

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ  
ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение  
высшего образования

«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. В. И. ВЕРНАДСКОГО»

ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ

Кафедра компьютерной инженерии и моделирования

**Сетевые средства мониторинга операционной системы Linux**

Отчет по лабораторной работе 6

по дисциплине «**Системное программное обеспечение**»

студента 3 курса группы ИВТ-б-о-202

Шор Константина Александровича

Направления подготовки 09.03.01 «Информатика и вычислительная техника»

Симферополь, 2023

## Лабораторная работа №6. Сетевые средства мониторинга операционной системы Linux

Цель работы: Получение навыков использования утилит мониторинга сети, сбор статической информации и представление её в графическом виде.

1. Написать скрипт для сбора статистики с интерфейса. Обеспечить его постоянной загрузкой активности

Общая статистика iptraf

```
File Actions Edit View Help
iptraf-ng 1.2.1
TCP: Connections (Source Host:Port) ----- Packets ----- Bytes ----- Flag ----- Iface -----
10.0.2.15:42524 > 5 200 --A- eth0
173.194.73.94:80 > 5 230 --A- eth0
10.0.2.15:53650 > 5 200 --A- eth0
80.77.169.239:443 > 5 230 --A- eth0
10.0.2.15:55346 > 7 693 --A- eth0
88.221.132.162:80 > 7 1204 --A- eth0
108.177.14.101:443 < 2 92 --A- eth0
10.0.2.15:58176 < 3 857 -PA- eth0
10.0.2.15:53100 < 0 679 --A- eth0
173.194.73.94:80 < 5 920 --A- eth0
10.0.2.15:55154 < 2 110 --A- eth0
108.177.14.119:443 < 2 175 -PA- eth0
10.0.2.15:45200 < 2 202 --A- eth0
34.117.65.55:443 < 2 200 -PA- eth0
10.0.2.15:35704 < 10 3367 -PA- eth0
35.244.181.201:443 < 10 5513 --A- eth0
TCP: 21 entries, the quieter you become, the more you are able to hear Active
UDP (1045 bytes) from 10.0.2.15:46640 to 142.251.1.198:443 on eth0
UDP (60 bytes) from 142.251.1.198:443 to 10.0.2.15:46640 on eth0
UDP (101 bytes) from 142.251.1.198:443 to 10.0.2.15:46640 on eth0
UDP (54 bytes) from 142.251.1.198:443 to 10.0.2.15:46640 on eth0
UDP (73 bytes) from 10.0.2.15:46640 to 142.251.1.198:443 on eth0
UDP (62 bytes) from 10.0.2.15:46640 to 142.251.1.198:443 on eth0
UDP (57 bytes) from 142.251.1.198:443 to 10.0.2.15:46640 on eth0
Bottom Time: 0:00 Drops: 0
Packets captured: 15762 TCP flow rate: 0.00 kbps
q-quit r-refresh s-scroll k-more TCP info i-chg actv win S-sort TCP X-exit
```

# iptraf-ng 1.2.1

Statistics for eth0

	Total Packets	Total Bytes	Incoming Packets	Incoming Bytes	Outgoing Packets	Outgoing Bytes
Total:	828	914976	664	901025	164	13951
IPv4:	828	914960	664	900995	164	13951
IPv6:	0	0	0	0	0	0
TCP:	10	400	5	200	5	200
UDP:	810	914566	659	900795	150	13751
ICMP:	0	0	0	0	0	0
Other IP:	0	0	0	0	0	0
Non-IP:	0	0	0	0	0	0
Broadcast:	0	0	0	0	0	0

Total rates: 1300.66 kbps  
147 pps

Broadcast rates: 0.00 kbps  
0 pps

Incoming rates: 1280.37 kbps  
137 pps

IP checksum errors: 0

Outgoing rates: 20.08 kbps  
20 pps

2. Обеспечить сбор данных для формирования графика активности с использованием утилиты mrtg

### Установка

```
(kali㉿kali)-[/home]
$ sudo apt install mrtg snmp snmpd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
snmp is already the newest version (5.9.3+dfsg-2).
snmp set to manually installed.
snmpd is already the newest version (5.9.3+dfsg-2).
snmpd set to manually installed.
The following additional packages will be installed:
  libsnmp-session-perl
Suggested packages:
  mrtg-contrib
The following NEW packages will be installed:
  libsnmp-session-perl mrtg
0 upgraded, 2 newly installed, 0 to remove and 558 not upgraded.
Need to get 548 kB of archives.
After this operation, 1,659 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

### Экспорт

```
(kali㉿kali)-[/home]
$ export MIBS=/usr/share/mibs
```

### Создание папки и настройка прав доступа

```
(kali㉿kali)-[/var/www]
$ mkdir mrtg
mkdir: cannot create directory 'mrtg': Permission denied

(kali㉿kali)-[/var/www]
$ sudo mkdir mrtg

(kali㉿kali)-[/var/www]
$ sudo chown -R www-data:www-data /var/www/mrtg
```

## Конфигурация snmpd

```
root@kali: /var/www
File Actions Edit View Help
GNU nano 7.2 /etc/snmp/snmpd.conf *
agentaddress 127.0.0.1,[::1]

#####
# SECTION: Access Control Setup
#
# This section defines who is allowed to talk to your running
# snmp agent.
#
# Views
# arguments viewname included [oid]
#
# system + hrSystem groups only
view systemonly included .1.3.6.1.2.1.1
view systemonly included .1.3.6.1.2.1.25.1
#
# rocommunity: a SNMPv1/SNMPv2c read-only access community name
# arguments: community [default|hostname|network/bits] [oid | -V]
#
# Read-only access to everyone to the systemonly view
rocommunity public localhost
rocommunity6 public default -V systemonly
```



## Установка рабочей папки и mrtg

```
(root@kali)-[/var/www]
# systemctl restart snmpd.service

(root@kali)-[/var/www]
# cfmaker public@localhost > /etc/mrtg/mrtg.cfg
--base: Get Device Info on public@localhost:
--base: Vendor Id: Unknown Vendor - 1.3.6.1.4.1.8072.3.2.10
--base: Populating confcache
--base: Get Interface Info
--base: Walking ifIndex
--snpd: public@localhost: → 1 → ifIndex = 1
--snpd: public@localhost: → 2 → ifIndex = 2
--base: Walking ifType
--snpd: public@localhost: → 1 → ifType = 24
--snpd: public@localhost: → 2 → ifType = 6
--base: Walking ifAdminStatus
--snpd: public@localhost: → 1 → ifAdminStatus = 1
--snpd: public@localhost: → 2 → ifAdminStatus = 1
--base: Walking ifOperStatus
--snpd: public@localhost: → 1 → ifOperStatus = 1
--snpd: public@localhost: → 2 → ifOperStatus = 1
--base: Walking ifMtu
--snpd: public@localhost: → 1 → ifMtu = 65536
--snpd: public@localhost: → 2 → ifMtu = 1500
--base: Walking ifSpeed
--snpd: public@localhost: → 1 → ifSpeed = 100000000
--snpd: public@localhost: → 2 → ifSpeed = 1000000000
```

## Создание индексного файла для веб сервера

```
(root@kali)-[/var/www] - The Weeknd, Maroon 5, Ed Sheer
# indexmaker /etc/mrtg/mrtg.cfg > /var/www/mrtg/index.html
Adele, Ava Max
```

Создал файл VirtualHost для сервера

```
GNU nano 7.2 /etc/apache2/sites-available/mrtg.conf
Alias /mrtg "/var/www/mrtg/"
<Directory "/var/www/mrtg/">
  Options None
  AllowOverride None
  Require all granted
</Directory>
ServerName firs_server
<Directory "/var/www/mrtg/">
  Order allow,deny
  Allow from all
</Directory>
```

Скрипт обновления

```
#!/bin/bash
LANG=C
export $LANG
/usr/bin/mrtg /etc/mrtg/mrtg.cfg --logging /var/log/mrtg.log
```

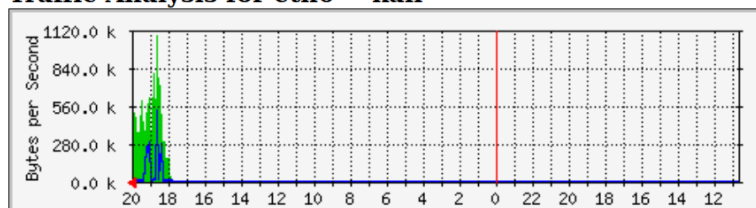
Настройка cron

```
* /4 * * * * /etc/mrtg/mrtg.sh
```

3. Сформировать график сетевой активности

## MRTG Index Page

Traffic Analysis for eth0 -- kali



**MRTG** MULTI ROUTER TRAFFIC GRAPHER  
version 2.17.10  
Tobias Oetiker <tohi@oetiker.ch>  
and Dave Rand <dlr@bungl.com>

4. Создать кольцевую БД rrd и обеспечить её постоянное обновление данными сетевой активности

### Создание колцевой БД

```
(root@kali)-[/var/local]
# rrdtool create eth0.rrd --step 300 DS:input:COUNTER:600:U:U\
DS:output:COUNTER:600:U:U RRA:AVERAGE:0.5:1:576 RRA:MAX:0.5:1:576\
RRA:AVERAGE:0.5:6:672 RRA:MAX:0.5:6:672 RRA:AVERAGE:0.5:24:732\
RRA:MAX:0.5:24:732 RRA:AVERAGE:0.5:144:1460 RRA:MAX:0.5:144:1460
```

### Создание скрипта обновления

```
GNU nano 7.2 /home/kali/rrd_cron.sh
#!/bin/bash
INPUT=`/sbin/ifconfig $1 |grep bytes | cut -d ' ' -f 14 | head -n1`
OUTPUT=`/sbin/ifconfig $1 |grep bytes | cut -d ' ' -f 14 | head -n2|tail -n1`
rrdtool update /var/local/eth0.rrd -t "input:output" N:$INPUT:$OUTPUT
```

### Настройка cron

```
*/* * * * * /var/local/eth1_update.sh
```

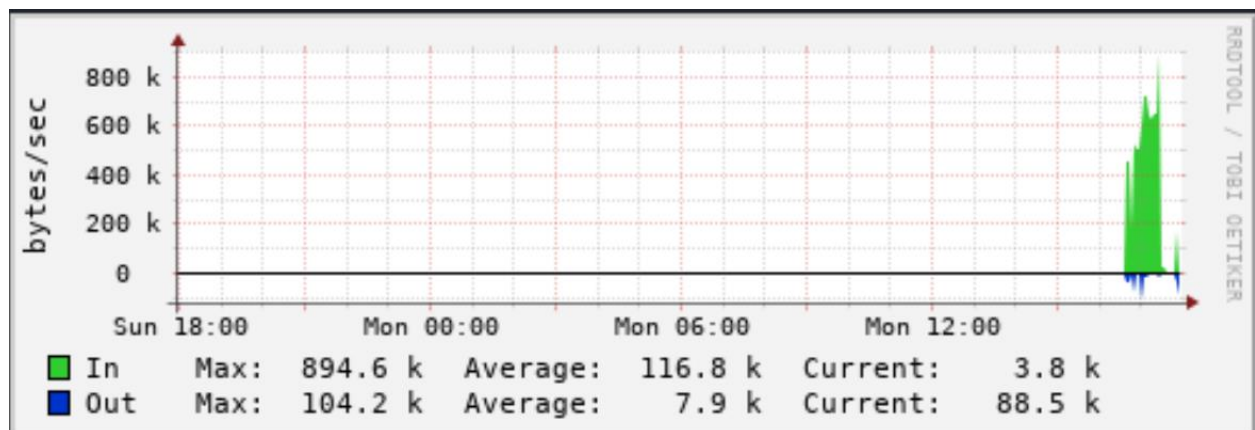


## 5. Сгенерировать график сетевой активности за заданный промежуток времени

### Генерация графика

```
(root@kali)-[/var/local]
# rrdtool graph net.png -v bytes/sec --slope-mode --imgformat PNG\
DEF:input=eth0.rrd:input:AVERAGE DEF:output=eth0.rrd:output:AVERAGE\
CDEF:output_neg=output,-1,* AREA:input#32CD32:"In " "GPRINT:input:MAX: Max\\: %6.1lf\
%s" "GPRINT:input:AVERAGE:Average\\: %6.1lf %S" "GPRINT:input:LAST:Current\\: %6.1lf\
%S\\n" HRULE:0#000000 AREA:output_neg#0033CC:"Out" "GPRINT:output:MAX: Max\\:\
%6.1lf %S" "GPRINT:output:AVERAGE:Average\\: %6.1lf %S"\
"GPRINT:output:LAST:Current\\: %6.1lf %S\\n"
```

### График



6. Проверить работоспособность при обращении к некоторым общедоступным веб-ресурсам при помощи утилит трассировки маршрута

Тело скрипта

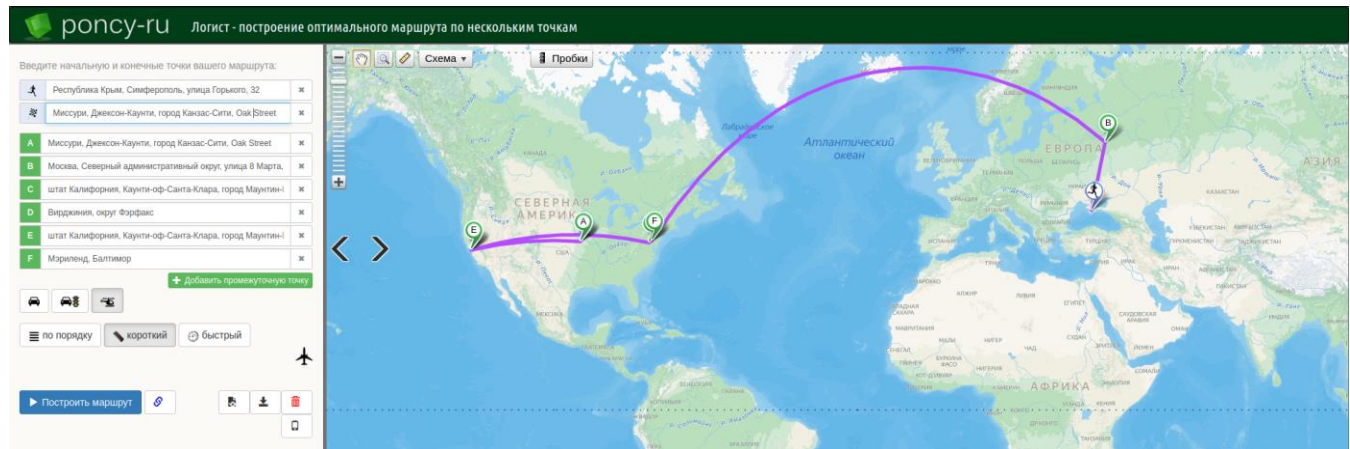
```
GNU nano 7.2 geo_traceroute.py S
import subprocess
import re
import requests
import sys
import pyperclip

if __name__ == '__main__':
    # доступ к первому аргументу
    arg1 = sys.argv[1]
    # ваш код с использованием переданных аргументов
    # Get traceroute information
    traceroute_output = subprocess.check_output(['traceroute', str(arg1)]).decode('utf-8')
    # Regular expression to match IP addresses in the traceroute output
    ip_regex = re.compile(r'\d+\.\d+\.\d+\.\d+')
    # Loop through each IP address in the traceroute output
    geo_list = []
    geo_prev = [0,0]
    for ip in ip_regex.findall(traceroute_output):
        # Get the location information for the IP address
        url = f'http://ip-api.com/json/{ip}?fields=lat,lon'
        response = requests.get(url)

        if response.status_code == 200:
            data = response.json()
            if 'lat' in data and 'lon' in data:
                geo = [data['lat'], data['lon']]
                if geo_prev != geo:
                    geo_list.append(geo)
                    geo_prev = geo
    geo_start = geo_list.pop(0)
    geo_end = geo_list.pop()
    geo_formatted = {"start":geo_start,"end":geo_end,"points":geo_list,"method":4,"optimization":2,"center":geo_start}
    text = f"http://news.cigarexpert.ru/route/{geo_formatted}"
    text = text.replace('\\', '\\')
    text = text.replace(' ', '')
    #text = text.replace('{', '%7B')
    #text = text.replace('}', '%7D')
    #text = text.replace('[', '%5B')
    #text = text.replace(']', '%5D')
    print(text)
    pyperclip.copy(text)
```

## Пример скрипта

```
(kali@kali)-[/var/local/geo_traceroute]
$ python3 geo_traceroute.py kaggle.com
http://news.cigarexpert.ru/route/{ "start": [44.9529, 34.0919], "end": [39.0997, -94.5785], "points": [[39.0997, -94.5785], [55.8004, 37.5557], [37.422, -122.084], [38.8754, -77.3853], [37.422, -122.084], [39.2891, -76.5583]], "method": 4, "optimization": 2, "center": [44.9529, 34.0919]}
```



**Вывод:** В ходе данной лабораторной работе я получил навыков использования утилит мониторинга сети, сбор статистической информации и представление ее в графическом виде, написал скрипты для выполнения данных задач, также проверил работу утилит и приобрел навыки написания скриптов