

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО
ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ,
МЕХАНИКИ И ОПТИКИ»


Факультет безопасности информационных технологий

Дисциплина:
«Управление мобильными устройствами»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 2
«Обработка и тарификация трафика NetFlow»

Выполнил:

студент гр. N3354, Гранов И.С.

 / Гранов И.С. /

Проверил:

аспирант, Федоров И.Р.

_____ / Федоров И.Р. /

Отметка о выполнении: _____

Цель работы:

Сконвертировать дампы NetFlow Collector'a в читабельный вид, реализовать в виде программного модуля обработчик данных сконвертированных дампов, построить график зависимости объема трафика от времени.

Задание (вариант #3):

Протарифицировать абонента с IP-адресом 192.168.250.27 с коэффициентом к: 1руб/Мб

Описание работы:

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.

Для реализации программного модуля была взята программа из предыдущей лабораторной работы (CDRHandler), после чего был допилен новый функционал, позволяющий получить .csv файл, необходимый для построения графика зависимости объема трафика от времени. Промежуточный csv файл для работы программы был получен при помощи утилиты nfdump, после чего скорректирован применением регулярных выражений в Notepad++.

Исходный код и все сопутствующие материалы представлены в удаленном репозитории, размещенном по адресу <https://github.com/UnkownUser13/Mobile-Device-Management/tree/master/lab1>

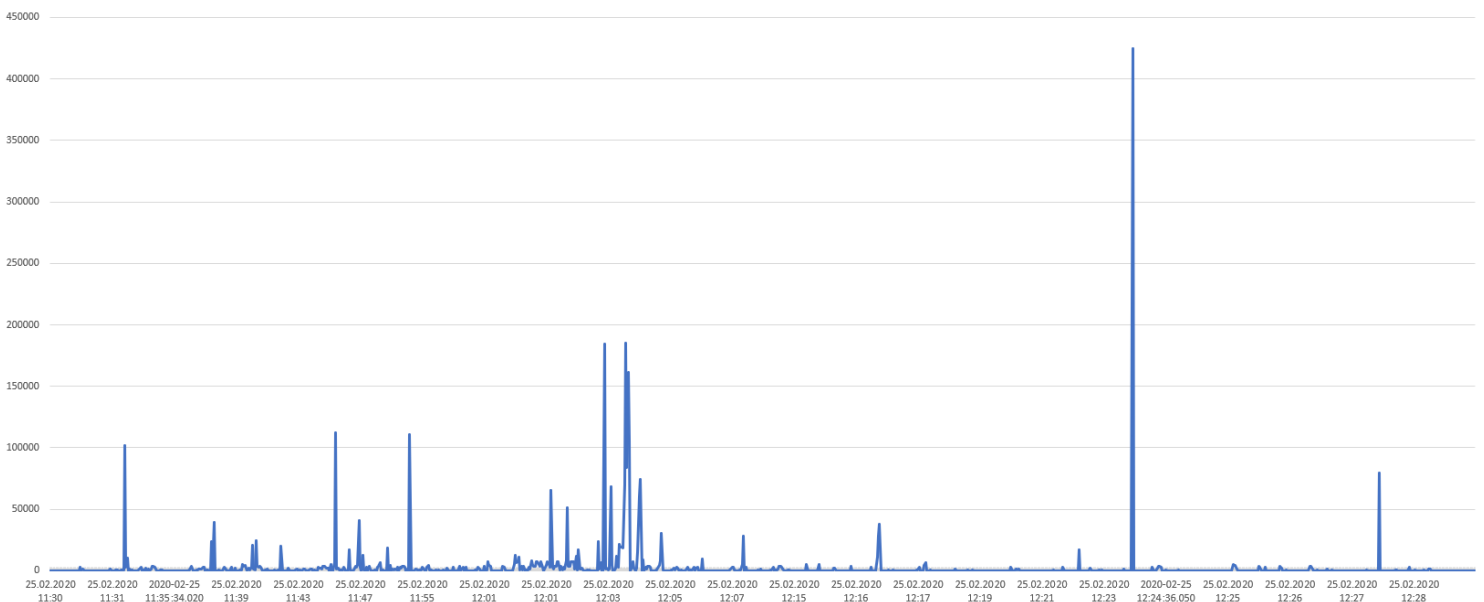
Пример работы программы на одной из рабочих станций автора:

```

2020-02-25 12:28:47.340 8.990 TCP 192.168.250.27:55511 149.154.167.92:443 4 204 1
2020-02-25 12:28:47.340 8.990 TCP 192.168.250.27:55510 196.55.253.206:4760 4 204 1
2020-02-25 12:28:47.360 9.000 TCP 192.168.250.27:55514 149.154.167.92:80 4 204 1
2020-02-25 12:28:55.340 8.990 TCP 192.168.250.27:55519 149.154.167.92:443 4 204 1
2020-02-25 12:28:55.340 8.990 TCP 192.168.250.27:55518 196.55.253.206:4760 4 204 1
2020-02-25 12:28:55.360 9.000 TCP 192.168.250.27:55522 149.154.167.92:80 4 204 1
2020-02-25 12:28:46.780 21.980 TCP 192.168.250.27:55507 81.19.104.163:443 8 670 1
2020-02-25 12:29:03.340 9.000 TCP 192.168.250.27:55525 196.55.253.206:4760 4 204 1
2020-02-25 12:29:03.340 9.010 TCP 192.168.250.27:55526 149.154.167.92:443 4 204 1
2020-02-25 12:29:03.360 9.010 TCP 192.168.250.27:55529 149.154.167.92:80 4 204 1
2020-02-25 12:28:46.780 25.980 TCP 192.168.250.27:55508 81.19.104.163:443 11 1084 1
2020-02-25 12:28:46.790 25.970 TCP 192.168.250.27:55509 81.19.104.163:443 11 1100 1
2020-02-25 12:29:11.350 8.990 TCP 192.168.250.27:55532 196.55.253.206:4760 4 204 1
2020-02-25 12:29:11.350 8.990 TCP 192.168.250.27:55533 149.154.167.92:443 4 204 1
2020-02-25 12:29:11.370 9.000 TCP 192.168.250.27:55536 149.154.167.92:80 4 204 1
2020-02-25 12:29:19.350 9.000 TCP 192.168.250.27:55539 196.55.253.206:4760 4 204 1
2020-02-25 12:29:19.350 9.010 TCP 192.168.250.27:55540 149.154.167.92:443 4 204 1
2020-02-25 12:29:19.370 9.000 TCP 192.168.250.27:55543 149.154.167.92:80 4 204 1
2020-02-25 12:29:27.350 8.990 TCP 192.168.250.27:55546 196.55.253.206:4760 4 204 1
2020-02-25 12:29:27.350 9.000 TCP 192.168.250.27:55550 149.154.167.92:80 4 204 1
2020-02-25 12:29:27.350 9.010 TCP 192.168.250.27:55547 149.154.167.92:443 4 204 1
2020-02-25 12:29:37.700 0.000 UDP 192.168.250.27:62598 192.168.250.1:53 2 156 1
2020-02-25 12:29:37.700 0.000 UDP 192.168.250.27:62599 192.168.250.1:53 2 156 1
2020-02-25 12:29:37.710 0.000 UDP 192.168.250.27:62600 192.168.250.1:53 2 158 1
2020-02-25 12:29:37.710 0.000 UDP 192.168.250.27:62601 192.168.250.1:53 2 158 1
2020-02-25 12:29:37.710 0.000 UDP 192.168.250.27:62602 192.168.250.1:53 2 156 1
2020-02-25 12:29:37.710 0.000 UDP 192.168.250.27:62603 192.168.250.1:53 2 156 1
2020-02-25 12:29:37.720 0.000 UDP 192.168.250.27:62604 192.168.250.1:53 2 176 1
2020-02-25 12:29:37.720 0.000 UDP 192.168.250.27:62605 192.168.250.1:53 2 176 1
2020-02-25 12:29:37.720 0.000 UDP 192.168.250.27:62606 192.168.250.1:53 2 154 1
2020-02-25 12:29:37.720 0.000 UDP 192.168.250.27:62607 192.168.250.1:53 2 154 1
2020-02-25 12:29:37.720 0.000 UDP 192.168.250.27:62608 192.168.250.1:53 2 154 1
2020-02-25 12:29:37.720 0.000 UDP 192.168.250.27:62609 192.168.250.1:53 2 154 1
2020-02-25 12:29:37.730 0.000 UDP 192.168.250.27:62610 192.168.250.1:53 2 152 1
2020-02-25 12:29:37.730 0.000 UDP 192.168.250.27:62611 192.168.250.1:53 2 152 1
2020-02-25 12:29:37.740 0.000 UDP 192.168.250.27:62612 192.168.250.1:53 2 156 1
2020-02-25 12:29:37.740 0.000 UDP 192.168.250.27:62613 192.168.250.1:53 2 156 1
2020-02-25 12:29:37.740 0.000 UDP 192.168.250.27:62614 192.168.250.1:53 2 152 1
2020-02-25 12:29:37.740 0.000 UDP 192.168.250.27:62615 192.168.250.1:53 2 152 1
2020-02-25 12:29:37.750 0.000 UDP 192.168.250.27:62616 192.168.250.1:53 2 160 1
2020-02-25 12:29:37.750 0.000 UDP 192.168.250.27:62617 192.168.250.1:53 2 160 1
2020-02-25 12:29:37.790 0.000 TCP 192.168.250.27:55560 195.122.177.183:443 5 224 1
2020-02-25 12:29:35.360 9.000 TCP 192.168.250.27:55554 149.154.167.92:443 4 204 1
2020-02-25 12:29:35.360 9.010 TCP 192.168.250.27:55553 196.55.253.206:4760 4 204 1
2020-02-25 12:29:35.380 9.000 TCP 192.168.250.27:55557 149.154.167.92:80 4 204 1
2020-02-25 12:29:43.350 9.000 TCP 192.168.250.27:55561 196.55.253.206:4760 4 204 1
2020-02-25 12:29:43.350 9.000 TCP 192.168.250.27:55562 149.154.167.92:443 4 204 1
2020-02-25 12:29:43.380 9.010 TCP 192.168.250.27:55565 149.154.167.92:80 4 204 1
User's [192.168.250.27] fee is 3326 RUB in whats.csv
PS C:\Users\IIIIIG00000R\Desktop> .\java -jar .\NFDRecorder.jar whats.csv 192.168.250.27 1

```

График зависимости объема трафика от времени для 192.168.250.27:



Вывод:

Улучшил понимание механизма расчета тарификации, реализовал программный модуль для тарификации трафика абонента.