Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина» (УрФУ)

Институт радиоэлектроники и информационных технологий – РтФ

Школа профессионального и академического образования

Отчет по дисциплине   
«Безопасность компьютерных сетей»

Лабораторная работа №5  
«Защита коммутаторов 2-го уровня»

Студенты: Клоченко И.Е., Юсупов Д.А.

Преподаватель: Ваулин С.С.

Группа: РИ-300024

Екатеринбург

2023

**Оглавление**

[1. Настройка базовых параметров коммутатора 3](#_Toc136207414)

[2. Настройка доступа к коммутатору по SSH 4](#_Toc136207415)

[3. Настройка защищенных магистральных каналов и портов доступа 7](#_Toc136207416)

[4. Настройка IP DHCP Snooping 17](#_Toc136207417)

[Вывод 23](#_Toc136207418)

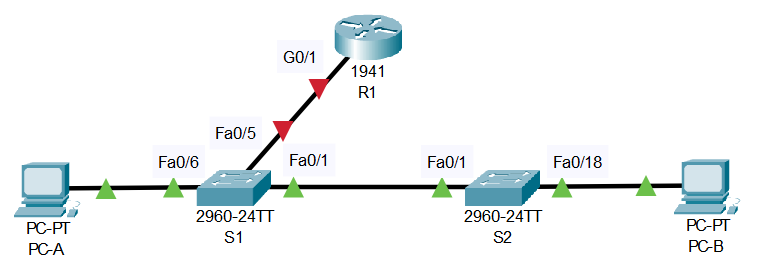
**Цель работы:**

Знакомство с опциями *Cisco* *Packet* *Tracer*, которые обеспечивают безопасность и предназначены для различных функций и протоколов защиты коммутаторов.

**Ход работы:**

## Настройка базовых параметров коммутатора

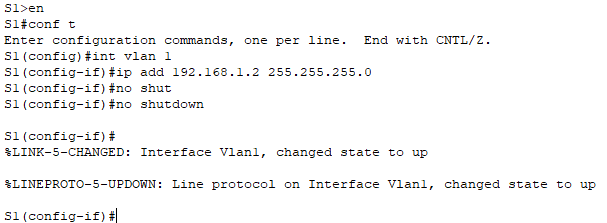
* 1. Собираем топологию сети.



**Рисунок 1**. Топология сети

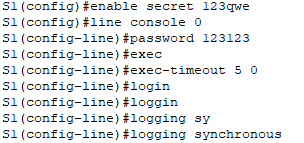
* 1. Настраиваем имена хостов, *IP*-адрес и пароли для доступа.

Для присвоения *IP*-адреса коммутаторам, необходимо использовать *VLAN* (*VLAN* 1) на каждом из них.



**Рисунок 2**. Присвоение IP адреса коммутатору S1

Далее настраиваем пароль для привилегированного режима и пароль для консоли.



**Рисунок 3**. Установка пароля для привилегированного режима и пароля для консоли

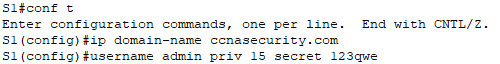
Аналогичные действия проводим на коммутаторе *S*2.

После настройки всех устройств в сети проверяем связь отправляя *ICMP* пакеты с *PC*-*A* на *R*1 и с *PC*-*A* на *PC*-*B*. Все успешно.

## Настройка доступа к коммутатору по SSH

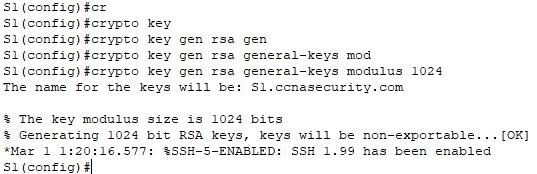
Выполняем настройку на коммутаторе *S*1. Настройка на коммутаторе *S*2 производится аналогичным образом.

* 1. Настраиваем доменное имя и привилегированного пользователя для входа через *SSH*-клиент.



**Рисунок 4**. Настройка доменного имени и привилегированного пользователя для входа по SSH

* 1. Генерируем пару ключей шифрования *RSA* для коммутатора.



**Рисунок 5**. Генерация пары ключей шифрования RSA для коммутатора S1

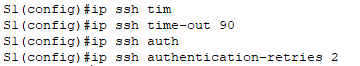
Включаем *SSH* версии 2 с помощью команды «*ip* *ssh* *version* 2» в режиме глобальной конфигурации.

Таким образом в выводе команды «*show* *ip* *ssh*» в привилегированном режиме будет следующий вывод:



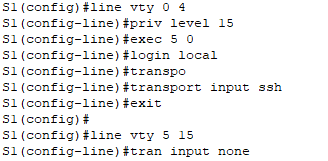
**Рисунок 6**. Вывод информации о SSH

* 1. Настраиваем время ожидания *SSH* и параметры аутентификации.



**Рисунок 7**. Настройка времени ожидания параметров аутентификации

* 1. Настраиваем входящие линии *vty*.

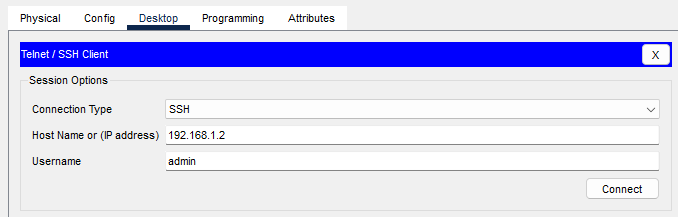


**Рисунок 8**. Настройка линий vty

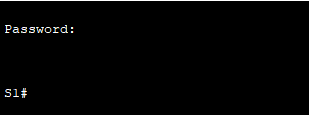
* 1. Настройка *SSH* клиента.

Так как *SSH* клиент уже установлен на *PC*-*A* и *PC*-*B*, процесс настройки пропускается.

* 1. Вход с *PC*-*A* на коммутатор *S*1 по *SSH*.



**Рисунок 9**. Вход по SSH (указание IP адреса и имени пользователя)



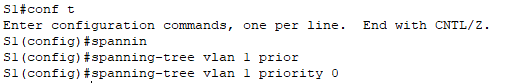
**Рисунок 10**. Вход по SSH (ввод пароля)

Вход успешно выполнен под именем пользователя *admin*. Если попытаться войти, используя *Telnet*, у нас ничего не получится, потому что ранее мы настроили подключение только по *SSH* на коммутаторе *S*1.

## Настройка защищенных магистральных каналов и портов доступа

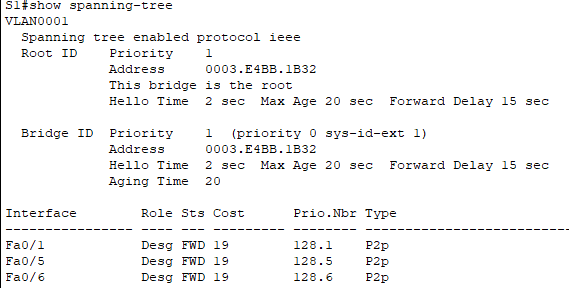
* 1. Защита магистральных портов

Настраиваем *S*1 в качестве корневого коммутатора. Устанавливаем для коммутатора *S*1 приоритет 0, чтобы он стал корневым коммутатором.



**Рисунок 11**. Установка приоритета для S1

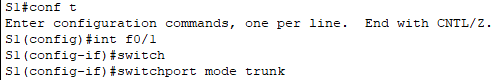
Проверяем, что коммутатор *S*1 стал корневым мостом, определяем используемые порты и их состояние.



**Рисунок 12**. Проверка информации spanning-tree

Порты *Fa*0/1,5,6 находятся в состоянии *FWD* (*Forward*), что означает обычное состояние порта, в котором отправляются и пакеты *BPDU*, и кадры с обычными данными.

Настраиваем порт *Fa*0/1 на *S*1 в качестве магистрального.



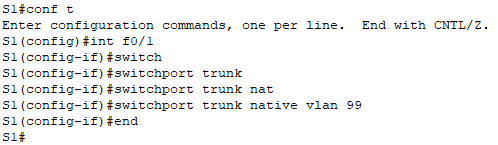
**Рисунок 13**. Настройка порта в качестве магистрального

Повторяем для коммутатора *S*2.

Убеждаемся, что порт *F*0/1 на коммутаторе *S*1 работает в магистральном (транкинговом) режиме.

Сейчас в качестве нативной *VLAN* используется *VLAN* 1.

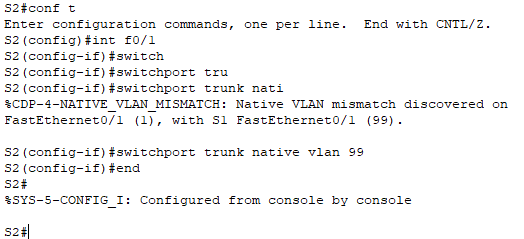
Установим в качестве нативной *VLAN* для интерфейса *F*0/1 коммутатора *S*1 неиспользуемую сеть *VLAN* 99.



**Рисунок 14**. Установка неиспользуемой VLAN в качестве нативного (S1)

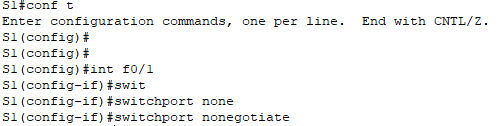
Сообщение «%*CDP*-4-*NATIVE\_VLAN\_MISMATCH*: *Native* *VLAN* *mismatch* *discovered* *on* *FastEthernet*0/1 (99), *with* *S*2 *FastEthernet*0/1 (1).» говорит о разнице *VLAN* на *S*1 (99) и *S*2 (1).

Установим в качестве нативной *VLAN* на магистральном интерфейсе *F*0/1 коммутатора *S*2 сеть *VLAN* 99.



**Рисунок 15**. Установка неиспользуемого VLAN в качестве нативного (S2)

Предотвращение использования *DTP* на коммутаторах *S*1 и *S*2.



**Рисунок 16**. Предотвращение использования DTP на коммутаторе S1

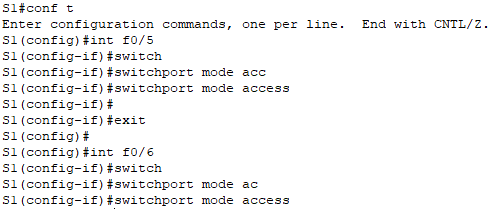
Аналогично на *S*2.

Проверяем вывод информации команды «*show* *interfaces* *f*0/1 *switchport*» на наличие строки «*Negotiation* *of* *Trunking*: *Off*».

Такая строка есть.

* 1. Защита портов доступа

Отключаем транкинг на портах доступа коммутатора *S*1.

****

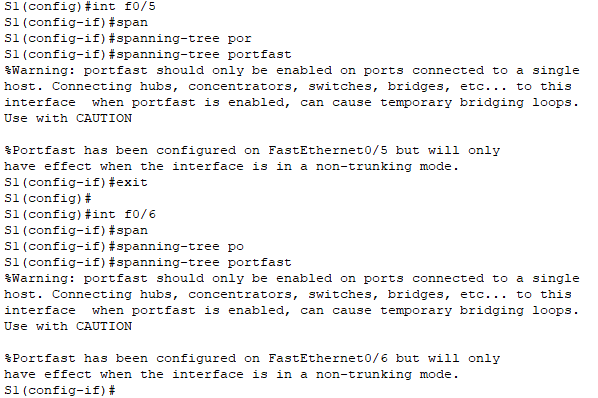
**Рисунок 17**. Отключение транкинга на портах доступа коммутатора S1

Порты доступа здесь это *f*0/5 и *f*0/6, к которым подключены *PC*-*A* и *R*1 соответственно.

Для коммутатора *S*2 аналогично (порт *f*0/18 – *PC*-*B*).

* 1. Защита от атак на *STP*

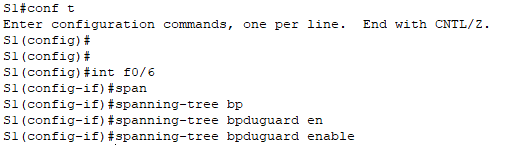
Включаем *PostFast* на портах доступа коммутаторов *S*1 и *S*2.



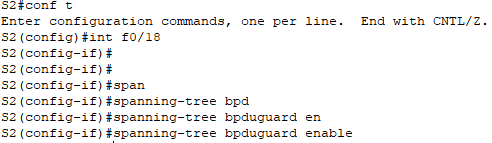
**Рисунок 18**. Включение PostFast на портах доступа S1

Аналогично для *S*2 (порт *f*0/18).

Включаем функцию *BPDU* *Guard* на порте *f*0/6 (*S*1 - *PC*-*A*) и *f*0/18 (*S*2 - *PC*-*B*).



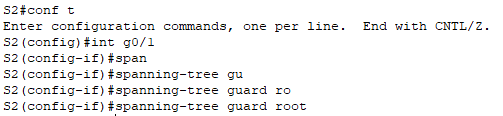
**Рисунок 19**. Включение BPDU Guard (S1)



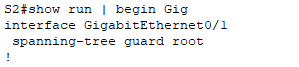
**Рисунок 20**. Включение BPDU Guard (S2)

Убедимся, что функция *BPDU* *Guard* включена. Функция включена.

Включаем *Root* *Guard* на *S*2.

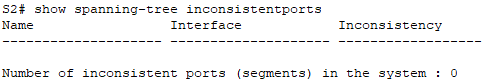


**Рисунок 21**. Включение Root Guard на S2



**Рисунок 22**. Проверка включенности функции Root Guard

Определим наличие портов, которые в настоящее время получают *BPDU* пакеты более высокого уровня.

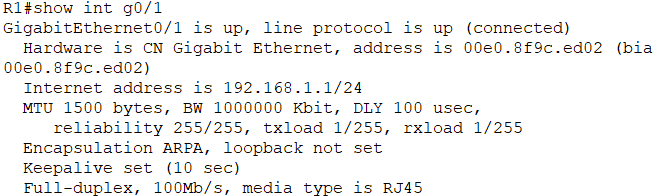


**Рисунок 23**. Порты, получающие BPDU пакеты более высокого уровня

*Loop* *Guard* включить не получилось, *CLI* ругается на команды.

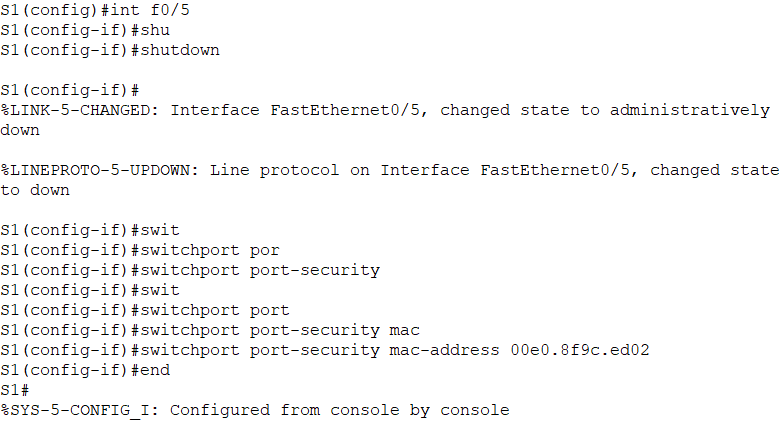
* 1. Настройка безопасности портов и отключение неиспользуемых портов.

Просмотрим *MAC*-адрес интерфейса *g*0/1 маршрутизатора *R*1.



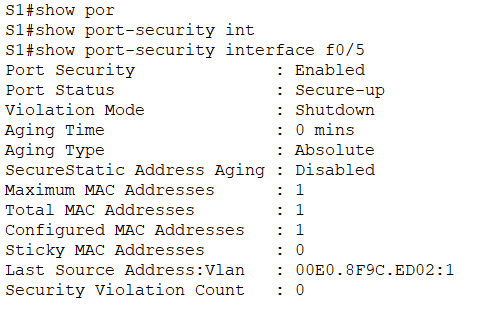
**Рисунок 24**. MAC-адрес интерфейса g0/1 маршрутизатора R1

Настраиваем базовый уровень безопасности портов доступа (*f*0/5, *f*0/6 – *S*1, *f*0/18 – *S*2).



**Рисунок 25**. Настройка базового уровня безопасности порта f0/5 (S1)

Проверяем, что безопасность портов настроена на интерфейсе *f*0/5.

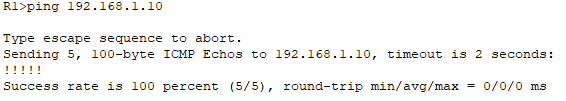


**Рисунок 26**. Проверка работы port-security

Аналогично для второго порта доступа *S*1 и порта доступа для *S*2

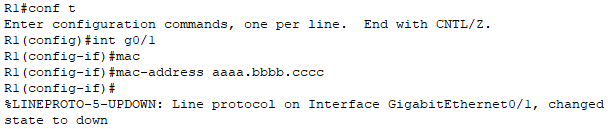
Состояние портов после настройки – *Secure*-*up*, что дословно переводится как «Защита поднята».

В *CLI* маршрутизатора *R*1 выполняем эхо-тестирование *PC*-*A*.



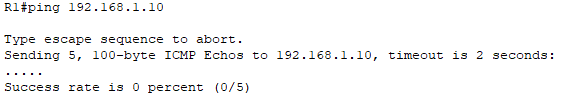
**Рисунок 27**. Успешное эхо-тестирование PC-A

Теперь нарушим правило безопасности: изменим *MAC*-адрес интерфейса маршрутизатора. Войдем в режим интерфейсной настройки для *Fast* *Ethernet* 0/1.



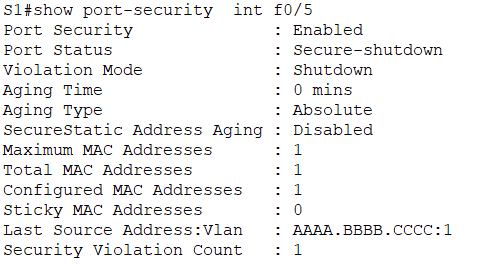
**Рисунок 28**. Изменение MAC-адреса на интерфейсе G0/1 для R1

Выполняем эхо-тестирование *PC*-*A* с *R*1.



**Рисунок 29**. Неудачное эхо тестирование PC-A

Убедимся, что безопасность портов была нарушена.

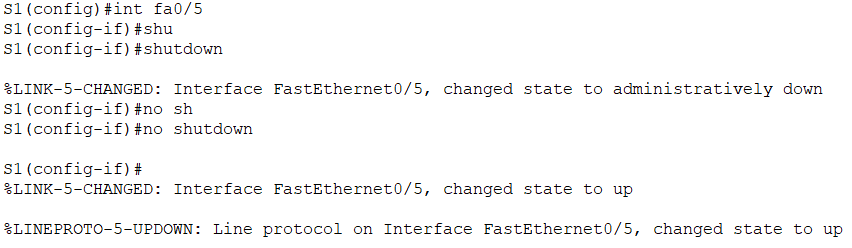


**Рисунок 30**. Проверка нарушения безопасности портов

Удаляем жестко закодированный *MAC*-адрес из маршрутизатора и снова включаем порт.

Выполняем эхо-тестирование *PC*-*A* с *R*1. Оно безуспешное, потому что порт принял состояние «*error* *disabled*».

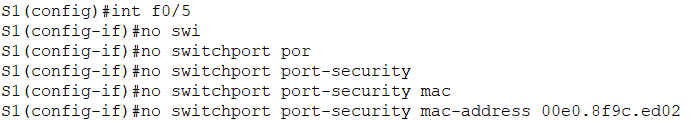
Сбрасываем состояние «*error* *disabled*» порта *Fa*0/5 коммутатора *S*1.



**Рисунок 31**. Сброс состояния «error disabled» на S1

Снова выполняем эхо-тестирование и в этот раз оно успешно.

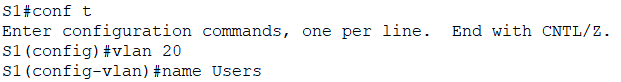
Удаляем базовую безопасность портов на порте *Fa*0/5 коммутатора *S*1.



**Рисунок 32**. Удаление базовой безопасности портов на порте Fa0/5 коммутатора S1

Отключаем неиспользуемые порты на *S*1 (*f*0/2-4, *f*0/7-24, *g*0/1-2) и *S*2 (*f*0/2-17, *f*0/19-24, *g*0/1-2).

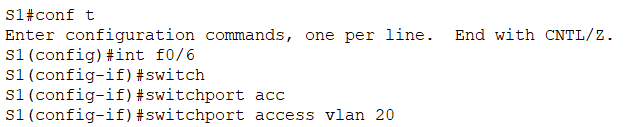
Перемещаем активные порты в сеть *VLAN*, отличную от *VLAN* 1. Настроим базовую *VLAN* для пользователей на *S*1 и *S*2.



**Рисунок 33**. Настройка VLAN 20 для Users на S1

Аналогично для *S*2.

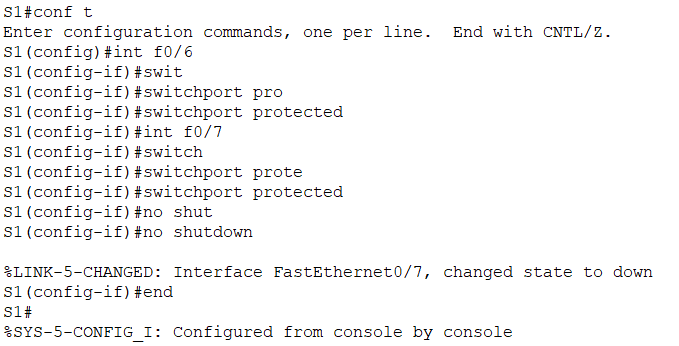
Добавляем текущие активные порты доступа (не магистральные) в новую *VLAN* 20.



**Рисунок 34**. Добавление текущих портов доступа в новую VLAN 20

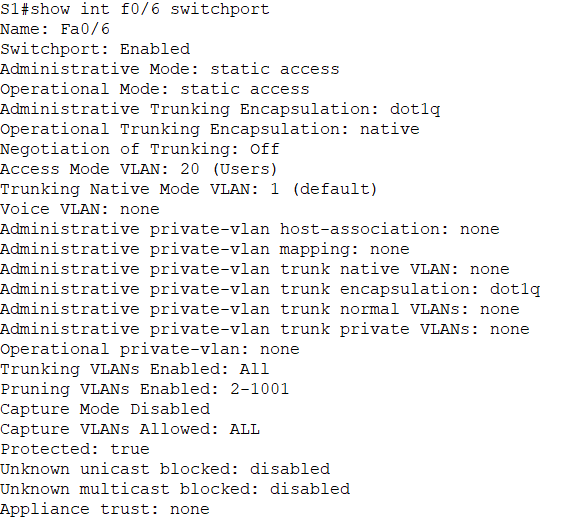
Аналогично для *S*2.

Настраиваем порт с функцией *PVLAN* *Edge*.



**Рисунок 35**. Настройка порта с функцией PVLAN Edge

Убедимся, что функция *PVLAN* *Edge* включена на порту *Fa*0/6.



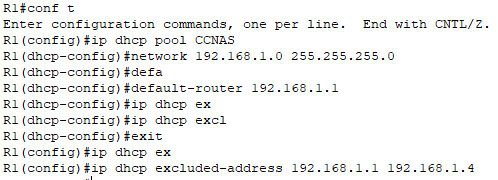
**Рисунок 36**. Проверка работы PVLAN Edge на порту Fa0/6

Деактивируем защищенный порт на интерфейсах *Fa*0/6 и *Fa*0/7.

## Настройка IP DHCP Snooping

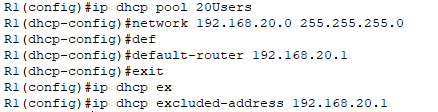
* 1. Настройка *DHCP*

Настроим *DHCP* на маршрутизаторе *R*1 для *VLAN* 1.



**Рисунок 37**. Настройка DHCP на R1 для VLAN 1\

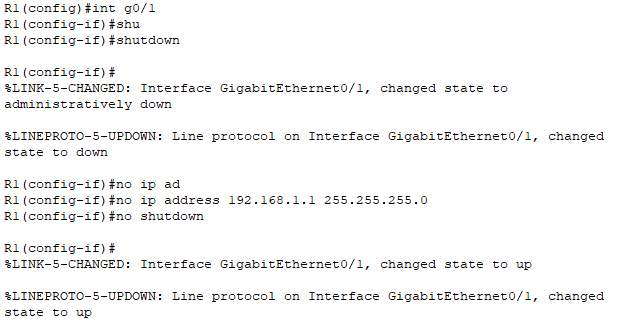
Настраиваем *DHCP* для *VLAN* 20 на *R*1.



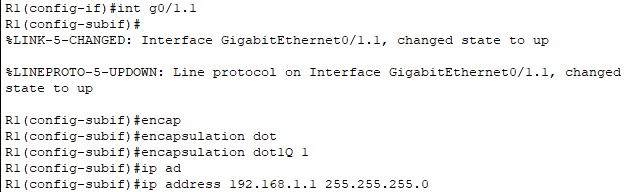
**Рисунок 38**. Настройка DHCP для VLAN 20 на R1

* 1. Настройка связи между сетями *VLAN*

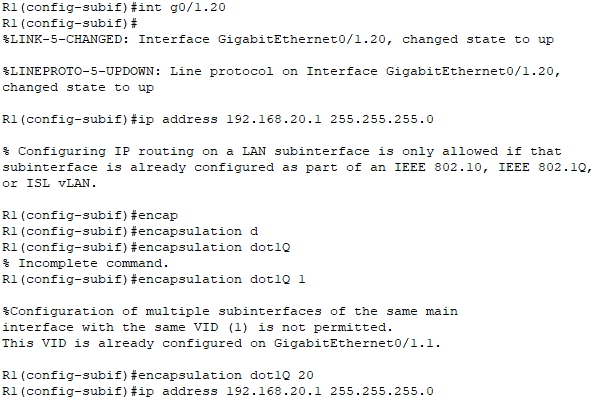
Настроим субинтерфейсы на маршрутизаторе *R*1.



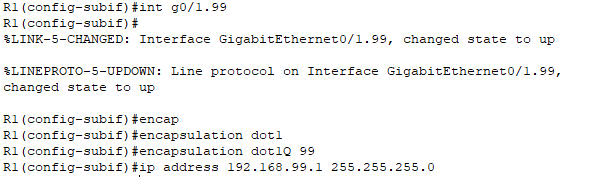
**Рисунок 39**. Удаление статической адресации



**Рисунок 40**. Создание субинтерфейса для VLAN 1

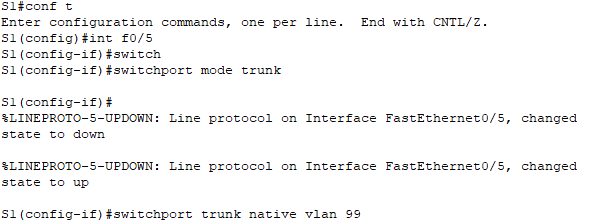


**Рисунок 41**. Создание субинтерфейса для VLAN 20



**Рисунок 42**. Создание субинтерфейса для VLAN 99

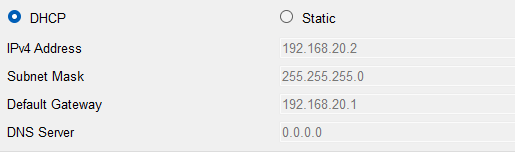
Настраиваем интерфейс *Fa*0/5 коммутатора *S*1 в качестве магистрального порта.



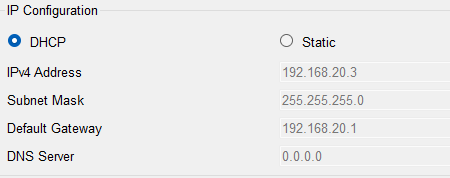
**Рисунок 43**. Настройка порта Fa0/5 в качестве магистрального

Сменим настройки на *PC*-*A* и *PC*-*B* со статической адресации на динамическую адресацию.

Проверяем функциональность *DHCP*.



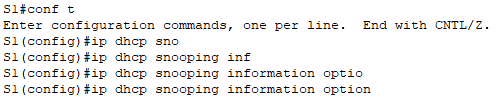
**Рисунок 44**. Сетевая конфигурация PC-A



**Рисунок 45**. Сетевая конфигурация PC-B

* 1. Настройка *DHCP* *Snooping*

Включаем глобально функцию *DHCP* *Snooping*.



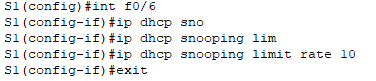
**Рисунок 46**. Включение DHCP Snooping

Включаем *DHCP* *Snooping* для *VLAN* 1,20.



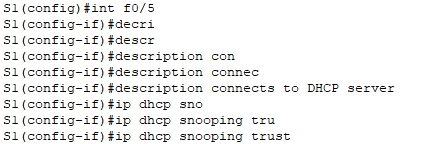
**Рисунок 47**. Включение DHCP Snooping для VLAN 1,20

Ограничиваем число *DHCP*-запросов на интерфейсе.



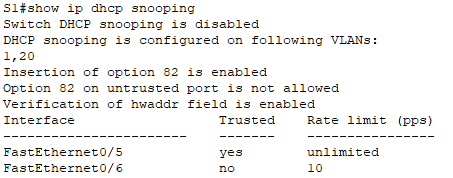
**Рисунок 48**. Ограничение числа DHCP-запросов на интерфейсе до 10

Определяем доверенные интерфейсы. Ответы *DHCP* разрешены только через доверенные порты.



**Рисунок 49**. Определение доверенных интерфейсов

Проверяем конфигурацию *DHCP* *Snooping*.



**Рисунок 50**. Проверка конфигурации DHCP Snooping

## Вывод

В ходе выполнения лабораторной работы ознакомились с защитными функциями и методами для коммутатора 2 уровня.

Настроены базовые параметры коммутаторов, маршрутизатора и оконечных устройств.

Проведена настройка доступа к коммутаторам по *SSH*.*\*

Проведена настройка защищенных магистральных каналов и портов доступа (настроены *PortFast*, *BPDU* *Guard*, *Root* *Guard*, *PVLAN* *Edge*).

Произведена настройка *DHCP* *Snooping*.