Cisco Packet Tracer. Отказоустойчивость маршрутизаторов и коммутаторов

Таблица адресации

Устройство	IP-адрес	Маска подсети	Шлюз по умолчанию	Сайт
HQ_Router	10.44.1.1	255.255.255.0	—	Metropolis Bank HQ

Задачи

Часть 1. Повышение надежности конфигурации IOS

Часть 2. Активация функции Cisco IOS Resilient Configuration

Общие сведения

В ходе выполнения этого упражнения вы повысите надежность конфигурации IOS маршрутизатора в сетевой инфраструктуре Metropolis. Затем вы включите функцию отказоустойчивости IOS на маршрутизаторе Cisco. Настройка IP-адресации, сети и сервисов уже завершена. Для развертывания отказоустойчивой конфигурации IOS будут использоваться клиентские устройства в сетевой инфраструктуре Metropolis.

Часть 1: Повышение надежности конфигурации IOS

Шаг 1: Откройте интерфейс командной строки на компьютере пользователя Sally.

a. Выберите узел **Metropolis Bank HQ** и выберите компьютер пользователя **Sally**.

b. Перейдите на вкладку **Desktop** (Рабочий стол) и щелкните значок **Command Prompt** (Командная строка).

Шаг 2: Выполните удаленное подключение к маршрутизатору HQ_Router.

a. Установите с маршрутизатором **HQ_Router** соединение по протоколу SSH. Для этого в командной строке введите **ssh –l admin 10.44.1.1**. В открывшемся окне введите пароль **cisco12345**.

b. В командной строке введите **enable**, а затем, после приглашения, пароль привилегированного режима **class**.

   В командной строке должно отображаться следующее:

   ```
   HQ_Router#
   ```

c. Было ли показано предупреждающее сообщение, препятствующее доступу неавторизованных пользователей к маршрутизатору HQ_Router?

   нет

Шаг 3: Создайте правовое уведомление на маршрутизаторе HQ_Router.

a. В командной строке `HQ_Router#` введите команду **configure terminal** для перехода в режим глобальной настройки.

b. В командной строке `HQ_Router(config)#` введите следующие команды:

```
banner motd #
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED
You must have explicit, authorized permission to access or configure this device.
Unauthorized attempts and actions to access or use this system may result in civil and/or
criminal penalties.
All activities performed on this device are logged and monitored.
#
```

c. В командной строке `HQ_Router(config)#` введите команды **end** и **logout** для завершения соединения с маршрутизатором **HQ_Router**.

d. Снова установите соединение по протоколу SSH с маршрутизатором **HQ_Router** с компьютера пользователя **Sally**. Пароль SSH — **cisco12345**.

Был ли показан какой-либо дополнительный текст или информационное сообщение при успешном подключении к **HQ_Router**? Что было показано?

Да, был показан баннер

Шаг 4: Настройте парольную защиту на маршрутизаторе HQ_Router.

a. В командной строке введите **enable**, а затем, после приглашения, пароль привилегированного режима **class**.

b. Войдите в режим глобальной конфигурации с помощью команды **configure terminal**. В командной строке `HQ_Router(config)#` введите следующие команды:

```
!шифрует незашифрованные пароли в running-config
service password-encryption

!все новые сконфигурированные пароли должны содержать не менее 10 символов
security passwords min-length 10
```

Часть 2: Активация функции Cisco IOS Resilient Configuration

Шаг 1: Просмотрите текущий образ IOS.

a. После подключения по протоколу SSH с компьютера **Sally** введите команду **exit** для возврата к командной строке `HQ_Router#`.

b. Введите команду **dir flash:** для просмотра текущего файла IOS.bin.

Как называется текущий файл .bin в команде flash?

c2900-universalk9-mz.SPA.151-4.M4.bin

Шаг 2: Обеспечьте защиту текущего образа и конфигурации.

a. В командной строке `HQ_Router#` введите команду **configure terminal** для перехода в режим глобальной настройки.

b. С помощью команды **secure boot-image** в командной строке `HQ_Router(config)#` активируйте резервное копирование образа IOS и запретите показ файла IOS в выводе содержимого каталога, а также удаление защищенного файла IOS.

c. Используйте команду **secure boot-config** в командной строке `HQ_Router(config)#`, чтобы сохранить защищенную копию текущей конфигурации и предотвратить удаление защищенного файла конфигурации.

d. Вернитесь в привилегированный режим EXEC с помощью команды **exit**. Введите команду **dir flash:** для просмотра текущего файла IOS.bin.

Показан ли в выводе файл IOS.bin? нет

e. В командной строке `HQ_Router#` введите команду **show secure bootset** для просмотра статуса образа Cisco IOS и резервного копирования конфигурации.

Предлагаемый способ подсчета баллов

Раздел упражнений	Вопрос	Максимальное количество баллов	Заработанные баллы
Часть 1. Повышение надежности конфигурации IOS	Шаг 2	10	
	Шаг 3	10	
Часть 2. Активация функции Cisco IOS Resilient Configuration	Шаг 1	10	
	Шаг 2	10	
Вопросы		**40**	
Балл Packet Tracer		**60**	
Общее число баллов		**100**	