Практическая работа №1

Тема: начальная конфигурация коммутатора CISCO

Цель работы: Проверка конфигурации коммутатора по умолчанию. Настройка базовых параметров коммутатора. Настройка баннера MOTD. Сохранение файлов конфигурации в NVRAM. Настройка коммутатора S2.

Используемые средства и оборудование: IBM/PC совместимый компьютер с пакетом Cisco Packet Tracer; лабораторный стенд Cisco.

1. Проверка конфигурации коммутатора по умолчанию.

Шаг 1: Вход в привилегированный режим.

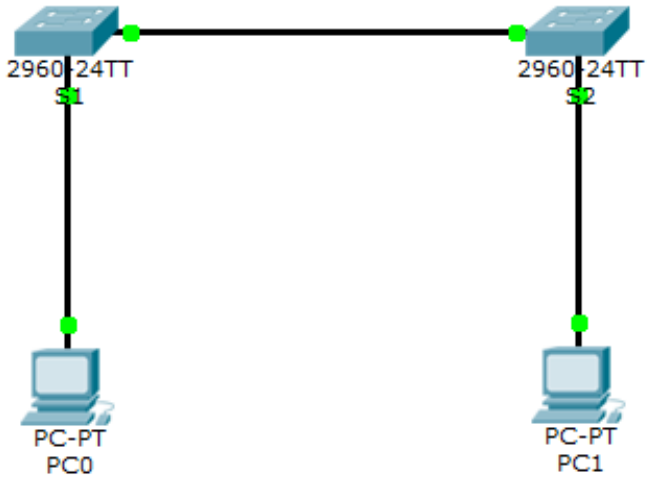

Рисунок 1 – Топология

К привилегированному набору команд относятся те, которые содержатся в пользовательском режиме, а также команда configure, при помощи которой выполняется доступ к остальным командным режимам. Щёлкаем S1 и открываем вкладку CLI. Нажимаем клавишу ВВОД. Переходим в привилегированный режим, выполнив команду enable.

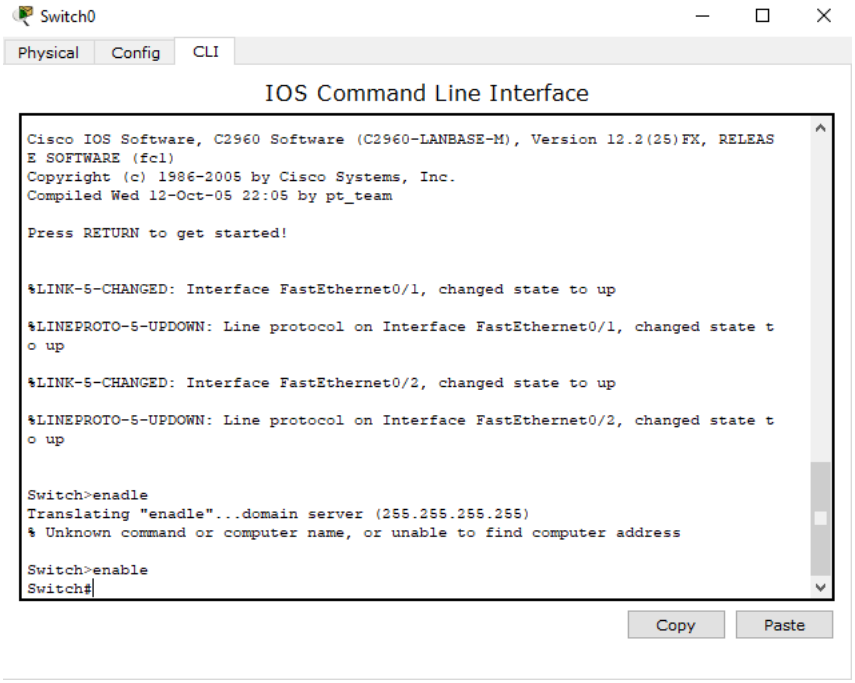

Рисунок 2 – Вход в привилегированный режим

Шаг 2: Просматриваем текущую конфигурацию коммутатора. Выполним команду show running-config. выполняем команду show running-config (рис. 3).

Switch# show running-config

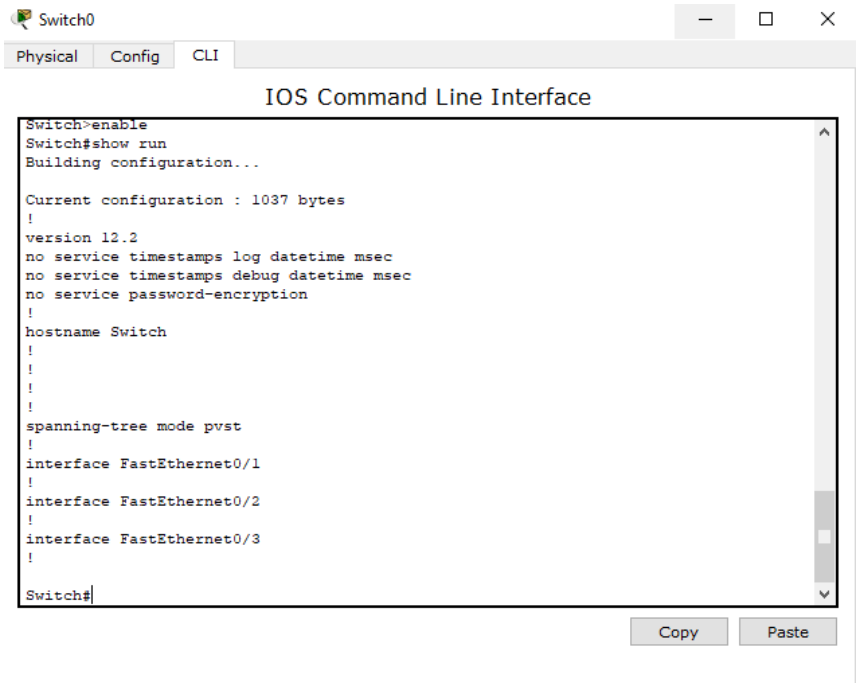

Рисунок 3 – Команда show running-config

2. Создание базовой конфигурации коммутатора

Шаг 1: Назначение коммутатору имени.

Switch# configure terminal

Switch(config)# hostname S1

S1(config)# exit

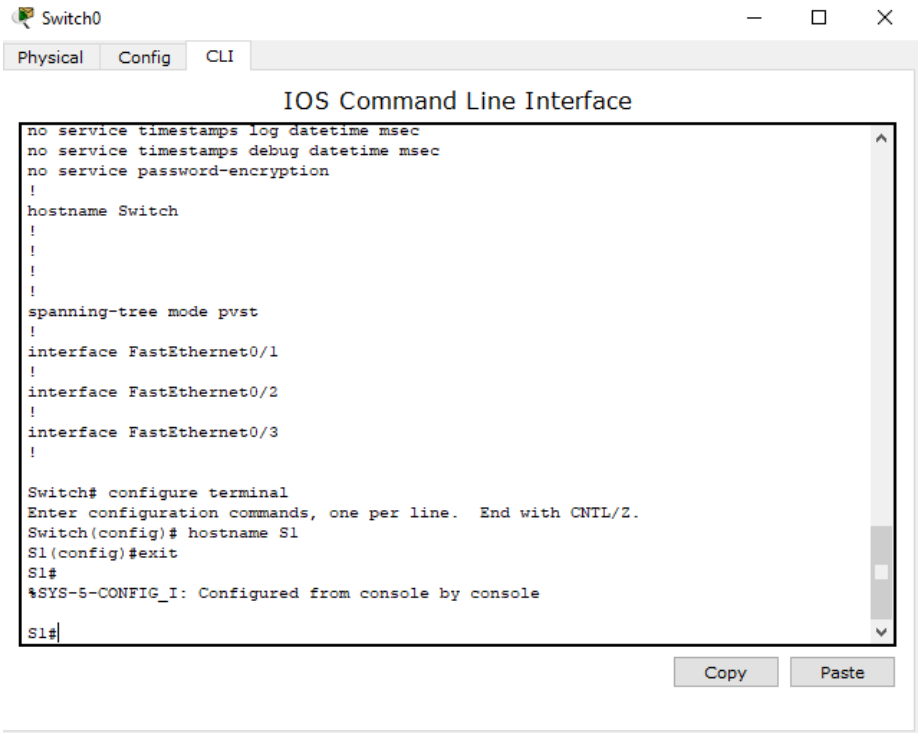

Рисунок 4 – Назначение коммутатору имени

Шаг 2: Безопасный доступ к консоли.

Для обеспечения безопасного доступа к консоли переходим в режим config-line и устанавливаем для консоли пароль letmein (рис. 5).

S1# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)# line console 0

S1(config-line)# password letmein

S1(config-line)# login

S1(config-line)# exit

S1(config)# exit

%SYS-5-CONFIG_I: Configured from console by console

S1#

Команда login нужна для того, чтобы при входе в консоль можно было установить запрос пароля и логина.

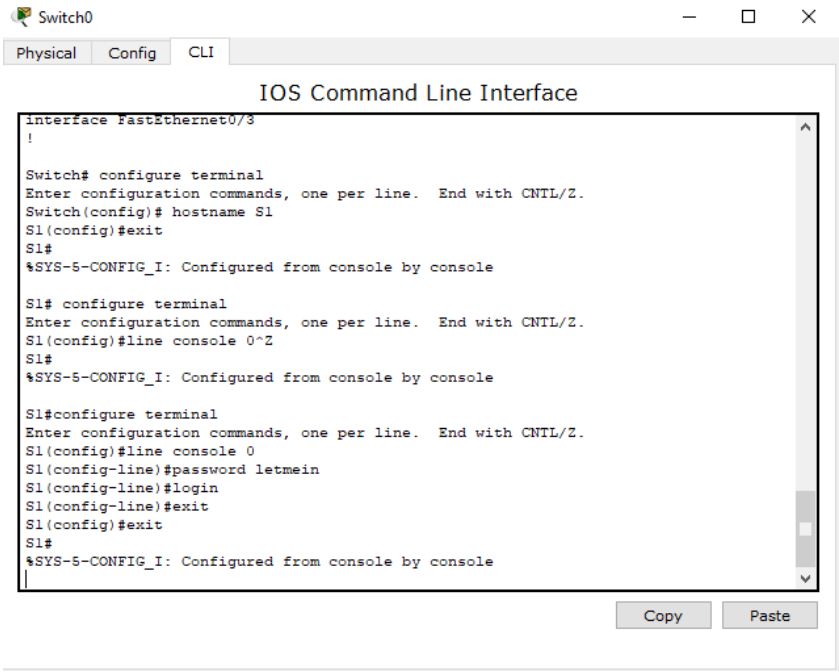

Рисунок 5 – Безопасный доступ к консоли

Шаг 3: Убедимся, что доступ к консоли защищён паролем.

Выполняем команду exit ещё раз, чтобы выйти из коммутатора.

Нажимаем клавишу <ВВОД>, после чего будет предложено ввести пароль:

User Access Verification

Password:

Первый пароль относится к консоли, который был задан для line con 0. Вводим этот пароль, чтобы вернуться в пользовательский режим.

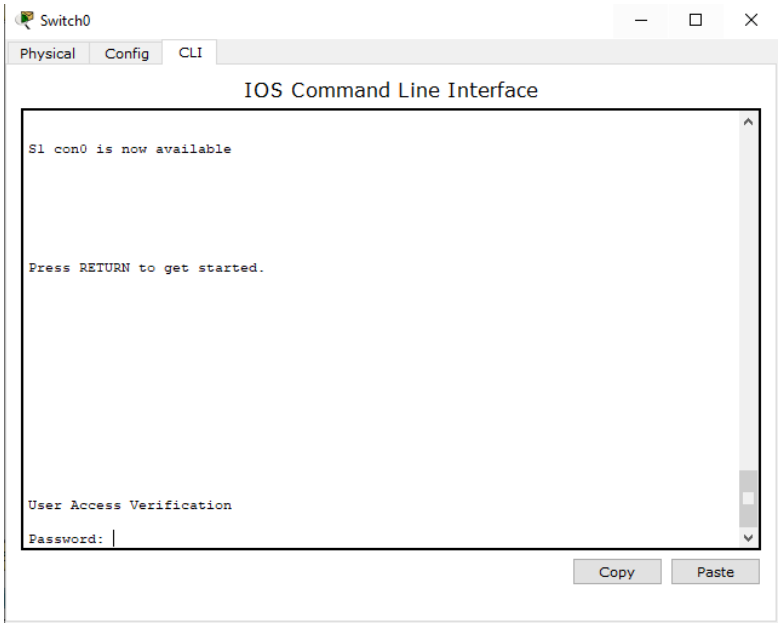

Рисунок 6 – Проверка доступа к консоли.

Шаг 4: Безопасный доступ в привилегированном режиме.

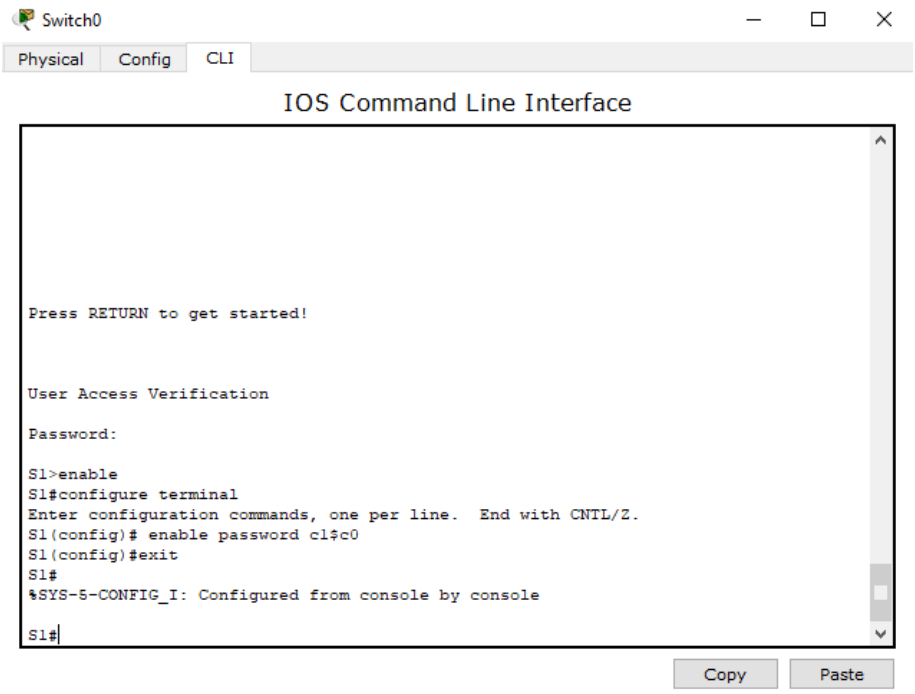

Рисунок 7 – Установка пароля для привилегированного режима.

Шаг 5: Убеждаемся, что доступ к привилегированному режиму защищён паролем.

Выполняем команду exit ещё раз, чтобы выйти из коммутатора. Нажимаем клавишу <ВВОД>, после чего будет предложено ввести пароль: User Access Verification Password: Первый пароль относится к консоли, который был задан для line con 0. Вводим этот пароль, чтобы вернуться в пользовательский режим. Вводим команду для доступа к привилегированному режиму. Вводим второй пароль, который был задан для ограничения доступа к привилегированному режиму (рис. 7).

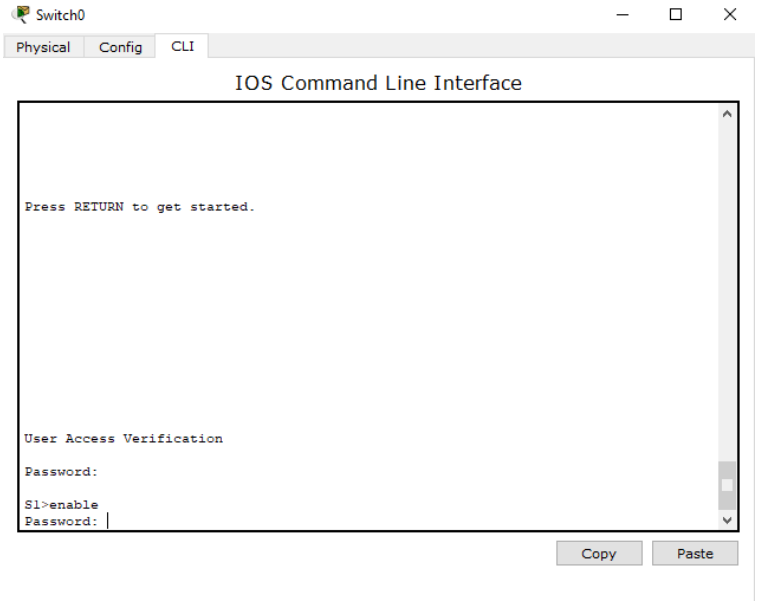

Рисунок 8 – Ввод пароля для входа в привилегированный режим

Проверяем конфигурацию, изучив содержимое файла running-configuration (рис. 9):

S1# show running-config

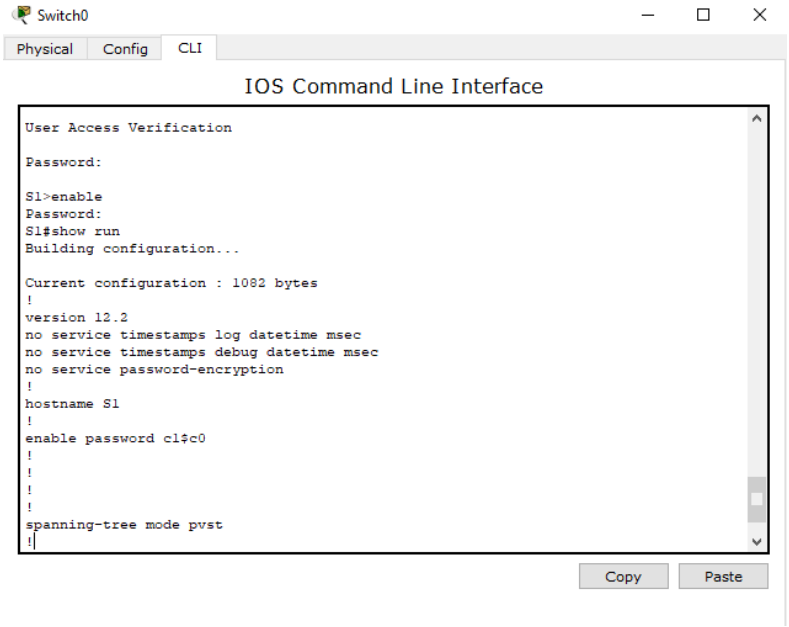

Рисунок 9 – Проверка конфигурации

Шаг 6: Настройка зашифрованного пароля для доступа к привилегированному режиму.

Пароль для enable нужно заменить на новый зашифрованный пароль с помощью команды enable secret.

Устанавливаем для команды «enable» пароль itsasecret (рис. 10).

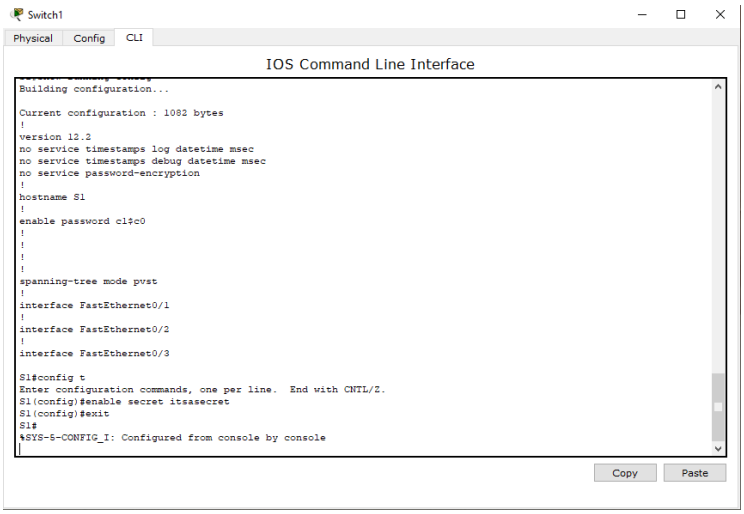

Рисунок 10 – Замена пароля на зашифрованный пароль

Шаг 7: Убеждаемся в том, что пароль «enable secret» добавлен в файл конфигурации.

Вводим команду show running-config ещё раз, чтобы проверить новый пароль enable secret (рис. 11).

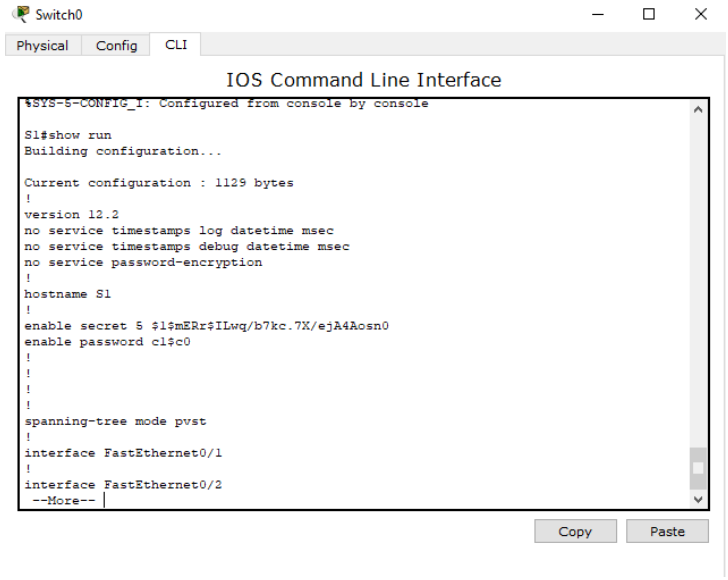

Рисунок 11 – Проверка зашифрованного пароля

Шаг 8: Шифрование паролей для консоли и привилегированного режима.

Сейчас мы зашифруем эти открытые пароли с помощью команды service password-encryption (рис. 12).

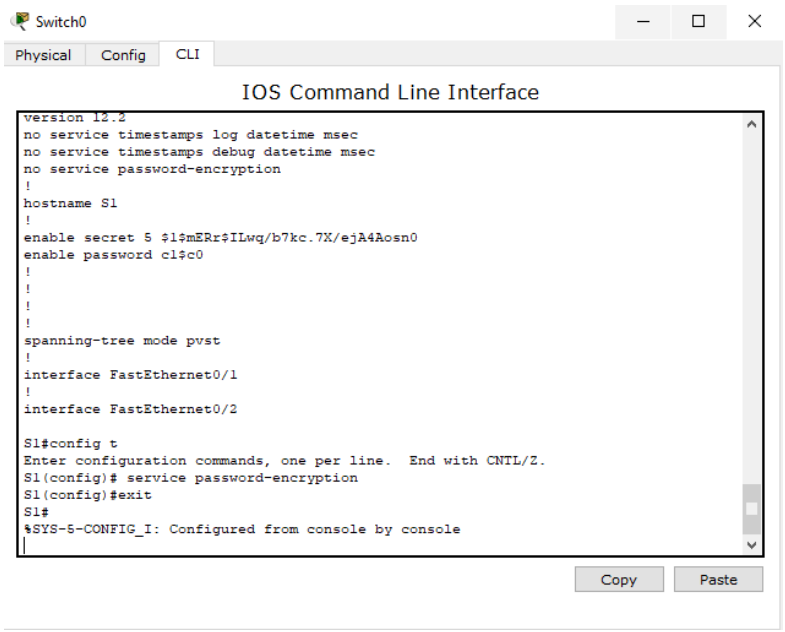

Рисунок 12 – Шифрование паролей

3. Настройка баннера MOTD

Шаг 1: Настройка сообщения ежедневного баннера (MOTD).

В набор команд Cisco IOS входит команда, которая позволяет настроить сообщение, которое будет показываться всем, кто входит в систему на коммутаторе. Это сообщение называется ежедневным баннером (MOTD). Текст баннера нужно заключить в двойные кавычки или использовать разделитель, отличный от любого символа в строке MOTD (рис. 13).

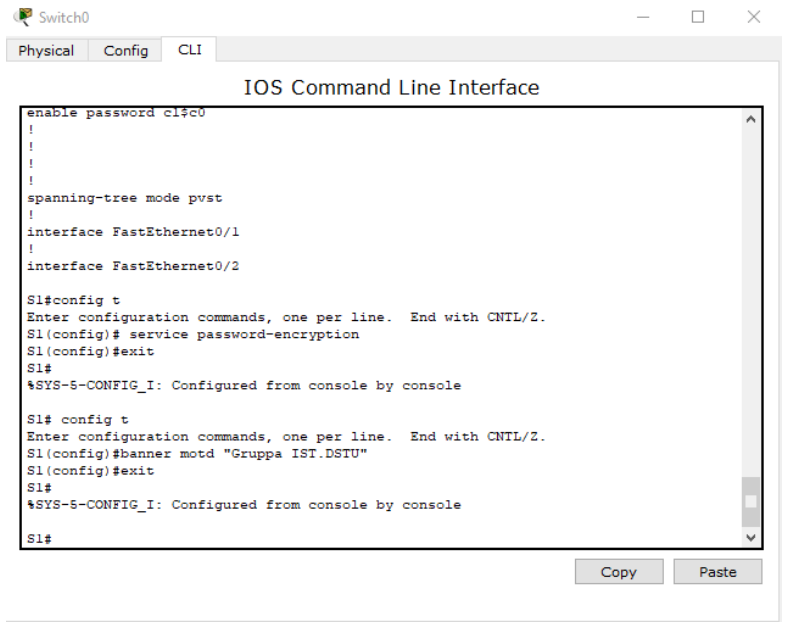

Рисунок 13 – Настройка сообщения ежедневного баннера MOTD

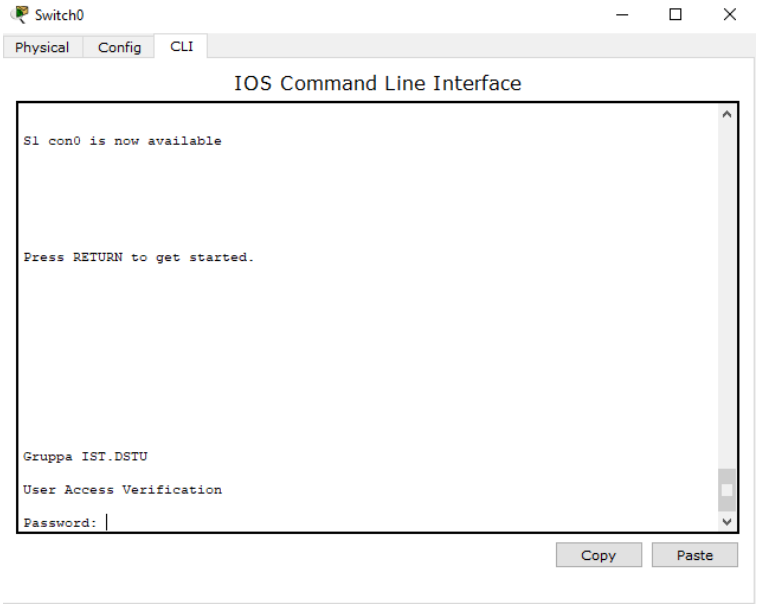

Рисунок 14 – Отображение ежедневного баннера MOTD

Чтобы при входе в коммутатор пользователю была доступна какая-либо полезная информация на всех коммутаторах должен быть баннер MOTD.

4. Сохранение файлов конфигурации в NVRAM

Шаг 1: Проверяем правильность конфигурации с помощью команды «show run» (рис. 15).

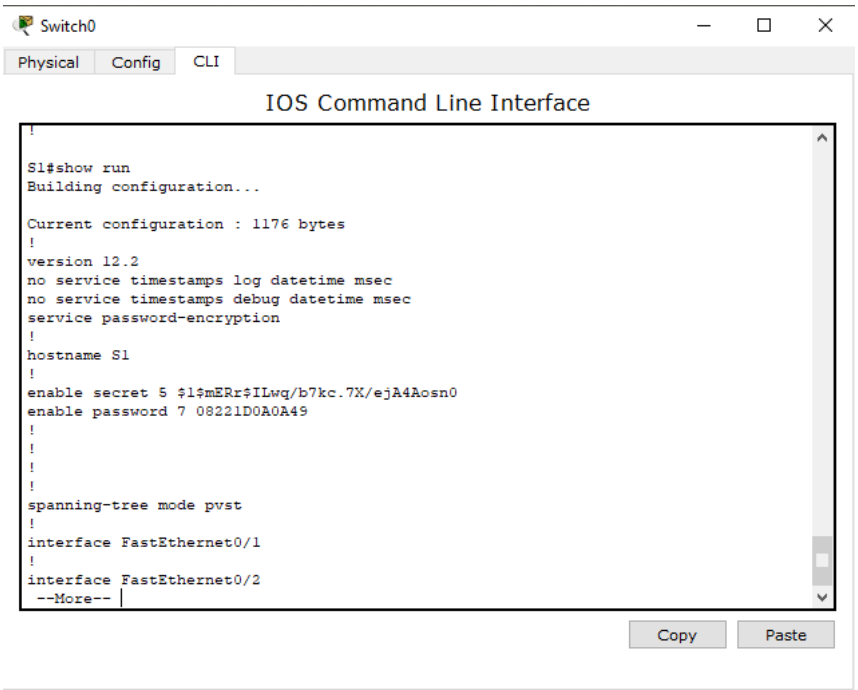

Рисунок 15 – Проверка правильности конфигурации

Шаг 2: Сохраняем файл конфигурации.

Мы завершили базовую настройку коммутатора. Теперь выполним резервное копирование файла конфигурации в NVRAM и проверим, чтобы внесённые изменения не потерялись после перезагрузки системы и отключения питания (рис. 16).

S1# copy running-config startup-config

Destination filename [startup-config]?[Enter]

Building configuration...

[OK]

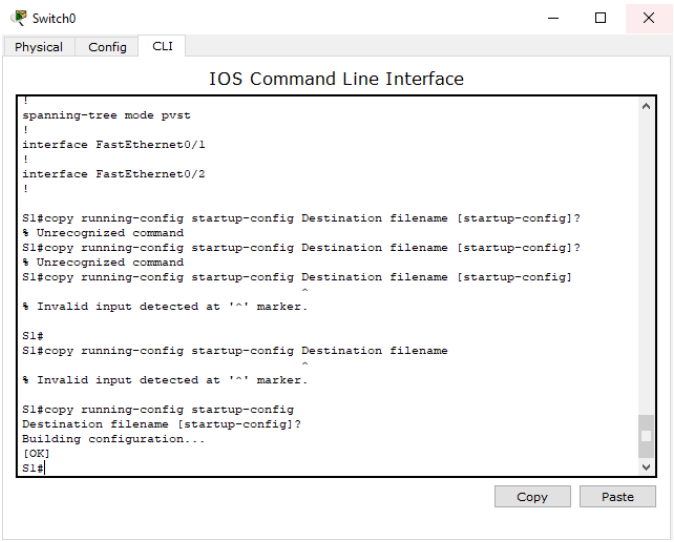

Рисунок 16 – Резервное копирование файла конфигурации в NVRAM

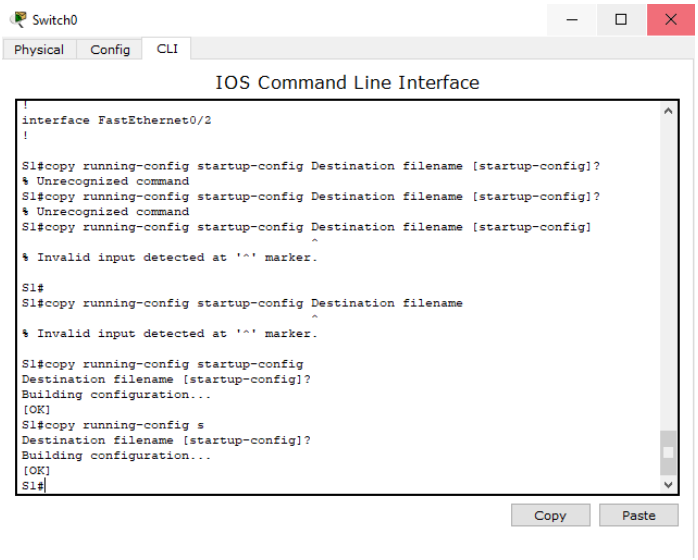

Рисунок 17 – Самая короткая версия команды copy running-config s

Шаг 3: Изучение начального файла конфигурации. Какая команда отображает содержимое NVRAM?

S1# show run

Все ли внесённые изменения были записаны в файл? Все внесённые изменения были записаны в файл.

5. Конфигурация S2

Мы завершили настройку коммутатора S1. Теперь настроим коммутатор S2. Настроим для коммутатора S2 следующие параметры. Имя устройства: S2 (рис. 18), защищаем доступ к консоли паролем letmein, устанавливаем для привилегированного режима пароль c1$c0 и задаем пароль «enable secret» для itsasecret, вводим следующее сообщение для пользователей, выполняющих вход в систему на коммутаторе: «Gruppa IST.DSTU», зашифровываем все открытые пароли, проверяем правильность конфигурации (рис. 19), сохраняем файл конфигурации, чтобы предотвратить его потерю в случае отключения питания коммутатора (рис. 20).

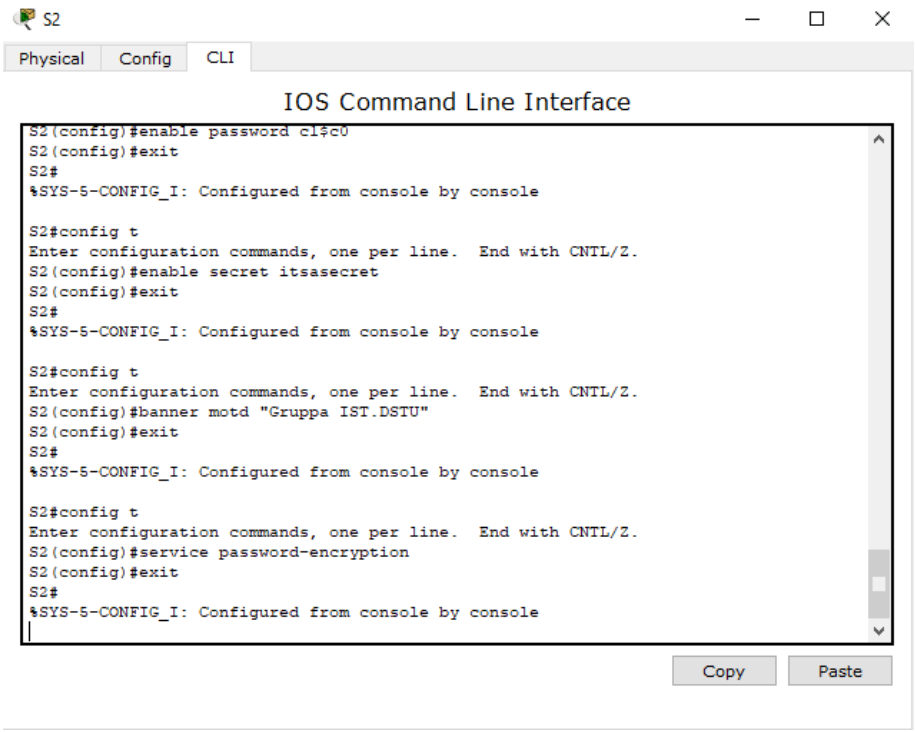

Рисунок 18 – Конфигурирование коммутатора S2

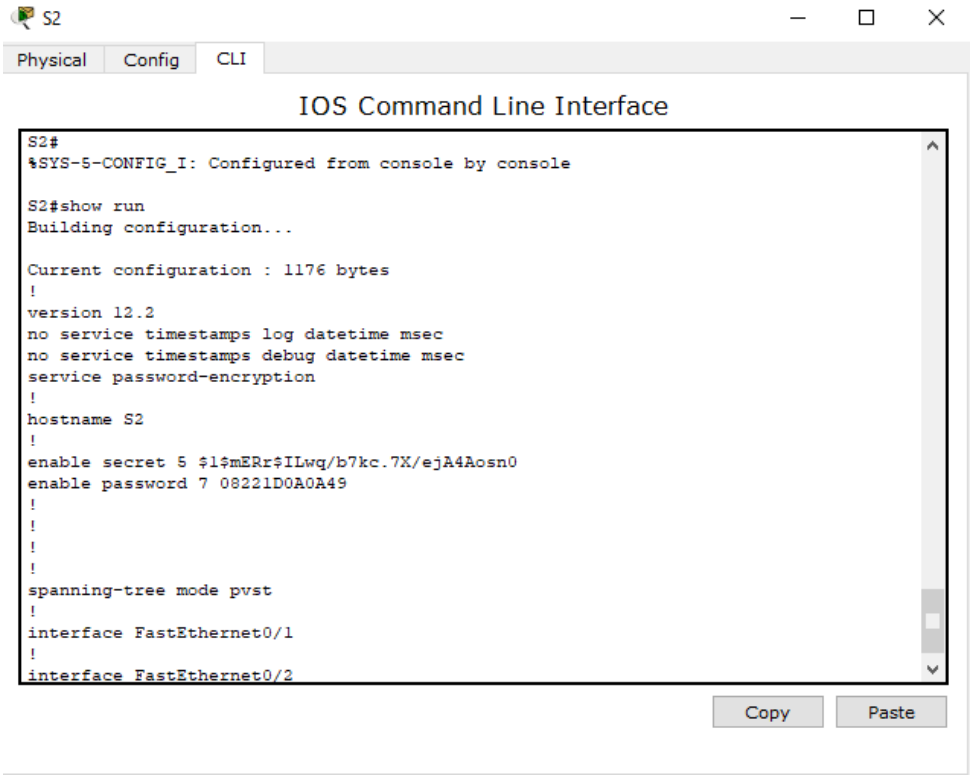

Рисунок 19 – Проверка правильности конфигурации

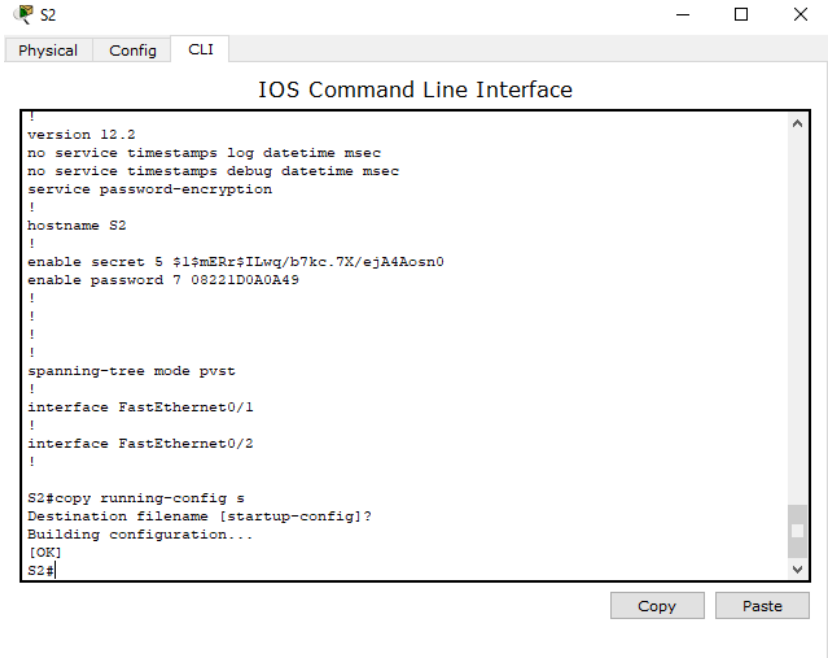

Рисунок 20 – Сохранение конфигурации

Контрольные вопросы

1. В привилегированном режиме доступны все команды коммутатора?

2. С помощью какой команды можно перейти в привилегированный режим?

3. С помощью какой команды можно просмотреть текущую конфигурацию коммутатора?

4. В какой режим нужно перейти, чтобы обеспечить безопасный доступ к консоли?

5. С помощью какой команды коммутатору можно назначить имя?

6. Какая команда осуществляет выход из коммутатора?

7. Для чего нужно шифрование паролей?

8. Как можно сократить команду show running-config?

9. С помощью какой команды можно зашифровать открытые пароли?

10. С помощью какой команды можно настроить зашифрованный пароль для доступа к привилегированному режиму?