

Packet Tracer. Настройка безопасного пароля и протокола SSH

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
RTA	G0/0	172.16.1.1	255.255.255.0	—
PCA	NIC	172.16.1.10	255.255.255.0	172.16.1.1
SW1	VLAN 1	172.16.1.2	255.255.255.0	172.16.1.1

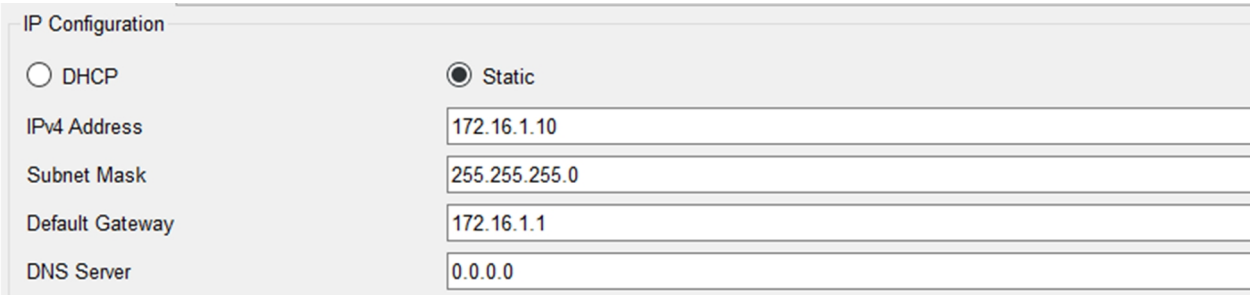
Сценарий

Администратор сети обратился к вам с просьбой подготовить **RTA** и **SW1** для развертывания. Перед его подключением к сети необходимо активировать функции безопасности.

Инструкции

Шаг 1: Настройка базовой безопасности на маршрутизаторе

- а. Настройте IP-адресацию на компьютере **PCA** в соответствии с таблицей адресации.



IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 172.16.1.10

Subnet Mask: 255.255.255.0

Default Gateway: 172.16.1.1

DNS Server: 0.0.0.0

- б. Используя терминал на **RTA**, установите консольное соединение с **PCA**.

- в. Настройте имя хоста как **RTA**.

- г. Настройте IP-адресацию на **RTA** и активируйте интерфейс.

- д. Зашифруйте все открытые пароли.

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

- е. Установите минимальную длину пароля 10.

```
RTA(config)# security password min-length 10
```

- ж. Установите надежный секретный пароль по своему выбору. **Примечание.** Выберите пароль, который вы будете помнить, или вам нужно будет сбросить его, если вы заблокированы на устройстве.

- з. Отключите DNS-поиск.

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

- и. Установите доменное имя **CCNA.com** (с учетом регистра для правильного расчета баллов программой Packet Tracer).

```
RTA(config)# ip domain-name CCNA.com
```

- к. Создайте произвольного пользователя с надежным шифрованным паролем.

```
RTA(config)# username any_user secret any_password
```

- л. Создайте 1024-разрядные RSA-ключи.

Примечание В программе Packet Tracer введите команду `crypto key generate rsa` и нажмите клавишу Enter для продолжения

```
RTA(config)# crypto key generate rsa
```

```
The name for the keys will be: RTA.CCNA.com
```

```
Choose the size of the key modulus in the range of 360 to 2048 for your  
General Purpose Keys. Choosing a key modulus greater than 512 may take  
a few minutes.
```

```
How many bits in the modulus [512]: 1024
```

- м. Заблокируйте на три минуты всех, кто, выполнив четыре попытки в течение двух минут, не смог войти в систему.

```
RTA(config)# login block-for 180 attempts 4 within 120
```

- н. Настройте все линии VTY для доступа по SSH и используйте профили локальных пользователей для аутентификации.

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

```
RTA(config-line)# transport input ssh
```

```
RTA(config-line)# login local
```

- о. Установите тайм-аут режима EXEC на 6 минут на линиях VTY.

```
RTA(config-line)# exec-timeout 6
```

- п. Сохраните конфигурацию в NVRAM.

```
Router#enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname RTA
RTA(config)#interface G0/0
RTA(config-if)#ip address 172.16.1.1 255.255.255.0
RTA(config-if)#no shutdown

RTA(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

RTA(config-if)#
RTA(config-if)#service password-encryption
RTA(config)#security password min-length 10
RTA(config)#enable secret class
% Password too short - must be at least 10 characters. Password not configured.
RTA(config)#enable secret class12345
RTA(config)#no ip domain-lookup
RTA(config)#ip domain-name CCNA.com
RTA(config)#username yaroslav secret any_password class12345
RTA(config)#crypto key generate rsa
The name for the keys will be: RTA.CCNA.com
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

RTA(config)#login block-for 180 attempts 4 within 120
*Mar 1 8:9:15.711: %SSH-5-ENABLED: SSH 1.99 has been enabled
RTA(config)#line vty 0 4
RTA(config-line)#transport input ssh
RTA(config-line)#login local
RTA(config-line)#exec-timeout 6
RTA(config-line)#end
RTA#
%SYS-5-CONFIG_I: Configured from console by console

RTA#w
Building configuration...
[OK]
RTA#
```

- п. Откройте командную строку на рабочем столе **PCA** , чтобы установить соединение SSH с **RTA**.

```
C:\> ssh /?
Packet Tracer PC SSH
Usage: SSH -l username target
C:\>
```

Шаг 2: Настройка базовых мер безопасности на коммутаторе

Настройте коммутатор **SW1** с соответствующими мерами безопасности. Для получения дополнительной помощи обратитесь к инструкциям по настройке маршрутизатора.

- а. Нажмите на **SW1** и выберите вкладку **CLI**.
- б. Настройте имя хоста как **SW1**.
- в. Настройте IP-адресацию на SW1 **VLAN1** и активируйте интерфейс.
- г. Настройте адрес шлюза по умолчанию.
- д. Отключите все неиспользуемые порты коммутатора.

Примечание. На коммутаторе рекомендуется отключить неиспользуемые порты. Один из способов сделать это - просто закрыть каждый порт с помощью команды «**shutdown**». Для этого потребуется доступ к каждому порту по отдельности. Существует метод быстрого внесения изменений в несколько портов одновременно с помощью **команды** `interface range`. На **SW1** все порты, кроме FastEthernet0/1 и GigabitEthernet0/1, могут быть выключены с помощью следующей команды:

```
SW1(config)# interface range F0/2-24, G0/2
SW1(config-if-range)# shutdown
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively
down
<Данные пропущены>
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively
down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to
administratively down
```

Команда использовала диапазон портов 2-24 для портов FastEthernet, а затем один диапазон портов GigabitEthernet0/2.

- е. Зашифруйте все открытые пароли.
- ж. Установите надежный секретный пароль по своему выбору.
- з. Отключите DNS-поиск.
- и. Установите доменное имя **CCNA.com** (с учетом регистра для правильного расчета баллов программой Packet Tracer).
- к. Создайте произвольного пользователя с надежным шифрованным паролем.
- л. Создайте 1024-разрядные RSA-ключи.
- м. Настройте все линии VTY для доступа по SSH и используйте профили локальных пользователей для аутентификации.
- н. Установите тайм-аут режима EXEC на 6 минут на всех линиях VTY.
- о. Сохраните конфигурацию в NVRAM.

```
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW1
SW1(config)#interface VLAN
% Incomplete command.
SW1(config)#interface VLAN1
SW1(config-if)#ip address 172.16.1.2 255.255.255.0
SW1(config-if)#no shutdown

SW1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

SW1(config-if)#ip default-gateway 172.16.1.1
SW1(config)#interface range F0/2-24, G0/2
SW1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
SW1(config-if-range)#exit
SW1(config)#service password-encryption
SW1(config)#enable secret class12345
SW1(config)#no ip domain-lookup
SW1(config)#ip domain-name CCNA.com
SW1(config)#username yaroslav secret class12345
SW1(config)#crypto key generate rsa
The name for the keys will be: SW1.CCNA.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

SW1(config)#line vty 0 4
*Mar 1 8:21:33.368: %SSH-5-ENABLED: SSH 1.99 has been enabled
SW1(config-line)#transport input ssh
SW1(config-line)#login local
SW1(config-line)#exec-timeout 6
SW1(config-line)#end
SW1#
%SYS-5-CONFIG_I: Configured from console by console
w
Building configuration...
[OK]
SW1#config t
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#line vty 15
SW1(config-line)#transport input ssh
SW1(config-line)#login local
SW1(config-line)#exec-timeout 6
SW1(config-line)#
```
