**Port Security**

**Описание**

Технология предназначена для контроля подключенных к коммутатору устройств и предотвращения аномалий или атак, нацеленных на переполнения таблицы MAC-адресов (CAM table overflow).  
  
С помощью Port Security устанавливается максимальное количество MAC адресов на конкретный свитчпорт (сетевой порт, оперирующий на 2-ом уровне OSI) или VLAN, и контролируется доступ по заданным MAC-адресам.

**Способы работы с MAC-адресами:**

* **Dynamic** — пропускает и запоминает (на заданный период времени) любые MAC-адреса, пока не достигнет разрешенного максимума;
* **Static** — пускает только заранее введенный руками MAC-адрес (может быть использовано вместе с Dynamic типом);
* **Sticky** — учит новые MAC-адреса, записывая их в конфигурацию;

**Действия в случае превышения полномочий:**

* **Potect** — в случае лишних или не заданных МАС-адресов не пускает новые, не генерирует сислог или SNMP трап, не роняет интерфейс;
* **Restrict** — то же, что и Protect, но плюс лог и/или SNMP трап. А еще отчитывается в счетчик под show port-security interface <name>:

https://habrastorage.org/files/435/f7a/2d0/435f7a2d01ad491db6db3a08ef5a729c.png

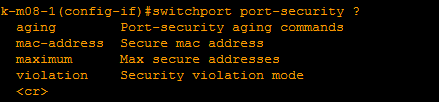
* **Shutdown** (выбран по умолчанию) — предыдущее действие, но плюс интерфейс переходит в статус *errdisable* и перестает передавать трафик;
* **Shutdown VLAN** — как и предыдущее, только в errdisable переходят все интерфейсе в данном VLAN'е;

**Конфигурация**

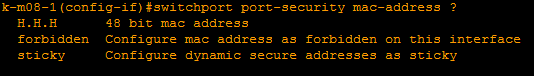
Port-Security может быть активирован только, если тип свитчпорта явно задан (т.е. или Access, или Trunk). Если порт динамический (что уже неправильно), Port-Security на нем включить не получиться.

**Access порты**

Технология задается посредством команды *switchport port-security…* в режиме конфигурации конкретного интерфейса, доступные опции:



* *aging* — задается временной интервал, после которого динамический МАС-адрес может быть переписан;
* *mac-address* — дает доступ к следующей ветке:



т.е. задаем разрешенные/запрещенные адреса или говорим железке их учить;

* *maximum* — указываем лимит разрешенных адресов.
* *violation* — задаем действие из перечисленных ранее.

Устанавливаем что нужно, что не нужно пропускаем. В конце активируем технологию командой switchport port-security без опций.  
  
В результате все выглядит примерно так:

— Если хотим разрешить неизвестно какие маки, лимитируя их количество 5-ю, ставим максимум на 5 и не задаем ничего статически. Опционально указываем время жизни.  
— Если известно, что за устройство стоит на втором конце провода и больше ничего там не будет и быть не должно — максимум=1, адрес прописываем статически.  
— Если ждем нового работника с новым ПК или лень узнавать MAC-адрес, ставим Sticky, после подключения перепроверяем.

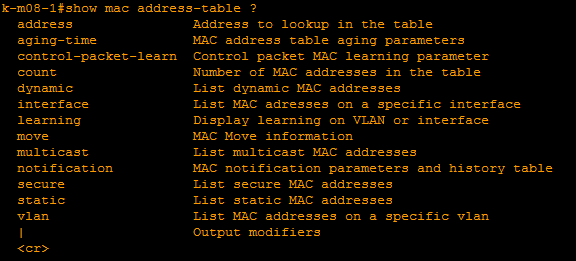
**Trunk порты**

То же самое, только можно указывать поведение не относительно физического интерфейса, а конкретного VLAN'а. Для этого к каждой из предыдущих команд в конце добавляется vlan .

**Проверка**

Не прибегая к *show run* информация касательно Port-Security может быть найдена:

* show port-security — отображает суммарно информацию об интерфейсах, их статус, количество адресов;
* show interface <name> switchport — более детальная информация (счетчики, отдельные опции);
* show mac address-table .. плюс опция, список ниже:

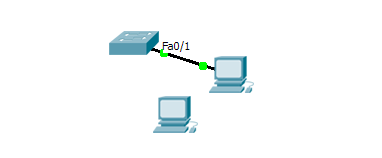


Команда проводит проверку актуальной информации о таблице MAC-адрессов. Например, нынешнее количество записей в таблице для конкретного VLAN'a и объем доступных записей проверяется посредством show mac address-table count vlan <id>:

**Задание 7.1:**

Рассмотрим базовые возможности по обеспечению безопасности на портах коммутаторов доступа.

**Топология:**



**Настройка:**

Для начала переведём порт в режим доступа (если порт находится в динамическом режиме то он просто не примет комманду switchport portsecurity)

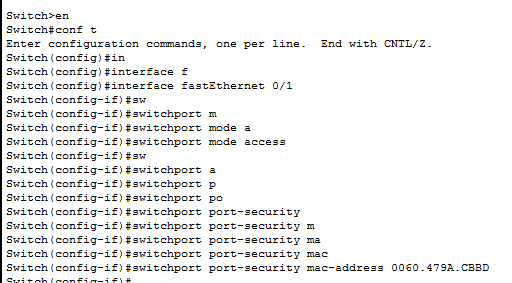
Switch(config-if)# switchport mode access

Теперь можно включать режим защиты портов:

Switch(config-if)# switchport port-security

По умолчанию, адреса источника динамически узнаются из приходящих на порт фреймов (в конфиг не записываются), но можно их прописать статически

Switch(config-if)# switchport port-security mac-address HH.HH.HH



или использовать динамическое обучение с записью в конфиг-файл:

Switch(config-if)# switchport port-security mac-address sticky



Для защиты от MAC Flood указываем количество разрешенных мак-адресов на порту (по умолчанию 1):

Switch(config-if)# switchport port-security maximum 1



Затем, нужно указать действие, которое будет применено, если свич получит на порту больше маков чем указанное максимально значение:

Switch(config-if)# switchport port-security violation protect



При превышении максимума, свич просто перестает форвардить пакеты с порта.

Switch(config-if)# switchport port-security violation restrict



В данном случае, свич перестает форвардить кадры и отсылает уведомление администратору

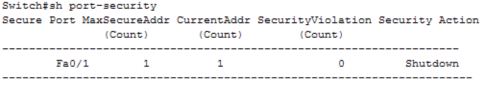
Switch(config-if)# switchport port-security violation shutdown



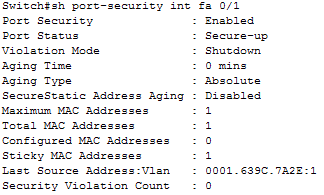
Режим по умолчанию. При превышении максимального значения порт отключается и отсылается уведомление администратору. Чтобы вернуть порт в нормальное состояние, нужно зайти на интерфейс и выполнить команды - shutdown и затем no shutdown.

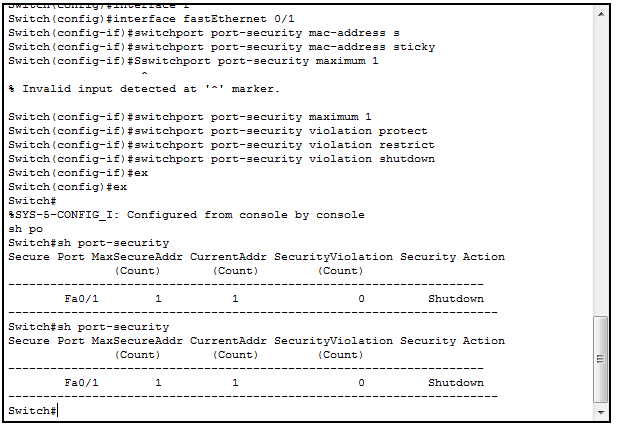
**Проверяем:**

После подключения первого ПК1 к порту коммутатора fa 0/1

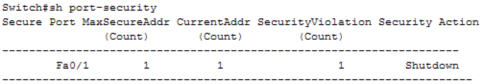


видим что счетчик сработал

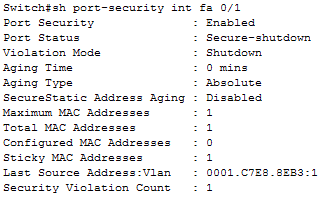


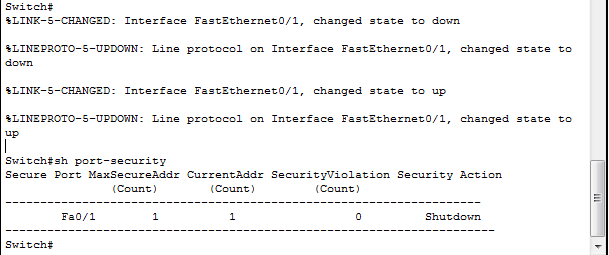


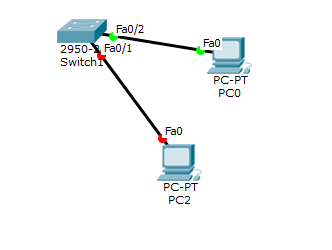
Теперь переподключаем кабель с ПК1 к ПК2



счетчик сработал второй раз и порт перешел в состояние shutdown

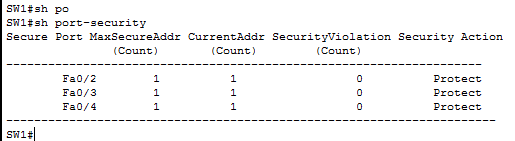




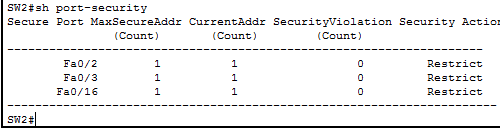


**Задание 7.2:**

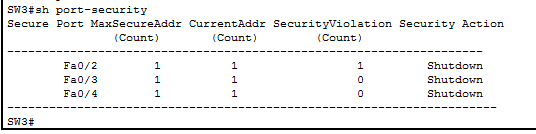
1. Скопировать файл с 1 лабораторной работой и открыть его.
2. Настроить port security все порты работающие в режиме access на коммутаторах SW1, SW2, SW3.
   1. SW1 в режиме violation protect



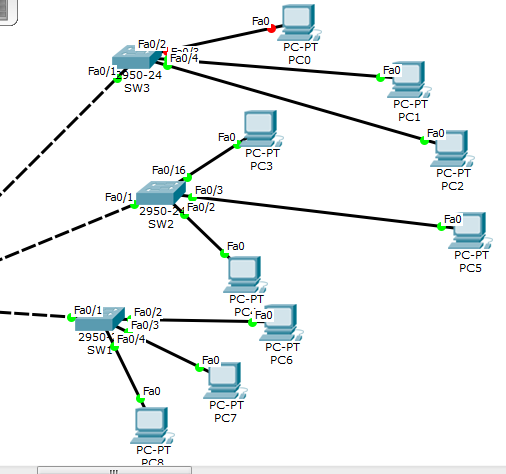
* 1. SW2 в режиме violation restrict



* 1. SW3 в режиме violation shutdown



1. Проверить работу Port Security



* 1. SW1 в режиме violation protect

Просто не отпровляет пакеты с незнакомыми mac

* 1. SW2 в режиме violation restrict

Не отпровляет пакеты с незнакомыми mac и создаёт log

* 1. SW3 в режиме violation shutdown

Отрубает порт вслучае незнакомого mac

1. Вывод

Контрольные вопросы:

1. Зачем использовать Port Security?

Для зашиты неиспользуемых портов

1. Способы работы и действия, предпринимаемые в случае превышения допустимого числа MAC-адресов?
   1. SW1 в режиме violation protect

Просто не отпровляет пакеты с незнакомыми mac

* 1. SW2 в режиме violation restrict

Не отпровляет пакеты с незнакомыми mac и создаёт log

* 1. SW3 в режиме violation shutdown

Отрубает порт вслучае незнакомого mac

1. Как конфигурировать Port Security?

Protect

Restrict

Shutdown

1. Просмотр информации о настроенных правах?

sh port-security