Installing Flow-Tools, Flow - Scan and RRDTool

based on Net-flow Howto (http://www.linuxgeek.org/netflow-howto.php)

Software Packages needed

"**Apache**- the web server

"**Perl5**

"**RRDTool**

```
"tar -zxvf rrdtool-1.0.45.tar.gz
"cd rrdtool-1.0.45
"./configure --enable-shared --prefix=/usr/local/rrdtool
"make install site-perl-install
```

"**flow-tools**

```
"tar -zxvf flow-tools-0.66.tar.gz
"cd flow-tools-0.66
"./configure
"make
"make install
```

This will install flow-tools to /usr/local/netflow.

"**Perl Modules**- In addition to Perl5, you will need the modules listed below.

Net::Patricia
Boulder::Stream
HTML::Table
ConfigReader::DirectiveStyle
Cflow

Download each of these from the lab server, and run the following

```
# perl Makefile.PL

# make

# make install
```

In case of ConfigReader, just copy the unzipped file to /usr/lib/perl5/site_perl/5.8.3/ConfigReader/

CFlow is included in the current flow-tools distribution so you do not need to download it separately. Please install it by doing the following:

```
"cd flow-tools-0.66
"cd contrib
"tar -zxvf Cflow-1.051.tar.gz
"cd Cflow-1.051
"perl Makefile.PL
"make
"make install
```

"**FlowScan**- This is the report generating application by Dave Plonka.

"**CUFlow**- This is the report module and graph generator written by Columbia University for FlowScan.

"**Support Files** - This includes the scripts and the updated FlowScan.pm module that are needed to complete the installation using this document.

Router Configuration

Global Mode

```
ip cef
ip flow-export version 5 peer-as
ip flow-export source interface fa0/1
ip flow-export destination 10.1.0.1  1001
ip flow-cache timeout active 1
```

Interface Configuration

```
ip route-cache flow
```

Unix PATH Variables

Make sure that your Netflow and RRDTools executables are in the PATH.

```
# echo $PATH
```

Add it to /etc/profile,

```
        if [ `id -u` = 0 ]; then
        pathmunge /sbin
        pathmunge /usr/sbin
        pathmunge /usr/local/sbin
        pathmunge /usr/local/rrdtool/bin
        pathmunge /usr/local/netflow/bin
        fi
```

or link the executables to /usr/local/bin

Flow-tools Configuration

Flow-tools don't need further configuration, if you are happy running it from the command line. But to be able to view graphs, few things needs to be added.

First create the approriate directories

```
#mkdir -p /var/netflow/
#mkdir -p /var/netflow/ft
#mkdir -p /var/netflow/rrds
#mkdir -p /var/netflow/scoreboard
```

Now copy the file 'linkme' from the support files to "/usr/local/netflow/bin/". The linkme file links the current flow capture file to flow-scan process later.

Start flow-capture

```
#/usr/local/netflow/bin/flow-capture -w /var/netflow/ft 0/0/2055 -S5 -V5 -E1G -n 287 -N 0 -R /
usr/local/netflow/bin/linkme
```

You can use the "flow-capture-init" file provided in the support files.

Configuring Flow-Scan

Since flow-tools will not process the raw flows, we will need additional tools to view the processed graphs. Download the file from the local server. And run the following commands

```
./configure --prefix=/var/netflow
make
make -n install
make install
cd cf
cp flowscan.cf /var/netflow/bin
cp CampusIO.cf /var/netflow/bin
cp SubNetIO.cf /var/netflow/bin
```

Now, replace the flowscan.pm file in the /var/netflow/bin, with the one provided with the support files.

Installaing CUFlow

We are using an additional graphing class. You can also use the already included with flow-tools, which are campusIO and subnetIO.

Download and untar CUFlow

copy CUFlow.pm and CUFlow.cf to /var/netflow/bin/

Edit the CUFlow.cf file in the /var/netflow/bin directory.

```
Subnet 10.1.0.0/20
Network 10.1.0.0/24 routers
OutputDir /var/netflow/rrds
Scoreboard 10 /var/netflow/scoreboard /var/www/html/flows/topten.html
Router 10.1.0.254 router1
```

Enabling Flow-Scan to work with CUFlow

Edit the /var/netflow/bin/flowscan.cf file to read the follows

```
FlowFileGlob /var/netflow/ft-v05*[0-9]
#ReportClasses CampusIO
ReportClasses CUFlow
```

Starting Flow-scan

use the “flowscan-init” file provided with the support files to start flow-scan.

Do a “tail -f /var/log/flowscan” to see if your flow-scan is working properly.

Web Interface

CUGrapher comes with a perl file that will provide an front end for viewing graphs.

Copy the CUGrapher.pl file to /var/www/cgi-bin/

Edit the CUGRapher.pl file to match the rrd file directory

```
my $rrddir = "/var/netflow/rrds";
```

You should now be able to generate graphs from the flow data.
