|  |
| --- |
| МИНОБРНАУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное учреждение высшего образования **«МИРЭА − Российский технологический университет»**  **РТУ МИРЭА** |

**Институт информационных технологий (ИИТ)**

**Кафедра практической и прикладной информатики (ППИ)**

**ОТЧЕТ ПО ПРАКТИЧЕСКОЙ РАБОТЕ**

по дисциплине «Основы сетевых технологий»

**Практическое занятие №8. Доступ к сетевым устройствам по протоколу SSH и обеспечение безопасности сетевых устройств.**

|  |  |  |  |
| --- | --- | --- | --- |
| Студент группы ИНБО-01-17 | *ИКБО-07-21, Хасанбаев И.А.* | (подпись) | |
| Преподаватель | *Пыхтин В.А.* | (подпись) | |
| Отчет представлен | «\_\_»\_\_\_\_\_\_2023г. | |  | |

Москва 2023 г.

**Задачи**

[**Часть 1: Разработка и внедрение схемы адресации разделенной на подсети IPv4-сети.** 3](#_Toc151741937)

[**Шаг 1:** **Создайте схему разделения на подсети, которая соответствует необходимому количеству подсетей и адресов узлов.** **Ошибка! Закладка не определена.**](#_Toc151741938)

[**Шаг 2:** **Заполните диаграмму, указав, где будут применяться IP-адреса узлов.** **Ошибка! Закладка не определена.**](#_Toc151741939)

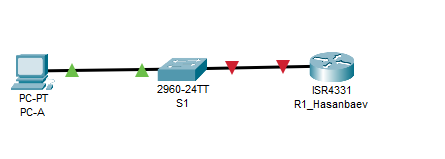
[**Часть 2: Настройка устройств** **Ошибка! Закладка не определена.**](#_Toc151741940)

[**Шаг 1: Настройте маршрутизатор.** **Ошибка! Закладка не определена.**](#_Toc151741941)

[**Шаг 2: Настройте интерфейсы ПК.** **Ошибка! Закладка не определена.**](#_Toc151741942)

[**Часть 3: Проверка сети и устранение неполадок.** **Ошибка! Закладка не определена.**](#_Toc151741943)

1. **Настройка основных параметров устройств.**
2. **Создайте сеть согласно топологии.**



1. топология

Таблица 1 – таблица адресаци

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Устройство** | **Интерфейс** | **IP-адрес** | **Маска подсети** | **Шлюз по**  **умолчанию** |
| R1\_Hasanbaev | G0/1 | 192.168.1.24 | 255.255.255.0 |  |
| S1 | VLAN 1 | 192.168.1.34 | 255.255.255.0 | 192.168.1.24 |
| PC-A | NIC | 192.168.1.44 | 255.255.255.0 | 192.168.1.24 |

1. **Настройте маршрутизатор.**

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

b. Войдите в режим глобальной конфигурации.

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 режим входа в систему по паролю. Обеспечьте закрытие сеанса линии связи через 5 минут отсутствия активности.

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

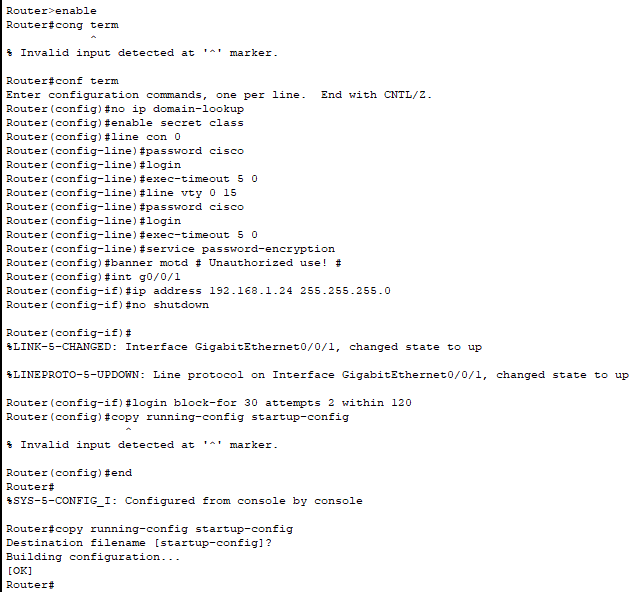
g. Зашифруйте открытые пароли.

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

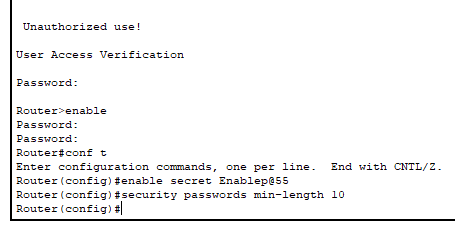
i. Настройте и активируйте на маршрутизаторе интерфейс G0/1, используя информацию, приведенную в таблице адресации.

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

k. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

****

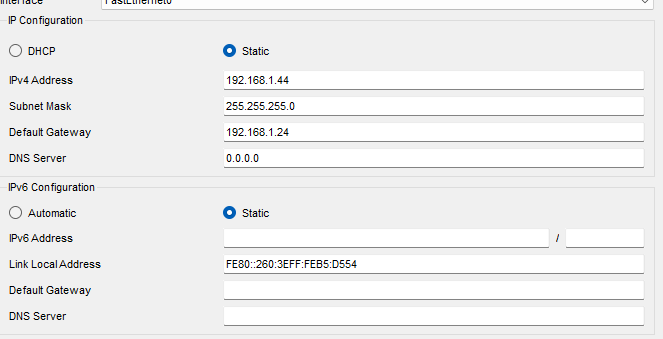
1. Настройка маршрутизатора
2. **Установите более надежные пароли**
3. Измените зашифрованный пароль привилегированного режима EXEC в соответствии с рекомендациями. Установите следующий пароль: Enablep@55.
4. Установите минимальную длину 10 символов для всех паролей.



1. Настройка маршрутизатора
2. **Настройте компьютер PC-A.**

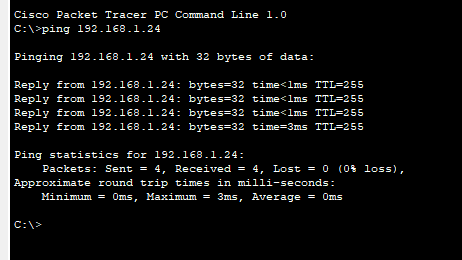
Настройте для PC-A IP-адрес и маску подсети.

Настройте для PC-A шлюз по умолчанию.



1. Настройка компьютера pc-a
2. **Проверьте подключение к сети.**

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

****

1. Эхо запрос
2. **Настройка маршрутизатора для доступа по протоколу SSH и обеспечение базовых мер безопасности**

Настройте аутентификацию устройств

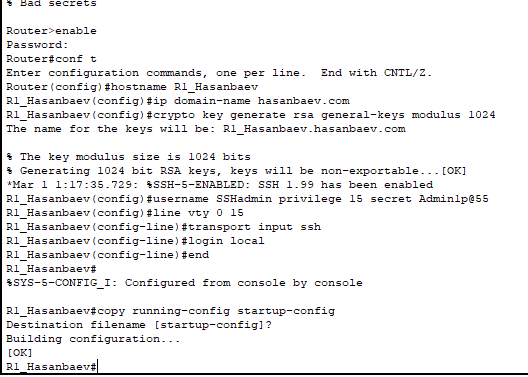
1. Задайте имя устройства.
2. Задайте домен для устройства.

Установите ключ шифрования с длиной 1024 би

Создайте имя пользователя в локальной базе учетных записей.

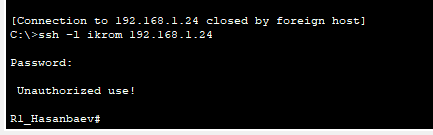
Активируйте протокол SSH на линиях VTY

Сохраните текущую конфигурацию в файл загрузочной конфигурации

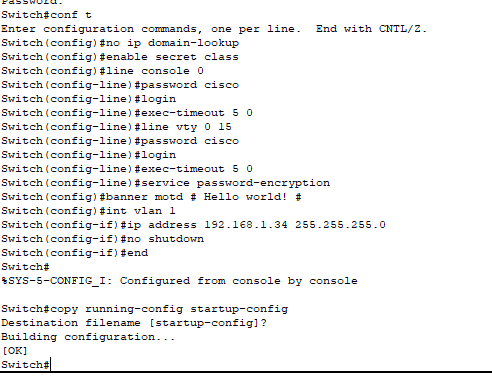


1. Настройка

Установите соединение с маршрутизатором по протоколу SSH



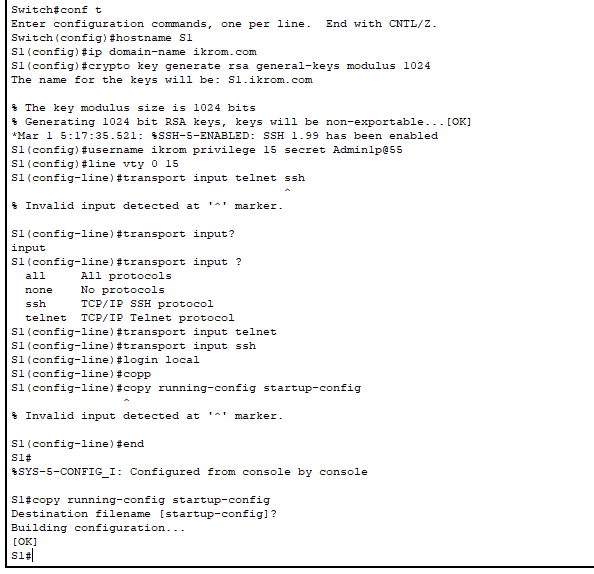
1. Соединение
2. **Настройка коммутатора для доступа по протоколу SSH и обеспечение базовых мер безопасности**
3. Подключитесь к коммутатору с помощью консольного подключения и активируйте привилегированный режим EXEC.
4. Войдите в режим конфигурации.
5. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.
6. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.
7. Назначьте cisco в качестве пароля консоли и включите режим входа в систему по паролю.
8. Обеспечьте закрытие сеанса линии связи через 5 минут отсутствия активности.
9. Назначьте cisco в качестве пароля VTY и включите вход по паролю. Обеспечьте закрытие сеанса линии связи через 5 минут отсутствия активности.
10. Зашифруйте открытые пароли.
11. Создайте баннер, который предупреждает о запрете несанкционированного доступа.
12. Настройте и активируйте на коммутаторе интерфейс VLAN 1, используя информацию, приведенную в таблице адресации.
13. Сделайте так, чтобы маршрутизатор блокировал попытки входа в систему на 30 секунд, если в течение 120 секунд будет дважды введен неверный пароль.
14. Сохраните текущую конфигурацию в файл загрузочной конфигурации.



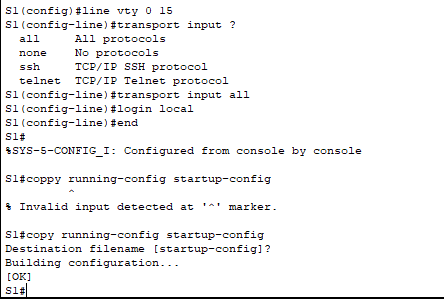
1. Настройка коммутатора

Настройте коммутатор для соединения по протоколу SSH

1. Настройте имя устройства, как указано в таблице адресации.
2. Задайте домен для устройства.
3. Создайте ключ шифрования с указанием его длины.
4. Создайте имя пользователя в локальной базе учетных записей.
5. Активируйте протоколы Telnet и SSH на линиях VTY.
6. Измените способ входа в систему таким образом, чтобы использовалась проверка пользователей по локальной базе учетных записей.



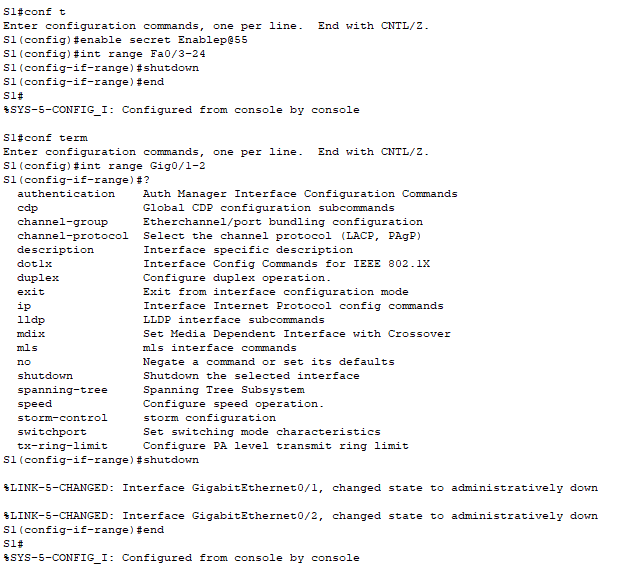
1. Настройка коммутатора по протоколу



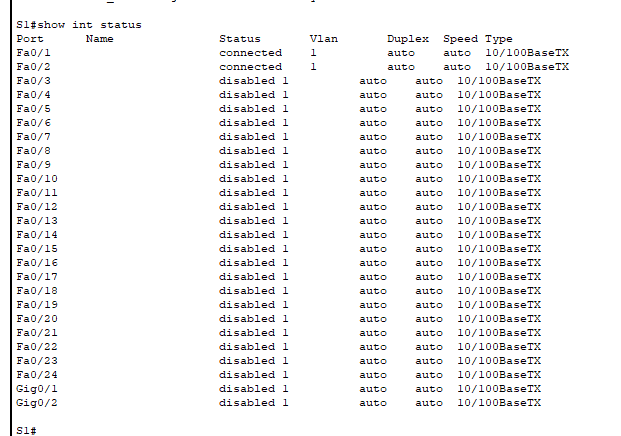
1. Настройка коммутатора

Установите более надежные пароли

Убедитесь, что все неиспользуемые порты отключены.

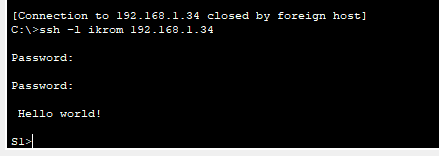


1. Надежные пароли и отключение портов



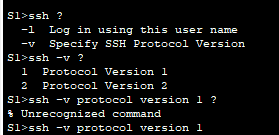
1. Отключенные порты

Установите соединение с коммутатором по протоколу SSH



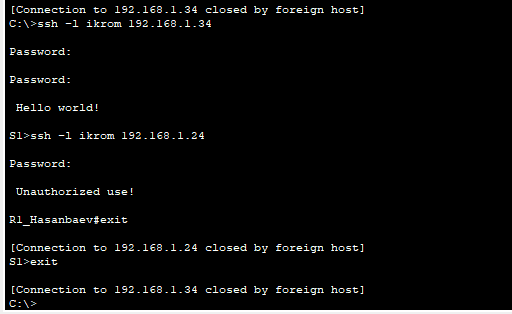
1. Подключение к коммутатору
2. **Настройка коммутатора для доступа по протоколу SSH и обеспечение базовых мер безопасности**

Посмотрите доступные параметры для клиента SSH в Cisco IOS.



1. Доступные параметры

Установите с коммутатора S1 соединение с маршрутизатором R1\_ФАМИЛИЯ по протоколу SSH



1. Установка соединения

З**аключение**

Обретены новые навыки и применены на практике.