СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

Р.Р. Фаткиева

Основы построения защищенных компьютерных сетей

Настройка ОС Cisco

СПбГЭТУ «ЛЭТИ», 2021 г.

2. ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ СЕТЕЙ. НАСТРОЙКА ОПЕРАЦИОННОЙ СИСТЕМЫ CISCO IOS. ПОЛЬЗОВАТЕЛЬСКИЙ И АДМИНИСТРАТИВНЫЙ РЕЖИМЫ. РЕЖИМЫ КОНФИГУРИРОВАНИЯ

Цель работы: изучение теоретического материала об основных функциях маршрутизатора, формирование практических навыков первоначальной настройки специализированной ОС Cisco IOS.

2.1. Общие сведения

Маршрутизатор–устройство, использующее одну и более метрик для определения оптимального пути передачи сетевого трафика на основе информации, полученной из заголовков сетевого уровня. К функциям маршрутизаторов относят:

1. фильтрацию пакетов, в соответствии с информацией, содержащейся в заголовках пакетов сетевого и транспортного уровня (адресами отправителя, получателя, информацией о протоколе, видами приложений источника и получателя);
2. поддержку сетей с избыточными активными связями, для осуществления передачи трафика через коммутируемые сети;
3. определение наилучшего маршрута передачи пакетов с возможными минимальными затратами и максимальной надежностью;

Рассмотрим работу маршрутизатора:

1. Дейтограмма, поступивший на порт маршрутизатора освобождается от заголовка физического уровня и передается канальному уровню.
2. Отбрасывание заголовка канального уровня и передача пакета сетевому уровню.
3. Извлечение и анализ заголовка сетевого уровня, проверка контрольной суммы, времени жизни, фильтрация пакетов при несовпадении уничтожение пакета.
4. Если пакет прошел все виды проверок, то маршрутизатором производится определение дальнейшего маршрута. Выбор маршрута продвижения пакета осуществляется путем сбора информации о других маршрутизаторах и узлах в сети, которые заносятся в таблицы маршрутизации, на основании которых затем выбирается наилучший маршрут для каждого конкретного пакета. Таблица маршрутизации включает по крайне мере следующие столбцы:

- сетевой адрес назначения;
- адрес следующего маршрутизатора;
- адрес порта, на который нужно направить пакет;
- характеристика пути (пропускная способность канала, отметка времени).

5. Передача пакета, адреса следующего маршрутизатора (или иного узла), номера выходного порта канальному и физическому уровням.

При поступлении очередного пакета маршрутизатор помещает его в буфер. При этом маршрутизаторы имеют несколько буферов для организации очередей каждой выходной линии, по одной для каждого отправителя. Когда линия освобождается, маршрутизатор берет пакет из следующей по кругу очереди. Некоторые алгоритмы позволяют устанавливать приоритет тем или иным очередям.

Управление маршрутизатором осуществляет операционная система сетевого взаимодействия, пример ее служит ОС Cisco IOS — это общий термин для группы сетевых операционных систем, используемых на сетевых устройствах Cisco. Часть операционной системы, которая непосредственно взаимодействует с аппаратным обеспечением компьютера, называется ядром.

Устройства Cisco IOS поддерживают множество команд. Каждая команда IOS имеет определенный формат или синтаксис и выполняется только в соответствующем режиме. Общий синтаксис — это команда, за которой следуют ключевые слова и аргументы. Ключевое слово — это особый параметр операционной системы. Аргумент — это значение или переменная, которые задает пользователь.

Пример:

```
Switch> traceroute 192.168.201.25
Traceroute - команда, 192.168.201.25 - определяемый пользователем аргумент.
```

IOS содержит огромное количество команд для того, чтобы получить список доступных команд и их краткое описание введи знак вопроса в любом режиме терминала.

2.2. Задание

Выполнить первоначальную настройку сетевых параметров ОС Cisco IOS маршрутизатора Cisco 2811 с рабочей станции администратора сети, используя данные в таблице 1.

Таблица 2.1

Параметр	*Значение*
IP-адрес интерфейса Fa0/0	192.168.1.2/24
IP-адрес интерфейса Fa0/1	192.168.2.3/ 30
Стандартный шлюз	192.168.1.1.25
Имя маршрутизатора	R1-7
Домен	net. institute
Пароль доступа enable	
Локальный пользователь/пароль	

Выбор пула адресов осуществлять в соответствие с номером, выданным преподавателем, длина пароля должна быть стойкой к перебору. В окне консоли клиента необходимо вводить числовые значения, которые требуются для получения результата. Настройку маршрутизатора Cisco 2811 осуществлять через рабочую станцию и консольный шнур с интерфейсом RS-232.

2.3. Порядок выполнения работы

1. В среде Cisco packet tracer осуществить выбор маршрутизатора Cisco 2811 и подключить к нему рабочую станцию через консольный шнур (консольный шнур выделен голубым цветом) с использованием интерфейса RS-232, Рис. 2.1.

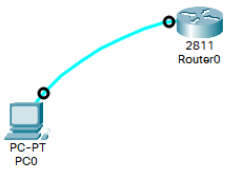

Рис. 2.1 Схема подключения

2. Инициировать работу терминального клиента (Рис 2.2) и осуществить

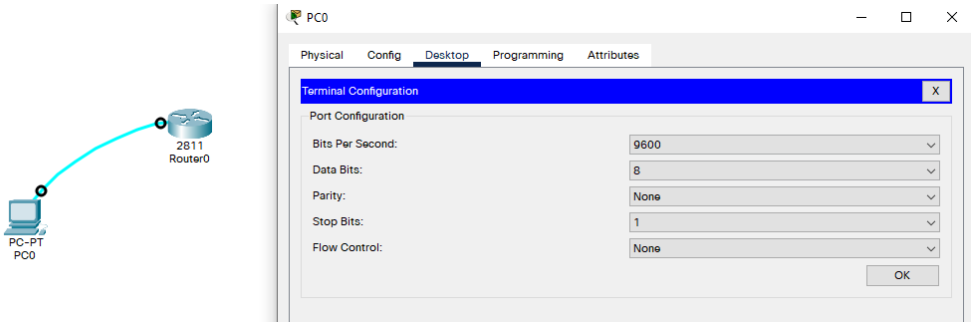

Рис. 2.2 Инициализация работы терминального клиента

проверку текущей конфигурации маршрутизатора, запустив терминальный клиент (Рис 1.3).

```
Router#show running-config
Building configuration...

Current configuration : 604 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!

Router#
```

Рис. 2.3 Текущая конфигурация маршрутизатора.

Осуществить проверку в файле конфигурации (Рис. 2.2, 2.3) наличие имени маршрутизатора, сервисов ведения логов, а также настройки сервис менеджера паролей (в файле конфигурации не задано имя маршрутизатора, отключен сервис ведения логов, а также не настроен сервис менеджера паролей).

4. Для формирования указанных настроек зафиксировать список команд, доступных в пользовательском режиме, просмотрим наличие соответствующих команд (Рис 2.4).

```
Router>?
Exec commands:
  <1-99>      Session number to resume
  connect     Open a terminal connection
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  ping        Send echo messages
  resume      Resume an active network connection
  show        Show running system information
  ssh         Open a secure shell client connection
  telnet      Open a telnet connection
  terminal    Set terminal line parameters
  traceroute  Trace route to destination
Router>
```

Рис. 2.4 Список доступных для пользователя команд

5. Используя команду «enable» осуществить переход в привилегированный режим (Рис.1.5).

```
Router>enable
Router#
```

Рис. 2.5 Использование команды «enable»

6. Выяснить уровень доступа в системе и текущую конфигурацию с помощью команды (Рис.2.6):
   router#show privilege
   router#show running-config

```
Router#show privilege
Current privilege level is 15
Router#show running-config
Building configuration...

Current configuration : 604 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!

Router#
```

Рис. 2.6. Проверка уровня доступа в системе и текущей конфигурации маршрутизатора

7. Сформировать список всех доступных команд для пользователя в привилегированном режиме (Рис 2.7).

```
Router#?
Exec commands:
  <1-99>      Session number to resume
  auto        Exec level Automation
  clear       Reset functions
  clock       Manage the system clock
  configure   Enter configuration mode
  connect     Open a terminal connection
  copy        Copy from one file to another
  debug       Debugging functions (see also 'undebug')
  delete      Delete a file
  dir         List files on a filesystem
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  erase       Erase a filesystem
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  mkdir       Create new directory
  more        Display the contents of a file
  no          Disable debugging informations
  ping        Send echo messages
  reload      Halt and perform a cold restart

Router#
```

Рис. 2.7 Перечень доступных команд в привилегированном режиме.

8. Настройку маршрутизатора выполнить в соответствии с указанными в задании параметрами (Рис.1.8):

configure terminal hostname R7
interface fastEthernet 0/1
ip address 192.168.100.26 255.255.255.252
no shutdown
interface fastEthernet 0/0
ip address 10.194.7.1 255.255.255.0
no shutdown
ip domain-name net.bank
ip route 0.0.0.0 0.0.0.0 192.168.100.25

```
Terminal
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R7
R7(config)#interface fastEthernet 0/1
R7(config-if)#ip address 192.168.100.26 255.255.255.255
Bad mask /32 for address 192.168.100.26
R7(config-if)#ip address 192.168.100.26 255.255.255.252
R7(config-if)#no shutdown

R7(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

R7(config-if)#interface fastEthernet 0/0
R7(config-if)#ip address 10.194.7.1 255.255.255.0
R7(config-if)#no shutdown

R7(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

R7(config-if)#ip domain-name net.bank
R7(config)#ip route 0.0.0.0 0.0.0.0 192.168.100.25
R7(config)#
```

Рис. 2.8 Основные настройки маршрутизатора

Перечисленные команды позволяют установить имя маршрутизатора, сформировать определённые интерфейсы, по котором будет осуществляться передача данных и присвоить им соответствующие IP-адреса. Кроме того, было выбрано доменное имя, а также в таблицу маршрутизации добавлен статический адрес.

9. Не забываем сохранить конфигурацию маршрутизатора, выполнив команду *write memory* (Рис. 2.9):

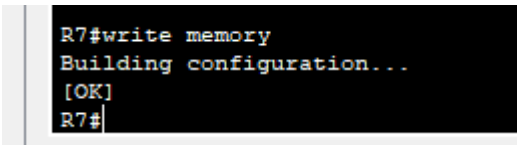

Рис. 2.9. Сохранение настроек маршрутизатора

10. Проверить сохранение настроек после отключения питания, установим модуль NM-ESW-161, после чего снова включим питание роутера (Рис 2.10).

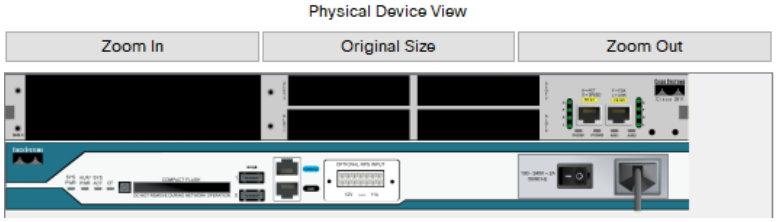

Рис. 2.10 Роутер с выключенным питанием (индикатор питания рядом с выключателем не горит)

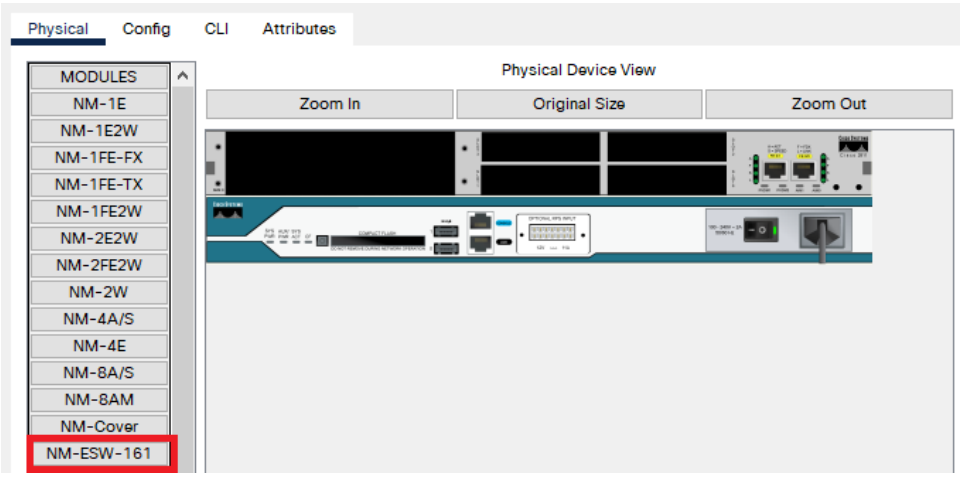

Рис. 2.11. Роутер с включённым питанием (индикатор питания рядом с выключателем горит зеленным цветом). Сетевой модуль установлен в роутер 2811 по умолчанию

11. Командой *sh ip interface brief* просмотреть сохранение подключенных интерфейсов и их имён (Рис 2.12).

```
R7#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        10.194.7.1      YES NVRAM  up                    down
FastEthernet0/1        192.168.100.26  YES NVRAM  up                    down
Vlan1                  unassigned      YES NVRAM  administratively down down
R7#
```

Рис. 2.12. Выполнение команды «show ip interface brief»

12. Используя команды *sh processes* и *sh file systems* осуществить мониторинг процессов загрузки процессора и памяти (Рис. 2.13).

```
Terminal                                                                    X
R7#
R7#
R7#show pr
R7#show pr
R7#show pro
R7#show proces
R7#show processes
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
 PID QTy       PC Runtime (ms)     Invoked  uSecs     Stacks TTY Process
   1 Csp 602F3AF0           0        1627      0 2600/3000   0 Load Meter
   2 Lwe 60C5BE00           4         136     29 5572/6000   0 CEF Scanner
   3 Lst 602D90F8        1676         837   2002 5740/6000   0 Check heaps
   4 Cwe 602D08F8           0           1      0 5568/6000   0 Chunk Manager
   5 Cwe 602DF0E8           0           1      0 5592/6000   0 Pool Manager
   6 Mst 60251E38           0           2      0 5560/6000   0 Timers
   7 Mwe 600D4940           0           2      0 5568/6000   0 Serial Backgrou
   8 Mwe 6034B718           0           1      0 2584/3000   0 OIR Handler
   9 Mwe 603FA3C8           0           1      0 5612/6000   0 IPC Zone Manage
  10 Mwe 603FA1A0           0        8124      0 5488/6000   0 IPC Periodic Ti
  11 Mwe 603FA220           0           9      0 4884/6000   0 IPC Seat Manage
  12 Lwe 60406818         124        2003     61 5300/6000   0 ARP Input
  13 Mwe 60581638           0           1      0 5760/6000   0 HC Counter Time
  14 Mwe 605E3D00           0           2      0 5564/6000   0 DDR Timers
  15 Msp 80164A38           0       79543      0 5608/6000   0 GraphIt
  16 Mwe 802DB0FC           0           2      011576/12000  0 Dialer event
  17 Cwe 801E74BC           0           1      0 5808/6000   0 Critical Bkgnd
  18 Mwe 80194D20           4        9549      010428/12000  0 Net Background
  19 Lwe 8011E9CC           0          20      011096/12000  0 Logger
  20 Mwe 80140160           8       79539      0 5108/6000   0 TTY Background

R7#show file system
File Systems:

       Size(b)       Free(b)      Type  Flags  Prefixes
*    255744000     221896413     flash     rw  flash:
       29688         23590      nvram     rw  nvram:
R7#
```

Рис. 2.13 Таблица загрузки процессора и памяти

13. Задать режим шифрования паролей пользователей в конфигурационном файле командой:

no service password-encryption

создать пользователя:

username noc1 secret test

username noc2 password test

проверить, что его пароль сохранён в открытом виде.

Включить режим шифрования паролей:

enable secret test2

show running-config

service password-encryption

show running-config

проверить, что пароль пользователя сохранён в зашифрованном виде (рис. 2.14, пароль пользователя «noc2» в начале записан в открытом виде, после включения утилиты шифрования тот же самый пароль записан уже в зашифрованном виде).

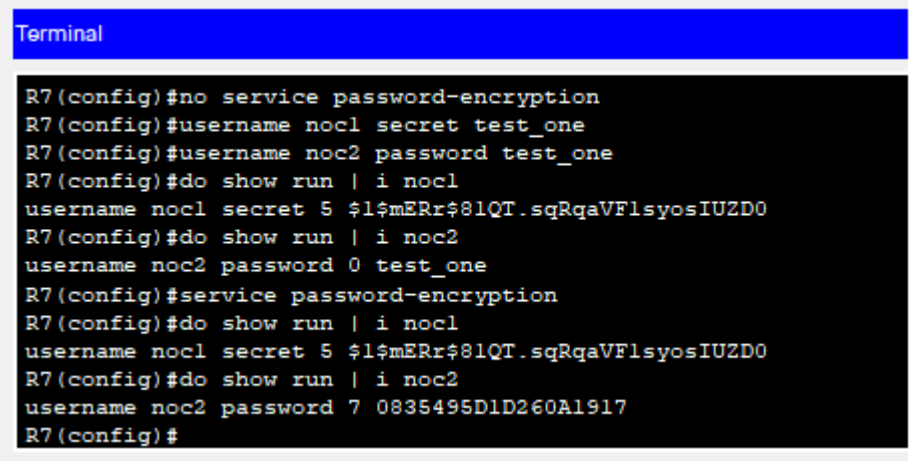

Рис.2.14. Использование механизмов шифрования паролей

14. Удалить созданных пользователей, с последующим заданием стойких к перебору паролей для новых пользователей. Сформировать пароль для доступа к привилегированному режиму (Рис. 1.15).

15. Разработать политику безопасности для доступа к межсетевого экрану. Для этого необходимо осуществить настройку механизма управления доступом к командам маршрутизатора, реализующего политику безопасности. Рассмотрим следующие роли и соответствующие им уровни безопасности:

- администратор безопасности;
- сетевой администратор;
- оператор.

Доступ администратору безопасности и сетевому администратору, может быть предоставлен только через консольную сессию. При этом могут быть выполнены основные команды по диагностике и настройке средств маршрутизации, коммутации и адресации. Пользователи, авторизованные на роль оператора, могут только просматривать диагностические данные на маршрутизаторе. Предусмотреть для каждой роли криптографическое закрытие паролей и обеспечение по защищенному каналу связи SSH. Результаты проведённой работы предоставлены на Рис. 2.16.

```
R7(config)#
R7(config)#line console 0
R7(config-line)#login local
R7(config-line)#exit
R7(config)#no username noc1
R7(config)#no username noc2
R7(config)#enable secret xkld7Hn434!2&^
R7(config)#username noc secret nTefa#51
R7(config)#end
R7#
%SYS-5-CONFIG_I: Configured from console by console
R7#exit



Press RETURN to get started!


User Access Verification

Username: noc
Password:

R7>

R7>en
Password:
Password:
Password:
R7#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R7(config)#
```

Рисунок 2.15 Установка паролей на переход в привилегированный режим.

Terminal

```
Press RETURN to get started!


User Access Verification

Username: noc
Password:

R7>
R7>
R7>en
Password:
R7#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R7(config)#
R7(config)#
R7(config)#username admin privilege 15 secret nTefa#51
R7(config)#enable secret 15 secret Rc@sxa&h
R7(config)#username engineer privilege 5 secret LwqndhR5
R7(config)#enable secret 5 secret Jnfbn&qd
R7(config)#username operator privilege 3 secret *mmfjj&D
R7(config)#enable secret 3 secret Mf88MMhl
R7(config)#privilege exec level 3 show running-config
R7(config)#privilege exec level 3 show startup-config
R7(config)#privilege exec level 3 show
R7(config)#privilege exec level 3 ping
R7(config)#privilege exec level 3 ssh
R7(config)#privilege exec level 3 telnet
R7(config)#privilege exec level 3 exit
R7(config)#privilege exec level 5 configure terminal
R7(config)#privilege exec level 5 configure
```

Рис. 1.16 а. Настройка механизма ролевого управления доступа к командам маршрутизатора

```
R7(config)#privilege configure level 5 ip
R7(config)#privilege configure level 5 no ip
R7(config)#privilege configure level 5 ip route
R7(config)#privilege configure level 5 no ip route
R7(config)#privilege configure level 5 ip router
R7(config)#privilege configure level 5 router
R7(config)#privilege configure level 5 no ip router
R7(config)#privilege configure level 5 no router
R7(config)#privilege configure level 5 interface
R7(config-line)#
R7(config-line)#end
R7#
%SYS-5-CONFIG_I: Configured from console by console

R7#exit
```

Рис. 1.16 б. Настройка механизма ролевого управления доступа к командам маршрутизатора

Контрольные вопросы

1. Перечисляйте механизмы реализации атак на маршрутизатор.
2. . Сформулируйте основные требования к средствам защиты маршрутизаторов.
3. Вычислить номер сети и номер узла для адреса 67.38.173.245 и маски 255.255.240.0
4. Вычислить номер сети и номер узла для адреса 192.168.74.66 и маски 255.255.255.192
5. Маска 255.255.254.0 и номер сети 192.168.74.0. Определить соответствующий блок адресов и их количество.
6. Маска 255.255.240.0 и номер сети 67.38.160.0. Определить соответствующий блок адресов и их количество.

СПИСОК ЛИТЕРАТУРЫ

1. Абдрахимов И.С. Решение задач по IP-адресации и статической маршрутизации. Учебно- методическое пособие. Иркутский государственный университет, 2010, http://window.edu.ru/resource/464/77464/files/manual.pdf

2. Использование командной строки. https://www.cisco.com/c/ru_ru/td/docs/ios/fundamentals/configuration/guide/12_4/cf_12_4_book/cf_cli-basics.html

3. Д.Н. Колегов. Лабораторный практикум по построению компьютерных сетей. Лабораторный практикум по основам построения защищенных компьютерных сетей. Томск: Томский государственный университет, 2013. – 140 с

4. Статья. Статическая маршрутизация Cisco. URL: http://pyatilistnik.org/staticheskaya-marshrutizatsiya-cisco/

5. Статья. Маршрутизация Cisco. URL: https://arny.ru/education/ccna-rs/materialy-cisco-ccna-marshrutizacziya/