

Addressing Table

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0/1	192.168.1.1	255.255.255.0	—
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
Server1	F0	192.168.1.3	255.255.255.0	192.168.1.1

Цели

Часть 1. Создание сети и настройка основных параметров устройства

Часть 2. Использование TFTP для резервного копирования и восстановления текущей конфигурации коммутатора

Часть 3. Использование TFTP для резервного копирования и восстановления текущей конфигурации маршрутизатора

Часть 4. Резервное копирование и восстановление текущих конфигураций с помощью флеш-памяти маршрутизатора

Общие сведения и сценарий

Сетевые устройства Cisco регулярно обновляются или меняют конфигурацию по ряду причин. В связи с этим необходимо регулярно создавать резервные копии последних конфигураций устройств и вести журнал изменений параметров. В производственных сетях для резервного копирования файлов конфигурации и образов IOS часто используется сервер TFTP. Сервер TFTP — это централизованный и безопасный способ хранения резервных копий файлов и их восстановления в случае необходимости. Используя централизованный сервер TFTP, можно создавать резервные копии файлов для различных устройств Cisco.

Помимо сервера TFTP, большинство современных маршрутизаторов Cisco могут создавать резервные копии и восстанавливать файлы локально с карты памяти CompactFlash (CF) или USB-накопителя. Карта памяти CF — это съемный модуль памяти, заменивший внутреннюю флеш-память ограниченного объема, которая использовалась в предыдущих моделях маршрутизаторов. Образ IOS для маршрутизатора находится на карте памяти CF и используется маршрутизатором для загрузки системы. Карты флеш-памяти большего объема

можно использовать для хранения резервных копий. Также для резервного копирования можно использовать съемный USB-накопитель.

В ходе этой лабораторной работы в режиме симуляции физического оборудования вам нужно будет сохранить резервную копию текущей конфигурации устройства Cisco на сервер TFTP или флеш-память, используя программное обеспечение сервера TFTP. Вы также создадите резервную копию текущей конфигурации на Flash.

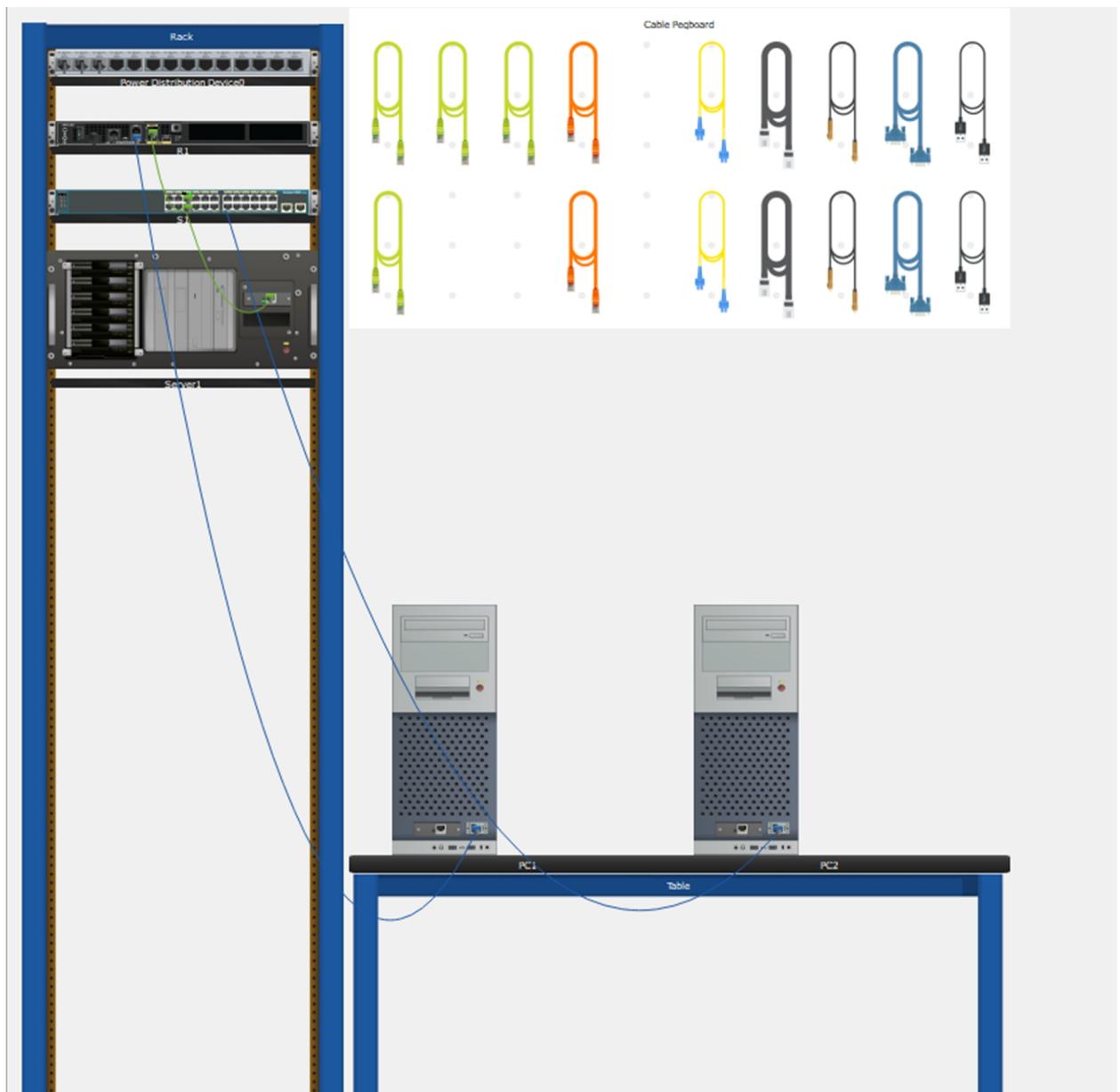
Часть 1. Создание сети и настройка основных параметров устройства

В части 1 вы построите кабельную топологию сети и сконфигурируете основные параметры, такие как IP-адреса интерфейсов для R1, S1 и Server1.

Примечание: Доступны два компьютера, позволяющие установить консольное подключение от одного ПК к маршрутизатору, а другого ПК — к коммутатору. Таким образом, вам не придется менять кабели во время выполнения задания.

Шаг 1. Создайте сеть.

Подключите сетевые кабели к устройствам в соответствии с топологией. Подключите консольный кабель от PC1 к R1. Подключите консольный кабель от PC2 к S1.



Шаг 2. Используйте вкладку CLI на маршрутизаторе для настройки основных параметров маршрутизатора.

- a. Откройте терминал до R1 с PC1. Выберите PC1 > Вкладка Desktop > Terminal и нажмите кнопку OK.
- b. Назначьте маршрутизатору имя устройства.
- c. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.
- d. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.
- e. Назначьте cisco в качестве пароля консоли и включите вход в систему по паролю.
- f. Установите cisco в качестве пароля виртуального терминала и активируйте вход.
- g. Зашифруйте открытые пароли.
- h. Создайте баннер, который предупреждает всех, кто обращается к устройству, видит баннерное сообщение Authorized Users Only.
- i. Настройте IP-адреса на интерфейсах, указанных в **таблице адресации**.
- j. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Примечание. Вопросительный знак (?) позволяет открыть справку с правильной последовательностью параметров, необходимых для выполнения этой команды.

```

Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#enable secret class
R1(config)#line con 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd "Some"
R1(config)#int g0/0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#w
Building configuration...
[OK]
R1#

```

Шаг 3. Используйте вкладку CLI на коммутаторе для настройки основных параметров коммутатора.

- a. Откройте терминал до S1 из PC2. Выберите PC2 > Вкладка Desktop > Terminal и нажмите кнопку OK.
- b. Присвойте коммутатору имя устройства.
- c. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.
- d. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.
- e. Назначьте cisco в качестве пароля консоли и включите вход в систему по паролю.
- f. Установите cisco в качестве пароля виртуального терминала и активируйте вход.

- g. Зашифруйте открытые пароли.
- h. отключение неиспользуемых интерфейсов
- i. Настройте подинтерфейсы для каждой VLAN, как указано в таблице IP-адресации.
- j. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Примечание. Вопросительный знак (?) позволяет открыть справку с правильной последовательностью параметров, необходимых для выполнения этой команды.

```

Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#enable secret class
S1(config)#line con 0
S1(config-line)#password cisco
S1(config-line)#loginn
^
% Invalid input detected at '^' marker.

S1(config-line)#login
S1(config-line)#exit
S1(config)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#int range f0/0-4, f0/7-24, g0/0-1
interface range not validated - command rejected
S1(config)#int range f0/1-4, f0/7-24, g0/0-1
interface range not validated - command rejected
S1(config)#int range f0/1-4, f0/7-24, g0/1-2
S1(config-if-range)#shutdown

S1(config-if-range)#exit
S1(config)#int vlan 1
S1(config-if)#ip address 192.168.1.11 255.255.255.0
S1(config-if)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#w
Building configuration...
[OK]
S1#

```

Шаг 4. На вкладке Desktop настройте сведения об IP-адресации для Server1 и проверьте подключение к S1 и R1.

- a. Проверка связи от Server1 до S1.
- b. Проверка связи от Server1 до R1.

Если команды ping завершились неудачно и связь установить не удалось, исправьте ошибки в основных настройках устройства.

```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=5ms TTL=128
Reply from 192.168.1.3: bytes=32 time=4ms TTL=128
Reply from 192.168.1.3: bytes=32 time=2ms TTL=128
Reply from 192.168.1.3: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 5ms, Average = 3ms

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=6ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 1ms
```

Часть 2. Использование TFTP для резервного копирования и восстановления текущей конфигурации коммутатора

В этой части выполняется резервное копирование на TFTP-сервер и восстановление конфигурации S1 с него.

Шаг 1. Запустите серверное приложение TFTP на сервере Server1.

На вкладке Services сервера Server1 включите приложение TFTP.

Приложение TFTP использует транспортный UDP-протокол уровня 4, который инкапсулируется в IP-пакет. Для передачи файлов по TFTP необходимы подключения 1-го и 2-го уровней (в данном случае Ethernet), а также подключение 3-го уровня (IP) между клиентом и сервером TFTP. В топологии локальной сети, представленной в данной лабораторной работе, в качестве протокола 1 и 2 уровня используется только Ethernet. В то же время передача данных по TFTP может быть выполнена и по WAN-соединениям, которые используют другие физические каналы 1-го уровня и протоколы 2-го уровня. Передача данных по TFTP возможна при условии, что между клиентом и сервером есть связь по IP, что можно проверить с помощью отправки команды ping. Если команды ping завершились неудачно и связь установить не удалось, исправьте ошибки в основных настройках устройства.

Примечание. Существует распространенное заблуждение, что файл можно передать по TFTP с помощью консольного подключения. Это не так, поскольку консольное подключение не использует IP-адрес. Клиентское устройство (маршрутизатор или коммутатор) с консольным подключением позволяет инициировать передачу данных по TFTP, но для успешной передачи файлов между клиентом и сервером должно быть установлено подключение по IP.

Шаг 2. Изучите применение команды copy на устройстве Cisco.

- Через консоль зайдите в коммутатор S1 и введите в окне командной строки привилегированного режима EXEC команду copy ?, что позволит получить параметры для источника (или исходного местоположения), а также другие доступные параметры копирования. В качестве источника можно указать flash: или flash0:. Если в качестве

источника указать просто имя файла, по умолчанию будет подразумеваться flash0:. Также в качестве источника можно указать running-config.

```
S1# copy ?
flash: Copy from flash: file system
ftp: Copy from ftp: file system
running-config Copy from current system configuration
scp: Copy from scp: file system
startup-config Copy from startup configuration
tftp: Copy from tftp: file system
S1# copy
```

- b. Выбрав местонахождение файла источника, введите символ ?, чтобы отобразить параметры для места назначения. В этом примере файловая система flash: для коммутатора S1 является файловой системой источником.

```
S1# copy flash: ?
ftp: Copy to ftp: file system
running-config Update (merge with) current system configuration
scp: Copy to scp: file system
startup-config Copy to startup configuration
tftp: Copy to tftp: file system
S1# copy flash:
```

Шаг 3. Передайте файл текущей конфигурации с коммутатора S1 на сервер TFTP на компьютере PC-A.

- a. На коммутаторе S1 перейдите в привилегированный режим EXEC и введите команду copy running-config tftp. Укажите адрес удаленного узла TFTP-сервера 192.168.1.3. Нажмите клавишу Enter (Ввод), чтобы принять имя файла назначения по умолчанию (s1-config), или укажите желаемое имя файла. Восклицательные знаки (!!) указывают на выполнение и успешное завершение передачи данных.

```
S1# copy running-config tftp:
Address or name of remote host []? 192.168.1.3
Destination filename [S1-config]?

Writing running-config....!
[OK - 1549 bytes]

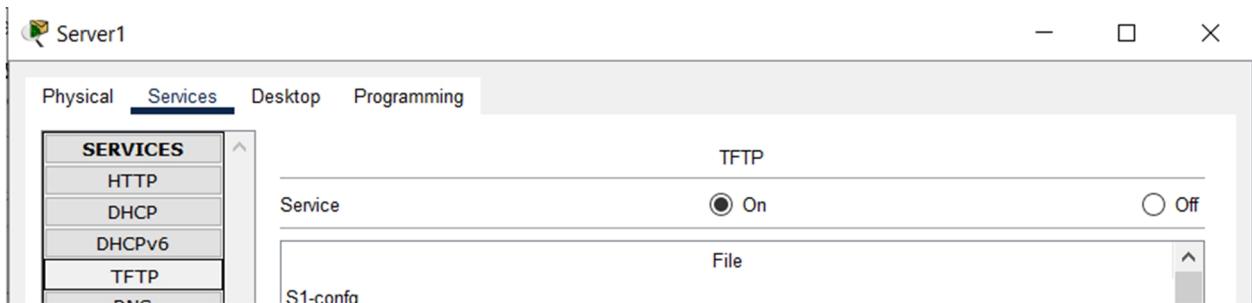
785 bytes copied in 0 secs
S1#
```

```
S1#copy running-config tftp
Address or name of remote host []? 192.168.1.3
Destination filename [S1-config]?

Writing running-config....!
[OK - 1511 bytes]

1511 bytes copied in 3 secs (503 bytes/sec)
S1#
```

- b. Проверьте каталог в приложении TFTP на сервере Server1 , чтобы убедиться, что файл был успешно передан. Выберите Server1 > вкладка Services > TFTP. Вы должны увидеть файл S1-Config, указанный в верхней части списка File.



Шаг 4. Измените текущую конфигурацию коммутатора и скопируйте запущенный файл конфигурации с сервера TFTP на коммутатор.

- На S1 создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.
- На коммутаторе S1 перейдите в привилегированный режим EXEC и введите команду `copy tftp: running-config`. Укажите адрес удаленного узла TFTP-сервера 192.168.1.3. Введите имя файла: `S1-config.txt`. Восклицательный знак (!) указывает на выполнение и успешное завершение передачи данных.

```

S1# copy tftp: running-config
Address or name of remote host []? 192.168.1.3
Source filename []? S1-config
Destination filename [running-config]?

Accessing tftp://192.168.1.3/S1-config...
Loading S1-config from 192.168.1.3: !
[OK - 1525 bytes]

1525 bytes copied in 0 secs
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#
Accessing tftp://192.168.1.3/S1-config...
Loading S1-config from 192.168.1.3: !
[OK - 1511 bytes]

1511 bytes copied in 0 secs
S1#
%SYS-5-CONFIG_I: Configured from console by console
|

```

- Ведите команду `show running-config`, чтобы просмотреть файл текущей конфигурации.

```

S1# show running-config
<output omitted>
interface Vlan1
ip address 192.168.1.11 255.255.255.0
!
ip default-gateway 192.168.1.1
!
banner motd ^CAuthorized Users Only! ^C
!
!
!
line con 0
password 7 0822455D0A16

```

```
login
!
<output omitted>
S1#
```

Примечание: Обратите внимание, что команда banner motd была добавлена после копирования запущенной конфигурации на сервер TFTP. Он все еще присутствует после того, как запущенная конфигурация была скопирована обратно с сервера TFTP.

Если вы не удалите загрузочную конфигурацию, процедура объединит рабочую конфигурацию с TFTP-сервера с текущей рабочей конфигурацией в коммутаторе или маршрутизаторе. Если в файл текущей конфигурации были внесены изменения, в копию TFTP будут добавлены соответствующие команды. В качестве альтернативы, если та же команда выполняется, она обновляет соответствующую команду в текущей рабочей конфигурации коммутатора или маршрутизатора.

Часть 3. Использование TFTP для резервного копирования и восстановления текущей конфигурации маршрутизатора

Процедуру резервного копирования и восстановления, приведенную в части 2, можно использовать и для маршрутизатора. В части 3 описывается резервное копирование и восстановление файла текущей конфигурации с помощью сервера TFTP.

Шаг 1. Перенесите текущую конфигурацию с R1 на сервер TFTP.

- Откройте программу Terminal на PC1 до R1.
- На маршрутизаторе R1 перейдите в привилегированный режим EXEC и введите команду copy running-config tftp. Укажите адрес удаленного узла TFTP-сервера, 192.168.1.3, и примите имя файла R1-config как имя по умолчанию.
- Убедитесь в том, что файл передан на сервер TFTP.

Шаг 2. Восстановите файл текущей конфигурации на маршрутизаторе.

Примечание: Если вы хотите полностью заменить текущий файл конфигурации файлом с TFTP-сервера, удалите файл загрузочной конфигурации с маршрутизатора и перезагрузите устройство. Затем настройте адрес интерфейса G0/0/0 для установки IP-подключения между TFTP-сервером и маршрутизатором.

- Удалите файл загрузочной конфигурации на маршрутизаторе.

```
R1#erase ?
  startup-config  Erase contents of configuration memory
R1#erase
R1#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]y[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
R1#
```

- Перезагрузите маршрутизатор.

```
R1#reload
System configuration has been modified. Save? [yes/no]:y
Building configuration...
[OK]
Proceed with reload? [confirm]
Initializing Hardware ...

System integrity status: 00000610
Rom image verified correctly
```

Примечание: Процент завершения будет временно ниже, пока вы не восстановите конфигурацию.

- Настройте интерфейс маршрутизатора G0/0/1, указав IP-адрес 192.168.1.1. Подождите, пока протокол связующего дерева (STP) не сойдется на S1.

- d. Проверьте подключение между маршрутизатором и Server1. Перед восстановлением подключения может потребоваться выполнить эхо-запрос несколько раз.

```
R1#ping 192.168.1.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
!!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

R1#
```

- e. Введите команду copy, чтобы передать файл конфигурации R1-config с TFTP-сервера на маршрутизатор. В качестве места назначения укажите running-config.

```
R1#copy running-config tftp
Address or name of remote host []? 192.168.1.3
Destination filename [R1-config]?

Writing running-config...!!!
[OK - 690 bytes]

690 bytes copied in 0 secs
R1#
```

- f. Убедитесь в том, что файл текущей конфигурации на маршрутизаторе обновлен. Запрос маршрутизатора должен быть изменен обратно на R1#, и процент завершения должен отражать, что вся ваша конфигурация восстановлена.



Часть 4. Резервное копирование и восстановление текущих конфигураций с помощью флеш-памяти маршрутизатора

Маршрутизаторы Cisco текущего поколения не имеют внутренней флэш-памяти. В этих устройствах используются карты памяти CompactFlash (CF). Это позволяет увеличить объем флеш-памяти и устанавливать обновления, не открывая корпус маршрутизатора. Помимо необходимых файлов, например, образов IOS, на картах памяти CF могут храниться и другие файлы, такие как копия текущей конфигурации.

Примечание. Если подключение карты памяти CF к маршрутизатору невозможно, его собственной флеш-памяти для сохранения резервной копии файла текущей конфигурации может не хватить. Тем не менее, прочтите инструкции и ознакомьтесь с командами.

Шаг 1. Отобразите файловые системы маршрутизатора.

Команда show file systems отображает доступные файловые системы маршрутизатора. Файловая система flash0: используется на маршрутизаторе по умолчанию, на что указывает символ звездочки (*) в начале строки. Файловая система flash0: также может обозначаться именем flash:. Общий размер flash0: составляет примерно 3 ГБ, а доступно около 2.5 ГБ. Сейчас единственными доступными файловыми системами являются flash0: и nvram:.

Примечание: Вам необходимо не менее 1 МБ (1 048 576 байт) свободного пространства. Чтобы определить размер флеш-памяти и ее доступный объем, в окне командной строки привилегированного режима EXEC введите команду show flash или dir flash:.

```
R1# show file systems
File Systems:

Size(b) Free(b) Type Flags Prefixes
* 3249049600 2761893177 flash rw flash:
29688 23590 nvram rw nvram:
```

Где находится файл загрузочной конфигурации?

Шаг 2. Скопируйте файл текущей конфигурации маршрутизатора во флеш-память.

Для этого введите команду copy в окно командной строки привилегированного режима EXEC. В данном примере файл копируется в систему flash0:, поскольку, как было показано выше, здесь доступен только один флеш-накопитель, и эта система используется по умолчанию. В качестве имени файла резервной копии текущей конфигурации используется R1-running-config-backup.

Примечание. Необходимо помнить, что в файловой системе IOS имена файлов чувствительны к регистру.

- Скопируйте файл текущей конфигурации во флеш-память.

```
R1# copy running-config flash:
Destination filename [running-config]? R1-running-config-backup
Building configuration...
[OK]
R1#
```

- Введите команду dir, чтобы проверить, скопирован ли файл текущей конфигурации во флеш-память.

```
R1# dir flash:
Directory of flash:/

6 -rw- 732 <no date> R1-running-config-backup
3 -rw- 486899872 <no date> isr4300-universalk9.03.16.05.S.155-3.S5-ext.SPA.bin
2 -rw- 28282 <no date> sigdef-category.xml
1 -rw- 227537 <no date> sigdef-default.xml

3249049600 bytes total (2761893177 bytes free)
```

- Введите команду more, чтобы посмотреть файл текущей конфигурации во флеш-памяти. Просмотрите выходные данные файла и найдите раздел Interface (Интерфейс). Обратите внимание на то, что для интерфейса GigabitEthernet0/1 команда no shutdown не указывается. Этот интерфейс отключен, если файл используется для обновления текущей конфигурации на маршрутизаторе.

```
R1# more flash:R1-running-config-backup
<output omitted>
interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
<output omitted>
```

Шаг 3. Удалите загрузочную конфигурацию и перезагрузите маршрутизатор.

- Удалите файл загрузочной конфигурации на маршрутизаторе.
- Перезагрузите маршрутизатор.

Примечание: Процент завершения будет временно ниже, пока вы не восстановите конфигурацию.

- Убедитесь в том, что на маршрутизаторе используется исходная конфигурация по умолчанию.

```

R1#erase
R1#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
R1#reload
System configuration has been modified. Save? [yes/no]:y
Building configuration...
[OK]
Proceed with reload? [confirm]
Initializing Hardware ...

System integrity status: 00000610
Rom image verified correctly

System Bootstrap, Version 15.4(3r)S5, RELEASE SOFTWARE
Copyright (c) 1994-2015 by cisco Systems, Inc.

Current image running: Boot ROM0

Last reset cause: LocalSoft
Cisco ISR4321/K9 platform with 4194304 Kbytes of main memory

no valid BOOT image found
Final autoboot attempt from default boot device...
File size is 0x1d0580a0
Located isr4300-universalk9.03.16.05.S.155-3.S5-ext.SPA.bin
Image size 486899872 inode num 12, bks cnt 102567 blk size 8*512
#####

```

Шаг 4. Восстановите файл текущей конфигурации из флеш-памяти.

- Скопируйте сохраненный файл текущей конфигурации из флеш-памяти для обновления файла текущей конфигурации.

```

Router# copy flash: running-config
Source filename []? R1-running-config-backup
Destination filename [running-config]?


```

```

732 bytes copied in 0.416 secs (1759 bytes/sec)
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#

```

- Команда **show ip interface brief** показывает состояние интерфейсов.

```

R1# show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0/0 unassigned YES NVRAM administratively down down
GigabitEthernet0/0/1 192.168.1.1 YES manual administratively down down
Vlan1 unassigned YES NVRAM administratively down down
R1#

```

- В Packet Tracer интерфейс G0/0/1 будет административно отключен. Войдите в режим настройки интерфейса и снова активируйте интерфейс. Задание должно быть выполнено на 100%.

