

Практическая работа №8

Вариант 6

Кирилл Денисов ИВБО-02-19

28 ноября 2021 г.

Таблица 1 — Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1_DENISOV	G0/1	192.168.1.6	255.255.255.0	—
S1	VLAN 1	192.168.1.16	255.255.255.0	192.168.1.6
PC-A	NIC	192.168.1.26	255.255.255.0	192.168.1.6

Часть 1. Настройка основных параметров устройств

Шаг 1.1. Создание сети согласно топологии

Создадим сеть для выполнения данного практического задания согласно топологии. (см. рисунок 1).

Шаг 1.2. Выполнение инициализации и перезагрузки маршрутизатора и коммутатора

Дождемся инициализации маршрутизатора и коммутатора S1 и выполним их перезагрузку.

Шаг 1.3. Настройка маршрутизатора

Подключимся к маршрутизатору R1_DENISOV и произведем его настройку в соответствии с заданием. Приведем текущую конфигурацию маршрутизатора.

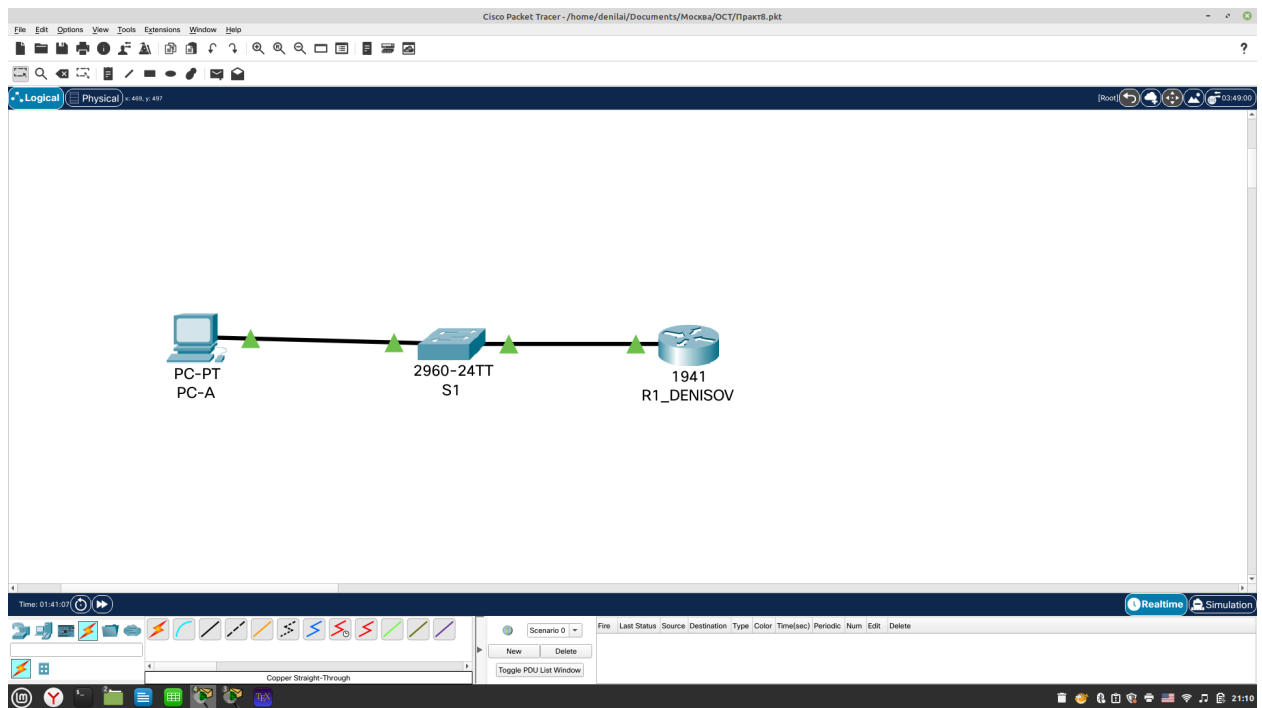


Рисунок 1 — Топология сети

```

1  R1_DENISOV#show running-config
2  Building configuration...
3
4  Current configuration : 1211 bytes
5  !
6  version 15.1
7  no service timestamps log datetime msec
8  no service timestamps debug datetime msec
9  service password-encryption
10 security passwords min-length 10
11 !
12 hostname R1_DENISOV
13 !
14 login block-for 30 attempts 2 within 120
15 !
16 enable secret 5 $1$mERr$5wXi8fVAu3dNc0gNCjvIQ1
17 !
18 ip cef
19 no ipv6 cef
20 !
21 username SSHadmin privilege 15 secret 5 $1$mERr$uMzC7If3IbCZVifeGQ3rg/
22 !
23 license udi pid CISCO1941/K9 sn FTX15244MJ5-
24 !
25 ip domain-name cisco-lab.ru
26 !

```

```

27 spanning-tree mode pvst
   !
29 interface GigabitEthernet0/0
   no ip address
31 duplex auto
   speed auto
33 shutdown
   !
35 interface GigabitEthernet0/1
   ip address 192.168.1.6 255.255.255.0
37 duplex auto
   speed auto
39 !
   interface Vlan1
41 no ip address
   shutdown
43 !
   ip classless
45 !
   ip flow-export version 9
47 !
   ip access-list extended sl_def_acl
49 deny tcp any any eq telnet
   deny tcp any any eq www
51 deny tcp any any eq 22
   permit tcp any any eq 22
53 !
   banner motd ^CAuthorized users only!^C
55 !
   line con 0
57 exec-timeout 5 0
   password 7 0822455D0A16
59 login
   !
61 line aux 0
   !
63 line vty 0 4
   exec-timeout 5 0
65 password 7 0822455D0A16
   login local
67 transport input ssh
   !
69 end

```

После проведения настройки сохраним текущую конфигурацию в файл загрузочной конфигурации с помощью команды `copy running-config startup-config`.

Шаг 1.4. Установка более надежных паролей

Согласно данным рекомендациям по лучшим практическим методикам надежные пароли, примеры которых приведены в этой лабораторной работе, необходимо всегда использовать в реальной работе. Однако для упрощения выполнения работы в остальных лабораторных работах данного курса используются пароли `cisco` и `class`.

Измените зашифрованный пароль привилегированного режима EXEC в соответствии с рекомендациями. Установите следующий пароль: **Enablep@55** с помощью команды `enable secret Enablep@55`.

Установим минимальную длину 10 символов для всех паролей с помощью команды `security passwords min-length 10`.

Шаг 1.5. Настройка компьютер PC-A Настроим для PC-A IP-адрес и маску подсети и шлюз по умолчанию в соответствии с заданием, приведенным в таблице 1 (см. рисунок 2).

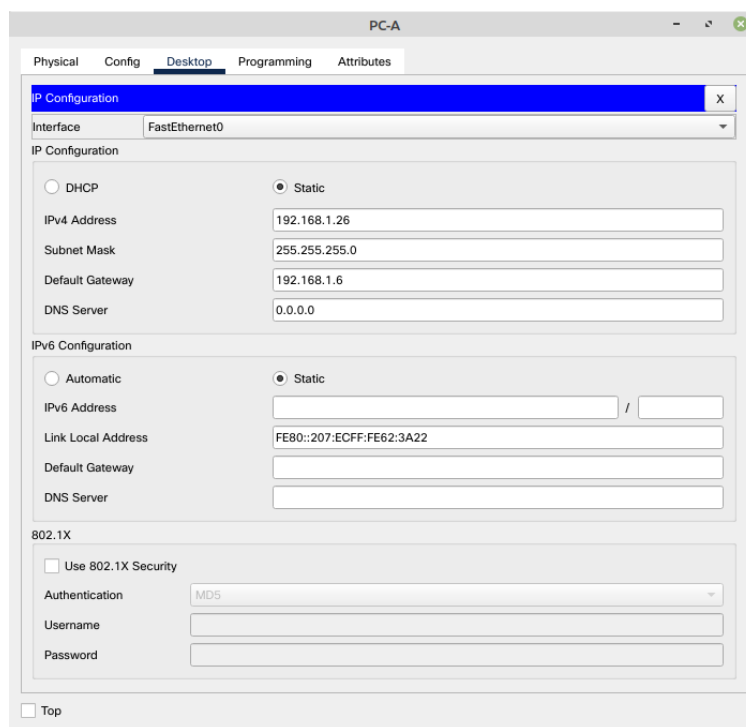


Рисунок 2

Шаг 1.6. Проверка подключения к сети

Пошлем с PC-A эхо-запрос на маршрутизатор R1_DENISOV . Убедимся, что эхо-запрос выполнен успешно (см. рисунок 3).

Часть 2. Настройка маршрутизатора для доступа по протоколу SSH и обеспечение базовых мер безопасности

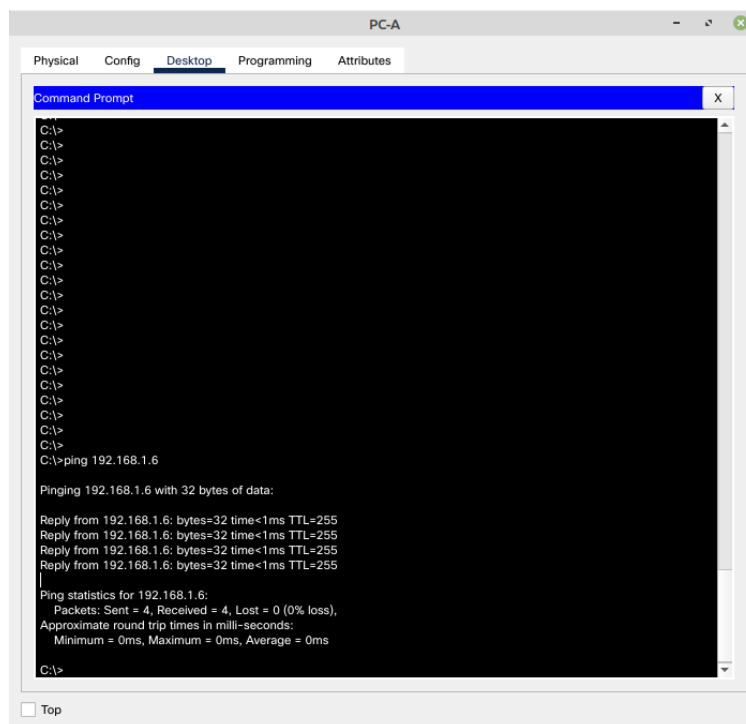


Рисунок 3 — Эхо запрос на маршрутизатор R1_DENISOV

Шаг 2.1. Настройка аутентификации устройств

Перейдем в режим глобальной конфигурации. Зададим имя для маршрутизатора с помощью команды `hostname R1_DENISOV`. Зададим домен для устройства с помощью команды `ip domain-name cisco-lab.ru`

Шаг 2.2. Создание ключа шифрования с указанием его длины

Перейдем в режим глобальной конфигурации. Создадим ключ шифрования с помощью команды `crypto key generate rsa modulus 1024`.

Шаг 2.3. Создание пользователя в локальной базе учетных записей

Перейдем в режим глобальной конфигурации. Создадим пользователя с помощью команды `username SSHadmin privilege 15 secret Admin1p@55`.

Шаг 2.4. Активация протокола SSH на линиях VTY

Перейдем в режим конфигурации линии с помощью команды `line vty 0 4`.

Активируем протокол SSH с помощью команды `transport input telnet ssh`.

Изменим способ входа в систему таким образом, чтобы использовалась проверка пользователей по локальной базе учетных записей с помощью команды `login local`.


```
C:\>  
C:\>  
C:\>telnet 192.168.1.6  
Trying 192.168.1.6 ...Open  
  
[Connection to 192.168.1.6 closed by foreign host]  
C:\>
```

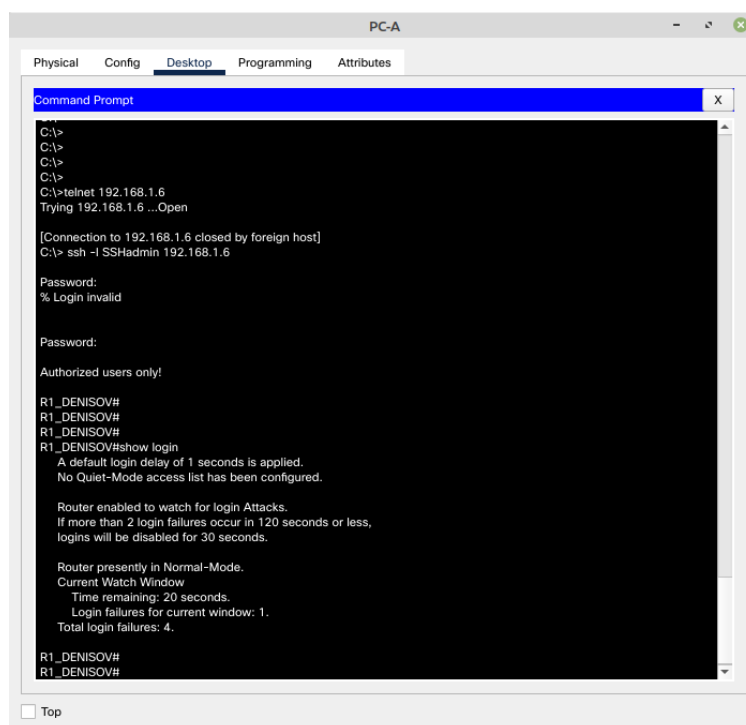
Рисунок 5 — Отклонение подключения к R1_DENISOV по протоколу telnet

Вопрос: Намеренно укажите неверное имя пользователя и пароль, чтобы проверить, будет ли заблокирован доступ к системе после двух неудачных попыток. Что произошло после ввода неправильных данных для входа в систему во второй раз?

Ответ: *Возможность подключения заблокирована на 30 секунд после того, как в течение 120 секунд неправильные данные были введены больше 2 раз.*

Вопрос: Из сеанса подключения к маршрутизатору с помощью консоли отправьте команду `show login`, чтобы проверить состояние входа в систему.

Ответ:



```
PC-A  
Physical Config Desktop Programming Attributes  
Command Prompt  
C:\>  
C:\>  
C:\>  
C:\>telnet 192.168.1.6  
Trying 192.168.1.6 ...Open  
  
[Connection to 192.168.1.6 closed by foreign host]  
C:\> ssh -l SSHadmin 192.168.1.6  
  
Password:  
% Login Invalid  
  
Password:  
  
Authorized users only!  
  
R1_DENISOV#  
R1_DENISOV#  
R1_DENISOV#  
R1_DENISOV#show login  
A default login delay of 1 seconds is applied.  
No Quiet-Mode access list has been configured.  
  
Router enabled to watch for login Attacks.  
If more than 2 login failures occur in 120 seconds or less,  
logins will be disabled for 30 seconds.  
  
Router presently in Normal-Mode.  
Current Watch Window  
Time remaining: 20 seconds.  
Login failures for current window: 1.  
Total login failures: 4.  
  
R1_DENISOV#  
R1_DENISOV#
```

Рисунок 6 — Результат работы команды `show login` на маршрутизаторе R1_DENISOV

Вопрос: По истечении 30 секунд повторите попытку подключения к R1_DENISOV по протоколу SSH и войдите в систему, используя имя SSHadmin

и пароль Admin1p@55. Что отобразилось после успешного входа в систему?

Ответ: По истечении 30 секунд попытка авторизации на маршрутизаторе R1_DENISOV прошла успешно. Таймаут истек. После совершения аутентификации видим приглашение для ввода привилегированного режима.

Вопрос: Войдите в привилегированный режим EXEC и введите в качестве пароля Enablep@55. Если вы неправильно вводите пароль, прерывается ли сеанс SSH после двух неудачных попыток в течение 120 секунд? Дайте пояснение.

Часть 3. Настройка коммутатора для доступа по протоколу SSH и обеспечение базовых мер безопасности

Шаг 3.1. Настройте основные параметры коммутатора

По аналогии с маршрутизатором R1_DENISOV , настроим коммутатор S1 . Приведем его конфигурацию.

```
1 S1#show running-config
Building configuration...

3
Current configuration : 1711 bytes
5 !
version 15.0
7 no service timestamps log datetime msec
no service timestamps debug datetime msec
9 service password-encryption
!
11 hostname S1
!
13 enable secret 5 $1$mERr$5wXi8fVAu3dNc0gNCjvIQ1
!
15 no ip domain-lookup
ip domain-name cisco-lab.ru
17 !
username SSHadmin secret 5 $1$mERr$uMzC7If3IbCZVifeGQ3rg/
19 !
spanning-tree mode pvst
21 spanning-tree extend system-id
!
23 interface FastEthernet0/1
!
25 interface FastEthernet0/2
shutdown
```



```
27 | !
    | interface FastEthernet0 /3
29 | shutdown
    | !
31 | interface FastEthernet0 /4
    | shutdown
33 | !
    | interface FastEthernet0 /5
35 | shutdown
    | !
37 | interface FastEthernet0 /6
    | shutdown
39 | !
    | interface FastEthernet0 /7
41 | shutdown
    | !
43 | interface FastEthernet0 /8
    | shutdown
45 | !
    | interface FastEthernet0 /9
47 | shutdown
    | !
49 | interface FastEthernet0 /10
    | shutdown
51 | !
    | interface FastEthernet0 /11
53 | shutdown
    | !
55 | interface FastEthernet0 /12
    | shutdown
57 | !
    | interface FastEthernet0 /13
59 | shutdown
    | !
61 | interface FastEthernet0 /14
    | shutdown
63 | !
    | interface FastEthernet0 /15
65 | shutdown
    | !
67 | interface FastEthernet0 /16
    | shutdown
69 | !
    | interface FastEthernet0 /17
71 | shutdown
    | !
73 | interface FastEthernet0 /18
    | shutdown
```

```

75 !
   interface FastEthernet0/19
77 shutdown
   !
79 interface FastEthernet0/20
   shutdown
81 !
   interface FastEthernet0/21
83 shutdown
   !
85 interface FastEthernet0/22
   shutdown
87 !
   interface FastEthernet0/23
89 shutdown
   !
91 interface FastEthernet0/24
   shutdown
93 !
   interface GigabitEthernet0/1
95 !
   interface GigabitEthernet0/2
97 shutdown
   !
99 interface Vlan1
   ip address 192.168.1.16 255.255.255.0
101 !
   banner motd ^CAuthorized users only!^C
103 !
   !
105 !
   line con 0
107 password 7 0822455D0A16
   login
109 exec-timeout 5 0
   !
111 line vty 0 4
   exec-timeout 5 0
113 password 7 0822455D0A16
   login local
115 transport input ssh
   line vty 5 15
117 exec-timeout 5 0
   password 7 0822455D0A16
119 login local
   transport input ssh
121 !
   end

```

Шаг 3.2. Настройка коммутатора для соединения по протоколу SSH

По аналогии с маршрутизатором R1_DENISOV произведем настройку коммутатора S1 для соединения по протоколу SSH.

Перейдем в режим глобальной конфигурации. Зададим имя для маршрутизатора с помощью команды `hostname R1_DENISOV`. Зададим домен для устройства с помощью команды `ip domain-name cisco-lab.ru`.

Создадим ключ шифрования с помощью команды `crypto key generate rsa modulus 1024`.

Создадим пользователя с помощью команды `username admin privilege 15 secret Enablep@55`.

Перейдем в режим конфигурации линии с помощью команды `line vty 0 4`.

Активируем протокол SSH с помощью команды `transport input telnet ssh`.

Изменим способ входа в систему таким образом, чтобы использовалась проверка пользователей по локальной базе учетных записей с помощью команды `login local`.

Шаг 3.3. Отключение неиспользуемых портов

Перейдем в режим глобальной конфигурации, затем в режим конфигурации множества интерфейсов с помощью команды `interface range FastEthernet0/2 - 24` и выключим их с помощью команды `shutdown`. После этого, все неиспользуемые порты будут отключены.

Шаг 3.4. Установка соединения с коммутатором по протоколу SSH

С компьютера PC-A установим подключение по протоколу SSH к интерфейсу SVI коммутатора S1. Подключение проведено успешно (см. рисунок 7), причем соединение по протоколу telnet отклоняется по соображениям безопасности.

Шаг 3.5. Проверка мер безопасности

Убедимся что протокол Telnet на коммутаторе отключен.

Подключимся к коммутатору по протоколу SSH и намеренно укажем неверное имя пользователя и пароль, чтобы проверить, будет ли заблокирован доступ к системе.

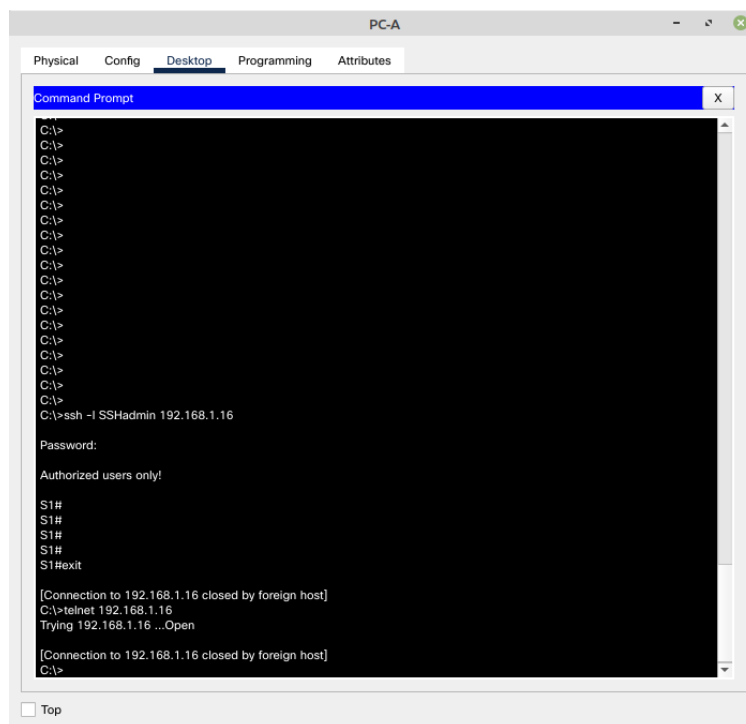


Рисунок 7 — Соединение с коммутатором S1 по протоколу SSH

По истечении 30 секунд повторим попытку подключения к R1_DENISOV по протоколу SSH и войдем в систему, используя имя пользователя **SSHadmin** и пароль **Admin1p@55**.

Часть 4. Настройка протокола SSH с использованием интерфейса командной строки (CLI) коммутатора

Шаг 4.1. Параметры для клиента SSH в Cisco IOS

Воспользуемся подсказкой «?» для команды **ssh** (см. рисунок 8).



Рисунок 8 — Параметры команды ssh в Cisco IOS

Шаг 4.2. Установка соединения с маршрутизатором R1_DENISOV по протоколу SSH с коммутатора S1

Чтобы подключиться к маршрутизатору R1_DENISOV по протоколу SSH, введем команду **ssh -l SSHadmin 192.168.1.6**. Это позволит нам войти в систему под именем SSHadmin. При появлении приглашения введите в качестве пароля **Admin1p@55** (см. рисунок 9).

