iftop: Top lista mrežnog prometa

Ono što je ***top*** za procese, to je ***iftop*** za mrežu. *To* je još jedan u nizu alata koji posuđuje ime od popularnog *top*-a, dok je "if" mnemonik od "interface". Namjena je ovog alata praćenje potrošnje mrežnih resursa portova vašeg poslužitelja i udaljenih klijenata. Za prikaz koristi *ncurses* sučelje, pa je alat vizualno dotjeran za naredbenu liniju. Radi preko standardnog sučelja PCAP, koje sigurno već imate instalirano na serveru, pa neće biti nikakvih dodatnih ovisnosti kod instaliranja.

Instalira se kao i svaki drugi paket:

```
# apt-get install iftop
```

Ovaj program od jedva 40 kB pokrećemo kao korisnik *root*, s dodatnim parametrima:

```
# iftop -f "not port domain"
```

"-f" uključuje filtriranje DNS prometa. Ukoliko želimo prikaz imena hostova, DNS upiti će smetati prikazu i kvariti statistiku prometa.

Sam program u radu izgleda ovako:

```
            10b         100b         1.00Kb       10.0Kb       100Kb        1.00Mb      10.0Mb
[redacted]:www          => 95-178-166-50.dsl.op:26679     0b    61.0Kb    15.3Kb
                        <=                                0b    1.40Kb     357b
[redacted]:www          => 95-178-132-47.dsl.op:29529   231Kb   46.2Kb    14.9Kb
                        <=                              5.56Kb  1.11Kb     584b
[redacted]:https        => 89-172-245-143.adsl.:54729     0b    14.8Kb    3.76Kb
                        <=                                0b     718b     258b
[redacted]:www          => crawl-66-249-66-187.:49240   208b     425b     106b
                        <=                              416b     634b     158b
[redacted]:www          => 95-178-132-47.dsl.op:29548   448b     90b      22b
                        <=                              2.84Kb   582b     146b
[redacted]:www          => 95-178-132-47.dsl.op:29547   448b     90b      22b
                        <=                              2.84Kb   582b     145b
[redacted]:www          => 95-178-132-47.dsl.op:29549   448b     90b      22b
                        <=                              2.84Kb   582b     145b
[redacted]:www          => 95-178-132-47.dsl.op:29545   448b     90b      22b
                        <=                              2.83Kb   580b     145b

TX:             cumm:   34.9MB   peak:   1.43Mb   rates:   1.43Mb   519Kb    295Kb
RX:                     2.63MB            373Kb            373Kb    88.3Kb   47.6Kb
TOTAL:                  37.5MB            1.80Mb           1.80Mb   607Kb    343Kb
```

I ovdje smo upotrijebili parametre, te prikaz nije "defaultan", podrazumijevan. Od brojnih mogućnosti koje podržava program uključeno je prikazivanje portova, njihovo pretvaranje iz numeričkog oblika u razumljiviji tekstualni oblik (npr. 80 -> www), te logaritamska skala (koja naglašava promet i prikladna je za "pojačanje" prikaza slabih prometa.

Sam prikaz je podijeljen u tri vodoravna polja. U gornjem dijelu, nazovimo ga statusnom linijom, prikazana ja skala koja pokazuje količinu prometa u sljedećem, glavnom ili radnom prostoru, tako da veličina stupca odgovara prometu. Ovo je lako uočljivo svakome koji program pokrene prvi put, no zgodna je stvar što se stupci ispisuju inverzno preko hostova, tako da nije izgubljena nijedna informacija, niti o tome koji su hostovi u pitanju, niti količina prometa po sesiji.

Zadnji dio ekrana su zbrojevi prometa. U prvoj liniji je ispisan promet u odlaznom smjeru: ukupan promet, vršni, te tri uprosječene vrijednosti za trenutan promet (unazad 2, 10 i 40 sekundi).

Linija ispod je funkcionalno ista, ali odnosi se na dolazni promet. U zadnjoj liniji nalaze se zbrojevi svih ovih vrijednosti, a prikaz putem stupaca se i ovdje događa, preko sve tri linije.

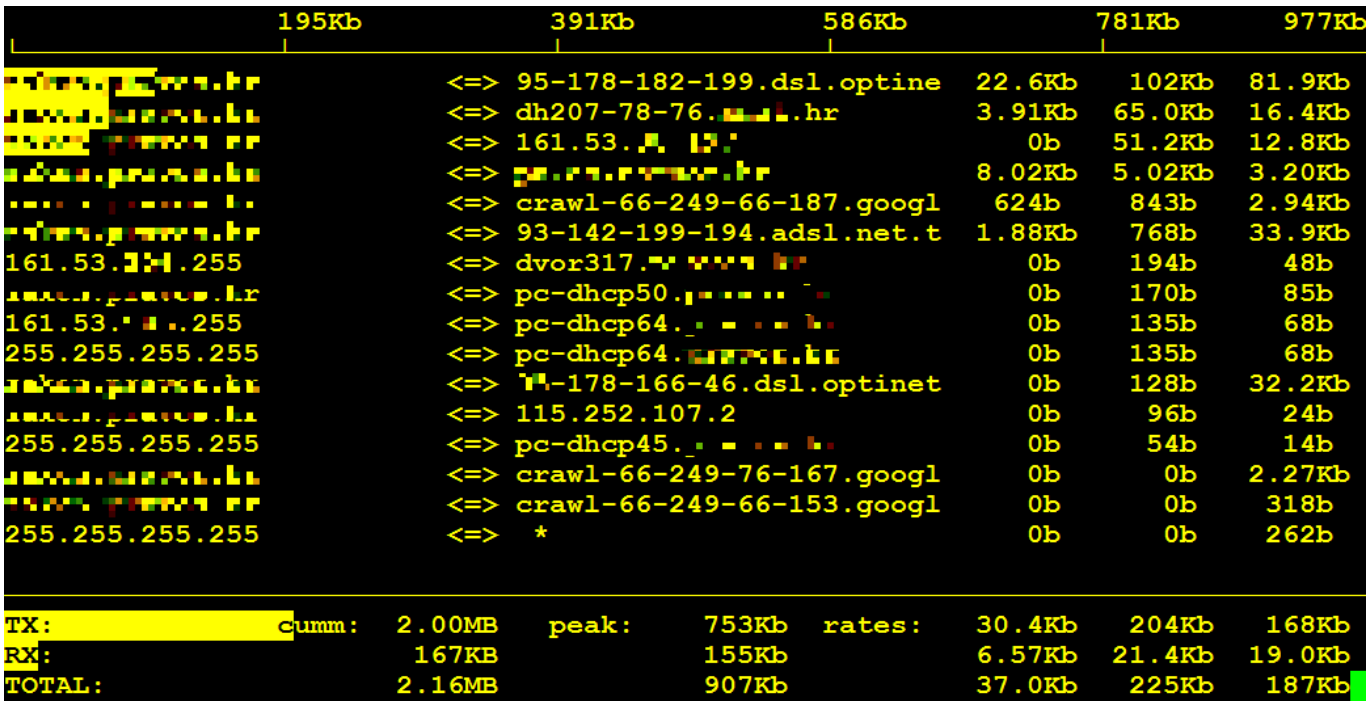
Sve dinamičke (*run-time*) opcije možete vidjeti ukoliko stisnete tipku "h" (pazite na veličinu slova, dakle sve opcije su *case-sensitive*):

```
                1.91Mb          3.81Mb          5.72Mb          7.63Mb     9.54Mb
└──────────────┴──────────────┴──────────────┴──────────────┴──────────────┘
Host display:                                 General:
 n - toggle DNS host resolution                P - pause display
 s - toggle show source host                   h - toggle this help display
 d - toggle show destination host              b - toggle bar graph display
 t - cycle line display mode                   B - cycle bar graph average
                                               T - toggle cummulative line totals
Port display:                                  j/k - scroll display
 N - toggle service resolution                 f - edit filter code
 S - toggle show source port                   l - set screen filter
 D - toggle show destination port              L - lin/log scales
 p - toggle port display                       ! - shell command
                                               q - quit
Sorting:
 1/2/3 - sort by 1st/2nd/3rd column
 < - sort by source name
 > - sort by dest name
 o - freeze current order

TX: p, version 0cumm:   5.44MB    peak:    2.36Mb  rates:    2.36Mb    523Kb    224Kb
RX:                      577KB               538Kb            29.2Kb   7.84Kb   38.6Kb
TOTAL:                  6.00MB              2.39Mb            2.39Mb    530Kb    262Kb
```

Parametara ima mnogo, no ne previše, što bi zbunjivalo, niti premalo, što bi smanjilo funkcionalnost. Kao što smo rekli, možete uključiti prikaz portova (sa "p"), njihov prikaz u razumljivijem obliku ("ssh" umjesto 22 se uključuje sa "N"), prikaz samo udaljenih ("D") ili samo lokalnih portova ("S"). S tipkama "j" i "k" možete pomicati ekran gore-dolje kako bi vidjeli više informacija, a sa "L" uključujete ili isključujete logaritamsku skalu.

Zanimljiva je i mogućnost koju uključujete s tipkom "t". Ona kompaktira ekran prikazujući samo ukupnu potrošnju po paru, izbacujući prikaz po smjeru u kojem promet putuje:



Ukoliko tipku stisnete još jednom, bit će prikazan samo *donwload*. Stisnite li još jednom tipku "t", bit će prikazan samo *upload*, a ponovljen stisak vraća sve na početni dvoredni prikaz.

iftop je ugodno iznenađenje, dovoljno je pregledan i jasan i uz to daje mnoštvo korisnih informacija. Kako ga usporediti sa sličnim programima? Na Portalu je objavljen članak o programu *nethogs*, koji se razlikuje od *iftopa* po tome što je orijentiran na lokalne procese koji troše najviše prometa. *Iftop* je orijentiran na sesije, pa možete vidjeti s kojim se udaljenim računalom odvija najjači promet.

Zajedno, *iftop* i *nethogs* su moćni alati u rukama sistemca koji zna što radi.

Za više informacija pogledajte *man* stranice.

Zdravko Rašić

čet, 2012-11-29 13:19 - Zdravko Rašić**Kuharice:** Linux [1]
Kategorije: Mreža [2]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1153

Links
[1] https://sysportal.carnet.hr/taxonomy/term/17
[2] https://sysportal.carnet.hr/taxonomy/term/29