МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего 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, mtr и tracemap. Работа с анализаторами протоколов tcpdump и wireshark»

РУКОВОДИТЕЛЬ:

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

(подпись)

СТУДЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Жолобов Д.М.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись)

17-АС

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

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

Нижний Новгород, 2020

**Часть 1.**

**Цель лабораторной работы:**

Получение базовых навыков по работе с утилитами ping, traceroute, mtr и tracemap.

**Задание:**

Вариант 6.

Исследуемые узлы в сети Internet :

www.rambler.ru

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

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

Параметры утилиты ping:

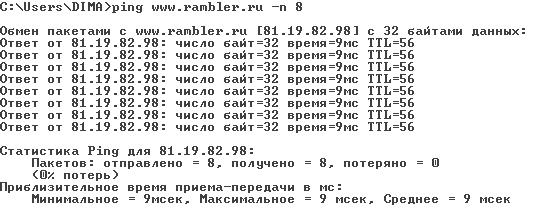
Число отправляемых пакетов N = 8

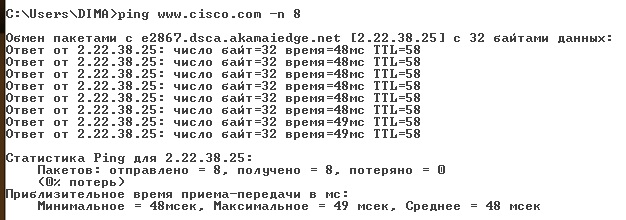
**Выполнение лабораторной работы:**

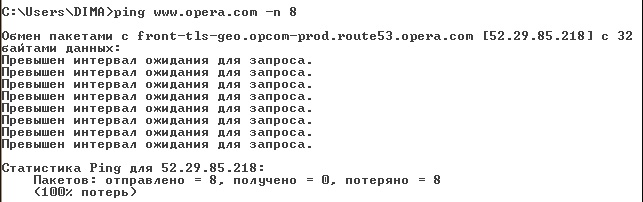
1. С помощью утилиты ping проверяем состояние связи с узлами:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Доменное имя** | **IP-адрес** | **Страна** | **Число потерянных запросов** | **Среднее время прохождения запросов, мс** | **TTL** |
| www.rambler.ru | 81.19.82.98 | Россия | 0 | 23 | 56 |
| [www.cisco.com](http://www.cisco.com) | 2.22.38.25 | Россия | 0 | 48 | 58 |
| [www.opera.com](http://www.opera.com) | 52.29.85.218 | Россия | 8 | - | - |

**Скриншоты:**

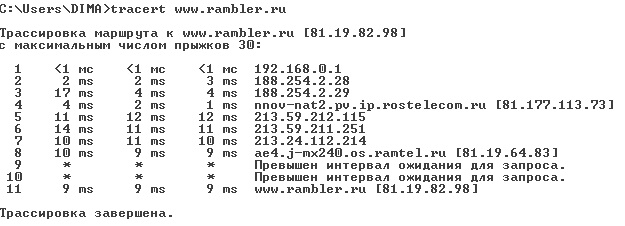




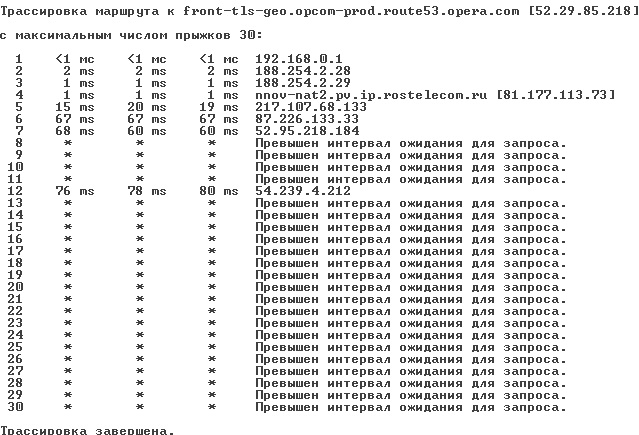


1. При помощи утилиты tracert производим трассировку узлов,заданных в таблице

**Скриншоты:**







По результатам составляем графики времени прохождения шлюзов для каждого узла (для 3-х пакетов), указываем наиболее узкие места в сети(выделены жирным в таблицах).

Узкое место там, где пакет держится дольше всего:

www.rambler.ru

|  |  |  |  |
| --- | --- | --- | --- |
| Количество прыжков | 1 пакет, мс | 2 пакет, мс | 3 пакет, мс |
| 1 | 1 | 1 | 1 |
| 2 | 2 | 2 | 3 |
| 3 | **17** | 4 | 4 |
| 4 | 4 | 2 | 1 |
| 5 | 11 | **12** | **12** |
| 6 | 14 | 11 | 11 |
| 7 | 10 | 11 | 10 |
| 8 | 10 | 9 | 9 |
| 9 | - | - | - |
| 10 | - | - | - |
| 11 | 9 | 9 | 9 |

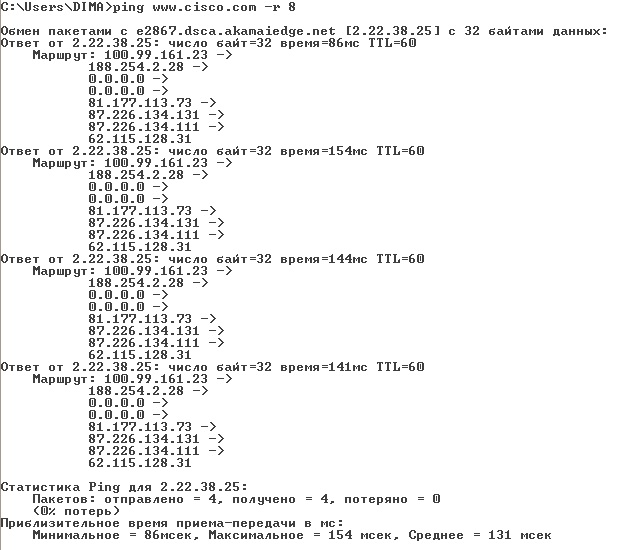
[www.cisco.com](http://www.cisco.com)

|  |  |  |  |
| --- | --- | --- | --- |
| Количество прыжков | 1 пакет, мс | 2 пакет, мс | 3 пакет, мс |
| 1 | 1 | 1 | 1 |
| 2 | 52 | 2 | 2 |
| 3 | 43 | 49 | 29 |
| 4 | 1 | 1 | 1 |
| 5 | **78** | **75** | **72** |
| 6 | 45 | 45 | 45 |
| 7 | 47 | 47 | 47 |
| 8 | 54 | 54 | 54 |
| 9 | 48 | 48 | 48 |

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

|  |  |  |  |
| --- | --- | --- | --- |
| Количество прыжков | 1 пакет, мс | 2 пакет, мс | 3 пакет, мс |
| 1 | 1 | 1 | 1 |
| 2 | 2 | 2 | 2 |
| 3 | 1 | 1 | 1 |
| 4 | 1 | 1 | 1 |
| 5 | 15 | 20 | 19 |
| 6 | 67 | 67 | 67 |
| 7 | 68 | 60 | 60 |
| 8 | - | - | - |
| 9 | - | - | **-** |
| 10 | - | **-** | - |
| 11 | - | - | - |
| 12 | **76** | **78** | **80** |
| 13 | - | - | - |
| 14 | - | - | - |
| 15 | - | - | - |
| 16 | - | - | - |
| 17 | - | - | - |
| 18 | - | - | - |

1. Получаем маршрут прохождения пакетов до одного из заданных в варианте узлов при помощи утилиты ping.



**Часть 2.**

**Цель лабораторной работы:**

Получение базовых навыков по работе с анализаторами протоколов tcpdump и wireshark.

**Задание:**

Вариант 6.

Исследуемые узлы в сети Internet :

[www.industry.su](http://www.industry.su)

1. **Работа с анализатором протоколов tcpdump**
2. Запустить tcpdump в режиме захвата всех пакетов, проходящих по сети. Количество захватываемых пакетов ограничить 10. Результаты протоколировать в файл.

|  |
| --- |
| tcpdump -c 10 -i 1 -w tcpdumpf.pcap |
|  |

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

|  |
| --- |
| tcpdump -c 5 -i 1host industry.su |
|  |

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.

|  |
| --- |
| ping industry.su |
|  |
| tcpdump -c3 -xx -i1dst host 194.58.112.165 and ip proto\icmp |
|  |

1. 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.

|  |
| --- |
| tracert industry.su |
|  |
| tcpdump -c 7 -xx -X -w tcpdumpfile.pcap dst host 194.58.112.165 |
|  |

1. Прочесть программой tcpdump созданный в предыдущем пункте файл

|  |
| --- |
| tcpdump -r tcpdumpfile.pcap |
|  |

1. **Работа с анализатором протоколов wireshark**
2. 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 вварианте 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.

|  |
| --- |
|  |
|  |