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\_\_\_

Скороходова В.А.\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**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

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

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

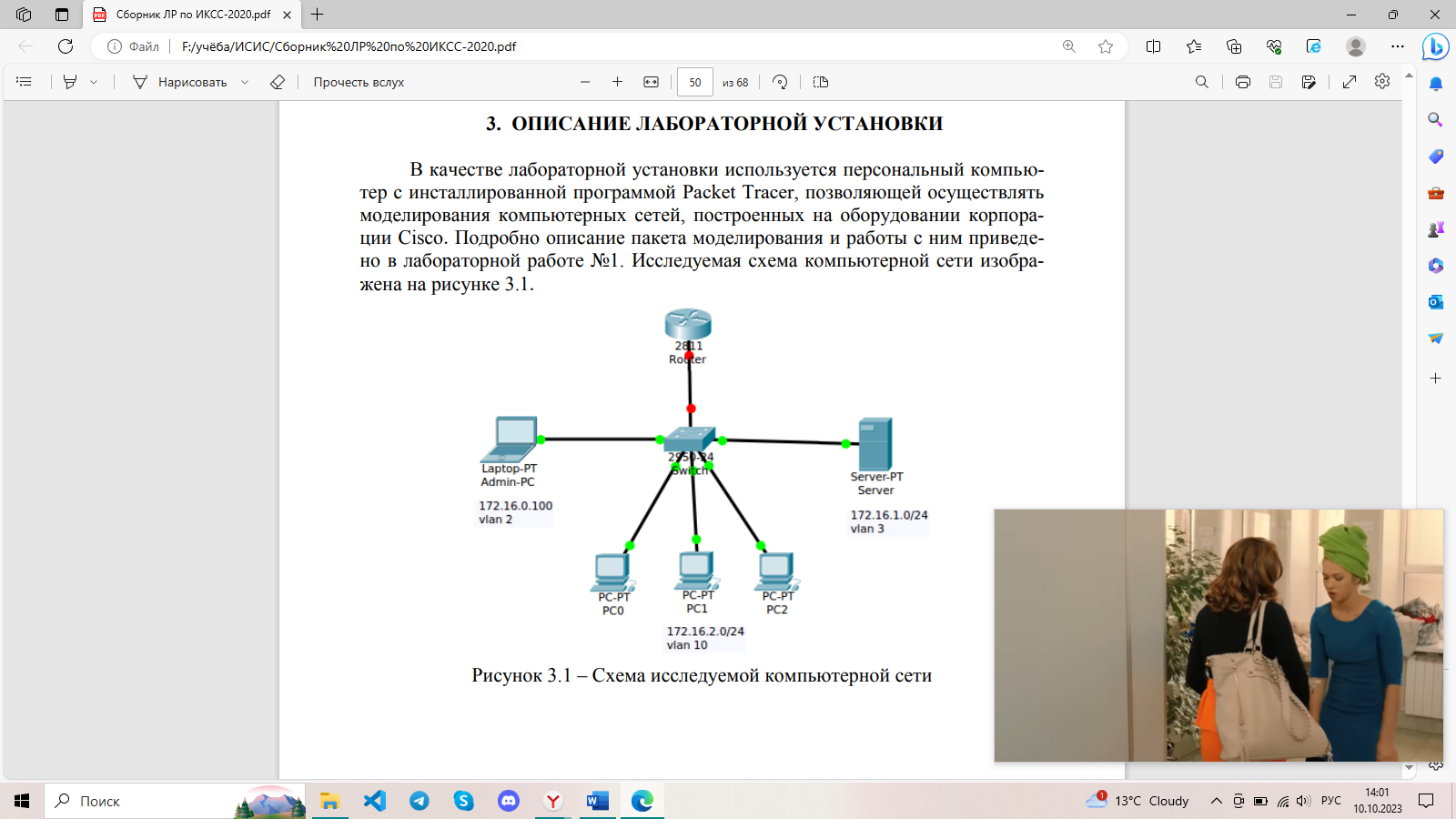


Рисунок 1 – Схема исследуемой сети

2.3. 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.

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

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

2.6. 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.

2.7. 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.

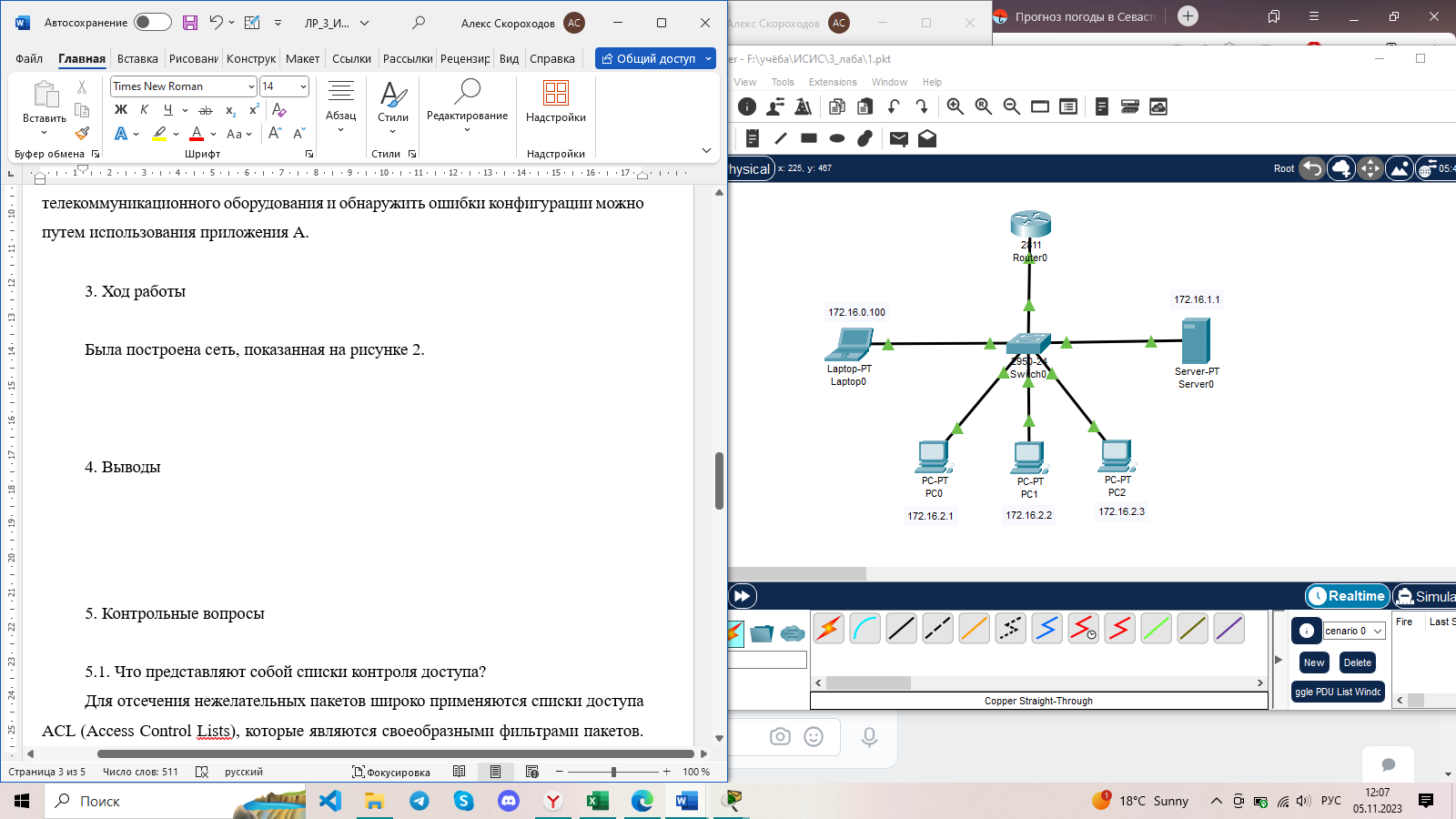


Рисунок 2 – Схема исследуемой сети

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.

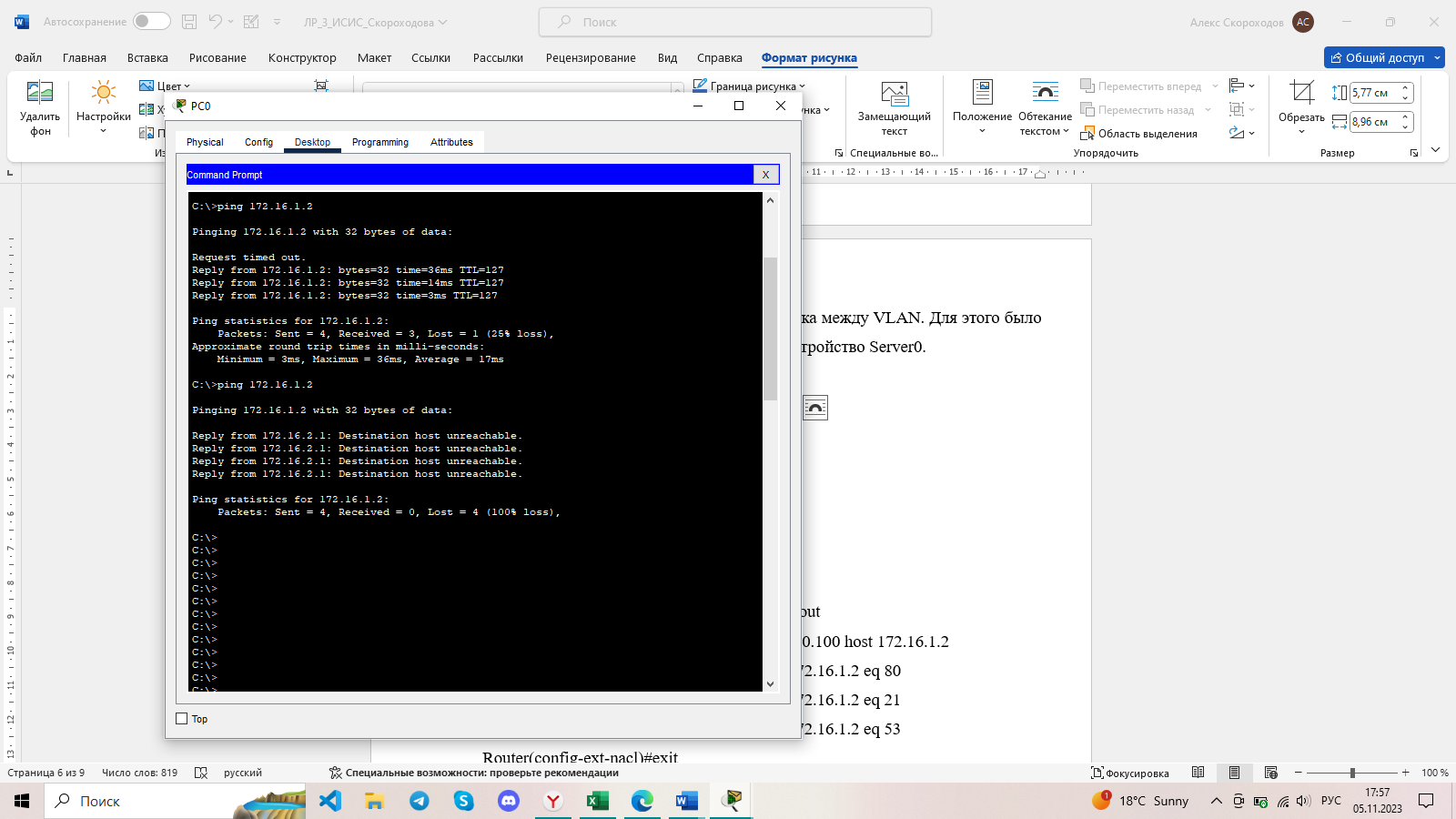


Рисунок 3 – Пингование с PC0 на Server0

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.

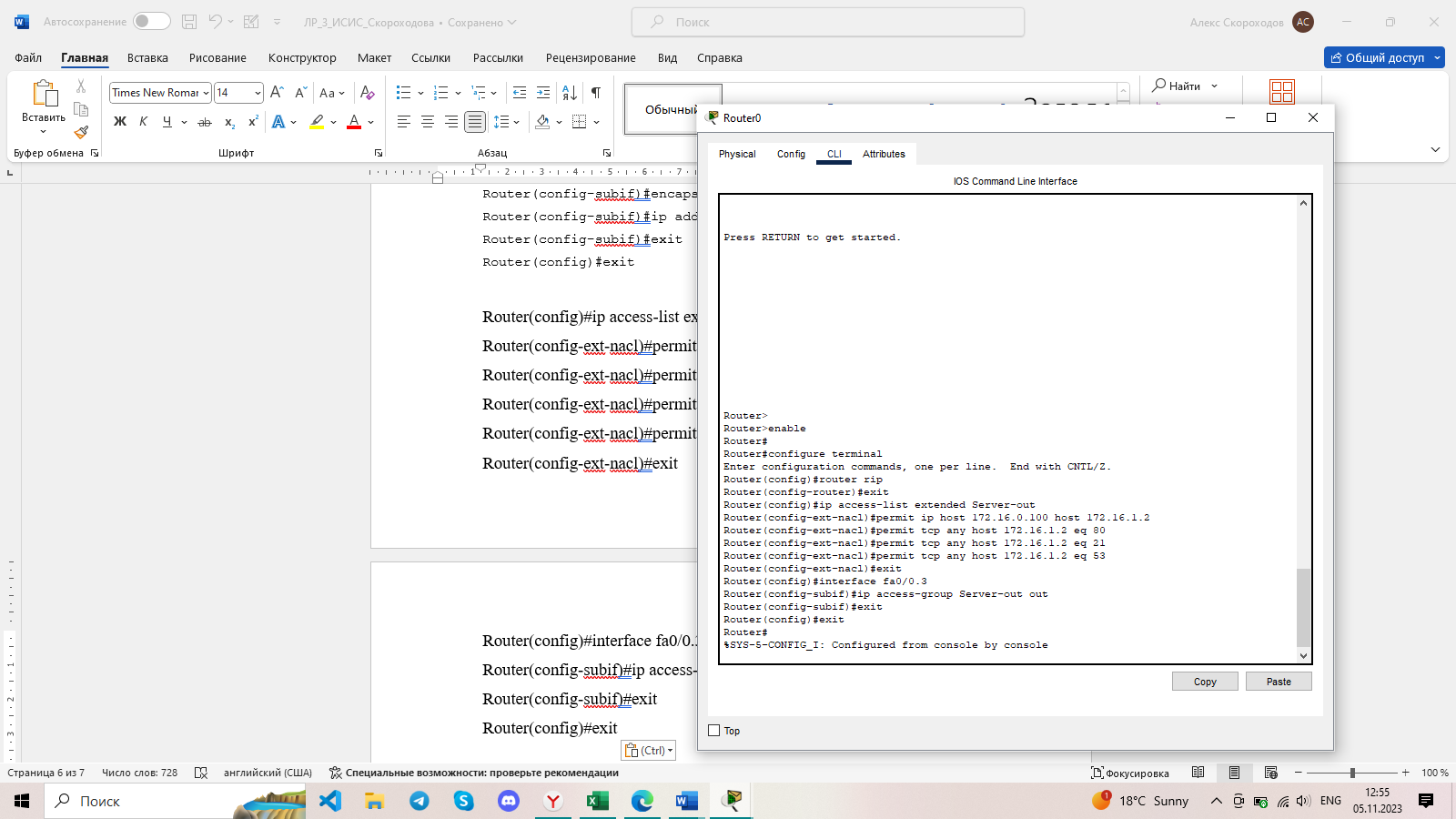


Рисунок 4 – Создание списка доступа

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.

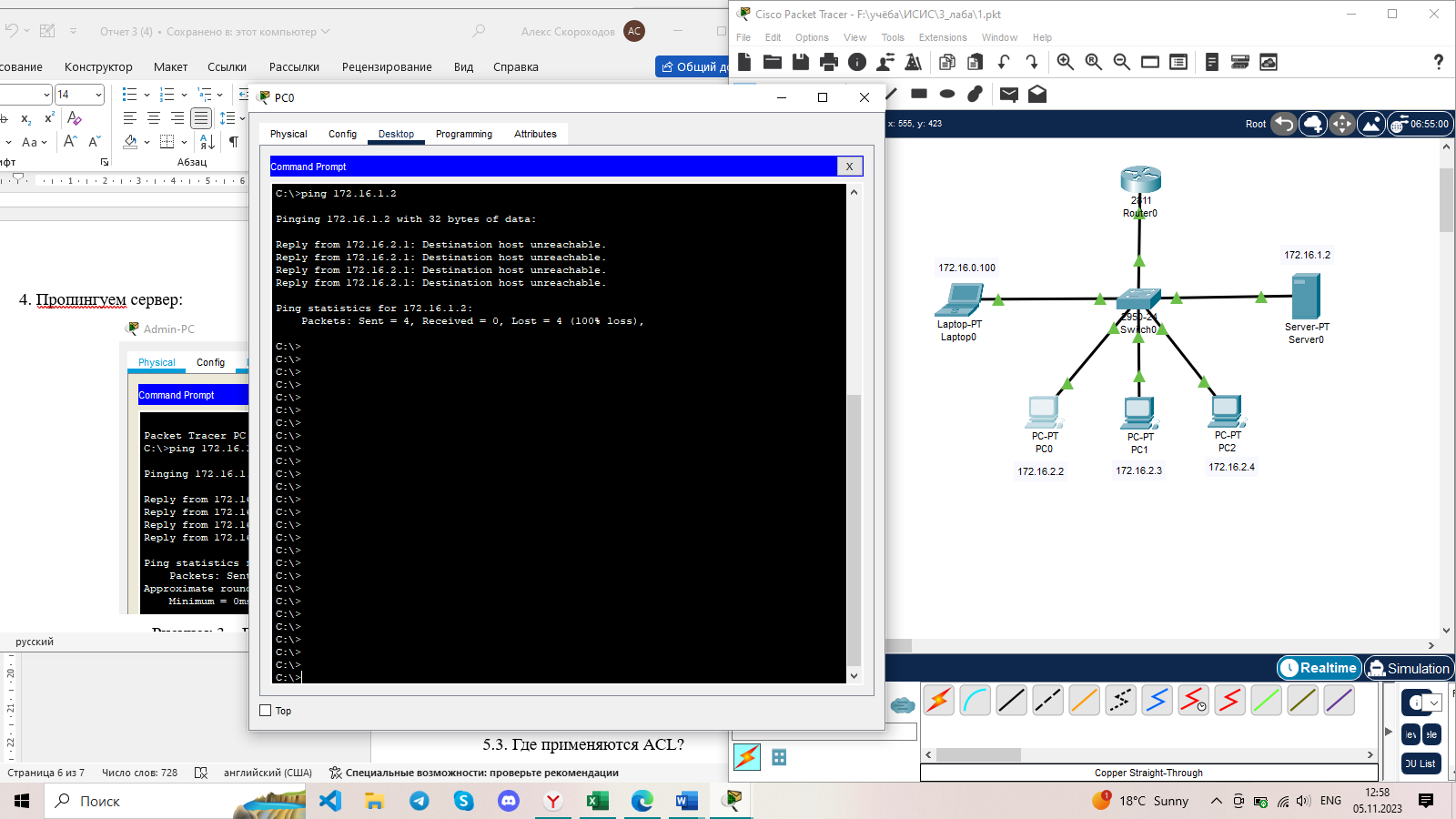
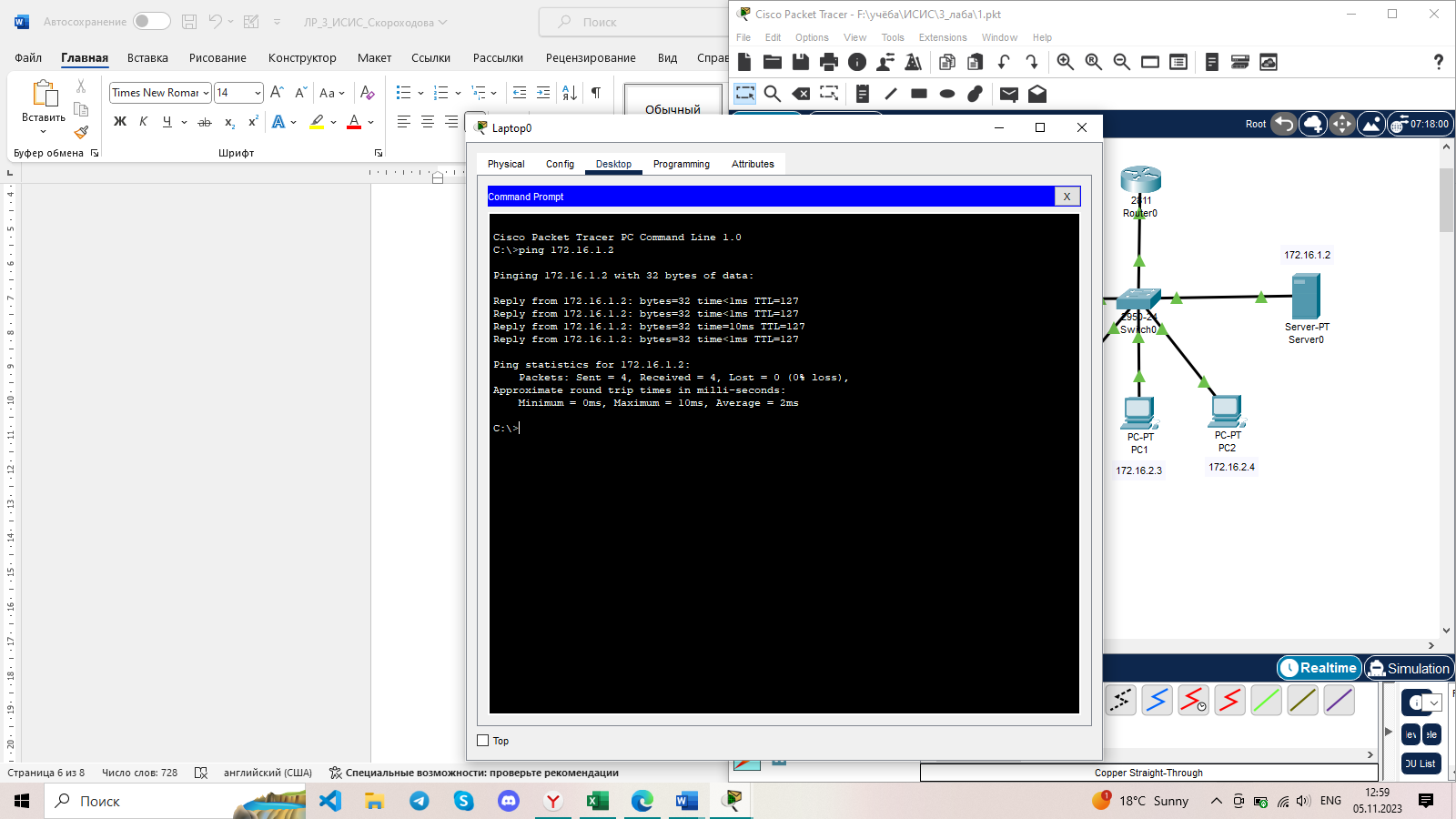


Рисунок 5 – Проверка достижимости сервера путем пингования с разных устройств

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.

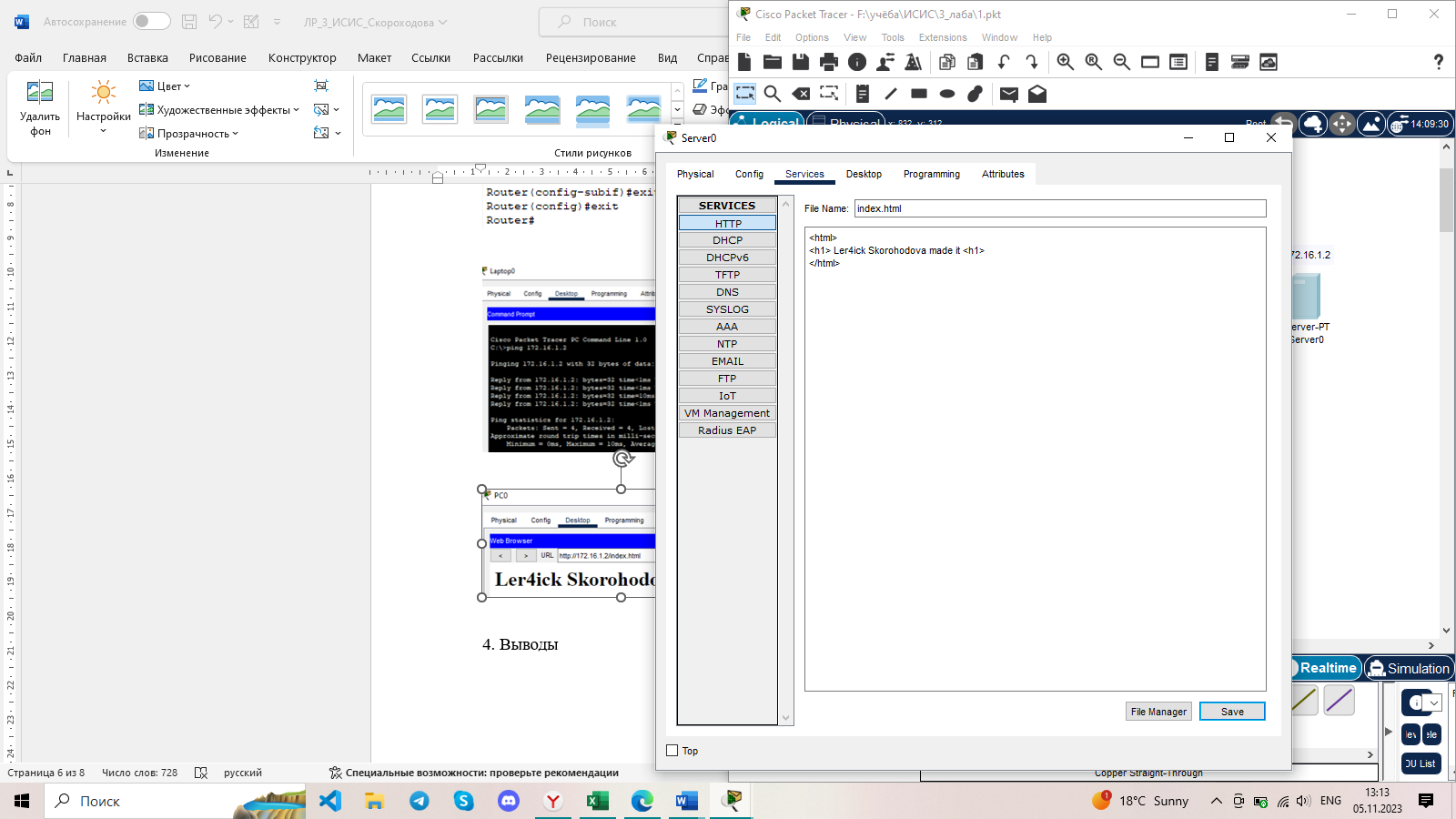


Рисунок 6 – Содержимое файла на сервере

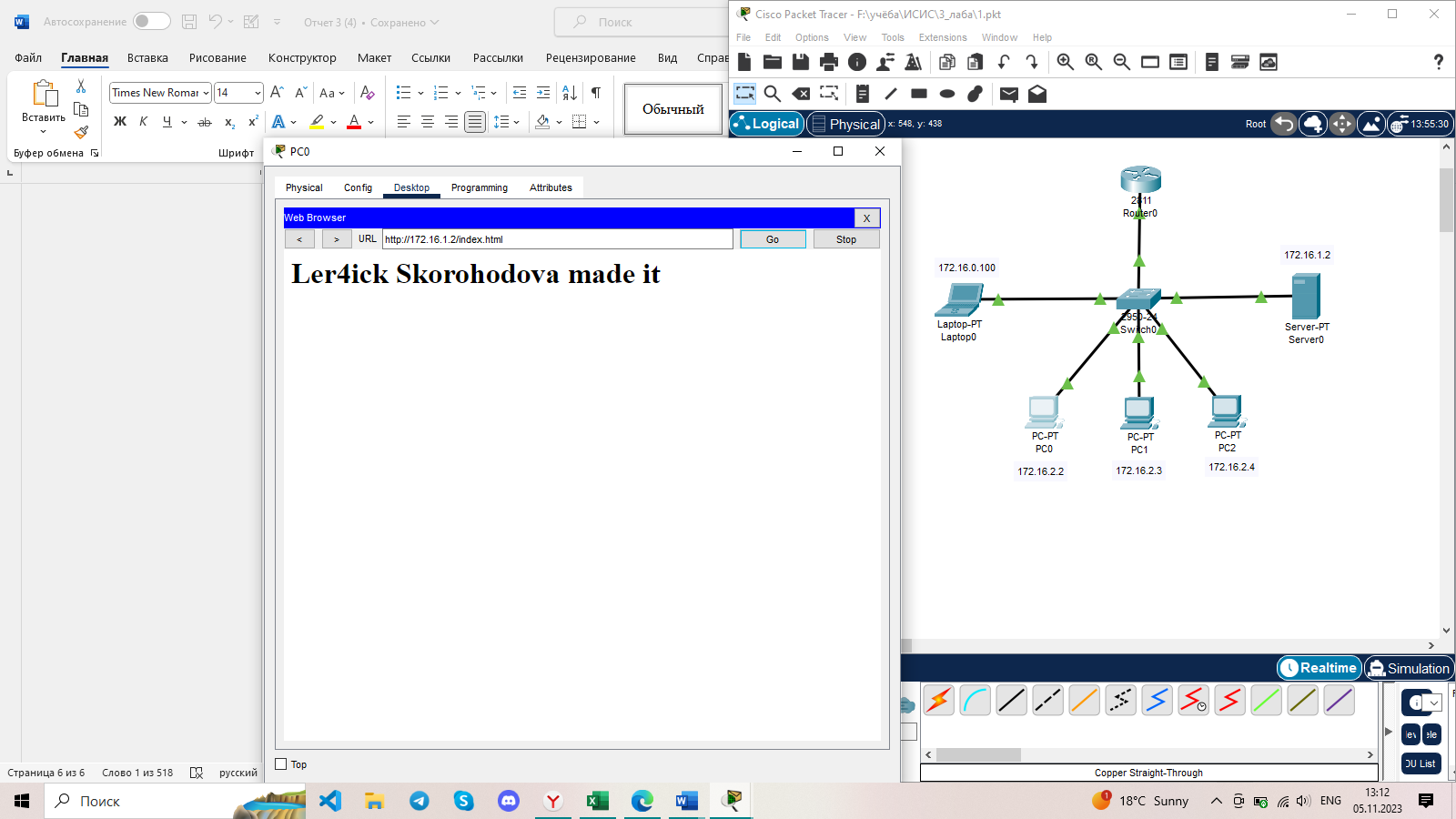


Рисунок 7 – Проверка доступа к файлу

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).

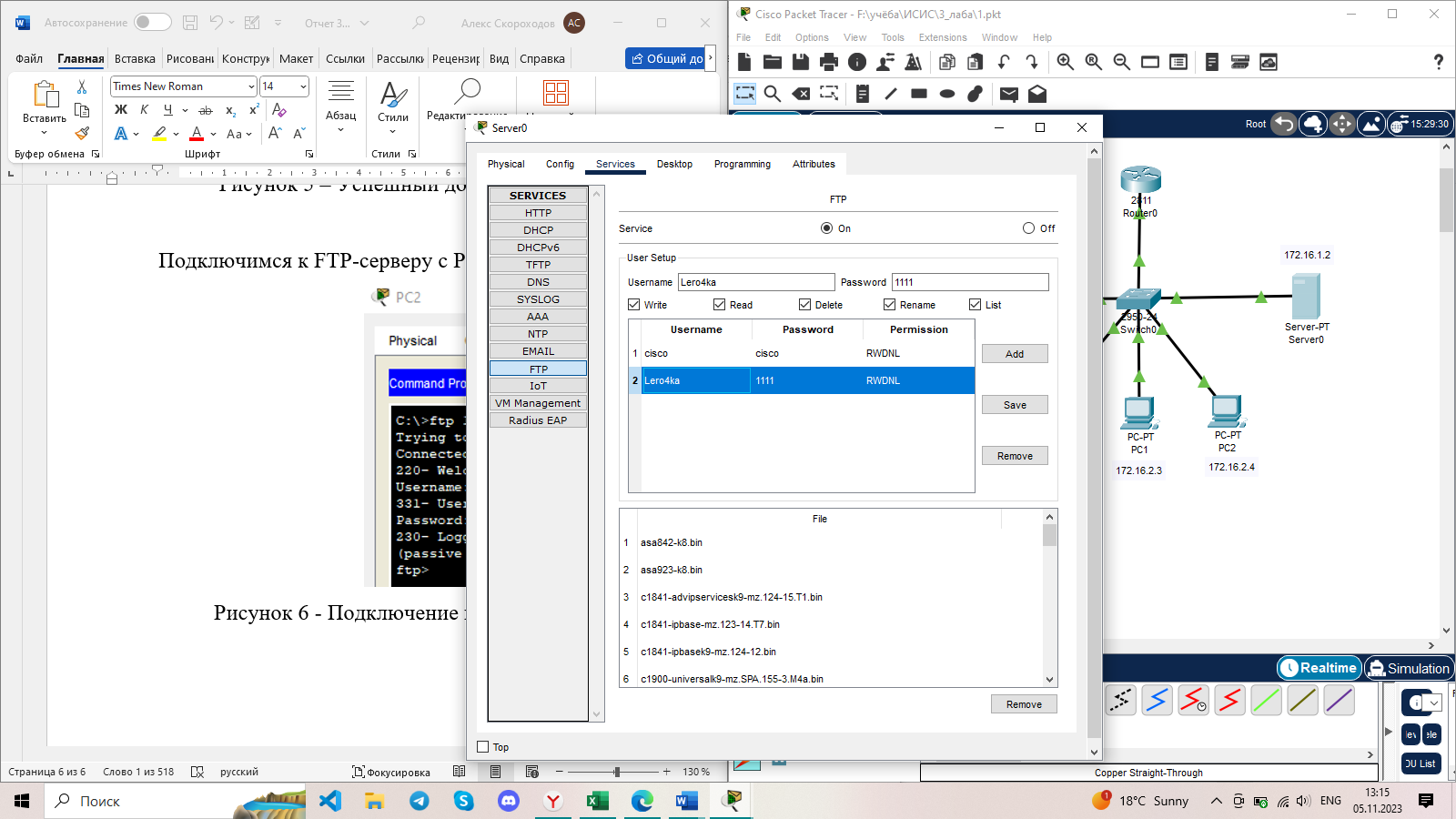


Рисунок 8 – Создание пользователя

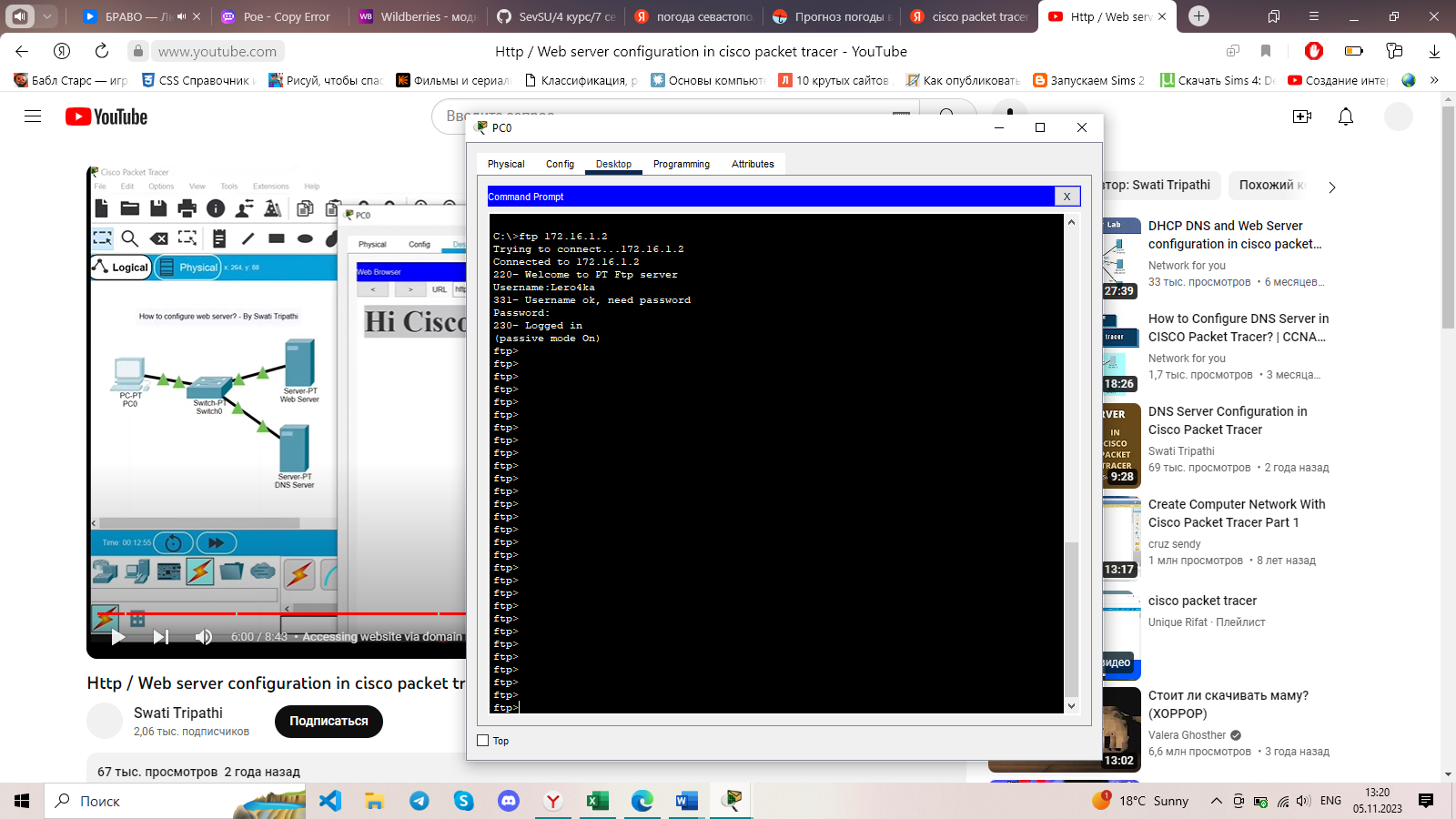


Рисунок 9 – Проверка подключения к FTP-серверу

4. 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.

5. Контрольные вопросы

**5.1. Что представляют собой списки контроля доступа?**

Для отсечения нежелательных пакетов широко применяются списки доступа ACL (Access Control Lists), которые являются своеобразными фильтрами пакетов. Они позволяют запретить или разрешить определенным хостам доступ к ресурсам сети. Например, в корпоративной сети администраторы могут запретить доступ к внутреннему серверу или в Интернет определенным пользователям, а остальным наоборот – разрешить.

5.2. Какой адрес является критерием для разрешения/запрещения пакета?

**5.3. Где применяются ACL?**

ACL применяются на маршрутизаторах и коммутаторах для управления трафиком в сети. Они используются для фильтрации и контроля передачи пакетов на основе определенных условий. ACL могут быть настроены на входящий или исходящий интерфейс маршрутизатора или коммутатора, чтобы определить, какие пакеты разрешены или запрещены на этом интерфейсе.

**5.4. Как задать элемент ACL и что такое инверсная маска?**

Элемент ACL задается с помощью адреса и маски подсети, которые определяют диапазон IP-адресов, для которых будет применяться соответствующее действие (разрешение или запрещение). Элемент ACL состоит из следующих частей:

IP-адрес: Это адрес источника или адрес назначения, к которому будет применяться ACL.

Маска подсети: Она определяет, какие биты в IP-адресе должны сравниваться при применении ACL. Маска подсети состоит из единиц и нулей, где единицы указывают биты, которые должны совпадать, а нули - биты, которые могут иметь любое значение.

Инверсная маска (Wildcard mask): Инверсная маска представляет собой инвертированную версию маски подсети. Она указывает, какие биты в IP-адресе могут отличаться при применении ACL. Инверсная маска получается путем инвертирования битов маски подсети. Например, если маска подсети равна 255.255.255.0, то инверсная маска будет равна 0.0.0.255.

**5.5. Как маршрутизатор обрабатывает элементы ACL?**

Маршрутизатор обрабатывает элементы ACL путем сравнения IP-адресов и портов входящих пакетов с заданными условиями в элементах ACL. Если условия в элементе ACL совпадают с пакетом, то маршрутизатор применяет соответствующее действие (разрешение или запрещение) к пакету. Если пакет соответствует разрешающему элементу ACL, он будет передан на соответствующий интерфейс для дальнейшей маршрутизации. В случае совпадения с запрещающим элементом ACL пакет будет отброшен и не будет маршрутизироваться дальше. Маршрутизатор обрабатывает элементы ACL в порядке их нахождения в списке, поэтому важно учитывать порядок элементов в списке ACL, чтобы правильно управлять трафиком в сети.

**5.6. Какой элемент всегда неявно присутствует в ACL?**

"deny all" или "deny any". Это означает, что если пакет не соответствует ни одному из предыдущих элементов ACL, то он будет запрещен по умолчанию.

**5.7. Как ACL применить к интерфейсу и затем его отменить?**

Для применения ACL к интерфейсу маршрутизатора или коммутатора используются команды конфигурации. В Cisco IOS, например, для применения ACL к интерфейсу входящего трафика используется команда ip access-group <имя\_ACL> in, а для применения ACL к интерфейсу исходящего трафика используется команда ip access-group <имя\_ACL> out. Здесь <имя\_ACL> - это имя или номер ACL, который вы хотите применить.

Чтобы отменить применение ACL к интерфейсу, вы можете использовать команду no ip access-group <имя\_ACL> in для входящего трафика или no ip access-group <имя\_ACL> out для исходящего трафика. Это удалит примененное ACL с указанного интерфейса.

**5.8. Чем отличается входной ACL от выходного?**

На входе весь поступающий трафик подвергается фильтрации. Нежелательные пакеты отбрасываются и уже только потом остальные пакеты маршрутизируются. Если же ACL настроены на выходе интерфейса, то трафик фильтруется сразу же после процесса маршрутизации.

5.9. Где в сети рекомендуется размещать ACL?

**5.10. Какими тремя командами можно проверить содержимое ACL и привязку к интерфейсу?**

show access-list: Эта команда отображает список всех созданных ACL на устройстве и их содержимое, включая условия и действия, определенные в каждом элементе ACL.

show ip interface <interface\_name>: Эта команда показывает конфигурацию интерфейса и включает информацию о привязке ACL к интерфейсу входящего или исходящего трафика.

show running-config: Эта команда выводит текущую конфигурацию устройства, включая все ACL, примененные к интерфейсам.

**5.11. Что фильтруют расширенные ACL?**

Расширенные ACL (Extended ACL) фильтруют трафик на основе более детальных условий, чем стандартные ACL. Они позволяют фильтровать пакеты по исходному и целевому IP-адресам, портам и протоколам. Расширенные ACL позволяют более гибко контролировать трафик в сети, так как они могут определять более сложные правила фильтрации на основе различных параметров пакета.

**5.12. Какую дополнительную функциональность имеют расширенные ACL по сравнению со стандартными?**

* Фильтрация на основе исходного и целевого IP-адреса: Расширенные ACL позволяют указывать конкретные IP-адреса и подсети в условиях фильтрации, что обеспечивает более точный контроль над трафиком.
* Фильтрация на основе портов и протоколов: Расширенные ACL позволяют фильтровать трафик на основе портов и протоколов, что позволяет контролировать доступ к конкретным сетевым службам или приложениям.
* Использование инверсной маски: Расширенные ACL могут использовать инверсную маску для определения несовпадающих битов в IP-адресе, что дает большую гибкость при настройке правил фильтрации.

**5.13. Можно ли, используя расширенные ACL, наложить ограничения на трафик к определённой TCP/IP службе?**

Да, используя расширенные ACL, можно наложить ограничения на трафик к определенной TCP/IP службе. Для этого в элементе ACL нужно указать соответствующий протокол (TCP или UDP) и номер порта, который используется для определенной службы. Например, чтобы ограничить доступ к веб-серверу (который обычно работает на порту 80), можно создать элемент ACL, который разрешает трафик только с определенного источника на целевой IP-адрес с использованием TCP-протокола и порта 80. Остальной трафик, направленный на этот порт, будет запрещен.

**5.14. Опишите процедуру создания именованного ACL.**

Создайте именованный ACL с помощью команды ip access-list <имя\_ACL>, где <имя\_ACL> - это имя, которое вы выбираете для ACL.

Определите условия и действия для каждого элемента ACL. Например, вы можете использовать команду permit или deny для разрешения или запрещения трафика, а затем указать соответствующие условия, такие как исходный и целевой IP-адрес, порт или протокол. Например:

permit tcp any host 192.168.0.10 eq 80

deny ip any any

```

Сохраните настройки ACL с помощью команды exit или end.

Примените созданный именованный ACL к интерфейсу или другой конфигурационной секции сетевого устройства с помощью соответствующей команды. Например, в Cisco IOS для применения ACL к интерфейсу входящего трафика используется команда ip access-group <имя\_ACL> in.

**5.15. Как отредактировать конкретную строку в числовом ACL?**

Для редактирования конкретной строки в числовом ACL требуется перезаписать всю строку с новыми значениями, включая измененные параметры. Невозможно отредактировать отдельный параметр внутри строки числового ACL без перезаписи всей строки.

**5.16. Как отредактировать конкретную строку в именованном ACL?**

Войдите в режим конфигурации устройства. Например, в Cisco IOS это делается с помощью команды configure terminal.

Войдите в режим редактирования именованного ACL с помощью команды ip access-list <имя\_ACL>, где <имя\_ACL> - это имя вашего ACL.

Используйте команду no <строка\_ACL> для удаления существующей строки ACL, которую вы хотите изменить.

Создайте новую строку ACL с требуемыми изменениями

5.17. Чем отличается форматы команд для ввода элементов числового и именованного ACL?