



vSwitch “*Promiscuous Mode*” Configuration Guide

www.xangati.com.

Table of Contents

1. Introduction.....	4
2. Installation Pre-Requisites.....	4
3. Enabling Promiscuous Mode for VMware vSwitches	5

About this Document

What is in this Document?

This document explains how to configure the virtual switches in your ESX host for use with the Xangati appliance. This procedure is necessary for each vSwitch that is to be monitored by the Xangati solution. The document explains how to use Promiscuous Mode without compromising existing security policies.

Document Conventions

1. The IP Address/Port/Values mentioned in the software installation process are for a particular network. Please make the required changes according to your network.
2. During installation anything enclosed in [] indicates default value/setting. You can make changes if required but must ensure that the format is maintained.
3. Some screen shots may be cut short for better readability.
4. <Enter> means hit the Enter key from the keyboard.

1. Introduction

In an ESX4.0 environment, Netflow is not available on vSwitches or dvSwitches. Netflow is available if the optional Cisco Nexus 1000V has been installed. Since it is usually desirable to know what is happening inside an ESX host, the question becomes how to get at the traffic. One option is to enable a “promiscuous” interface on the vSwitch inside the ESX host. Such an interface receives a copy of every packet that passes through the switch. It is similar to a port-mirror, or SPAN port on other devices.

This document shows how to enable promiscuous mode using the vSphere Client that is normally used to manage VMware environments.

The procedure below has three major components:

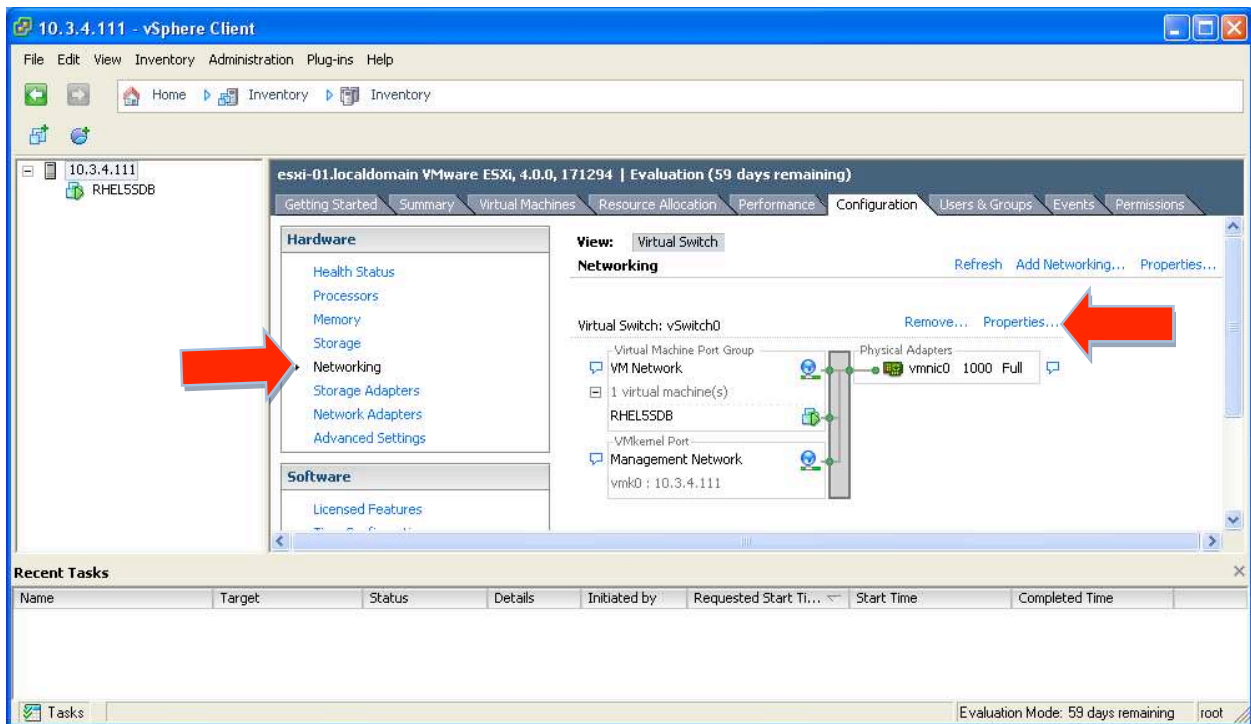
1. Set up a new Promiscuous Mode Port Group
2. Set the Xangati NIC to be a member of that Port Group
3. Setup a “pcap” Flow Source on the Xangati appliance that uses that NIC

2. Installation Pre-Requisites

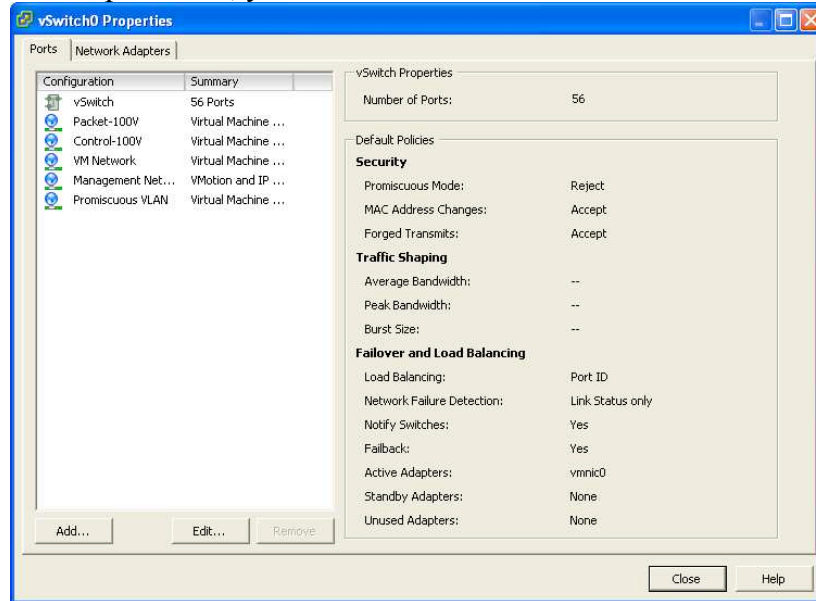
- An installed Xangati virtual appliance
 - Xangati for ESX
 - Xangati Management Dashboard Standard
 - Xangati Management Dashboard Enterprise
- A VMware ESX host running v3.5 or v4.x code
- Administrative access sufficient to modify vSwitch configuration on the ESX Server
- vCenter Server (if vCenter integration features are desired)

3. Enabling Promiscuous Mode for VMware vSwitches

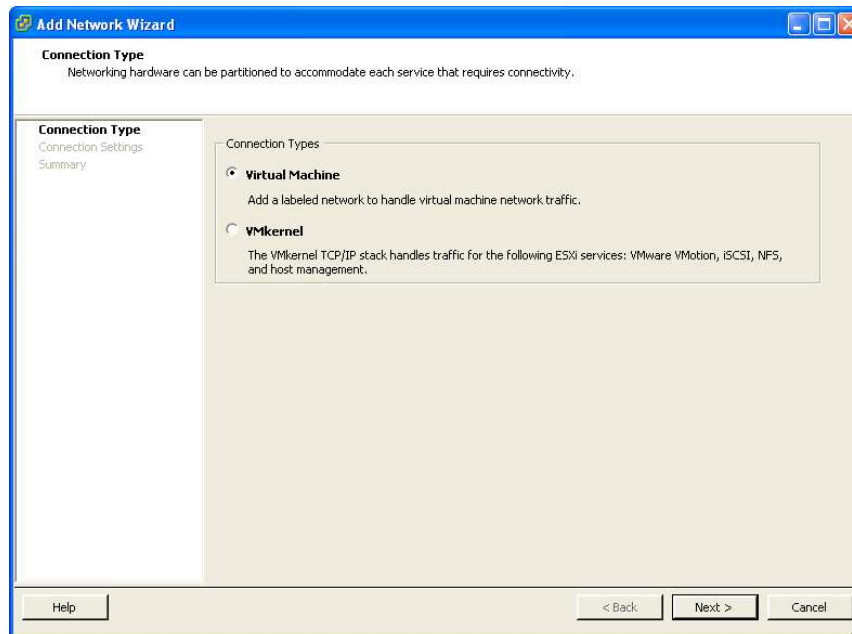
1. Log into the vSphere client and select the ESX host.
2. Choose the “Configuration Tab” and then “Networking” in the Hardware area.
3. The Virtual Switch summary page will appear as below.
4. Click on the “Properties” link.



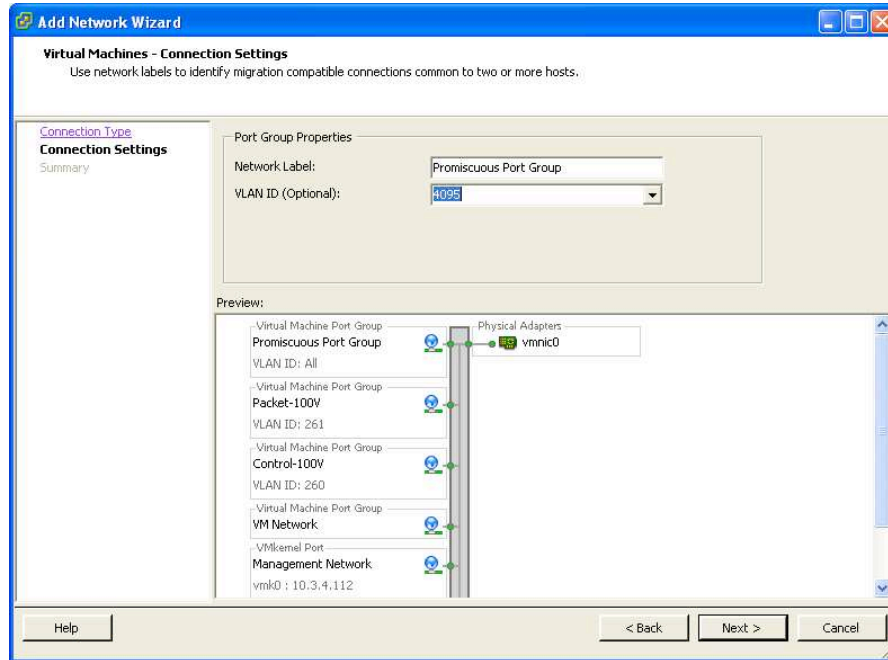
This opens up a window that allows you to modify the vSwitch configuration by port group. All the port groups on the “Ports” page are virtual. The items on the “Network Adapters” tab are real physical NIC cards in the server. By highlighting a port group, you can see a summary of its settings. In the example below, you can see that Promiscuous Mode is turned “Off” (Reject).



5. Create a new Port Group by pressing the “Add” button. The following dialog will appear:

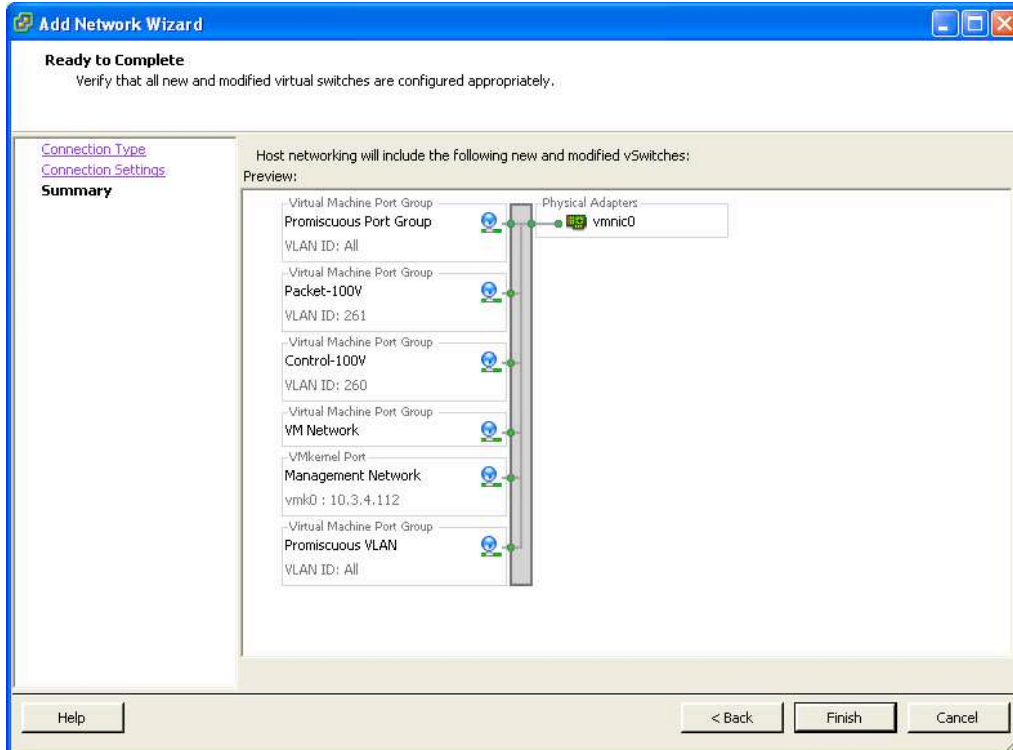


6. Select “Virtual Machine” and press Next. The following dialog will appear:



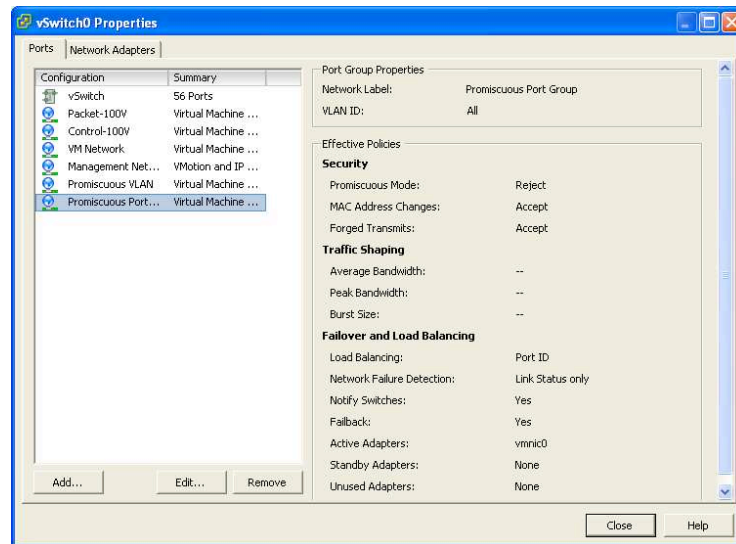
7. Enter a name, set the VLAN to 4095 and press Next. This is a special VMware VLAN that listens to all other VLANs.

8. Press “Finish” to complete setup of your Promiscuous Mode port group.

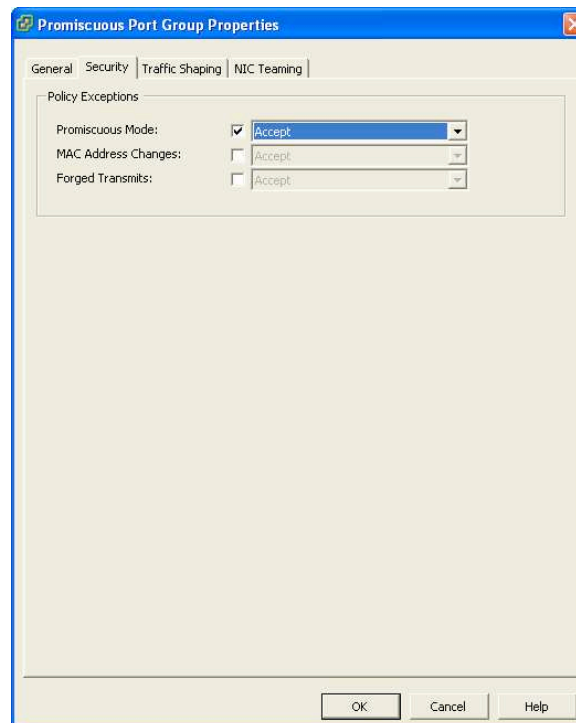


9. Set the Port Group to Promiscuous Mode

- Highlight your new Port Group and select “Edit”



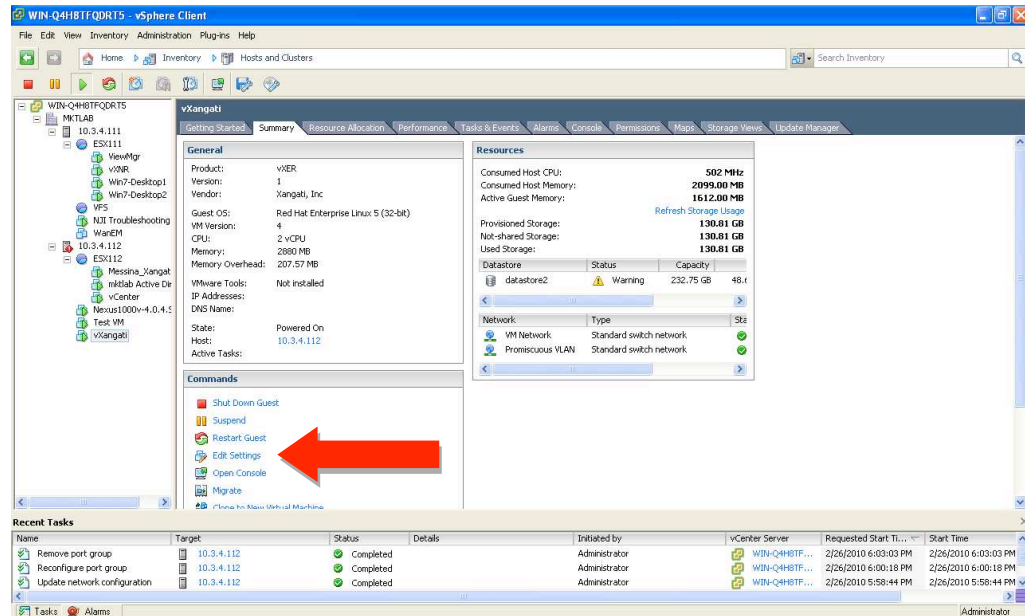
- Select the “Security” tab
- Select “Promiscuous Mode” and set the value to “Accept”



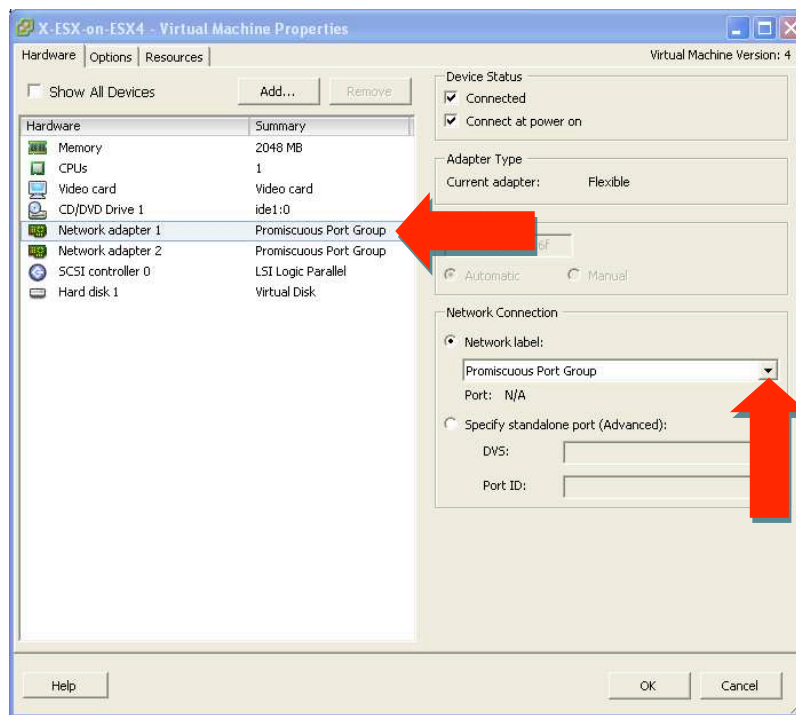
- Select “OK”

10. Ensure the Xangati VM has an interface in the Promiscuous Port Group you just created

- **Go to the Summary Tab for the Xangati VM and select “Edit Settings”**

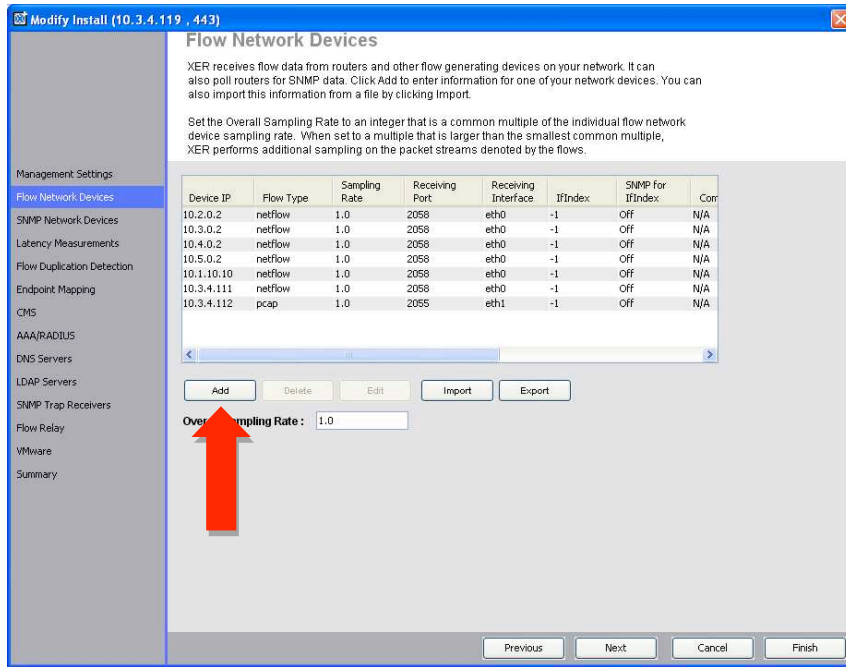


- **Highlight the NIC you wish to configure** (i.e. Network Adapter 1 in vCenter is eth0 in the Xangati Dashboard; Network Adapter 2 in vCenter is eth1 in the Xangati Dashboard, and so on).
- **Ensure it is mapped to the Promiscuous Port Group you created in step 7**

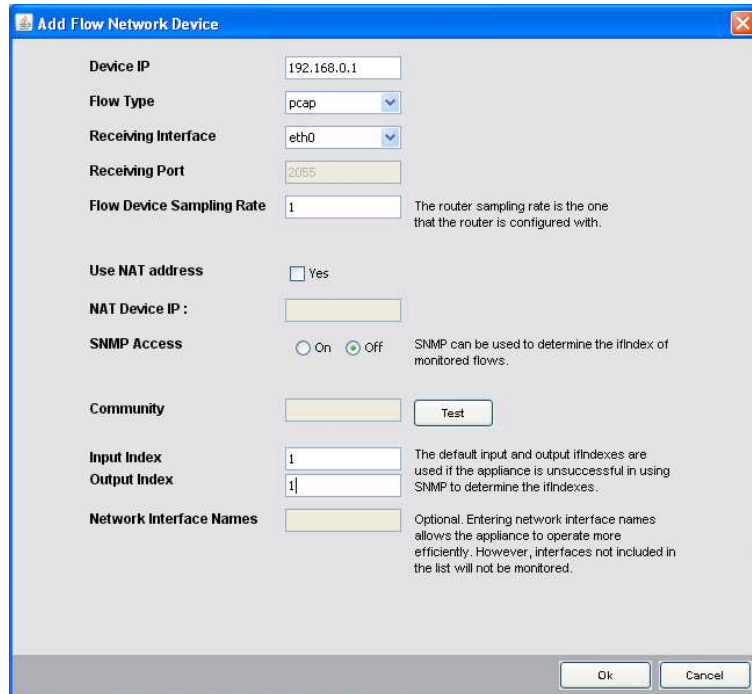


11. Open the Xangati Management console

12. Open Setup>Flow Network Devices from the top Menu bar:



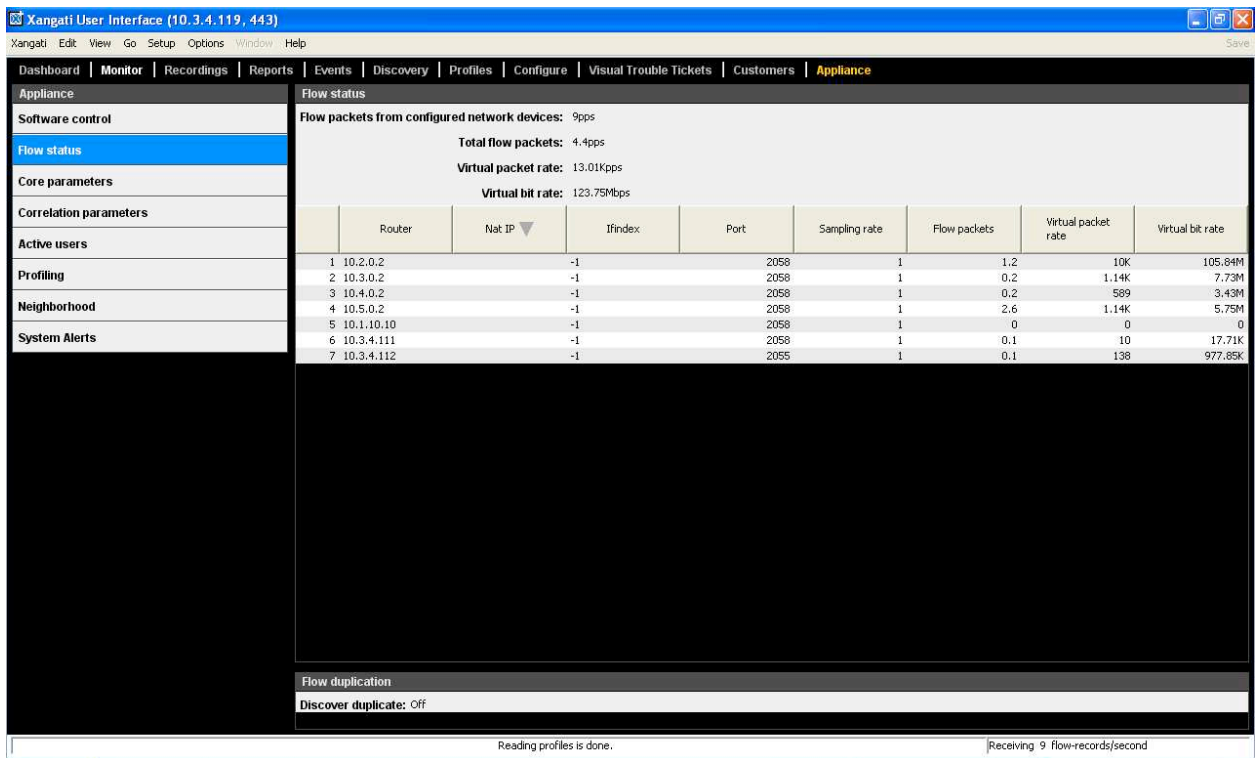
13. Add a Flow Source for the vNIC that you modified in step 8



- Enter the ESX host’s management IP address as the Device IP.
- The Flow Source will be *pcap*

- **Set the receiving interface according to the interface you set up as a member of the Promiscuous Mode Port Group in step 8.** (i.e. Network Adapter 1 in vCenter is eth0 in the Xangati Dashboard, Network Adapter 2 in vCenter is eth1 in the Xangati Dashboard, and so on).
- **Set the Input/Output index fields to “1” unless this is for a second/third/etc vSwitch.** If this is the 2nd or higher pcap source from the same Source IP address, as would be the case if you are using multiple vSwitches, you will increment this with each additional flow source you create. (i.e. You configure a 2nd flow source for an additional vSwitch in your environment. The Source IP Address remains the ESX Host, but the Input and Output index would both be set to “2”).
- **All other fields can be left at their default value**
- **Press “OK” to continue**

14. Verify that you are capturing packets on your new Flow Source (Appliance>Flow Status)



15. Repeat this entire process from step 4 as necessary for other vSwitches. Each vSwitch to be monitored must have:

- **A promiscuous mode port group**
- **A Xangati interface assigned to that port group**
- **A properly configured “flow source” in order to receive and process flows**