



How to monitor network traffic inside an ESXi host

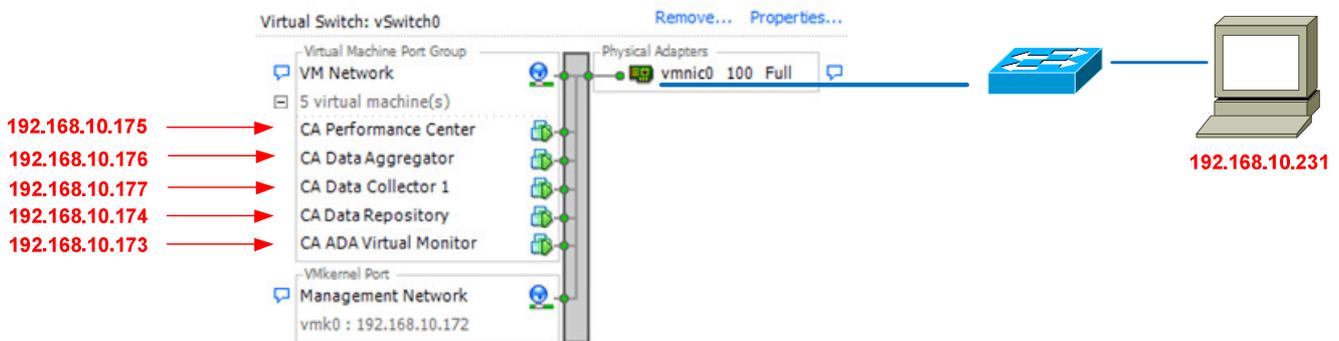
created by: Rainer Bemsel - Version 1.0 - Dated: Dec/30/2012

I've done several packet analyses on physical wired environment which was easy and pretty straight forward to set up. But with all virtualization efforts, you may need to analyze inside an ESX host. With a standard NIC and all connected virtual machines, it won't work. You will get packets captured from the initiator to the responder, but nothing more.

Let's have a look on my virtual machine, called "CA ADA Virtual Monitor", where I've installed Wireshark. When pinging from this host to 192.168.10.175, I was able to collect packets.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------------|----------------|----------------|----------|--------|---|
| 81 | 5.62135100 | 192.168.10.173 | 192.168.10.175 | ICMP | 74 | Echo (ping) request id=0x0200, seq=2304/9, ttl=128 |
| 82 | 5.62146100 | 192.168.10.175 | 192.168.10.173 | ICMP | 74 | Echo (ping) reply id=0x0200, seq=2304/9, ttl=64 |
| 104 | 6.61159800 | 192.168.10.173 | 192.168.10.175 | ICMP | 74 | Echo (ping) request id=0x0200, seq=2560/10, ttl=128 |
| 105 | 6.61172700 | 192.168.10.175 | 192.168.10.173 | ICMP | 74 | Echo (ping) reply id=0x0200, seq=2560/10, ttl=64 |
| 129 | 7.61157900 | 192.168.10.173 | 192.168.10.175 | ICMP | 74 | Echo (ping) request id=0x0200, seq=2816/11, ttl=128 |
| 130 | 7.61165700 | 192.168.10.175 | 192.168.10.173 | ICMP | 74 | Echo (ping) reply id=0x0200, seq=2816/11, ttl=64 |
| 148 | 8.61146400 | 192.168.10.173 | 192.168.10.175 | ICMP | 74 | Echo (ping) request id=0x0200, seq=3072/12, ttl=128 |
| 149 | 8.61156000 | 192.168.10.175 | 192.168.10.173 | ICMP | 74 | Echo (ping) reply id=0x0200, seq=3072/12, ttl=64 |

I also ping'd from 192.168.10.231 to 192.168.10.175 and from 192.168.10.174 to 192.168.10.175. Those packets were not seen in Wireshark.



Why is that so?

Network switches make use of forwarding tables to know what devices are connected on what network port. That traffic will only flow between those two network ports. Packet Analyzer won't see that traffic, unless the traffic is coming from them. In a physical environment you configure a set of ports to be mirrored to the port, where Wireshark attached Host is connected. This configuration makes copies from all traffic going from specific port(s) to a destination port. On my virtual host, I don't have a SPAN port.



DISCLAIMER

This Technical Tip or TechNote is provided as information only. I cannot make any guarantee, either explicit or implied, as to its accuracy to specific system installations / configurations. Readers should consult each Vendor for further information or support.

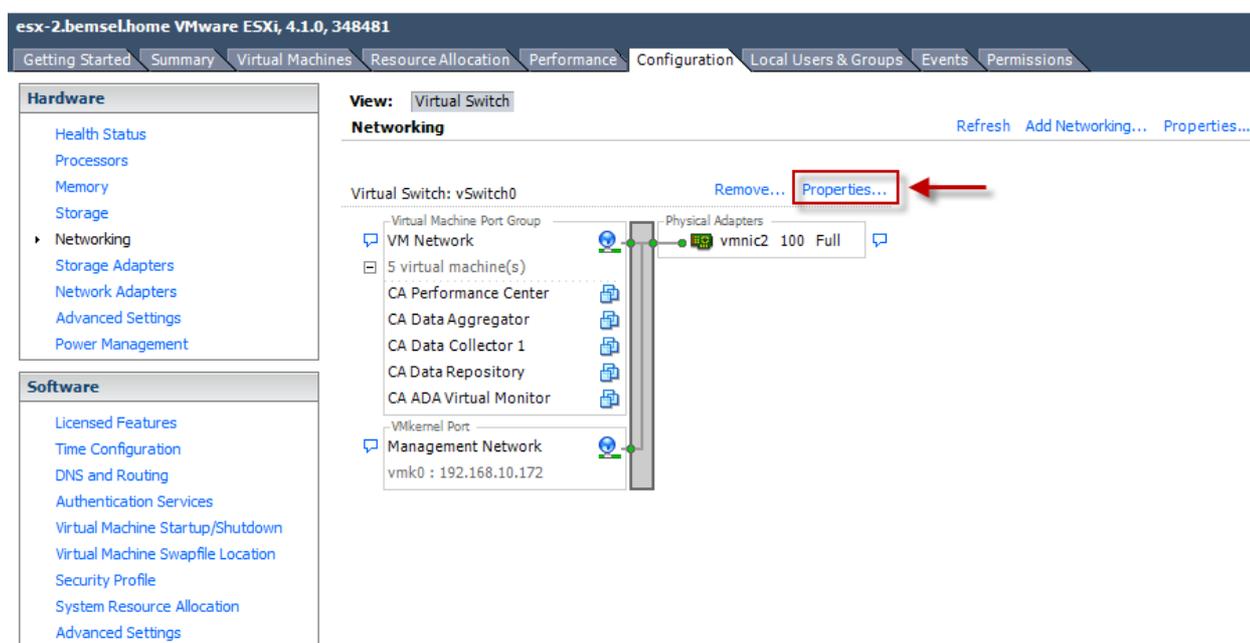
Although I believe the information provided in this document to be accurate at the time of writing, I reserve the right to modify, update, retract or otherwise change the information contained within for any reason and without notice. This technote has been created after studying the material and / or practical evaluation by myself. All liability for use of the information presented here remains with the user.

The use of any packet capture tool requires some network configuration on the VMware ESXi host. You must create a dedicated "Management" port group. You could also create a "Monitor" port group under which all your virtual machines will reside, although you may choose to use an existing port group. Promiscuous mode must be enabled for the "Monitor" (or previously existing) port group and disabled for the "Management" port group.

In the example below, vSwitch0 has a Management Network port group, as well as, an existing port group, VM Network, that acts as the "Monitor" port group.

To configure the vSwitch use the VMware vSphere Client

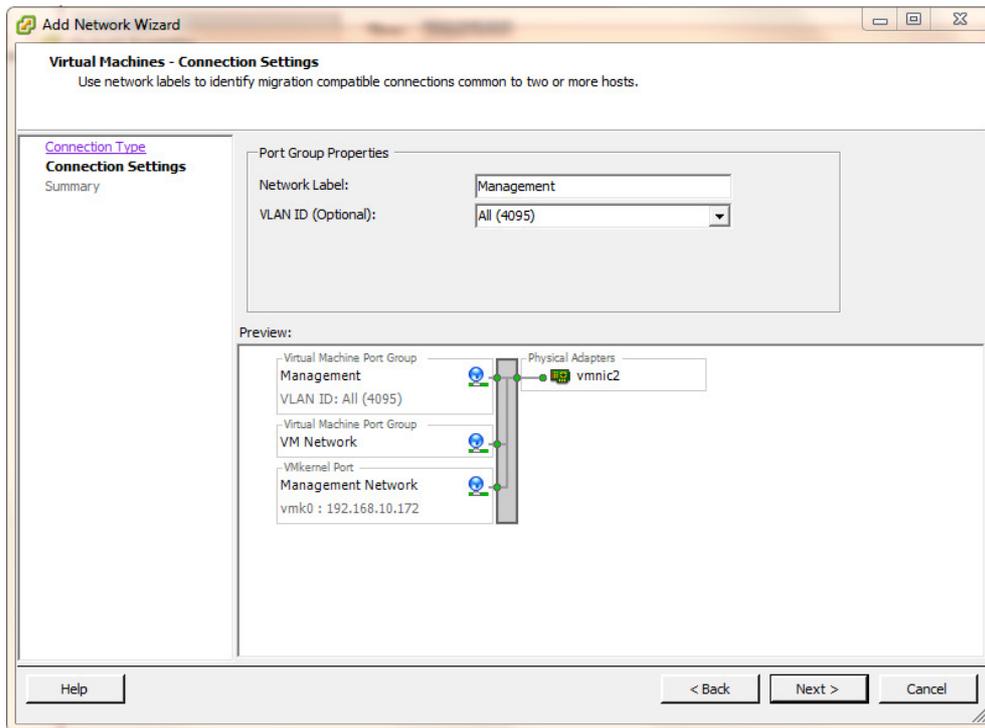
1. Select the Configuration tab for the ESXi Machine
2. Select Networking, located in the Hardware Panel
3. Determine which vSwitch does not host any application traffic that will be monitor by Packet Analyzer. Click on Properties



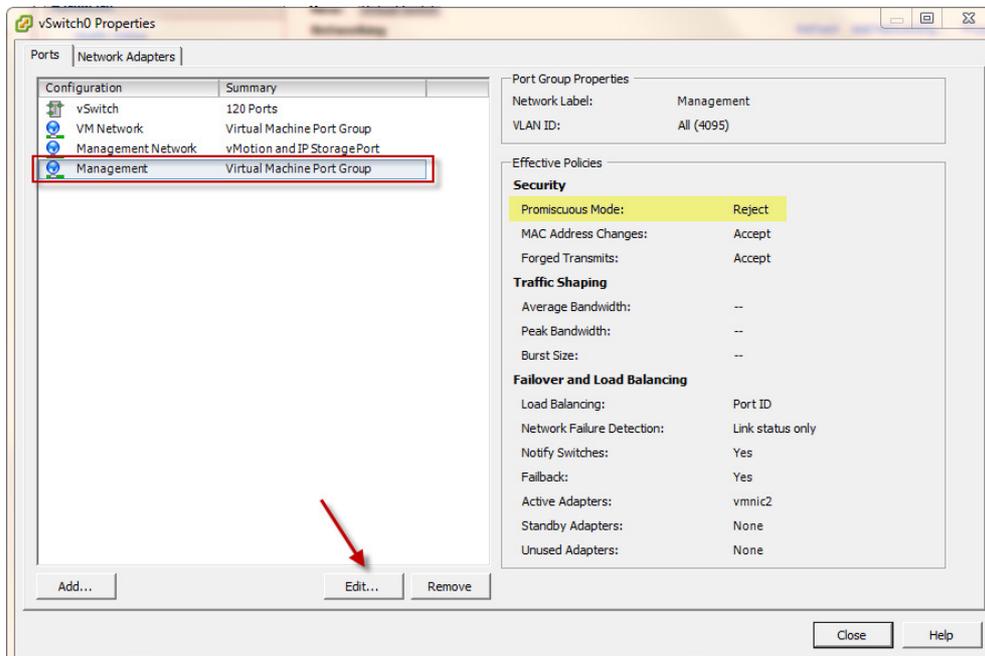
Note: If the ESX host only has one vSwitch connected to the physical network then both the Management and Monitor port groups will exist on the same vSwitch.

4. On the Port tab, click Add
5. Select Virtual Machine as the connection type.
6. Enter Management as the Network Label and select All (4095) for VLAN ID.

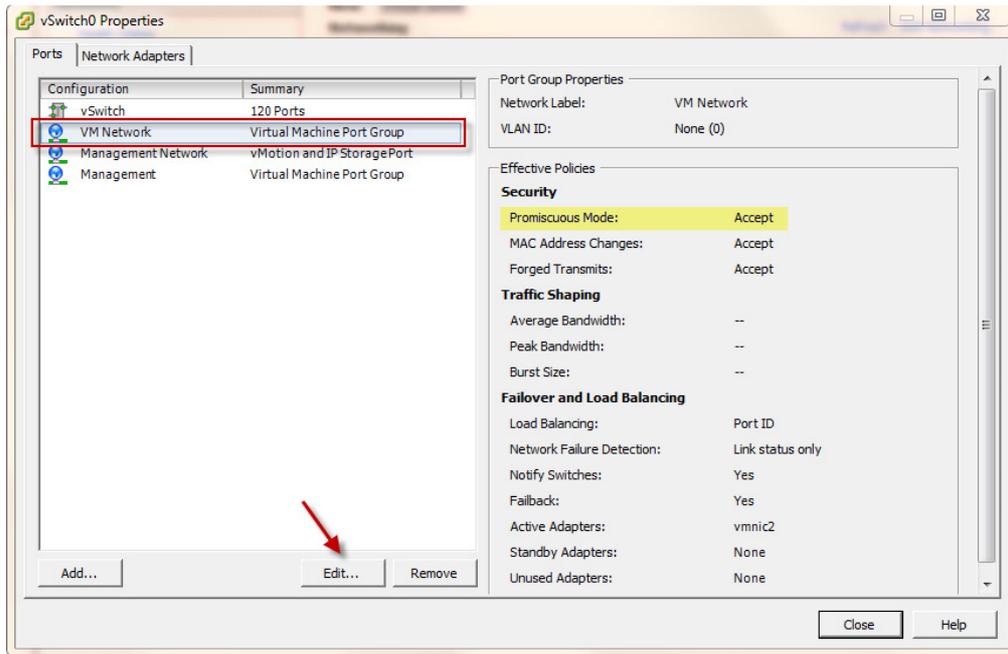
Note: You may choose to enter the specific VLAN ID that has the application traffic you wish to monitor



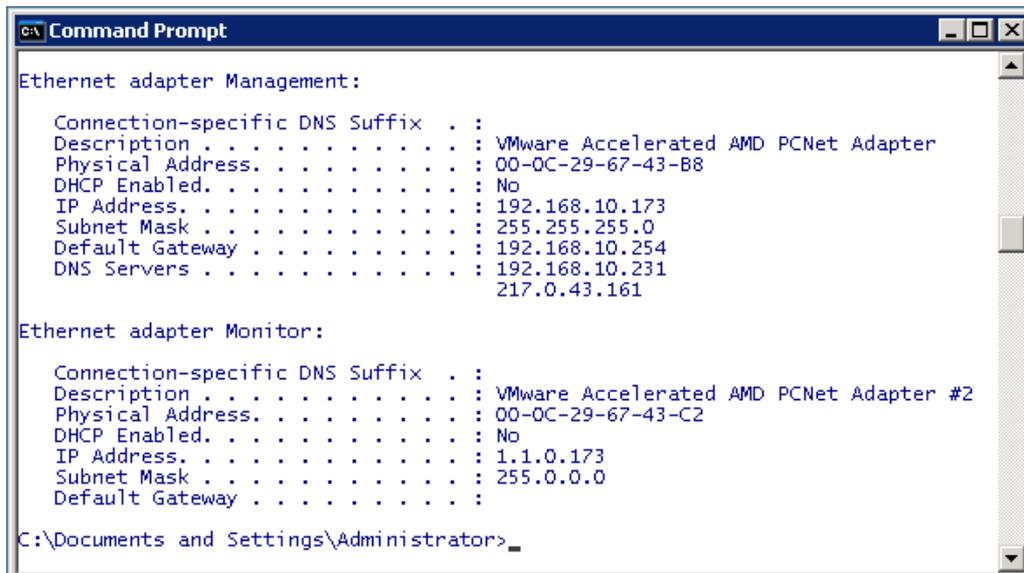
7. Click Next and Finish
8. Go back to Properties and select the newly created Management port group from the list in the Ports tab and click Edit



9. Click OK
10. Determine which Switch hosts the application traffic that will be monitor by Wireshark
11. Select the port group from the Ports tab and click on Edit.

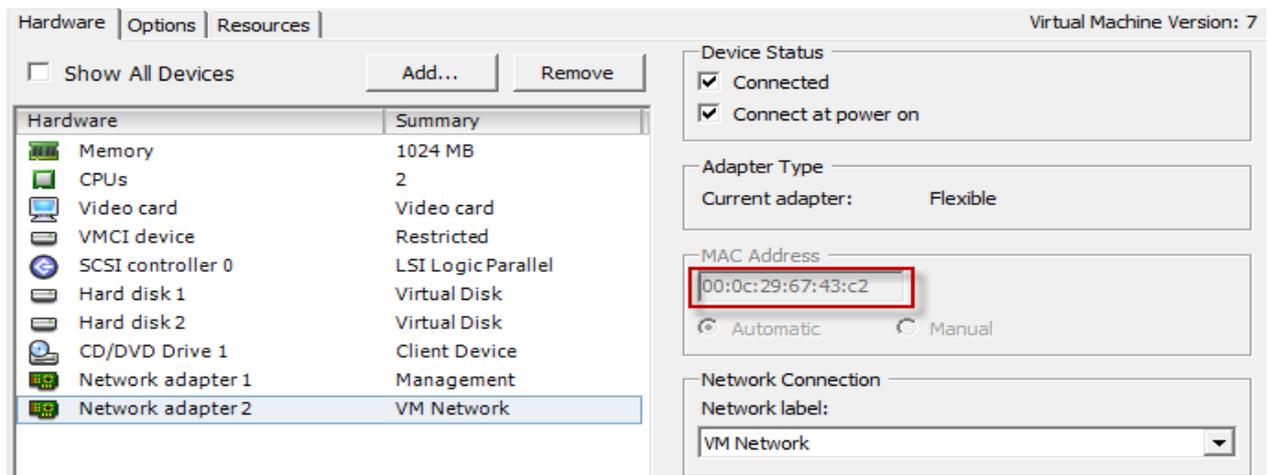
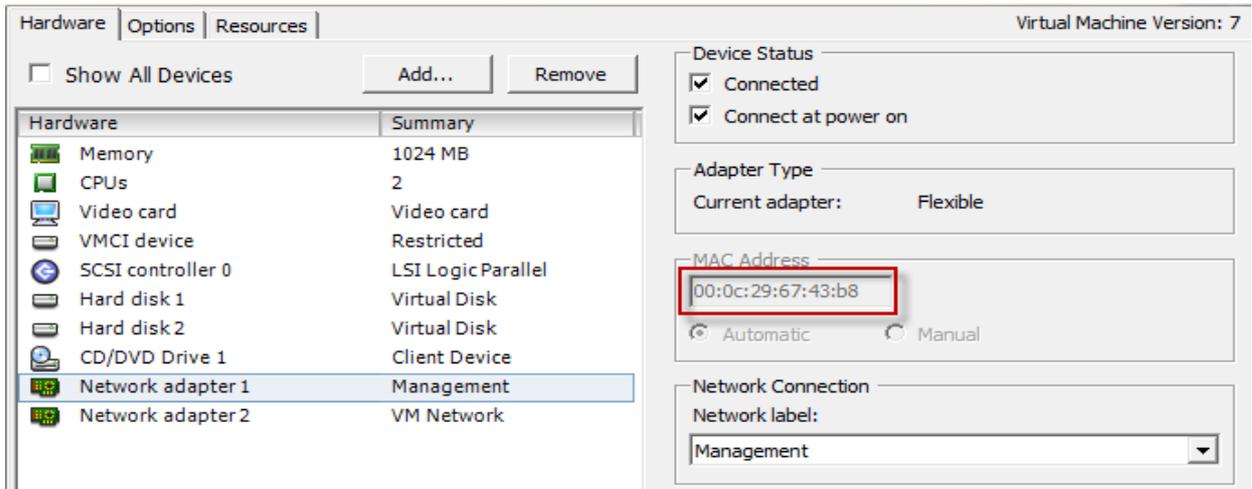


12. Check the Promiscuous Mode option and set as Accept
13. In vSphere Client select the Wireshark PC and add another Network adapter if necessary and make a note of their MAC addresses

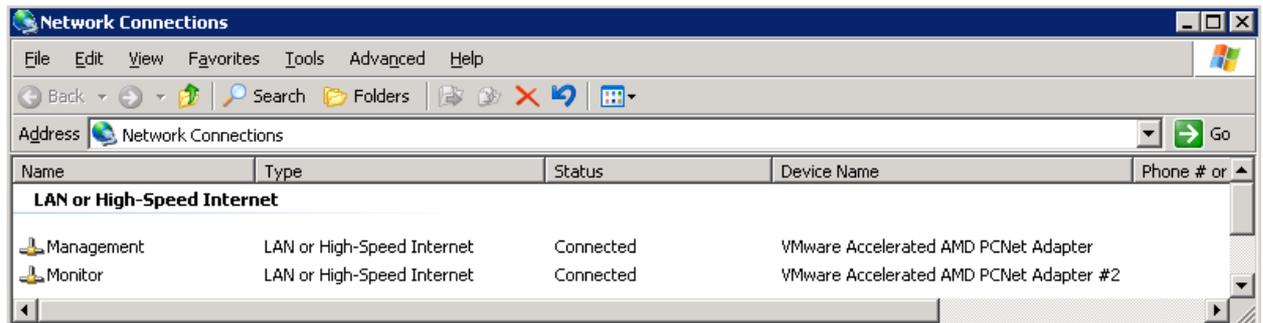


14. I did rename the Adapter to differentiate them easily. The Network Adapter 1 (*Ethernet Adapter Management*) will be connected with Management and Network Adapter 2 (*Ethernet Adapter Monitor*) will be connected with VM Network.

15. You can easily verify the proper assignment by comparing their MAC Addresses



Network Connections on WireShark PC



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------------|----------------|----------------|----------|--------|---|
| 449 | 18.2603520 | 192.168.10.173 | 192.168.10.175 | ICMP | 74 | Echo (ping) request id=0x0200, seq=256/1, ttl=128 |
| 450 | 18.2604050 | 192.168.10.175 | 192.168.10.173 | ICMP | 74 | Echo (ping) reply id=0x0200, seq=256/1, ttl=64 |
| 456 | 19.2453770 | 192.168.10.173 | 192.168.10.175 | ICMP | 74 | Echo (ping) request id=0x0200, seq=512/2, ttl=128 |
| 457 | 19.2454380 | 192.168.10.175 | 192.168.10.173 | ICMP | 74 | Echo (ping) reply id=0x0200, seq=512/2, ttl=64 |
| 473 | 20.2453160 | 192.168.10.173 | 192.168.10.175 | ICMP | 74 | Echo (ping) request id=0x0200, seq=768/3, ttl=128 |
| 474 | 20.2453660 | 192.168.10.175 | 192.168.10.173 | ICMP | 74 | Echo (ping) reply id=0x0200, seq=768/3, ttl=64 |
| 489 | 21.2453500 | 192.168.10.173 | 192.168.10.175 | ICMP | 74 | Echo (ping) request id=0x0200, seq=1024/4, ttl=128 |
| 490 | 21.2454070 | 192.168.10.175 | 192.168.10.173 | ICMP | 74 | Echo (ping) reply id=0x0200, seq=1024/4, ttl=64 |
| 772 | 39.7143630 | 192.168.10.231 | 192.168.10.175 | ICMP | 74 | Echo (ping) request id=0x0001, seq=12660/29745, ttl=128 |
| 773 | 39.7144320 | 192.168.10.175 | 192.168.10.231 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=12660/29745, ttl=64 |
| 783 | 40.7152290 | 192.168.10.231 | 192.168.10.175 | ICMP | 74 | Echo (ping) request id=0x0001, seq=12661/30001, ttl=128 |
| 784 | 40.7152940 | 192.168.10.175 | 192.168.10.231 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=12661/30001, ttl=64 |
| 793 | 41.7161760 | 192.168.10.231 | 192.168.10.175 | ICMP | 74 | Echo (ping) request id=0x0001, seq=12662/30257, ttl=128 |
| 794 | 41.7162370 | 192.168.10.175 | 192.168.10.231 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=12662/30257, ttl=64 |
| 803 | 42.7172020 | 192.168.10.231 | 192.168.10.175 | ICMP | 74 | Echo (ping) request id=0x0001, seq=12663/30513, ttl=128 |
| 804 | 42.7172650 | 192.168.10.175 | 192.168.10.231 | ICMP | 74 | Echo (ping) reply id=0x0001, seq=12663/30513, ttl=64 |
| 920 | 54.5727370 | 192.168.10.174 | 192.168.10.175 | ICMP | 98 | Echo (ping) request id=0x760b, seq=1/256, ttl=64 |
| 921 | 54.5727720 | 192.168.10.175 | 192.168.10.174 | ICMP | 98 | Echo (ping) reply id=0x760b, seq=1/256, ttl=64 |
| 931 | 55.5724520 | 192.168.10.174 | 192.168.10.175 | ICMP | 98 | Echo (ping) request id=0x760b, seq=2/512, ttl=64 |
| 932 | 55.5725060 | 192.168.10.175 | 192.168.10.174 | ICMP | 98 | Echo (ping) reply id=0x760b, seq=2/512, ttl=64 |
| 952 | 56.5733750 | 192.168.10.174 | 192.168.10.175 | ICMP | 98 | Echo (ping) request id=0x760b, seq=3/768, ttl=64 |
| 953 | 56.5734340 | 192.168.10.175 | 192.168.10.174 | ICMP | 98 | Echo (ping) reply id=0x760b, seq=3/768, ttl=64 |

Again pinging from Wireshark PC to 192.168.10.231, from 192.168.10.231 to 192.168.10.175 and from 192.168.10.174 to 192.168.10.175. Now I can see ICMP packets from any internal and external hosts

Reference Networking Configuration tab

esx-2.bemselhome VMware ESXi, 4.1.0, 348481

Getting Started Summary Virtual Machines Resource Allocation Performance Configuration Local Users & Groups Events Permissions

Hardware

- Health Status
- Processors
- Memory
- Storage
- Networking
- Storage Adapters
- Network Adapters
- Advanced Settings
- Power Management

Software

- Licensed Features
- Time Configuration
- DNS and Routing
- Authentication Services
- Virtual Machine Startup/Shutdown
- Virtual Machine Swapfile Location
- Security Profile
- System Resource Allocation
- Advanced Settings

View: Virtual Switch

Networking Refresh Add Networking... Properties...

Virtual Switch: vSwitch0 Remove... Properties...

Virtual Machine Port Group

- VM Network
 - 5 virtual machine(s)
 - CA Performance Center
 - CA Data Aggregator
 - CA Data Collector 1
 - CA Data Repository
 - CA ADA Virtual Monitor

VMkernel Port

- Management Network
 - vmk0 : 192.168.10.172

Physical Adapters

- vmnic2 100 Full

Virtual Machine Port Group

- Management
 - 1 virtual machine(s) | VLAN ID: All (4095)
 - CA ADA Virtual Monitor

