**Лабораторная работа № 8.**

**Выполнил студент: Выонг Чыонг Шон**

**Группа: ИКБО-05-19**

Топология

****

Таблица Адресации

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Устройство | Интерфейс | IP-адрес | Маска подсети | Шлюз по умолчанию |
| R1\_VUONG | G0/1 | 192.168.1.38 | 255.255.255.0 | - |
| S1 | VLAN1 | 192.168.1.48 | 255.255.255.0 | 192.168.1.38 |
| PC-A | NIC | 192.168.1.58 | 255.255.255.0 | 192.168.1.38 |

**Задачи:**

**Часть 1: Настройка основных параметров устройства**

**Шаг 1:** **Создайте сеть согласно топологии.**

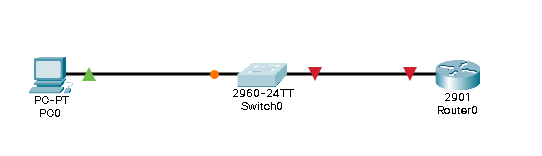
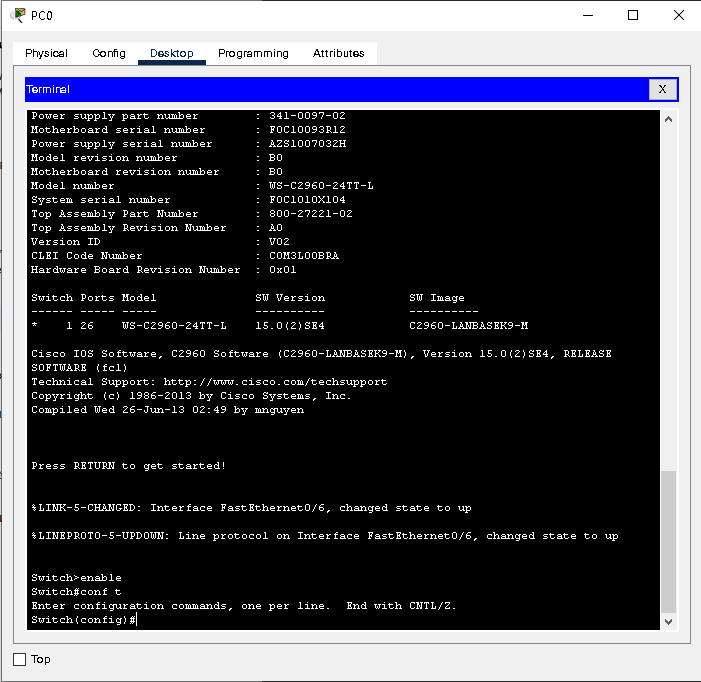
****

Рис.1: топологии

**Шаг 2:** **Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.**

1. Подключитесь к коммутатору с помощью консоли и перейдите в режим глобальной настройки.



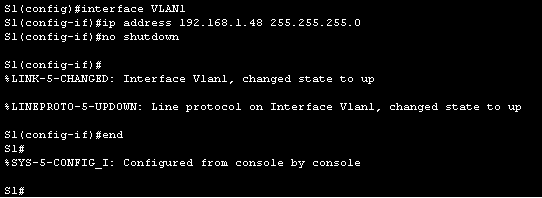
1. Назначьте коммутатору имя узла в соответствии с таблицей адресации.



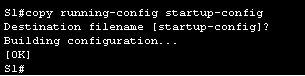
1. Отключите поиск DNS.



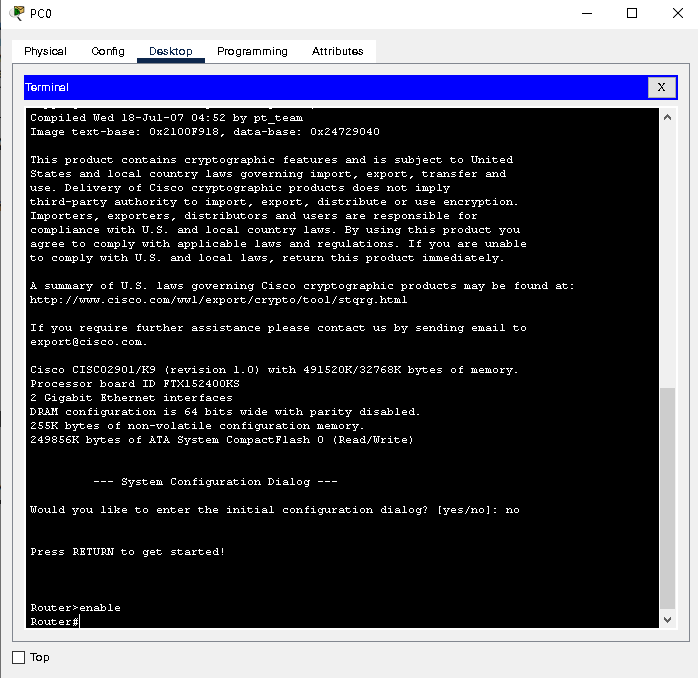
1. Настройте и включите интерфейс SVI для сети VLAN 1.



1. Сохраните файл текущей конфигурации в файл загрузочной конфигурации



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



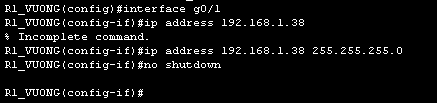
1. Войдите в режим конфигурации.



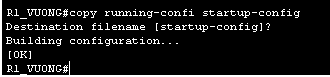
1. Назначьте маршрутизатору имя устройства



1. Укажите и активируйте IP-адреса и маски подсети для интерфейсов G0/1.



1. Сохраните файл текущей конфигурации в файл загрузочной конфигурации



**Шаг 3:** **Настройте маршрутизатор**

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



1. Войдите в режим глобальной конфигурации.



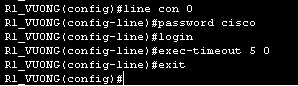
1. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.



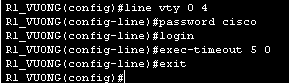
1. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC



1. Назначьте **cisco** в качестве пароля консоли и включите режим входа в систему по паролю. Обеспечьте закрытие сеанса линии связи через 5 минут отсутствия активности.



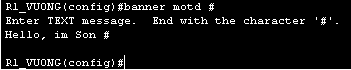
1. Назначьте **cisco** в качестве пароля VTY и включите вход по паролю. Обеспечьте закрытие сеанса линии связи через 5 минут отсутствия активности.



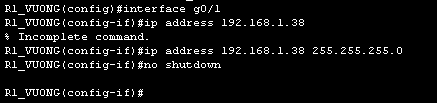
1. Зашифруйте открытые пароли.



1. Создайте баннер, который предупреждает о запрете несанкционированного доступа



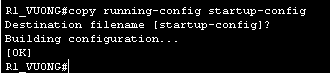
1. Настройте и активируйте на маршрутизаторе интерфейс G0/1, используя информацию, приведенную в таблице адресации.



1. Сделайте так, чтобы маршрутизатор блокировал попытки входа в систему на 30 секунд, если в течение 120 секунд будет дважды введен неверный пароль.



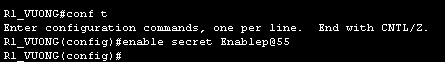
1. Сохраните текущую конфигурацию в файл загрузочной конфигурации.



**Шаг 4:** **Установите более надежные пароли.**

**Примечание**. Согласно данным рекомендациям по лучшим практическим методикам надежные пароли, примеры которых приведены в этой лабораторной работе, необходимо всегда использовать в реальной работе. Однако для упрощения выполнения работы в остальных лабораторных работах данного курса используются пароли cisco и class.

1. Измените зашифрованный пароль привилегированного режима EXEC в соответствии с рекомендациями. Установите следующий пароль: **Enablep@55**

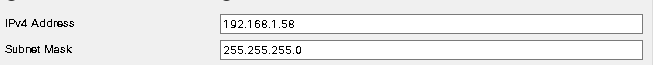


1. Установите минимальную длину 10 символов для всех паролей.



**Шаг 5:** **Настройте компьютер PC-A**

1. Настройте для PC-A IP-адрес и маску подсети.

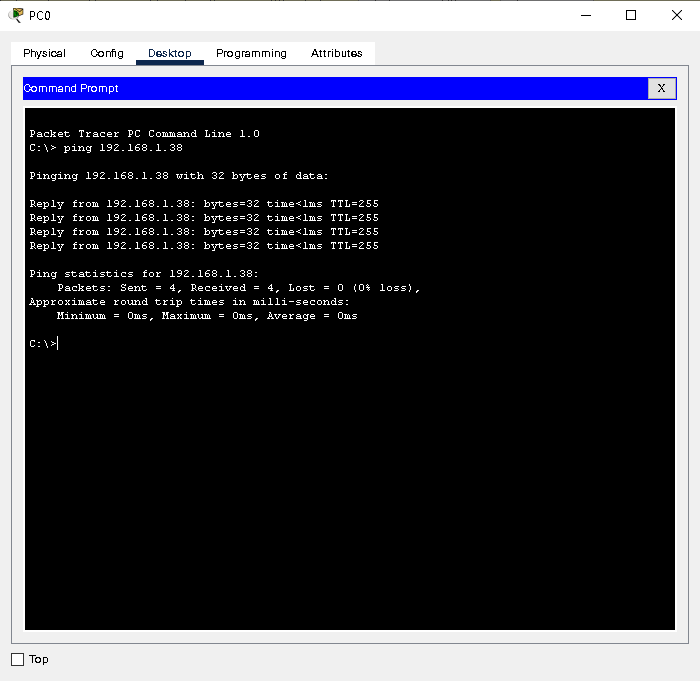


1. Настройте для PC-A шлюз по умолчанию.



**Шаг 6:** **Проверьте подключение к сети.**

Пошлите с PC-A эхо-запрос на маршрутизатор R1\_ФАМИЛИЯ. Убедитесь, что эхо-запрос выполнен успешно.



**Часть 2:** **Настройка маршрутизатора для доступа по протоколу SSH и обеспечение базовых мер безопасности**

**Шаг 1:** **Настройте аутентификацию устройств**

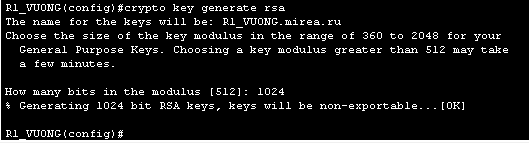
При генерации ключа шифрования в качестве его части используются имя устройства и домен. Поэтому эти имена необходимо указать перед вводом команды **crypto key**.

1. Задайте домен для устройства.



**Шаг 2:** **Создайте ключ шифрования с указанием его длины.**

1. Установите ключ шифрования с длиной 1024 бит.



**Шаг 3:** **Создайте имя пользователя в локальной базе учетных записей.**

1. Создайте имя пользователя и пароль для него с максимальными привилегиями. Используйте имя пользователя **SSHadmin** и пароль **Admin1p@55**.

**Примечание**. Уровень привилегий 15 дает пользователю права администратора



**Шаг 4:** **Активируйте протокол SSH на линиях VTY**

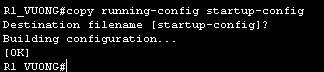
1. Активируйте протокол SSH на входящих линиях VTY.



1. Измените способ входа в систему таким образом, чтобы использовалась проверка пользователей по локальной базе учетных записей.



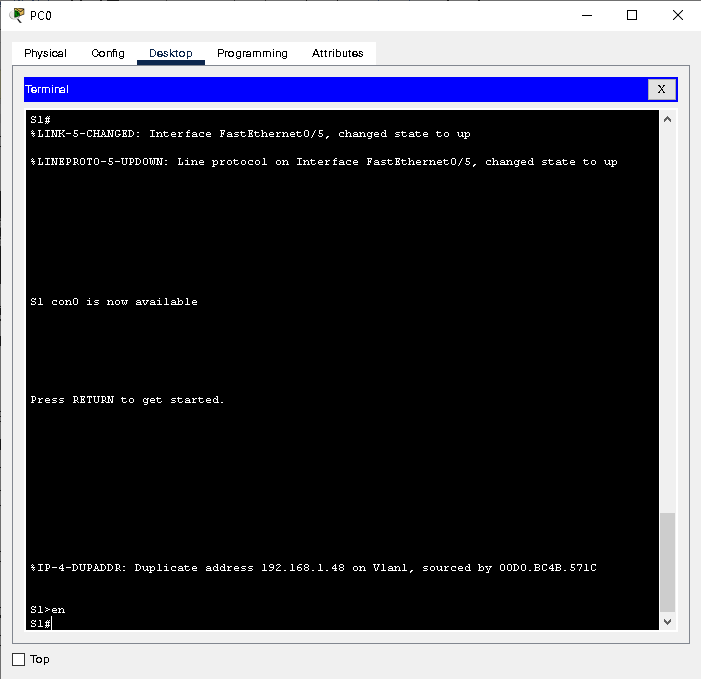
**Шаг 5:** **Сохраните текущую конфигурацию в файл загрузочной конфигурации.**

****

**Часть 3:** **Настройка коммутатора для доступа по протоколу SSH и обеспечение базовых мер безопасности**

**Шаг 1:** **Настройте основные параметры коммутатора.**

1. Подключитесь к коммутатору с помощью консольного подключения и активируйте привилегированный режим EXEC.



1. Войдите в режим конфигурации.



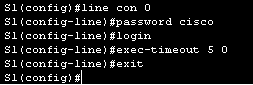
1. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов



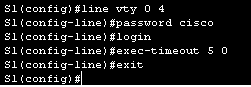
1. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.



1. Назначьте **cisco** в качестве пароля консоли и включите режим входа в систему по паролю. Обеспечьте закрытие сеанса линии связи через 5 минут отсутствия активности.



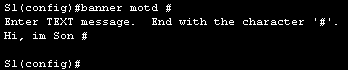
1. Назначьте **cisco** в качестве пароля VTY и включите вход по паролю. Обеспечьте закрытие сеанса линии связи через 5 минут отсутствия активности.



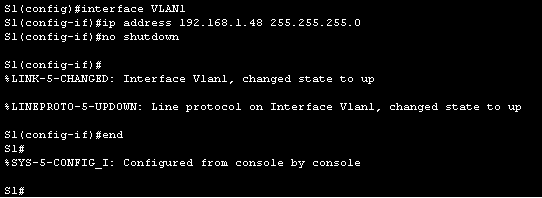
1. Зашифруйте открытые пароли.



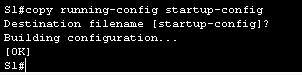
1. Создайте баннер, который предупреждает о запрете несанкционированного доступа.



1. Настройте и активируйте на коммутаторе интерфейс VLAN 1, используя информацию, приведенную в таблице адресации.



1. Сохраните текущую конфигурацию в файл загрузочной конфигурации



**Шаг 2: Настройте коммутатор для соединения по протоколу SSH**

Для настройки протокола SSH на коммутаторе используйте те же команды, которые применялись для аналогичной настройки маршрутизатора в части 2.

1. Задайте домен для устройства



1. Создайте ключ шифрования с указанием его длины.



1. Создайте имя пользователя в локальной базе учетных записей.



1. Активируйте протоколы Telnet и SSH на линиях VTY



1. Измените способ входа в систему таким образом, чтобы использовалась проверка пользователей по локальной базе учетных записей.



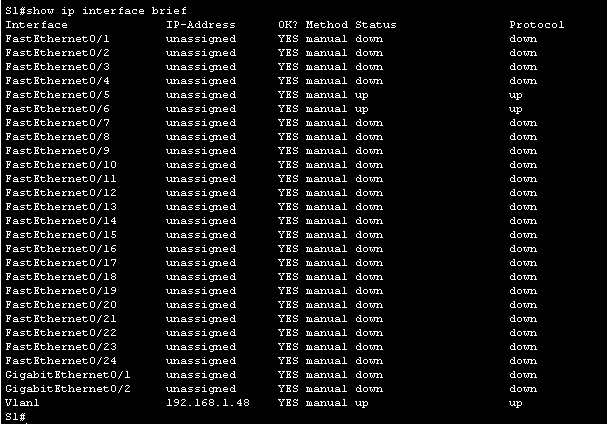
**Шаг 3:** **Установите более надежные пароли.**

1. Измените зашифрованный пароль привилегированного режима EXEC в соответствии с рекомендациями. Установите следующий пароль: **Enablep@55**

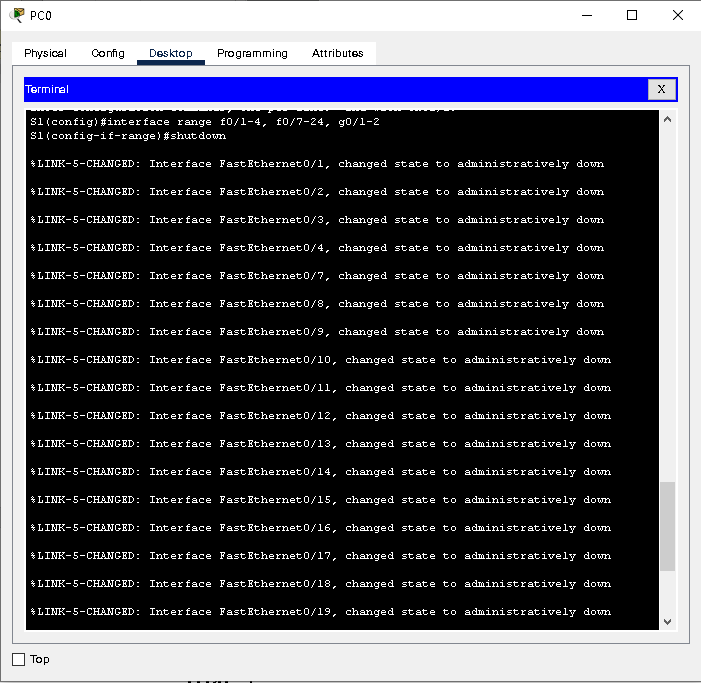


**Шаг 4:** **Убедитесь, что все неиспользуемые порты отключены.**

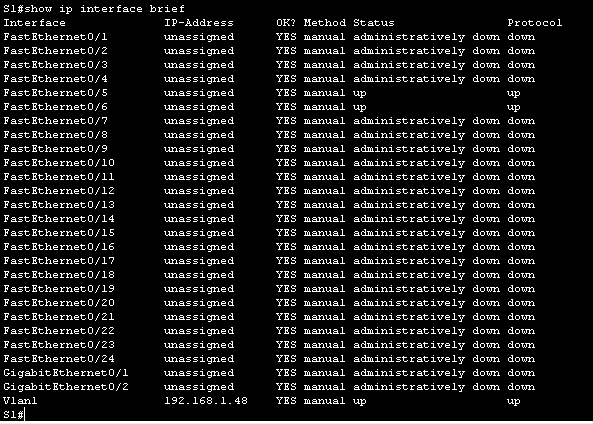
1. Состояние портов коммутатора



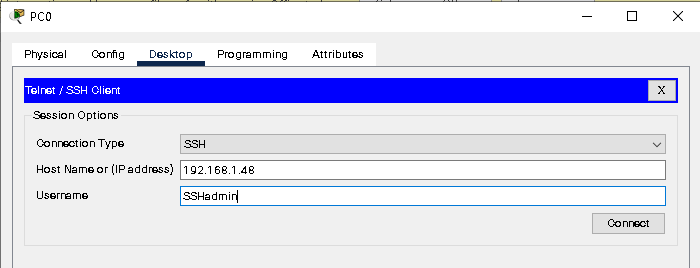
1. Чтобы отключить сразу несколько интерфейсов, воспользуйтесь командой **interface range**

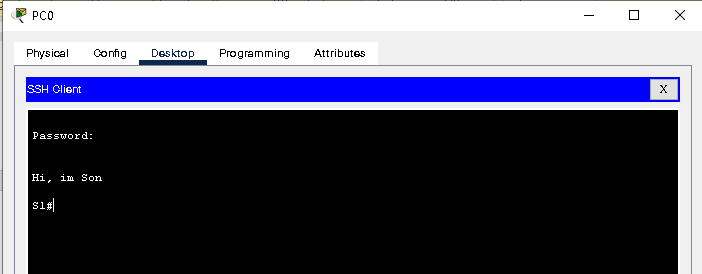


1. Проверьте состояние портов коммутатора.



**Шаг 5:** **Установите соединение с коммутатором по протоколу SSH**

****

****

**Часть 4:** **Настройка протокола SSH с использованием интерфейса командной строки (CLI) коммутатора**

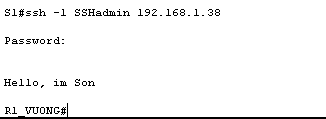
**Шаг 1:** **Посмотрите доступные параметры для клиента SSH в Cisco IOS.**

Используйте вопросительный знак (?), чтобы отобразить варианты параметров для команды **ssh**.



**Шаг 2:** **Установите с коммутатора S1 соединение с маршрутизатором R1 по протоколу SSH.**

1. Чтобы подключиться к маршрутизатору R1\_VUONG по протоколу SSH, введите команду **ssh –l SSHadmin 192.168.1. 38**. Это позволит вам войти в систему под именем **SSHadmin**. При появлении приглашения введите в качестве пароля **Admin1p@55**.



1. Чтобы вернуться к коммутатору S1, не закрывая сеанс SSH с маршрутизатором R1\_ФАМИЛИЯ, нажмите комбинацию клавиш Ctrl+Shift+6. Отпустите клавиши Ctrl+Shift+6 и нажмите x. Отображается приглашение привилегированного режима EXEC коммутатора.



1. Чтобы вернуться к сеансу SSH на R1, нажмите клавишу Enter в пустой строке интерфейса командной строки. Чтобы увидеть окно командной строки маршрутизатора, нажмите клавишу Enter еще раз.



1. Чтобы завершить сеанс SSH на маршрутизаторе R1, введите в командной строке маршрутизатора команду exit.



**Защита лабораторной работы (Ответы на вопросы):**

1. Как предоставить доступ к сетевому устройству нескольким пользователям, у каждого из которых есть собственное имя пользователя?

* Нужно настроить доступ по SSH и создать несколько пользователей при помощи команды username.