Пример настройки Port Security

Функция **Port Security** позволяет настроить какой-либо порт коммутатора так, чтобы доступ к сети через него мог осуществляться только определёнными устройствами. Устройства, которым разрешено подключаться к порту определяются по MAC-адресам. MAC-адреса могут быть изучены динамически или вручную настроены администратором сети. Помимо этого, функция Port Security позволяет ограничивать количество изучаемых портом MAC-адресов, тем самым, ограничивая количество подключаемых к нему узлов.

Существует два режима работы функции Port Security:

- **Permanent** (Постоянный) — занесённые в таблицу коммутации MAC-адреса никогда не устаревают. Изученные MAC-адреса будут сохранены в текущей конфигурации коммутатора (running-config) и могут быть сохранены в NVRAM командой copy.
- **Delete on Timeout** (Удалить при истечении времени) — занесённые в таблицу коммутации MAC-адреса устареют и будут удалены после истечения времени, заданного командой switchport port-security aging.

Изученные портом с включенной функцией Port Security адреса называются безопасными MAC-адресами.

Если на порту достигнуто максимальное количество изученных безопасных MAC-адресов и рабочая станция с MAC-адресом неизвестным порту попытается получить к нему доступ, происходит нарушение безопасности. Их количество подсчитывается и хранится в счетчике нарушений безопасности (violation count).

При изменении режима работы функции Port Security на порту счетчик нарушений безопасности будет очищен, а записи с безопасными MAC-адресами, ранее занесенные в таблицу коммутации как постоянные будут преобразованы в динамические. Когда функция Port Security на порту отключается (disable), все записи с безопасными MAC-адресами удаляются вместе со счетчиками нарушений безопасности. При изменении конфигурации соответствующей VLAN динамические записи с безопасными MAC-адресами удаляются.

При увеличении ранее настроенного на порту значения максимального количества изучаемых адресов, уже изученные MAC-адреса останутся неизменными. При уменьшении ранее настроенного на порту значения максимального количества изучаемых адресов, команда отклоняется.

Нарушение безопасности происходит при превышении максимального числа MAC-адресов, изученных портом с функцией Port Security. Если оно произошло, порт может выполнить одно из следующих действий:

- **Защитить (Protect)**. Отбрасываются все кадры с неизвестным MAC-адресом источника. Сообщение о событии не регистрируется в системном журнале. Счетчик нарушений безопасности не увеличивается.
- **Ограничить (Restrict**). Отбрасываются все кадры с неизвестным MAC-адресом источника. Сообщение о событии регистрируется в системном журнале. Счетчик нарушений безопасности увеличивается.
- **Выключить (Shutdown)**. Порт переходит в состояние error-disabled и немедленно отключается. Сообщение о событии регистрируется в системном журнале.

Функция Port Security оказывается весьма полезной при построении домовых сетей, сетей провайдеров Интернет и локальных сетей с повышенным требованием по безопасности, где требуется исключить доступ незарегистрированных рабочих станций к услугам сети.

> **Примечание**
>
> Порт с включенной функцией Port Security имеет следующие ограничения:
>
> - функция Port Security не может быть включена одновременно с 802.1X, MAC (управление доступом на основе MAC), WAC и IMPB;
> - если порт указан в качестве порта назначения для функции зеркалирования трафика, функция Port Security не может быть включена;
> - если порт является портом-участником агрегированного канала, функция Port Security не может быть включена.

Примечание к настройке

Рассматриваемый пример настройки подходит для следующих серий коммутаторов: DGS-1250, DGS-1510, DGS-1520, DGS-3130, DGS-3630, DXS-3610.

Задача 1

В локальной сети требуется запретить подключение дополнительных рабочих станций через самовольно установленные коммутаторы и/или точки доступа. Для этого надо ограничить количество изучаемых портом коммутатора адресов одним MAC-адресом.

Решается эта задача при помощи функции **Port Security**.

Схема сети представлена на рисунке 1.

Подключенный к порту 1/0/2 управляемого коммутатора **ПК 1** получит доступ к сети. **ПК 2** и **ПК 3** подключены к порту 1/0/18 управляемого коммутатора через неуправляемый коммутатор. Доступ к сети в один момент времени получит только один из них.

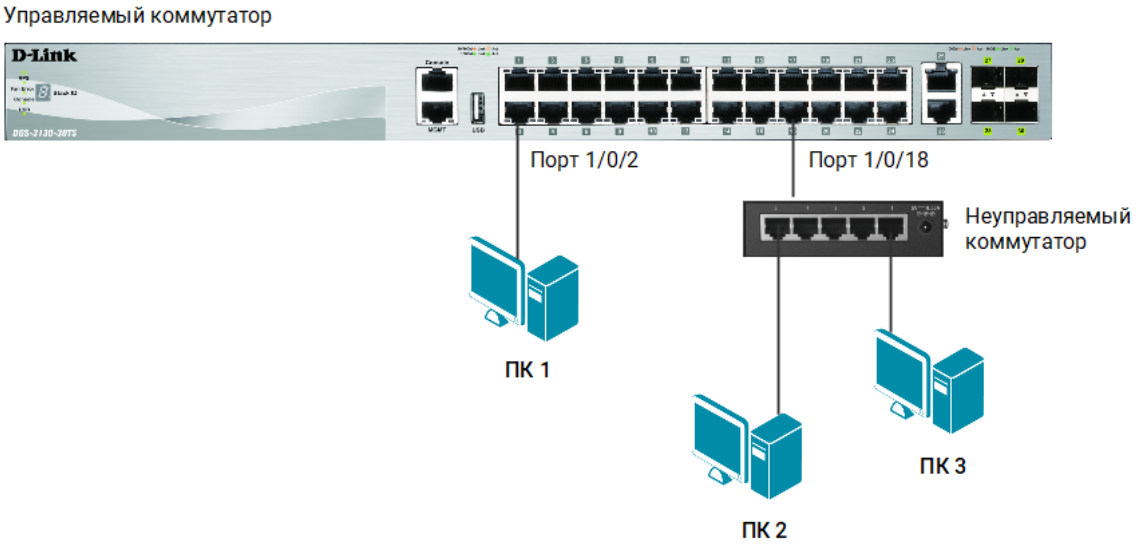

Рисунок 1. Схема подключения

Настройка коммутатора

1. Включите на портах 1/0/1-24 функцию **Port Security** и установите максимальное количество изучаемых каждым портом MAC-адресов равное 1:

```
Switch# configure terminal
Switch(config)#interface range ethernet 1/0/1-24
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switchport port-security maximum 1
```

2. Установите режим работы фунции Delete on Timeout (Удалить при истечении времени):

```
Switch(config-if-range)#switchport port-security mode delete-on-timeout
```

3. Укажите действие при превышении максимального числа MAC-адресов — Ограничить (Restrict):

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

4. Настройте время жизни для динамически изученных MAC-адресов равное 3 минутам:

```
Switch(config-if-range)# switchport port-security aging time 3
Switch(config-if-range)#end
```

Задача 2

В локальной сети требуется исключить доступ незарегистрированных рабочих станций к услугам сети. Для этого нужно запретить динамическое изучение MAC-адресов указанными или всеми портами коммутатора. В этом случае доступ к сети получат только те рабочие станции, MAC-адреса которых указаны в статической таблице коммутации.

Решается эта задача при помощи функции Port Security.

Схема сети представлена на рисунке 2.

Для **ПК 1** и **ПК 2** создаются статические записи в таблице MAC-адресов коммутатора. Динамическое изучение коммутатором MAC-адресов отключается для портов 1/0/1-24. При подключении к коммутатору новых рабочих станций в будущем, в таблице коммутации потребуется создать статические записи для них.

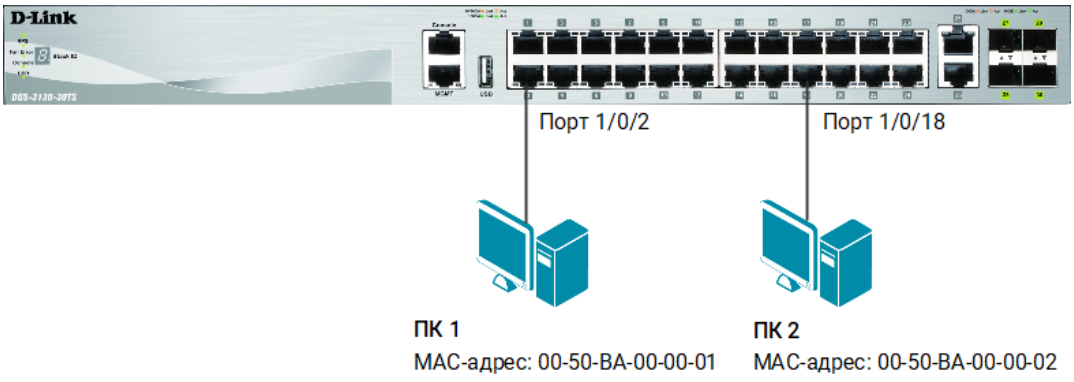

Рисунок 2. Схема подключения

Настройка коммутатора

1. Активизируйте функцию **Port Security** на портах 1/0/1-24 и запретите изучение MAC-адресов, установив параметр **maximum** равным 0:

```
Switch# configure terminal
Switch(config)#interface range ethernet 1/0/1-24
Switch(config-if-range)#switchport port-security
```

```
Switch(config-if-range)#switchport port-security maximum 0
```

2. В таблице коммутации вручную создайте статические записи для MAC-адресов рабочих станций, подключённых к портам 1/0/2 и 1/0/18 (команды вводятся в одну строку):

```
Switch(config)#mac-address-table static 0050.BA00.0001 vlan 1 interface ethernet 1/0/2
Switch(config)#mac-address-table static 0050.BA00.0002 vlan 1 interface ethernet 1/0/18
```

> **Внимание!**
>
> Замените указанные в командах MAC-адреса на реальные адреса рабочих станций, подключенных к коммутатору.