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:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Рыкова А.В.

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

(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 3.

Исследуемые узлы в сети Internet :

[www.industry.su](http://www.industry.su) [www.tdpoland.pl](http://www.tdpoland.pl) [www.mysql.com](http://www.mysql.com)

Параметры утилиты ping:

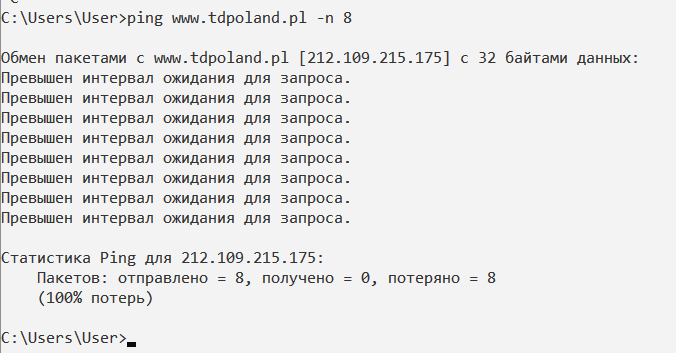
Число отправляемых пакетов N = 8

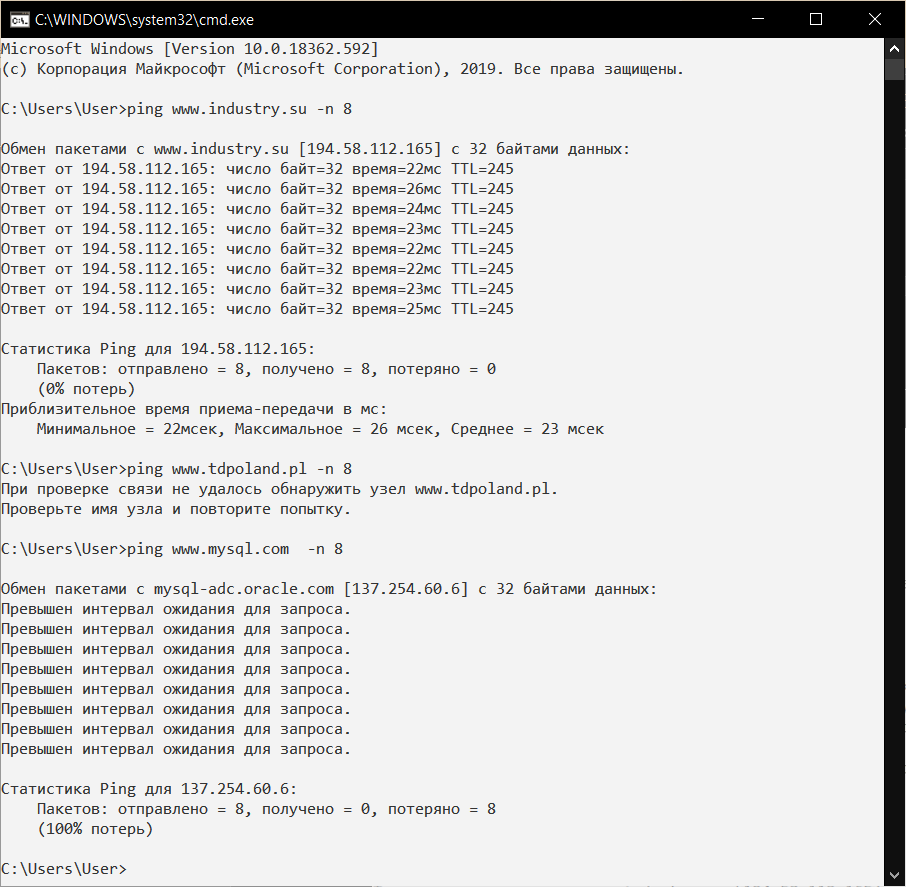
**Выполнение лабораторной работы:**

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.industry.su](http://www.industry.su) | 194.58.112.165 | Россия | 0 | 23 | 245 |
| [www.tdpoland.pl](http://www.tdpoland.pl) | 212.109.215.175 | Россия | 8 | - | - |
| [www.mysql.com](http://www.mysql.com) | 137.254.60.6 | США | 8 | - | - |

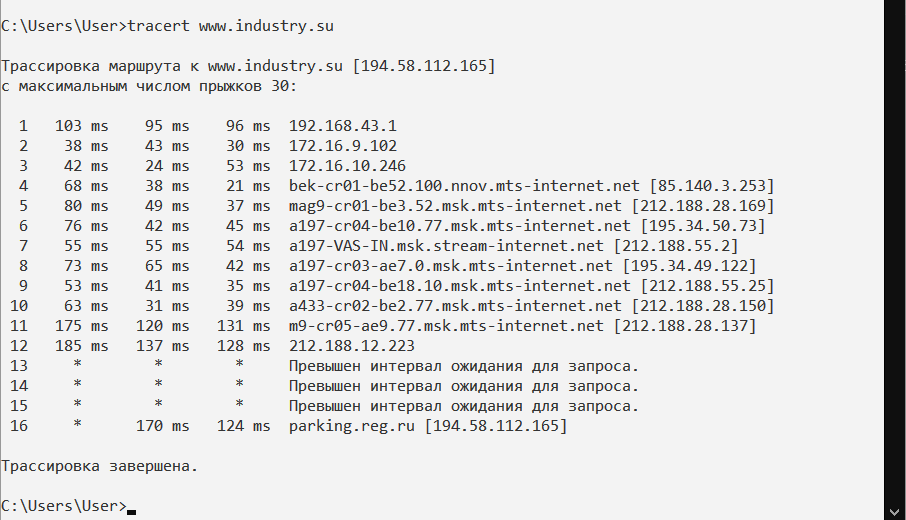
**Скриншоты:**

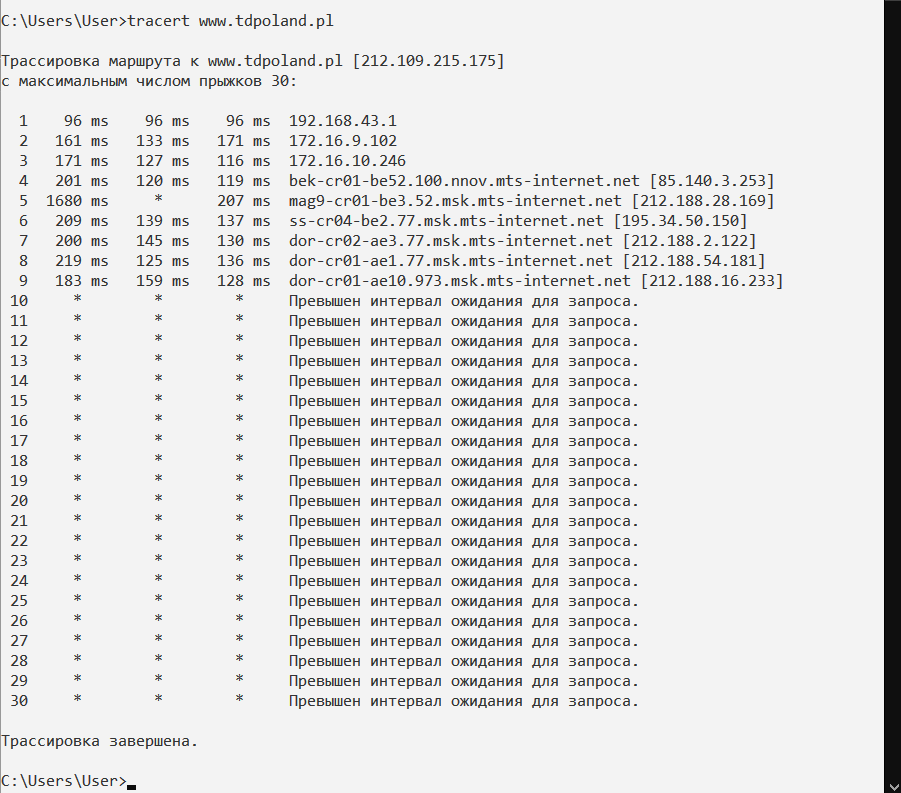


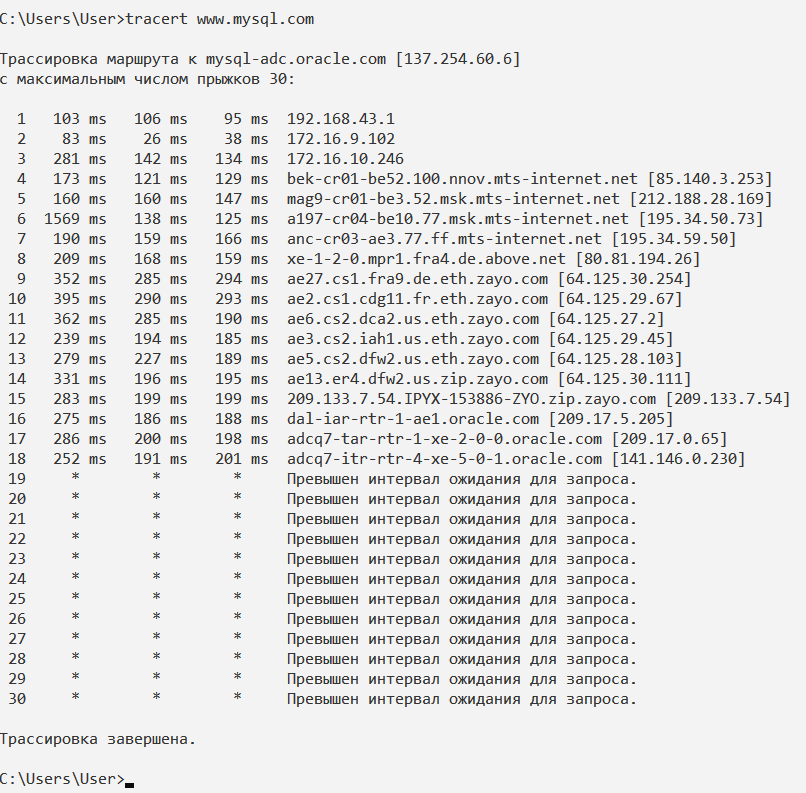


1. При помощи утилиты tracert производим трассировку узлов, заданных в таблице

**Скриншоты:**





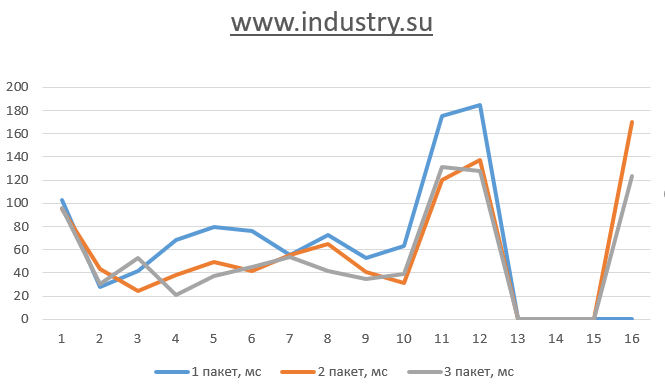


По результатам составляем графики времени прохождения шлюзов для каждого узла (для 3-х пакетов), указываем наиболее узкие места в сети(выделены жирным в таблицах).

Узкое место там, где пакет держится дольше всего:

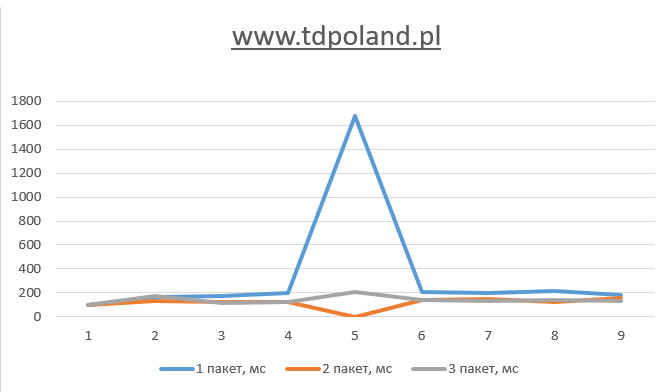
[www.industry.su](http://www.industry.su)

|  |  |  |  |
| --- | --- | --- | --- |
| Количество прыжков | 1 пакет, мс | 2 пакет, мс | 3 пакет, мс |
| 1 | 103 | 95 | 96 |
| 2 | 28 | 43 | 30 |
| 3 | 42 | 24 | 53 |
| 4 | 68 | 38 | 21 |
| 5 | 80 | 49 | 37 |
| 6 | 76 | 42 | 45 |
| 7 | 55 | 55 | 54 |
| 8 | 73 | 65 | 42 |
| 9 | 53 | 41 | 35 |
| 10 | 63 | 31 | 39 |
| 11 | 175 | 120 | **131** |
| 12 | **185** | 137 | 128 |
| 13 | \* | \* | \* |
| 14 | \* | \* | \* |
| 15 | \* | \* | \* |
| 16 | \* | **170** | 124 |



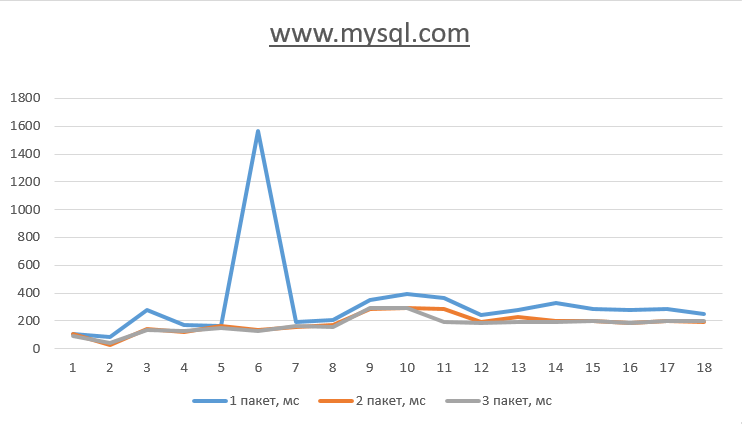
[www.tdpoland.pl](http://www.tdpoland.pl)

|  |  |  |  |
| --- | --- | --- | --- |
| Количество прыжков | 1 пакет, мс | 2 пакет, мс | 3 пакет, мс |
| 1 | 96 | 96 | 96 |
| 2 | 161 | 133 | 171 |
| 3 | 171 | 127 | 116 |
| 4 | 201 | 120 | 119 |
| 5 | **1680** | \* | **207** |
| 6 | 209 | 139 | 137 |
| 7 | 200 | 145 | 130 |
| 8 | 219 | 125 | 136 |
| 9 | 183 | **159** | 128 |

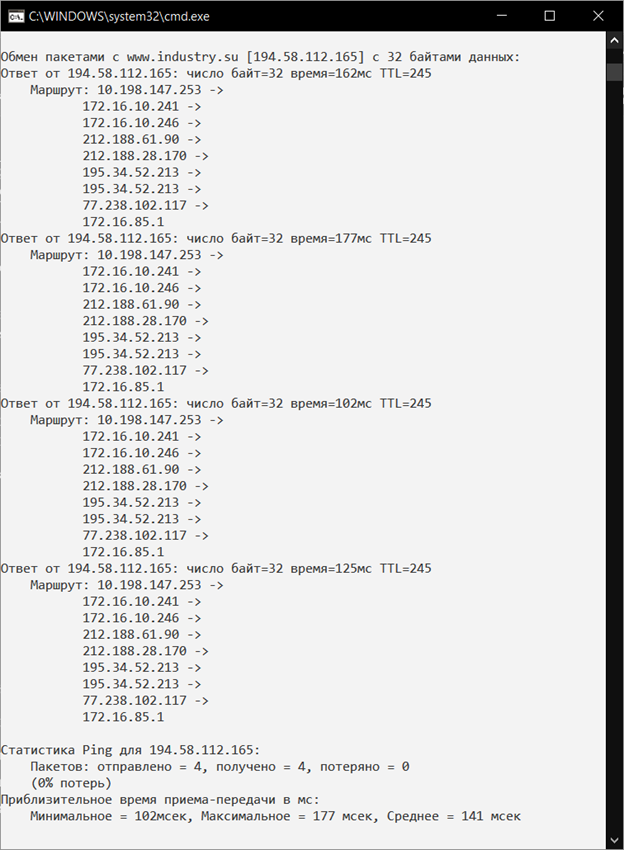


[www.mysql.com](http://www.mysql.com)

|  |  |  |  |
| --- | --- | --- | --- |
| Количество прыжков | 1 пакет, мс | 2 пакет, мс | 3 пакет, мс |
| 1 | 103 | 106 | 95 |
| 2 | 83 | 26 | 38 |
| 3 | 281 | 142 | 134 |
| 4 | 173 | 121 | 129 |
| 5 | 160 | 160 | 147 |
| 6 | **1569** | 138 | 125 |
| 7 | 190 | 159 | 166 |
| 8 | 209 | 168 | 159 |
| 9 | 352 | 285 | **294** |
| 10 | 395 | **290** | 293 |
| 11 | 362 | 285 | 190 |
| 12 | 239 | 194 | 185 |
| 13 | 279 | 227 | 189 |
| 14 | 331 | 196 | 195 |
| 15 | 283 | 199 | 199 |
| 16 | 275 | 186 | 188 |
| 17 | 286 | 200 | 198 |
| 18 | 252 | 191 | 201 |



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 3.

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.

|  |
| --- |
|  |
|  |