NAME

pktstat − display packet activity on a crt

SYNOPSIS

pktstat [**−1BcFlnpPtT**] [**−a** *abbrev*] [**−A** *file*] [**−i** *interface*] [**−k** *keeptime*] [**−m** *maxbps*] [**−w** *waittime*] [*filter-expr*]

DESCRIPTION

The **pktstat** program displays a real-time summary of packet activity on an interface. Each line displays the data rate associated with different classes of packets.

pktstat understands the following command line options:

−1 Single-shot (batch) mode. **pktstat** collects data for *waittime* seconds (see **−w** option) then emits a line indicating the number of flows detected, and the period of data capture in seconds. Then, each flow line is printed in the form of the number of data link octets associated with the flow, the number of data link frames (packets), and then the flow description.

−a *abbrev*
Add *abbrev* to the list of abbreviation patterns. (See below for details.)

−A *file*
Read abbreviation patterns from the given *file*. (See **Abbreviations**, below.) If the option **−A none** is given, then default abbreviation files are not loaded.

−B Display data rates in bytes per second (Bps) instead of in bits per second (bps).

−c Do not combine some packet classes into one class. For example, TCP connections are kept as two separate flows.

−F Show full hostnames. Normally, hostnames are truncated to the first component of their domain name before display.

−i *interface*
Listen on the given interface. If not specified, a suitable interface is chosen.

−k *keeptime*
When no packets have been seen for a particular class, retain an entry on the display for this many screen seconds. Defaults to 10.

−l Display and sort flows by when they were last seen. (Incompatible with **−t**)

−m *maxbps*
Fix the maximum bit rate for the interface at *maxbps* instead of auto-detecting it.

−n Do not try and resolve hostnames or service port numbers.

−p Show packet counts instead of bit counts.

−P Do not try to put the interface into promiscuous mode.

−t "Top" mode. Sorts the display by bit count (or packet count if **−p** was given) instead of by the name.

−T Show totals.

−w *waittime*
Refresh the display every *waittime* seconds. The default is 5 seconds.

filter-expr

Only consider packets matching the given *filter-expr*. If no filter is provided, all packets are considered. See `tcpdump`(8) for information on valid expressions.

If the terminal supports it, the display briefly highlights in bold new connections or old connections carrying data after a period of inactivity.

Simple statistics about the interface are also displayed such as the current and average bit rates (measured just above the data link layer). Load averages refer to bit rate decayed averages for the last 1, 5 and 15 minutes.

During display, the following keystrokes are recognised:

q	quit
Ctrl-L	redraw screen
t	toggle the **-t** flag (top mode)
T	toggle the **-T** flag (totals mode)
w	allows changing of the **-w** flag value (wait time)
n	toggle the **-n** flag (numeric display)
p	toggle the **-p** flag (packets instead of bits)
b | **B**	toggle the **-B** flag (bps or Bps)
f | **F**	toggle the **-F** flag (full hostnames)
r	reset collected statistics (min, max, etc.), flush flow history and reset DNS/service and fragment caches
l	show and sort flows by when they were last active
?	toggle display of help/status text at the bottom of the display

Packet classes

All packet classes, or flows, are "tagged" with a descriptive string, such as `tcp ftpserver:20524 <-> cathexis:17771`.

In addition to being tagged, some protocol-state information can be associated with a flow. This is displayed immediately below a flow line. Descriptive information for FTP, HTTP, X11 and SUP connections is determined from simple decoding of some packets. If the connection is 'open', it is introduced with a right angle shape (+), otherwise it is introduced with a hyphen character.

```
tcp www:80 <-> hamartia:19179
+ GET /index.html
```

Abbreviations

Abbreviation patterns are a way of further combining flows. As packets are decoded, their flow name is constructed at the various protocol layers. At address combining stage (where arrows such as '`->`' are inserted) and at the final display stage, flow names are checked against a list of abbreviation patterns, and the abbreviation's name substituted if a match is found. For example, the pattern `* <-> *:domain` will match DNS packets in both the UDP and TCP layers.

Abbreviations take the form [*abbrev*@]*pattern*. The *pattern* part can contain the wildcard character, asterisk '*' which matches zero or more non-space characters. The space character matches one or more whitespace characters. Leading and trailing spaces are ignored.

If the optional *abbrev* is not specified, the the pattern text itself is used as the abbreviation.

Patterns are checked in the order given on the command line or in the files, i.e. as soon as one of the patterns matches a tag, no further patterns are considered. Recall that patterns can be applied multiple times to a tag.

A patterns file can contain blank lines, which are ignored. Comment lines that commence with a '#' character are also ignored.

After processing all command line abbreviations and abbreviation files, **pktstat** looks for and loads the files `.pktstatrc`, `$HOME/.pktstatrc` and `/var/opt/UNItools/etc/pktstatrc`. This behaviour is suppressed by supplying an **−A none** option.

EXAMPLES

Here are the contents of my `.pktstatrc` file:

```
dns @ udp *:domain <-> *
dns @ udp * <-> *:domain
irc @ udp 192.168.0.81:6666 <-> *
```

SEE ALSO

`bpf`(4), `tcpdump`(8)

AUTHORS

David Leonard, `leonard@users.sourceforge.net`

BUGS

DNS lookups can take too much time, possibly leading to missed packets.

The data rates do not take into account data link framing overhead or compression savings at the data link layer.

The direction of traffic is not taken into account: both ingress and egress data rates are combined. If you want to separate them, you will need to use a filter expression.

Descriptive information for X11, FTP, HTTP and SUP flows is derived from the very first packets sent on those protocols. If you start **pktstat** after any of these flows have commenced, there may be no description available for them.