% Monitoring Netflow with NFsen
%
% Network Monitoring and Management

Introduction

Goals

* Build the nfdump package from source

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.

We will use the latest definition from Ubuntu's launchpad site:

- Add this line to the file /etc/apt/sources.list:

~~~~~~
deb-src http://apt.ws.nsrc.org:3142/archive.ubuntu.com/ubuntu precise main restricted universe m
~~~~~~

Then:

$ sudo apt-get update

To build the packages, we'll need the following files:

~~~~~~
https://launchpad.net/ubuntu/+archive/primary/+files/nfdump_1.6.6-1.debian.tar.gz
https://launchpad.net/ubuntu/+archive/primary/+files/nfdump_1.6.6.orig.tar.gz
https://launchpad.net/ubuntu/+archive/primary/+files/nfdump_1.6.6-1.dsc
~~~~~~

They have already been downloaded for you to:

~~~~~~
http://noc.ws.nsrc.org/downloads/nfdump_1.6.6-1.debian.tar.gz
http://noc.ws.nsrc.org/downloads/nfdump_1.6.6.orig.tar.gz
http://noc.ws.nsrc.org/downloads/nfdump_1.6.6-1.dsc
~~~~~~

So let's get them from the NOC:

~~~~~~
cd /tmp/
wget http://noc.ws.nsrc.org/downloads/nfdump_1.6.6-1.debian.tar.gz
wget http://noc.ws.nsrc.org/downloads/nfdump_1.6.6.orig.tar.gz
wget http://noc.ws.nsrc.org/downloads/nfdump_1.6.6-1.dsc
~~~~~~

Extract the source:

~~~~~~
sudo dpkg-source -x --no-check nfdump_1.6.6-1.dsc

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

Install prerequisites:

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
sudo apt-get build-dep nfdump
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

One more package is required for building:

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
sudo apt-get install flow-tools-dev
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Build the tool:

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
cd nfdump-1.6.6
sudo dpkg-buildpackage -rfakeroot -b
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

The package is now built in the "proper" way, let's install it:

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
cd ..
ls -l nfdump*.deb
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Installation:

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
sudo dpkg --install nfdump_1.6.6-1_i386.deb
sudo dpkg --install nfdump-flow-tools_1.6.6-1_i386.deb
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```