

## C o m m u n i t i e s

All Communities ▾ [Blogs ▾](#)

Communities &gt; Blogs

## VMware Networking Blog

[Data Center of the Future](#) | [Main](#) | [Which NIC is my VM using?](#) | [Load Balancing Visibility with vSphere](#)

March 26, 2009

## Down and Dirty Network Troubleshooting Using Traces

The first time I saw a network trace, I was totally captivated. I was a young network systems programmer working on an IBM mainframe. The network operator had a Spectron Datascope that he could patch into any of the 9.6kbps links connecting the front end processor with the remote offices. My fascination remained, and I progressed from that datascope to using GTF traces and eventually wrote my own multi-tasking real-time trace analysis package in IBM System/370 assembler.

While this was a labor of love stemming from my complete fascination with the subject, I found trace analysis was the most useful tool in my network troubleshooting bag of tricks. Traces did not lie—they showed exactly what was or wasn't going on. Additionally, they gave me a more thorough understanding of network protocols.

Fast forward to today. We have more network tools, but networks have become a lot more complex and dispersed. Cisco and others have had port mirroring in many of their switches for a long time. SPAN or Switch Port Analyzer (as Cisco called the feature) enabled the network admin to selectively and non-disruptively replicate traffic from switch ports to another switch port connected to a protocol analyzer or a PC running Wireshark or similar. The SPAN capability eventually evolved to Remote SPAN (RSPAN) and Encapsulated RSPAN (ERSPAN). The latter enabling routing of GRE encapsulated SPAN traffic to any point in the network (given sufficient bandwidth, of course!).

## Tracing on a Virtual Switch

So what about virtual networks and virtual switches? How do you probe vswitch traffic? Fortunately, there is a simple and well-proven method for capturing traffic traversing a vswitch. The method involves setting up a guest VM (e.g. Windows, Linux) with Wireshark or other third party trace "sniffing" software. Simply:

- Create a new port group with Promiscuous Mode=Accept in the Port Security options.
- Set the VLAN to the VLAN ID you wish to trace, or set VLAN=4095 to trace traffic for all VLANs on that vswitch (assuming VST mode)

And there you have it. Start Wireshark in the VM and monitor through the Console.

## Forthcoming Options ...

With the Cisco Nexus 1000V with our forthcoming release, you will have another alternative. The Nexus 1000V supports SPAN and ERSPAN (see complete feature comparison [here](#)), so the network folks can use the same methods and techniques whether it be a virtual or physical network. The ERSPAN capability means you can redirect the trace traffic to any point without setting up a specialized sniffing VM on the host and vswitch in question.

Posted by Guy Brunsdon on March 26, 2009 | [Permalink](#) | [BOOKMARK](#)   

## TrackBack

TrackBack URL for this entry:

<http://www.typepad.com/services/trackback/6a00d8341c328153ef01156f612fc3970b>Listed below are links to weblogs that reference [Down and Dirty Network Troubleshooting Using Traces](#):

## Comments

 You can follow this conversation by subscribing to the [comment feed](#) for this post.



Hi,

very nice and useful post! Another great tool for troubleshooting is NetFlow, i've just posted a video tutorial about it at this link: <http://www.hunexr.com/2009/03/video-tutorial-netflow-your-ultimate-tool-for-traffic-visibility-in-your-v3-environment/>

## VMware Blogs

- [The Console \(VMware Mgmt\)](#)
- [VMTN Blog \(Technical News\)](#)
- [Developer Center Blog](#)
- [ESXi Chronicles](#)
- [Team Fusion](#)
- [Uptime \(Business Continuity\)](#)
- [VI Team Blog](#)
- [Virtualization for SAP Solutions](#)
- [VIXAPI Blog](#)
- [VMware Code Central Blog](#)
- [VMware Communities Blog](#)
- [VMware Knowledge Base Blog](#)
- [VMware Knowledge Base Weekly Digest](#)
- [VMware Networking Blog](#)
- [VMware PhD \(Education\)](#)
- [VMware Security Blog](#)
- [VMware Storage Blog](#)
- [VMware ThinApp Blog](#)
- [VMware vApp Developer Blog](#)
- [VMware: Virtual Reality](#)
- [VMware View Blog](#)
- [VMware View-Point](#)
- [VMware Virtual Disk Development Kit Blog](#)
- [VMware vSphere Blog](#)
- [VMworld Team](#)
- [VROOM \(Performance\)](#)
- [vSphere PowerCLI Blog](#)
- [Workstation Zealot](#)

## Recent Comments

- [creative recreation](#) on [F5 Accelerates Long Distance vMotion](#)
- [Ju](#) on [IPv6 and vSphere 4.1](#)
- [NAVEEN](#) on [vnic bandwidth? ... ignore what the guest VM tells you!](#)
- [Jaime](#) on [Jumbo Frames in vSphere 4.0](#)
- [Guy Brunsdon](#) on [VMware vSphere + Cisco Nexus 1000V bundles program extended in 2010](#)

## Categories

ms: http://myip.net/2009/03/27/2009-03-27-06:42:AM.html?utm\_source=feedburn&utm\_medium=email&utm\_campaign=feedburn

hope it can be useful as well.

Regards

---

Posted by: [Hany Michael](#) | [March 27, 2009 at 06:42 AM](#)



Thanks Hany. Great work on the video ...keep it coming!

Netflow v5 export is one of those little known options with ESX. Its main purpose is to provide an understanding of traffic flows within the network. The Cisco Nexus 1000V will enhance the capability to Netflow V5 and V9.

---

Posted by: [Guy Brunson](#) | [March 27, 2009 at 11:42 PM](#)



Guy, thank you for your comment on my humble video, I agree with you about NetFlow v5, and one of the main reasons why I'm very enthusiastic about the Cisco N1000v is the Netflow v9, I'm finally in the private beta and I look forward to testing this feature on it. I believe also the new vShield Zones from VMware will have some kind of traffic visibility based on NetFlow or sFlow if I'm not mistaken, I just watched the VMworld-Europe 2009 session and it looks promising.

Regards

---

Posted by: [Hany Michael](#) | [March 28, 2009 at 07:58 AM](#)

## Post a comment

If you have a TypeKey or TypePad account, please [Sign In](#).

Name:

Email Address: (Not displayed with comment.)

URL:

☐ Remember personal info?

Comments:

[Preview](#)

[Post](#)

### Archives

[August 2010](#)

[July 2010](#)

[June 2010](#)

[May 2010](#)

[April 2010](#)

[March 2010](#)

[February 2010](#)

[January 2010](#)

[December 2009](#)

[November 2009](#)

[Subscribe to this blog's feed](#)