Managing Virtualized Networks

This technical guide examines what the ideal on-premises network management system would look like and examines managed network monitoring and management services as options.
Finding the Right Management and Monitoring Tools

The days of being able to touch the network edge are over. It no longer lives in a box at the top of the rack. Instead, it’s inside the server, and as enterprises have embraced server virtualization, the network edge has extended into the hypervisor. For a while, network managers were happy to let this go. The early embedded virtual switches lacked a lot of functionality and virtualized environments were fairly static. You could hand the server teams a bunch of IP addresses and VLANs to play with and forget about it.

With virtual infrastructure becoming dynamic, network managers can’t be idle anymore. Virtual machines are mobile. Clouds are rolling in. Those static environments are ancient history. Network managers have a choice to make. They can continue to abdicate the virtualized edge to systems and virtualization teams, or they can reassert control and do what they do best.

The virtual network can’t remain invisible to the network manager. IT departments need management and monitoring technologies that help them respond to changes in the virtual network. As virtual and cloud infrastructures become more dynamic, IT also needs to adopt new network technologies like virtual overlay networks and software-defined networking that make network infrastructure more dynamic and automated.

This technical guide on managing virtual networks offers you a roadmap to reclaim control over the virtualized edge of your data center network. This guide addresses how to integrate the management of virtual and physical networks, both through technology and organizational change.

Shamus McGillicuddy
Director of news and features, TechTarget’s Networking Media Group
Five Steps to Integrate and Manage Virtual Networks

Nearly 60% of organizations have noted a slow-down in their virtualization initiatives, according to a new Nemertes Research study. The complexity of systems—specifically the complexity of network configurations—are often cited as a key barrier to the continued adoption of virtualization. The ability for enterprises to virtualize their network configurations and to fully define these configurations in software is the key to boosting virtualization adoption again. As your organization’s network virtualization effort goes forward, here are some tips that should help you maximize to tie those efforts into server and storage virtualization.

Tip 1: Evaluate your organizational structure and optimize your network policies and procedures

Advancements in storage, server and network virtualization have allowed enterprises to do things in the data center that simply weren’t possible on a physical network. Yet the separation in many organizations between IT and network teams hasn’t enabled them to reap the full rewards of these new capabilities. Many network teams view virtualization as the responsibility of the server team and are not in a hurry to embrace virtualized switches or virtual network appliances. Many are still happy to have traffic come out of the virtual infrastructure, route it through physical network components, and then go back into virtual space. IT organizations should make sure that the roles, responsibilities, policies and procedures of these teams are clarified and revised to embrace virtualization’s capabilities. It’s only a matter of time before virtualization takes hold in networking the way it has with servers and storage, so resistance is futile.
Tip 2: Consider your monitoring tools and your management framework
Traditional monitoring tools and management frameworks have struggled to keep up with the adoption of server virtualization. Network virtualization will only add to these challenges. Now is an excellent time to re-evaluate your monitoring tools and management framework. Using virtualization as a catalyst, consider how you can create an integrated “single pane of glass” view of servers and virtualized network infrastructure that can and will be sharing physical host resources with other workloads, moving from place to place, or spread across internal data centers and public/private clouds.

Tip 3: Embrace open standards whenever possible
Cisco and VMware are clearly leading in the market share battle for data center virtualization, virtual switching and programmable networks, and they will likely have significant market positions in SDNs. Both have vowed to support open standards like OpenFlow and OpenStack. Yet their current solutions and product roadmaps don’t necessarily enforce these standards. Enterprises would do well to consider whether any purchase decisions might lead them further down the path of being locked into a proprietary solution. Both of these vendors will be quick to point out all of the advanced features and capabilities their proprietary solutions can deliver. Don’t take the bait. Opt instead for an open standards approach that won’t limit your options. As a side benefit, embracing open standards should simplify the transition of applications to or from cloud environments.

Tip 4: Start evaluating and planning for software-defined networking (SDN)
Software-defined networking (SDN) is the next major trend in enterprise IT. The adoption of SDN will balloon over the next three years. SDN supports network virtualization, but organizations are struggling to assess the roles of SDN and other network virtualization techniques in their current network roadmaps. Your best approach is to try out both to see which solution or combination of solutions is best suited to your environment and would yield the greatest cost savings and increased agility.
Enterprises that embrace network virtualization and use it to push their overall adoption of virtualization will see the greatest return on their investment. To ensure success, however, IT may need to re-think both its traditional organizational structure and enterprise system management tooling capabilities. Organizations can further protect their virtualization investments by embracing open standards whenever possible. Finally, determine now how software-defined networks can increase your agility and reduce deployment challenges and costs. —Henry Svendblad
Network Traffic Analysis in a Virtualized Environment

Over the years, network administrators have come up with tried-and-true methods for analyzing and troubleshooting the physical network, using SNMP and NetFlow for data collection or protocol analyzers to look at raw network frames and packets. But what happens now that we’ve moved into the era of virtual networks? The good news is that existing network traffic analysis strategies can be used in virtual networks with just a few small differences.

Virtual networks work very much the same as physical networks. In many cases, only the names of network devices have changed. For example:

- A network interface card (NIC) is now a “virtual NIC” (vNIC).
- A switch is now a “virtual switch” (vSwitch). vSwitches work very similarly to physical switches but don’t have the config ability commonly found in traditional switches (such as showing the MAC addresses).
- Multiple vSwitches can be created on each host, and ports on a vSwitch are usually broken down into port groups for specific purposes, such as production or management.
- VLANs are fully supported, and a switch port can be either an access port or a trunk port, just like the in world of physical switches.
- Physical hosts that house the virtual switches are connected to the physical network with real physical server NICs and cables, which are called “up-links” in a virtual infrastructure.
- Features like promiscuous mode, NIC teaming and load balancing all exist in a virtual environment.
These features have changed:

- **Spanning-tree protocol** is not needed.
- Network traffic cannot flow from one switch to another on the same host.
- Port groups exist in the virtual network but not in the physical network (they may be similar to **Cisco SmartPort**).
- You can’t see the virtual switches or physical cables connecting to the vNICS (and there are no more flashing lights to look at in the wiring closet for most of the servers).

**VIRTUAL NETWORK TRAFFIC ANALYSIS USING SNMP AND NETFLOW**

Just as in the physical network infrastructure, to **analyze network traffic** in the virtual world you’ll use SNMP or NetFlow to collect data across multiple points of the infrastructure and then analyze it with a network performance management and monitoring tool. Examples of more general network performance monitoring tools include **What’s Up Gold** and **Solarwinds Orion**. More specific NetFlow collectors and analyzers include **Plixer Scrutinizer** and **Solarwinds NetFlow Traffic Analyzer**.

Of course you can still do a generic **Internet Control Message Protocol (ICMP) monitoring** with an element manager like HP OpenView, but it’s preferable to do that in addition to some level of utilization and error checking.

Prior to vSphere5, utilizing NetFlow to monitor the virtual infrastructure was not an option. However, once you **implement vSphere 5** (assuming you have the edition with the vSphere Distributed Switch) you can enable NetFlow v5 at the port-group level on an individual dvPort or on an uplink.

By doing so, you’ll be able to monitor the following:

- IntRA-host virtual machine traffic (virtual machine-to-virtual machine traffic on the same host)
- IntER-host virtual machine traffic (virtual machine-to-virtual machine traffic on different hosts)
- Virtual machine-to-physical infrastructure traffic
While SNMP will only give you basic statistics about the network traffic sent, traffic received and errors, NetFlow goes much further by providing IP pairings and protocols. In other words, you can see who the “top talkers” are and who is talking to whom. For example, with SNMP you might see that a network interface has reached its throughput capacity, but that’s all. With NetFlow, you would see that HTTP is taking up 95% of the interface utilization, and that a specific user’s PC (looked up by DNS) is talking to an Internet website that streams rock concerts, for example. None of these options will show you inside the packets or allow you to decode any data. In this blog, you’ll find more detailed information on [VMware’s vSphere 5 NetFlow implementation](#).

One of the best vSphere network performance monitoring and troubleshooting tools is [Xangati for vSphere (which is free) and the Xangati management dashboard](#). Both versions use NetFlow to collect data about the virtual infrastructure but combine it with other traditional performance metrics from vCenter to provide a very powerful performance monitoring and troubleshooting tool for vSphere infrastructures. The free version monitors a single host, while the management dashboard allows you to monitor many hosts and virtual networks from a single interface.

Note that if you are using Hyper-V instead of vSphere, Microsoft has announced that in Windows Server 2012 Hyper-V, the extensible virtual switch will support the addition of the open source Hyper-V sFlow agent that could then be monitored by sFlow collectors, such as the [InMon sFlowTrend Tool](#).

**VIRTUAL NETWORK TRAFFIC ANALYSIS WITH PACKET DECODE**

What if you want to do a packet decode from the virtual network? In order to do [Deep Packet Inspection](#) on a physical network, you would connect your protocol analyzer (which would be running on a laptop, for example) to a switch port and then configure SPAN (or RSPAN if the traffic is on a different switch) to mirror traffic from a single switch port, multiple ports or an entire VLAN.

Now that most of our data centers’ servers are virtualized, much of the
traffic does not even hit the physical network—so the traditional packet capture method is only useful in certain instances, such as analyzing your Internet connection or a connection to an iSCSI SAN.

Prior to vSphere 5, to use a protocol analyzer on the virtual infrastructure you took a VM running a protocol analyzer, created a new port group, configured it for promiscuous mode (so that all packets are sent to all ports), and then moved the VM that you wanted to analyze to that port group (for security reasons you don’t want to enable promiscuous mode on a production port group). For details on that, see my post titled “Using a Network Packet Analyzer on a VMware vSphere Virtual Network” (which you would follow if you are still using vSphere 4.x or if you have vSphere 5 but don’t have the distributed virtual switch running).

In the vSphere 5 Enterprise Plus, however, the port-mirroring functionality allows you to quickly and easily mirror any dvPort to another port, or you can choose a VLAN to encapsulate these mirrored packets by selecting the “Encapsulations VLAN” box when configuring distributed virtual switch port mirroring.

Once enabled, port mirroring provides visibility into:
- IntRA-host virtual machine traffic (virtual machine-to-virtual machine traffic on the same host)
- IntER-host virtual machine traffic (virtual machine-to-virtual machine traffic on different hosts)

If you are a Hyper-V user, note that in Hyper-V 3 port mirroring is a new feature of the extensible switch.

Analyzing and troubleshooting the network once your servers are virtualized really isn’t that different from performing these same tasks with physical servers in the physical network. You have two different paths to get this done depending on the level of detail you need. Using NetFlow is the best choice for high-level traffic analysis and bottleneck identification, where port mirroring with a protocol analyzer is what you would do to perform deep-packet analysis in the virtual infrastructure. —David Davis
How to Gain Virtual Network Overlay Visibility

With VMware pushing software-defined data center, and with a host of network vendors developing technology around VXLAN network overlays, it’s likely the network virtualization standard will work its way out of the test labs and into production environments. Now network managers must find a way to monitor and troubleshoot VXLANs, but VXLAN monitoring and visibility tools don’t really exist yet. So in the meantime, network pros will have to adapt existing strategies for VXLAN environments.

Virtual Extensible LAN (VXLAN), which was introduced last year by Cisco and VMware at VMworld (along with support from Arista, Brocade and Broadcom), is a Layer 3 encapsulation protocol that overcomes the limitations of virtual LANs (VLANS) in virtual environments and in multi-tenant networks. With VXLAN, engineers can spin up thousands more virtual networks that can stretch longer distances across data centers.

Last year, VXLAN gained the spotlight at VMWorld, with vendors launching a slew of third-party services such as load balancing and traffic QoS for virtual networks, but very little of this technology addressed the need for VXLAN monitoring and visibility.

THE VXLAN VISIBILITY CHALLENGE
VXLAN introduces the same visibility challenges as most encapsulation methods. Essentially, end-to-end traffic is hidden inside the tunnel, so you must be able to strip away the encapsulation for sustained monitoring and troubleshooting. This is crucial for viewing traffic traversing the backbone, or between data centers where VXLAN will most likely show up.
**VXLAN MONITORING TOOLS: WHAT’S AVAILABLE?**

Most network management vendors have yet to implement specific support for VXLAN, but there are a few options out there that can help today:

**FLOW ANALYSIS**

Riverbed’s Cascade team announced it would support the IPFIX records produced by VMware’s vSphere Distributed Virtual Switch (VDS), which provide intra-VXLAN flow details. This is the first flow-analysis vendor to step up to support VXLAN. Others may follow but will lag in availability. Also, we have yet to see other infrastructure vendors add support for the new IPFIX templates that will be important for checking VXLAN traffic outside of the virtual distributed switch. Additionally, in theory, sFlow supports VXLAN today, though vendors will need to build or extend an sFlow analysis tool to reveal the details therein.

**WIRESHARK AND DEEP TROUBLESHOOTING**

Wireshark already had VXLAN decodes in place, which were added in November 2011 and have been part of the mainline code since version 1.8.0. Other packet analysis tools can still be used but may not have a formalized decode yet. Check with your favorite vendor to find out for sure.

**PACKET-BASED MONITORING**

Looks like we are all out of luck here until the packet-inspection monitoring vendors add this. It won’t be difficult for them because they already support looking inside other tunneling protocols such as Generic Routing Encapsulation and GPRS Tunneling Protocol; this is just an adaption. Make sure you make a point of asking your tools vendor for this feature—they commonly prioritize enhancements based on customer requests.

**NETWORK MONITORING SWITCHES**

Some of these monitoring access devices can strip VLAN headers so that monitoring can proceed based on actual packet contents. Being able to strip
both VXLAN and VLAN headers would be especially useful for preconditioning traffic for analysis. None of the network monitoring switch providers has added VXLAN stripping yet, though several have told me that this is on their roadmaps.

**NCCM NEEDED FOR VXLAN ENVIRONMENTS**

Network managers will also need Network Change and Configuration Management (NCCM) to manage multivendor configuration of VXLANs. Today, this can only be defined or configured on an element-by-element basis outside of vSphere. While many NCCM vendors have stated plans to support VXLAN in the future, none currently offers much more than backup and restore services for device configurations that have already been set up using element management tools.

If VMware’s bets pay off and VXLAN becomes commonplace, you can bet that more support will be forthcoming among network management vendors. In the meantime, make the best of what you have and keep pressing your vendors to add VXLAN support if they don’t offer it today. —Jim Frey
HENRY SVENDBLAD is a principal research analyst with Nemertes Research, where he conducts both primary benchmark research and custom research, advises vendor and enterprise clients, writes thought-leadership reports, and delivers strategic seminars. A seasoned senior-level IT executive, Svendblad leads research on advanced carrier services with an emphasis on emerging trends, vendor management, business continuity/disaster recovery, security and cloud strategies.

DAVID DAVIS is the author of the VMware vSphere video training library from Train Signal. He has written hundreds of virtualization articles published on the Web, is a vExpert, VCP, VCAP-DCA, and CCIE #9369, with more than 18 years of enterprise IT experience. His personal website is VMwareVideos.com.

JIM FREY is managing research director at Enterprise Management Associates. Frey has 24 years of experience in the computing industry developing, deploying, managing and marketing software and hardware products, with the last 18 of those years spent in network management, straddling both enterprise and service provider sectors. At Enterprise Management Associates, Frey is responsible for the network management practice area.