Monitoring Netflow with NFsen

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. "rtrX>" or "mysql>") imply that you are executing commands on remote equipment, or within another program.

Export flows from a Cisco router

This is an example for doing this from the **Campus X** border router, r1-bdr-campusX, to the PC named pc1-campusX.ws.nsrc.org. In each of your groups 1 to 6 you must choose one person to type in the commands to set up your border router for Netflow and the management server where the Netflow exports will go. IOS can send Netflow messages to up to 2 devices, but we will use only 1 for now.

Login to the border router:

```
$ telnet r1-bdr-campusX
Username: cndlab
Password:
Router1>enable
Password:
```

Enter the enable password…

Configure FastEthernet0/1 to generate netflow. Substitute X with your group number and Y with one PC and Z with another PC in your group.

```
r1-bdr-campusX# configure terminal
r1-bdr-campusX(config)# interface FastEthernet 0/1
r1-bdr-campusX(config-if)# ip flow ingress
r1-bdr-campusX(config-if)# ip flow egress
r1-bdr-campusX(config-if)# exit
r1-bdr-campusX(config)# ip flow-export destination 100.68.X.130 9996
r1-bdr-campusX(config)# ip flow-export version 5
r1-bdr-campusX(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.

```
r1-bdr-campusX(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:

```
r1-bdr-campusX(config)#ip flow-top-talkers
r1-bdr-campusX(config-flow-top-talkers)#top 20
r1-bdr-campusX(config-flow-top-talkers)#sort-by bytes
r1-bdr-campusX(config-flow-top-talkers)#end
```

Now we'll verify what we've done.

```
r1-bdr-campusX# show ip flow export
r1-bdr-campusX# show ip cache flow
```

See your “top talkers” across your router interfaces

```
r1-bdr-campusX# show ip flow top-talkers
```

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

```
r1-bdr-campusX#wr mem
```

You can exit from the router now:

```
r1-bdr-campusX#exit
```

We are now exporting NetFlow data from your router to your management server. You can verify that these flows are arriving by logging in on this PC and typing:

```
sudo tcpdump -v -n -i eth1 udp port 9996
```

And this will show you the flows from your border router.

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 wget
```

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

Installing and setting up NfSen

The instructors will have already downloaded a copy of the nfsen archive to the local workshop webserver. We will take that copy, rather than downloading from the Internet.

```
$ cd /usr/local/src
$ sudo -s
# wget http://www.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://www.ws.nsrc.org/downloads/nfsen-socket6.patch
# patch -p0 < nfsen-socket6.patch
# cd etc
# cp nfsen-dist.conf nfsen.conf
# editor nfsen.conf
```

The last command above will start your editor; edit the nfsend.conf file to do the following:

Set the $BASEDIR variable:

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

Adjust the tools path to where items actually reside:

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

Set HTMLDIR to work with Apache on Ubuntu 14.04

```
$HTMLDIR="/var/www/html/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:

```
# 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).
```

```
%sources=(
'r1-bdr-campusX' => {'port'=>'9996','col'=>'#ff0000','type'=>'netflow'},
```

```
);
```

Now save and exit from the file.

Create the netflow user on the system

```
# useradd -d /var/netflow -G www-data -m -s /bin/false netflow
```

STOP Being ROOT

```
# exit
$
```

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:

Make sure you have PHP installed:

```
$ sudo apt-get install php5
```

Verify that flows are arriving

Assuming that you are exporting flows from a router to your collector box on port 9996 you can check for arriving data using tcpdump:

```
sudo tcpdump -v -n -i eth1 udp port 9996
```

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
```

Looking at the web page

You can find the nfsen page here:

```
http://pc1-campusX.ws.nsrc.org/nfsen/nfsen.php
```

Optional Tasks

If you wanted to add more sources...

Go back to where you extracted your nfsen distribution:

```
$ cd /usr/local/src/nfsen-1.3.6p1
$ EDITOR etc/nfsen.conf
```

Update your sources for new items that you might have. (Sample only! We are not configured to do this in our classroom.)

```
%sources = (
'rtrX' => {'port' => '9996', 'col' => '#e4e4e4' },
'rtr2' => {'port' => '9002', 'col' => '#0000ff' },
'rtr3' => {'port' => '9003', 'col' => '#00cc00' },
'rtr4' => {'port' => '9004', 'col' => '#000000' },
'rtr5' => {'port' => '9005', 'col' => '#ff0000' },
'rtr6' => {'port' => '9006', 'col' => '#ffff00' },
);
```

Save and exit from the nfsen.conf file“. Remember, you've updated nfsen.conf so you must re-run the install script:

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

Now start and stop nfsen:

```
$ sudo service nfsen stop
$ sudo service nfsen start
```

That's it!

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!).