

Министерство образования и науки Российской Федерации Федеральное государственное
бюджетное образовательное учреждение высшего профессионального
образования «Российский экономический университет им. Г.В. Плеханова»
Московский приборостроительный техникум

ЛАБОРАТОРНАЯ РАБОТА № 4

«Защита маршрутизатора для административного доступа.»

Выполнил: Кочарян Эрик Робертович
студент группы КС – 3 – 17
Принял преподаватель
Володин И.М.
преподаватель ФГБОУВПО
"РЭУ им. Г.В. Плеханова"

Москва, 2021 г

Ход работы.

1) Топология (Рис.1).

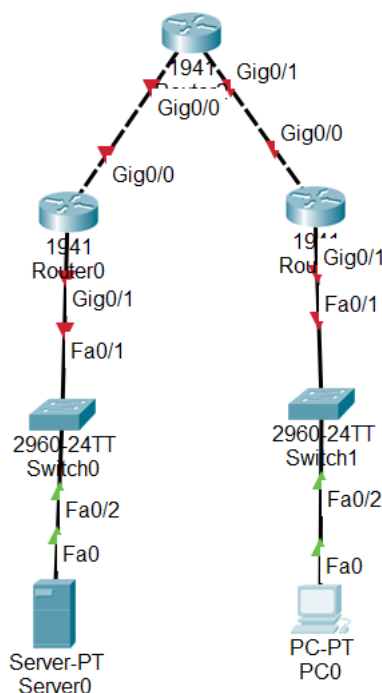


Рис.1 — Топология.

2) Настройка маршрутизации (Рис.2).

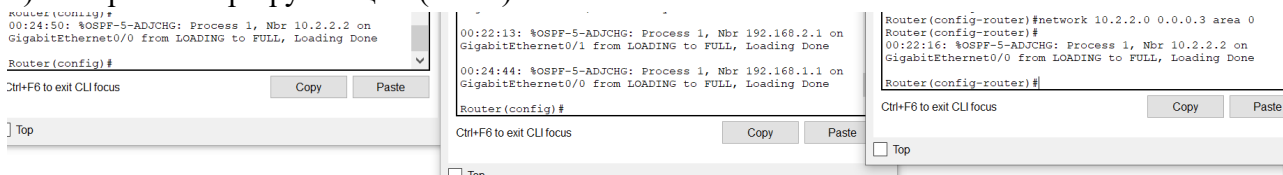


Рис.2 — Настроена маршрутизация.

3) Переключение интерфейсов G0/1 в пассивный режим (Рис.3).

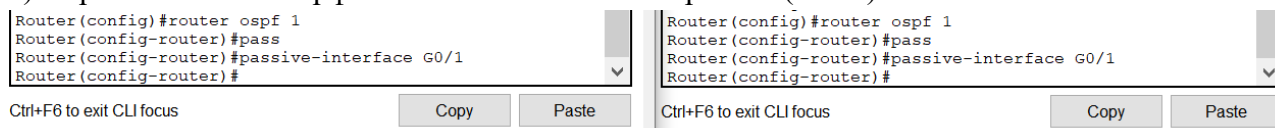


Рис.3 — Пассивные интерфейсы маршрутизаторов R0,R1.

4) С TFTP сервера обновляем прошивку на маршрутизаторах (Рис.4).

```
Router#copy tftp: flash:  
Address or name of remote host []? 192.168.1.2  
Source filename []? c1900-universalk9-mz.SPA.155-3.M4a.bin  
Destination filename [c1900-universalk9-mz.SPA.155-3.M4a.bin]?  
  
Accessing tftp://192.168.1.2/c1900-universalk9-mz.SPA.155-3.M4a.bin....  
Loading c1900-universalk9-mz.SPA.155-3.M4a.bin from 192.168.1.2:  
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
[OK - 33591768 bytes]  
  
33591768 bytes copied in 6.223 secs (566767 bytes/sec)  
Router#boot sys  
Router#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)#boot system flash c1900-universalk9-mz.SPA.155-3.M4a.bin
```

Рис.4 — Обновление прошивки.

5) Устанавливаем пароль и используем алгоритм шифрования (Рис.5).

```
Router(config)#enable algorithm-type scrypt secret cisco
Router(config)#
```

Рис.5 — Пароль.

6) Настройка консоли (Рис.6).

```
Router(config)#line console 0
Router(config-line)#pass
Router(config-line)#password cisco
Router(config-line)#exe
Router(config-line)#exec-timeout 5 0
Router(config-line)#lo
Router(config-line)#login
Router(config-line)#loggi
Router(config-line)#logging s
Router(config-line)#logging synchronous
```

Рис.6 — Настройка консоли.

7) Настройка порта AUX (Рис.7).

```
Router(config-line)#line aux 0
Router(config-line)#pass
Router(config-line)#password cisco
Router(config-line)#exe
Router(config-line)#exec-timeout 5 0
Router(config-line)#login
```

Рис.7 — Настройка порта aux.

8) Настройка пароля на линиях line vty 0 4 (Рис.8).

```
Router(config-line)#line vty 0 4
Router(config-line)#pass
Router(config-line)#password cisco
Router(config-line)#exe
Router(config-line)#exec-timeout t
Router(config-line)#exec-timeout 5 0
Router(config-line)#tra
Router(config-line)#transport i
Router(config-line)#transport input a
Router(config-line)#transport input all
Router(config-line)#login
```

Рис.8 — Настройка.

9) Шифрование паролей (Рис.9).

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

Рис.9 — Шифрование пароля.

10) Настройка предупреждающего баннера (Рис.10).

```
Router(config)#banner motd $Unauthorized access strictly prohibited!$
Router(config)#
```

Рис.10 — Баннер.

11) Создание учетной записи с паролем (Рис.11).

```
Router(config)#username admin algorithm-type scrypt secret cisco
Router(config)#
```

Рис.11 — Создание учетной записи.

12) Настройка доменного имени (Рис.12).

```
Router(config)#ip domain-name cisco.com
Router(config)#
```

Рис.12 — Доменное имя.

13) Создание привилегированного пользователя (Рис.13).

```
Router(config)#username Admin privilege 15 algorithm-type scrypt secret cisco
```

Рис.13 — Создание привилегированного пользователя.

14) На линию 0 4 задаем уровень привилегий 15 (Рис.14).

```
Router(config-line)#line vty 0 4
Router(config-line)#privilege level 15
Router(config-line)#
```

Рис.14 — Уровень привилегий.

15) Генерация крипто ключей (Рис.15).

```
Router(config)#hostname R1
R1(config)#crypto key generate rsa
The name for the keys will be: R1.cisco.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]
```

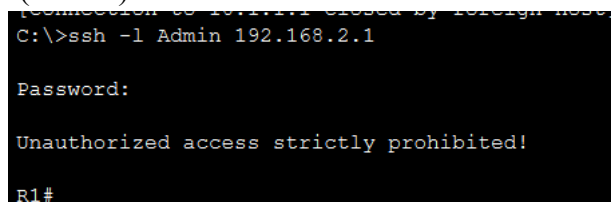
Рис.15 — Генерация ключей.

16) Изменение версии ssh на 2 (Рис.16).

```
R1(config)#ip ssh ver 2
```

Рис.16 — Изменение версии.

17) Проверка доступа (Рис.17).



```
Connection to 192.168.2.1 closed by foreign host.
C:\>ssh -l Admin 192.168.2.1

Password:
Unauthorized access strictly prohibited!

R1#
```

Рис.17 — Подключение по ssh.

18) Защита загрузочного образа (Рис.18).

```
R1(config)#secure boot-image
%IOS_RESILIENCE-5-IMAGE_NOTFOUND: Running image not found on removable disk
R1(config)#secure boot-config
%IOS_RESILIENCE-5-CONFIG_RESIL_ACTIVE: Successfully secured config archive
[flash:.runcfg-19930301-005057.ar]
R1(config)#
```

Рис.18 — Защита.

19) Настройте список ACL на маршрутизаторе R1, который ограничит доступ к протоколу SNMP в локальной сети 192.168.2.0 (Рис.19).

```
R1(config)#ip access-list standard PERMIT-SNMP
R1(config-std-nacl)#permit 192.168.1.0 0.0.0.255
R1(config-std-nacl)#exit
R1(config)#snmp-server view SNMP-RO iso included
```

Рис.20 — Настройка.

20) Список ACL PERMIT-SNMP, настроенный на шаге 19, будет ограничивать доступ по протоколу SNMP к локальной сети (Рис.21).

```
R1(config)#snmp-server group SNMP-G1 v3 priv read SNMP-RO access PERMIT-SNMP
```

Рис.21 — Настройка.

21) Настройка источника синхронизации времени (Рис.22).

```
R1(config)#do clock set 20:12:00 Dec 17 2021
R1(config)#ntp authentication-key 1 md5 NTPpassword
R1(config)#ntp trusted-key 1
R1(config)#ntp authenticate
R1(config)#ntp master 3
```

Рис.22 — Настройка.

22) Настройка клиента NTP (Рис.23).

```
Router(config)#ntp authentication-key 1 md5 NTPpassword
Router(config)#ntp trusted-key 1
Router(config)#ntp authenticate
Router(config)#ntp server 10.2.2.1
Router(config)#ntp update-calendar
Router(config)#show ntp associations
^
% Invalid input detected at '^' marker.

Router(config)#do show ntp associations

address          ref clock      st   when    poll   reach  delay      offset
~10.2.2.1        127.127.1.1    3    7        16     1      0.00      908824731106
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
Router(config)#
```

Рис.23 — Настройка.

23) Проверка полученного времени (Рис.24).

```
Router(config)#do show clock
20:18:28.298 UTC Fri Dec 17 2021
Router(config)#
```

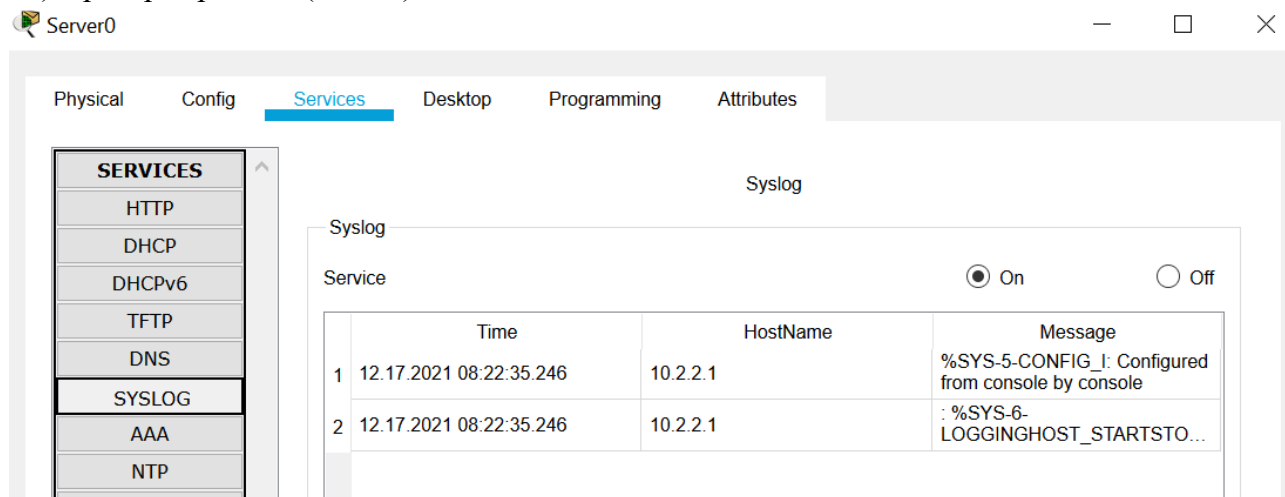
Рис.24 — Время.

24) Настройка syslog (Рис.25).

```
R1(config)#service timestamps log datetime msec
R1(config)#logging host 192.168.1.2
R1(config)#ex
R1#
*дек 17, 20:22:35.2222: SYS-5-CONFIG_I: Configured from console by console
*дек 17, 20:22:35.2222: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.2 port
CLI initiated
```

Рис.25 — Настройка.

25) Проверка работы (Рис.26).



The screenshot shows the Cisco IOS GUI with the 'Services' tab selected. On the left, the 'SERVICES' list includes HTTP, DHCP, DHCPv6, TFTP, DNS, **SYSLOG**, AAA, and NTP. The main area displays the 'Syslog' configuration with the 'Service' toggle set to 'On'. Below this, a table shows two log messages:

	Time	HostName	Message
1	12.17.2021 08:22:35.246	10.2.2.1	%SYS-5-CONFIG_I: Configured from console by console
2	12.17.2021 08:22:35.246	10.2.2.1	: %SYS-6-LOGGINGHOST_STARTSTO...

Рис.26 — Полученные данные.

26) Настройка цепочки ключей на маршрутизаторе (Рис.27).

А тут произошел вылет cisco packet tracer и файл не сохранился.

Контрольные вопросы.

1. Объясните, чем важны защита доступа к маршрутизатору и мониторинг сетевых устройств.

Защита доступа к маршрутизатору важна для нейтрализации несанкционированного доступа к устройству и сети.

2. Какие преимущества протокол SSH имеет перед Telnet?

Протокол ssh является безопасным протоколом удаленного доступа на оборудования благодаря возможности шифрования трафика в отличии от Telnet. Протокол ssh предпочтительнее в использовании.

4. Почему использование централизованных серверов журналов лучше, чем маршрутизаторов, ведущих журнал только локально?

Для удобства хранения и доступа к журналам.