intERLab AIT March 2008
Network Management Workshop
NFSen Lab Documents

NFdump
[Nfdump is the netflow flow collector]

1. Now install nfdump

apt-get install nfdump

Installed tools are :
nfcapd nfdump nfreplay nfexpire nftest nfgen

NFSen

1. Now get nfsen

$ wget http://superb-west.dl.sourceforge.net/sourceforge/nfsen/nfsen-1.2.4.tar.gz

2. Setting up NfSen

$ tar -xzf nfsen-1.2.4.tar.gz
$ cd nfsen-1.2.4
$ cd etc

Edit the nfsen-dist.conf:

- set the basedir variable

$BASEDIR = "/var/nfsen";

- set the users:

$USER = "netflow"
$WWWUSER = 'www-data'
$WWWGROUP = 'www-data'

- add sources:

%sources = (

'bbgw' => { 'port' => '2005', 'col' => '#0000ff' },
);

//// 'ident' => { 'port' => '<portnum>', 'col' => '<colour>' }

- set the path for the PREFIX where to find the nfdump tools:

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

- set the buffer size to something small, so we see data quickly
-

Receive buffer size for nfcapd - see man page nfcapd(1)
$BUFFLEN = 2000;

save and exit

3. Create a netflow user on the system.

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

4. Initiating nfsen

cp nfsen-dist.conf nfsen.conf
cd ..

perl install.pl etc/nfsen.conf

[press 'yes' to the perl promt']

5. Starting Nfsen

cd /var/nfsen/bin
./nfsen.rc start

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

Watch your browser at http://localhost/nfsen/nfsen.php

Thank you.