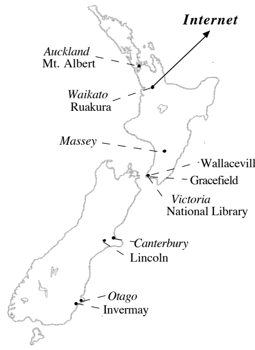
Measuring Traffic with

NeTraMet

Nevil Brownlee
The University of Auckland

Dallas IETF, Wed 6 Dec 95



TuiaNet Sites

Kawaihiko sites

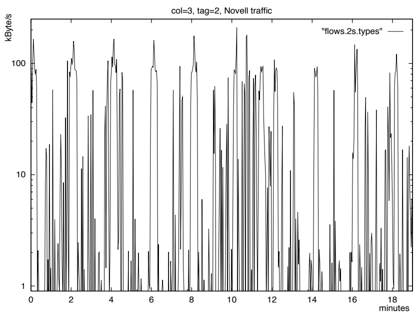
Other Tuia sites

New Zealand

== LAN Traffic, 2s samples

- **Default rule set classifies traffic by Peer type, producing an aggregate flow for each type**
- **Flows were collected at 2-second intervals on a moderately busy LAN, with IP, IPX, EtherTalk, DECnet and VAX Cluster traffic**
- **Flow data file processed by fd_filter program to compute packet and byte rates, then by fd_extract to produce data file for plotting**
- **Plots produced using gnuplot**

Plot of Novell traffic on a LAN (2s samples)



--- Exploring your LAN

- **Straightforward to write rule files to look at any protocol(s) on a LAN**
- **Rule file can select flows using any combination of attributes**
- **nm_rc - part of the NeMaC distribution - displays ‘top n’ flows at spcified intervals**
- **Following two slides were collected from a PC meter on an Ethernet**
- **A Unix workstation with an FDDI card allows NeTraMet to measure FDDI traffic**

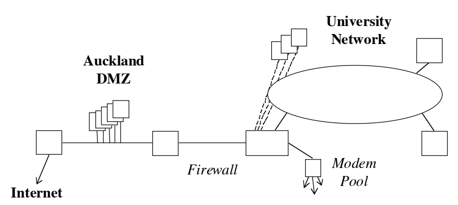
Protocols and Broadcasts %

```
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  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.
```

Ip traffic % by port

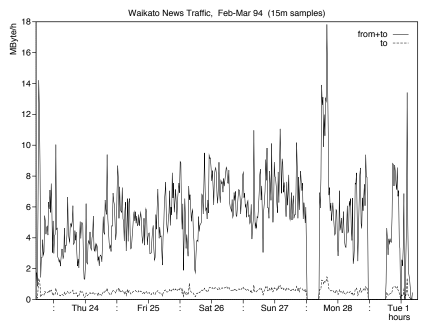
```
Meter 130.216.4.32: using rule set 5
#Format: topdus tooctets  frompdus fromoctets  sourcepeertype \
           sourcetranstype sourcetransaddress desttransaddress   \
           sourcepeeraddress destpeeraddress

#---  130.216.4.32 eth0  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.
```

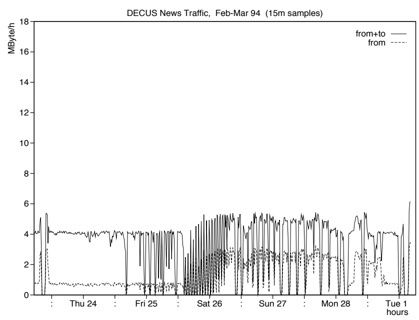

== Auckland network topology



‘Auckland’ Rule Table

- **Classes of flows:**
  - **Auckland–Auckland** **ignore**
  - **Auckland–Local** **count Source–Dest**
  - **Auckland–NZ** **count Source–Tuia site**
  - **Auckland–World** **count Source–World**
  - **Local–NZ** **count Source–NZ**
  - **Local–World** **count Source–World**
- **Traffic types (by IP port number):**
  - **ICMP** **FTP Control**
  - **NNTP (News)** **Local FTP data**
  - **SMTP (Mail)** **Remote FTP data**
  - **DNS (Domain)** **Other TCP**
  - **Telnet** **Other UDP**
  - **Local–World** **count Source–World**





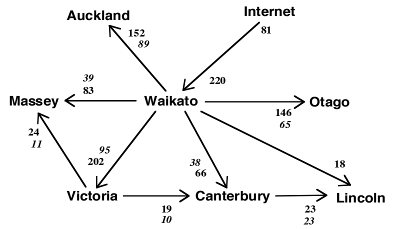
== NZ-Australia traffic volume

- **Around mid-1994 NZGate (Waikato) were considering whether to install a separate link to Australia**
- **Rule file written to measure NZ-AU traffic traversing NZGate. This included about 600 popular Australian networks**
- **Resulting traffic figures showed there was enough direct traffic to justify a 128 kbps direct link**
- **Australian networks have been using rules files with > 1700 rules**

== Kawaihiko Traffic Matrices

- NeTraMet meters (40 MHz 386) on the DMZ at each of the seven NZ universities
- Single rule file classifies flows into:
  - Tuia (Academic/Research) or Commercial
  - Connecting site
  - NZ network or 'World'
- Above info collected via Class andKind attributes
- Single NeMaC at Auckland downloads rule files and collects flow data at 5-minute intervals
- Results processed to produce traffic matrices and other statistics as required

Kawaihiko Traffic Flows



Bold = total kbps Italic = News kbps

--- Finding unexpected flows

- The Kawaihiko rule file tests for every known New Zealand network
- 'Unknown' NZ nets appear within the New Zealand CIDR blocks
- Peer (IP) addresses for 'Unknown' NZ nets are reported back to produce a weekly report
- The Rule tables are updated weekly to include new networks
- Some new networks can generate surprising amounts of traffic!

--- Estimating link capacity

- Kawaihiko sites agree to pay for specified amounts of link capacity, in this case Frame Relay CIR
- Need a good way of estimating how much capacity is needed for each link
- Two types of plots seem helpful:
  - Distributions of traffic rates (kbps)
  - Traffic vs Time-of-day, hourly average + 5-min max
- Third quartile of rate distribution seems a reasonable estimate

Total and News Distributions