Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина» (УрФУ)

Институт радиоэлектроники и информационных технологий – РтФ

Школа профессионального и академического образования

Отчет по дисциплине   
«Безопасность компьютерных сетей»

Лабораторная работа №5  
«Знакомство с операционной системой *IOS* и

симулятором *Cisco* *Packet* *Tracer*»

Студенты: Клоченко И.Е., Юсупов Д.А.

Преподаватель: Ваулин С.С.

Группа: РИ-300024

Екатеринбург

2023

**Оглавление**

[1. Моделирование простой сети 3](#_Toc134392540)

[2. Операционная система Cisco IOS 9](#_Toc134392541)

[3. Создание локальных пользователей 11](#_Toc134392542)

[4. Настройка удаленного доступа 14](#_Toc134392543)

[5. Дополнительные инструменты 16](#_Toc134392544)

[Вывод 20](#_Toc134392545)

**Цель работы:**

Знакомство с ОС *IOS* (*CLI*) и симулятором *CPT* (*Cisco* *Packet* *Tracer*).

**Ход работы:**

## Моделирование простой сети

* 1. Запускаем *CPT* (установлен *CPT* версии 8.2.1.0118).
  2. Найдем характеристики коммутатора *Cisco* *Catalyst* 2960-24*TT*:

Число портов 10/100: 24

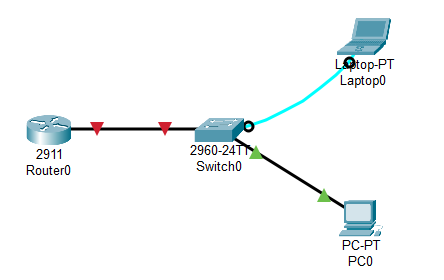
Число портов 10/100/1000: 2

Максимум *VLAN*: 64

Пропускная способность Гбит/сек: 8,8

Максимум *MAC* адресов: 8000

* 1. Собираем топологию сети, аналогичную рисунку 3 в методических указаниях.



**Рисунок 1**. Собранная топология сети

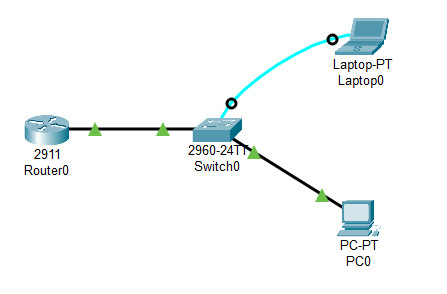
При сборке топологии сети использовались связи:

Коммутатор – Лаптоп: *Console* – *RS*-232 – консольный кабель

Коммутатор – ПК: *FastEthernet*0/1 – *FastEthernet* 0 – сетевой кабель

Маршрутизатор – Коммутатор: *GigabitEthernet*0/0 – *GigabitEthernet*0/1 – сетевой кабель.

* 1. Переходим в *CLI* устройства *Router*0. Переходим в пользовательский режим, отказываясь от запуска конфигурационного диалога. Переходим в режим конфигурации интерфейса для *Switch*0. Включаем интерфейс и присваиваем *IP* адрес 192.168.0.1 с маской 255.255.255.0. После этого рабочая область приняла следующий вид:



**Рисунок 2**. Топология сети после включения маршрутизатора и присвоения ему адреса

Первой командой мы перевели статус порта *Gib*0/0 в *Up*, что означает что мы включили интерфейс и включили линейный протокол для интерфейса. Визуально изменились «треугольники» на проводе подключения маршрутизатор-коммутатор на зеленые, были красные.

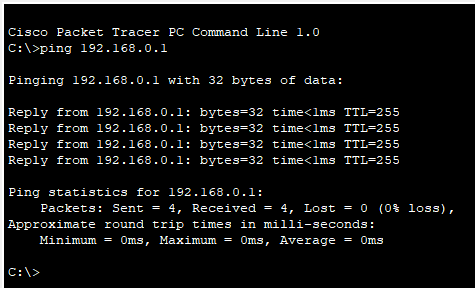
* 1. Возвращаемся в режим глобальной конфигурации. Назначаем имя маршрутизатору. После этого приглашение строки изменилось: начало приглашения сменилось на установленное нами имя.



**Рисунок 3**. Назначение имени маршрутизатору

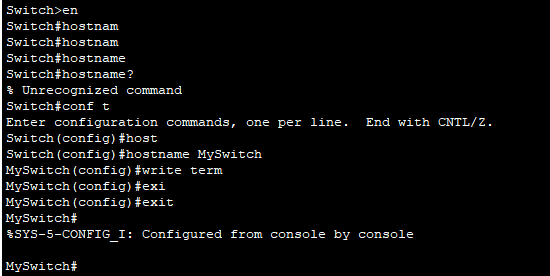
Меняем имя маршрутизатора в рабочей области на то же, что мы указали в *CLI*.

* 1. Открываем конфигурацию *IP* для *PC*0. Устанавливаем статический *IP* адрес 192.168.0.2/24. Затем переходим в командную строку (*Command* *promt*). Выполняем эхо-тестирование маршрутизатора.

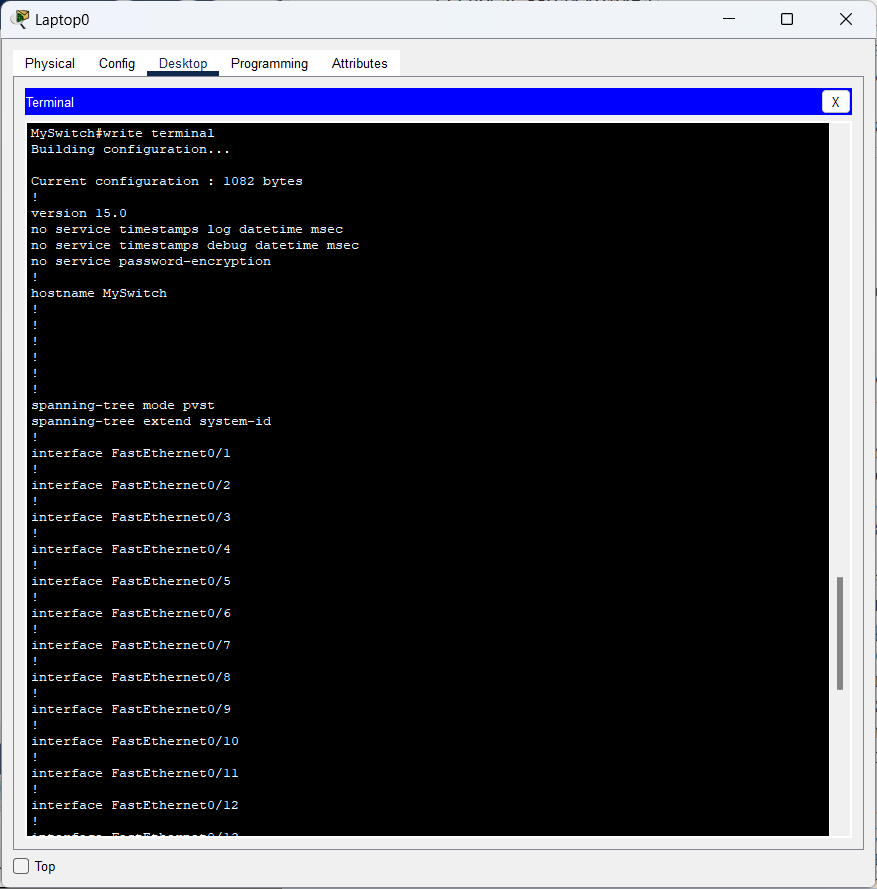


**Рисунок 4**. Эхо-тестирование маршрутизатора после установки статического адреса для ПК

* 1. Переходим в терминал на *Laptop*. Присваиваем имя *MySwitch* коммутатору.

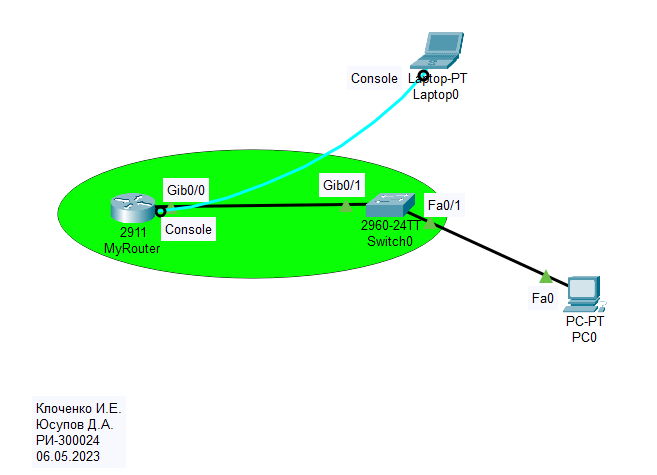


**Рисунок 5**. Присвоение имени коммутатору



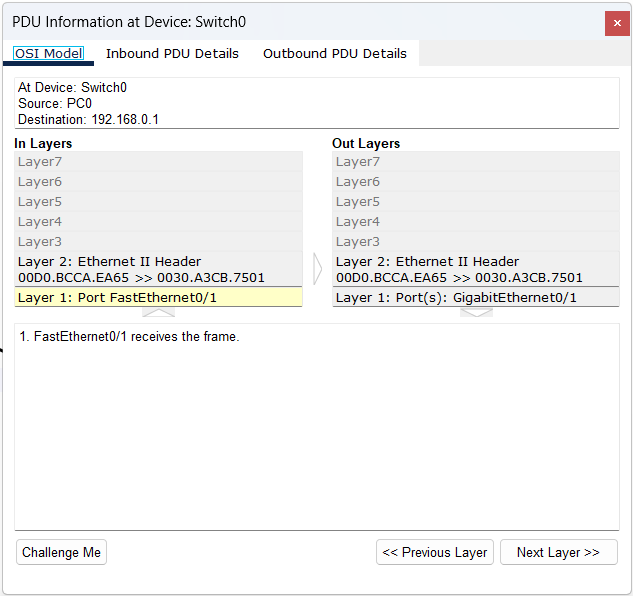
**Рисунок 6**. Сохранение настроек

* 1. Удаляем консольное подключение от ПК к коммутатору и прокладываем новое консольное подключение от ПК к маршрутизатору. Изменилось приглашение на *MyRouter* и отобразилась история команд для маршрутизатора, которые мы вводили ранее.
  2. Подпишем названия интерфейсов на концах каждой линии связи. Также добавим надпись с ФИО участников бригады, номер группы и текущую дату. Визуально отделим маршрутизатор и коммутатор от клиентских устройств.

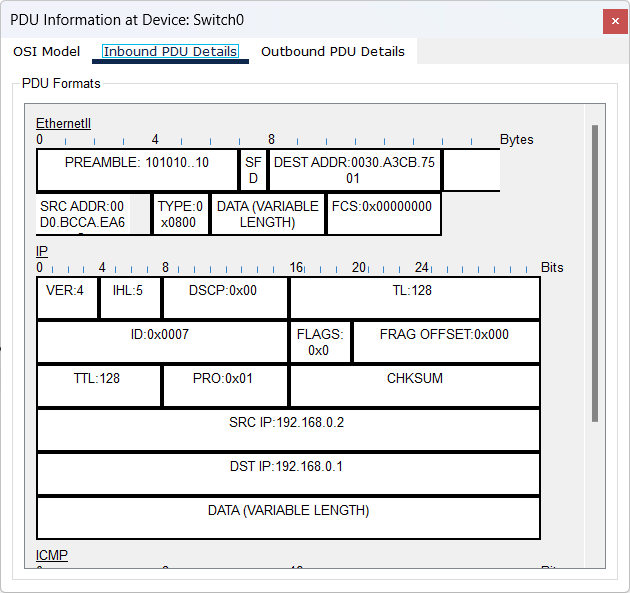


**Рисунок 7**. Визуальные модификации в топологии сети

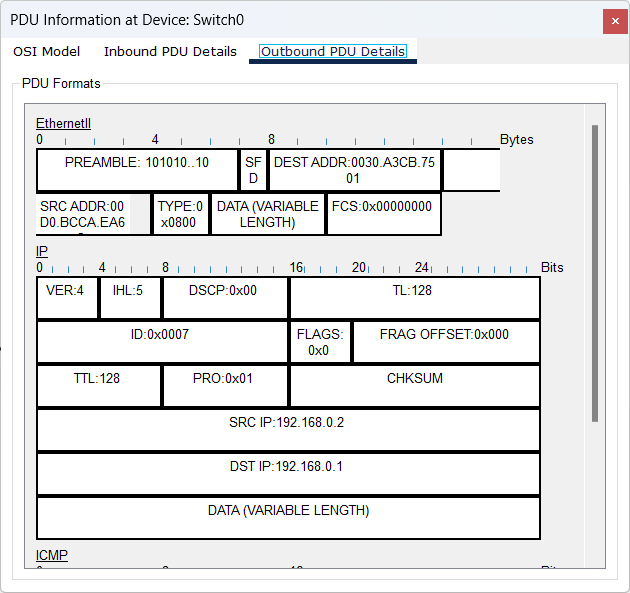
* 1. Переключаем систему в режим пошаговой симуляции. Выставляем в фильтрах для *IPv*4 *ICMP*. Выполняем эхо-тестирование от *Router*0 от *PC*0. Наблюдаем обмен пакетами. Выбираем случайный пакет и просматриваем его содержимое (параметры).



**Рисунок 8**. Параметр OSI Model



**Рисунок 9**. Параметр Inbound PDU Details



**Рисунок 10**. Параметр Outbound PDU Details

* 1. Сохраняем файл проекта. Файл проекта имеет расширение .*pkt* и размер 43,5 КБ.
  2. Выполняем перезагрузку сети. Пробуем провести эхо-тестирование *Route*0 от *PC*0. Это-тестирование завершается неудачей, потому что все те настройки, которые мы указывали для маршрутизатора не были сохранены и после перезагрузки сети они «слетели», что дало неудачу при эхо-тестировании. Избежать этого можно сохранив настройки в память (*write* *memory*) для маршрутизатора при последующей настройке.

## Операционная система Cisco IOS

* 1. Подключаемся к консоли маршрутизатора *Router*0. Заходим в привилегированный режим и выполняем команду «*show* *version*».

В ее выводе получаем:

* + - *Version* 15.1(4)*M*4 – версия программного обеспечения.
    - *flash*0:*c*2900-*universalk*9-*mz*.*SPA*.151-1.*M*4.*bin* – файл образа ОС.
    - С2900 – модель маршрутизатора
    - *cisco*2911 *uptime* *is* 9 *minutes*, 25 *seconds* – время, прошедшее с загрузки
  1. Определим, какие носители доступны устройству.
* *WORD* *Directory* *or* *file* *name*
* *flash*0: *Directory* *or* *file* *name*
* *flash*1: *Directory* *or* *file* *name*
* *flash*: *Directory* *or* *file* *name*
* *nvram*: *Directory* *or* *file* *name*
  1. Определим текущую загрузку центрального процессора: 0 %.
  2. Определим команды, доступные в обоих режимах: пользовательском и привилегированном.

Таблица 1. Сравнение набора команд в пользовательском и привилегированном режимах

|  |  |  |  |
| --- | --- | --- | --- |
| Команда | Пользовательский режим | Привилегированный режим | Оба |
| <1-99> | + | + | + |
| *auto* | - | + | - |
| *clear* | - | + | - |
| *clock* | - | + | - |
| *configure* | - | + | - |
| *connect* | + | + | + |
| *copy* | - | + | - |
| *debug* | - | + | - |
| *delete* | - | + | - |
| *dir* | - | + | - |
| *disable* | + | + | + |
| *disconnect* | + | + | + |
| *enable* | + | + | + |
| *erase* | - | + | - |
| *exit* | + | + | + |
| *logout* | + | + | + |
| *mkdir* |  | + | - |
| *more* | - | + | - |
| *no* | - | + | - |
| *ping* | + | + | + |
| *reload* | - | + |  |
| *resume* | + | + | + |
| *show* | + | + | + |
| *ssh* | + | + | + |
| *telnet* | + | + | + |
| *terminal* | + | + | + |
| *traceroute* | + | + | + |
| *undebug* | - | + | - |
| *vlan* | - | + | - |
| *write* | - | + | - |

* 1. Устанавливаем в качестве имени устройства *MyRouter*. Просматриваем текущую и стартовые конфигурации. В текущей конфигурации *hostname* *MyRouter*, а в стартовой – *Router*.
  2. Скопируем текущую конфигурацию в стартовую. Теперь *hostname* в стартовой и текущей конфигурациях принял значение *MyRouter*.

## Создание локальных пользователей

* 1. Создаем двух новых пользователей в *CLI* для *Router*0: первого с использованием слова *secret*, второго с использованием *password*.

Посмотрим появившееся строки в *running*-*config*:



**Рисунок 11**. Отображение созданных пользователей в running-config

Как видим, команды *secret* и *password* ведут себя по разному, хоть и выполняют одну и ту же базовую функцию – создать пароль для пользователя. Разница лишь в том, что *password* записывает в конфигурацию пароль в «чистом» виде, а *secret* записывает хэш пароля, вместо самого пароля.

С точки зрения безопасности, логичнее использовать *secret*, так как если злоумышленник получит доступ к конфигурации, а именно к прочтению, то эксплуатировать явно указанный пароль (*password*) будет и быстрее, и легче, чем хэш пароля (*secret*).

* 1. Попробуем зашифровать пароль, созданный командой *password*.



**Рисунок 12**. Шифрование password пароля



**Рисунок 13**. Отображение зашифрованного пароля в текущей конфигурации

Стоит обратить внимание, что цифры, идущие после слов *password* и *secret* обозначают тип шифрования пароля.

Здесь:

* 0 – это *plain* *text* – открытый незашифрованный пароль
* 5 – *md*5 хэш пароля
* 7 – шифрование от *Cisco* (*Cisco* *Type* 7).
  1. Используя команду *no*, удалим пользователя *looser*.



**Рисунок 14**. Удаление пользователя looser



**Рисунок 15**. Изменения в текущей конфигурации

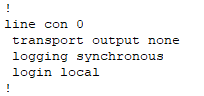
* 1. Переходим в режим конфигурации консольного подключения.

После перехода приглашение стало не *MyRouter*(*config*), а *MyRouter*(*config*-*line*).

Введем команду, указывающую на необходимость аутентификации по локальной базе пользователей при входе через текущую линию *con* 0. Устанавливаем пароль для входа в привилегированный режим (уже в режиме глобальной конфигурации).

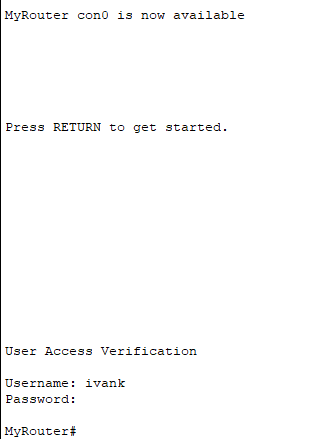
* 1. Отключим оповещение попыток обращения к несуществующему серверу. Также отключим вывод событий системного журнала.

Выполним просмотр текущей конфигурации, не выходя из режима конфигурирования. Итоговая конфигурация консольной линии:



**Рисунок 16**. Текущая конфигурация консольного подключения

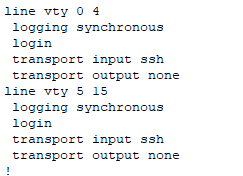
* 1. Завершаем сеанс работы в консоли, предварительно сохранив настройки конфигурации, и войдем в сеанс снова. Нас встречает форма верификации пользователя.



**Рисунок 17**. Аутентификация пользователя ivank

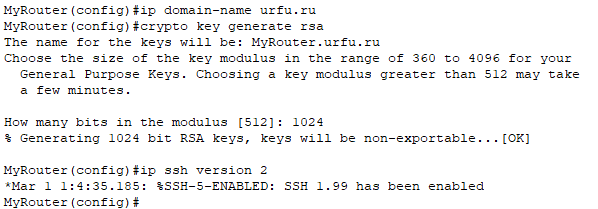
## Настройка удаленного доступа

* 1. На этапе перезагрузки сети и проверки эхо-тестированием маршрутизатора настройки маршрутизатора уже были восстановлены после утраты, поэтому пропускаем этот пункт.
  2. Переходим в контекст настройки линий *VTY*. Вводим команды для настройки локальной аутентификации и отключения исходящих подключений при использовании неправильных команд. Дополнительно указываем в явном виде использование протокола *SSH* для входящих подключений. Итоговая текущая конфигурация виртуальных терминальных линий:



**Рисунок 18**. Текущая конфигурация виртуальных терминальных линий

* 1. Дополнительно к предыдущим настройкам в режиме глобальной конфигурации задаем доменную зону, в которой находится устройство, для нее создаем пару ключей *RSA* и явно указываем используемую версию протокола *SSH*.



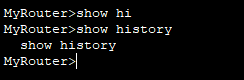
**Рисунок 19**. Дополнительные настройки для SSH подключения

* 1. На рабочем столе *PC*0 запускаем *SSH*/*Telnet* клиент, указываем *IP* адрес маршрутизатора, имя созданного пользователя и подключаемся к устройству. Вводим пароль при подключении.



**Рисунок 20**. Подключение по SSH протоколу

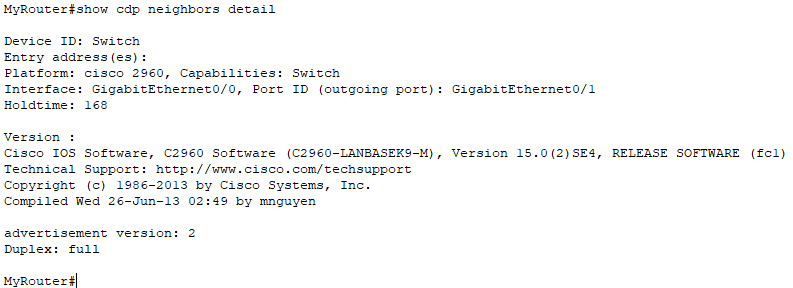
* 1. Проверим журнал ранее введенных команд:



**Рисунок 21**. Журнал ранее введенных команд (при подключении по SSH)

## Дополнительные инструменты

* 1. В привилегированном режиме выполняем команду «*show* *cdp*». Сообщения протокола отправляются с интервалом в 1 минуту. Выведем информацию о соседях:



**Рисунок 22**. Детальная информация о соседях

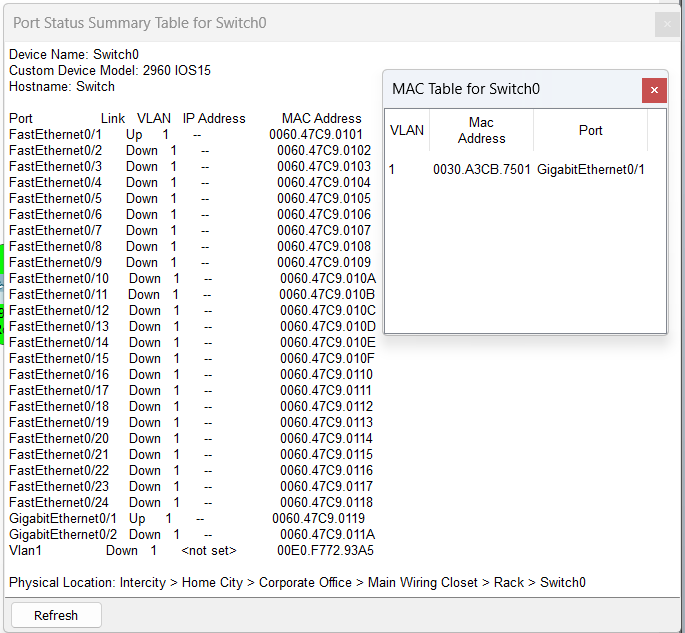
В пользу можно отнести обнаружение соседних устройств (позволяет обмениваться информацией о своем соседстве), получение информации о соседних устройствах (может быть полезно для администратора сети), возможность автоматической настройки путем передачи информации о параметрах и возможностях устройств.

Вредом могут служить то же предоставление информации о соседних устройствах (уязвимость безопасности), перегрузка сети (*CDP* периодически отправляет на соседние устройства сообщения, что может вызвать дополнительный трафик в сети; в условиях сетей с высокой нагрузкой или ограниченной пропускной способностью).

Включение *CDP*: Включение *CDP* обычно имеет смысл, когда требуется получать информацию о соседних устройствах и использовать ее для настройки и мониторинга сети. Например, администраторы сети могут использовать *CDP* для автоматического обнаружения и настройки новых устройств в сети.

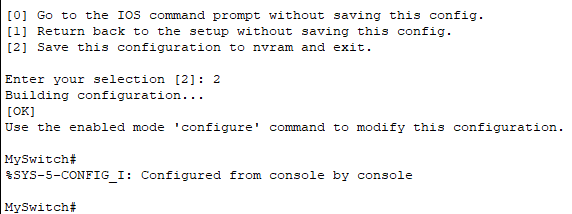
Выключение *CDP*: если в сети есть угроза безопасности или если необходимо ограничить доступ к информации о соседних устройствах; в случаях если трафик ограничен.

* 1. В режиме пошаговой симуляции устанавливаем отслеживание *CDP* пакетов. Тип *Ethernet*-кадра, используемый в *CDP* – 802.3 *SNAP*.
  2. Получим таблицу интерфейсов и таблицу *MAC* адресов для коммутатора, не используя *CLI*.



**Рисунок 23**. Таблица интерфейсов и таблица MAC адресов для коммутатора

* 1. В глобальном режиме консоли коммутатора выполняем команду *setup*. Отвечаем на вопросы мастера начальной настройки.



**Рисунок 24**. Завершение начальной настройки коммутатора

* 1. Перезагружаем коммутатор. Проследим за этапами загрузки устройства. Она состоит из следующих стадий:
* *Bootstrap* *loader*: Загрузчик (*Boot* *Loader*) загружается и инициализируется. В данном выводе загрузчик называется "*C*2960 *Boot* *Loader* (*C*2960-*HBOOT*-*M*) *Version* 12.2(25*r*) *FX*, *RELEASE* *SOFTWARE* (*fc*4)". Он отвечает за поиск и загрузку операционной системы (*Cisco* *IOS*) коммутатора.
* Проверка аппаратных компонентов: Коммутатор выполняет тестирование аппаратных компонентов, таких как процессор, память и порты. В выводе видно успешное прохождение различных тестов, включая тесты регистров *CPU*, памяти и интерфейсов.
* Загрузка *Cisco* *IOS*: Операционная система *Cisco* *IOS* загружается с устройства хранения (*flash*) коммутатора. В данном случае используется *Cisco* *IOS* версии 15.0(2) *SE*4.
* Инициализация *flash*-памяти: происходит инициализация и проверка *flash*-памяти коммутатора. В выводе видно информацию о количестве файлов и свободном месте на *flash*-памяти.
* Проверка обновления загрузчика (*Bootloader* *upgrade*): здесь проверяется необходимость обновления загрузчика. В данном случае обновление загрузчика не требуется.
* Загрузка завершена: В конце вывода видно информацию о коммутаторе, его модели, версии *Cisco* *IOS* и других характеристиках.

## Вывод

В ходе лабораторной работы было проведено знакомство с *Cisco* *Packet* *Tracer* и ОС *IOS*.

Была смоделирована простая сеть из ПК, коммутатора, маршрутизатора и ноутбука с разъемом *RS*-232 для консольного подключения к устройствам.

Проведена базовая настройка коммутатора и маршрутизатора (назначение имен, установление пароля для входа в привилегированный режим, назначение *IP* адресов устройствам).

Проведена процедура создания локальных пользователей для маршрутизатора с использованием «секретного» пароля.

Было настроено консольное подключение с выключением излишнего и неудобного вывода (например, журнала) консоли при вводе команд.

Было настроено удаленное подключение через протокол *SSH*.

Было проведено ознакомление с протоколом *CDP*, а также рассмотрено содержимое пакета *CDP*, рассмотрено назначение этого протокола, выведены плюсы, минусы и условия использования этого протокола (когда включить и когда выключить).

Была проведена начальная настройка коммутатора с помощью мастера начальной настройки.

В целом освоена работа с *CLI* и ОС *IOS* на устройствах.

Просмотрен и проанализирован процесс загрузки устройства, в частности коммутатора.