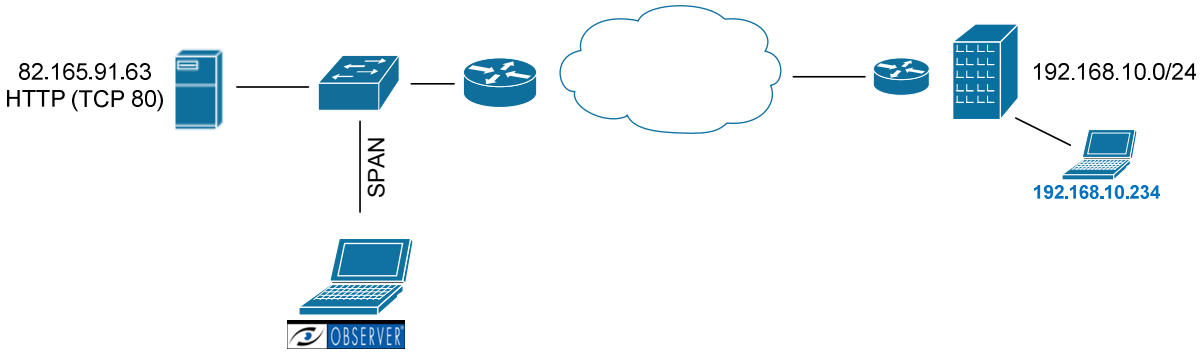
Observer Filter: SYN SYN/ACK

created by: Rainer Bemsel – **Version** 1.0 – **Dated:** Feb/20/2012

This document outlines the steps to create a filter for syn and syn-ack packets being captured by Observer from Network Instruments.

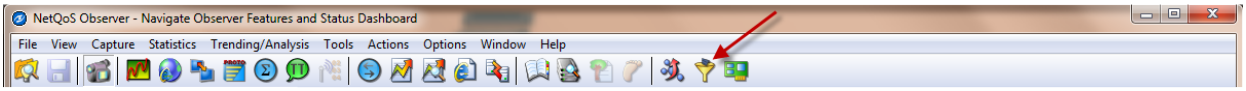
In my scenario, I want to verify SYN and SYN/ACK packets between those two hosts.



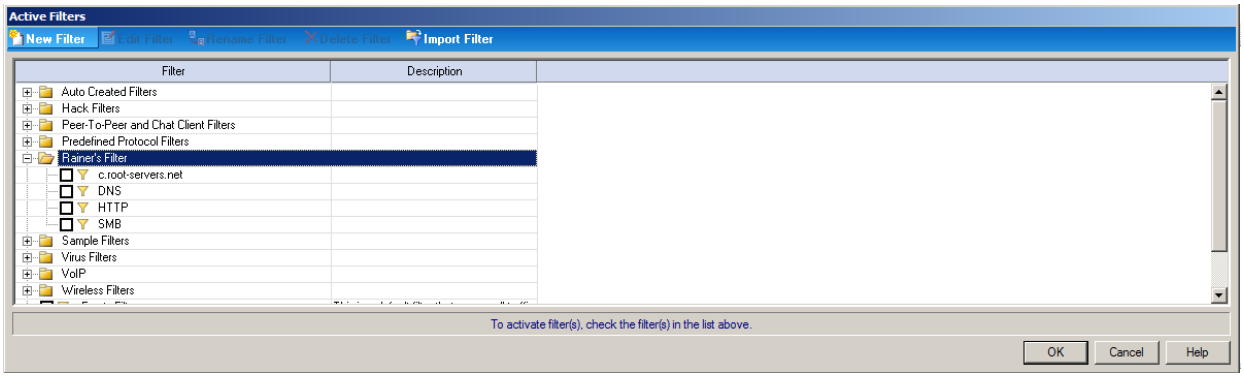
I am not interested in capturing all kind of data, just the two of them.

Start Observer and make sure you are connected with the SPAN port.

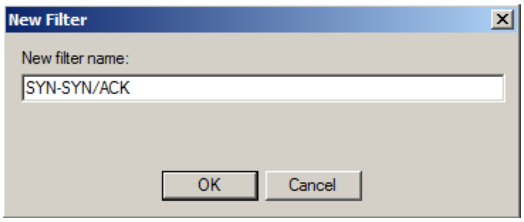
Click on Filter



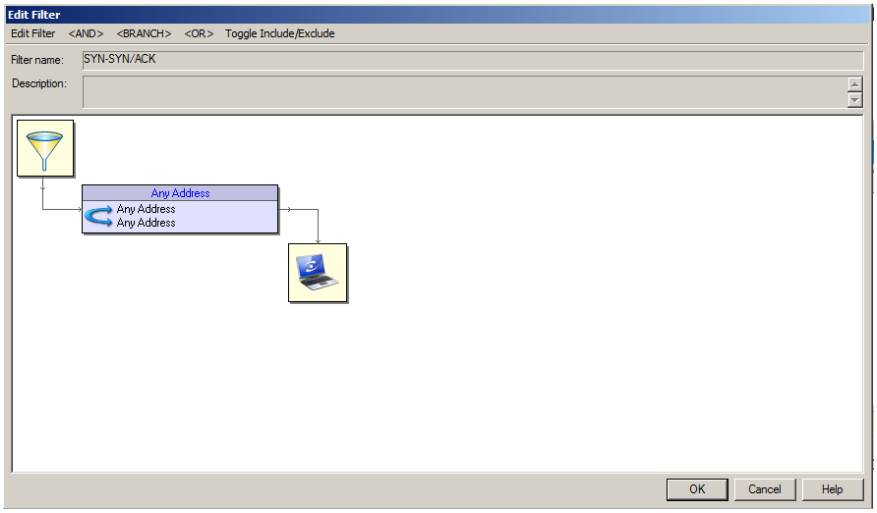
Click on New Filter (you may want to choose predefined Folder)



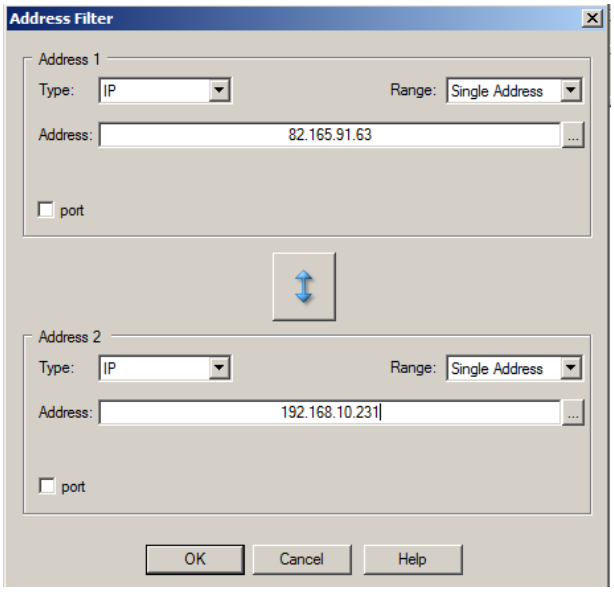
Give it a descriptive name

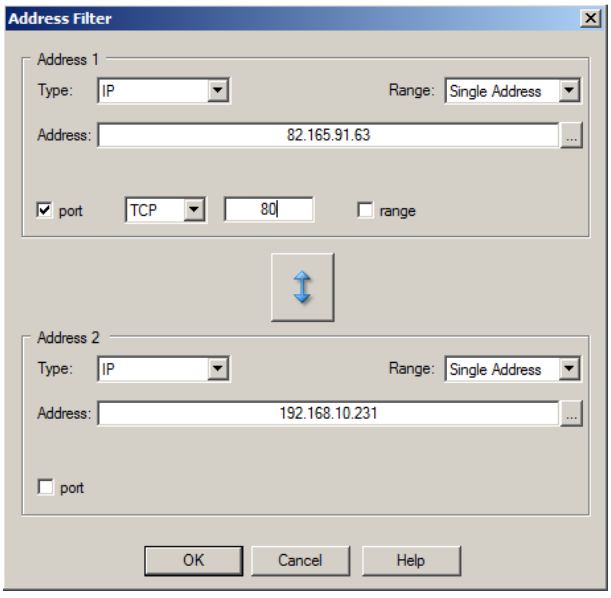


The filter editor will open and a standard filter is being provided



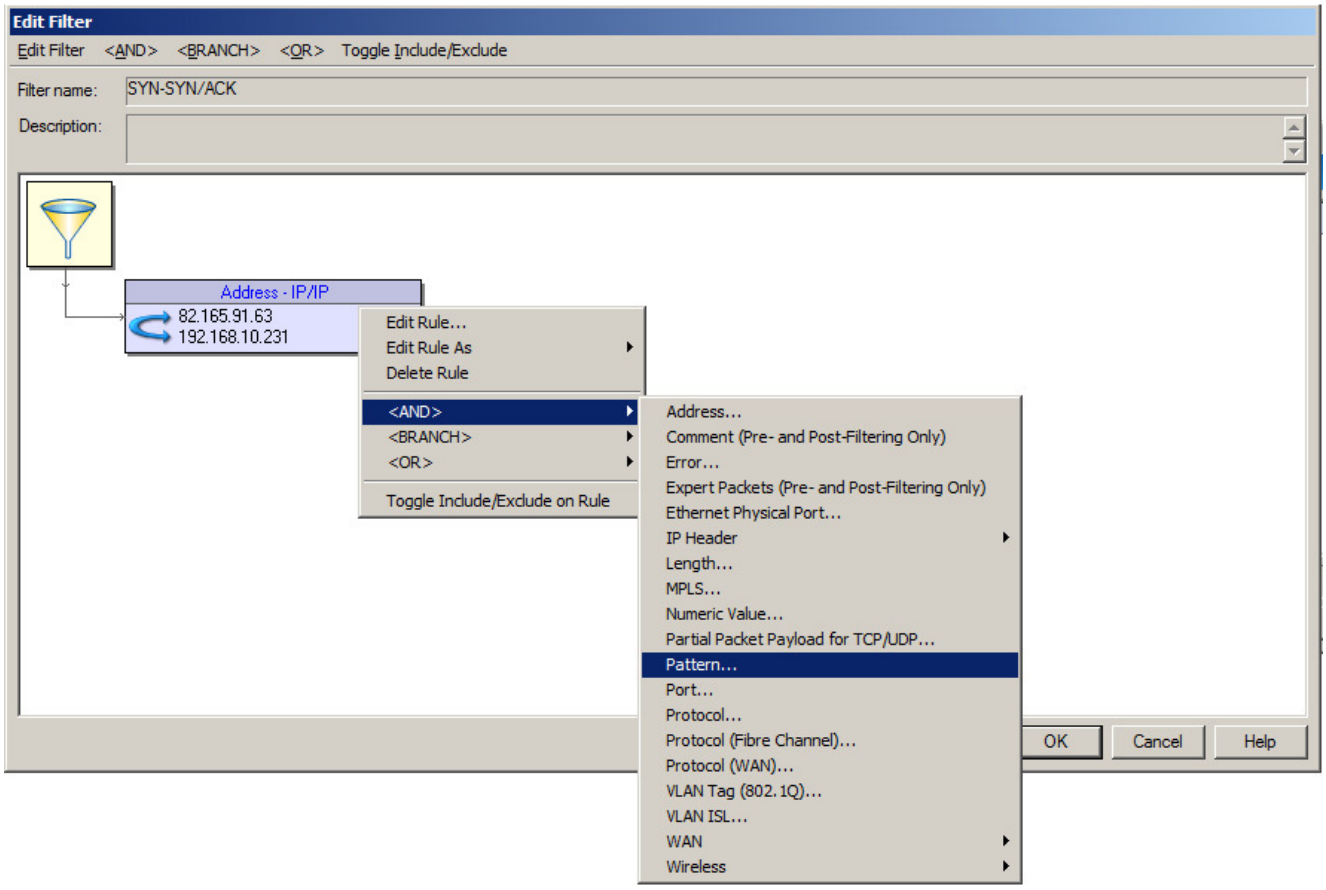
Change the Type from Hardware to IP and provide IP address pair, you want to monitor.



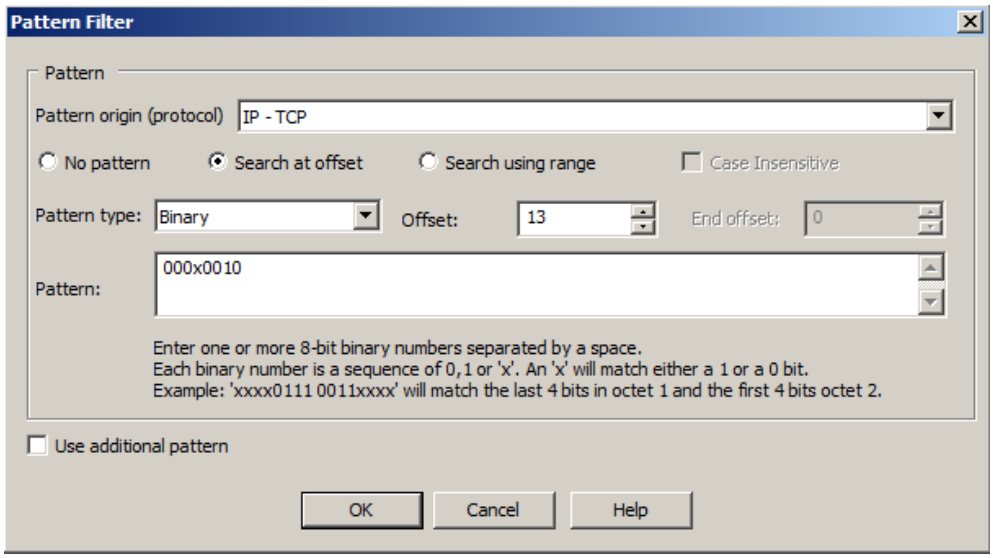


I also active the port on the server side and added TCP port 80 for HTTP Traffic

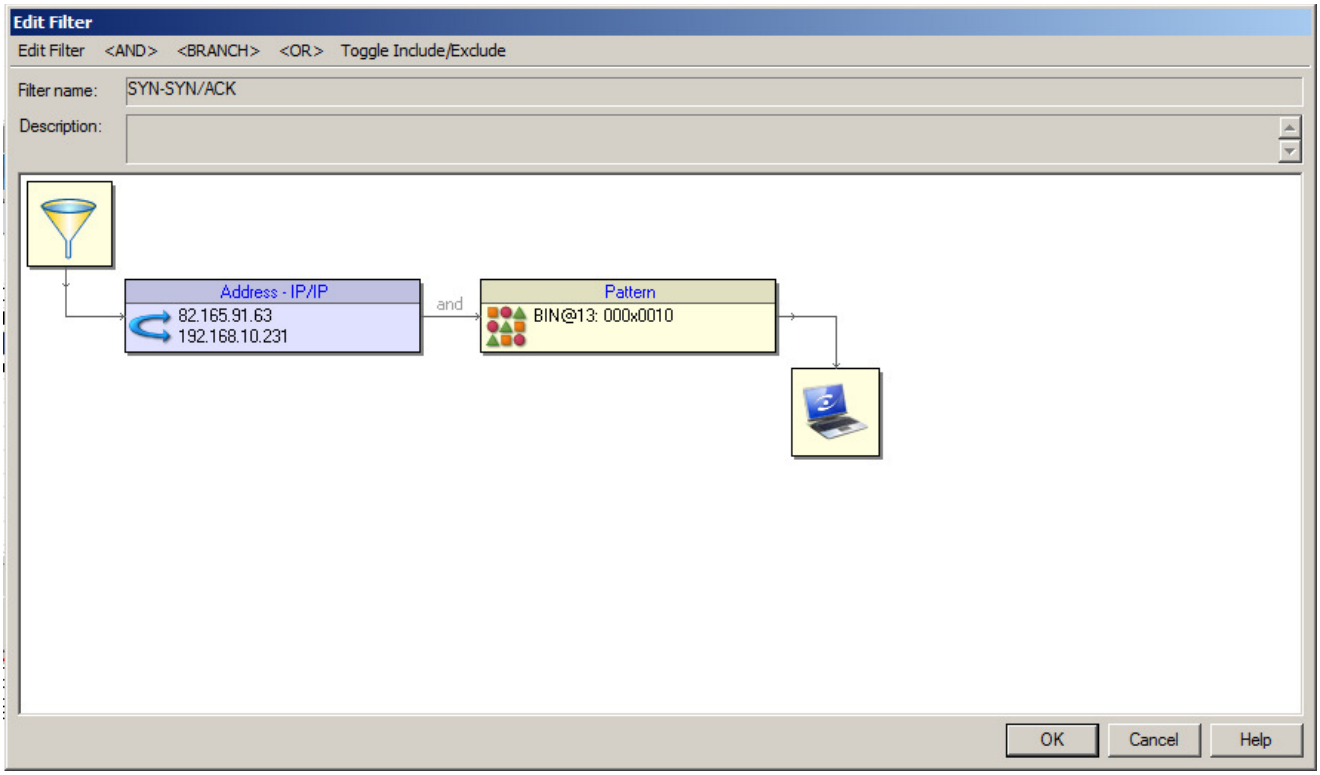
The filter has been created. Now roll-over with the mouse pointer on the filter and right-click to add another filter



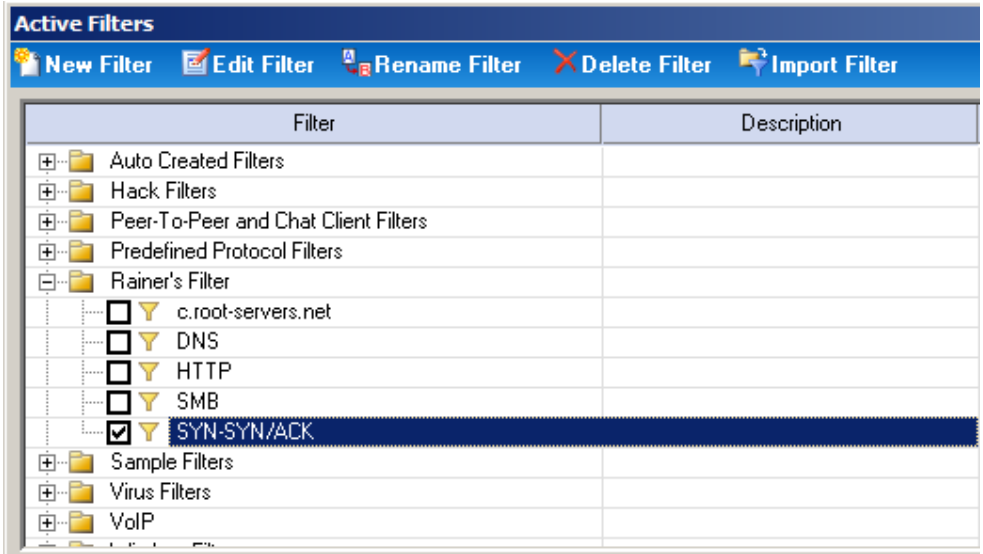
To capture SYN and SYN/ACK Packets you need to add following Pattern to the previous filter



The complete filter looks like that



Now, you want to use the newly created filter. To activate the filter, mark the checkbox



Click on Start. The yellow indicate captured packets.