

Государственное бюджетное профессиональное образовательное учреждение
«Нижегородский радиотехнический колледж»

ОП.11 Компьютерные сети

ОТЧЁТ
по практической работе № 16.4.6

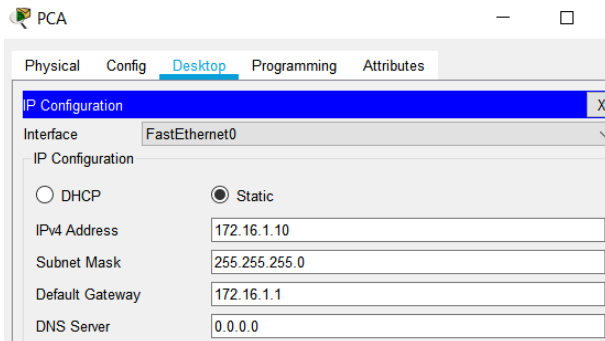
Тема «Настройка безопасного пароля и протокола SSH»

Выполнил:
обучающийся группы 2ИСиП19-1
Мамонов Антон

Проверил:
Преподаватель
Еремеев В. А.

Нижний Новгород
2021г

Часть 1. Настройка базовой безопасности на маршрутизаторе



Настройка IP-адресации. Переименовываем и настраиваем IP-адресацию на RTA и активируем интерфейс

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname RTA
RTA(config)#int g 0/0
RTA(config-if)#ip add 172.16.1.1 255.255.255.0
RTA(config-if)#no shut
```

Зашифруйте все открытые пароли. Установите минимальную длину пароля 10. Установите надежный секретный пароль по своему выбору.

```
RTA(config-if)#service password-encryption
RTA(config)#security password min-length 10
RTA(config)#enable secret cisco
% Password too short - must be at least 10 characters. Password not
configured.
RTA(config)#enable secret 1234567890
```

Отключите DNS-поиск. Установите доменное имя **CCNA.com**.

```
RTA(config)#no ip domain-lookup
RTA(config)#ip domain-name CCNA.com
```

Создайте произвольного пользователя с надежным шифрованным паролем. Создайте 1024-разрядные RSA-ключи. Заблокируйте на три минуты всех, кто, выполнив четыре попытки в течение двух минут, не смог войти в систему.

```
RTA(config)#username pooshka secret pooooooshka
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
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

RTA(config)#login block-for 180 attempts 4 within 120
*Mar 1 8:14:48.951: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Настройте все линии VTY для доступа по SSH и используйте профили локальных пользователей для аутентификации. Установите тайм-аут режима EXEC на 6 минут на линиях VTY.

```
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)#copy runnin
RTA(config-line)#end
```

Сохраните конфигурацию в NVRAM.

```
RTA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Откройте командную строку на рабочем столе **РСА**, чтобы установить соединение SSH с **RTA**.

```
C:\>ssh /?
Packet Tracer PC SSH

Usage: SSH -l username target
```

Часть 2. Настройка базовых мер безопасности на коммутаторе

Настройте имя хоста как **SW1**. Настройте IP-адресацию на интерфейс. Настройте адрес шлюза по умолчанию.

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW1
SW1(config)#int vlan 1
SW1(config-if)#ip add 172.16.1.2 255.255.255.0
SW1(config-if)#no shut

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)#exit
SW1(config)#ip def 172.16.16.1
```

Отключите все неиспользуемые порты коммутатора.

```
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
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down
```

Зашифруйте все открытые пароли. Установите надежный секретный пароль по своему выбору. Отключите DNS-поиск. Установите доменное имя **CCNA.com**.

```
SW1(config-if-range)#service password-encryption
SW1(config)#enable secret 1234567890
SW1(config)#no ip domain-lookup
SW1(config)#ip domain-name CCNA.com
```

Создайте произвольного пользователя с надежным зашифрованным паролем. Создайте 1024-разрядные RSA-ключи.

```
SW1(config)#username pooshka secret pooshka
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 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
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

Настройте все линии VTY для доступа по SSH и используйте профили локальных пользователей для аутентификации. Установите тайм-аут режима EXEC на 6 минут на всех линиях VTY.

```
SW1(config)#line vty 0 4
*Mar 1 8:30:11.787: %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(config)#line vty 0 15
SW1(config-line)#transport input ssh
SW1(config-line)#login local
SW1(config-line)#exec-timeout 6
```

Сохраните конфигурацию в NVRAM.

```
SW1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Вывод: во время выполнения лабораторной работы я научился настройке базовой безопасности на маршрутизаторе и также настройке базовых мер безопасности на коммутаторе.