**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**

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

*Откройте окно конфигурации*

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**

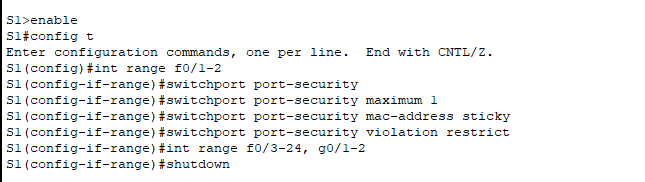
г.     Настройте параметры реакции на нарушения таким образом, чтобы порты Fast Ethernet 0/1 и 0/2 не отключались при нарушении, но создавалось уведомление о нарушении безопасности и пакеты из неизвестного источника удалялись.

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

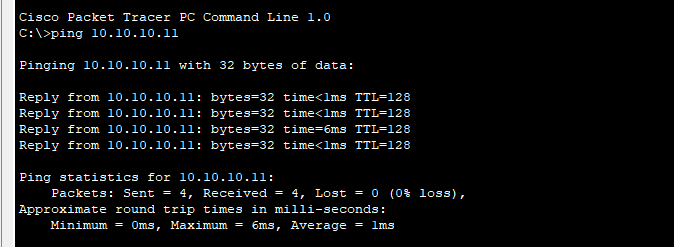
д.     Отключите все неиспользуемые порты. Используйте ключевое слово**range**Чтобы данную конфигурацию можно было применить одновременно на всех портах.

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

S1(config-if-range)#**shutdown**

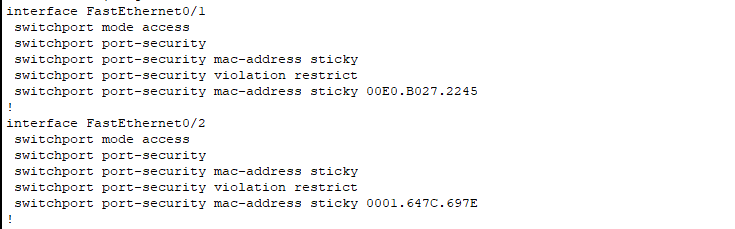


**Часть 2.Проверка работы функции безопасности портов**

1. От **PC1**, отправьте эхо-запрпосы к **PC2**.
2. 

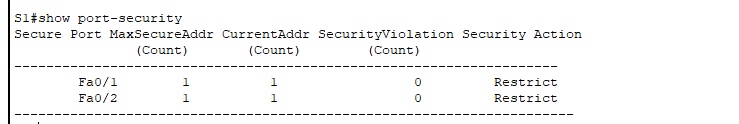
б.     running configuration. Убедитесь, что функция обеспечения безопасности портов включена, а MAC-адреса компьютеров **PC1** и **PC2** добавлены в текущую конфигурацию.

S1# **show run | begin interface**

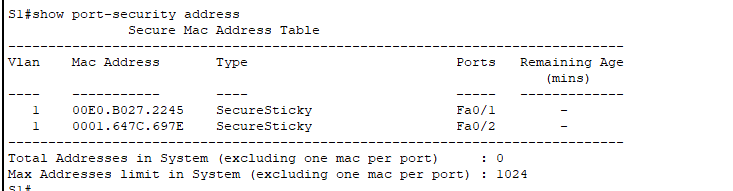


в.     Используйте команды show port security для отображения информации о конфигурации.

S1#**show port-security**

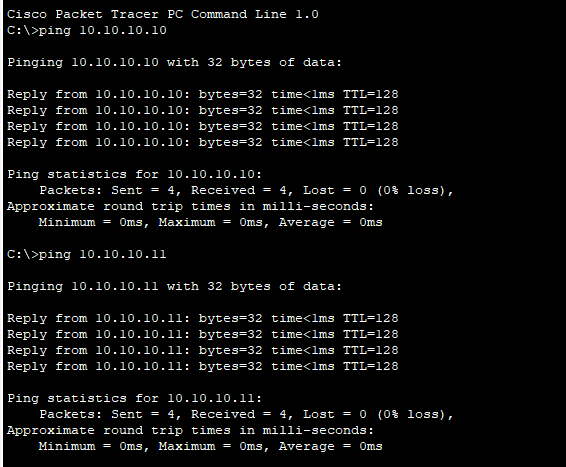


S1#**show port-security address**

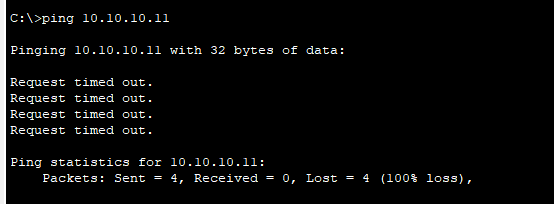


г.     Подключите компьютер злоумышленника**Rogue Laptop** к любому неиспользуемому порту коммутатора и обратите внимание на индикаторы состояния канала; они должны гореть красным.

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

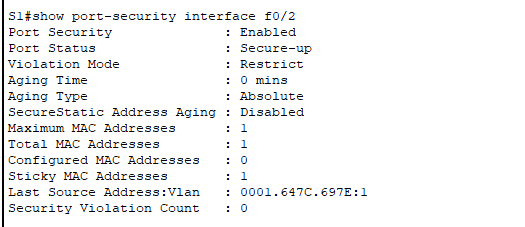


е.      Отключите **PC2**и подключите **Rogue Laptop**к F0/2, к которому ПК2 был первоначально подключен. Убедитесь. что **Rogue Laptop**не может отправлять эхо-запросы на узел **PC1**.



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

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



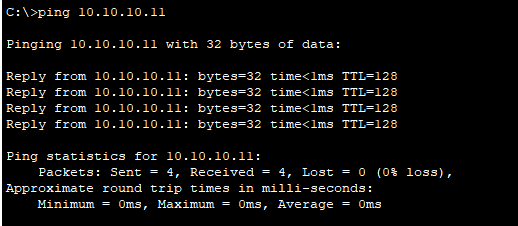
*Закройте окно настройки.*

Вопрос:

Сколько нарушений произошло?

1

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



Вопрос:

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

*Конец документа*