Санкт-Петербургский Политехнический Университет Петра Великого

Институт металлургии, машиностроения и транспорта

Кафедра «Мехатроника и роботостроение»

Отчет по лабораторной работе

Дисциплина «Сети ЭВМ»

Тема: «. Средства анализа пакетного трафика. Утилита Tcpdump (Windump)»

Выполнил:

Студент гр. 33328/1

Е. Э. Хомутов

Санкт-Петербург

2018

Цель работы

• Ознакомление с принципами работы программ анализа пакетного

трафика;

• Практическое освоение приемов сбора и анализа трафика с помощью

утилиты Tcpdump (Windump);

• Получение навыков расшифровки выходных результатов работы

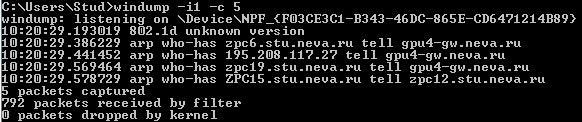
утилиты Tcpdump.(Windump).

Программа работы.

1. Запустить программу Tcpdump, ознакомиться с форматом вывода и

основными опциями (–c, –e, –q, –n, –x).

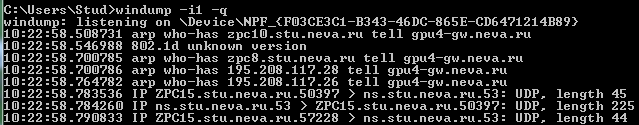
-c выход после обработки count пакетов



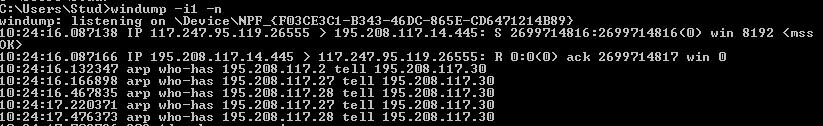
-e выводит заголовки канального уровня в каждой новой строке



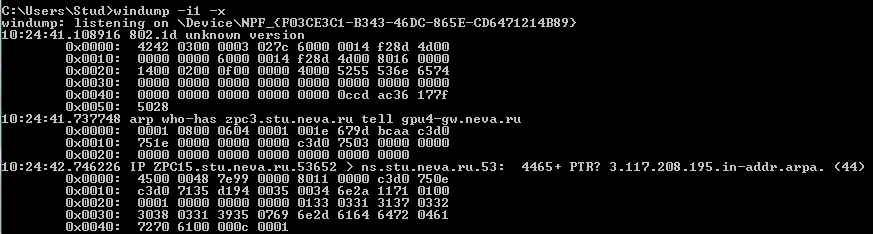
-q выводит информацию в сокращенном виде



-n не преобразовывать адреса (т.e. адрес хоста, номер порта и т.д.) в имена



-x выводит каждый пакет в шестнадцатеричном виде

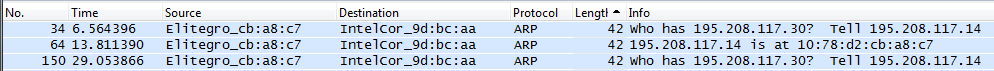


11 NVP-II Network Voice Protocol – 8бит -протокол верхнего уровня

2. Средствами программы Tcpdump определить минимальный и

максимальный размер пакетов в сети.

Остановив перехват пакетов и включив сортировку по возрастанию размера пакета, определим, что максимальный размер: , минимальный -42 байт





3. Запустить программу Tcpdump с записью необработанных

результатов в файл Rowdump.

4. Во время работы программы Tcpdump по п.3 выполнить операции

в соответствии с индивидуальным заданием:

a) Обратиться к WEB-серверу.

b) Обратиться к FTP-серверу

c) Выполнить команду Ping . Сохранить результат в файле ping.txt

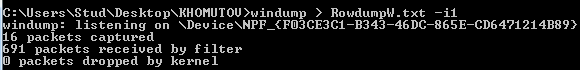
d) Выполнить команду Traceroute. Сохранить результат в файле

trace.txt

Пункты 3-4 рекомендуется выполнять по подпунктам:

a) Запустить программу Tcpdump с записью необработанных

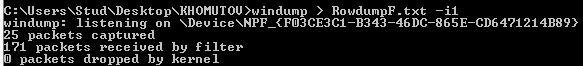
результатов в файл RowdumpW. Обратиться к WEB-серверу.



После ответа сервера остановить Tcpdump.

b) Запустить программу Tcpdump с записью необработанных

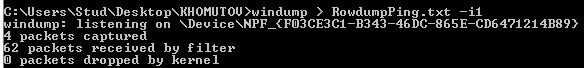
результатов в файл RowdumpF. Обратиться к FTP-серверу.

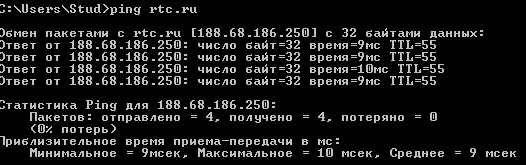


После ответа сервера остановить Tcpdump.

c) Запустить программу Tcpdump с записью необработанных

результатов в файл RowdumpPing. Выполнить команду Ping .



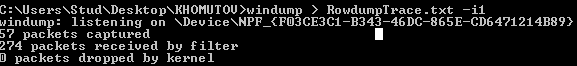


Сохранить результат (вывод команды Ping) в файле ping.txt.

Остановить Tcpdump.

d) Запустить программу Tcpdump с записью необработанных

результатов в файл RowdumpTrace. Выполнить команду tracert.





Сохранить результат в файле trace.txt. Остановить Tcpdump.

5. Обработать файл Rowdump (файлы RowdumpW, RowdumpF,

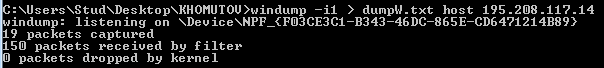
RowdumpPing, RowdumpTrace) с целью вывода только пакетов,

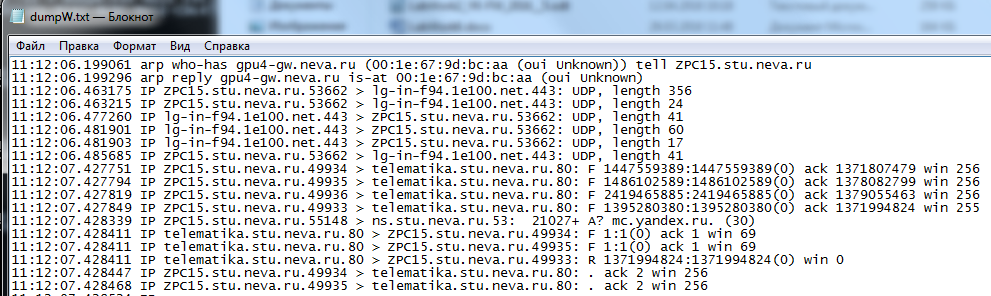
отправленных или принятых Вашим компьютером (вывод Tcpdump для всех

пакетов вашего компьютера). Сохранить результаты в файлах dumpW.txt,

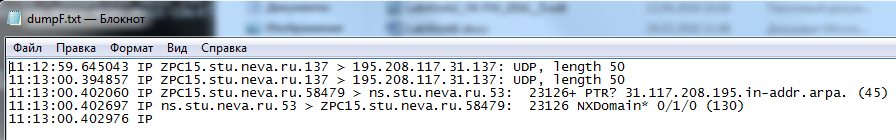
dumpF.txt, dumping.txt. dumptrace.txt соответственно. Пометить в файлах .txt

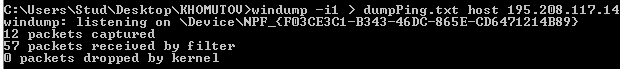
пакеты, относящиеся к п. 4 (a, b, c, d соответственно).

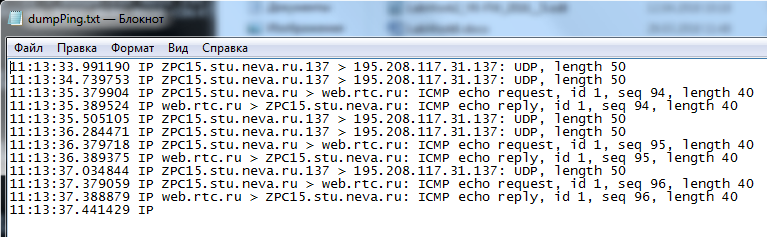


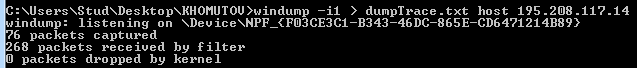


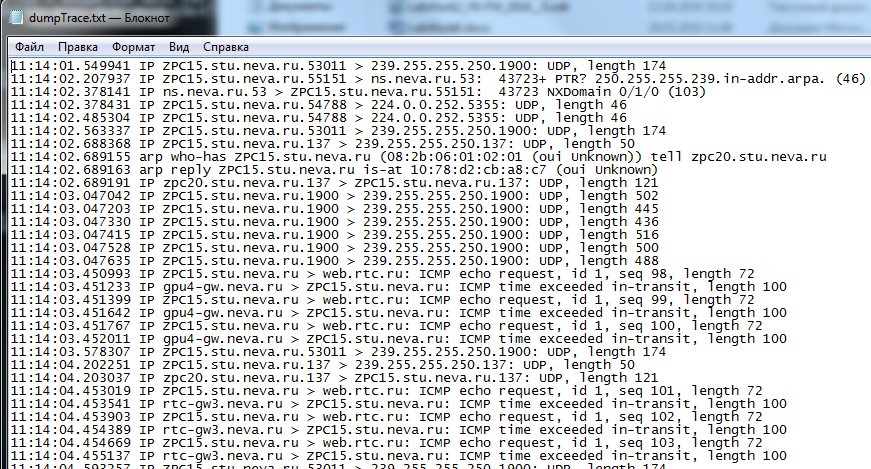












В отчете представить:

1. Номер рабочего места 15 и IP-адрес ПК – 195.208.117.14

2. Команды (с комментариями) и результаты для опций по п.1.

3. Для каждой опции привести вывод 3-4 пакетов. При выводе IPпакетов

с опцией –x, расшифровать заголовок IP-пакета.

4. Команды (с комментариями), использованные при выполнении п. 2,

и полученные результаты.

5. Команды, использованные при выполнении пп. 3, 4, 5.

6. Распечатки файлов ping.txt и trace.txt.

7. Распечатки фрагментов (не более 1 стр.) файлов dumpW.txt,

dumpF.txt, dumping.txt. dumptrace.txt dump2.txt с помеченными пакетами,

относящимися к пп. 4 a, b, c, d, соответственно. Определить значение

задержки эхо-отклика (icmp) по файлу dumpPing.txt, сравнить с результатом

в файле ping.txt.

8. Выводы по всем пунктам работы.