

## › Einleitung

Es kommt immer mal wieder vor, dass Trafficwerte über einen bestimmten Zeitraum hinweg überwacht werden müssen. Dafür kann es verschiedene Gründe geben. Zum Beispiel einen überdurchschnittlich starken Trafficwert auf einem Proxy ab einem bestimmten Monat.

Um den Traffic nun zu analysieren gibt es verschiedene Tools. Ich gehe hier nur kurz auf vnstat & iptraf ein. vnstat bietet eine sehr übersichtliche aber unaufgeschlüsselte Ansicht. iptraf dagegen ist sehr flexibel in der Auswertung und Darstellung.

## › vnstat

Installiert werden kann vnstat über

```
apt-get install vnstat
```

Nach der Installation müssen Sie dem Programm noch mitteilen, welche NIC Sie auswerten möchten. Verwenden Sie dazu folgenden Befehl

```
vnstat -u -i eth0
```

Das Tool zeichnet nun die Werte auf. Um die aktuellen Werte angezeigt zu bekommen müssen Sie erst die Datenbank aktualisieren:

```
vnstat -u
```

Anschließend können Sie sich die Werte nach verschiedenen Kriterien ausgeben lassen:

```
vnstat --help
vnStat 1.4 by Teemu Toivola

-q, --query          query database
-h, --hours          show hours
-d, --days          show days
-m, --months         show months
-w, --weeks          show weeks
-t, --top10         show top10
-s, --short          use short output
-u, --update         update database
-i, --iface          change interface (default: eth0)
-?, --help          short help
-v, --version        show version
-tr, --traffic       calculate traffic
```

See also "--longhelp" for complete options list and "man vnstat".

```

$ vnstat
Database updated: Mon Mar  8 22:15:00 2004

inet (eth0)

  received:      1,002,061 MB (24.6%)
 transmitted:    3,068,177 MB (75.4%)
  total:         4,070,238 MB

-----+-----+-----
          rx      |      tx      |    total
-----+-----+-----
yesterday    335 MB |   6,881 MB |   7,216 MB
  today      1,493 MB |   9,808 MB |  11,301 MB
-----+-----+-----
estimated    1,610 MB |  10,579 MB |  12,189 MB

```

```

(with 2 interfaces)
$ vnstat

          rx      /      tx      /    total      / estimated
Local (eth0):
  yesterday    7,564 MB /   4,140 MB /  11,704 MB
  today         33 MB /   112 MB /   145 MB /   195 MB

Internet (eth1):
  yesterday    807 MB /  12,361 MB /  13,168 MB
  today      1,079 MB /   708 MB /   1,787 MB /  2,423 MB

```

```

vnstat -t

inet (eth0)

#      day      rx      |      tx      |    total
-----+-----+-----
 1  10.02.04    1235 MB |   2217 MB |   3452 MB
 2   01.03.04   923.66 MB |   2138 MB |   3061 MB
 3   09.02.04    958 MB |   1597 MB |   2555 MB
 4   07.02.04    976 MB |   1316 MB |   2292 MB
 5   08.02.04   1064 MB |    538 MB |   1602 MB
 6   05.02.04    772 MB |    575 MB |   1347 MB
 7   02.03.04   291.16 MB |  945.70 MB |   1236 MB
 8   06.02.04    480 MB |    601 MB |   1081 MB
 9   03.03.04   237.72 MB |  651.66 MB |   889.38 MB
10   04.02.04    352 MB |    454 MB |    806 MB
-----+-----+-----

```

```
$ vnstat -d
```

```
inet (eth0)
```

day	rx	tx	total
24.02.	4.38 MB	2.86 MB	7.24 MB
25.02.	2.51 MB	2.45 MB	4.97 MB
26.02.	2.42 MB	2.26 MB	4.69 MB
27.02.	2.29 MB	2.17 MB	4.47 MB
28.02.	199.82 MB	50.39 MB	250.21 MB
29.02.	262.74 MB	390.82 MB	653.56 MB
01.03.	923.66 MB	2,138 MB	3,061 MB
02.03.	291.16 MB	945.70 MB	1,236 MB
03.03.	237.72 MB	651.66 MB	889.38 MB
04.03.	13.92 MB	464.40 MB	478.32 MB
05.03.	2.28 MB	2.12 MB	4.40 MB
06.03.	2.26 MB	2.12 MB	4.39 MB
07.03.	2.26 MB	2.12 MB	4.39 MB
08.03.	2.37 MB	2.18 MB	4.55 MB
estimated	2 MB	2 MB	4 MB

```
$ vnstat -m
```

```
inet (eth0)
```

month	rx	tx	total
Mar '03	15,959 MB	18,823 MB	34,782 MB
Apr '03	24,645 MB	20,440 MB	45,085 MB
May '03	31,314 MB	39,103 MB	70,417 MB
Jun '03	28,116 MB	42,988 MB	71,104 MB
Jul '03	27,552 MB	33,924 MB	61,476 MB
Aug '03	37,498 MB	38,189 MB	75,687 MB
Sep '03	19,750 MB	17,488 MB	37,238 MB
Oct '03	3,999 MB	4,492 MB	8,491 MB
estimated	18,479 MB	20,758 MB	39,237 MB

```
$ vnstat -w
```

```
inet (eth0)
```

	rx	tx	total
last 7 days	3,999 MB	4,492 MB	8,491 MB
last week	3,725 MB	3,645 MB	7,370 MB
current week	715 MB	977 MB	1,692 MB
estimated	2,929 MB	4,003 MB	6,932 MB



## › iptraf

iptraf bietet im Gegensatz zu vnstat eine Grafische Oberfläche über die sich das Programm konfigurieren lässt.

Die Installation erfolgt über

```
apt-get install iptraf
```

Nachfolgend ein paar Screenshots über die Anzeige- & Auswertungsmöglichkeiten

```
IPTraf
Statistics for eth0
-----

```

	Total Packets	Total Bytes	Incoming Packets	Incoming Bytes	Outgoing Packets	Outgoing Bytes
<b>Total:</b>	43028	13175747	43028	13175747	0	0
<b>IP:</b>	42975	12477966	42975	12477966	0	0
<b>TCP:</b>	37915	11812706	37915	11812706	0	0
<b>UDP:</b>	3483	518500	3483	518500	0	0
<b>ICMP:</b>	1204	95825	1204	95825	0	0
<b>Other IP:</b>	373	50935	373	50935	0	0
<b>Non-IP:</b>	53	4198	53	4198	0	0

```

Total rates:      3954.4 kbits/sec      Broadcast packets:      26
                  1654.4 packets/sec    Broadcast bytes:       1662

Incoming rates:   3954.4 kbits/sec
                  1654.4 packets/sec

Outgoing rates:   0.0 kbits/sec
                  0.0 packets/sec

IP checksum errors: 0

Elapsed time: 0:00
X-exit

```

```
IPTraf
Proto/Port ----- Pkts --- Bytes --- PktsTo - BytesTo PktsFrom BytesFrom
-----
TCP/www      6064  1960227  3490  387688  2574  1572539
TCP/8088     1328  411655  647   71848  681   339807
TCP/webcache 545   209710  269   21707  276   188003
TCP/pop3     508   169510  220   8952   288   160558
TCP/smtp     177   86150   88    79197  89    6953
UDP/domain   352   40643   192   13357  160   27286
TCP/netbios-ss 160   22112   86    9408   74    12704
UDP/netbios-ns 164   15530   130   10337  34    5193
TCP/https    22    7533    12    1553   10    5980
TCP/telnet   45    4649    25    2052   20    2597
TCP/ftp      25    1269    13    746    12    523
UDP/netbios-dg 5     1177    3     703    2     474
TCP/rntp     7     578     4     213    3     365
TCP/74       6     564     6     564    0     0
TCP/40       9     540     9     540    0     0
UDP/bootps   1     328     1     328    0     0
UDP/bootpc   1     328     0     0      1     328
UDP/rntp     8     608     4     304    4     304
TCP/81       7     332     5     252    2     80
TCP/tproxy   9     508     9     508    0     0
26 entries ----- Elapsed time: 0:00
Protocol data rates (kbits/s): 165.25 in 537.00 out 702.25 total
Up/Down/PgUp/PgDn-scroll window S-sort X-exit

```

```

IPtraf
----- PktsIn ----- IP In - BytesIn - InRate PktsOut ----- IP Out BytesOut OutRate -----
Ethernet HW addr: 0050dac010e9 on eth0
| 90 90 6401 0.0 128 127 8530 0.0
Ethernet HW addr: 0030f212f000 on eth0
| 133 133 8958 0.0 163 141 15589 2.0
Ethernet HW addr: 01005e000005 on eth0
| 75 75 11482 2.4 0 0 0 0.0
Ethernet HW addr: 00d0baccceb47 on eth0
| 0 0 0 0.0 18 0 1152 0.2
Ethernet HW addr: 0180c2000000 on eth0
| 18 0 1152 0.2 0 0 0 0.0
Ethernet HW addr: 00000c4340a0 on eth0
| 0 0 0 0.0 26 26 3724 0.6
Ethernet HW addr: 006097b77e2e on eth0
| 0 0 0 0.0 2 0 120 0.0
Ethernet HW addr: ffffffff on eth0
| 47 4 3672 0.4 0 0 0 0.0
Ethernet HW addr: 0050733f6b21 on eth0
| 0 0 0 0.0 4 0 240 0.0
Ethernet HW addr: 003094152f01 on eth0
| 0 0 0 0.0 15 15 2786 0.2
-----
16 entries ----- Elapsed time: 0:00 ----- InRate and OutRate are in kbits/sec -----
Up/Down/PgUp/PgDn-scroll window S-sort X-exit

```