fast processing.

SUGGESTED APPLICATIONS AND PLATFORMS	
ATIP	Supports up to 48 10G SFP/SFP+ ports for use with the NTO 7300 chassis or Vision ONE

ACTIVE NETWORK MONITORING AND ASSESSMENT

SCENARIO

Network performance and user experience are critical aspects of your business. It is vital to understand customers' perception of your website, application, and network services. New applications introduce potential network bottlenecks that must be quickly identified and corrected. Not knowing impacts your revenue stream.

IXIA SOLUTION

Hawkeye™ is an operational solution for distributed production network and field use. It is designed for network assessments with active monitoring to measure, control, solve, and verify network infrastructure with predictable traffic injection. It is based on an open framework for integration with Operation Support System (OSS)/Element Management System (EMS) and IT environments.

Hawkeye continually measures network performance and service status. If there is an issue, Hawkeye helps you identify it, quantify it, and ultimately resolve it—before your customers experience it.

Using a combination of hardware and software agents, Hawkeye simulates application traffic and sends key performance metrics to a central console for fast action. Active traffic does not wait for user traffic to find issues. Measurements range from network quality to user experience, enabling administrators to improve overall network uptime and detect network performance issues before they impact end-users.

SUGGESTED APPLICATIONS AND PLATFORMS	
Hawkeye	Automate network performance checks and improve the application delivery experience with choice of software endpoints or plug-and-play XR2000 and XRPi hardware endpoint
XR2000 and XRPi Hardware Endpoint	Works with Hawkeye to provide: • Active network and application assessment and monitoring • Advanced routing support • Active traffic generation supporting 150+ applications • Up to line-rate generation • Endpoint-to-endpoint tests: UDP, TCP traffic, voice, video, and traffic mixes
Test endpoints	Supplied software endpoints for a wide variety of operating systems, including: • Microsoft Windows • Windows CE/Mobile • Linux, including Embedded Linux • Mac OS, IOS • Android • Virtual machines running on any hypervisor or cloud

ROSS JONES

Network Manager at Cook Children's Health

The Ixia solution has **cut the time it takes to diagnose performance problems** from days to hours.

Security
SOLUTIONS

ixia

SCENARIO

According to Kaspersky Lab, nearly 90% of companies have suffered a security incident, with enterprises paying an average of $551,000 to resolve it. Protecting your network means more than just adding the latest security tools. How you implement those defenses makes a huge difference in their performance and uptime.

Deployment of any inline tool in the network carries the risk of the tool becoming a point of failure. Should the inline tool become unavailable, it can bring the network link down, making a critical segment of the network unavailable and affecting uptime. To avoid this risk, customers need a fail-safe solution that can protect the network from tool failures while allowing inline tools to protect the network from incoming threats.

Security resilience starts at the foundation of the network, with robust bypass switches and intelligent distribution of packets to inline security tools.

IXIA SECURITY RESILIENCE SOLUTIONS

An Ixia Security Fabric™ ensures every security tool is online and operating at peak performance. Ixia offers the widest range of fail-safe bypass switches, attack surface filters, and intelligent network packet brokers (NPBs) to deliver resilient security solutions.

Simple Resiliency

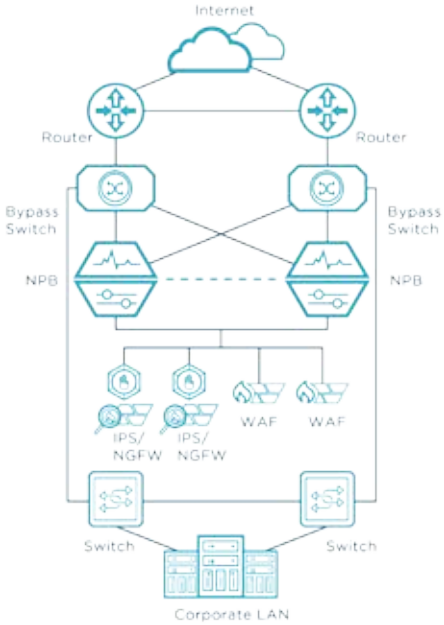
A simple alternative to reduce the risk of planned and unplanned downtime is to deploy a simple high-speed bypass switch in front of every firewall and other security appliance—a switch with the ability to continually monitor all inline devices and make sure they are ready to receive traffic. If any device goes down unexpectedly, the bypass steers traffic around it until the device is returned to a ready state. This eliminates the risk of a single device failure causing a network outage.

The bypass ensures network traffic can still be inspected by all other functioning security appliances and keeps the overall network up and running. The best bypass switches operate at line-rate speed and have no impact on network availability. In addition, once a bypass switch is installed, planned maintenance, such as configuration changes, deployment of new appliances, or device upgrades, can be performed without impact to the network, as the bypass will route traffic around the offline device. Since 70–90% of all downtime is associated with maintenance, this simple change can dramatically increase application uptime.

While extremely useful for reducing downtime, the bypass makes a trade-off between availability and security inspection, since traffic is simply routed around any security device that is unable to respond. Fortunately, there is an even better, more resilient security solution.

HIGH AVAILABILITY

To reduce downtime even further and maximize resiliency, you can deploy your security fabric with high availability (HA) using redundant modular bypass switches and NPBs. If you use an NPB capable of being deployed in redundant active-active mode, you will have automatic and instantaneous recovery of any device in your security architecture.



Security Fabric with Maximum Strength HA

In the maximum-strength security architecture, dual bypass switches and dual NPBs enable full recovery from the failure of any inline device in the security architecture. The bypass switches deployed in active-standby mode monitor the health of all devices, including the NPBs, and reroute traffic from one to another, should an outage be detected. In the case of a failure on one branch, security is completely maintained, and users will detect no service or application outage.

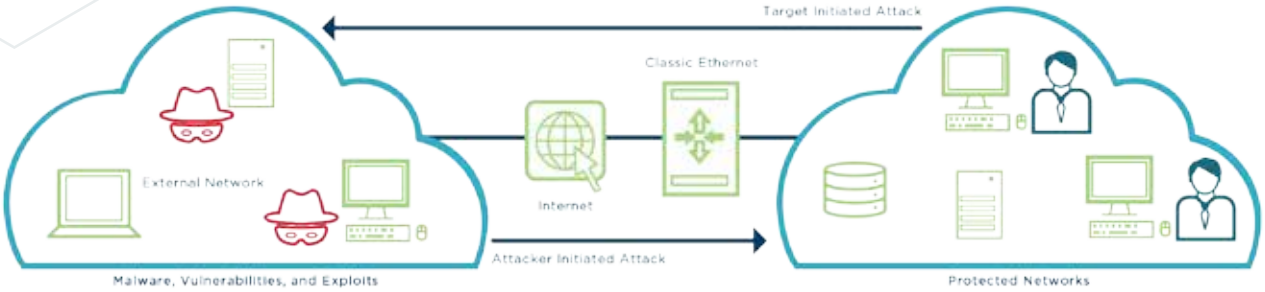
The NPBs configured for HA with complete synchronization in active-active mode provide load balancing during normal conditions and are configured for full protection of all traffic if one goes down. Again, users experience no downtime, and security monitoring is completely unaffected.

The benefits of an Ixia Security Fabric include:

- High availability by eliminating downtime from security tool maintenance, upgrades, or failures
- Optimal performance by filtering and load-balancing traffic to and from multiple tools
- Operational efficiency by reducing security alerts
- Significant ROI by making more efficient use of security tool capacities

With Ixia's Security Fabric, creating a self-healing, highly available security architecture has never been easier.

SUGGESTED PLATFORMS	
iBypass	Fiber, 40G, SR, 50µm, QSFP+ Cages
iBypass VHD	high-density 12-segment 10Gbps Intelligent Bypass Switch
10/100/1Gb Copper Bypass Switch	Copper Ethernet interfaces up to 1G
xStream™ 40	40GE visibility for fiber network monitoring tools
Vision ONE	40GE all-in-one tool for lossless visibility for both inline and out-of-band tools with an intuitive GUI and support for ATIP, AFM, PCM, SSL decryption



SCENARIO

Network security is a top concern of every enterprise. Each computer with access to the Internet or offering a service to the Internet must be protected from security threats. The average cost of a breach is now over $4 million per incident, a 29% increase since 2013 and 5% from last year[1].

Malware security attacks take many forms: viruses, worms, trojans, rootkits, spyware, malicious adware, scareware, and lately, ransomware. These attacks often succeed with the cooperation of computer users—through e-mail, web pages, FTP transfers, instant messaging, peer-to-peer file sharing, online games, and careless software installation. Other attacks happen just by virtue of being connected to the Internet: denial of service (DoS) attacks against company sites; vulnerability attacks against web, email, FTP, and other services; and password-login attacks.

In addition to user education, enterprises use a variety of network security devices to protect their sites and services. These include:

- **Firewalls** – Filter access to a network based on IP addresses and protocols. NG firewalls use DPI to filter based on internal protocols and contents.
- **VPN gateways** – Provide secure access to remote employees and partners. These devices use IPsec encryption to protect traffic from trusted sites.
- **IDS/IPS systems** – Protection against hacking. These sophisticated devices recognize a wide range of unusual network usage, looking for indications of misuse.

  IDS systems notify administrators of possible breaches, whereas IPS systems block access, often by programming the firewall.
- **URL filtering** – Prevent access to suspect web sites. These devices watch all web, FTP, and other access, and prevent access to sites on a vendor-supplied list.
- **Anti-malware, anti-spam gateways** – Prevent malware from entering the enterprise. These similar functions look at the content of e-mail, web, FTP, and other data entering the enterprise. This type of prevention is often also present on individual computer systems.
- **Threat sandbox gateways** – verify data or files do not contain malware by either executing or inspecting them in a sandbox before letting them enter the network.
- **DLP gateways** – prevent valuable data from leaving the enterprise. This appliance inspects traffic exiting the enterprise, looking for proprietary or improper data sent by deliberate user action or as a result of malware attacks.

Many of these functions are now combined into a single appliance, called a unified threat management (UTM) system or on a next-generation firewall.

IXIA SOLUTIONS

Ixia offers a complete network test and assessment product that measures security:

- **Effectiveness** – the ability to detect and prevent all forms of attacks.
- **Accuracy** – the ability to accurately perform its function, without significant "false-positive" results.
- **Performance** – the ability to enforce security mechanisms while maintaining acceptable network performance. Security enforcement mechanisms must continue to pass good traffic even under the most aggressive attacks.

The Ixia BreakingPoint Application and Threat Intelligence (ATI) service provides comprehensive intelligence for optimizing and hardening the resiliency of IT infrastructures, including product updates, authentic application protocols, real-world security attacks, and responsive support:

- **Known vulnerabilities** – Over 37,000 known security vulnerabilities, organized by type, are available. Attacks are updated frequently to stay current with hacker activity.
- **Attack evasions** – Attacks are frequently masked by use of packet fragmentation and other sophisticated techniques. Ixia applies evasions to known vulnerabilities to increase effectiveness testing.
- **Massive DDoS attacks** – simulate DDoS and botnet attacks to measure cyber infrastructure resiliency. Ixia uses its own test ports' customized logic and scale to mount large-scale DDoS attacks.
- **Encryption** – IPsec encryption is used in two ways. Encryption with "good" traffic serves to measure VPN gateway throughput. Encryption with "attack" traffic tests security effectiveness and accuracy for attacks delivered over secure connections.
- **Multiplay traffic** – Sends real-world, stateful traffic to measure security appliance performance. This means that the true, realistic performance, including QoE, of security mechanisms can be measured—not just raw throughput.

1. Ponemon Institute's 2016 Cost of Data Breach Report, 2016

FEATURES	OPTIONS
Known vulnerabilities	• Tens of thousands of known vulnerabilities • Over 360 simulated applications • Bi-directional application • Evasion techniques
DDoS	• 30+ attack types • Virtually unlimited scale
Encryption	• IPsec • SSL/TLS
Multiplay traffic	• Data • Voice • Video • City-scale subscribers • QoE measurements

In conjunction with Ixia's hardware and other test applications, Ixia offers a complete test solution for network devices that provide functions other than security.

Ixia's IxLoad-IPsec is designed to measure the performance of VPN gateways that are used to connect organizations' multiple sites and to connect remote users to corporate networks. IPsec is also used in 3G and 4G networks to protect communications between handsets and internal wireless gateways.

IxLoad-IPsec tests performance of VPN gateways of all types in several ways:

- **Connections** – How many site-to-site and user connections can be concurrently supported?
- **Connection rate** – How rapidly can new connections be established?
- **Throughput** – What is the maximum data rate that a gateway can sustain?
- **Interoperability** – Can the gateway support the numerous encryption and authentication protocols in use today?

SUGGESTED APPLICATION	
BreakingPoint/ BreakingPoint VE Application and Threat Intelligence (ATI) Subscription	Continuous real-time data feeds to ensure current application and threat intelligence at all times
IxLoad/IxLoad VE	Highly scalable SSL and IPsec encryption to validate the performance and scale of security infrastructure
TrafficREWIND™	Uses the production network insight captured in ATI Processor metadata to bolster BreakingPoint traffic realism, improving fault analysis and device/ architecture validation before deployment.
SUGGESTED LOAD MODULES	
PerfectStorm	Application traffic and security attacks at 960 Gbps with the load of 720 million concurrent wired and wireless users from a single 11U chassis
PerfectStorm ONE	Enterprise-ready portable appliance for 10/1GE real-world, high-stress testing with up to 80Gbps of application traffic
CloudStorm	Cloud-scale, multi-terabit application delivery and network security test platform
SUGGESTED CHASSIS	
XGS12 Chassis	Industry's highest 100/40/10GE port densities in 11RU vertical rack space, reducing space requirements and simplifying management
XGS2 Chassis	Two-slot ultra-high-performance 3RU Chassis

BreakingPoint

IxLoad

PerfectStorm

PerfectStorm ONE

CloudStorm

XGS12

XGS2

FASTER SECURITY BREACH DETECTION

SCENARIO

Cybersecurity is a top priority for almost every large enterprise in the world today. With security breaches on the rise and the threat posed to companies large and small, network and security administrators are on the alert and must keep systems safe from the twin threats of intruders and malware. The good news is there are a growing number of tools to address these risks.

However, as traffic continues to grow, much of it comes from known bad IP address sites and geo-locations that never need to hit your security tools. Plus, IT now spends an increasing amount of time—and money—analyzing traffic logs and flagging false positives.

IXIA SOLUTIONS

Ixia ThreatARMOR packs a powerful one-two punch by protecting networks against malicious IP addresses while alleviating the burden on time-strapped IT security teams. To enhance the security performance of enterprise networks, ThreatARMOR automatically eliminates known bad IP addresses and unwanted geo-location traffic.

This enables network firewalls and intrusion prevention systems to more efficiently focus on blocking malware and identifying threats from all other IP addresses. Additionally, ThreatARMOR's geo-blocking capabilities scrub traffic from foreign countries off networks thereby preventing attacks from affecting network availability.

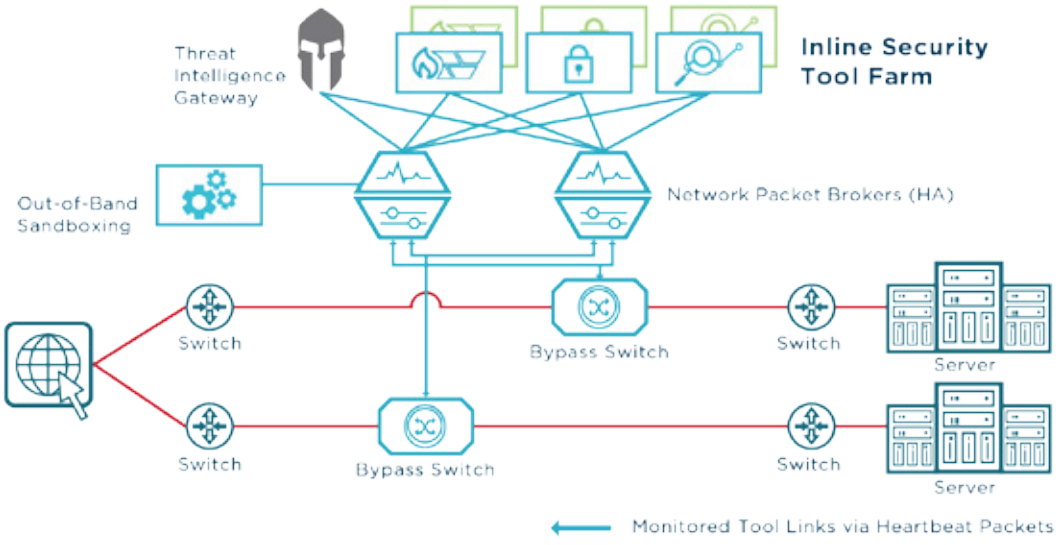
This proactive approach not only reduces unnecessary traffic but increases IT productivity. By blocking known bad IP addresses and unwanted geo-location traffic using the most up-to-date information, ThreatARMOR boosts the performance of your network security infrastructure. It also eliminates the need for IT security administrators to spend hours analyzing unwanted traffic and false positives. The ROI is impressive: ThreatARMOR eliminates 30% of alert-generating connection attempts and yields 15 times ROI in a single year.

SUGGESTED PLATFORM	
ThreatARMOR	1U security appliance with inline blocking, inline monitor-only, and out-of-band monitor-only modes; always-on ATI cloud security service

JON OLTSIK

ESG Senior Principal Analyst and Founder ESG's Cybersecurity Service

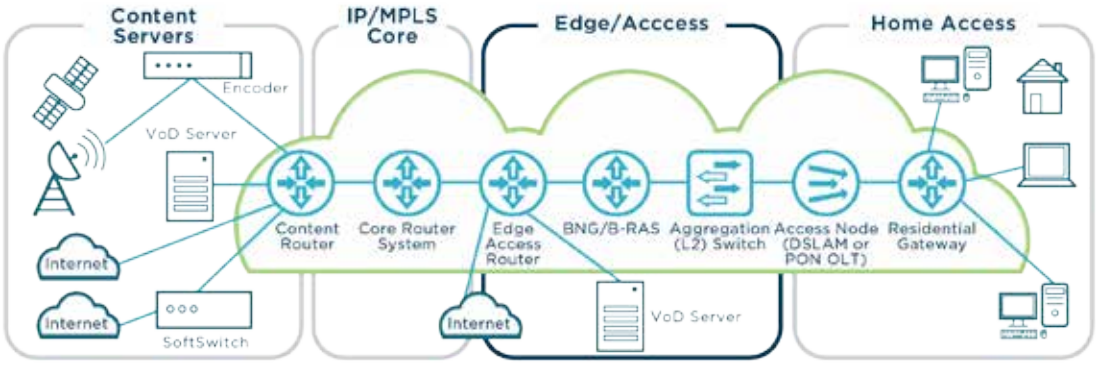
What's killing security is not technology, it's operations. Companies are looking for ways to **reduce** their **overall operations requirements** and need **easy- to-use, high performance solutions, like ThreatARMOR,** to help them do that.



Test
SOLUTIONS

ixia

BROADBAND ACCESS AND SERVICES TESTING



SCENARIO

"Broadband" describes high-speed Internet access for end customers via wireless, cable, or Digital Subscriber Line (DSL). Broadband requires numerous protocols and devices to work together seamlessly to provide reliable customer Internet access, especially when rolling out new services that consume larger and larger amounts of bandwidth. Without sufficient testing of broadband network protocols, equipment, and network topologies, business suffers due to unreliable customer access.

Testing services over broadband access is a critical factor in providing excellent quality of experience (QoE) to end-users, whether they are enterprises, service providers, or individual customers. Coupled with this, networks need to support both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) seamlessly in order to mitigate the transition risks as more customers consider the shift to IPv6.

IXIA SOLUTIONS

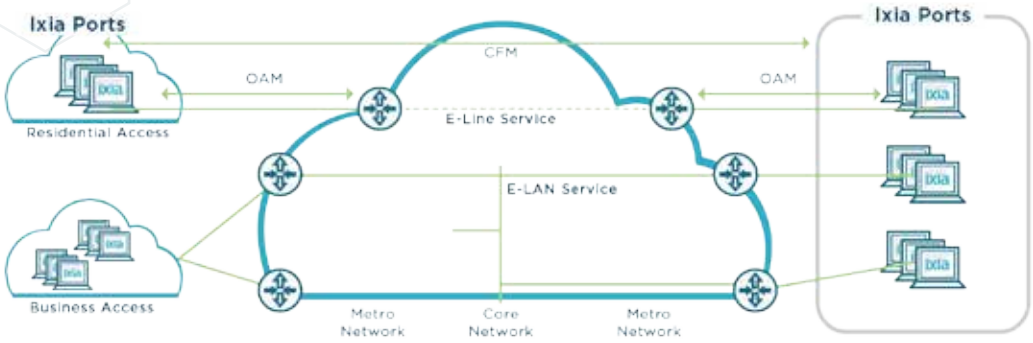
Ixia specializes in testing network components and topologies, helping to ensure broadband reliability. Ixia's platform emulates network protocols and simulates network devices to help answer critical questions, such as:

- Does my broadband implementation conform to industry standards?
- Does my ANCP implementation allow full monitoring of my network topology and state?
- Can my BRAS, LAC, or LNS scale and still meet QoS objectives?
- Can I test and verify SLAs?
- Can my network handle subscriber session flapping?
- Can my network support IPv4/IPv6 subscribers and services while maintaining SLAs?

Ixia helps NEMs and service providers meet the challenges of broadband deployment and maintenance with award-winning solutions that ensure performance, conformance, and scalability.

SUGGESTED APPLICATIONS	
IxNetwork®/ IxNetwork VE	Full L2–3 testing with wire-rate traffic generation and protocols: • PPPv4/v6/Dual-Stack PPP (PPPoE, PPPoEoA, PPPoA), L2TPv2, ANCP, DHCPv4/v6, DS Lite, 6rd, IGMP/MLD/802.1x/Cisco and HP Web-Auth/Cisco NAC
IxANVL™	Protocol conformance testing with: PPP, L2TP, DHCPv4/v6, 802.1x
IxLoad®/IxLoad VE	L4–7 services testing over broadband access
Network Emulator II	Emulates real-world network impairment conditions in the lab to validate network-based products, applications, and services
SUGGESTED LOAD MODULES	
Novus™ 100 GE QSFP28	Testing of 100/50/25GE over copper multi-mode and single-mode; designed for large-port-count testbeds
Novus ONE	Complete L2–7 network and application testing in a portable appliance Novus 10G/1G/100M: High-density dual-PHY tri-speed solution for ultra-high-scale and performance testing
Novus 10G/1G/100M	High-density dual-PHY tri-speed solution for ultra-high-scale and performance testing
PerfectStorm™	Highly-scalable platform to validate the application delivery performance and QoE over access networks
PerfectStorm ONE™	Enterprise-ready portable appliance for 10/1GE real-world, high-stress testing with up to 80Gbps of application traffic
CloudStorm 100GE	Cloud-scale, multi-terabit application delivery and network security test platform
SUGGESTED CHASSIS	
XGS12™ Chassis	Industry's highest 100/40/10GE port densities in 11RU vertical rack space, reducing space requirements and simplifying management
XGS2™ Chassis	Two-slot ultra-high-performance 3RU Chassis

CARRIER ETHERNET TESTING



ALEXANDRE RAYMOND
Senior VP of Product Development, Orthogone Technologies

We've teamed with **the best in the industry** to help us validate and measure the performance of our Ethernet MAC and PCS IP cores.

SCENARIO

Carrier Ethernet services are growing rapidly, driven by next-generation virtual private network (VPN) services and mobile backhaul. A suite of protocols is required to achieve carrier-grade scale, reliability, and management. Carrier Ethernet requires the use of Ethernet at the user-to-network interface (UNI) and can be delivered via a variety of metro and core technologies, including an Internet Protocol (IP)/ Multiprotocol Label Switching (MPLS) core.

The Metro Ethernet Forum (MEF) has defined technical specifications to advance the development and deployment of Carrier Ethernet services.

- **MEF 9** outlines conformance-oriented service testing and is the basis for performance tests
- **MEF 14** defines testing of performance service attributes, including QoS functional requirements
- **MEF 21, 24**, and **25** constitute a test suite for UNI type 2, including link OAM, E-LMI, service OAM, protection, enhanced UNI attributes and L2CP handling

The MEF specifications allow carriers to deliver services using any underlying technologies. The table lists the protocols used for routing, switching, and network management.

As the demand for Carrier Ethernet private line (E-Line) and Ethernet transparent Local Area Network (E-LAN) services continues to grow, so does the need for fault management. Ethernet operation, administration, and maintenance (OAM) covers Ethernet link monitoring and diagnosis. Ethernet connectivity fault management (CFM) defines protocols that monitor end-to-end services.

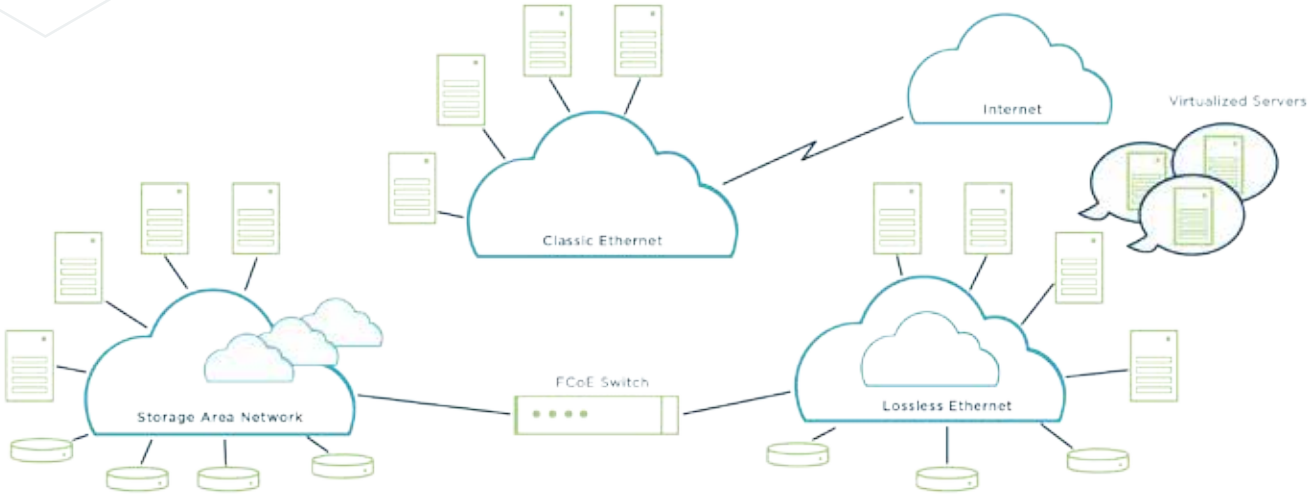
IXIA SOLUTIONS

Ixia's MEF conformance tests verify both Carrier Ethernet conformance requirements and network performance.

IxANVL has the widest coverage of Carrier Ethernet and MEF conformance in the industry. Ixia emulation functionality tests common Carrier Ethernet routing protocols, including MPLS, layer 2 switching, and Provider Backbone Bridge Traffic Engineering (PBB-TE). Ixia's solutions include support for Institute of Electrical and Electronics Engineers (IEEE) 802.3ah, IEEE 802.1ag, and International Telecommunication Union Telecommunications (ITU-T) Standard Y.1731.

USE	PROTOCOL
Routing	MPLS, VPLS, BFD (bidirectional forwarding detection)
Switching	QinQ (802.1ad), PBB-TE (802.1Qay) PBB/MAC-in-MAC (802.1ah) RSTP/MSTP, LACP, MVRP/MMRP VLAN (802.1Q)
Management	Ethernet OAM (802.3ah) Service OAM (ITU-T Y.1731) E-LMI (MEF 16)
Timing	1588v2 (IEEE), Synchronous Ethernet (ITU-T) CES (MEF18)

SUGGESTED APPLICATIONS	
IxNetwork/ IxNetwork VE	Full L2–3 testing with wire-rate traffic generation and protocols: • PPPv4/v6/Dual-Stack PPP (PPPoE, PPPoEoA, PPPoA), L2TPv2, ANCP, DHCPv4/v6, DS Lite, 6rd, IGMP/MLD/802.1x/Cisco and HP Web-Auth/Cisco NAC
IxANVL	Protocol conformance testing, with: • MEF9, MEF21, MEF24, and MEF25 conformance suites • PBB, 802.1Q, and MVRP/MMRP conformance suites
BreakingPoint/ BreakingPoint VE	Stress data center/cloud infrastructures using peak application user load from hundreds of applications to configure virtualized environments for optimal performance and capacity
Network Emulator II	Emulates real-world network impairment conditions in the lab to validate network-based products, applications, and services
SUGGESTED LOAD MODULES	
Novus 100 GE QSFP28	Testing of 100/50/25GE over copper multi-mode and single-mode; designed for large-port-count testbeds
Novus ONE	Complete L2–7 network and application testing in a portable appliance
Novus 10G/1G/100M	High-density dual-PHY tri-speed solution for ultra-high-scale and performance testing
PerfectStorm	Application traffic and security attacks at 960 Gbps with the load of 720 million concurrent wired and wireless users from a single 11U chassis
PerfectStorm ONE	Enterprise-ready portable appliance for 10/1GE real-world, high-stress testing with up to 80Gbps of application traffic
CloudStorm 100GE	Cloud-scale application delivery and network security test platform
SUGGESTED CHASSIS	
XGS12 Chassis	Industry's highest 100/40/10GE port densities in 11RU vertical rack space, reducing space requirements and simplifying management
XGS2 Chassis	Two-slot ultra-high-performance 3RU Chassis



SCENARIO

The adoption of cloud computing is being driven by the proliferation of rich Internet applications, anywhere broadband access, and infrastructure elasticity enabled by virtualization. As consumers and enterprises become more dependent on services and applications running in the cloud, network performance becomes a key metric to ensuring end-user QoE and key service level agreements requirements are met.

To match increasing demand while minimizing capital expenditure (CAPEX) and operational expenditure (OPEX), data centers must provide state-of-the-art services while lowering cost, power consumption, and design complexity.

Proper handling of Ethernet traffic categorized as north–south traffic or east–west traffic, is critical to data center performance—requiring a variety of testing and techniques. Individual components, sub-systems, and the data center as a whole must be thoroughly tested to ensure dependable capacity, flexible performance, reliable operation, and high security.

Each area has specialized testing or visibility requirements:

- **Data center compute/server infrastructure** – As enterprises migrate their data and applications to the cloud and leverage virtualized server infrastructures, it is essential to measure application performance through all stages—on-premises physical servers, virtual machines, and a fully-hosted cloud. In addition, access to east–west traffic that may never cross a physical switch port requires specialized technology that is compatible with hypervisor environments and can tap into the data flows.
- **Virtualization** – Assessing data center virtual infrastructure elasticity and capacity requires tools that can test in the context of an end-to-end environment, measuring the performance of virtual switches, firewalls, and servers, in addition to generating a diverse set of client–server, server–server, and server–storage application traffic originating from both within and outside of virtual machines.
- **Network infrastructure and storage** – The convergence of local area network (LAN) and storage area network (SAN) traffic requires a multi-level testing approach, from the storage network fibre channel over Ethernet networks to the Ethernet switching infrastructure to the convergence of the two with lossless Ethernet.
- **End-to-end service delivery** – Measurement of end-to-end transactional latencies and application throughput across voice, video, and data applications is essential to ascertaining the collective impact that data center storage, network, and computer infrastructures have on end-user QoE.
- **Security** – The increasing use of virtualized cloud infrastructures in enterprise and service provider data centers introduces unforeseen security issues that require comprehensive and continuous testing to detect and overcome.
- **Higher speed Ethernet** – Rapid expansion of intra– and inter–data center Ethernet traffic means that 40, 100, and even 400GE interfaces will need to be tested.

IXIA SOLUTIONS

Ixia's applications deliver scalable converged data center emulation and integrated traffic generation/wizard for performance testing of data center switches and converged network adapters (CNAs).

Ixia's solutions address the testing challenges of application-aware devices and service-delivery infrastructures. IxLoad supports an extensive library of multi-play protocols, realistic subscriber modeling capabilities, and the industry's highest application scale for assessing Device Under Test/System Under Test (DUT/SUT) performance and end-user QoE.

Ixia BreakingPoint addresses the application controller, application delivery, and deep packet inspection (DPI) requirements and key differentiators through the emulation of hundreds of applications, live malware, and user behavior.

Ixia Virtualized Testing

Ixia's virtualization testing solution offers a user-friendly interface for virtual ports management, which supports asset discovery through integration with popular virtualization platforms.

Ixia's virtualized testing solution tests:

- Virtualized server capacity
- Service scalability and elasticity
- Virtualized switching and firewall performance
- Virtual desktop infrastructure
- Virtual or physical devices with a realistic mixture of application and data storage traffic using stateful L4–7 traffic generation
- IP protocol functionality and convergence in virtual environments, including QoS, VM migration, VLAN leakage, and IGMP group join/leave latencies using L2–3 protocol emulation and traffic
- I/O storage for CNA manufacturers
- L2MP
- NFV
- SDN/OpenFlow

IXIA VE SOLUTIONS

Ixia's Virtual Edition (VE) of IxNetwork, IxLoad, and BreakingPoint validate the performance of virtual and physical data center infrastructures. VE provides a software-based version of Ixia's traditional hardware ports and enables cost-effective functional testing. These ports are easy to deploy in a virtual environment and allow quick scaling and test configuration changes.

They also allow scaling of the test software to earlier in the development process, where performance loading (which requires hardware) is not needed.


IxNetwork


IxLoad


BreakingPoint


Developer


Network Emulator II


Novus 100GE QSFP28


Novus ONE


Novus 10G/1G/100M


PerfectStorm


PerfectStorm ONE


CloudStorm


XGS12


XGS2

SUGGESTED APPLICATIONS	
IxNetwork/ IxNetwork VE	Full L2–3 testing, with protocol emulation for: • Fibre Channel over Ethernet • Data center Ethernet • Lossless Ethernet protocols
IxLoad/IxLoad VE	Delivers comprehensive functional and performance testing to validate user QoE in physical and virtual networks. IxLoad VE emulates web, video, voice, storage, VPN, wireless, infrastructure, and encapsulation/security protocols to create realistic scenarios to measure the QoE of services delivered over virtual and physical infrastructure.
BreakingPoint/ BreakingPoint VE	Stress data center/cloud infrastructures using peak application user load from hundreds of applications to configure virtualized environments for optimal performance and capacity
Developer	Agile application performance and security resilience test tool to help developers find bugs early
Network Emulator II	Emulates real-world network impairment conditions in the lab to validate network-based products, applications, and services
SUGGESTED LOAD MODULES	
Novus 100GE QSFP28	Testing of 100/50/25GE over copper multi-mode and single-mode; designed for large-port-count testbeds
Novus ONE	Complete L2–7 network and application testing in a portable appliance
Novus 10G/1G/100M	High-density dual-PHY tri-speed solution for ultra-high-scale and performance testing
PerfectStorm	Application traffic and security attacks at 960 Gbps with the load of 720 million concurrent wired and wireless users from a single 11U chassis
PerfectStorm ONE	Enterprise-ready portable appliance for 10/1GE real-world, high-stress testing with up to 80Gbps of application traffic
CloudStorm™	Cloud-scale multi-terabit application delivery and network security test platform
SUGGESTED CHASSIS	
XGS12 Chassis	Industry's highest 100/40/10GE port densities in 11RU vertical rack space, reducing space requirements and simplifying management
XGS2 Chassis	Two-slot ultra-high-performance 3RU Chassis

SCENARIO

Developers today are expected to deliver innovative software programs quickly and efficiently, yet they are running into a number of obstacles. For example, testing for defects is a critical step in the software coding process, but it can seriously stall the development cycle. Tight budgets and high complexity can limit the effectiveness of testing tools. And, the cost of fixing bugs during the development cycle is four times higher than in the initial coding stages. This makes early prevention key to reducing software development risks, delays, and costs.

IXIA DEVOPS TESTING SOLUTION

Ixia Developer is an agile application performance and security resilience test tool that helps developers find bugs early in the development cycle. Ixia Developer features an integrated debugger that helps locate the primary source of defects. An easy-to-use, fast, and responsive web-based user interface significantly reduces the time it takes to move from test configuration to actual packets on the network. And by leveraging a robust Application and Threat Intelligence (ATI) engine, Ixia Developer always includes the most up-to-date apps and security strikes:

- More than 290 apps included (Gmail, Facebook, etc.)
- More than 30,000 security strikes included
- Ability to import and replay any packet capture

For developers, early bug detection allows them to iterate more quickly and test more often, while enhancing on-time delivery of new software.

Deploying Ixia Developer is as easy as downloading the small footprint virtual machine (VM) image and running it. Developers can deploy Ixia Developer directly on their machines, or it can be deployed in a hypervised private or public cloud.

Key benefits of Ixia Developer include:

- Set breakpoints and execute step-by-step or to next breakpoint
- Investigate issues faster using the built-in debugger and capture engines
- Define and run your tests in seconds using the intuitive and fast HTML5 web UI
- Automate your tests using REST APIs and/or CLI
- Deliver continuous capture
- Offer built-in roadmap feedback loop

For business leaders, Ixia Developer boosts the bottom line by eliminating the costly rework associated with late-stage defect discovery, providing a greater return on technology investments.

HIGHER SPEED ETHERNET SOLUTIONS

Ixia is the leading provider of test solutions for higher speed Ethernet (HSE) components, networks, devices, and systems. Our application-focused family of load modules offers you the industry's most scalable solution for testing converged multi-play services, application delivery, and network security platforms for both wired and wireless networks.

Our load modules operate within our standard Ixia Chassis that support 1 to 12 load modules each, depending on chassis features.

CloudStorm is Ixia's industry-first 2.4 terabit application and security test solution that not only meets today's need, but that of the future. CloudStorm delivers three times application and four times Secure Sockets Layer (SSL)-emulation scale over any other test system. Each CloudStorm load module supports two native QSFP28 100GE interfaces with an innovative architecture that allows concurrent emulation of complex applications, unprecedented SSL encrypted applications, and a large volume of distributed denial of service (DDoS) traffic to validate that your network infrastructure is high performing and secure.

Novus is Ixia's next-generation architecture and test solution that satisfies the test needs of both high-density, multi-rate switch/router makers and the organizations implementing the network equipment. Supporting eight native QSFP28 100GE ports per load module, Novus enables interoperability and functional testing, as well as high-port count performance testing. The load module is also 25GE-capable.

Ixia's 400GE load modules are the world's first 400Gbps HSE test solution so meet the growing bandwidth requirements of ever-evolving data networks. Leading the way to a new testing paradigm, this is a developer tool kit to help network equipment manufacturers shorten development and test time—accelerating pre-standard 400GE networking hardware.

No matter what your Ethernet test needs are—whether 400GE, 100GE, 50GE, 25GE, 10GE, or 1GE—Ixia has the flexible load modules to satisfy your requirements.

SUGGESTED HSE LOAD MODULES
400GE AND 100GE/50GE/25GE Load Modules
• 400GE Load Modules • Xcellon-Multis QSFP28 100/50/25GE
100GE/25GE Load Modules
• Novus and Novus-R QSFP28 100/25GE
100GE/40GE/10GE Load Modules
• CloudStorm 100GE • PerfectStorm 100GE • Xcellon-Multis CXP 100/40/10GE
100GE/40GE Load Modules
• Xcellon-Multis CFP4 Enhanced 100GE • Xcellon-Lava Dual-Speed 100/40GE Reduced Performance HSE
REDUCED PERFORMANCE HSE
40/10GE Load Modules
• PerfectStorm 40/10GE • PerfectStorm ONE 40/10GE • Xcellon-Flex Combo 40/10GE • Xcellon-Multis QSFP 40/10GE • Xcellon-Flex QSFP+ 40GE

400GE Load Modules

Xcellon-Multis QSFP28

Novus

CloudStorm

PerfectStorm

Xcellon-Multis CXP

Xcellon-Multis CFP4 Enhanced

Xcellon-Lava Dual-Speed

PerfectStorm 40GE

PerfectStorm ONE

Xcellon-Flex Combo

Xcellon-Multis QSFP

Xcellon-Flex QSFP+

SCENARIO

Wi-Fi is now running mission-critical applications in homes, offices, hospitals, and many other places. Mission-critical applications require high-performing Wi-Fi devices to maximize uptime and improve user experience. However, most Wi-Fi IoT devices are still only qualified with basic throughput test cases. This woefully inadequate test strategy exposes companies to the risk of business applications failing in the field.

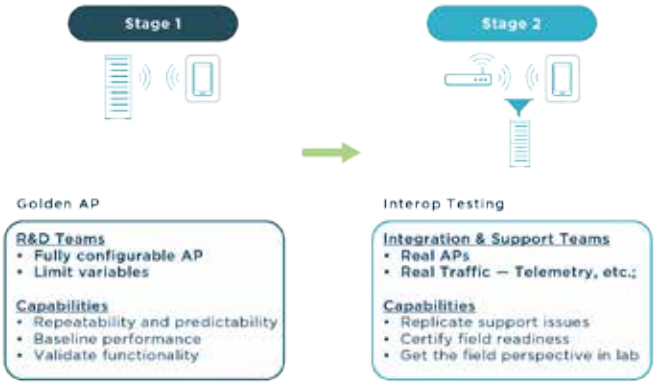
IXIA SOLUTIONS

To meet user expectations for anywhere, anytime access to mission-critical applications, Wi-Fi IoT device vendors need a comprehensive test strategy. Ixia IoT enables users to characterize IoT device performance over distance, channel models, roaming, ecosystems, and interence, while validating interoperability, stability, and functionality. We have designed Ixia IoT to address Wi-Fi device validation with a staged test approach that addresses the needs of teams involved in the early stages of the product life cycle (design/development), as well as later stages (pre-deployment/integration/support).

Customers will be able to better assess their wireless IoT implementations by being able to do the following:

- Build robust, high-performance client devices using fully configurable simulators and an exhaustive built-in test library
- Simplify testbeds with an integrated product that also drastically cuts costs and time associated with setting up and maintaining testbeds
- Easily achieve network scale with built-in golden AP and client simulation to build better ecosystem client devices
- Reduce debugging cycles with real-time L1–7 statistics and KPIs
- Improve release cycles with an automated testbed

Ixia's IoT test solution introduces a staged test approach for comprehensively characterizing IoT device performance before release.



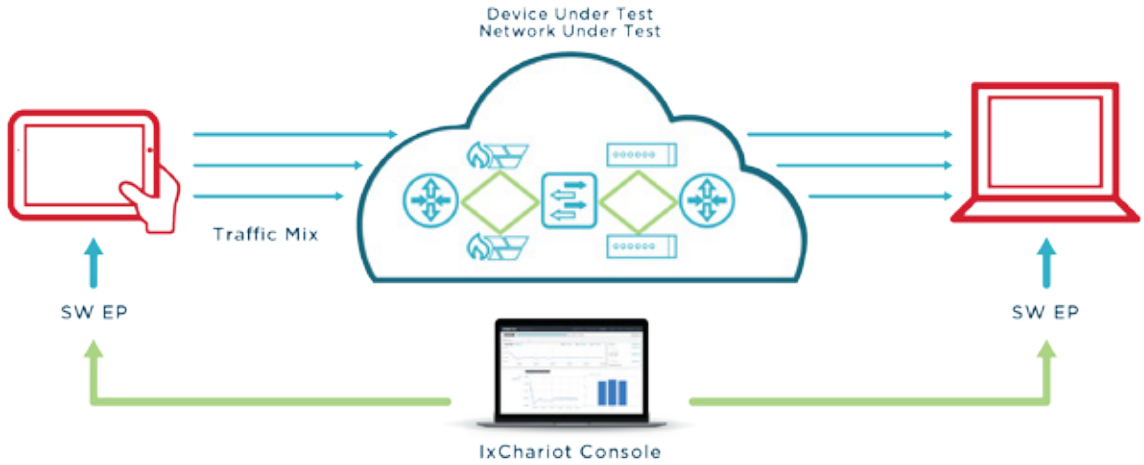
The first stage, design and development, involves a golden access point (AP) model, where the entire network (the AP and the distribution network) and test conditions are simulated. Ixia's custom-designed hardware drives much of this simulation, making it a highly reliable and precise testbed. This model gives a high degree of repeatability and predictability to the tester and it is ideal for baselining and benchmarking the performance of devices under various conditions.

Ixia IoT provides:

- Fully configurable golden AP with support for 4x4 multiple input and multiple output (MIMO) and full line-rate throughput
- Real APs, applications, and traffic for interoperability testing
- Built-in tests for characterizing performance over distance, roams, ecosystems, interference, and data plane traffic
- Channel modeling based on TGn specifications
- Real-time L1–7 statistics and KPIs

SUGGESTED APPLICATIONS	
Ixia IoT	Comprehensive test and assessment for IoT devices
SUGGESTED LOAD MODULES	
Golden AP Simulation Load Modules	L2–7 and L1–7 RF WaveBlades
Golden Client Load Module	Simulation and interop solution for L2–7 testing
WLAN Interference Simulation Load Module	Interference generation (Wi-Fi, Bluetooth, Microwave, Gaussian White Noise)
SUGGESTED CHASSIS	
IxVeriWave™ Chassis	Nine-slot or two-slot chassis for Golden AP, Golden Client, and WLAN Interference Simulation load modules

IP NETWORK ASSESSMENT AND DIAGNOSTICS



SCENARIO

As networks and applications grow in size and complexity, maintaining network performance becomes mission critical. New applications introduce potential network bottlenecks that must be quickly identified and corrected. With the frequency of network changes, the flexibility and availability of network assessment tools is essential.

IXIA SOLUTIONS

With IxChariot™, Ixia provides high-precision analysis and troubleshooting of application performance across network backbones. Thin endpoint clients called Performance Endpoints run on most computer operating systems and are deployed at key nodes within a network. A mixture of real-world traffic profiles, including multiplay services, is used to characterize network behavior.

When problems are reported, tests are run from central management points, such as the network operations center, and results are analyzed to identify network bottlenecks and degraded services.

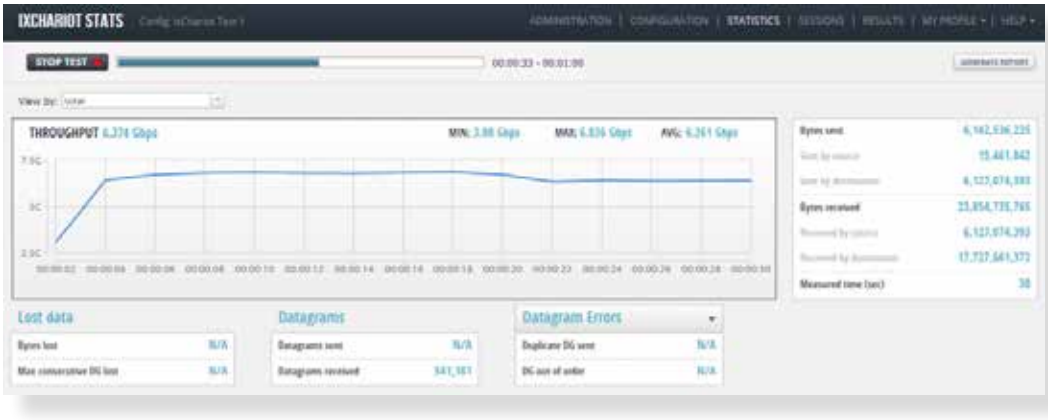
IxChariot tests devices or wide area network (WAN) links to verify key metrics, such as latency, failover time, packet loss, and throughput. IxChariot works with any size network/device and is capable of simulating hundreds of supplied protocols across thousands of network endpoints. Using sophisticated traffic patterns with optional Quality of Service (QoS) variations, IxChariot measures throughput, jitter, packet loss, end-to-end delay, Mean Opinion Score (MOS), and Medium Dependent Interface (MDI).

IxChariot console is available in two editions. The IxChariot Server Edition is hosted on a Linux server and is accessed through a web interface. The IxChariot Desktop Edition is installed as a heavy client on Windows personal computers (PCs) or servers. Both editions share the same licensing and are compatible with the same endpoints, so users can select the best option for their use case.

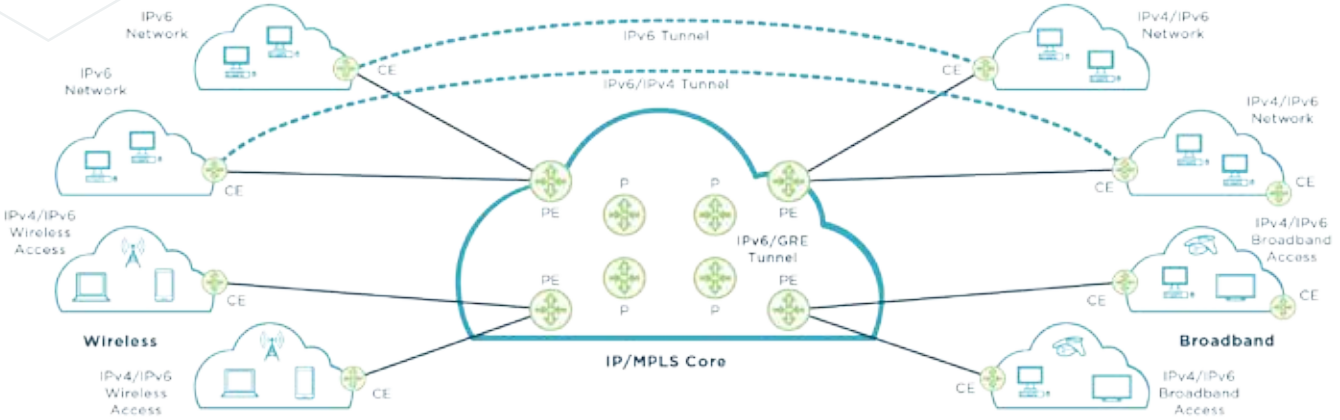
SAMPLE OF IXCHARIOT-SUPPORTED PROTOCOLS	
Topic	**Supported Protocols**
Management	Citrix and Microsoft Remote Desktop
Database	Oracle, SAP, and SQL Server
E-mail	Microsoft Exchange, POP, and Lotus Notes
Peer-to-peer	Kazaa, BitTorrent
IM, Online meeting	RealMedia, NetMeeting, AIM, ICQ, MSN Messenger, Yahoo Messenger
Data	HTTP, FTP, DNS, NNTP, POP, Telnet

SUGGESTED APPLICATIONS AND PLATFORMS	
IxChariot	Network assessment software with test scripts for more than 170 protocols, available in: • Server Edition - installed on server or in the cloud, users access with a Web browser • Desktop Edition - installed as a windows application
XR2000 and XRPi Hardware Endpoint	Works with IxChariot to provide: • Active network and application assessment and monitoring • Advanced routing support • Active traffic generation supporting 150+ applications • Up to line-rate generation • Endpoint-to-endpoint tests: UDP, TCP traffic, voice, video, and traffic mixes
Test endpoints	Supplied software endpoints for a wide variety of operating systems, including: • Microsoft Windows • Windows CE/Mobile • Linux, including Embedded Linux • Unix • Mac OS, IOS • Android • Virtual machines in hypervisors or cloud

IxChariot


IXCHARIOT STATS
ADMINISTRATION | CONFIGURATION | STATISTICS | SESSIONS | RESULTS | MY PROFILE | HELP
STOP TEST
THROUGHPUT
Lost data
Datagrams
Datagram Errors

IPV6 TESTING



SCENARIO

IPv4 addresses are exhausted, and many organizations are shifting to IPv6. Given the extent to which IPv4 addresses are embedded in networks and applications, IPv4 and IPv6 addresses will coexist for decades. Upgraded network architectures need to support IPv4 and IPv6 technologies and associated transition/translation mechanisms and scale to accommodate a significant increase in clients and services.

IPv6 testing requires emulating the full range of protocols used in today's IPv4, IPv6, and transitional dual-stack networks, as well as fully stressing the data plane and associated tunneling/translation implementations of each device.

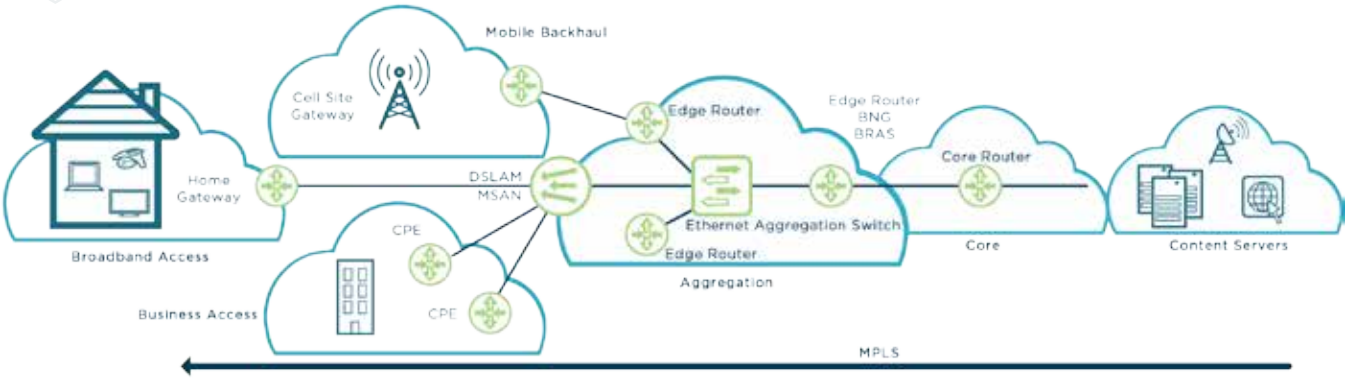
IXIA SOLUTIONS

Ixia equips NEMs and service providers with test plans and tools to fully evaluate the readiness of each device, system, or end-to-end network. Testing will answer critical questions such as:

- Can my system correctly assign and scale IPv4 and IPv6 addresses for Internet access?
- Is my system capable of ensuring QoS for both IPv4 and IPv6 traffic for increasing subscribers and load?
- Are my tunneling and translation implementations robust?
- What is my NAT table capacity and forwarding performance?
- How is application responsiveness and performance impacted when transition or translation mechanisms are pushed to their limits?
- Is my dual-stack core network capable of supporting the increased load of mixed IPv4/IPv6 routing?

SUGGESTED APPLICATIONS	
IxNetwork/ IxNetwork VE	Full L2–3 switch and router testing, with optional traffic generation and protocols: • Routing – BGP4/BGP4+, OSPFv2/ OSPFv3, ISISv4/ISISv6, RIP/RIPng, PIM-SM/SSMv4, PIM-SM/SSMv6 • Broadband access – PPPv4/v6/ dual-stack PPP, DHCPv4 client/server, DHCPv6 client/ server, PPPv4/PPPv6/dual-stack PPP over L2TPv2 LAC and LNS, IGMP/MLD, IPv6 stateless auto-configuration, DS Lite, 6rd
IxANVL	Protocol conformance testing, with: • Routing – RIP, RIPng, OSPFv2/v3, ISISv4/v6, BGP-4, BGP4+ • MPLS – RSVP-TE, RSVP-TE P2MP, LDP, VPWS/PWE3, VPLS-LDP, VPLS-BGP, L3 MPLS VPN, 6VPE • IP multicast – IGMPv1/v2/v3, MLDv1/v2, PIM-SM/SSMv4/v6, PIM-BSR • Switching – STP/RSTP, MSTP, link aggregation (LACP) • Broadband – PPPoX, DHCPv4 client/server, DHCPv6 client/server, L2TPv2
IxLoad/IxLoad VE	Comprehensive and scalable support for IPv6 service emulations and transition technologies such as 6RD/DSLite, SLAAC, and PPTP.
BreakingPoint/ BreakingPoint VE	Stress data center/cloud infrastructures using peak application user load from hundreds of applications to configure virtualized environments for optimal performance and capacity
SUGGESTED LOAD MODULES	
Novus 100GE QSFP28	Testing of 100/50/25GE over copper multi-mode and single-mode; designed for large-port-count testbeds
Novus ONE	Complete L2–7 network and application testing in a portable appliance
Novus 10G/1G/100M	High-density dual-PHY tri-speed solution for ultra-high-scale and performance testing
PerfectStorm	Application traffic and security attacks at 960 Gbps with the load of 720 million concurrent wired and wireless users from a single 11U chassis
PerfectStorm ONE	Enterprise-ready portable appliance for 10/1GE real-world, high-stress testing with up to 80Gbps of application traffic
CloudStorm	Cloud-scale, multi-terabit application delivery and network security test platform
SUGGESTED CHASSIS	
XGS12 Chassis	Industry's highest 100/40/10GE port densities in 11RU vertical rack space, reducing space requirements and simplifying management
XGS2 Chassis	Two-slot ultra-high-performance 3RU Chassis

MPLS TESTING



SCENARIO

Driven by massive growth in data traffic, service providers are moving toward a single packet network infrastructure that supports multiple services at lower operational costs.

Success and familiarity with Multiprotocol Label Switching (MPLS) in the core is driving service providers to deploy it into non-core network services, such as access, aggregation, and backhaul networks supporting broadband, business, and mobility services.

Additionally, with MPLS-transport profile (MPLS-TP), an industry standard is emerging to enable connection-oriented packet transport to meet the growing demand. MPLS is under active development with new mechanisms and applications emerging from the standards bodies, continually increasing its popularity.

As MPLS-based technologies and services continue to evolve, deploy, and increase in scale, the test challenges become increasingly complex. Ixia continues to provide the most comprehensive test capability for validating the MPLS infrastructure and the services it supports.

IXIA SOLUTIONS

Ixia helps answer critical MPLS questions, such as:

- Can my device or network reliably deliver multiple MPLS-based VPN services—L2, L3 (unicast, multicast)—simultaneously?
- Does my device maintain thousands of MPLS tunnels and pseudo-wires with the required level of forwarding performance?
- Are MPLS-TP features working properly? Can I interoperate with other vendors?
- Does my device conform to the latest MPLS-related standards?
- Does MPLS traffic engineering provide sub-50ms recovery?

SUGGESTED APPLICATIONS	
IxNetwork/ IxNetwork VE	Full L2–3 switch and router testing, with integrated traffic generation and optional protocols and features, including: • Routing and switching protocols • MPLS protocols • MPLS-TP protocols and features (supported on IxNetwork only) • VPLS protocols • IP multicast protocols • High availability • IPv4/IPv6 traffic generation
IxANVL	Protocol conformance testing, with: • RIP/NG, OSPFv2/v3, BGP4/4+, ISISv4/v6, VRRP • LDP, RSVP-TE, MPLS, PWE3, L2 VPN, L3 VPN, VPLS, LSP-Ping, VCCV, mLDP
Network Emulator II	Emulates real-world network impairment conditions in the lab to validate network-based products, applications, and services
SUGGESTED LOAD MODULES	
Novus 100GE QSFP28	Testing of 100/50/25GbE over copper multi-mode and single-mode; designed for large-port count testbeds
Novus ONE	Complete L2-7 network and application testing in a portable appliance
Novus 10G/1G/100M	High-density dual-PHY tri-speed solution for ultra-high-scale and performance testing
SUGGESTED CHASSIS	
XGS12 Chassis	Industry's highest 100/40/10GE port densities in 11RU vertical rack space, reducing space requirements and simplifying management
XGS2 Chassis	Two-slot ultra-high-performance 3RU Chassis

MULTIPLAY NETWORK TESTING

SCENARIO

Media convergence is fueling the growth and complexity of today's IP networks. To effectively compete, service providers must deliver differentiated multiplay services, including Voice over Internet Protocol (VoIP), peer-to-peer (P2P) gaming, Internet Protocol Television (IPTV), streaming media, high-speed Internet, and mobile services over converged networks. There are numerous challenges associated with the delivery of multiplay services due to the different characteristics of voice, video, and data traffic:

- Voice traffic consumes fairly low bandwidth, but is highly sensitive to network jitter
- Video services require a steady stream of high bandwidth traffic and are severely impacted by packet reordering and loss
- Data services, such as web browsing, file transfer, and other end-user interactive applications, have varying requirements

Proper QoS provisioning, performance analysis, and capacity planning are key requirements for ensuring a successful service rollout and sustained growth.

Today's data center networks support a complex application delivery infrastructure that must recognize, prioritize, and manage application traffic with differentiated classes of service. The emergence of integrated service routers (ISRs), application-aware firewalls, server load balancers, WAN accelerators, and devices that use DPI, enabled service providers to deliver superior application performance and security while improving user QoE.

Equipment vendors need a comprehensive test solution for validating the functional capabilities, performance, and scalability of their next-generation hardware platforms. Enterprises and service providers face similar challenges as they attempt to ensure that their networks can deliver on performance and availability requirements, while maintaining proper QoS for all mission-critical data, voice, and video traffic.

SUGGESTED APPLICATIONS AND PLATFORMS

Protocol	Options
Data	HTTP/2, HTTP (1.0/1.1), SSLv2, SSLv3, TLSv1.1, TLS 1.2, TCP, FTP, TFTP, SMTP, POP3, IMAP, Database, SMB, NFS, iSCSI, DNS, DHCP, LDAP and RADIUS
Video	IGMPv2/3, MLDv1/2, RTSP, RTP/UDP, Adobe Flash Player, Microsoft Silverlight Player, Apple HLS Player, Adobe HDS, and MPEG DASH
Voice	SIP, WebRTC, MGCP, H.323, H.248 (Megaco), Cisco SCCP (Skinny), RTP and SRTP, Audio, Conversational Video, File Transfer (MSRP) – only with SIP and Fax over IP (T.38) (only with SIP)
Replay Traffic	AppReplay – Replays stateful and stateless captures to simulate emerging and propriety Internet traffic
Application Mixes	AppLibrary – A continually expanding and updated library of pre-defined application flows and application mixes of the most current internet applications

IXIA SOLUTIONS

The requirements for testing application-aware devices are complex and resource-intensive. You need to exercise devices beyond their limits to ensure optimal functionality, performance, availability, and reliability.

Ixia's IxLoad is the industry's most scalable and integrated solution for converged multiplay service delivery testing. It is an ideal solution for assessing the performance of application-aware DPI-capable devices.

IxLoad delivers multiplay service emulation in a single testbed, including IPTV/Video on Demand (VoD), VoIP, P2P, web, file transfer protocol (FTP), streaming, and e-mail. Ixia's platform delivers ultra-high-performance that scales to millions of subscribers. Subscriber modeling accomplishes true traffic testing by emulating dynamic user community behavior. IxLoad generates per-subscriber QoE analysis on key metrics, including video and audio quality, channel change times, application latency, and response times.

IxLoad supports Authentication, Authorization, and Accounting (AAA)/Remote Authentication Dial-In User Service (RADIUS) services, Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Lightweight Directory Access Protocol (LDAP) to assess critical infrastructure components. It uses DDoS and vulnerability attack traffic generation to validate the impact of malicious traffic on multiplay services.

IxLoad emulates subscribers with a complete mix of multiplay traffic, measures the scalability of the converged service delivery infrastructure, validates the impact of P2P on revenue-generating services, such as IPTV and VoIP, and ensures QoE on a per-subscriber and/or per-service basis.

IxLoad enables application performance testing using:

- Realistic stateful emulation of application services
- Application replay to record and replay stateful transactions to test devices that handle emerging and proprietary protocols
- QoE detective for granular instant insight into per-user, per-IP and per-VLAN issues

BreakingPoint and IxNetwork solutions also complement IxLoad's functionality.

IxNetwork provides wire-rate traffic generation with service modeling that builds realistic, dynamically-controllable data plane traffic. IxNetwork offers the industry's best test solution for functional and performance testing by using comprehensive emulation for routing, switching, MPLS, IP multicast, broadband, authentication, Carrier Ethernet, and data center bridging (DCB) protocols.

BreakingPoint enables the creation of real-world legitimate traffic with full control of the load capacity and detailed per-simulated host reporting. It offers robust Common Internet File System (CIFS) and web application testing capabilities for WAN acceleration.

SUGGESTED APPLICATIONS	
IxLoad/IxLoad VE	Delivers comprehensive performance testing for validating user quality of experience of multiplay services. IxLoad works by emulating web, video, voice, storage, VPN, wireless, infrastructure, and encapsulation/security protocols to create realistic scenarios.
IxNetwork/ IxNetwork VE	Full L2–3 switch and router testing, with optional protocols: • Routing protocols • Integrated broadband access protocol emulation with service traffic generation testing • Application traffic over routes
BreakingPoint/ BreakingPoint VE	Stress data center/cloud infrastructures using peak application user load from hundreds of applications to configure virtualized environments for optimal performance and capacity
Network Emulator II	Emulates real-world network impairment conditions in the lab to validate network-based products, applications, and services
SUGGESTED LOAD MODULES	
PerfectStorm	Application traffic and security attacks at 960 Gbps with the load of 720 million concurrent wired and wireless users from a single 11U chassis
PerfectStorm ONE	Enterprise-ready portable appliance for 10/1GE real-world, high-stress testing with up to 80Gbps of application traffic
CloudStorm	Cloud-scale, multi-terabit application delivery and network security test platform
Novus ONE NP	Complete L2–7 network and application testing in a portable appliance
Novus 10G/1G/100M NP	High-density dual-PHY tri-speed solution for high-scale and performance testing
SUGGESTED CHASSIS	
XGS12 Chassis	Industry's highest 100/40/10GE port densities in 11RU vertical rack space, reducing space requirements and simplifying management
XGS2 Chassis	Two-slot ultra-high-performance 3RU Chassis

IxLoad

IxNetwork

BreakingPoint

Network Emulator II

PerfectStorm

PerfectStorm ONE

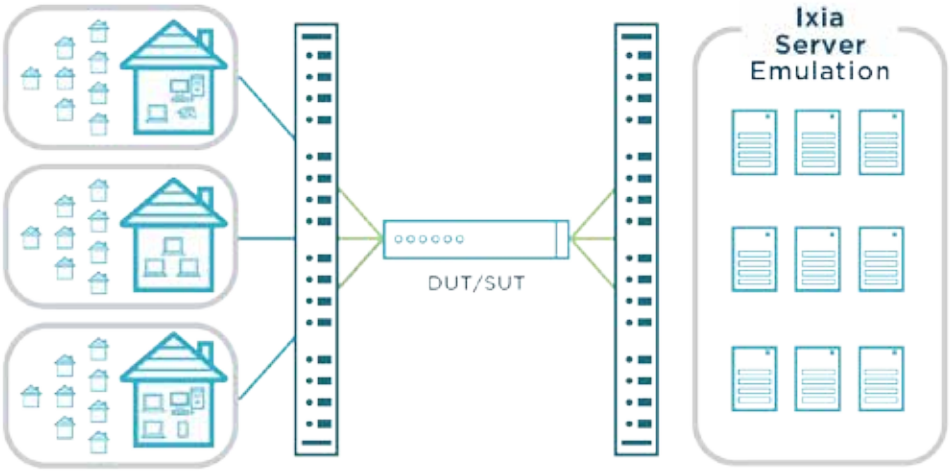
CloudStorm

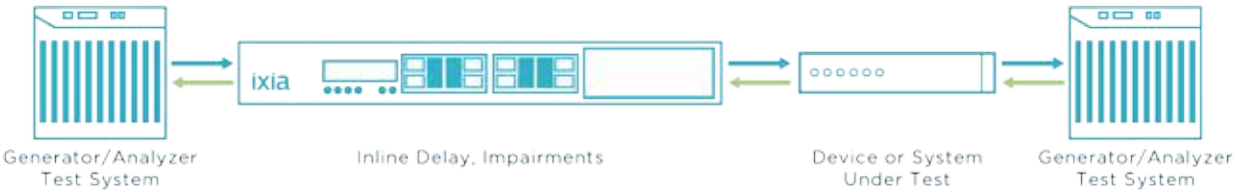
Novus ONE

Novus 10G/1G/100M

XGS12

XGS2





SCENARIO

As customers develop or deploy new products, they need assurance that those products will function properly in real network conditions that occur in live-production Local Area Network (LAN)/WAN networks. In live networks, the network or the application may experience delays and the effects of those delays should be simulated in a controlled testing environment. The reaction of products and applications to worst-case network conditions is an important consideration as you bring new products and applications into the network.

IXIA SOLUTIONS

Ixia's Network Emulator II is a precision test instrument for 10GE, 1GE, and 100MbE impairment. The device allows users to accurately emulate the real network conditions that occur over live-production LAN/WAN networks. By emulating realistic and worst-case network conditions in the lab, users can validate and test the performance of new hardware, protocols, and applications to prevent failures in production networks.

Emulate real-world networks in the lab:

- Create a real-world testing environment by reproducing realistic network conditions and behavior
- Test validation, performance, and interoperability
- Test products and applications to characterize end-user experience under real-world conditions
- Precisely reproduce and quickly resolve issues occurring in the field

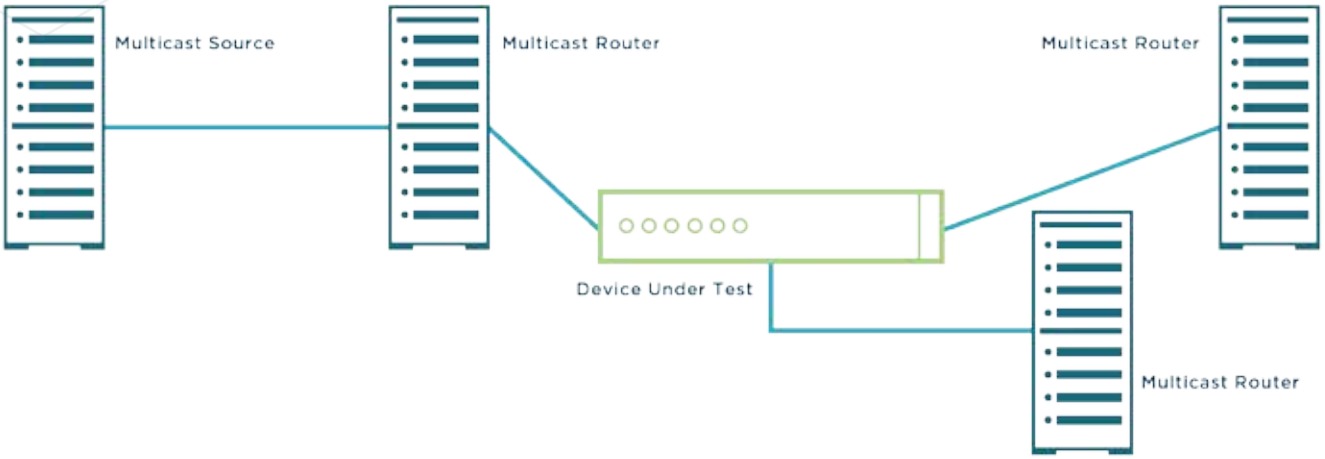
The Network Emulator II offers a rich feature set to allow testing in a controlled lab environment with repeatable and predictable impairments. Network Emulator II enables you to:

- Test the effect of delay on the network and application performance
- Determine how applications will perform when distributed across data centers
- Test data center backup in a real-life environment
- Cause outage and degrade scenarios to trigger and validate fail-over protection
- Combine with IxNetwork, IxLoad, and BreakingPoint test systems to create a complete test environment that includes real-world impairments

SUGGESTED PLATFORM	
Network Emulator II	Rack-mountable 1U eight-port emulator with Ethernet 10GE, 1GE, and 100MbE Network Emulator Software available in eight-port or two-port licenses.

Network Emulator II

PROTOCOL CONFORMANCE TESTING



SCENARIO

Today's communications protocols are complex. Every day, new protocol specifications, Request for Comments (RFCs), and enhancements are published by standards organizations. Service providers must make sure that the devices they deploy perform correctly. NEMs seek to ensure that their products conform to industry standards and interoperate successfully with other vendors' products.

Early conformance testing ensures higher product quality. This quality has a significant payoff—problems found after deployment can cost 100 times more to fix than those found in the lab. Security loopholes and vulnerabilities resulting from erroneous protocol implementations can damage a company's reputation and incur legal liability.

IXIA SOLUTIONS

Ixia's IxANVL is the industry standard and leader for automated network protocol validation. IxANVL's tests are used to determine whether a device's protocol implementation meets specifications, how well a device handles traffic from non-compliant network components, and the effect of new features on existing software through regression testing.

SUGGESTED APPLICATIONS	
IxANVL	Comprehensive protocol conformance testing
SUGGESTED LOAD MODULES	
Novus 100GE QSFP28	Testing of 100/50/25GE over copper multi-mode and single-mode; designed for large-port-count testbeds
Xcellon-Multis	Testing of 100/40/10GE and 100/25GE using fan-out technology; supports mid-range to high-scale protocol testing
SUGGESTED CHASSIS	
XGS12-SD Chassis	Industry's highest 100/40/10GE port densities in 11RU vertical rack space, reducing space requirements and simplifying management
XGS2-SD Chassis	Two-slot ultra-high-performance 3RU Chassis

FAMILY	CONFORMANCE TESTS
Routing	RIP/NG, OSPFv2/v3, BGP4/4+, ISISv4/v6, VRRP
MPLS	LDP, RSVP-TE, MPLS, PWE3, L2 VPN, L3 VPN, VPLS, LSP-Ping, VCCV, mLDP
Multicast	IGMPv2/v3, MLDv1/v2, PIM-SMv4/v6, PIM-DM, DVMRP, IGMP/MLD snooping
Carrier Ethernet	MEF9, Ethernet CFM/OAM, service OAM, PBB MEF OAM/ELMI/service OAM, G8031
High Availability	BFD, OSPF-GR
IP	IPv4, DHCPv4/v6, ICMP, IPv6, IPv6CP, ICMPv6, NDP, AutoConfig, PMTU, GRE, GPT, IPv6ov4
TCP	TCP core, TCP advanced, TCP high performance
Data Center	FIP, FCoE, FCF, DCBX
Bridging	STP, RSTP, MSTP, VLAN, GRE, QinQ EAPOL(802.1x), PPP, MLPPP, IPCP, LACP, 802.1ad, LLDP
Layer 4–7	HTTP, telnet
Security	L2TPsec, IPsecv4/v6, IKEv1/v2
Voice	SIP
Storage	iSCSI
Mobile IP	Home agent, correspondent node, mobile node
Broadband	PPP, PPTP, L2TP, ANCP, PPPoX, LACP

IxANVL

SCENARIO

Networks and network devices are becoming increasingly complex. Enterprise expansion, data center convergence, and new service deployments require that diversified networking technologies and devices operate together seamlessly.

As multiple special-purpose networks converge into a single network carrying voice, video, data, and wireless traffic, it is critical that device manufacturers verify the scalability, stability, and performance of their switches and routers.

Service providers must carry multiplay services on a single IP network in order to offer increasingly popular applications, such as YouTube, Facebook, and P2P exchange. The demand for a larger capacity and more services increases the complexity and scale of modern networks and devices. Providers must validate service differentiation based on configured QoS policies and SLAs, in addition to determining the service impact on existing network structures from new applications.

Within the data center, LAN and SAN traffic have traditionally used separate Ethernet and fibre channel networks. Cost-effective 10GE networks have provided the economic incentive to combine these networks using a new generation of DCB components, including fibre channel over Ethernet (FCoE) switches and SANs.

IXIA SOLUTIONS

Ixia's solutions comprehensively test the interoperability, performance, and scale of networking devices. Ixia's IxNetwork offers the industry's most complete test solution for functional and performance testing by emulating routing, switching, MPLS, IP multicast, broadband, and authentication protocols.

Ixia test ports accurately emulate an Internet-scale networking environment containing thousands of routers and switches and millions of routes and reachable hosts. Millions of traffic flows can be easily customized to stress and track data plane performance.

Subscriber modeling simulates user communities that match the behavior of city-size groups using multiplay services, such as web, e-mail, FTP, P2P, VoIP, and video. Ixia's testing capabilities scale to stress the largest and most powerful networking devices.

Ixia load modules, consisting of multiple test ports, provide network interfaces of all types. Our mainstay Ethernet interfaces operate over the full range from 10Mbps through 100Gbps speeds and newly evolving needs for 400Gbs. Line-rate traffic is generated to characterize the performance and reliability of data forwarding.

To test complex scenarios, Ixia's solutions:

- Model millions of services with deterministic traffic profiles
- Define different rate-controllable traffic profiles on a per-service basis
- Validate SLAs through dynamic modification of traffic profiles
- Produce service-and subscriber-level statistics

Use the IxNetwork graphical user interface (GUI) to easily configure complex L2–3 VPN topology simulations. Tests scale to stress the performance of the most powerful border gateway protocol (BGP)- and MPLS-capable routers. Each central processing unit (CPU)–equipped test port advertises hundreds of label distribution protocol (LDP) sessions and thousands of forwarding equivalence classes (FECs), as well as hundreds of VPN sessions and thousands of VPN routes. Wire-speed traffic can be generated over the VPN topology to simultaneously test data and control planes.

Ixia test applications are perfect for both interactive test development and automated execution. Easy-to-use GUIs and wizards help you create complex emulations and traffic. Aggregated, per-user, per-virtual local area network (VLAN), and per-VPN statistics quickly identify any failure or diminished service. The event scheduler provides powerful GUI-based automation, and its ScriptGen tool offers an easy, one-click GUI-to-script automation solution. A number of integrated tests provide standards-based test methodologies. IxNetwork supplies full-featured Application Program Interfaces (APIs) for automated testing.

ROUTING AND SWITCHING PROTOCOL EMULATION	
Technology	**Protocols**
Routing	RIP, RIPng, OSPFv2/v3, ISISv4/v6, EIGRP, EIGRPv6, BGP4+, BGP+
MPLS	RSVP-TE, RSVP-TE P2MP, LDP, PWE, L3 MPLS VPN, 6PE, GMPLS, MPLS-OAM
VPLS	VPLS-LDP, VPLS-BGP
High availability	BFD
IP multicast	IGMPv1/v2/v3, MLDv1/v2, PIM-SM/SSM, PIM-BSR, Multicast VPN, VPNv6, MSDP
Switching	STP/RSTP/MSTP, PVST+, RPVST+, Link Aggregation (LACP)
Broadband	ANCP, PPPoX, DHCPv4/v6, client/server, L2TPv2, RADIUS Attributes for L2TP
Authentication	802.1x, WebAuth, Cisco NAC
Traffic	Ethernet, IPv4, IPv6, VLAN, MPLS multi-label, L2/L3 MPLS, VPN, VPLS, 6VPE, Multicast, Multicast VPN

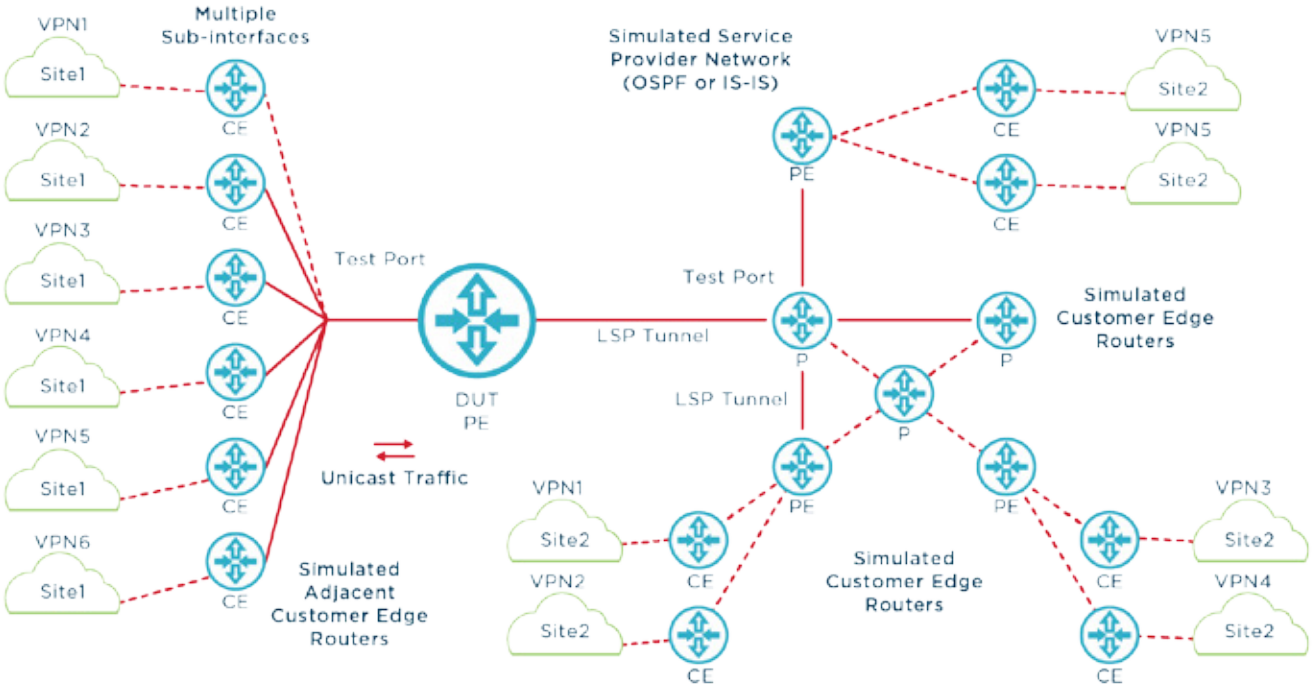
SUGGESTED APPLICATION	
IxNetwork/ IxNetwork VE	Full L2–3 switch and router testing, with optional protocols: • Routing protocols • Broadband testing • Application traffic over routes
SUGGESTED LOAD MODULES	
Novus 100GE QSFP28	Testing of 100/50/25GE over copper multi-mode and single-mode; designed for large-port-count testbeds
Novus ONE	Complete L2–7 network and application testing in a portable appliance
Novus 10G/1G/100M	High-density dual-PHY tri-speed solution for ultra-high-scale and performance testing
SUGGESTED CHASSIS	
XGS12 Chassis	Industry's highest 100/40/10GE port densities in 11RU vertical rack space, reducing space requirements and simplifying management
XGS2 Chassis	Two-slot ultra–high–performance 3RU Chassis

IxNetwork

KEVIN DEIERLING

Vice President Marketing, Mellanox Technologies

Big data and faster solid state storage is driving the rapid adoption of our 25, 50, and 100 Gbps Ethernet networking gear.



AUTOMOTIVE ETHERNET TESTING

SCENARIO

Automotive technology has changed over time to a moving combination of integrated computer systems—advanced driver assistance systems (ADAS), adaptive cruise control, hybrid engines, Internet access, and Bluetooth connection. To ensure optimal design, functionality, performance, safety, security, and interoperability of these connected cars, automakers and their suppliers need comprehensive test solutions to validate devices, systems, applications, and even the entire in-vehicle network.

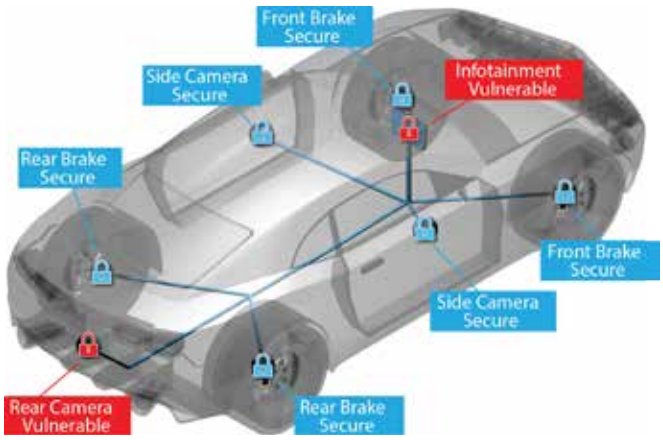
Automotive manufacturers have relied on complex and custom solutions to perform testing as they develop and integrate new technologies. The use of an Ethernet backbone now requires open, standard solutions that deliver testing across the whole automotive ecosystem. Ixia's unique automotive Ethernet test solutions include conformance, wireless, application, and security validation.

IXIA SOLUTIONS

Ixia products enable real-world validation of in-vehicle fixed, wireless, and security technologies, empowering the automotive industry to build best-in-class in-vehicle infotainment and always-on networking.

- Automotive Conformance Testing: Quickly validate the interoperability and standards compliance of vehicle, technology that links autos and mobile devices to each other and to transportation infrastructure with Ixia's conformance test solution.
- Automotive Wireless Testing: Ensure an always-on user experience by validating connectivity within the vehicle to onboard systems, sensors, and user devices and beyond the vehicle to ensure mobile data services and security.
- Automotive Applications Testing: Validate that multimedia applications perform optimally over any device and network by understanding how your applications and services will perform under real-world in-car conditions, attacks, and impairments.
- Automotive Security Testing: Ensure the safety and security of connected cars by testing the systems designed to protect the in-vehicle network from cyberattacks. Ixia security solutions validate security capabilities using line-rate application traffic and real-world security attacks.

SUGGESTED APPLICATIONS	
IxNetwork/ IxNetwork VE	Full L2–3 testing, with emulation of: • Link OAM (802.3ah), Service OAM - IEEE 802.1ag, ITU-T Y.1731 • QinQ, PBB/PBB-TE, STP/RSTP/MSTP, LACP
IxANVL	• Validate protocol conformance to specific standards • Increase interoperability between devices • Identify software issues in early product lifecycle
IxLoad/IxLoad VE	Full L4–7 testing, with options for: • SIP, H.323, MGCP, H.248, SCCP • RTP/RTCP/SRTP • Audio, video, fax, instant messaging
BreakingPoint/ BreakingPoint VE	Control global threat intelligence at Internet-scale to create massive high-fidelity simulation and testing conditions for battle-testing infrastructures, devices, applications, and people
SUGGESTED LOAD MODULES	
Novus 100GE QSFP28	Testing of 100/50/25GE over copper multi-mode and single-mode; designed for large-port-count testbeds
Novus ONE	Complete L2–7 network and application testing in a portable appliance
Novus 10G/1G/100M	High-density dual-PHY tri-speed solution for ultra-high-scale and performance testing
PerfectStorm	Application traffic and security attacks at 960 Gbps with the load of 720 million concurrent wired and wireless users from a single 11U chassis
PerfectStorm ONE	Enterprise-ready portable appliance for 10/1GE real-world, high-stress testing with up to 80Gbps of application traffic
CloudStorm 100GE	Cloud-scale application delivery and network security test platform
SUGGESTED CHASSIS	
XGS12 Chassis	Industry's highest 100/40/10GE port densities in 11RU vertical rack space, reducing space requirements and simplifying management
XGS2 Chassis	Two-slot ultra-high-performance 3RU Chassis



CHIP DESIGN PERFORMANCE TESTING

SCENARIO

Trends such as cloud computing and network functions virtualization (NFV) are pushing the boundaries of network capacity. To support this demand, network equipment manufacturers and chip manufacturers need to keep up by delivering ultra-high-density devices powered by state-of-the-art system-on-a-chip (SoC) solutions.

Producing an SoC, each capable of handling terabits of traffic across hundreds of ports at speeds up to 100Gbps is a lengthy process. But with increased time-to-market pressures, all major chip manufacturers are looking to accelerate their development cycles. The cost associated with fixing bugs after chip 'tape out' is substantial and can cost millions of dollars. To de-risk schedules, testing needs to happen early and often—pre-silicon.

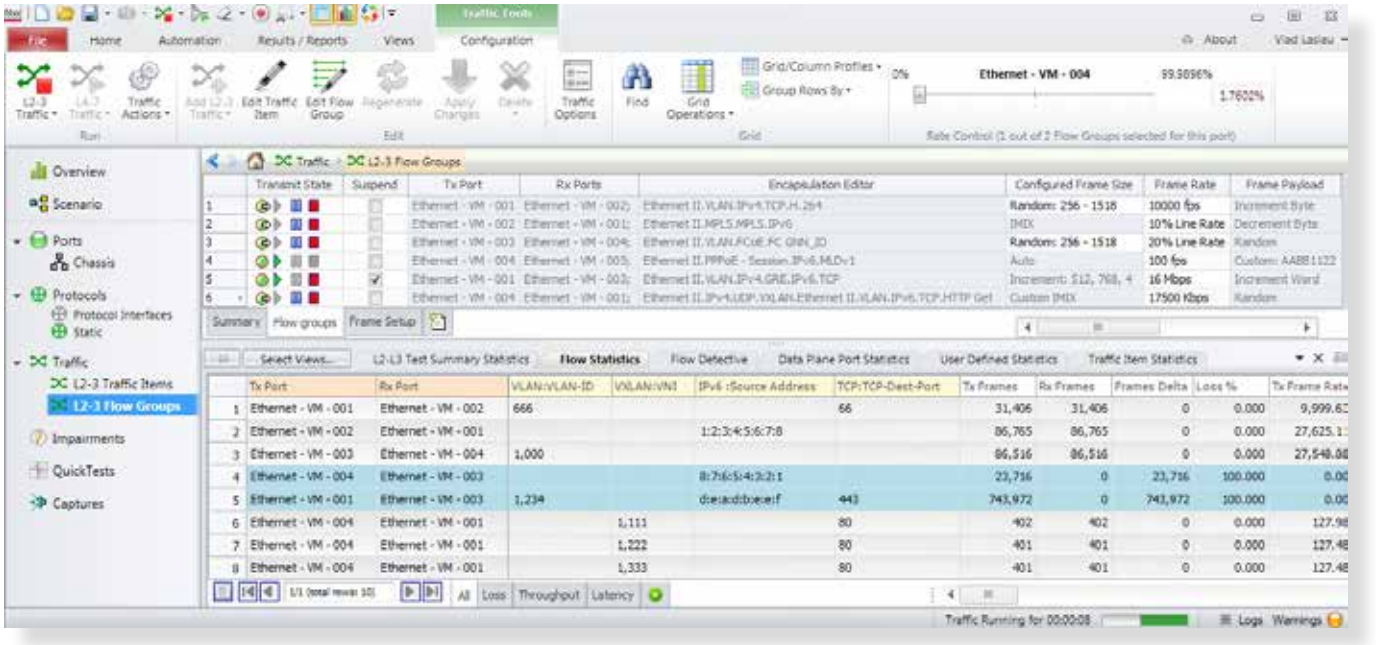
IXIA SOLUTIONS

Ixia's IxVerify is the industry's only test solution purpose-built for "pre-silicon" validation. With this solution, Ixia and its partners are leading the way in transforming the Electronic Document Access (EDA) market by offering virtualized test solutions that work in conjunction with existing and new-age EDA systems—leveraging virtualization to reduce costs and offer increased flexibility.

IxVerify extends Ixia's intellectual property and test expertise into the EDA space. It enables new and improved test methodologies to simplify pre-silicon testing and shifts testing further into the development cycle.

IxVerify provides hundreds of predefined packet templates for testing Ethernet and transport control protocol (TCP)/IP protocols and is capable of generating high volumes of traffic. With its ability to run hundreds of virtualized test ports at once, it offers the unique ability to dynamically shape traffic to ensure zero packet loss at maximum emulation speeds.

IxVerify is the perfect solution for de-risking complex networking chip design and development and ensures faster time to market for the next generation of networking devices.



SCENARIO

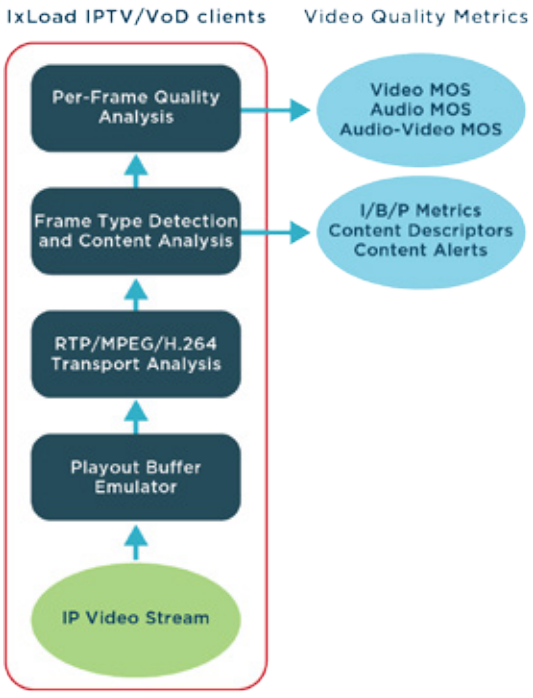
As more content is offered in high definition (HD) and service providers charge a premium for it, subscribers are likely to churn faster when dissatisfied. Degradation in audio/visual QoE leads today's consumer to competitor solutions that offer a better end-user experience. With traffic levels high and expected to grow for the foreseeable future, service providers are challenged to assess video quality with real-world traffic loads in pre-deployment testing.

Customers need to be able to:

- Measure the ability of a transport network to carry video data
- Determine the optimal user session limits of edge and origin media servers, content proxies, etc.
- Stress-test middleware devices, such as encoder systems and DRM
- Measure the perceived quality of the video delivered to the end user
- Determine the total number of streams a CDN can handle
- Test performance of key IPTV infrastructure services

IXIA SOLUTIONS

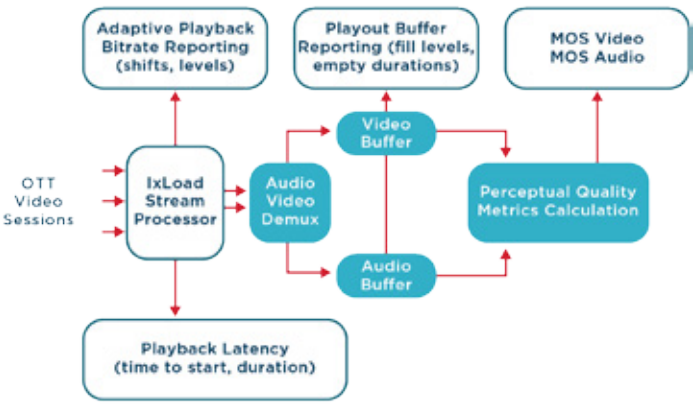
Ixia provides a comprehensive test solution for video delivery platforms with IxLoad. IxLoad delivers the industry's most scalable and flexible solution for realistic load testing of over the top (OTT), VoD, IPTV media, and cache platforms to validate end-to-end video delivery architectures. Emulate thousands of interactive on-demand and live streaming user sessions and measure real-time video quality.



This Ixia solution enables customers to:

- Emulate adaptive streaming behavior that dynamically up-shifts or down-shifts the media stream to deterministically play back streams of different quality
- Create static profiles of user behavior that are fixed on different playback levels to deterministically play back streams of different quality with no network heuristic at play
- Define subscribers' activities and flexible channel viewing sequence with scenario editor
- Support data, voice, and video protocols simultaneously to emulate a multiplay subscriber environment with intelligent, real-time issue isolation mechanism

SUGGESTED APPLICATION	
IxLoad/IxLoad VE	Delivers the industry's most scalable and flexible solution for realistic load testing of OTT, VoD, IPTV media, and cache platforms to validate end-to-end video delivery architectures; emulate thousands of interactive on-demand and live streaming user sessions and measure real-time video quality
SUGGESTED LOAD MODULES	
PerfectStorm	Application traffic and security attacks at 960 Gbps with the load of 720 million concurrent wired and wireless users from a single 11U chassis
PerfectStorm ONE	Enterprise-ready portable appliance for 10/1GE real-world, high-stress testing with up to 80Gbps of application traffic
CloudStorm	Cloud-scale, multi-terabit application delivery and network security test platform
Novus-NP 10G/1G/100M	High-density dual-PHY tri-speed solution for high-scale and performance testing
SUGGESTED CHASSIS	
XGS12 Chassis	Industry's highest 100/40/10GE port densities in 11RU vertical rack space, reducing space requirements and simplifying management
XGS2 Chassis	Two-slot ultra-high-performance 3RU Chassis



TCP video quality assessment using IxLoad

SCENARIO

The "virtualization" of traditional networks promises vast and enduring benefits. In replacing proven technologies with new techniques, a new approach is needed to reduce complexity, mitigate risk, and get it right the first time.

Technology becomes more open, provisioning is more fluid, and networks are more application-aware. Through increased agility and software-based control, virtualization delivers dramatic cost savings and a new networking model that fast-tracks delivery of high-value services. At the very least, virtualized network functions (VNFs) need to deliver the same or better performance than the traditional network. With false starts likely to impact the brand, as well as the budget, new and old strategies are needed to quantify the benefits of virtualization and overcome challenges.

DEMYSTIFY THE PROCESS, DELIVER ON THE PROMISE

With virtualization, everything known—and proven—becomes unknown and unproven again. Complexity increases. New network elements introduce new vulnerabilities. Visibility is lost as the traditional physical boundaries become blurred in the cloud.

To transcend the hype and achieve the very real benefits, vital questions need to be answered:

- What benefits do we hope to achieve?
- Which functions should be virtualized, and when?
- How will migration to commercial hardware—and the cloud—impact the user experience?
- How do we maintain visibility as everything scales?
- How do we know it worked?

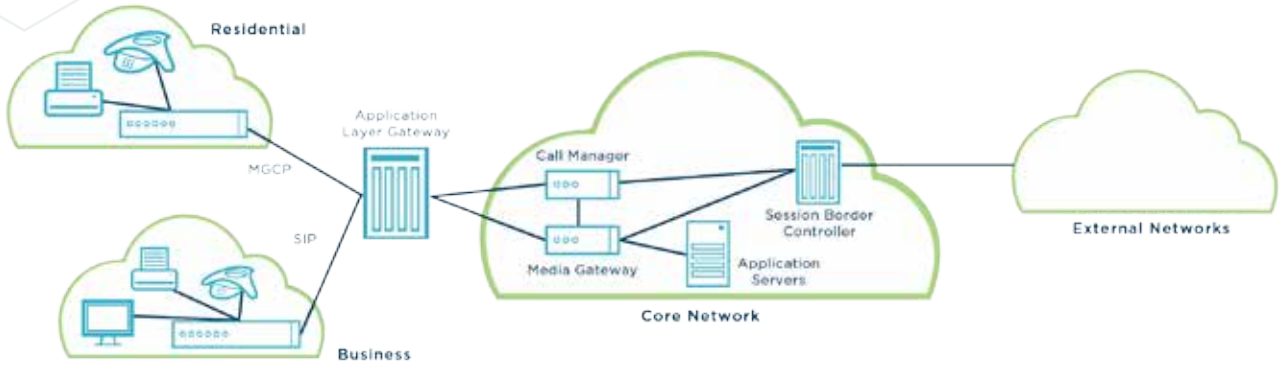
Throughout the migration process, enterprises and service providers must weigh the trade-offs between quality and cost and flexibility and control.

IXIA SOLUTIONS

Today's networks need to adapt quickly and facilitate change. Strategies like NFV and Software Defined Networking (SDN) provide powerful flexibility gains by moving functions like Customer Premises Equipment (CPE), BRAS, load balancing, firewalls, and Evolved Packet Core (EPC)/IP Multimedia Subsystem (IMS) components off dedicated hardware onto virtualized servers.

Ixia provides the industry's only life-cycle solution for eliminating the guesswork and validating the benefits of virtualization each step of the way.

SUGGESTED APPLICATIONS	
IxNetwork/IxNetwork VE	Full L2–3 testing, with emulation of: • Link OAM (802.3ah), Service OAM - IEEE 802.1ag, ITU-T Y.1731 • QinQ, PBB/PBB-TE, STP/RSTP/MSTP, LACP • VE provides a software edition of the application
IxLoad/IxLoad VE	Delivers comprehensive functional and performance testing to validate user QoE in physical and virtual networks. IxLoad VE emulates web, video, voice, storage, VPN, wireless, infrastructure, and encapsulation/security protocols to create realistic scenarios to measure the QoE of services delivered over virtual and physical infrastructure
BreakingPoint/ BreakingPoint VE	Control global threat intelligence at Internet-scale to create massive high-fidelity simulation and testing conditions for battle-testing infrastructures, devices, applications, and people
IxChariot	Employs endpoints that traverse firewalls to assess performance between private and cloud networks—without compromising security
SUGGESTED LOAD MODULES	
Novus 100GE QSFP28	Testing of 100/50/25GE over copper multi-mode and single-mode; designed for large-port-count testbeds
Novus ONE	Complete L2–7 network and application testing in a portable appliance
Novus 10G/1G/100M	High-density dual-PHY tri-speed solution for ultra-high-scale and performance testing
PerfectStorm	Application traffic and security attacks at 960 Gbps with the load of 720 million concurrent wired and wireless users from a single 11U chassis
PerfectStorm ONE	Enterprise-ready portable appliance for 10/1GE real-world, high-stress testing with up to 80Gbps of application traffic
CloudStorm 100GE	Cloud-scale application delivery and network security test platform
SUGGESTED CHASSIS	
XGS12 Chassis	Industry's highest 100/40/10GE port densities in 11RU vertical rack space, reducing space requirements and simplifying management
XGS2 Chassis	Two-slot ultra-high-performance 3RU Chassis



SCENARIO

VoIP is a major component of service providers' consumer and business offerings. Modern deployments now call for millions of simultaneous VoIP endpoints.

Although VoIP connections have a low bandwidth requirement, they are very sensitive to latency and jitter. Care must be taken to enforce appropriate QoS policies for voice traffic, balanced with the QoS requirements associated with video and data services.

IXIA SOLUTIONS

The IxANVL Session Initiation Protocol (SIP) suite tests the conformance of devices to SIP.

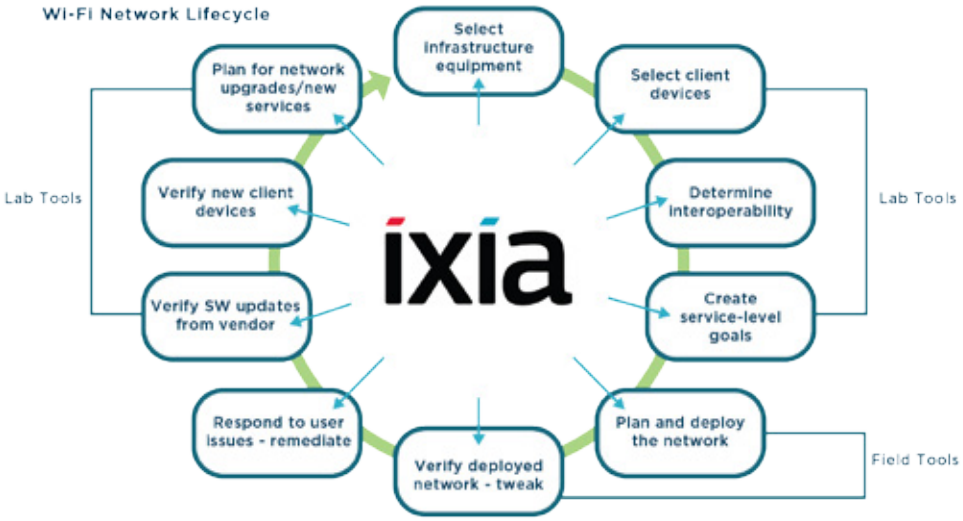
Ixia supports video and data protocols in addition to VoIP—making it perfect for testing a wide variety of components, including:

- SIP proxies and registrars
- MGCP and H.248 media gateways and media gateway controllers
- H.323 gatekeepers
- Call agents and call managers
- SBCs and ALGs
- Multiplay delivery networks
- VoIP services in NGN and IMS architectures

IXLOAD INCLUDES FEATURES ESSENTIAL TO FULL VOIP PROTOCOL TESTING:

- Very large-scale operation emulating more than 1 million subscribers per chassis
- Realistic, complex call flows
- Flexible test case creation through state machine and message content control
- Broad audio codec support: G.711 A-Law, G.711 µ-Law, G.729 A/B, G.726, G.723.1, and iLBC
- Support for H.264 codec media: video-conferencing
- Full user authentication and registration parameters
- Link layer and security protocols
- Library of prebuilt test cases
- Capture/replay can be used to test other protocols

SUGGESTED APPLICATIONS	
IxLoad/IxLoad VE	Most scalable and flexible solution for realistic load testing of VoIP platforms to validate end-to-end voice delivery architectures; it emulates thousands of user sessions with dynamic call flows and measures real-time voice quality
IxChariot	Live network testing, with SIP call emulation
BreakingPoint/ BreakingPoint VE	Control global threat intelligence at Internet-scale to create massive high-fidelity simulation and testing conditions for battle-testing infrastructures, devices, applications, and people
IxANVL	Protocol conformance testing with SIP conformance suite
Network Emulator II	Emulates real-world network impairment conditions in the lab to validate network-based products, applications, and services
SUGGESTED LOAD MODULES	
PerfectStorm	Application traffic and security attacks at 960 Gbps with the load of 720 million concurrent wired and wireless users from a single 11U chassis
PerfectStorm ONE	Enterprise-ready portable appliance for 10/1GE real-world, high-stress testing with up to 80Gbps of application traffic
CloudStorm	Cloud-scale, multi-terabit application delivery and network security test platform
Novus-NP 10G/1G/100M	High-density dual-PHY tri-speed solution for high-scale and performance testing
SUGGESTED CHASSIS	
XGS12 Chassis	Industry's highest 100/40/10GE port densities in 11RU vertical rack space, reducing space requirements and simplifying management
XGS2 Chassis	Two-slot ultra-high-performance 3RU Chassis



SCENARIO

Once used mainly for low-priority data, today's Wi-Fi networks carry real-time, multimedia traffic in consumer, service provider, and enterprise network environments worldwide. Mobile clients continue to grow in both numbers and complexity of application usage.

With Wi-Fi evolving from a "nice to have" to a primary network medium, poor performance now places brand reputation, profitability models, customer satisfaction, and even lives at risk. Today's wireless LANs (WLANs), Wi-Fi enabled devices, and mobile applications must deliver unprecedented quality, reliability, and security—without fail—to mitigate these risks and fully leverage mobility. Wi-Fi needs to become "carrier grade."

Although a majority of the Wi-Fi device shipments today are made up of smart phones, tablets, e-readers, and laptops, there is a growing trend of Wi-Fi becoming the sole access technology for several application-specific devices, including:

- Home – security cameras, set-top-boxes, media players, thermostats, etc.
- Hospitals – patient monitors, infusion pumps, oxygen monitoring devices, etc.
- Industry – machine diagnostics, sensors, smart grids, etc.

For most of these devices, good Wi-Fi connectivity is critical to their functioning and the QoE delivered to the end user.

Each critical component of the dynamic WLAN ecosystem must be tested, assessed, and optimized throughout the product or service lifecycle:

- Enterprise and service provider access points (APs)
- WLAN controllers
- Wi-Fi-enabled client devices (laptops, smartphones, printers, scanners, healthcare monitors, etc.)
- Live deployed WLANs and future upgrades

Equipment manufacturers, service providers, and users alike need actionable insight into performance if they are to thrive in today's highly competitive market.

This means validating:

- Functionality
- Interoperability
- Performance
- QoE
- Scalability

Assessments should begin by obtaining baseline performance measurements and then progress to load testing to simulate realistic live network environments. The quality of the user experience should be measured in metrics relevant to each individual application—voice, data, video, etc.—in the presence of diverse client and traffic mixes.

IXIA SOLUTION

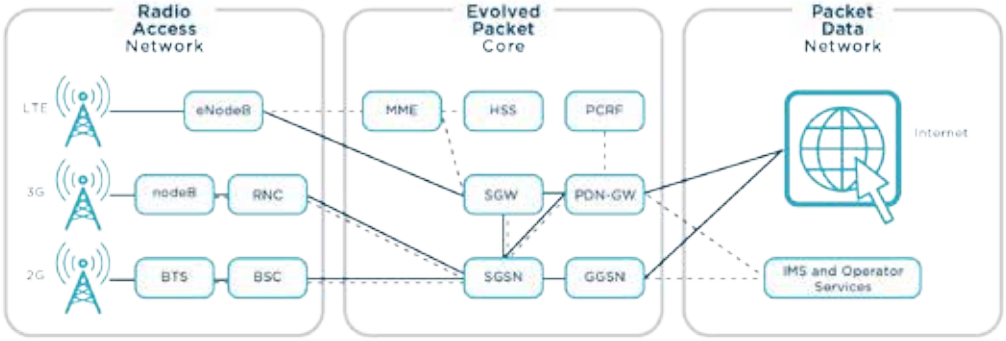
The industry's premier Wi-Fi test solution, Ixia's IxVeriWave represents the gold standard in evaluating Wi-Fi performance and site readiness. The world's leading WLAN infrastructure and mobile device manufacturers, service providers, system integrators, and enterprises use IxVeriWave to measure and optimize performance, reliability, and scalability throughout the product/service lifecycle.

Employing a client-centric, user-focused model, IxVeriWave delivers:

- Proactive problem resolution by using integrated capture and extensions to rapidly identify and isolate issues
- Automation that enables the creation of thousands of test cases while speeding test cycles and reducing cost
- World-leading L1–7 802.11ac testing backed by Ixia's 11 years of experience in Wi-Fi Test and Measurement
- Ability to generate thousands of clients and traffic flows used to test specific features, such as QoS, power save, and roaming
- Test-grade repeatability, so you get the same result each time you run the test by eliminating the variability due to clients and environment
- Testing with hundreds of clients without need of hundreds of laptops using IxVeriWave's support for 500 clients per port
- High performance of 1.7 Gbps per port, so clients can achieve full theoretical rate

SUGGESTED APPLICATIONS	
IxVeriWave	Test and validate Wi-Fi performance of WLAN networks by recreating real-world scenarios
SUGGESTED CHASSIS	
IxVeriWave Chassis	Nine-slot or two-slot chassis
SUGGESTED LOAD MODULES	
Golden Client Load Modules	L2–7 and L1–7 RF WaveBlades
SISO Simulation Load Modules	WBW3604, WBW1604N
DFS and Interference Simulation Load Modules	WBW1604N

IxVeriWave



SCENARIO

LTE technology continues to rise, and 5G mobile trials are starting. With subscriber numbers and network traffic from smartphones and media-rich applications exploding worldwide, evolving LTE and 5G deployments present mobile operators and infrastructure equipment providers with complex new challenges as they transition from 2G and 3G networks.

Faced with rampant change, mobile service and equipment providers must be fully confident in the performance, scalability, security, mobility, and interoperability of their products and services. Most failures occur at high scale or under extreme conditions, and the risks of rolling out devices, networks, and services without conducting comprehensive testing beforehand are tremendous.

Vendors and network operators need an efficient means of prototyping live networks in the lab on a metro/city scale to validate performance under load. End-to-end, pre-deployment service validation should closely model the services the live network will carry using real application traffic and measuring user QoE.

Proactively stressing networks and components in the lab prior to live deployment ensures the optimal user experience:

- Increased capacity requirements in both the access (base stations) and core networks
- Improved performance requirements—throughput, lower latency, etc.—for increasing video traffic and data-hungry applications
- Higher QoE expectations among customers—voice quality and video quality
- New business models and tiered rate plans that maximize revenue
- Security threats increasing in number and complexity

With many networks involving equipment from multiple vendors, specific configurations and traffic mixes must be modeled in order to benchmark scalability, avoid bottlenecks, and ensure security. Lifecycle testing is required to:

- Evaluate scalability and breaking points of individual devices and configurations
- Optimize network design and system test in the lab
- Debug problems occurring on the deployed network
- Streamline change as new devices, firmware upgrades, and other changes are introduced

Optimizing for the Long-Term

In deploying modern LTE access networks, optimizing the performance of evolved node B (eNodeB) base stations and "small cell" low-power access points is essential.

In the evolved packet core (EPC), operators must cope with dramatic spikes in signaling traffic that can overwhelm infrastructures and increase the risk of network outages and billing errors.

Mobile network operators and infrastructure equipment manufacturers will continue to invest hundreds of millions each year to deliver and deploy scalable, resilient LTE infrastructures. To ensure the success of new products and services, they must first validate based on guaranteed quality. In addition, they must validate the ability to support and deliver converged voice, data, and video services.

Ixia's breakthrough wireless test solutions and deep wireless expertise help vendors and mobile operators develop and implement best practices for existing and emerging wireless technologies in the most cost-effective and efficient manner.

IXIA SOLUTIONS

Ixia provides the industry's most comprehensive wireless test portfolio, encompassing both deep functional testing and high-scale capacity and performance testing across multiple technology generations. Equipment manufacturers and mobile operators rely on Ixia's solutions to comprehensively fulfill their wireless testing needs. Our industry-leading test capabilities cover wireless access and wireless core, including the 3G packet core, 3G circuit switched core, 3G radio access network, LTE access, LTE evolved packet core, IMS, and Signalizing System 7 (SS7)/ public switched telephone network (PSTN) interconnect.

Ixia's wireless solutions are best of breed for:

- Complete end-to-end testing from the wireless edge to the Internet core
- Traffic and subscriber scalability and capacity planning
- Real-world subscriber modeling
- Quality of experience measurements
- Multi-UE emulation
- VoLTE testing

IXIA DEVICE EMULATIONS	
DUT	**Emulated Nodes**
eNode B	UE, eNode B, MME, SGW
MME	HSS, eNode B, SGW, MME
SGW	MME, eNode B, PDN-GW
PDN-GW	SGW, PCRF, SGW, IP Core
Network	UE, IP Core

SUGGESTED APPLICATIONS	
IxLoad/IxLoad VE	Test end-to-end performance of wireless LTE networks and components with emulation of multiplay services
BreakingPoint/ BreakingPoint VE	Control global threat intelligence at Internet-scale to create massive high-fidelity simulation and testing conditions for battle-testing infrastructures, devices, applications, and people
SUGGESTED LOAD MODULES	
PerfectStorm	Application traffic and security attacks at 960 Gbps with the load of 720 million concurrent wired and wireless users from a single 11U chassis
PerfectStorm ONE	Enterprise-ready portable appliance for 10/1GE real-world, high-stress testing with up to 80Gbps of application traffic
XAir2	Industry's highest UE density and feature-rich testing platform, providing unparalleled LTE performance in the smallest footprint
SUGGESTED CHASSIS	
XGS12 Chassis	Industry's highest 100/40/10GE port densities in 11RU vertical rack space, reducing space requirements and simplifying management
XGS2 Chassis	Two-slot ultra–high–performance 3RU chassis

IxLoad

BreakingPoint

PerfectStorm

PerfectStorm ONE

XAir2

XGS12

XGS2

Support

ixia

IXIA GLOBAL SUPPORT

We understand that you must deliver higher-quality, higher-performing products and services to market faster than ever before. Ixia's global support team is committed to helping you successfully achieve these Increasingly demanding business requirements.

Key benefits and services we provide as part of your active Ixia product support include:

- Get best-practices advice and quick resolution of product issues by accessing our technology and product experts in global support centers strategically located across APAC, EMEA, and North America through whatever method best suits your team—via phone, e-mail, or online
- Gain direct hands-on assistance and local-language support through field support teams in many regions
- Obtain proactive assistance with your team's ramp up on new Ixia products and features
- Maximize the capability and productivity of your Ixia products to test new scenarios
- Reduce risk to your critical projects and time to market through fast, expert support and managed escalation processes to ensure responsive issue resolution
- Access expert automation advice and script debugging assistance for your engineers
- Protect your Ixia test system investment and minimize downtime with full-service hardware repair (RMA) and rapid on-site interchange of field-replaceable hardware modules
- Maximize the return on your Ixia solutions investment through access to the latest software releases with all new features, enhancements, and patches
- Access full support materials online at any time to find answers and solutions in our extensive knowledge base, download the latest software releases, manage licensing, and access the latest product documentation and release notes
- Upgrade to higher levels of support with our premium support service, which offers many additional benefits that include expedited hardware repair, increased access and proactive support, customized support plans, and quarterly reporting

The global support team is your advocate within Ixia and key to getting the most from your Ixia investment. They work seamlessly with your Ixia field sales managers, system engineers, and all other Ixia teams to ensure that you get what you need when you need it to be successful.

ENRICHING YOUR TEST-SOLUTION EXPERIENCE

Service providers and enterprises frequently require additional expertise to properly evaluate the performance and interoperability of the multi-vendor devices and systems that make up their networks.

Although critical to successful launches, testing is often downplayed and frequently back-ended in project plans. Even when testing needs are accommodated, sufficient priority is often not given to test automation and full integration of testing into the service delivery lifecycle process. When proper testing is overlooked, performance and QoS suffer. Test automation and integration into a service delivery lifecycle are key to ensuring quality, performance, and efficient time to market.

The Ixia professional services team of highly experienced testing experts is here to help you achieve the optimal testing solution for your unique requirements. We understand that fast results will drive project success. From project management, best-practice recommendations, and training to full testing and automation services, we have a robust set of service options that you can combine or use independently.

COMPREHENSIVE INTEGRATED TEST SOLUTIONS

- **Project management** – An experienced Ixia project manager manages your test effort from start to finish. All aspects of a proper QA process—test plan development, personnel and equipment allocation, test development, automation, regression, and reporting—are actively monitored and documented.
- **Test process optimization** – Solutions targeted to your specific test needs help you get the most out of your Ixia test equipment and applications. We help you focus on what, when, and where to test and include trend analysis.
- **Test automation** – Enables you to perform cost-effective, efficient, and repeatable lifecycle testing that enables you to deliver top-quality products. Automation speeds testing from days to hours. Automation also helps you meet shipping and deployment deadlines.
- **Strategic placement** – Testing is integrated into service delivery release lifecycle.

INDUSTRY-LEADING TESTING RESIDENT EXPERTISE

- **Testing solution experts** – With your resources at a premium, Ixia can provide you with critical access to trained experts to assist on urgent and late product development testing, customer PoCs, real-world solution demonstrations, and test lab setup, development, and ongoing maturation.
- **Jumpstart training** – Provides personalized, on-site training. We take two days to introduce your team to Ixia products, followed by three days focusing on using Ixia products for your testing requirements. You will receive specific use examples that can be replicated for future projects.

TESTING AS A SERVICE (TAAS)

- Provides efficient, robust, and cost-effective testing services to your organization
- Packages industry standard test plans, reports, and methodologies that can be applied to various aspects of an infrastructures' lifecycle
- Addresses the needs of QA labs and IT departments, as well as pre-and post-production networks and systems for service providers, enterprises, and NEMs
- Bundles solutions (hardware, software, and services) to leverage our testing expertise along with our best-of-market testing products

CYBER SECURITY TAAS

Ixia Cyber Range training has been developed with an emphasis on real-world operations and self-enabling your security team.

The objective is to instruct students on how to conduct offensive and defensive operations, taking into account personnel roles and responsibilities in a Cyber Range environment. Learning modules cover offensive operations, including attack and exploit vectors and target simulations; defensive operations from a network/security operations centers (NOC/SOC) perspective; and lab exercises.

Acronyms

ixia

ACRONYMS

ACRONYM	DEFINITION
AAA	Authentication, Authorization, and Accounting
ACI	Application Centric Infrastructure
ADAS	Advanced Driver Assistance Systems
AFM	Advanced Feature Module
ALG	Application Layer Fateway
ANCP	Access Node Control Protocol
AP	Access Point
APAC	Asia Pacific
API	Application Program Interface
APM	Application Performance Monitor
ATI	Application and Threat Intelligence
ATIP	Application and Threat Intelligence Processor
ATM	Asynchronous Transfer Mode
BaseT	Baseband Twisted Pair
BERT	Bit Error Rate Testing
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BNG	Broadband Network Gateway
BRAS	Broadband Remote Access Server
BRAS	Broadband Remote Access Server
BSC	Base Station Controller
BTS	Base Transceiver Station
CAPEX	Capital Expenditure
CDN	Content Delivery Network
CE	Customer Edge
CFM	Connectivity Fault Management
CFP	Complementary Feedback Pair
CLI	Command Line Interface
CPE	Customer Premises Equipment
CPU	Central Processing Unit
CXP	Copper connector for higher-speed Ethernet
DCB	Data Center Bridging
DCBX	Data Center Bridging Capability Exchange Protocol
DDoS	distributed denial of service
DHCP	Dynamic Host Configuration Protocol
DHCPv4	Dynamic Host Configuration Protocol version 4
DLP	Data Loss Prevention
DNS	Domain Name System
DoS	Denial of Service
DPI	Deep Packet Inspection
DRM	Digital Rights Management

ACRONYM	DEFINITION
DS	Disc Storage
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
DS Lite	Dual-Stack Lite
DUT	Device Under Test
E1	European Basic Multiplex Rate (30 voice channels; 2.048 Mbps)
EAPOL	Extensible Authentication Protocol Over Local Area Network
EDA	Electronic Document Access
E-LAN	Ethernet transparent local area network
E-Line	Ethernet private line
E-LMI	Ethernet Local Management Interface
EMEA	Europe Middle East Africa
EMS	Element Management System
EP	Extended Protocol
EPC	Evolved Packet Core
EPL	Ethernet Private Line
ERSPAN	Encapsulated Remote SPAN
ESXi	VMware hypervisor
EVPL	Ethernet Virtual Private Line (data service)
FC	Fibre Channel
FCF	Fibre Channel Forwarder (ethernet switch)
FCoE	Fibre Channel over Ethernet
FEC	Forward Error Correction/ forwarding equivalency classes
FIP	Fibre Channel over Ethernet (FCOE) Initialization Protocol
FTP	File Transfer Protocol
Gbps	Gigabits per second
GE	Gigabit Ethernet
GGSN	Gateway GPRS (General Packet Radio Service) Service Node
GPT	General Purpose Timer
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
HA	High Availability
HSS	High-Speed Serial
HTTP	Hypertext Transfer Protocol (world wide web protocol)
I/O	Input/Output
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Gateway Message Protocol

ACRONYM	DEFINITION
IKE	Internet Key Exchange
IMS	IP Multimedia Subsystem
IOS	Internet Operating System
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Security Protocol
IPTV	Internet Protocol Television
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPv6ov4	Internet Protocol verion 6 over version 4
iSCSI	Internet Small Computer Systems Interface
ISDN	Integrated Services Digital Network
ISFP-GR	Intelligent Small-Form-Factor Pluggable Module
ISIS	Intermediate System to Intermediate System
IT	Information Technology
ITU-T	International Telecommuniaction Union Telecommunications Standard
J1	Japanese System at 1.54 Megabits/second (24 channels)
KVM	Kernel Virtual Machine
L	Layer
L2CP	Layer 2 Control Protocol
L2MP	Layer 2 Multilink Protocol
L2TPv2	Layer 2 Tunneling Protocol v2
L4-7	Layer 4–7
LAC	L2TP Access Concentrator
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDP	Label Distribution Protocol
LSP	Label Switched Path
LSP-Ping	Label Switched Path Ping
MAC	Media Access Control
MbE	Multi-Bit Error or Multi-byte Extension
MDI	Medium Dependent Interface
MEF	Metro Ethernet Forum
MGCP	Media Gateway Control Protocol
MHz	Mega Hertz
MIMO	Multiple Input Multiple Output
MLD	Multicast Listener Discovery Protocol
mLDP	Multicast Label Distribution Protocol

ACRONYM	DEFINITION
MLPPP	Multi-Link Point-To-Point Protocol
MME	Mobility Management Entity (3GPP)
MMRP	Multiple Multicast Registration Protocol
MOS	Mean Opinion Score
MPLS	Multi-Protocol Label Switching
MPLS-TP	Multiprotocol Label Switching-transport profile
MSTP	Multiple Spanning Tree Protocol
MVRP	Multicast VLAN Registration Protocol
NAC	Network Access Control
NAT	Network Address Translation
NDP	Neighbor Discovery Protocol
NEM	Network Equipment Manufacturer
NFV	Network Functions Virtualization
NGFW	Next-Generation Firewal
NGN	Next-Generation Network
NNTP	Network News Transfer Protocol (RFC 977)
NPB	Network Packet Broker
NPM	Network Performance Monitor
NSX	VMware's network virtualization platform
NTO	Net Tool Optimizer
OAM	Operations Administration and Maintenance (ethernet protocol)
OPEX	Operational Expenditure
OSPF	Open Shortest Path First
OSS	Operation Support System
OTT	Over the Top
P	Provider
P2P	Peer-to-Peer
PBB	Provider Backbone Bridge
PBB-TE	Provider Backbone Bridge Traffic Engineering
PC	Personal Computer
PCM	Pulse Code Modulation
PCRF	Policy and Charging Rules Function
PDN-GW	Public Data Network Gateway
PE	Provider Edge
PIM	Protocol Independent Multicast
PIM-BSR	Protocol Independent Multicast Base Station Repeater
PMTU	Path Maximum Transmission Unit
PoC	Proof of Concept
PON OLT	Passive Optical Network Optical Line Termination

ACRONYM	DEFINITION
POP	Point of Presence
POS	Packet over SONET
PPP	Point-to-Point Protocol
PPPoA	Point-to-Point Protocol over ATM
PPPoE	Point-to-Point Protocol over Ethernet
PPPoEoA	Point-to-Point Protocol over Ethernet over ATM
PPPoX	Point-to-Point Protocol over X (anything)
PPPv4	Point-to-Point Protocol version 4
PSTN	Public Switched Telephone Network
PWE3	Pseudo-Wire Emulation Edge to Edge
QA	Quality Assurance
QinQ	Queue in Queue
QoE	Quality of Experience
QoS	Quality of Service
QSFP	Quad Small Form-Facotor Pluggable
RADIUS	Remote Authentication Dial-In User Service
REST	Representational State Transfer
RFC	Request for Comment
RIP	Routing Information Protocol
RIP/NG	Routing Information Protocol Next Generation
RIPng	Routing Information Protocol Next Generation
RMA	Random Multiple Access
RMON	Remote Network Monitoring
RNC	Radio Network Controller
RSTP	Rapid Spanning Tree Protocol
RSVP	Resource Reservation Protocol-Traffic Engineering
RSVP-TE	Resource Reservation Protocol-Traffic Engineering
RTCP	Real-Time Control Protocol
RTP	Real-Time Transport Protocol (digital switched telephony)
RU	Rack Unit
SAN	Storage Area Network
SAP	Session Announcement Protocol
SBC	Session Border Controller
SCCP	Skinny Client Control Protocol
SD	Standard Definition
SDN	Software Defined Networking
SFP	Small Form-factor Pluggable (optical transceiver module)
SGSN	Serving GPRS (General Packet Radio Service) Service Node

ACRONYM	DEFINITION
SGW	Signaling Gateway or Security Gateway (IPSec)
SIGTRAN	Signaling Transport
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SoC	System on a Chip
SONET	Synchronous Optical Networking
SPAN	Switch Port Analyzer
SQL	Search and Query Language
SR	Send and Receive
SRTP	Secure Real-Time Transport Protocol
SS7	Signaling System 7
SSL	Secure Socket Layer
SSM	Security Services Module
STP	Spanning Tree Protocol
SUT	System Under Test
T1	T-carrier 1 (digital transmission line, 1.544 Mbps, 24 voice channels)
TAAS	Testing as a Service
TCP	Transport Control Protocol
TLS	Transport Layer Security
U	Unit of measurement for rackmount equipment (U is 1.75in or 4.44cm)
UC	Unified Communications
UDP	User Datagram Protocol
UE	User Experience
UI	User Interface
UNI	User Network Interface
UTM	Unified Threat Management
VCCV	Virtual Circuit Connectivity Verification
VE	Virtual Edition
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNF	Virtualized Network Function
VoD	Video on Demand
VoIP	Voice over Internet Protocol
vPB	Virtual Packet Broker
VPLS	Virtual Private LAN Segment
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WLAN	Wireless Local Area Network
WM	Windows Mobile

WE MAKE APPLICATIONS
STRONGER

ixia

For more information please contact:

AVIZENT
Network Solutions

Official Partner

Avizent Network Solutions | +44 7858 929 008 info@avizent.com | www.avizent.com