Пример настройки функции Port Security

Функция **Port Security** позволяет настроить какой-либо порт коммутатора так, чтобы доступ к сети через него мог осуществляться только определенными 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 три режима работы функции Port Security:

- **Permanent** (Постоянный) — занесенные в таблицу коммутации MAC-адреса никогда не устаревают, даже если истекло время, установленное таймером FDB Aging Time, или коммутатор был перезагружен.
- **Delete on Timeout** (Удалить при истечении времени) — занесенные в таблицу коммутации MAC-адреса устареют после истечения времени, установленного таймером FDB Aging Time, и будут удалены. Если состояние канала связи на подключенном порте изменяется, MAC-адреса, изученные на нем, удаляются из таблицы коммутации, что аналогично выполнению действий при истечении времени, установленного таймером FDB Aging Time.
- **Delete on Reset** (Удалить при сбросе настроек) — занесенные в таблицу коммутации MAC-адреса будут удалены после перезагрузки коммутатора.

При подключении неавторизованного пользователя к порту коммутатора, он будет заблокирован, а коммутатор отправит сообщение SNMP Trap или создаст запись в Log-файле, если администратор настроил выполнение этих действий. Порт коммутатора будет отбрасывать трафик, поступающий с неизвестного MAC-адреса.

Примечание к настройке

Рассматриваемые примеры настройки подходят для коммутаторов с D-Link-like CLI. Замените указанные в командах MAC-адреса на реальные адреса рабочих станций, подключенных к коммутатору.

Задача № 1

В локальной сети требуется запретить подключение дополнительных рабочих станций через самостоятельно установленные коммутаторы и/или точки доступа. Для этого необходимо ограничить количество изучаемых портом коммутатора

адресов одним MAC-адресом. Решить эту задачу можно при помощи функции Port Security.

Рабочая станция **ПК 1**, подключенная к порту 2 управляемого коммутатора, получит доступ к сети. Рабочие станции **ПК 2** и **ПК 3** подключены к порту 18 управляемого коммутатора через неуправляемый коммутатор. Доступ к сети в один момент времени получит только один из них.

Схема сети представлена на рисунке 1.

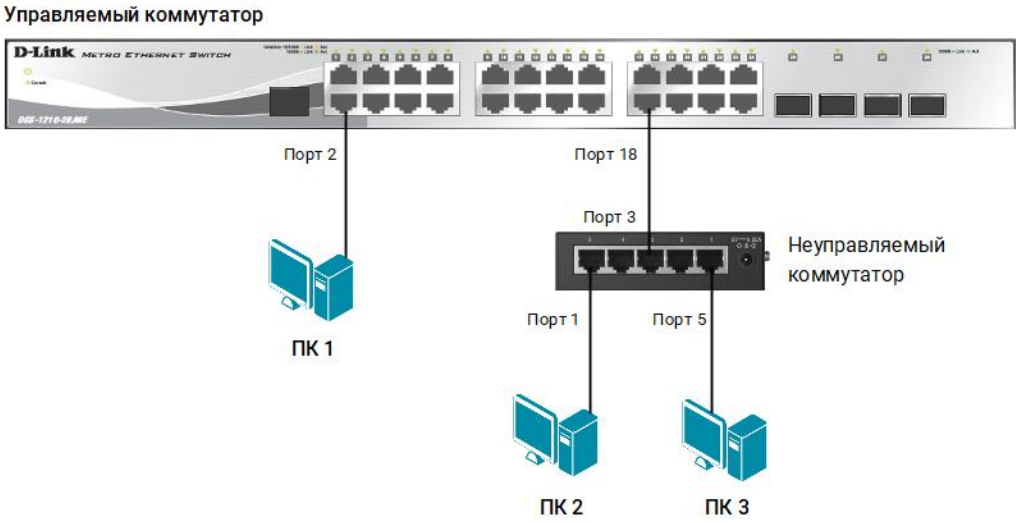

Рис. 1 Схема подключения

Настройка коммутатора

1. Включите на всех портах коммутатора функцию Port Security и установите максимальное количество изучаемых каждым портом MAC-адресов равное 1:

```
config port_security all admin_state enable max_learning_addr 1
```

2. Установите режим Delete on Timeout:

```
config port_security all lock_address_mode DeleteOnTimeout
```

3. Настройте время жизни для динамически изученных MAC-адресов (время указано в секундах):

```
config fdb aging_time 180
```

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. Решить эту задачу можно при помощи функции Port Security.

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

Схема сети представлена на рисунке 2.

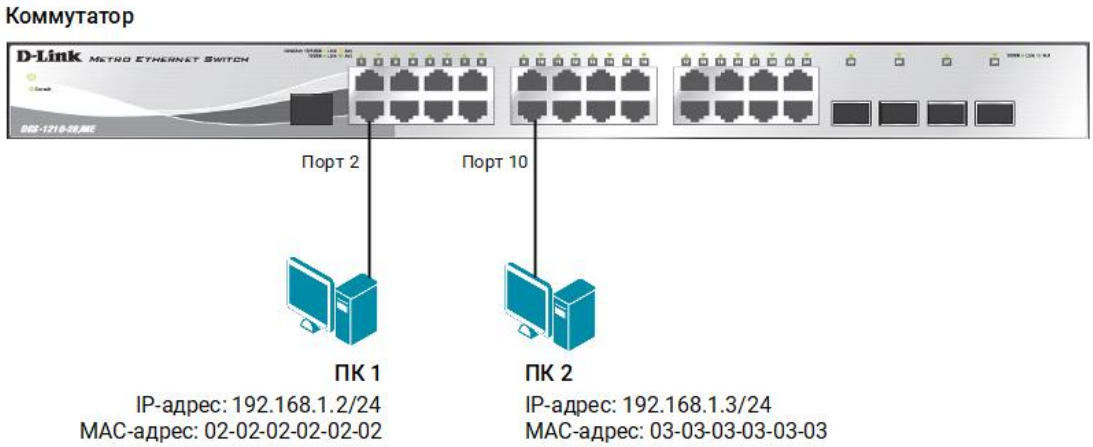

Рис. 2 Схема подключения

Настройка коммутатора

1. Активизируйте функцию Port Security на всех портах коммутатора и запретите изучение MAC-адресов:

```
config port_security 1-24 admin_state enable max_learning_addr 0
```

2. В таблице коммутации вручную создайте статические записи для MAC-адресов рабочих станций, подключённых к портам 2 и 10:

```
create fdb default 02-02-02-02-02-02 port 2
create fdb default 03-03-03-03-03-03 port 10
```