Network Monitoring and Management

## Configure Your Router to Export Flows

1. Export flows from a router

This is a sample for doing this from the Group 1 router, rtr1.ws.nsrc.org to the PC named pc1.ws.nsrc.org or 10.10.1.1. In each of your groups 1 through 9 you must choose one person to type in the commands to set up router for Netflow and one PC where the Netflow exports will go. IOS can unfortunately not send Netflow messages to more than 1 or 2 devices, so we will use only 1 now.

For example, if our router is rtr1, or 10.10.1.254 (Group 1 gateway):

Log in on the router:

```
# ssh cisco@10.10.1.254
rtr1.ws.nsrc.org> enable
```

Enter the enable password...

Configure FastExthernet 0/0 to generate netflow:

```
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 9996
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 persisted 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
```

and on the machine where flows are being exported to you can verify that they are arriving by doing (as root):

```
        # tcpdump -v udp port 9996
```

In addition (_PLEASE NOTE_) we are re-exporting NetFlow data from the gateway router to all the PCs in the classroom. You can verify that these flows are arriving by typing:

```
        # tcpdump -v udp port 9009
```

For the exercises we'll assume you are on a PC where flows are only arriving from the gateway router and we'll use the 9009 port.

## Configure Your Collector

1. Install NFdump
   NFdump is the Netflow flow collector

   We install several additional packages that we will need a bit later:

Only install these if you did not already install mrtg and rrdtool:

```
   # apt-get install rrdtool
   # apt-get install librrds-perl
   # apt-get install librrdp-perl
   # apt-get install mrtg
   # apt-get install libmailtools-perl
```

If mrtg and rrdtool are already installed, then you just need these:

```
   # apt-get install librrd-dev
   # apt-get install nfdump
   # apt-get install libmailtools-perl
```

Or, on a single line:

```
   # apt-get install rrdtool mrtg librrds-perl librrdp-perl librrd-dev nfdump \
                libmailtools-perl
```

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

2. Installing and Setting up NfSen (logged in as root)

```
   # cd /usr/local/src
   # wget http://noc.ws.nsrc.org/downloads/nfsen-1.3.5.tar.gz
   # tar xvzf nfsen-1.3.5.tar.gz
   # cd nfsen-1.3.5
```

```
   # 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'
```

Adjust the tools path to where items actually reside:

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

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=(
   'rtrX'=>{'port'=>'9996','col'=>'#ff0000','type'=>'netflow'},
     'gw'=>{'port'=>'9009','col'=>'#0000ff','type'=>'netflow'},
   );
```

Now save and exit from the file.

3. Create the netflow user on the system

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

4. 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-1.3.5
```

Now, finally, we install:

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

Start NfSen

```
cd /var/nfsen/bin
./nfsen start
```

5. View flows via the web:

   This should not be necessary, but just in case:

```
   # apt-get install php5
```

You can find the nfsen output here:

   http://pcN.ws.nsrc.org/nfsen/nfsen.php

(Below is only if there are problems)

Note that in /usr/local/src/nfsen-1.3.5/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


6. Verify that flows are arriving

Assuming that you are exporting flows from a router, or routers, to
your collector box on port 9009 you can check for arriving data using
tcpdump:

   # tcpdump -v udp port 9009
   # tcpdump -v udp port 9996

OPTIONAL


7. Installing the PortTracker plugin (Optional or as reference)

```
# apt-get install bison flex
# cd /usr/local/src
# wget http://noc.ws.nsrc.org/downloads/nfdump-1.6.3p1.tar.gz
# tar xvzf nfdump-1.6.3p1.tar.gz
# cd nfdump-1.6.3p1
# ./configure
# make
```

- Go the PortTracker directory in the nfsen source distribution:

   # cd /usr/local/src/nfsen-1.3.5/contrib/PortTracker

   # editor do_compile

      # path of nfdump sources
      NFDUMP="/usr/local/src/nfdump-1.6.3p1"

      # path of rrd include file rrd.h
      RRDINCLUDE=/usr/include

      # path of rrd library
      LIBRRD=/usr/lib

- Compile nftrack:

```
   # ./do_compile

...

   # cp nftrack /usr/bin/

- Make a directory for the nftrack data

   # mkdir -p /var/log/netflow/porttracker
   # chown www-data /var/log/netflow/porttracker

- Set the nftrack data directory in the PortTracker.pm module:

   # editor PortTracker.pm

    Find the line:

                my $PORTSDBDIR = "/data/ports-db";

        and change it to:

        my $PORTSDBDIR = "/var/log/netflow/porttracker";

    ...

- Install the plugins into the NFSen distribution

   # cp PortTracker.pm /var/nfsen/plugins/
   # cp PortTracker.php /var/www/nfsen/plugins/

- Add the plugin definition to the nfsen.conf configuration

   # cd /usr/local/src/nfsen-1.3.5
   # editor etc/nfsen.conf

    Find the plugins section and make it look like this:

       @plugins = (
           [ 'live',   'PortTracker'],
       );

    ...

- Re-run the installation (answer questions)

   # perl install.pl etc/nfsen.conf

- Initialize portracker database files

   # sudo -u www-data nftrack -I -d /var/log/netflow/porttracker

    (This can take a LONG time! - 8 GB worth of files will be created)

- Set the permissions so the netflow user running nfsen, and the www-data
  user running the Web interface, can access the porttracker data:

   # chown -R netflow:www-data /var/log/netflow/porttracker
   # chmod -R 775 /var/log/netflow/porttracker
```

- Reload:

```
   # /var/nfsen/bin/nfsen reload
```

- Check for success:

```
   # grep -i 'porttracker.*success' /var/log/syslog
Nov 27 02:46:13 noc nfsen[17312]: Loading plugin 'PortTracker': Success
Nov 27 02:46:13 noc nfsen[17312]: Initializing plugin 'PortTracker': Success
```

- Wait some minutes, and go the the nfsen GUI

```
    http://pcN.ws.nsrc.org/nfsen/nfsen.php
```

... and select the Plugins tab.

If you get an error "Cannot Read Stats file", check the /var/log/netflow/porttracker directory for 2 additional files: portstat24.txt and portstat.txt like this:

```
        # ls -l /var/log/netflow/porttracker/portstat*
        -rw-r--r-- 1 netflow www-data     677 2011-11-17 14:30 /var/log/netflow/
porttracker/portstat24.txt
        -rwxrwxr-x 1 netflow www-data     638 2011-11-17 14:30 /var/log/netflow/
porttracker/portstat.txt
```

8. If you wanted to add more sources...

Go back to where you extracted your nfsen distribution.

```
   # cd /usr/local/src/nfsen-1.3.5
   # editor etc/nfsen.conf
```

Update your sources for new items that you might have.
(Sample only!)

```
        %sources = (
        'rtr' => {'port' => '9000', 'col' => 'e4e4e4' },
        'rtr2' => { 'port' => '9001', 'col' => '#0000ff' },
        'rtr3' => { 'port' => '9002','col' => '#00cc00' },
        'rtr4' => { 'port' => '9003','col' => '#000000' },
        'rtr5' => { 'port' => '9004','col' => '#ff0000' },
        'rtr6' => { 'port' => '9005','col' => '#ffff00' },
        );
```

Save and exit from the nfsend.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:

```
   # /var/nfsen/bin/nfsen stop
   # /var/nfsen/bin/nfsen start
```

You can add the nfsen startup script to /etc/init.d/rc.local
or somewhere similar to start it at bootup.)