Packet Tracer. Настройка функции Switch Port Security

Топология

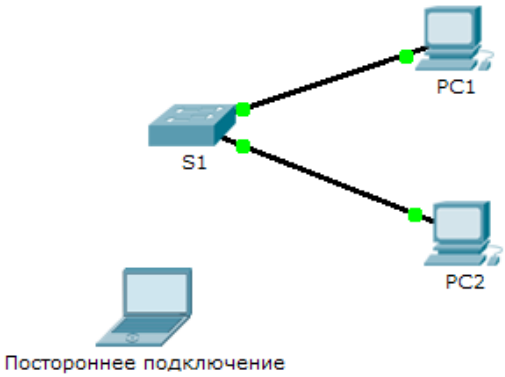

Таблица адресации

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

Исходные данные

В этом упражнении необходимо настроить и проверить функцию безопасности порта на коммутаторе. Функция безопасности порта позволяет ограничить входящий трафик порта за счёт ограничения числа MAC-адресов, которые могут использоваться для отправки трафика через этот порт.

Часть 1. Настройка функции безопасности порта

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

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

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

d. Настройте уровень нарушения безопасности таким образом, чтобы в случае атаки порты 0/1 и 0/2 Fast Ethernet оставались включёнными, а пакеты, поступающие от неизвестных источников, отбрасывались.

e. Отключите все неиспользуемые порты. Совет. Чтобы данную конфигурацию можно было применить одновременно на всех портах, используйте ключевое слово **range**.

Часть 2. Проверка функции безопасности портов

a. Отправьте эхо-запрос от узла **PC1** на **PC2**.

b. Проверьте, включена ли функция безопасности портов, и были ли добавлены MAC-адреса узлов PC1 и **PC2** в текущую конфигурацию.

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

d. Включите порт и убедитесь, что **постороннее подключение** может отправлять эхо-запросы на узлы **PC1** и **PC2**. После проверки выключите порт, используемый **посторонним подключением**.

e. Отключите **PC2** и подключите **постороннее подключение** к порту узла **PC2**. Убедитесь, что **постороннее подключение** не может отправлять эхо-запросы на узел **PC1**.

f. Отобразите нарушения безопасности порта, подключённого к **постороннему подключению**.

g. Отключите **постороннее подключение** и снова подключите узел **PC2**. Проверьте, может ли узел **PC2** отправлять эхо-запросы на узел **PC1**.

h. Почему узел **PC2** может отправлять эхо-запросы на **PC1**, а **постороннее подключение** не может?