МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ

ФЕДЕРАЦИИ ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Институт информационных технологий

кафедра «Информационные системы»

Лабораторная работа №3

«Исследование способов назначения списков контроля доступа в локальных

компьютерных сетях»

по дисциплине «Инфокоммуникационные системы и сети»

**Выполнил**: ст. гр. ИС/б-20-1-о\_\_\_

Галенин А. К. \_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Проверил:** Чернега В.С. \_\_\_\_\_

**Севастополь**

2023 г.

1. ЦЕЛЬ РАБОТЫ

Исследование методов контроля доступа к сетевым ресурсам и способов составления списков ограничения доступа, приобретение практических навыков составления стандартных и расширенных списков доступа, а также конфигурации сетевого оборудования.

2. ПОСТАНОВКА ЗАДАЧИ

1. Изучить теоретический материал, относящийся к составлению и применению списков доступа (выполняется в процессе домашней подготовки).

2. Создать в рабочем окне Packet Tracer схему сети, изображенную на рисунке 1.

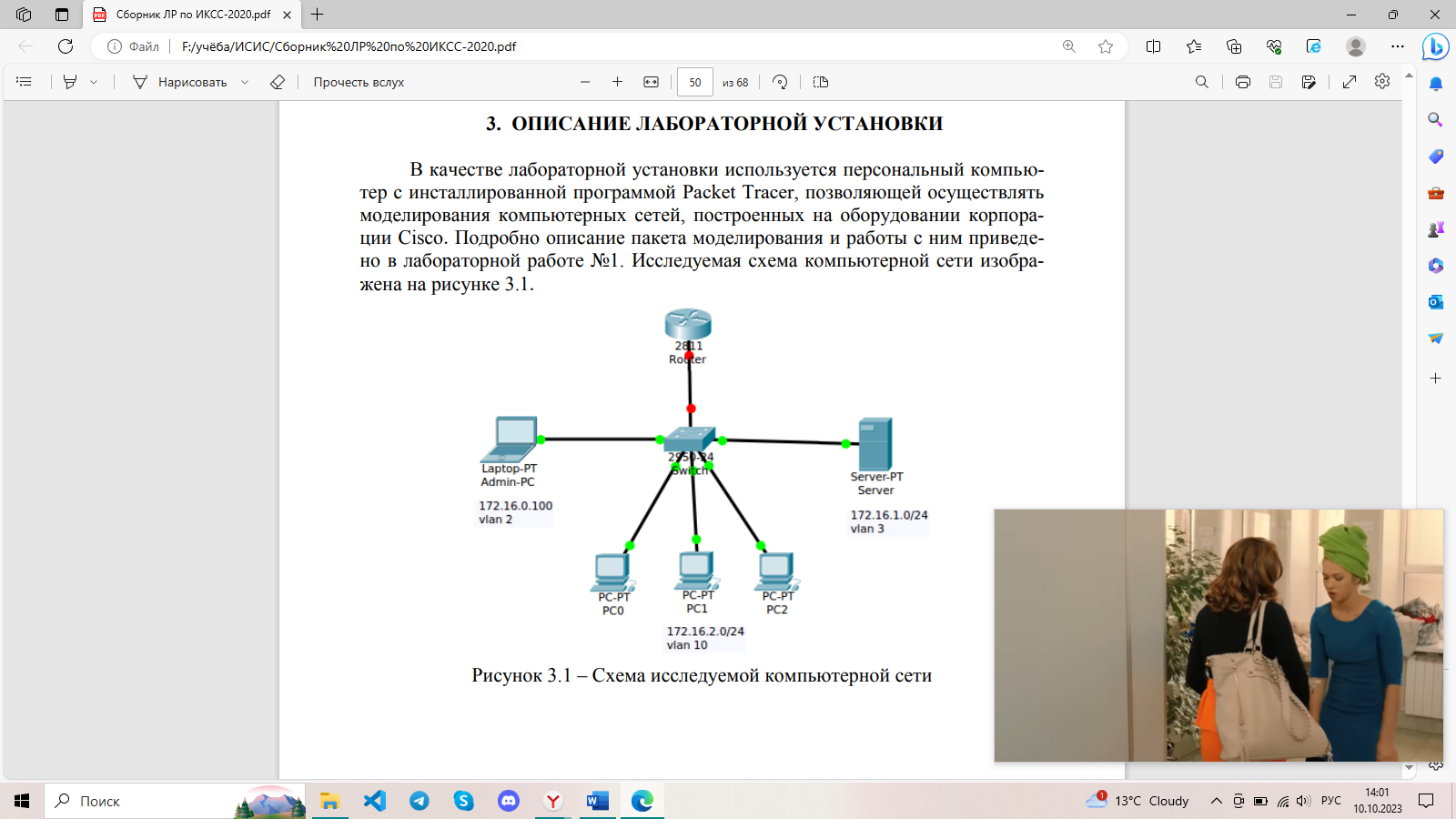


Рисунок 1 – Схема исследуемой сети

3. Сконфигурировать коммутатор таким образом, чтобы компьютер администратора c адресом 172.16.0.100 находился в vlan 2, сервер с адресом 172.16.1.0/24 размещался в vlan 3, а рабочие станции представляли собой подсеть vlan 10 с адресом 172.16.2.0/24. Конфигурацию оборудования выполнить с командной строки.

4. Сконфигурировать оборудования т.о., чтобы доступ к серверу имел только администратор.

5. Проверить путем пингования, что требования, изложенные в п.2.3 и 2.4, выполнены.

6. Переконфигурировать оборудования т.о., чтобы пользователи рабочих станций РС0-РС2 имели доступ к файл-серверу и к HTTP (порт80) и FTP (порт21) серверам. При этом предусмотреть функционирование DNS (порт 53) сервера.

. Сформулировать выводы по результатам исследований.

Примечание: проверить правильность конфигурации телекоммуникационного оборудования и обнаружить ошибки конфигурации можно путем использования приложения А.

3. ХОД РАБОТЫ

Была построена сеть, показанная на рисунке 2. Устройствам были присвоены IP-адреса, также показанные на рисунке 2.

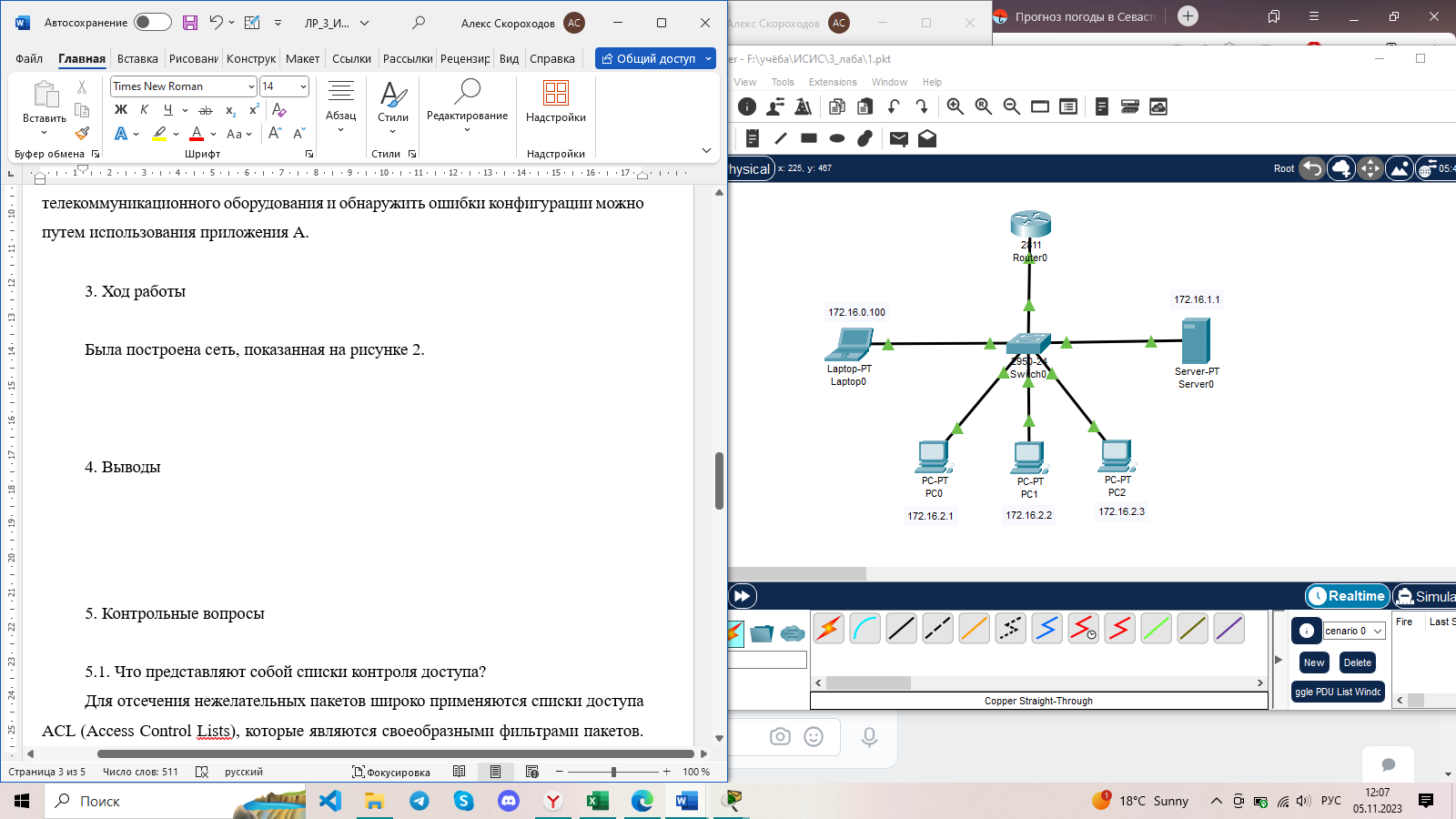


Рисунок 2 – Схема исследуемой сети

Для удобства была заполнена таблица 1, отображающая информацию о сетевых адресах устройств.

Таблица 1 – Сетевые адреса

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Устройство | Интерфейс | IP-адрес | Маска | Шлюз |
| Router 0 | Gig0/0.2 | 172.16.0.1/24 | 255.255.255.0 |  |
| Gig0/0.3 | 172.16.1.1/24 | 255.255.255.0 |
| Gig0/0.10 | 172.16.2.1/24 | 255.255.255.0 |
| Laptop | Fa0/0 | 172.16.0.100 | 255.255.255.0 | 172.16.0.1 |
| PC0 | Fa0/0 | 172.16.2.2 | 255.255.255.0 | 172.16.2.1 |
| PC1 | Fa0/0 | 172.16.2.3 | 255.255.255.0 | 172.16.2.1 |
| PC2 | Fa0/0 | 172.16.2.4 | 255.255.255.0 | 172.16.2.1 |
| Server | Fa0/0 | 172.16.1.2 | 255.255.255.0 | 172.16.1.1 |

Далее было проведено создание VLAN на устройстве Switch0, полный код представлен в листинге 1.

Листинг 1 – Создание списка VLAN на коммутаторе

Switch(config)#vlan 10

Switch(config-vlan)#name vlan10

Switch(config-vlan)#exit

Switch(config)#vlan 2

Switch(config-vlan)#name vlan2

Switch(config-vlan)#exit

Switch(config)#vlan 3

Switch(config-vlan)#name vlan3

Switch(config-vlan)#exit

Далее необходимо было настроить сеть таким образом, чтобы трафик мог идти между различными VLAN. Для этого на роутере были введены команды, представленные в листинге 2. На интерфейсе, подключенному к коммутатору (fa0/0) были созданы три сабинтерфейса для трех VLAN соответвенно.

Листинг 2 – Создание подинтерфейсов интерфейса fa0/0

Router(config)#interface fa0/0

Router(config-if)#description Switch

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#interface fa0/0.2

Router(config-subif)#

%LINK-5-CHANGED: Interface FastEthernet0/0.2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.2, changed state to up

Router(config-subif)#description Admin

Router(config-subif)#encapsulation dot1q 2

Router(config-subif)#ip address 172.16.0.1 255.255.255.0

Router(config-subif)#exit

Router(config)#interface fa0/0.3

Router(config-subif)#

%LINK-5-CHANGED: Interface FastEthernet0/0.3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.3, changed state to up

Router(config-subif)#description Server

Router(config-subif)#encapsulation dot1q 3

Router(config-subif)#ip address 172.16.1.1 255.255.255.0

Router(config-subif)#exit

Router(config)#interface fa0/0.10

Router(config-subif)#

%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.10, changed state to up

Router(config-subif)#description Users

Router(config-subif)#encapsulation dot1q 10

Router(config-subif)#ip address 172.16.2.1 255.255.255.0

Router(config-subif)#exit

Router(config)#exit

Затем была проверена достижимость трафика между VLAN. Для этого было осуществлено пингование с устройства PC0 на устройство Server0. На рисунке 3 показан результат пингования. Как видно, узлы достижимы, хоть и находятся в разных VLAN.

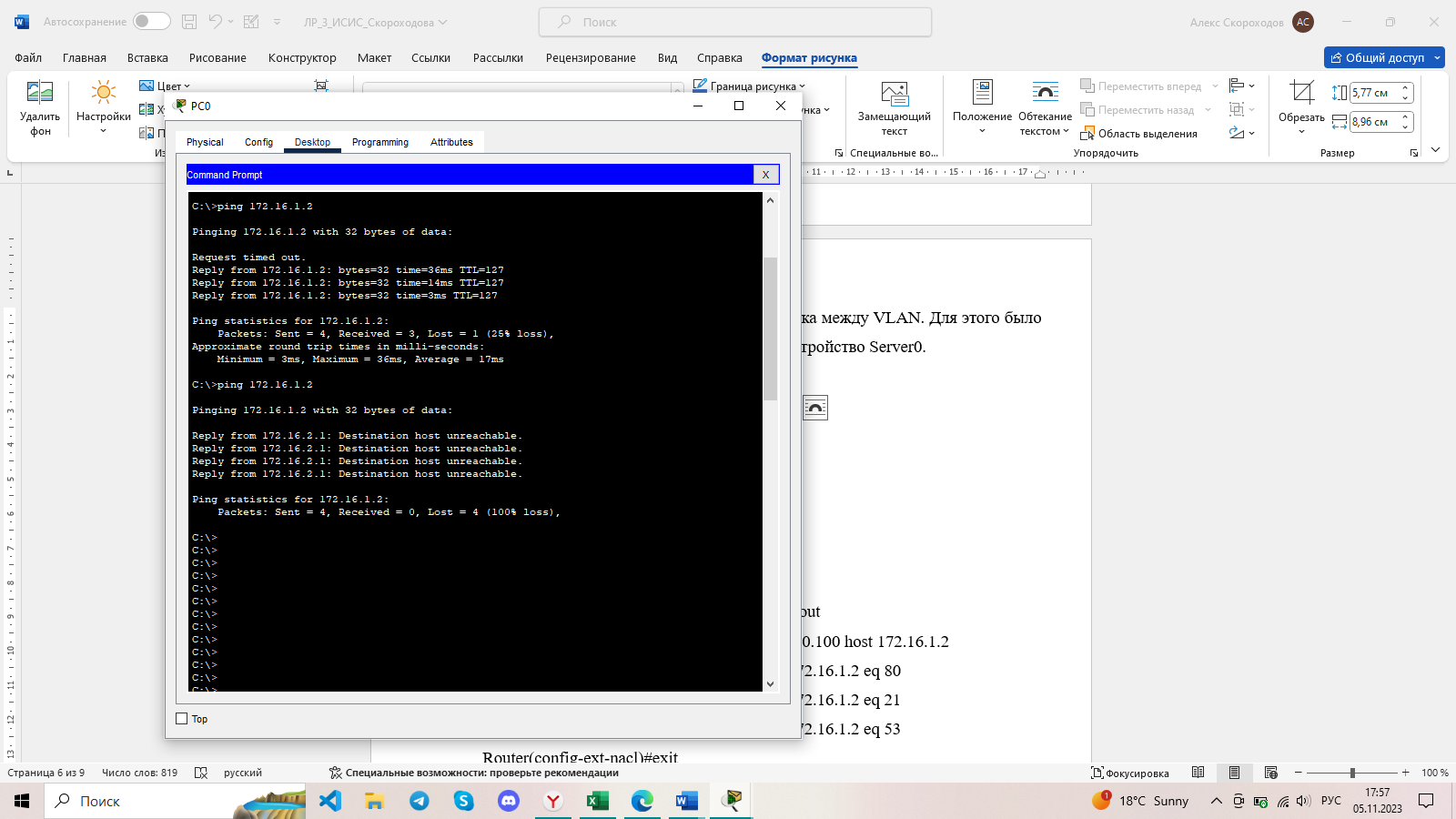


Рисунок 3 – Пингование с PC0 на Server0

Далее требовалось сконфигурировать сеть таким образом, чтобы доступ к серверу имел только компьютер администратора (Laptop0). Для этого на роутере был создан список доступа с необходимыми параметрами. Также необходимо было, чтобы пользователи рабочих станций РС0-РС2 имели доступ к файл-серверу и к HTTP (порт80) и FTP (порт21) серверам. При этом предусмотреть функционирование DNS (порт 53) сервера. На рисунке 4 представлен список доступа, который решает поставленные задачи.

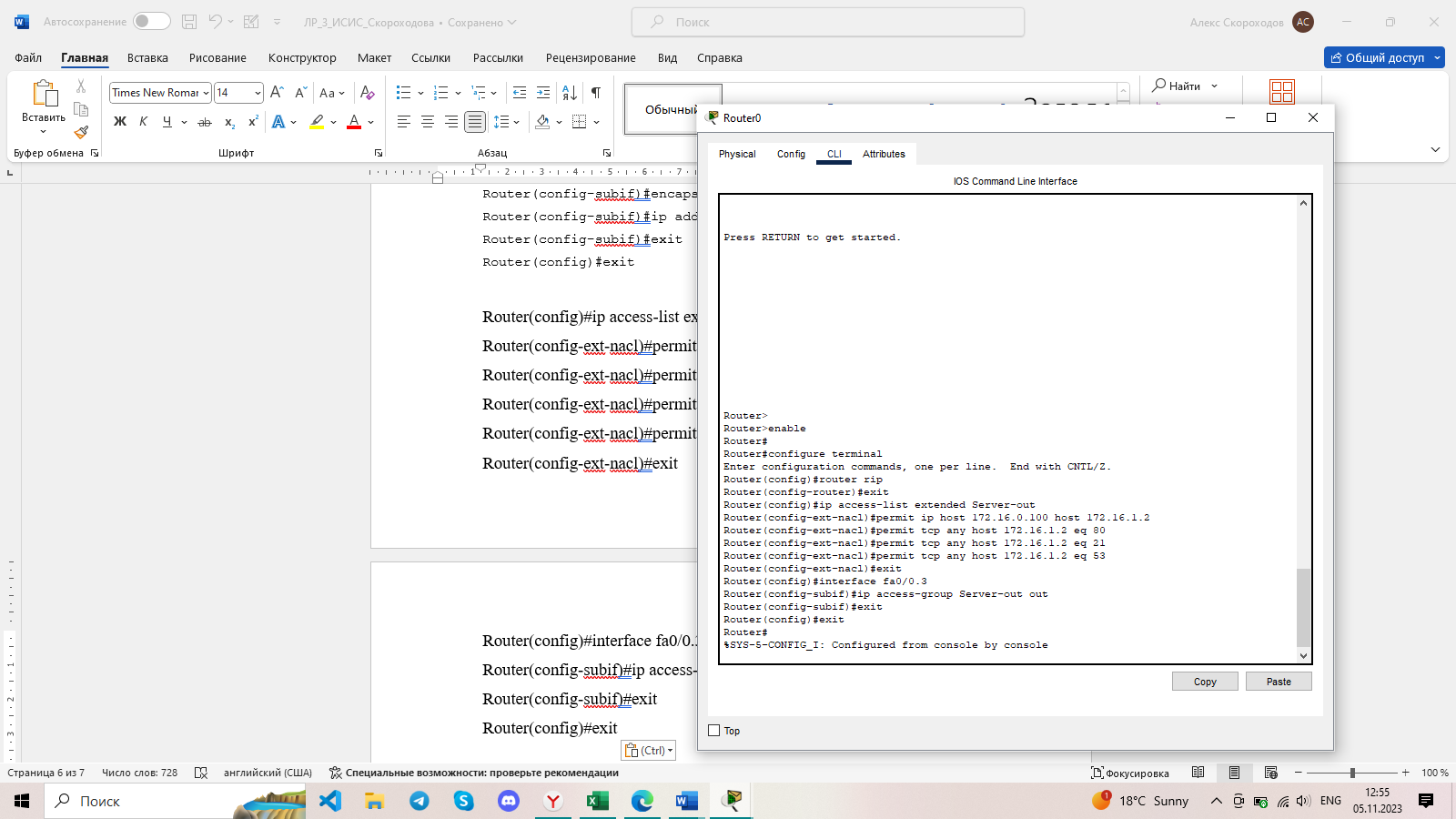


Рисунок 4 – Создание списка доступа

На рисунке 5 представлен результат проверки достижимости трафика между Server0 и другими устройствами. Как видно, трафик с компьютера администратора достигает сервер, а другое устройство уже нет.

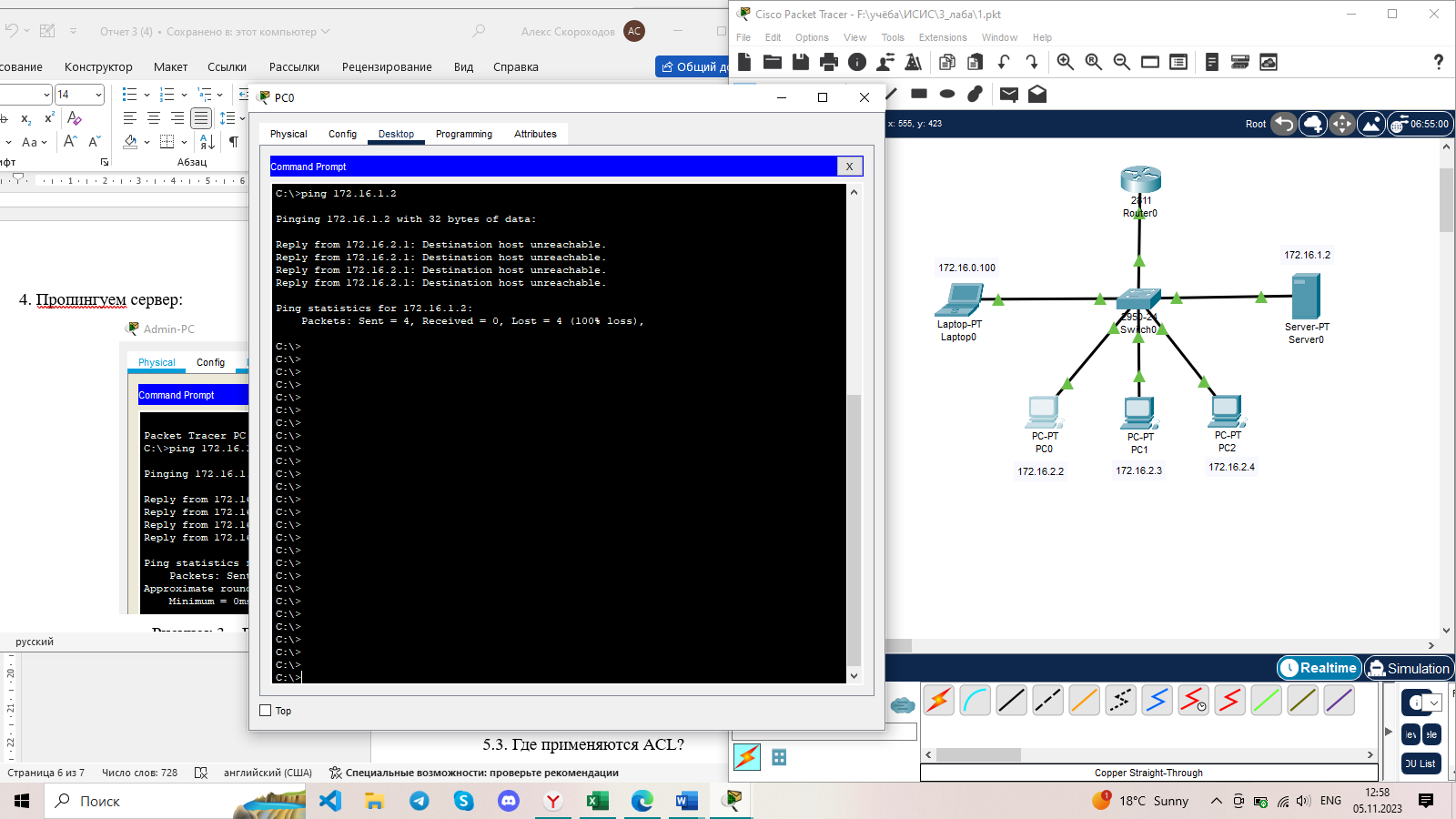
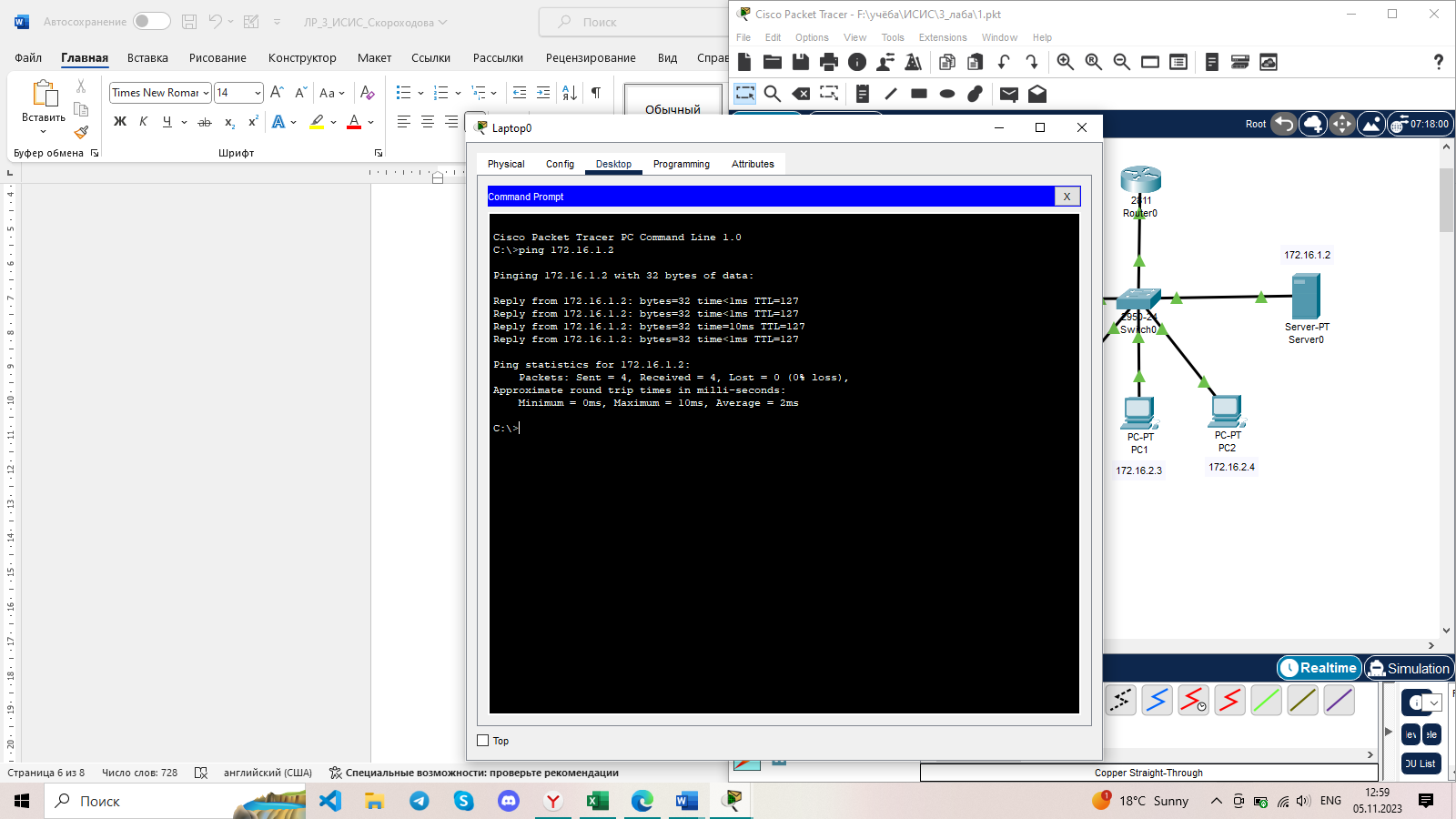


Рисунок 5 – Проверка достижимости сервера путем пингования с разных устройств

Также необходимо проверить, что пользователи рабочих станций РС0-РС2 имеют доступ к файл-серверу и к HTTP (порт80) и FTP (порт21) серверам.

Для этого на устройстве Server0 во вкладке «Сервисы» был создан файл index.html, код которого показан на рисунке 6.

Далее с устройства PC0 был проверен доступ к этому файлу. Результат на рисунке 7. Как видно, доступ есть.

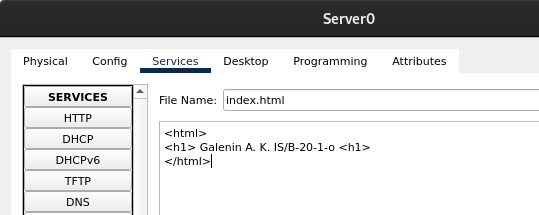


Рисунок 6 – Содержимое файла на сервере

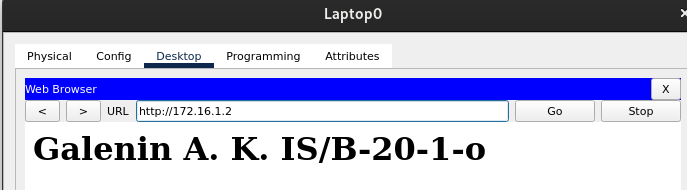


Рисунок 7 – Проверка доступа к файлу

Для проверки FTP на устройстве Server0 во вкладке FTP был создан пользователь, логин и пароль которого представлены на рисунке 8.

Затем на устройстве РС0 было осуществлено подключение к FTP-серверу (рисунок 9).

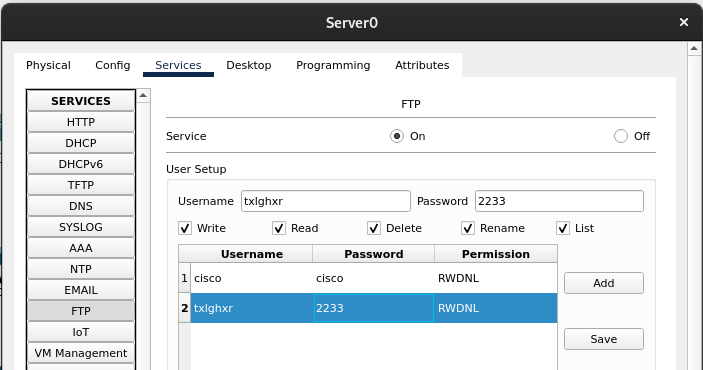


Рисунок 8 – Создание пользователя

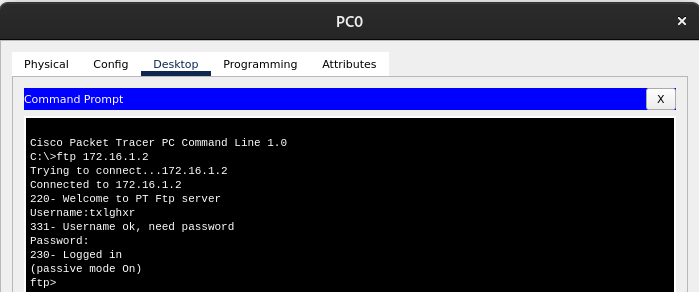


Рисунок 9 – Проверка подключения к FTP-серверу

ВЫВОДЫ

В ходе выполнения данной лабораторной работы были исследованы методы контроля доступа к сетевым ресурсам и способы составления списков ограничения доступа, приобретены практические навыки составления стандартных и расширенных списков доступа, а также конфигурации сетевого оборудования.