% 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.

Configure Your Collector

Note: if you are working in pairs then only the PC which is receiving
netflow packets needs to install nfdump and nfsen. However you can install
it on the other one as well, just for practice.

Install NFDump and associated software

NFdump is part of the Netflow flow collector tools, which includes:

nfcapd, nfdump, nfreplay, nfexpire, nftest, nfgen

There is a package in Ubuntu, but it's too old - so we're going to build
it from source. First, check you have the build tools and dependencies:

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

Now proceed to download and build. Note that only the last step
(make install) has to be done as root.

~~~~~~
$ cd
$ wget http://noc.ws.nsrc.org/downloads/nfdump-1.6.10.tar.gz
$ tar xvzf nfdump-1.6.10.tar.gz
$ cd nfdump-1.6.10
$ ./configure --help   # optional, shows the build settings available
$ ./configure --enable-nfprofile --enable-nftrack
$ make
$ sudo make install
~~~~~~

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.<YEAR><MON><DAY><HR><MIN>`

Process the file(s) with nfdump:

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

You should get some useful information :)

If you see the error "Verify map id 5: ERROR: Expected 7 elements in map, but found 2!", you can ignore it. This is a known issue in the v5 module of nfdump-1.6.10 and will be fixed in the next release.

Installing and setting up NfSen

Download and compile. The patch is to fix a problem reported at <http://sourceforge.net/p/nfsen/bugs/31/>

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ cd
$ wget http://noc.ws.nsrc.org/downloads/nfsen-1.3.6p1.tar.gz
$ tar xvzf nfsen-1.3.6p1.tar.gz
$ cd nfsen-1.3.6p1
$ wget http://noc.ws.nsrc.org/downloads/nfsen-socket6.patch
$ patch -p0 < nfsen-socket6.patch
$ cd etc
$ cp nfsen-dist.conf nfsen.conf
$ editor nfsen.conf
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Set the $BASEDIR variable

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

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. You would not do this on a production system.

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

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

Find the %sources definition, and change it to:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
%sources=(
'rtrX' => {'port'=>'9001','col'=>'#0000ff','type'=>'netflow'},
 );
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

(substitute your group's router for rtrX). Now save and exit from the file.

Create the netflow user on the system

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

Install NfSen and start it

Change directory back to just inside the source directory:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ cd
$ cd 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
sudo update-rc.d nfsen defaults 20
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Start NfSen

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

Check that nfcapd processes have been started:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
ps auxwww | grep nfcapd
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

View flows via the web:

You can find the nfsen page here:

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

If you are working in pairs, then both of you should point your web browser
to the PC which is receiving flows.

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

You can have multiple routers in your network all sending flows to the same
collector, by configuring each one to send netflow data to a different port.
This allows nfsen to show distinct data from each source.

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

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

~~~~~~
```
%sources = (
    'rtrX'  => { 'port' => '9001', 'col' => '#0000ff', 'type' => 'netflow' },
    'rtrY'  => { 'port' => '9002', 'col' => '#00ff00', 'type' => 'netflow' },
    'gw'    => { 'port' => '9996', 'col' => '#ff0000', 'type' => 'netflow' },
);
```
~~~~~~

- 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 : gw rtrY
Continue? [y/n] y

Add source 'gw'
Add source 'rtrY'

Start/restart collector on port '9002' for (rtr2)[pid]
```
~~~~~~

Start/restart collector on port '9996' for (gw)[pid]

Restart nfsend:[pid]
~~~~~~
~~~~~~