Monitoring Netflow with NFsen

Network Monitoring and Management

Introduction

Goals

- Learn how to install the Nfsen family of 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-NfSen.txt 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 \
nfdump libmailtools-perl php5 bison flex
```

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

If prompted to “Make /etc/mrtg.cfg owned by and readable only by root?” select “” and press ENTER to continue.

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:

```
%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
```

Press ENTER when prompted for the path to Perl.

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! :-)).