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 №1

«Исследование способов построения виртуальных локальных

компьютерных сетей»

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 принципов работы коммутаторов и виртуальных локальных сетей, способов конфигурации коммутаторов для построения виртуальных локальных сетей, приобретение практических навыков конфигурации коммутаторов и исследования функционирования виртуальных сетей.

2. Постановка задачи

2.1 Изучить теоретический материал, относящийся к разделу «Локальные компьютерные сети». Особое внимание следует уделить подразделу «Виртуальные локальные сети» и устройству и конфигурации коммутаторов. (Выполняется в процессе домашней подготовки).

2.2 Построить в окне эмулятора Packet Tracer локальную сеть на основе одного коммутатора. Задать узлам сети IP-адреса. Количество серверов и рабочих станций определяется вариантом задания (Таблица 1).

2.3 Исследовать достижимость сетевых узлов путем их пингования. Результаты пингования сохранить для отчета.

2.4 Разделить сеть, построенную на этапе 2.2, на виртуальные сети способом группирования портов. Количество коммутаторов, виртуальных сетей и рабочих станций в виртуальных сетях определяется вариантом задания (Таблица 2).

2.5 Исследовать пингованием достижимость сетевых узлов внутри каждой из виртуальных сетей и между виртуальными сетями. После настройки VLAN посмотреть текущую конфигурацию сети командами: show running-config, show vlan, show vlan brief, show mac address-table. Результаты пингования и просмотра конфигурации включить в отчет.

2.6 Повторить п.2.4 и 2.5 при условии, что в сети существует два коммутатора. Виртуальные сети включают компьютеры, соединенные как с первым, так и со вторым коммутаторами. Количество линий связи меду коммутаторами равно количеству виртуальных сетей.

2.7 Повторить п.2.6 при использовании транковых соединений между коммутаторами.

2.8 Построить сеть, изображенную на рисунке 2.8 (1.4), и сконфигурировать ее так, чтобы обеспечить обмен пакетами между виртуальными сетями и исследовать корректность функционирования сети.

Таблица 1 – Вариант задания

|  |  |  |  |
| --- | --- | --- | --- |
| Вариант | Количество РС | Количество серверов | Количество ноутбуков |
| 9 | 3 | 3 | 3 |

Таблица 2 – Вариант задания

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Вариант | Количество | | | | |
| РС | серверов | ноутбуков | коммутаторов | VLAN |
| 9 | 3 | 3 | 3 | 2 | 2 |

3. Ход работы

3.1. Была построена локальная сеть на основе одного коммутатора, представленная на рисунке 1. Количество устройств соответствует варианту задания в таблице 1. Всем устройствам были присвоены IP-адреса, данные соответствия приведены в таблице 3.

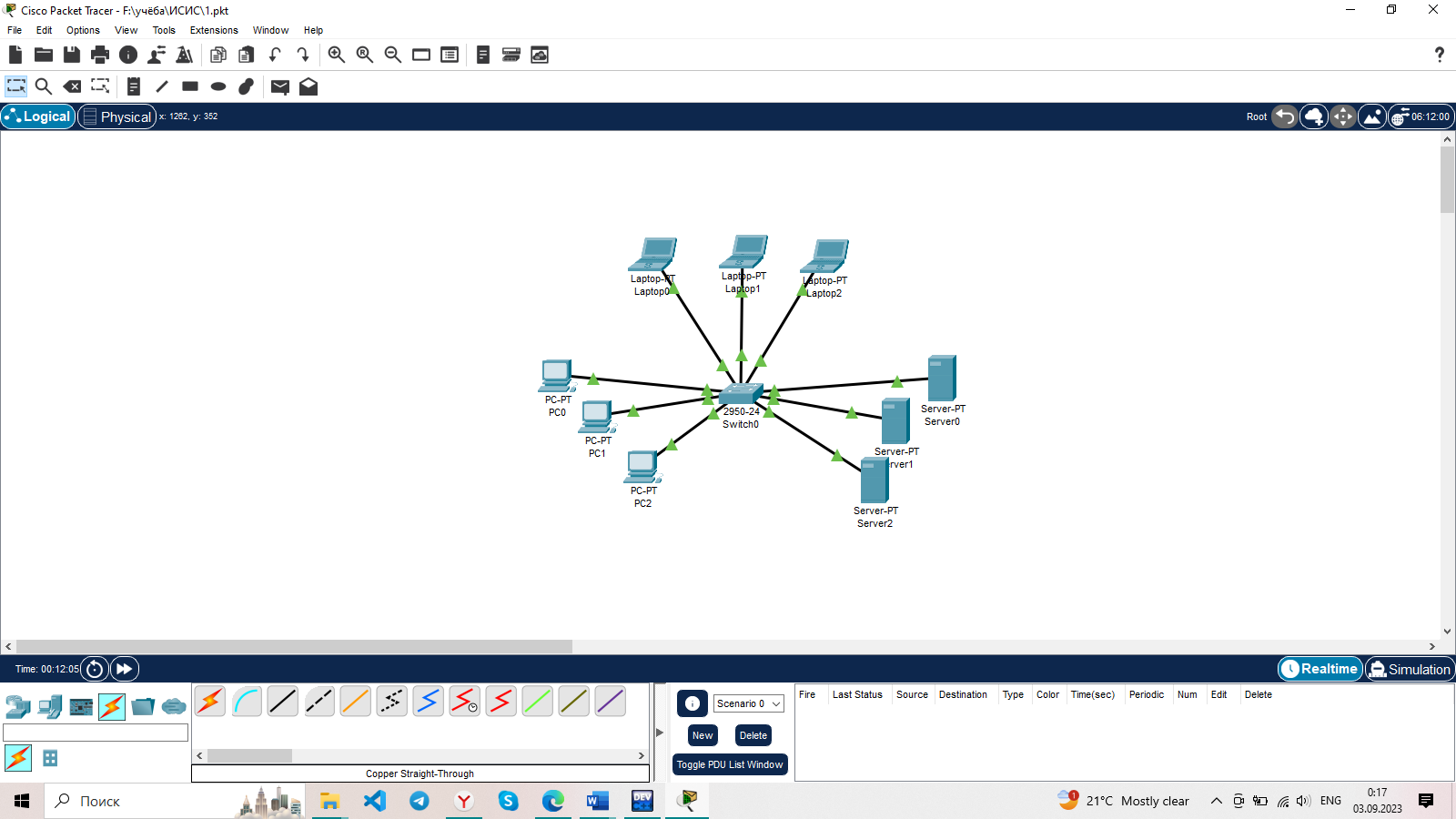


Рисунок 1 – Локальная сеть на одном коммутаторе

Таблица 3 - Устройства и соответствующие им IP-адреса

|  |  |  |
| --- | --- | --- |
| Сетевое имя | IP-адрес | Маска подсети |
| Laptop-PT Laptop0 | 192.168.19.1 | 255.255.255.0 |
| Laptop-PT Laptop1 | 192.168.19.2 | 255.255.255.0 |
| Laptop-PT Laptop2 | 192.168.19.3 | 255.255.255.0 |
| РС-РТ РС0 | 192.168.19.4 | 255.255.255.0 |
| РС-РТ РС1 | 192.168.19.5 | 255.255.255.0 |
| РС-РТ РС2 | 192.168.19.6 | 255.255.255.0 |
| Server-РТ Server0 | 192.168.19.7 | 255.255.255.0 |
| Server-РТ Server1 | 192.168.19.8 | 255.255.255.0 |
| Server-РТ Server2 | 192.168.19.9 | 255.255.255.0 |

3.2. Была проверена достижимость узлов путем пингования. Результаты пингования отображены на рисунке 2. Как можно видеть, потери данных не произошло.

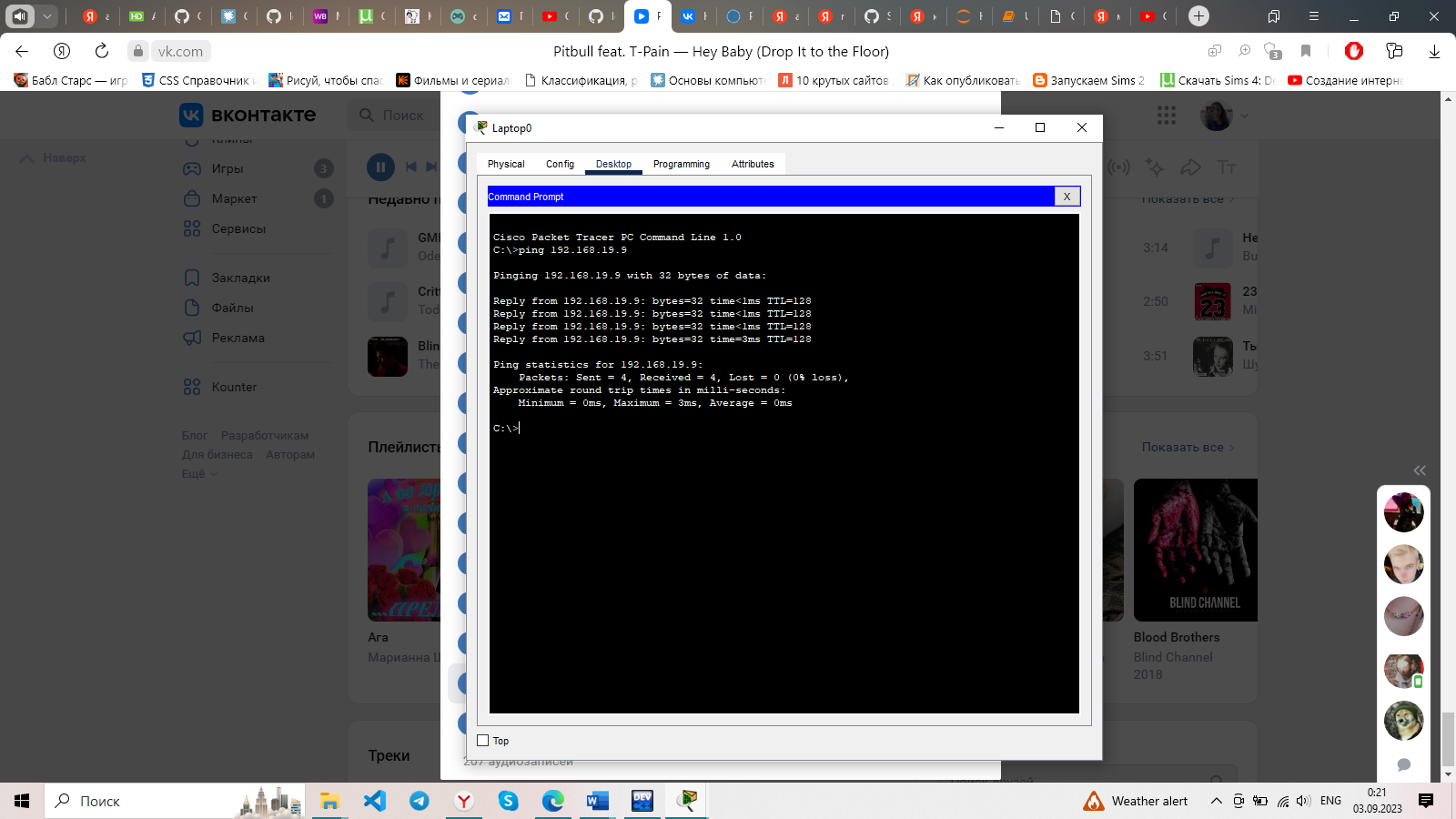


Рисунок 2 – Результат пингования с Laptop0 на Server2

3.3. Построенная сеть была разделена на виртуальные сети (рисунок 3). Количество коммутаторов, виртуальных сетей и рабочих станций в виртуальных сетях определяется вариантом задания, указанным в таблице 2.

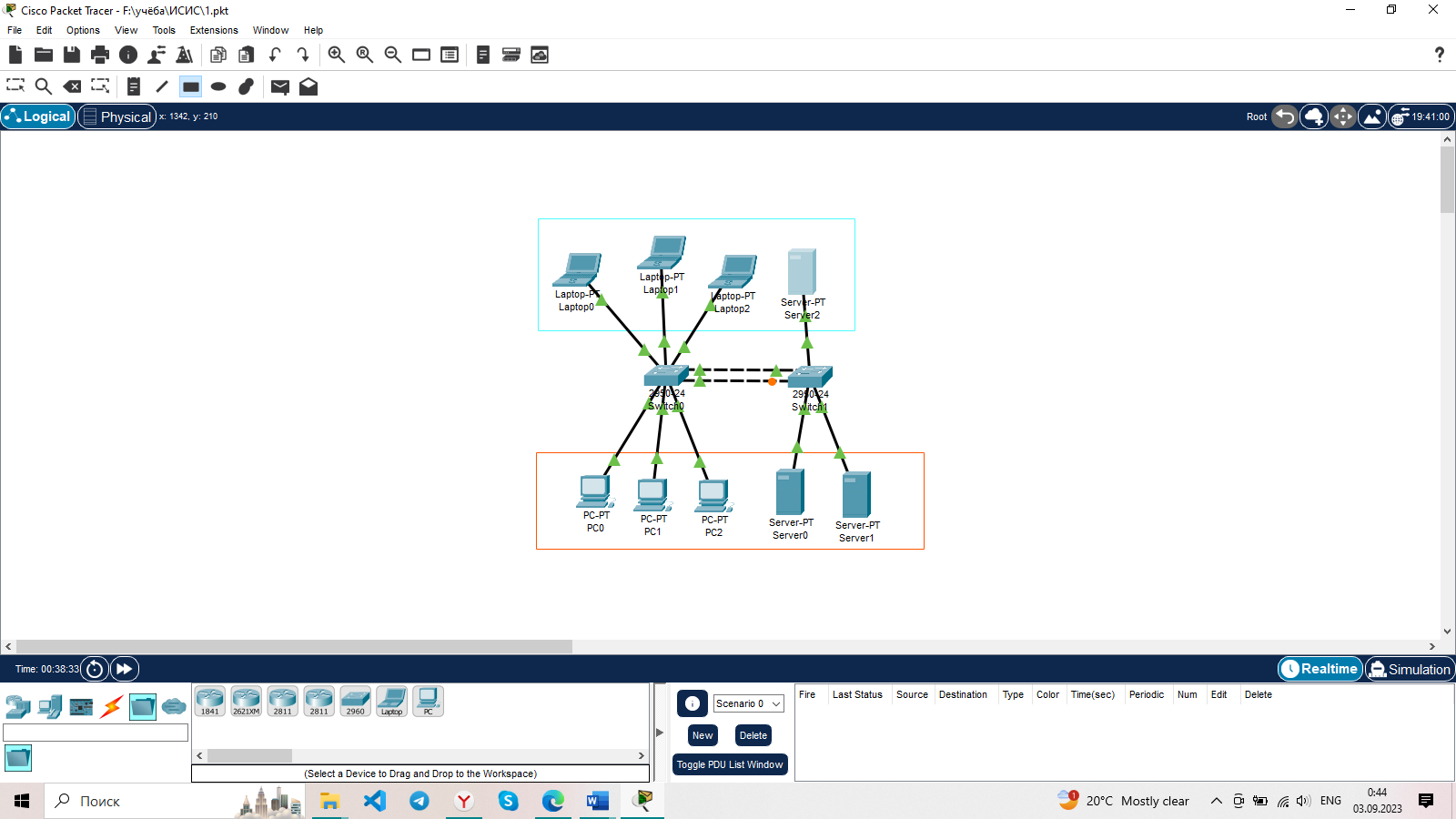


Рисунок 3 – Локальная сеть, разделенная на виртуальные сети

На каждом коммутаторе были созданы 2 VLAN, которым были присвоены имена «one», «two». Пример показан на рисунке 4.

Далее хосты были способом группирования портов объединены по сетям следующим образом:

Laptop0, Laptop1, Laptop2, Server2 – VLAN11 «one»;

Server0, Server1, PC0, PC1, PC2 – VLAN2 «two».

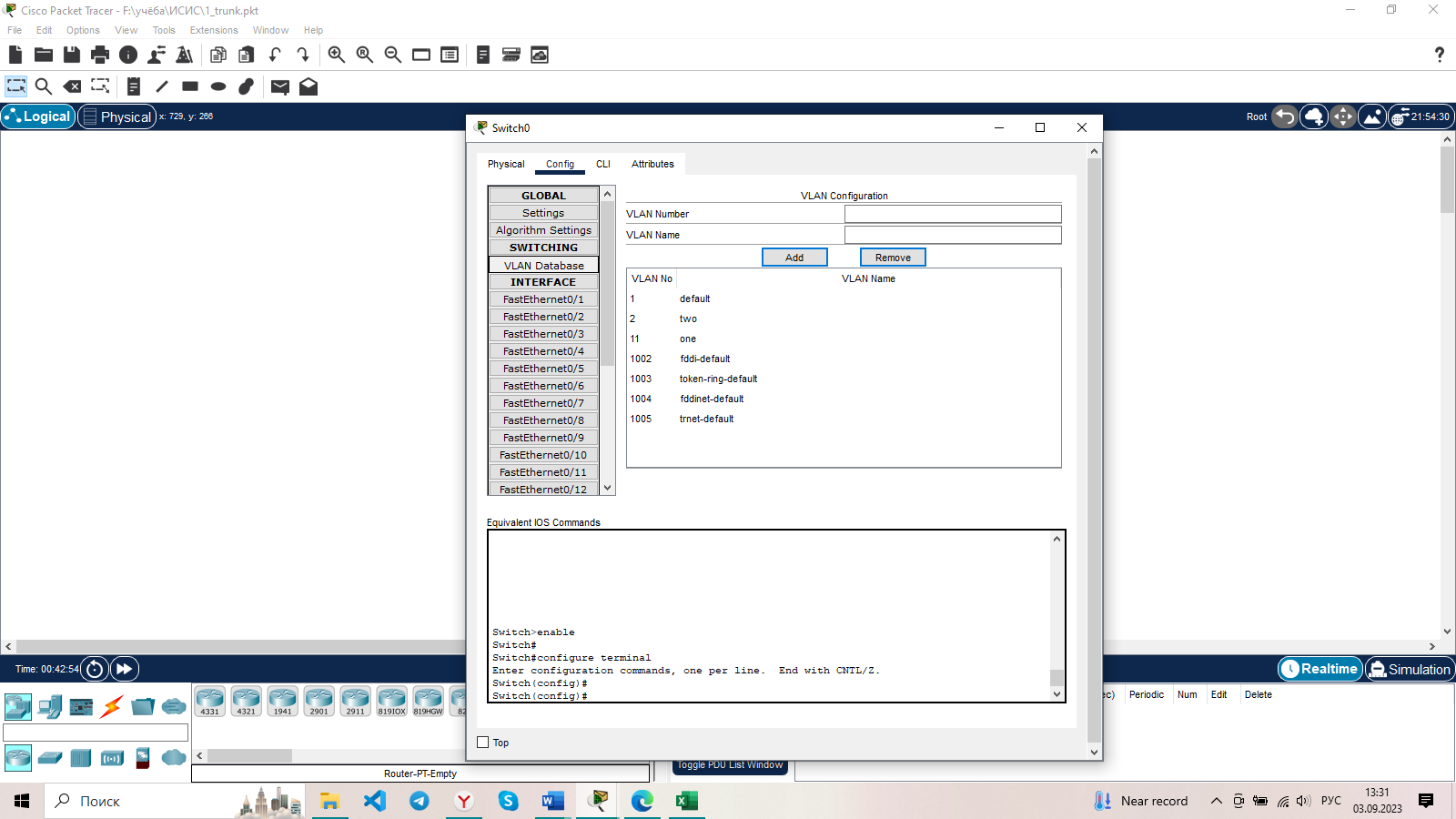


Рисунок 4 – Список VLAN’ов на коммутаторах

3.4. Была исследована достижимость узлов путем пингования.

На рисунке 5 представлен случай, когда передача сообщения происходит между устройствами, подключенным к разным коммутаторам, но принадлежащих одной VLAN. Как видно, при пинговании потери данных не происходит.

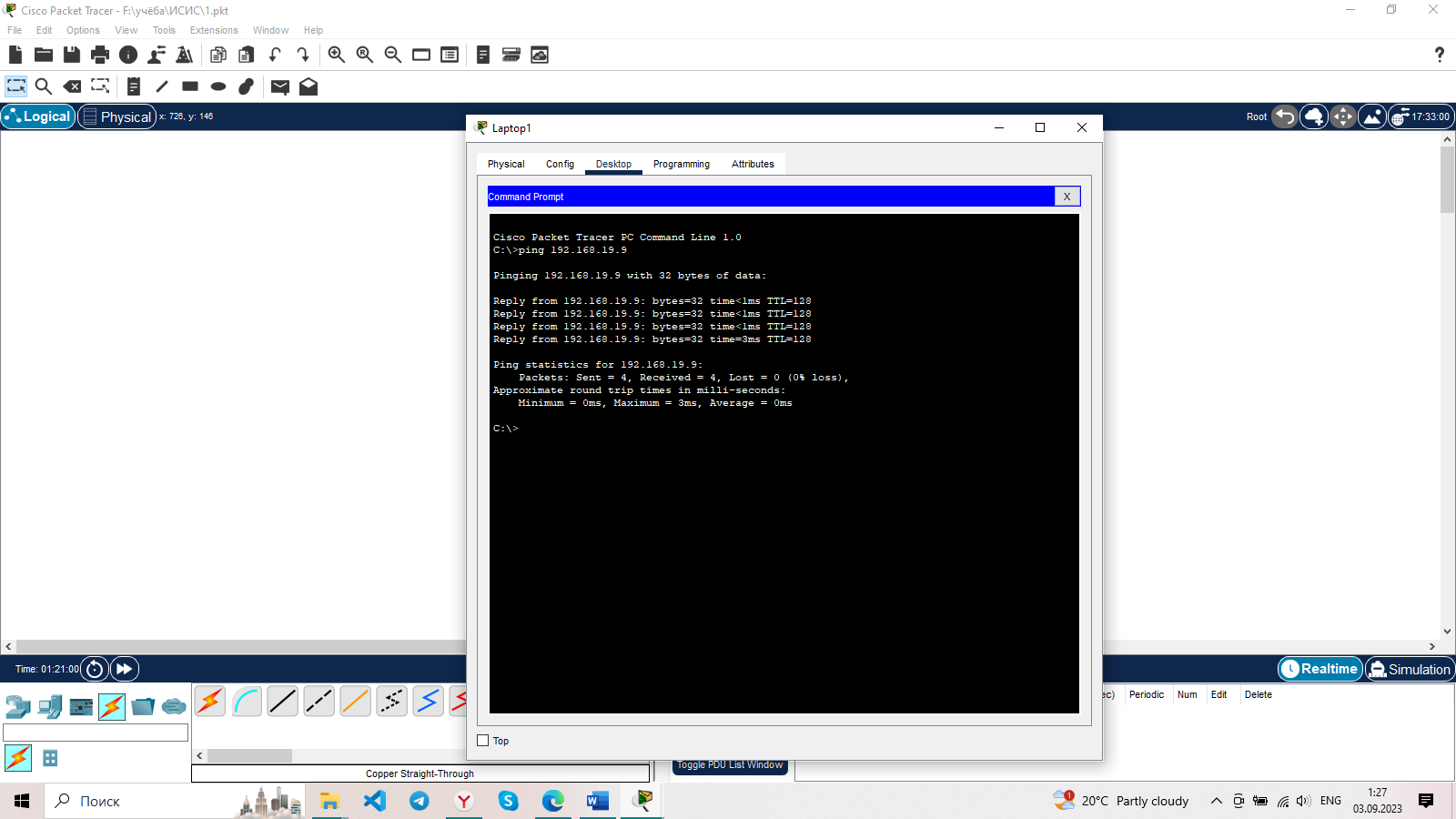


Рисунок 5 – Пингование с устройства Laptop1 на устройство Server2 (подключены к разным коммутаторам, но в одной VLAN)

На рисунке 6 представлен результат пингования, в случае если устройства подключены к разным коммутаторам и принадлежат разным VLAN. Из-за того, что устройства относятся к разным VLAN, происходят 100% потери данных.

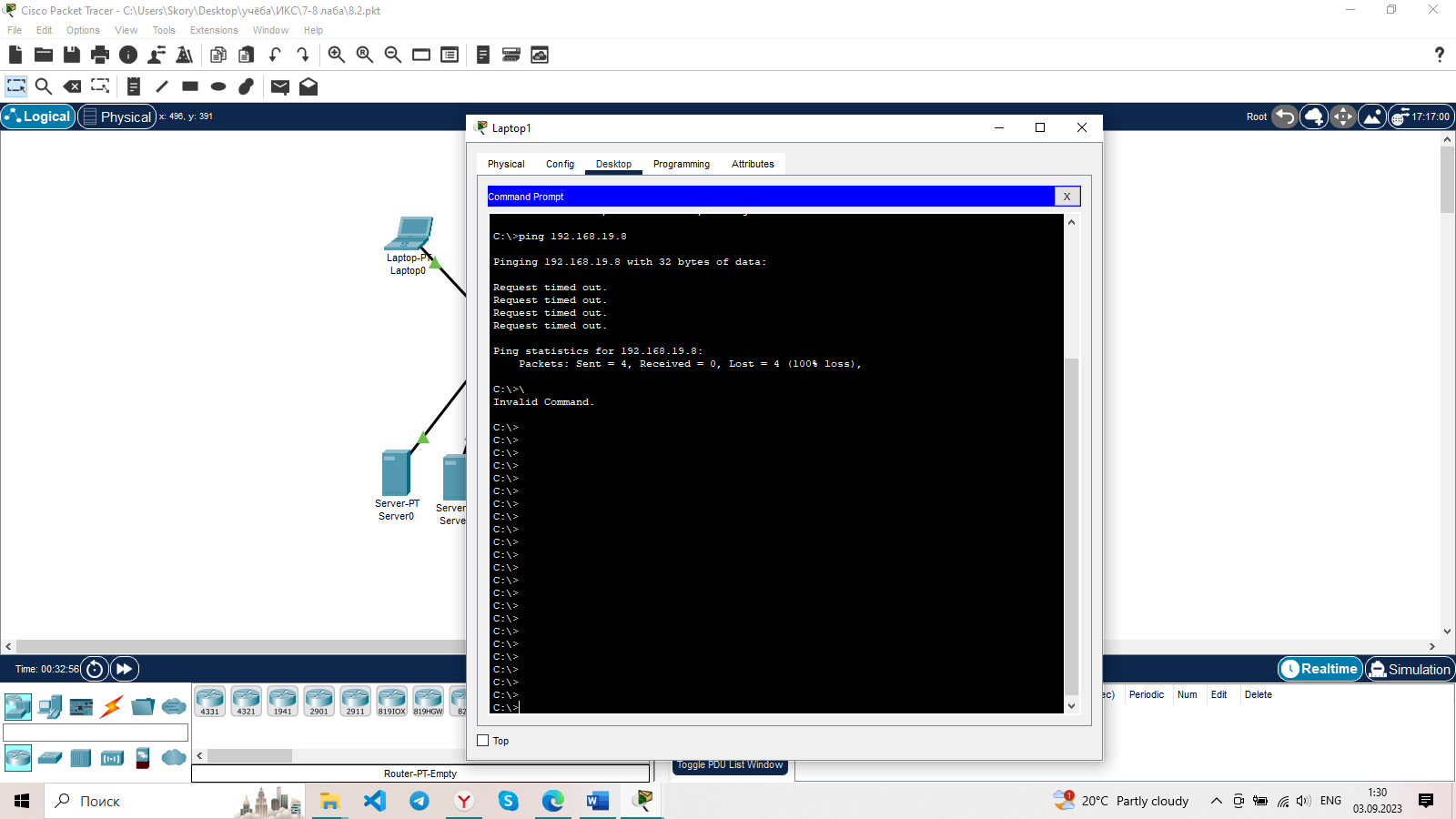


Рисунок 6 – Пингование с Laptop1 на Server1 (разные коммутаторы и VLAN)

На рисунке 7 представлен результат отправки сообщения, в случае если устройства находятся на одном коммутаторе, но принадлежат разным VLAN. Из-за того, что устройства относятся к разным VLAN, происходят 100% потери данных.

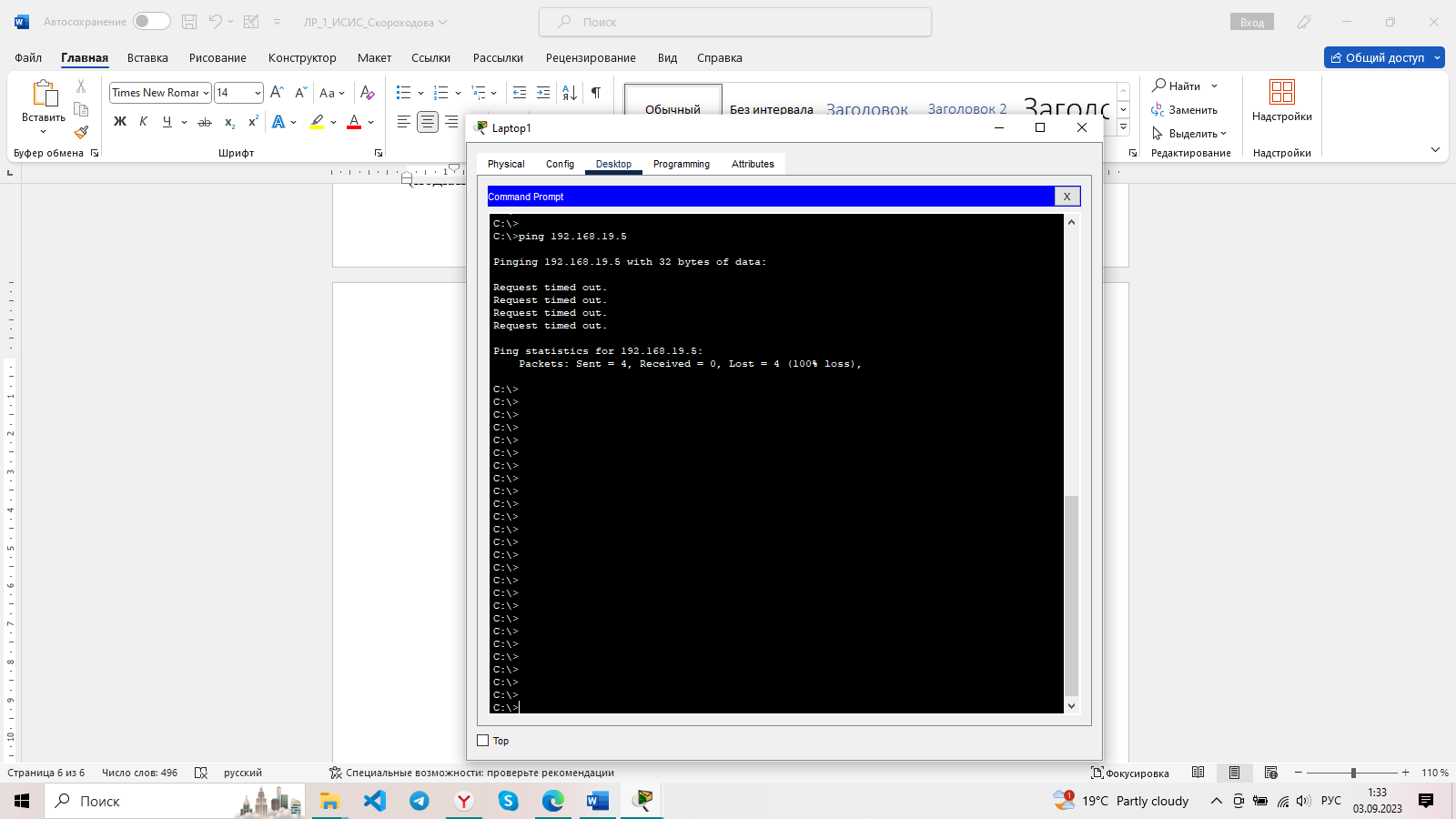


Рисунок 7 – Пингование с Laptop1 на PC1 (один коммутатор, но разные VLAN)

На рисунке 8 представлен случай, когда передача сообщения происходит между устройствами, подключенным к одному коммутатору и принадлежащих одной VLAN. Как видно, при пинговании потери данных не происходит.

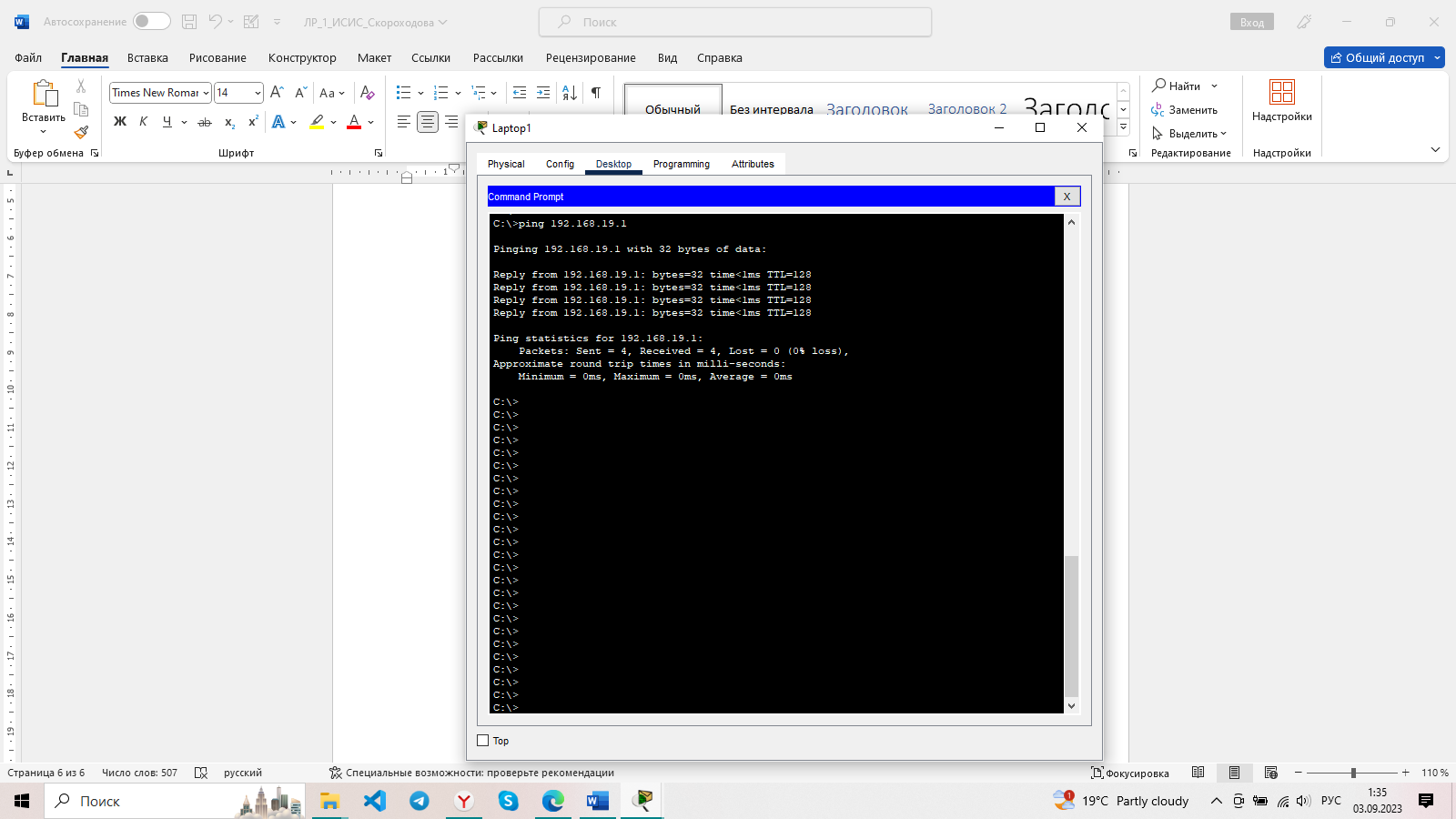


Рисунок 8 – Пингование с Laptop1 на Laptop0 (на одном коммутаторе и VLAN)

После настройки VLAN с помощью команд show running-config, show vlan, show vlan brief, show mac address-table была просмотрена текущая конфигурация сети. Все команды выполнялись на коммутаторе Switch0.

Для просмотра подробной информации о всех VLAN’ах была использована команда: # show vlan. На рисунке 9 видно, какие порты каким VLAN принадлежат. Как пример, порты, соединяющие устройства из VLAN «one» записаны в таблице напротив этой VLAN.

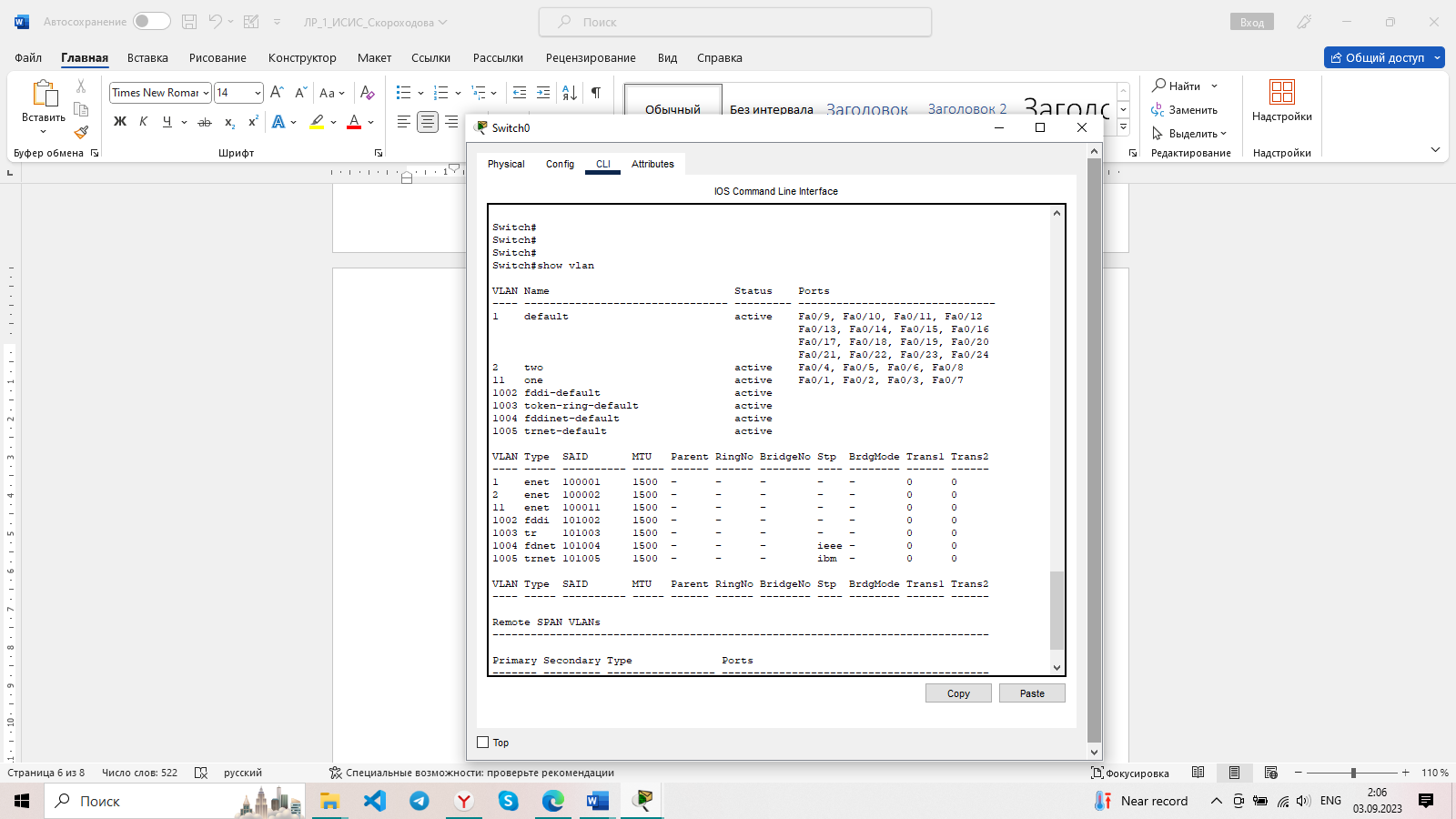


Рисунок 9 – Просмотр информации о VLAN и их портах

Для сокращенного отображения информации о всех VLAN использовалась команда: # show vlan brief. Результат представлен на рисунке 10.

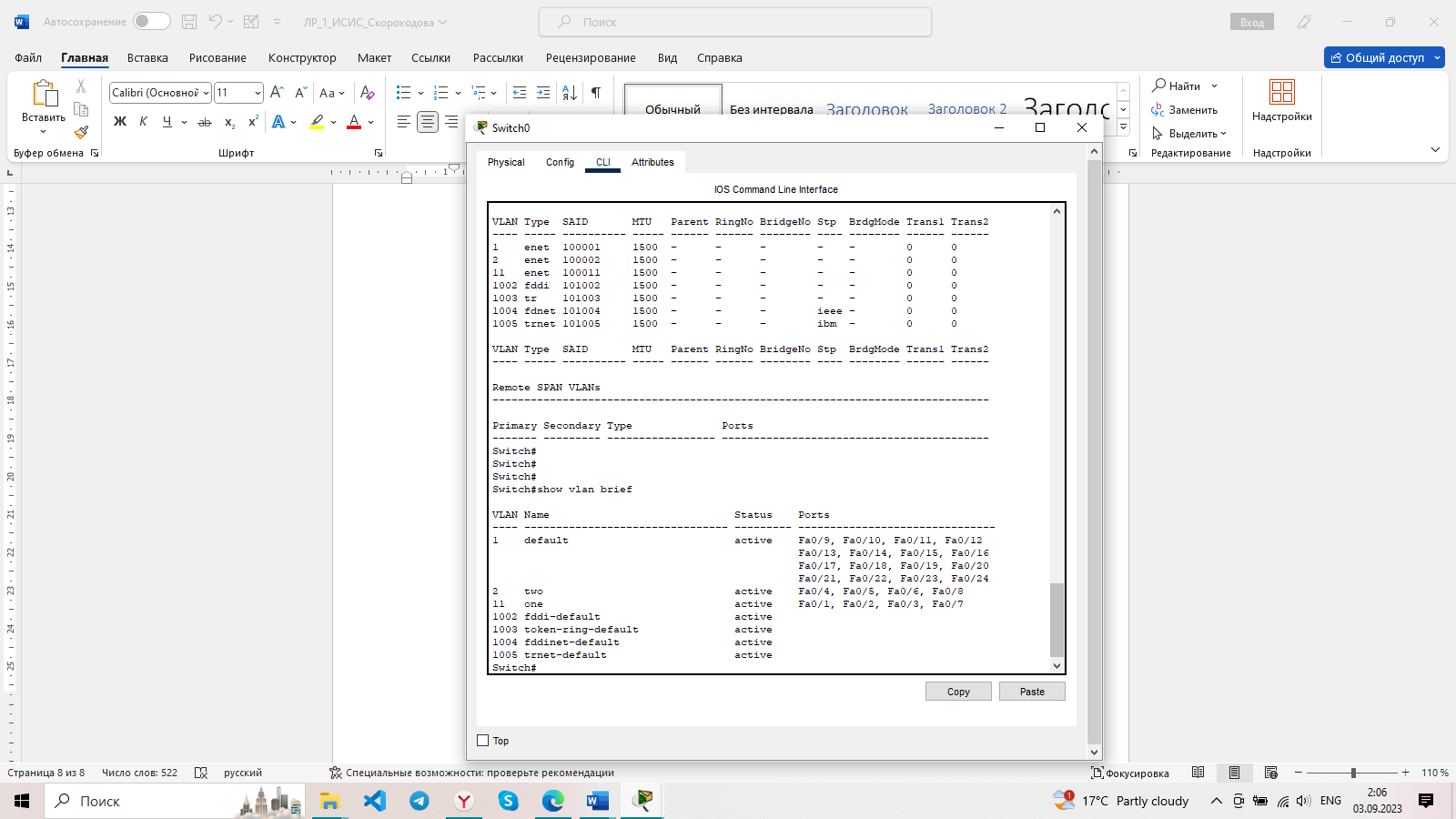


Рисунок 10 – Сокращенный просмотр информации о VLAN и их портах

Команда show running-config показывает текущую конфигурацию устройства. В данном случае это устройство Switch0. На рисунке 11 представлен результат работы команды.

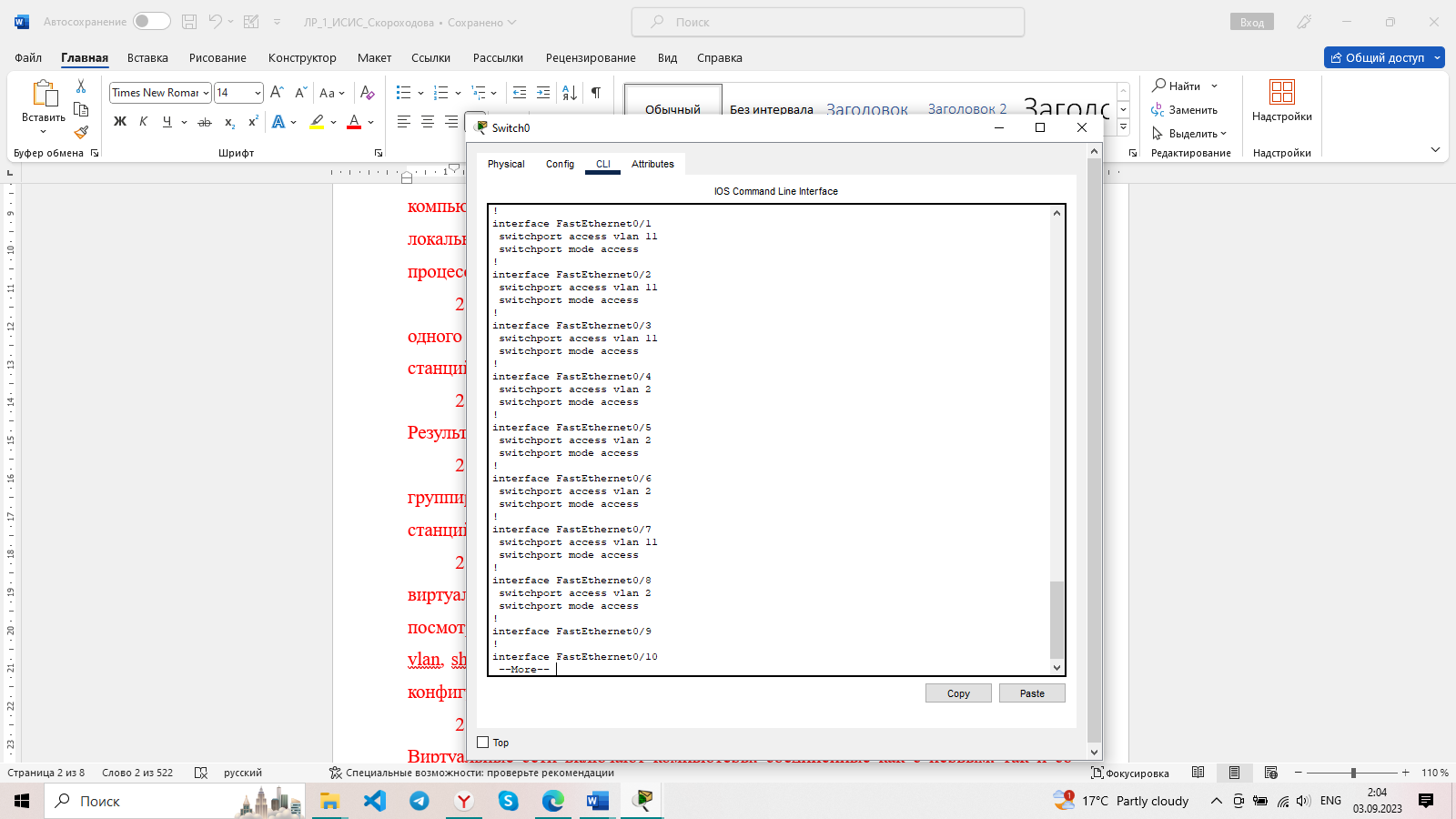


Рисунок 11 – Результат работы команды show running-config

Команда show mac address-table показывает мак-таблицу устройства, результат на рисунке 12.

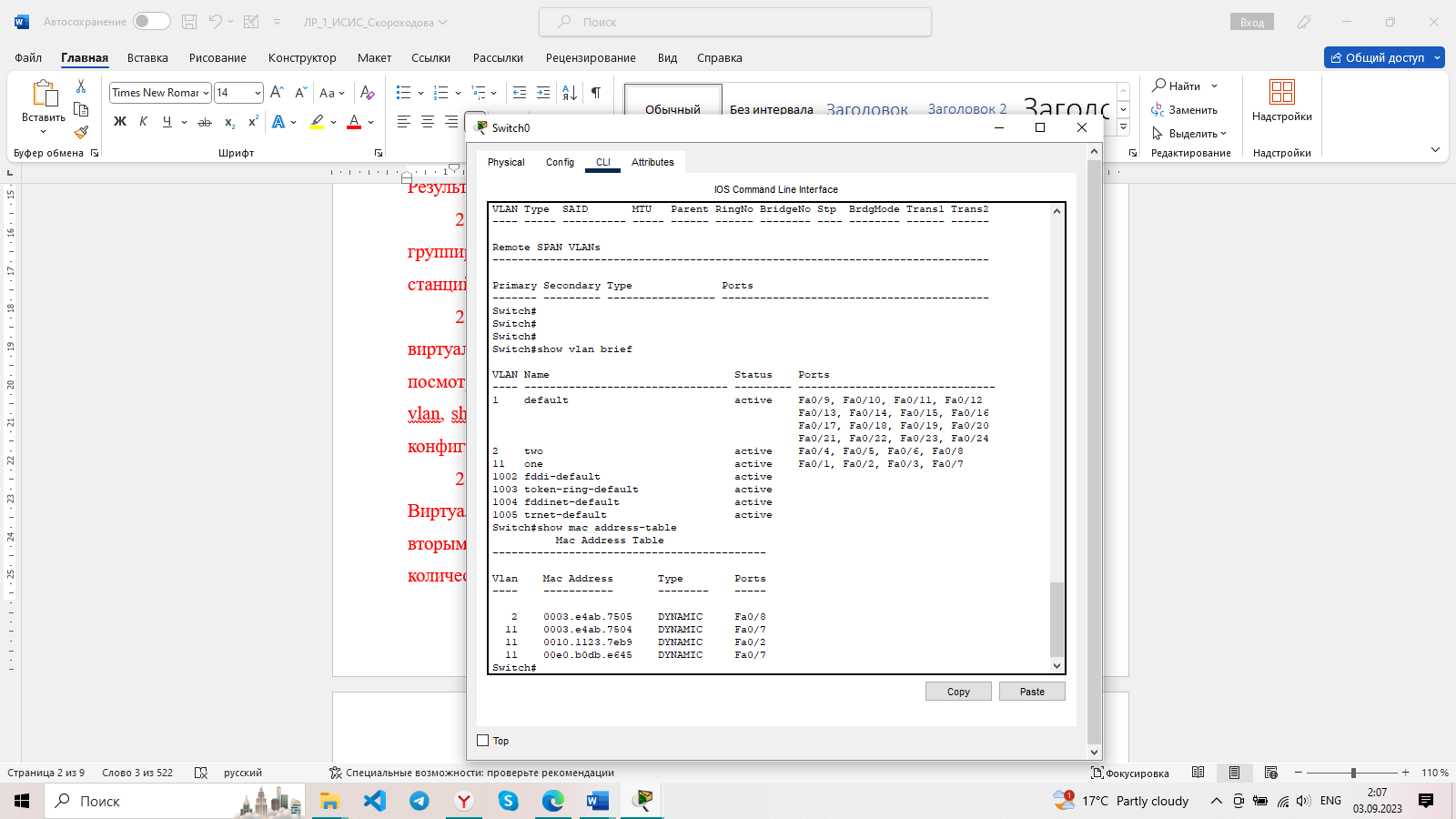


Рисунок 12 – Таблица физических адресов устройств, подключенных к Switch0

3.5. Далее соединение между коммутаторами было заменено на транковое.

На рисунке 13 представлен результат проверки достижимости сетевых узлов внутри виртуальной сети и между виртуальными сетями. Пингование осуществлялось с устройства PC0, находящемся в VLAN 2, на устройство Server0 (находящемся в той же VLAN), и передача сообщения прошла успешно. Затем было произведено пингование на устройство Server2, которое находится в другой VLAN, и произошли утечки информации.

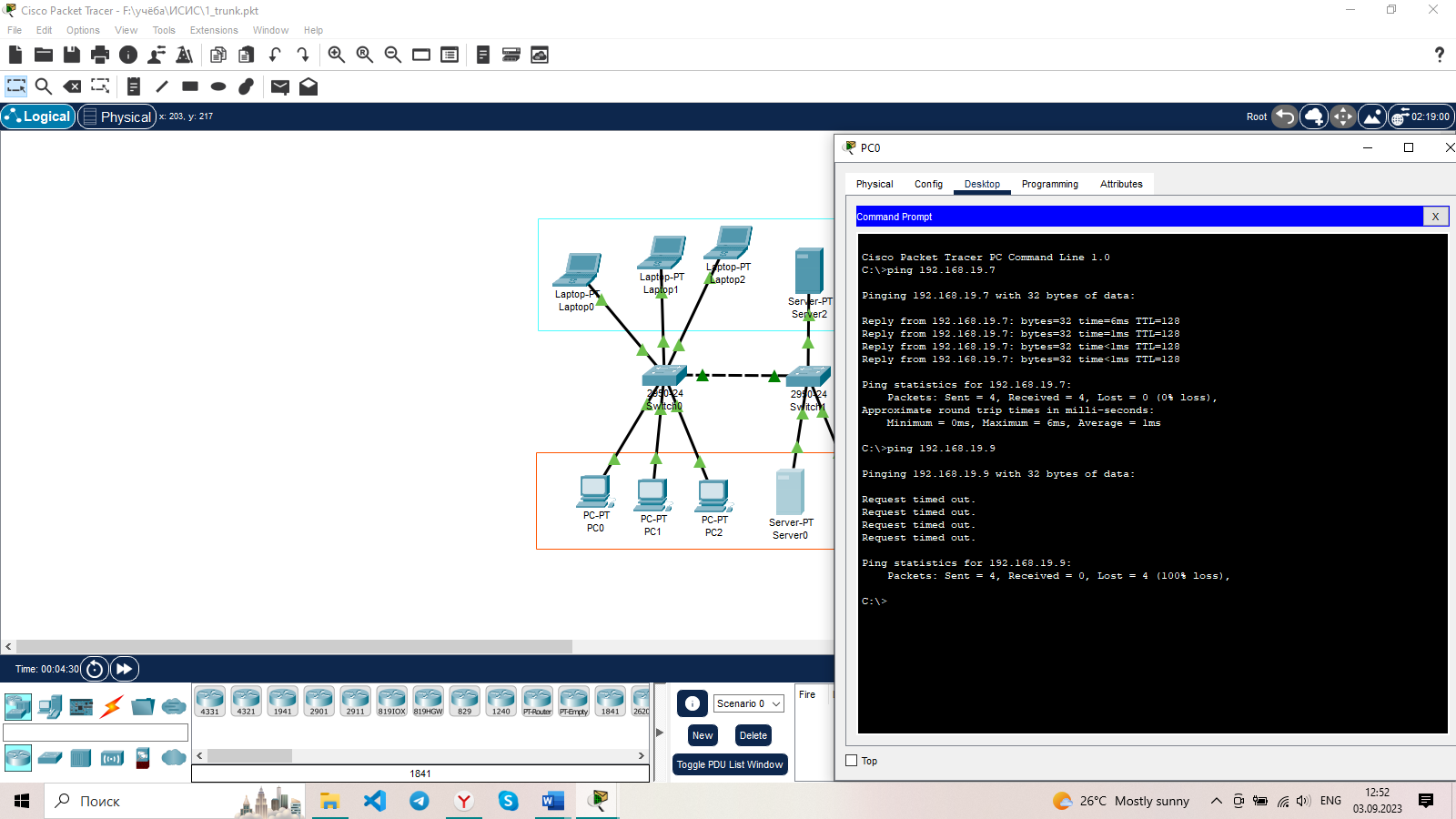


Рисунок 13 – Результаты пингования в одной VLAN и между VLAN’ами

3.6. Требовалось построить сеть, изображенную на рисунке 1.4 (приложение А), и сконфигурировать ее так, чтобы обеспечить обмен пакетами между виртуальными сетями и исследовать корректность функционирования сети. Построенная сеть изображена на рисунке 14. В таблице 4 приведена информация об оконечных устройствах и IP-адресах, соответствующих им.

Таблица 4 - Устройства и соответствующие им IP-адреса

|  |  |  |
| --- | --- | --- |
| Сетевое имя | IP-адрес | Маска подсети |
| РС-РТ РС0 | 172.16.1.5 | 255.255.255.0 |
| РС-РТ РС1 | 172.16.2.2 | 255.255.255.0 |
| РС-РТ РС2 | 172.16.1.3 | 255.255.255.0 |
| РС-РТ РС3 | 172.16.2.4 | 255.255.255.0 |

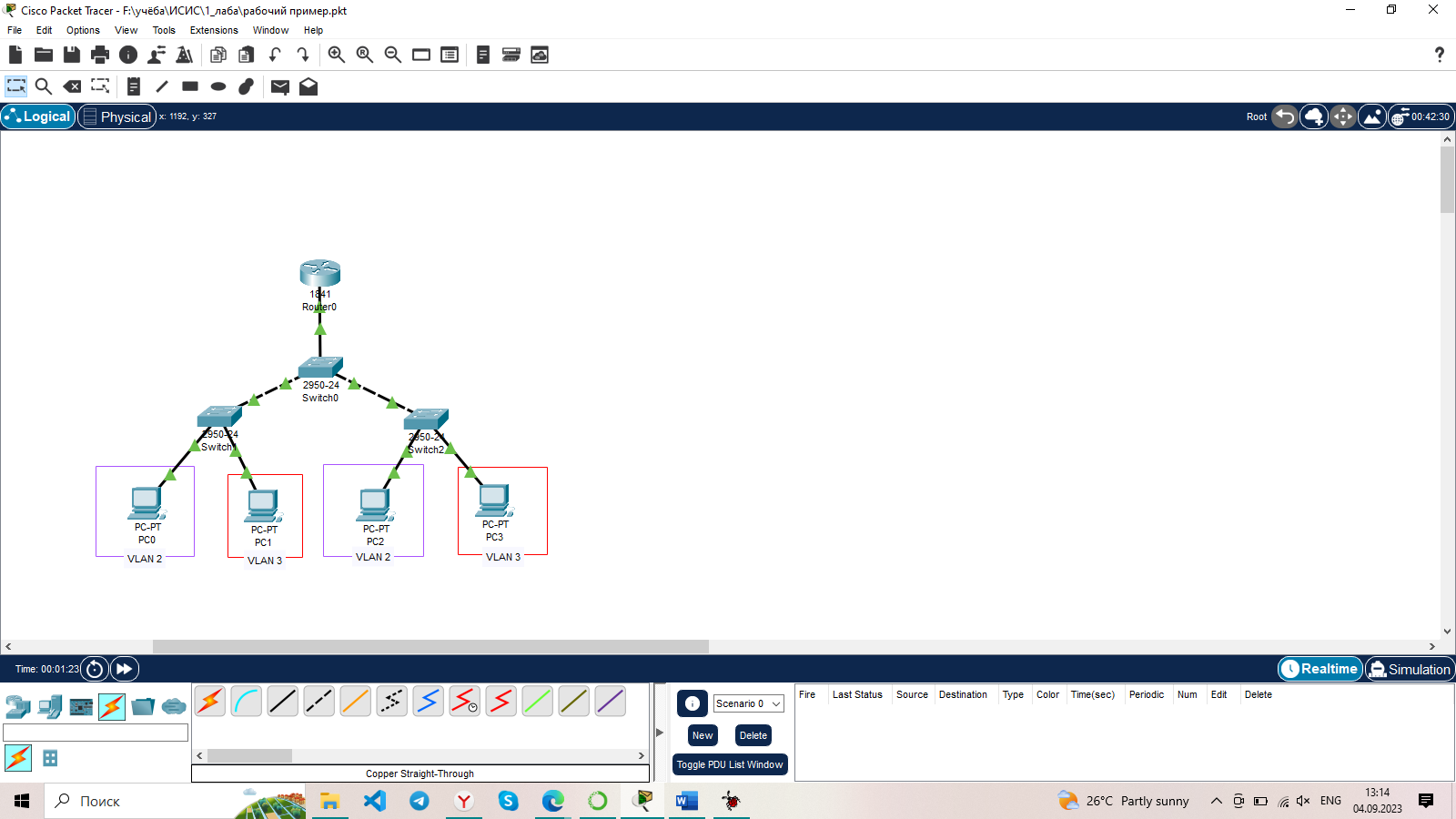


Рисунок 14 – InterVlan routing на маршрутизаторе

Далее на роутере, а затем и на коммутаторе (Switch0) были введены команды, представленные на рисунках 15-16.

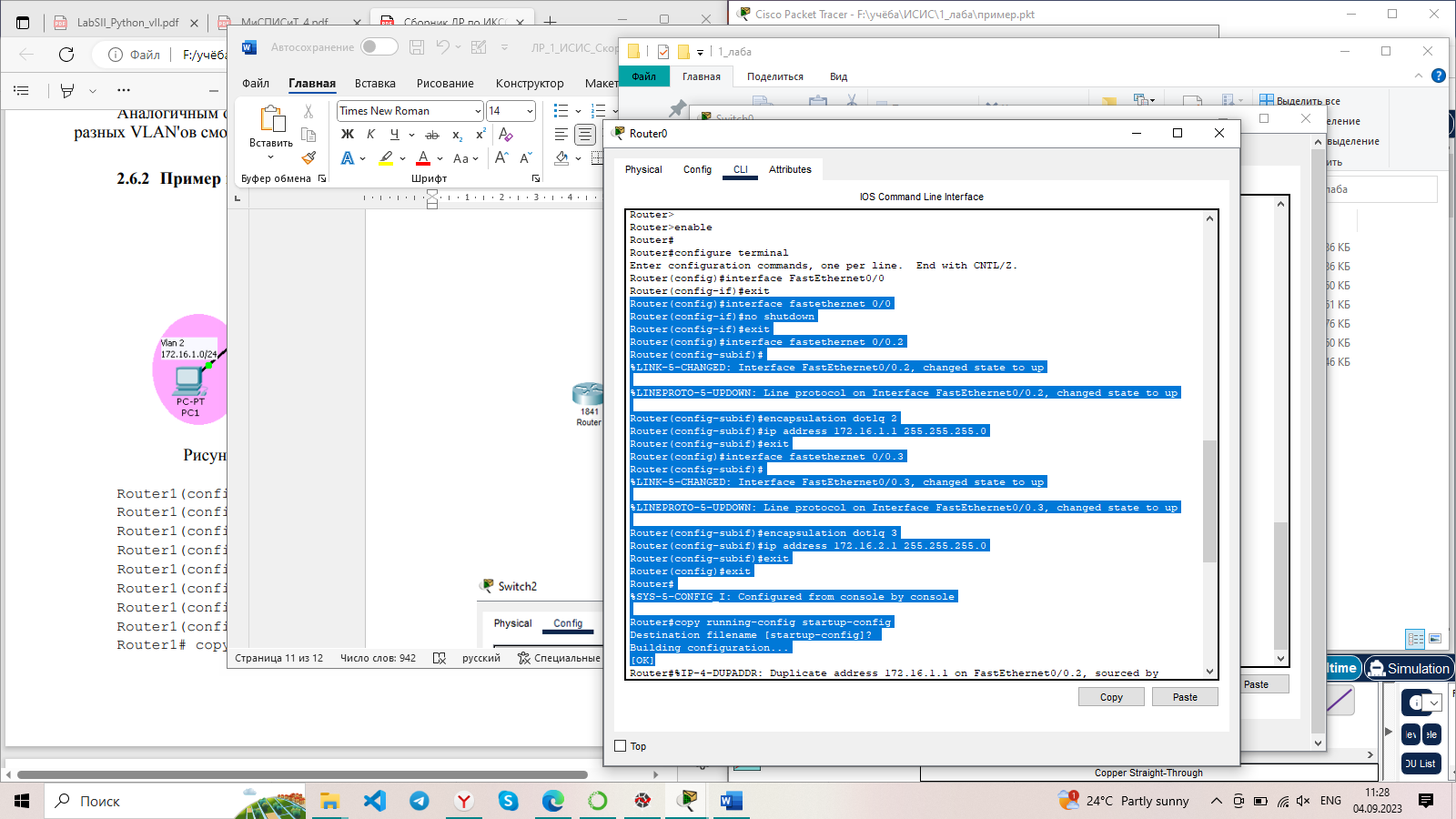


Рисунок 15 – Список команд на Router0

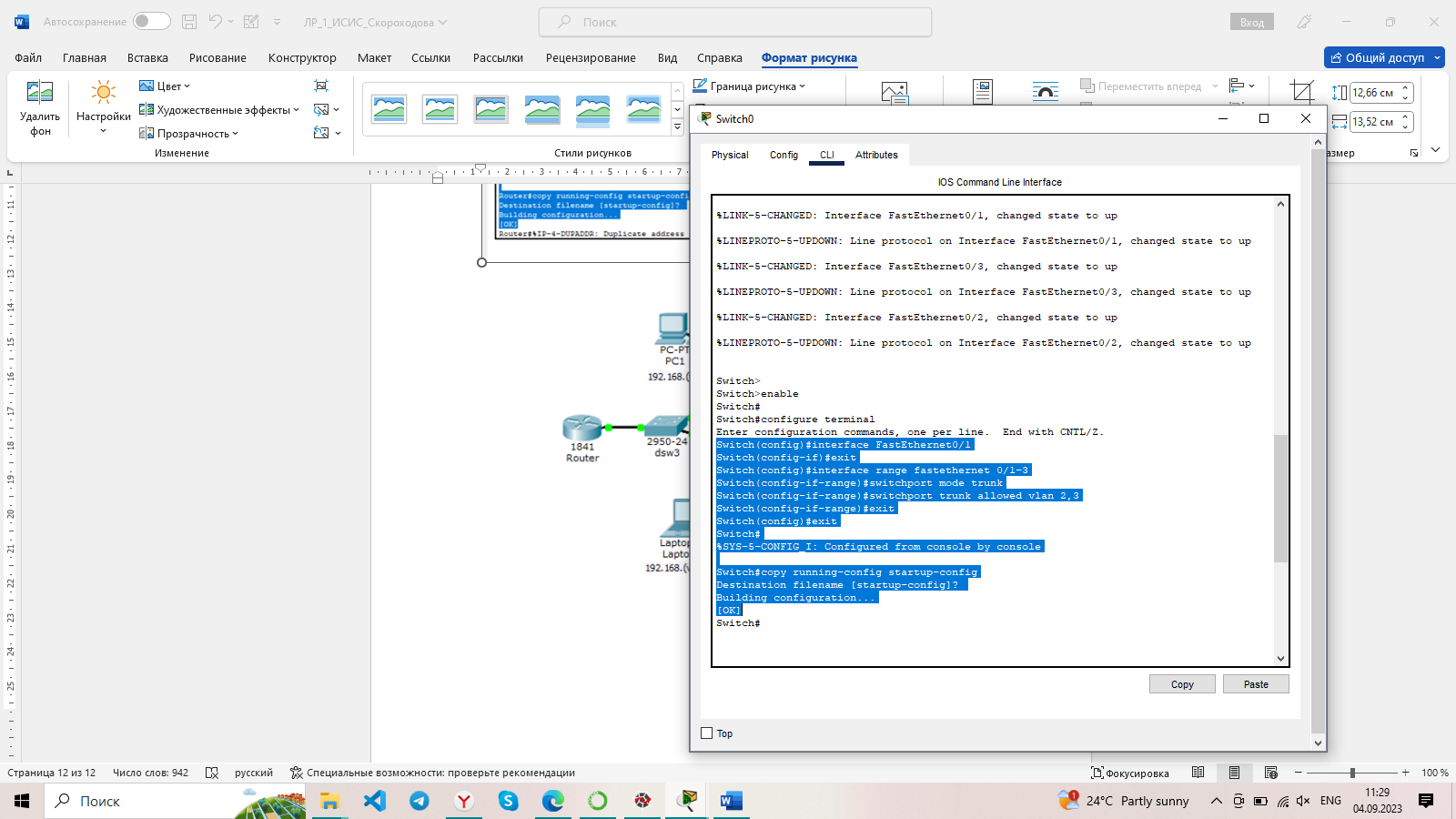


Рисунок 16 – Список команд на Switch0

Далее была проверена достижимость устройств, находящихся в разных VLAN. C устройства PC2, которое принадлежит к VLAN 3, были отправлены сообщения на PC3, принадлежащий VLAN 2. На рисунке 17 видно, что отправка сообщений прошла успешно.

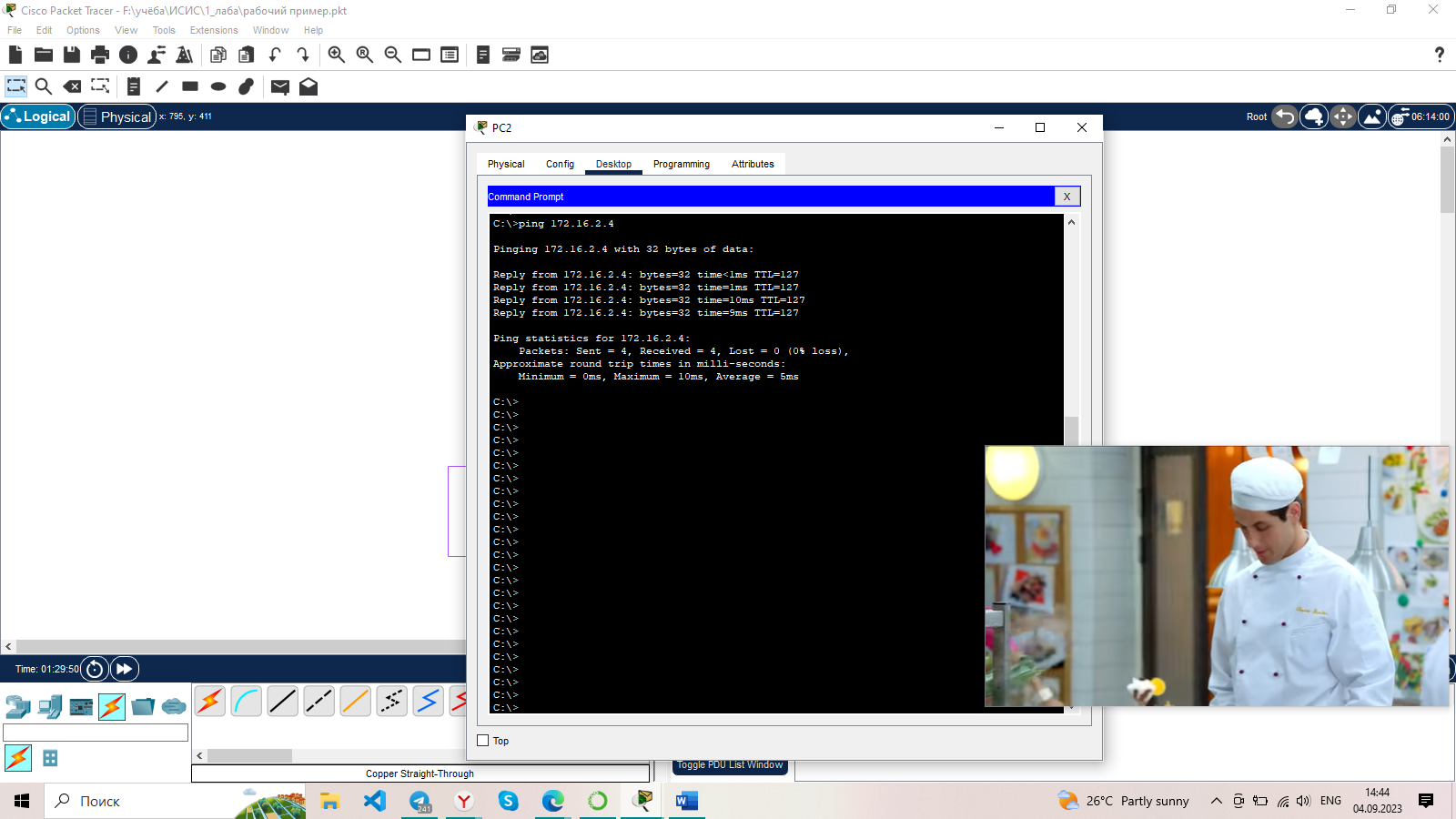


Рисунок 17 – Отправка сообщения с PC2 на PC3

Можно сделать вывод, что настройка маршрутизации между VLAN была произведена корректно, сеть работает исправно.

4. Выводы

В ходе лабораторной работы было проведено исследование принципов работы коммутаторов и виртуальных локальных сетей, способов конфигурации коммутаторов для построения виртуальных локальных сетей, произведено приобретение практических навыков конфигурации коммутаторов и исследования функционирования виртуальных сетей.

5. Контрольные вопросы

5.1. Что такое виртуальные локальные сети и зачем они применяются?

**Виртуальной локальной сетью** называется совокупность узлов (рабочих станций и серверов) некоторой компьютерной сети, трафик которой, в том числе широковещательный, на канальном уровне полностью изолирован от трафика других узлов этой сети. Основное назначение VLAN – недопущение трафика из одной сети в другую.

5.2. Зачем применяется разбиение сети на VLAN-ы?

Построение системы с использованием технологии VLAN позволяет уменьшить широковещательный трафик внутри сети, тем самым снижается нагрузка на сетевые устройства и улучшается производительность системы в целом. Улучшение безопасности – Устройства из разных подсетей VLAN не могут общаться друг с другом, что уменьшает шансы произвести несанкционированный доступ к устройствам системы.

5.3. Расскажите, как функционирует неуправляемый коммутатор после включения питания.

Неуправляемый коммутатор автоматически распределяет скорость и трафик между всеми клиентами сети. Неуправляемые коммутаторы широко используются в малых сетях с небольшим количеством (5-12) подключенных пользователей. Достоинством является простота в управлении и подключении.

5.4. Что означают понятия «агрегирование» и «зеркалирование» портов?

5.5. В чем состоит отличие портов доступа от магистральных (транковых) портов?

В коммутаторах имеется две разновидности портов: порты доступа (access port) и магистральные, транковые (trunk port) порты. Порт доступа принадлежит только одной виртуальной сети. Магистральный порт способен пропускать кадры многих VLAN. Чтобы коммутатор мог определить принадлежность кадра к определенной виртуальной сети, в заголовок кадра вставляется идентификатор ─ специальная метка (англ слово тег) с номером VLAN. Такой кадр называется тегированным (помеченным). Тег добавляется коммутатором к заголовку кадра при поступлении его от рабочей станции на порт коммутатора, а при передаче кадра компьютеру, приписанному к данной виртуальной сети, тег коммутатором изымается.

5.6. С какой целью в коммутационном оборудовании установлен консольный порт?

5.7. Как обеспечивает передача пакетов между изолированными виртуальными сетями?

5.8. В чем состоит суть процедуры interVLAN routing?

5.9. Сравните способы организации interVLAN routing?

Существует несколько способов организации interVLAN routing (маршрутизации между виртуальными локальными сетями). Рассмотрим и сравним два наиболее распространенных способа: маршрутизация на маршрутизаторе и маршрутизация на коммутаторе с поддержкой многоуровневых VLAN.

Маршрутизация на маршрутизаторе:

Преимущества:

Маршрутизатор предлагает больше гибкости и расширенных функций маршрутизации, таких как настройка более сложных маршрутизационных протоколов (например, OSPF, BGP) и применение политик маршрутизации.

Маршрутизатор может обеспечивать маршрутизацию между VLAN с использованием различных интерфейсов, включая физические порты и виртуальные интерфейсы.

Недостатки:

Возможно требуется дополнительное оборудование в виде маршрутизатора, что может быть дороже и сложнее в управлении.

Маршрутизация на маршрутизаторе может вносить задержки в процессе маршрутизации пакетов между VLAN.

Маршрутизация на коммутаторе с поддержкой многоуровневых VLAN:

Преимущества:

Маршрутизация выполняется на коммутаторе, что позволяет использовать одно устройство для коммутации и маршрутизации, что может быть более экономично и просто в управлении.

Маршрутизация внутри коммутатора обычно выполняется аппаратно, что обеспечивает более высокую производительность и меньшие задержки.

Недостатки:

Функциональность маршрутизации на коммутаторе может быть ограничена по сравнению с отдельным маршрутизатором. Некоторые продвинутые функции маршрутизации и маршрутизационные протоколы могут быть недоступны.

Маршрутизация на коммутаторе обычно ограничена определенным количеством VLAN или уровней многоуровневых VLAN.

Выбор между этими способами зависит от конкретных требований сети, бюджета и предпочтений администратора. Если требуются продвинутые функции маршрутизации или большая гибкость, маршрутизация на маршрутизаторе может быть предпочтительной. Если ценится простота в управлении и лучшая производительность, маршрутизация на коммутаторе может быть предпочтительной. В некоторых сценариях может быть целесообразно использовать комбинацию обоих методов для достижения оптимальных результатов.

5.10. С какой целью используется протокол VTP?

Протокол VTP (англ. VLAN Trunking Protocol) – это протокол, разработанный корпорацией Cisco, который используется для обмена информацией о виртуальных сетях VLAN. VTP помогает упрощать операции с VLAN'ами в организации – добавление, удаление, изменение параметров, а также оптимизирует трафик.

5.11. Поясните принцип работы протокола VTP?

Протокол VTP объединяет физически подключённые друг к другу коммутаторы в именованные области, называемые доменами VTP. В одной организации таких доменов может быть несколько. Только коммутаторы, относящиеся к одному и тому же сетевому домену, могут совместно использовать конфигурационную информацию о данной виртуальной сети.