# Пример настройки Port Security через Web-интерфейс

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.

На коммутаторах серий DGS-1250, DGS-1510, DGS-1520, DGS-3130, DGS-3630, DXS-3610 поддерживаются два режима работы функции Port Security:

- **Permanent** (Постоянный) — занесённые в таблицу коммутации MAC-адреса никогда не устаревают и не будут удалены до тех пор, пока пользователь не удалит записи вручную.
- **Delete on Timeout** (Удалить при истечении времени) — занесенные в таблицу коммутации MAC-адреса устареют и будут удалены после истечения времени старения.

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

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.

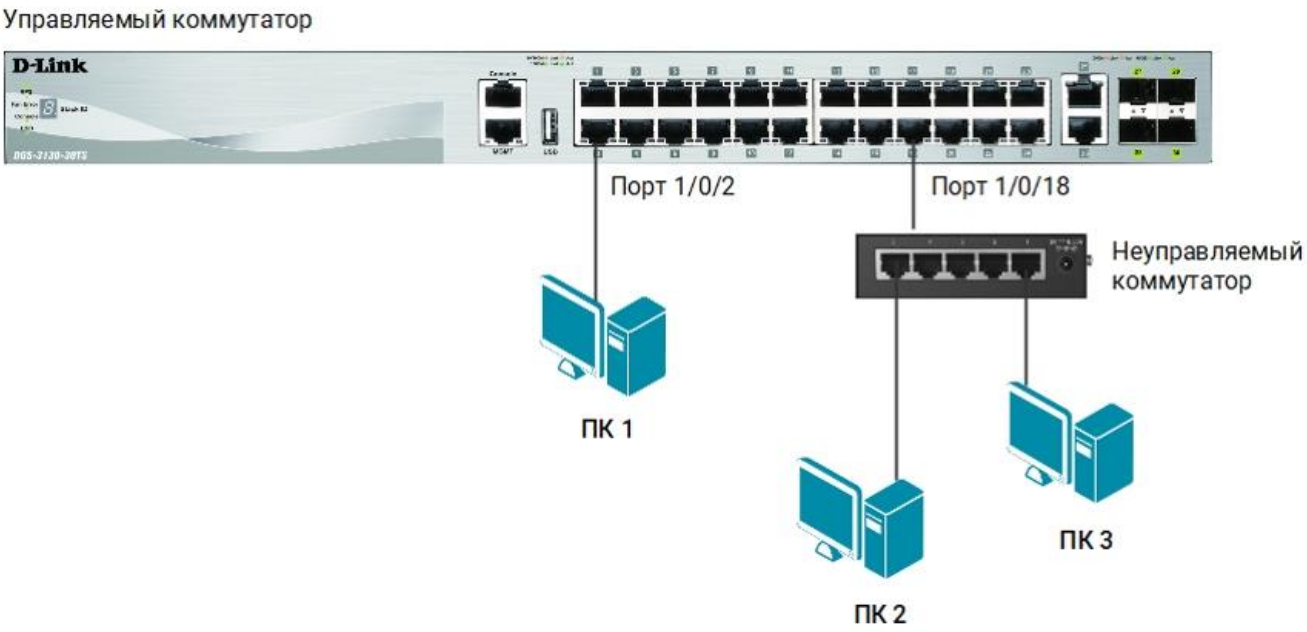
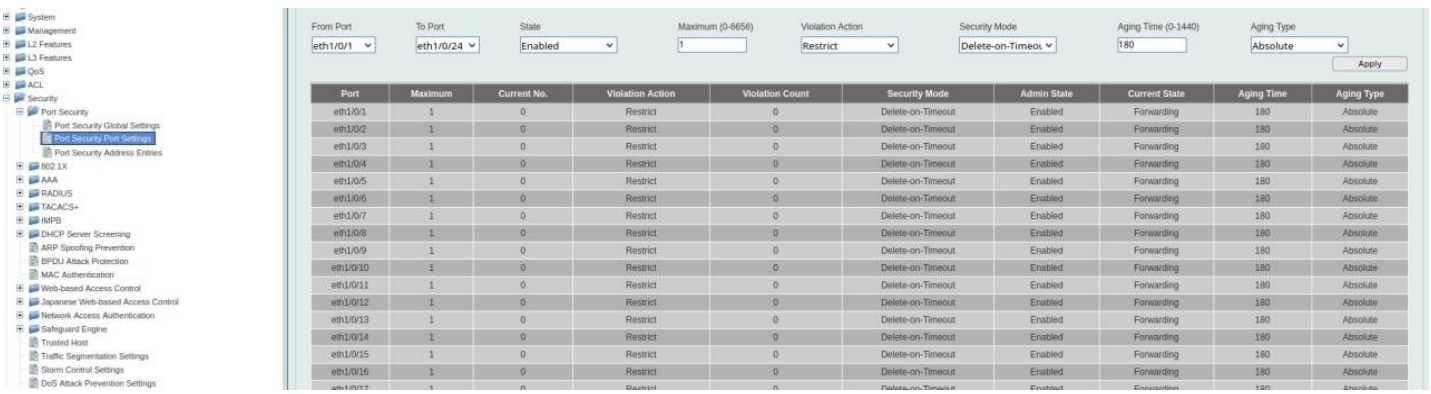



Рис. 1 Схема подключения

## Настройка коммутатора

1. В меню слева выберите **Security** → **Port Security** → **Port Security Port Settings** и укажите диапазон портов, для которых необходимо активировать функционал Port Security, выбрав соответствующие значения в полях **From Port** и **To Port** (в примере порты 1/0/1 – 1/0/24).
2. В списке **State** выберите **Enabled**.



3. В поле **Maximum** укажите максимальное количество изучаемых каждым портом MAC-адресов равное 1.
4. В списке **Violation** выберите действие при превышении максимального числа MAC-адресов — **Restrict** (Ограничить).
5. В списке **Security Mode** выберите режим работы функции – **Delete-on-Timeout** (Удалить при истечении времени).
6. В поле **Aging Time** укажите время старения для динамически изученных MAC-адресов равное 3 минутам (180 с).
7. Нажмите **Apply**.
8. Чтобы сохранить выполненные настройки, в левом верхнем углу нажмите **Save**, выберите **Save Configuration** и нажмите **Apply**.