iptraf

Oct 2019

Iptraf is an interactive and colorful IP Lan monitor. It shows individual connections and the amount of data flowing between the hosts.

Install iptraf on CentOS/RHEL/Red Hat/Fedora Linux

```
yum install iptraf -y
```

Using iptraf

From the command line, simply enter:

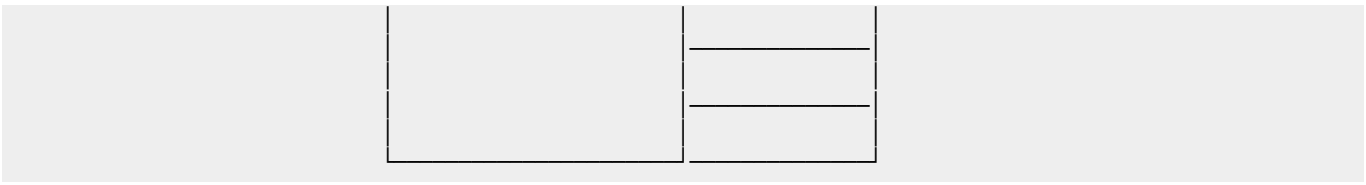
```
iptraf-ng
```

This will start the iptraf application.

```
iptraf-ng 1.1.4

                                  ┌──────────────────────────────┐
                                  │ IP traffic monitor           │
                                  │ General interface statistics │
                                  │ Detailed interface statistics│
                                  │ Statistical breakdowns...    │
                                  │ LAN station monitor          │
                                  ├──────────────────────────────┤
                                  │ Filters...                   │
                                  ├──────────────────────────────┤
                                  │ Configure...                 │
                                  ├──────────────────────────────┤
                                  │ About...                     │
                                  ├──────────────────────────────┤
                                  │ Exit                         │
                                  └──────────────────────────────┘




 Displays current IP traffic information
 Up/Down-Move selector  Enter-execute
```

Select IP traffic monitor, and you will see an interface list:

```
                                  ┌──────────────────────────────┐
                              ┌ Select Interface ──┐            │
                              │ All interfaces     │statistics  │
                              │ lo                 │ statistics │
                              │ eth0               │owns...     │
                              │ eth1               │r           │
                              │ eth3               ├────────────┤
                              │ eth2               │            │
                              │                    ├────────────┤
```



Select the desired interface to start monitoring (or just select All interfaces):

```
 iptraf-ng 1.1.4
┌ TCP Connections (Source Host:Port) ──────────────────────── Packets ──── Bytes ─ Flag  Iface ──────┐
│┌10.43.30.13:22                                          >    2199       288584   -PA-  eth0       │
│└10.14.2.54:5053                                         >    2120       106550   --A-  eth0       │
│┌127.0.0.1:38974                                         >   10428      1336680   --A-  lo         │
│└127.0.0.1:6382                                          >    9480       417120   -PA-  lo         │
│┌127.0.0.1:34210                                         >       2           80   --A-  lo         │
│└127.0.0.1:6380                                          =       0            0   ----  lo         │
│┌127.0.0.1:6380                                          =       0            0   ----  lo         │
│└127.0.0.1:34212                                         >       1           40   --A-  lo         │
│┌127.0.0.1:63244                                         >     276        16572   --A-  lo         │
│└127.0.0.1:6380                                          >     158        27946   -PA-  lo         │
│┌10.43.30.13:58778                                       >     208        32364   -PA-  eth0       │
│└10.43.30.11:5672                                        >     208         9574   --A-  eth0       │
│┌127.0.0.1:42348                                         >     384        19200   --A-  lo         │
│└127.0.0.1:705                                           >     192        13056   -PA-  lo         │
│┌10.43.30.13:58772                                       >      42         3694   -PA-  eth0       │
└ TCP:    114 entries ──────────────────────────────────────────────────────────────────────── Active ─┘
┌──────────────────────────────────────────────────────────────────────────────────────────────────────┐
│ UDP (1344 bytes) from 12.43.30.13:10444 to 239.0.11.11:6009 on eth3                                  │
│ UDP (1344 bytes) from 12.43.30.13:10444 to 239.0.11.11:6003 on eth3                                  │
│ UDP (1344 bytes) from 12.43.30.13:10444 to 239.0.11.11:6008 on eth3                                  │
│ UDP (1344 bytes) from 12.43.30.13:10444 to 239.0.11.11:6009 on eth3                                  │
│ UDP (216 bytes) from 12.43.30.13:10444 to 239.0.11.11:6001 on eth3                                   │
│ UDP (1344 bytes) from 12.43.30.13:10444 to 239.0.11.11:6008 on eth3                                  │
│ UDP (1344 bytes) from 12.43.30.13:10444 to 239.0.11.11:6003 on eth3                                  │
└ Bottom ──────── Elapsed time:   0:01 ──────────────────────────────────────────────────────────────┘
 Packets captured:                            356591   │  TCP flow rate:         23.69 kbps
 Up/Dn/PgUp/PgDn-scroll  M-more TCP info   W-chg actv win  S-sort TCP  X-exit
```

While this gives a lot of information, it is more a 'Wireshark' style output.

General Interface Statistics is a good one for monitoring bandwidth.

```
 iptraf-ng 1.1.4
┌ Iface ──────────── Total ──────── IPv4 ──────── IPv6 ──────── NonIP ── BadIP ──────── Activity ──────┐
│ lo                 17660         17660             0             0         0          300.90 kbps      │
│ eth0                3102          3102             0             0         0           36.31 kbps      │
│ eth1                   0             0             0             0         0            0.00 kbps      │
│ eth3              208374        208374             0             0         0        36554.82 kbps      │
│ eth2                  11            11             0             0         0            0.50 kbps      │
│                                                                                                      │
│                                                                                                      │
│                                                                                                      │
│                                                                                                      │
│                                                                                                      │
│                                                                                                      │
│                                                                                                      │
│                                                                                                      │
│                                                                                                      │
│                                                                                                      │
│                                                                                                      │
│                                                                                                      │
│                                                                                                      │
│                                                                                                      │
│                                                                                                      │
│                                                                                                      │
│                                                                                                      │
│                                                                                                      │
└──────────────────────────────────────────────────────────────────────────────────────────────────────┘
```

```
└ Elapsed time:   0:01 ──────────────────── Total, IP, NonIP, and BadIP are packet counts ──────────────┘
 Up/Down/PgUp/PgDn-scroll window  X-exit
```