Практическая работа №1.

«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. Ход работы

1.1. ПРОВЕРКА КОНФИГУРАЦИИ КОММУТАТОРА ПО УМОЛЧАНИЮ

Шаг 1: Вход в привилегированный режим.

В привилегированном режиме доступны все команды коммутатора. Но в связи с тем, что многими из привилегированных команд задаются рабочие параметры, привилегированный доступ должен быть защищён паролем во избежание несанкционированного использования.

Для выполнения лабораторной работы создаем топологию, представленную на рис. 1.1.

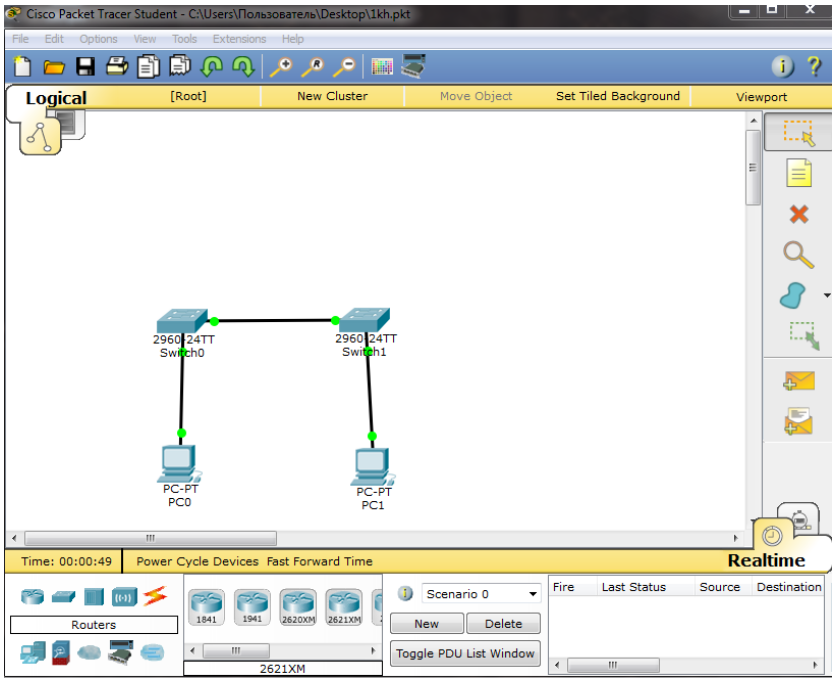

Рис. 1.1. Топология

					09.03.02.090000.000 ЛР		
Изм	Лист	№ докум.	Подпись	Дата			
Разраб.		Климова Ю.В.			Практическая работа «начальная конфигурация коммутатора CISCO»	Литера	Лист 1 / Листов 18
Провер.		Берёза А.Н.					
Н. контр.						ИСОиП (филиал) ДГТУ в г. Шахты Кафедра Информатика	
Утв							

К привилегированному набору команд относятся те, которые содержатся в пользовательском режиме, а также команда configure, при помощи которой выполняется доступ к остальным командным режимам.

a. Щёлкаем S1 и открываем вкладку CLI. Нажимаем клавишу ВВОД.

b. Переходим в привилегированный режим, выполнив команду enable (рис. 1.2). Switch> enable

Switch#

Обращаем внимание на то, что изменённая в конфигурации строка будет отражать привилегированный режим.

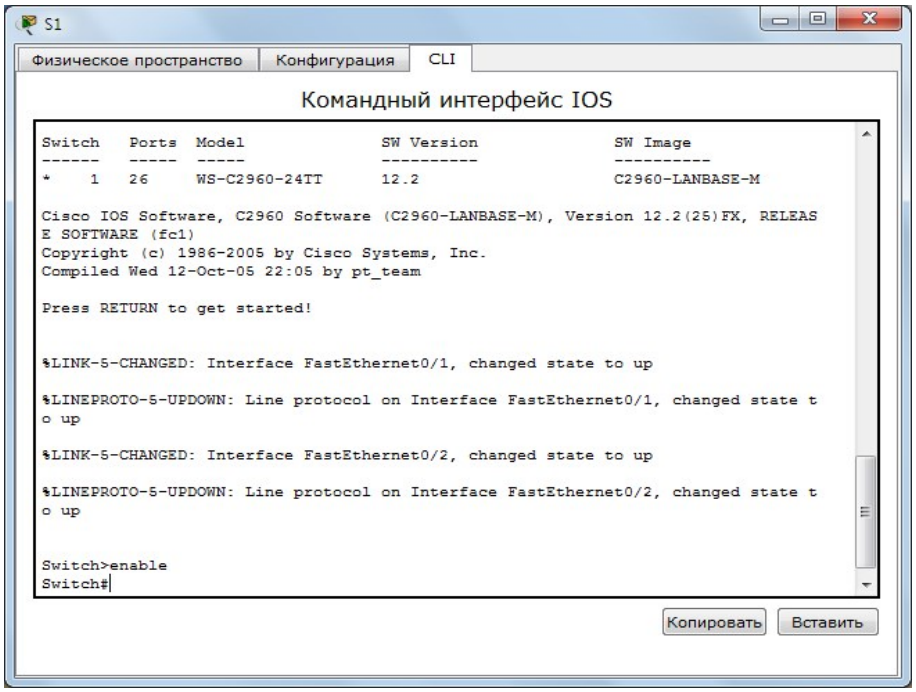

Рис. 1.2. Вход в привилегированный режим

Шаг 2: Просматриваем текущую конфигурацию коммутатора.

a. Выполняем команду show running-config (рис. 1.3).

Switch# show running-config

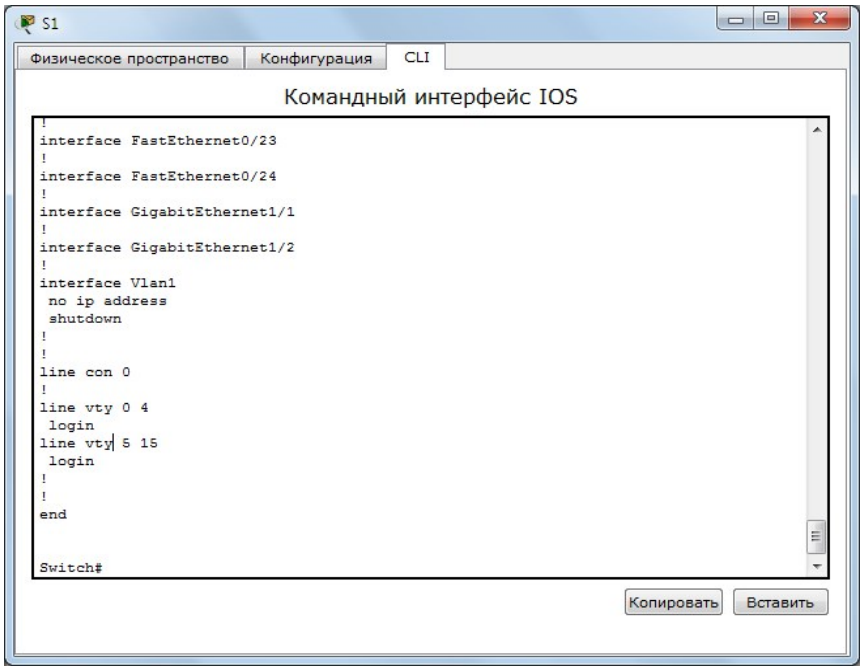

Рис. 1.3. Команда show running-config

2.2. Создание базовой конфигурации коммутатора

Шаг 1: Назначение коммутатору имени.

Для настройки параметров коммутатора, возможно, потребуется переключаться между режимами настройки. Обращаем внимание на то, как изменяется строка приглашения при переходе по разделам коммутатора (рис.1.4).

Switch# configure terminal

Switch(config)# hostname S1

S1(config)# exit

S1#

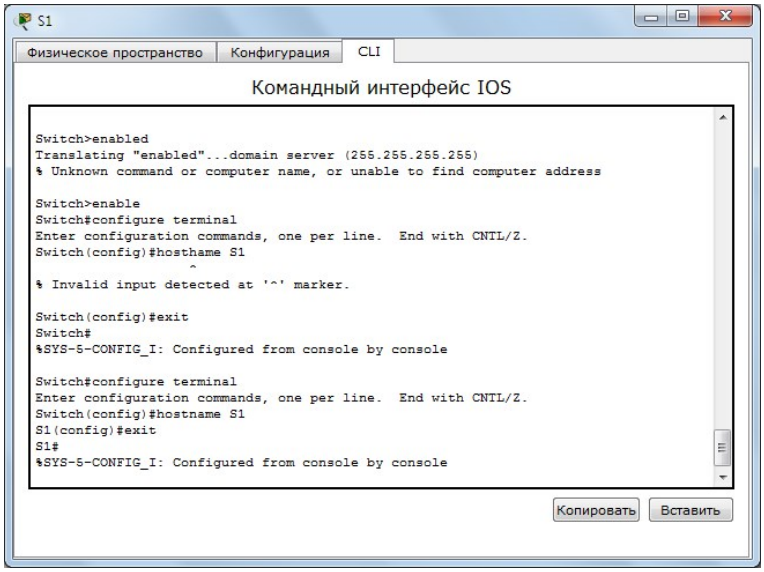

Рис. 1.4. Назначение коммутатору имени

Шаг 2: Безопасный доступ к консоли.

Для обеспечения безопасного доступа к консоли переходим в режим config-line и устанавливаем для консоли пароль letmein (рис. 1.5).

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#

Для чего нужна команда login?

Чтобы при входе в консоль можно было установить запрос пароля и логина.

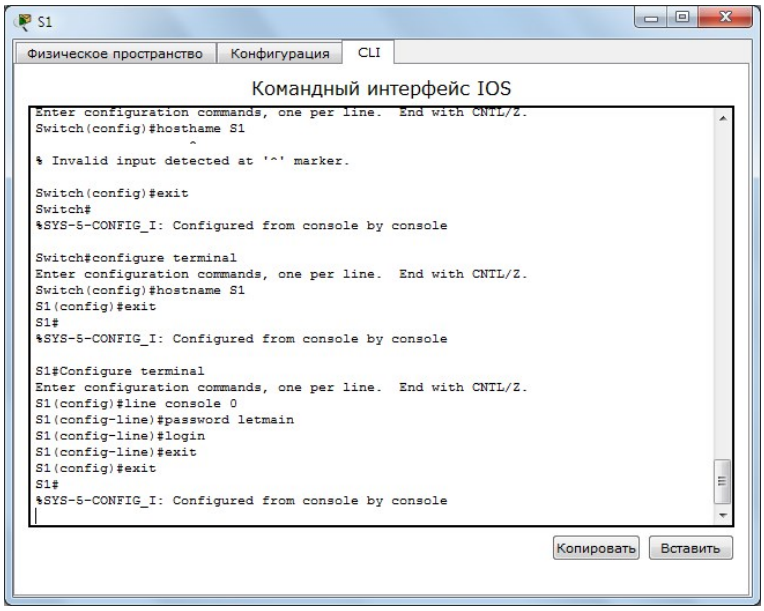

Рис. 1.5. Безопасный доступ к консоли

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

Выходим из привилегированного режима, чтобы убедиться, что для консольного порта установлен пароль (рис. 1.6).

S1# exit

Switch con0 is now available Press RETURN to get started.

User Access Verification Password:

S1>

Примечание. Если коммутатор не выводит запрос на ввод пароля, значит, вы не настроили параметр login в шаге 2.

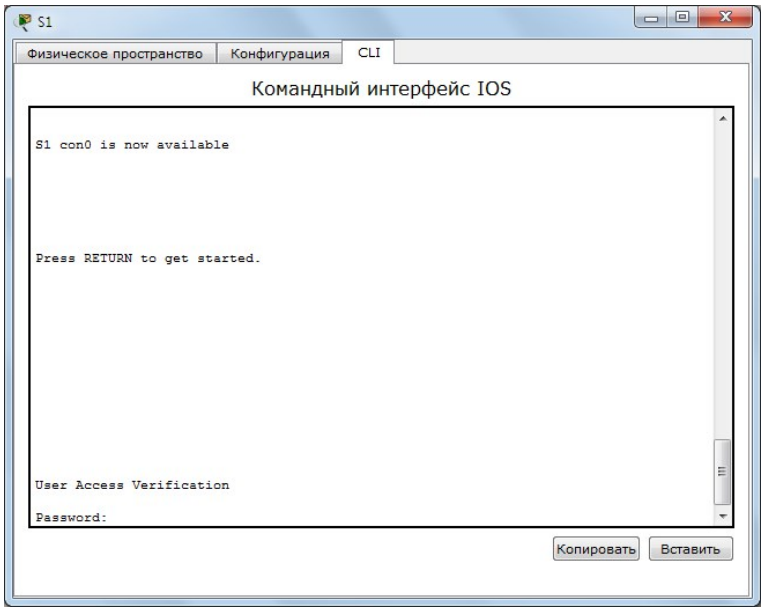

Рис. 1.6. Проверка доступа к консоли

Шаг 4: Безопасный доступ в привилегированном режиме.

Устанавливаем для enable пароль c1$c0. Этот пароль ограничивает доступ к привилегированному режиму (рис. 1.7).

Примечание. Символ 0 в c1$c0 – это цифра ноль, а не буква «О». Этот пароль не будет действительным, пока вы его не зашифруете в шаге 8.

S1> enable

S1# configure terminal

S1(config)# enable password c1$c0

S1(config)# exit

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

S1#

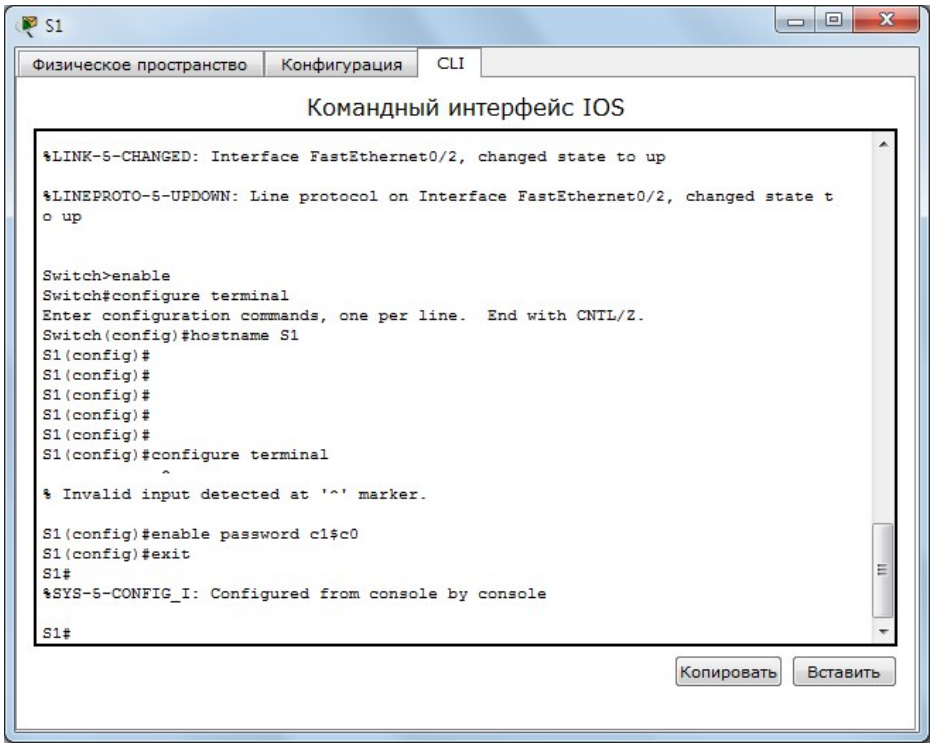

Рис. 1.7. Установка пароля для привилегированного режима

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

a. Выполняем команду exit ещё раз, чтобы выйти из коммутатора.

b. Нажимаем клавишу <ВВОД>, после чего будет предложено ввести пароль: User Access Verification Password:

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

d. Вводим команду для доступа к привилегированному режиму.

e. Вводим второй пароль, который был задан для ограничения доступа к привилегированному режиму (рис. 1.8).

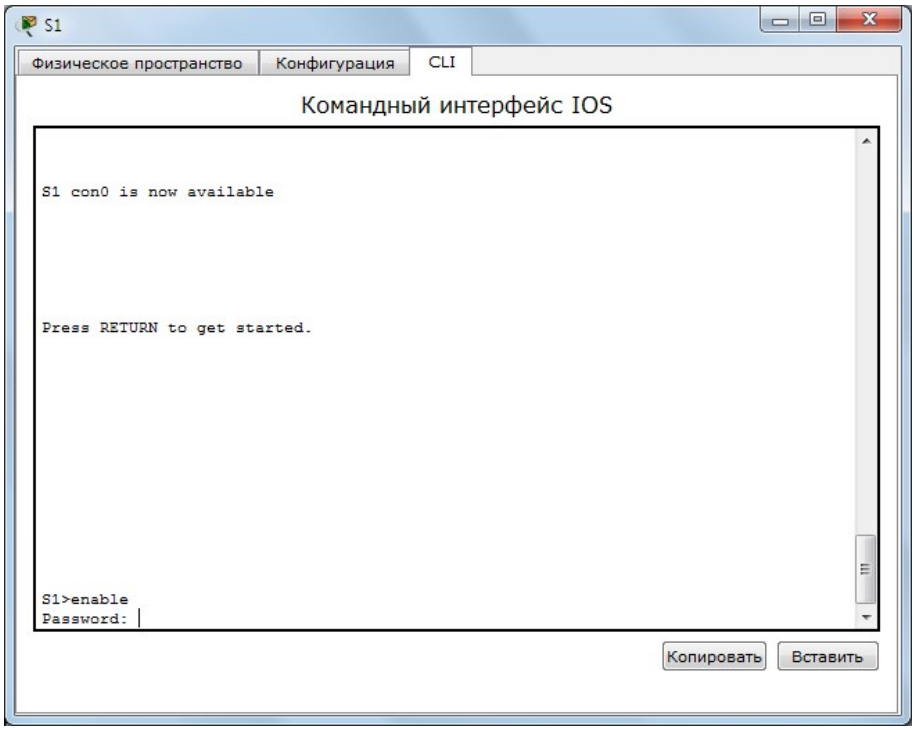

Рис. 1.8. Ввод пароля для входа в привилегированный режим

f. Проверяем конфигурацию, изучив содержимое файла running-configuration (рис. 1.9):

S1# show running-config

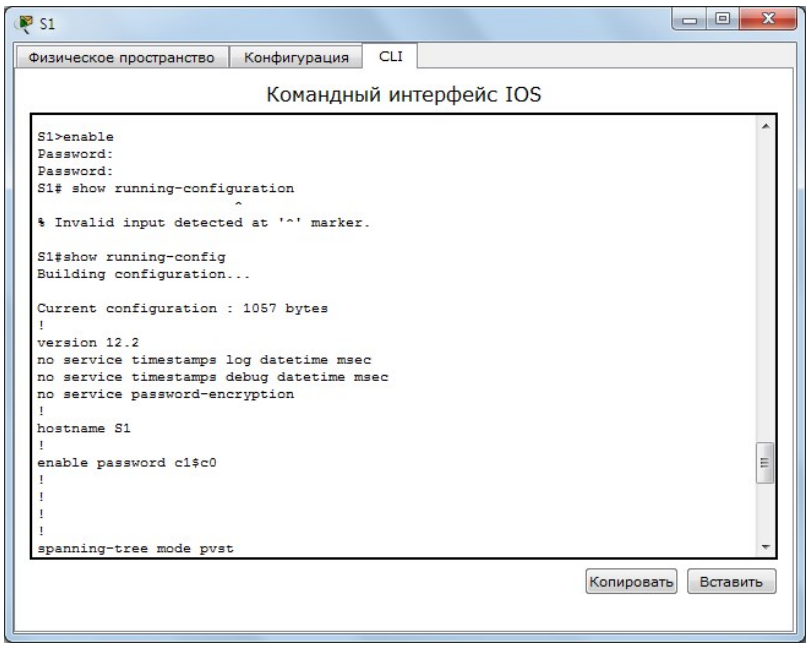

Рис. 1.9. Проверка конфигурации

Пароли для консоли и привилегированного режима отображаются в виде обычного текста. Это может представлять риск для системы безопасности, если за вашими действиями наблюдают из-за спины.

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. 1.10).

S1# config t

S1(config)# enable secret itsasecret

S1(config)# exit

S1#

Примечание. Пароль enable secret переопределяет пароль enable. Если для коммутатора заданы оба пароля, для перехода в привилегированный режим нужно ввести пароль enable secret.

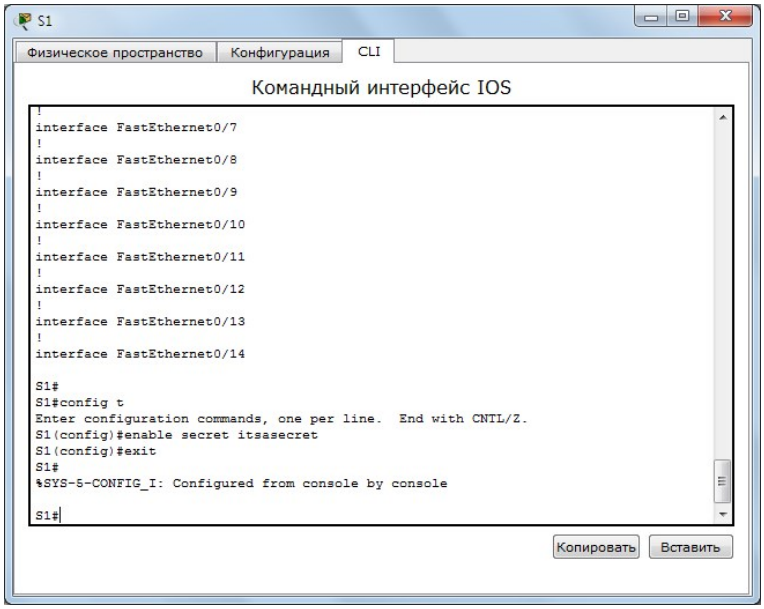

Рис. 1.10. Замена пароля на зашифрованный пароль

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

a. Вводим команду show running-config ещё раз, чтобы проверить новый пароль enable secret (рис. 1.11).

Примечание. Команду show running-config можно сократить до S1# show run

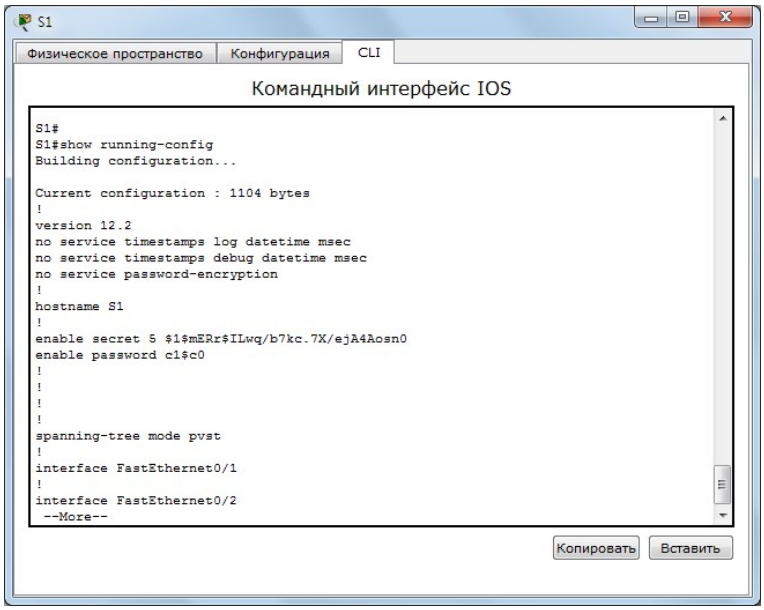

Рис. 1.11. Проверка зашифрованного пароля

b. Что отображается при выводе пароля enable secret?

1mERr$ILwq/b7kc.7X/ejA4Aosn0

c. Почему пароль enable secret отображается не так, как заданный пароль?

Потому что пароль enable secret зашифрован, а заданный пароль хранится в виде обычного текста

Шаг 8: Шифрование паролей для консоли и привилегированного режима.

Как было видно в шаге 7, пароль enable secret зашифрован, а пароли enable и console хранятся в виде обычного текста. Сейчас мы зашифруем эти открытые пароли с помощью команды service password-encryption (рис. 1.12).

S1# config t

S1(config)# service password-encryption

S1(config)# exit

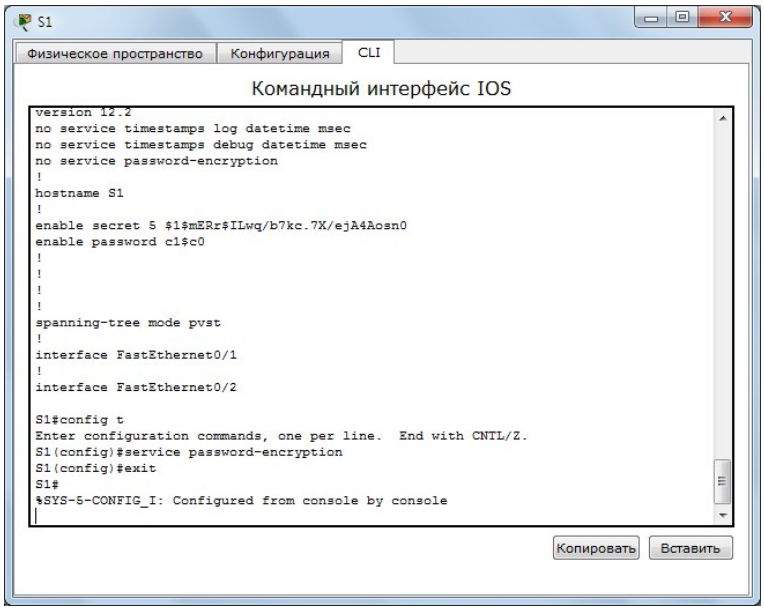

Рис. 1.12. Шифрование паролей

Если установить на коммутаторе другие пароли, они будут храниться в файле конфигурации в виде обычного текста или в зашифрованном виде?

Если на коммутаторе установить другие пароли, они будут храниться в файле конфигурации в зашифрованном виде.

2.3. 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. 1.13).

S1# config t

S1(config)# banner motd "Gruppa 3-7. NPI"

S1(config)# exit

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

S1#

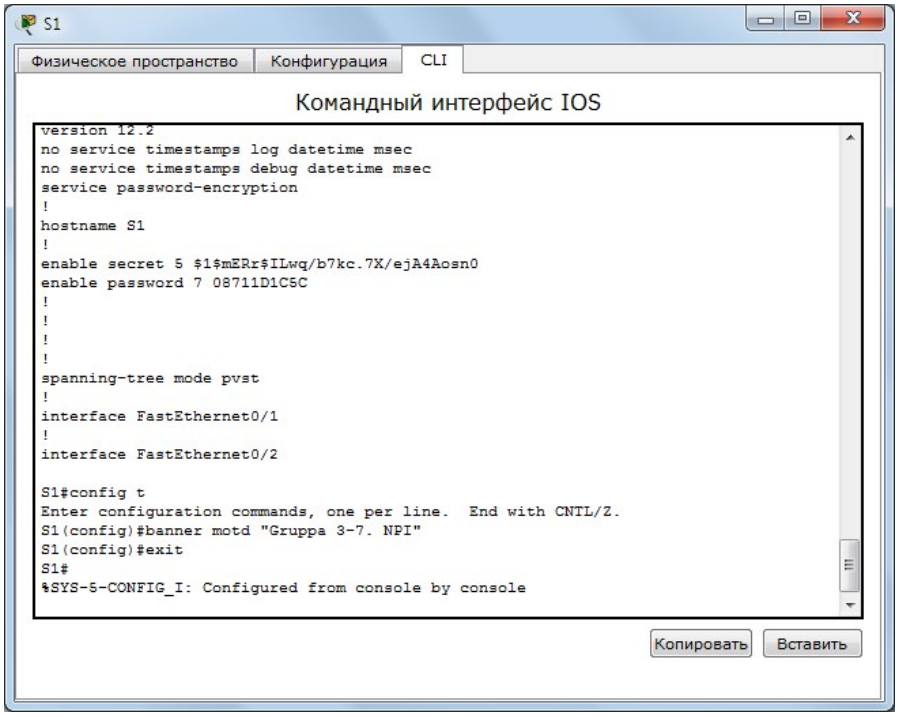

Рис. 1.13. Настройка сообщения ежедневного баннера MOTD

Когда будет отображаться этот баннер?

После ввода пароля и входа в консоль коммутатора (рис. 1.14).

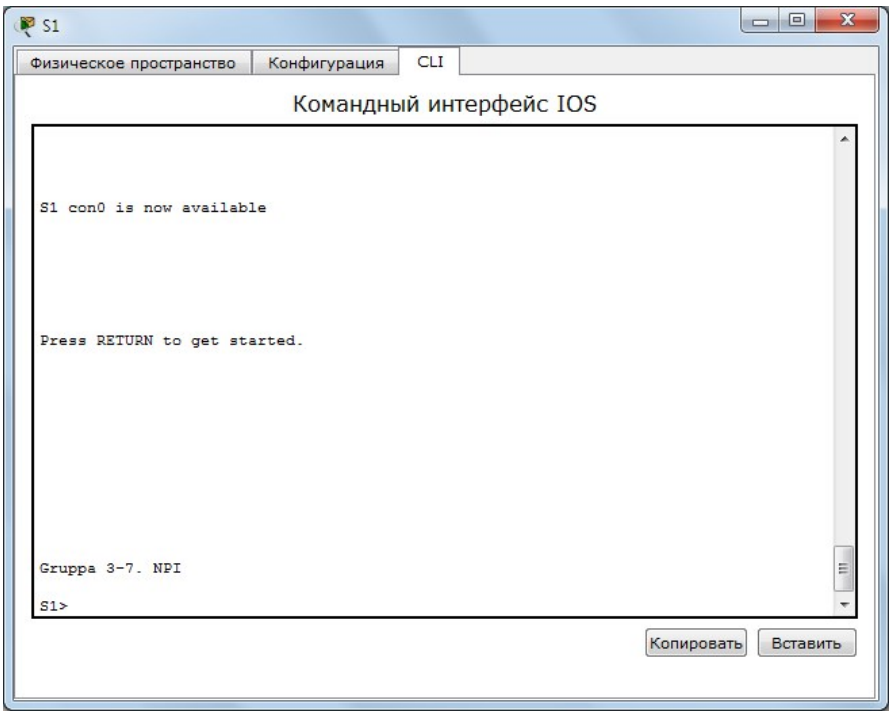

Рис. 1.14. Отображение ежедневного баннера MOTD

Зачем на всех коммутаторах должен быть баннер MOTD?

Чтобы при входе в коммутатор пользователю была доступна какая-либо полезная информация.

2.4. Сохранение файлов конфигурации в NVRAM

Шаг 1: Проверяем правильность конфигурации с помощью команды «show run» (рис. 1.15).

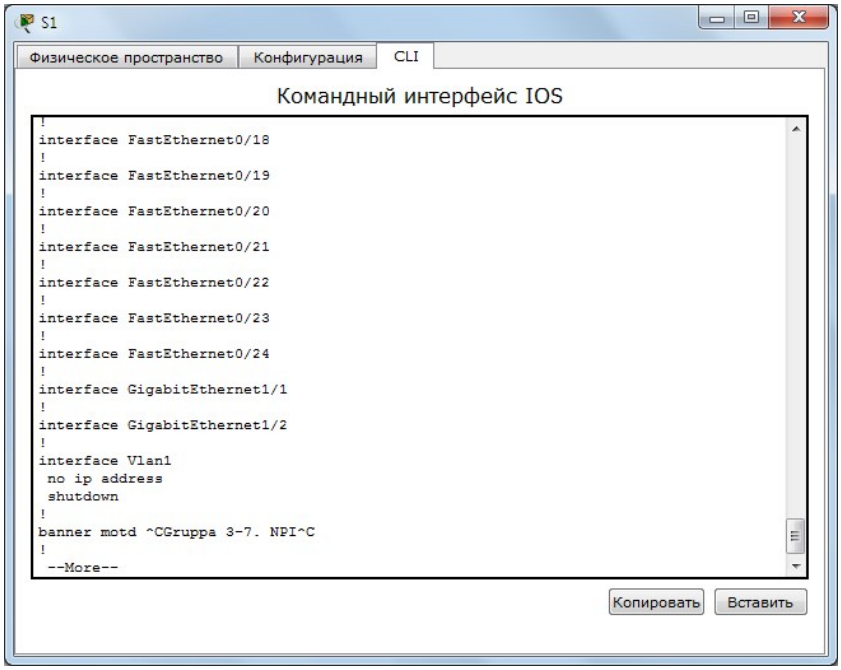

Рис. 1.15. Проверка правильности конфигурации

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. 1.16).

S1# copy running-config startup-config Destination filename [startup-config]?[Enter] Building configuration...

[OK]

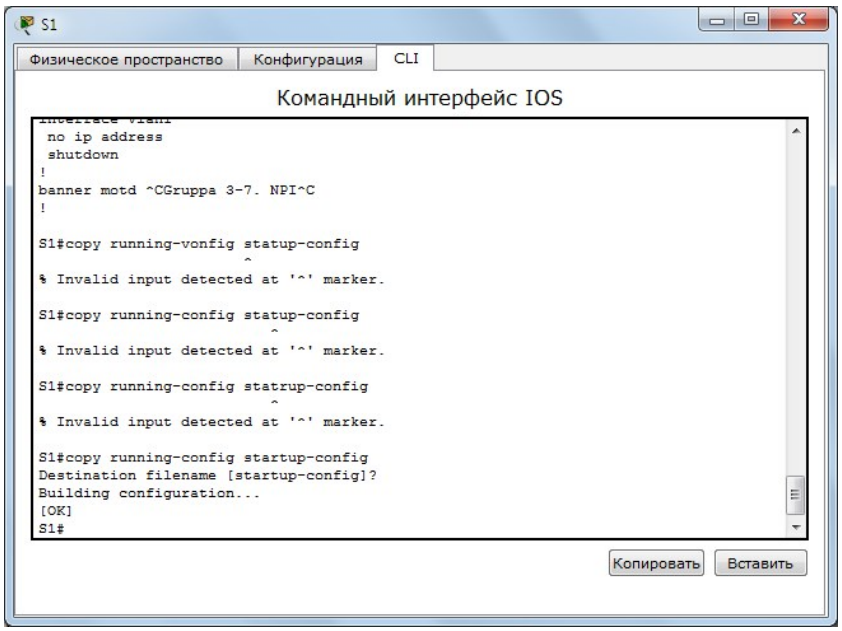

Рис. 1.16. Резервное копирование файла конфигурации в NVRAM

Какова самая короткая версия команды copy running-config startup-config?

copy running-config s (рис. 1.17)

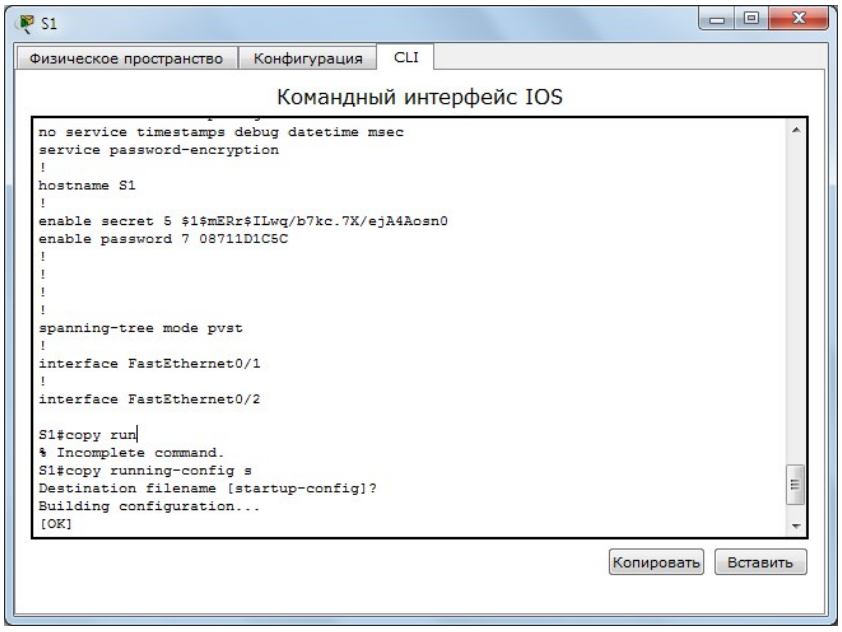

Рис. 1.17. Самая короткая версия команды copy running-config startupconfig

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.*

2.5. Конфигурация S2

Мы завершили настройку коммутатора S1. Теперь настроим коммутатор S2.

Настроим для коммутатора S2 следующие параметры. a. Имя устройства: S2 (рис. 1.18).

b. Защищаем доступ к консоли паролем letmein (рис. 1.18).

c. Устанавливаем для привилегированного режима пароль c1$c0 и задаем пароль «enable secret» для itsasecret (рис. 1.18).

d. Вводим следующее сообщение для пользователей, выполняющих вход в систему на коммутаторе:
«Gruppa 3-7. NPI» (рис. 1.18).

d. Зашифровываем все открытые пароли (рис. 1.18).

e. Проверяем правильность конфигурации (рис. 1.19).

f. Сохраняем файл конфигурации, чтобы предотвратить его потерю в случае отключения питания коммутатора (рис. 1.20).

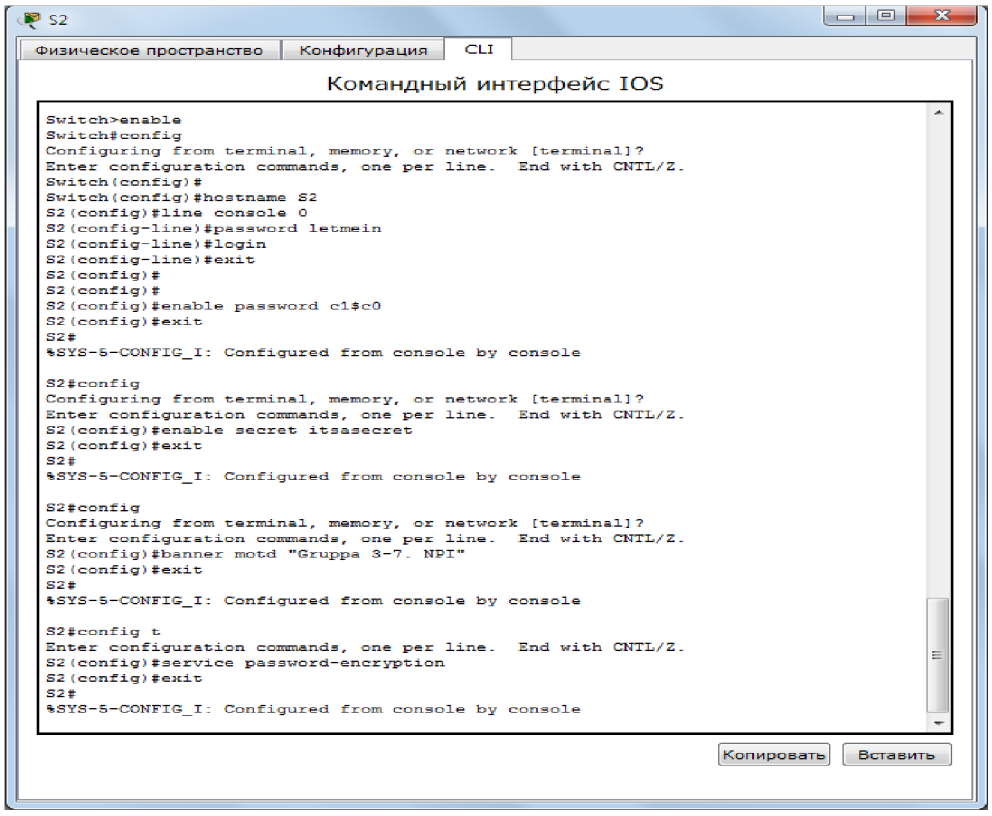

Рис. 1.18. Конфигурирование коммутатора S2

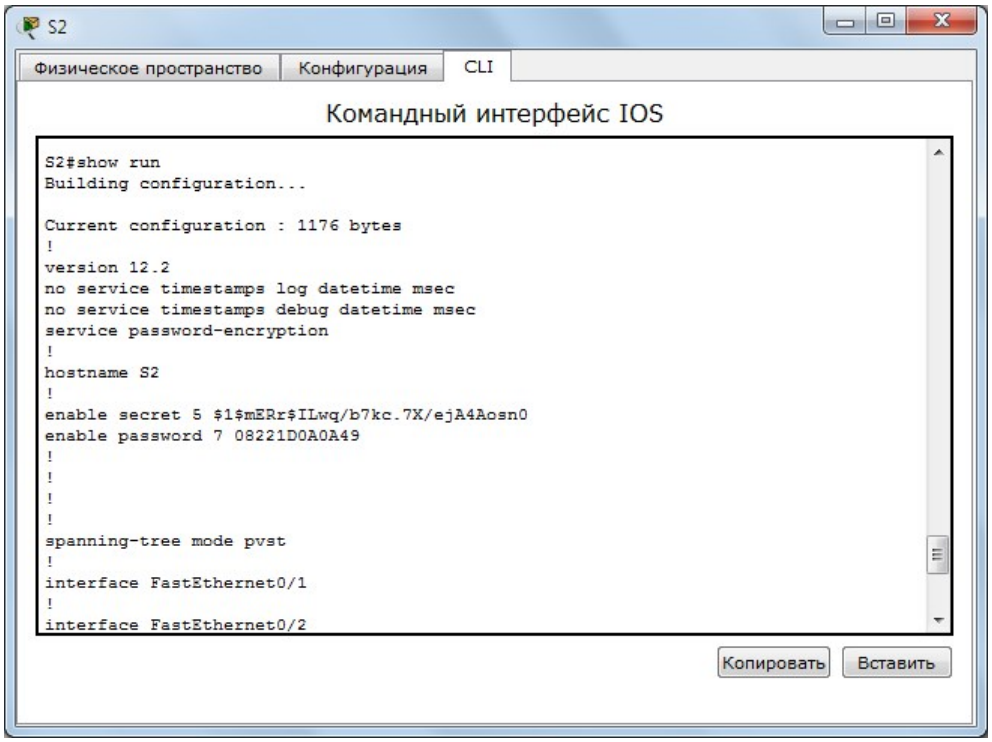

Рис. 1.19. Проверка правильности конфигурации

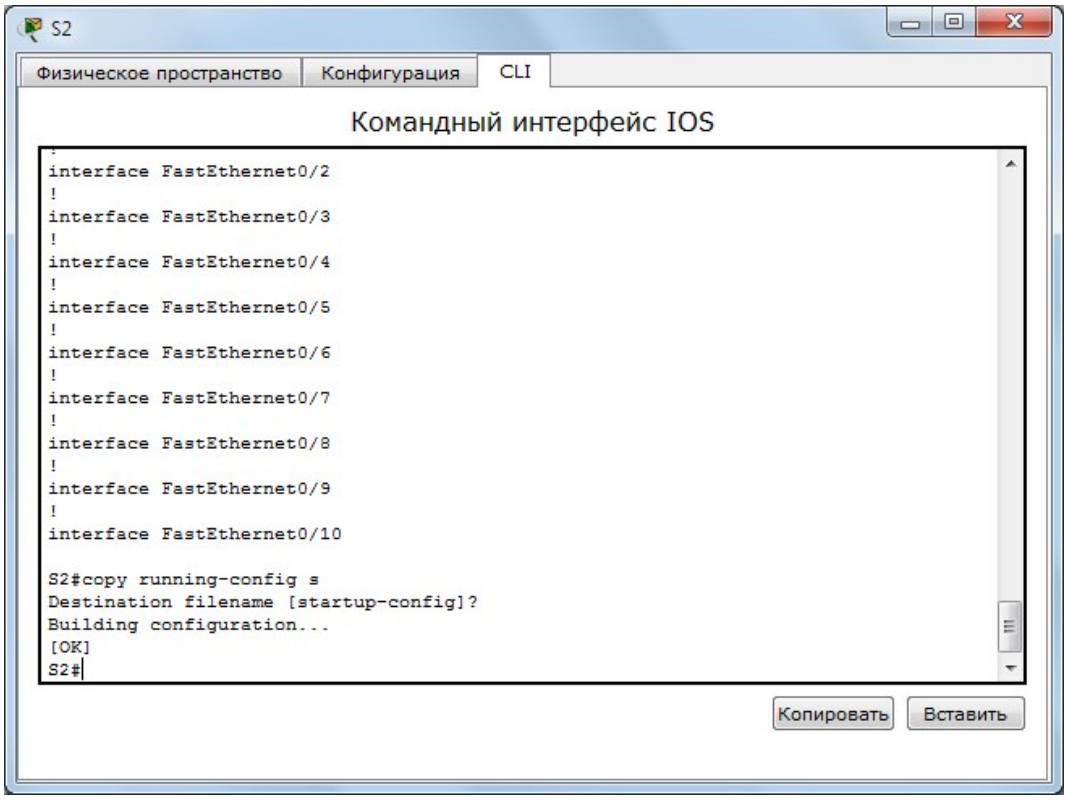

Рис. 1.20. Сохранение конфигурации

4. 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?