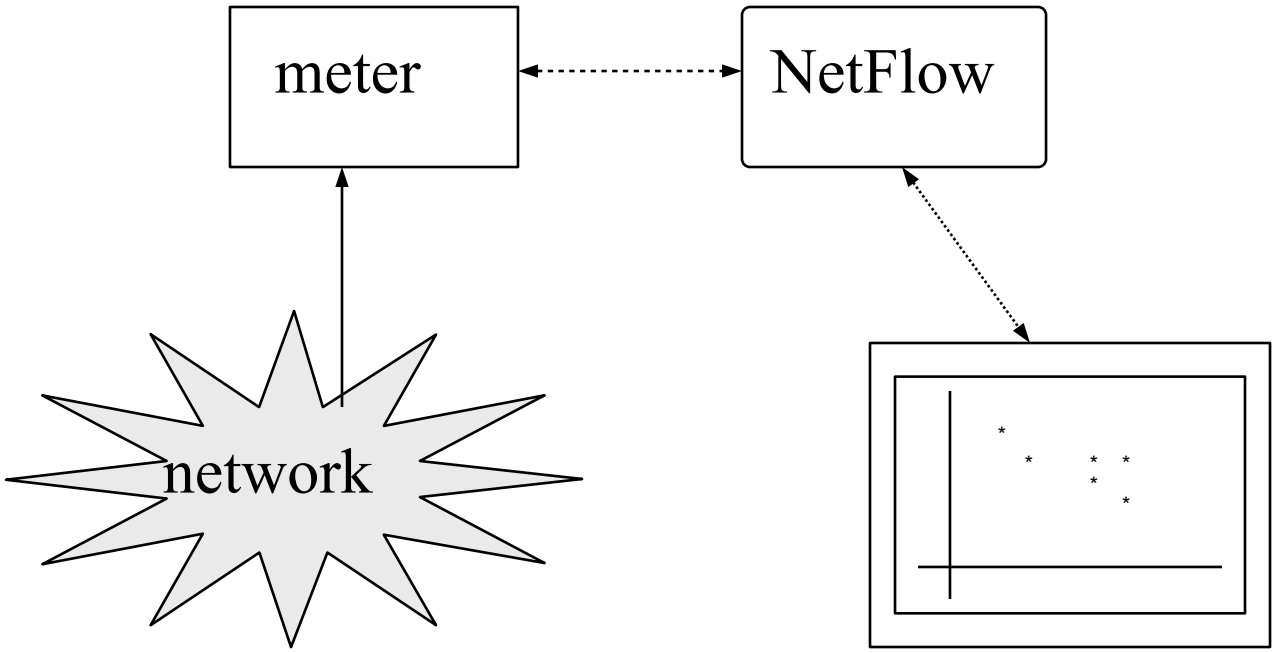
NetFlow

a Network Traffic Flow Analyser

Nevil Brownlee
The University of Auckland

Montreal IETF, June 96

System Overview



Traffic Flow Attributes

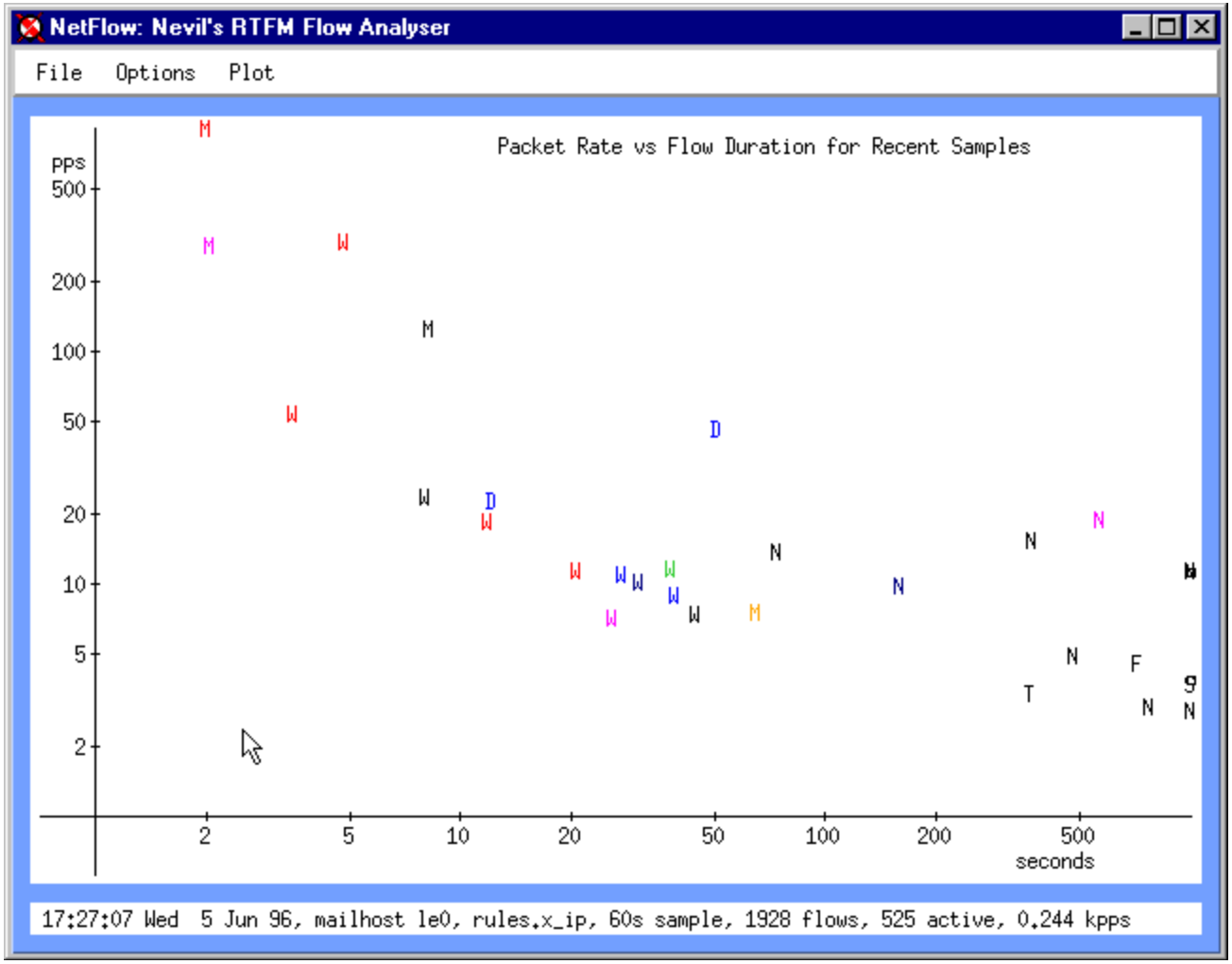
- NetFlow collects data from NeTraMet meter once every *sample* interval
- The attributes read are:
  - Times: First and Last packet arrival
  - Packet Counts: Forward and Backward
  - Byte Counts: Forward and Backward
  - Flow Kind: Computed by meter
- It requires only 8 packet exchanges to collect about 80 flows

NetFlow Displays

- **Plots: Quantity vs Flow Duration**
  Quantity can be packet/byte rate, or packet/byte count
- **Selected flows can be from *last* sample, *recent* sample, or *all* samples**
- **Plot symbol from FlowKind attribute**
- **Colour indicates time since last packet seen (black -> green -> red -> purple)**
- **Click on a point to display flow information**

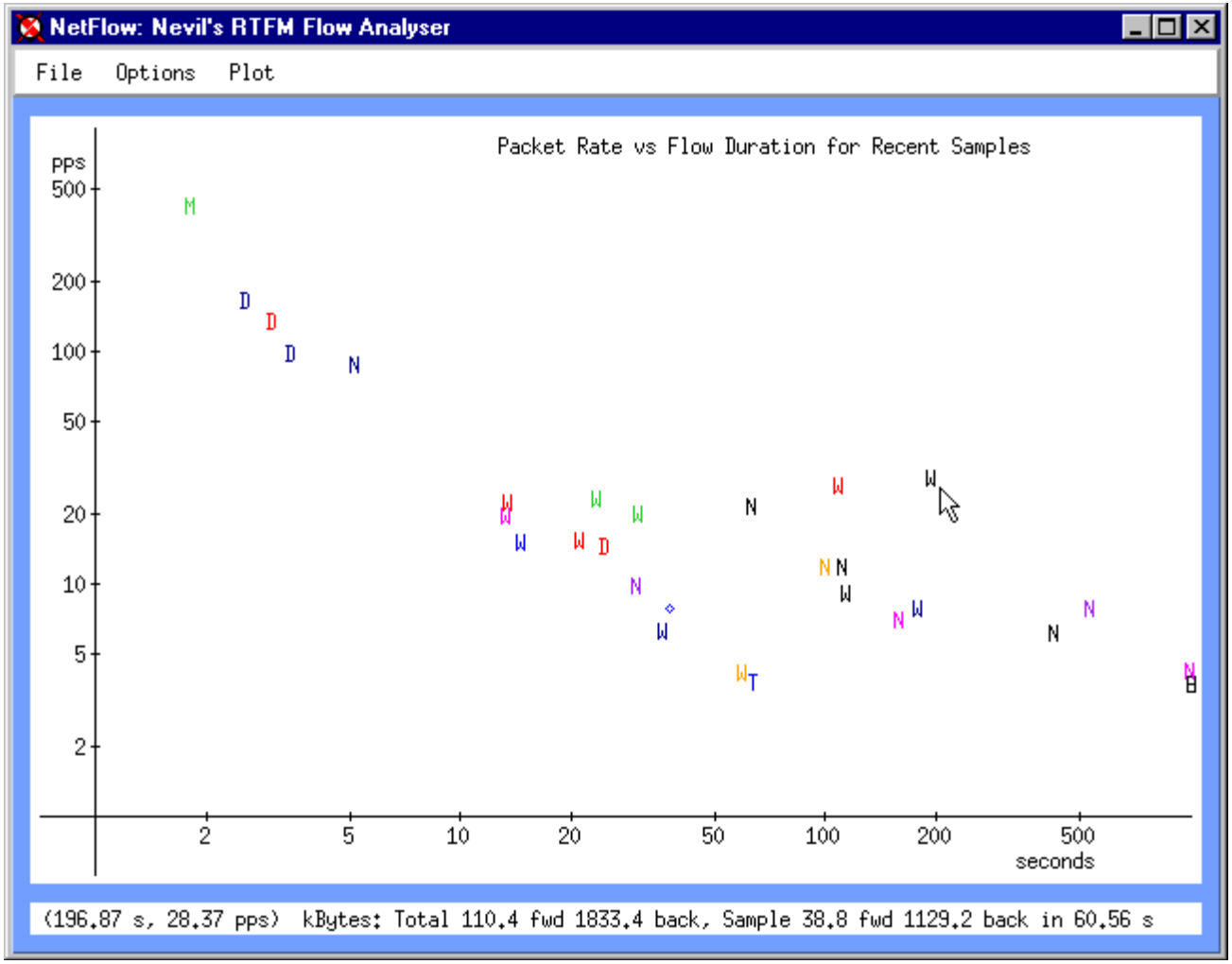
Example Plots

- The following plots were collected at the University of Auckland's Internet gateway. This is a lightly loaded Ethernet
- NeTraMet was running on a SPARC 20
- Number of active flows varies with sample interval, e.g. 240 for 20s samples
- Longer sample intervals, say 1 or 2 minutes, seem to work best overall



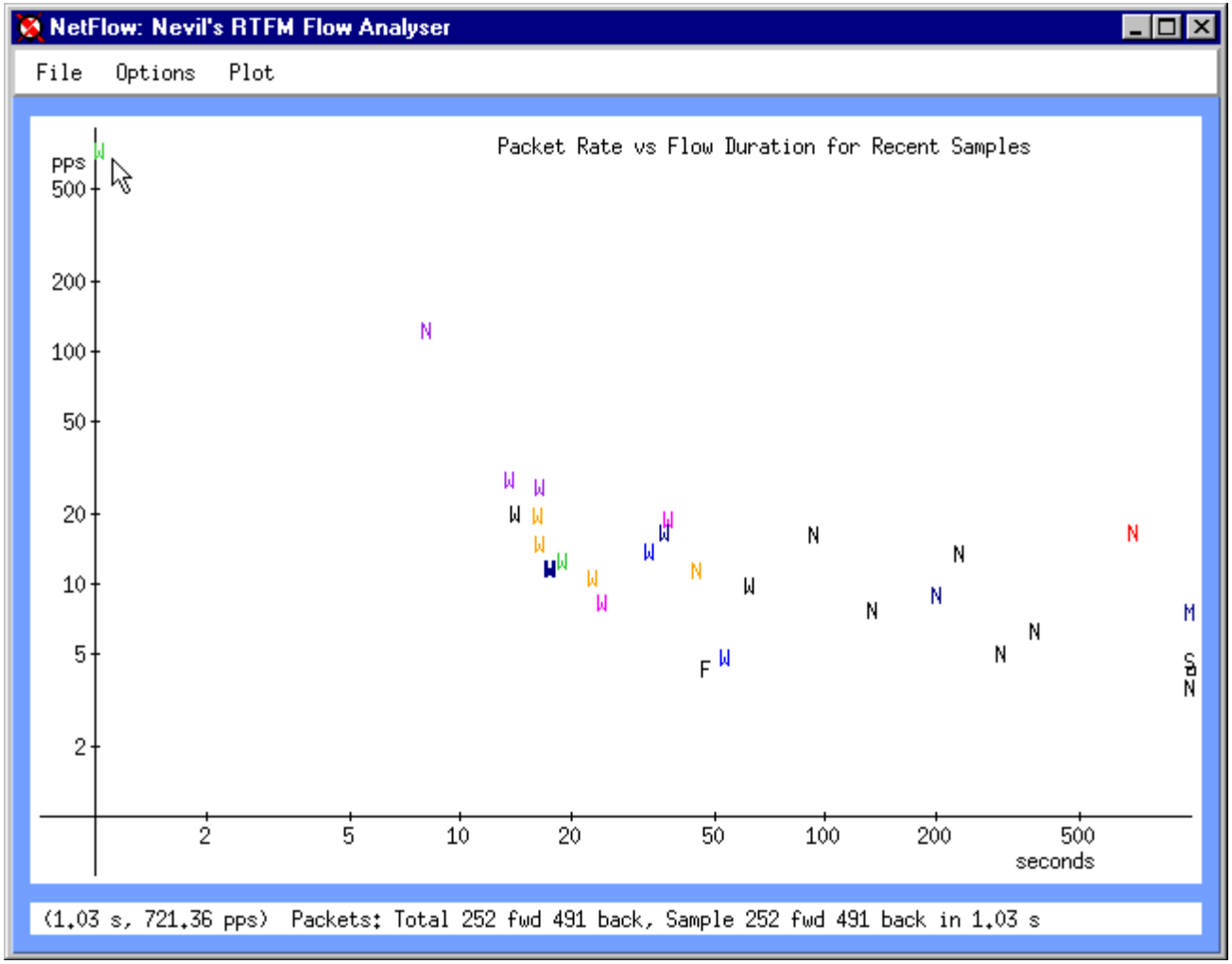
Typical packet-rate plot: short-term / high-rate and long-term / low rate flows

Typ-pps.GIF
5 Jun 96



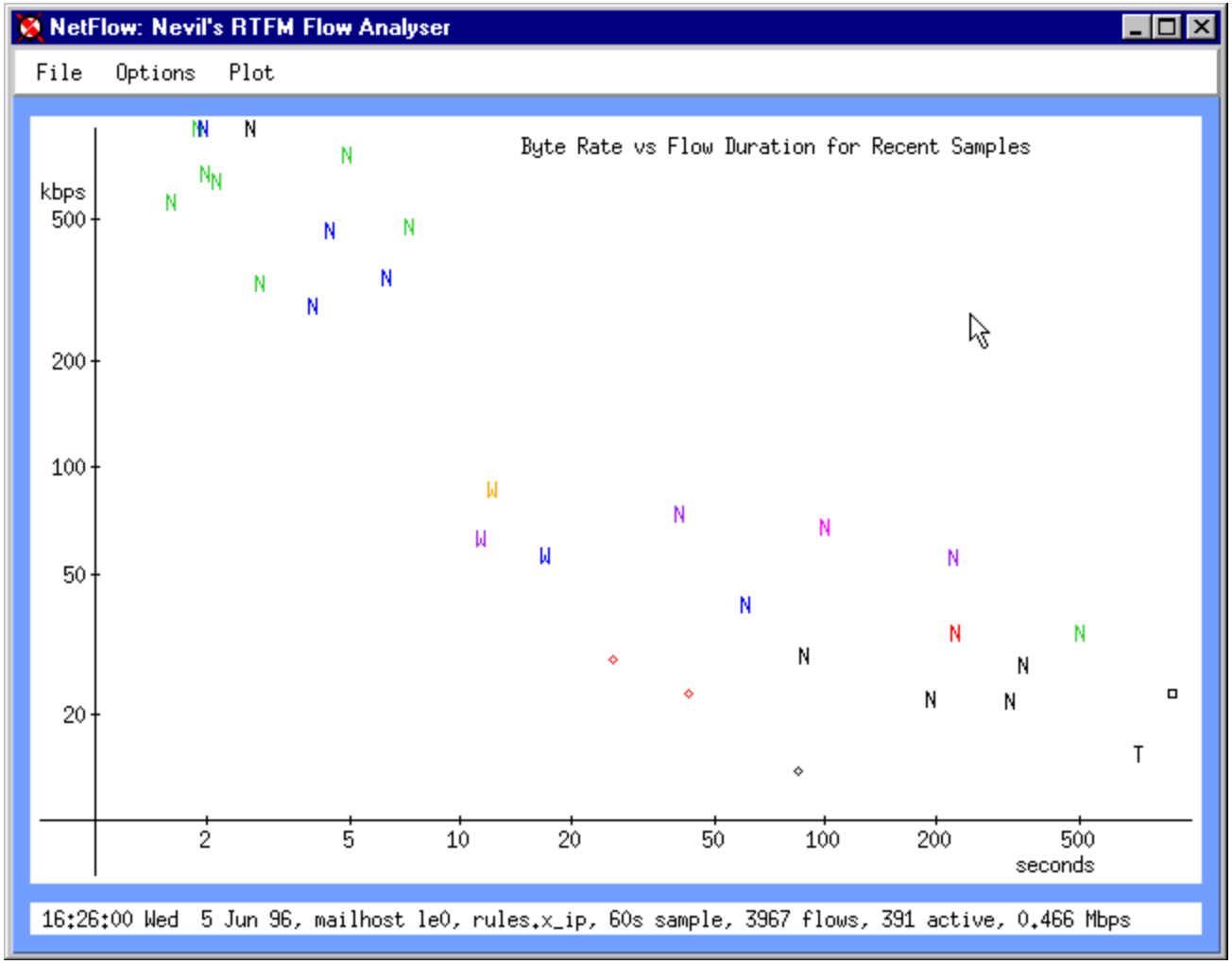
Packet-rate plot: pointer indicates 3-minute WWW flow, byte counts displayed

W3min-pps.GIF
5 Jun 96



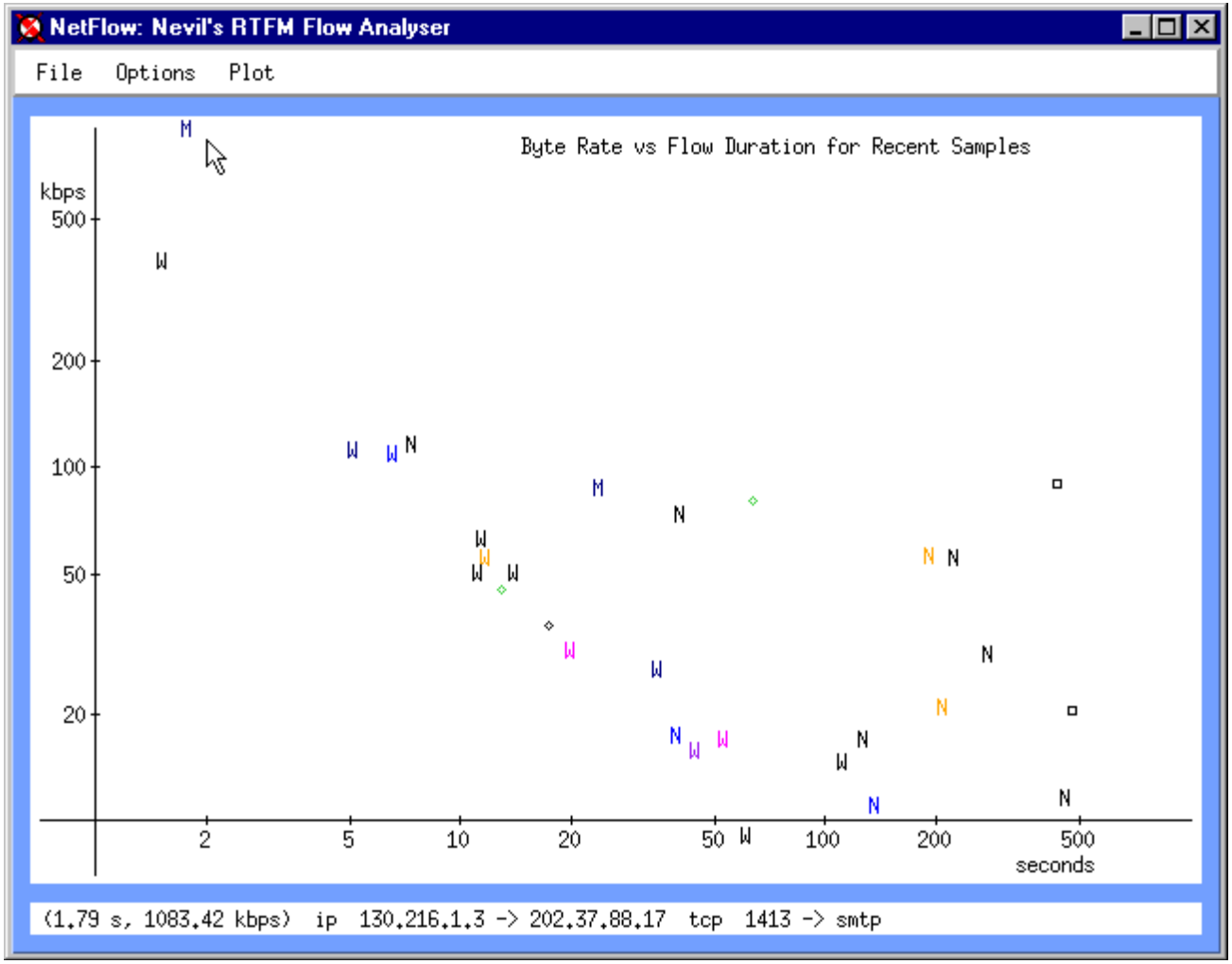
Web flow: short burst with high packet rate, packet counts displayed

Wspike-pps.GIF
5 Jun 96



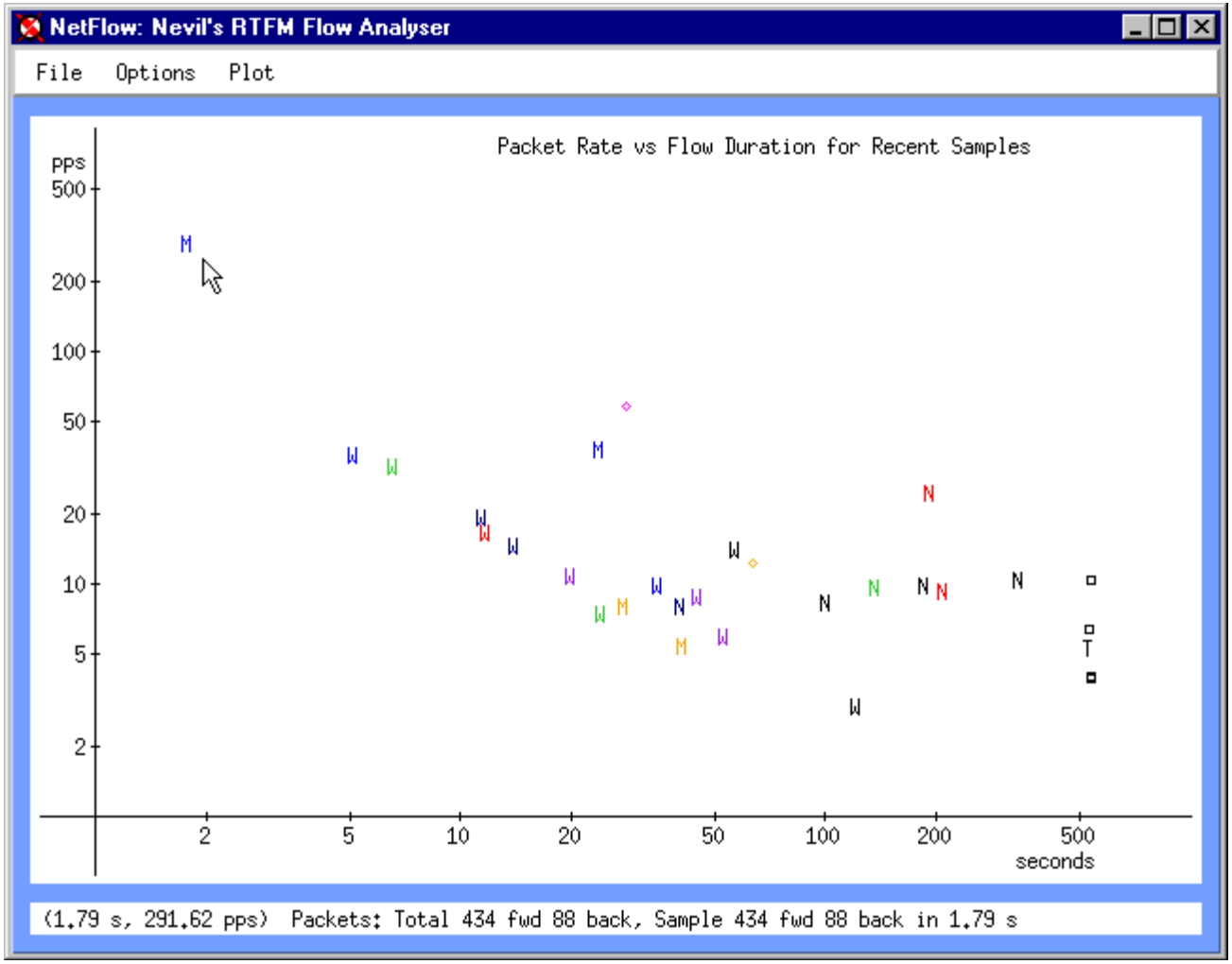
Cluster of short NNTP flows, probably news browsing by a user

Ncluster-pps.GIF
5 Jun 96



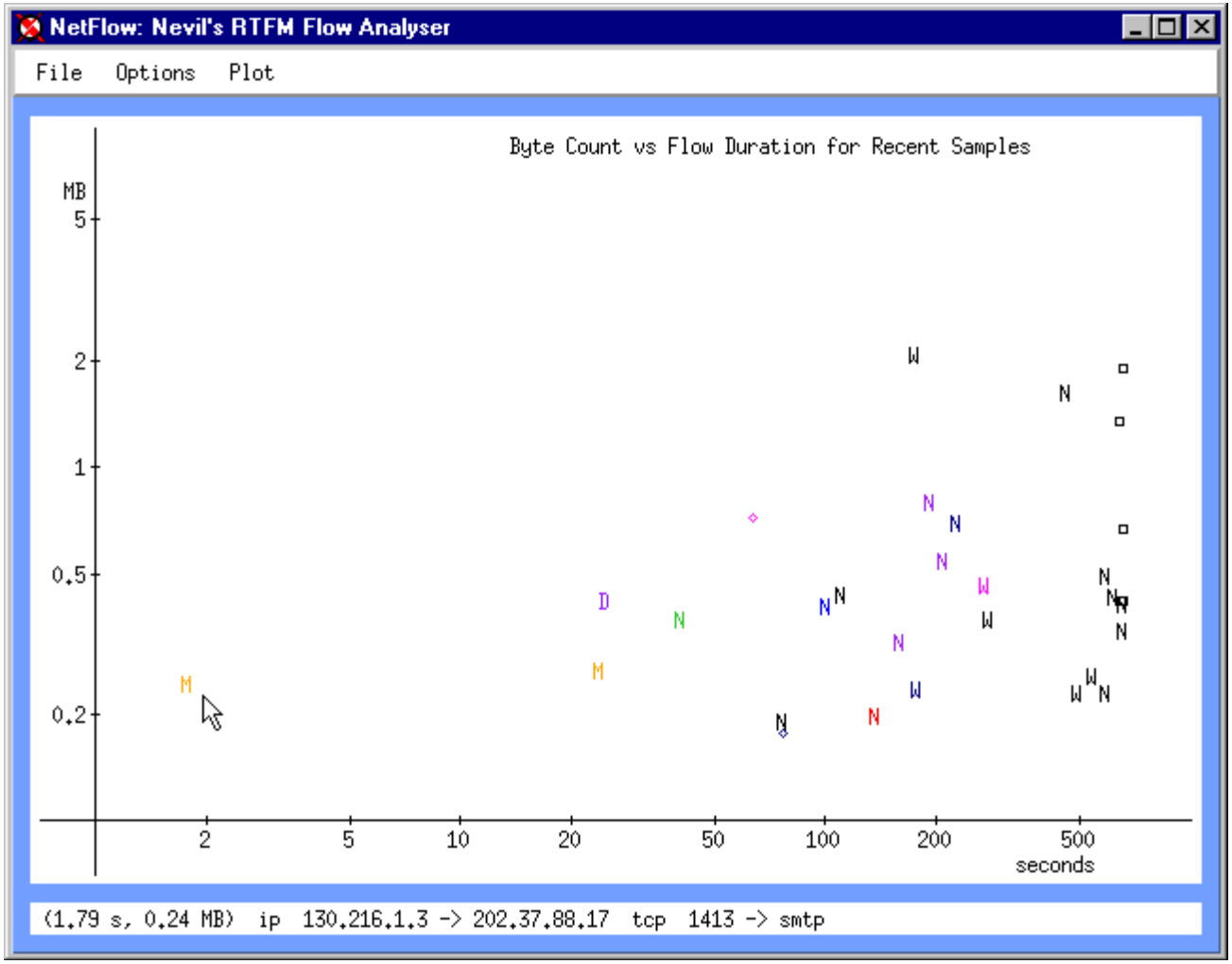
(Local) information server: data rate plot for short, high rate flow

KB-kbps.GIF
5 Jun 96



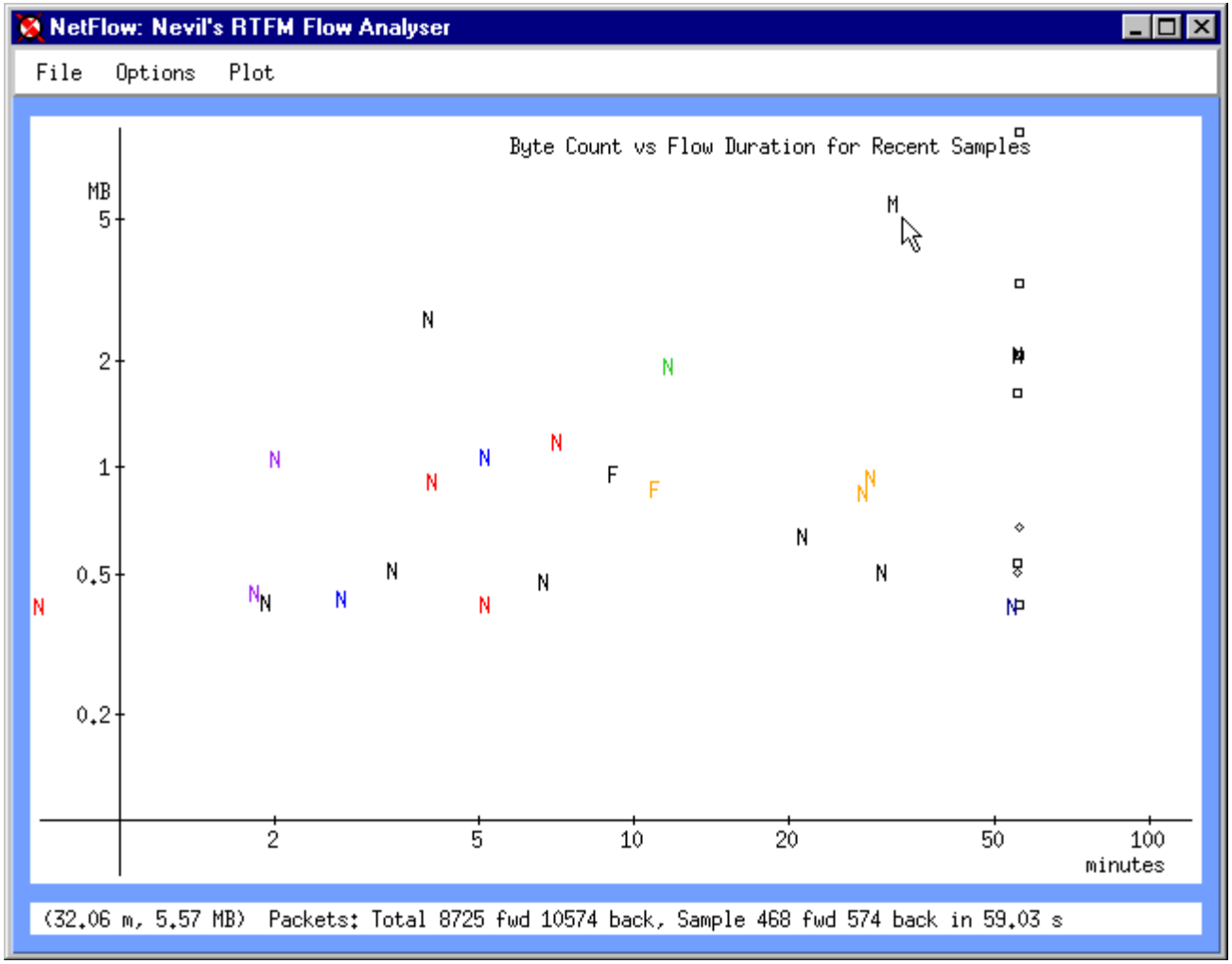
(Local) information server: packet rate plot for same short, high rate flow

KB-pps.GIF
5 Jun 96



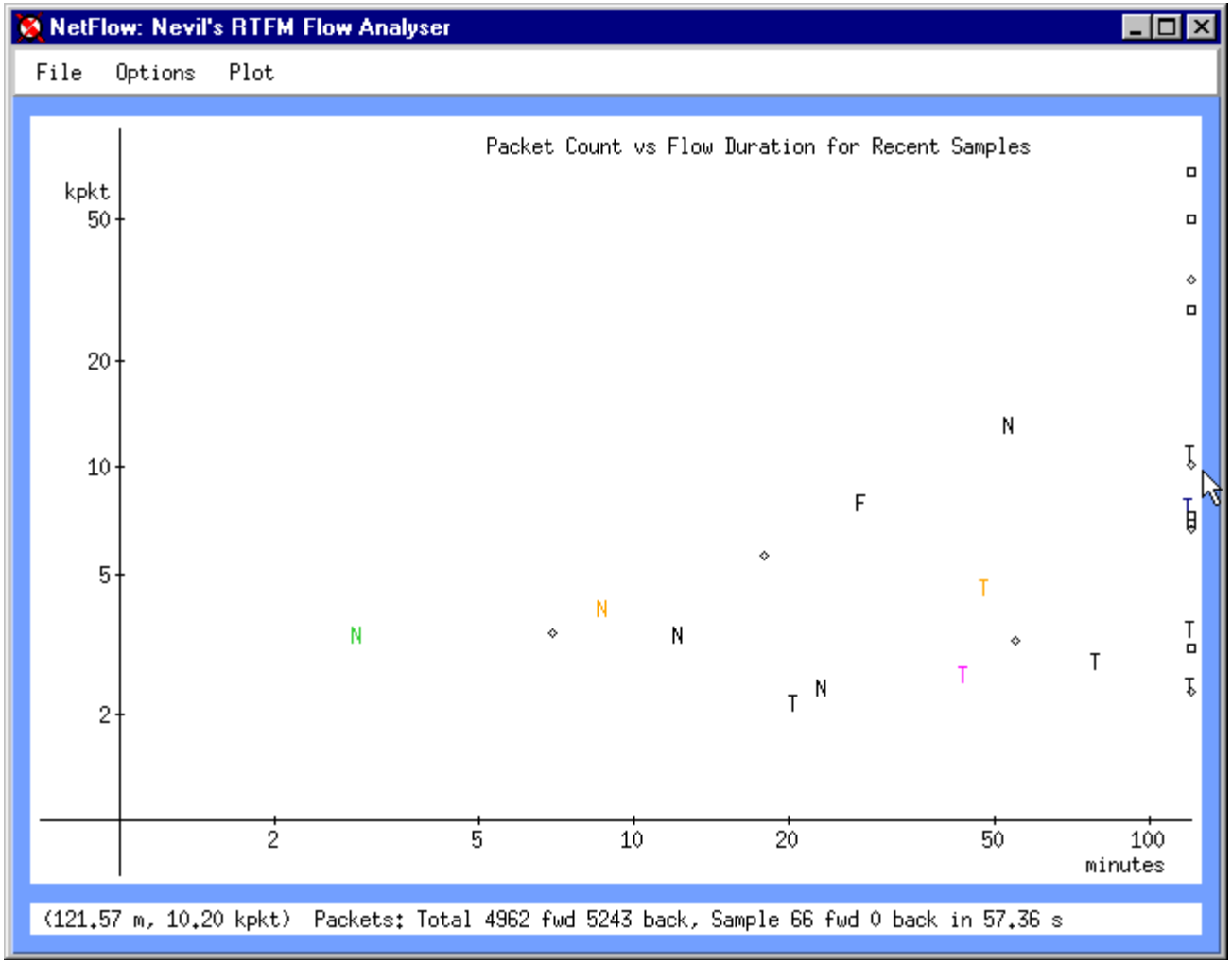
(Local) information server: total data bytes for same short, high rate flow

KB-MB.GIF
5 Jun 96



Typical long-term total data plot: pointer indicates an SMTP flow

Typ-MB.GIF
5 Jun 96



Typical long-term total packets plot: pointer indicates a MUD flow

MUD-kpps.GIF
5 Jun 96

To Find Out More

- NetFlow will be available as part of the NeTraMet distribution version 3.4
- Irix and Solaris binary versions are available, as well as full sources
- For details look at the RTFM Web page:
  http://www.auckland.ac.nz/net/Internet/rtfm/TOP.html