NAME
rastrip – strip **argus(8)** data file.

SYNOPSIS
rastrip [**−M** [replace] [+|-]*dsr* [-M ...]] [**raoptions**] [**--** *filter-expression*]

DESCRIPTION
Rastrip reads **argus** data from an *argus-data* source, strips the records based on the criteria specified on the command line, and outputs a valid *argus-stream*. This is useful to reduce the size of argus data files. Rastrip always removes argus management transactions, thus having the same effect as a 'not man' filter expression.

OPTIONS
Rastrip, like all ra based clients, supports a number of **ra options** including filtering of input argus records through a terminating filter expression. See **ra(1)** for a complete description of **ra options**. **rastrip(1)** specific options are:

−M [+|-]dsr
> Strip specified dsr (data set record).

> Supported dsrs are:
> | | |
> |---|---|
> | **flow** | flow key data (proto, saddr, sport, dir, daddr, dport) |
> | **time** | time stamp fields (stime, ltime). |
> | **metric** | basic ([s|d]bytes, [s|d]pkts, [s|d]rate, [s|d]load) |
> | **agr** | aggregation stats (trans, avgdur, mindur, maxdur, stdev). |
> | **net** | network objects (tcp, esp, rtp, icmp data). |
> | **vlan** | VLAN tag data |
> | **mpls** | MPLS label data |
> | **jitter** | Jitter data ([s|d]jit, [s|d]intpkt) |
> | **ipattr** | IP attributes ([s|d]ipid, [s|d]tos, [s|d]dsb, [s|d]ttl) |
> | **suser** | src user captured data bytes (suser) |
> | **duser** | dst captured user data bytes (duser) |
> | **mac** | MAC addresses (smac, dmac) |
> | **icmp** | ICMP specific data (icmpmap, inode) |
> | **encaps** | Flow encapsulation type indications |

In the default mode, without the -M option, rastrip removes the following default set of dsrs: encaps, agr, vlan, mpls, mac, icmp, ipattr, jitter, suser, duser

−M replace
> Replace the existing file with the newly striped file.

INVOCATION
A sample invocation of **rastrip(1)**. This call reads **argus(8)** data from **inputfile** and strips the default dsr set but keeps MAC addresses and writes the result to **outputfile**:

rastrip -M +mac -r inputfile -w outputfile

This call removes only captured user data and timings and writes the result to stdout:

rastrip -M -suser -M -duser -M -time -r inputfile

COPYRIGHT

SEE ALSO
>   **ra(1), rarc(5), argus(8),**

FILES
AUTHORS
>   Carter Bullard (carter@qosient.com).

BUGS