% 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. And, if you chose pc1 to receive flows from router 1 (rtr1), then it should, also, receive flows from router 2 (rtr2):

These exercises work on the example of doing the following:

```
Group 1, Router 1
-----------------
rtr1 ==> pc1 on port 9001
rtr1 ==> pc5 on port 9002

Group 2, Router 2
-----------------
rtr2 ==> pc5 on port 9001
rtr2 ==> pc1 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@rtr1.ws.nsrc.org
rtr1.ws.nsrc.org> enable
```
~~~~~~

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

or, if ssh is not configured yet:

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

Remember - This is an EXAMPLE for the following situation:

```
rtr1 ==> pc1 on port 9001
rtr1 ==> pc5 on port 9002
```

Group 2, 3, 4, 5, 6, 7, 8 and 9 will do something different.

The following configures the FastEthernet 0/0 interface to export flows.

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
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 retained 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
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Wait a few seconds and you should see something that looks like:

```
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
13:01:19.027039 IP (tos 0x0, ttl 255, id 1407, offset 0, flags [none], proto UDP (17), length 58
    rtr1.ws.nsrc.org.64190 > pc1.ws.nsrc.org.9001: UDP, length 552
```

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

Update, start and automate the NfSen Software

NfSen is a graphical web based front end for the nfdump netflow tools. On
your virtual machines both nfdump and NfSen have already been largely
installed, but still need some specific configuration before they can be
run.

For details on installing these tools you can refer to the install guide
linked in the workshop agenda pages.

Update NfSen for the devices that are sending you flows:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
cd /var/nfsen/etc/
sudo editor nfsen.conf
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Find the %sources definition, and change it to match the routers sending you flows. Change rtrA to be your group's router number and rtrB to be the neighbor router sending you flow information (for example, "rtr1" and "rtr2" for Group 1):

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

Now save and exit from the file.

Reconfigure NfSen.

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

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

You should see:

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

Add source 'rtrB'

Reconfig done!

You may have to restart NFsen
```

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ sudo /etc/init.d/nfsen stop
§ sudo /etc/init.d/nfsen start
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

View flows via the web:

You can find the nfsen page here:

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

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! :-)).