Packet Tracer - Реализация безопасности порта

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0
PC2	NIC	10.10.10.11	255.255.255.0
Постороннее подключение	NIC	10.10.10.12	255.255.255.0

Задача

Часть 1. Настройка функции безопасности портов

Часть 2. Проверка работы функции безопасности портов

Общие сведения

В этом упражнении вы будете настраивать и проверять безопасность портов на коммутаторе. Безопасность порта позволяет вам ограничить доступность порта, ограничивая MAC-адреса, которым разрешено отправлять трафик в порт.

Часть 1. Настройка функции безопасности портов

а. Перейдите в командную строку **S1** и включите функцию безопасности на портах 0/1 и 0/2 интерфейса Fast Ethernet.

```
S1(config)# interface range f0/1 – 2
S1(config-if-range)# switchport port-security
```

б. Укажите только одно устройство в качестве максимума для доступа к портам 0/1 и 0/2 интерфейса Fast Ethernet.

```
S1(config-if-range)# switchport port-security maximum 1
```

в. Настройте функцию безопасности портов таким образом, чтобы MAC-адрес устройства распознавался динамически и добавлялся в текущую конфигурацию.

```
S1(config-if-range)# switchport port-security mac-address sticky
```

г. Настройте параметры реакции на нарушения таким образом, чтобы порты Fast Ethernet 0/1 и 0/2 не отключались при нарушении, но создавалось уведомление о нарушении безопасности и пакеты из неизвестного источника удалялись.

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

д. Отключите все неиспользуемые порты. Используйте ключевое слово**range** Чтобы данную конфигурацию можно было применить одновременно на всех портах.

```
S1(config-if-range)# interface range f0/3 - 24 , g0/1 - 2
S1(config-if-range)# shutdown
```

```
S1>enable
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int range f0/1-2
S1(config-if-range)#switchport port-security
S1(config-if-range)#switchport port-security maximum 1
S1(config-if-range)#switchport port-security mac-address sticky
S1(config-if-range)#switchport port-security violation restrict
S1(config-if-range)#int range f0/3-24, g0/1-2
S1(config-if-range)#shutdown
```

Часть 2.Проверка работы функции безопасности портов

a. От **PC1**, отправьте эхо-запрпосы к **PC2**.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.10.11

Pinging 10.10.10.11 with 32 bytes of data:

Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time=6ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 1ms
```

b.

б. running configuration. Убедитесь, что функция обеспечения безопасности портов включена, а MAC-адреса компьютеров **PC1** и **PC2** добавлены в текущую конфигурацию.

```
S1# show run | begin interface
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 00E0.B027.2245
!
interface FastEthernet0/2
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0001.647C.697E
!
```

в. Используйте команды show port security для отображения информации о конфигурации.

```
S1# show port-security
S1#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
---------------------------------------------------------------------
        Fa0/1        1           1                0         Restrict
        Fa0/2        1           1                0         Restrict
---------------------------------------------------------------------
```

```
S1# show port-security address
S1#show port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
   1    00E0.B027.2245    SecureSticky                  Fa0/1         -
   1    0001.647C.697E    SecureSticky                  Fa0/2         -
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
S1#
```

г. Подключите компьютер злоумышленника**Rogue Laptop** к любому неиспользуемому порту коммутатора и обратите внимание на индикаторы состояния канала; они должны гореть красным.

д. Включите порт и убедитесь, что **Rogue Laptop** может отправлять эхо-запросы на узлы **PC1** и **PC2**. После проверки выключите порт, используемый **Rogue Laptop.**

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:

Reply from 10.10.10.10: bytes=32 time<1ms TTL=128
Reply from 10.10.10.10: bytes=32 time<1ms TTL=128
Reply from 10.10.10.10: bytes=32 time<1ms TTL=128
Reply from 10.10.10.10: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.10.10.11

Pinging 10.10.10.11 with 32 bytes of data:

Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

е. Отключите **PC2**и подключите **Rogue Laptop**к F0/2, к которому ПК2 был первоначально подключен. Убедитесь. что **Rogue Laptop** не может отправлять эхо-запросы на узел **PC1**.

```
C:\>ping 10.10.10.11

Pinging 10.10.10.11 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.10.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

ж. Отобразите нарушения безопасности порта, подключенного к **Rogue Laptop** .

```
S1# show port-security interface f0/2
```

```
S1#show port-security interface f0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0001.647C.697E:1
Security Violation Count   : 0
```

Сколько нарушений произошло?

1

з. Отключите **Rouge Laptop** и подключите **PC2**. Проверить что **PC2** может достигнуть **PC1**. (ping)

```
C:\>ping 10.10.10.11

Pinging 10.10.10.11 with 32 bytes of data:

Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Почему узел **PC2** может отправлять эхо-запросы на **PC1**, а **Rouge Laptop** не может?

Они имеют разные mac адреса и свитч блокирует кадры от злоумышленника