

Table of Contents

Cara Memonitor Traffic Jaringan di Linux 1

NLOAD 1

HTTPRY 2

IFTOP 3

IPTRAF 4

Cara Memonitor Traffic Jaringan di Linux

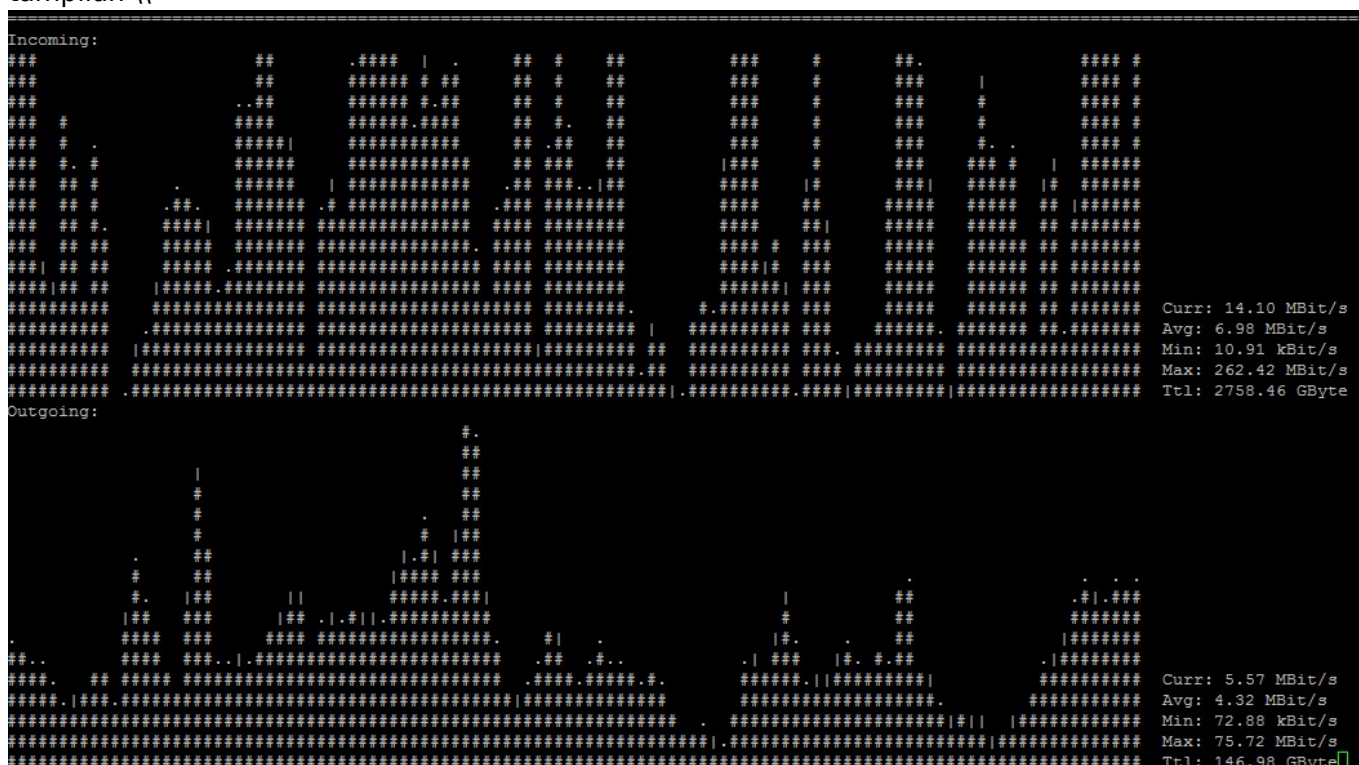
Berikut ini adalah daftar linux command / aplikasi yang dapat digunakan untuk memonitor traffic networking.

NLOAD

Perintah

```
nload
```

tampilan \\\



cara install

```
# fedora or centos
$ yum install nload -y

# ubuntu/debian
$ sudo apt-get install nload
```

HTTPrY

Httpry adalah tools monitoring traffic port 80 untuk linux dan Untuk dapat menggunakan httpry anda harus menginstall paket epel

```
yum install epel-release -y
yum install httpry -y
```

Berikut ini adalah cara penggunaan httpry

```
httpry -i eth0
```

dan outputnya kurang lebih seperti ini

```
[root@uvcms1 abuse]# httpry -i eth0
httpry version 0.1.8 -- HTTP logging and information retrieval tool
Copyright (c) 2005-2014 Jason Bittel <jason.bittel@gmail.com>
Starting capture on eth0 interface
2020-09-26 15:47:53      139.99.53.101    36.77.47.183    <      -      -
-      HTTP/1.1      403      Forbidden
2020-09-26 15:47:53      36.77.47.183      139.99.53.101    >      GET
kediripost.co.id      /wp-
content/themes/korankoran/includes/sharrre.php?url=http%3A%2F%2Fkediripost.c
o.id%2F2020%2F09%2F26%2Fdhito-tiba-tiba-datang-ke-nu%2F&type=googlePlus
HTTP/1.1      -      -
2020-09-26 15:47:53      36.77.47.183      139.99.53.101    >      GET
kediripost.co.id      /wp-
content/themes/korankoran/includes/sharrre.php?url=http%3A%2F%2Fkediripost.c
o.id%2F2020%2F09%2F26%2Fdhito-tiba-tiba-datang-ke-nu%2F&type=stumbleupon
HTTP/1.1      -      -
2020-09-26 15:47:53      139.99.53.101      143.204.82.117    >      GET
www.stumbleupon.com      /services/1.01/badge.getinfo?
```

Anda bisa menghilangkan keterangan header httpry version dengan cara menambahkan **-q**

```
httpry -q -i eth0
```

Apabila anda hanya ingin mengambil traffic 50 baris anda bisa menggunakan

```
httpry -q -i eth0 -n 30
```

Anda juga dapat menyimpan output pada file dengan cara

```
httpry -q -i eth0 -n 30 -o /path/nama-file.txt
```

atau bisa juga

```
httprry -q -i eth0 -n 30 >> /path/nama-file.txt
```

Apabila anda ingin memfilter post,get,head anda bisa menggunakan

```
httprry -q -i eth0 -n 30 -m post,head
```

Apabila anda ingin memfilter source traffic dari ip tertentu berikut ini perintahnya

```
httprry -q -i eth0 -n 30 'src host 139.99.53.101'
```

dan untuk filter traffic berdasarkan destinasi ip address, anda bisa menggunakan perintah

```
httprry -q -i eth0 -n 30 'dst host 139.99.53.101'
```

IFTOP

Perintah Command

```
$ sudo iftop -n
```

Tampilan

	12.5kb	25.0kb	37.5kb	50.0kb	62.5kb
192.168.1.2	=> 195.221.84.4	6.67kb	6.18kb	5.80kb	
	<=	10.2kb	9.90kb	9.41kb	
192.168.1.2	=> 70.82.8.51	5.36kb	5.59kb	5.25kb	
	<=	7.24kb	7.99kb	7.60kb	
192.168.1.2	=> 217.126.101.254	4.70kb	4.76kb	4.43kb	
	<=	4.48kb	4.76kb	4.51kb	
192.168.1.2	=> 96.242.40.175	4.29kb	4.72kb	4.49kb	
	<=	4.48kb	4.76kb	4.58kb	
192.168.1.2	=> 108.216.65.96	3.70kb	3.75kb	3.54kb	
	<=	2.76kb	3.39kb	3.26kb	
192.168.1.2	=> 173.255.230.5	0b	1.58kb	1.01kb	
	<=	0b	686b	455b	
192.168.1.2	=> 130.127.255.220	736b	662b	690b	
	<=	1.09kb	0.98kb	1.03kb	
192.168.1.2	=> 23.236.59.231	1.12kb	576b	504b	
	<=	1.64kb	941b	840b	
192.168.1.2	=> 216.33.130.209	208b	208b	208b	
	<=	208b	208b	208b	
192.168.1.2	=> 74.125.135.125	0b	158b	99b	
	<=	0b	122b	76b	
TX:	cum: 53.0kB	peak: 33.2	rates: 27.0kb	28.5kb	26.5kb
RX:	64.6kB	36.4kb	32.1kb	33.8kb	32.3kb
TOTAL:	118kB	69.6kb	59.1kb	62.3kb	58.8kb

Instalasi

```
# fedora or centos
yum install iftop -y

# ubuntu or debian
```

```
$ sudo apt-get install iftop
```

IPTRAF

Perintah

```
$ sudo iptraf
```

Tampilan

```
IPTraff
TCP Connections (Source Host:Port) ———— Packets ——— Bytes lags Iface
[192.168.1.2:42053 > 2 152--A- eth0
[54.236.180.90:9999 > 1 96-PA- eth0
[192.168.1.2:55015 > 12 624--A- eth0
[216.33.130.209:5222 > 12 624--A- eth0
[192.168.1.2:57880 = 16 2168CLOSED eth0
[38.127.167.7:443 = 13 8964CLOSED eth0
[192.168.1.2:50999 > 8 563--A- eth0
[74.125.135.125:5222 > 8 6738-PA- eth0
[192.168.1.2:40465 > 2 152--A- eth0
[54.236.180.90:9999 > 1 96-PA- eth0
[192.168.1.2:51067 > 1 52--A- eth0
[74.125.135.125:5222 > 1 52--A- eth0
[192.168.1.2:43164 > 1 88-PA- eth0
TCP: 10 entries ———— Active ———

UDP (92 bytes) from 192.168.1.2:55012 to 217.126.101.254:11352 on eth0
UDP (92 bytes) from 65.34.190.57:44084 to 192.168.1.2:32821 on eth0
UDP (121 bytes) from 192.168.1.2:55012 to 217.126.101.254:11352 on eth0
UDP (153 bytes) from 65.34.190.57:44084 to 192.168.1.2:32821 on eth0
UDP (92 bytes) from 70.82.8.51:64962 to 192.168.1.2:40257 on eth0
UDP (140 bytes) from 192.168.1.2:32821 to 65.34.190.57:44084 on eth0
Bottom ———— Elapsed time: 0:00 ———
Pkts captured (all interfaces): 991 | TCP flow rate: 0.00 kbits/s
Up/Dn/PgUp/PgDn-scroll M-more TCP info W-chg actv win S-sort TCP X-ex
```

Install

```
# Centos (base repo)
$ yum install iptraf

# fedora or centos (with epel)
$ yum install iptraf-ng -y

# ubuntu or debian
$ sudo apt-get install iptraf iptraf-ng
```

From:

<https://www.pusathosting.com/kb/> - **PusatHosting Wiki**

Permanent link:

<https://www.pusathosting.com/kb/linux/command-monitor-traffic-network?rev=1601110611>

Last update: **2020/09/26 04:56**

