**Лабораторная работа №2.**

**Защита портов коммутатора.**

**Студент Кущ Артем, БПМ-18-1.**

Оглавление

[Теоретическая часть 3](#_Toc35970546)

[Команды 3](#_Toc35970547)

[Практическая часть 4](#_Toc35970548)

[Настройка схемы 4](#_Toc35970549)

[IP-адреса: 5](#_Toc35970550)

[Анализ MAC-адресов в CAM таблице 5](#_Toc35970551)

[CDP 6](#_Toc35970552)

[Дуплекс, скорость, отключение портов 7](#_Toc35970553)

[Настройка безопасности портов 8](#_Toc35970554)

[Вывод 10](#_Toc35970555)

# Теоретическая часть

## Команды

show cdp – получение информации о «соседях» посредством протокола cdp

show mac address-table– просмотр CAM-таблицы коммутатора

show arp – просмотр данных arp протокола

show interfaces status – просмотр статуса интерфейсов

clear mac address-table – очистка CAM-таблицы коммутатора

shutdown – выключение порта

no shutdown– включение порта

duplex – определение режима дуплекса порта (full half auto)

speed – определение режима скорости порта (10 100 auto)

switchport mode access – перевод порта в режим доступа (access); задается на настраиваемом интерфейсе

switchport port-security - включение функции безопасности порта; задается на настраиваемом интерфейсе

switchport port-security maximum <количество адресов> - настройка функции безопасности порта; максимальное количество адресов на порту

switchport port-security violation <реакция на нарушение> - настройка функции безопасности порта; реакция на нарушение настройки безопасности

switchport port-security mac-address <MAC-адрес / sticky> - настройка функции безопасности порта; привязка статического адреса или установление режима sticky.

show port-security – просмотр настроек безопасности

show port-security interface <имя интерфейса> – просмотр настроек безопасности на данном интерфейсе

show port-security address – просмотр адресов настроек безопасности

interface range <имя интерфейса> – обращение к диапазону интерфейсов

CDP:

*show cdp neighbors*

*show cdp neighbors detail = show cdp entry \**

Настройка:

*cdp timer 5* - время в секундах через которое отправлять пакеты cdp  
*cdp holdtime 10* - время в секундах через которое пакет cdp от соседа считать не действительным  
*no cdp run / cdp run* - отключает\включает протокол CDP на устройстве

*no cdp enable / cdp enable* - отключает\включает протокол CDP на интерфейсе

Прочее:

*show cdp*

*show cdp traffic*

*show cdp interface*

# Практическая часть

## Настройка схемы

1. Собрал схему.

enable

configure terminal

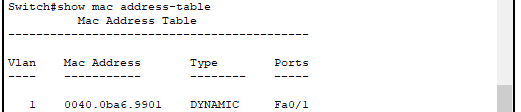
interface vlan 1

ip address 192.168.1.1 255.255.255.0

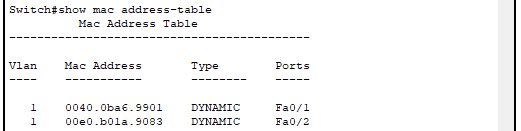
no shutdown

end

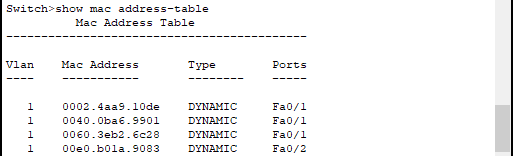
1. С помощью скрипта настроил каждый коммутатор. Каждому задал уникальный IP адрес.
2. Добавил два PC: к первому и последнему коммутатору соответственно. Каждому присвоил IP адрес.
3. Проверил соединение с каждым устройством с помощью команды ***ping.***
4. Прописал команду ***show mac address-table*** на 1 коммутаторе, получил MAC-адрес порта, через который подключен другой коммутатор:

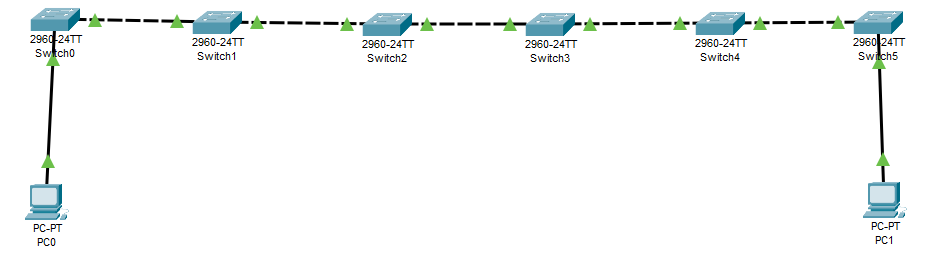


1. Прописал команду ping 192.168.1.10 (IP-адрес PC), чтобы получить MAC-адрес порта, через который подключен PC-0. После снова прописал ***show mac address-table:***



1. Пропинговал ещё несколько коммутаторов:



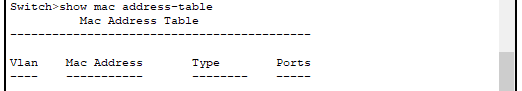


## IP-адреса:

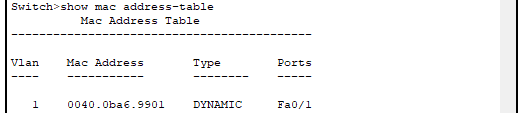
* PC:
  + 192.168.1.10-11
* Switch:
  + 192.168.1.1-6

## Анализ MAC-адресов в CAM таблице

1. Выберем коммутатор, допустим, №1. Выполним ***reload*** с сохранением настроек.
2. На данный момент таблица пуста:



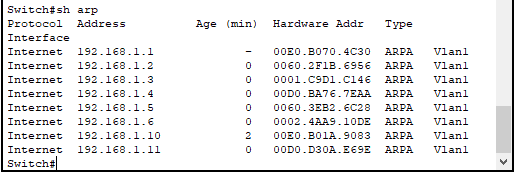
Но спустя некоторое время в ней появился один MAC-адрес, подключенный через порт ***f0/1***:

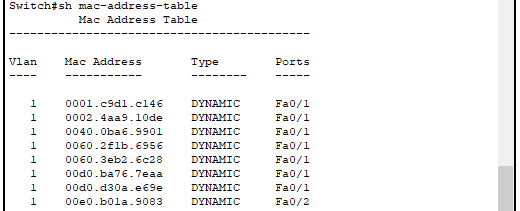


Давайте посмотрим ARP-таблицу ***show arp***. Она пуста, что логично:



1. Попробуем выяснить, какое устройство имеет MAC-адрес **0040.0ba6.9901**. Для этого нужно пропинговать все устройства в сети.
2. Посмотрим на ARP-таблицу и CAM-таблицу:





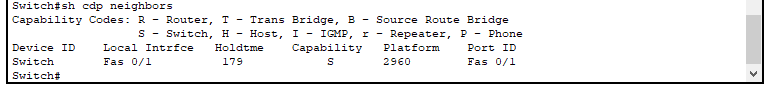
1. IP с MAC-адресом **0040.0ba6.9901** найдено не было. Отсюда следует вывод, что данный MAC-адрес принадлежит устройству Switch-0.

Все остальные адреса принадлежат остальным коммутаторам и PC.

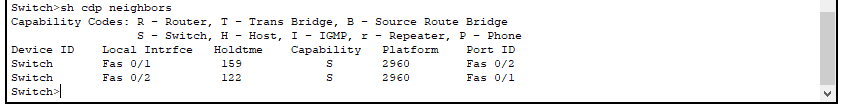
## CDP

1. Команда ***sh cdp neighbors*** показывает соседние устройства. Например:

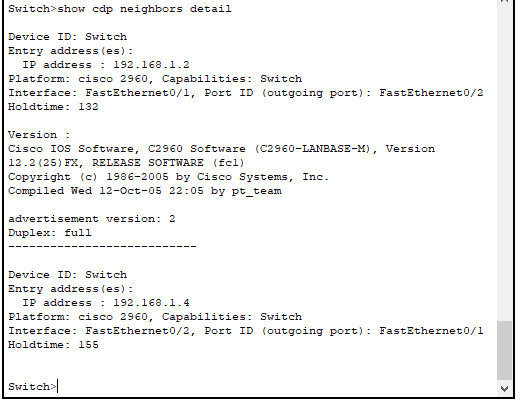
Для коммутатора №1:



Для коммутатора №3:



1. Команда ***show cdp neighbors detail*** отображает подробную информацию о соседе:



enable

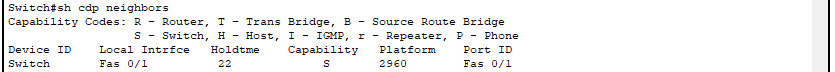
configure terminal

interface f0/1

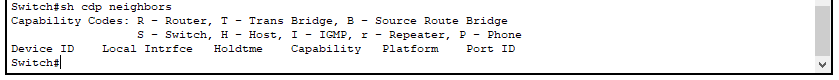
no cdp enable

end

1. Чтобы выключить CDP-обнаружение нужно выполнить данный скрипт:



По истечению времени сосед пропадает из списка:



## Дуплекс, скорость, отключение портов

1. Не работает:
   1. Разные настройки дуплекса на соединенных портах.
   2. Разные настройки скорости на соединенных портах.
   3. Один из портов отключен.
2. Работает:
   1. Правильно настроен дуплекс.
   2. Правильно настроена скорость.
   3. Порты включены.

## Настройка безопасности портов

1. Все порты находятся в режиме ***access*** (не dynamic!!!).
2. Настроил тестовый порт ***f0/3*** на Switch-0 с помощью скрипта:
3. Теперь подключим тестовый коммутатор к порту ***f0/3.*** Настроим сам коммутатор с помощью скрипта:

enable

configure terminal

interface f0/3

switchport mode access

switchport port-security

switchport port-security maximum 1

switchport port-security violation shutdown

no shutdown

end

enable

configure terminal

interface vlan 1

ip address 192.168.1.100 255.255.255.0

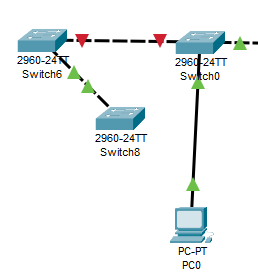
no shutdown

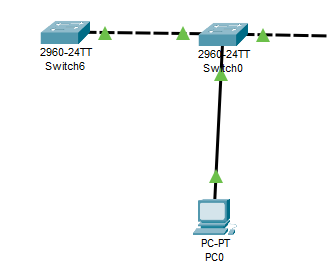
end

1. Все работает отлично до тех пор, пока к новому коммутатору не попробует подсоединиться какое-либо устройство.

Создадим ещё один коммутатор. Зададим ему IP адрес и включим порт. Сразу после этого Switch-0 отключит порт ***f0/3***.

**Было: Стало:**





1. Теперь попробуем расширить количество устройств. Вернемся к нашей начальной сети.

Мы хотим отключать доступ порт ***f0/2*** в том случае, если MAC-адрес устройства окажется другим. Например, в случае использование другого PC в этом же порту. А также ограничить максимальное количество устройств в сети.

Для этого нужно настроить Switch-0.

enable

configure terminal

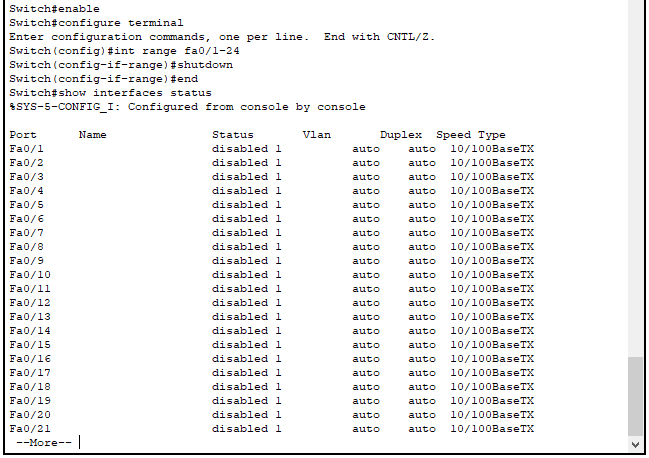
int range fa0/1-24

shutdown

end

show interfaces status

* 1. Отключим все порты с помощью скрипта и сразу проверим:



* 1. Все проделано верно. Порты отключены.
  2. Теперь настроим порт ***f0/2:***
     1. Введем команду на PC-0 ***ipconfig /all.*** Физический MAC-адрес **00E0.B01A.9083.**
     2. Выполним скрипт на коммутаторе:

enable

configure terminal

int range fa0/2

switchport mode access

switchport port-security

switchport port-security maximum 1

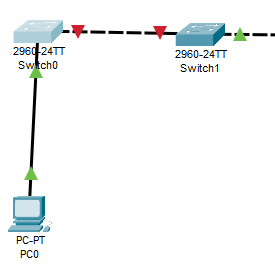
switchport port-security violation shutdown

switchport port-security mac-address 00E0.B01A.9083

no shutdown

end

* 1. PC-0 успешно подключен:



* 1. Теперь займемся настройкой порта ***f0/1***. Нужно ограничить максимальное количество устройств в сети. Но отключать порт на этот раз не будем, а просто обойдемся блокировкой пересылки пакетов.
     1. Выполним скрипт на коммутаторе:

enable

configure terminal

int f0/1

switchport mode access

switchport port-security

switchport port-security maximum 7

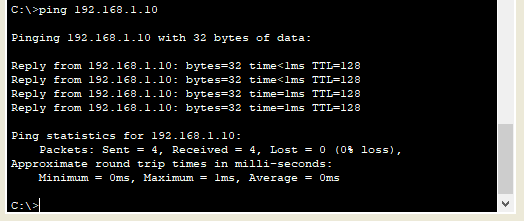
switchport port-security violation protect

no shutdown

end

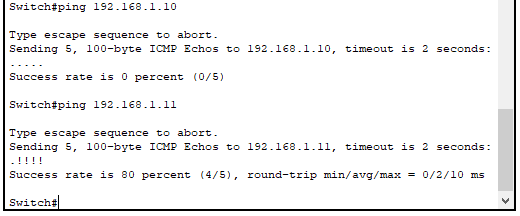
* + 1. Все работает.
  1. Проверим нашу настройку. Зайдем в терминал PC-1 и пропингуем PC-0.

Успешно.

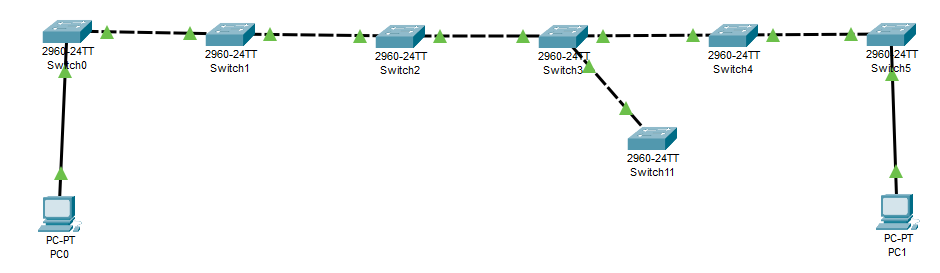


Теперь добавим в нашу схему коммутатор, зададим ему IP и подключим в любой свободный порт. Так как устройств стало больше допустимых, пакеты просто не доходят от нового коммутатора.

* 1. В итоге, с коммутатора не удалось достучаться до PC-0, но удалось до PC-1.



Итоговая схема такова:



# Вывод

Собрал сеть из 5 коммутаторов, подключил в нее 2 PC и защитил.