% Monitoring Netflow with NFsen
%
% Network Monitoring and Management

Introduction

Goals

* Learn how to export flows from a Cisco router
* Learn how to install the Nfsen family of tools
* Install the optional PortTracker plugin

Notes

* Commands preceded with "$" imply that you should execute the command as
  a general user - not as root.
* Commands preceded with "#" imply that you should be working as root.
* Commands with more specific command lines (e.g. "RTR-GW>" or "mysql>")
  imply that you are executing commands on remote equipment, or within
  another program.

Export flows from a Cisco router

During this exercise we will ask that you export flows from your router to two PCs in the classroom. You should work together as a group. That is, for group 1, users of pc1, pc2, pc3, pc4 should work together and pick one machine where network flows will arrive.

In addition, you will export a second flow from your group's router to a PC in the group next to yours. That is, for example, if group 2 has chosen pc5 to be the PC that receives flows, then the second flow you export will go to pc5.

These exercises work on the example of doing the following:

Flow 1 export ==> rtr1 ==> pc1 on port 9001
Flow 2 export ==> rtr1 ==> pc5 on port 9002

You may select the combination that works for your groups.

Here are the groups that should work together:

* group 1 and 2
* group 3 and 4
* group 5 and 6
* group 7 and 8

If there is a group 9 please see the instructors.

~~~~~~
$ ssh cisco@10.10.1.254
rtr1.ws.nsrc.org> enable
~~~~~~

or, if ssh is not configured yet:

~~~~~~
$ telnet 10.10.1.54
Username: cisco
Password:
Router1>enable
Password:
~~~~~~

Enter the enable password...

Configure FastEthernet0/0 to generate netflow:
(substitute Y with the PC numbers receiving the flows and X for your group number)

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
rtr1.ws.nsrc.org# configure terminal
rtr1.ws.nsrc.org(config)# interface FastEthernet 0/0
rtr1.ws.nsrc.org(config-if)# ip flow ingress
rtr1.ws.nsrc.org(config-if)# ip flow egress
rtr1.ws.nsrc.org(config-if)# exit
rtr1.ws.nsrc.org(config)# ip flow-export destination 10.10.1.1 9001
rtr1.ws.nsrc.org(config)# ip flow-export destination 10.10.2.5 9002
rtr1.ws.nsrc.org(config)# ip flow-export version 5
rtr1.ws.nsrc.org(config)# ip flow-cache timeout active 5
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

This breaks up long-lived flows into 5-minute fragments. You can
choose any number of minutes between 1 and 60. If you leave it at
the default of 30 minutes your traffic reports will have spikes.

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
rtr1.ws.nsrc.org(config)# snmp-server ifindex persist
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

This enables ifIndex persistence globally. This ensures that the
ifIndex values are persisted during router reboots.

Now configure how you want the ip flow top-talkers to work:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
rtr1.ws.nsrc.org(config)#ip flow-top-talkers
rtr1.ws.nsrc.org(config-flow-top-talkers)#top 20
rtr1.ws.nsrc.org(config-flow-top-talkers)#sort-by bytes
rtr1.ws.nsrc.org(config-flow-top-talkers)#end
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Now we'll verify what we've done.

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
rtr1.ws.nsrc.org# show ip flow export
rtr1.ws.nsrc.org# show ip cache flow
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

See your "top talkers" across your router interfaces

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
rtr1.ws.nsrc.org# show ip flow top-talkers
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

If it all looks good then write your running-config to non-volatile
RAM (i.e. the startup-config):

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
rtr1.ws.nsrc.org#wr mem
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

You can exit from the router now:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
rtr1.ws.nsrc.org#exit
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Verify that flows are arriving from your router to the PC chosen to receive
flows in your group:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

```
$ sudo tcpdump -v udp port 9001
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Verify that flows are arriving from the router in the group next to you to the PC chosen to receive flows in your group (you may have to wait until the group next to you is ready and exporting flows to your PC):

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ sudo tcpdump -v udp port 9002
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Configure Your Collector

Install NFdump and friends

NFdump is the Netflow flow collector. We install several additional packages that we will need a bit later:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ sudo apt-get install rrdtool mrtg librrds-perl librrdp-perl librrd-dev \
nfdump libmailtools-perl php5 bison flex
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

This will install, among other things, nfcapd, nfdump, nfreplay, nfexpire, nftest, nfgen, php5

Installing and setting up NfSen

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
cd /usr/local/src
sudo wget http://noc.ws.nsrc.org/downloads/nfsen-1.3.6p1.tar.gz
sudo tar xvzf nfsen-1.3.6p1.tar.gz
cd nfsen-1.3.6p1
cd etc
sudo cp nfsen-dist.conf nfsen.conf
sudo editor nfsen.conf
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Set the $BASEDIR variable

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$BASEDIR="/var/nfsen";
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Adjust the tools path to where items actually reside:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
# nfdump tools path
$PREFIX = '/usr/bin';
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Set the users appropriately so that Apache can access files:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$WWWUSER = 'www-data';
$WWWGROUP = 'www-data';
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Set the buffer size to something small, so that we see data quickly

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
# Receive buffer size for nfcapd - see man page nfcapd(1)
$BUFFLEN = 2000;
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Find the %sources definition, and change it to:

(substitute X with your group number. substitute
 Y with the PC Number receiving the flows).

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
%sources=(
'rtr1' => {'port'=>'9001','col'=>'#0000ff','type'=>'netflow'},
'rtr2' => {'port'=>'9002','col'=>'#00ff00','type'=>'netflow'},
 ;
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Now save and exit from the file.

Create the netflow user on the system

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ sudo useradd -d /var/netflow -G www-data -m -s /bin/false netflow
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Initiate NfSen.

Any time you make changes to nfsen.conf you will have to do this step again.

Make sure we are in the right location:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ cd /usr/local/src/nfsen-1.3.6p1
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Now, finally, we install:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ sudo perl install.pl etc/nfsen.conf
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Start NfSen

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
sudo /var/nfsen/bin/nfsen start
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

View flows via the web:

You can find the nfsen page here:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
http://pcX.ws.nsrc.org/nfsen/nfsen.php
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

(Below is only if there are problems)

Note that in /usr/local/src/nfsen-1.3.6p1/etc/nfsen.conf there is a variable
$HTMLDIR that you may need to configure. By default it is set like this:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$HTMLDIR="/var/www/nfsen/";
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

In some cases you may need to either move the nfsen directory in your web
structure, or update the $HTMLDIR variable for your installation.

If you move items, then do:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ /etc/init.d/apache2 restart
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Install init script

In order to have nfsen start and stop automatically when the system starts,
add a link to the init.d diretory pointing to the nfsen startup script:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ sudo ln -s /var/nfsen/bin/nfsen /etc/init.d/nfsen
$ update-rc.d nfsen defaults 20
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Done! Move on to the second Exercise

Appendix

On some newer Linux distribution releases (Fedora Core 16 and above, Ubuntu
12.04 LTS and above, etc.) you may see error like this when starting nfsen
version 1.6.6:

```
    Subroutine Lookup::pack_sockaddr_in6 redefined at
    /usr/share/perl/5.14/Exporter.pm line 67.
    at /var/nfsen/libexec/Lookup.pm line 43
```

nfsen will still load and function properly, so you can ignore this error
for now (or solve the problem and give back to the nfsen project! :-)).