Конфигурация безопасности коммутатора

Топология

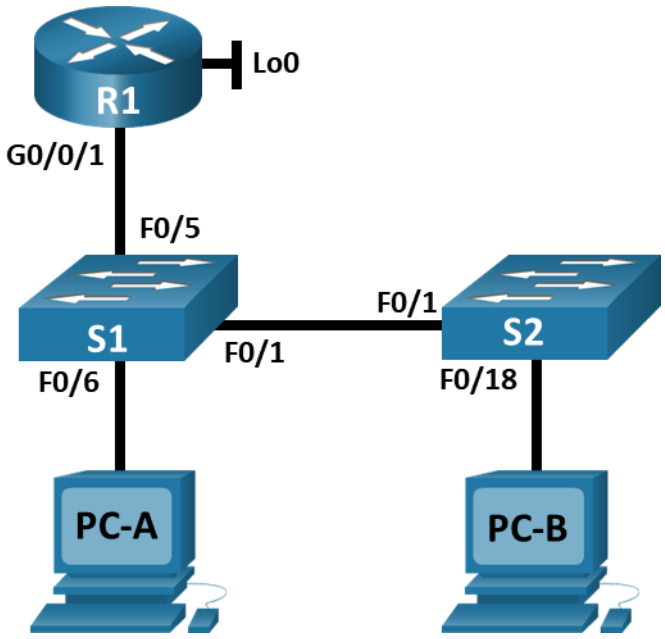

Таблица адресации

Устройство	interface/vlan	IP-адрес	Маска подсети
R1_ФАМИЛИЯ	G0/0/1	192.168.X+10.1	255.255.255.0
	Loopback 0	10.10.1.1	255.255.255.0
S1	VLAN X+10	192.168.X+10.201	255.255.255.0
S2	VLAN X+10	192.168.X+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_ФАМИЛИЯ.
- 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

Шаг 2. Настройте маршрутизатор R1_ФАМИЛИЯ.

a. Загрузите следующий конфигурационный скрипт на R1_ФАМИЛИЯ.

```
enable
configure terminal
hostname R1_ФАМИЛИЯ
no ip domain lookup
ip dhcp excluded-address 192.168.X+10.1 192.168.X+10.9
ip dhcp excluded-address 192.168.X+10.201 192.168.X+10.202
!
ip dhcp pool Students
 network 192.168.X+10.0 255.255.255.0
```

```
 default-router 192.168.X+10.1
 domain-name CCNA2.Lab-7
!
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.X+10.1 255.255.255.0
 no shutdown
!
line con 0
 logging synchronous
 exec-timeout 0 0
```

b. Проверьте конфигурацию сетевых интерфейсов на R1_ФАМИЛИЯ.

```
R1_Belosludtsev#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES unset  administratively down down
GigabitEthernet0/0/1   192.168.12.1    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
R1_Belosludtsev#
```

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.

Настройка коммутатора S1:

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#int f0/1
S1(config-if)#desc Link to S2
S1(config-if)#exit
S1(config)#int f0/5
S1(config-if)#desc Link to R1
S1(config-if)#exit
S1(config)#int f0/6
S1(config-if)#desc Link to PC-A
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.12.1
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

Настройка коммутатора S2:

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#no ip domain-lookup
S2(config)#int f0/1
S2(config-if)#desc Link to S1
S2(config-if)#exit
S2(config)#int f0/18
S2(config-if)#desc Link to PC-B
S2(config-if)#exit
S2(config)#ip default-gateway 192.168.12.1
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console
```

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.**

```
S1(config)#vlan 12
S1(config-vlan)#name Management
S1(config-vlan)#exit
S1(config)#
```

```
S2(config)#vlan 12
S2(config-vlan)#name Management
S2(config-vlan)#exit
S2(config)#
```

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.

```
S1(config)#interface vlan 12
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan12, changed state to up

S1(config-if)#ip address 192.168.12.201 255.255.255.0
S1(config-if)#description Management SVI
S1(config-if)#no shutdown
S1(config-if)#
```

```
S2(config)#interface vlan 12
S2(config-if)#
%LINK-5-CHANGED: Interface Vlan12, changed state to up

S2(config-if)#ip address 192.168.12.202 255.255.255.0
S2(config-if)#description Management SVI
S2(config-if)#no shutdown
S2(config-if)#
```

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

```
S1(config)#vlan 333
S1(config-vlan)#name Native
S1(config-vlan)#exit
S1(config)#
```

```
S2(config)#vlan 333
S2(config-vlan)#name Native
S2(config-vlan)#exit
S2(config)#
```

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

```
S1(config)#vlan 999
S1(config-vlan)#name ParkingLot
S1(config-vlan)#exit
S1(config)#
```

```
S2(config)#vlan 999
S2(config-vlan)#name ParkingLot
S2(config-vlan)#exit
S2(config)#
```

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 Vlan12, changed state to up

S1(config-if)#switchport trunk native vlan 333
S1(config-if)#
```

```
S2(config)#interface f0/1
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 333
S2(config-if)#%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on VLAN0333. Port
consistency restored.

%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on VLAN0001. Port consistency
restored.


S2(config-if)#
```

b. Убедитесь, что режим транкинга успешно настроен на всех коммутаторах с помощью команды **show interface trunk** на обоих 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       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,12,333,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,12,333,999

S1#
```

```
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       1,12,333,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,12,333,999

S2#
```

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

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

```
S2(config)#interface f0/1
S2(config-if)#switchport nonegotiate
```

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

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

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

```
S2#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)#interface range f0/5-6
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 12
S1(config-if-range)#exit
S1(config)#
```

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

```
S2(config)#interface f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 12
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.

```
S1(config)#interface range f0/2-4, f0/7-24, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 999
S1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down
```

```
S2(config)#interface range f0/2-17, f0/19-24, g0/1-2
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchpot access vlan 999
                    ^
% Invalid input detected at '^' marker.

S2(config-if-range)#switchport access vlan 999
S2(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down
```

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

```
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     Link to R1         connected    12          auto    auto  10/100BaseTX
Fa0/6     Link to PC-A       connected    12          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#show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1     Link 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    Link to PC-B       connected    12          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
```

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:

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

```
S1(config)#interface f0/6
S1(config-if)#switchport 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
S1(config-if)#switchport port-security aging type inactivity
                                                 ^
% Invalid input detected at '^' marker.

S1(config-if)#switchport port-security aging ?
  time  Port-security aging time
S1(config-if)#switchport port-security aging
```

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

```
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
```

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)#interface f0/18
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#
```

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-if)#switchport port-security max 2
S2(config-if)#switchport port-security violation protect
S2(config-if)#switchport port-security aging time 60
```

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

```
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        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

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 12
```

b. Настройте магистральные порты на S2 как доверенные порты.

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

```
S2(config)#interface f0/1
S2(config-if)#ip dhcp snooping trust
S2(config-if)#exit
S2(config)#inteface f0/18
                ^
% Invalid input detected at '^' marker.

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

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

```
S2#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
12
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
S2#
```

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

```
C:\Users\Student> ipconfig /release
C:\Users\Student> ipconfig /renew
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /release
Port is not using DHCP.
C:\>ipconfig /renew

   IP Address.....................: 192.168.12.10
   Subnet Mask....................: 255.255.255.0
   Default Gateway................: 192.168.12.1
   DNS Server.....................: 0.0.0.0

C:\>
```

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

```
S2#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  ------------------
00:01:C9:3E:E6:68   192.168.12.10    0           dhcp-snooping  12    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.

```
S1(config)#interface range f0/5-6
S1(config-if-range)#spanning-tree portfast
```

```
S2(config)#interface f0/18
S2(config-if)#spa
S2(config-if)#spanning-tree portfast
```

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

```
S1(config)#interface f0/6
S1(config-if)#sp
S1(config-if)#spa
S1(config-if)#spanning-tree bpduguard enable
S1(config-if)#
```

```
S2(config)#interface f0/18
S2(config-if)#spanning-tree bpduguard enable
S2(config-if)#
```

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

```
S1#show spanning-tree interface f0/6 detail


Port 6 (FastEthernet0/6) of VLAN0012 is designated forwarding
  Port path cost 19, Port priority 128, Port Identifier 128.6
  Designated root has priority 32780, address 0060.7015.8702
  Designated bridge has priority 32780, address 0060.7015.8702
  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 default


S1#
```

Шаг 7. Проверьте наличие сквозного подключения.

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

PC-A -> PC-B:

```
C:\>ping 192.168.12.10

Pinging 192.168.12.10 with 32 bytes of data:

Reply from 192.168.12.10: bytes=32 time<1ms TTL=128
Reply from 192.168.12.10: bytes=32 time=6ms TTL=128
Reply from 192.168.12.10: bytes=32 time<1ms TTL=128
Reply from 192.168.12.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.12.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 1ms
```

PC-B -> PC-A:

```
C:\>ping 192.168.12.11

Pinging 192.168.12.11 with 32 bytes of data:

Reply from 192.168.12.11: bytes=32 time<1ms TTL=128
Reply from 192.168.12.11: bytes=32 time<1ms TTL=128
Reply from 192.168.12.11: bytes=32 time<1ms TTL=128
Reply from 192.168.12.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.12.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

PC-A -> S1:

```
C:\>ping 192.168.12.201

Pinging 192.168.12.201 with 32 bytes of data:

Reply from 192.168.12.201: bytes=32 time<1ms TTL=255
Reply from 192.168.12.201: bytes=32 time<1ms TTL=255
Reply from 192.168.12.201: bytes=32 time<1ms TTL=255
Reply from 192.168.12.201: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.12.201:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

PC-A -> S2:

```
C:\>ping 192.168.12.202

Pinging 192.168.12.202 with 32 bytes of data:

Reply from 192.168.12.202: bytes=32 time<1ms TTL=255
Reply from 192.168.12.202: bytes=32 time<1ms TTL=255
Reply from 192.168.12.202: bytes=32 time<1ms TTL=255
Reply from 192.168.12.202: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.12.202:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

PC-B -> R1:

```
C:\>ping 192.168.12.1

Pinging 192.168.12.1 with 32 bytes of data:

Reply from 192.168.12.1: bytes=32 time=1ms TTL=255
Reply from 192.168.12.1: bytes=32 time<1ms TTL=255
Reply from 192.168.12.1: bytes=32 time=13ms TTL=255
Reply from 192.168.12.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.12.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 3ms

C:\>
```

Вопросы для защиты теоретической части (глава 11)

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

Для того, чтобы предотвратить атаки 2-го уровня, которые являются одними из самых простых для развертывания хакерами, но эти угрозы также можно смягчить с помощью некоторых распространенных решений 2-го уровня.

Если активный с включенной безопасностью и к этому порту подключено более одного устройства, порт перейдет в состояние error-disabled.

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

Максимальное количество защищенных MAC-адресов, которые можно настроить, зависит от коммутатора и IOS. Может быть 8192

Коммутатор может быть настроен на изучение MAC-адресов на защищенном порту одним из трех способов:

1. Ручная конфигурация. Администратор вручную настраивает статический MAC-адрес(а)

2. Динамическое изучение. Текущий MAC-адрес источника для устройства, подключенного к порту, автоматически защищается, но не добавляется в конфигурацию запуска. Если коммутатор перезагружен, порт должен будет повторно узнать MAC-адрес устройства.

3. Динамическое изучение – Sticky. Администратор может включить коммутатор для динамического изучения MAC-адреса и «привязать» его к работающей. Сохранение текущей конфигурации передаст динамически изученный MAC-адрес в NVRAM.

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

Устаревание безопасности порта может использоваться для установки времени устаревания статических и динамических защищенных адресов на порту:

- Абсолютный. Защищенные адреса порта удаляются по истечении указанного времени устаревания.
- По таймеру неактивности. Безопасные адреса на порту удаляются, только если они неактивны в течение указанного времени.

Чтобы повторно включить порт, сначала используйте команду shutdown, затем используйте команду no shutdown, чтобы сделать порт работоспособным, как показано в примере.

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

shutdown (default) Порт немедленно переходит в состояние отключения по ошибке, выключает светодиод порта и отправляет сообщение системного журнала. Для этого режима предусмотрено увеличение значения счётчика нарушений. Когда безопасный порт находится в состоянии отключения по ошибке, администратор должен повторно включить его, введя команды shutdown и no shutdown.

restrict (ограничение) Порт отбрасывает пакеты с неизвестными адресами источника, пока вы не удалите достаточное количество безопасных MAC-адресов, чтобы опуститься ниже максимального значения или пока не увеличится максимальное значение. Этот режим вызывает увеличение счетчика нарушений безопасности и генерирует сообщение системного журнала (syslog).

protect (защита) Это наименее безопасный из режимов нарушения безопасности. Порт отбрасывает пакеты с неизвестными адресами источника, пока вы не удалите

достаточное количество безопасных MACадресов, чтобы опуститься ниже максимального значения или пока не увеличится максимальное значение. Нет сообщений в системном журнале (syslog).

Суть уязвимости заключается в том, что протокол DTP включен по умолчанию на всех современных коммутаторах Cisco. При этом каждый порт коммутатора настроен в режиме Dynamic Auto. То есть порт будет ожидать инициации транка со стороны соседа.

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

DHCP Snooping - это технология безопасности уровня 2, предназначенная для защиты от атак с использованием протокола.

Динамическая проверка ARP (DAI) требует отслеживания DHCP и помогает предотвратить атаки ARP

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

1. Включить отслеживание DHCP на глобальном уровне.
2. Включите отслеживание DHCP на выбранных VLAN.
3. Включить DAI на выбранных VLAN.
4. Настройте доверенные интерфейсы для отслеживания DHCP и проверки ARP.

Чтобы нейтрализовать атаки манипуляций с протоколом STP, используем средства защиты PortFast и Bridge Protocol Data Unit (BPDU) Guard

7. Какие шаги необходимо предпринять для устранения угрозы VLAN Hopping?

Шаг 1. Отключите согласование DTP (автоматические магистральные каналы) на немагистральных портах с помощью команды интерфейсной настройки switchport mode access.

Шаг 2. Отключите неиспользуемые порты и назначьте их неиспользуемой VLAN.

Шаг 3. Вручную включите магистральный канал на магистральном порту с помощью команды интерфейсной настройки switchport mode trunk.

Шаг 4. Установите для native VLAN, VLAN, отличную от VLAN 1, с помощью команды switchport trunk native vlan vlan_number.

8. Что рекомендуется сделать при использовании сети native VLAN? Какие два типа портов коммутаторов используются на коммутаторах Cisco в составе средств защиты от атак DHCP-спуфинга?

Установить для native VLAN, VLAN, отличную от VLAN 1.

Два типа портов коммутаторов Cisco, используемых для защиты от DHCP-спуфинга:

1) Порты доверенные (trusted ports) - принимают DHCP-ответы.

2) Порты недоверенные (untrusted ports) - DHCP-ответы с них отбрасываются.

9. Почему устройства уровня 2 считаются самым слабым звеном в инфраструктуре безопасности компании? Где хранятся динамически определяемые MAC-адреса, когда включена функция sticky learning?

Устройства уровня 2 (коммутаторы) считаются самым слабым звеном в инфраструктуре

безопасности компании, так как:

- Они работают на канальном уровне и лишены средств контроля на сетевом уровне.
- Зачастую имеют минимальные встроенные средства безопасности.
- Подвержены большому количеству потенциальных атак (VLAN Hopping, MAC Spoofing и др.).

Сохранение текущей конфигурации передаст динамически изученный MAC-адрес в NVRAM