**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,**

**СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»**

**(СПбГУТ)**

Факультет Инфокоммуникационных сетей и систем

Кафедра Защищенных систем связи

Дисциплина Принципы организации глобальных вычислительных сетей

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №10**

CDP, LLDP, NTP, TFTP

*(тема отчета)*

Направление/специальность подготовки

11.03.02 Инфокоммуникационные технологии и системы связи

*(код и наименование направления/специальности)*

Студенты группы ИКТЗ-83:

Громов А. А

*(Ф.И.О., № группы) (подпись)*

Миколаени М. С,

*(Ф.И.О., № группы) (подпись)*

Проверил:

Ушаков И. А., ст. преп.

*(Ф.И.О., должн.) (подпись)*

Оглавление

[10.1.5 - Packet Tracer - Создание карты сети с помощью протокола CDP 3](#_Toc98839084)

[10.2.6 - Packet Tracer - Создание карты сети с помощью протокола LLDP 7](#_Toc98839085)

[10.3.4 - Packet Tracer. Настройка и проверка протокола NTP 14](#_Toc98839086)

[10.6.10 - Packet Tracer - Резервное копирование файлов конфигурации 17](#_Toc98839087)

[10.6.12 – Packet Tracer - Use TFTP and flash to manage configuration files 20](#_Toc98839088)

[10.6.13 - Packet Tracer - Исследование и выполнение процедур восстановления пароля - Режим симуляции физического оборудования 26](#_Toc98839089)

[10.7.6 - Packet Tracer - Использование TFTP-сервера для обновления образа Cisco IOS 28](#_Toc98839090)

# 10.1.5 - Packet Tracer - Создание карты сети с помощью протокола CDP

Топология

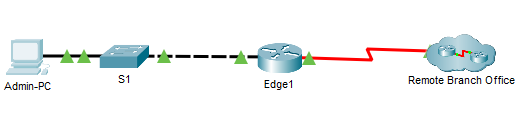
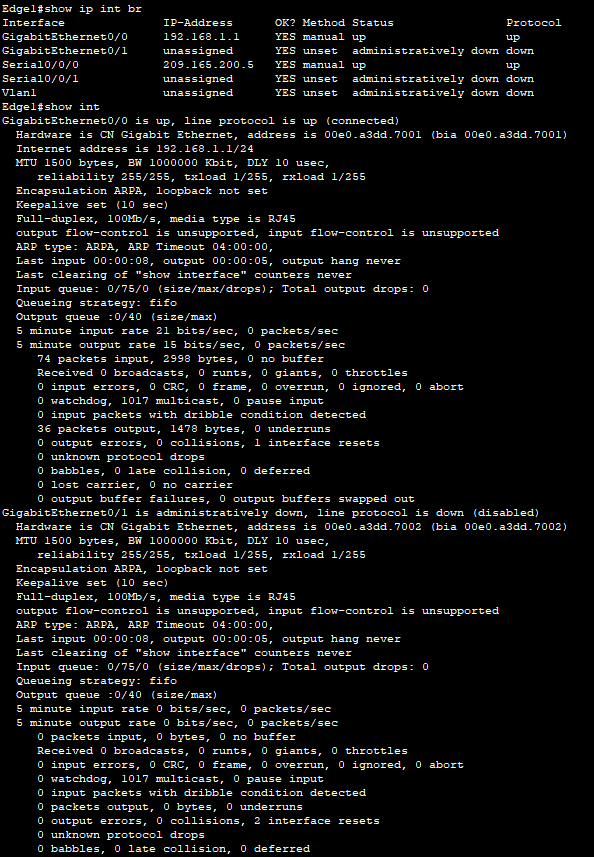


Таблица адресации

| **Устройство** | **Интерфейс** | **IP-адрес** | **Маска подсети** | **Интерфейс локальной сети и подключенный сосед** |
| --- | --- | --- | --- | --- |
| Edge 1 | G0/0 | 192.168.1.1 | 255.255.255.0 | G0/1 — S1 |
| *Граница 1* | S0/0/0 | *пусто* | *пусто* | S0/0/0 — ISP |
| Remote branch Office | S0/0/1 | 209.165.200.10 | *пусто* | S0/0/1 — ISP |
| пустReо | пусто | пусто | пусто | пусто |

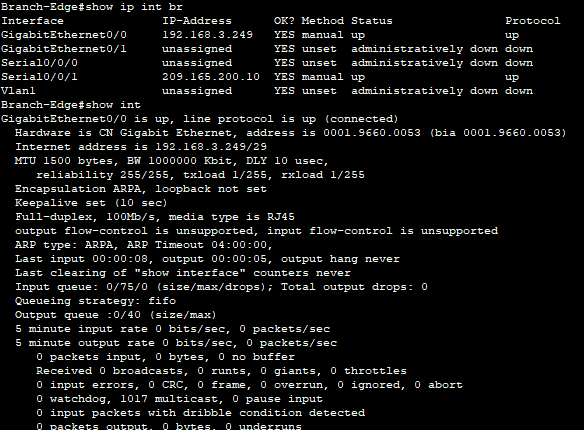
Часть 1. Удаленный доступ к сетевым устройствам по протоколу SSH

в.

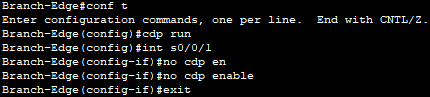


Часть 2: Получение сведений о соседних устройствах с помощью протокола CDP

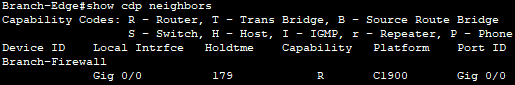
А.



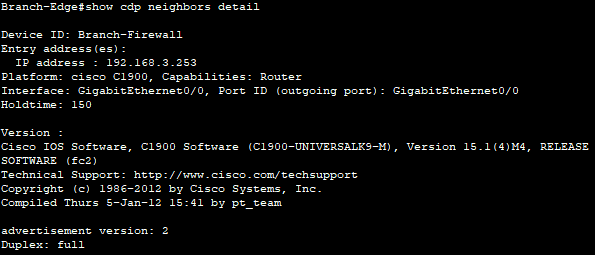
В.



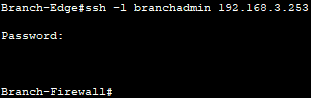
Г.



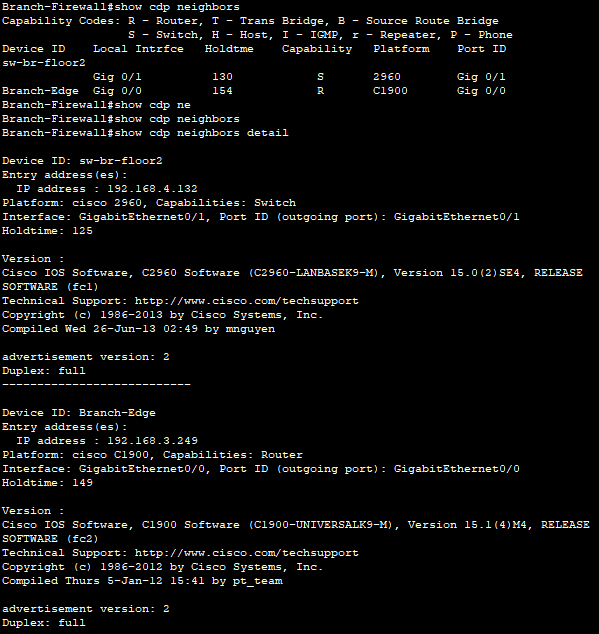
Д.



Е.



Ж.



# 10.2.6 - Packet Tracer - Создание карты сети с помощью протокола LLDP

Таблица адресации

| Устройство | Интерфейс | IP-адрес | Маска подсети | Интерфейс локальной сети и подключенный сосед |
| --- | --- | --- | --- | --- |
| Периметр | G0/0 | 192.168.1.1 | 255.255.255.0 | *Пустой экран* |
| *Периметр* | S0/0/0 | *Пустой экран* | *Пустой экран* | S0/0/0 — ISP |
| *Пустой экран* | SVI | 192.168.1.2 | *Пустой экран* | *пусто* |
| *Пустой экран* | G0/0 | 209.165.200.10 | *Пустой экран* | G0/0 - ISP |

Цели

Создайте карту сети с помощью протокола LLDP и удаленного доступа по протоколу SSH.

Общие сведения и сценарий

Старшему администратору сети необходимо сопоставить сеть удаленного филиала и обнаружить сведения обо всех устройствах в сети. Вы должны задокументировать имена всех сетевых устройств, их IP-адреса и маски подсетей, имена физических интерфейсов, посредством которых сетевые устройства соединены друг с другом.

Для создания карты сети нужно использовать удаленный доступ по протоколу SSH и применить протокол LLDP для получения сведений о соседних сетевых устройствах. Поскольку протокол LLDP является протоколом уровня 2, его можно использовать для сбора сведений об устройствах, которым не назначены IP-адреса. Полученную информацию следует внести в таблицу адресации. Кроме того, потребуется создать диаграмму топологии сети удаленного филиала Remote Branch Office.

IP-адрес сети удаленного филиала — 209.165.200.10. Учетные данные для локального и удаленного административного доступа:

Локальная сеть

Username: admin01

Password: S3cre7P@55

Сеть филиала

Username: RBOadmin

Password: S3cre7P@55

Инструкция

Часть 1: Удаленный доступ к сетевым устройствам по протоколу SSH

В первой части вам предстоит удаленно подключиться с Admin-PC к маршрутизатору Edge1, являющемуся шлюзом. Затем вам потребуется подключиться с маршрутизатора Edge1 к сети удаленного филиала Remote Branch Office по протоколу SSH.

a.     На компьютере Admin-PC откройте интерфейс командной строки.

б.     Подключитесь по протоколу SSH к маршрутизатору, являющемуся шлюзом, которому присвоен IP-адрес 192.168.1.1. Для этого используйте следующие учетные данные: имя пользователя — admin01, пароль — S3cre7P@55.

PC> ssh –l admin01 192.168.1.1

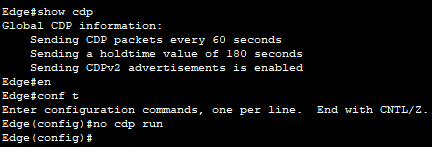
Открытая система

Password:

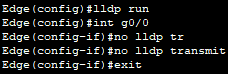
Edge#

Примечание. Обратите внимание: вы попадаете сразу в исполнительский режим EXEC. Это связано с тем, что учетной записи пользователя admin01 предоставлены разрешения уровня 15.

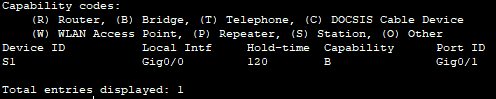
в.     Маршрутизатор Edge ранее был настроен на использование CDP. Коммутатор S1 уже настроен на использование LLDP. Выполните команду show cdp, чтобы убедиться, что CDP в данный момент активен. Отключите CDP, выполнив следующую команду:



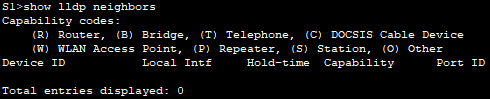
г.     LLDP может быть сконфигурирован для передачи и приема на определенном интерфейсе. Настройте Edge таким образом, чтобы он получал сообщения LLDP от S1, но не отправлял сообщения S1 в целях безопасности включить LLDP.



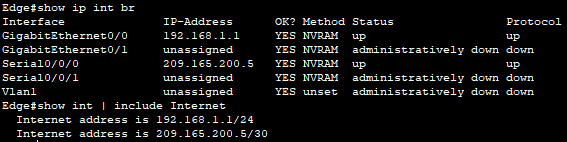
д.     Используйте команду show lldp neighbors, чтобы убедиться, что Edge получает сообщения от S1.



е.     Подключайтесь к S1 с помощью SSH от пограничного маршрутизатора, используя учетные данные admin01. Выполните команду show lldp neighbors. Обратите внимание, что S1 не получил информацию от Edge.



ж.     Выйдите из соединения с S1, чтобы вернуться к интерфейсу командной строки пограничного маршрутизатора. Выполните команды show ip interface brief и show interfaces, чтобы отобразить сведения о физических интерфейсах маршрутизатора Edge1, соответствующих IP-адресах и масках подсетей, а затем внесите необходимую информацию в таблицу адресации.



з.     В сеансе с пограничным маршрутизатором подключитесь с помощью SSH к удаленному RBO Office по адресу 209.165.200.10 с именем пользователя RBOadmin и тем же паролем, что и для admin01.

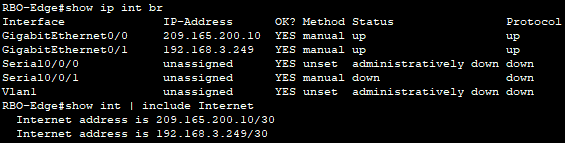
Вопрос:

Какие из отсутствовавших ранее сведений можно внести в таблицу адресации после подключения к сети удаленного филиала Remote Branch Office по адресу 209.165.200.10?

Часть 2: Получение сведений о соседних устройствах с помощью протокола LLDP

Вы удаленно подключены к маршрутизатору Branch-Edge. Приступите к сбору сведений о подключенных сетевых устройствах с помощью протокола LLDP.

a.     Выполните команды show ip interface brief и show interfaces, чтобы отобразить сведения о сетевых интерфейсах маршрутизатора RBO-Edge, соответствующих IP-адресах и масках подсетей. Внесите в таблицу адресации отсутствующие сведения, необходимые для создания карты сети.

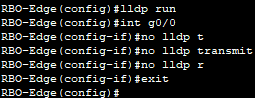


б.     В целях обеспечения безопасности протокол LLDP следует использовать только в случае необходимости, поэтому, возможно, потребуется включить LLDP. Выполните команду show lldp, чтобы проверить состояние протокола.

RBO-Edge# show lldp

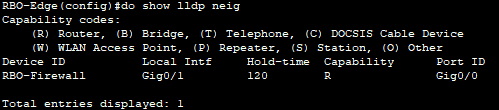
% LLDP is not enabled (LLDP не включен)

в.     Вам необходимо включить протокол CDP, однако широковещательную рассылку информации LLDP при этом рекомендуется организовать только для внутренних сетевых устройств, а не для внешних сетей. Узнайте, какой интерфейс подключен к Интернету, выполнив команду show ip interface brief. Включите протокол LLDP и полностью отключите LLDP на интерфейсе, подключенном к Интернету.



г.     Выполните команду show lldp neighbors, чтобы найти соседние сетевые устройства.

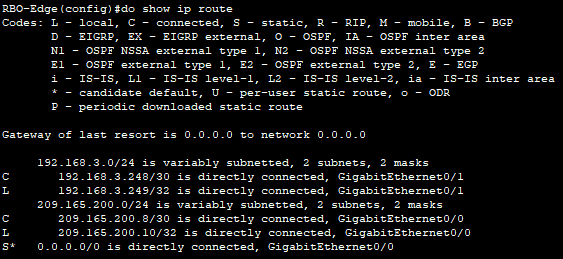
Примечание. LLDP будет показывать только подключенные устройства, на которых также работает LLDP.



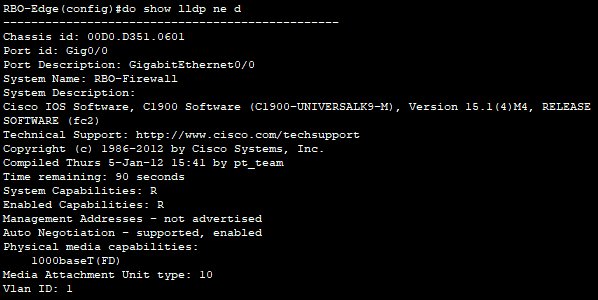
Вопрос:

Обнаружено ли соседнее сетевое устройство? К какому типу устройств оно относится? Какое имя ему присвоено? Через какой интерфейс подключено это устройство? Указан ли IP-адрес устройства? Внесите эти сведения в таблицу адресации.

д.     Используйте команду show ip route для определения адреса устройства, найденного с помощью команды show lldp neighbors. Основываясь на сведениях о локальном адресе в таблице маршрутизации и длине префикса сети, используйте эту информацию для определения адреса соседа.



е.     Чтобы найти дополнительную информацию от соседнего устройства, используйте команду show lldp neighbors detail:



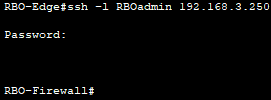
Вопрос:

Какая еще потенциально конфиденциальная информация содержится в результатах выполнения команды, помимо IP-адреса соседнего устройства?

Примечание. Текущая версия Packet Tracer не предоставляет адрес управления соседнего устройства. В этом задании несколько адресов соседних устройств были предоставлены в таблице адресации.

ж.     Подключайтесь к соседнему устройству с помощью SSH, чтобы обнаружить другие устройства, которые могут быть его соседями.

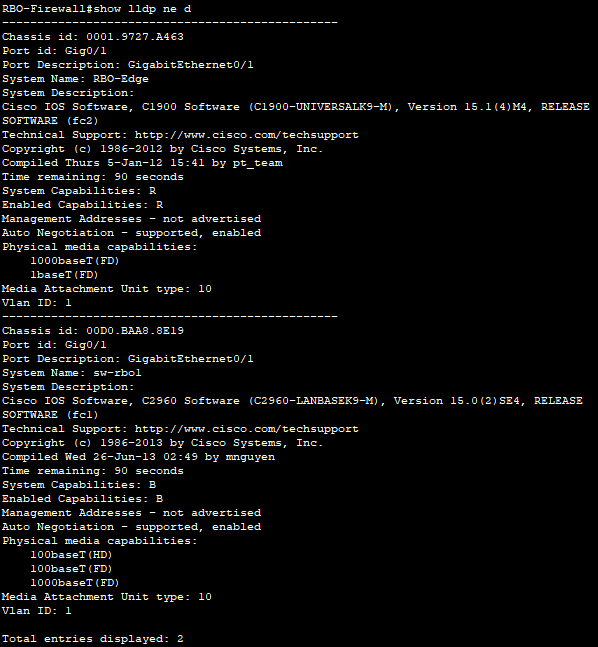
Примечание. Для подключения по протоколу SSH используйте те же имя пользователя и пароль, которые использовались при подключении к сети удаленного филиала Remote Branch Office.



Вопрос:

Какие сведения отображаются в командной строке после успешного подключения по протоколу SSH?

з.     Вы удаленно подключены к следующему соседу. Выполните команды show cdp neighbors и show cdp neighbors detail, чтобы найти другие подключенные соседние устройства.

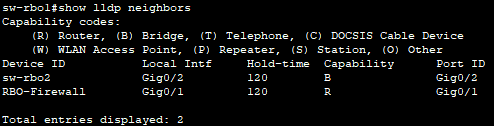


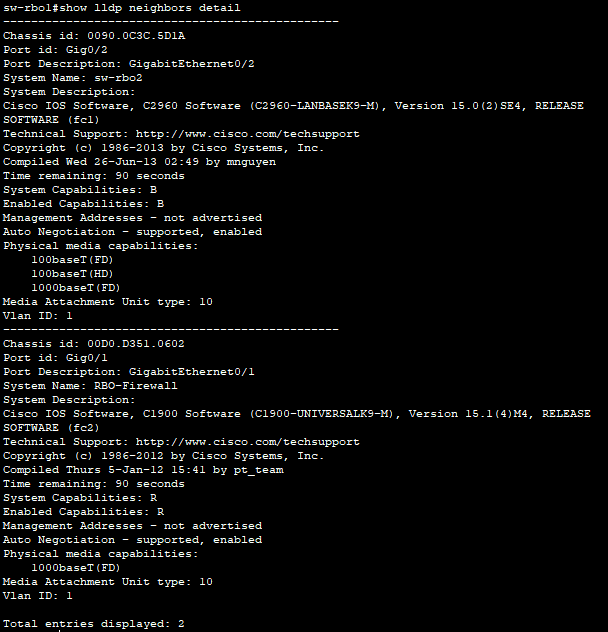
Вопрос:

К каким типам сетевых устройств относятся соседи этого устройства? Внесите сведения о новых обнаруженных устройствах в таблицу адресации. Укажите их имена хостов, интерфейсы и IP-адреса.

Добавьте новое имя устройства рядом с записью SVI для адреса 192.168.4.131.

и.     Подключитесь к SVI для адреса 192.168.4.131, используя SSH и учетные данные, использовавшиеся ранее. Если появится запрос на ввод секретного пароля, используйте тот же пароль, что и для RBOAdmin. Выполните команды show cdp neighbors и show cdp neighbors detail, чтобы найти другие подключенные соседние устройства.





Вопрос:

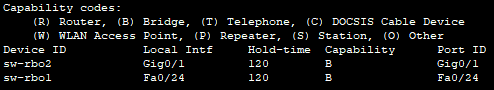
К каким типам сетевых устройств относятся соседи этого устройства? Внесите сведения о новых обнаруженных устройствах в таблицу адресации. Укажите их имена хостов, интерфейсы и IP-адреса.

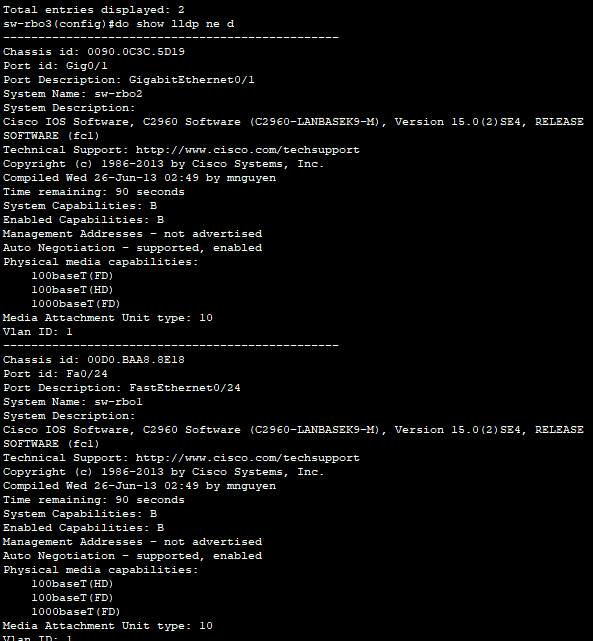
Поместите новое имя устройства рядом с записью SVI для адреса 192.168.4.132.

к.     Подключитесь к SVI для адреса 192.168.4.133, используя SSH и учетные данные, использовавшиеся ранее. Выполните команду show lldp, вы должны получить сообщение:

% LLDP is not enabled (LLDP не включен)

Включить lldp глобально, как в шаге C. Нет необходимости настраивать параметры передачи или получения, поскольку они по умолчанию активированы. Выполните команды show cdp neighbors и show cdp neighbors detail, чтобы найти другие подключенные соседние устройства.





Вопрос:

К каким типам сетевых устройств относятся соседи этого устройства? Внесите сведения о новых обнаруженных устройствах в таблицу адресации. Укажите их имена хостов, интерфейсы и IP-адреса. Возможно, будет полезно повторно подключиться к ранее обнаруженным устройствам, чтобы отобразить соседей еще раз, чтобы завершить всю таблицу адресации теперь, когда все устройства настроены для LLDP.

л.     Создайте топологию сети удаленного филиала Remote Branch Office, используя сведения, которые были получены с помощью протокола LLDP.

# 10.3.4 - Packet Tracer. Настройка и проверка протокола NTP

Топология

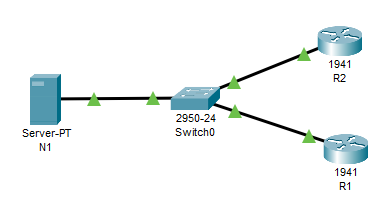


Таблица адресации

|  |  |  |  |
| --- | --- | --- | --- |
| Устройство | Интерфейс | IP-адрес | Маска подсети |
| N1 | NIC | 209.165.200.225 | 255.255.255.0 |
| R1 | G0/0 | 209.165.200.226 | 255.255.255.0 |
| R2 | G0/0 | 209.165.200.227 | 255.255.255.0 |

Цели

В этом упражнении вам предстоит настроить протокол NTP на узлах R1 и R2 для синхронизации времени.

Общие сведения и сценарий

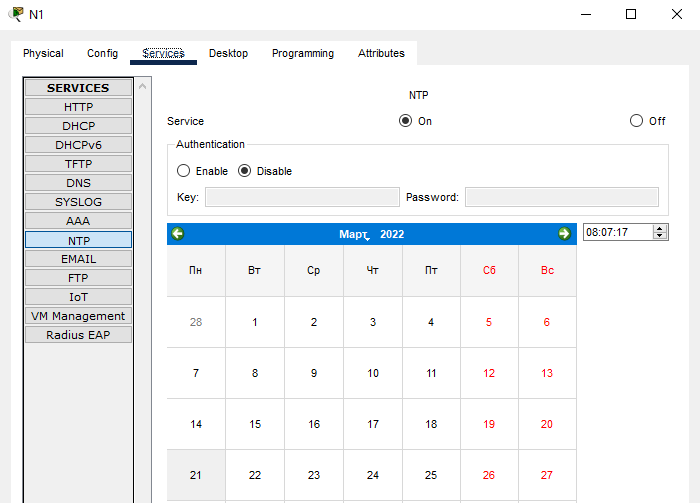
Протокол сетевого времени (NTP) служит для синхронизации времени между распределенными серверами времени и клиентами. Существует довольно много приложений, для которых требуется синхронизация времени, однако в этой лабораторной работе рассматриваются взаимосвязанные события, указанные в системном журнале, и другие связанные со временем события на нескольких сетевых устройствах. В качестве транспортного протокола NTP использует протокол UDP . Все операции обмена данными по протоколу NTP выполняются по времени в формате UTC.

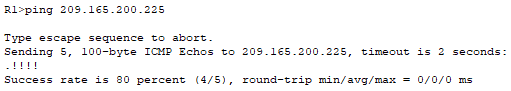
Сервер NTP обычно получает данные о времени из достоверного источника, такого как атомные часы, к которым подключен сервер. После этого сервер распределяет полученные данные о времени по сети. NTP чрезвычайно эффективен. Для синхронизации двух устройств с точностью до миллисекунды друг от друга требуется не более одного пакета в минуту.

Инструкция

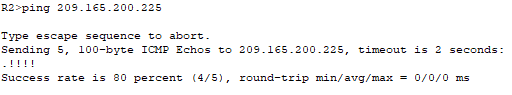
Шаг 1: Сервер NTP

a.     В этой топологии сервер N1 уже настроен в качестве NTP-сервера. Проверьте его конфигурацию в разделе Services (Службы) > NTP.

б.     С помощью утилиты ping проверьте связь маршрутизатора R1 с сервером N1 (209.165.200.225). Ping должен пройти успешно.



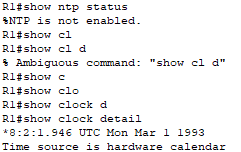
в.     С помощью утилиты ping повторите проверку связи сервера N1 с маршрутизатором R2.



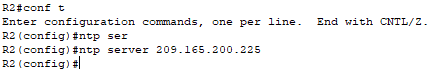
Шаг 2. Настройка клиентов NTP

Устройства Cisco можно настроить таким образом, чтобы они обращались к NTP-серверу для синхронизации своих часов. Это важно для согласования времени на всех устройствах. Настройте R1 и R2 в качестве NTP-клиентов для синхронизации их часов. Маршрутизаторы R1 и R2 будут использовать сервер N1 в качестве NTP-сервера.

a.     Проверьте текущие настройки NTP и часов, как показано ниже:



б.     Настройте R1 и R2 в качестве клиентов NTP. Выполните команду ntp server, чтобы указать NTP-сервер, как показано ниже:



в.     Повторите эту конфигурацию на R2.

Шаг 3: Проверка настроек NTP

a.     Снова проверьте время на R1 и R2, чтобы убедиться в том, что они синхронизированы:

R1# show clock detail

12:7:18.451 UTC Sat Oct 12 2019

Time source is NTP

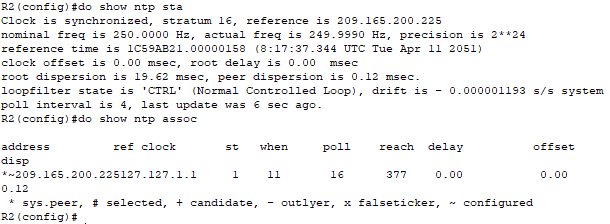
Примечание. При выполнении этой операции на физических маршрутизаторах следует подождать несколько минут, пока часы на R1 и R2 синхронизируются. С Packet Tracer вы может е использовать кнопку Fast Forward Time для ускорения синхронизации.

Выполните ту же команду на R2.

Вопрос:

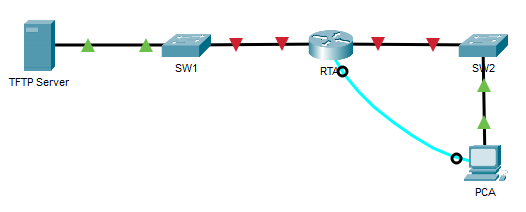
Синхронизированы ли часы на маршрутизаторах? - Да

б. Проверьте состояние NTP и NTP сопоставления с помощью следующих команд для проверки работы и конфигурации NTP.



# 10.6.10 - Packet Tracer - Резервное копирование файлов конфигурации

Топология



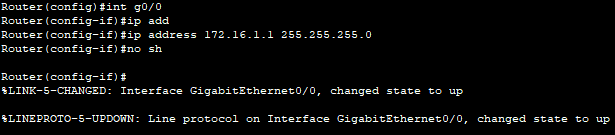
Инструкция

Часть 1. Установка соединения с TFTP-сервером

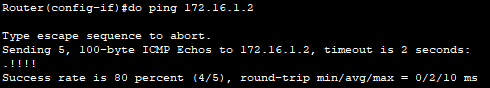
**Примечание.** Поскольку это новый маршрутизатор, первоначальная настройка будет выполняться через консольное подключение к маршрутизатору.

a.     Нажмите **PCA**, откройте вкладку **Desktop** (Рабочий стол), выберите **Terminal** (Терминал), чтобы открыть окно командной строки **RTA**.

б.     Настройте и включите **Gigabit Ethernet 0/0**. IP-адрес должен совпадать с адресом шлюза по умолчанию для **TFTP-сервера**.



в.     Проверьте связь с **TFTP-сервером**. При необходимости устраните неполадки.



Часть 2: Перенос файла конфигурации с TFTP-сервера

a.     В привилегированном режиме EXEC введите следующую команду:

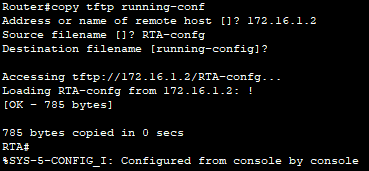
Router# **copy tftp running-config**

Address or name of remote host []? **172.16.1.2**

Source filename []? **RTA-confg**

Destination filename [running-config]?

Маршрутизатор должен возвратить следующие данные:

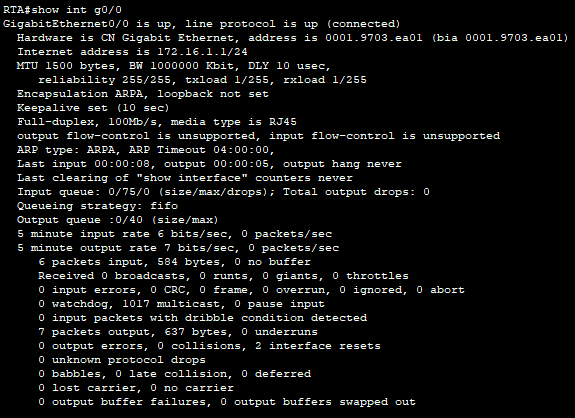


б.     Выполните команду, чтобы отобразить текущую конфигурацию.

**Вопрос:**

в.     Выполните соответствующую команду **show**, чтобы отобразить состояние интерфейса.

**Вопрос:**



г.     Устраните все проблемы, связанные с интерфейсами, и проверьте связь между PCA и сервером TFTP.

Часть 3. Резервное копирование конфигурации и образа IOS на TFTP-сервер

a.     Измените имя узла **RTA** на **RTA-1**.

б.     Сохраните конфигурацию в NVRAM.

в.     Скопируйте конфигурацию на **TFTP-сервер** с помощью команды **copy** :

RTA-1# **copy running-config tftp:**

Address or name of remote host []? **172.16.1.2**

Destination filename [RTA-1-confg]?

г.     Выполните эту команду, чтобы отобразить файлы из флеш-памяти.

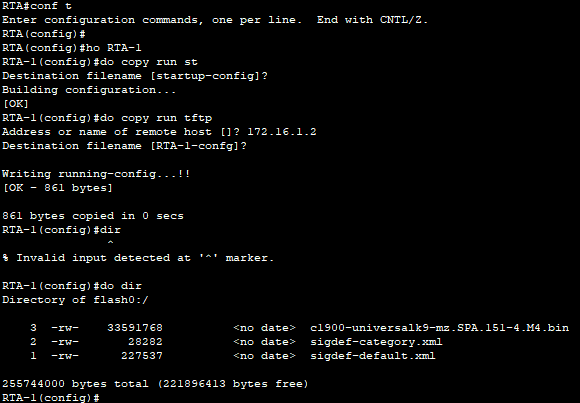
д.     Скопируйте образ IOS на **TFTP-сервер** с помощью следующей команды:

RTA-1# **copy flash tftp:**

Source filename []? **c1900-universalk9-mz.SPA.151-4.M4.bin**

Address or name of remote host []? **172.16.1.2**

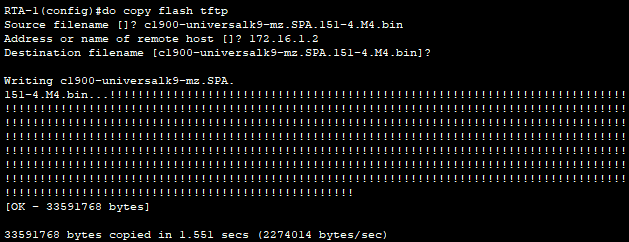
Destination filename [c1900-universalk9-mz.SPA.151-4.M4.bin]?



**Вопрос:**

Какой специальный символ неоднократно показывает, что файл IOS успешно копируется на TFTP-сервер?

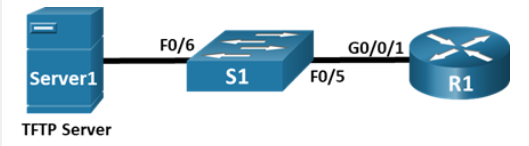
е. Откройте TFTP-сервер и перейдите на вкладку Службы, выберите TFTP и прокрутите список файлов IOS.



**Вопрос:**

# 10.6.12 – Packet Tracer - Use TFTP and flash to manage configuration files

Топология



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.

Current configuration : 813 bytes

!

version 15.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

service password-encryption

!

hostname R1

!

enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1

!

no ip cef

no ipv6 cef

!

no ip domain-lookup

!

spanning-tree mode pvst

!

interface GigabitEthernet0/0/0

no ip address

duplex auto

speed auto

shutdown

!

interface GigabitEthernet0/0/1

ip address 192.168.1.1 255.255.255.0

duplex auto

speed auto

!

interface Vlan1

no ip address

shutdown

!

ip classless

!

ip flow-export version 9

!

banner motd ^C YOU ARE NOW IN RESTRICTED AREA ^C

!

line con 0

password 7 0822455D0A16

login

!

line aux 0

!

line vty 0 4

password 7 0822455D0A16

login local

line vty 5 15

password 7 0822455D0A16

login local

!

end.

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

*S1(config)#do show run*

Building configuration...

Current configuration : 1571 bytes

!

version 12.2

no service timestamps log datetime msec

no service timestamps debug datetime msec

service password-encryption

!

hostname S1

!

enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1

!

no ip domain-lookup

!

spanning-tree mode pvst

spanning-tree extend system-id

!

interface Vlan1

ip address 192.168.1.11 255.255.255.0

!

ip default-gateway 192.168.1.1

!

banner motd ^C YOU ARE NOW IN RESTRICTED AREA ^^C

!

line con 0

password 7 0822455D0A16

login

!

line vty 0 4

password 7 0822455D0A16

login local

line vty 5 15

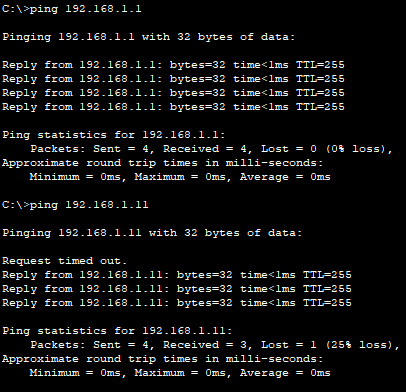
password 7 0822455D0A16

login local

!

endастройки.

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



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 Server1включите 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.

*Откройте окно конфигурации*

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

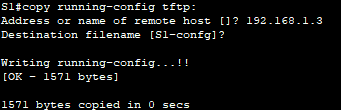
startup-config Copy to startup configuration

tftp: Copy to tftp: file system

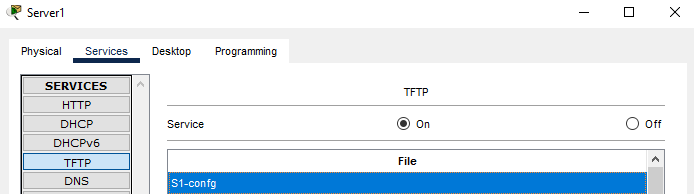
S1# **copy flash:**

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.



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-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.

c.     Введите команду show running-config, чтобы просмотреть файл текущей конфигурации.

*Закройте окно настройки.*

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*те окно конфигурации*

a.     Откройте программу Terminal на PC1 до R1.

b.     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.

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 Server1. Перед восстановлением подключения может потребоваться выполнить эхо-запрос несколько раз.

e.     Введите команду copy, чтобы передать файл конфигурации R1-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#, и процент завершения должен отражать, что вся ваша конфигурация восстановлена.

*Закройте окно настройки.*

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:.*ойте окно конфигурации*

R1# **show file systems**

File Systems:

Size(b) Free(b) Type Flags Prefixes

\* 3249049600 2761893177 flash rw flash:

29688 23590 нврам rw nvram:**опрос:**

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.**

a.     Скопируйте файл текущей конфигурации во флеш-память.

R1# **copy running-config flash:**

Destination filename [running-config]? **R1-running-config-backup**

Building configuration...

[OK]

R1#

b.     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)

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# **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.

a.     Удалите файл загрузочной конфигурации на маршрутизаторе.

b.     Перезагрузите маршрутизатор.

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

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.

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#

b.     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#

# 10.6.13 - Packet Tracer - Исследование и выполнение процедур восстановления пароля - Режим симуляции физического оборудования

Часть 1. 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.

**Вопросы:**

Для чего необходим регистр конфигурации? – Для выбора поведения устройства при загрузке

С помощью какой команды можно изменить регистр конфигурации в глобальном режиме конфигурации? – С помощью команды config-register

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

Шаг 2. Определите значения регистра конфигурации и их функции.

**Вопросы:**

Изучите и опишите поведение маршрутизатора со следующими значениями регистра конфигурации:

**0x2102**

**0x2142**

Чем отличаются эти значения регистра конфигурации? 2142 игнорирует конфигурационные файлы, сохраненные в nvram, при загрузке.

Часть 2. Описание процедуры восстановления пароля для отдельного маршрутизатора Cisco

Во второй 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.

1. Пе

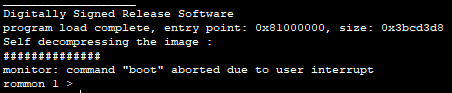
Шаг 2. С помощью Packet Tracer выполните восстановление enable password и secret password на маршрутизаторе Cisco 2911.

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.



d.     Измените значение регистра конфигурации и перезагрузитесь.

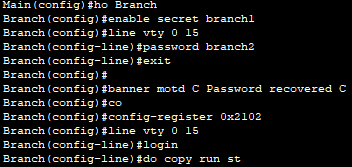
rommon 1 > **confreg 0x2142**

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:



Show version 

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.

**Вопросы:**

Как определить текущий параметр регистра конфигурации? show version

Опишите процесс перехода в режим ROMMON.

Какие команды необходимы для входа в интерфейс ROMMON?

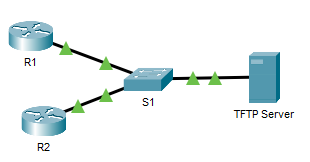
Какое сообщение должно появиться во время загрузки маршрутизатора? - Сontinue with configuration dialog?

Зачем загрузочную конфигурацию необходимо загрузить в текущую?

Почему важно вернуть исходное значение регистра конфигурации после восстановления пароля?

# 10.7.6 - Packet Tracer - Использование TFTP-сервера для обновления образа Cisco IOS

Топология



Инструкция

Часть 1: Обновление образа IOS на устройстве Cisco

Шаг 1: Обновление образа IOS на маршрутизаторе.

a. Получите доступ к TFTP-серверу и включите службу TFTP.

б. Запишите образы IOS, доступные на TFTP-сервере.



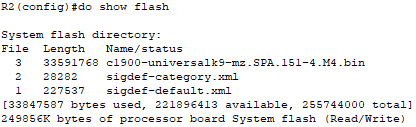
Вопрос:

Какие образы IOS, хранящиеся на сервере, совместимы с 1941?

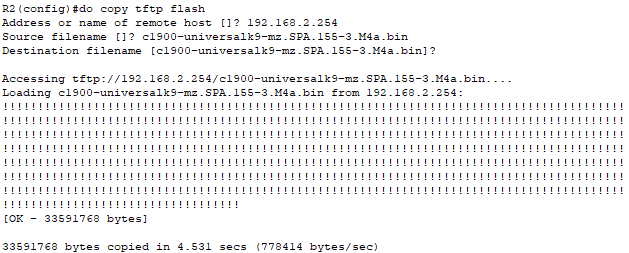


Откройте окно конфигурации

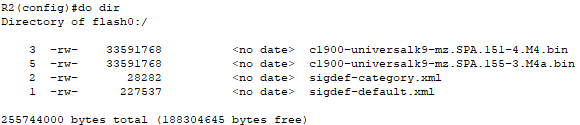
в. На маршрутизаторе R2 введите команду show flash: и запишите доступный объём флеш-памяти.



г. Скопируйте образ CISCO1941/K9 IOS версии 15.5 для маршрутизатора 1941 с сервера TFTP на R2.



д. Убедитесь в том, что образ IOS скопирован во флеш-память.



Вопрос:

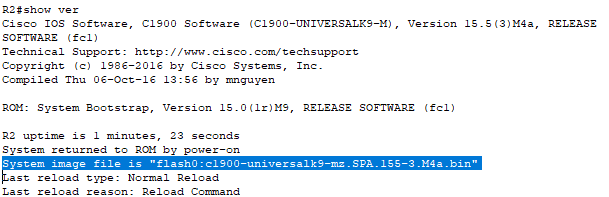
Сколько образов IOS находится во флеш-памяти? - Два

е. Используйте команду boot system, чтобы загрузить образ IPBase 15.5 при следующей перезагрузке.



ж. Сохраните конфигурацию и перезагрузите маршрутизатор R2.

з. Используйте команду show version для проверки загрузки обновленного образа IOS после перезагрузки R2.

Шаг 2: Обновите образ IOS на коммутаторе.

Откройте окно конфигурации

a. Получите доступ к TFTP-серверу и скопируйте образ c2960-lanbasek9-mz.150-2.SE4.bin на коммутатор S1.

б. Используйте команду boot system для настройки коммутатора для загрузки нового образа IOS при загрузке.

в. Перезагрузите коммутатор S1 и убедитесь, что новый образ был загружен в память.



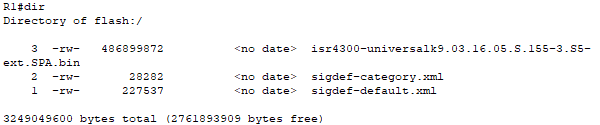
г. Закройте окно конфигурации TFTP, если оно все еще открыто.

Закройте окно настройки.

Часть 2. Создание резервной копии образа IOS на TFTP-сервере

Откройте окно конфигурации

a. На R1 просмотрите содержимое флеш-памяти и запишите образ IOS.



б. Используйте команду copy, чтобы выполнить резервное копирование образа IOS из флеш-памяти маршрутизатора R1 на TFTP-сервер.

в. Получите доступ к TFTP-серверу и убедитесь, что образ IOS скопирован на TFTP-сервер.

