

NAME

smacqp — pipeline command interface to SMACQ

DESCRIPTION

"Smacqp" is an extensible component system for analyzing streams of structured data. This manpage describes the use of the runtime system. At runtime, multiple modules are loaded and formed into a pipeline described by the user. The first module in the pipeline is responsible for producing data from some source. Subsequent modules operate on that data, filter out data, or produce data.

The runtime program **smacqp** has a command-line syntax much like a Unix shell. For example, the following command assembles 3 modules (**pcapfile**, **uniq**, and **print**):

```
smacqp pcapfile - | uniq srcip | print srcip dstip
```

(Note: when running this command from a shell, you must escape the `|` symbols by putting them in quotes or putting a backslash before them).

The **pcapfile** module reads a tcpdump-style file from stdin and produces a data record for each packet. Each data record is then passed to the **uniq** module which, in this case, filters out all duplicate occurrences of the same value in the **srcip** field. Finally, all data items that have not been filtered out are passed to **print** which prints out the **srcip** and **dstip** fields for each record.

The **uniq** and **print** modules are polymorphic, meaning that they can operate on any type of data. In contrast, the **pcapfile** module always produces records of type **packet**. Each type has a corresponding module that defines how it is accessed.

See the **smacq(1)** manpage for information on the modules available in SMACQ by default.

SEE ALSO

smacq(1), **smacqq(1)**