

**Министерство науки и высшего образования Российской
Федерации**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

Факультет безопасности информационных технологий

Дисциплина:

ОТЧЁТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 2:

“ Обработка и тарификация трафика NetFlow”

Вариант 14

Выполнил:

Студент группы N3351

Нгуен Туан Ань

Проверил:

Аспирант ФБИТ

Университет ИТМО

Федоров И.Р.

Санкт-Петербург, 2020 г.

Цель работы

Реализование простейшее правило тарификации для услуг типа “Интернет” по общему объему трафика NetFlow за отчетный период. Работа включает в себя 4 этапа:

- Привести данный файл в читабельный вид
- Сформировать собственный файл для тарификации любого формата, с которым удобно работать
- Построить график зависимости объема трафика от времени
- Протарифицировать трафик

Описание реализованной работы

Вариант 14:

Протарифицировать абонента с IP-адресом 192.168.250.39

с коэффициентом k: 0,5руб/Мб после достижения 1000Мб

Правила тарификации услуг “Интернет”:

$$X = Q * k,$$

где X - итоговая стоимость, Q - общий объем трафика NetFlow за отчетный период, k - множитель тарифного плана (у каждого варианта свой).

➤ *Предобразование данного файла в читабельный вид*

```
$ nfdump -r nfcapd.202002251200 -o "fmt:%sa,%da,%byt,%ts,%te" |
```

```

192.168.250.27, 196.55.253.206, 204,2020-02-25 12:29:43.350,2020-02-25 12:29:52.350
192.168.250.27, 149.154.167.92, 204,2020-02-25 12:29:43.350,2020-02-25 12:29:52.350
192.168.250.27, 149.154.167.92, 204,2020-02-25 12:29:43.380,2020-02-25 12:29:52.390
192.168.250.3, 192.168.250.1, 186,2020-02-25 12:29:52.760,2020-02-25 12:29:52.760
192.168.250.1, 192.168.250.3, 995,2020-02-25 12:29:52.760,2020-02-25 12:29:52.760
192.168.250.3, 93.92.192.5, 2969,2020-02-25 12:29:52.770,2020-02-25 12:29:52.770
93.92.192.5, 217.15.20.194, 2528,2020-02-25 12:29:52.770,2020-02-25 12:29:52.770
192.168.250.41, 95.100.188.86, 6971,2020-02-25 12:29:52.830,2020-02-25 12:29:52.830
192.168.250.41, 192.168.250.1, 144,2020-02-25 12:29:52.830,2020-02-25 12:29:52.830
95.100.188.86, 217.15.20.194, 7156,2020-02-25 12:29:52.830,2020-02-25 12:29:52.830
192.168.250.1, 192.168.250.41, 768,2020-02-25 12:29:52.860,2020-02-25 12:29:52.860
104.122.242.221, 217.15.20.194, 40262,2020-02-25 12:29:12.670,2020-02-25 12:29:53.210
192.168.250.41, 104.122.242.221, 4600,2020-02-25 12:29:12.610,2020-02-25 12:29:53.210
104.122.246.192, 217.15.20.194, 1.9 M,2020-02-25 12:29:08.980,2020-02-25 12:29:53.390
192.168.250.41, 104.122.246.192, 35157,2020-02-25 12:29:08.900,2020-02-25 12:29:53.390
136.243.148.229, 217.15.20.194, 5224,2020-02-25 12:27:47.100,2020-02-25 12:29:54.810
192.168.250.59, 136.243.148.229, 2401,2020-02-25 12:27:47.050,2020-02-25 12:29:54.810
192.168.250.41, 192.168.250.1, 122,2020-02-25 12:29:55.180,2020-02-25 12:29:55.180
192.168.250.1, 192.168.250.41, 900,2020-02-25 12:29:55.180,2020-02-25 12:29:55.180
31.13.92.36, 217.15.20.194, 1756,2020-02-25 12:28:50.140,2020-02-25 12:29:55.360
192.168.250.41, 31.13.92.36, 2335,2020-02-25 12:28:50.060,2020-02-25 12:29:55.360
192.168.250.41, 17.253.123.201, 737,2020-02-25 12:29:56.770,2020-02-25 12:29:56.770
17.253.123.201, 217.15.20.194, 3477,2020-02-25 12:29:56.780,2020-02-25 12:29:56.780
92.118.38.58, 217.15.20.194, 1031,2020-02-25 12:29:46.030,2020-02-25 12:29:56.920
192.168.250.3, 92.118.38.58, 972,2020-02-25 12:29:46.040,2020-02-25 12:29:56.920
summary: total flows: 17449, total bytes: 220.0 M, total packets: 417314, avg bps: 248857, avg pps: 59, avg bpp: 527

```

➤ Формирование собственного файла для тарификации

```

$ touch data.txt
$ nfdump -r nfcapd.202002251200 -o "fmt:%sa,%da,%byt,%ts,%te" >> data.txt

```

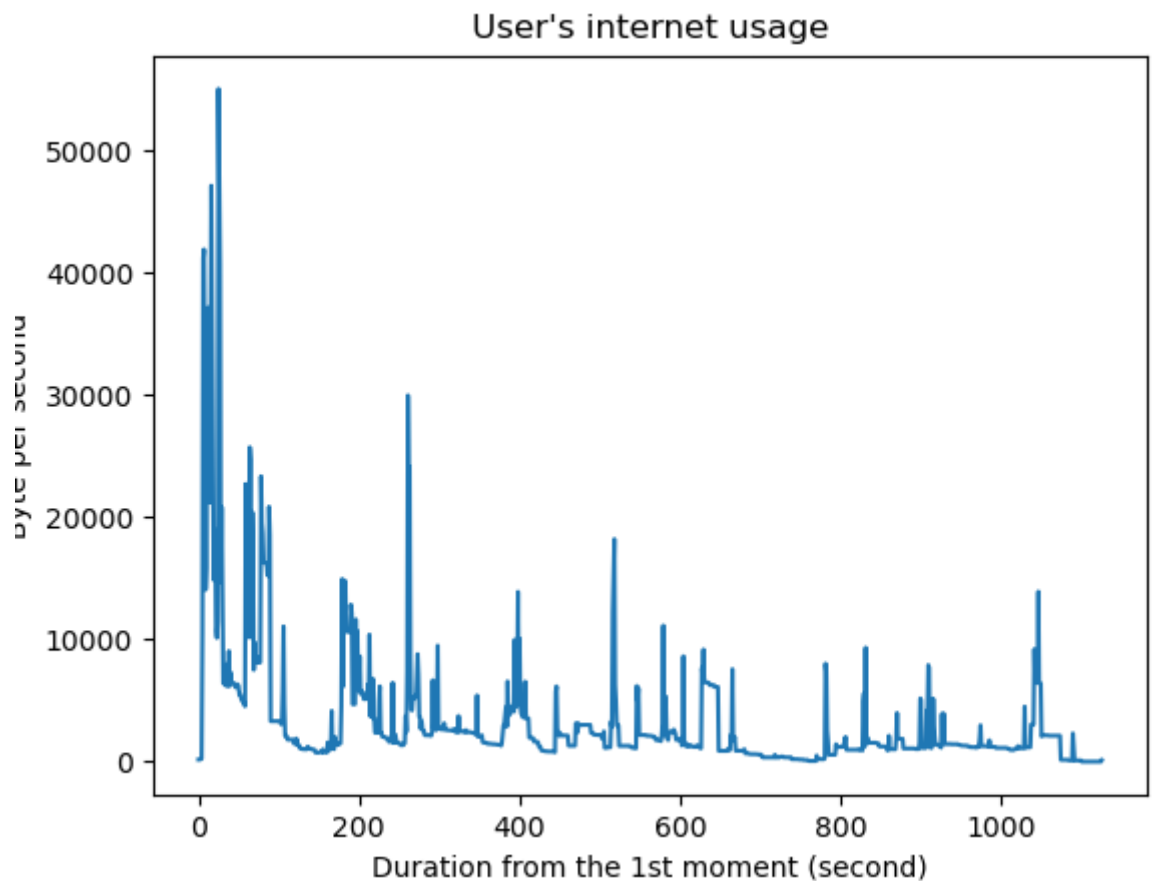
➤ Построение графика зависимости объема трафика от времени

- Ввод: файл netflow с и IP-адресом (192.168.250.39)
- Вывод: график зависимости объема трафика от времени

```

>>> import graphic
>>> graphic.show("192.168.250.39")
█

```



➤ **Тарификация Интернет**

- Ввод: файл netflow с и IP-адресом (192.168.250.39)
- Вывод: тарификации услуг “Интернет”

```
Type "help", "copyright", "credits" or "license" for more information.  
>>> import bill  
>>> bill.total("192.168.250.39")  
3.4954071044921875 data traffic  
price: 1.2477035522460938 rub
```

Вывод

NetFlow — это протокол, разработанный компанией Cisco и предназначенный для сбора информации об IP-трафике внутри сети. Маршрутизаторы Cisco анализируют проходящий через интерфейс трафик, суммируют данные и отправляют статистику в формате NetFlow на специальный узел, называемый NetFlow Collector.

NetFlow часто используется для ведения биллинга или для анализа трафика сети.

Протокол существует в нескольких версиях, последняя версия 9 предназначена для учёта трафика между АС (Автономная Система) и в импортируемых данных имеет несколько дополнительных полей таких как АС источника, АС назначения и пр., но обычно, для биллинга в несложной сети внутри одной АС достаточно информации, содержащейся в данных NetFlow версии 5.