

The purpose of this document is to outline the steps for setting up Packet Cloning in CA|NetQoS Reporter Analyzer (version 9.1 SP1). During my study to compare another Netflow collecting device with Reporter Analyzer, I wanted to forward Netflow data from my primary collector to another device. Flow cloning can be used to leverage other tools without sending flow to two destinations from the router. This idea is even worse, when having a remote location router sending to more than one destination. That's why packet cloning is a nice handy feature.



SIMPLE RECIPE

1. First, create the file FlowCloneDef.ini in <D:\NetQoS\Netflow\bin> using Notepad. The first line of the INI file must either be:

```
/use defaults; take default setup (use first available NIC to send flows on UDP 9995)  
OR  
/port=9994; (Use and change this to modify the port flow data is exported on ...  
|port= must be on the first line of the .ini file)
```

Note: Port number is a global setting. You cannot use different port numbers

2. The subsequent lines should contain the destinations:

```
/dest ip=192.168.0.146 ; send cloned packets to 192.168.10.79  
/dest ip=192.168.0.144 ; send cloned packets to 192.168.10.2
```

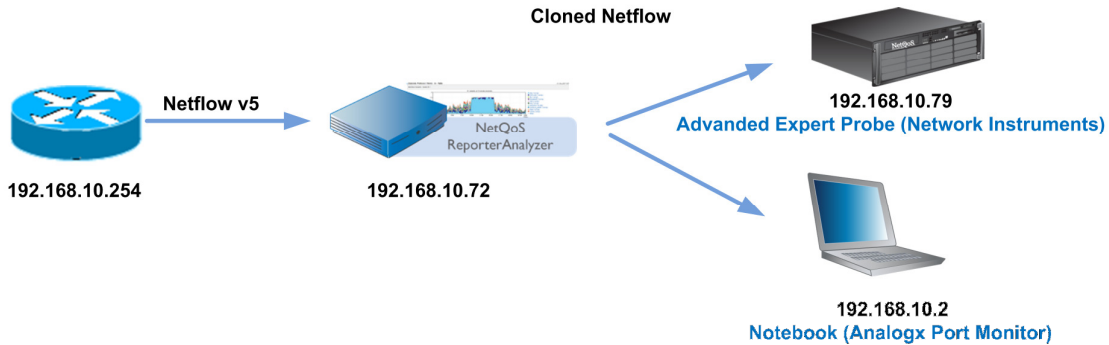
3. Save the file and close.
4. Next, edit the Harvester database with these commands (in a cmd prompt on the Harvester server):

```
C:> mysql harvester  
mysql> update parameter_descriptions set defaultvalue='Y' where parameter='EnableFlowCloner';  
mysql> exit
```

5. Finally restart the NetQoS Harvester service to initiate flow export.

Finally, here's my practical follow through.

Given following scenario to configure



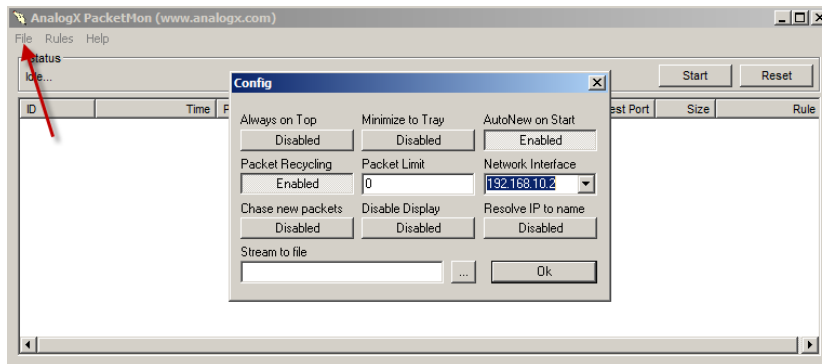
Step 1 - Set up Filter for Packet Monitor on Notebook to see incoming netflow data

This will show immediate changes, when switching on Packet Cloning on Reporter Analyzer. I'll have my notebook ready to receive packets.

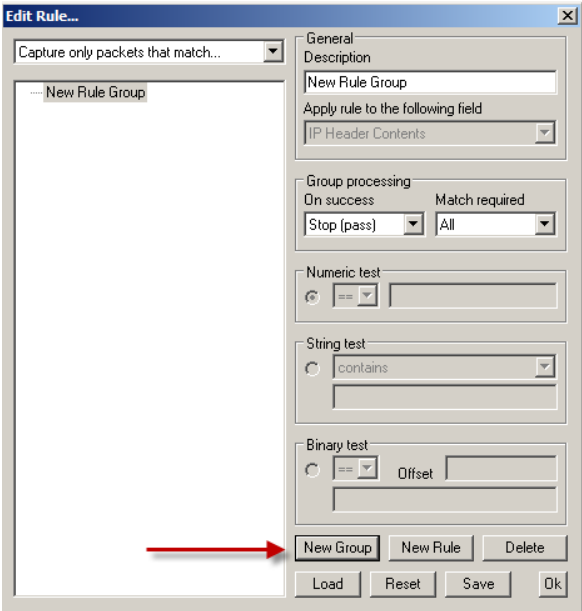
To download this freeware, go to: <http://www.analogx.com/contents/download/Network/pmon/Freeware.htm>

To create a filter to display only UDP 9995

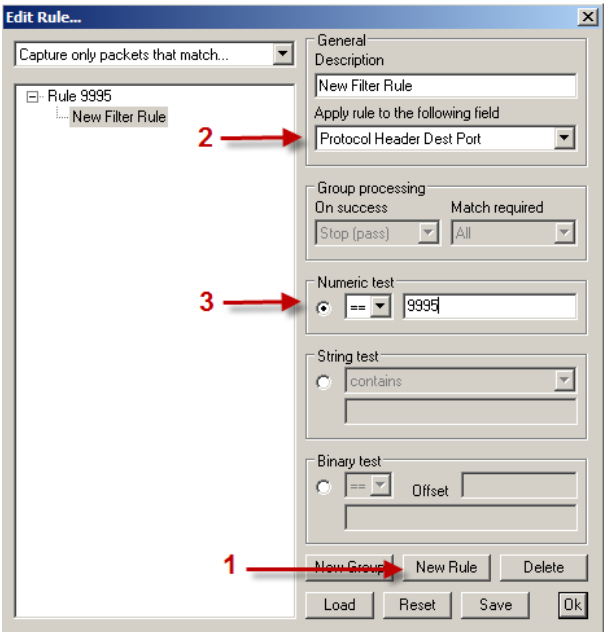
Click on Rules -> Edit Active Rules



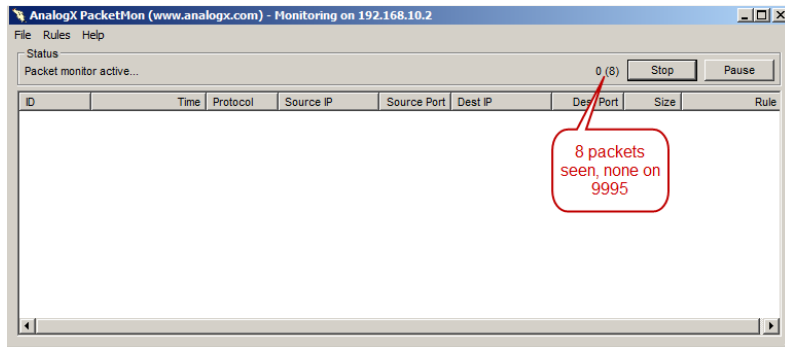
Create New Group - you may want to give it a new description as well



Create New Filter Rule



Click on Start



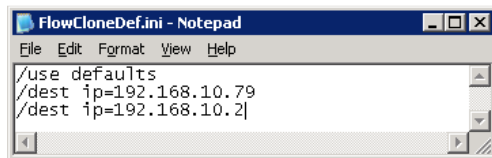
Note: Make sure that your Windows Firewall is open for UDP 9995

Step 2 - Configure Reporter Analyzer to clone packets and forwarding them to the destinations

Verify path of NFFlowCloneEngine.dll - you may want to run a search and make a note of the folder

Name	In Folder	Size	Type	Date Modified	Attributes
NFFlowCloneEngine.dll	D:\NetQoS\Netflow\bin	24 KB	Application Extension	3/4/2011 8:03 PM	A

Create a file named FlowCloneDef.ini in the same directory where the NFFlowCloneEngine.dll is located



Run following SQL Command to enable the feature

```
mysql harvester  
update parameter_descriptions set defaultvalue='Y' where parameter='EnableFlowCloner';  
exit
```

Restart Harvester Service

```
C:\Documents and Settings\Administrator>net stop "NetQoS Harvester"  
The NetQoS Harvester service was stopped successfully.  
C:\Documents and Settings\Administrator>net start "NetQoS Harvester"  
The NetQoS Harvester service is starting.  
The NetQoS Harvester service was started successfully.
```

You should see incoming packets in a few moments after restarting Harvester Service on the notebook

AnalogX PacketMon (www.analogx.com) - Monitoring on 192.168.10.2

Status: Packet monitor active... 11 (971) [Stop] [Pause]

ID	Time	Protocol	Source IP	Source Port	Dest IP	Dest Port	Size	Rule
1	00:02:03:50:608	UDP	192.168.10.254	10000	192.168.10.2	9995	388	Rule 9995
2	00:02:04:04:600	UDP	192.168.10.254	10000	192.168.10.2	9995	436	Rule 9995
3	00:02:04:19:872	UDP	192.168.10.254	10000	192.168.10.2	9995	1108	Rule 9995
4	00:02:04:30:605	UDP	192.168.10.254	10000	192.168.10.2	9995	340	Rule 9995
5	00:02:04:51:618	UDP	192.168.10.254	10000	192.168.10.2	9995	388	Rule 9995
6	00:02:05:08:876	UDP	192.168.10.254	10000	192.168.10.2	9995	1348	Rule 9995
7	00:02:05:18:609	UDP	192.168.10.254	10000	192.168.10.2	9995	148	Rule 9995
8	00:02:05:32:603	UDP	192.168.10.254	10000	192.168.10.2	9995	340	Rule 9995
9	00:02:05:44:631	UDP	192.168.10.254	10000	192.168.10.2	9995	244	Rule 9995
10	00:02:05:57:609	UDP	192.168.10.254	10000	192.168.10.2	9995	484	Rule 9995
11	00:02:06:15:613	UDP	192.168.10.254	10000	192.168.10.2	9995	484	Rule 9995

To verify, if Packet Cloning has been switched on simply run following SQL Query (a handy command for troubleshooting - DefaultValue switched to "Y" means on)

```
C:\Documents and Settings\Administrator>mysql harvester
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4779
Server version: 5.1.45-enterprise-commercial-advanced MySQL Enterprise Server - Advanced Edition (Commercial)

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> select * from parameter_descriptions where parameter='EnableFlowCloner';
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Parameter | Level | Type | DefaultValue | Description | Label |
+-----+-----+-----+-----+-----+-----+-----+-----+
| EnableFlowCloner | System | string | Y | Indicates whether the flow cloner is to be enabled. Valid values are 'Y' or 'N'. | Enable Flow Cloner |
+-----+-----+-----+-----+-----+-----+-----+-----+
1 row in set (0.00 sec)

mysql> _
```

For lab usage, you may want to create two Batch-Files, where you can easily switch on or off.

EnableFlowClone.CMD

```
mysql -D harvester -e "update parameter_descriptions set defaultvalue='y' where parameter='EnableFlowCloner'"
net stop "NetQoS Harvester"
net start "NetQoS Harvester"
```

DisableFlowClone.CMD

```
mysql -D harvester -e "update parameter_descriptions set defaultvalue='n' where parameter='EnableFlowCloner'"
net stop "NetQoS Harvester"
net start "NetQoS Harvester"
```

In Reporter Analyzer Documentation, there are a few more options being mentioned, what can be done with Netflow Cloning. Consider to have a look, because it also outlines the limitations.

If you are interested in how to configure Network Instruments Advanced Expert Probe to become a NetFlow Collector, go to my website under the section Network Instruments.

