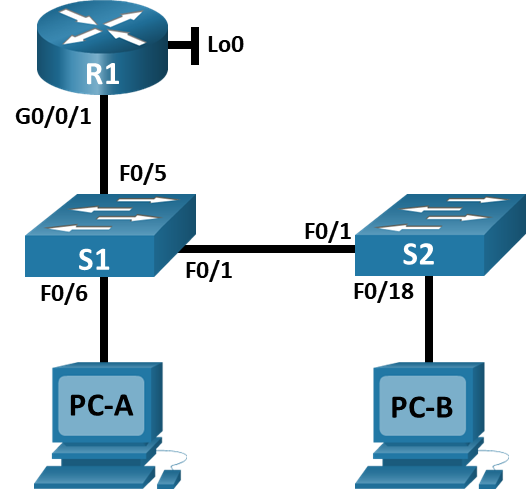
Лабораторная работа - Конфигурация безопасности коммутатора

# Топология



# Таблица адресации

| Устройство | interface/vlan | IP-адрес | Маска подсети |
| --- | --- | --- | --- |
| R1 | G0/0/1 | 192.168.10.1 | 255.255.255.0 |
| R1 | Loopback 0 | 10.10.1.1 | 255.255.255.0 |
| S1 | VLAN 10 | 192.168.10.201 | 255.255.255.0 |
| S2 | VLAN 10 | 192.168.10.202 | 255.255.255.0 |
| PC A | NIC | DHCP | 255.255.255.0 |
| PC B | NIC | DHCP | 255.255.255.0 |

# Цели

Часть 1. Настройка основного сетевого устройства

* Создайте сеть.
* Настройте маршрутизатор R1.
* Настройка и проверка основных параметров коммутатора

Часть 2. Настройка сетей VLAN

* Сконфигруриуйте VLAN 10.
* Сконфигруриуйте SVI для VLAN 10.
* Настройте VLAN 333 с именем Native на S1 и S2.
* Настройте VLAN 999 с именем ParkingLot на S1 и S2.

Часть 3: Настройки безопасности коммутатора.

* Реализация магистральных соединений 802.1Q.
* Настройка портов доступа
* Безопасность неиспользуемых портов коммутатора
* Документирование и реализация функций безопасности порта.
* Реализовать безопасность DHCP snooping .
* Реализация PortFast и BPDU Guard
* Проверка сквозной связанности.

# Общие сведения и сценарий

Это комплексная лабораторная работа, нацеленная на повторение ранее изученных функций безопасности уровня 2.

**Примечание**: Маршрутизаторы, используемые в практических лабораторных работах CCNA, - это Cisco 4221 с Cisco IOS XE Release 16.9.3 (образ universalk9). В лабораторных работах используются коммутаторы Cisco Catalyst 2960 с Cisco IOS версии 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах. Правильные идентификаторы интерфейса см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

**Примечание**: Убедитесь, что все настройки коммутатора удалены и загрузочная конфигурация отсутствует. Если вы не уверены, обратитесь к инструктору.

# Необходимые ресурсы

* 1 Маршрутизатор (Cisco 4221 с универсальным образом Cisco IOS XE версии 16.9.3 или аналогичным)
* 2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель)
* 2 ПК (ОС Windows с программой эмуляции терминалов, такой как Tera Term)
* Консольные кабели для настройки устройств Cisco IOS через консольные порты.
* Кабели Ethernet, расположенные в соответствии с топологией

# Инструкции

## Настройка основного сетевого устройства

### Создайте сеть.

1. Создайте сеть согласно топологии.
2. Инициализация устройств

### Настройте маршрутизатор R1.

* + - 1. 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

* + - 1. Проверьте текущую конфигурацию на R1, используя следующую команду:

R1>en

Password:

R1#show ip interface brief

Interface IP-Address OK? Method Status Protocol

GigabitEthernet0/0/0 unassigned YES NVRAM up down

GigabitEthernet0/0/1 192.168.10.1 YES manual up up

GigabitEthernet0/0/2 unassigned YES unset up down

Loopback0 10.10.1.1 YES manual up up

Vlan1 unassigned YES NVRAM administratively down down

### Настройка и проверка основных параметров коммутатора

* + - 1. Настройте описания интерфейса для портов, которые используются в S1 и S2.

S1(config)#interface fa0/1

S1(config-if)#description Link to S2

S1(config-if)#interface fa0/6

S1(config-if)#description Link to Users

S1(config-if)#

* + - 1. Установите для шлюза по умолчанию для VLAN управления значение 192.168.10.1 на обоих коммутаторах.

S1(config)#ip default-gateway 192.168.10.1

S1(config)#copy run startup-config

## Настройка сетей VLAN на коммутаторах.

### Сконфигруриуйте VLAN 10.

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

S1(config)#vlan 10

S1(config-vlan)#name Management

S2(config)#vlan 10

S2(config-vlan)#name Management

### 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.

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

S2(config)#vlan 333

S2(config-vlan)#name Native

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

S2(config-vlan)#vlan 999

S2(config-vlan)#name ParkingLot

## Настройки безопасности коммутатора.

### Релизация магистральных соединений 802.1Q.

* + - 1. Настройте все магистральные порты Fa0/1 на обоих коммутаторах для использования VLAN 333 в качестве native VLAN.
      2. Убедитесь, что режим транкинга успешно настроен на всех коммутаторах.

S1#sh interface trunk

Port Mode Encapsulation Status Native vlan

Fa0/1 on 802.1q trunking 333

Port Vlans allowed on trunk

Fa0/1 1-1005

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 1-1005

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

* + - 1. Отключить согласование DTP F0/1 на S1 и S2.

S1(config-if)#switchport nonegotiate

S1#show interfaces f0/1 switchport | include Negotiation

Negotiation of Trunking: Off

S2#show interfaces f0/1 switchport | include Negotiation

Negotiation of Trunking: Off

### Настройка портов доступа

* + - 1. На S1 настройте F0/5 и F0/6 в качестве портов доступа и свяжите их с VLAN 10.

S1(config-if)#int range fa0/5-6

S1(config-if)#switchport mode access

S1(config-if)#switchport access vlan 10

* + - 1. На S2 настройте порт доступа Fa0/18 и свяжите его с VLAN 10.

S2(config-if)#int fa0/18

S2(config-if)#switchport mode access

S2(config-if)#switchport access vlan 10

### Безопасность неиспользуемых портов коммутатора

* + - 1. На S1 и S2 переместите неиспользуемые порты из VLAN 1 в VLAN 999 и отключите неиспользуемые порты.

S1(config)#int range f0/2-4,fa0/7-24,g0/1-2

S1(config-if-range)#shutdown

S1(config-if-range)#sw mode access

S1(config-if-range)#sw access vlan 999

* + - 1. 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 auto auto 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 connected 10 auto auto 10/100BaseTX

Fa0/6 Link to Users connected 10 auto auto 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

Fa0/11 disabled 999 auto auto 10/100BaseTX

Fa0/12 disabled 999 auto auto 10/100BaseTX

Fa0/13 disabled 999 auto auto 10/100BaseTX

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 disabled 999 auto auto 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

Gig0/1 disabled 999 auto auto 10/100BaseTX

Gig0/2 disabled 999 auto auto 10/100BaseTX

### 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.

* + - 1. 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.

S1#show port-security interface f0/6

Port Security : Disabled

Port Status : Secure-down

Violation Mode : Shutdown

Aging Time : 0 mins

Aging Type : Absolute

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 1

Total MAC Addresses : 0

Configured MAC Addresses : 0

Sticky MAC Addresses : 0

Last Source Address:Vlan : 0000.0000.0000:0

Security Violation Count : 0

* + - 1. На S1 включите защиту порта на F0 / 6 со следующими настройками:
* Максимальное количество записей MAC-адресов: **3**
* Режим безопасности: **restrict**
* Aging time: **60 мин.**
* Aging type: **неактивный**

S1(config)#int fa0/6

S1(config-if)#sw port-security

S1(config-if)#switchport port-security maximum 3

S1(config-if)#switchport port-security violation restrict

S1(config-if)#switchport port-security aging time 60

* + - 1. 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 : Absolute

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 3

Total MAC Addresses : 0

Configured MAC Addresses : 0

Sticky MAC Addresses : 0

Last Source Address:Vlan : 0000.0000.0000:0

Security Violation Count : 0

S1#show port-security address

Secure Mac Address Table

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

Vlan Mac Address Type Ports Remaining Age

(mins)

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

10 000A.41BB.7B46 DynamicConfigured FastEthernet0/6 -

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

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

Max Addresses limit in System (excluding one mac per port) : 1024

* + - 1. 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.

S2(config)#int fa0/18

S2(config-if)#switchport port-security

S2(config-if)#switchport port-security mac-address sticky

* + - 1. Настройте следующие параметры безопасности порта на S2 F / 18:
* Максимальное количество записей MAC-адресов: **2**
* Тип безопасности: **Protect**
* Aging time: **60 мин.**

S2(config-if)#sw port-security maximum 2

S2(config-if)#sw port-security violation protect

S2(config-if)#sw port-security aging time 60

* + - 1. Проверка функции безопасности портов на S2 F0/18.

S2#

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed state to up

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 : 1

Last Source Address:Vlan : 0030.F2C5.2EDE:10

Security Violation Count : 0

S2#show port-security address

Secure Mac Address Table

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

Vlan Mac Address Type Ports Remaining Age

(mins)

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

10 0030.F2C5.2EDE SecureSticky Fa0/18 -

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

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

Max Addresses limit in System (excluding one mac per port) : 1024

### Реализовать безопасность DHCP snooping.

S2(config)#ip dhcp snooping

S2(config)#ip dhcp snooping vlan 10

S2(config)#int fa0/1

S2(config-if)#ip dhcp snooping trust

S2(config-if)#int f0/18

S2#sh ip dhcp snooping

Switch DHCP snooping is enabled

DHCP snooping is configured on following VLANs:

10

Insertion of option 82 is enabled

Option 82 on untrusted port is not allowed

Verification of hwaddr field is enabled

Interface Trusted Rate limit (pps)

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

FastEthernet0/1 yes unlimited

FastEthernet0/18 no 5

* + - 1. S2# В командной строке на PC-B освободите, а затем обновите IP-адрес.

C:\Users\Student> **ipconfig /release**

C:\Users\Student> **ipconfig /renew**

C:\>ipconfig /release

IP Address......................: 0.0.0.0

Subnet Mask.....................: 0.0.0.0

Default Gateway.................: 0.0.0.0

DNS Server......................: 0.0.0.0

C:\>ipconfig /renew

IP Address......................: 192.168.10.11

Subnet Mask.....................: 255.255.255.0

Default Gateway.................: 192.168.10.1

DNS Server......................: 0.0.0.0

* + - 1. Проверьте привязку отслеживания DHCP с помощью команды **show ip dhcp snooping binding**.

S2#sh ip dhcp snooping binding

MacAddress IpAddress Lease(sec) Type VLAN Interface

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

00:30:F2:C5:2E:DE 192.168.10.11 0 dhcp-snooping 10 FastEthernet0/18

### Total number of bindings: 1 Реализация PortFast и BPDU Guard

* + - 1. Настройте PortFast на всех портах доступа, которые используются на обоих коммутаторах.

S1(config)#int f0/6

S1(config-if)#spanning-tree portfast

%Warning: portfast should only be enabled on ports connected to a single

host. Connecting hubs, concentrators, switches, bridges, etc... to this

interface when portfast is enabled, can cause temporary bridging loops.

Use with CAUTION

%Portfast has been configured on FastEthernet0/6 but will only

have effect when the interface is in a non-trunking mode.

* + - * 1. Включите защиту BPDU на портах доступа VLAN 10 S1 и S2, подключенных к PC-A и PC-B.

S1(config)# interface f0/6

S1(config-if)# spanning-tree bpduguard enable

S2(config)# interface f0/18

S2(config-if)# spanning-tree bpduguard enable

* + - 1. Убедитесь, что защита BPDU и PortFast включены на соответствующих портах.

S1#show spanning-tree interface f0/6 detail

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

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

Designated root has priority 32778, address 00E0.F7AB.2805

Designated bridge has priority 32778, address 00E0.F7AB.2805

Designated port id is 128.6, designated path cost 19

Timers: message age 16, forward delay 0, hold 0

Number of transitions to forwarding state: 1

The port is in the portfast mode

### Link type is point-to-point by defaultПроверьте наличие сквозного ⁪подключения.

Проверьте PING свзяь между всеми устройствами в таблице IP-адресации. В случае сбоя проверки связи может потребоваться отключить брандмауэр на хостах.

C:\>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:

Reply from 192.168.10.10: bytes=32 time=20ms TTL=128

Reply from 192.168.10.10: bytes=32 time=8ms TTL=128

Reply from 192.168.10.10: bytes=32 time<1ms TTL=128

Reply from 192.168.10.10: bytes=32 time=9ms TTL=128

Ping statistics for 192.168.10.10:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 20ms, Average = 9ms

C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time<1ms TTL=255

Reply from 192.168.10.1: bytes=32 time=17ms TTL=255

Reply from 192.168.10.1: bytes=32 time<1ms TTL=255

Reply from 192.168.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 17ms, Average = 4ms

C:\>ping 192.168.10.201

Pinging 192.168.10.201 with 32 bytes of data:

Request timed out.

Reply from 192.168.10.201: bytes=32 time<1ms TTL=255

Reply from 192.168.10.201: bytes=32 time<1ms TTL=255

Reply from 192.168.10.201: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.201:

Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.202

Pinging 192.168.10.202 with 32 bytes of data:

Request timed out.

Reply from 192.168.10.202: bytes=32 time<1ms TTL=255

Reply from 192.168.10.202: bytes=32 time<1ms TTL=255

Reply from 192.168.10.202: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.202:

Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>

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?

1. Отсутствие значения таймера для оставшегося возраста в минутах при использовании динамического обучения (sticky learning) на порту S2 связано с тем, что при динамическом обучении MAC-адреса устанавливаются на порту на основе трафика, который проходит через порт. Это позволяет устройству динамически "запоминать" MAC-адреса, которые в него заходят, и связывать их с портом на основе трафика, который оно видит.
   1. 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?

Проблема заключается в том, что порт 18 на PC-B настроен как порт без доступа (access port), который не пропускает трафик DHCP, и поэтому PC-B не может получить IP-адрес через DHCP.

* 1. Что касается безопасности порта, в чем разница между типом абсолютного устаревания и типом устаревание по неактивности?

1. Тип абсолютного устаревания (Absolute Aging):
2. - Этот тип устаревания включает в себя механизм, при котором запись о MAC-адресе удаляется из таблицы MAC (MAC-таблицы) после определенного времени, независимо от активности устройства с данным MAC-адресом.
3. Тип устаревания по неактивности (Inactivity Aging):
4. - Этот тип устаревания предусматривает удаление записи о MAC-адресе из таблицы MAC только в случае отсутствия активности (отсутствия трафика) от устройства с этим MAC-адресом в течение определенного времени.