Бюджетное учреждение высшего образования

Ханты-Мансийского автономного округа – Югры

«Сургутский государственный университет»

ОТЧЕТ

ПО ПРАКТИЧЕСКОЙ РАБОТЕ

ПО ДИСЦИПЛИНЕ:

СЕТИ И ТЕЛЕКОММУНИКАЦИИ

ПО ТЕМЕ:

4.5.2

Выполнил:

Студент группы 606-12

Демьянцев Виталий Владиславович

Проверил:

Жебель Владислав Александрович

Сургут 2024

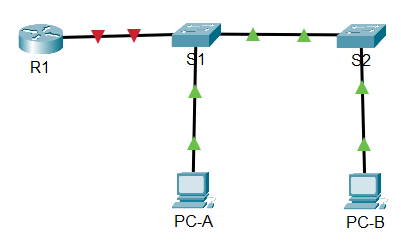
# Часть 1. Создание сети и настройка основных параметров устройства

В первой части лабораторной работы вам предстоит создать топологию сети и настроить базовые

параметры для узлов ПК и коммутаторов.

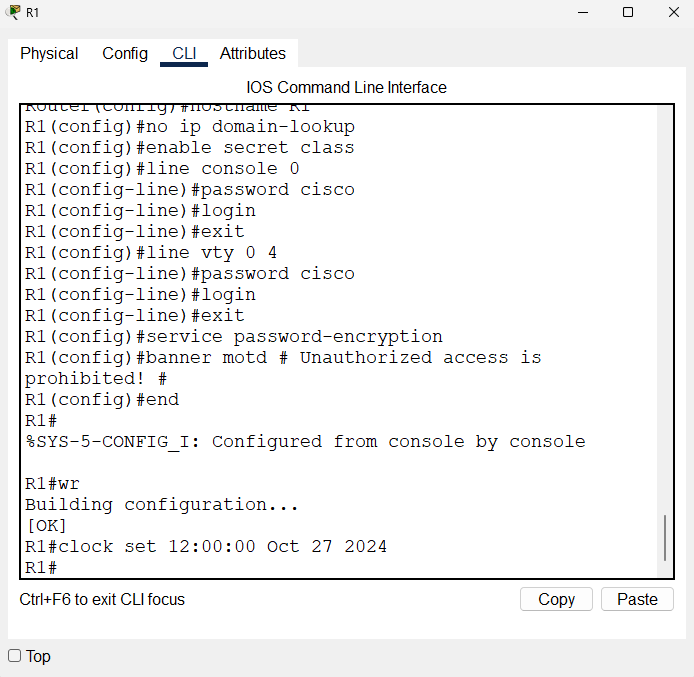
## Шаг 1. Создайте сеть согласно топологии.

Подключите устройства, как показано в топологии, и подсоедините необходимые кабели.



## Шаг 2. Настройте базовые параметры для маршрутизатора.

1. Подключитесь к маршрутизатору с помощью консоли и активируйте привилегированный режим EXEC.
2. Войдите в режим конфигурации.
3. Назначьте маршрутизатору имя устройства.
4. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.
5. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.
6. Назначьте cisco в качестве пароля консоли и включите вход в систему по паролю.
7. Установите cisco в качестве пароля виртуального терминала и активируйте вход.
8. Зашифруйте открытые пароли.
9. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.
10. Сохраните текущую конфигурацию в файл загрузочной конфигурации.
11. Настройте на маршрутизаторе время..
12. Закройте окно настройки.



## Шаг 3. Настройте базовые параметры каждого коммутатора.

a. Присвойте коммутатору имя устройства.

b. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

c. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.

d. Назначьте cisco в качестве пароля консоли и включите вход в систему по паролю.

e. Установите cisco в качестве пароля виртуального терминала и активируйте вход.

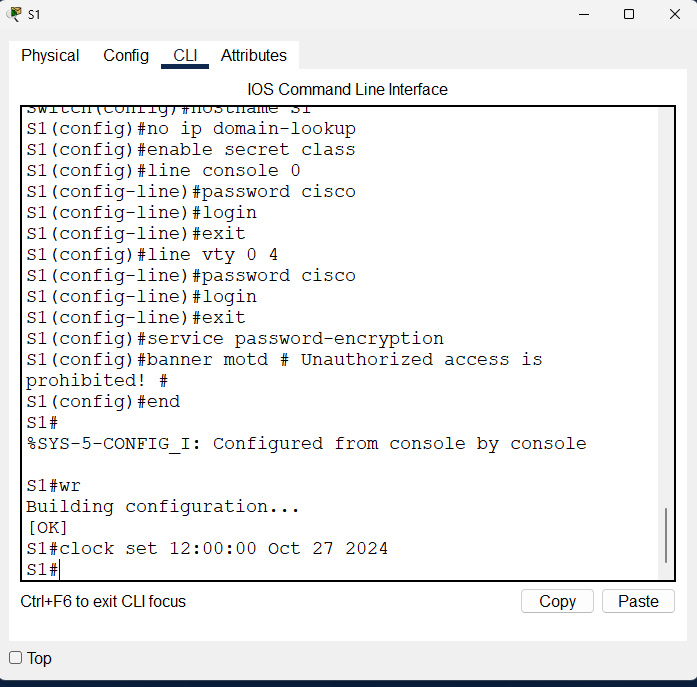
f. Зашифруйте открытые пароли.

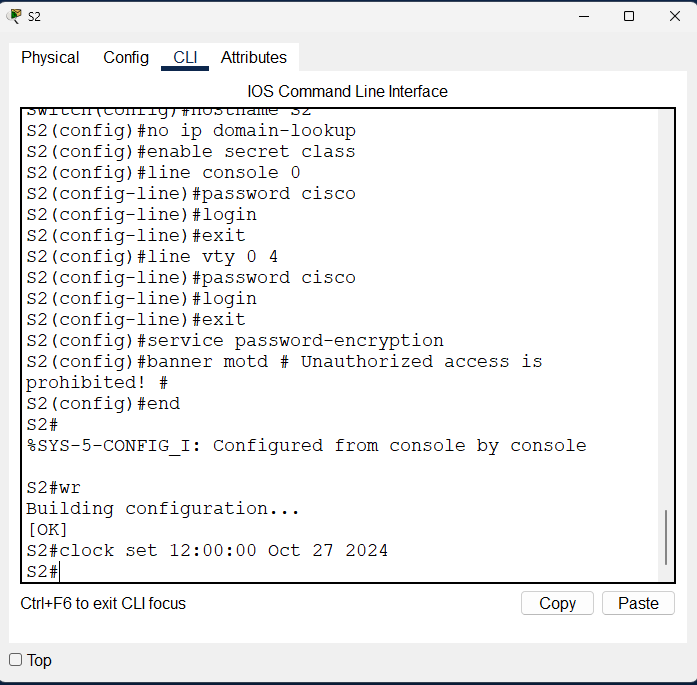
g. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.

h. Настройте на коммутаторах время.

i. Сохранение текущей конфигурации в качестве начальной.

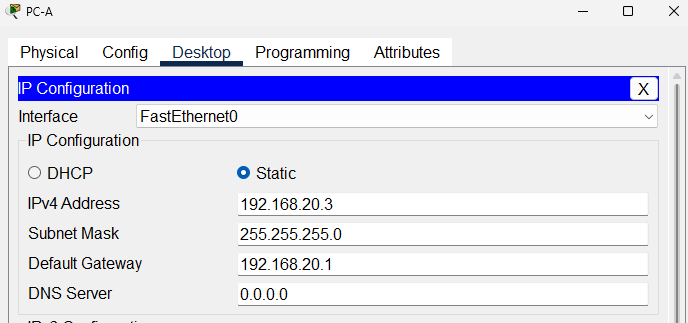
Закройте окно настройки.

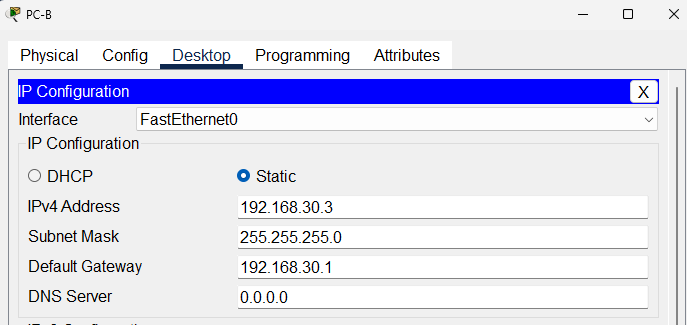




## Шаг 4. Настройте узлы ПК.

Адреса ПК можно посмотреть в таблице адресации.





# Часть 2. Создание сетей VLAN и назначение портов коммутатора

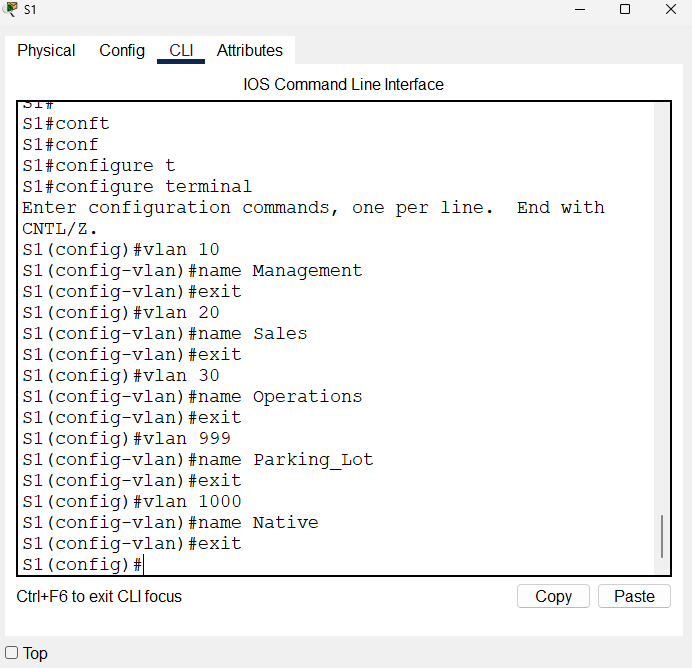
Во второй части вы создадите VLAN, как указано в таблице выше, на обоих коммутаторах. Затем вы

назначите VLAN соответствующему интерфейсу и проверите настройки конфигурации. Выполните

следующие задачи на каждом коммутаторе.

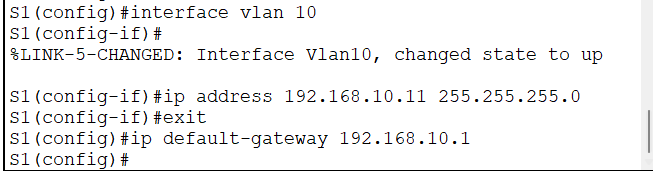
## Шаг 1. Создайте сети VLAN на коммутаторах.

a. Создайте и назовите необходимые VLAN на каждом коммутаторе из таблицы выше. Откройте окно конфигурации



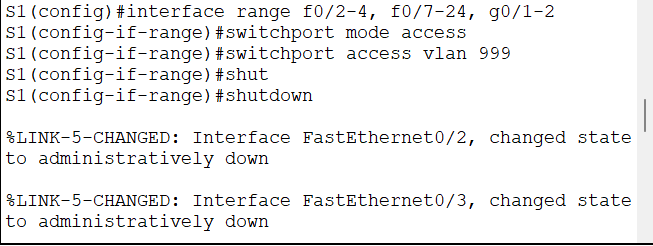
b. Настройте интерфейс управления и шлюз по умолчанию на каждом коммутаторе, используя

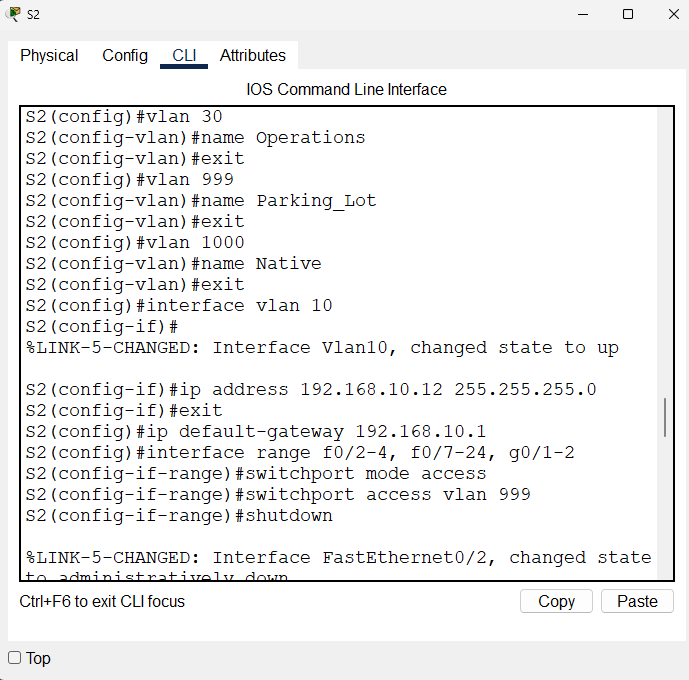
информацию об IP-адресе в таблице адресации.



c. Назначьте все неиспользуемые порты коммутатора VLAN Parking\_Lot, настройте их для

статического режима доступа и административно деактивируйте их.

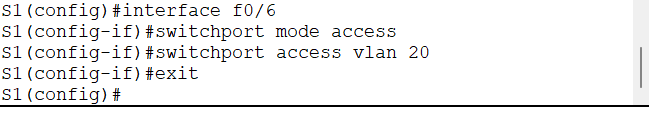


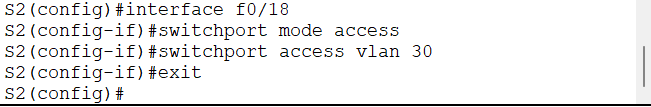


## Шаг 2. Назначьте сети VLAN соответствующим интерфейсам коммутатора.

a. Назначьте используемые порты соответствующей VLAN (указанной в таблице VLAN выше) и

настройте их для режима статического доступа.





b. Убедитесь, что VLAN назначены на правильные интерфейсы.

# Часть 3. Конфигурация магистрального канала стандарта 802.1Q между коммутаторами

## Шаг 1. Вручную настройте магистральный интерфейс F0/1 на коммутаторах S1 и S2.

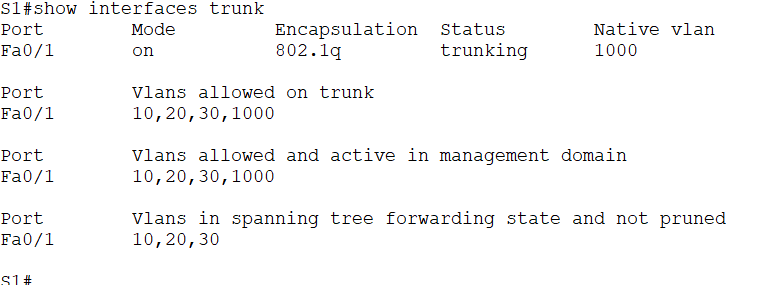
a. Настройка статического транкинга на интерфейсе F0/1 для обоих коммутаторов.

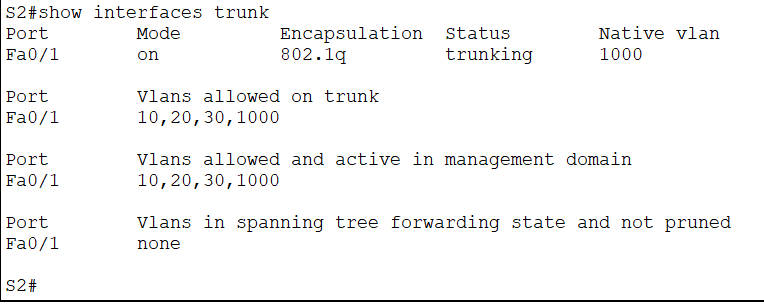
Откройте окно конфигурации

b. Установите native VLAN 1000 на обоих коммутаторах.

c. Укажите, что VLAN 10, 20, 30 и 1000 могут проходить по транку.

d. Проверьте транки, native VLAN и разрешенные VLAN через транк.



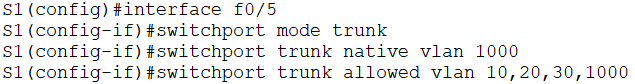


## Шаг 2. Вручную настройте магистральный интерфейс F0/5 на коммутаторе S1.

a. Настройте интерфейс S1 F0/5 с теми же параметрами транка, что и F0/1. Это транк до

маршрутизатора.

b. Сохраните текущую конфигурацию в файл загрузочной конфигурации.



c. Проверка транкинга.

Вопрос:

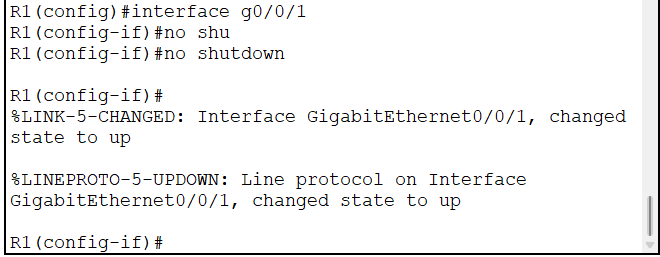
Что произойдет, если G0/0/1 на R1 будет отключен?

# Часть 4. Настройка маршрутизации между сетями VLAN

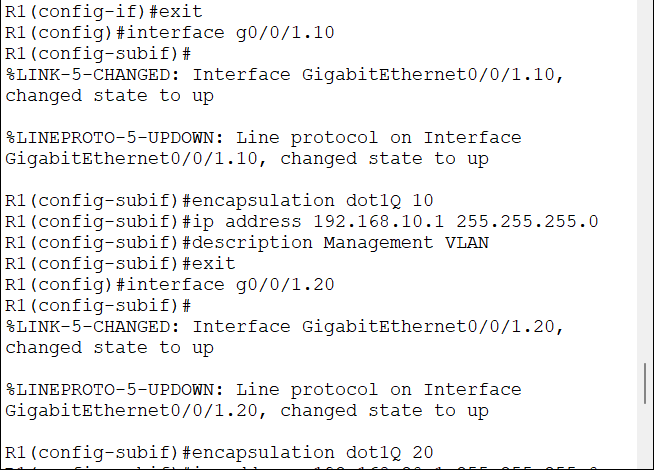
## Шаг 1. Настройте маршрутизатор.

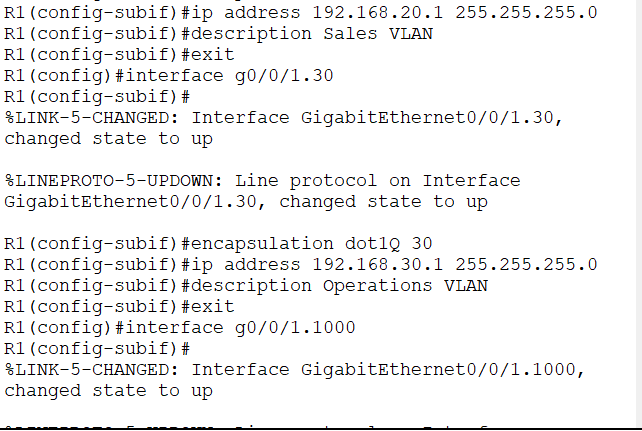
Откройте окно конфигурации

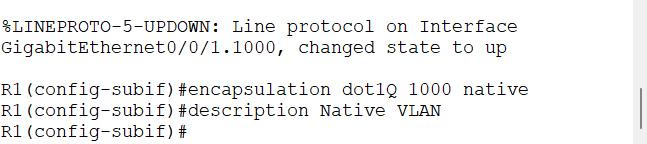
1. При необходимости активируйте интерфейс G0/0/1 на маршрутизаторе.



1. Настройте подинтерфейсы для каждой VLAN, как указано в таблице IP-адресации. Все подинтерфейсы используют инкапсуляцию 802.1Q. Убедитесь, что подинтерфейсу для native VLAN не назначен IP-адрес. Включите описание для каждого подинтерфейса.







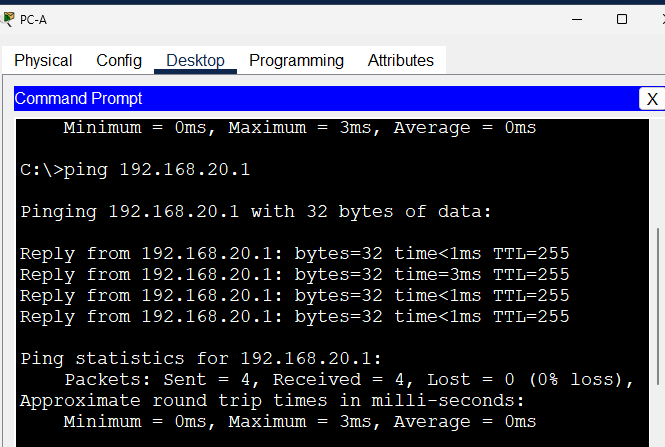
1. Убедитесь, что вспомогательные интерфейсы работают

# Часть 5. Проверьте, работает ли маршрутизация между VLAN

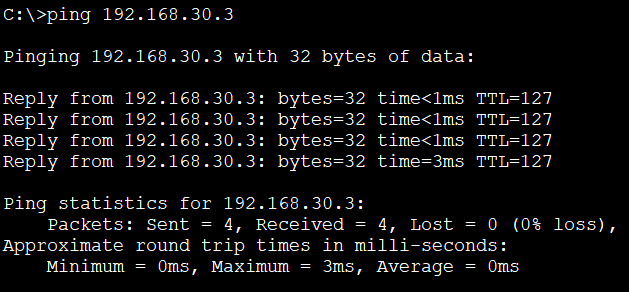
## Шаг 1. Выполните следующие тесты с PC-A. Все должно быть успешно.

Примечание. Возможно, вам придется отключить брандмауэр ПК для работы ping

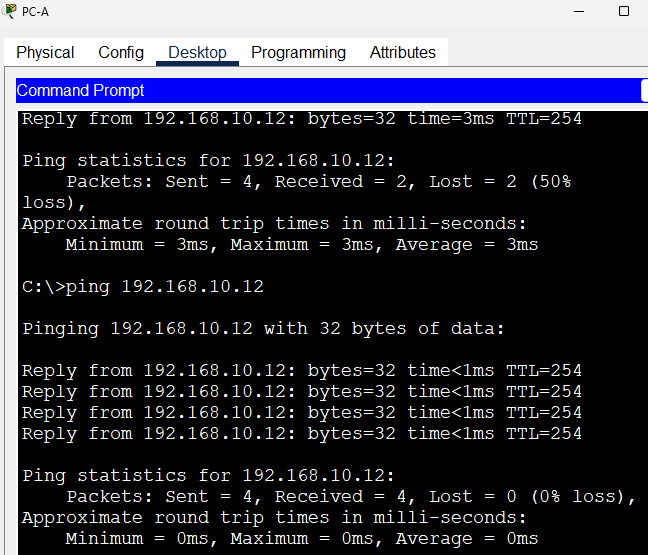
1. Отправьте эхо-запрос с PC-A на шлюз по умолчанию.



1. Отправьте эхо-запрос с PC-A на PC-B.



1. Отправьте команду ping с компьютера PC-A на коммутатор S2.



## Шаг 2. Пройдите следующий тест с PC-B

В окне командной строки на PC-B выполните команду tracert на адрес PC-A.

Вопрос:

Какие промежуточные IP-адреса отображаются в результатах?

