f

nm_rc

a Remote Console for NeTraMet

Version 4.1

Nevil Brownlee

Information Technology Systems & Services
The University of Auckland
Auckland, New Zealand

November 1997

1. Introduction

nm_rc is a simple 'remote console' program for NeTraMet. It combines NeMaC and fd_filter with a display formatter so as to produce - every sss seconds - an easily-understood listing of the 'busiest nnn' flows observed by a NeTraMet meter.

There are many possible uses for nm_rc, including the following ..

Regular display of traffic flows from a meter.

For example, if you have a meter on your gateway network, it could be controlled by NeMaC, which would download its rule file (and perhaps an emergency rule file) and then collect its traffic flow data at regular intervals, say every 15 minutes. You could also run nm_rc to display the 5 busiest flows every 20 seconds, using the meter's current rule file, but perhaps specifying a different set of attributes to be displayed. This would provide a simple way to keep an eye on your gateway traffic without interfering with the normal flow data collections.

Developing new rule files

Using nm_rc to download rule files to a test meter simplifies the development environment. To do this without nm_rc, you started NeMaC as a background job then looked at the flow data file it produced. Now you can run nm_rc as a foreground job and see the resulting flow data directly.

2. Starting nm_rc

nm_rc takes command line options, many of which are identical to those used by NeMaC. They are:

-a sss Specifies number of seconds collections are to lag after their 'synchronised' time (see -u below for more details).

-c sss Secified required collection interval in seconds.

-g sss Specifies meter's garbage collection interval in seconds.

-h pp Sets meter's HighWaterMark as a percentage.

-i sss Sets meter's InactivityTimeout in seconds.

-m pppp Specifies the UDP port to use for communication with the NeTraMet meter. By default this is port 161 (SNMP).

-n nnn Specifies number of flows to display after each collection; default is 10, i.e. nm_rc displays the 'top ten' flows.

-o pp Sets meter's FloodMark as a percentage.

-p 'Plain' output; output will be in the same format as used for NeMaC's flow data files.

-r rulefile Gives the name of the rule file to be downloaded to the meter. A rule file name ***must*** be specified. nm_rc will only monitor one meter.

-u Specifies that samples should be unsynchronised; samples are taken on startup, then at the end of each collection interval (-c seconds). By default samples after the first are synchronised, i.e. taken at times which are a multiple of the collection interval.

Following the options, the name of a meter and its write SNMP community should appear on the command line.

From version 4.1, the NeTraMet meter is able to run more than one rule set at the same time. For example, you can run an 'nm_rc' rule set while another 'daily logging' rule set continues to run normally. The meter uses 'Owner Names' to help distinguish its rule sets. You can specify an Owner Name for nm_rc by specifying it on the command line, after the write community name, e.g.

```
    nm_rc -c30 -r rules.x_ip 130.216.234.237 test Net-Ops
```

The Owner Name is an alphameric string with a maximum length of 16 characters. It may contain any characters except a blank. In the example above we used `Net-Ops` for nm_rc's Owner Name. If an Owner Name is not specified, 'nm_rc' is used.

The above command would cause nm_rc to begin analysing flow data from meter 130.216.234.237 with write SNMP community 'test'. The rule file 'rules.x_ip' would be read and downloaded to the meter, and that meter's flow data would be collected every 30 seconds and displayed.

When nm_rc execution terminates normally (by interrupting nm_rc using the Control-C key), nm_rc will stop its rule set from executing, and delete it from the meter. This leaves the meter continuing to run its other rule sets, with no trace remaining of nm_rc's rule sets or the flows it measured.

If two users wish to run nm_rc at the same time, they need to agree to use different Owner Names, otherwise both might use 'nm_rc' by default, which is bound to cause confusion!

3. Specifying which attributes to display

The list of attributes displayed by nm_rc is specified by a format statement in a rule file, exactly as it would be for NeMaC.

In versions 2 and 3 of nm_rc you could run nm_rc without specifying a rule file; this allowed you to observe whatever rule set was running on the meter. From version 4.1 you must specify a rule file; nm_rc downloads this and displays the traffic it observes.

If the rule file does not have a format statement, nm_rc will provide a default one which displays source/destination peer and transport addresses as well as packet and byte rates.

The format being used is always displayed when nm_rc starts up.

4. Displayed form of the attributes

If the 'plain' option is set (-p), attributes are displayed exactly as they would appear in a NeMaC flow data file.

Note that nm_rc's PDU and Octet counts are the numbers of PDUs and bytes counted for a flow since the last sample. They are the values fd_filter would have produced from a flow data file; in an fd_filter file they would have been 'rate' attribute values.

Other attributes are displayed as follows:

Addresses	Always appear the same as in NeMaC
FirstTime	Integer+unit, e.g. 3s, 4m, 5h, 5d. The time displayed is the difference between LastTime and FirstTime, i.e. it is the lifetime of the flow
LastTime	Integer. As in NeMaC this is the meter's SysUptime value (centiseconds) when the last packet was seen
SourcePeerType, DestPeerType	3-char string, e.g. 'ip ', 'ipx'
ToPDUs, FromPDUs	Integer+suffix, e.g. 3, 4k, 5M, 6G
ToOctets, FromOctets	Integer+suffix+B, e.g. 3B, 4kB, 5MB, 6GB
SourceTransType, DestTransType	3-char string, e.g. 'udp', 'tcp'
SourceTransAddress, DestTransAddress	String for well-known ports (e.g. telnet, www), integer otherwise

5. Form of nm_rc display

When you start nm_rc it prints a few lines of information, exactly the same as NeMaC does. These are an identifying line (including the nm_rc version number), the MIB file being used, and a summary of the rule file (if there was one).

The next line displayed is a `#Format` line, showing which attributes have been requested and how they are to be set out on each output line.

After that nm_rc displays a `#---` line when it collects each set of flow data, followed by the top n flows specified by the -n option).

The #--- line shows which meter and interface nm_rc is monitoring, how many flows were active, the total packet and byte rates for the sample, and the sample collection time.

Every flow line begins with a percentage, which shows how much the flow contributed to the total traffic.

6. Example output from nm_rc

The following outputs were collected from meter 130.216.4.32 using rule files from NeTraMet's examples/ directory. The meter parameters are set as follows:

-i10 InactivityTimeout: flows may be recovered 10 seconds after they've been collected

-h20 HighwaterMark: the meter should intensify its garbage collection efforts when more than 20% of its flows are in use

-g11 The meter should search for recoverable flows every 11 seconds

The last three parameters were set like this so as to force idle flows to be recovered quickly. This allows one to get an idea of the flow lifetimes by displaying the FirstTime attribute.

Note that the first sample in each run has some flows left over from the last rule file; these are idle after the first sample and wil be recovered by the garbage collector.

Note also that IPX peer addresses in these listings show all ten bytes of the Novell addresses. The first four bytes are the host's Novell network number, the last six are its MAC address. To produce this the meter and nm_rc were rebuilt with the FULL_IPX option set on; the default (in the release files) is to have FULL_IPX off, producing only four-byte network numbers.

rules.rc.pr+bc - traffic by protocol, showing broadcast flows in detail.

Broadcast flows have FlowClass set to 1. 10-second samples

```
manager> ./nm_rc -c10 -i10 -h20 -g11 -rrules.rc.pr+bc 130.216.4.32 passwd
nm_rc: Remote Console for NeTraMet: V3.3
Using MIB file: /dept/ccc/nevil/au-snmp/mib/mib.txt
Meter 130.216.4.32: set 4 sizes set to 13 rules + 1 counts
Rule 10 added to table 4
Meter 130.216.4.32: using rule set 4
#Format: sourcepeertype  topdus  tooctets  flowclass  sourcepeeraddress
#---  130.216.4.32 eth0  9 flows   4kpps 829kBps  10:56:22 Mon  6 Nov 95  ---
 81%  ipx   21k    7MB  0  0.0.0.0.0.0.0.0.0.0
 12%  ip     9k    1MB  0  0.0.0.0
  2%  at     3k  227kB  0  0.0.0
  2%  oth    2k  207kB  0  00-00
  0%  ipx    91   34kB  0  0.0.0.0.0.0.0.0.0.0
  0%  ip     57    5kB  0  0.0.0.0
  0%  dec    27    2kB  0  0.0.0
  0%  oth    10   610B  0  00-00
  0%  ipx     1    64B  1  130.216.0.31.0.0.0.0.0.0
#---  130.216.4.32 eth0  38 flows  347pps 103kBps  10:56:30 Mon  6 Nov 95  ---
 90%  ipx    2k  925kB  0  0.0.0.0.0.0.0.0.0.0
  6%  ip    604   69kB  0  0.0.0.0
  1%  at    206   16kB  0  0.0.0
  0%  oth   120    9kB  0  00-00
  0%  at      3   861B  1  0.134.0
  0%  oth     9   809B  1  00-00
  0%  ipx     6   752B  1  130.216.0.31.0.0.0.0.0.0
  0%  ip      2   684B  1  130.216.122.0
  0%  oth    10   612B  1  00-00
  0%  oth     4   512B  1  60-07
#---  130.216.4.32 eth0  55 flows  419pps 127kBps  10:56:40 Mon  6 Nov 95  ---
 84%  ipx    3k    1MB  0  0.0.0.0.0.0.0.0.0.0
```

```
  7%  ip    917  100kB  0  0.0.0.0
  2%  ipx    52   26kB  1  130.216.2.3.0.0.0.0.0.0
  1%  ipx    52   25kB  1  130.216.0.31.0.0.0.0.0.0
  1%  at    243   19kB  0  0.0.0
  0%  oth    92    6kB  0  00-00
  0%  ipx     8    3kB  1  130.216.0.23.0.0.0.0.0.0
  0%  ip      4    2kB  1  130.216.3.0
  0%  oth     7    1kB  1  00-00
  0%  at      3   861B  1  0.134.0
#---  130.216.4.32 eth0  60 flows  198pps  21kBps  10:56:50 Mon  6 Nov 95  ---
 44%  ip    827   95kB  0  0.0.0.0
 36%  ipx   715   78kB  0  0.0.0.0.0.0.0.0.0.0
  8%  at    238   18kB  0  0.0.0
  2%  oth    93    5kB  0  00-00
  1%  ip      6    3kB  1  130.216.4.0
  0%  ipx     7    1kB  1  130.216.0.31.0.0.0.0.0.0
  0%  ip      7    1kB  1  130.216.99.0
  0%  ip      3    1kB  1  130.216.122.0
  0%  oth     7    1kB  1  00-00
  0%  at      3   861B  1  0.134.0
```

From this example we see that most of the traffic is IPX, with IP, EtherTalk and some other traffic. Broadcasts account for about 1% of the displayed traffic, which is reassuring.

rules.rc.ipx - a detailed look at the IPX flows, one-minute samples

```
manager> ./nm_rc -c60 -n5 -i10 -h20 -g11 -rrules.rc.ipx 130.216.4.32 passwd
nm_rc: Remote Console for NeTraMet: V3.3
Using MIB file: /dept/ccc/nevil/au-snmp/mib/mib.txt
Meter 130.216.4.32: set 5 sizes set to 20 rules + 1 counts
Rule 10 added to table 5
Rule 20 added to table 5
Meter 130.216.4.32: using rule set 5
#Format: firsttime topdus tooctets  frompdus fromoctets   sourcepeertype \
  sourcepeeraddress destpeeraddress  sourcetranstype sourcetransaddress  \
  desttransaddress
#---  130.216.4.32 eth0  4 flows   15pps   1kBps  11:26:00 Mon  6 Nov 95  ---
 67%    7s  609  60kB     0    0B   ip  0.0.0.0 0.0.0.0  0 0 0
 12%    7s  139  11kB     0    0B   ipx 0.0.0.0.0.0.0.0.0.0 \
                    0.0.0.0.0.0.0.0.0.0  0 0000 0000
 12%    7s  132  11kB     0    0B   at  0.0.0 0.0.0  0 0 0
  6%    7s   75   6kB     0    0B   oth 00-00 00-00  0 0 0
#---  130.216.4.32 eth0  18 flows    1pps  153Bps  11:26:02 Mon  6 Nov 95  ---
 47%    1s   30   2kB    30   2kB   ipx 130.216.0.31.0.192.27.0.16.82 \
                    130.216.0.119.0.0.0.0.0.1  ncp  4003 0000
 16%    2s   11  716B    11  792B   ipx 130.216.0.31.0.128.199.218.14.130 \
                    130.216.0.1.0.0.0.0.0.1  ncp  4003 0000
  8%    1s    4  744B     0    0B   ipx 130.216.0.19.0.192.168.71.61.238 \
                    130.216.0.31.255.255.255.255.255.255  px netbios 0000
  8%    2s    4  744B     0    0B   ipx 130.216.0.29.0.128.72.137.65.142 \
                    130.216.0.31.255.255.255.255.255.255  px netbios 0000
  7%    1s    5  336B     5  330B   ipx 130.216.0.31.0.128.72.129.218.65 \
                    130.216.0.1.0.0.0.0.0.1  ncp  4003 0000
#---  130.216.4.32 eth0  134 flows  204pps  61kBps  11:27:00 Mon  6 Nov 95  ---
 66%   42s   3k 176kB    3k   2MB   ipx 130.216.0.31.0.128.72.133.44.254 \
                    130.216.0.1.0.0.0.0.0.1  ncp  4003 0000
 14%   40s  939  60kB   939 485kB   ipx 130.216.0.31.0.128.72.138.28.75 \
                    130.216.0.1.0.0.0.0.0.1  ncp  4003 0000
  7%   58s  899  64kB   899 215kB   ipx 130.216.0.31.0.128.72.129.218.65 \
                    130.216.0.1.0.0.0.0.0.1  ncp  4003 0000
  4%   10s  433  47kB   433 112kB   ipx 130.216.0.31.0.0.232.2.76.202 \
                    130.216.0.1.0.0.0.0.0.1  ncp  4003 0000
  1%   28s  139   8kB   166  40kB   ipx 130.216.0.31.0.192.168.41.148.177 \
                    130.216.0.1.0.0.0.0.0.1  ncp  4003 0000
#---  130.216.4.32 eth0  34 flows   82pps  14kBps  11:28:00 Mon  6 Nov 95  ---
 81%    2m   2k 152kB    2k 534kB   ipx 130.216.0.31.0.128.72.129.218.65 \
                    130.216.0.1.0.0.0.0.0.1  ncp  4003 0000
  3%    2m   52  26kB     0    0B   ipx 130.216.2.3.0.0.27.48.206.155 \
                    130.216.2.3.255.255.255.255.255.255  0 sap 0000
  2%    2m  150  10kB   150  12kB   ipx 130.216.0.31.0.192.27.0.16.82 \
                    130.216.0.119.0.0.0.0.0.1  ncp  4003 0000
  1%    2m   85   5kB    85   8kB   ipx 130.216.0.31.0.0.232.2.78.246 \
                    130.216.0.1.0.0.0.0.0.1  ncp  4003 0000
  1%    2m   30   9kB   30   2kB   ipx 130.216.0.1.0.0.0.0.0.1 \
                    130.216.0.31.0.128.72.138.37.20  ncp  ncp 0000
#---  130.216.4.32 eth0  168 flows  141pps  19kBps  11:29:00 Mon  6 Nov 95  ---
 75%    3m   3k 522kB    3k 342kB   ipx 247.58.231.46.0.0.0.0.0.1 \
                    130.216.0.31.0.192.223.68.245.229  spx  9000 9000
  8%    3m  381  24kB  381  70kB   ipx 130.216.0.31.0.128.72.129.218.65 \
                    130.216.0.1.0.0.0.0.0.1  ncp  4003 0000
  2%    3m   53  26kB    0    0B   ipx 130.216.2.3.0.0.27.48.206.155 \
                    130.216.2.3.255.255.255.255.255.255  0 sap 0000
  1%    3m  150  10kB  150  12kB   ipx 130.216.0.31.0.192.27.0.16.82 \
                    130.216.0.119.0.0.0.0.0.1  ncp  4003 0000
  1%    3m   85   5kB   85   8kB   ipx 130.216.0.31.0.0.232.2.78.246 \
                    130.216.0.1.0.0.0.0.0.1  ncp  4003 0000
#---  130.216.4.32 eth0  141 flows  243pps  71kBps  11:30:00 Mon  6 Nov 95  ---
 56%   44s   3k 177kB    3k   2MB   ipx 130.216.0.31.0.128.72.133.44.254 \
                    130.216.0.1.0.0.0.0.0.1  ncp  4003 0000
 21%   32s   2k 115kB    2k 806kB   ipx 130.216.0.31.0.128.72.138.28.75 \
                    130.216.0.1.0.0.0.0.0.1  ncp  4003 0000
 13%   12s   1k  78kB    1k 483kB   ipx 130.216.0.31.0.128.72.130.69.34 \
                    130.216.0.1.0.0.0.0.0.1  ncp  4003 0000
  2%    4m  538  34kB  538  91kB   ipx 130.216.0.31.0.128.72.129.218.65 \
                    130.216.0.1.0.0.0.0.0.1  ncp  4003 0000
  0%    4m   75   5kB   75  32kB   ipx 130.216.0.31.0.128.72.133.234.254 \
                    130.216.0.1.0.0.0.0.0.1  ncp  4003 0000
```

All the flows are IPX ncp flows. The last sample shows several users accessing files on server 1 of network 130.216.0.1; the busiest has moved 2MB from server to host in 44 seconds, etc.

There are some netbios broadcasts; evidence of nt clinets using IPX as a transport protocol. Novell sap broadcasts are seen from time to time, taking 2 to 3% of the LAN bandwidth.

rules.rc.ports - all traffic, classified by ports, 10-second samples

```
manager> ./nm_rc -c10 -i10 -h20 -g11 -rrules.rc.ports 130.216.4.32 passwd
nm_rc: Remote Console for NeTraMet: V3.3
Using MIB file: /dept/ccc/nevil/au-snmp/mib/mib.txt
Meter 130.216.4.32: using rule set 1
Meter 130.216.4.32: set 5 sizes set to 69 rules + 4 counts
Rule 10 added to table 5
Rule 20 added to table 5
Rule 30 added to table 5
Rule 40 added to table 5
Rule 50 added to table 5
Rule 60 added to table 5
Meter 130.216.4.32: using rule set 5
#Format: firsttime topdus tooctets  frompdus fromoctets  \
  sourcepeertype sourcetranstype sourcetransaddress desttransaddress
#---  130.216.4.32 eth0  83 flows   4kpps 913kBps  11:31:17 Mon  6 Nov 95  ---
 27%   56s   5k 292kB    5k   2MB   ipx ncp  4003 0000
 26%    1m   3k 177kB    3k   2MB   ipx ncp  4003 0000
 20%    5m   5k 373kB    5k   2MB   ipx ncp  4003 0000
 13%    5m   4k 756kB    4k 456kB   ipx spx  9000 9000
  1%   44s  639  41kB  639 117kB   ipx ncp  4003 0000
  1%   33s  570  37kB  570 114kB   ipx ncp  4003 0000
  1%    5m  616  40kB  616  72kB   ipx ncp  4003 0000
  0%    5m  450  28kB  450  41kB   ipx ncp  4003 0000
  0%    5m  156  45kB  156  13kB   ipx ncp  ncp 0000
  0%    5m  468  28kB  468  29kB   ipx ncp  4003 0000
#---  130.216.4.32 eth0  22 flows  169pps  48kBps  11:31:20 Mon  6 Nov 95  ---
 88%    3s  629 379kB  691  41kB   ipx ncp  ncp 0000
  4%    3s  102  22kB    0    0B   ip  udp  snmp 0
  1%    3s   26   9kB    0    0B   ipx px   netbios 0000
  1%    3s   73   5kB    0    0B   ip  tcp  telnet 0
  0%    3s   10   5kB    0    0B   ip  udp  nbio 0
  0%    3s   41   4kB    0    0B   oth 0 0 0
  0%    3s   67   4kB    0    0B   at  atp  0 0
  0%    3s    8   1kB    5  424B   ip  tcp  22 1023
  0%    3s    6   2kB    0    0B   ip  tcp  xwin 0
  0%    1s    3  855B     0    0B   at  rtmr 0 0
#---  130.216.4.32 eth0  24 flows  527pps 161kBps  11:31:30 Mon  6 Nov 95  ---
 92%   14s   2k   1MB    2k 132kB   ipx ncp  ncp 0000
  2%   14s  474  36kB     0    0B   ip  tcp  telnet 0
  2%   14s  214  34kB     0    0B   ip  udp  snmp 0
  1%   14s  196  17kB     0    0B   at  atp  0 0
  0%   14s  155  12kB     0    0B   oth 0 0 0
  0%   14s   22   4kB    10   1kB   ip  tcp  22 1023
  0%   13s   43   4kB     0    0B   ipx spx  9000 9000
  0%    6s    6   3kB     0    0B   ip  udp  520 520
  0%   14s   43   3kB     0    0B   ipx 0 4001 4005
  0%   13s   26   2kB     0    0B   ip  udp  137 137
#---  130.216.4.32 eth0  26 flows  350pps 106kBps  11:31:40 Mon  6 Nov 95  ---
 86%   23s   1k 849kB    1k  71kB   ipx ncp  ncp 0000
  3%   23s  205  33kB     0    0B   ip  udp  snmp 0
  2%   23s  330  26kB     0    0B   ip  tcp  telnet 0
  2%   19s   49  24kB     0    0B   ipx px   sap 0000
  1%   23s  151  15kB     0    0B   oth 0 0 0
  1%   22s  138  14kB     0    0B   ipx spx  9000 9000
  1%   23s  162  13kB     0    0B   at  atp  0 0
  0%   23s   18   3kB     9  954B   ip  tcp  22 1023
  0%    4s   44   3kB     0    0B   ip  tcp  pop 0
  0%   23s   29   2kB     0    0B   ipx 0 4001 4005
#---  130.216.4.32 eth0  26 flows  257pps  43kBps  11:31:50 Mon  6 Nov 95  ---
 68%   34s  740 254kB   710  45kB   ipx ncp  ncp 0000
  8%   34s  238  37kB     0    0B   ip  udp  snmp 0
  6%   34s  386  28kB     0    0B   ip  tcp  telnet 0
  5%    9s    8  12kB     8  12kB   ipx ncp  4006 4002
  3%   34s  163  14kB     0    0B   oth 0 0 0
  3%   34s  175  14kB     0    0B   at  atp  0 0
  1%   34s   21   4kB    12   1kB   ip  tcp  22 1023
  0%   34s   12   3kB     0    0B   ip  udp  nbio 0
  0%   34s   31   2kB     0    0B   ipx 0 4001 4005
  0%   33s   15   1kB     0    0B   ip  udp  137 137
#---  130.216.4.32 eth0  32 flows  270pps  33kBps  11:32:00 Mon  6 Nov 95  ---
 33%   43s  306  71kB   310  41kB   ipx ncp  ncp 0000
 26%   43s  881  87kB     0    0B   at  atp  0 0
 12%   43s  594  42kB     0    0B   ip  tcp  telnet 0
 10%   43s  206  34kB     0    0B   ip  udp  snmp 0
  3%   43s  134  12kB     0    0B   oth 0 0 0
  3%    6s   25   2kB    21  10kB   ip  tcp  1323 8080
  1%   43s   22   4kB    10   1kB   ip  tcp  22 1023
  1%   43s   12   4kB     0    0B   ip  udp  nbio 0
  0%   42s   32   3kB     0    0B   ip  udp  137 137
  0%    7s    6   3kB     0    0B   ip  udp  520 520
```

rules.rc.ip - a detailed look at the IP flows, 30-second samples

```
manager> ./nm_rc -c30 -i10 -h20 -g11 -rrules.rc.ip 130.216.4.32 passwd
nm_rc: Remote Console for NeTraMet: V3.3
Using MIB file: /dept/ccc/nevil/au-snmp/mib/mib.txt
Meter 130.216.4.32: using rule set 1
Meter 130.216.4.32: set 5 sizes set to 49 rules + 1 counts
Rule 10 added to table 5
Rule 20 added to table 5
Rule 30 added to table 5
Rule 40 added to table 5
Meter 130.216.4.32: using rule set 5
#Format: topdus tooctets  frompdus fromoctets  sourcepeertype \
  sourcetranstype sourcetransaddress desttransaddress   \
  sourcepeeraddress destpeeraddress
#---  130.216.4.32 eth0  36 flows   2kpps 419kBps  11:33:02 Mon  6 Nov 95  ---
 88%   20k  10MB   20k   1MB  ipx ncp  ncp 0000 0.0.0.0.0.0.0.0.0.0 \
                                       0.0.0.0.0.0.0.0.0.0
  2%    2k 365kB     0    0B  ip  udp  snmp 0   0.0.0.0 0.0.0.0
  2%    4k 317kB     0    0B  ip  tcp  telnet 0 0.0.0.0 0.0.0.0
  1%    3k 232kB     0    0B  at  atp  0 0      0.0.0 0.0.0
  1%    2k 157kB     0    0B  oth 0 0 0 00-00 00-00
  0%   808 109kB     0    0B  ip  tcp  xwin 0   0.0.0.0 0.0.0.0
  0%   207  37kB   105  11kB  ip  tcp  22 1023  0.0.0.0 0.0.0.0
  0%   129  39kB     0    0B  ip  udp  nbio 0   0.0.0.0 0.0.0.0
  0%    73  28kB     0    0B  ipx 0 sap 0000    0.0.0.0.0.0.0.0.0.0 \
                                       0.0.0.0.0.0.0.0.0.0
  0%   275  27kB     0    0B  ip  udp  137 137  0.0.0.0 0.0.0.0
#---  130.216.4.32 eth0  33 flows   11pps   1kBps  11:33:05 Mon  6 Nov 95  ---
 33%    32   3kB    34  11kB  ip  udp  snmp 0   130.216.3.0 130.216.4.0
 13%    32   4kB    37   2kB  ip  tcp  telnet 0 130.216.10.0 130.216.118.0
  7%    25   2kB    26   1kB  ip  tcp  telnet 0 130.216.123.0 130.216.10.0
  6%    13   2kB    13  780B  ip  tcp  telnet 0 130.216.10.0 130.216.193.0
  5%     6   2kB     3  232B  ip  tcp  xwin 0   130.216.3.0 130.216.4.0
  3%     6   1kB     4  424B  ip  tcp  22 1023  130.216.3.0 130.216.4.0
  3%    16   1kB     0    0B  ip  udp  snmp 0   130.216.4.0 130.216.4.0
  3%    10  600B    12  720B  ip  tcp  telnet 0 130.216.122.0 130.216.10.0
  2%     4  392B     5  496B  ip  udp  137 137  130.216.60.0 130.216.4.0
  1%     4  344B     4  347B  ip  udp  snmp 0   130.216.4.0 130.216.1.0
#---  130.216.4.32 eth0  68 flows   65pps   7kBps  11:33:30 Mon  6 Nov 95  ---
 12%   194  12kB   194  15kB  ip  tcp  telnet 0 130.216.123.0 130.216.10.0
  9%   119   7kB   119  14kB  ip  tcp  telnet 0 130.216.73.0 130.216.10.0
  9%   114  14kB   109   7kB  ip  tcp  telnet 0 130.216.10.0 130.216.118.0
  7%   102   6kB   103  10kB  ip  tcp  telnet 0 130.216.122.0 130.216.10.0
  7%    61  12kB    33   3kB  ip  tcp  22 1023  130.216.3.0 130.216.4.0
  5%    83   8kB    86   5kB  ip  tcp  telnet 0 130.216.10.0 130.216.193.0
  4%    94   9kB     0    0B  ip  udp  snmp 0   130.216.4.0 130.216.4.0
  3%    24   3kB    24   6kB  ip  udp  snmp 0   130.216.3.0 130.216.4.0
  2%    27   3kB    27   3kB  ip  udp  snmp 0   130.216.4.0 130.216.1.0
  1%    11   1kB    26   3kB  ip  udp  137 137  130.216.60.0 130.216.4.0
#---  130.216.4.32 eth0  73 flows   61pps   7kBps  11:34:00 Mon  6 Nov 95  ---
 12%   197  12kB   198  16kB  ip  tcp  telnet 0 130.216.123.0 130.216.10.0
  8%   111   7kB   112  13kB  ip  tcp  telnet 0 130.216.73.0 130.216.10.0
  7%   112   7kB   113  10kB  ip  tcp  telnet 0 130.216.122.0 130.216.10.0
  7%    28   4kB    38  12kB  ip  udp  snmp 0   130.216.3.0 130.216.4.0
  6%    59  11kB    31   3kB  ip  tcp  22 1023  130.216.3.0 130.216.4.0
  5%   112  11kB     0    0B  ip  udp  snmp 0   130.216.4.0 130.216.4.0
  3%    32   3kB    33   4kB  ip  udp  snmp 0   130.216.4.0 130.216.1.0
  2%    24   2kB    43   4kB  ip  udp  137 137  130.216.60.0 130.216.4.0
  2%    19   4kB     0    0B  ip  udp  nbio 0   130.216.96.0 255.255.255.0
  1%    18   2kB    13  900B  ip  tcp  telnet 0 130.216.10.0 130.216.193.0
```

Most traffic is telnet sessions. The peer addresses show source and destination addresses as Class C subnet numbers. The snmp flow from subnet 4 to subnet 3 is probably nm_rc collecting flow data from the meter. Netbios broadcasts over udp indcate traffic from nt clients.

7. Author's Address

Please send any comments, suggestions, bug reports to me, Nevil Brownlee, i.e.

n.brownlee@auckland.ac.nz