Бюджетное учреждение высшего образования

Ханты-Мансийского автономного округа – Югры

«Сургутский государственный университет»

ОТЧЕТ

ПО ПРАКТИЧЕСКОЙ РАБОТЕ

ПО ДИСЦИПЛИНЕ:

СЕТИ И ТЕЛЕКОММУНИКАЦИИ

ПО ТЕМЕ:

11.6.2

Выполнил:

Студент группы 606-12

Демьянцев Виталий Владиславович

Проверил:

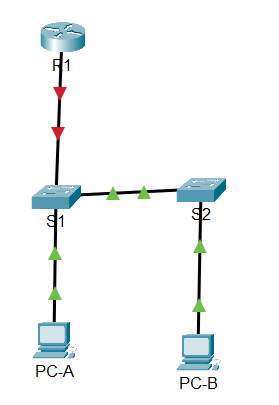
Жебель Владислав Александрович

Сургут 2024

# Часть 1. Настройка основного сетевого устройства

## Шаг 1. Создайте сеть.

a. Создайте сеть согласно топологии.



b. Инициализация устройств

## Шаг 2. Настройте маршрутизатор R1.

a. Загрузите следующий конфигурационный скрипт на R1.

Откройте окно конфигурации

enable

configure terminal

hostname R1

no ip domain lookup

ip dhcp excluded-address 192.168.10.1 192.168.10.9

ip dhcp excluded-address 192.168.10.201 192.168.10.202

!

ip dhcp pool Students

network 192.168.10.0 255.255.255.0

default-router 192.168.10.1

domain-name CCNA2.Lab-11.6.1

!

interface Loopback0

ip address 10.10.1.1 255.255.255.0

!

interface GigabitEthernet0/0/1

description Link to S1

ip dhcp relay information trusted

ip address 192.168.10.1 255.255.255.0

no shutdown

!

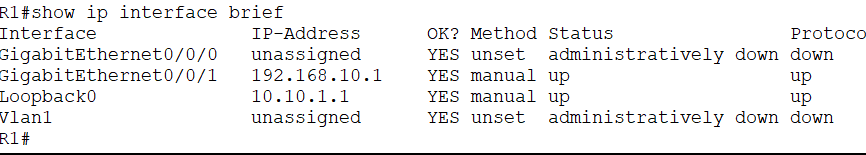
line con 0

logging synchronous

exec-timeout 0 0

b. Проверьте текущую конфигурацию на R1, используя следующую команду:

R1# show ip interface brief



c. Убедитесь, что IP-адресация и интерфейсы находятся в состоянии up / up (при необходимости

устраните неполадки).

## Шаг 3. Настройка и проверка основных параметров коммутатора

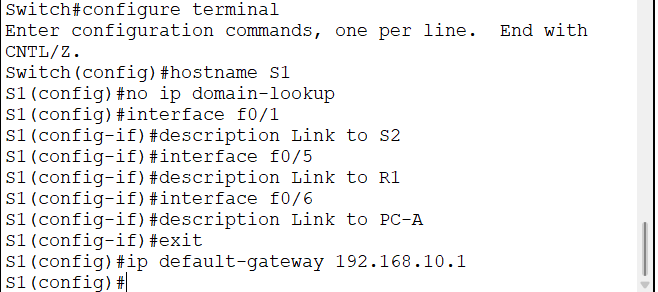
a. Настройте имя хоста для коммутаторов S1 и S2.

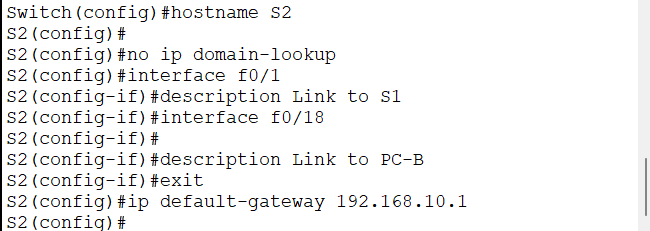
b. Запретите нежелательный поиск в DNS.

c. Настройте описания интерфейса для портов, которые используются в S1 и S2.

d. Установите для шлюза по умолчанию для VLAN управления значение 192.168.10.1 на обоих

коммутаторах.





# Часть 2. Настройка сетей VLAN на коммутаторах.

## Шаг 1. Сконфигруриуйте VLAN 10.

Добавьте VLAN 10 на S1 и S2 и назовите VLAN - Management.





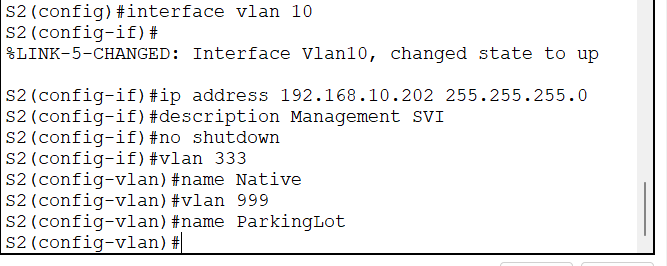
## Шаг 2. Сконфигруриуйте SVI для VLAN 10.

Настройте IP-адрес в соответствии с таблицей адресации для SVI для VLAN 10 на S1 и S2. Включите

интерфейсы SVI и предоставьте описание для интерфейса.

## Шаг 3. Настройте VLAN 333 с именем Native на S1 и S2.

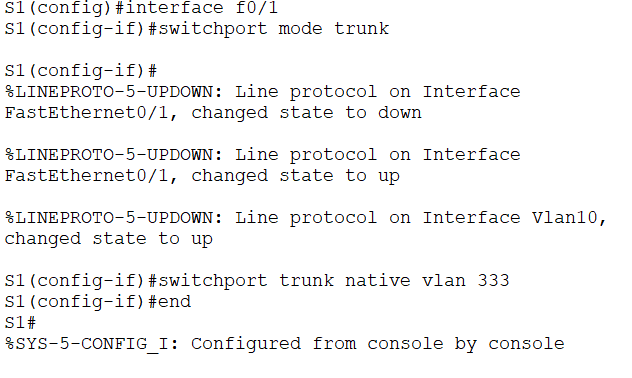
## Шаг 4. Настройте VLAN 999 с именем ParkingLot на S1 и S2.



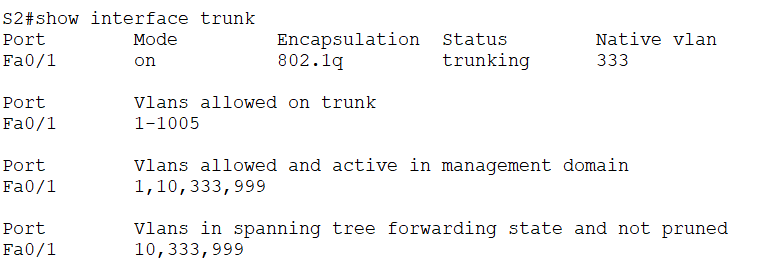
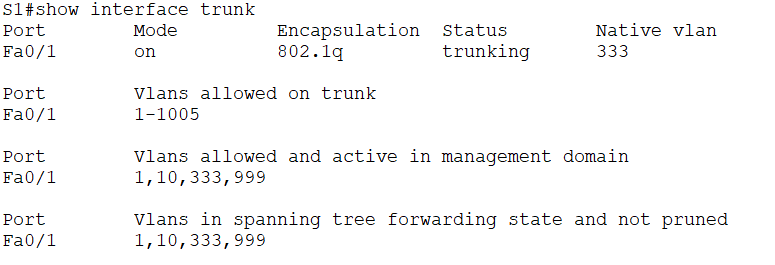
# Часть 3. Настройки безопасности коммутатора.

## Шаг 1. Релизация магистральных соединений 802.1Q.

a. Настройте все магистральные порты Fa0/1 на обоих коммутаторах для использования VLAN 333 в качестве native VLAN.



b. Убедитесь, что режим транкинга успешно настроен на всех коммутаторах.



S1# show interface trunk

Port Mode Encapsulation Status Native vlan

Fa0/1 on 802.1q trunking 333

Port Vlans allowed on trunk

Fa0/1 1-4094

Port Vlans allowed and active in management domain

Fa0/1 1,10,333,999

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1 1,10,333,999

S2# show interface trunk

Port Mode Encapsulation Status Native vlan

Fa0/1 on 802.1q trunking 333

Port Vlans allowed on trunk

Fa0/1 1-4094

Port Vlans allowed and active in management domain

Fa0/1 1,10,333,999

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1 1,10,333,999

c. Отключить согласование DTP F0/1 на S1 и S2.

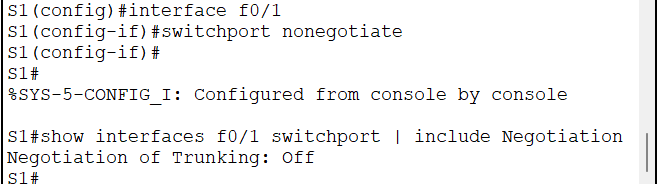
d. Проверьте с помощью команды show interfaces.

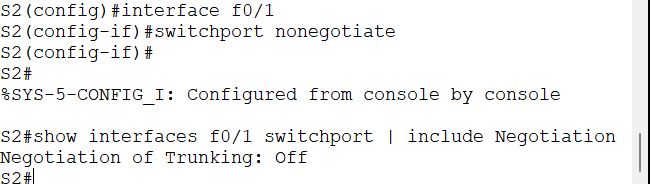
S1# show interfaces f0/1 switchport | include Negotiation

Negotiation of Trunking: Off

S1# show interfaces f0/1 switchport | include Negotiation

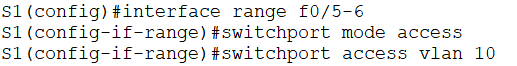
Negotiation of Trunking: Off



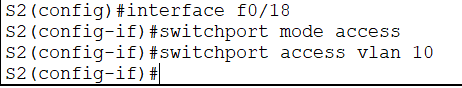


## Шаг 2. Настройка портов доступа

a. На S1 настройте F0/5 и F0/6 в качестве портов доступа и свяжите их с VLAN 10.

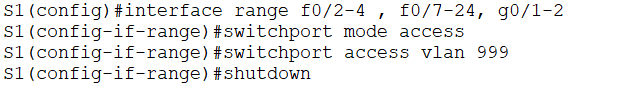


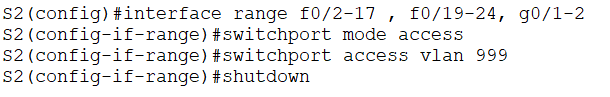
b. На S2 настройте порт доступа Fa0/18 и свяжите его с VLAN 10.



## Шаг 3. Безопасность неиспользуемых портов коммутатора

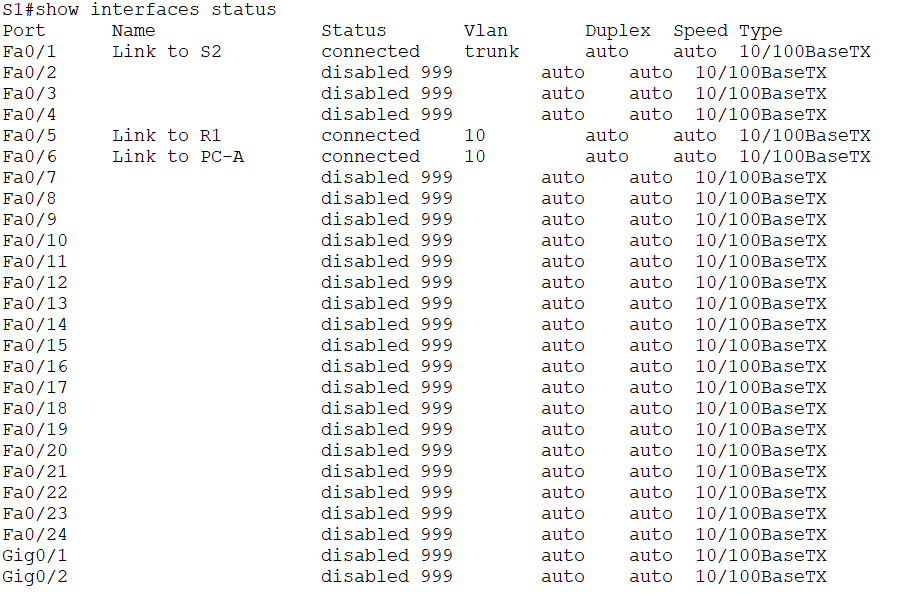
a. На S1 и S2 переместите неиспользуемые порты из VLAN 1 в VLAN 999 и отключите неиспользуемые порты.

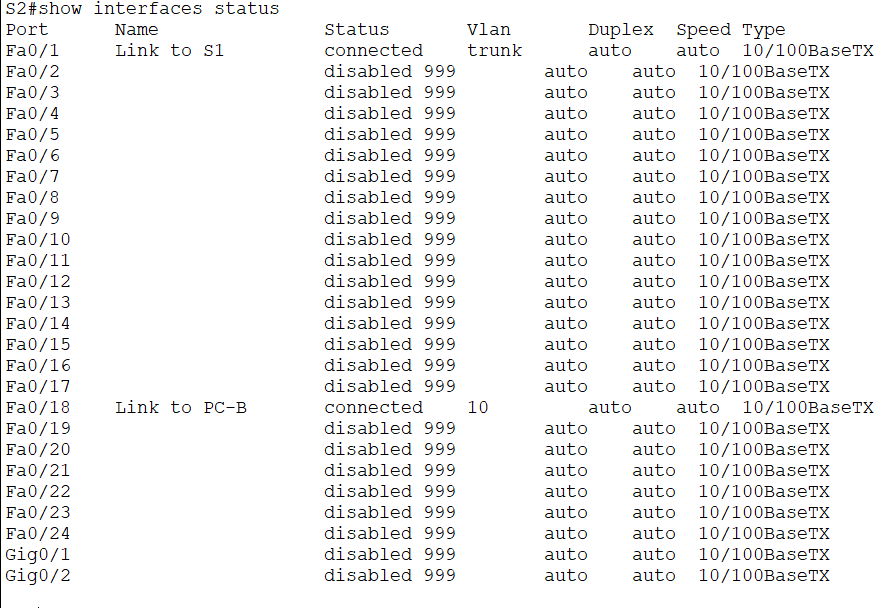




b. Убедитесь, что неиспользуемые порты отключены и связаны с VLAN 999, введя команду show.

S1# show interfaces status





Port Name Status Vlan Duplex Speed Type

Fa0/1 Link to S2 connected trunk a-full a-100 10/100BaseTX

Fa0/2 disabled 999 auto auto 10/100BaseTX

Fa0/3 disabled 999 auto auto 10/100BaseTX

Fa0/4 disabled 999 auto auto 10/100BaseTX

Fa0/5 Link to R1 connected 10 a-full a-100 10/100BaseTX

Fa0/6 Link to PC-A connected 10 a-full a-100 10/100BaseTX

Fa0/7 disabled 999 auto auto 10/100BaseTX

Fa0/8 disabled 999 auto auto 10/100BaseTX

Fa0/9 disabled 999 auto auto 10/100BaseTX

Fa0/10 disabled 999 auto auto 10/100BaseTX

<output omitted>

S2# show interfaces status

Port Name Status Vlan Duplex Speed Type

Fa0/1 Link to S1 connected trunk a-full a-100 10/100BaseTX

Fa0/2 disabled 999 auto auto 10/100BaseTX

Fa0/3 disabled 999 auto auto 10/100BaseTX

<output omitted>

Fa0/14 disabled 999 auto auto 10/100BaseTX

Fa0/15 disabled 999 auto auto 10/100BaseTX

Fa0/16 disabled 999 auto auto 10/100BaseTX

Fa0/17 disabled 999 auto auto 10/100BaseTX

Fa0/18 Link to PC-B connected 10 a-full a-100 10/100BaseTX

Fa0/19 disabled 999 auto auto 10/100BaseTX

Fa0/20 disabled 999 auto auto 10/100BaseTX

Fa0/21 disabled 999 auto auto 10/100BaseTX

Fa0/22 disabled 999 auto auto 10/100BaseTX

Fa0/23 disabled 999 auto auto 10/100BaseTX

Fa0/24 disabled 999 auto auto 10/100BaseTX

Gi0/1 disabled 999 auto auto 10/100/1000BaseTX

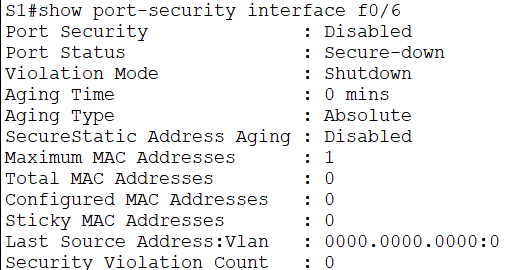
Gi0/2 disabled 999 auto auto 10/100/1000BaseTX

## Шаг 4. Документирование и реализация функций безопасности порта.

Интерфейсы F0/6 на S1 и F0/18 на S2 настроены как порты доступа. На этом шаге вы также настроите безопасность портов на этих двух портах доступа.

a. На S1, введите команду show port-security interface f0/6 для отображения настроек по

умолчанию безопасности порта для интерфейса F0/6. Запишите свои ответы ниже.



Конфигурация безопасности порта по умолчанию

|  |  |
| --- | --- |
| Функция | Настройка по умолчанию |
| Защита портов | Disabled |
| Максимальное количество записей MAC-адресов | 1 |
| Режим проверки на нарушение безопасности | Shutdown |
| Aging Time | 0 mins |
| Aging Type | Absolute |
| Secure Static Address Aging | Disabled |
| Sticky MAC Address | 0 |

b. На S1 включите защиту порта на F0 / 6 со следующими настройками:

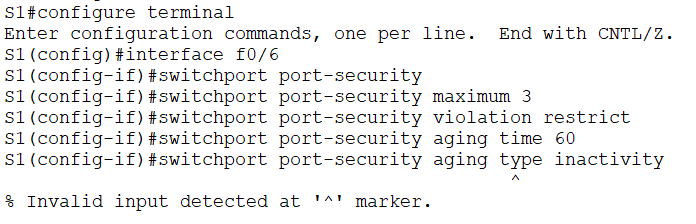
o Максимальное количество записей MAC-адресов: 3

o Режим безопасности: restrict

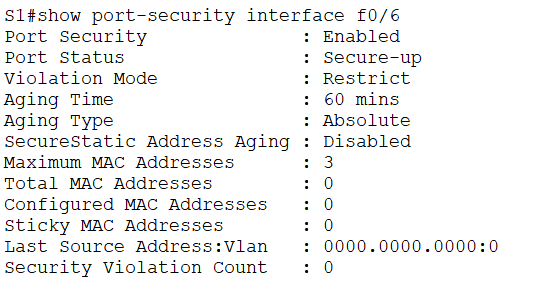
o Aging time: 60 мин.

o Aging type: неактивный

c. Verify port security on S1 F0/6.



S1# show port-security interface f0/6



Port Security : Enabled

Port Status : Secure-up

Violation Mode : Restrict

Aging Time : 60 mins

Aging Type : Inactivity

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 3

Total MAC Addresses : 1

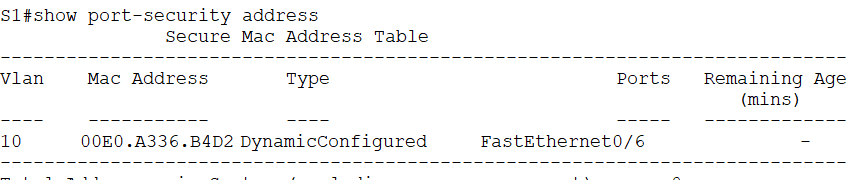
Configured MAC Addresses : 0

Sticky MAC Addresses : 0

Last Source Address:Vlan : 0022.5646.3411:10

Security Violation Count : 0

S1# show port-security address



Secure Mac Address Table

-----------------------------------------------------------------------------

Vlan Mac Address Type Ports Remaining Age

(mins)

---- ----------- ---- ----- -------------

10 0022.5646.3411 SecureDynamic Fa0/6 60 (I)

-----------------------------------------------------------------------------

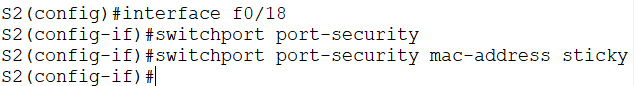
Total Addresses in System (excluding one mac per port) : 0

Max Addresses limit in System (excluding one mac per port) : 8192

d. Включите безопасность порта для F0 / 18 на S2. Настройте каждый активный порт доступа таким

образом, чтобы он автоматически добавлял адреса МАС, изученные на этом порту, в текущую

конфигурацию.

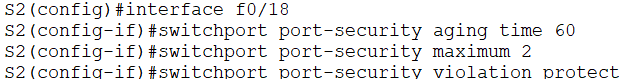


e. Настройте следующие параметры безопасности порта на S2 F / 18:

o Максимальное количество записей MAC-адресов: 2

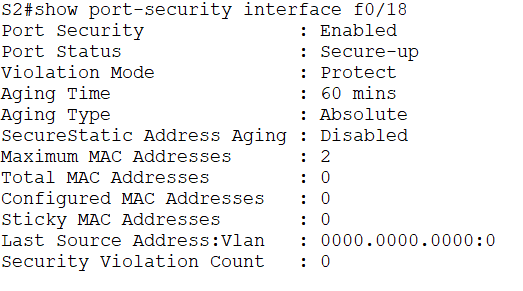
o Тип безопасности: Protect

o Aging time: 60 мин.



f. Проверка функции безопасности портов на S2 F0/18.

S2# show port-security interface f0/18



Port Security : Enabled

Port Status : Secure-up

Violation Mode : Protect

Aging Time : 60 mins

Aging Type : Absolute

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 2

Total MAC Addresses : 1

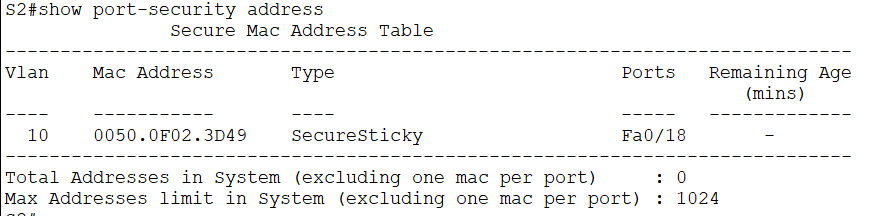
Configured MAC Addresses : 0

Sticky MAC Addresses : 0

Last Source Address:Vlan : 0022.5646.3413:10

Security Violation Count : 0

S2# show port-security address



Secure Mac Address Table

-----------------------------------------------------------------------------

Vlan Mac Address Type Ports Remaining Age

(mins)

---- ----------- ---- ----- -------------

10 0022.5646.3413 SecureSticky Fa0/18 -

-----------------------------------------------------------------------------

Total Addresses in System (excluding one mac per port) : 0

Max Addresses limit in System (excluding one mac per port) : 8192

## Шаг 5. Реализовать безопасность DHCP snooping.

a. На S2 включите DHCP snooping и настройте DHCP snooping во VLAN 10.



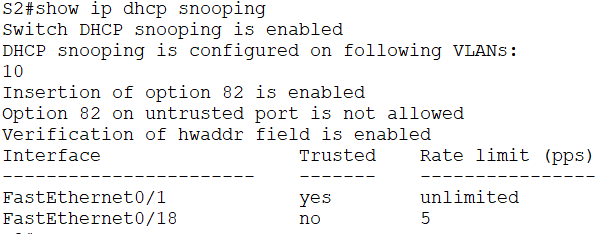
b. Настройте магистральные порты на S2 как доверенные порты.



c. Ограничьте ненадежный порт Fa0/18 на S2 пятью DHCP-пакетами в секунду.



d. Проверка DHCP Snooping на S2.



S2# show ip dhcp snooping

Switch DHCP snooping is enabled

DHCP snooping is configured on following VLANs:

10

DHCP snooping is operational on following VLANs:

10

DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled

circuit-id default format: vlan-mod-port

remote-id: 0cd9.96d2.3f80 (MAC)

Option 82 on untrusted port is not allowed

Verification of hwaddr field is enabled

Verification of giaddr field is enabled

DHCP snooping trust/rate is configured on the following Interfaces:

Interface Trusted Allow option Rate limit (pps)

----------------------- ------- ------------ ----------------

FastEthernet0/1 yes yes unlimited

Custom circuit-ids:

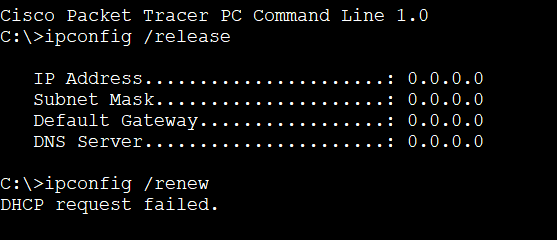
FastEthernet0/18 no no 5

Custom circuit-ids:

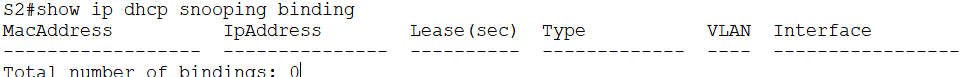
e. В командной строке на PC-B освободите, а затем обновите IP-адрес.

C:\Users\Student> ipconfig /release

C:\Users\Student> ipconfig /renew



f. Проверьте привязку отслеживания DHCP с помощью команды show ip dhcp snooping binding.



S2# show ip dhcp snooping binding

MacIp адресAddress Lease(sec) Type VLAN Interface

------------------ --------------- ---------- ------------- ---- --------------------

00:50:56:90:D0:8E 192.168.10.11 86213 dhcp-snooping 10 FastEthernet0/18

Total number of bindings: 1

## Шаг 6. Реализация PortFast и BPDU Guard

a. Настройте PortFast на всех портах доступа, которые используются на обоих коммутаторах.



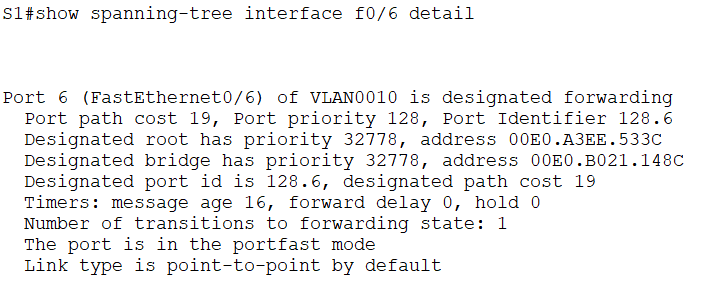


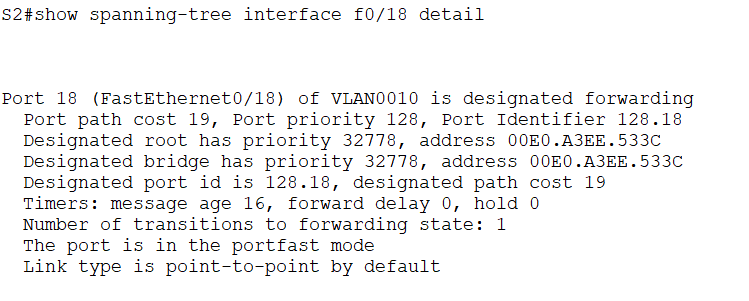
b. Включите защиту BPDU на портах доступа VLAN 10 S1 и S2, подключенных к PC-A и PC-B.





c. Убедитесь, что защита BPDU и PortFast включены на соответствующих портах.





S1# show spanning-tree interface f0/6 detail

Port 8 (FastEthernet0/6) of VLAN0010 is designated forwarding

Port path cost 19, Port priority 128, Port Identifier 128.6.

<output omitted for brevity>

Number of transitions to forwarding state: 1

The port is in the portfast mode

Link type is point-to-point by default

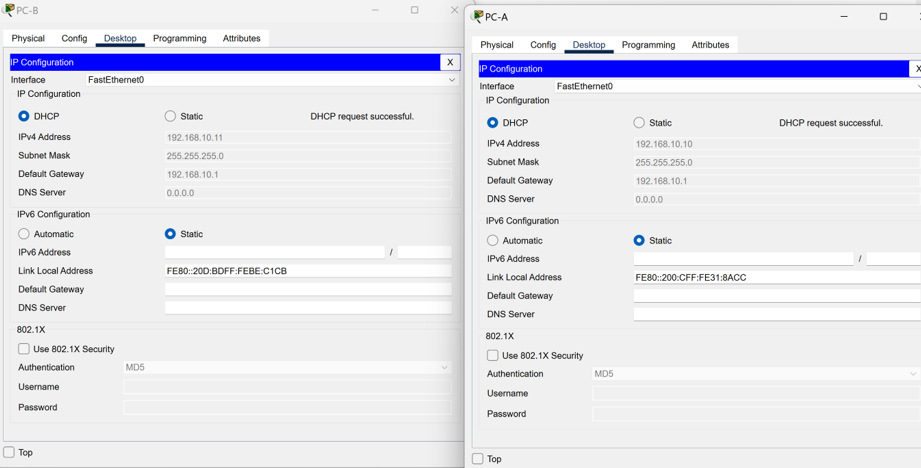
Bpdu guard is enabled

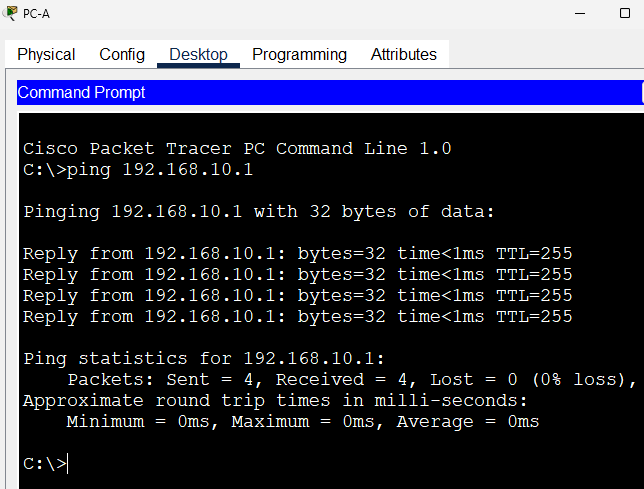
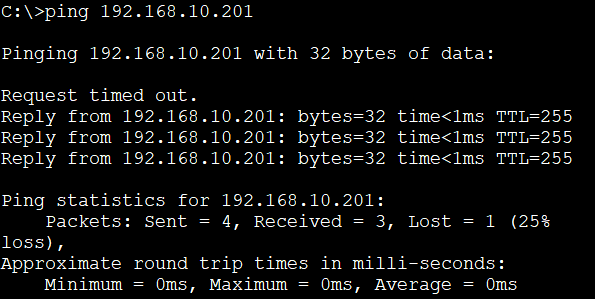
BPDU: sent 128, received 0

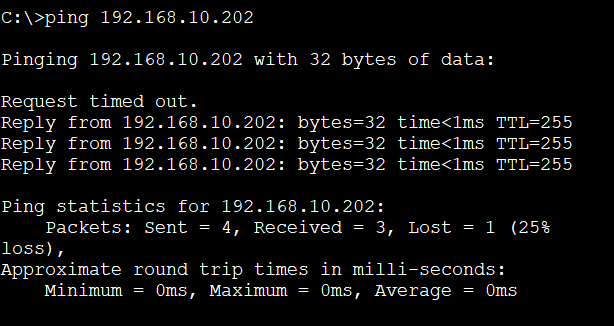
## Шаг 7. Проверьте наличие сквозного ⁪подключения.

Проверьте PING свзяь между всеми устройствами в таблице IP-адресации. В случае сбоя проверки

связи может потребоваться отключить брандмауэр на хостах.





Вопросы для повторения

1. С точки зрения безопасности порта на S2, почему нет значения таймера для оставшегося возраста в минутах, когда было сконфигурировано динамическое обучение - sticky?

Когда включено **sticky learning**, коммутатор автоматически сохраняет MAC-адреса, обнаруженные на порту, в конфигурацию. Однако эти адреса не подлежат процессу **старения (aging)**, так как они сохраняются в конфигурации и не удаляются по таймеру. Таким образом, нет необходимости в установке таймера для оставшегося времени, поскольку эти адреса являются статичными, пока не будут вручную удалены или изменены.

2. Что касается безопасности порта на S2, если вы загружаете скрипт текущей конфигурации на S2,

почему порту 18 на PC-B никогда не получит IP-адрес через DHCP?

На порту 18 настроено ограничение на количество MAC-адресов (2 MAC-адреса), и оба из них являются **sticky** MAC-адресами, которые уже привязаны к порту. В этом случае, если обнаружен новый MAC-адрес, порт не будет принимать новый DHCP-запрос, так как в конфигурации уже есть два закрепленных адреса. Более того, так как нарушенная ситуация настроена как **protect**, то коммутатор не будет генерировать сообщения в консоли или системных журналах, и не увеличится счетчик нарушений, что затруднит диагностику.

3. Что касается безопасности порта, в чем разница между типом абсолютного устаревания и типом

устаревание по неактивности?

 **Inactivity**: Если выбран этот тип старения, то адреса, привязанные к порту, будут удалены только в случае отсутствия трафика от этих MAC-адресов в течение указанного времени. Это означает, что если с устройства не будет отправляться трафик, то его MAC-адрес будет удален по истечении заданного времени.

 **Absolute**: Если выбран этот тип старения, все закрепленные адреса на порту будут удалены строго через установленное время, независимо от наличия или отсутствия трафика с этих адресов. Это означает, что время старения для всех адресов одинаково и не зависит от активности на порту.