**Лабораторная работа № 5**

**Контроль над подключением узлов к портам коммутатора.**

**Функция Port Security**

**Цель:** научиться управлять подключением узлов к портам коммутатора и изучить настройку функции Port Security на коммутаторах D-Link.

1. **Краткие теоретические сведения**

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 МАС-адресам. МАС-адреса могут быть изучены динамически или вручную настроены администратором сети. Помимо этого функция Port Security позволяет ограничивать количество изучаемых портом МАС-адресов, тем самым, ограничивая количество подключаемых к нему узлов.

Существует три режима работы функции Port Security:

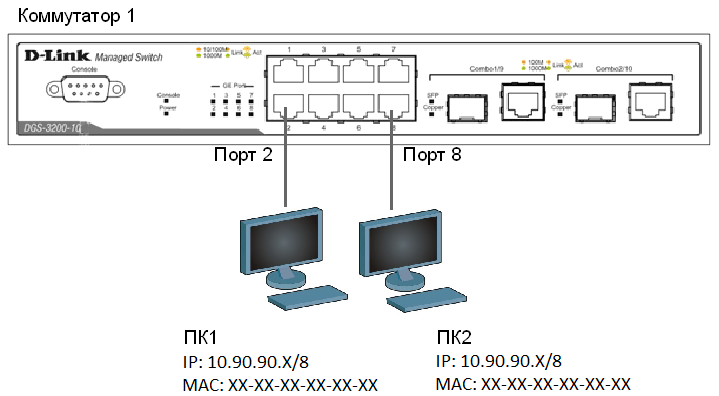
* *Permanent* (Постоянный) – занесенные в таблицу коммутации МАС-адреса никогда не устаревают, даже если истекло время, установленное таймером Aging Time или коммутатор был перезагружен.
* *Delete on Timeout* (Удалить при истечении времени) – занесенные в таблицу коммутации МАС-адреса устареют после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

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

Используя функцию Port Security можно полностью запретить динамическое изучение МАС-адресов указанными или всеми портами коммутатора. В этом случае доступ к сети получат только те пользователи, МАС-адреса которых указаны в статической таблице коммутации.

**2. Порядок выполнения**

Собрать схему согласно рисунку ниже. В качестве IP и MAC адресов использовать реальные адреса, установленные в конфигурациях сетевых адаптеров учебных компьютеров.



**Задание 1**

**Управление количеством подключаемых к портам коммутатора пользователей, путем ограничения максимального количества**

**изучаемых МАС-адресов**

Сбросьте настройки коммутатора к заводским настройкам по умолчанию командой:

reset config

Проверьте информацию о настройках Port Security:

show port\_security

Установите максимальное количество изучаемых портом № 8 МАС-адресов равным 2, а портом № 2 равным 1 и включите функцию на всех портах:

config port\_security ports 8 admin\_state enable max\_learning\_addr 2

config port\_security ports 2 admin\_state enable max\_learning\_addr 1

**Подключите ПК1 и ПК2 к портам 2 и 8 коммутатора соответственно.**

Посмотрите MAC-адреса, которые стали известны портам 2 и 8:

show fdb port 2

show fdb port 8

Проверьте, соответствуют ли зарегистрированные адреса адресам рабочих станций:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Проверьте информацию о настройках Port Security на портах коммутатора:

show port\_security ports 1-24

Настройте запись в log-файл MAC-адресов, подключающихся к порту станций и отправку сообщений SNMP Trap:

enable port\_security trap\_Log

Выполните тестирование доступности узлов командой ping от ПК1 к ПК2 и наоборот.

**Подключите ПК1 к порту 8, а ПК2 к порту 2.**

Повторите тестирование соединения между рабочими станциями командой ping.

Проверьте информацию в log-файле коммутатора:

show log

Какой вы сделаете вывод?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Сохраните конфигурацию и перезагрузите коммутатор:

save

reboot

Выполните тестирование соединения между рабочими станциями командой ping.

Какой вы сделаете вывод? Сохраняется ли информация о привязке MAC-port?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Настройте на порте 2 работу функции Port Security в режиме Permanent и максимальное количество изучаемых адресов равное 1:

config port\_security ports 2 admin\_state enable max\_learning\_addr 1 lock\_address\_mode Permanent

Сохраните конфигурацию и перезагрузите коммутатор:

save

reboot

Проверьте информацию о настройках Port Security на портах коммутатора:

show port\_security ports 1-24

Какой вы сделаете вывод? Сохраняется информации о привязке MAC-порт?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Очистите информацию о привязке MAC-порт на порте 2:

clear port\_security\_entry port 2

Отключите работу функции Port Security на порте 2 и приведите настройки в исходное (по умолчанию) состояние:

config port\_security ports 2 admin\_state disable max\_learning\_addr 1 lock\_address\_mode DeleteOnReset

Посмотрите время таймера блокирования (он соответствует времени жизни MAC-адреса в таблице коммутации):

show fdb aging\_time

Запишите это значение \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Изменить время действия таймера можно с помощью настройки времени жизни MAC-адреса в таблице коммутации (время указано в секундах):

config fdb aging\_time 20

Измените режим работы функции Port Security на Delete on Timeout:

config port\_security ports 2 admin\_state disable max\_learning\_addr 1 lock\_address\_mode DeleteOnTimeout

Проверьте MAC-адреса, которые стали известны порту 2:

show fdb port 2

Проверьте информацию о настройках Port Security на портах коммутатора:

show port\_security ports 1-24

Выполните тестирование соединения между ПК1 и ПК2 командой ping.

Какой вы сделаете вывод? Сохраняется информации о привязке MAC-порт?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Отключите работу функции Port Security на портах:

config port\_security ports 1-24 admin\_state disable

Отключите функцию записи в log-файл и отправки SNMP Trap:

disable port\_security trap\_Log

*Примечание: после выполнения обучения имеется возможность отключить функцию динамического изучения MAC-адресов, тогда в таблице коммутации сохранятся изученные адреса. Таким образом, текущая конфигурация сети будет сохранена, и дальнейшее подключение новых устройств без ведома администратора будет невозможно. Новые устройства можно добавить путем создания статических записей в таблице коммутации.*

**Задание 2**

**Настройка защиты от подключения к портам, основанной на статической таблице MAC-адресов**

**Подключите компьютер ПК1, через который управляете коммутатором, к порту №1**

Сбросьте настройки коммутатора к заводским настройкам командой:

reset system

Активизируйте функцию Port Security на портах 2-24 и запретите изучение МАС-адресов (параметр *max\_learning\_addr* установить равным 0):

config port\_security ports 2-24 admin\_state enable max\_learning\_addr 0

Проверьте состояние портов:

show ports

Подключите ПК2 к порту №8 и проверьте соединение между ПК1 и ПК2 командой ping.

Проверьте состояние таблицы коммутации:

show fdb

Имеются ли там записи для порта №8? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

В таблице коммутации для порта 8 вручную создайте статическую запись для MAC-адреса рабочей станции ПК2.

**Внимание**! **Замените указанные в команде МАС-адрес на реальный адрес рабочей станции, подключаемой к коммутатору.**

create fdb default ХХ-ХХ-ХХ-ХХ-ХХ-ХХ port 8

Проверьте созданные статические записи в таблице коммутации:

show fdb

Проверьте информацию о настройках Port Security на портах коммутатора:

show port\_security ports 1-24

Проверьте соединение между ПК1 и ПК2 командой ping.

**Переключите ПК2 из порта 8 в порт 2.**

Повторите тестирование командой ping.

Какой вы сделаете вывод?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_