Использование TFTP и Flash для управления файлами конфигурации и выполнение процедур восстановления пароля. Настройка протоколов CDP, LLDP и NTP

Топология

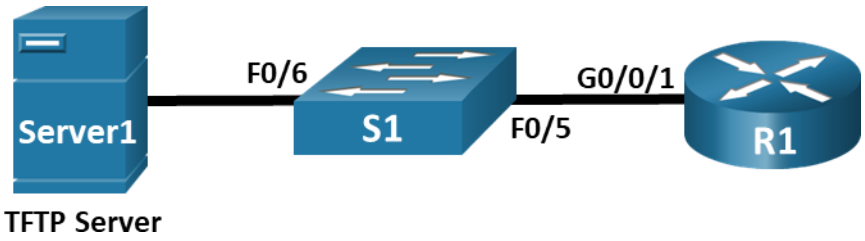

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1_ФАМИЛИЯ	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
S2 (с шага №7)	VLAN 1	192.168.1.12	255.255.255.0	192.168.1.1
TFTP Server	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

Часть 5. Изучение регистра конфигурации

Часть 6. Описание процедуры восстановления пароля для отдельного маршрутизатора Cisco

Часть 7. Добавление нового коммутатора S2 и настройка его основных параметров

Часть 8. Обнаружение сетевых ресурсов с помощью протокола CDP

Часть 9. Обнаружение сетевых ресурсов с помощью протокола LLDP

Часть 10. Настройка и проверка NTP

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.

Цель этого задания — изучение процедуры восстановления или сброса пароля на определенном маршрутизаторе Cisco. Такой пароль ограничивает доступ к привилегированному режиму EXEC и режиму конфигурации на устройствах Cisco. Пароль можно восстановить, однако надежный пароль хранится в зашифрованном виде и в случае утери должен быть заменен новым паролем.

Чтобы обойти пароль, пользователь должен быть знаком с режимом ROMMON (монитор ПЗУ), а также с настройкой регистра конфигурации для маршрутизаторов Cisco. ROMMON — это базовая программа с интерфейсом командной строки, которая хранится в ПЗУ и может использоваться для устранения неполадок загрузки и восстановления маршрутизатора в случаях, если не удается обнаружить IOS.

В этой работе вы изучите назначение и настройки регистра конфигурации для устройств Cisco. а затем подробно рассмотрите и опишете процедуру восстановления пароля для отдельного маршрутизатора Cisco. Наконец, с помощью Packet Tracer вы будете практиковать процедуру с помощью регистра конфигурации для восстановления пароля на маршрутизаторе Cisco 2911.

Протокол Cisco Discovery Protocol (CDP) — собственный протокол Cisco для обнаружения сетевых ресурсов, функционирующий на канальном уровне. Он служит для обмена информацией, например именами устройств и версиями ПО IOS, с другими физически подключенными устройствами Cisco. Протокол Link Layer Discovery Protocol (LLDP) — это не зависящий от производителя протокол для обнаружения сетевых ресурсов, функционирующий на канальном уровне. В основном он используется сетевыми устройствами в локальной сети (LAN). Сетевые устройства сообщают соседям такие данные о себе, как идентификаторы и сведения о функциональных возможностях.

Протокол сетевого времени (NTP) служит для синхронизации времени между распределенными серверами времени и клиентами. В качестве транспортного протокола NTP использует протокол UDP. Все операции обмена данными по протоколу NTP выполняются по времени в формате UTC.

Сервер NTP обычно получает данные о времени из достоверного источника, такого как атомные часы, к которым подключен сервер. Затем он распределяет это время по сети. Протокол NTP чрезвычайно эффективен; для синхронизации времени на двух компьютерах с временной разницей в пределах миллисекунды требуется отправлять не более одного пакета в минуту

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_ФАМИЛИЯ, S1 и TFTP Server.

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_ФАМИЛИЯ**. Подключите консольный кабель от **PC2** к **S1**.

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

a. Откройте терминал до R1_ФАМИЛИЯ с PC1. Выберите **PC1** > Вкладка **Desktop** > **Terminal** и нажмите кнопку **ОК**.

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.

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 **ОК**.

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.

Шаг 4. На вкладке Desktop настройте сведения об IP-адресации для TFTP Server и проверьте подключение к S1 и R1_ФАМИЛИЯ.

a. Проверка связи от **TFTP Server** до **S1**.

b. Проверка связи от **TFTP Server** до **R1_ФАМИЛИЯ**.

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

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 TFTP Server.

На вкладке Services сервера **TFTP Server** 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.

a. 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 источника.

```
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-confg**), 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-confg]?

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

785 bytes copied in 0 secs
S1#
```

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

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

a. На **S1** создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.

b. 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-confg.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-confg
```

```
Destination filename [running-config]?

Accessing tftp://192.168.1.3/S1-confg...
Loading S1-confg 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#
```

c. Просмотрите файл текущей конфигурации на 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_ФАМИЛИЯ на сервер TFTP.

a. Откройте программу **Terminal** на **PC1** до **R1_ФАМИЛИЯ**.

b. На маршрутизаторе **R1_ФАМИЛИЯ** 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_ФАМИЛИЯ-config** как имя по умолчанию.

c. Убедитесь в том, что файл передан на сервер TFTP.

Шаг 2. Восстановите файл текущей конфигурации на маршрутизаторе.

Примеччание: 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.

a. Удалите файл загрузочной конфигурации на маршрутизаторе.

b. Перезагрузите маршрутизатор.

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

c. 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 **TFTP Server**. Перед восстановлением подключения может потребоваться выполнить эхо-запрос несколько раз.

e. Введите команду **copy**, чтобы передать файл конфигурации **R1_ФАМИЛИЯ-config** с TFTP-сервера на маршрутизатор. В качестве места назначения укажите **running-config**.

f. Убедитесь в том, что файл текущей конфигурации на маршрутизаторе обновлен. Запрос маршрутизатора должен быть изменен обратно на **R1_ФАМИЛИЯ#**, 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:**.

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_ФАМИЛИЯ-running-config-backup**.

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

a. Скопируйте файл текущей конфигурации во флеш-память.

```
R1_ФАМИЛИЯ# copy running-config flash:
Destination filename [running-config]? R1_ФАМИЛИЯ-running-config-backup
Building configuration...
[OK]
R1_ФАМИЛИЯ#
```

b. Введите команду **dir flash:** на R1_ФАМИЛИЯ, чтобы проверить, скопирован ли файл текущей конфигурации во флеш- память.

c. 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_ФАМИЛИЯ# more flash:R1_ФАМИЛИЯ-running-config-backup
```

Шаг 3. Удалите загрузочную конфигурацию и перезагрузите маршрутизатор.

a. Удалите файл загрузочной конфигурации на маршрутизаторе.

b. Перезагрузите маршрутизатор.

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

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

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

b. Отобразите состояние интерфейсов на R1_ФАМИЛИЯ.

c. В Packet Tracer интерфейс G0/0/1 будет административно отключен. Войдите в режим настройки интерфейса и снова активируйте интерфейс.

Часть 5. Изучение регистра конфигурации

Чтобы восстановить или сбросить пароль, вы получите доступ к интерфейсу ROMMON, чтобы дать маршрутизатору команду игнорировать загрузочную конфигурацию при загрузке. При загрузке войдите в привилегированном режиме EXEC, перезапишите текущую конфигурацию сохраненной конфигурацией запуска. Затем вы восстановите или сбросите пароль и восстановите процесс загрузки маршрутизатора, чтобы включить конфигурацию запуска.

Регистр конфигурации маршрутизатора играет ключевую роль в процессе восстановления пароля. В первой части этой работы вы узнаете предназначение регистра конфигурации маршрутизатора и функции некоторых его значений.

Шаг 1. Опишите предназначение регистра конфигурации.

Для чего необходим регистр конфигурации?

С помощью какой команды можно изменить регистр конфигурации в глобальном режиме конфигурации?

С помощью какой команды можно изменить регистр конфигурации в ROMMON режиме?

Шаг 2. Определите значения регистра конфигурации и их функции.

Изучите и опишите поведение маршрутизатора со следующими значениями регистра конфигурации:

0x2102

0x2142

Чем отличаются эти значения регистра конфигурации?

Часть 6. Описание процедуры восстановления пароля для отдельного маршрутизатора Cisco

Во этой части вам необходимо описать точную процедуру восстановления или сброса пароля для отдельного маршрутизатора Cisco серии 2900 и ответить на вопросы, исходя из полученных результатов.

Шаг 1. Подробно опишите процесс восстановления пароля для отдельного маршрутизатора Cisco.

Изучите и опишите шаги и команды, необходимые для восстановления или сброса простого или защищенного пароля на вашем маршрутизаторе Cisco. Кратко изложите шаги своими словами.

Шаг 2. С помощью Packet Tracer выполните восстановление enable password и secret password на маршрутизаторе R1_ФАМИЛИЯ.

Представьте, что вы только что вернулись с недельной конференции. Вы пытаетесь войти в основной маршрутизатор компании, но пока вас не было, кто-то изменил пароль включения. Вам не удается войти в маршрутизатор.

a. С рабочего стола ноутбука используйте режим терминала для подключения к маршрутизатору. Поскольку пароли вам неизвестны, вы не сможете войти в систему.

b. В режиме симуляции физического оборудования перейдите к виду маршрутизатора в стойке сзади и выключите маршрутизатор.

c. Включите маршрутизатор и быстро вернитесь в режим терминала на ноутбуке и введите **Ctrl+c** до завершения отображения меток загрузки хэша (#####). Если вы недостаточно быстро действовали, нажмите кнопку включения питания маршрутизатора еще раз. Вы должны оказаться в режиме ROMMON.

   Примечание.На реальном оборудовании вам может потребоваться ввести **Alt-B** вместо **Ctrl-c**

   ```
   rommon 1 >
   ```

   Примечание. Для выполнения этой процедуры на реальном оборудовании вы должны физически находиться рядом с маршрутизатором. Важно, чтобы корпорация обеспечивала сильную физическую безопасность для всех сетевых устройств.

d. Измените значение регистра конфигурации и перезагрузитесь.

   ```
   rommon 1 > confreg 0x2142
   rommon 2 > reset
   ```

e. Убедитесь, что вы ввели **N** в вопрос начальной настройки диалогового окна. Вы будете находиться в пользовательском режиме EXEC. Перейдите в привилегированный режим EXEC.

f. Скопируйте файл загрузочной конфигурации в текущую конфигурацию. Запрос маршрутизатора должен был измениться на Main#

g. Внесите следующие изменения в текущую конфигурацию:

   1) Измените запрос маршрутизатора на Branch.

   2) Измените секретный пароль на **branch1**.

   3) Измените пароли строки консоли vty на **branch2**.

   4) Добавьте баннер «Password recovered».

   5) Проверьте значение регистра конфигурации.

   6) Измените регистр конфигурации на 0x2102 в режиме глобальной конфигурации.

      ```
      Branch(config)# config-register 0x2102
      ```

   7) Сохранение текущей конфигурации в качестве начальной.

h. Перезагрузите маршрутизатор и войдите в систему с новыми паролями.

i. Изучите текущую конфигурацию маршрутизатора. Обратите внимание, что интерфейсы находятся в выключеном режиме. Повторно активируйте интерфейсы G0/0 и G0/2.

Шаг 3. Ответьте на вопросы о процедуре восстановления пароля.

Используя процедуру восстановления пароля, ответьте на приведенные ниже вопросы.

Как определить текущий параметр регистра конфигурации?

Опишите процесс перехода в режим ROMMON.

Какие команды необходимы для входа в интерфейс ROMMON?

Какое сообщение должно появиться во время загрузки маршрутизатора?

Зачем загрузочную конфигурацию необходимо загрузить в текущую?

Почему важно вернуть исходное значение регистра конфигурации после восстановления пароля?

Часть 7. Добавление нового коммутатора S2 и настройка его основных параметров

Шаг 1. Добавление нового устройства согласно топологии.

Добавьте еще один коммутатор, как показано в топологии, и подсоедините необходимые кабели. Удалять TFTP сервер не нужно!

Шаг 3. Настройте базовые параметры коммутатора S2.

a. Присвойте коммутатору имя устройства.

b. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

c. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.

d. Назначьте **cisco** в качестве пароля консоли и включите вход в систему по паролю.

e. Назначьте **cisco** в качестве пароля VTY и включите вход в систему по паролю.

f. Зашифруйте открытые пароли.

g. Создайте баннер, который предупреждает всех, кто обращается к устройству, видит баннерное сообщение «Только авторизованные пользователи!».

h. Отключите неиспользуемые интерфейсы.

i. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Часть 8. Обнаружение сетевых ресурсов с помощью протокола CDP

На устройствах Cisco протокол CDP включен по умолчанию. Воспользуйтесь CDP, чтобы обнаружить порты, к которым подключены кабели.

a. На R1_ФАМИЛИЯ используйте соответствующую команду **show cdp**, чтобы определить, сколько интерфейсов включено CDP, сколько из них включено и сколько отключено.
Сколько интерфейсов участвует в объявлениях CDP? Какие из них активны?

b. На R1_ФАМИЛИЯ используйте соответствующую команду **show cdp**, чтобы определить версию IOS, используемую на S1.

```
R1_ФАМИЛИЯ # show cdp entry  S1
```

Какая версия IOS используется на S1?

c. На S1 используйте соответствующую команду **show cdp**, чтобы определить, сколько пакетов CDP было выданных.

```
S1# show cdp traffic
```

Сколько пакетов имеет выход CDP с момента последнего сброса счетчика?

d. Настройте SVI для VLAN 1 на S1 и S2, используя IP-адреса, указанные в таблице адресации выше. Настройте шлюз по умолчанию для каждого коммутатора на основе таблицы адресов.

e. На R1_ФАМИЛИЯ выполните команду **show cdp**

entry S1. Какие дополнительные сведения

доступны теперь?

f. Отключить CDP глобально на всех устройствах.

Часть 9. Обнаружение сетевых ресурсов с помощью протокола LLDP

На устройствах Cisco протокол LLDP может быть включен по умолчанию. Воспользуйтесь LLDP, чтобы обнаружить порты, к которым подключены кабели.

a. Введите соответствующую команду **lldp**, чтобы включить LLDP на всех устройствах в топологии.

b. На S1 выполните соответствующую команду **lldp**, чтобы предоставить подробную информацию о S2.

```
S1# show lldp entry S2
```

Что такое chassis ID для коммутатора S2?

c. Соединитесь через консоль на всех устройствах и используйте команды LLDP, необходимые для отображения топологии физической сети только из выходных данных команды show.

Часть 10. Настройка NTP

В части 10 необходимо выполнить синхронизацию времени для Syslog и отладочных функций. Если время не синхронизировано, сложно определить, какое сетевое событие стало причиной данного сообщения.

Шаг 1. Выведите на экран текущее время.

Введите команду для отображения текущего времени на R1_ФАМИЛИЯ. Запишите отображаемые сведения о текущем времени в следующей таблице.

Дата	Время	Часовой пояс	Источник времени

Шаг 2. Установите время.

Установите текущее время на маршрутизаторе R1_ФАМИЛИЯ. Введенное время должно быть в формате UTC.

Шаг 3. Настройте главный сервер NTP.

Настройте R1_ФАМИЛИЯ в качестве сервера NTP с уровнем слоя 4.

Шаг 4. Настройте клиент NTP.

a. Выполните соответствующую команду на S1 и S2, чтобы просмотреть настроенное время. Запишите текущее время, в следующей таблице.

Дата	Время	Часовой пояс

b. Настройте S1 и S2 в качестве клиентов NTP. Используйте соответствующие команды NTP для получения времени от интерфейса G0/0/1 R1_ФАМИЛИЯ, а также для периодического обновления календаря или аппаратных часов коммутатора.

Шаг 5. Проверьте настройку NTP.

a. Используйте соответствующую команду **show**, чтобы убедиться, что S1 и S2 синхронизированы с R1_ФАМИЛИЯ.

b. Выполните соответствующую команду на S1 и S2, чтобы просмотреть настроенное время и сравнить ранее записанное время.