Leveraging vSphere 5.0

For Optimal Visibility and Efficiency

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

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 to position Net Optics as the leading provider of intelligent access and monitoring architecture solutions in both 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 two years in a row; won 2011 Best of FOSE honors; received the coveted 2011 Red Herring Top 100 North America Award 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.

Leveraging vSphere 5.0 for Optimal Visibility and Efficiency

vSphere 5.0 is generating excitement throughout the industry as customers race to discover how this flagship solution best fits into their own environments. Now, Net Optics' Phantom™ Virtual Tap delivers intelligent strategies to ensure that customers gain the full security and performance advantages promised by VMware's important new resource.

For abundant reasons, vSphere 5.0 is being hailed across the industry as a major advance. We at Net Optics are particularly excited because this new resource closely fits our own agenda of driving virtualization adoption, making implementation substantially easier and more beneficial. As the new hypervisor core of VMware's Cloud Infrastructure Suite; vSphere 5.0 is up to four times more powerful than its predecessor, offering welcome enhancements such as the ability to handle virtual machines of up to 1TB of memory and 32 virtual CPUs processing one million IOPs/sec and 36Gb/sec of network traffic. We believe that over the next 12-18 months enterprise customers will migrate from previous versions of vSphere to version 5.0 as the new version proves itself in the field.

Net Optics' commitment to virtualization motivated us to develop solutions specifically tailored for VMware ESX. We innovated our Phantom Virtual Tap to align with VMware's virtualization architecture and ensure security in the new environment.

However, despite this positive momentum, every technology advance brings its own unique set of issues, and vSphere 5.0 is no exception. This may be an ideal time to place the product under deeper scrutiny. Sometimes, amid an avalanche of well-intentioned acclaim, relevant facts may be overlooked or concerns not resolved.

The good news is that by employing the Phantom Virtual Tap as a visibility resource—as opposed to relying on a SPAN-based approach—customers can realize the substantial security and performance benefits offered by VMware's new product, without risk. In the following pages, I discuss some specific concerns regarding visibility, efficiency, and other issues arising with vSphere 5.0 adoption and examine how they can be resolved.

Port Mirroring Raises Visibility Challenges

vSphere 5.0's built-in mirroring exposes SPAN's inherent visibility limitations

What is the ideal way to deliver on the substantial visibility promised by VMware's new solution? In my opinion, SPAN is not the optimal direction to take. Many of vSphere 5.0's enhancements were made to the VMware Distributed Switch (VDS), including NetFlow™ support and improvements in Port Mirroring (called Switch Port Analyzer or SPAN on Cisco switches).

Once a port mirroring session is configured with a destination—a virtual machine, a vmknic or an uplink port—the distributed switch copies packets to the destination. SPAN's port mirroring function lets a network send a copy of the packets seen on a switch port to a monitoring device connected to another switch port. In VMware vSphere 5.0, a distributed switch provides a similar port mirroring capability to that available on a physical network switch. So far so good.

SPAN remains highly controversial. One engineer, who has deep knowledge of, and experience with virtualization, including many company-wide implementations, puts it bluntly: "To achieve port mirroring by using SPAN, you might have to sacrifice thirty to fifty percent of your available bandwidth." The limitations of SPAN are familiar to Net Optics customers, who generally avoid it for the following reasons:

- A SPAN port provides an unfiltered view of traffic traversing one or multiple ports on a virtual switch. That port sees only what the switch is processing—while small packet errors or oversubscription on a monitored port remain invisible. *(figure 1)*
- An avalanche of SPAN traffic is not consumable in a meaningful way. Capturing and forwarding all data requires a termination point that can "accept" that data, understand it, organize it and make sense of it. Capturing 100 percent of the data and sending it on requires a filtering capability as well as an instrumentation layer tool to process data and act on it.
- SPAN reduces virtual switch capacity by up to 50 percent: Because switch capacity is limited, whatever traffic is being mirrored reduces production throughput.

Only the Phantom Virtual Tap offers continuous monitoring through vMotion. SPAN ports must work independently of the machine layer or context. Therefore, they cannot offer the machine context that Phantom Tap is able to do through its tight integration with vCenter.

Solving SPAN Degradation Issues with Phantom Virtual Tap

The solution to these concerns about SPAN lies in using Net Optics Phantom Virtual Tap to augment the VMware Virtual Switch, VMware Distributed Switch or the Cisco Nexus 1000v switch. Customers can choose from three meaningful ways to accomplish this:

- Passive packet capture performed at the kernel layer—below the switch—neatly eliminates the chronic throughput degradation that is an inescapable side effect of using SPAN

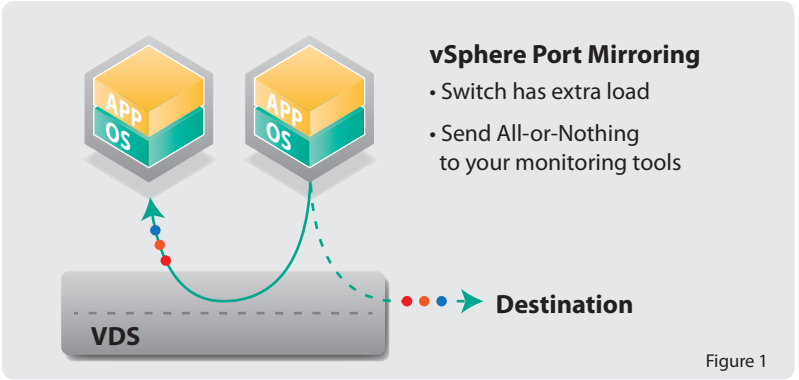


Figure 1

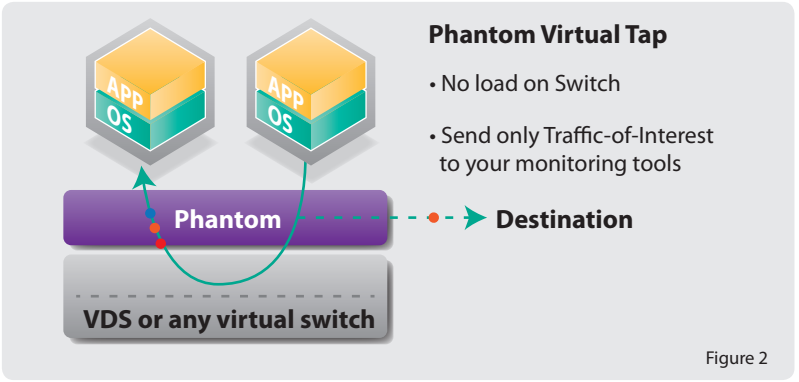


Figure 2

- Phantom Virtual Tap's monitoring policy lets you capture only traffic of interest. After all, why monitor back-up traffic? *(figure 2)*
- Sophisticated tunneling support allows captured traffic to reach the right tool or destination at 10 Gbps—optimizing network and tool utilization

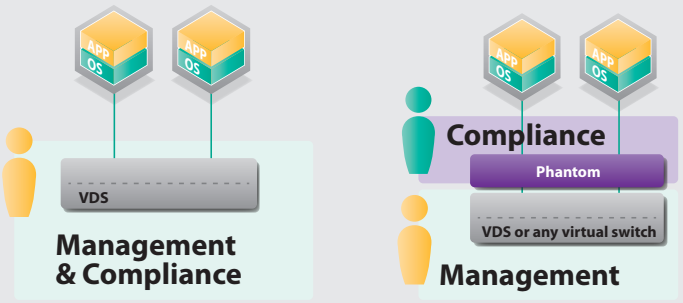
The Net Optics Phantom Virtual Tap has earned widespread industry recognition, including 2011 Best of FOSE, as a breakthrough virtualization enabler that bridges and unites physical and virtual environments. The hypervisor-specific Phantom Virtual Tap brings unrivaled total visibility of inter-VM traffic to VMware ESX and ESXi environments without interfering with traffic. It's the first solution that offers the much-needed ability to send traffic to both physical and virtual tools, which saves customers the cost of deploying separate virtual tools. By delivering 100 percent visibility of inter-VM traffic passing between virtual servers, the Tap reveals previously invisible traffic to support customer security, regulatory compliance, and manageability needs. Compatibility with best-of-breed hypervisors and virtual switches lets companies find and resolve security breaches before they can affect the data center.

SPAN Ports and Separation of Duties—Inherent Conflicts?

When it comes to mirroring and Separation of Duties (SOD), any virtual environment presents an inherent conflict. Because security governance, management and operations differ widely, their respective processes must be rigorously segregated to avoid potential conflicts of interest. Privileged user monitoring focuses on scrutinizing, analyzing and reporting the activities of users with high levels of access to the data—and why let a privileged user manage the very system created to monitor him or her at all?

Therefore, it's only sensible to be able to identify and sometimes block privileged user access to confidential and private data. This is done by modifying applications, schema or table structure, or by creating/modifying user accounts or permissions.

But in the case of SPAN, this port mirroring does indeed conflict with underlying SOD precepts. A SPAN port does not separate different types of traffic (or machines) and may thus present data that is consumed by a mix of resources in a corporation.



SOD Failure: Learning the Hard Way

The potential damage caused by SOD failure can't be overstated: Earlier this year, at a U.S. subsidiary of a Japanese pharmaceutical company, a disgruntled ex-IT administrator wrought havoc with the computer infrastructure, taking down 88 virtual servers, including the company's email and Blackberry servers, order tracking system, and financial management software. The perpetrator's attack accessed the Internet via Wi-Fi at a local McDonald's restaurant, logging into a vSphere management console that he had secretly set up before leaving the company. The security breach cost a pretty penny as the company was unable to ship products, cut checks, or access email. The hacker also gained unauthorized access to the company's network from his home Internet connection using administrative passwords he possessed as an employee. Naturally, losses were severe.

Figure 3

The Added Cost of Monitoring
Implementing monitoring on multiple ESX servers
using VMware vSphere 5.0 standard pricing as a baseline

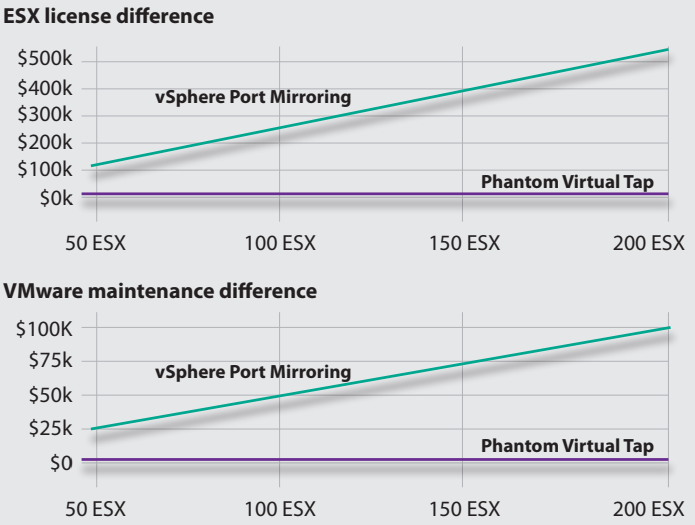


Figure 4

Sticker Shock: the True Cost of SPAN Port Configuration:

From an engineering standpoint, configuring VMware vSphere 5.0's port mirroring (SPAN) function is complex and available only to the highest "Enterprise Plus" echelon of VMware customers, which automatically excludes a significant number of users. Several issues affect the overall cost of the monitoring solution: first, a significant price increase in the VMware licensing required to install the additional licenses that enable port mirroring; and second, configuring the port mirroring deployment itself. *(figure 4)*

One configuration scenario calls for using a SPAN port and additional hardware in a complex manipulation of the original packet VLAN ID. The other involves multiplexing vSphere 5.0's server network traffic and SPAN traffic in order to separate that traffic from the normal network flows. This approach reduces throughput and requires adding yet more switches into the mix. By contrast, the Phantom Virtual Tap can simply send traffic of interest directly to the correct instrumentation layer tool. Other cost advantages of Phantom are due to smart filtering at the ESX (hence no waste of bandwidth transporting traffic of no interest) and its support of all flavors of vSwitches including Cisco's Nexus 1000v.

Multiple Phantom licensing and maintenance fees are less expensive than VMware's, while offering more benefits and capabilities to reduce the overall solution cost significantly and provide added value.

Partnering with VMware to Answer Virtualization Challenges

Net Optics is deeply committed to supporting VMware's goals, and to helping customers gain the full benefit of vSphere 5.0 in expediting and easing virtualization adoption. Requiring no changes and creating no single point of failure, the Phantom Tap fully supports vSphere 5.0. Providing the high capacity needed to match port density and traffic volumes and integrating kernel-level monitoring into the heart of the hypervisor switching system, the Phantom Virtual Tap enables advanced monitoring and access control in dynamic and distributed virtual environments. Most importantly, the Phantom Virtual Tap delivers the unrivaled visibility needed by virtual networks and exposes all inter-VM traffic passing between virtual servers. This helps ensure vSphere 5.0's acceptance and provides customers the ability to achieve security, regulatory compliance, and manageability.

Smart Strategies for Your Future with vSphere 5.0 and the Phantom Virtual Tap

It's a sure bet that vSphere 5.0 is going to play a major role in the business and technology environment to come. Much as in the physical switching world, dedicated access layer solutions offer significant benefits in comparison to switching layer devices. For these and many more reasons, the Phantom Virtual Tap is now vital to reinforcing vSphere 5.0's security capabilities, allowing you to see 100 percent of your virtual data on VMware ESX & ESXi. For more information, visit the Phantom Virtual Tap online at www.netoptics.com or call (408) 737-7777.

Net Optics, Inc.

5303 Betsy Ross Drive
Santa Clara, CA 95054

(408) 737-7777

twitter.com/netoptics

www.netoptics.com