МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий

Кафедра информатики и систем управления

Отчет по лабораторной работе №1

по дисциплине

Сети и телекоммуникации

«Работа с утилитами ping, traceroute.

Работа с анализаторами протоколов tcpdump и wireshark»

РУКОВОДИТЕЛЬ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Гай В.Е

(подпись)

СТУДЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Лашук А.Д.

(подпись)

Группа: 17-АС

Работа защищена «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_

С оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Нижний Новгород, 2020

**Цель работы:**

Получение базовых навыков по работе с утилитами ping, traceroute и с анализаторами протоколов tcpdump и wireshark.

**Порядок выполнения работы:**

**1 Часть:**

1. С помощью утилиты ping проверить состояние связи с узлами. Число отправляемых запросов N берется из таблицы 2. Результаты выполнения сохранить для отчета.

2. При помощи утилиты traceroute произвести трассировку узлов. Результаты протоколировать в файл. По результатам составить графики времени прохождения шлюзов для каждого узла (для 3-х пакетов), указать наиболее узкие места в сети.

3. Получить маршрут прохождения пакетов до одного из заданных в варианте узлов при помощи утилиты ping. Результаты протоколировать в файл.

**2 Часть:**

**Работа с анализатором протоколов tcpdump**

1. Запустить tcpdump в режиме захвата всех пакетов, проходящих по сети. Количество захватываемых пакетов ограничить 10. Результаты протоколировать в файл.

2. Запустить tcpdump в режиме перехвата широковещательного трафика (фильтр по MACадресу). Количество захватываемых пакетов ограничить 5. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня).

3. Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определенный IP-адрес (возможные адреса можно посмотреть на схеме ЛВС лаб. 521). При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 3. Для генерирования пакетов возпользоваться утилитой ping.

4. Запустить tcpdump в режиме сохранения данных в двоичном режиме так, чтобы он перехватывал пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 7. Результат работы программы писать в файл.

5. Прочесть программой tcpdump созданный в предыдущем пункте файл

**Работа с анализатором протоколов wireshark**

1. Захватить 5-7 пакетов широковещательного трафика (фильтр по IP-адресу). Результат сохранить в текстовый файл.

2. Захватить 3-4 пакета ICMP, полученных от определенного узла. Для генерирования пакетов возпользоваться утилитой ping. Результат сохранить в текстовый файл.

3. Перехватить пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. По результатам построить диаграмму Flow Graph. Диаграмму сохранить либо в виде текстового файла либо в виде изображения.

4. Прочесть файл, созданный программой tcpdump. Сравнить с тем, что было получено утилитой wireshark.

Вариант 6:

[www.rambler.ru](http://www.rambler.ru)

[www.cisco.com](http://www.cisco.com)

[www.opera.com](http://www.opera.com)

1)

Число отправляемых пакетов 6.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Доменное имя | IP-адрес | Страна | Число потерянных запросов | Среднее время прохождения запроса, мс | TTL |
| [www.rambler.ru](http://www.rambler.ru) | 81.19.82.98 | Россия | 0 | 13 | 56 |
| [www.cisco.com](http://www.cisco.com)  e2867.dsca.akamaiedge.net | 2.22.38.25 | США | 0 | 29 | 57 |
| [www.opera.com](http://www.opera.com)  front-tls-geo.opcom-prod.route53.opera.com | 52.58.116.196 | США | 6 | Превышен интервал ожидания для запроса. |  |

2)

Трассировка маршрута к www.rambler.ru [81.19.82.98]

с максимальным числом прыжков 30:

1 2 ms 5 ms 1 ms 192.168.0.1 [192.168.0.1]

2 15 ms 2 ms 5 ms dynamicip-95-79-247-253.pppoe.nn.ertelecom.ru [95.79.247.253]

3 6 ms 3 ms 5 ms lag-3-438.bgw01.nn.ertelecom.ru [91.144.185.248]

4 7 ms 8 ms 11 ms ertelecom.w-ix.ru [193.106.112.151]

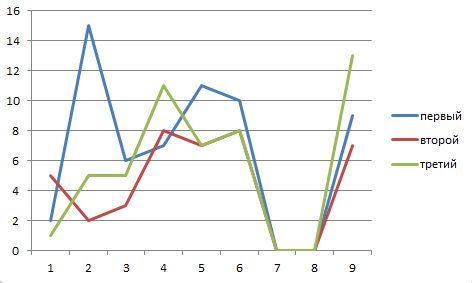
5 11 ms 7 ms 7 ms rambler.w-ix.ru [193.106.112.214]

6 10 ms 8 ms 8 ms ae4.j-mx240.kr.ramtel.ru [81.19.64.85]

7 \* \* \* Превышен интервал ожидания для запроса.

8 \* \* \* Превышен интервал ожидания для запроса.

9 9 ms 7 ms 13 ms www.rambler.ru [81.19.82.98]



Трассировка маршрута к www.cisco.com [2.22.38.25]

с максимальным числом прыжков 30:

1 2 ms 1 ms 5 ms 192.168.0.1 [192.168.0.1]

2 6 ms 8 ms 4 ms dynamicip-95-79-247-253.pppoe.nn.ertelecom.ru [95.79.247.253]

3 2 ms 5 ms 1 ms lag-3-438.bgw01.nn.ertelecom.ru [91.144.185.248]

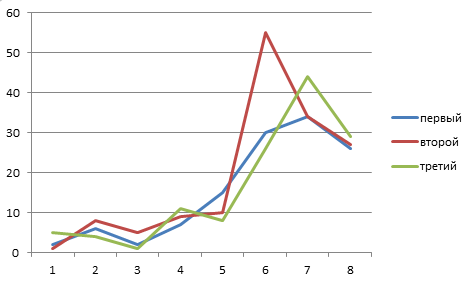
4 7 ms 9 ms 11 ms ertelekom-ic-313399-mow-b4.c.telia.net [62.115.12.110]

5 15 ms 10 ms 8 ms mow-b4-link.telia.net [62.115.12.109]

6 30 ms 55 ms 26 ms s-bb3-link.telia.net [62.115.116.232]

7 34 ms 34 ms 44 ms s-b5-link.telia.net [62.115.137.159]

8 26 ms 27 ms 29 ms a2-22-38-25.deploy.static.akamaitechnologies.com [2.22.38.25]



Трассировка маршрута к front-tls-geo.opcom-prod.route53.opera.com [52.58.116.196]

с максимальным числом прыжков 30:

1 5 ms 5 ms \* 192.168.0.1 [192.168.0.1]

2 \* \* \* Превышен интервал ожидания для запроса.

3 7 ms 4 ms 5 ms lag-3-438.bgw01.nn.ertelecom.ru [91.144.185.248]

4 13 ms 10 ms 17 ms 99.82.182.1

5 49 ms 60 ms 48 ms 99.82.182.0

6 \* \* \* Превышен интервал ожидания для запроса.

7 \* \* \* Превышен интервал ожидания для запроса.

8 45 ms \* 1319 ms 52.93.111.179

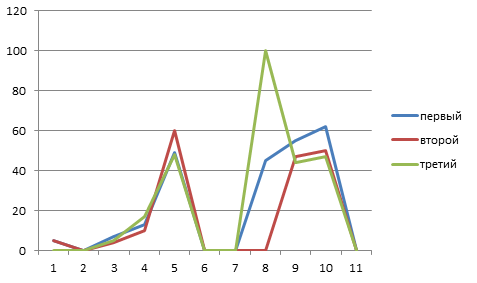
9 55 ms 47 ms 44 ms 54.239.107.29

10 62 ms 50 ms 47 ms 54.239.5.134

11 \* \* \* Превышен интервал ожидания для запроса.

12 \* \* \* Превышен интервал ожидания для запроса.

13 \* \* \* Превышен интервал ожидания для запроса.



**Наиболее узкие места в сети**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| [www.rambler.ru](http://www.rambler.ru) | | | [www.cisco.com](http://www.cisco.com) | | | [www.opera.com](http://www.opera.com) | | |
| 1 пакет | 2 пакет | 3 пакет | 1 пакет | 2 пакет | 3 пакет | 1 пакет | 2 пакет | 3 пакет |
| 15 | 8 | 13 | 34 | 55 | 44 | 62 | 60 | 1319 |

3)

C:\Users\Acer>ping -n 1 -r 9 www.cisco.com

Обмен пакетами с e2867.dsca.akamaiedge.net [23.32.100.29] с 32 байтами данных:

Ответ от 23.32.100.29: число байт=32 время=76мс TTL=57

Маршрут: 109.184.107.6 ->

188.254.2.28 ->

81.177.113.61 ->

87.226.134.112 ->

195.2.1.107 ->

195.2.1.93 ->

95.101.13.129 ->

23.32.100.29 ->

23.32.100.29

Статистика Ping для 23.32.100.29:

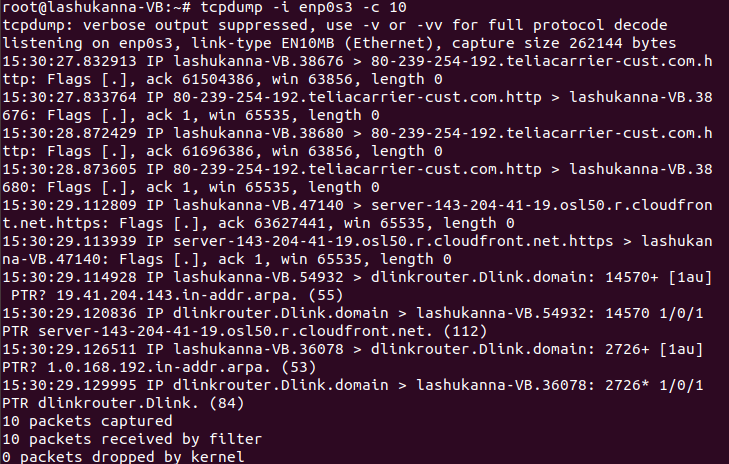
Пакетов: отправлено = 1, получено = 1, потеряно = 0

Приблизительное время приема-передачи в мс:

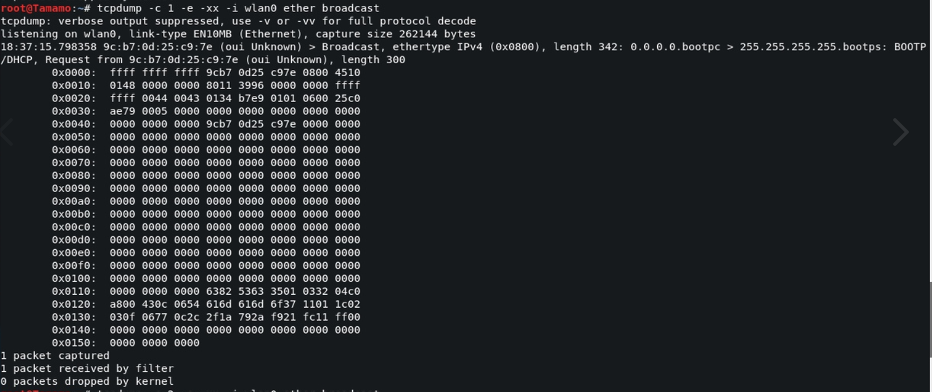
Минимальное = 76мсек, Максимальное = 76 мсек, Среднее = 76 мсек

Часть 2:

1. Запустить tcpdump в режиме захвата всех пакетов, проходящих по сети. Количество захватываемых пакетов ограничить 10.

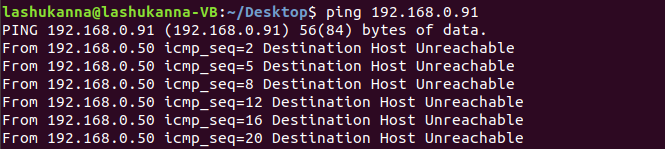


2) Запустить tcpdump в режиме перехвата широковещательного трафика. Включить распечатку пакета в шестнадцатеричной системе(включая заголовок канального уровня).

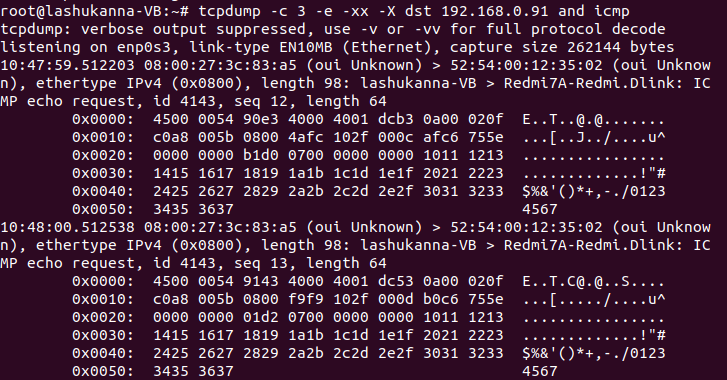


3)

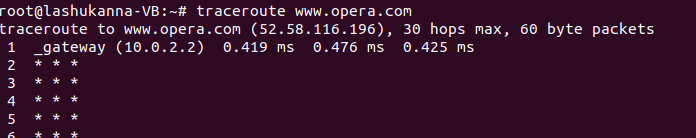
Генерируем пакеты с помощью утилиты ping



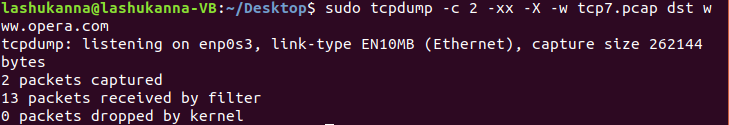
Перехватываем пакеты icmp, отправленные на 192.168.0.91



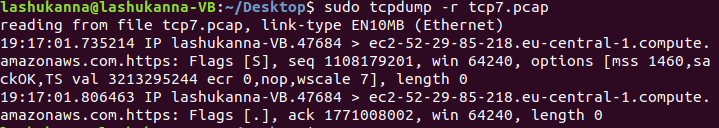
4) Запустить tcpdump в режиме сохранения данных в двоичном режиме так, чтобы он перехватывал пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 7. Результат работы программы писать в файл.



Перехватываем пакеты и записываем их в файл

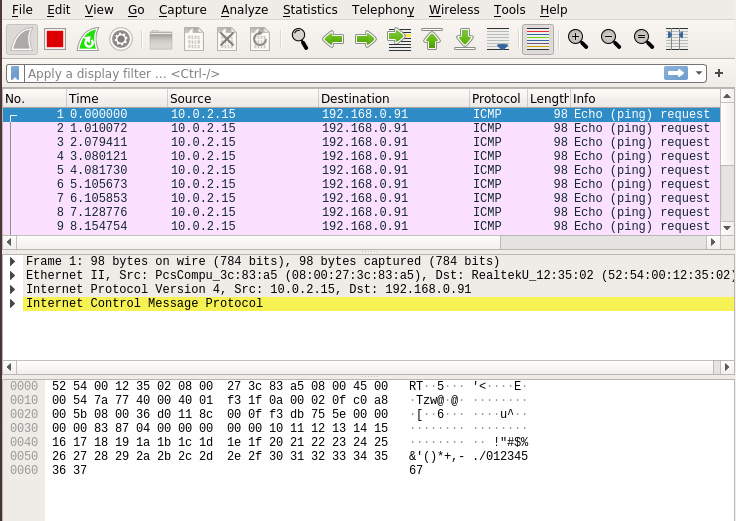


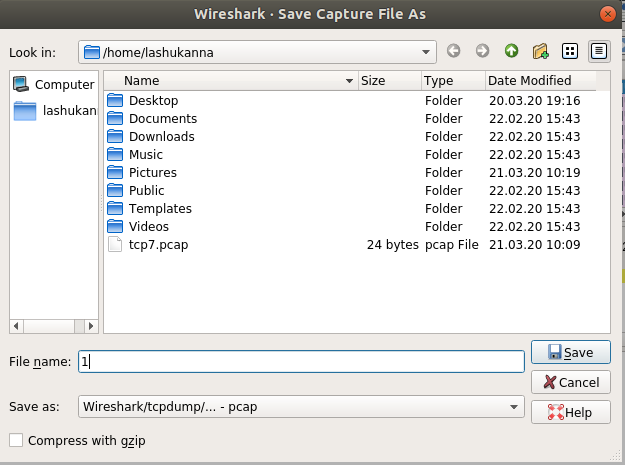
5) Прочесть программой tcpdump созданный в предыдушем пункте файл.



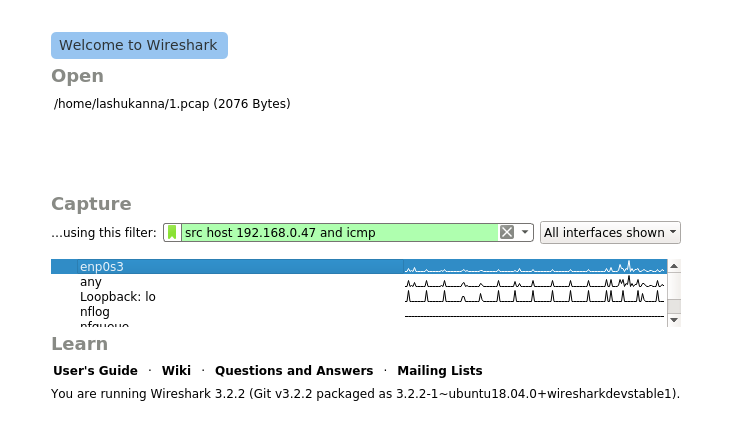
**Работа с анализатором протоколов wireshark**

1. Перехватить пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. По результатам построить диаграмму Floe Graph. Диаграмму сохранить в виде текстового файла(либо в виде изображения).

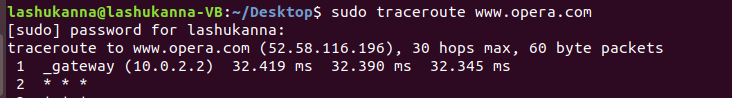


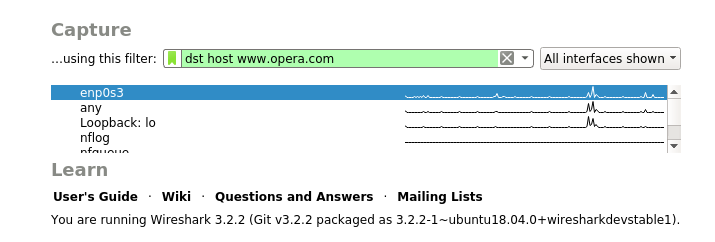


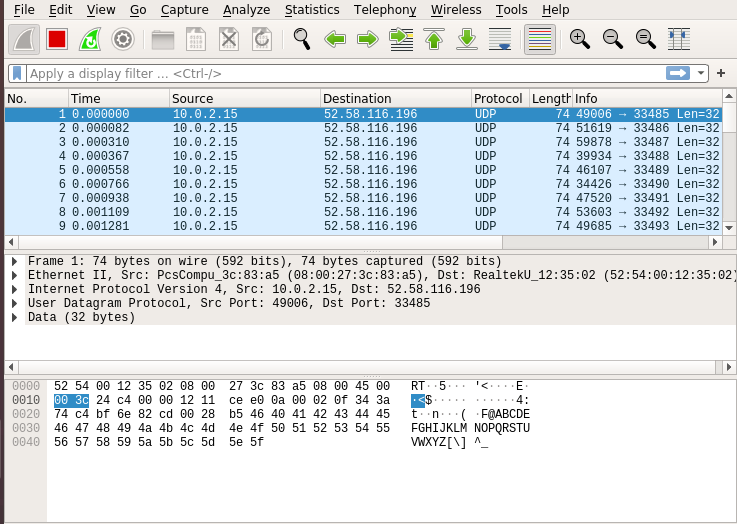
1. Захватить 3-4 пакета ICMP, полученных от определенного узла. Для генерирования пакетов воспользоваться утилитой ping. Результат сохранить в текстовый файл.

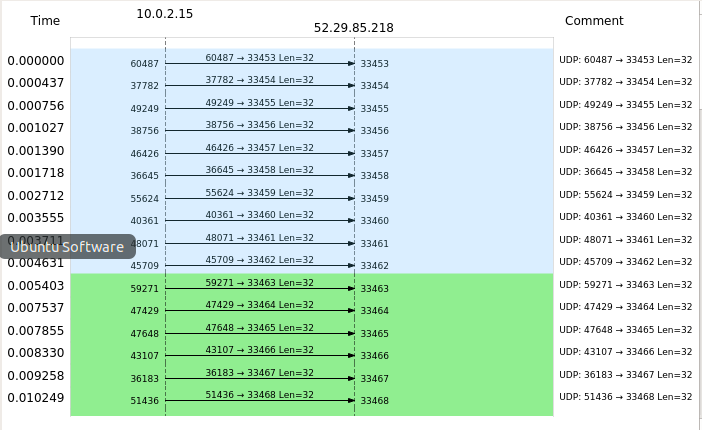


3) Перехватить пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. По результатам построить диаграмму Floe Graph. Диаграмму сохранить в виде текстового файла(либо в виде изображения).









4) Прочесть файл, созданный программой tcpdump. Сравнить с тем, что было получено утилитой wireshark.

