**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.КРАТКАЯ ТЕОРИЯ**

Сетевой коммутатор (жарг. свитч, свич от англ. switch — переключатель) — устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети. Коммутатор работает на канальном (втором) уровне модели OSI. Коммутаторы были разработаны с использованием мостовых технологий и часто рассматриваются как многопортовые мосты. Для соединения нескольких сетей на основе сетевого уровня служат маршрутизаторы (3 уровень OSI).

В отличие от концентратора (1 уровень OSI), который распространяет трафик от одного подключённого устройства ко всем остальным, коммутатор передаёт данные только непосредственно получателю (исключение составляет широковещательный трафик всем узлам сети и трафик для устройств, для которых неизвестен исходящий порт коммутатора). Это повышает производительность и безопасность сети, избавляя остальные сегменты сети от необходимости (и возможности) обрабатывать данные, которые им не предназначались.

Принцип работы коммутатора. Коммутатор хранит в памяти (т.н. ассоциативной памяти) таблицу коммутации, в которой указывается соответствие MAC-адреса узла порту коммутатора. При включении коммутатора эта таблица пуста, и он работает в режиме обучения. В этом режиме поступающие на какой-либо порт данные передаются на все остальные порты коммутатора. При этом коммутатор анализирует фреймы (кадры) и, определив MAC-адрес хоста-

отправителя, заносит его в таблицу на некоторое время. Впоследствии,

если на один из портов коммутатора поступит кадр, предназначенный для хоста, MACадрес которого уже есть в таблице, то этот кадр будет передан

только через порт, указанный в таблице. Если MAC-адрес хостаполучателя не ассоциирован с каким-либо портом коммутатора, то кадр будет отправлен на все порты, за исключением того порта, с которого он был получен. Со временем коммутатор строит таблицу для всех активных MAC-адресов, в результате трафик локализуется.

Стоит отметить малую латентность (задержку) и высокую скорость пересылки на каждом порту интерфейса.

Режимы коммутации. Существует три способа коммутации. Каждый из них — это комбинация таких параметров, как время ожидания и надёжность передачи.

* С промежуточным хранением (Store and Forward). Коммутатор читает всю информацию в кадре, проверяет его на отсутствие ошибок, выбирает порт коммутации и после этого посылает в него кадр.
* Сквозной (cut-through). Коммутатор считывает в кадре только адрес назначения и после выполняет коммутацию. Этот режим уменьшает задержки при передаче, но в нём нет метода обнаружения ошибок.
* Бесфрагментный (fragment-free) или гибридный. Этот режим является модификацией сквозного режима. Передача осуществляется после фильтрации фрагментов коллизий (первые 64 байта кадра анализируются на наличие ошибки и при её отсутствии кадр обрабатывается в сквозном режиме).

Задержка, связанная с «принятием коммутатором решения», добавляется к времени, которое требуется кадру для входа на порт коммутатора и выхода с него, и вместе с ним определяет общую задержку коммутатора.

Буфер памяти. Для временного хранения фреймов и последующей их отправки по нужному адресу коммутатор может использовать буферизацию. Буферизация может быть также использована в том случае, когда порт пункта назначения занят. Буфером называется область памяти, в которой коммутатор хранит передаваемые данные.

Буфер памяти может использовать два метода хранения и отправки фреймов: буферизация по портам и буферизация с общей памятью. При буферизации по портам пакеты хранятся в очередях (queue), которые связаны с отдельными входными портами. Пакет передаётся на выходной порт только тогда, когда все фреймы, находившиеся впереди него в очереди, были успешно переданы. При этом возможна ситуация, когда один фрейм задерживает всю очередь из-за занятости порта его пункта назначения. Эта задержка может происходить даже в том случае, когда остальные фреймы могут быть переданы на открытые порты их пунктов назначения.

При буферизации в общей памяти все фреймы хранятся в общем буфере памяти, который используется всеми портами коммутатора. Количество памяти, отводимой порту, определяется требуемым ему количеством. Такой метод называется динамическим распределением буферной памяти. После этого фреймы, находившиеся в буфере, динамически распределяются по выходным портам. Это позволяет получить фрейм на одном порте и отправить его с другого порта, не устанавливая его в очередь.

Коммутатор поддерживает карту портов, в которые требуется отправить фреймы. Очистка этой карты происходит только после того, как фрейм успешно отправлен.

Поскольку память буфера является общей, размер фрейма ограничивается всем размером буфера, а не долей, предназначенной для конкретного порта. Это означает, что крупные фреймы могут быть переданы с меньшими потерями, что особенно важно при асимметричной коммутации, то есть, когда порт с шириной полосы пропускания 100 Мб/с должен отправлять пакеты на порт 10 Мб/с.

Возможности и разновидности коммутаторов. Коммутаторы подразделяются на управляемые и неуправляемые (наиболее простые).

Более сложные коммутаторы позволяют управлять коммутацией на сетевом (третьем) уровне модели OSI. Обычно их именуют соответственно, например, «Layer 3 Switch» или сокращенно «L3 Switch». Управление коммутатором может осуществляться посредством Web-интерфейса, интерфейса командной строки (CLI), протокола SNMP, RMON и т. п.

Многие управляемые коммутаторы позволяют настраивать дополнительные функции: VLAN, QoS, агрегирование, зеркалирование. Многие коммутаторы уровня доступа обладают такими расширенными возможностями, как сегментация трафика между портами, контроль трафика на предмет штормов, обнаружение петель, ограничение количества изучаемых macадресов, ограничение входящей/исходящей скорости на портах, функции списков доступа и т.п.

Сложные коммутаторы можно объединять в одно логическое устройство — стек — с целью увеличения числа портов. Например, можно объединить 4 коммутатора с 24 портами и получить логический коммутатор с 90 ((4\*24)-6=90) портами либо с 96 портами (если для стекирования используются специальные порты).

**2. ХОД РАБОТЫ**

**2.1.** **ПРОВЕРКА КОНФИГУРАЦИИ КОММУТАТОРА ПО УМОЛЧАНИЮ**

* 1. **Проверка конфигурации коммутатора по умолчанию.**

Шаг 1: Вход в привилегированный режим.

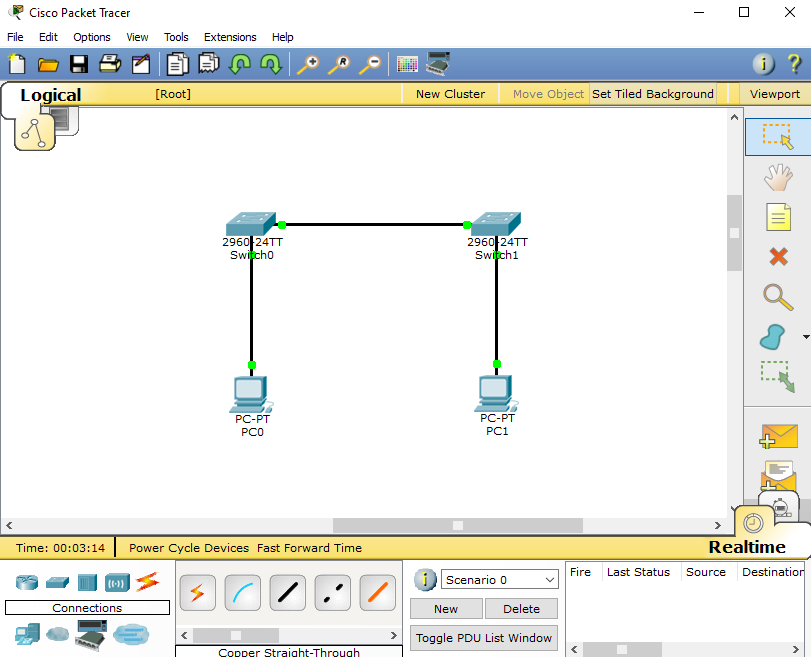


Рисунок 1.1. Топология

Щёлкаем Switch1 и открываем вкладку CLI. Нажимаем клавишу ВВОД. Переходим в привилегированный режим, выполнив команду enable.

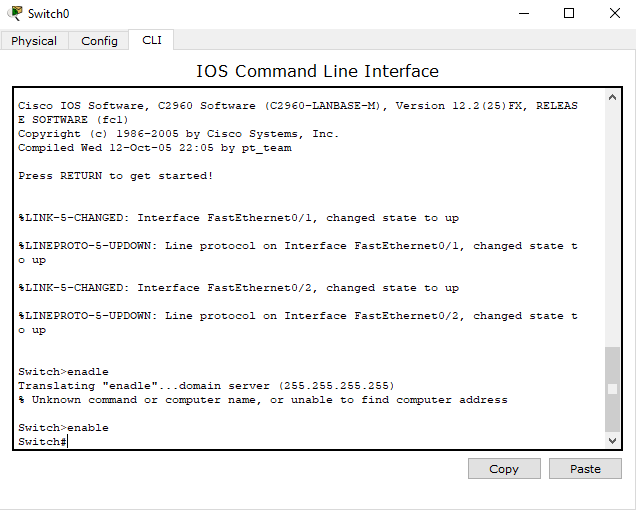


Рисунок 1.2. Вход в привилегированный режим.

Шаг 2: Просматриваем текущую конфигурацию коммутатора.

Выполним команду show running-config.

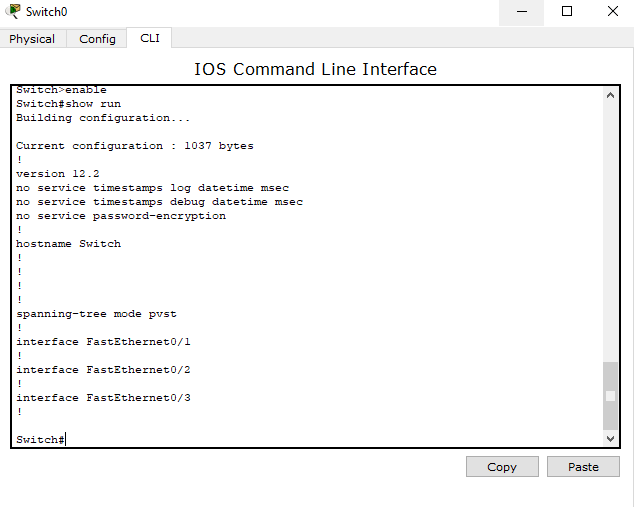


Рисунок 1.3. Команда show running-config.

**2.2 Создание базовой конфигурации коммутатора**

Шаг 1: Назначение коммутатору имени.

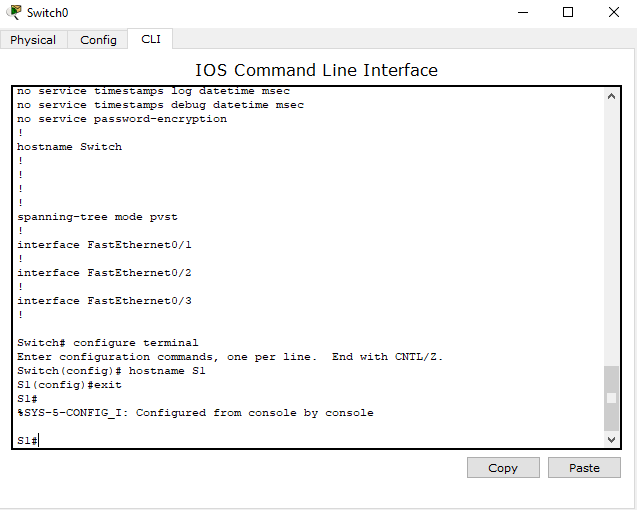


Рисунок 1.4. Назначение коммутатору имени.

Шаг 2: Безопасный доступ к консоли.

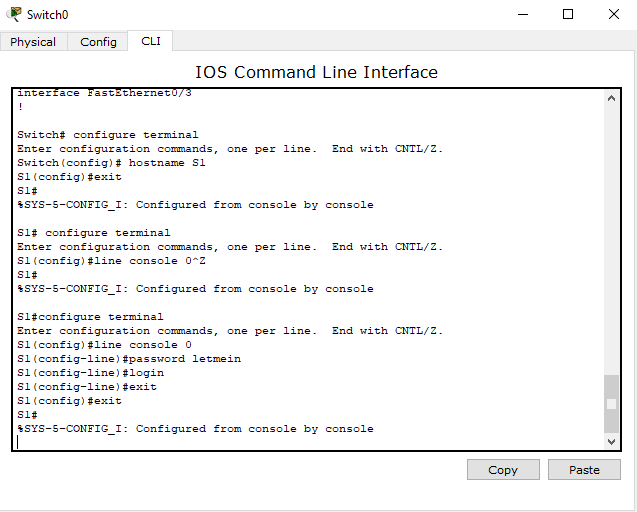


Рисунок 1.5 Безопасный доступ к консоли

Шаг 3: Убедимся что доступ к консоли защищён паролем.

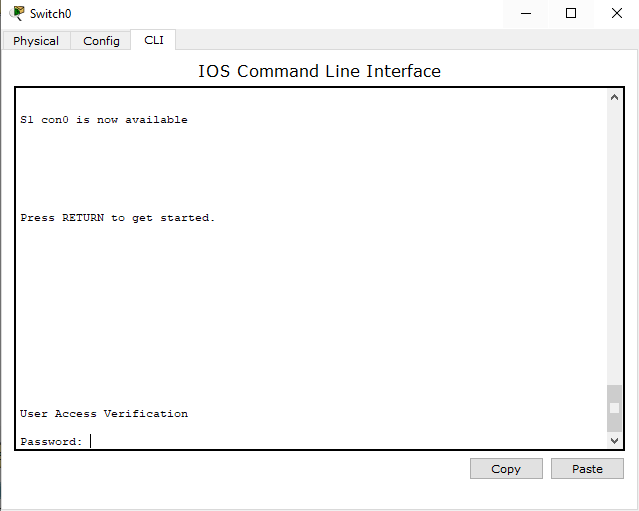


Рисунок 1.6. Проверка доступа к консоли.

Шаг 4: Безопасный доступ в привилегированном режиме.

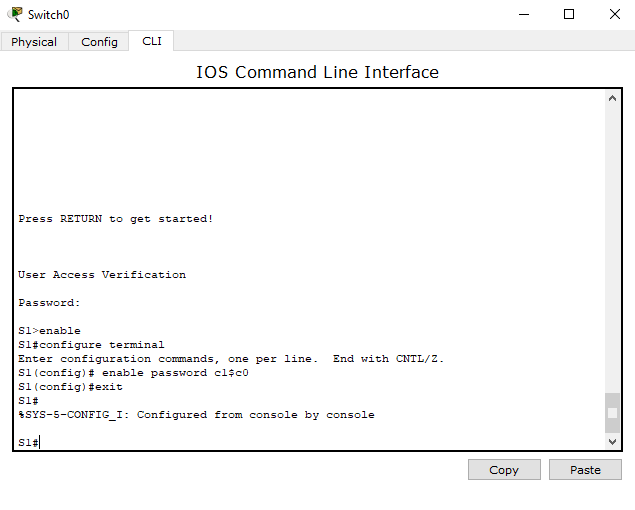


Рисунок 1.7. Установка пароля для привилегированного режима.

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. 1.8).

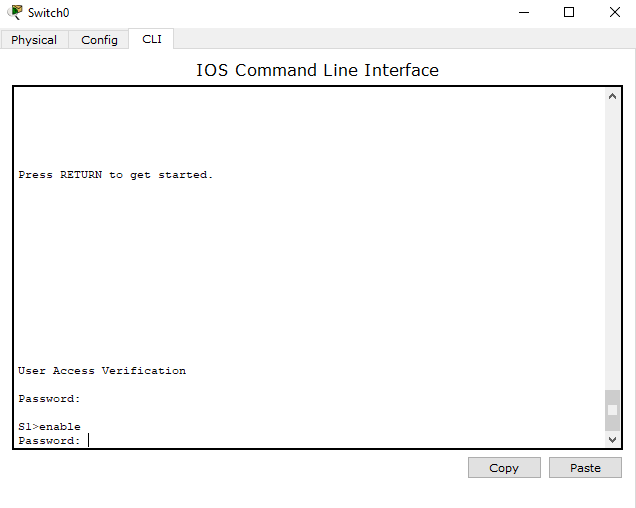


Рис. 1.8. Ввод пароля для входа в привилегированный режим

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

S1# show running-config

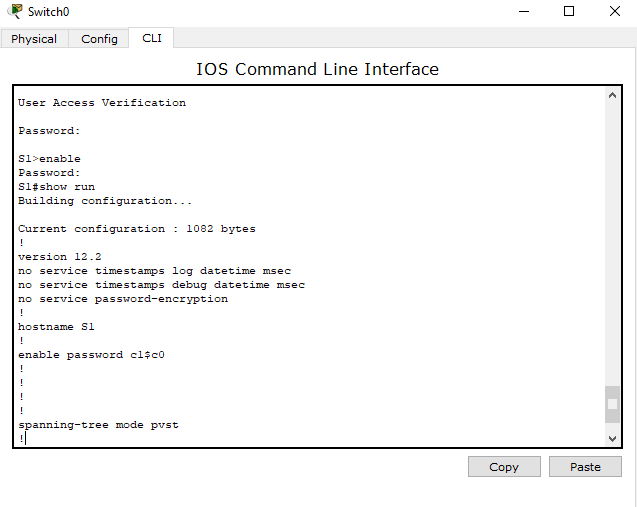


Рис. 1.9. Проверка конфигурации

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. 1.10).

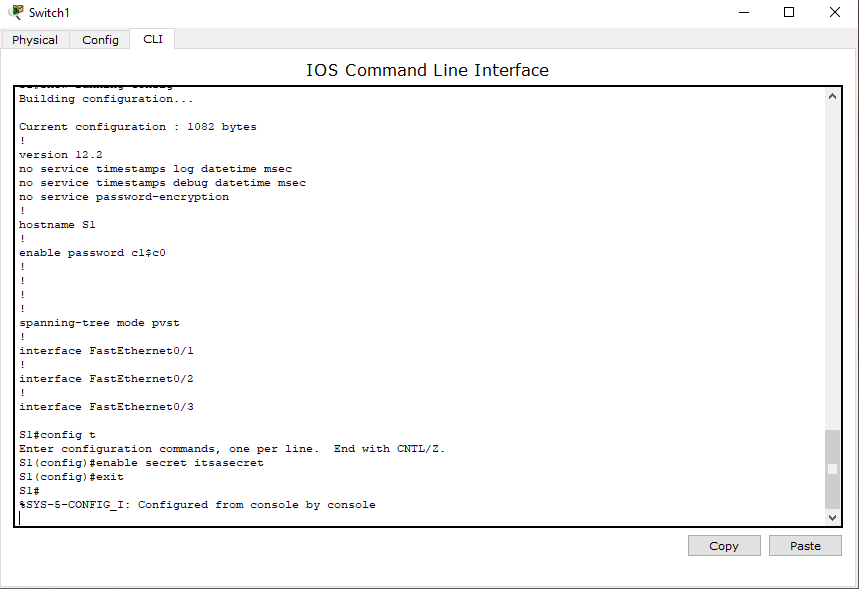


Рис. 1.10. Замена пароля на зашифрованный пароль

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).

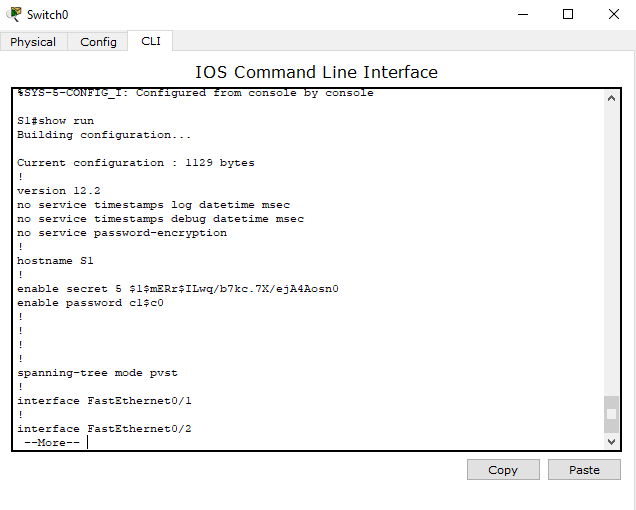


Рис. 1.11. Проверка зашифрованного пароля

Шаг 8: Шифрование паролей для консоли и привилегированного режима.

Сейчас мы зашифруем эти открытые пароли с помощью команды service password-encryption (рис. 1.12).

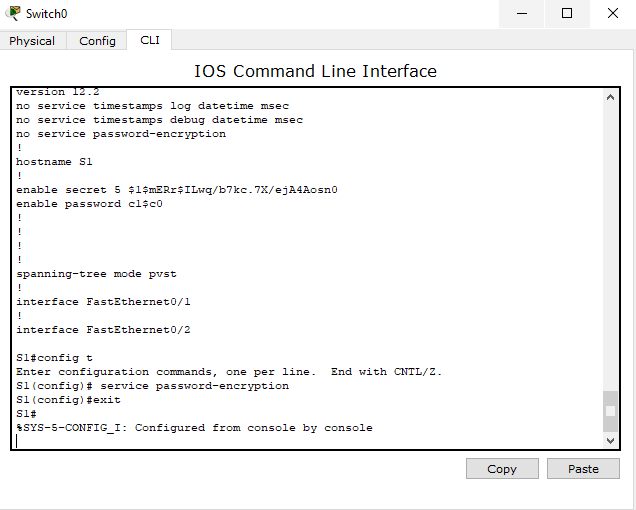


Рис. 1.12. Шифрование паролей

**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).

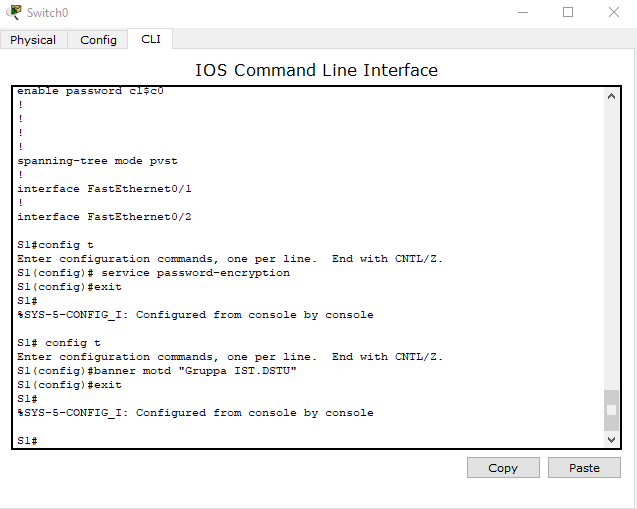


Рис. 1.13. Настройка сообщения ежедневного баннера MOTD

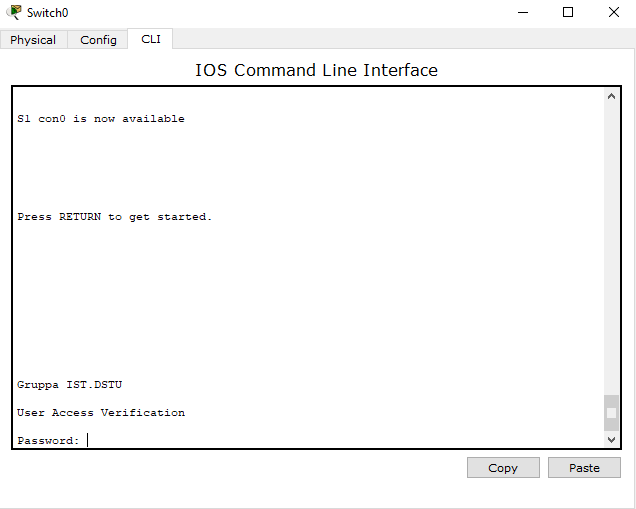


Рис. 1.14. Отображение ежедневного баннера MOTD

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

**2.4. СОХРАНЕНИЕ ФАЙЛОВ КОНФИГУРАЦИИ В NVRAM**

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

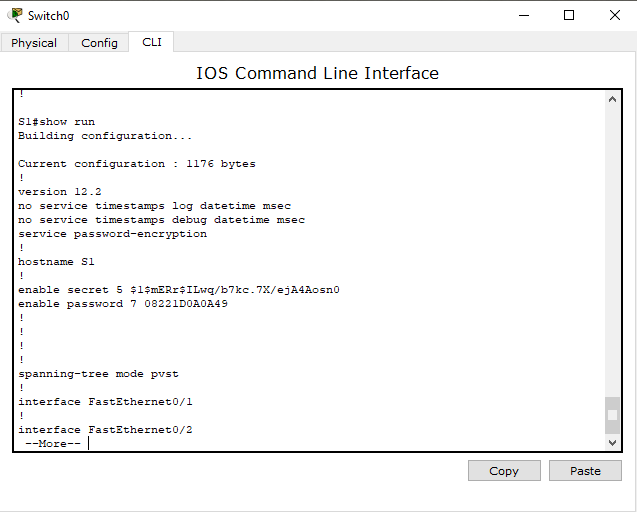


Рис. 1.15. Проверка правильности конфигурации

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]

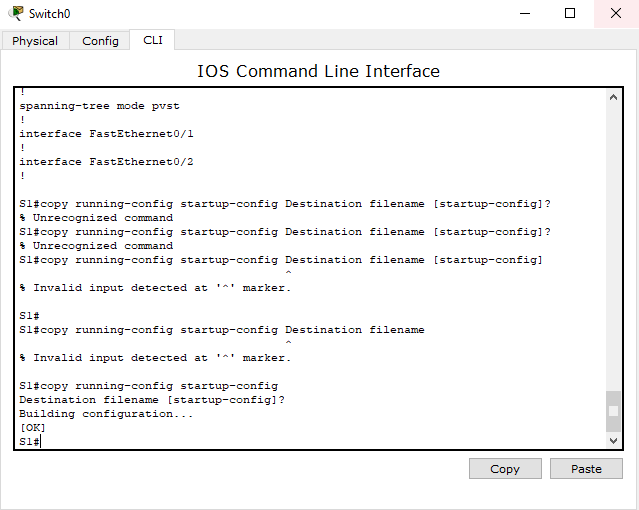


Рис. 1.16. Резервное копирование файла конфигурации в NVRAM

Какова самая короткая версия команды copy running-config startup-config? *copy running-config s* (рис. 1.17)

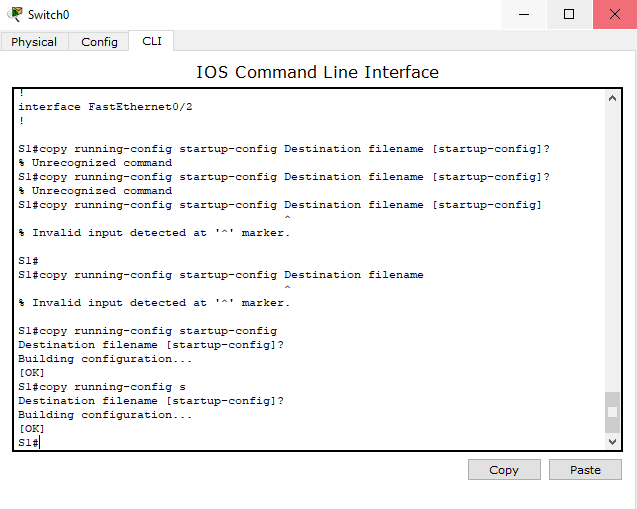


Рис. 1.17. Самая короткая версия команды copy running-config startupconfig

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

S1# show run

*Все 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.

Имя устройства: S2 (рис. 1.18).

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

Устанавливаем для привилегированного режима пароль

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

Вводим следующее сообщение для пользователей,

выполняющих вход в систему на коммутаторе:

«Gruppa IST.DSTU» (рис. 1.18).

Зашифровываем все открытые пароли (рис. 1.18).

Проверяем правильность конфигурации (рис. 1.19).

Сохраняем файл конфигурации, чтобы предотвратить его

потерю в случае отключения питания коммутатора (рис. 1.20).

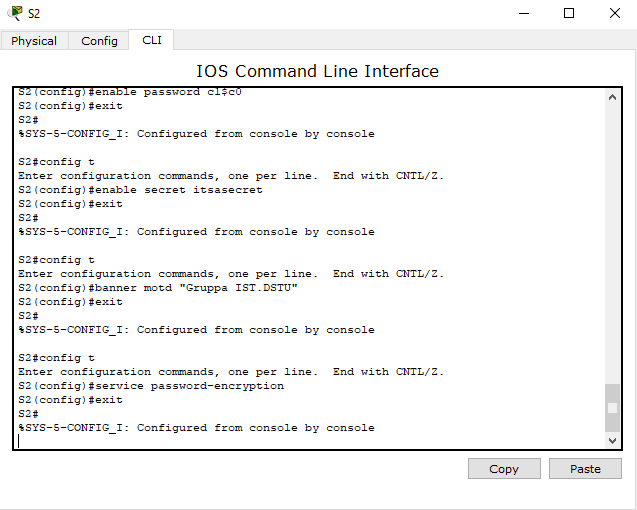


Рис. 1.18. Конфигурирование коммутатора S2

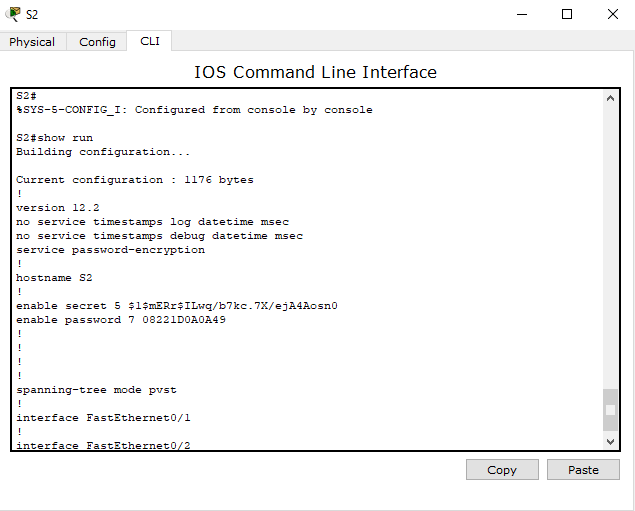


Рис. 1.19. Проверка правильности конфигурации

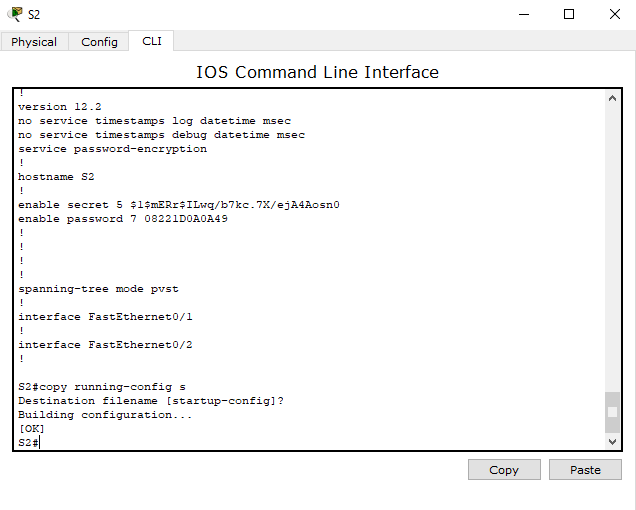


Рис. 1.20. Сохранение конфигурации

**3. 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?