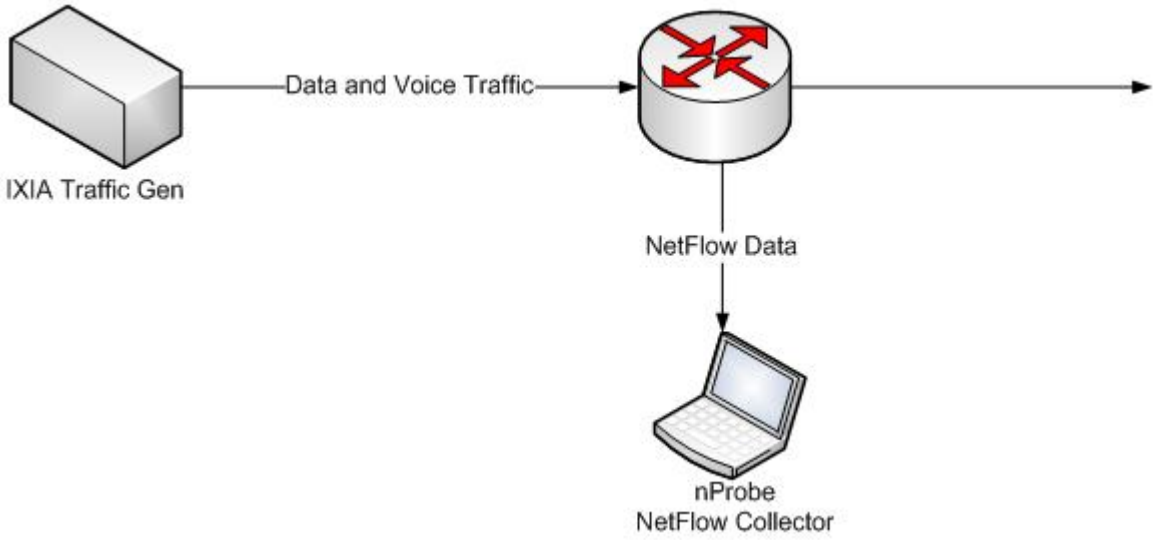
NetFlow Data Collection using nTop and nProbe

Kyurim Rhee

Sept-22-2010

Purpose:
To collect NetFlow data using nTop and nProbe NetFlow probe.

Lab Setup
We have set up a voice and data traffic generated by IXIA traffic generator which the traffic was passed through a designated router. The router was configured to send NetFlow data to my PC which collected the NetFlow data using nProbe. Below is a diagram of our lab layout.



Running the nProbe:

First nProbe must be initiated:

```
nProbe shut down

C:\Program Files\nProbe-Win32>nprobe /c -h
Running nProbe for Win32.

Welcome to nprobe v.5.8.1 ($Revision: 1659 $) for Win32

Built on 08/09/10 08:49:49
Copyright 2002-10 by Luca Deri <deri@ntop.org>

Usage:
nprobe -n <host:port|none> [-i <interface|dump file>] [-t <lifetime timeout>]
             [-d <idle timeout>] [-l <queue timeout>] [-s <scan cycle>] [-N]
             [-p <aggregation>] [-f <filter>] [-a] [-b <level>]
             [-P <path>] [-F <dump timeout>] [-D <format>]
             [-u <in dev idx>] [-O <out dev idx>]
```

Install nProbe service and have it collect the NetFlow data at a given directory on your local machine:

```
C:\Program Files\nProbe-Win32>nprobe /I nprobe -i1 -Dt -Pc:/fastbit -csv-sepa
CreateService failed - The specified service already exists. (0x431)

C:\Program Files\nProbe-Win32>
C:\Program Files\nProbe-Win32>nprobe /I nprobe -i1 -Dt -Pc:/fastbit -csv-separat
or
C:\Program Files\nProbe-Win32>
C:\Program Files\nProbe-Win32>
C:\Program Files\nProbe-Win32>nprobe /r nprobe
Stopping nprobe.
nprobe stopped.
nprobe removed.

C:\Program Files\nProbe-Win32>nprobe /i nprobe -i0:2055 -3 -Pc:\flow
nprobe installed.

C:\Program Files\nProbe-Win32>nprobe /r nprobe
nprobe removed.

C:\Program Files\nProbe-Win32>nprobe /i nprobe -i0:2055 -3 -Pc:\flows
nprobe installed.

C:\Program Files\nProbe-Win32>nprobe /r my_nprobe
my_nprobe removed.

C:\Program Files\nProbe-Win32>nprobe /r nprobe
Stopping nprobe.
nprobe stopped.
nprobe removed.

C:\Program Files\nProbe-Win32>nprobe /i nprobe -3 2055 -Pc:\flows
nprobe installed.

C:\Program Files\nProbe-Win32>_
```

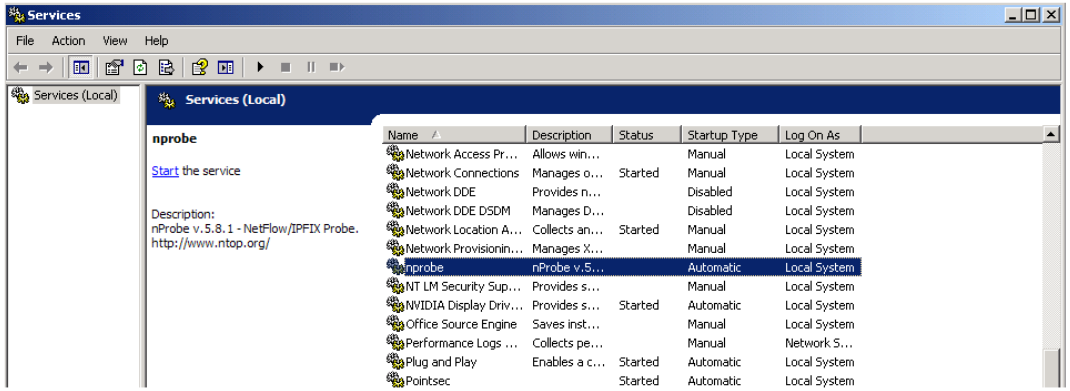
Didn't Work

Remove nProbe

Install nProbe at C:\flows

Start the nProbe service:

go to Windows Control Panel-->Administrative -->Tools--> Services--> and manually Start/Stop Services



NetFlow Data Format

We were successful in collecting the NetFlow data. The data is delimited with " | " and contain the following parameters:

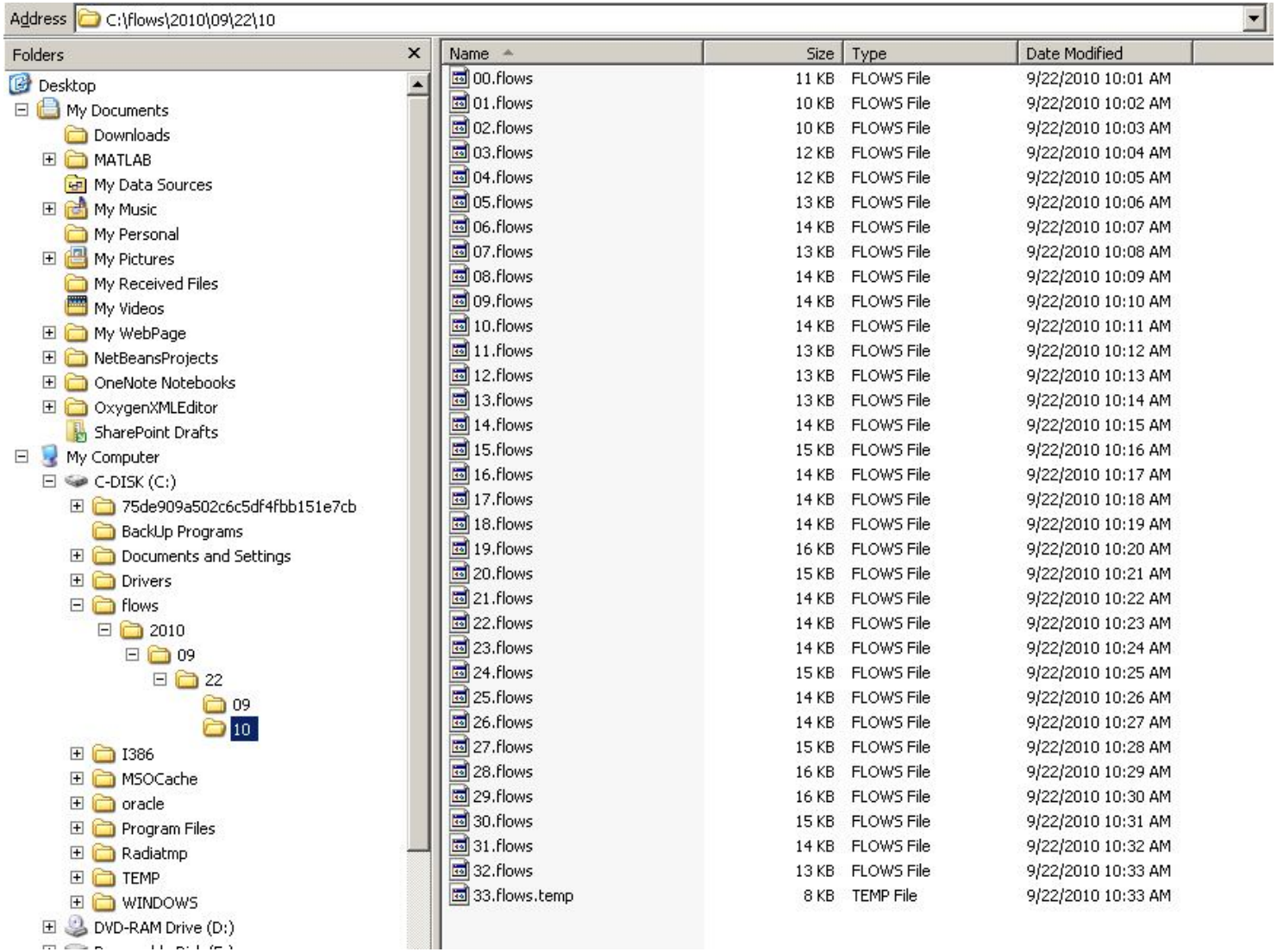
```
IPV4_SRC_ADDR|IPV4_DST_ADDR|IPV4_NEXT_HOP|INPUT_SNMP|OUTPUT_SNMP|IN_PKTS|IN_BYTES|FIRST_SWITCHED|LAST_SWITCHED|L4_SRC_PORT|L4_DST_PORT|TCP_FLAGS|PROTOCOL|SRC_TOS|SRC_AS|DST_AS|IPV4_SRC_MASK|IPV4_DST_MASK
192.168.1.109|192.168.1.13 |0            |147       |0          |1      |76      |1285164039    |1285164215   |123        |123        |16       |17      |16     |0     |0     |0            |0
```

IPV4_SRC_ADDR	Source IP Address
IPV4_DST_ADDR	Destination IP Address
IPV_NEXT_HOP	
INPUT_SNMP	
OUTPUT_SNMP	
IN_PKTS	Total Number of Packets received in this time frame
IN_BYTES	Total Number of Bytes received in this time frame
FIRST_SWITCHED	Start Time stamp
LAST_SWITCHED	Stop Time stamp
L4_SRC_PORT	Layer4 Source Port number
L4_DST_PORT	Layer4 Destination Port Number
TCP_FLAGS	Check Chart
PROTOCOL	Check Chart
SRC_TOS	Check Chart
SRC_AS	Source Autonomous System
DST_AS	Destination Autonomous System
IPV4_SRC_MASK	
IPV4_DST_MASK	

Collection Interval

This NetFlow data is collected in every 1 minute interval. nProbe will collect the NetFlow data and organize it by creating directories in "Year/Month/Date/Hour" manner.

The following is a snapshot of 33 minutes of NetFlow data gathered on 2010-09-22 between 10:00AM - 10:33AM.



For more information on nTop & nProbe, visit:

http://www.ntop.org/news.php