Packet Tracer - Настройка базовых параметров маршрутизатора - Режим симуляции физического оборудования

Топология

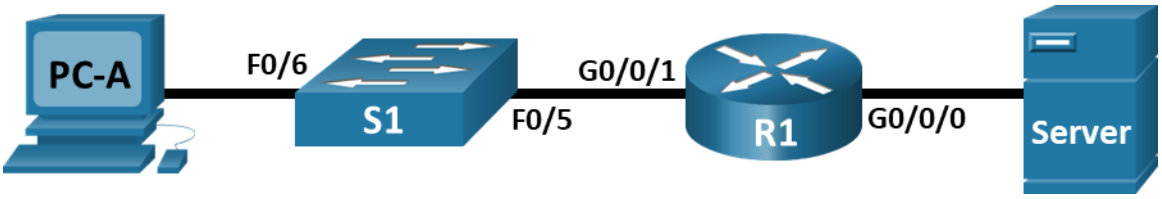

Таблица адресации

Устройство	Интерфейс	IP адрес/префикс	Шлюз по умолчанию
R1	G0/0/0	192.168.0.1 /24	—
		2001:db8:acad::1 /64	
		fe80::1	
	G0/0/1	192.168.1.1 /24	
		2001:db8:acad:1::1 /64	
		fe80::1	
	Loopback0	10.0.0.1 /24	
		2001:db8:acad:2::1/64	
		fe80::1	
PC-A	NIC	192.168.1.10 /24	192.168.1.1
		2001:db8:acad:1::10 /64	fe80::1
Server	NIC	192.168.0.10 /24	192.168.0.1
		2001:db8:acad::10 /64	fe80::1

Задачи

Часть 1. Настройка топологии и инициализация устройств

Часть 2. Настройка устройств и проверка подключения

Часть 3. Отображение сведений о маршрутизаторе

Общие сведения и сценарий

Это комплексная лабораторная работав режиме симуляции физического оборудования (PTPM), нацеленная на повторение ранее изученных команд IOS для маршрутизатора. В первой и второй частях вам предстоит подключить кабели к оборудованию и выполнить базовую настройку конфигураций и параметров IPv4-интерфейса на маршрутизаторе.

В третьей части вам нужно будет настроить удаленное подключение к маршрутизатору с помощью протокола SSH, а также использовать команды IOS для получения от устройства данных, необходимых для того, чтобы ответить на вопросы о маршрутизаторе.

В целях повторения в этой лабораторной работе представлены команды, необходимые для определенных конфигураций маршрутизатора.

Инструкции

Часть 1. Настройка топологии и инициализация устройств

Шаг 1. Подключите кабели сети согласно приведенной топологии.

a. Нажмите на **Cisco 4321 ISR**, **Cisco 2960 Switch** и **Server**, которые находятся на полке **Shelf** и перетащите а стойку **Rack**.

b. Нажмите на **PC** на полке **Shelf** и перетащите на стол **Table**.

c. Кабель устройств, как указано в схеме топологии. Используйте **медные прямые** кабели для сетевых подключений.

d. Подключите **консольный кабель** от **PC** до **Cisco 4321 ISR**.

e. Включите **Cisco 4321 ISR**, **PC-A** и **Server**. Кнопка питания для **Server** находится в правом нижнем углу. Коммутатор 2960 должен включаться автоматически.

Часть 2. Настройка устройств и проверка подключения

Шаг 1. Настройте интерфейсы ПК.

a. Настройте на компьютере **PC-A** IP-адрес, маску подсети и параметры основного шлюза.

b. Настройте на сервере **Server** IP-адрес, маску подсети и параметры основного шлюза.

Шаг 2. Настройте маршрутизатор.

a. Подключитесь к маршрутизатору с помощью консоли и активируйте привилегированный режим EXEC.

b. Войдите в режим конфигурации.

c. Назначьте маршрутизатору имя устройства.

d. Укажите имя домена **ccna-lab.com**.

e. Зашифруйте открытые пароли.

f. Настройте в системеограничение на минимальный 12-значный пароль.

g. Настройте имя пользователя **SSHadmin** с зашифрованным паролем **55HAdm!n2020**

h. Создайте набор криптоключей с 1024 битным модулем.

i. Назначьте **$cisco!PRIV*** в качестве пароля доступа к привилегированному режиму EXEC.

j. Назначьте **$cisco!!CON*** в качестве пароля консоли. Настройте сеансы на отключение после четырех минут бездействия и включите вход в систему.

k. Установите **$cisco!!VTY*** в качестве пароля vty. Далее нужно настроить линии VTY, чтобы принимались только SSH-подключения. Настройте сеансы для отключения после четырех минут бездействия и включите вход с помощью локальной базы данных.

l. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.

m. Включите маршрутизацию IPv6.

n. Настройте все три интерфейса маршрутизатора с информацией адресации IPv4 и IPv6 из таблицы адресации выше. Настройте все три интерфейса с описаниями. Включите все три интерефейса.

Маршрутизатор не должен разрешать вход в систему VTY в течение двух минут, если в течение 60 секунд произошло три неудачных попытки входа.

o. Настройте на маршрутизаторе время.

p. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Что произойдет, если перезагрузить маршрутизатор до того, как будет выполнена команда **copy running-config startup-config**?

Содержимое запущенной конфигурации в оперативной памяти будет удалено во время перезагрузки

Шаг 3. Проверьте подключение к сети.

a. Используя командную строку на **PC-A**, проверьте связь эхо-запросами до IPv4- и IPv6-адресов сервера **Server**.

Успешно ли выполнена проверка связи?

Да

b. С **PC-A** получите удаленный доступ к маршрутизатору **R1** с помощью клиента Telnet/SSH.

Используя клиент Telnet/SSH на PC-A, откройте сеанс SSH на IPv4-адрес интерфейса замыкания на себя R1. Убедитесь, что для параметра Тип подключения (Connection Type) установлен в значение **SSH** , и используйте **sShadmin** в качестве имени пользователя. При появлении запроса введите пароль **55Hadm!n2020**.

Удаленный доступ был настроен успешно?

Да

c. Используя клиент Telnet/SSH на **PC-A**, откройте сеанс SSH на IPv6-адрес интерфейса Loopback R1. Убедитесь, что для параметра Тип подключения (Connection Type) установлен в значение **SSH**, и используйте **SSHadmin** в качестве имени пользователя. При появлении запроса введите пароль **55Hadm!n2020**.

Удаленный доступ был настроен успешно?

Да

Почему использование протокола Telnet считается угрозой безопасности?

Он не зашифрован -> пароли можно легко просмотреть с помощью анализатора пакетов.

Часть 3. Отображение сведений о маршрутизаторе

В третьей части вам предстоит использовать команду **show** в сеансе SSH, чтобы получить информацию из маршрутизатора.

Шаг 1. Установите SSH-подключение к R1.

Используя клиент Telnet/SSH на **PC-A**, откройте сеанс SSH на IPv6-адрес интерфейса Loopback **R1** и войдите в систему как **sShadmin** с паролем **55Hadm! n2020**.

Шаг 2. Получите основные данные об аппаратном и программном обеспечении.

a. Используйте команду **show version**, чтобы ответить на вопросы о маршрутизаторе.

Как называется образ IOS, под управлением которой работает маршрутизатор?

isr4300-universalk9.03.16.05.S.155-3.S5-ext.SPA.bin.

PTLCКакой объем энергонезависимого ОЗУ (NVRAM) имеет маршрутизатор?

32768K bytes

PTLCКаким объемом флеш-памяти обладает маршрутизатор?

3223551K bytes

b. **PTLC**Зачастую команды **show** могут выводить несколько экранов данных. Фильтрация выходных данных позволяет пользователю отображать лишь нужные разделы выходных данных. Чтобы включить команду фильтрации, после команды **show** введите прямую черту (**|**), после которой следует ввести параметр и выражение фильтрации. Чтобы отобразить все строки выходных данных, которые содержат выражение фильтрации, можно согласовать выходные данные с оператором фильтрации с помощью ключевого слова **include**. Настройте фильтрацию для команды **show version** и используйте команду **show version | include register**, чтобы ответить на следующий вопрос.

Каков был бы процесс загрузки маршрутизатора при следующей перезагрузке, если регистр конфигурации был 0x2142?

маршрутизатор обойдет конфигурацию запуска и запустится в командной строке пользовательского режима. Если первоначальная загрузка завершается неудачей, маршрутизатор переходит в режим ROMMON.

Шаг 3. Отобразите загрузочную конфигурацию.

a. Выполните команду **show startup-config** на маршрутизаторе, чтобы ответить на следующие вопросы.

Как пароли представлены в выходных данных?

Пароли шифруются с помощью команды service password-encryption.

b. Введите команду **show running-config | section vty** .

Что происходит в результате выполнения этой команды?

покажет только те строки конфигурации, которые относятся к настройкам VTY линий

Шаг 4. Отобразите таблицу маршрутизации на маршрутизаторе.

Выполните команду **show ip route** на маршрутизаторе, чтобы ответить на следующие вопросы.

Какой код используется в таблице маршрутизации для обозначения сети с прямым подключением?

Сколько записей маршрутов закодированы с символом «C» в таблице маршрутизации? 3

Шаг 5. Отобразите на маршрутизаторе сводный список интерфейсов.

a. Выполните команду **show ip interface brief** на маршрутизаторе, чтобы ответить на следующий вопрос.

Какая команда позволяет изменить состояние портов Gigabit Ethernet с DOWN на UP?

no shutdown

b. Чтобы проверить параметры IPv6 на маршрутизаторе **R1** выполните команду **show ipv6 int brief**.

В чем смысл части **[up/up]** вывода?

c. На сервере**Server** измените его конфигурацию таким образом, чтобы он больше не имел статического IPv6-адреса. Затем введите команду **ipconfig** на **Server**, чтобы проверить конфигурацию IPv6.

Какой IPv6-адрес назначен на **Server**?

2001:db8:acad:a:d428:7de2:997c:b05a

Каким будет шлюз по умолчанию для этого сервера **Server**?

fe80::1

От компьютера **PC-B** отправьте эхо-запрос на локальный адрес канала шлюза по умолчанию маршрутизатора **R1**. Была ли проверка успешной?

Да

От сервера **Server** отправьте эхо-запрос на индивидуальный IPv6-адрес маршрутизатора **R1** 2001:db8:acad:a::1. Была ли проверка успешной?

Да

Вопросы для повторения

1. Во время диагностики проблемы подключения сети технический специалист решает, что интерфейс не был включен. Какую команду **show** следует использовать специалисту для выявления и устранения этой неполадки?

show ip interface brief

2. Во время диагностики проблемы подключения сети технический специалист решает, что интерфейсу была назначена неверная маска подсети. Какую команду **show** следует использовать специалисту для выявления и устранения этой неполадки?

show startup-config

