

Практическая работа №1

Вариант 6

Кирилл Денисов ИВБО-02-19

17 февраля 2022 г.

Таблица 1 — Таблица адресации

Устройство	Интерфейс	IP-адрес
R1_DENISOV	VLAN 6	192.168.1.8 /24
		2001:db8:acad::2 /64
		fe80::2
PC-A	NIC	192.168.1.16 /24
		2001:db8:acad::3 /64
		fe80::3

Часть 1. Создание сети и проверка настроек коммутатора по умолчанию

Шаг 1.1. Создайте сеть согласно топологии Соединили устройства согласно предложенной топологии. Установили консольное подключение к коммутатору, необходимое для первичной настройки устройства, когда конфигурация соединений по SSH и Telnet не настроена (см. рисунок 1).

Шаг 1.2. Проверьте настройки коммутатора по умолчанию Проверим, что коммутатор не имеет файла конфигурации, сохраненного в энергонезависимой памяти (NVRAM). На коммутаторе присутствуют 24 интерфейса FastEthernet, 2 интерфейса GigabyteEthernet, 16 линий vty. В исходном состоянии VLAN 1 не настроен, адреса не заданы.

Изучим сведения о OS коммутатора с помощью команды *# show version*. Чтобы включить интерфейс необходимо ввести команду *no shutdown*, находясь в режиме конфигурации данного интерфейса.

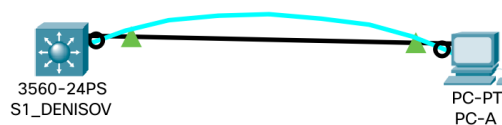


Рисунок 1 — Топология сети

По умолчанию имя vlan 1 — Vlan 1.

Изучив флеш-память, видим, что образу Cisco OS присвоено имя c3560-advipservicesk9-mz.122-37.SE1.

Часть 2. Настройка базовых параметров сетевых устройств

Шаг 2.1. Настройте базовые параметры коммутатора. Введем следующие команды в консоль коммутатора, находясь в режиме конфигурации.

```

no ip domain-lookup
2  hostname S1_DENISOV
service password-encryption
4  enable secret class
banner motd #
6  Unauthorized access is strictly prohibited. #

```

Назначим адреса IPV4 и IPV6 VLAN 6 коммутатора согласно заданию. Чтобы включить поддержку IP6 на коммутаторе 3560, необходимо выполнить следующие действия.

```

conf t
2  sdm prefer dual-ipv4-and-ipv6 default
wr
4  reload
conf t
6  ipv6 unicast-routing

```

Ассоциируем все порты коммутатора с данным виртуальным интерфейсом, используя команды *switchport mode access* и *switchport access vlan6*? находясь в режиме конфигурации выбранных интерфейсов, активируем интерфейс (см. рисунки 2 и 3).

Ограничим доступ к коммутатору по линиям консоли и vty, установив

VLAN Name	Status	Ports
1 default	active	
6 VLAN0006	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	
S1_DENISOV#		

Рисунок 2 — Сведения о vlan 6

```

interface Vlan6
  mac-address 00d0.ba14.5b01
  ip address 192.168.1.8 255.255.255.0
  ipv6 address FE80::2 link-local
  ipv6 address 2001:DB8:ACAD::2/64
  !

```

Рисунок 3 — Запись о vlan 6 в текущем файле конфигурации

пароль `cisco`. Настроим локальную авторизацию на данных линиях командой `login`, находясь в режиме конфигурации данных линий.

Установим возможность удаленного соединения к коммутатору по протоколу Telnet, выполним команды `transport input telnet`, находясь в режиме конфигурации линий `vtu`.

Шаг 2.2. Настройте IP-адрес на компьютере PC-A. Проведем аналогичные действия с PC-A. Настроим IPv4 и IPv6, шлюз по умолчанию 192.168.1.1, имитировав маршрутизатор (см. рисунок 4).

Часть 3. Проверка сетевых подключений

Шаг 3.1. Протестируйте сквозное соединение, отправив эхо-запрос. Проверим сетевое соединение между устройствами (см. рисунок 5), отправив эхо-запрос на PC-A по адресу 192.168.1.16.

Проверим конфигурацию виртуального интерфейса `vlan 6` с помощью команды `show interface vlan6` (см. рисунок 6).

Полоса пропускания интерфейса `Vlan 6` = 100 Mib/s. `Vlan 6` находится во включенном состоянии.

Configuration

☐ DHCP ☒ Static

IPv4 Address: 192.168.1.16

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: 2001:DB8:ACAD::3 / 64

Link Local Address: FE80::3

Default Gateway: FE80::1

DNS Server:

Рисунок 4 — Сетевые настройки PC-A

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.16, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
S1_DENISOV#
```

Рисунок 5 — Эхо запрос к PC-A

```
S1_DENISOV#show interfaces vlan6
Vlan6 is up, line protocol is up
Hardware is CPU Interface, address is 00d0.ba14.5b01 (bia 00d0.ba14.5b01)
Internet address is 192.168.1.8/24
MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00
Last input 21:40:21, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  1682 packets input, 530955 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicast)
  0 runs, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
 563859 packets output, 0 bytes, 0 underruns
  0 output errors, 23 interface resets
  0 output buffer failures, 0 output buffers swapped out
S1_DENISOV#
```

Рисунок 6 — Результат работы команды show interface vlan6

Шаг 3.2. Проверьте удаленное управление коммутатором

Проверим удаленное подключение к коммутатору по протоколу Telnet, выполнив команду *telnet 192.168.1.8* из терминала PC-A. В качестве пароля линии введем **cisco**. Для входа в привилегированный режим будем использовать пароль **class**. Результаты подключения приведены на рисунке 7.

Часть 4. Управление таблицей MAC-адресов

Шаг 4.1. Запишите MAC-адрес узла

```
C:\>telnet 192.168.1.18
Trying 192.168.1.18 ...
% Connection timed out; remote host not responding
C:\>telnet 192.168.1.8
Trying 192.168.1.8 ...Open
Unauthorized access is strictly prohibited.

User Access Verification

Password:
S1_DENISOV>
S1_DENISOV>
S1_DENISOV>
S1_DENISOV>en
Password:
S1_DENISOV#
```

Рисунок 7 — Telnet подключение к коммутатору

Воспользуемся командой *ipconfig /all*, чтобы узнать физический адрес сетевой интерфейсной платы PC-A. Physical Address.....: 000D.BDAA.C015

Шаг 4.2. Определите MAC-адреса, полученные коммутатором. Воспользуемся командой *show mac address-table* на коммутаторе, чтобы вывести таблицу известных MAC-адресов (см. рисунок 8). Как видим, это адрес узла PC-A.

Vlan	Mac Address	Type	Ports
----	-----	-----	-----
6	000d.bdaa.c015	DYNAMIC	Fa0/1

S1_DENISOV#

Ctrl+F6 to exit CLI focus

Рисунок 8 — Таблица MAC-адресов на коммутаторе

Шаг 4.3. Перечислите параметры команды *show mac address-table*

Выведем параметры команды *show mac address-table* (см. рисунок ??)

В данной таблице при использовании параметра *dynamic* мы видим только один адрес.

Шаг 4.4. Назначьте статический MAC-адрес

Назначим статический MAC-адрес предварительно очистив таблицу MAC-адресов командой *clear mac address-table dynamic* (см. рисунок 10).

```

S1_DENISOV#show mac address-table ?
dynamic    dynamic entry type
interfaces interface entry type
static     static entry type
<cr>
S1_DENISOV#show mac address-table

```

Рисунок 9 — Параметры команды show mac address-table

```

<cr>
S1_DENISOV#clear mac address-table dy
S1_DENISOV#clear mac address-table dynamic
S1_DENISOV#
S1_DENISOV#
S1_DENISOV#
S1_DENISOV#show mac address-table dynamic
      Mac Address Table
-----
Vlan  Mac Address      Type    Ports
----  -
S1_DENISOV#

```

Рисунок 10 — Очистка таблицы MAC-адресов

Отправив эхо-запрос с узла PC-A обнаружим, что в таблицу снова попал физический адрес PC-A — это говорит о работе протокола ARP.

Назначим статический адрес PC-A для интерфейса vlan 6 с помощью команды `# mac address-table static 000D.BDAA.C015 vlan 6 interface fastethernet 0/6`. После этого в таблице MAC-адресов появится запись о том, что статический адрес добавлен (см. рисунок 11).

```

Vlan  Mac Address      Type    Ports
----  -
      6  000d.bdaa.c015    STATIC  Fa0/6
S1_DENISOV#

```

Рисунок 11 — Добавление статического адреса

Ответы на вопросы

1. Auto-MDIX Ethernet интерфейс Auto-MDIX способен автоматически определять какой вид порта требуется, при использовании Auto-MDIX тип используемого кабеля не имеет значения. Можно использовать как прямой, так и перекрестный кабель.
2. SSH обеспечивает шифрование передаваемых и отправляемых данных, защищая данные от перехвата. Telnet не обеспечивает шифрование данных. При использовании данных подключений используется протокол TCP транспортного уровня. Порт SSH – 22, Telnet – 23.
3. Данный интерфейс нужен для проверки отправки пакетов от устройства самому себе. Также данный интерфейс может быть зарезервирован для дальнейшего расширения сети. С помощью истории команд можно более быстро и продуктивно выполнять однотипные команды, а также позволяет увидеть, какие команды были запущены ранее.
4. В таблице содержится информация об известных сетевых и физических адресах устройств сети, которые были получены в результате работы протокола ARP. Также имеется информация о типе данных записей — статическая или динамическая. Данные попадают в таблицу, после того, как устройства отзываются на ARP запрос от коммутатора, который посылается им периодически всем устройствам в сети.
5. Заголовок кадра содержит управляющую информацию, определяемую протоколом канального уровня для используемой логической топологии и среды передачи данных.
Управляющая информация кадра уникальна для каждого типа протокола. Она используется протоколом уровня 2 и предоставляет функциональные возможности, требуемые коммуникационной средой.