**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.

**Краткая теория**

Сетевой коммутатор (от англ. switch — переключатель) — устройство 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, который распространяет трафик от одного подключённого устройства ко всем остальным, коммутатор передаёт данные только непосредственно получателю (исключение - 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») 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.

Коммутатор анализирует фреймы (кадры) и, определив MAC-адрес

хоста-отправителя, заносит его в таблицу на время. Если на один из портов коммутатора поступит кадр, предназначенный для хоста, MAC-адрес которого уже есть в таблице, то он будет передан только через порт, указанный в таблице. Если MAC-адрес хоста-получателя 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 - 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 использована и в случае, когда порт пункта назначения занят. Буфер – это область памяти, в которой коммутатор хранит передаваемые данные. Буфер может использовать два метода хранения и отправки фреймов: по портам и 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. Возможна ситуация, когда один фрейм задерживает всю очередь из-за занятости порта его пункта назначения. 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. Этот 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 , 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).

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. Они обладают такими расширенными возможностями, как сегментация трафика между портами, контроль трафика на предмет штормов, обнаружение петель, ограничение количества изучаемых mac-адресов, 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).

ХОД РАБОТЫ

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 создала топологию, представленную на рис. 1

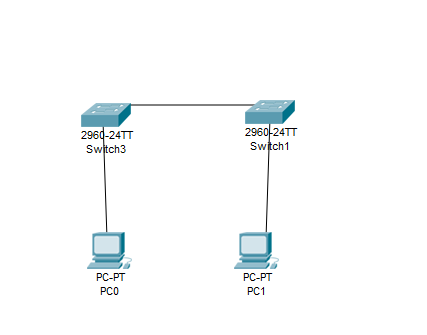


Рис. 1. Топология

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

a. Щёлкнула Switch1 и открываем вкладку CLI. Нажала клавишу ВВОД.

b. Перешла в привилегированный режим, выполнив команду enable

Switch> enable

Switch#

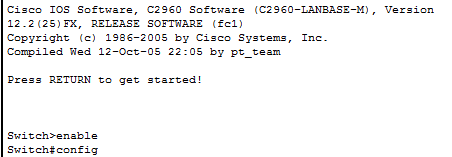


Рис. 2. Вход в привилегированный режим

Шаг 2: Просматривала текущую конфигурацию коммутатора.

a. Выполняем команду show running-config

Switch# show running-config

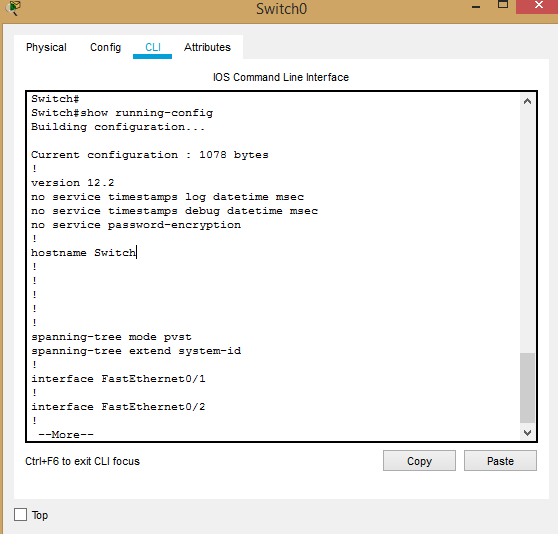


Рис. 1.3. Команда show running-config

b. Ответила на вопросы.

Сколько у маршрутизатора интерфейсов FastEthernet? 24

Сколько у маршрутизатора интерфейсов Gigabit Ethernet? 2

Каков диапазон значений, отображаемых в vty-линиях? 0-4, 5-15

Какая команда отображает текущее содержимое NVRAM?

Switch# show startup-config

startup-config is not present

Почему коммутатор отвечает сообщением startup-config is not present? Потому что файл конфигурации не сохранён в памяти

2. Создание базовой конфигурации коммутатора

Шаг 1: Назначение коммутатору имени.

Для настройки параметров коммутатора, возможно, потребуется переключаться между режимами настройки.

Switch# configure terminal

Switch(config)# hostname S1

S1(config)# exit

S1#

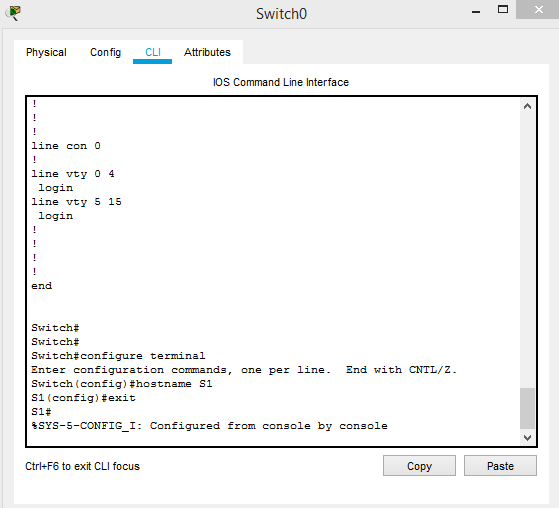


Рис. 4. Назначение коммутатору имени

Шаг 2: Безопасный доступ к консоли.

Для обеспечения безопасного доступа к консоли перешла в режим config-line и установила для консоли пароль letmein

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.

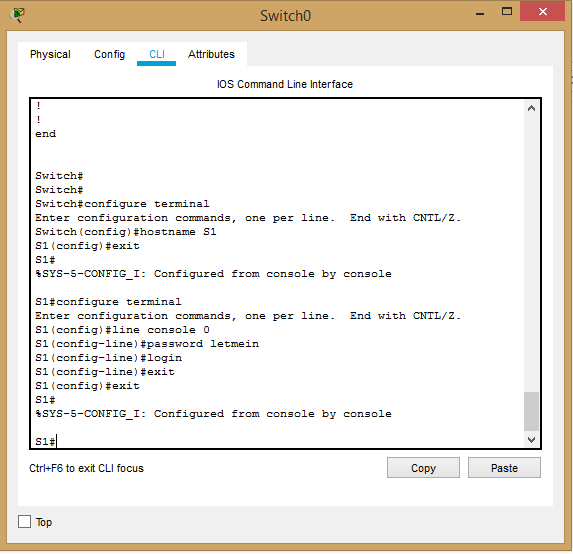


Рис. 1.5. Безопасный доступ к консоли

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

Выхшла из привилегированного режима, чтобы убедиться, что для консольного порта установлен пароль

S1# exit

Switch con0 is now available

Press RETURN to get started

User Access Verification

Password:

S1>

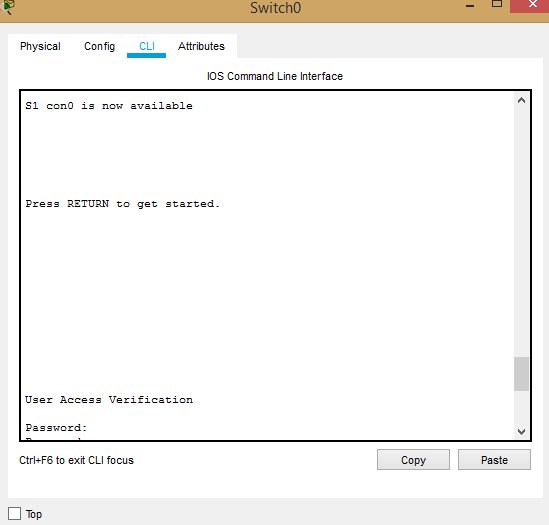


Рис. 6. Проверка доступа к консоли

Шаг 4: Безопасный доступ в привилегированном режиме.

Установила для enable пароль c1$c0. Этот пароль ограничивает доступ к привилегированному режиму

S1> enable

S1# configure terminal

S1(config)# enable password c1$c0

S1(config)# exit

%SYS-5-CONFIG\_I: Configured from console by console

S1#

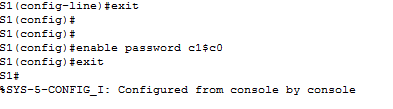


Рис. 7. Установка пароля для привилегированного режима

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

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

b. Нажала 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. Ввела этот пароль, чтобы вернуться в пользовательский режим.

d. Ввела команду для доступа к привилегированному режиму.

e. Ввела второй пароль, который был задан для ограничения доступа к привилегированному режиму



Рис. 8. Ввод пароля для входа в привилегированный режим

f. Проверяем конфигурацию, изучив содержимое файла running-configuration

S1# show running-config

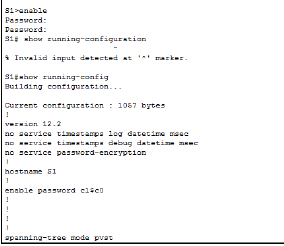


Рис. 9. Проверка конфигурации

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. Устанавила для команды «enable» пароль itsasecret

S1# config t

S1(config)# enable secret itsasecret

S1(config)# exit

S1#

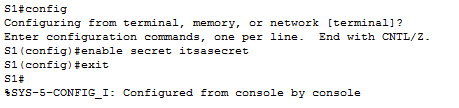


Рис. 10. Замена пароля на зашифрованный пароль

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

a. Ввела команду show running-config ещё раз, чтобы проверить новый пароль enable secret

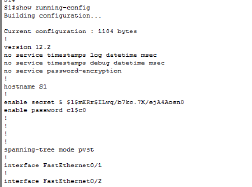


Рис. 11. Проверка зашифрованного пароля

b. Что отображается при выводе пароля enable secret?

$1$mERr$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. Зашифровала эти открытые пароли с помощью команды service password-encryption

S1# config t

S1(config)# service password-encryption

S1(config)# exit

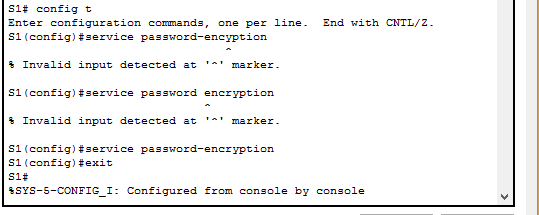


Рис. 12. Шифрование паролей

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.

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

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. 13. Настройка сообщения ежедневного баннера MOTD

Когда будет отображаться этот баннер?

После ввода пароля и входа в консоль коммутатора



Рис.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»

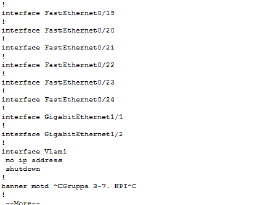


Рис. 15. Проверка правильности конфигурации

Шаг 2: Сохраняем файл конфигурации.

Завершила базовую настройку коммутатора,затем выполнила резервное копирование файла конфигурации в NVRAM и проверила, чтобы внесённые изменения не потерялись после перезагрузки системы и отключения питания

S1# copy running-config startup-config

Destination filename [startup-config]?[Enter]

Building configuration...

[OK]

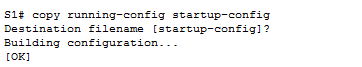


Рис16. Резервное копирование файла конфигурации в NVRAM

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



Рис. 17. Самая короткая версия команды

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

Завершила настройку коммутатора S1,затем настроила коммутатор S2.

Настроила для коммутатора S2 следующие параметры.

a. Имя устройства: S2

b. Защитила доступ к консоли паролем letmein

c. Установила для привилегированного режима пароль c1$c0 и задала пароль «enable secret» для itsasecret

d. Ввела сообщение для пользователей, выполняющих вход в систему на коммутаторе:

«Gruppa 3-7. NPI»

d. Зашифровала все открытые пароли

e. Проверила правильность конфигурации

f. Сохранила файл конфигурации, чтобы предотвратить его потерю в случае отключения питания коммутатора

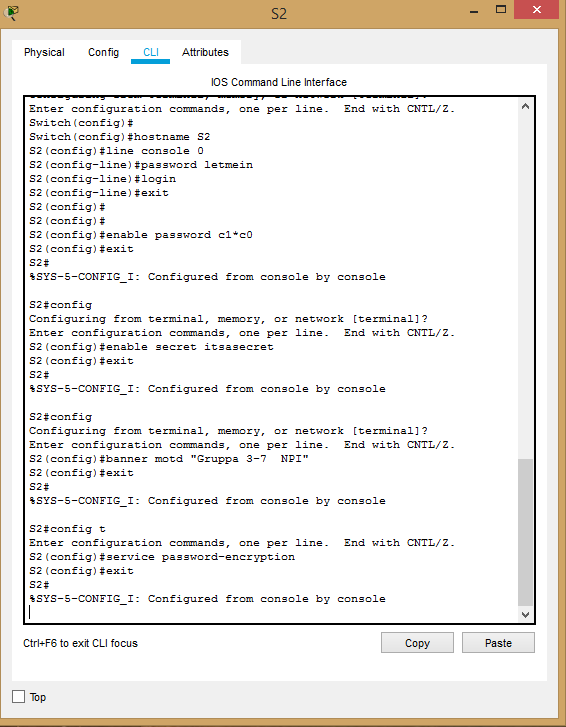


Рис. 1.18. Конфигурирование коммутатора S2

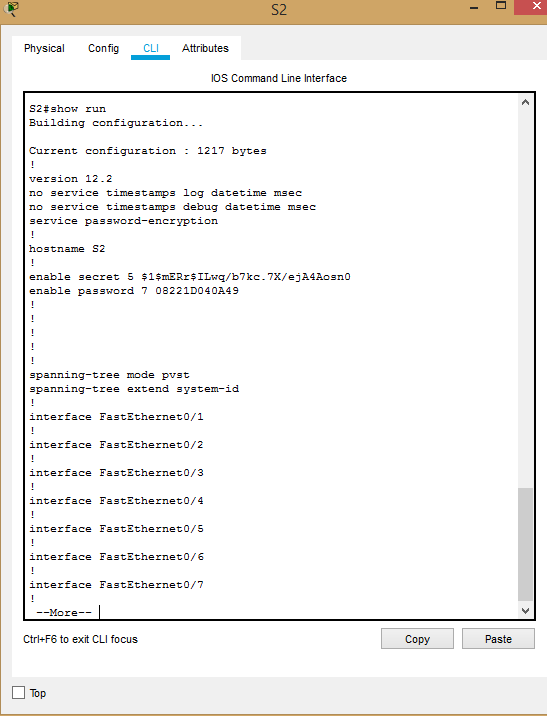


Рис. 1.19. Проверка правильности конфигурации

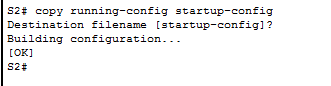


Рис. 1.20. Сохранение конфигурации

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?