# Лабораторная работа № 1. Команды диагностики сети

**Цель работы:**

* Изучить принципы работы простейших средств мониторинга сети.
* Получить навыки решения задач, связанных с мониторингом сети.

**Теоретические основы.**

1. **Протокол icmp**

Протокол icmp (интернет-протокол контрольных сообщений) стека протоколов tcp/ip предназначен для передачи между сетевыми устройствами сообщений об ошибках и контрольных сообщений при помощи ip-пакетов.

В протоколе icmp определены несколько типов сообщений, в том числе см. таблицу 2.1.

**Табл. 2.1 –** Несколько типов сообщений в протоколе

|  |  |  |
| --- | --- | --- |
| Destination unreachable | Time to live exceeded | Parameter problem |
| Source quench | Redirect | Echo |
| Echo reply | Timestamp | Timestamp reply |
| Information request | Information reply | Address request |
| Address reply |  |  |

Например, если маршрутизатор получает пакет, который он не может доставить по указанному в нем адресу, отправителю передается icmp-сообщение о недостижимости адреса (destination unreachable).

1. **Ping: проверка соединения с определенным интерфейсом.**

Программа ping использует протокол icmp.

Эта команда посылает пакет эхо-запроса на другой ip-адрес и ожидает ответа. Она чаще всего используется для того, чтобы посмотреть, «жив ли» другой компьютер. Ответ на запрос содержит также данные о том, как долго пакет путешествовал до адресата. Можно использовать команду ping с различными опциями: число посланных пакетов (от1 до 10), время жизни пакета ( time to live –ttl, от 1 до 255ms), размер пакета (от 16 до 8192 байт), время ожидания (timeout, до 9999 ms) и разрешать или нет фрагментацию каждого пакета.

Формат команды в ос windows:

Ping [-t] [-a] [-n count] [-l size] [-f] [-i ttl] [-v tos]

[-r count] [-s count] [[-j host-list] | [-k host-list]]

[-w timeout] destination-list

Options:

-t выполнение команды до прерывания (ctrl+c)

-a разрешать адреса в имена

-n count число отправляемых пакетов.

-l size размер буфера отправки

-f установить флаг "не фрагментировать".

-i ttl установить время жизни.

-w timeout время ожидания ответа в мс.

-v tos задание типа службы (поле "type of service").

-r count запись маршрута для указанного числа переходов.

-s count штамп времени для указанного числа переходов.

-j host-list свободный выбор маршрута по списку узлов.

-k host-list жесткий выбор маршрута по списку узлов.

Destination-list список рассылки.

1. **Программа tracert. Определение промежуточных сетевых интерфейсов между хостами. Трассировка маршрута.**

Программа трассировки маршрута использует протокол icmp.

Эта утилита очень похожа на ping, за исключением того, что она показывает все другие ip-адреса (интерфейсы), которые пакет проходит до своего места назначения. Дополнительно можно изменять различные опции, ассоциированные с trace route: максимальное число дозволяемых промежуточных узлов (maximum hops, от 1 до 255) и timeout (до 9999 ms).

Формат команды в ос windows:

Tracert [-d] [-h maximum\_hops] [-j host-list] [-w timeout] target\_name

Options:

-d не разрешать адреса в имена.

-h maximum\_hops наибольшее число промежуточных узлов.

-j host-list трассировка через определенный список хостов

-w timeout время ожидания каждого ответа в мс.

1. **Программа netstat. Сетевая статистика.**

Программа **netstat** используется для просмотра активных соединений каждого протокола, таблиц маршрутизации, а так же детализирует статистику передачи данных.

Формат команды в ос windows:

Netstat [-a] [-e] [-n] [-s] [-p имя] [-r] [интервал]

-a отображение всех подключений и ожидающих портов.

(подключения со стороны сервера обычно не отображаются).

-e отображение статистики ethernet. Этот ключ может применяться вместе

С ключом -s.

-n отображение адресов и номеров портов в числовом формате.

-p имя отображение подключений для протокола "имя": tcp или udp.

Используется вместе с ключом -s для отображения статистики по протоколам. Допустимые значения "имя": tcp, udp или ip.

-r отображение содержимого таблицы маршрутов.

-s отображение статистики по протоколам. По умолчанию выводятся данные для tcp, udp и ip. Ключ -p позволяет указать подмножество выводящихся данных.

Интервал повторный вывод статистических данных через указанный интервал в секундах. Для прекращения вывода данных нажмите клавиши ctrl+c. Если параметр не задан, сведения о текущей конфигурации выводятся один раз.

**Инструментарий.**

В работе будут использоваться сети, соединенные с рабочей станцией линками разных типов. Первая сеть (194.85.33.0) доступна через спутниковый канал связи, проходящий через спутниковый ретранслятор на геостационарной орбите с пропускной способностью 512 кбит/с. Вторая сеть 217.23.64.0 доступна через наземный волоконно-оптический канал связи с пропускной способностью 2 мбит/с, третья сеть 212.194.38.0 входит в состав корпоративной сети вуза и доступна в локальной сети с пропускной способностью 10/100 мбит/с.

**Ход работы.**

**Задание 1. Ping.**

Выполните команду ping в командной строке с различными значениями параметров -t, -n, -l, -i,-w. Какие наблюдения и выводы вы сделали?

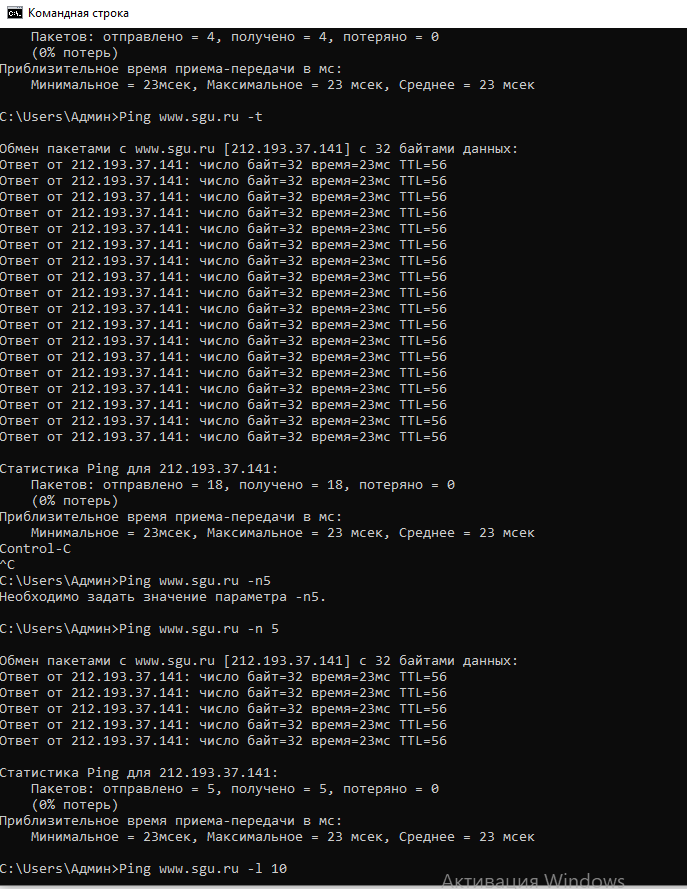
Ping www.sgu.ru

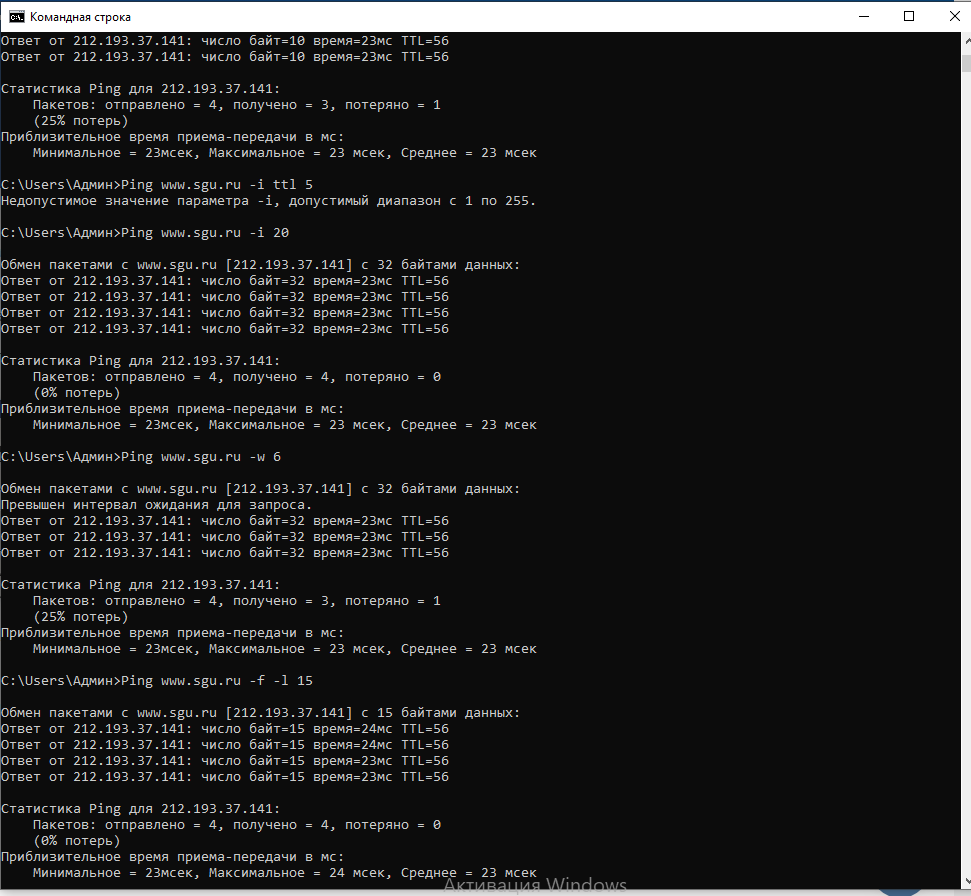
Ping www.microsoft.com

Ping www.sun.com

Ping 212.193.38.83

Выполните ping к тем же хостам с параметром –f, увеличивая параметр -l size. При каком значении размера перестают получаться ответы? При 1500 .





**Задание 2. Tracert.**

Выполните команду tracert в командной строке с различными значениями параметров. Какие наблюдения и выводы вы сделали?

Используйте, например,

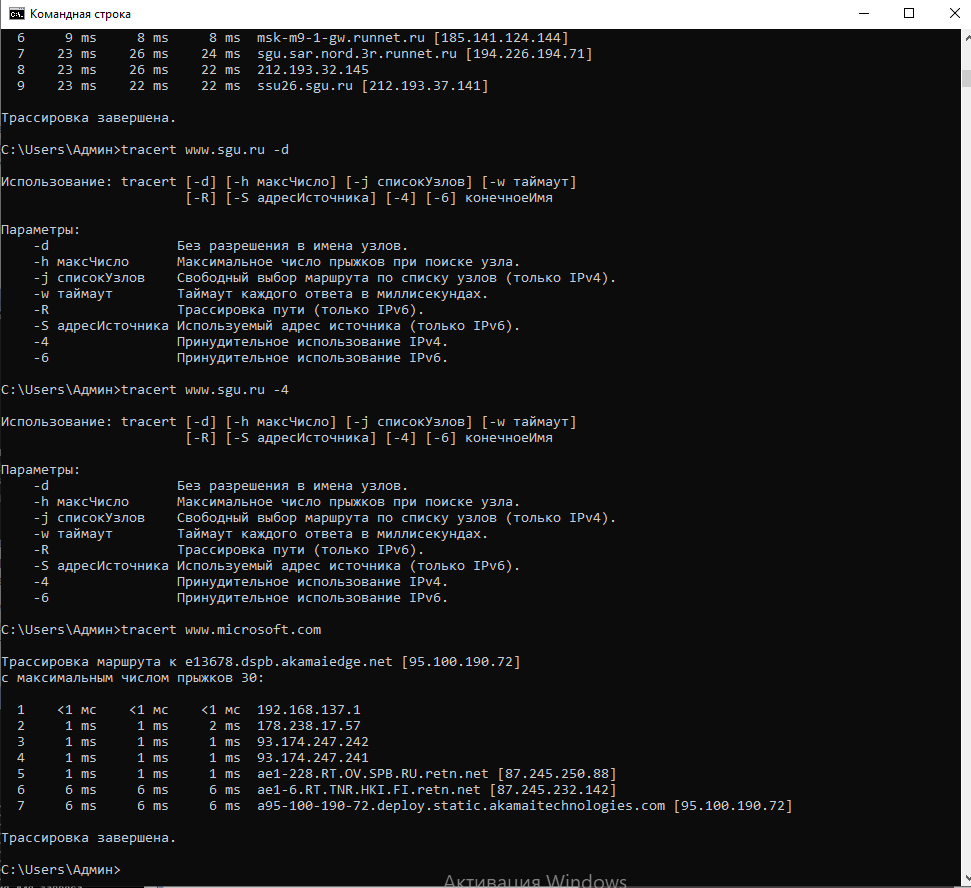
Ping www.sgu.ru

Ping www.microsoft.com

Ping www.sun.com

Ping 212.193.38.83

tracert позволяет определить на каком участке сети (между какими маршрутизаторами) возникла проблема



**Задание 3. Поисковые сервисы европейского и российского ip-регистров.**

Определите, кому принадлежат сети 194.85.33.0 (москва), 217.23.64.0 (cаратов), 212.193.38.0 (саратов). Для этого используйте поисковые аппараты http://www.ripe.net/db/whois/whois.html и http://www.ripn.net:8080/nic/whois/index.html. Пользуясь данными этих информационных систем, попробуйте определите географическое расположение сетей. Попробуйте изобразить топологическую схему соединения этих сетей. Поместите ее на рис. 2.1.

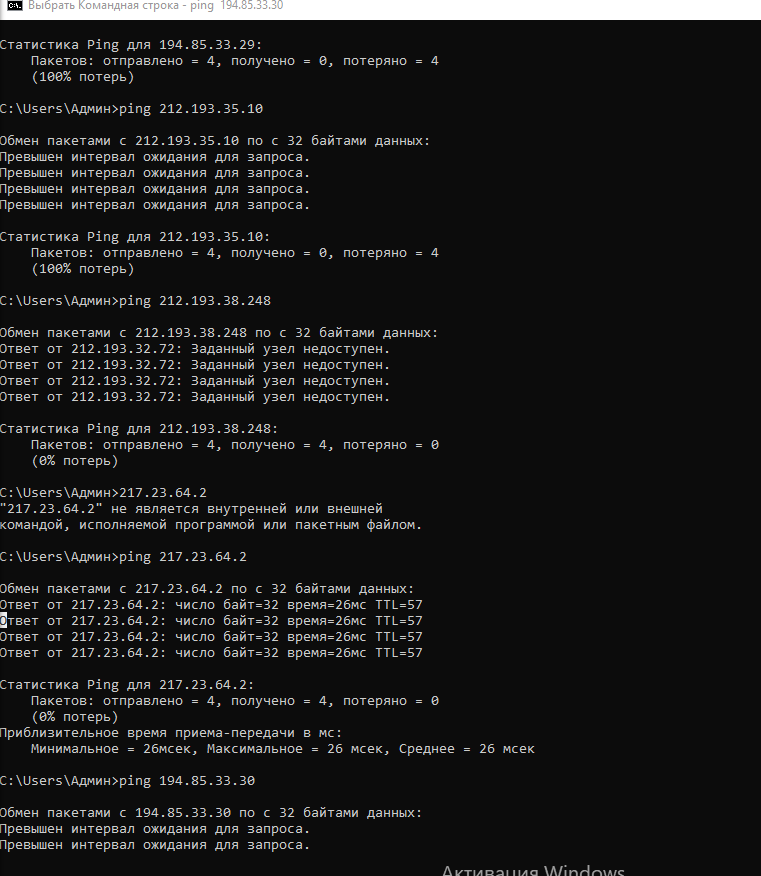
SO01871_

**Рис.2.1 –**Для заполнения топологии сети

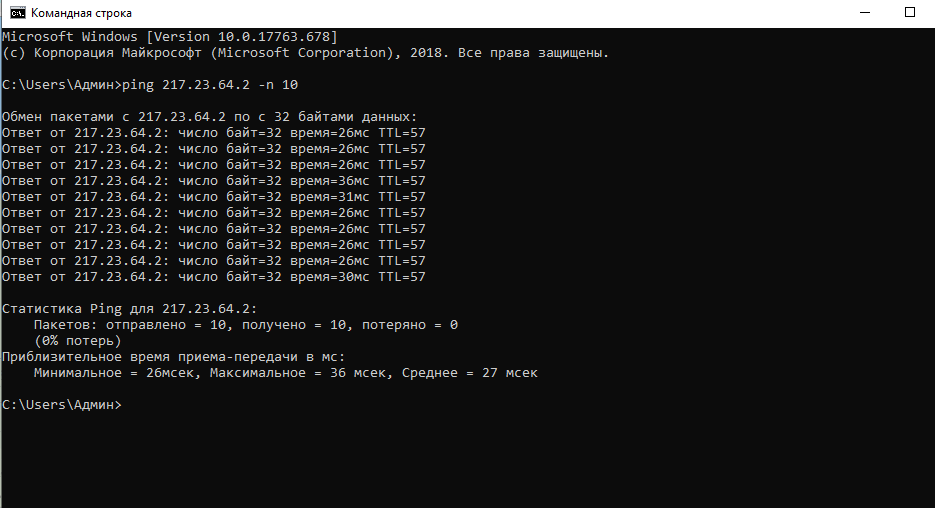
**Задание 4. Использование программы ping для исследования параметров сети.**

1. Приведите сравнительные результаты выполнения команд ping по адресам 194.85.33.29, 194.85.33.30, 217.23.64.2, 212.193.38.248, 212.193.35.10 по параметрам «время отклика», ttl в форме таблицы. Объясните полученные различия.

|  |  |
| --- | --- |
| 194.85.33.29 | Нет данных (см. скриншот) |
| 194.85.33.30 | Нет данных (см. скриншот) |
| 217.23.64.2 | 57 |
| 212.193.38.248 | Нет данных (см. скриншот) |
| 212.193.35.10 | Нет данных (см. скриншот) |



1. Соберите средние времена прохождения 10 пакетов на указанные адреса. Сравните с р4езультатами, полученными при использовании сервиса ping в интерфейсе looking glass на сайте http://noc.runnet.ru. Объясните полученные различия.



Среднее время через кмд= 27,9мс (локально)

**Через сайт: Command:**ping 217.23.64.2

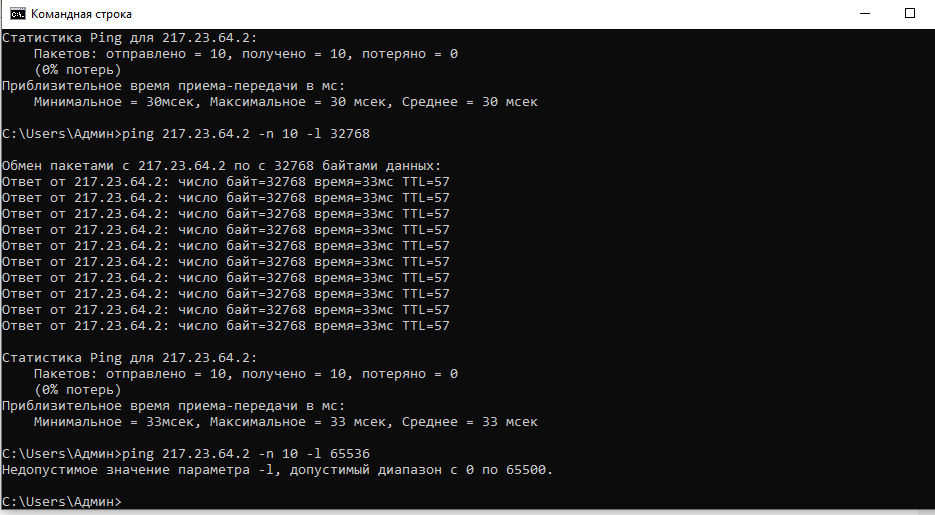
Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 217.23.64.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 148/149/152 ms (проходит через сервис, это занимает время, поэтому дольше)

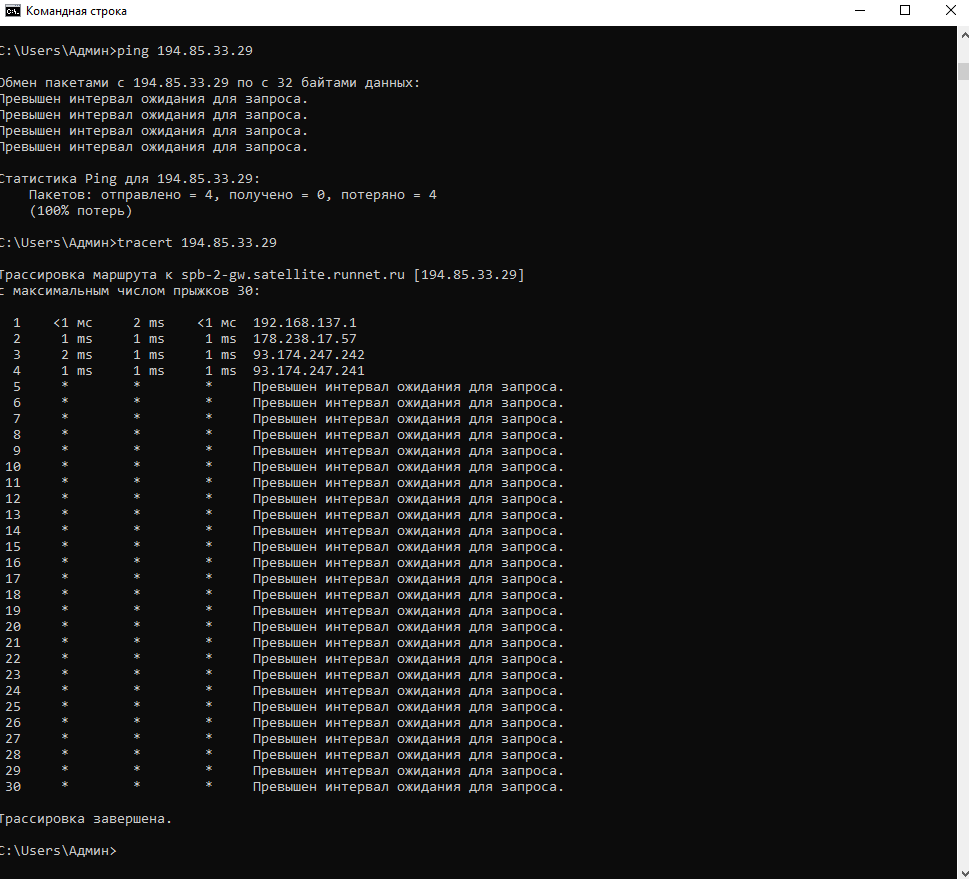
1. Соберите усредненные времена прохождения 10 пакетов увеличивающегося размера по указанным адресам. Начните с 64 байт и каждый раз удваивайте размер пакета. При каком размере пакета потери превышают 50 %. Как влияет время ожидания отклика на процент прохождения пакетов этого размера. При каком времени ожидания отклика потери для пакетов зафиксированного размера не возникают?



Потери не превыщают ноль процентов ни в каком случае, ограничение идет по размеру пакета.

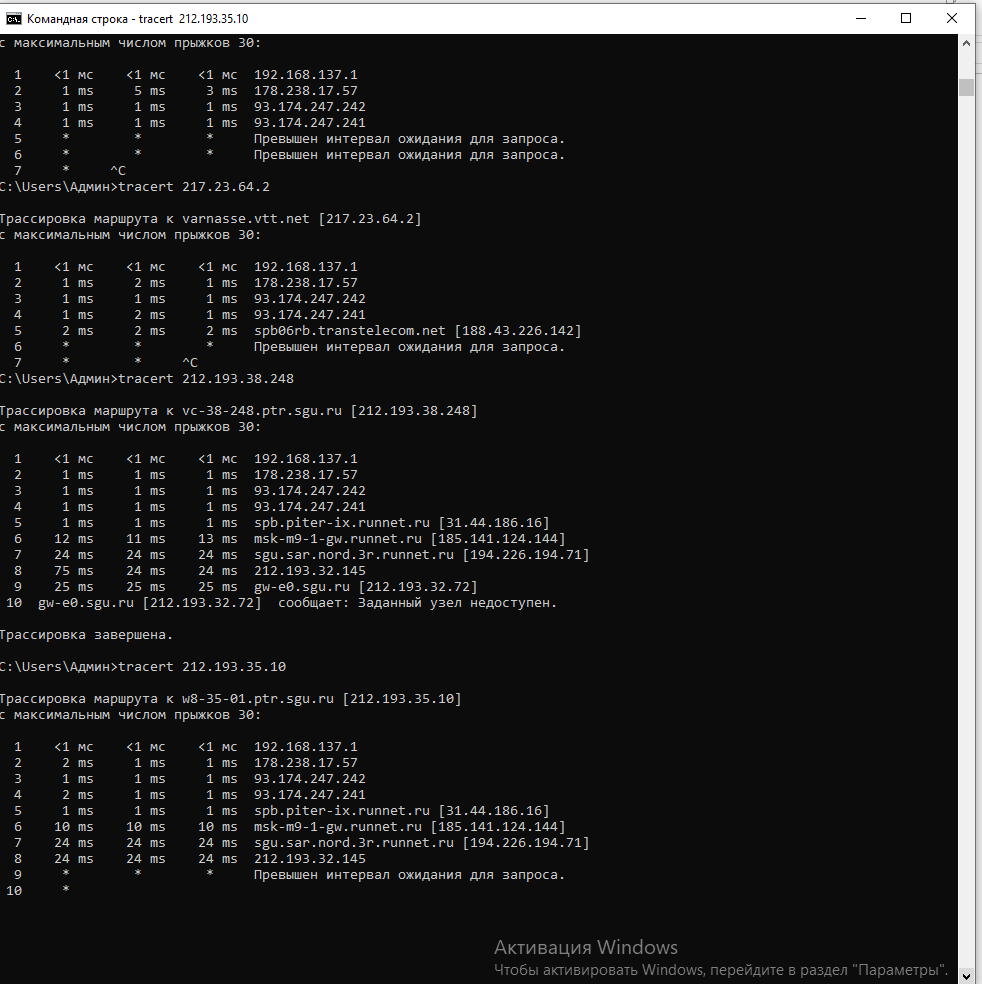
1. Представьте результаты измерений в форме таблиц, наилучшим образом проявляющим, по вашему мнению, обнаруженные зависимости.
2. Используя программу ping, оцените вклад разных сетевых участков, по которым проходит эхо-пакет между вашей рабочей станцией и интерфейсом 194.85.33.29.

traПревышен интервал ожидания для запроса, поэтому делаю для другого (194.85.33.29)



**Задание 5. Использование программы tracert для анализа соединений в сети.**

1. Приведите сравнительные результаты выполнения команд tracert по адресам 194.85.33.29, 194.85.33.30, 217.23.64.2, 212.193.38.248, 212.193.35.10. Объясните полученные различия. Различия в кол-ве адресов, во времени, в кол-ве предоставляемой информации (см. скриншот)



1. Выполните трассировку к адресу 212.193.38.248 и к адресу 217.23.64.2 со стороны сайта http://noc.runnet.ru. Приведите полученные результаты. КАК лукинг

**Router:**msk-m9-3-gw.runnet.ru  
**Command:**trace 212.193.38.248

Type escape sequence to abort.

Tracing the route to vc-38-248.ptr.sgu.ru (212.193.38.248)

1 xe-0-0-0.msk-m9-1-gw.runnet.ru (194.85.40.49) 0 msec 4 msec 0 msec

2 sgu.sar.nord.3r.runnet.ru (194.226.194.71) 16 msec 16 msec 12 msec

3 212.193.32.145 [AS 9111] 16 msec 16 msec 16 msec

4 gw-e0.sgu.ru (212.193.32.72) [AS 9111] 12 msec 16 msec 12 msec

5 ? ? ?

**Router:**msk-m9-3-gw.runnet.ru  
**Command:**trace 217.23.64.2

Type escape sequence to abort.

Tracing the route to varnasse.vtt.net (217.23.64.2)

1 xe-0-0-0.msk-m9-1-gw.runnet.ru (194.85.40.49) 0 msec 0 msec 0 msec (большой вклад)

2 spb-bm18-1-gw.runnet.ru (185.141.124.145) 8 msec 12 msec 8 msec

3 sap-b3-link.telia.net (80.239.194.254) [AS 1299] 12 msec 8 msec 8 msec

4 s-bb4-link.telia.net (80.91.250.99) [AS 1299] [MPLS: Label 25378 Exp 0] 24 msec

s-bb3-link.telia.net (80.91.249.79) [AS 1299] [MPLS: Label 25221 Exp 0] 20 msec 24 msec

5 s-b5-link.telia.net (62.115.114.165) [AS 1299] 16 msec

s-b5-link.telia.net (62.115.119.109) [AS 1299] 24 msec

s-b5-link.telia.net (80.91.253.227) [AS 1299] 20 msec

6 transtelecom-ic-303467-s-b3.c.telia.net (213.248.99.222) [AS 1299] 20 msec 16 msec 20 msec

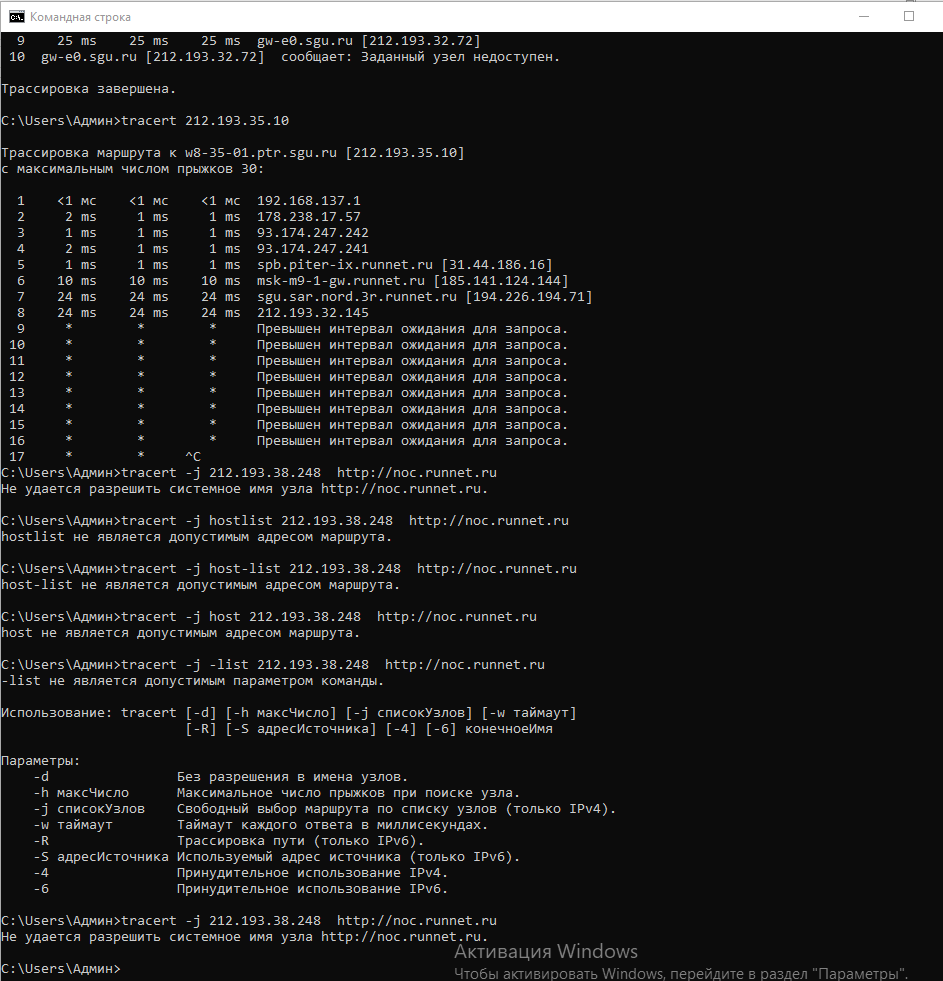
7 srv06.transtelecom.net (217.150.41.246) [AS 20485] [MPLS: Label 25408 Exp 2] 64 msec 52 msec 52 msec

8 VolgaTTK-gw.transtelecom.net (217.150.41.245) [AS 20485] 52 msec 56 msec 52 msec

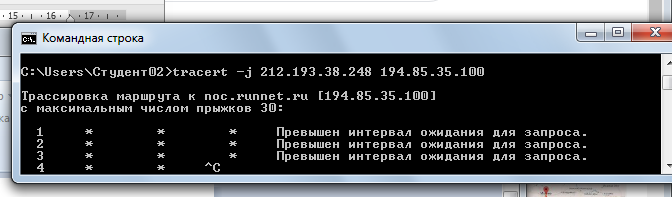
9 fregat-gw02-gi0-1-31.vtt.net (217.23.72.221) [AS 15974] 52 msec 52 msec 52 msec

10 vpn-gw-eth3-41.vtt.net (217.23.86.46) [AS 15974] 52 msec 56 msec 56 msec

11 ? ? ?



1. Используя данные, полученные в результате выполнения трассировки и отправки эхо-пакетов между интерфейсами 212.193.38.248 и 194.85.35.100, оцените вклад разных участков сетей, соединяющих эти интерфейсы, в среднее время прохождения пакетов между ними. Превышен интервал ожидания для запроса



Эта утилита очень похожа на ping, за исключением того, что она показывает все другие ip-адреса (интерфейсы), которые пакет проходит до своего места назначения. Дополнительно можно изменять различные опции, ассоциированные с trace route: максимальное число дозволяемых промежуточных узлов (maximum hops, от 1 до 255) и timeout (до 9999 ms).

Формат команды в ос windows:

Tracert [-d] [-h maximum\_hops] [-j host-list] [-w timeout] target\_name

Options:

-d не разрешать адреса в имена.

-h maximum\_hops наибольшее число промежуточных узлов.

-j host-list трассировка через определенный список хостов

-w timeout время ожидания каждого ответа в мс.

1. Используя полученную в ходе выполнения всех заданий информацию, уточните схему задания 1, изобразите на ней обнаруженные вами промежуточные интерфейсы и линки сети, объединяющей подсети 194.85.33.0, 217.23.64.0, 212.193.38.0. какие адреса по ним выходят

**Router:**msk-m9-3-gw.runnet.ru  
**Command:**ping 212.193.38.0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 212.193.38.0, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

Подсети неработоспособны. (см. текст выше). Такое сообщение выходит по всем айпи адресам.

Схема:

194.85.33.29 (росниирос, москва)

194.85.33.30 (саратов)

217.23.64.2 (саратов)

212.193.38.248 (саратов)

212.193.35.10 (саратов)