NeTraMet Tutorial

nuts, bolts and SRL rulesets

Nevil Brownlee
CAIDA, SDSC, UC San Diego *and*
The University of Auckland
nevil@caida.org

CAIDA, San Diego, Dec 2003

RTFM Overview

- Three components: Meters, Meter Readers and Managers
- Managers configure meters by downloading rulesets to specify what flows they are to measure
- *RTFM flows* are very general, specified by a set of *end-point attribute* values
- Flows are *bi-directional.* The meter maintains two sets of counts, one for each flow direction
- A ruleset configures an RTFM meter to gather flow data. It must
  - Specify flows of interest
  - Determine each flow's direction (which endpoint is the source?)
  - Specify any required data reduction, e.g. computed or distribution-valued attributes to be saved
- *NeTraMet* is Nevil's open-source implementation of RTFM

NeTraMet Documentation

- Yes, there *is* some documentation
- *Using NeTraMet for Production Traffic Measurement,*
  `http://www.caida.org/outreach/papers/2001/NTMintro/`
- The RTFM RFCs
  - 2722 Traffic Flow Measurement: Architecture
  - 2723 Traffic Flow Measurement:
    Simple Ruleset Language (SRL)
- Text files in the NeTraMet distribution
  `doc/NeTraMet`
- NeTraMet home page
  `http://www2.auckland.ac.nz/net/NeTraMet/`

Getting NeTraMet installed

- Download from a NeTraMet distribution site, e.g.
  `ftp://ftp.auckland.ac.nz/pub/iawg/NeTraMet`
- Normal *nix install
  - `tar zxf NeTraMet50.tar.gz`
  - `cd NeTraMet50`
  - `./configure`
  - `make`
  - `sudo make install`

Ruleset 1: test-ucsd.srl

```
define UCSD_SUB   = 132.239/16;
define UCSD_EXTRN = 137.110/16;
define CAIDA      = 192.172.226/24;

   if SourcePeerType == IPv4 save;
   else ignore;  # Not IP

   if PairInterface == 1 {
      if SourcePeerAddress == (UCSD_SUB, UCSD_EXTRN, CAIDA) save, {
         save SourceInterface;
         count;
         }
      }

set test_ucsd;
statistics;
format
  FlowRuleSet FlowIndex FirstTime SourcePeerType
  "   " SourceInterface SourcePeerAddress SourcePeerMask
  "   " ToPDUs FromPDUs
  ;
```

Running the ruleset

```
sudo dd_ntm -V -L72 -I2 -i/dev/dag0 -wtest -t500000 -f300000
```

```
srl test-ucsd.srl
```

```
nm_rc -c30 -r test-ucsd.rules localhost test
```

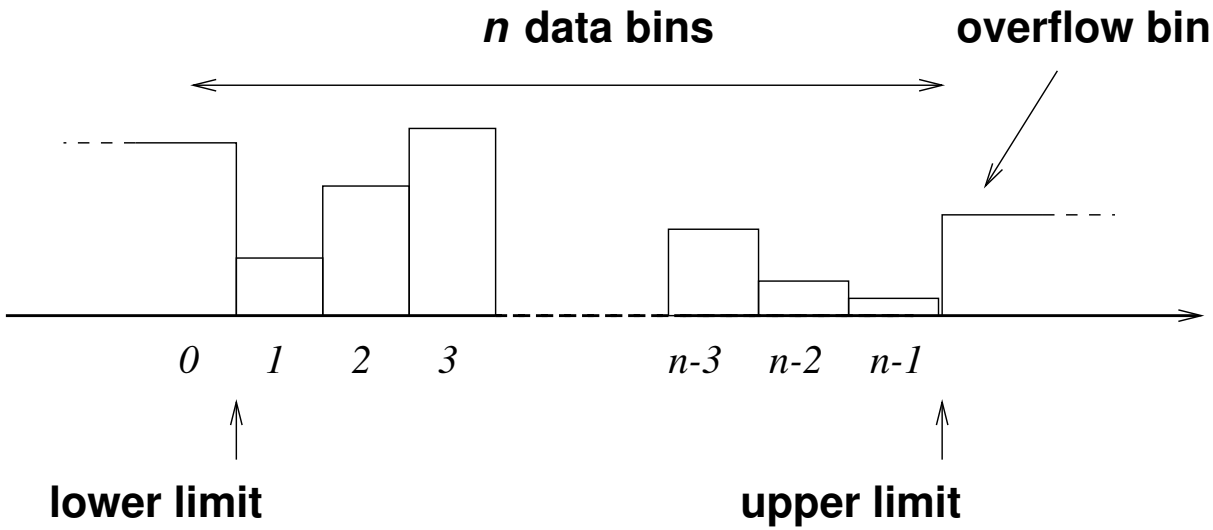
```
NeMaC -c30 -r test-ucsd.rules -F test-ucsd.fdf localhost test t-u
```

Note: NeTraMet, dd_ntm and NeMaC display help via –help option

Example flow data file: test-ucsd.fdf

```
##NeTraMet v5.0:  -c30 -r test-ucsd.rules  localhost /dev/dag0  300000 fl
#Format: flowruleset flowindex firsttime sourcepeertype  sourceinterface
ompdus
#Time: 20:06:42 Tue  9 Dec 2003 localhost Flows from 0 to 43006429
#Ruleset: 3  test_dirn test-ucsd.rules  t-u
#Stats: aps=49222 apb=0 mps=51540 mpb=0 lsp=0 avi=47.1 mni=36.0 mas=3704
3 67572 43006424 1  1 132.239.0.0 255.255.0.0  154 617
3 67573 43006424 1  1 192.172.226.0 255.255.255.0  5 4
3 67574 43006425 1  1 137.110.0.0 255.255.0.0  2 4
#EndData: localhost
#Time: 20:07:00 Tue  9 Dec 2003 localhost Flows from 43006428 to 4300823
#Stats: aps=48858 apb=0 mps=50130 mpb=0 lsp=0 avi=48.3 mni=44.0 mas=3735
3 67572 43006424 1  1 132.239.0.0 255.255.0.0  37840 112372
3 67573 43006424 1  1 192.172.226.0 255.255.255.0  989 1244
3 67574 43006425 1  1 137.110.0.0 255.255.0.0  2504 3523
#EndData: localhost
```

RTFM/NeTraMet *distribution*-valued attributes



- D-V attributes include ToTurnaroundTime (ms)
- RFC 2724 specifies fixed limits and number of bins
- *Dynamic distribution* collection scheme
  - Store up to 100 actual values(max NeTraMet bins)
  - Bin after that, choosing limits based on observed data
  - Actual values are a time series, but do *not* have fixed time steps between values

Ruleset 2: Packet sizes for low-numbered ports

```
   if SourcePeerType == IPv4 save;
   else ignore;

   if SourceTransAddress == 0 & 255.128 {  # Low-numbered port
         # Note: both attribute and value are ANDed with mask
      save SourceTransAddress;
      save ToPacketsize       = 80.0.0!0 & 2.0.40!1500;
      save FromPacketSize     = 80.0.0!0 & 2.0.40!1500;
       # 80 bins, 2=>log binning, scale *10e0, 40..1500 bytes
      count;
      }

set low_ports_pktsz;
statistics;
format
  FlowRuleSet FlowIndex FirstTime SourcePeerType
  "   " SourceTransType SourceTransAddress
  "   " ToPDUs FromPDUs "   " ToOctets FromOctets
  "   (" ToPacketsize ") (" FromPacketsize ")"
  ;
```

Example flow data file: low_ports_pktsz.fdf

```
##NeTraMet v5.0:  -c60 -r low-ports-pktsz.rules  localhost /dev/dag0  300000 flows
  starting at 21:16:57 Tue  9 Dec 2003
#Format: flowruleset flowindex firsttime sourcepeertype  sourcetranstype
  sourcetransaddress  topdus frompdus  tooctets fromoctets
 (topacketsize) (frompacketsize)
#Ruleset: 3  low_ports_pktsz low-ports-pktsz.rules  l-p
#Stats: aps=50574 apb=0 mps=52250 mpb=0 lsp=0 avi=46.9 mni=37.0 mas=40967 maf=98 lss=0
3 68205 43427970 1  6 80  163230 182564  152634265 24976652  (2 0 40 1500  80 0 0 0
  18553 59 8 5033 4098 17 2807 51 88 1119 203 183 71 59 191 82 16 54 56 69 107 69 187
  72 71 85 633 100 76 99 306 59 162 506 233 153 1222 993 323 1276 1971 338 758 245 196
  807 745 512 785 726 405 646 567 499 604 777 335 714 1009 14732 392 1207 389 335 417
  350 363 337 236 4570 442 393 553 612 576 1076 435 547 4 548 1559 76973)
 (2 0 40 1500  80 0 0 0  125285 44 15 1115 11509 0 11380 102 0 2345 10 743 17 32 52
  28 51 5 8 41 33 42 26 28 25 7 15 16 26 24 15 52 25 33 45 84 32 192 72 74 89 115 188
  206 300 853 1038 705 931 1044 1807 2013 1990 2084 1437 1056 1125 970 471 1185 4
  48 551 450 486 575 331 320 561 238 354 227 219 257 142 382 165 144 204 128 83 3044)
3 68208 43427970 1  6 25  18113 17316  1432436 5902110  (2 0 40 1500  80 0 0 0
  1219 0 0 127 53 1 6716 47 1 1351 20 655 843 19 30 3 32 580 105 469 286 748 136 984
  217 483 644 148 984 107 46 28 33 301 38 15 6 2 0 4 37 24 241 18 6 0 0 1 0 0 0 6 1 0
  0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)
 (2 0 40 1500  80 0 0 0  460 1 30 248 659 5 4571 905 9 2790 69 38 111 32 1281 56 79
  252 573 169 15 44 28 26 73 142 916 6 17 10 0 4 0 0 1 0 2 2 0 4 1 2 0 2 3 1 1 0 0 3
  0 1 2 2 3 51 3 0 3 181 4 17 2 0 2 1 5 5 5 12 4 1 105 8 6 43 654 41 233 50 2231)
#EndData: localhost
```

NeTraMet *streams*

- *Streams* are bi-directional 5-tuples
- Streams combine to produce an RTFM *flow*
  - NeTraMet can build distributions giving data about streams
  - Stream sizes and durations
  - Turnaround times for request-response pairs (DNS and ICMP Echo)
  - Interarrival times for packets in streams, or in a whole flow
- See also `doc/NeTraMet/distrib-notes.txt`

Ruleset 3: stream sizes for p2p nodes

```
optimise 3;  # Also checks for duplicate node addresses

   if SourcePeerType == IPv4 save;
   else ignore;

   if SourcePeerAddress == 66.24.171.223 {
      if SourceTransAddress == 1671 {
         store FlowClass := 1;  store FlowKind := 1; }
      }

   ###  lots more statements like this for the other nodes

   else if SourcePeerAddress == 213.23.141.134 {
      if SourceTransAddress == 4661 {
         store FlowClass := 2;  store FlowKind := 173; }
      }
   if FlowClass == 0 nomatch;  # FlowKind remembers which node

   save SourcePeerAddress;  Save SourceTransAddress;
   save TotalStreams;  save TwoWayStreams;
   save TCPStreams;  save UDPStreams;
   save ToFlowPDUs        = 60.0.0!0 & 2.0.2!1000;
   save FromFlowPDUs      = 60.0.0!0 & 2.0.2!1000;
   count;
```

Other topics

- Difference files, fd_filter
  - `fd_filter xxx.flt xxx.fdf > xxx.dif`
  - Difference attributes are d_*, e.g. d_ToPDUs d_FromOctets

- Working with distributions: Nevil's Perl programs
  - `lib/rt_dist.pm` routines to read/write/select flows
  - `at_merge.pl` merges flows for specified attribute ranges
  - `plt_dist.pl` makes .plt files from .dif or .fdf files
  - `plt_stat.pl` makes .plt file with distribution statistics (min, mean, max, 10,25,50,75,90 percentile)