**Port security**

Port security — функция коммутатора, позволяющая указать MAC-адреса хостов, которым разрешено передавать данные через порт. После этого порт не передает пакеты, если MAC-адрес отправителя не указан как разрешенный. Кроме того, можно указывать не конкретные MAC-адреса, разрешенные на порту коммутатора, а ограничить количество MAC-адресов, которым разрешено передавать трафик через порт.

Используется для предотвращения:

* несанкционированной смены MAC-адреса сетевого устройства или подключения к сети,
* атак направленных на переполнение таблицы коммутации.

**Безопасные MAC-адреса**

Коммутатор поддерживает такие типы безопасных MAC-адресов:

Статические MAC-адреса:

* задаются статически командой switchport port-security mac-address mac-address в режиме настройки интерфейса,
* хранятся в таблице адресов,
* добавляются в текущую конфигурацию коммутатора;

Динамические MAC-адреса:

* динамически выучиваются,
* хранятся только в таблице адресов,
* удаляются при перезагрузке коммутатора;

Sticky MAC-адреса:

* могут быть статически настроены или динамически выучены,
* хранятся в таблице адресов,
* добавляются в текущую конфигурацию коммутатора. Если эти адреса сохранены в конфигурационном файле, после перезагрузки коммутатора, их не надо заново перенастраивать.

**Режимы реагирования на нарушения безопасности**

Нарушением безопасности для port security считаются ситуации:

* максимальное количество безопасных MAC-адресов было добавлено в таблицу адресов и хост, чей MAC-адрес не записан в таблице адресов пытается получить доступ через интерфейс,
* адрес, выученный или настроенный как безопасный на одном интерфейсе, появился на другом безопасном интерфейсе в том же VLAN'е.

На интерфейсе могут быть настроены такие режимы реагирования на нарушения безопасности:

* **protect** — когда количество безопасных MAC-адресов достигает максимального ограничения, настроенного на порту, пакеты с неизвестным MAC-адресом отправителя отбрасываются до тех пор, пока не будет удалено достаточное количество безопасных MAC-адресов, чтобы их количество было меньше максимального значения, или увеличено максимальное количество разрешенных адресов. Оповещения о нарушении безопасности нет. Режим protect не рекомендуется настраивать для транка. Этот режим выключает запоминание адресов, когда какой-либо VLAN достигает максимума адресов, даже если порт не достиг максимального ограничения.
* **restrict** — когда количество безопасных MAC-адресов достигает максимального ограничения настроенного на порту, пакеты с неизвестным MAC-адресом отправителя отбрасываются до тех пор, пока не будет удалено достаточное количество безопасных MAC-адресов, чтобы их количество было меньше максимального значения, или увеличено максимальное количество разрешенных адресов. В этом режиме при нарушении безопасности отправляется оповещение — отправляется SNMP trap, сообщение syslog и увеличивается счетчик нарушений (violation counter).
* **shutdown** — нарушение безопасности приводит к тому, что интерфейс переводится в состояние error-disabled и выключается немедленно, и выключается LED порта. Отправляется SNMP trap, сообщение syslog и увеличивается счетчик нарушений (violation counter). Когда порт в состоянии error-disabled, вывести из этого состояния его можно введя команду *errdisable recovery cause psecure-violation* или вручную включить интерфейс введя в режиме настройки интерфейса shutdown и no shutdown. Это режим по умолчанию.

**Настройка port security**

Port security настраивается в режиме настройки интерфейса. На многих коммутаторах Cisco по умолчанию порт находится в режиме dynamic auto, однако этот режим не совместим с функцией port security. Поэтому интерфейс надо перевести в режим trunk или access.

*switch(config-if)# switchport mode <access | trunk>*

Включение port security на интерфейсе (после этого включены настройки по умолчанию):

*switch(config-if)# switchport port-security*

Так как после команды switchport port-security, сразу включается Port security с настройками по умолчанию, то ее стоит давать вначале только если настройки по умолчанию подходят.

Если требуется исправить какие-то параметры, то сначала нужно их исправить, а затем включить функцию.

*switch(config)# interface Fastethernet0/3*

*switch(config-if)# switchport mode access*

*switch(config-if)# switchport port-security maximum 2*

*switch(config-if)# switchport port-security*

**Совместимость port security с другими функциями коммутатора**

Port security несовместима с такими функциями коммутатора:

* порт на котором включен DTP (switchport mode dynamic),
* интерфейс переведенный в режим третьего уровня (no switchport),
* SPAN destination port

Port security совместима с такими функциями коммутатора:

* Trunk port,
* SPAN source port,
* Tunneling port,
* Protected port,
* Voice VLAN port,
* IP Source Guard,
* Dynamic ARP Inspection.