Конфигурация безопасности коммутатора

Топология

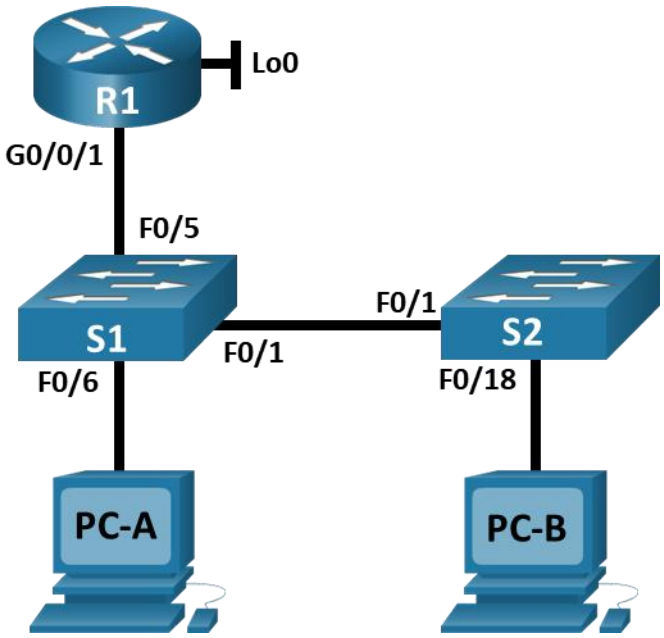


Таблица адресации

Устройство	interface/vlan	IP-адрес	Маска подсети
R1_ФАМИЛИЯ	G0/0/1	192.168.31.1	255.255.255.0
	Loopback 0	10.10.1.1	255.255.255.0
S1	VLAN 31	192.168.31.201	255.255.255.0
S2	VLAN 31	192.168.31.202	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_ФАМИЛИЯ.

Конфигурация безопасности коммутатора

- Настройка и проверка основных параметров коммутатора

Часть 2. Настройка сетей VLAN

- Сконфигруриуйте VLAN X+10.
- Сконфигруриуйте SVI для VLAN X+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.

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

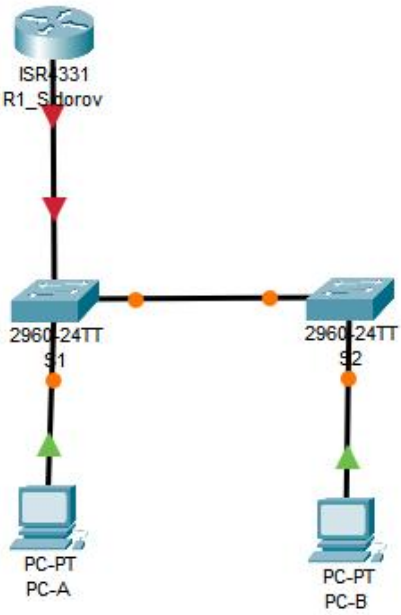
Часть 1. Настройка основного сетевого устройства

Шаг 1. Создайте сеть.

a. Создайте сеть согласно топологии.

b. Инициализация устройств

Конфигурация безопасности коммутатора



Шаг 2. Настройте маршрутизатор R1_ФАМИЛИЯ.

a. Загрузите следующий конфигурационный скрипт на R1_ФАМИЛИЯ.

```
Router(config)#hostname R1_Sidorov
R1_Sidorov(config)#no ip domain-lookup
R1_Sidorov(config)#ip dhcp excluded-address 192.168.31.1 192.168.31.9
R1_Sidorov(config)#ip dhcp excluded-address 192.168.31.201 192.168.31.202
R1_Sidorov(config)#ip dhcp pool Students
R1_Sidorov(dhcp-config)#network 192.168.31.0 255.255.255.0
R1_Sidorov(dhcp-config)#default-router 192.168.31.1
R1_Sidorov(dhcp-config)#domain-name CCNA2.Lab-7
R1_Sidorov(dhcp-config)#exit
R1_Sidorov(config)#interface Loopback0

R1_Sidorov(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R1_Sidorov(config-if)#ip address 10.10.1.1 255.255.255.0
R1_Sidorov(config-if)#exit
R1_Sidorov(config)#interface g0/0/1
R1 Sidorov(config-if)#description Link to S1
R1_Sidorov(config-if)#no shutdown

R1_Sidorov(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up

R1_Sidorov(config-if)#line con 0
R1_Sidorov(config-line)#logging sync
R1_Sidorov(config-line)#logging synchronous
R1_Sidorov(config-line)#exec-timeout 0 0
R1_Sidorov(config-line)#exit
R1_Sidorov(config)#
            R1_Sidorov(config)#ip dhcp relay information trust-all
```

b. Проверьте конфигурацию сетевых интерфейсов на R1_ФАМИЛИЯ.

Конфигурация безопасности коммутатора

```
R1_Sidorov(config)#do show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES unset  administratively down down
GigabitEthernet0/0/1   192.168.31.1    YES manual up                    up
GigabitEthernet0/0/2   unassigned      YES unset  administratively down down
Loopback0              10.10.1.1       YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

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.X+10.1 на обоих коммутаторах.

```
Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#int F0/5
S1(config-if)#description Connection to Router
S1(config-if)#exit
S1(config)#int F0/1
S1(config-if)#description Connection to S2
S1(config-if)#exit
S1(config)#int F0/6
S1(config-if)#description Connection to PCA
S1(config-if)#exit
```

```
S1(config)#ip default-gateway 192.168.31.1
S1(config)#do write memory
Building configuration...
[OK]
```

```
Switch(config)#hostname S2
S2(config)#no ip domain-lookup
S2(config)#int f0/1
S2(config-if)#description Connection to S1
S2(config-if)#exit
S2(config)#int f0/18
S2(config-if)#description Connection to PCB
S2(config-if)#exit
```

```
S2(config)#ip default-gateway 192.168.31.1
S2(config)#do write memory
Building configuration...
[OK]
```

Часть 2. Настройка сетей VLAN на коммутаторах.

Шаг 1. Сконфигуриуйте VLAN X+10.

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

Шаг 2. Сконфигуриуйте SVI для VLAN X+10. Настройте IP-адрес в соответствии с таблицей адресации для SVI для VLAN X+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.

```
S1(config)#vlan 31
S1(config-vlan)#name Management
S1(config-vlan)#exit
S1(config)#interface vlan 31
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan31, changed state to up

S1(config-if)#ip address 192.168.31.201 255.255.255.0
S1(config-if)#description Management Vlan
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#vlan 333
S1(config-vlan)#name Native
S1(config-vlan)#exit
S1(config)#vlan 999
S1(config-vlan)#name ParkingLot
S1(config-vlan)#exit
S1(config)#do write memory
Building configuration...
[OK]
```

```
S2(config)#vlan 31
S2(config-vlan)#name Management
S2(config-vlan)#exit
S2(config)#int vlan 31
S2(config-if)#
%LINK-5-CHANGED: Interface Vlan31, changed state to up

S2(config-if)#ip address 192.168.31.202 255.255.255.0
S2(config-if)#description Management Vlan
S2(config-if)#no shut
S2(config-if)#exit
S2(config)#vlan 333
S2(config-vlan)#name Native
S2(config-vlan)#exit
S2(config)#vlan 999
S2(config-vlan)#name ParkingLot
S2(config-vlan)#exit
S2(config)#do write memory
Building configuration...
[OK]
```


Конфигурация безопасности коммутатора

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.

```
S1(config)#interface f0/1
S1(config-if)#switchport mode trunk

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan31, changed state to up
switchport trunk native vlan 333
S1(config-if)#exit
```

```
S2(config)#int f0/1
S2(config-if)#switchport mode trunk

S2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan31, changed state to up
%SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlan id 333 on
FastEthernet0/1 VLAN1.

%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/1 on VLAN0001. Inconsistent local
vlan.


S2(config-if)#switchport trunk native vlan 333
S2(config-if)#%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on VLAN0333.
Port consistency restored.
```

b. Убедитесь, что режим транкинга успешно настроен на всех коммутаторах с помощью команды **show interface trunk** на обоих коммутаторах.

```
S1(config)#do 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       1,31,333,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       31,999
```

```
S2(config)#do 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       1,31,333,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,31,333,999
```

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

Конфигурация безопасности коммутатора

```
S1(config)#int f0/1
S1(config-if)#switchport none
S1(config-if)#switchport nonegotiate
S1(config-if)#exit
S1(config)#

S2(config)#int f0/1
S2(config-if)#switchport non
S2(config-if)#switchport nonegotiate
S2(config-if)#exit
S2(config)#
```

d. Проверьте с помощью команды **show interfaces**. Пример:

```
S1(config)#do show interfaces f0/1 switchport | include Negotiation
Negotiation of Trunking: Off

S2(config)#do 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 X+10.

```
S1(config)#int range f0/5-6
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 31
S1(config-if-range)#exit
```

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

```
S2(config)#int f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 31
S2(config-if)#exit
```

Шаг 3. Безопасность неиспользуемых портов коммутатора

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

```
interface range not validated - command rejecte
S1(config)#int range f0/2-4, f0/7-24
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 999
S1(config-if-range)#shutdown
```

```
S1(config)#int range g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 999
S1(config-if-range)#shutdown
```

```
S2(config)#int range f0/2-17, f0/19-24, g0/1-2
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 999
S2(config-if-range)#shutdown
```

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

Конфигурация безопасности коммутатора

```
S1(config)#do show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1     Connection 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     Connection to Rout connected    31         auto    auto  10/100BaseTX
Fa0/6     Connection to PCA  connected    31         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
```

```
S2(config)#do show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1     Connection to S1   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                        disabled 999         auto    auto  10/100BaseTX
Fa0/6                        disabled 999         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    Connection to PCB  connected    31         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
```


Конфигурация безопасности коммутатора

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.

```
S1(config)#do 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
```

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

- Максимальное количество записей MAC-адресов: **3**
- Режим безопасности: **restrict**
- Aging time: **60 мин.**

```
S1(config)#int f0/6
S1(config-if)#switchport-security maximum
                             ^
% Invalid input detected at '^' marker.

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
S1(config-if)#switchport port-security aging type inactivity
```

c. Проверьте настройки защиты порта (**port-security**) на S1 для интерфейса F0/6. Далее просмотрите выходные данные команды **show port-security address**.

```
S1(config)#do 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
```


Конфигурация безопасности коммутатора

```
S1(config)#do show port-security address
               Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

d. Включите безопасность порта для F0/18 на S2. Настройте каждый активный порт доступа таким образом, чтобы он автоматически добавлял адреса MAC, изученные на этом порту, в текущую конфигурацию.

```
S2(config)#int f0/18
S2(config-if)#switchport port-security
S2(config-if)#exit
```

e. Настройте следующие параметры безопасности порта на S2 F0/18:

- Максимальное количество записей MAC-адресов: **2**
- Тип безопасности: **Protect**
- Aging time: **60 мин.**

```
S2(config)#int f0/18
S2(config-if)#switchport port-security
S2(config-if)#exit
S2(config)#int f0/18
S2(config-if)#switchport port-secuirty maximum 2
                                ^
% Invalid input detected at '^' marker.

S2(config-if)#switchport port-security maximum 2
S2(config-if)#switchport port-security violation protect
S2(config-if)#switchport aging time 60
                         ^
% Invalid input detected at '^' marker.

S2(config-if)#switchport port-security aging time 60
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#exit
```

f. Проверьте настройки защиты порта (**port-security**) на S2 для интерфейса F0/18. Далее просмотрите выходные данные команды **show port-security address**.

```
S2(config)#do 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        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```


Конфигурация безопасности коммутатора

```
S2(config)#do show port-security address
               Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

Шаг 5. Реализовать безопасность DHCP snooping.

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

```
S2(config)#ip dhcp snooping
S2(config)#ip dhcp snooping vlan 31
```

b. Настройте магистральные порты на S2 как доверенные порты.

```
S2(config)#int f0/1
S2(config-if)#ip dhc
S2(config-if)#ip dhcp snooping trus
S2(config-if)#ip dhcp snooping trust
```

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

```
S2(config)#int f0/18
S2(config-if)#ip dhcp snooping limit rate 5
S2(config-if)#exit
```

d. Проверьте DHCP Snooping на S2 с помощью команды **show ip dhcp snooping**.

```
S2(config)#do show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
31
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
```

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

```
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.......................: 192.168.31.10
   Subnet Mask......................: 255.255.255.0
   Default Gateway..................: 192.168.31.1
   DNS Server.......................: 0.0.0.0
```

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

Конфигурация безопасности коммутатора

```
S2#sho ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----
------------------
00:D0:58:C1:AC:BD   192.168.31.10    0           dhcp-snooping  31    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 X+10 для S1 и S2, подключенных к PC-A и PC-B.

```
S1(config)#int f0/5
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 FastEthernet0/5 but will only
have effect when the interface is in a non-trunking mode.
S1(config-if)#exit
```

```
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.
S1(config-if)#spanning-tree bpduguard enable
S1(config-if)#exi
```

```
S2(config)#int f0/18
S2(config-if)#span
S2(config-if)#spanning-tree p
S2(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 FastEthernet0/18 but will only
have effect when the interface is in a non-trunking mode.
S2(config-if)#spanning-tree bp
S2(config-if)#spanning-tree bpduguard enable
S2(config-if)#exit
```

c. Убедитесь, что защита BPDU и PortFast включены на соответствующих портах с помощью команды **show spanning-tree interface f0/6 detail**.


```
Port 5 (FastEthernet0/5) of VLAN0031 is designated forwarding
  Port path cost 19, Port priority 128, Port Identifier 128.5
  Designated root has priority 32799, address 00D0.583€.79A3
  Designated bridge has priority 32799, address 00D0.583€.79A3
  Designated port id is 128.5, designated path cost 19
  Timers: message age 1€, 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 default


S1#show spanning-tree interface f0/€ detail



Port € (FastEthernet0/€) of VLAN0031 is designated forwarding
  Port path cost 19, Port priority 128, Port Identifier 128.€
  Designated root has priority 32799, address 00D0.583€.79A3
  Designated bridge has priority 32799, address 00D0.583€.79A3
  Designated port id is 128.€, designated path cost 19
  Timers: message age 1€, 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 default

S2#show spanning-tree interface f0/18 detail



Port 18 (FastEthernet0/18) of VLAN0031 is designated forwarding
  Port path cost 19, Port priority 128, Port Identifier 128.18
  Designated root has priority 32799, address 00D0.583€.79A3
  Designated bridge has priority 32799, address 00D0.BC14.2C3A
  Designated port id is 128.18, designated path cost 19
  Timers: message age 1€, 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 default
```

Шаг 7. Проверьте наличие сквозного подключения.

Отправьте эхо-запрос между всеми устройствами в таблице IP-адресации.


```
C:\>ping 192.168.31.1

Pinging 192.168.31.1 with 32 bytes of data:

Reply from 192.168.31.1: bytes=32 time<1ms TTL=255
Reply from 192.168.31.1: bytes=32 time<1ms TTL=255
Reply from 192.168.31.1: bytes=32 time<1ms TTL=255
Reply from 192.168.31.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.31.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.31.201

Pinging 192.168.31.201 with 32 bytes of data:

Request timed out.
Reply from 192.168.31.201: bytes=32 time=1ms TTL=255
Reply from 192.168.31.201: bytes=32 time<1ms TTL=255
Reply from 192.168.31.201: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.31.201:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.31.202

Pinging 192.168.31.202 with 32 bytes of data:

Request timed out.
Reply from 192.168.31.202: bytes=32 time<1ms TTL=255
Reply from 192.168.31.202: bytes=32 time=1ms TTL=255
Reply from 192.168.31.202: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.31.202:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 10.10.1.1

Pinging 10.10.1.1 with 32 bytes of data:

Reply from 10.10.1.1: bytes=32 time<1ms TTL=255
Reply from 10.10.1.1: bytes=32 time<1ms TTL=255
Reply from 10.10.1.1: bytes=32 time<1ms TTL=255
Reply from 10.10.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.10.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Отправка ping с PC-B

Конфигурация безопасности коммутатора

```
C:\>ping 192.168.31.10

Pinging 192.168.31.10 with 32 bytes of data:

Reply from 192.168.31.10: bytes=32 time<1ms TTL=128
Reply from 192.168.31.10: bytes=32 time<1ms TTL=128
Reply from 192.168.31.10: bytes=32 time<1ms TTL=128
Reply from 192.168.31.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.31.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.31.1

Pinging 192.168.31.1 with 32 bytes of data:

Reply from 192.168.31.1: bytes=32 time<1ms TTL=255
Reply from 192.168.31.1: bytes=32 time<1ms TTL=255
Reply from 192.168.31.1: bytes=32 time<1ms TTL=255
Reply from 192.168.31.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.31.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.31.201

Pinging 192.168.31.201 with 32 bytes of data:

Request timed out.
Reply from 192.168.31.201: bytes=32 time<1ms TTL=255
Reply from 192.168.31.201: bytes=32 time<1ms TTL=255
Reply from 192.168.31.201: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.31.201:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.31.202

Pinging 192.168.31.202 with 32 bytes of data:

Request timed out.
Reply from 192.168.31.202: bytes=32 time<1ms TTL=255
Reply from 192.168.31.202: bytes=32 time<1ms TTL=255
Reply from 192.168.31.202: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.31.202:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```


Отправка ping с PC-A

Конфигурация безопасности коммутатора

```
R1_Sidorov#ping
Protocol [ip]:
Target IP address: 192.168.31.201
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.31.201, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms

R1_Sidorov#ping
Protocol [ip]:
Target IP address: 192.168.31.202
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.31.202, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms
```

Отправка ping с R1_Sidorov

```
S1#ping
Protocol [ip]:
Target IP address: 192.168.31.202
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.31.202, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms

S1#ping
Protocol [ip]:
Target IP address: 192.168.31.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.31.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Отправка ping с S1

Вопросы для защиты теоретической части (глава 11)

1. Вопрос: Для чего необходимо обеспечить безопасность портов коммутатора? Что произойдет, если к порту с включенной безопасностью подключают более одного устройства и почему?

Ответ: Обеспечение безопасности портов коммутатора необходимо для предотвращения несанкционированного доступа к сети и защиты от атак, таких как атаки мак-флуда или атаки переполнения камеры MAC-адресов. Если к порту с включенной безопасностью подключают более одного устройства, то возникает риск возникновения мак-флуда или атаки переполнения камеры MAC-адресов, что может привести к отказу в обслуживании (DoS) или возможности злоумышленнику проникнуть в сеть.

2. Вопрос: Какое минимальное и максимальное количество MAC-адресов может быть разрешено на одном порту коммутатора? Опишите все существующие способы изучения MAC-адресов на коммутаторе.

Ответ: Минимальное количество MAC-адресов, разрешенных на одном порту коммутатора, - один. Максимальное количество зависит от настроек коммутатора, но обычно оно ограничено одним MAC-адресом. Существующие способы изучения MAC-адресов на коммутаторе включают в себя статическое изучение MAC-адресов, динамическое изучение с помощью протокола MAC-адресного изучения (MAC-адреса), а также изучение с использованием механизма статического изучения (sticky learning).

3. Вопрос: Опишите существующие типы устаревания безопасности порта. Каким образом можно активировать отключенный по ошибке порт коммутатора?

Ответ: Существующие типы устаревания безопасности порта включают в себя статическое устаревание, динамическое устаревание и устаревание по неприкосновенности. Чтобы активировать отключенный по ошибке порт коммутатора, вы можете использовать команду no shutdown в режиме конфигурации интерфейса.

4. Вопрос: Дайте характеристику режимам нарушения безопасности порта. В чем заключается опасность включенного протокола согласования DTP?

Ответ: Режимы нарушения безопасности порта включают в себя отклонение, отключение и защиту. Отклонение позволяет записывать нарушения в системный журнал без принятия каких-либо мер. Отключение отключает порт, если нарушение безопасности обнаружено. Защита автоматически закрывает порт и предотвращает дальнейшие нарушения. Опасность включенного протокола согласования DTP заключается в том, что злоумышленник может использовать этот протокол для внедрения в сеть с целью выполнения атак вроде атаки мак-флуда или атаки переполнения камеры MAC-адресов.

5. Вопрос: Опишите суть технологии DHCP Snooping. Для чего может понадобиться динамическая проверка ARP?

Ответ: DHCP Snooping - это технология, которая используется для защиты сети от атак DHCP-отравления или от других атак, связанных с DHCP. Он контролирует передачу DHCP-сообщений на недоверенных портах и регистрирует информацию о DHCP-клиентах. Динамическая проверка ARP может потребоваться для защиты сети от атак перехвата ARP или от других атак, связанных с ARP, путем мониторинга ARP-таблиц и предотвращения подмены MAC-адресов.

6. Вопрос: Перечислите рекомендации по настройке портов с помощью динамической проверки ARP. Почему необходимо включать функции BPDU Guard И PortFast?

Ответ: Рекомендации по настройке портов с использованием динамической проверки ARP включают в себя настройку доверенных портов для устройств, которые отправляют ARP-запросы, и настройку недоверенных портов для всех остальных портов. Включение функций BPDU Guard и PortFast необходимо для обеспечения безопасности сети и предотвращения возможных атак, таких как атаки на мак-адреса и атаки на маршрутизаторы.

Конфигурация безопасности коммутатора

7. Вопрос: Какие шаги необходимо предпринять для устранения угрозы VLAN Hopping?
Ответ: Для устранения угрозы VLAN Hopping необходимо настроить протоколы безопасности VLAN, такие как Private VLANs, а также настроить механизмы защиты от атак, такие как DHCP Snooping и Dynamic ARP Inspection.

8. Вопрос: Что рекомендуется сделать при использовании сети native VLAN? Какие два типа портов коммутаторов используются на коммутаторах Cisco в составе средств защиты от атак DHCPспуфинга?
Ответ: При использовании сети native VLAN рекомендуется настроить разрешение безопасности порта для всех портов, находящихся в сети native VLAN. Два типа портов коммутаторов Cisco, используемых в качестве средств защиты от атак DHCP-спуфинга, включают в себя доверенные порты и недоверенные порты.

9. **Вопрос: Почему устройства уровня 2 считаются самым слабым звеном в инфраструктуре безопасности компании? Где хранятся динамически определяемые MAC-адреса, когда включена функция sticky learning?**
Ответ: Устройства уровня 2 считаются самым слабым звеном в инфраструктуре безопасности компании, потому что они имеют ограниченные механизмы защиты и могут быть подвержены различным атакам, таким как атаки мак-адресов и атаки переполнения камеры MAC-адресов. Динамически определяемые MAC-адреса, когда включена функция sticky learning, хранятся во временном кэше коммутатора.

