МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«Санкт-Петербургский национальный исследовательский университет  
информационных технологий, механики и оптики»

Лабораторная работа №1

Выполнил студенты группы М3204:  
Наскальнюк Никита Андреевич

САНКТ-ПЕТЕРБУРГ  
2018

**Назначение**

Приобретение знаний и умений, необходимых для решения задач, возникающих в сетях связи.

**Цель работы**

Формирование представлений о функциональных возможностях основных сетевых утилит, доступных через командную строку в ОС Windows или через терминал в ОС Linux.

**Перечень используемого оборудования и ПО**

Персональный компьютер с установленной ОС Windows или ОС Linux.

**Порядок выполнения работы**

1. Запустить командную строку с правами учетной записи администратора.

2. Выполнить следующую последовательность действий для каждой из приведенных в таблице 1 сетевых утилит.

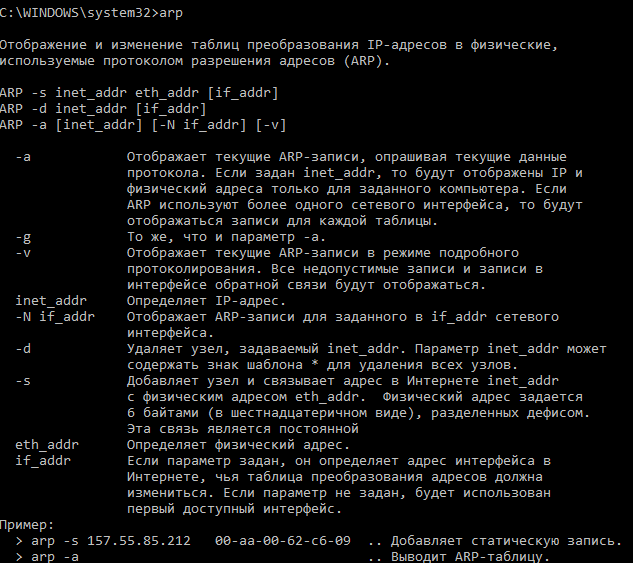


Рис.1.1 - **arp** без параметров, а также параметром справки

Таблица 1.1 - Параметры сетевой утилиты **arp**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Группа параметры** | | | | | |
| **1 группа - параметры настройки** | | | **2 группа - параметры отображения** | | |
| Номер | Обозначение | Назначение | Номер | Обозначение | Назначение |
| 1 | -d | Удаляет узел, задаваемый inet\_addr | 1 | -a | Отображает текущие ARP-записи |
| 2 | -s | Добавляет узел и связывает inet\_addr с физическим адресом eth\_addr | 2 | -g | То же, что и параметр -a |
| 3 |  |  | 3 | -v | Отображает текущие ARP-записи в режиме подробного протоколирования |
| 4 |  |  | 4 | -N if\_addr | Отображает ARP-записи для заданного в if\_addr сетевого интерфейса |

Таблица 1.2 - Значение параметров 1 группы сетевой утилиты **arp**

|  |  |  |
| --- | --- | --- |
| **Номер** | **Обозначение параметра** | **Значение параметра** |
| 1 | -d | inet\_addr (IP-адрес) |
| 2 | -s | inet\_addr (IP-адрес), eth\_inet (физический адрес) |



Рис.1.2 – **arp** вывод с параметром -d



Рис.1.3 - **arp** вывод с параметром -s

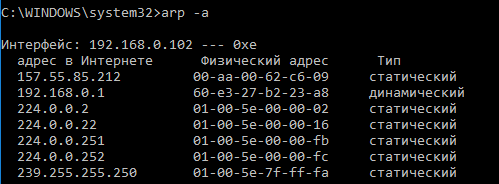


Рис.1.4 - **arp** вывод с параметром -а

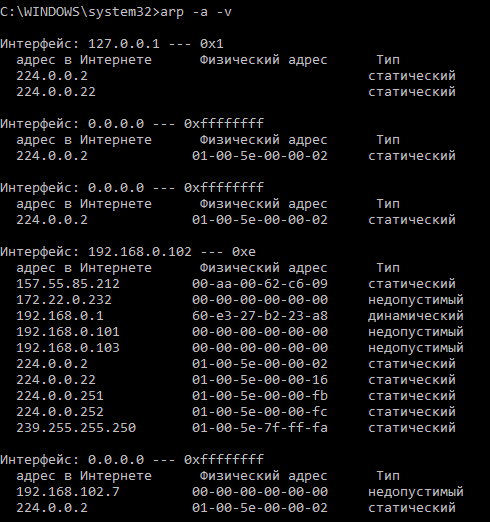


Рис.1.5 - **arp** вывод с параметром -v в сочетании с параметром -а

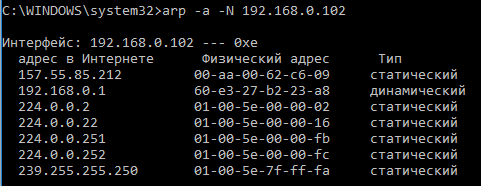


Рис.1.6 - **arp** вывод с параметром -N в сочетании с параметром –а

Таблица.1.3 - Параметры сетевой утилиты **arp**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Группа параметров** | | | | | |
| **1 группа 1 категория** | | | **2 группа 1 категория** | | |
| № | Обозначение | Назначение | № | Обозначение | Назначение |
|  |  |  | 1 | -a –v | Отображает текущие ARP-записи в режиме подробного протоколирования, опрашивая текущие данные протокола |
|  |  |  | 2 | -a -N if\_addr | Отображает ARP-записи для заданного в if\_addr сетевого интерфейса, опрашивая текущие данные протокола |

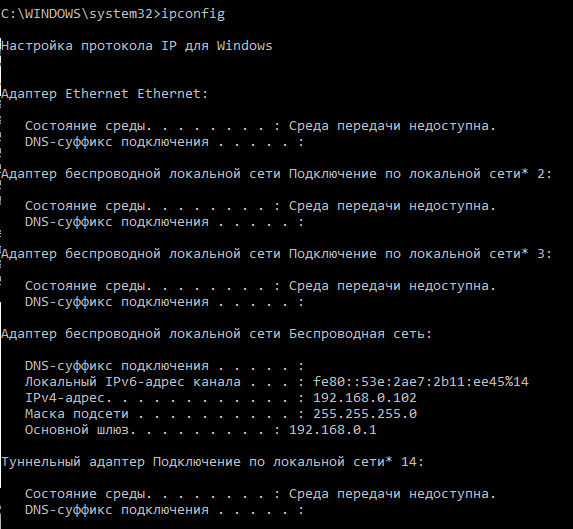
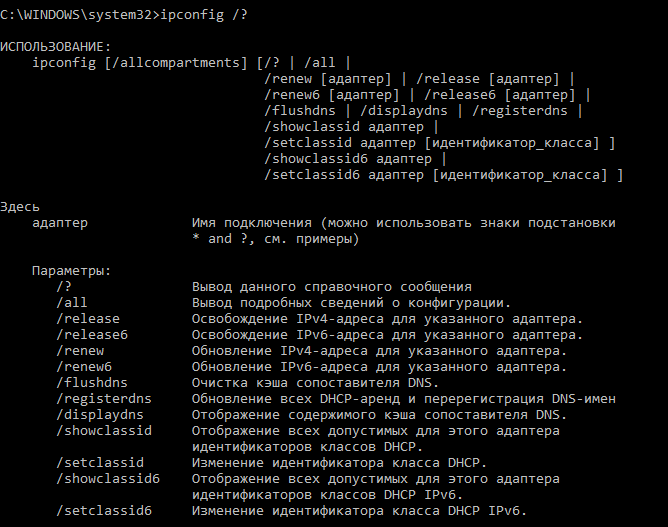


Рис.2.1 - **ipconfig** вывод без параметра



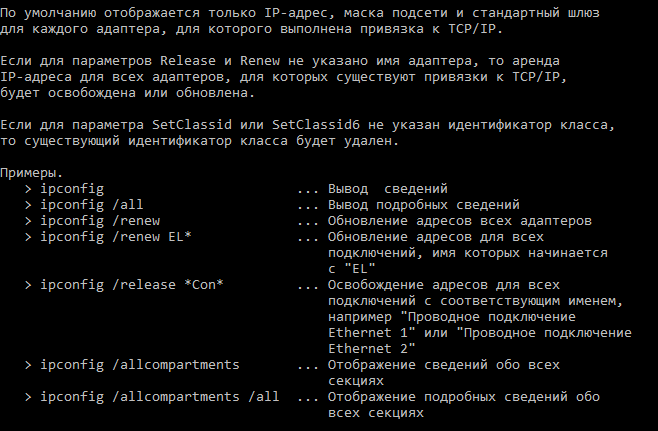


Рис.2.2 - **ipconfig** вывод с параметром справки

Таблица 2.1 - Параметры сетевой утилиты **ipconfig**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Группа параметров** | | | | | |
| **1 группа - параметры настройки** | | | **2 группа - параметры отображения** | | |
| **№** | **Обозначение** | **Назначение** | **№** | **Обозначение** | **Назначение** |
| 1 | /release | Освобождение адреса IPv4 для указанного адаптера. | 1 | /all | Вывод подробных сведений о конфигурации |
| 2 | /release6 | Освобождение адреса IPv6 для указанного адаптера. | 2 | /displaydns | Отображение содержимого кэша сопоставителя DNS. |
| 3 | /renew | Обновление адреса IPv4 для указанного адаптера. | 3 | /showclassid | Отображение всех допустимых для этого адаптера идентификаторов класса DHCP. |
| 4 | /renew6 | Обновление адреса IPv6 для указанного адаптера. | 4 | /showclassid6 | Отображение всех допустимых для этого адаптера идентификаторов класса DHCP IPv6. |
| 5 | /flushdns | Очистка кэша сопоставителя DNS. |  |  |  |
| 6 | /registerdns | Обновление всех DHCP-аренд и перерегистрация DNS-имён. |  |  |  |
| 7 | /setclassid | Изменение идентификатора класса DHCP. |  |  |  |
| 8 | /setclassid6 | Изменение идентификатора класса DHCP IPv6. |  |  |  |

Таблица 2.2 - Значение параметров 1 группы сетевой утилиты **ipconfig**

|  |  |  |
| --- | --- | --- |
| **№** | **Обозначения параметра** | **Значение параметра** |
| 1 | /release | адаптер (имя подключения) |
| 2 | /release6 | адаптер (имя подключения) |
| 3 | /renew | адаптер (имя подключения) |
| 4 | /renew6 | адаптер (имя подключения) |
| 5 | /setclassid | идентификатор класса DHCP |
| 6 | /setclassid6 | идентификатор класса DHCP IPv6 |

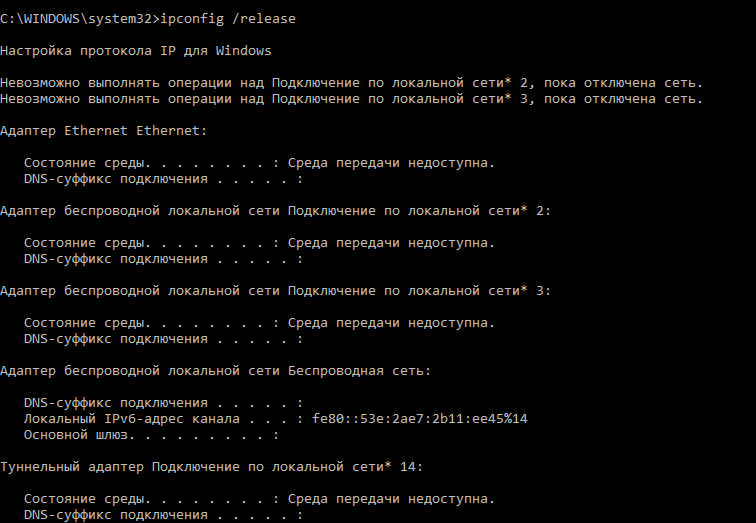


Рис.2.3 - **ipconfig** вывод с параметром /release



Рис.2.4 - ipconfig вывод с параметром /renew

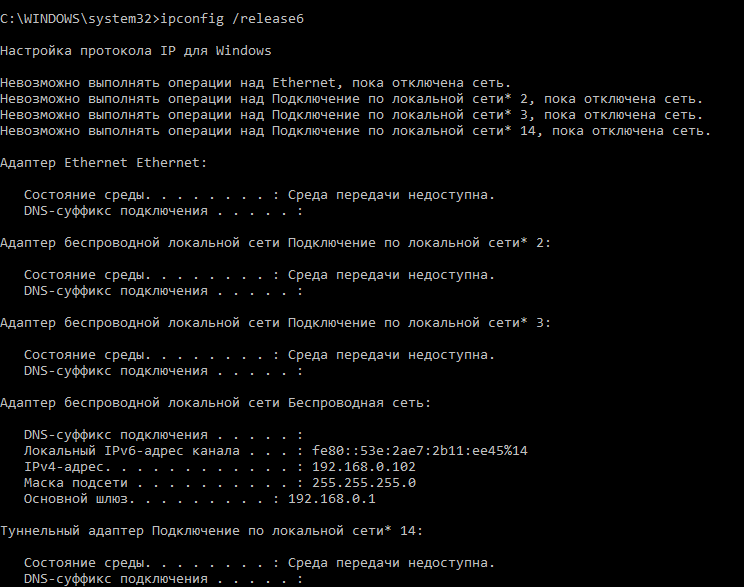


Рис.2.5 - **ipconfig** вывод с параметром /release6

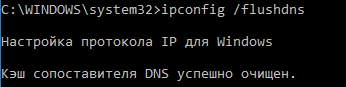


Рис.2.6 - **ipconfig** вывод с параметром /flushdns

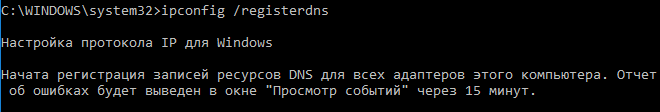


Рис.2.7 - **ipconfig** вывод с параметром /registerdns

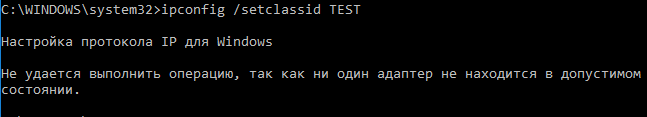


Рис.2.8 - **ipconfig** вывод с параметром /setclassid

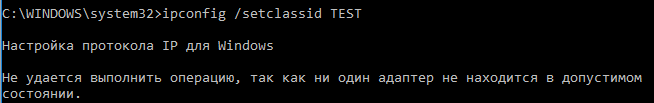
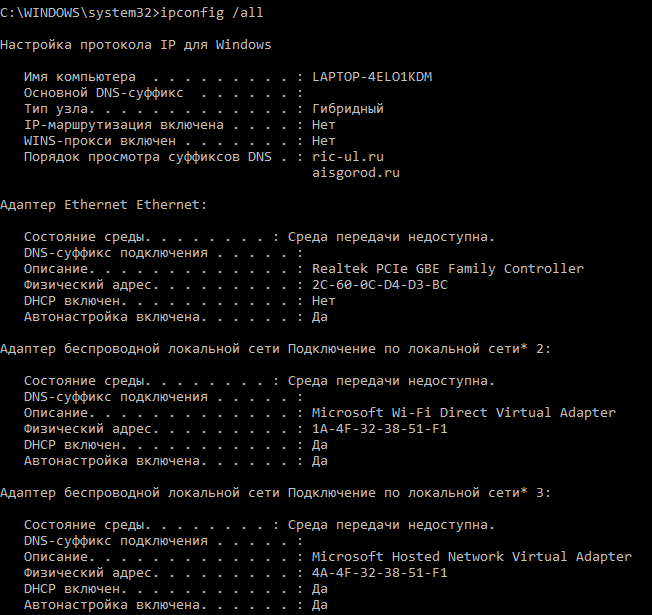


Рис.2.9 - **ipconfig** вывод с параметром /setclassid6



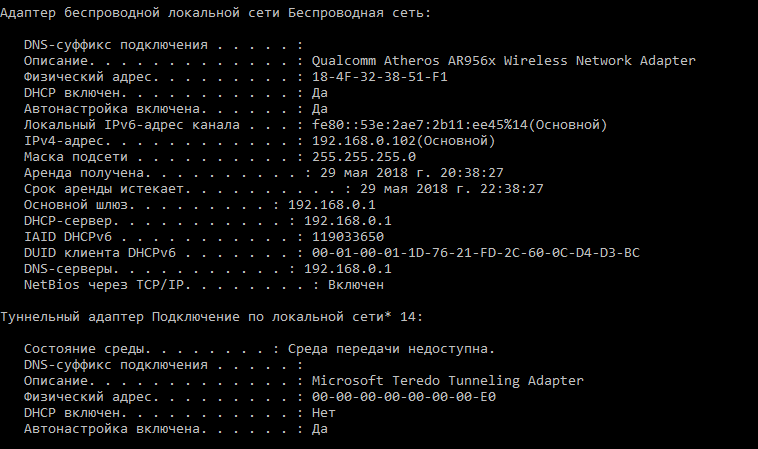


Рис.2.10 - **ipconfig** вывод с параметром /all

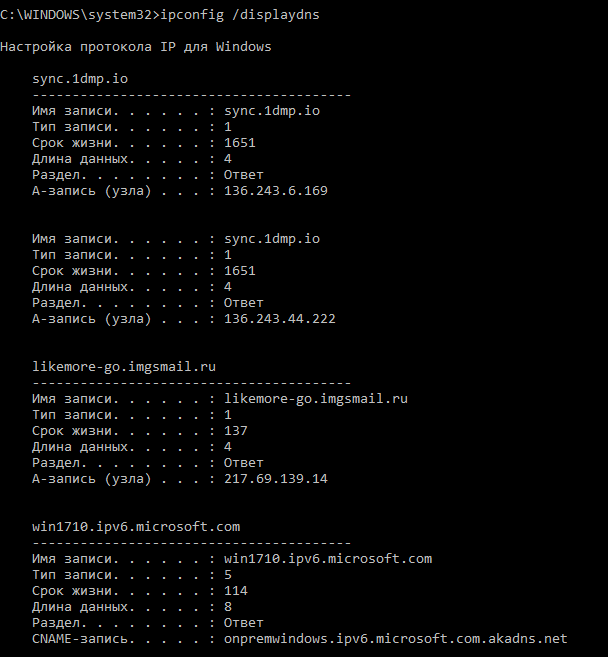


Рис.2.11 - **ipconfig** вывод с параметром /displaydns

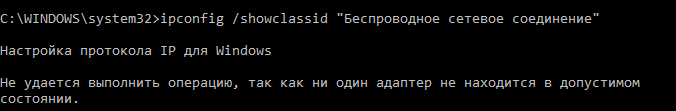


Рис.2.12 - **ipconfig** вывод с параметром /showclassid

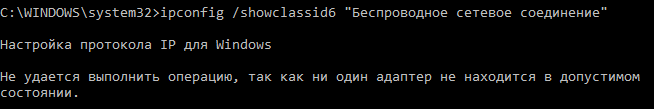


Рис.2.13 - **ipconfig** вывод с параметром /showclassid6

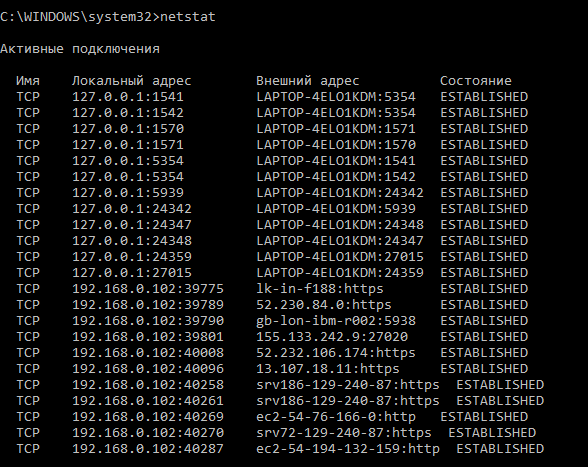


Рис.3.1 - **netstat** вывод без параметра

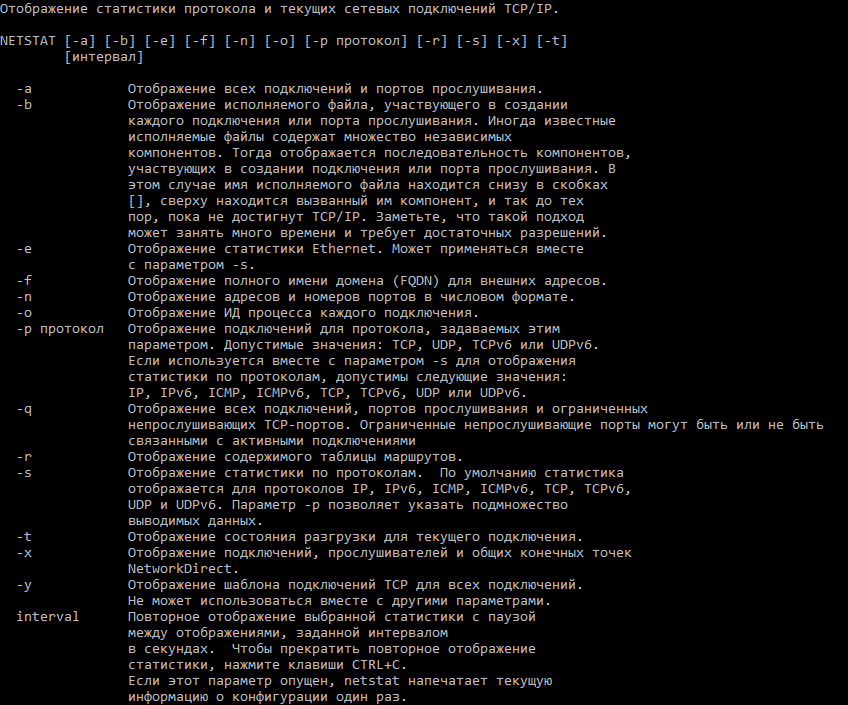
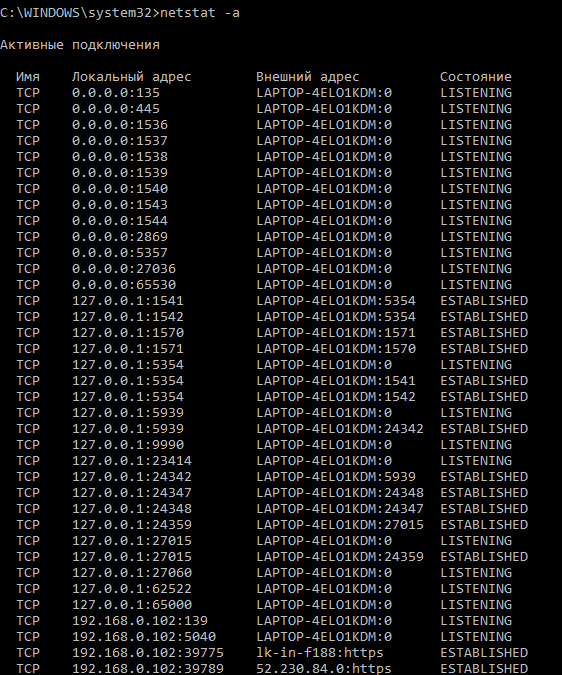


Рис.3.2 - **netstat** вывод с параметром справки

Таблица 3.1 - Параметры сетевой утилиты netstat

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Группа параметров** | | | | | |
| **1 группа - параметры настройки** | | | **2 группа - параметры отображения** | | |
| **№** | **Обозначение** | **Назначение** | **№** | **Обозначение** | **Назначение** |
|  |  |  | 1 | -a | Отображение всех подключений и ожидающих портов |
|  |  |  | 2 | -b | Отображение исполняемого файла, участвующего в создании каждого подключения, или ожидающего порта |
|  |  |  | 3 | -e | Отображение статистики Ethernet. |
|  |  |  | 4 | -f | Отображение полного имени домена (FQDN) для внешних адресов |
|  |  |  | 5 | -n | Отображение адресов и номеров портов в числовом формате |
|  |  |  | 6 | -o | Отображение кода (ID) процесса каждого подключения |
|  |  |  | 7 | -p | Отображение подключений для протокола, задаваемых этим параметром |
|  |  |  | 8 | -r | Отображение содержимого таблицы маршрутов |
|  |  |  | 9 | -s | Отображение статистики протокола |
|  |  |  | 10 | -t | Отображение текущего подключения в состоянии "offload" |



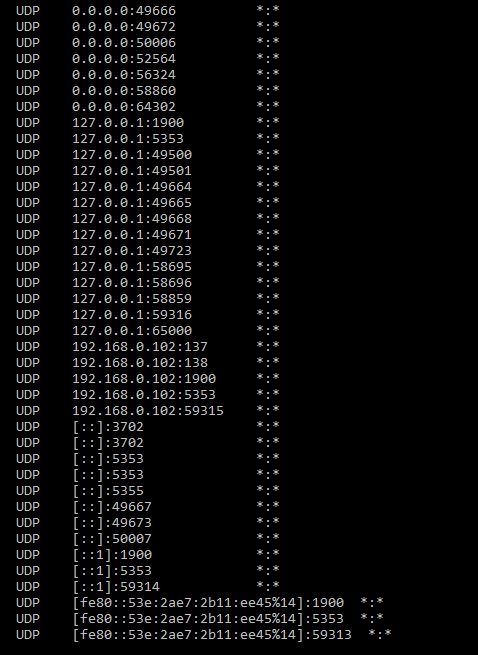


Рис.3.3 - **netstat** вывод с параметром –а



Рис.3.4 - **netstat** вывод с параметром -b

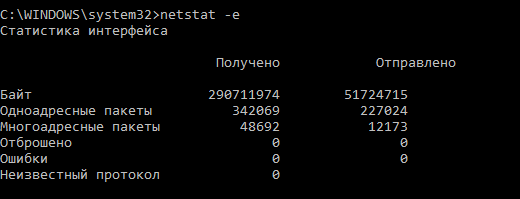


Рис.3.5 - **netstat** вывод с параметром -e

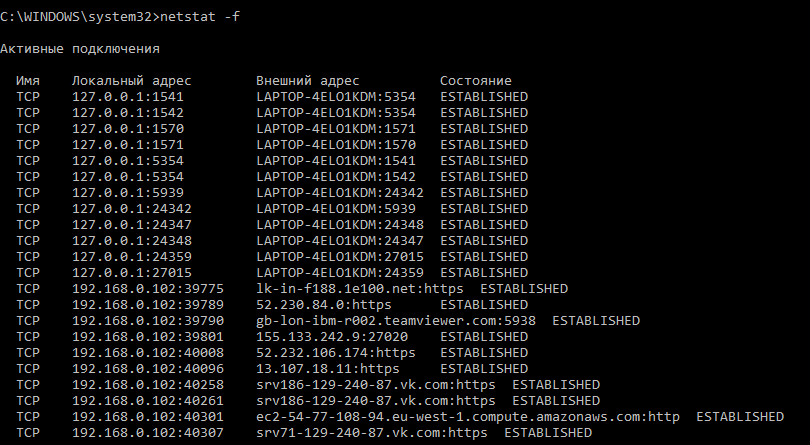


Рис.3.6 – **netstat** вывод с параметром –f

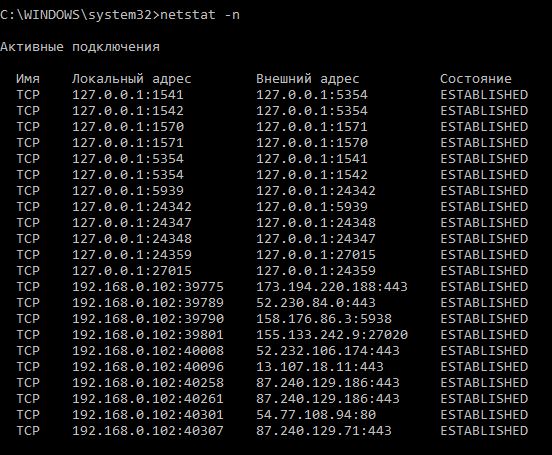


Рис.3.7 - **netstat** вывод с параметром –n

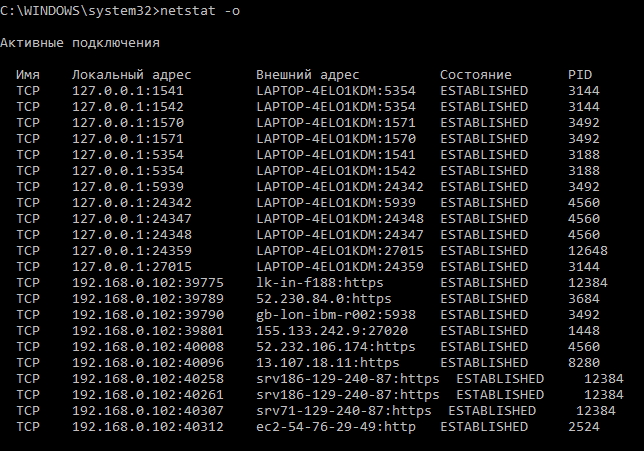


Рис.3.8 - **netstat** вывод с параметром –o

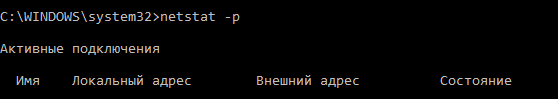


Рис.3.9 - **netstat** вывод с параметром -p

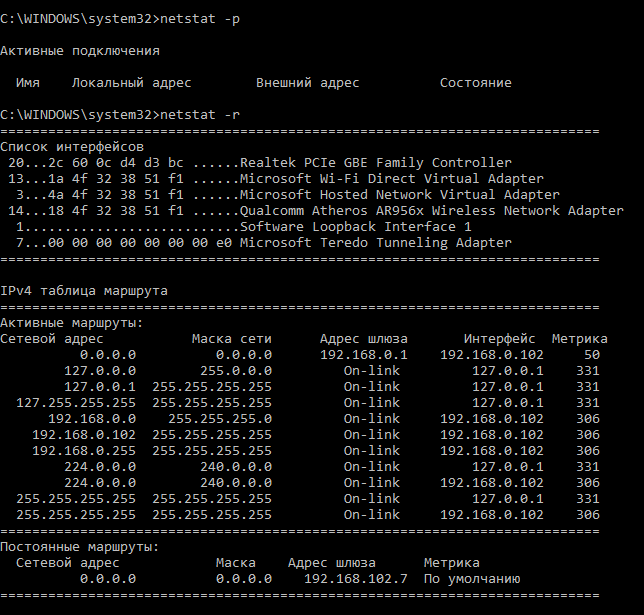




Рис.3.10 - **netstat** вывод с параметром –r

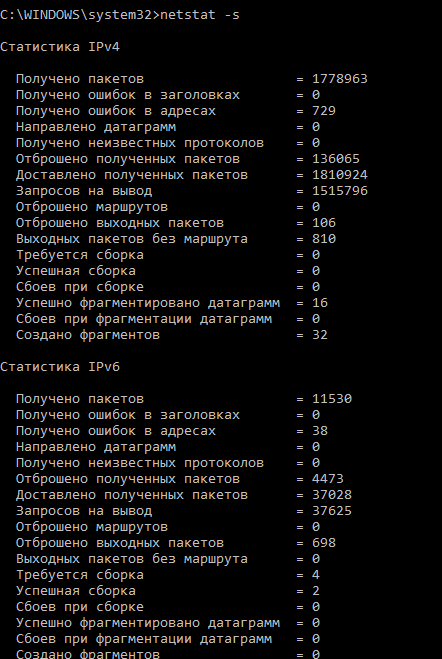




Рис.3.11 - **netstat** вывод с параметром –s

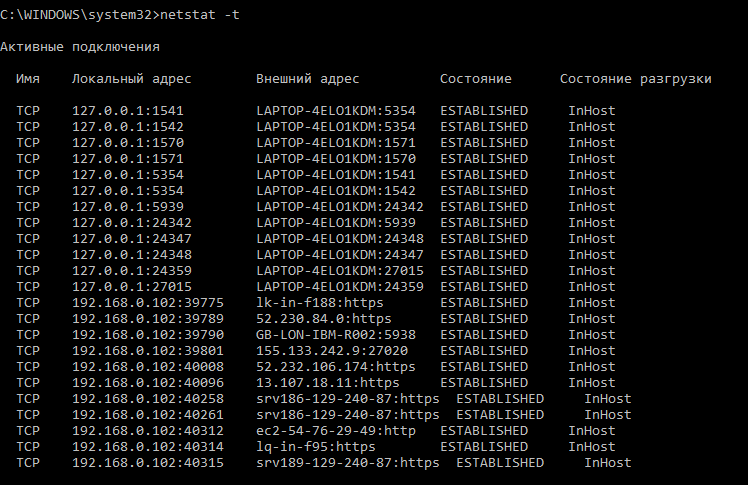
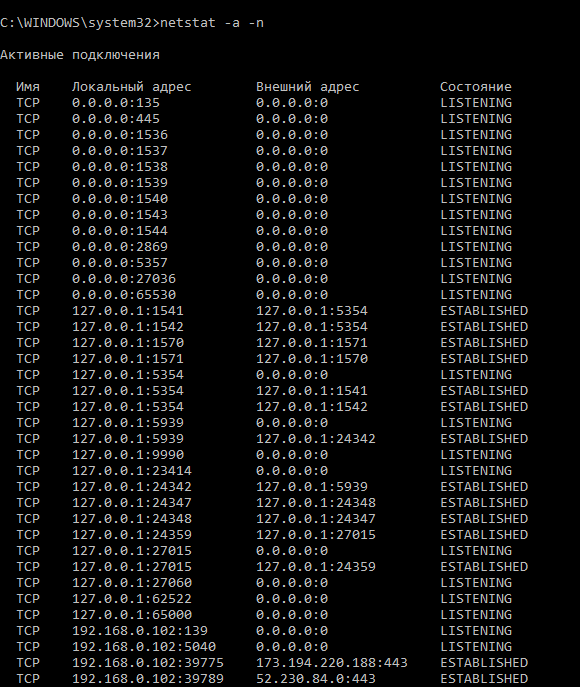
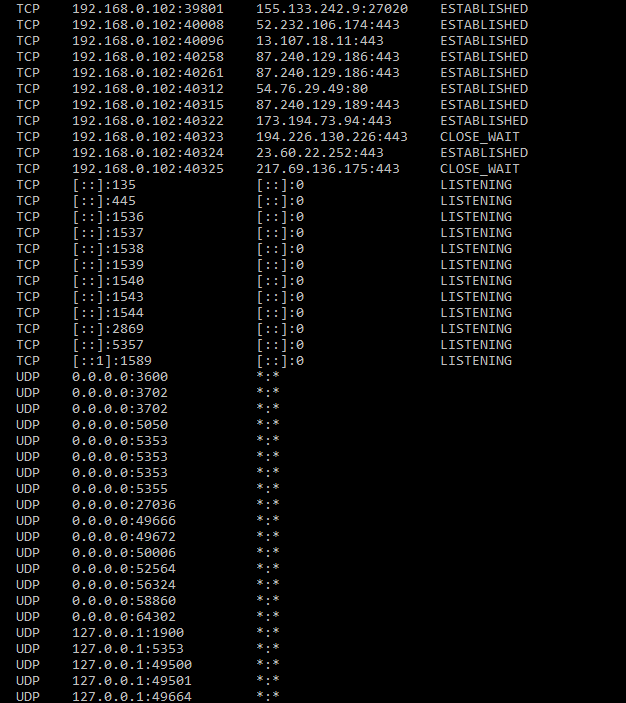


Рис.3.12 - **netstat** вывод с параметром –t

Таблица.3.2 - Параметры сетевой утилиты **netstat**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Группа параметров** | | | | | |
| **1 группа 1 категория** | | | **2 группа 1 категория** | | |
| **№** | **Обозначение** | **Назначение** | **№** | **Обозначение** | **Назначение** |
|  |  |  | 1 | -a -n | Отображение всех подключений и ожидающих портов с отображением номеров портов и IP-адресов в числовом формате. |
|  |  |  | 2 | -a -f | Отображение всех подключений и ожидающих портов с отображением полных DNS-имен узлов, участвующих в соединении. |
|  |  |  | 3 | -a -b | Получить список всех сетевых соединений и связанных с ними программ. |
|  |  |  | 4 | -e -v | Отображается информация об обмене данными через отдельные сетевые интерфейсы, кроме суммарной статистики. |
|  |  |  | 5 | -e -s | Дополнительно к статистике Ethernet, отображается статистика для протоколов IP, ICMP, TCP, UDP. |
|  |  |  | 6 | -s -p | Получить статистику только по протоколу ICMP. |





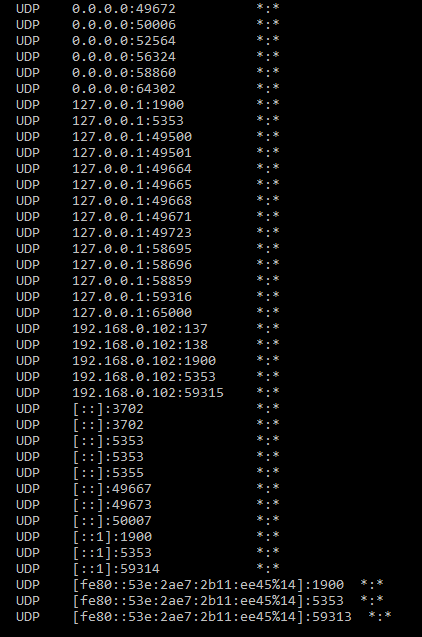
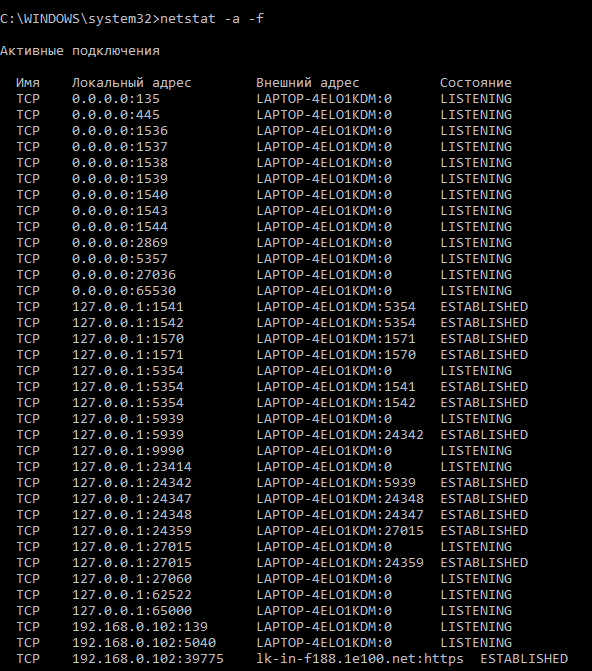


Рис.3.13 - **netstat** вывод с параметрами -а –n



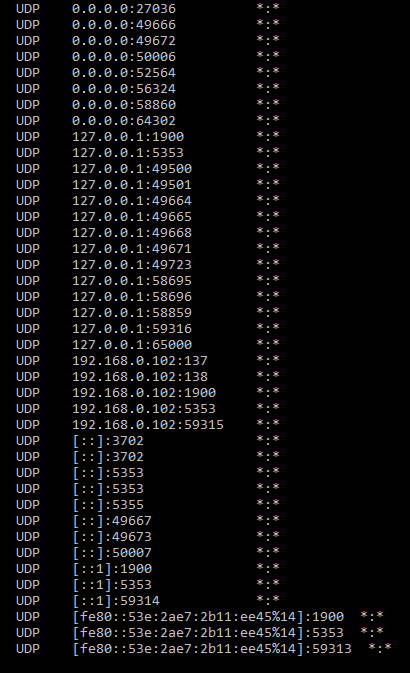
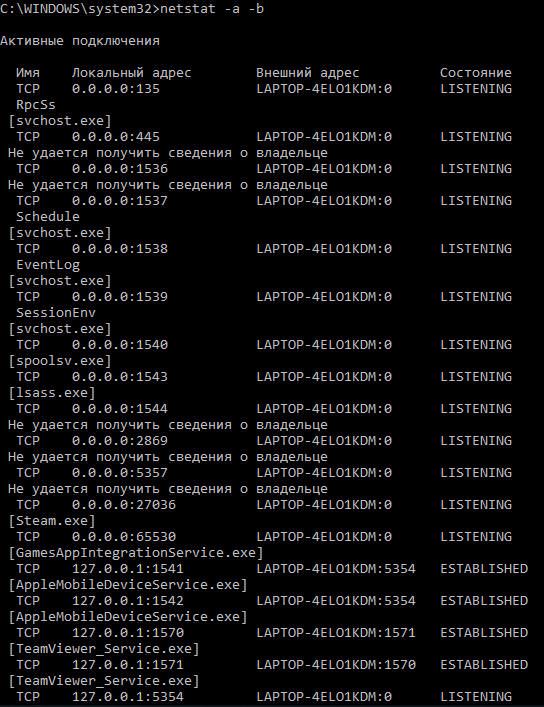


Рис.3.14 - **netstat** вывод с параметрами -а –f



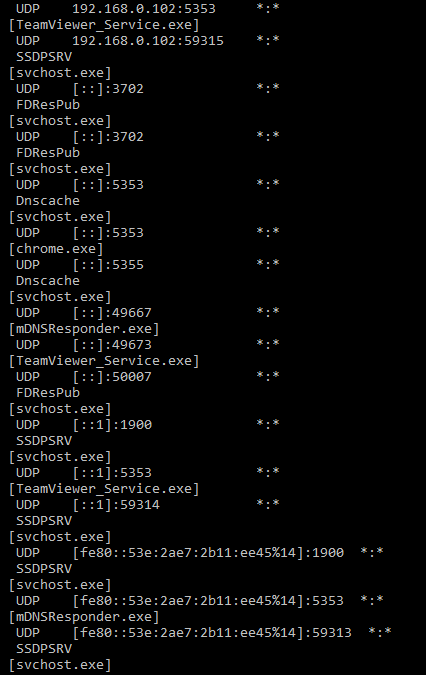
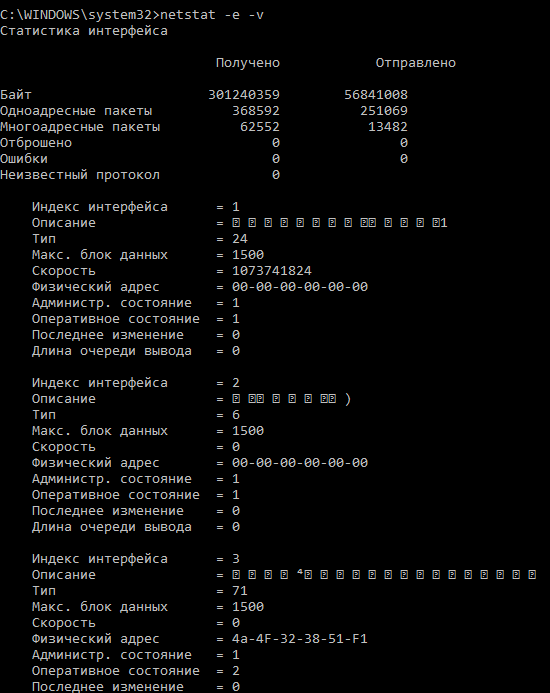


Рис.3.15 - **netstat** вывод с параметрами -а –b



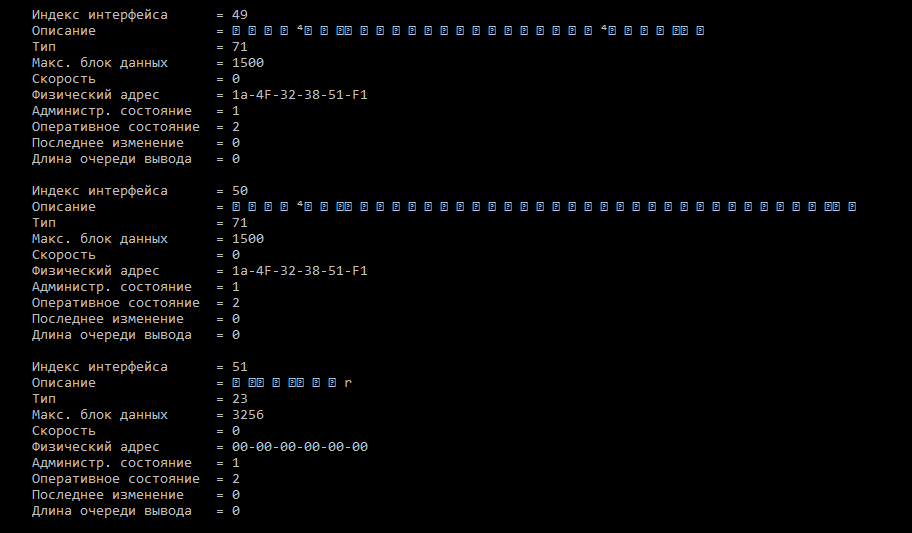
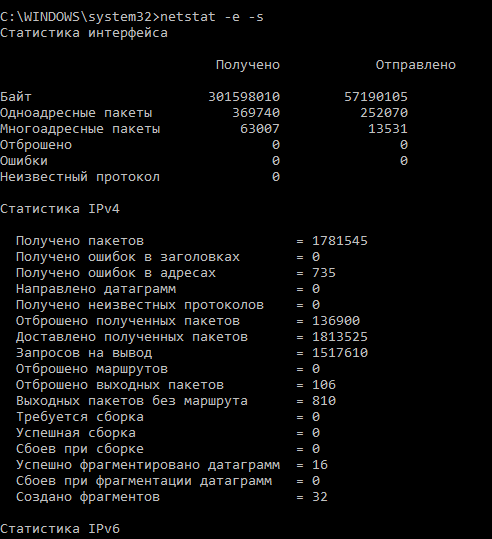


Рис.3.16 - **netstat** вывод с параметрами -e -v



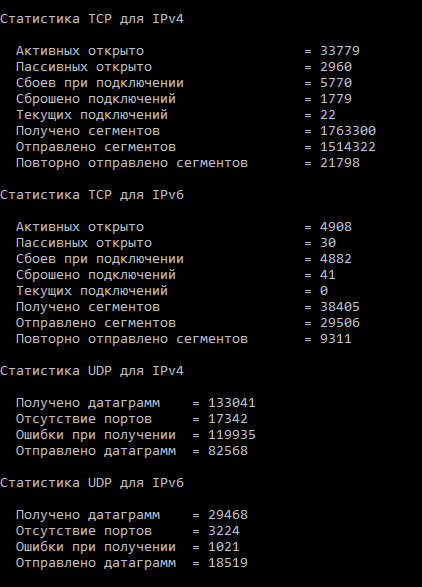


Рис.3.17 - **netstat** вывод с параметрами -e –s

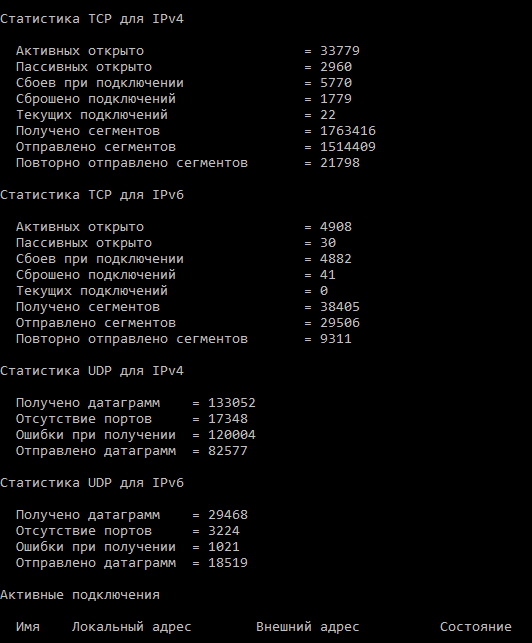


Рис.3.18 - **netstat** вывод с параметрами -s -p



Рис.4.1 - **ping** вывод без параметра, а также вывод справки

Таблица 4.1 - Параметры сетевой утилиты **ping**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Группа параметров** | | | | | |
| **1 группа - параметры настройки** | | | **2 группа - параметры отображения** | | |
| **№** | **Обозначение** | **Назначение** | **№** | **Обозначение** | **Назначение** |
| 1 | -t | Проверка связи с указанным узлом до прекращения. |  |  |  |
| 2 | -a | Определение имён узлом по адресам. |  |  |  |
| 3 | -n | Число отправляемых запросов эха. |  |  |  |
| 4 | -l | Размер буфера отправки. |  |  |  |
| 5 | -f | Установка в пакете флага, запрещающего фрагментацию (только IPv4). |  |  |  |
| 6 | -i | Задание срока жизни пакетов. |  |  |  |
| 7 | -v | Задание типа службы (только IPv4). |  |  |  |
| 8 | -r | Запись маршрута для указанного числа прыжков (только IPv4). |  |  |  |
| 9 | -s | Отметка времени для указанного числа прыжков (только IPv4). |  |  |  |
| 10 | -j | Свободный выбор маршрута по списку узлов (только IPv4). |  |  |  |
| 11 | -k | Жёсткий выбор маршрута по списку узлов (только IPv4). |  |  |  |
| 12 | -w | Тайм-аут для каждого ответа (в мс). |  |  |  |
| 13 | -R | Использование заголовка для проверки также и обратного маршрута (только IPv4). |  |  |  |
| 14 | -S | Используемый адрес источника. |  |  |  |
| 15 | -4 | Принудительное использование протокола IPv4. |  |  |  |
| 16 | -6 | Принудительное использование протокола IPv6. |  |  |  |

Таблица 4.2 - Значение параметров 1 группы сетевой утилиты **ping**

|  |  |  |
| --- | --- | --- |
| **№** | **Обозначения параметра** | **Значение параметра** |
| 1 | -n | Число запросов |
| 2 | -l | Размер пакета |
| 3 | -i | Срок жизни пакета |
| 4 | -v | Тип обеспечения |
| 5 | -r | Число прыжков |
| 6 | -s | Число прыжков |
| 7 | -j | Список узлов |
| 8 | -k | Список узлов |
| 9 | -w | Тайм-аут |
| 10 | -S | IP-адрес |

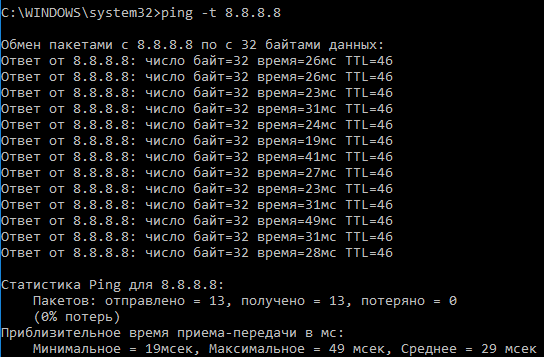


Рис.4.2 - **ping** вывод с параметром –t

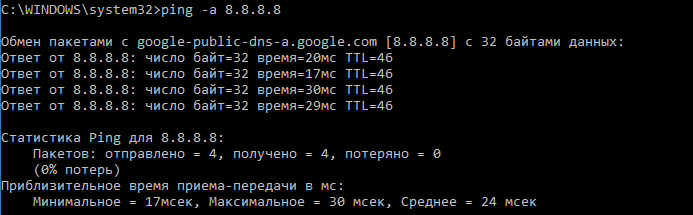


Рис.4.3 - **ping** вывод с параметром –a

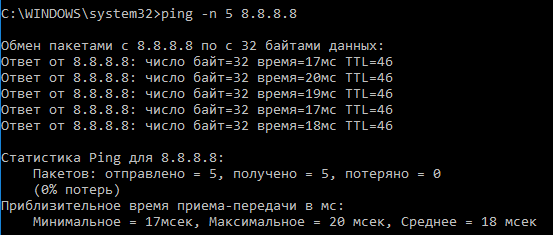


Рис.4.4 – **ping** вывод с параметром –n

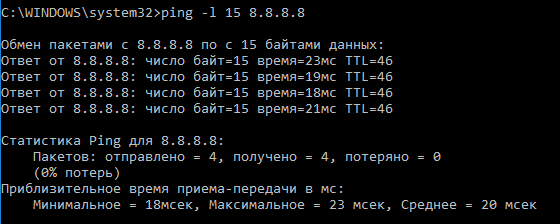


Рис.4.5 - **ping** вывод с параметром –l

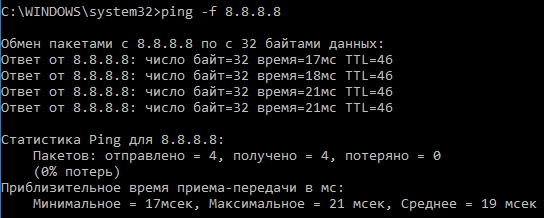


Рис.4.6 - **ping** вывод с параметром -f

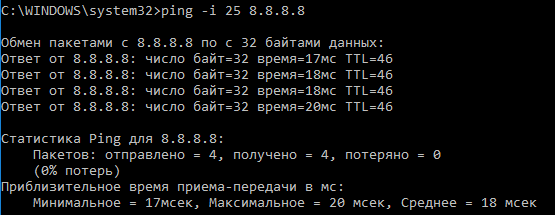


Рис.4.7 - **ping** вывод с параметром –i

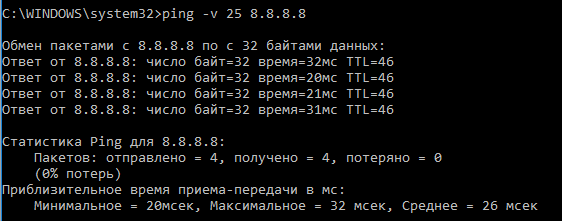


Рис.4.8 - **ping** вывод с параметром –v

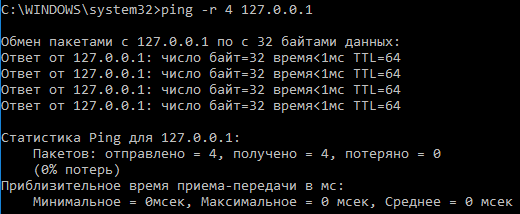


Рис.4.9 - **ping** вывод с параметром –r

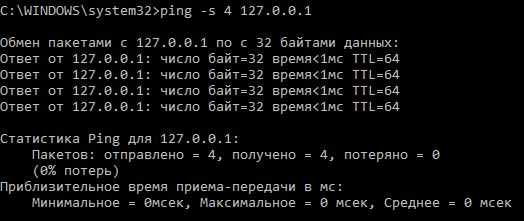


Рис.4.10 - **ping** вывод с параметром –s

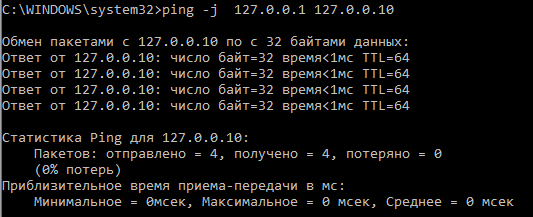


Рис.4.11 - **ping** вывод с параметром –j

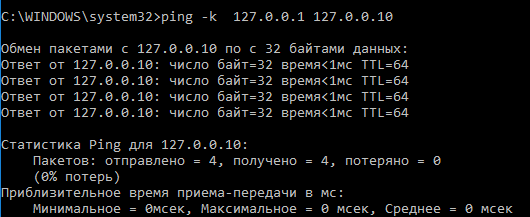


Рис.4.12 - **ping** вывод с параметром –k

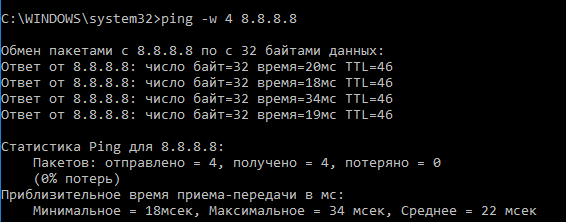


Рис.4.13 - **ping** вывод с параметром –w

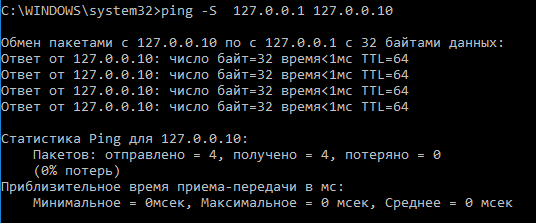


Рис.4.14 - **ping** вывод с параметром –S

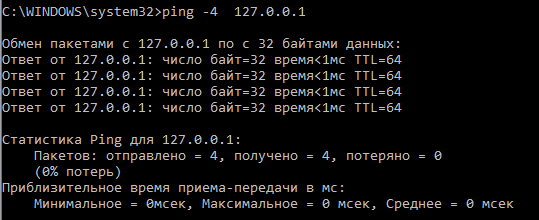


Рис.4.15 - **ping** вывод с параметром -4

Таблица.4.3 - Параметры сетевой утилиты ping

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Группа параметров** | | | | | |
| **1 группа 1 категория** | | | **2 группа 1 категория** | | |
| **№** | **Обозначение** | **Назначение** | **№** | **Обозначение** | **Назначение** |
|  |  |  | 1 | (-t -n) -a -l -f -i -v (-r -s -j -k) -w -S -4 | Можно выбрать любой из этих параметров, либо все сразу, кроме тех, что в (). Настройка всех параметров, что указываются в выводе с параметрами. |

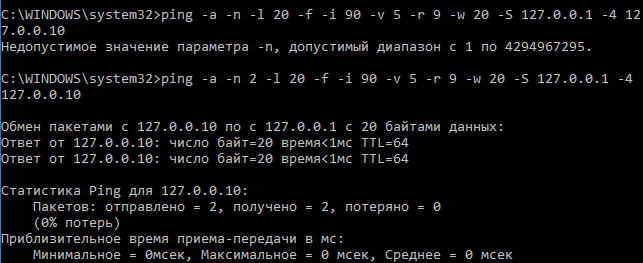
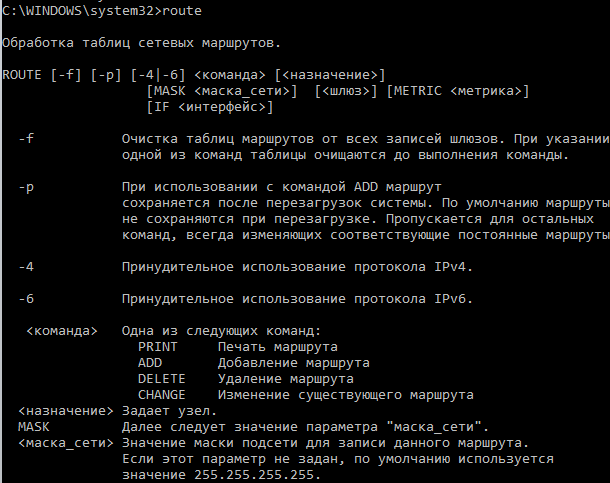


Рис.4.16 - **ping** 2 группа вывод с параметрами (-t -n) -a -l -f -i -v (-r -s -j -k) -w -S -4



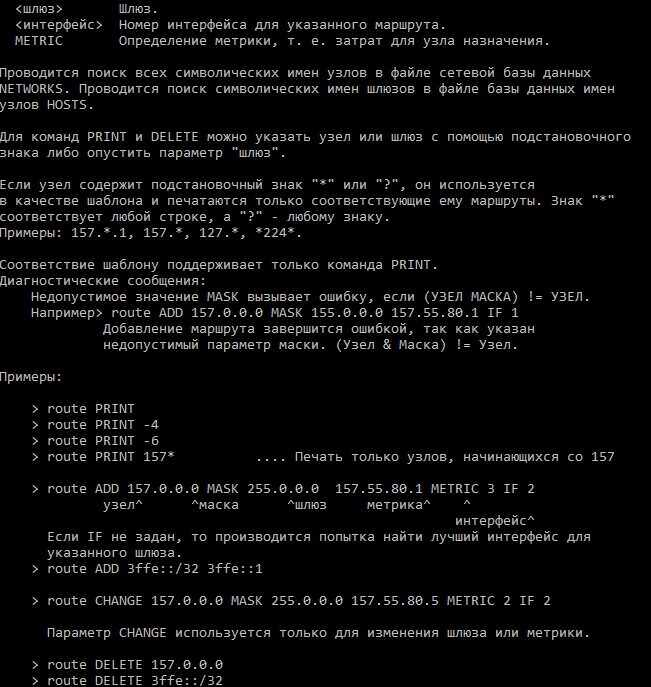


Рис.5.1 - **route** вывод без параметра и вывод справки (для корректной работы необходимо ввести параметры)

Таблица 5.1 - Параметры сетевой утилиты **route**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Группа параметров | | | | | |
| 1 группа - параметры настройки | | | 2 группа - параметры отображения | | |
| № | Обозначение | Назначение | № | Обозначение | Назначение |
| 1 | -f | Очистка таблиц маршрута от записей всех шлюзов. | 1 | command | PRINT (печать маршрута). |
| 2 | -p | При использовании с командой ADD задаёт сохранение маршрута при перезагрузки системы. |  |  |  |
| 3 | -4 | Обязательное использование протокола IPv4. |  |  |  |
| 4 | -6 | Обязательное использование протокола IPv6. |  |  |  |
| 5 | command | Одна из команд: ADD (добавление маршрута), DELETE (удаление маршрута), CHANGE (изменение маршрута). |  |  |  |
| 6 | destination | Адресуемый узел. |  |  |  |
| 7 | MASK | Указывает, что следующий параметр является маской сети. |  |  |  |
| 8 | netmask | Значение маски подсети. |  |  |  |
| 9 | gateway | Шлюз. |  |  |  |
| 10 | interface | Номер интерфейса. |  |  |  |
| 11 | METRIC | Определение метрики (цена для адресуемого узла). |  |  |  |

Таблица 5.2 - Значение параметров 1 группы сетевой утилиты **route**

|  |  |  |
| --- | --- | --- |
| № | Обозначения параметра | Значение параметра |
| 1 | [command] | PRINT, ADD, DELETE, CHANGE |
| 2 | [destination] | IP-адрес адресуемого узла |
| 3 | MASK | [netmask] |
| 4 | [netmask] | Маска сети точки назначения |
| 5 | [gateway] | IP-адрес шлюза |
| 6 | [interface] | Индекс интерфейса |
| 7 | METRIC | Метрика стоимости маршрута |



Рис.5.2 - **route** вывод с параметром -f



Рис.5.3 - **route** вывод с параметром -p -4 [command]

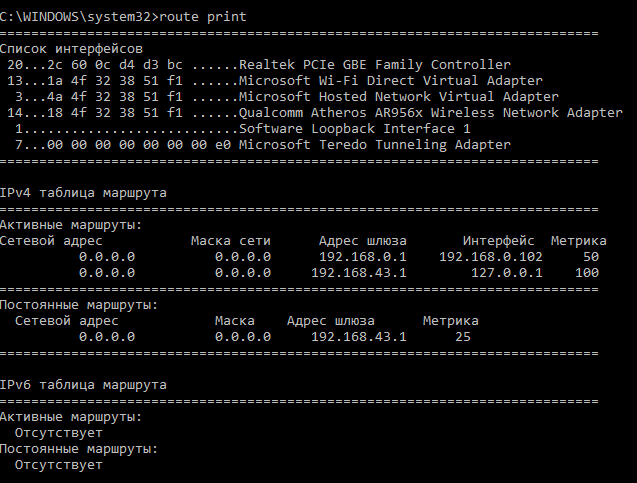


Рис.5.4. - **route** вывод с параметром [command] = PRINT

Таблица.5.3 - Параметры сетевой утилиты **route**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Группа параметров** | | | | | |
| **1 группа 1 категория** | | | **2 группа 1 категория** | | |
| **№** | **Обозначение** | **Назначение** | **№** | **Обозначение** | **Назначение** |
| 1 | [command]=DELETE [destination] | Удаление маршрута |  |  |  |
| 2 | [command]=ADD [destination][gateway] | Добавление маршрута с указанием шлюза с маской = 255.255.255.255 |  |  |  |
| 3 | [command]=ADD [destination] MASK [netmask] [gateway] | Добавление маршрута с указанием маски и шлюза. |  |  |  |
| 4 | (-p) (-4) [command] [destination] (MASK [netmask]) [gateway] (METRIC) (IF [interface]) | ( ) - параметр, который необязательно указывать. Добавление маршрута со всеми указанными параметрами. |  |  |  |



Рис.5.5 - route вывод с параметрами [command]=DELETE [destination]



Рис.5.6 - **route** вывод с параметрами [command]=ADD [destination][gateway]



Рис.5.7 - **route** вывод с параметрами [command]=ADD [destination] MASK [netmask] [gateway]

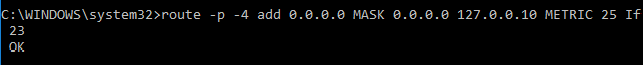


Рис.5.8 - **route** вывод с параметрами (-p) (-4) [command] [destination] (MASK [netmask]) [gateway] (METRIC) (IF [interface])

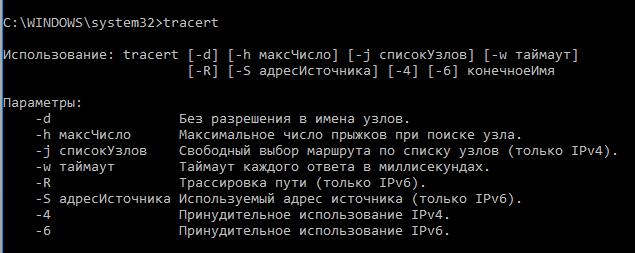


Рис.6.1 - **tracert** вывод без параметра и вывод справки

Таблица 6.1 - Параметры сетевой утилиты **tracert**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Группа параметров** | | | | | |
| **1 группа - параметры настройки** | | | **2 группа - параметры отображения** | | |
| **№** | **Обозначение** | **Назначение** | **№** | **Обозначение** | **Назначение** |
| 1 | -d | Запрет использования разрешений в именах узлов. | 1 | -R | Отображение траcсировки пути (только IPv6). |
| 2 | -h | Настройка максимального числа прыжков при поиске узла. |  |  |  |
| 3 | -j | Настройка свободного выбора маршрута по списку узлов (только IPv4). |  |  |  |
| 4 | -w | Настройка таймаута каждого ответа в миллисекундах. |  |  |  |
| 5 | -S | Использовать указанный адрес источника (только IPv6). |  |  |  |
| 6 | -4 | Принудительное использование IPv4. |  |  |  |
| 7 | -6 | Принудительное использование IPv6. |  |  |  |

Таблица 6.2 - Значение параметров 1 группы сетевой утилиты tracert

|  |  |  |
| --- | --- | --- |
| № | Обозначения параметра | Значение параметра |
| 1 | -h | Максимальное количество прыжков |
| 2 | -j | Список узлов |
| 3 | -w | Таймаут в миллисекундах |
| 4 | -S | IP-адрес источника |

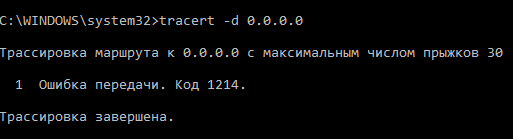


Рис.6.2 - **tracert** вывод с параметром -d

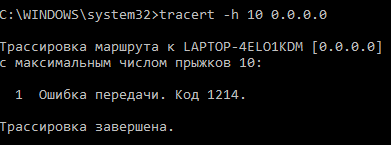


Рис.6.3 - **tracert** вывод с параметром –h

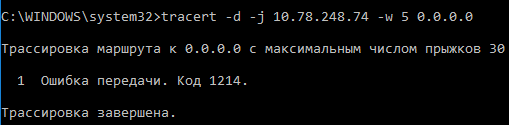


Рис.6.4 - **tracert** вывод с параметром –j

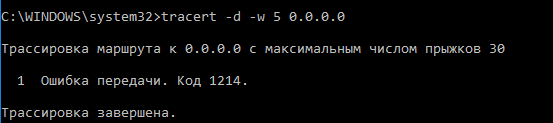


Рис.6.5 - **tracert** вывод с параметром –w

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Группа параметров** | | | | | |
| **1 группа 1 категория** | | | **2 группа 1 категория** | | |
| **№** | **Обозначение** | **Назначение** | **№** | **Обозначение** | **Назначение** |
| 1 | -d -h -j -w -4 | Можно использовать любой из этих параметров в любом количестве. Настраивает все указанные параметры. |  |  |  |

**Вывод**

1. **Arp** - отображение и изменение таблиц преобразования IP-адресов в физические, используемые протоколом разрешения адресов. При запуске утилиты без параметров выводится справочная информация, а параметра справки для этой утилиты нет. Есть возможность изменения arp-записей.
2. **Ipconfig** используется для отображения текущих настроек протокола TCP/IP и для обновления некоторых параметров, задаваемых при автоматическом конфигурировании сетевых интерфейсов при использовании протокола DHCP. При запуске утилиты без параметров выводится информация о базовых сетевых настройках для всех сетевых адаптеров, присутствующих в системе. При запуске утилиты с параметром справки выводится справочная информация. При запуске утилиты с параметрами настройки можно менять некоторые сетевые настройки адаптеров. При запуске утилиты с параметрами отображения выводится разная информация о сетевых настройках адаптеров.
3. **Netstat** предназначена для получения сведений о состоянии сетевых соединений и слушаемых на данном компьютере портах TCP и UDP, а также, для отображения статистических данных по сетевым интерфейсам и протоколам. При запуске утилиты без параметров выводится статистика соединений, а с параметром справки выводится справочная информация. При запуске утилиты с параметром справки выводится справочная информация. При запуске утилиты с параметрами отображения показывает нам статистику в нужном виде. Не имеет параметра настройки.
4. **Ping** используется для обмена служебной и диагностической информацией в сети используется специальный протокол управляющих сообщений ICMP. Команда позволяет выполнить отправку управляющего сообщения типа Echo Request (тип равен 8 и указывается в заголовке ICMP-сообщения) адресуемому узлу и интерпретировать полученный от него ответ в удобном для анализа виде. В поле данных отправляемого icmp-пакета обычно содержатся символы английского алфавита. В ответ на такой запрос, опрашиваемый узел должен отправить icmp-пакет с теми же данными, которые были приняты, и типом сообщения Echo Reply (код типа в ICMP-заголовке равен 0) . Если при обмене icmp-сообщениями возникает какая-либо проблема, то утилита ping выведет информацию для ее диагностики. При запуске утилиты без параметров выводится справочная информация. Параметра справки для этой утилиты нет. У утилиты нет параметров отображения.
5. Утилита **Route** позволяет провести обработку записей сетевых маршрутов. При запуске утилиты без параметров выводится справочная информация. При запуске утилиты с параметром справки выводится справочная информация. При запуске утилиты с параметрами настройки можно обрабатывать записи сетевых маршрутов.
6. Утилита трассировки маршрута до заданного узла tracert используется, чтобы получить цепочку узлов, через которые проходит IP-пакет, адресованный конечному узлу, имя или IP-адрес которого задается параметром командной строки. При запуске утилиты без параметров выводится справочная информация. Параметра справки для этой утилиты нет. При запуске утилиты с параметрами настройки можно менять настройки трассировки маршрута на необходимые. У утилиты нет параметров отображения.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«Санкт-Петербургский национальный исследовательский университет  
информационных технологий, механики и оптики»

Лабораторная работа №2

Выполнил студент группы М3204:  
Наскальнюк Никита Андреевич

САНКТ-ПЕТЕРБУРГ  
2018

**Назначение**

Приобретение навыков по решению основных видов задач, возникающих в сетях связи.

**Цель работы**

Получение навыков по решению задачи определения доступности сетевого узла при различных вариантах его размещения;

Получение навыков по решению задач управления параметрами сетевых узлов, необходимых для организации связи;

Получение навыков по решению задач управления сетевыми соединениями между информационными приложениями, работающими на сетевых узлах;

Получение навыков по решению задач маршрутизации в сетях связи.

**Перечень используемого оборудования и ПО**

1) Персональный компьютер с установленной ОС Windows, ОС Linux или ОС Mac

2) Командная строка в ОС Windows или терминал в ОС Linux и ОС Mac

3) Сетевое устройство, находящееся в локальной сети и осуществляющее маршрутизацию в глобальную сеть.

**Выполнение работы**

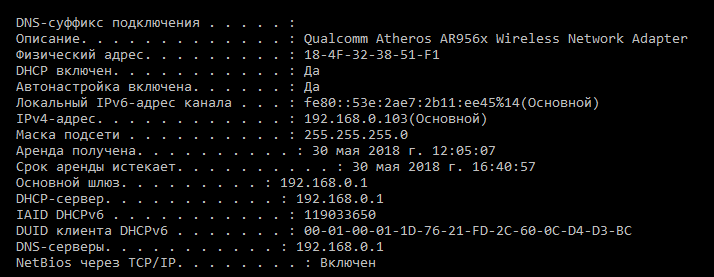


Рис.1.1 Сетевые параметры компьютера LAPTOP-4ELO1KDM (физический адрес, сетевой адрес, маска подсети, адрес подсети). Команда ipconfig /all

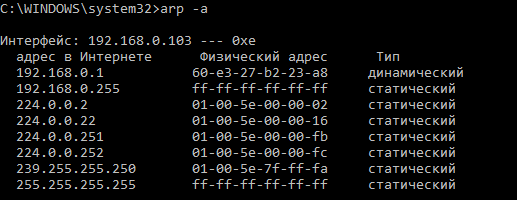


Рис.1.2 Сетевые устройства в локальной сети (физический адрес, сетевой адрес).

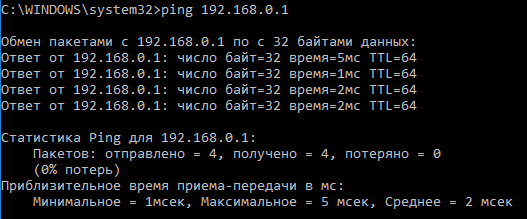


Рис.1.3 Проверка доступности 192.168.0.1

Таблица 1.1 – Сетевые параметры

|  |  |  |  |
| --- | --- | --- | --- |
| **Устройство** | | **LAPTOP-4ELO1KDM 192.168.0.103** | |
| **№** | **Сетевой параметр** | **Значение** | **Назначение** |
| 1 | Физический адрес | 18-4F-32-38-51-F1 | позволяет уникально идентифицировать каждый узел сети |
| 2 | Сетевой адрес | 192.168.0.103 | нужен для идентификации компьютеров в сети, для адресации данных – для связи компьютеров между собой |
| 3 | Маска подсети | 255.255.255.0 | указывает на то, какая часть IP-адреса является идентификатором сети, а какая —идентификатором узла. |
| 4 | Адрес подсети | 192.168.0.0 | определение подсети IP-адресов. |

Таблица 1.2 – Сетевые параметры

|  |  |  |  |
| --- | --- | --- | --- |
| **Устройство** | | **Маршрутизатор 192.168.0.1** | |
| **№** | **Сетевой параметр** | **Значение** | **Назначение** |
| 1 | Физический адрес | 60-e3-27-b2-23-a8 | Позволяет уникально идентифицировать каждый узел сети |
| 2 | Сетевой адрес | 192.168.0.1 | нужен для идентификации компьютеров в сети, для адресации данных – для связи компьютеров между собой |

Таблица 1.3 – Доступность узла

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Сетевой адрес устройства** | **Доменное имя устройства** | **Среднее время приема – передачи,мс** |
| 1 | 192.168.0.1 | - | 2 |

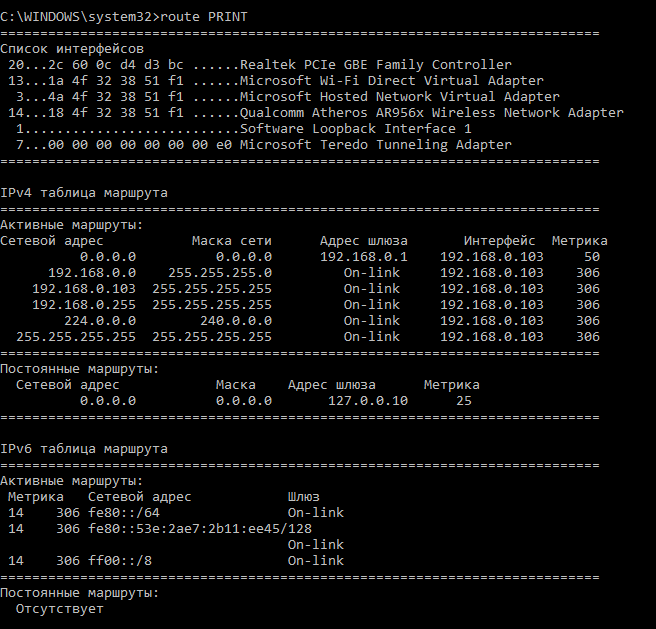


Рис. 2.1 Маршрутизация на устройстве LAPTOP-4ELO1KDM

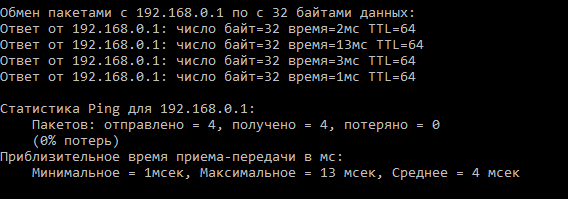


Рис.2.2 Проверка доступности

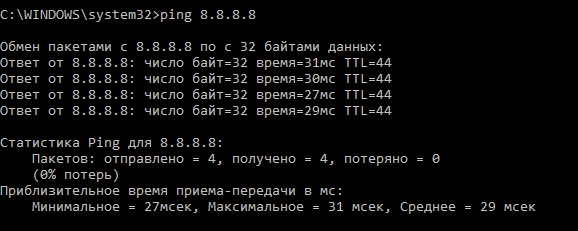


Рис.2.3 Проверка доступности 8.8.8.8

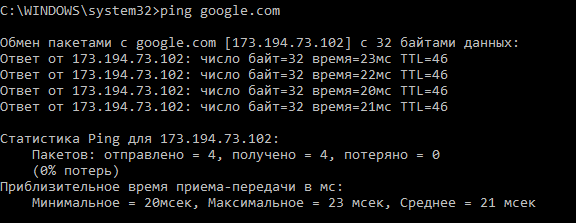


Рис.2.4 Проверка доступности 173.194.73.102

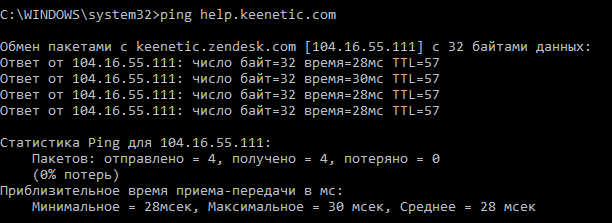


Рис.2.5 Проверка доступности 104.16.55.111

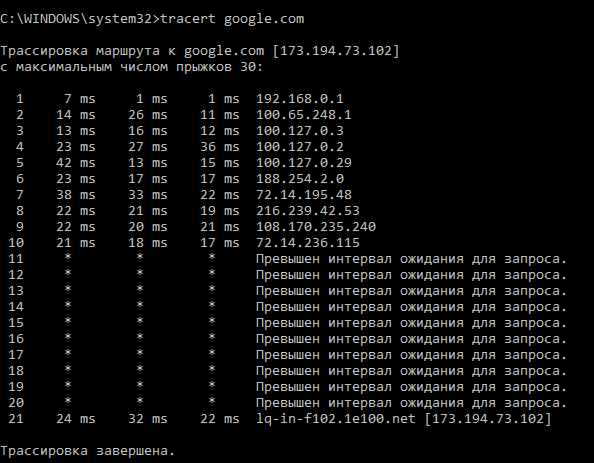


Рис.2.6 Сетевые устройства между LAPTOP-4ELO1KDM и 173.194.73.102

Таблица 2.1 – Доступность узла

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Сетевой адрес устройства** | **Доменное имя устройства** | **Среднее время приема – передачи,мс** |
| 1 | 8.8.8.8 | Google.com | 29 |
| 2 | 87.240.182.224 | Help.keenetic.com | 28 |
| 3 | 192.168.0.1 | - | 4 |

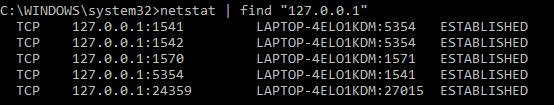


Рис.2.7 Netstat соединения по loopback

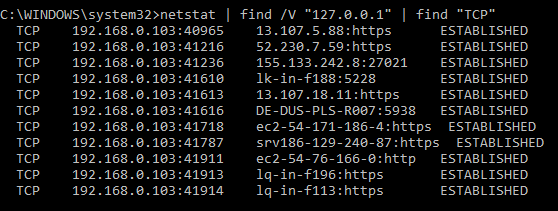


Рис.2.8 Netstat соединения по TCP



Рис.2.9 Netstat соединения по UDP

Таблица 2.2

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Название параметра** | **Значение параметра** | |
|  |  | **TCP** | **UDP** |
| 1 | Сетевой адрес локальный | 127.0.0.1 | - |
| 2 | Порт локальный | 1541, 1542, 1570, 5354, 24359 | - |
| 3 | Сетевой адрес внешний | 192.168.0.103 | - |
| 4 | Порт внешний | 40965-41914 | - |
| 5 | Состояние | Established | - |

# 

Рис.2.9 Netstat соединения по UDP



Рис.2.10 Yandex Browser соединения по TCP

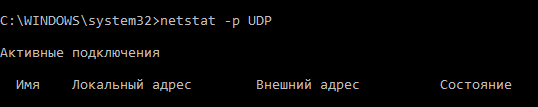


Рис.2.11 Yandex Browser соединения по UDP

# Вывод

**Ipconfig**

1. От сетевой карты.
2. Для всех типов интерфейсов обязателен параметр, по которому можно его уникально идентифицировать.
3. При выполнении команды ipconfig /all выдается вся информация о данном интерфейсе, которая указывает на доступ к ней.

**Arp**

1. Используется протокол arp.
2. Динамическая запись собирается протоколом, а статический адрес можно добавить с помощью ключа -s.
3. Для любого сетевого интерфейса в таблице всегда будет широковещательный адрес.

**Ping**

1. Команда ping использует протокол ICMP.
2. -
3. Команда route может быть заменена командой netstat с ключом -r.

**Netstat**

1. Воспользоваться ключом -b и командой find с ключом -C.
2. Все.
3. Как правило, 0.0.0.0 — это не маршрутизируемый мета-адрес, который не связан с каким-то конкретным физическим устройством. Если говорить о серверах, то здесь адрес может использоваться вместо любого IPv4 адреса, который принадлежит этой машине, проще говоря, он может быть аналогом локальной петли 127.0.0.1. Если рассматривать этот адрес в контексте маршрутизации, то здесь он используется в качестве маршрута по умолчанию.

**Route**

1. 0
2. С помощью команды ADD
3. netstat -r

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«Санкт-Петербургский национальный исследовательский университет  
информационных технологий, механики и оптики»

Лабораторная работа №3

Выполнил студенты группы М3204:  
Наскальнюк Никита Андреевич

САНКТ-ПЕТЕРБУРГ  
2018

### Цель работы:

Организация безопасных и небезопасных сетевых соединений для удаленного управления устройствами сетей связи.

### Назначение:

1. Приобретение знаний по организации удаленного управления устройствами сетей связи.
2. Формирование навыков по управлению устройствами сетей связи

### Перечень используемого оборудования и ПО:

1. Персональный компьютер с установленной ОС Windows, OC Linux или ОС Mac.
2. ПО Putty
3. Маршрутизатор

### Ход выполнения работы:

Telnet:

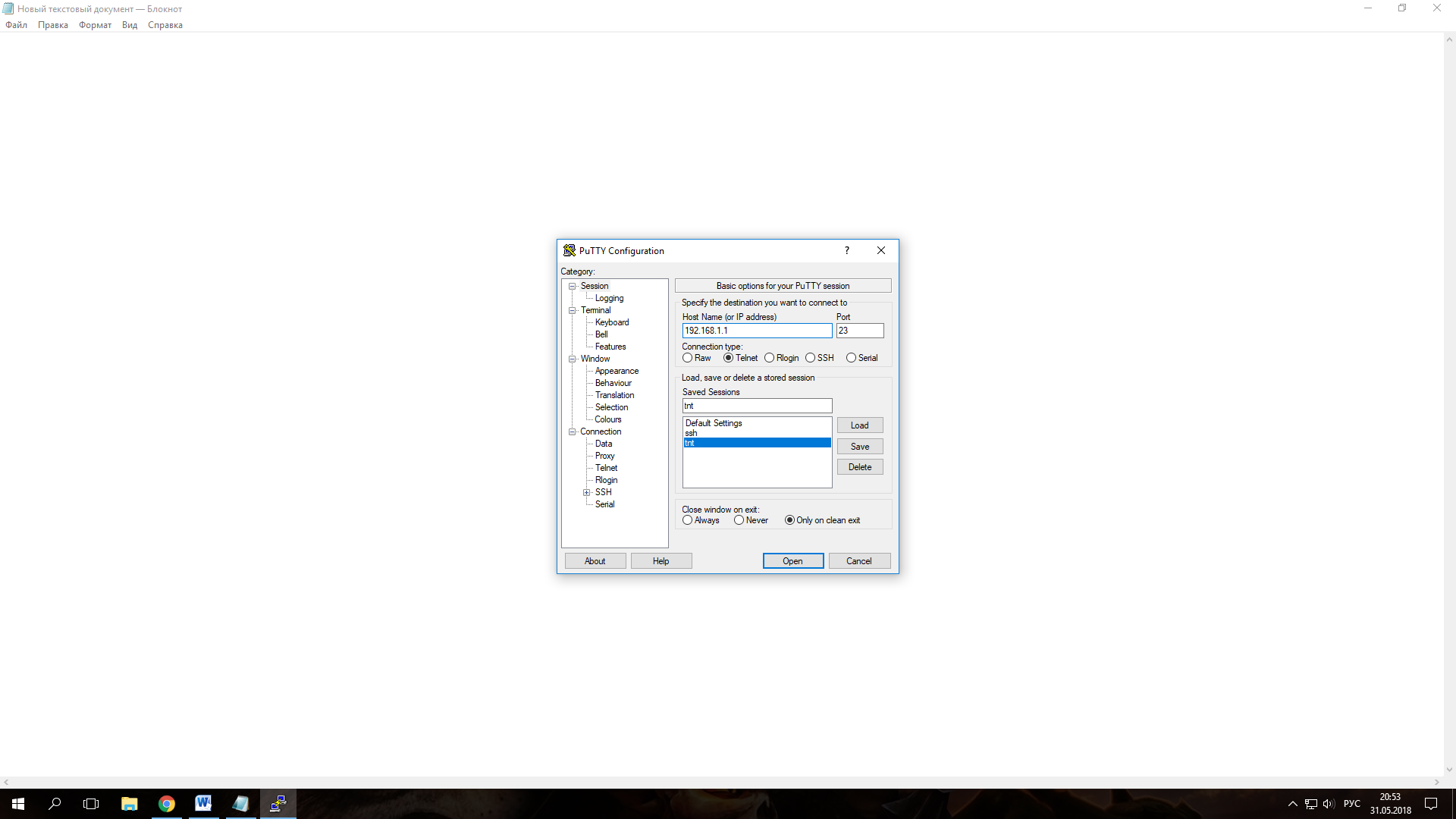
1. Запустили программу. Настроили сетевые параметры для организации сеанса управления по протоколу Telnet. 

Рис.1 - Сетевые параметры для организации сеанса управления по протоколу Telnet.

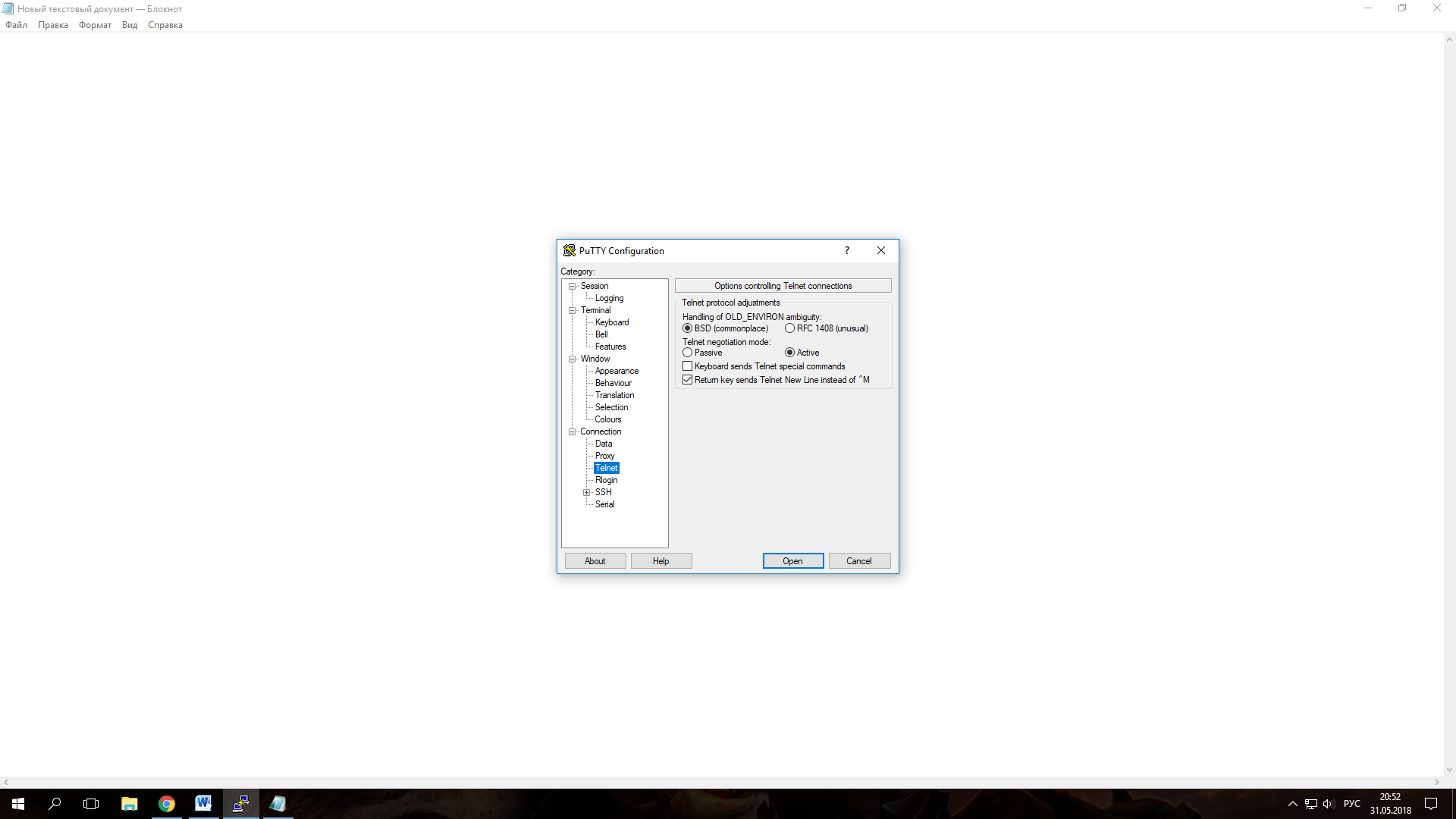
1. Сохранили сетевые параметры для организации сеанса управления по протоколу Telnet. Настроили дополнительные параметры соединения по протоколу Telnet. 

Рис.2 - Дополнительные параметры соединения по протоколу Telnet

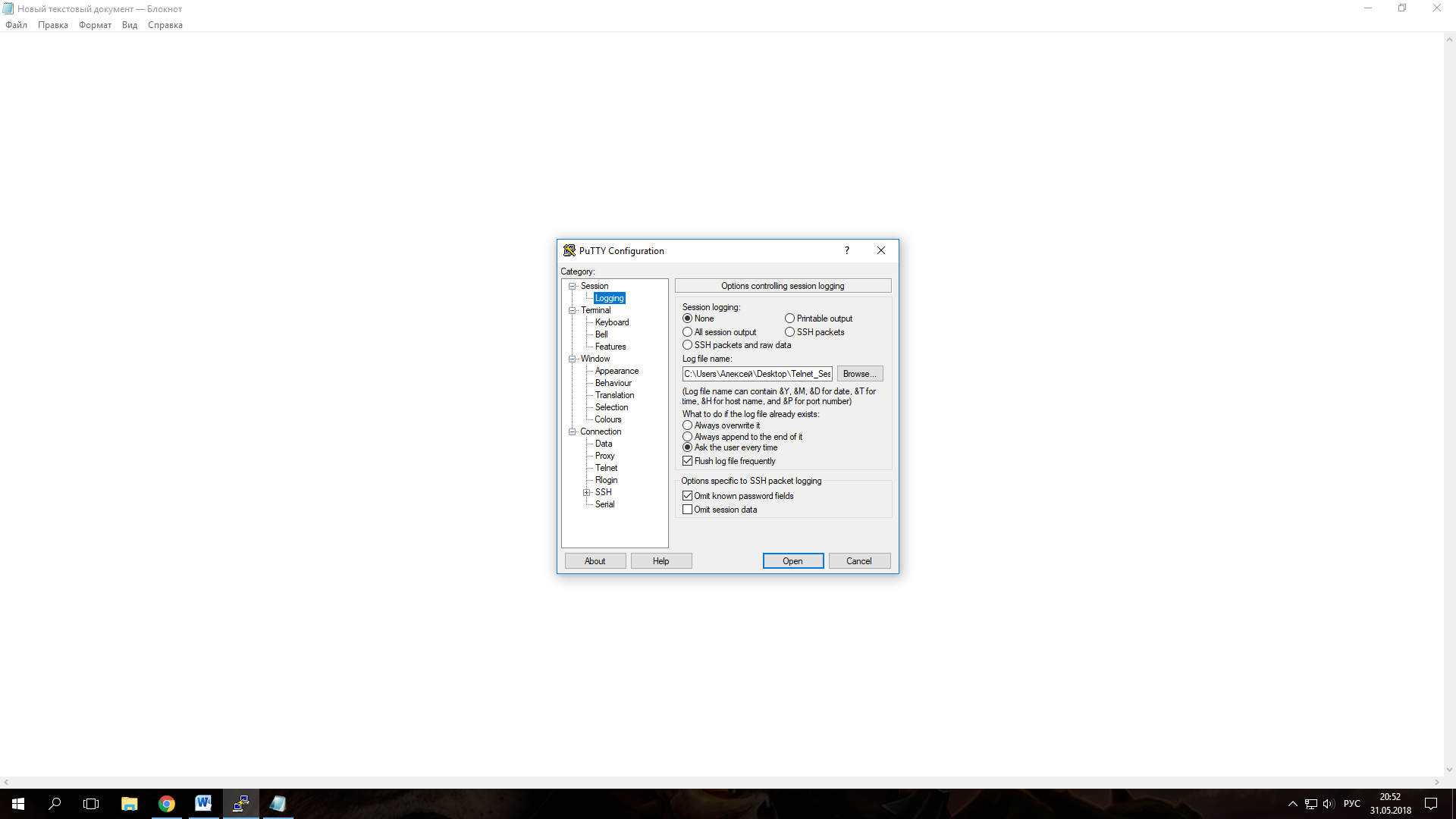
1. Настроили запись сеанса управления по протоколу Telnet в журнал событий. 

Рис.3 - Настройки записи сеанса управления по протоколу Telnet в журнал событий

1. На основе данных рисунка «Таблица сетевых соединений протокол Telnet» заполнили таблицу

Таблица -

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№** | **Название устройства** | **Сетевой адрес устройства** | **Название протокола** | **Номер порта** | **Роль агента, реализующего протокол** |
| 1 | ПК | 192.168.1.61 | telnet | 49787 | клиент |
| 2 | Роутер | 192.168.1.1 | telnet | 23 | сервер |

SSH:

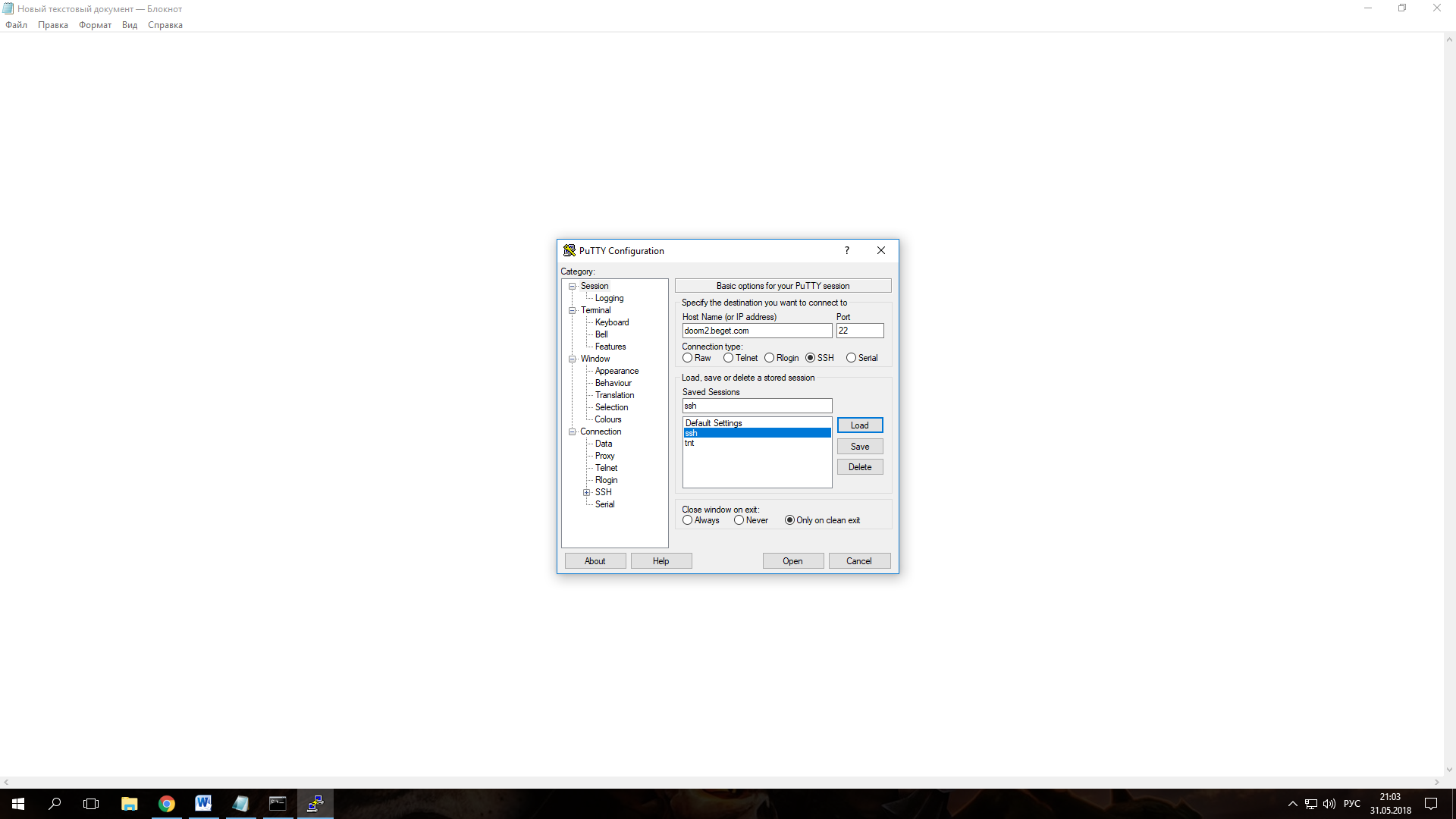
1. Настроили сетевые параметры для организации сеанса управления по протоколу SSH. На маршрутизаторе было недоступно подключение по SSH протоколу, поэтому было выполнено подключение к удаленному серверу. 

Рис.1 - Сетевые параметры для организации сеанса управления по протоколу SSH

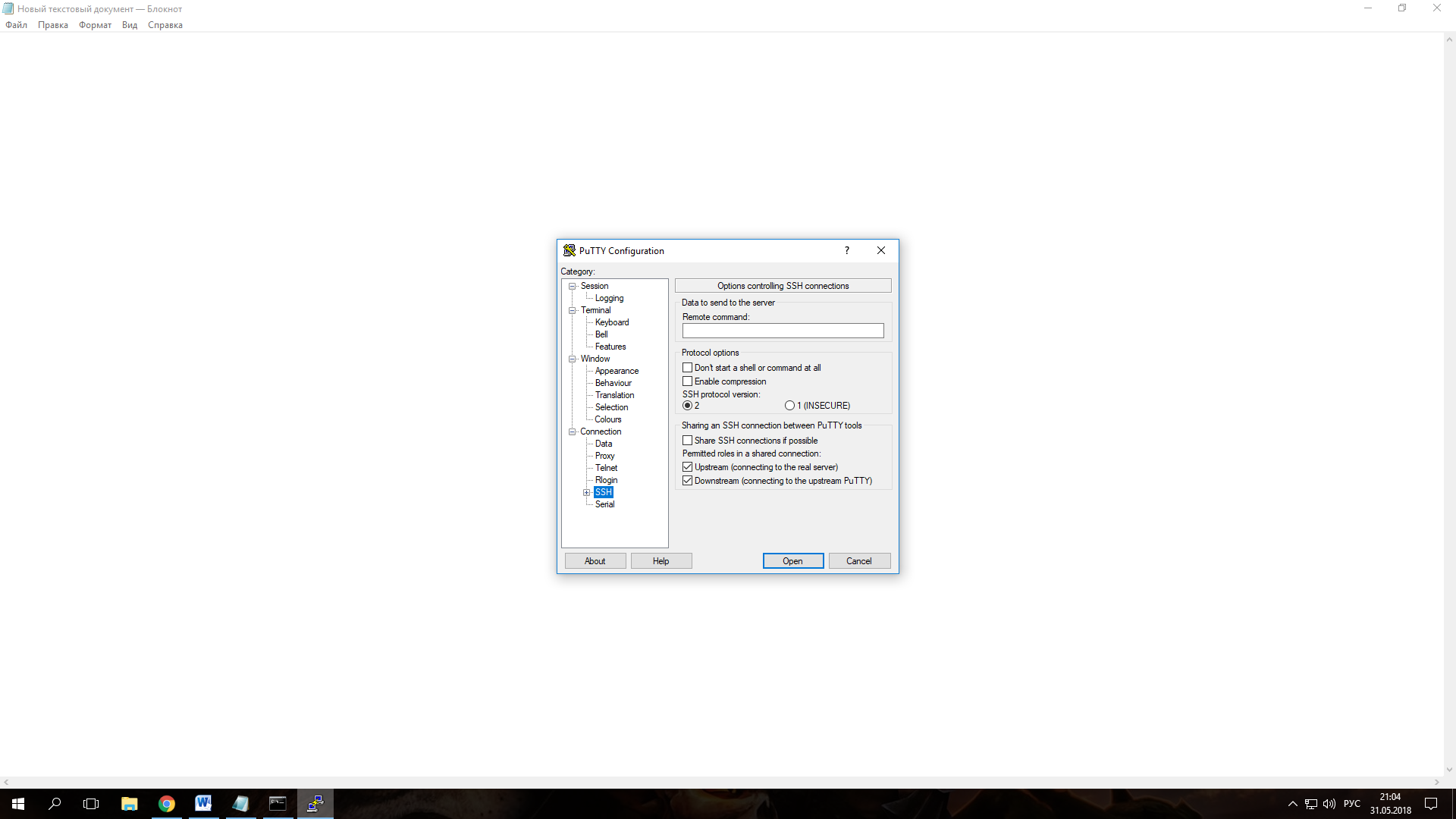
1. Настроили дополнительные параметры соединения по протоколу SSH 

Рис.2 - Дополнительные параметры соединения по протоколу SSH

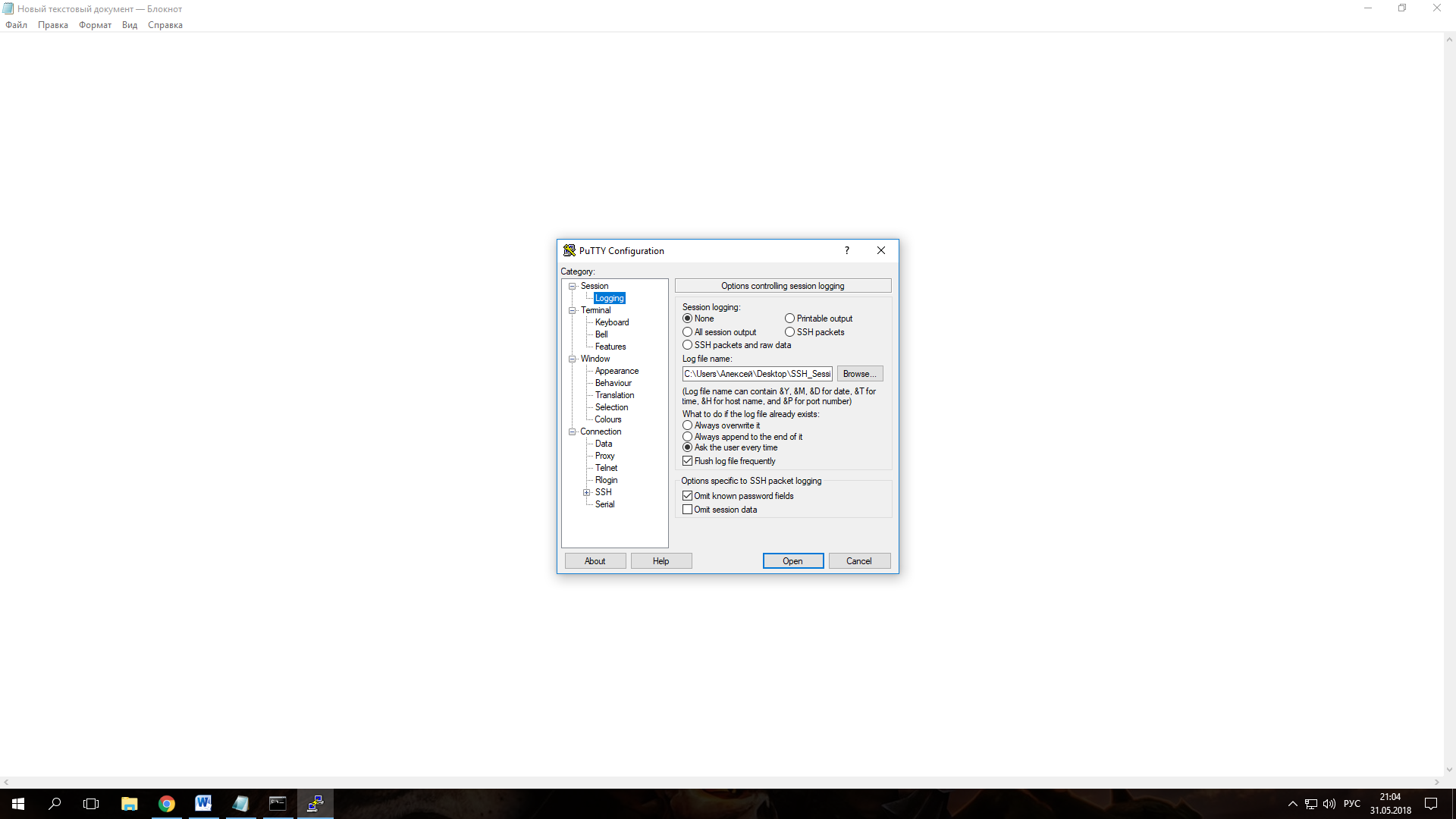
1. Настроили журнал для записи событий во время сеанса управления по протоколу SSH. 

Рис.3 - Настройки записи сеанса

1. Запустили сеанс управления по протоколу SSH. Завершили сеанс управления по протоколу SSH. Проверили наличие записи сеанса в журнале событий. 

Рис.4 - Запись в журнале событий

|  |
| --- |
| Информация файла журнала событий SSH\_Session\_Logging.log |
|  |

На основе данных рисунка «Таблица сетевых соединений протокол SSH» заполнить таблицу

Таблица

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№** | **Название устройства** | **Сетевой адрес устройства** | **Название протокола** | **Номер порта** | **Роль агента, реализующего протокол** |
| 1 | ПК | 192.168.42.140 | ssh | 51626 | клиент |
| 2 | Удален.сервер | m1 | ssh | 22 | сервер |

### Вывод:

Особенности организации удаленного управления устройствами сетей связи

1. Организация удаленного управления предусматривает выполнение следующих шагов: определения сетевого адреса удаленного устройства, выбор протокола соединения, определение порта соединения, открытие соединения.
2. Записи в журнал событий необходимо выполнять для дальнейшей обработки информации, полученной в ходе удаленного управления устройством, а также для отладки соединения при возникновении ошибок.

Удаленное управление через небезопасные сетевые соединения

1. Для организации небезопасных соединений используется протокол telnet.
2. В протоколе не предусмотрено использование ни шифрования, ни проверки подлинности данных.

Удаленное управление через безопасные сетевые соединения

1. Для организации безопасного соединения используется протокол SSH.
2. Протокол предусматривает шифрование передаваемых данных, а также имеет возможность проверять подлинность данных с помощью ключей RSA.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ  
 ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«Санкт-Петербургский национальный исследовательский университет  
информационных технологий, механики и оптики»

Факультет информационных технологий и программирования

Кафедра информационных систем

Лабораторная работа № 4

Телекоммуникационные системы и технологии  
Исследование основных способов обеспечения безопасности в сетях связи

Выполнил студент группы № М3204:  
Наскальнюк Никита Андреевич

Санкт – Петербург  
2018

Лабораторная работа 4

Исследование основных способов обеспечения безопасности в сетях связи

1 Назначение

Приобретение знаний и умений по решению основных задач обеспечения безопасности, возникающих в сетях связи.

2 Цель работы

Формирование навыков по использованию основных инструментов фильтрации трафика в сетях связи – брандмауэров и iptables.

3 Перечень используемого оборудования и ПО

1. Персональный компьютер с установленной ОС Windows, или ОС Linux или ОС Mac
2. Брандмауэр Windows в ОС Windows или сетевая утилита Iptables в ОС Linux и ОС Maс

4 Порядок выполнения работы

4.1 Работа с брандмауэром Windows

4.1.1 Включение брандмауэра Windows (*Панель управления 🡪 Система и безопасность 🡪 Брандмауэр Windows 🡪 Включение и отключение брандмауэра Windows*). Сделать скриншот и сохранить его. Формат названия файла скриншота «Включение Брандмауэра»

4.1.2 Настройка брандмауэра Windows (*Панель управления 🡪 Система и безопасность 🡪 Брандмауэр Windows 🡪 Дополнительные параметры 🡪 Брандмауэр Windows в режиме повышенной безопасности*). **Определить активный профиль**. Сделать скриншот и сохранить его. Формат названия файла скриншота «Профили Брандмауэра Windows»

Настроить активный профиль в параметры по умолчанию (*Панель управления 🡪 Система и безопасность 🡪 Брандмауэр Windows 🡪 Дополнительные параметры 🡪 Брандмауэр Windows в режиме повышенной безопасности 🡪 Свойства брандмауэра Windows*). Сделать скриншот и сохранить его. Формат названия файла скриншота «Настройка активного профиля»

4.1.3 Настройка входящих подключений (*Панель управления 🡪 Система и безопасность 🡪 Брандмауэр Windows 🡪 Дополнительные параметры 🡪 Правила для входящих подключений*). **Настроить отображение правил только активного профиля** (*Фильтровать по профилю*). Сделать скриншот и сохранить его. Формат названия файла скриншота «Активные правила входящих подключений»

4.1.4 Создать правила для входящих подключений.

1) Правило блокирующее программу для активного профиля (выбрать самостоятельно из программ, установленных на ПК. Например, Skype). Сделать скриншот и сохранить его. Формат названия файла скриншота «Входящее подключение. Блокировка программы <название программы>»

Проверить отработку правила

-запуском программы. Сделать скриншот и сохранить его. Формат названия файла скриншота «Входящее подключение. блокировка приложения <название приложения>.Проверка1»

-просмотром активных соединений в netstat с отображением приложения, инициализирующего подключение «Входящее подключение. Блокировка приложения <название приложения>.Проверка2»

2) Правило блокирующее 22 порт (ssh) по протоколу TCP для активного профиля. Сделать скриншот и сохранить его. Формат названия файла скриншота «Входящее подключение. Блокировка порта <номер порта>».

Проверить отработку правила попыткой подключения с другого компьютера через putty по ssh. Сделать скриншот и сохранить его. Формат названия файла скриншота «Входящее подключение. Блокировка порта <номер порта>.Проверка»

3) Правило блокирующее сетевой адрес с локальной сети. Сделать скриншот и сохранить его. Формат названия файла скриншота «Входящее подключение. Блокировка сетевого адреса <сетевой адрес>»

Проверить отработку правила с помощью сетевой утилиты ping со второго компьютера. Сделать скриншот и сохранить его. Формат названия файла скриншота «Входящее подключение. Блокировка сетевого адреса <сетевой адрес>.Проверка»

4.1.5 Настройка исходящих подключений (*Панель управления 🡪 Система и безопасность 🡪 Брандмауэр Windows 🡪 Дополнительные параметры 🡪 Правила для исходящих подключений*). **Настроить отображение правил только активного профиля** (*Фильтровать по профилю*). Сделать скриншот и сохранить его. Формат названия файла скриншота «Активные правила исходящих подключений»

4.1.6 Создать правила для исходящих подключений.

1) Правило блокирующее программу для активного профиля (выбрать самостоятельно из программ, установленных на ПК. Например, putty). Сделать скриншот и сохранить его. Формат названия файла скриншота «Исходящее подключение. Блокировка приложения <название приложения>»

Проверить отработку правила

-запуском программы. Сделать скриншот и сохранить его. Формат названия файла скриншота «Исходящее подключение. блокировка приложения <название приложения>.проверка1»

-просмотром активных соединений в netstat с отображением приложения, инициализирующего подключение «Исходящее подключение. Блокировка приложения <название приложения>.проверка2»

2) Правило блокирующее 80,443 порт (http, https) по протоколу TCP для активного профиля. Сделать скриншот и сохранить его. Формат названия файла скриншота «Исходящее подключение. Блокировка портов <номер портов>».

Проверить отработку правила путем перехода на произвольный url адрес. Сделать скриншот и сохранить его. Формат названия файла скриншота «Исходящее подключение. Блокировка портов <номер портов>.Проверка»

3) Правило блокирующее сетевой адрес с локальной сети. Сделать скриншот и сохранить его. Формат названия файла скриншота «Исходящее подключение.Блокировка сетевого адреса <сетевой адрес>».

Проверить отработку правила с помощью сетевой утилиты ping. Сделать скриншот и сохранить его. Формат названия файла скриншота «Исходящее подключение. Блокировка сетевого адреса <сетевой адрес>.Проверка»

Открываем брэндмауэр Windows:

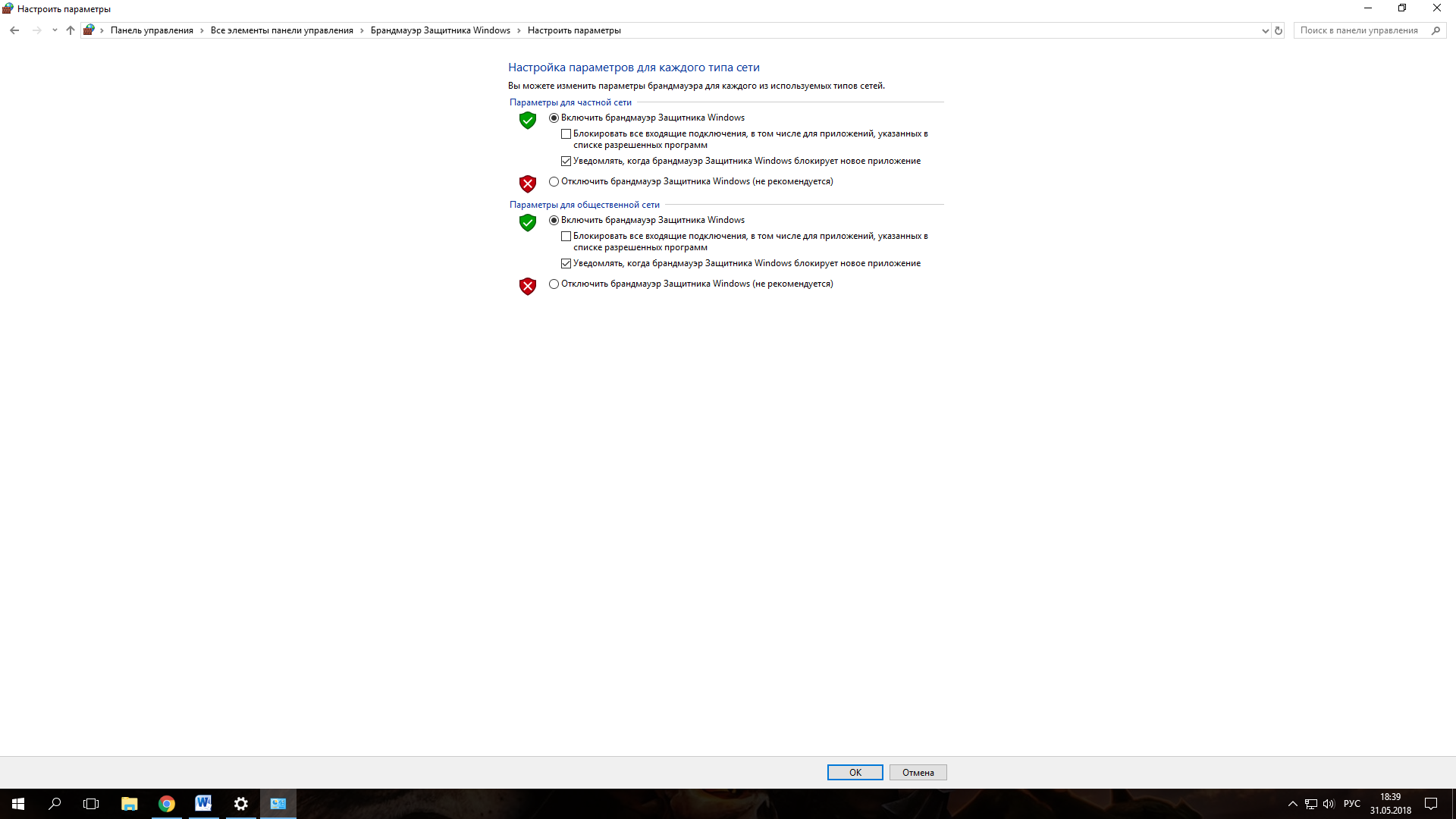


Рис. 1 - «Включения межсетевого экрана»

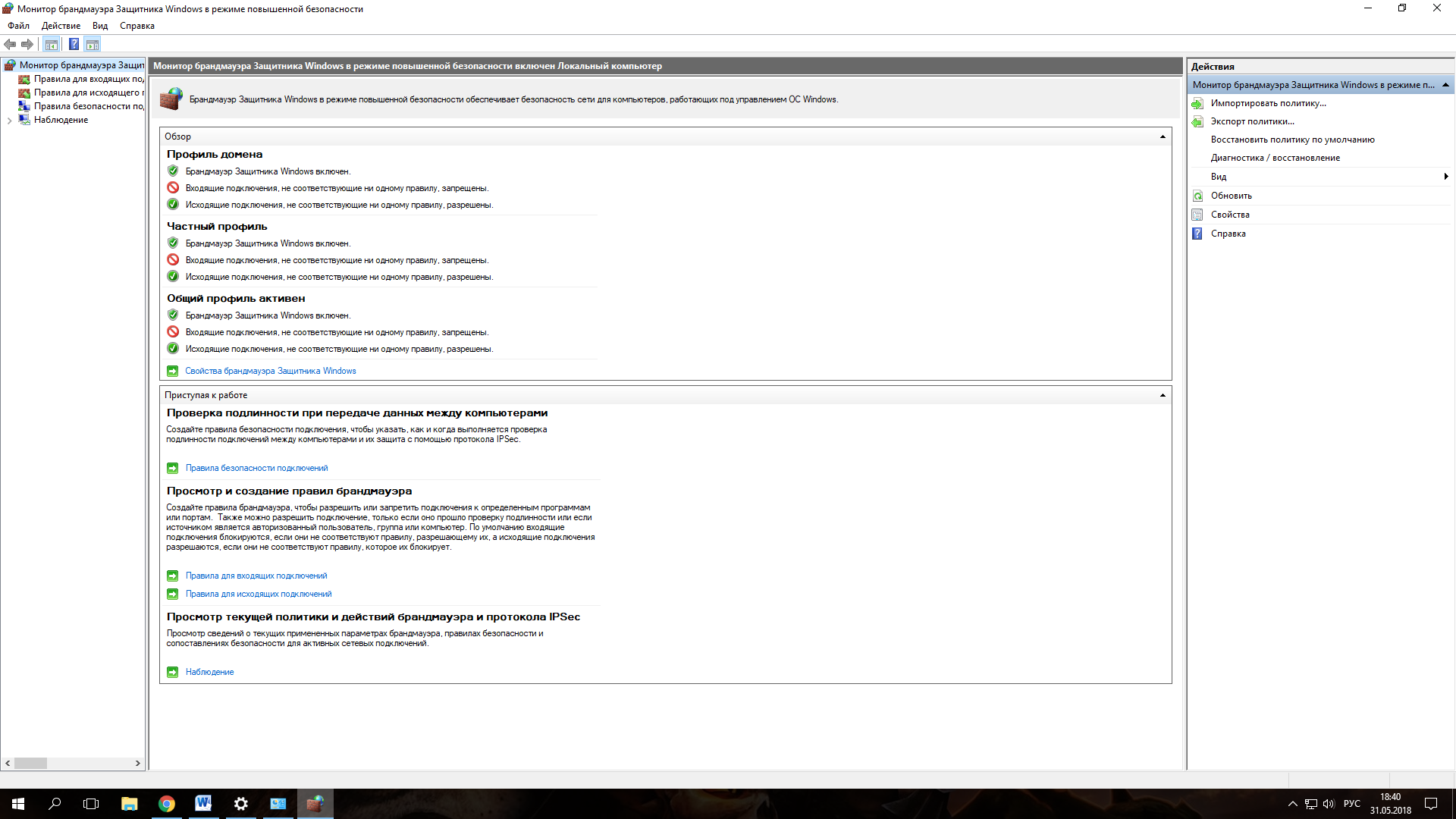


Рис. 2 - «Профили по умолчанию межсетевого экрана»

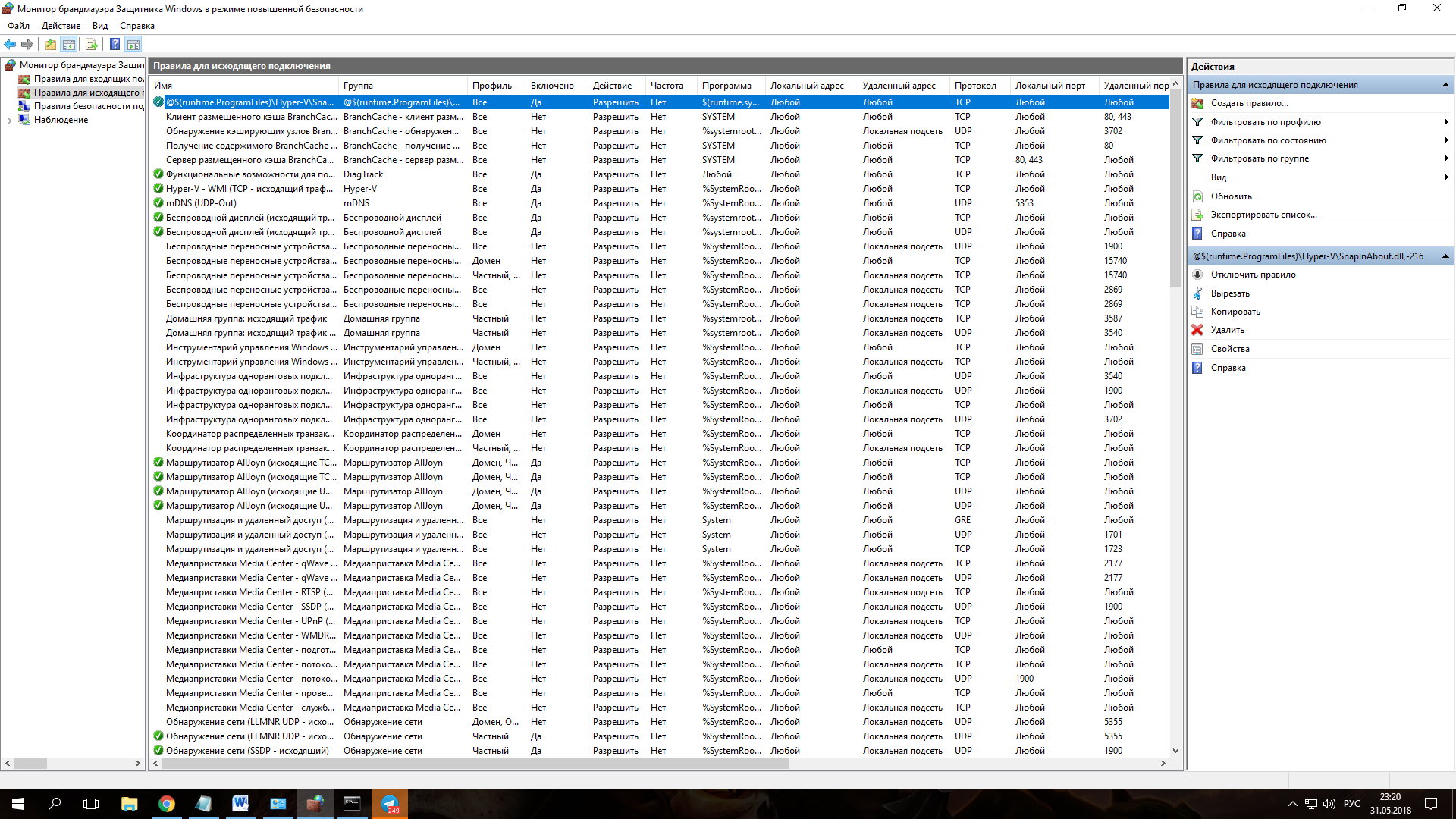
Исходящее подключение. 

Рис. 3 - «Правила для Исходящих подключения»

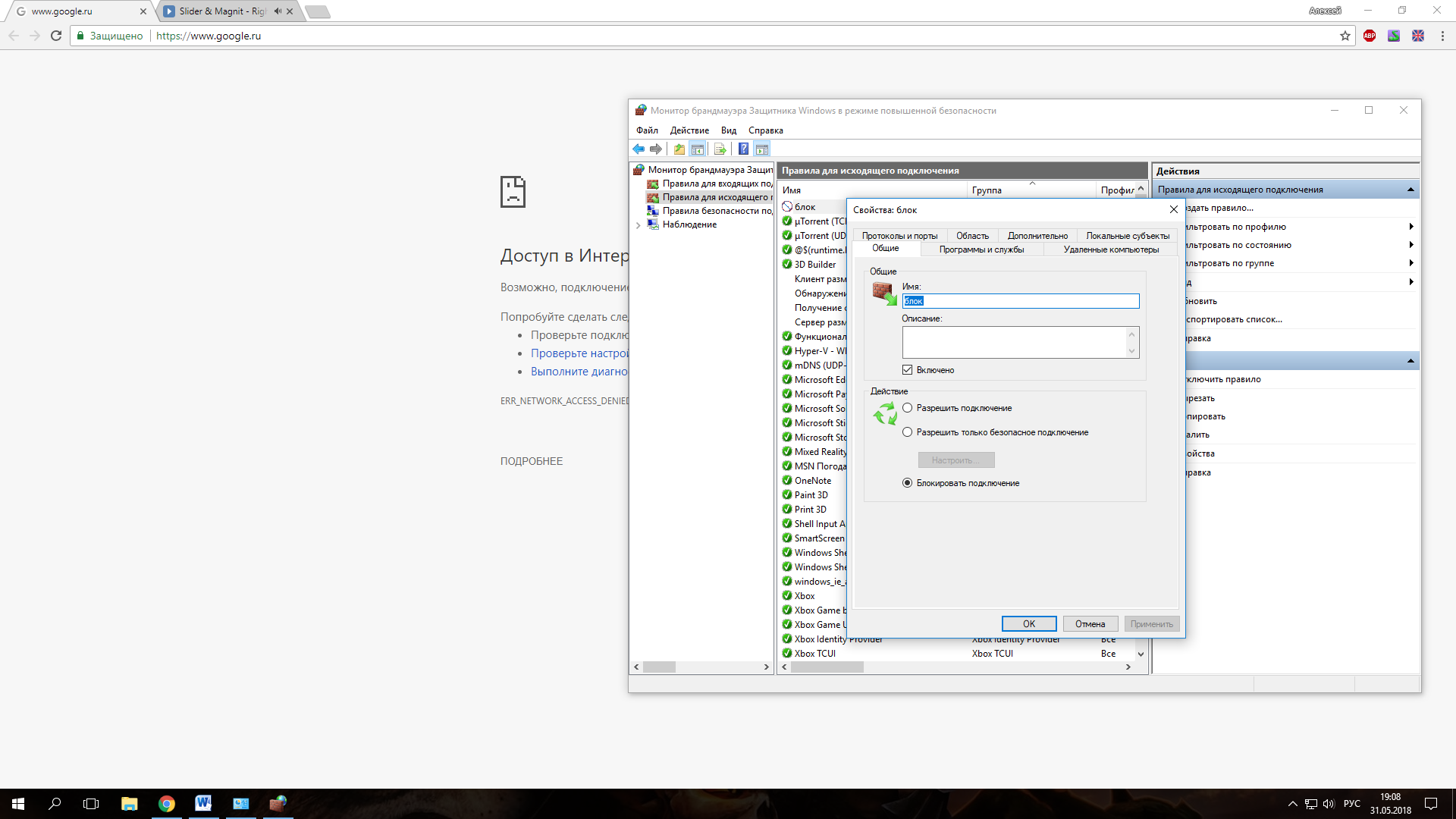


Рис. 4 - «Блокировка приложения Google Chrome»

Для проверки попробуем открыть вкладку в chrome.

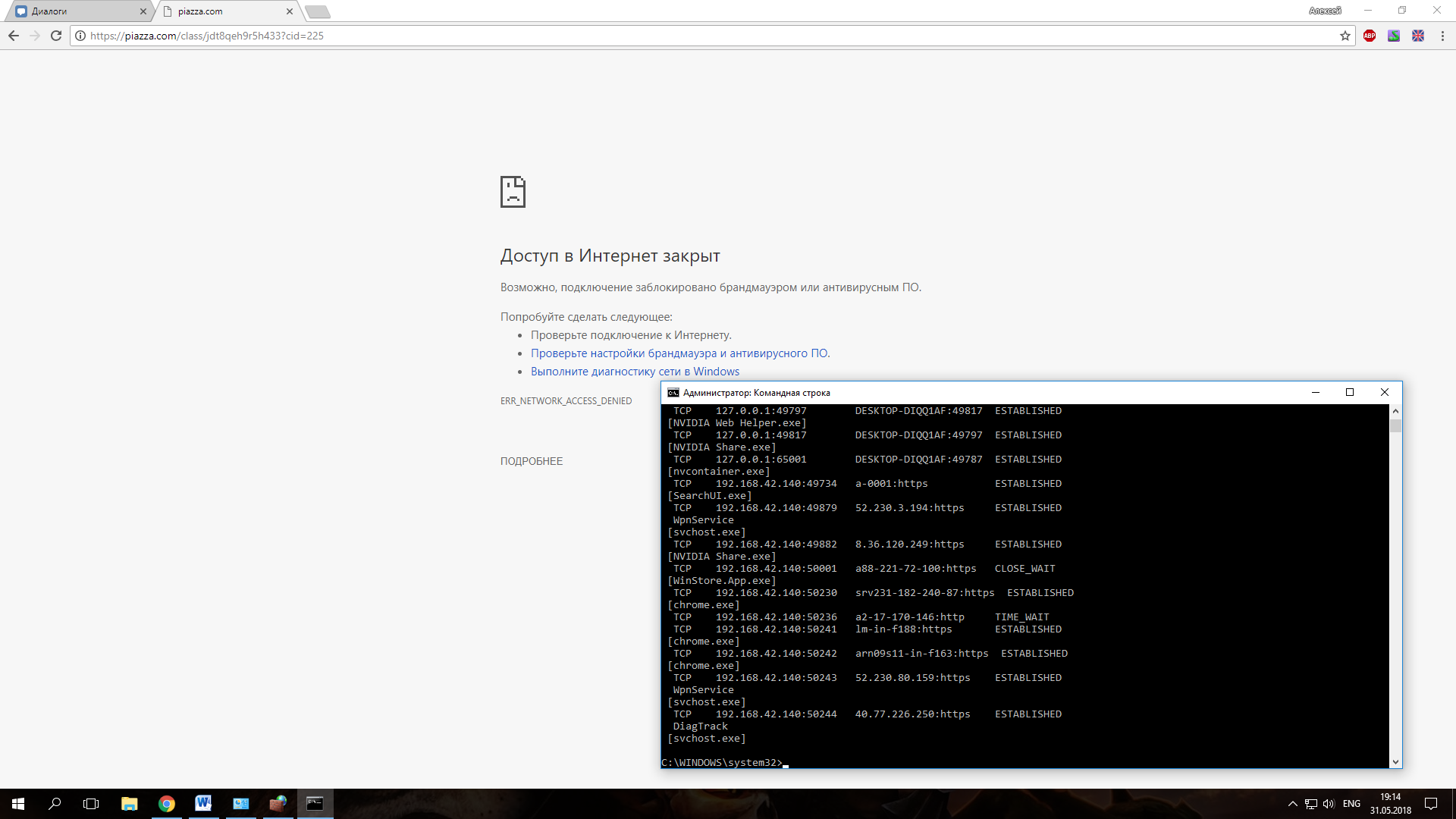
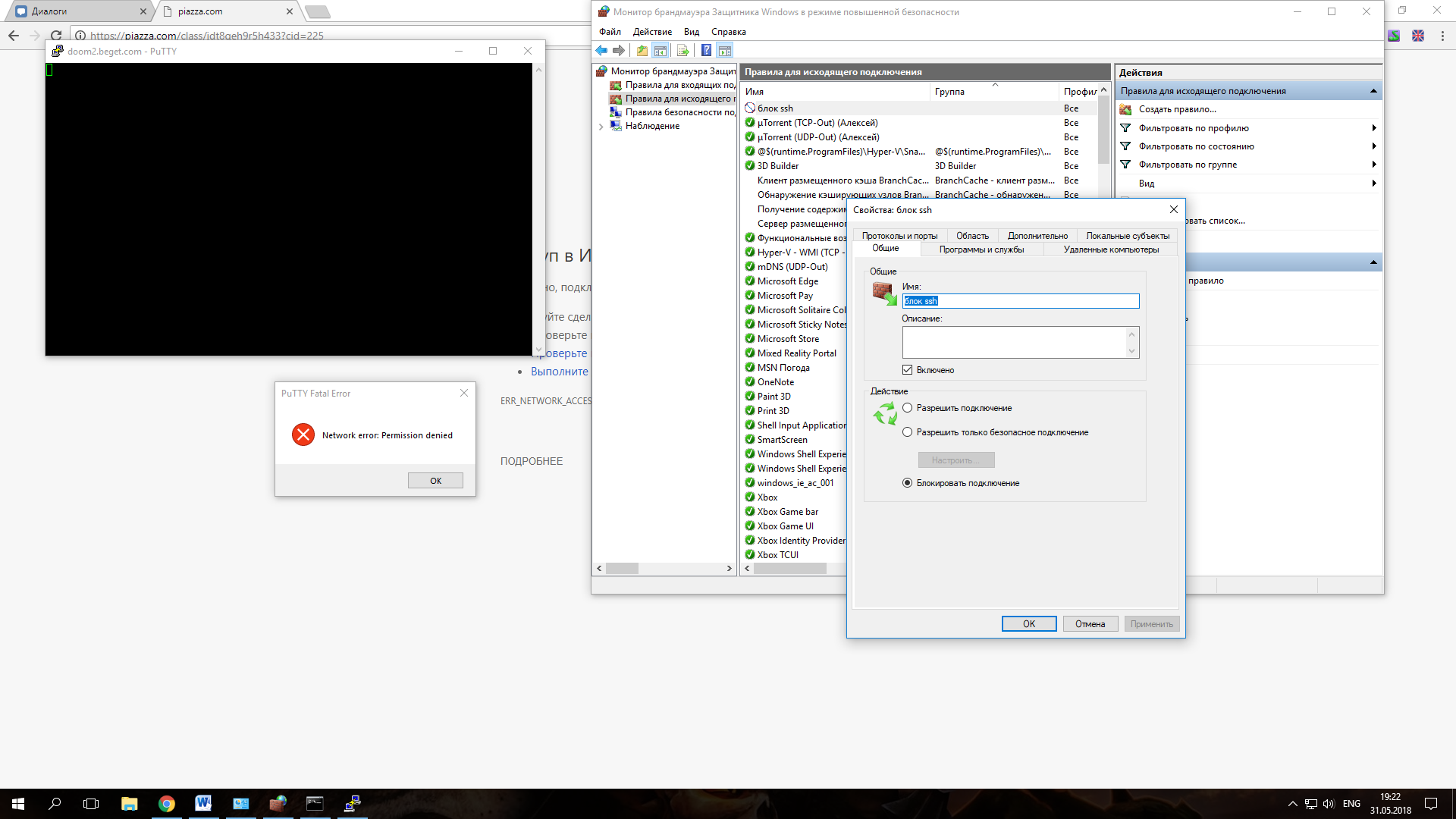


Рис. 5 «Блокировка приложения Google Chrome.Проверка2»

Рис. Рис. 6 - «Блокировка порта ssh»

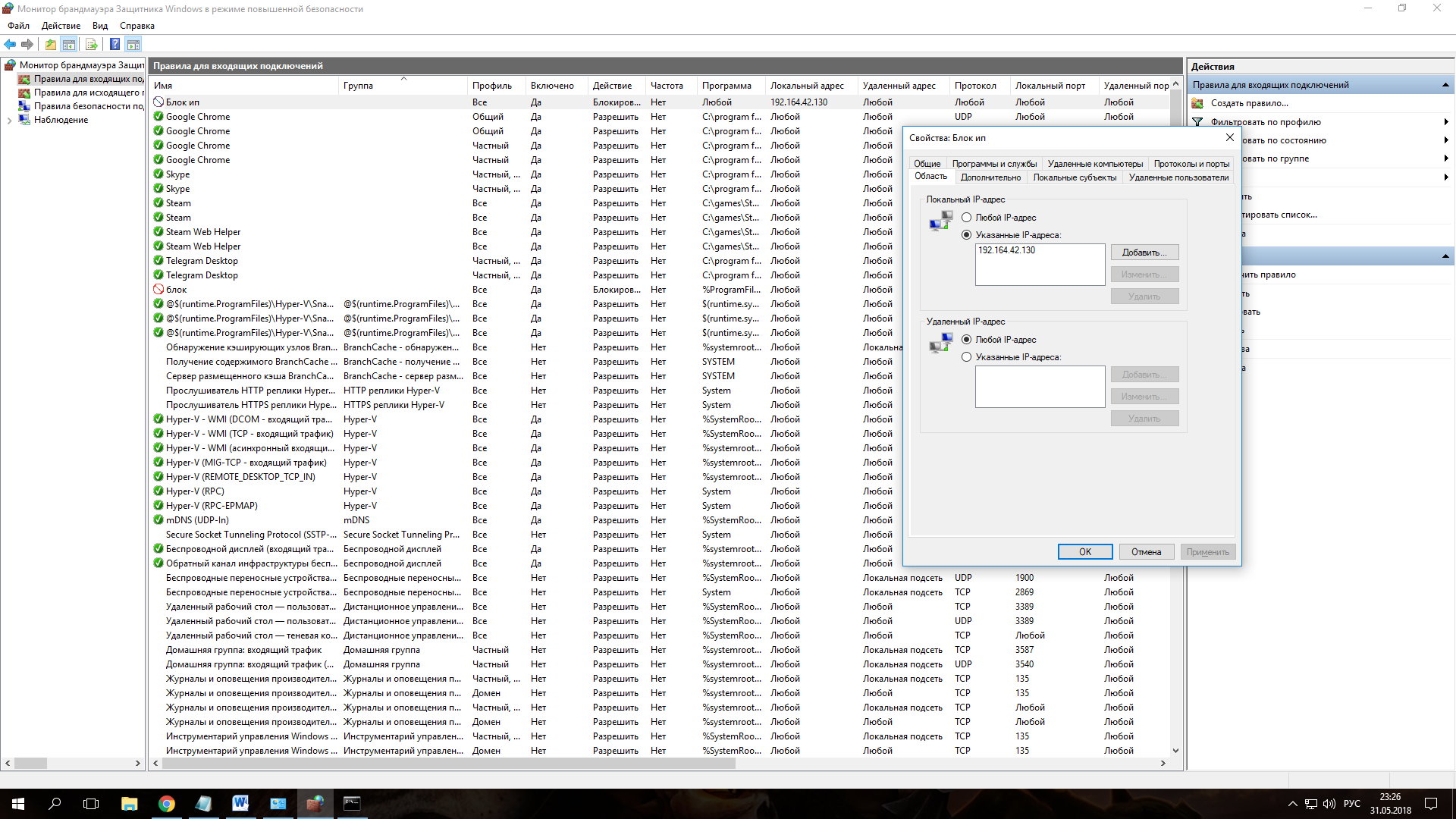


Рис. 9 - «Блокировка сетевого адреса»

Для проверки воспользуемся командой ping.



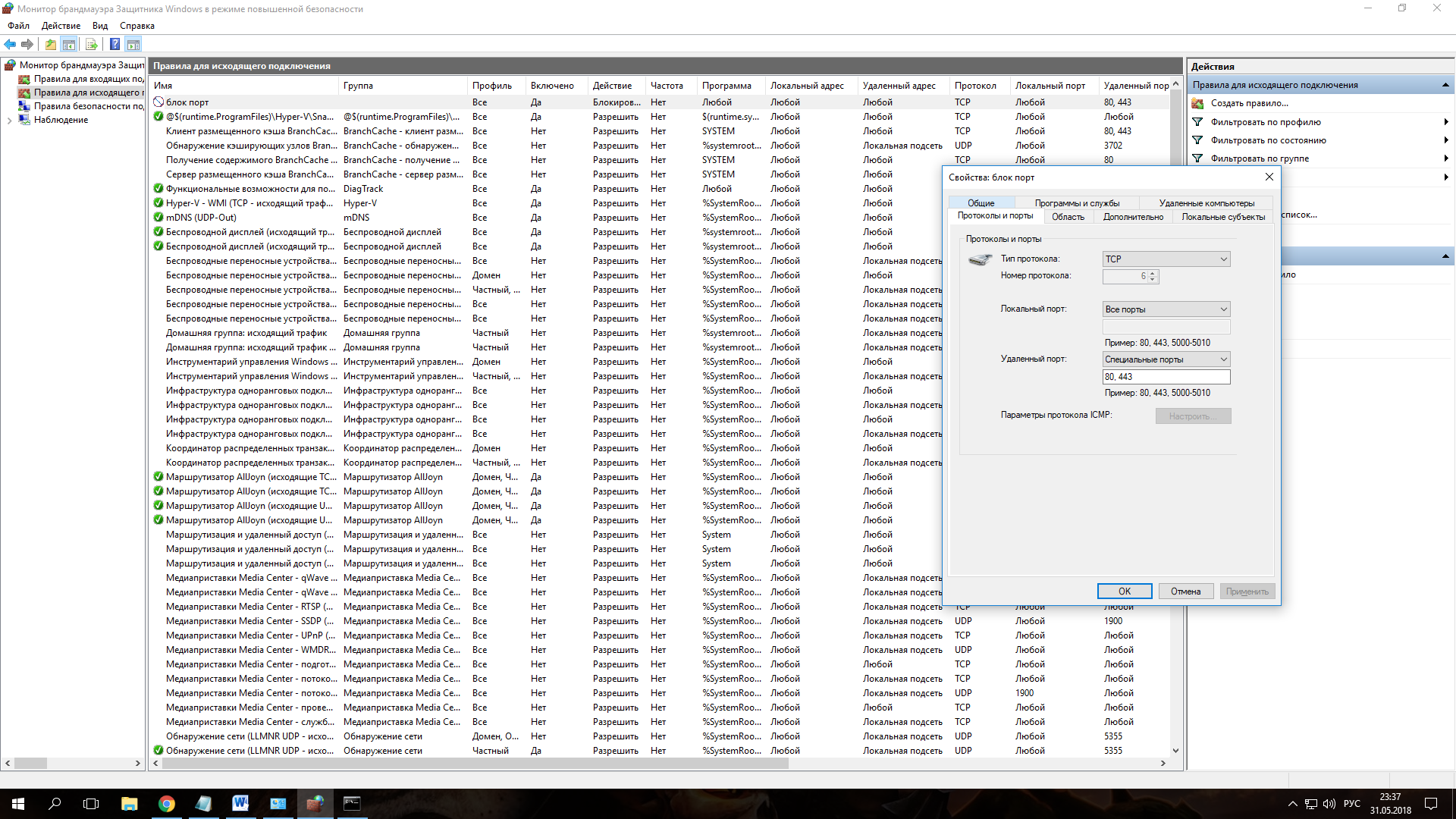
Рис. 10 - «Блокировка сетевого адреса. Проверка» 

Рис. 11 - «Блокировка порта 80, 443»

Для проверки откроем вкладку в chrome.

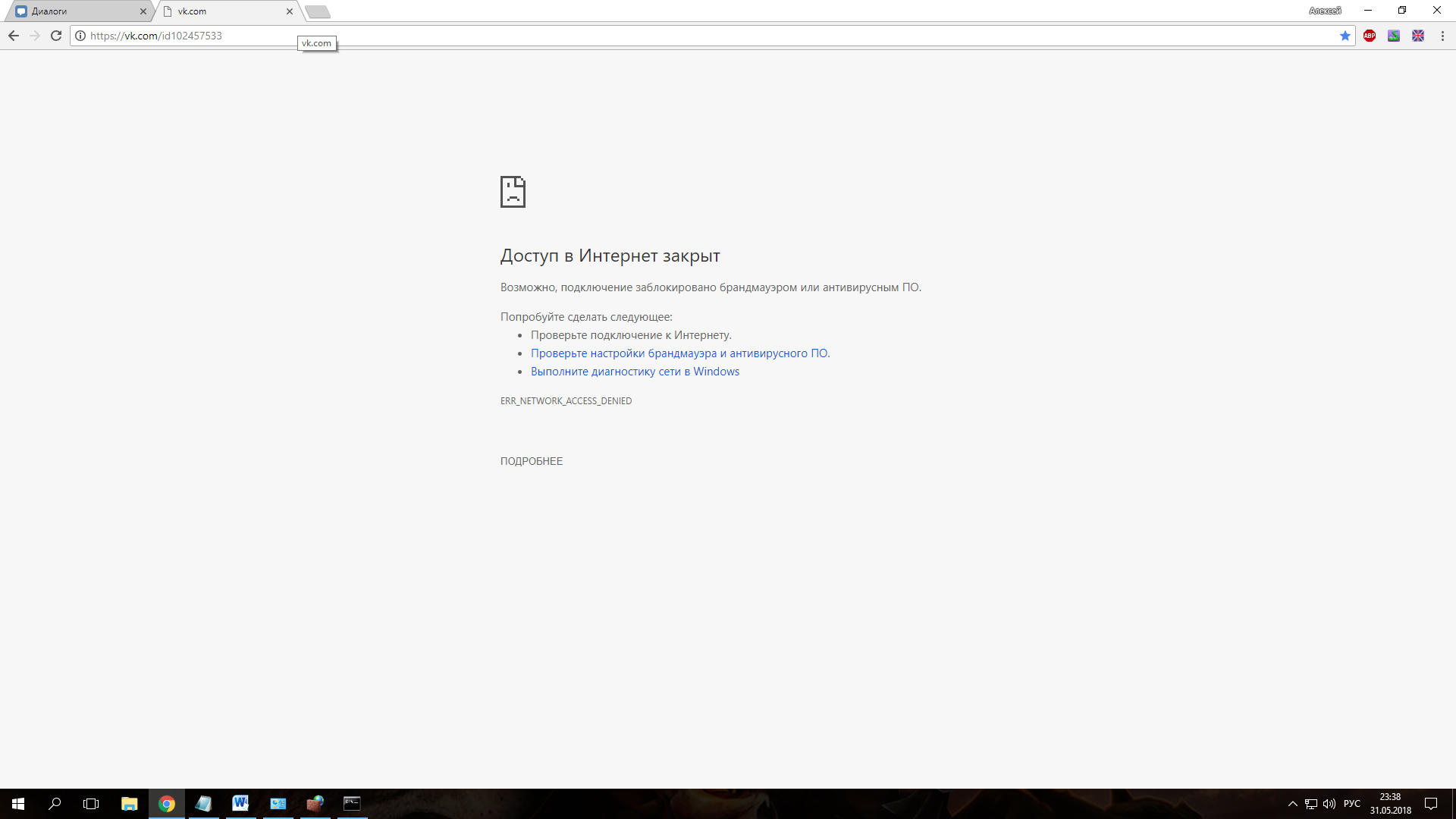


Рис. 16 - «Блокировка порта 80, 443.Проверка»

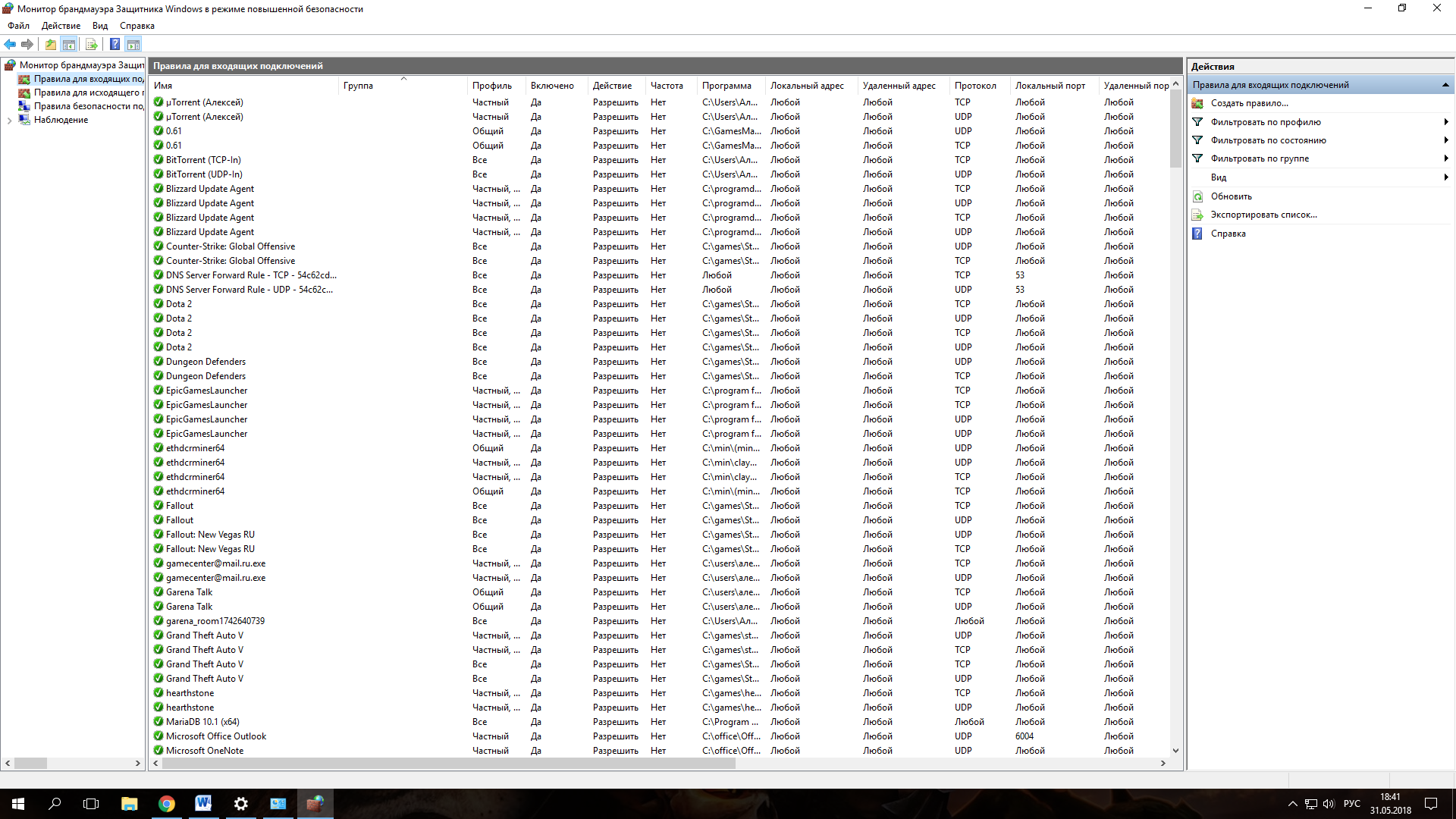
Входящие подключения. 

Рис. 12 - «Правила для входящего подключения»

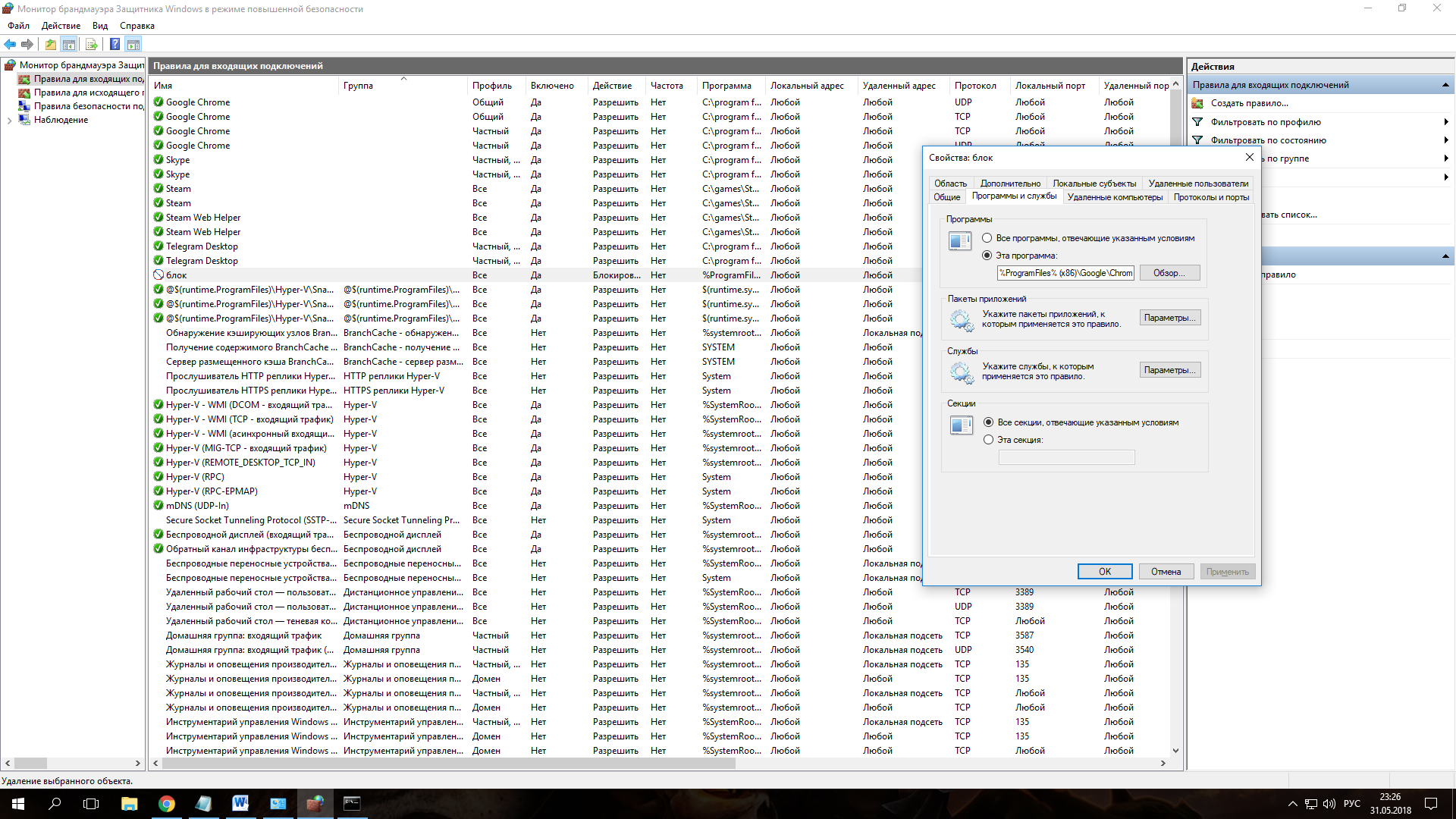


Рис. 13 - «Блокировка приложения Google Chrome»

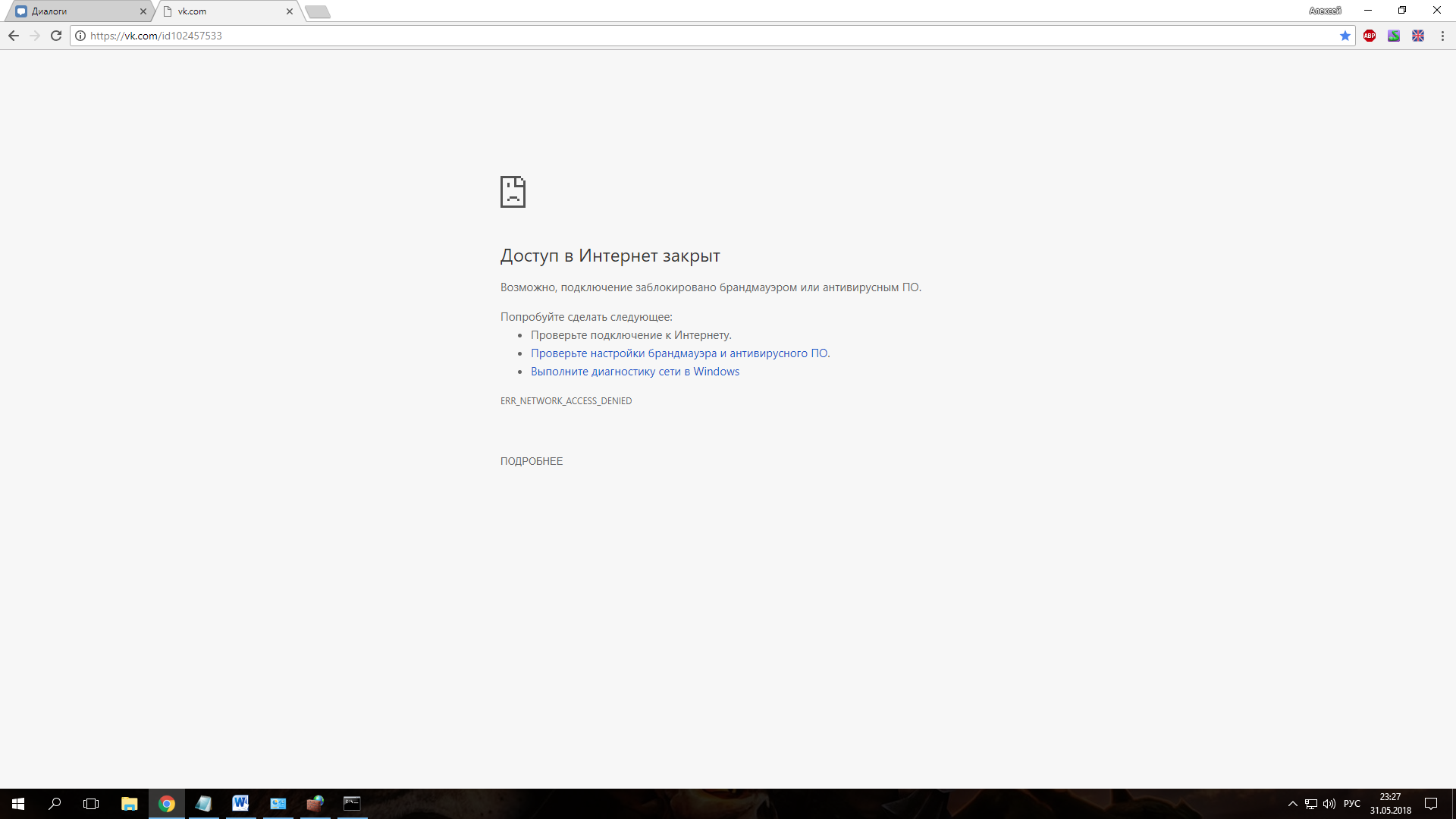


Рис. 14 - «Блокировка приложения Google Chrome.Проверка»

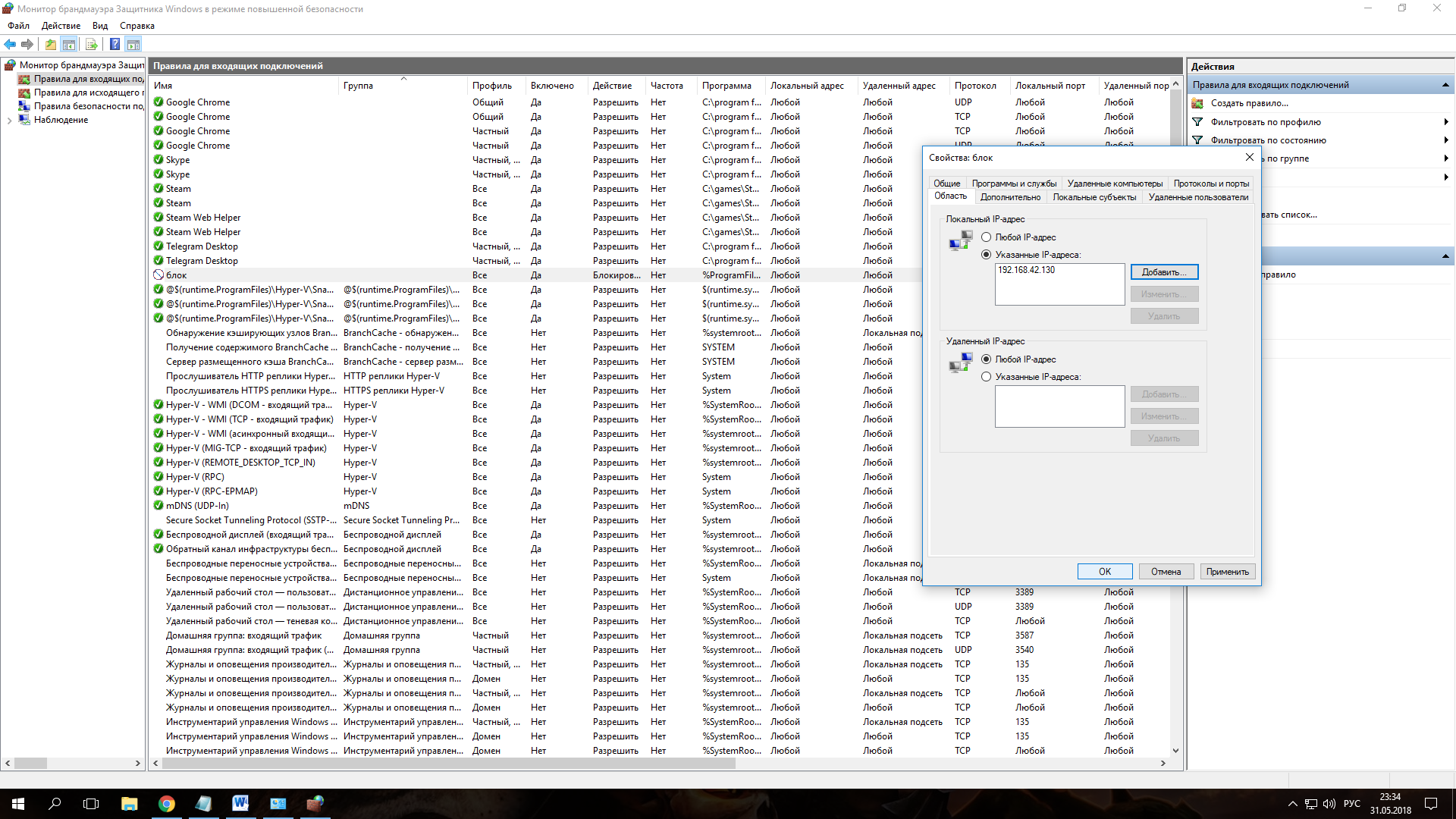


Рис. 17 - «Блокировка сетевого адреса» 

Рис. 18 - «Блокировка сетевого адреса. Проверка»

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«Санкт-Петербургский национальный исследовательский университет  
информационных технологий, механики и оптики»

Лабораторная работа №5

Выполнил студенты группы М3204:  
Наскальнюк Никита Андреевич

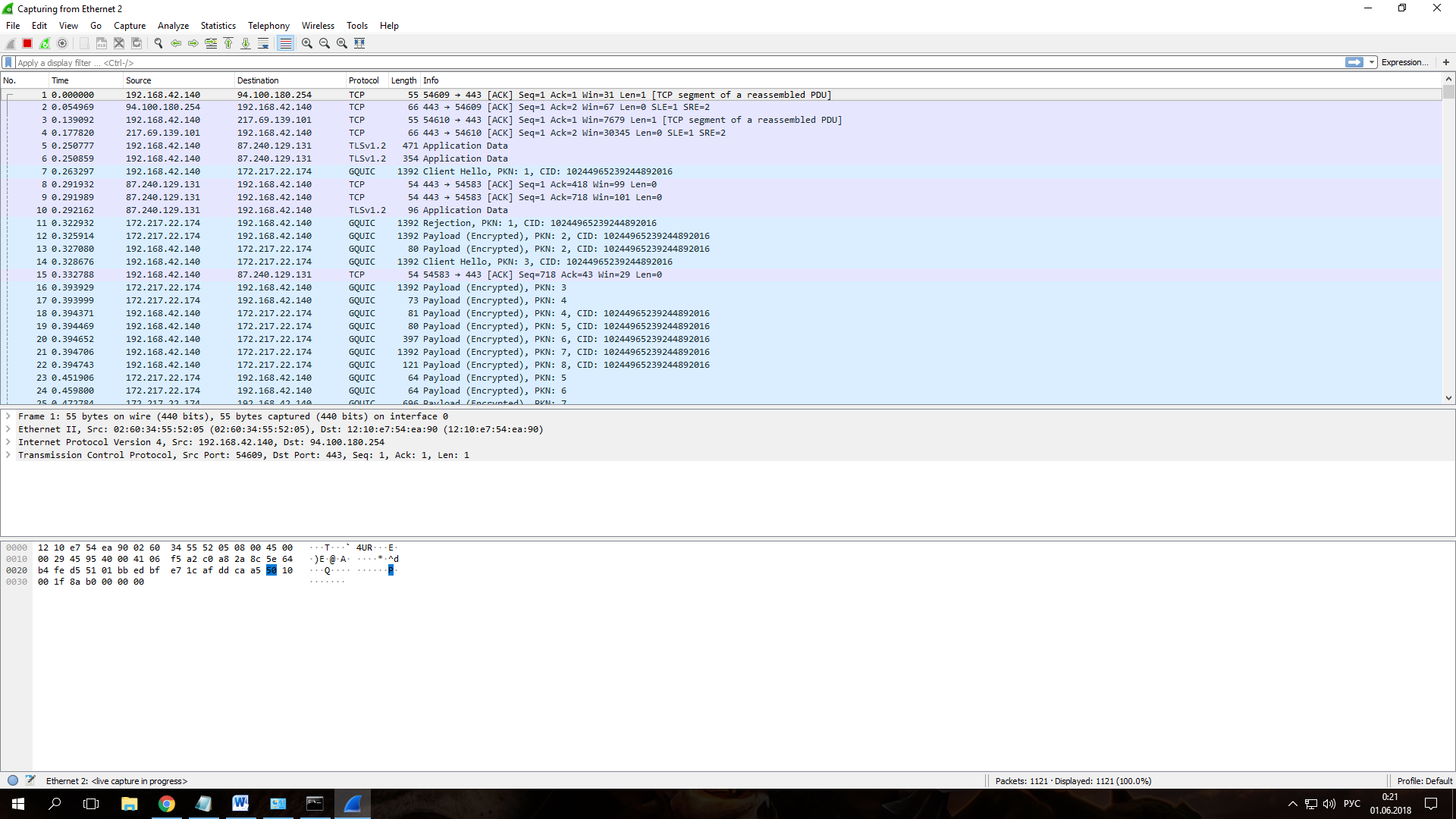
САНКТ-ПЕТЕРБУРГ  
2018

## *Цель работы*

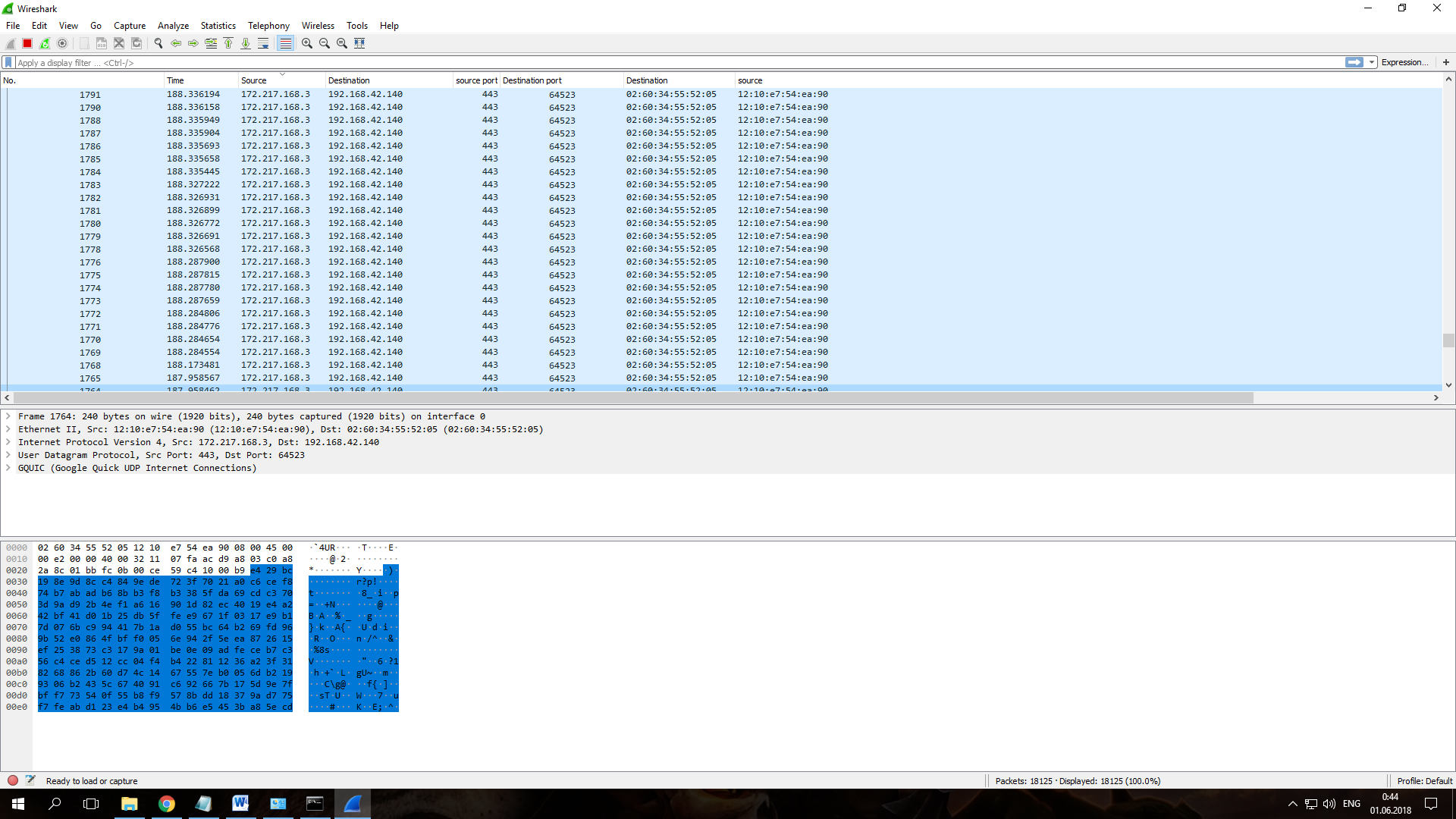
Формирование навыков по использованию основных программных инструментов анализа сетевого трафика.

## *Перечень используемого оборудования и ПО*

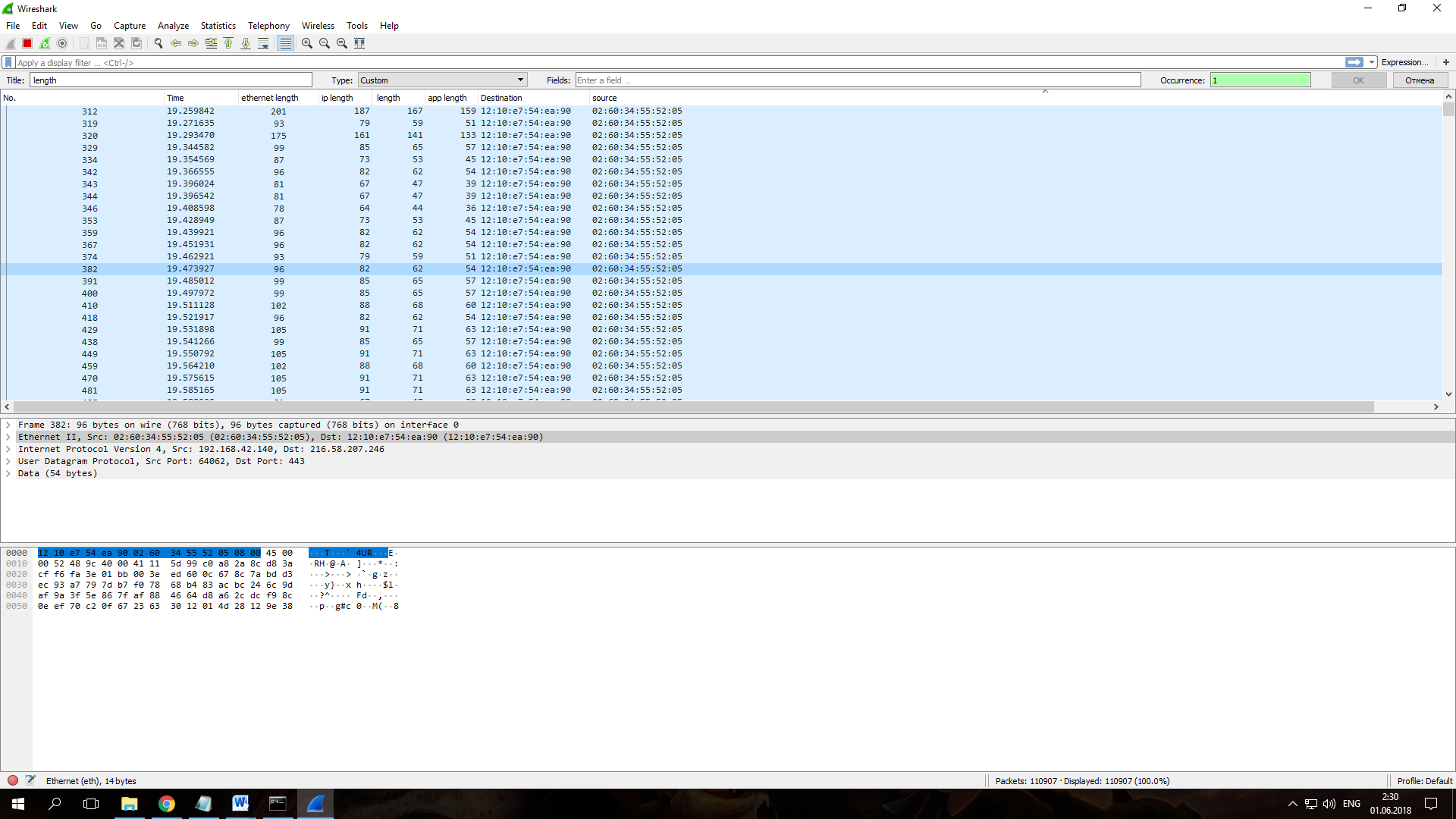
1) Персональный компьютер с ОС Windows, OC Linux или ОС Mac

2) ПО Wireshark 

*Рис. 1. “Список доступных интерфейсов для захвата”*



*Рис.2.”Отображение по адресам”*



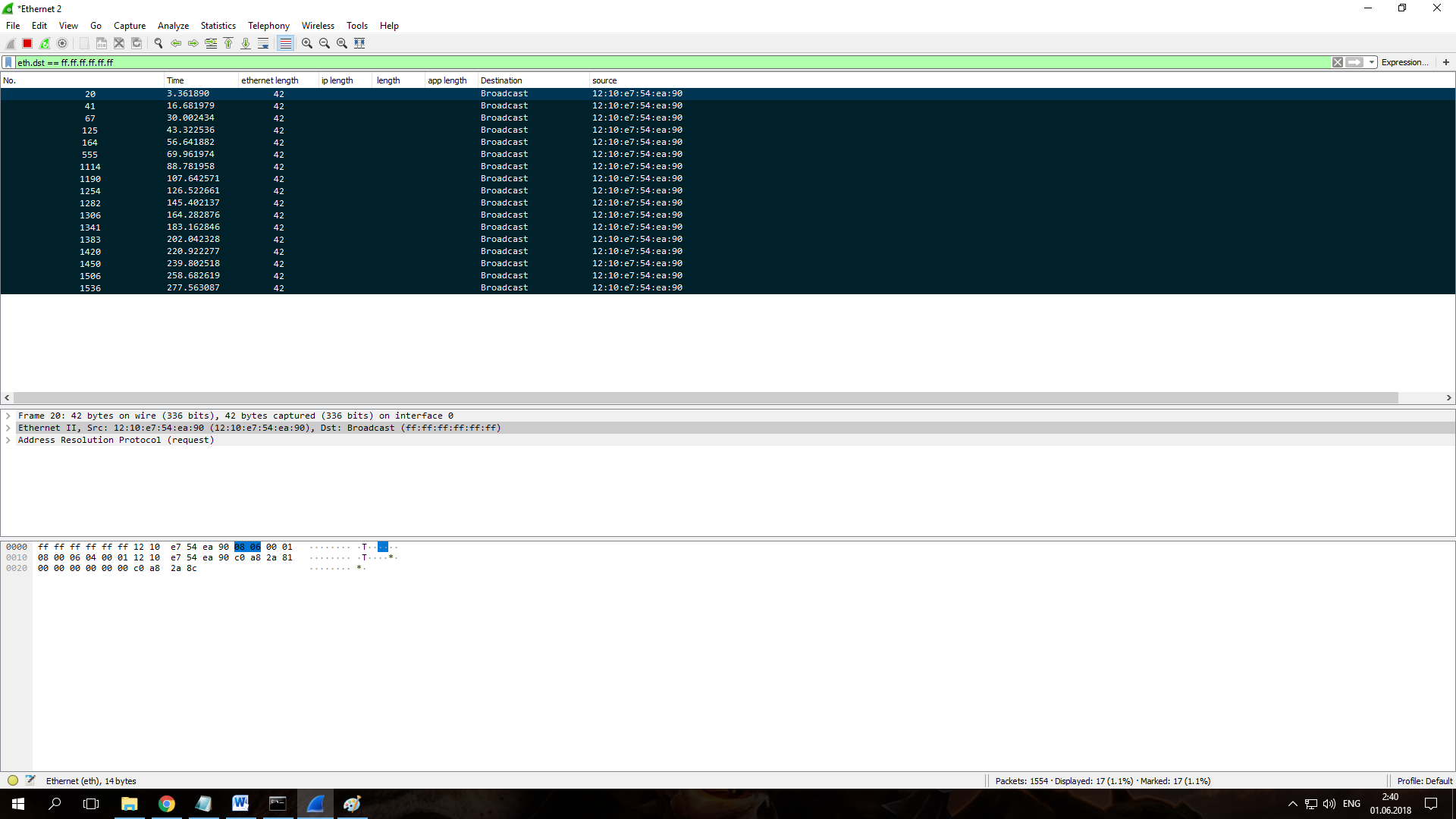
*Рис. 3. “Отображение по длинам”*

Таблица 1 – Длины протоколов

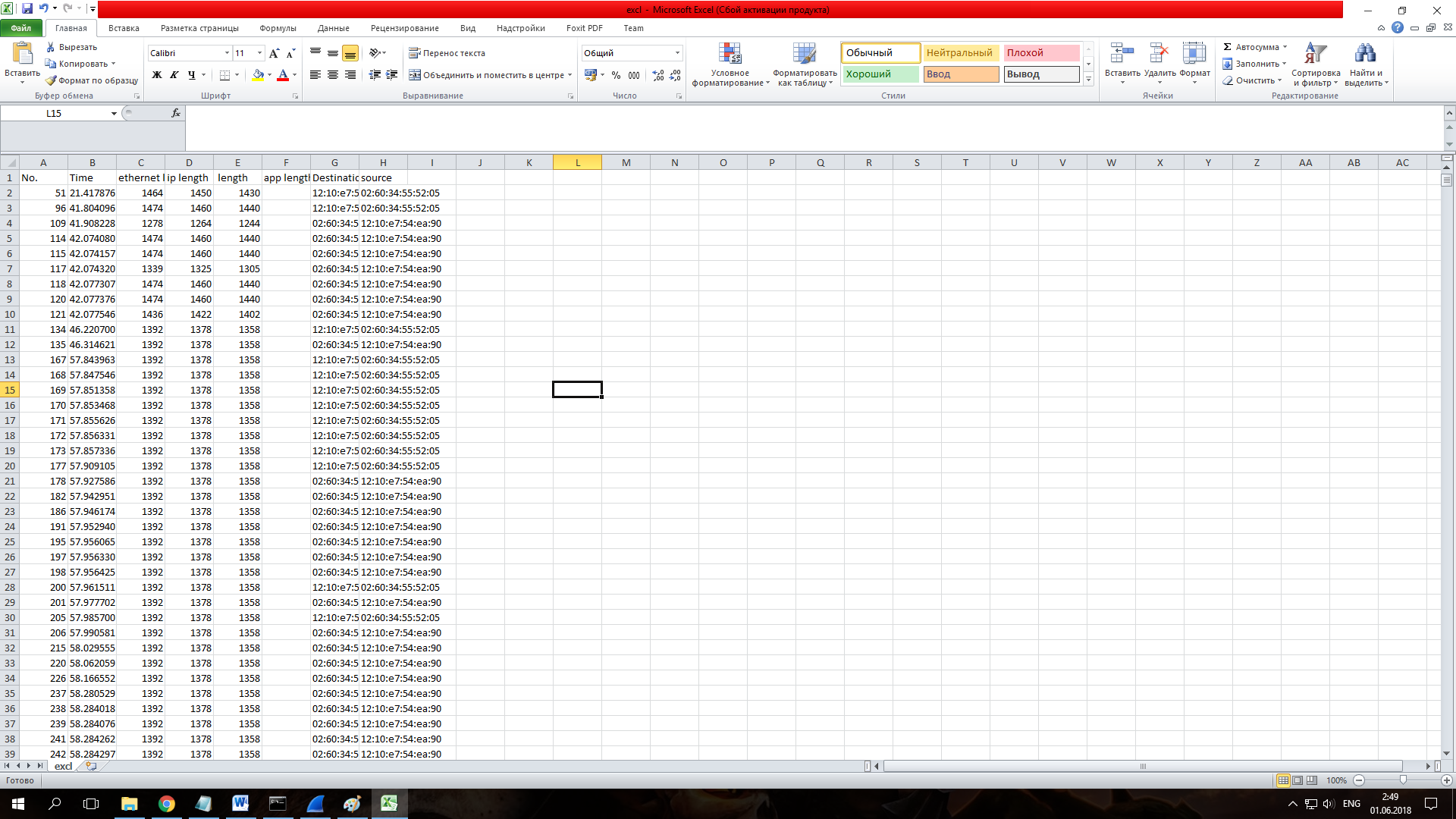
|  |  |  |
| --- | --- | --- |
| **№** | **Параметр** | **Значение** |
| 1 | Длина протокола канального уровня |  |
| 2 | Длина протокола сетевого уровня |  |
| 3 | Длина протокола транспортного уровня |  |

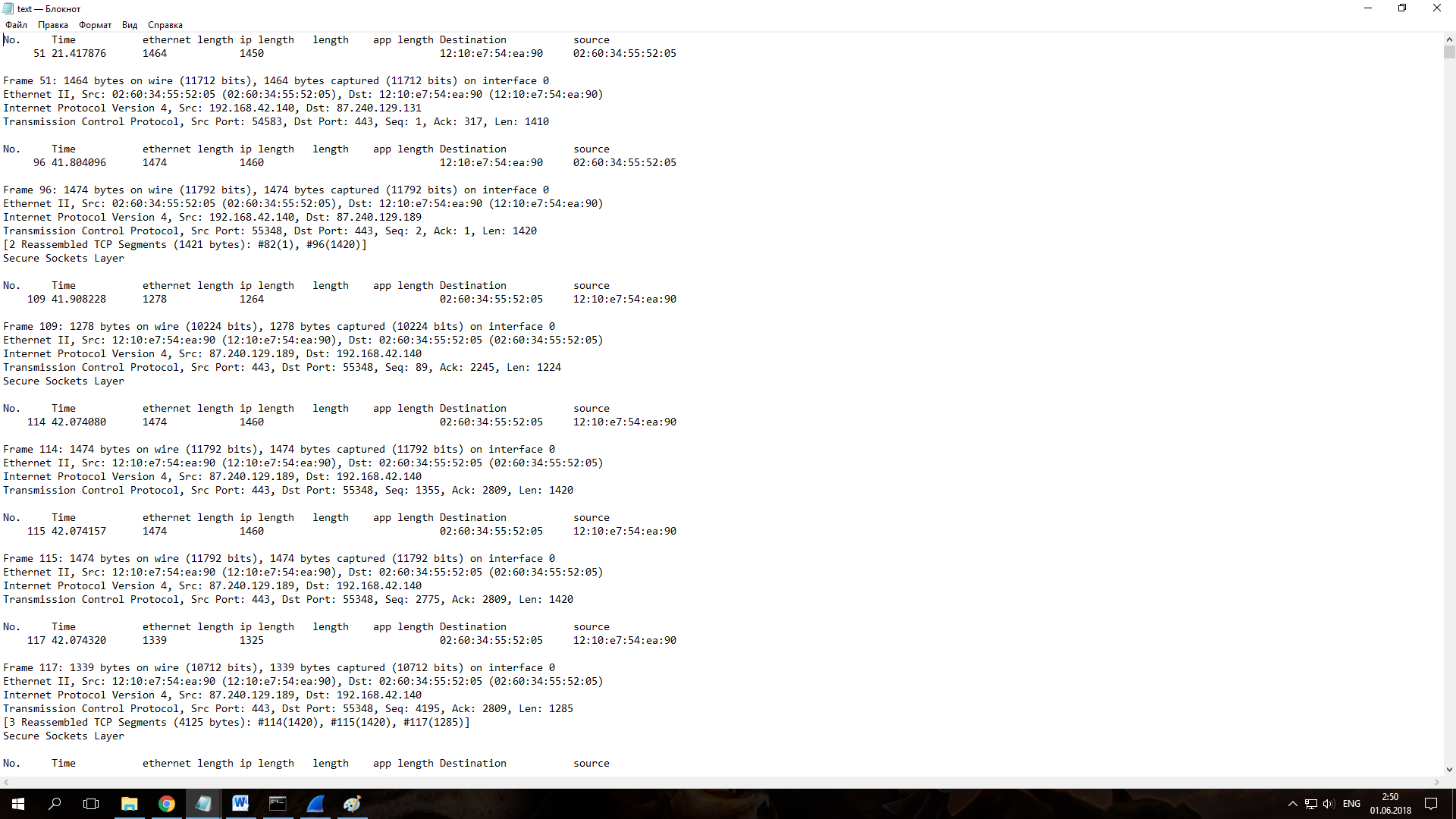
Таблица 2 – Фильтры отображения в wireshark

|  |  |  |
| --- | --- | --- |
| **№** | **Название фильтра** | **Фильтр в Wireshark** |
| 1 | Кадров Ethernet, отправляемых с сетевого интерфейса | eth.src == 70:1c:e7:f4:9d:bd |
| 2 | Кадров Ethernet, только принимаемых на сетевой интерфейс | eth.dst == 70:1c:e7:f4:9d:bd |
| 3 | Кадров Ethernet и отправляемых, и принимаемых сетевым интерфейсом | eth.src == 70:1c:e7:f4:9d:bd or eth.dst == 70:1c:e7:f4:9d:bd |
| 4 | Пакетов IP, только отправляемых с сетевого интерфейса | ip.src == 192.168.1.38 |
| 5 | Пакетов IP, только принимаемых на сетевой интерфейc | ip.dst == 192.168.1.38 |
| 6 | Пакетов IP и отправляемых, и принимаемых сетевым интерфейсом | ip.src == 192.168.1.38 or ip.dst == 192.168.1.38 |
| 7 | Сегментов TCP, только отправляемых с сетевого интерфейса – на порты 80, 443 (http, https) | (tcp.dstport == 80 || tcp.dstport == 443) && ip.src == 192.168.1.38 |
| 8 | Сегментов TCP, только принимаемых на сетевой интерфейс – с портов 80, 443 (http, https) | (tcp.srcport == 80 || tcp.srcport == 443) && ip.dst == 192.168.1.38 |
| 9 | Сегментов TCP и отправляемых, и принимаемых сетевым интерфейсом | (ip.dst == 192.168.1.38 || ip.dst == 192.168.1.38) && tcp |
| 10 | Датаграмм UDP, только отправляемых с сетевого интерфейса – на порт 53 (dns) | udp.dstport == 53 && ip.src == 192.168.1.38 |
| 11 | Датаграмм UDP, только принимаемых на сетевой интерфейс – с порта 53 (dns) | udp.srcport == 53 && ip.dst == 192.168.1.38 |
| 12 | Датаграмм UDP и отправляемых, и принимаемых сетевым интерфейсом | (ip.dst == 192.168.1.38 || ip.src == 192.168.1.38) && udp |
| 13 | Сообщений протокола arp | arp |
| 14 | Сообщений протокола icmp | icmp |
| 15 | Сообщений протокола dns | dns |
| 16 | Сообщений протокола http | http |



*Рис. 4. “Маркировка широковещательных кадров ethernet”* 

*Рис. 5. “Маркировка пакетов по размеру”* 

*Рис. 6. “Экспорт захвата в excel”* 

*Рис.7. “Экспорт захвата в txt”*

# Выводы

## Особенности процедуры анализа сетевого трафика

Данная процедура заключается в использовании фильтров, чтобы отображались необходимые пакеты, а также в отображении определенных столбцов, чтобы видеть только необходимые данные.

Для анализа используются сетевые и физические адреса, адреса портов (источник и получатель), длины кадров на разных уровнях и протоколы.

Результаты отображаются в виде таблицы, в которой обозначены искомые пакеты и поля информации об этих пакетах.

## Структура и функции программных инструментов анализа сетевого трафика

Программный инструмент анализа сетевого трафика имеет панель инструментов с кнопками и вкладками, предоставляющими доступ к его функциям, поле для ввода фильтра, таблицу в которой отражены выбранные пакеты, а также область внизу, в которой можно посмотреть более подробную информацию о конкретном пакете.

Функции: захват и остановка захвата трафика, использование фильтров, настройка отображения данных, сохранение и экспорт в файлы различных типов.

Start capturing packets - начать захват пакетов, которые в данный момент проходят через наш интерфейс.

Stop capturing packets - прекратить захват пакетов, которые в данный момент проходят через наш интерфейс.

Apply filter - отображает только те пакеты, которые удовлетворяют введенному нами фильтру.

Edit->Preferences->Columns - позволяет настроить столбцы, в которых будут отображаться данные о пакетах.

File->SaveAs - сохранение захваченных пакетов в какой-либо тип данных

File->ExportSpecifiedPackets - экспорт в специфические типы данных (txt, excel, csv и т.д.)