Лабораторная работа №2.
Защита портов коммутатора.

Студент Кущ Артем, БПМ-18-1.

Оглавление

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

```
enable
configure terminal

interface vlan 1
ip address
192.168.1.1
255.255.255.0
no shutdown
end
```

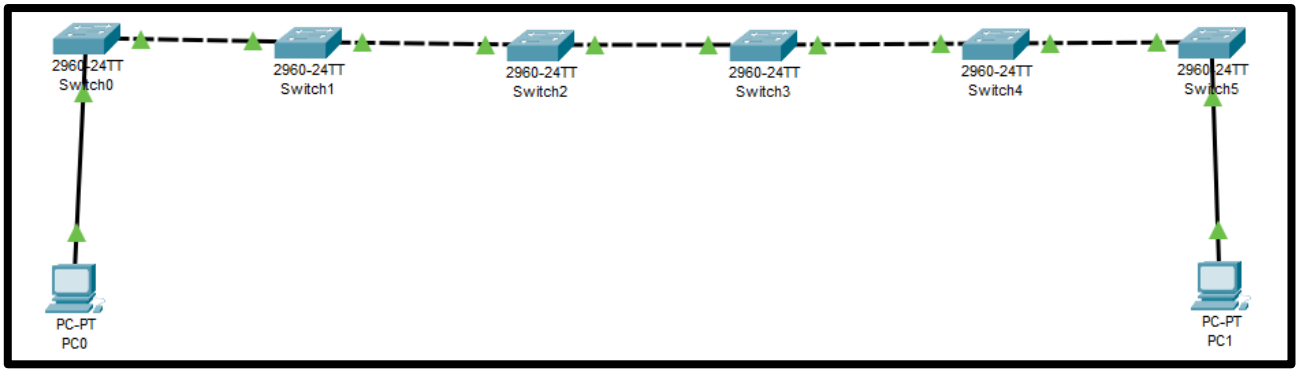
```
Switch#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0040.0ba6.9901    DYNAMIC     Fa0/1
```

6) 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:***

```
Switch#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0040.0ba6.9901    DYNAMIC     Fa0/1
   1    00e0.b01a.9083    DYNAMIC     Fa0/2
```

7) Пропинговал ещё несколько коммутаторов:

```
Switch>show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0002.4aa9.10de    DYNAMIC     Fa0/1
   1    0040.0ba6.9901    DYNAMIC     Fa0/1
   1    0060.3eb2.6c28    DYNAMIC     Fa0/1
   1    00e0.b01a.9083    DYNAMIC     Fa0/2
```



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:

```
Switch>show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
```

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

```
Switch>show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0040.0ba6.9901    DYNAMIC     Fa0/1
```

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

```
Switch>show arp
```

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

```
Switch#sh arp
Protocol  Address          Age (min)  Hardware Addr   Type
Interface
Internet  192.168.1.1            -   00E0.B070.4C30  ARPA   Vlan1
Internet  192.168.1.2            0   0060.2F1B.6956  ARPA   Vlan1
Internet  192.168.1.3            0   0001.C9D1.C146  ARPA   Vlan1
Internet  192.168.1.4            0   00D0.BA76.7EAA  ARPA   Vlan1
Internet  192.168.1.5            0   0060.3EB2.6C28  ARPA   Vlan1
Internet  192.168.1.6            0   0002.4AA9.10DE  ARPA   Vlan1
Internet  192.168.1.10           2   00E0.B01A.9083  ARPA   Vlan1
Internet  192.168.1.11           0   00D0.D30A.E69E  ARPA   Vlan1
Switch#
```

```
Switch#sh mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.c9d1.c146    DYNAMIC     Fa0/1
   1    0002.4aa9.10de    DYNAMIC     Fa0/1
   1    0040.0ba6.9901    DYNAMIC     Fa0/1
   1    0060.2f1b.6956    DYNAMIC     Fa0/1
   1    0060.3eb2.6c28    DYNAMIC     Fa0/1
   1    00d0.ba76.7eaa    DYNAMIC     Fa0/1
   1    00d0.d30a.e69e    DYNAMIC     Fa0/1
   1    00e0.b01a.9083    DYNAMIC     Fa0/2
```

5) 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:

```
Switch#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform    Port ID
Switch       Fas 0/1          179            S       2960        Fas 0/1
Switch#
```

   Для коммутатора №3:

```
Switch>sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform    Port ID
Switch       Fas 0/1          159            S       2960        Fas 0/2
Switch       Fas 0/2          122            S       2960        Fas 0/1
Switch>
```

2) Команда ***show cdp neighbors detail*** отображает подробную информацию о соседе:

```
Switch>show cdp neighbors detail

Device ID: Switch
Entry address(es):
  IP address : 192.168.1.2
Platform: cisco 2960, Capabilities: Switch
Interface: FastEthernet0/1, Port ID (outgoing port): FastEthernet0/2
Holdtime: 132

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version
12.2(25)FX, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

advertisement version: 2
Duplex: full
---------------------------

Device ID: Switch
Entry address(es):
  IP address : 192.168.1.4
Platform: cisco 2960, Capabilities: Switch
Interface: FastEthernet0/2, Port ID (outgoing port): FastEthernet0/1
Holdtime: 155


Switch>
```

3) Чтобы выключить CDP-обнаружение нужно выполнить данный скрипт:

```
enable
configure terminal
interface f0/1
no cdp enable
end
```

```
Switch#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform    Port ID
Switch       Fas 0/1          22             S       2960        Fas 0/1
```

По истечению времени сосед пропадает из списка:

```
Switch#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform    Port ID
Switch#
```

Дуплекс, скорость, отключение портов

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

Настройка безопасности портов

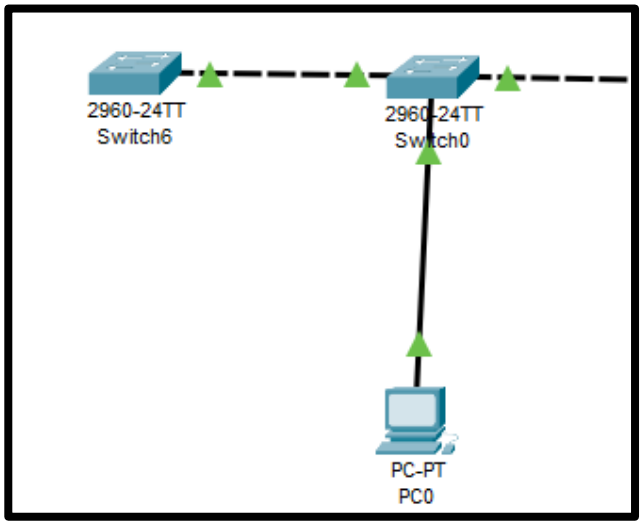
1) Все порты находятся в режиме ***access*** (не dynamic!!!).
2) Настроил тестовый порт ***f0/3*** на Switch-0 с помощью скрипта:
3) Теперь подключим тестовый коммутатор к порту ***f0/3.*** Настроим сам коммутатор с помощью скрипта:

```
enable
configure terminal
interface vlan 1
ip address 192.168.1.100 255.255.255.0
no shutdown
end
```

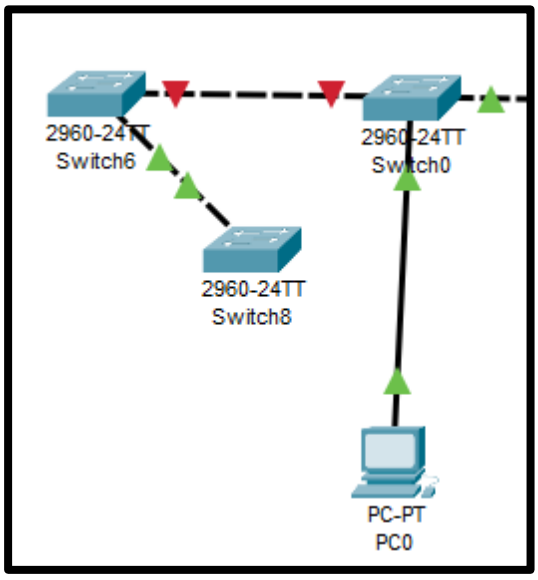
```
enable
configure terminal
interface f0/3
switchport mode access
switchport port-security
switchport port-security maximum 1
switchport port-security violation shutdown
no shutdown
end
```

4) 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:



5) 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.
   a. Отключим все порты с помощью скрипта и сразу проверим:

```
enable
configure terminal
int range fa0/1-24
shutdown
end
show interfaces status
```

```
Switch#enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int range fa0/1-24
Switch(config-if-range)#shutdown
Switch(config-if-range)#end
Switch#show interfaces status
%SYS-5-CONFIG_I: Configured from console by console

Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        disabled 1          auto    auto  10/100BaseTX
Fa0/2                        disabled 1          auto    auto  10/100BaseTX
Fa0/3                        disabled 1          auto    auto  10/100BaseTX
Fa0/4                        disabled 1          auto    auto  10/100BaseTX
Fa0/5                        disabled 1          auto    auto  10/100BaseTX
Fa0/6                        disabled 1          auto    auto  10/100BaseTX
Fa0/7                        disabled 1          auto    auto  10/100BaseTX
Fa0/8                        disabled 1          auto    auto  10/100BaseTX
Fa0/9                        disabled 1          auto    auto  10/100BaseTX
Fa0/10                       disabled 1          auto    auto  10/100BaseTX
Fa0/11                       disabled 1          auto    auto  10/100BaseTX
Fa0/12                       disabled 1          auto    auto  10/100BaseTX
Fa0/13                       disabled 1          auto    auto  10/100BaseTX
Fa0/14                       disabled 1          auto    auto  10/100BaseTX
Fa0/15                       disabled 1          auto    auto  10/100BaseTX
Fa0/16                       disabled 1          auto    auto  10/100BaseTX
Fa0/17                       disabled 1          auto    auto  10/100BaseTX
Fa0/18                       disabled 1          auto    auto  10/100BaseTX
Fa0/19                       disabled 1          auto    auto  10/100BaseTX
Fa0/20                       disabled 1          auto    auto  10/100BaseTX
Fa0/21                       disabled 1          auto    auto  10/100BaseTX
 --More--
```

b. Все проделано верно. Порты отключены.

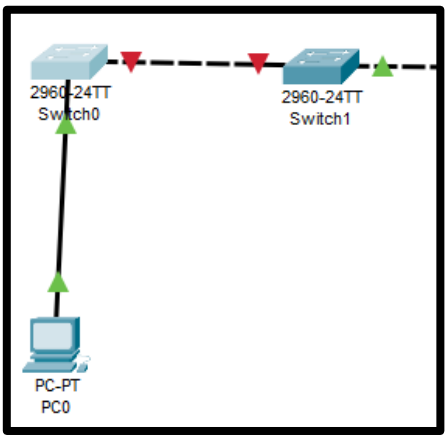
c. Теперь настроим порт ***f0/2:***

   i. Введем команду на PC-0 ***ipconfig /all.*** Физический MAC-адрес **00E0.B01A.9083.**

   ii. 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
```

d. PC-0 успешно подключен:



e. 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.

   i. Выполним скрипт на коммутаторе:

   ii. Все работает.

```
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
```

f. Проверим нашу настройку. Зайдем в терминал PC-1 и пропингуем PC-0. Успешно.

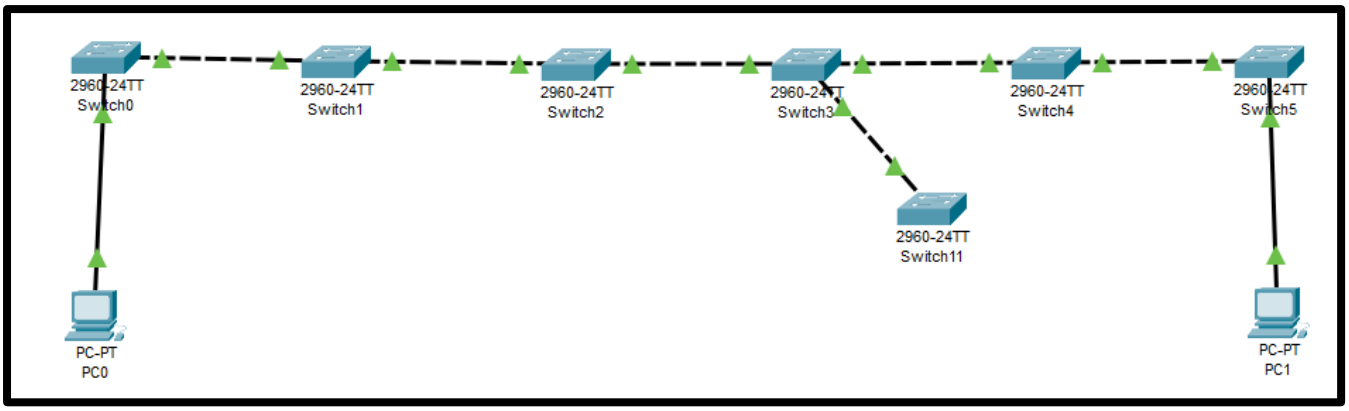
```
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time=1ms TTL=128
Reply from 192.168.1.10: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

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.

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

```
Switch#ping 192.168.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Switch#ping 192.168.1.11

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.11, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/2/10 ms

Switch#
```

Итоговая схема такова:



Вывод

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