% Monitoring Netflow with NFsen
%
% Network Monitoring and Management

# Introduction

## Goals

* Learn how to install the nfdump and NfSen tools

## 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.

## Assumption

This assumes you have already configured your router to export flows to a PC in your group and that your neighbor group has configured a router to export flows to the same PC. See exercise1-flow-export for additional details.

# Configure Your Collector

## Install NFDump and associated software

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 \
libmailtools-perl php5 bison flex
~~~~~~

If prompted to "Make /etc/mrtg.cfg owned by and readable only by root?" select "<Yes>" and press ENTER to continue.

### Building and installing nfdump

We are still missing some tools:

nfcapd, nfdump, nfreplay, nfexpire, nftest, nfgen

There is a package in Ubuntu, but it’s too old - so we’ve built a newer one which is ready to download from the NOC:

~~~~~~
cd /tmp/
wget http://noc.ws.nsrc.org/downloads/nfdump_1.6.6-1_i386.deb
wget http://noc.ws.nsrc.org/downloads/nfdump-flow-tools_1.6.6-1_i386.deb
~~~~~~

Installation:

~~~~~~
sudo dpkg --install nfdump_1.6.6-1_i386.deb
sudo dpkg --install nfdump-flow-tools_1.6.6-1_i386.deb
~~~~~~

### Testing nfcapd and nfdump

```
mkdir /tmp/nfcap-test
nfcapd -E  -p 9001 -l /tmp/nfcap-test
```

... after a while, a series of flows should be dumped on your screen.

Stop the tool with CTRL+C, then look at the contents of /tmp/nfcap-test

```
$ ls -l /tmp/nfcap-test
```

You should see one or more files called nfcapd.2013xxyyzz

Process the file(s) with nfdump:

```
nfdump -r /tmp/nfcap-test/nfcapd.2013xxyyzz | less
nfdump -r /tmp/nfcap-test/nfcapd.2013xxyyzz -s srcip/bytes
```

You should get some useful information :)

## 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
sudo wget http://noc.ws.nsrc.org/downloads/nfsen-socket6.patch
sudo patch -p0 < nfsen-socket6.patch
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:

~~~~~~
%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
~~~~~~

## Install NfSen and start it

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
~~~~~~

Press ENTER when prompted for the path to Perl.

## 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
~~~~~~

Start NfSen

~~~~~~
~~~~~~

~~~~~~
sudo service nfsen start
~~~~~~

## View flows via the web:

You can find the nfsen page here:

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

You may see a message such as:

~~~~~~
Frontend - Backend version missmatch!
~~~~~~

This will go away if you reload the page, it’s not a problem.

Done! Move on to the third lab, exercise3-NfSen-PortTracker

* NOTES:

## Adding sources

To add new sources to nfsen, the way to proceed is as follows:

- edit /var/nfsen/etc/nfsen.conf, and add the source, for example:

~~~~~~
%sources = (
    ’rtrX’ => { ’port’ => ’900X’, ’col’ => ’#0000ff’, ’type’ => ’netflow’ },
    ’rtrY’ => { ’port’ => ’900Y’, ’col’ => ’#00ff00’, ’type’ => ’netflow’ },
    ’rtr10’ => { ’port’ => ’9010’, ’col’ => ’#ff0000’, ’type’ => ’netflow’ }, # <- new
);
~~~~~~

- Reconfigure NfSen.

You will need to run this every time you modify /var/nfsen/etc/nfsen.conf:

~~~~~~
$ sudo /etc/init.d/nfsen reconfig
~~~~~~

You should see:

```
New sources to configure : rtr10
Continue? [y/n] y

Add source ’rtr10’

Reconfig done!
```