

Лабораторная работа

Настройка коммутатора и оконечного устройства

Топология

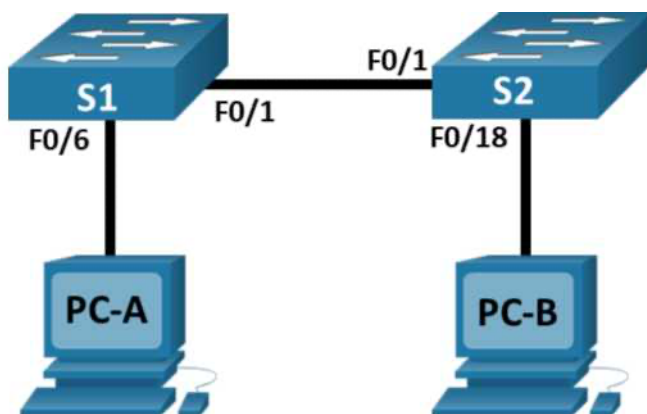


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети
S1	VLAN 1	192.168.1.1	255.255.255.0
S2	VLAN 1	192.168.1.2	255.255.255.0
PC-A	Сетевой адаптер	192.168.1.10	255.255.255.0
PC-B	Сетевой адаптер	192.168.1.11	255.255.255.0

Задачи

Часть 1. Настройка основных параметров сетевого устройства

Часть 2. Проверка и тестирование подключения к сети

Общие данные

Коммутаторы Cisco имеют особый интерфейс, который называется **виртуальным интерфейсом коммутатора**. На виртуальном интерфейсе коммутатора можно настроить IP-адрес (адрес управления). Это позволяет получить удалённый доступ к коммутатору для настройки и отображения параметров.

В этой лабораторной работе вам необходимо развернуть сеть с двумя оконечными узлами и двумя коммутаторами.

Используя консольное подключение, вы должны настроить основные параметры коммутаторов: имя узла, локальные пароли, IP-адрес виртуального интерфейса коммутатора и баннер.

Вы также должны настроить IP-адреса и маски подсети на компьютерах и обеспечить соединение (в обе стороны) между этими двумя оконечными устройствами.

Вам необходимо будет продемонстрировать доступ по протоколу Telnet к коммутаторам для удалённой настройки, используя виртуальный интерфейс коммутатора.

Примечание: В лабораторной работе используются коммутаторы Cisco с ОС Cisco IOS. В зависимости от модели устройства и версии ОС Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые приведены ниже в качестве примеров в данной лабораторной работе.

Примечание: Убедитесь в том, что все настройки на коммутаторах и загрузочная конфигурация отсутствуют.

Необходимые ресурсы

- 2 коммутатора Cisco с ОС Cisco IOS
- 2 ПК (ОС Windows с установленной программой эмуляции терминала)
- Консольные кабели для подключения к устройствам Cisco IOS через консольные порты.
- Кабели Ethernet для подключения устройств в соответствии с Топологией

Часть 1. Настройка основных параметров сетевого устройства

В этой части необходимо создать простую сеть с двумя оконечными узлами и двумя коммутаторами. Используя консольное подключение, вы должны настроить основные параметры коммутаторов: имя узла, локальные пароли, IP-адрес виртуального интерфейса коммутатора и баннер.

Также необходимо настроить на компьютерах IP-адрес и маску подсети.

Шаг 1. Настройка топологии сети

В этом шаге вам необходимо соединить устройства кабелями в соответствии с Топологией сети.

- а. Разверните сеть в соответствии с заданной Топологией.
- б. Осуществите консольное подключение устройства S1 с компьютером PC-A и устройства S2 с компьютером PC-B.
- в. Включите устройства.
- г. Осмотрите сетевые подключения.

Шаг 2. Настройка основных параметров коммутатора.

На этом шаге требуется настроить основные параметры коммутатора: имя узла и IP-адрес виртуального интерфейса коммутатора. Назначение IP-адреса виртуальному интерфейсу на коммутаторе — это первый шаг. На следующем шаге необходимо выбрать протокол, используемый для удаленной настройки коммутатора. Два наиболее распространённых протокола — это Telnet и SSH.

- а. Подключитесь с компьютера PC-A к коммутатору S1 через консольное подключение с помощью одной из программ эмуляции терминала. Если в энергонезависимой памяти (NVRAM) коммутатора отсутствуют сохранённые файлы конфигурации, вы должны оказаться в пользовательском режиме.

b. Перейдите в привилегированный режим.

```
Switch>enable
```

```
Switch#
```

c. Перейдите в режим глобальной конфигурации и назначьте имя коммутатора **в соответствии с Вашим вариантом**.

```
Switch#configure terminal
```

```
Switch(config)#hostname S1
```

```
S1(config)#
```

d. Запретите в случае ввода неверных команд поиск в службе доменных имен (DNS).

```
S1(config)#no ip domain-lookup
```

```
S1(config)#
```

e. Введите локальные пароли.

Настройте пароль доступа к привилегированному режиму коммутатора.

```
S1(config)#enable secret class
```

```
S1(config)#
```

Ограничьте доступ к консольному подключению. Первоначальная конфигурация по умолчанию не запрашивает пароль при консольном подключении.

```
S1(config)#line con 0
```

```
S1(config-line)#password cisco
```

```
S1(config-line)#login
```

```
S1(config-line)#exit
```

```
S1(config)#
```

f. Настройте линии виртуального соединения (VTY), чтобы можно было подключиться к коммутатору для выполнения удалённой настройки по протоколу Telnet. Если не указать пароль для линии VTY, то нельзя будет подключиться к коммутатору по протоколу Telnet.

```
S1(config)#line vty 0 4
```

```
S1(config-line)#password cisco
```

```
S1(config-line)#login
```

```
S1(config-line)#exit
```

g. Зашифруйте все пароли.

```
S1(config)#service password-encryption
```

```
S1(config)#exit
```

h. Проверьте введенные пароли и настройки доступа к пользовательскому и привилегированному режимам.

Какое сочетание клавиш используется для перехода из режима глобальной конфигурации в привилегированный режим?

i. Перейдите в режим глобальной конфигурации и настройте баннерное сообщение, которое будет отображаться перед входом в пользовательский режим.

```
S1#config t
```

```
S1(config)#banner motd #
```

```
Enter Text message. End with the character '#'.  
Unauthorized access is strictly prohibited. #
```

j. В соответствии с Таблицей адресации и своим вариантом

настройте IP-адрес виртуального интерфейса коммутатора **vlan 1** для получения возможности удалённой настройки коммутатора.

```
S1#(config)#interface vlan 1
S1(config-if)#ip address 192.168.1.1 255.255.255.0
S1(config-if)#no shut
S1(config-if)#exit
S1(config)#
```

к. Выполните настройку коммутатора **S2** с компьютера **PC-B**:

Имя устройства: **s2**

Запретите в случае ввода неверных команд поиск в службе доменных имен.

Введите локальные пароли.

Настройте пароль доступа к привилегированному режиму коммутатора: **class**

Настройте пароль доступа к консоли коммутатора: **cisco**

Настройте пароль доступа к линии виртуального соединения (**VTY**): **cisco**

Зашифруйте все пароли.

Проверьте введенные пароли и настройки доступа к пользовательскому и привилегированному режимам.

Настройте соответствующий баннер.

В соответствии с **Таблицей адресации и своим вариантом** настройте IP-адрес виртуального интерфейса коммутатора **vlan 1** для получения возможности удалённой настройки коммутатора.

Шаг 3. Настройка оконечных узлов PC-A и PC-B.

а. Настройте статические IP-адреса и маску подсети на компьютерах **PC-A** и **PC-B** в соответствии с **Таблицей адресации и своим вариантом**. Процедура присвоения IP-адреса на компьютере под управлением ОС **Windows** выполняется по-разному и зависит от версии ОС.

б. Проверьте настройки **PC-A** и **PC-B** и подключения между ними.

Часть 2. Проверка и тестирование подключения сети

В части 2 нужно проверить текущую конфигурацию коммутатора, протестировать сквозное подключение (в обе стороны) между двумя оконечными устройствами и коммутаторами, а также возможность удалённой настройки коммутатора по протоколу **Telnet**.

Шаг 1. Отобразите конфигурацию коммутатора.

а. Используя команду **show run** отобразите текущую конфигурацию коммутатора S1. Ниже представлен возможный пример конфигурации. Произведенные выше настройки выделены **жёлтым** цветом. Остальные параметры конфигурации коммутатора, предусмотренные в **IOS**, остались со значениями по умолчанию.

```
S1#show run
Building configuration...

Current configuration : 1233 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S1
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
!
no ip domain-lookup
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
```

```
!  
interface FastEthernet0/8  
!  
interface FastEthernet0/9  
!  
interface FastEthernet0/10  
!  
interface FastEthernet0/11  
!  
interface FastEthernet0/12  
!  
interface FastEthernet0/13  
!  
interface FastEthernet0/14  
!  
interface FastEthernet0/15  
!  
interface FastEthernet0/16  
!  
interface FastEthernet0/17  
!  
interface FastEthernet0/18  
!  
interface FastEthernet0/19  
!  
interface FastEthernet0/20  
!  
interface FastEthernet0/21  
!  
interface FastEthernet0/22  
!  
interface FastEthernet0/23  
!  
interface FastEthernet0/24  
!  
interface GigabitEthernet0/1  
!  
interface GigabitEthernet0/2  
!  
interface Vlan1  
  ip address 192.168.1.1 255.255.255.0  
!  
  banner motd ^CUnauthorized access is strictly  
prohibited.^C  
!  
!  
!  
line con 0  
  password 7 0822455D0A16
```



```

login
!
line vty 0 4
password 7 0822455D0A16
login
line vty 5 15
login
!
!
end

```

b. Используя команду **show ip interface brief**, отобразите состояние интерфейсов коммутатора. Проверьте состояние виртуального интерфейса **vlan 1**. Он должен находиться в состоянии **up/up** и иметь назначенный **IP**-адрес. Порт **F0/6** коммутатора **S1** также должен быть включен, так как согласно Топологии к нему подключён компьютер **PC-A**. Поскольку все порты коммутатора по умолчанию входят в сеть **vlan 1**, имеется возможность удаленной настройки коммутатора по **IP**-адресу, который был настроен для сети **vlan 1**.

```

S1#show ip interface brief

```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/1	unassigned	YES	manual	up	up
FastEthernet0/2	unassigned	YES	manual	down	down
FastEthernet0/3	unassigned	YES	manual	down	down
FastEthernet0/4	unassigned	YES	manual	down	down
FastEthernet0/5	unassigned	YES	manual	down	down
FastEthernet0/6	unassigned	YES	manual	up	up
FastEthernet0/7	unassigned	YES	manual	down	down
FastEthernet0/8	unassigned	YES	manual	down	down
FastEthernet0/9	unassigned	YES	manual	down	down
FastEthernet0/10	unassigned	YES	manual	down	down
FastEthernet0/11	unassigned	YES	manual	down	down
FastEthernet0/12	unassigned	YES	manual	down	down
FastEthernet0/13	unassigned	YES	manual	down	down
FastEthernet0/14	unassigned	YES	manual	down	down
FastEthernet0/15	unassigned	YES	manual	down	down
FastEthernet0/16	unassigned	YES	manual	down	down
FastEthernet0/17	unassigned	YES	manual	down	down
FastEthernet0/18	unassigned	YES	manual	down	down
FastEthernet0/19	unassigned	YES	manual	down	down
FastEthernet0/20	unassigned	YES	manual	down	down
FastEthernet0/21	unassigned	YES	manual	down	down
FastEthernet0/22	unassigned	YES	manual	down	down
FastEthernet0/23	unassigned	YES	manual	down	down
FastEthernet0/24	unassigned	YES	manual	down	down
GigabitEthernet0/1	unassigned	YES	manual	down	down
GigabitEthernet0/2	unassigned	YES	manual	down	down
Vlan1	192.168.1.1	YES	manual	up	up

```

S1#

```

c. Отобразите текущую конфигурацию и состояние подключенных интерфейсов коммутатора **S2**.

Шаг 2. Проверьте сквозное подключение.

a. На компьютере **PC-A** откройте окно командной строки.

b. Проверьте настройки IP-адреса и маски подсети PC-A с помощью команды

```
ipconfig /all
```

c. С помощью команды ping отправьте эхо-запрос на IP-адрес виртуального интерфейса коммутатора S1.

```
ping 192.168.1.1
```

Проверка соединения должно быть успешной.

d. Отправьте эхо-запрос на IP-адрес виртуального интерфейса коммутатора S2.

```
ping 192.168.1.2
```

Проверка соединения должно быть успешной.

e. Отправьте эхо-запрос на IP-адрес компьютера PC-B.

```
ping 192.168.1.11
```

Проверка соединения должно быть успешной.

f. Прodelайте аналогичные действия на компьютере PC-B.

Примечание. Если проверка соединения с помощью команды ping была неуспешной, найдите ошибку в настройках основных параметров устройств, а также проверьте кабели, IP-адреса и маски.

Шаг 3. Проверьте удалённый доступ к коммутатору.

На данном шаге необходимо получить удалённый доступ к виртуальному интерфейсу коммутатора S1 (S2) по протоколу Telnet. В данной лабораторной работе компьютер PC-A (PC-B) и коммутатор S1 (S2) находятся рядом. Но, в реальных условиях, коммутаторы и компьютеры могут находиться на значительном расстоянии. Протокол Telnet не является безопасным, т.к. при его использовании все данные, включая пароли и команды, передается в виде простого текста. Однако в данной лабораторной работе для проверки удалённого доступа использован этот протокол. В последующих лабораторных работах для удалённого доступа к сетевым устройствам будет использован протокол SSH.

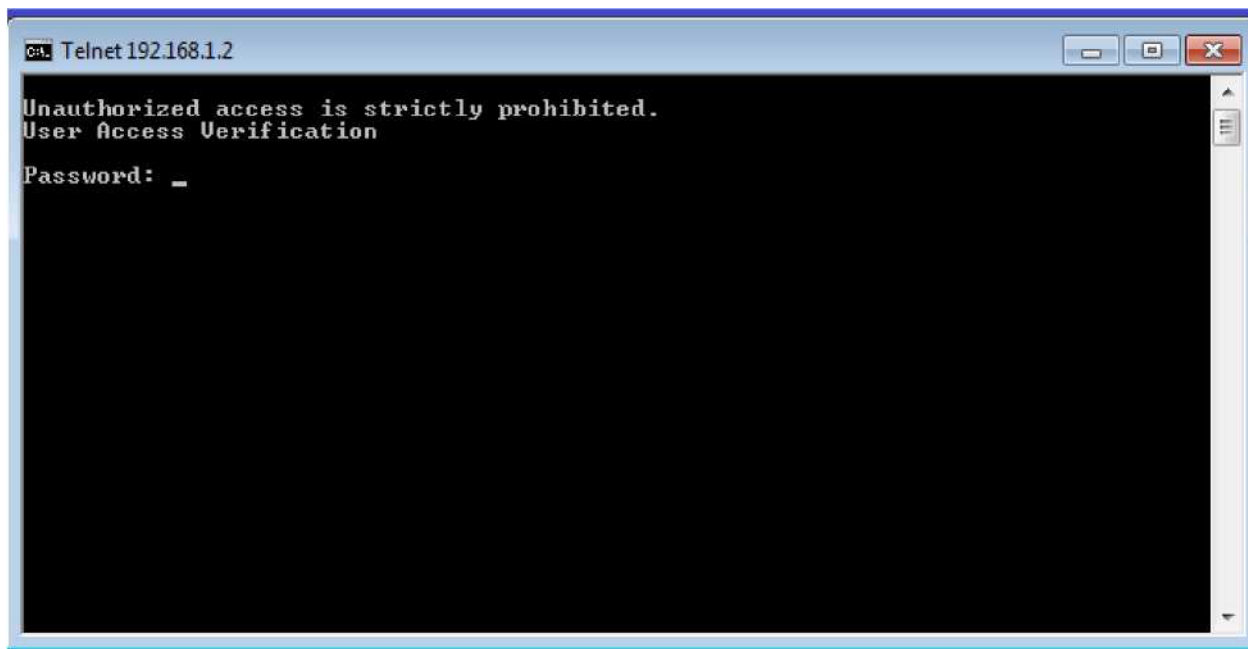
Примечание. Некоторые версии ОС Windows по умолчанию не поддерживает Telnet. Клиентское программное обеспечение протокола Telnet должно быть установлено с правами администратора. Для этого откройте окно командной строки и введите команду

```
pkgmgr /iu: "TelnetClient"
```

a. Для удаленного подключения к коммутатору S1 по IP-адресу виртуального интерфейса, в окне командной строки на компьютере PC-A введите команду:

```
telnet 192.168.1.1
```

На экране должны появиться показанные ниже сообщения.



b. Введите пароль **cisco**, и перейдите в командную строку пользовательского режима коммутатора S1. Введите команду **enable** для перехода в привилегированный режим. Введите пароль **class** и выполните команду **show run**.

c. Введите команду **quit**, для завершения сеанса клиента Telnet и возврата в командную строку ОС Windows.

d. Прodelайте аналогичные действия и на компьютере PC-B для коммутатора S2.

Вопросы на закрепление

Почему для первоначальной настройки коммутатора используется консольное подключение?

Почему одни порты FastEthernet коммутаторов включены, а другие выключены?

Какие условия необходимы для удаленного подключения к коммутатору по протоколу Telnet или SSH?

Что может помешать установить связь между компьютерами с помощью команды ping?