Министерство науки высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»

Факультет безопасности информационных технологий

Управление мобильными устройствами

Лабораторная работа №2
Обработка и тарификация трафика NetFlow

Выполнил: студент группы N3351
Заднепровский Кирилл Дмитриевич
Вариант 5

Проверил: инженер ФБИТ,
Университет ИТМО,
Фёдоров Иван Романович

Санкт-Петербург
2020

Цель работы: написать программный модуль для обработки и тарификации трафика NetFlow.

Задачи: обработка файла-дампа созданного nfcapd, формирование собственного файла для тарификации, выборка нужных строк для обработки, тарификация выбранных записей, построение графика зависимости объема трафика от времени.

Задание лабораторной работы

Правила тарификации услуг “Интернет”:

X = Q * k,где

•X–итоговая стоимость,

•Q –общий объем трафика NetFlow за отчетный период,

•k–множитель тарифного плана

Исходные данные

Абонент - 192.168.250.59

k = 1

$k_{беспл}$ = 1000 Мб

Файл nfcapd.202002251200, содержащий трафик NetFlow v5 для разных абонентов

Практическая часть

С помощью утилиты nfdump исходный файл с трафиком был конвертирован в формат csv. Также в нем было оставлен только трафик для абонента 192.168.250.59.

```
kirill@kirill-N150SC:~$ nfdump -o csv -r nfcapd 'ip 192.168.250.59' > 192.168.2
50.59.csv
```

Рисунок 1. Выполненная команда с опциями

ts	te	td	sa	da	sp	dp	pr	flg	fwd	stos	ipkt	ibyt	opkt	obyt	in	out	sas	das	smk	dmk	dtos	dir	nh	nhb	svln	dvln	ismc
2020-02-25 11:51:04	2020-02-25 11:51:04	0.000	192.168.250.59	192.168.250.1	50360	53	UDP	.....	0	0	2	126	0	0	1	0	0	0	0	0	0	0.0.0.0	0.0.0.0	0	0	0:00:00:00:
2020-02-25 11:51:04	2020-02-25 11:51:04	0.000	192.168.250.1	192.168.250.59	53	50360	UDP	.....	0	0	2	676	0	0	0	1	0	0	0	0	0	0.0.0.0	0.0.0.0	0	0	0:00:00:00:
2020-02-25 11:51:04	2020-02-25 11:51:04	0.000	192.168.250.59	17.253.123.204	50024	80	TCP	CE....	0	0	7	519	0	0	1	4	0	0	0	0	0	0.0.0.0	0.0.0.0	0	0	0:00:00:00:
2020-02-25 11:51:04	2020-02-25 11:51:04	0.000	192.168.250.59	192.168.250.1	53646	53	UDP	.....	0	0	2	146	0	0	1	0	0	0	0	0	0	0.0.0.0	0.0.0.0	0	0	0:00:00:00:
2020-02-25 11:51:04	2020-02-25 11:51:04	0.000	192.168.250.1	192.168.250.59	53	53646	UDP	.....	0	0	2	146	0	0	0	1	0	0	0	0	0	0.0.0.0	0.0.0.0	0	0	0:00:00:00:
2020-02-25 11:51:04	2020-02-25 11:51:04	0.000	192.168.250.59	192.168.250.1	64789	53	UDP	.....	0	0	2	128	0	0	1	0	0	0	0	0	0	0.0.0.0	0.0.0.0	0	0	0:00:00:00:
2020-02-25 11:51:04	2020-02-25 11:51:04	0.000	192.168.250.1	192.168.250.59	53	64789	UDP	.....	0	0	2	1054	0	0	0	1	0	0	0	0	0	0.0.0.0	0.0.0.0	0	0	0:00:00:00:
2020-02-25 11:51:04	2020-02-25 11:51:04	0.000	192.168.250.59	192.168.250.1	50025	53	TCP	CE....	0	0	3	168	0	0	1	0	0	0	0	0	0	0.0.0.0	0.0.0.0	0	0	0:00:00:00:
2020-02-25 11:51:04	2020-02-25 11:51:04	0.000	192.168.250.1	192.168.250.59	53	50025	TCP	.E.A..	0	0	2	120	0	0	0	1	0	0	0	0	0	0.0.0.0	0.0.0.0	0	0	0:00:00:00:
2020-02-25 11:51:04	2020-02-25 11:51:04	0.000	192.168.250.59	54.76.9.103	50026	443	TCP	CE....	0	0	17	2779	0	0	1	4	0	0	0	0	0	0.0.0.0	0.0.0.0	0	0	0:00:00:00:
2020-02-25 11:51:04	2020-02-25 11:51:04	0.000	192.168.250.59	192.168.250.1	60330	53	UDP	.....	0	0	2	132	0	0	1	0	0	0	0	0	0	0.0.0.0	0.0.0.0	0	0	0:00:00:00:
2020-02-25 11:51:04	2020-02-25 11:51:04	0.000	192.168.250.1	192.168.250.59	53	60330	UDP	.....	0	0	2	660	0	0	0	1	0	0	0	0	0	0.0.0.0	0.0.0.0	0	0	0:00:00:00:
2020-02-25 11:51:04	2020-02-25 11:51:04	0.000	192.168.250.59	52.50.170.249	50027	443	TCP	CE....	0	0	19	4238	0	0	1	4	0	0	0	0	0	0.0.0.0	0.0.0.0	0	0	0:00:00:00:
2020-02-25 11:51:04	2020-02-25 11:51:04	0.000	192.168.250.59	192.168.250.1	58122	53	UDP	.....	0	0	2	118	0	0	1	0	0	0	0	0	0	0.0.0.0	0.0.0.0	0	0	0:00:00:00:
2020-02-25 11:51:04	2020-02-25 11:51:04	0.000	192.168.250.59	192.168.250.1	55941	53	UDP	.....	0	0	2	156	0	0	1	0	0	0	0	0	0	0.0.0.0	0.0.0.0	0	0	0:00:00:00:
2020-02-25 11:51:04	2020-02-25 11:51:04	0.000	192.168.250.59	192.168.250.1	64067	53	UDP	.....	0	0	2	132	0	0	1	0	0	0	0	0	0	0.0.0.0	0.0.0.0	0	0	0:00:00:00:
2020-02-25 11:51:04	2020-02-25 11:51:04	0.000	192.168.250.59	192.168.250.1	63028	53	UDP	.....	0	0	2	140	0	0	1	0	0	0	0	0	0	0.0.0.0	0.0.0.0	0	0	0:00:00:00:
2020-02-25 11:51:04	2020-02-25 11:51:04	0.000	192.168.250.1	192.168.250.59	53	58122	UDP	.....	0	0	2	682	0	0	0	1	0	0	0	0	0	0.0.0.0	0.0.0.0	0	0	0:00:00:00:
2020-02-25 11:51:04	2020-02-25 11:51:04	0.000	192.168.250.1	192.168.250.59	53	55941	UDP	.....	0	0	2	658	0	0	0	1	0	0	0	0	0	0.0.0.0	0.0.0.0	0	0	0:00:00:00:
2020-02-25 11:51:04	2020-02-25 11:51:04	0.000	192.168.250.1	192.168.250.59	53	64067	UDP	.....	0	0	2	620	0	0	0	1	0	0	0	0	0	0.0.0.0	0.0.0.0	0	0	0:00:00:00:
2020-02-25 11:51:04	2020-02-25 11:51:04	0.000	192.168.250.1	192.168.250.59	53	63028	UDP	.....	0	0	2	844	0	0	0	1	0	0	0	0	0	0.0.0.0	0.0.0.0	0	0	0:00:00:00:
2020-02-25 11:51:04	2020-02-25 11:51:04	0.000	192.168.250.59	192.168.250.1	58828	53	UDP	.....	0	0	2	130	0	0	1	0	0	0	0	0	0	0.0.0.0	0.0.0.0	0	0	0:00:00:00:
2020-02-25 11:51:04	2020-02-25 11:51:04	0.000	192.168.250.59	192.168.250.1	51992	53	UDP	.....	0	0	2	124	0	0	1	0	0	0	0	0	0	0.0.0.0	0.0.0.0	0	0	0:00:00:00:
2020-02-25 11:51:04	2020-02-25 11:51:04	0.000	192.168.250.1	192.168.250.59	53	58828	UDP	.....	0	0	2	736	0	0	0	1	0	0	0	0	0	0.0.0.0	0.0.0.0	0	0	0:00:00:00:
2020-02-25 11:51:04	2020-02-25 11:51:04	0.000	192.168.250.59	17.188.133.34	50028	443	TCP	CE....	0	0	15	1634	0	0	1	4	0	0	0	0	0	0.0.0.0	0.0.0.0	0	0	0:00:00:00:
2020-02-25 11:51:04	2020-02-25 11:51:04	0.000	192.168.250.1	192.168.250.59	53	51992	UDP	.....	0	0	2	1078	0	0	0	1	0	0	0	0	0	0.0.0.0	0.0.0.0	0	0	0:00:00:00:

Рисунок 1. Фрагмент, полученного файла

Полученный файл позволяет выполнять тарификацию любого формата.

Так как правило тарификации по заданию содержит только суммарный объем трафика и множитель тарифного плана, а файл содержит трафик для единственного абонента, в программной реализации обрабатывались значения следующих полей:

- ts – Время начала передачи
- ibyt – Количество байт

Для реализации данного программного модуля был выбран язык программирования высокого уровня Python 3, так как его применение удобно при решении прикладных задач, а также в его стандартную библиотеку входят модуль по обработке csv файлов и модуль для построения графиков.

Исходный код размещен на GitHub: https://github.com/kirillNvrsk/MDM2

```
Объем траффика: 8497255 b, 8497.255Kb

Цена: 7497.254999999999
```

Рисунок 2. Вывод результата работы программы

Так как объем трафика составил менее 1000 Мб, согласно заданию, единица учета была уменьшена.

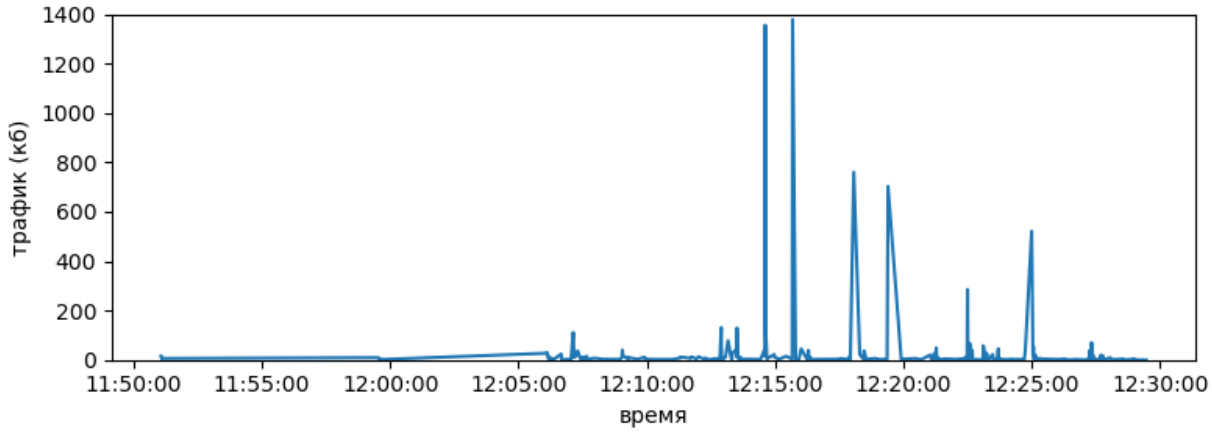

Рисунок 3. График зависимости объема трафика от времени, построенный программой

Выводы: в процессе выполнения лабораторной работы были изучены основы обработки трафика NetFlow v5, правила тарификации для услуги «Интернет» по

объему трафика. Был разработан программный модуль, позволяющий произвести тарификацию абонента, указанного в варианте, а также построить график зависимости объема трафика от времени.