

**NAME**

**racolor.conf** – **racolor** resource file.

**SYNOPSIS**

**racolor.conf**

**DESCRIPTION**

This configuration is a color configuration file for ratop.1. It is modeled after a ralabel(1) configuration file. This configuration would be referenced in a **ratop.1 rarc.5** configuration file, using the RA\_COLOR\_CONFIG variable.

The concept is to provide a number of painting strategies for any or all fields in an argus record. This allows the user to specify the order of the painting, hopefully to get a useful end result.

The method used is flow filter based field painting, which uses the standard flow filter strategies to provide a general purpose coloring scheme.

The concept is similar to racluster()'s fall through matching scheme. Fall through the list of filters, if it matches, use the color specification to paint specific fields in the record. If you want to continue through the list, once there is a match, add a "cont" to the end of the matching rule.

The format is:

```
filter="ra filter" color="field[,field,...]:COLOR[+ATTRIBUTE]" [cont]
```

filter can be any working ra flow record filter, contained in double quotes

color is composed of a comma separated list of fields, that will be painted using the ncurses supported COLOR(s) and an optional ATTRIBUTE(s).

each line can be followed with an optional "cont" inue label, to indicate that it should not stop with this match, but keep going down the list.

A working example color specification is:

```
filter="udp"           color="proto:VIOLET"           cont
filter="tcp"          color="saddr,daddr,proto:WHITE" cont
filter="tcp and port http" color="dport:GREEN"           cont
filter="tcp"          color="sport:BLUE+DIM"         cont
filter="dst port domain" color="dport:CYAN+DIM"         cont
filter="dst port imaps" color="dport:MAGENTA+DIM"      cont
filter="src pkts gt 50" color="spkts,dpkts,sbytes,dbytes:RED+BLINK"
filter="src co CN"    color="all:RED+BLINK"
```