The New Intelligent Network

Building a Smarter, Simpler Architecture
## Table of Contents

- What Does It Take to Create a Secure, High-Performance Architecture? . 4
- Optimizing and Defending Next-Generation Networks .......................... 4
- Designing a Scalable, Unified and Self-Healing Infrastructure ............. 5
- Gaining Network Cohesion and Coherence ....................................... 6
- Warning the Tools of Impending Threats ....................................... 6
- The Role of Automation in the New Ecosystem: Heartbeat Packets and Load Balancing Enable Robust Security and Network Health .......................................................... 7
- The Heartbeat of a Healthy Network—Intelligent Packets That Anticipate Network Bursts and Tool Failure ........................................... 7
- Load Balancing: Cost-Effective Relief for Oversubscription of Inline Monitoring Devices ................................................................. 8
- Inline Load Balancing Offers Unique Opportunities .......................... 8
- A Vision for the Network Ahead ...................................................... 9
Building a Smarter, Simpler Architecture: How Converged Access and Application Intelligence Let You Handle Complex Network Needs for Visibility, Protection and Productivity

Customers around the world frequently describe to me their visions of the arriving IT environment—an ecosystem that’s open, flexible, scalable and robust; that lets companies enhance their application intelligence, fortify security, and seize fast-arising business opportunities.

However, people also share their concerns about increasing network growth and complexity. Companies are virtualizing rapidly and consolidating their data centers, which leads to spiraling throughput. Much of this growth in throughput is due to higher virtual machine densities on physical servers and the momentum of 10G Ethernet adoption. Additionally, IT is being consumerized by smartphones and tablets; the workforce is increasingly mobile, and applications grow richer by the day. All of these factors combine to drive traffic through the network at a breathtaking rate—and the impact of all these trends on the larger organization is profound.

What Does It Take to Create a Secure, High-Performance Architecture?

The emerging network ecosystem has its own unique set of needs. For one, it demands substantially more robust and intelligent security. In addition, it needs instantaneous and automated problem resolution if it is not to fall victim to its own size and success.

Predictably, the stakes keep rising with network size and complexity. Amid competition quick to exploit vulnerability, any menace to efficiency translates into a company-wide business issue. So it is vital that an organization protect its network against burgeoning threats, maintain highest availability and respond quickly to such issues as unplanned traffic bursts and tool errors or failure.

As Bob Laliberte states in an influential essay, “...today’s networks are fraught with granular security requirements, layers of segmentation, bursty communication protocols, and latency-sensitive applications. To address network performance, security, and operations needs, large organizations are implementing an assortment of management tools to improve network monitoring and centralize command-and-control.” Risks to the network include:

- **Data interception** by an unauthorized third party who could deploy it to harmful purposes.
- **Availability challenges** as companies and networks grow to span global geographies; lost connectivity or data availability can cause business interruption and revenue loss.
- **Intrusion** at a weak access or entry point can make valuable data vulnerable to intruders and open the way to viruses and Trojan horses.

Optimizing and Defending Next-Generation Networks

When Bob Laliberte speaks in his essay of the Intelligent Management Aggregation Network—or IMAN—he points out something that I have been asserting for a long time,
namely that visibility is the key to achieving higher levels of security and reliability in a next-generation network. As he states, “… [organizations] will need more comprehensive network visibility to help them address new network management, operations, and security requirements. This in turn will drive the IMAN into the networking market mainstream.”

How can we help to bring about such total visibility for a company? I believe that as customers build ultra high-security, high-performance architectures, the need increases for communication between the access architecture and the diverse and complex security tools they have implemented. Only with such intelligent communication can a network’s tools fulfill their respective purposes and keep the network running up to customer expectations.

Access is a major visibility engine. Its whole purpose is to show information intelligently and in context. Information without context would be chaotic and useless, but accurate information about the state of the network—where and what are the potential issues—is vital to resolving those issues promptly and fully.

**Designing a Scalable, Unified and Self-Healing Infrastructure**

A next-generation network ecosystem needs high scalability and availability, along with ultra-high performance and the ability to locate, diagnose and resolve problems through intelligent analysis. Scalability addresses quality of service (QoS), which should never downgrade, even when a load expands multiple times—for example, when the number of users or transactions per user skyrockets. A system must be able to maintain its Service Level Agreements (SLA) and handle traffic smoothly in order to support the company’s larger business goals and competitiveness.

That network also needs to be extremely solid and fault-tolerant, offering constant monitoring and high network intelligence for accurate decision-making. The more automated, the better it can conduct reliable, effective failure recovery and management.

To address the many looming, persistent threats multiple tools have grown up alongside the network fabric, each with its own specific purpose. These tools are so integral to the network that they actually help to drive and define it. Tools constantly face new urgencies and must evolve to stay ahead of the fast-arising threats to network security and availability. They are familiar to us as firewalls, proxy servers, encryption capabilities, logical security, access controls, anti-virus software, and auditing systems such as log management. Many of these tools are major capital investments for a company, running into half a million dollars. To recap briefly those tools I’m referring to here:

- **Firewalls**, usually residing between the private local network and the internet, enabling traffic flowing through it to be authenticated, monitored, logged, and reported. These firewalls in particular, given today’s data avalanche, are at risk of becoming oversubscribed and losing their effectiveness. (Palo Alto Networks delivers a truly unique, next-generation firewall that provides policy-based visibility. It also classifies traffic by accurately identifying the application—rather than just port/protocol information, as well as providing graphical visualization of applications on the network with an unprecedented level of detail.)

- **Inline security devices** are increasingly essential to 10 Gigabit network links carrying critical business applications and data, voice, and video traffic. These include Intrusion
Prevention Systems (IPSs), Data Loss Prevention (DLP) devices, Web Application Firewalls (WAFs), Database Activity Monitors (DAMs), and Application Performance Management (APM) tools. Adding to the pressure, these tools are growing more complex and demanding of processing power.

- **Encryption** converts readable text into indecipherable ciphertext, negating the encrypted text’s usefulness to an unauthorized viewer. Decryption restores ciphertext to usefulness.
- **Proxy servers** hide the true address of a client workstation and can also serve as a firewall which enforces authentication and acts as a middleman for user requests.
- **Antivirus software** such as McAfee and Symantec systems locate and dispose of malicious content.
- **Logical security** includes software safeguards such as user ID and password access, authentication, access rights and authority levels.
- **Auditing systems** track and record what happens over an organization's network.
- **Log management solutions** centrally collect audit trails for analysis and forensics. They track, record, and identify and index unauthorized users trying to access the network for a valuable audit trail of those activities.

**Gaining Network Cohesion and Coherence**

Until very recently, network architects thought of the network in terms of separate segments—core, cloud, remote sites. This was a viewpoint born of budgets, accountability and technology, and it shaped the network infrastructure. Each tool typically operated independently, performed a unique function, and targeted a particular position or segment of the network.

In a next-generation ecosystem, however, I foresee all of those tools functioning together intelligently as a cohesive entity, irrespective of their various vendor origins—McAfee, NetScout, CA, Cisco, Oracle, and so forth. We are building Net Optics’ high-visibility monitoring access offerings in such a way that they can serve as the common interface and control point to weave that solution together.

**Warning the Tools of Impending Threats**

In a secure, next-generation architecture, the access function needs the ability to communicate with the security tools. Access and tools should operate seamlessly in tandem to protect the network and avoid not only attacks but unplanned traffic bursts, tool errors or failure.

Today’s IT teams still spend far too much time in reactive mode, a sub-optimal if not downright risky situation. The ability to discover and resolve potential issues proactively, before they can damage the network, is essential. Extensive, state-of-the-art monitoring and instrumentation capabilities are important elements of tomorrow’s networking platform. We must arm our IT staff with uncompromising, total visibility into system health, device performance, and operational status of the network. For maximum tool effectiveness, we must provide those tools with timely, intelligent insight on what the network traffic consists of, where is it going, and to whom. In a next-generation platform, this process delivers the ability to anticipate the type and flow of arriving traffic in order to warn tools pre-emptively of trouble on the way.

The process of determining the nature of traffic that is traveling to each tool improves
Increasingly, automation plays a major role in keeping the network healthy.

As I discussed in my previous eBook, The Secret to Surviving the Network Deluge, lack of visibility in a complex system puts the entire infrastructure at risk. Failure or inability to intervene quickly, accurately and effectively in a deteriorating situation can lead to cascading consequences, as deceptively minor issues rapidly escalate to system-wide catastrophe.

Historically, management tools are connected to networks via SPAN/mirror ports or external Taps but this approach may not offer needed scalability. This is where the Intelligent Management Aggregation Network comes in. You may have seen it referred to as a matrix switch or Traffic Visibility Network (TVN). The IMAN—rather than the tools themselves—makes that connection into network equipment via the SPAN/mirror ports or network taps. The IMAN proceeds to capture network behavior and feeds the data to the tools.

In my opinion, this concept is going to be the wave of the future as traffic expands. The approach gives the network the robust scalability and total visibility it needs to handle emerging security and functionality challenges. This is the solution that I first spoke of at the beginning of this discussion: that “golden” connectivity and communication of access architecture and security tools. Only with such intelligent communication can the tools perform optimally and keep the network in good health.

The Role of Automation in the New Ecosystem: Heartbeat Packets and Load Balancing Enable Robust Security and Network Health

Increasingly, automation plays a major role in keeping the network healthy. When we can automate our awareness of potential tool failure or degradation—and the earlier the better—then human error and system vulnerability are far easier to counteract. The whole network becomes a dimension safer. Automation enables continuous improvement as each outage and potential issue is diagnosed and a record of proactive avoidance steps is set down by engineers to speed resolution going forward.

The Heartbeat of a Healthy Network—Intelligent Packets That Anticipate Network Bursts and Tool Failure

The Intelligent Packet or “iPacket” is an elegant, simple and ingenious way to ensure awareness of network status and health. The iPacket’s early warning system greatly enhances the effectiveness of network security—enabling immediate intervention to avert an impact on QoS or availability. The operation of these packets between devices is instrumental in building the single-system intelligent network architecture that we need for handling future traffic loads.

Configurable iPackets, such as those in our Net Optics iBypass HD™ Switch, speed in both directions through critical tools to monitor the health of the tool. Should a tool fail or become oversubscribed, iBypass HD can respond with a choice of fail-open or fail-closed behavior. Fail-open condition allows traffic to flow directly across the network link, bypass...
the down tool, and ensure continued application availability. Fail-closed status downs the network ports—blocking traffic flow and enabling attached switches and routers to take corrective action, keeping applications available by rerouting traffic through another path. Using link fault detection and iPacket checking, a bypass switch can detect the following types of failures:

- **Power supply failure** on the IPS
- A **bad cable** between the bypass switch and the IPS
- **Accidental disconnection** of a cable between the bypass switch and the IPS during system maintenance, for example
- **IPS software** not functioning or functioning too slowly due to high traffic loads, etc
- **IPS hardware** failure

Additionally, the iBypass can even start to engage other network security tools once it realizes that the current set will probably be unable to keep up with the growth and increase in traffic. This amounts to intelligent action of the tools to reposition themselves.

Load Balancing: Cost-Effective Relief for Oversubscription of Inline Monitoring Devices

Equipment failure is not, of course, the only threat to the optimal contribution of monitoring and security tools. Oversubscription, another major concern, causes critical tools to underperform, dropping packets and missing messages. Skyrocketing traffic and high-speed 10-Gbps links place severe pressure on performance analyzers, IPSs and other tools that inspect traffic to block data leaks and malware. Load balancing not only prevents oversubscription, it also delivers the best value from 1G tool investments by leveraging them on 10G links.

Security tool performance relies on the complexity of the security rule base. A security device with a long, complicated rule base does not perform at as high a level as one with a limited policy; in other words, there is a trade-off between security and performance. Net Optics’ suite of load balancing options actually allows customers to shift an entire network’s load of traffic from a primary network to a standby back-up if an issue arises. Load balancing across multiple security, performance and lawful intercept tools offers intelligent assurance that all tools can keep up with the traffic they receive.

Inline Load Balancing Offers Unique Opportunities

Organizations rely on inline tools not only to prevent attacks but to prevent information loss and achieve regulatory compliance. In the case of an out-of-band tool becoming oversubscribed, it’s a fairly straightforward task to replicate a tool and load-balance the affected traffic. However, load balancing of inline tools raises the stakes and presents unique challenges, since these can interfere with network traffic—or even bring down a business-critical link.

Because they deal with bidirectional traffic flows, conventional monitoring load balancers may not be able to meet inline load balancing requirements. To address this need, Net Optics developed xBalancer™—purpose-built for inline load balancing. xBalancer stands out among other load-balancing approaches for a number of capabilities, including its linear scalability and cost-effectiveness. xBalancer enables replication of existing tools, with traffic load-balanced so that tools operate in parallel. This scheme enables two
tools to perform twice the work; three tools to perform three times the work, and so forth. Scaling is linear, making the solution ideally cost-effective amid doubling and even quadrupling traffic volumes.

A Vision for the Network Ahead

If a network lags in security or responsiveness under growing pressures or falls short of the ability to self-diagnose and heal; if it becomes too complex and demands extensive, time-consuming, disruptive and costly upgrades in order to scale—then it becomes a negative weight, slowing a company’s ability to seize new opportunities and grow.

The software in such a situation can consume operational time, cause slowdowns and other headaches, and become an obstacle to change. Because the network is so fundamental to the success of the enterprise, I envision ongoing gains in manageability and security, along with deployment of new monitoring capabilities that can scale and upgrade smoothly, to simplify operations. Such a network frees up users across the enterprise to work confidently and securely at their core tasks and goals.

The new network architecture must be automatically capable of anticipating type and flow of traffic and warning IT teams of looming threats and failures—intelligently determining which traffic is to be sent to which tools—those that are ready and able to handle all bandwidth and traffic patterns. The best approach going forward is for every aspect of the network to interoperate coherently and intelligently, no matter what their proprietary origin. I believe Net Optics is capable of creating that unifying and enabling architecture, allowing tools to contribute their full value and return on investment.

Notes

2. Ibid.

About the Author

Bob Shaw, President and CEO, Net Optics, Inc.

As President and Chief Executive Officer of Net Optics since 2001, Bob Shaw is responsible for conceiving and implementing corporate vision and strategy, positioning Net Optics as the leading provider of intelligent access and monitoring architecture solutions in both the physical and virtual environments. Under Shaw’s guidance, Net Optics has achieved consistent double-digit growth, launched more than 35 new products, acquired over 8000 customers, and expanded its global presence in over 81 countries. The company is included in the elite Inc. 5000 list of highest performing companies for the second year in a row and won 2011 Best of FOSE honors. In addition, Net Optics received the coveted 2011 Red Herring Top 100 North America and Top 100 Global Awards for promise and innovation, the 2011 Best Deployment Scenario Award for Network Visibility, and many other accolades. Shaw’s leadership experience spans startups to Fortune 200 organizations, where he held Senior Vice Presidential executive positions. Shaw earned both a Bachelor of Arts degree in Business and a Bachelor of Science degree in Economics from Geneva College in Pennsylvania.