Лабораторная работа №3. Подключение к сетевому оборудованию

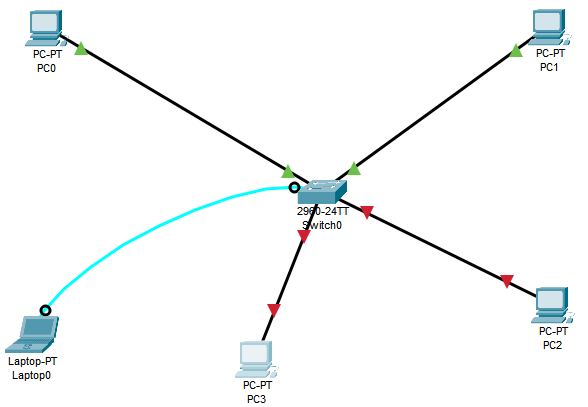
*Сегодня мы начнём осваивать управление коммутаторами Cisco при помощи командной строки.*

*Способы подключения сетевого оборудования:*

* *С помощью консольного кабеля;*
* *По Telnet/SSH;*
* *Web-интерфейс;*
* *Специализированное ПО (SDM, IME, CSM);*

*Для подключения необходимо:*

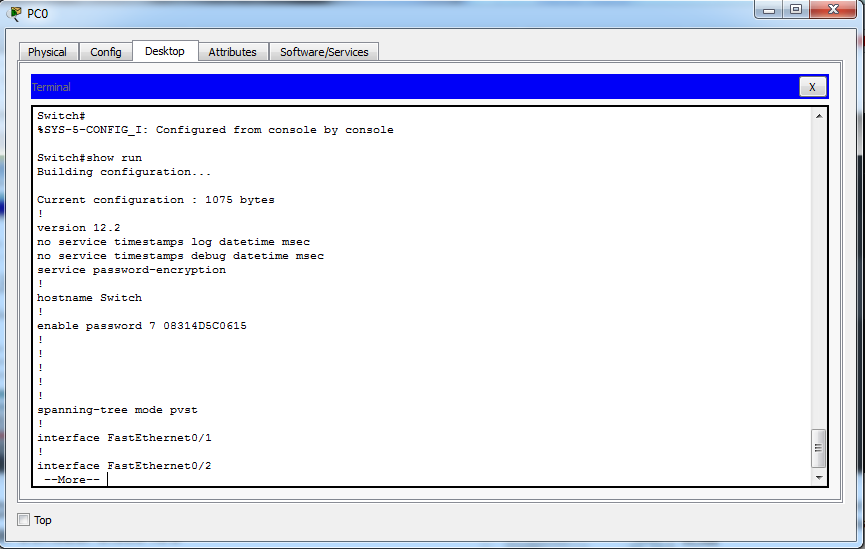
* *Компьютер;*
* *Консольный кабель;*
* *Переходник USB-to-Com;*
* *ПО (Putty/SecureCRT)*



Рассмотрим процесс подключения коммутатора в Cisco Packet Tracer:

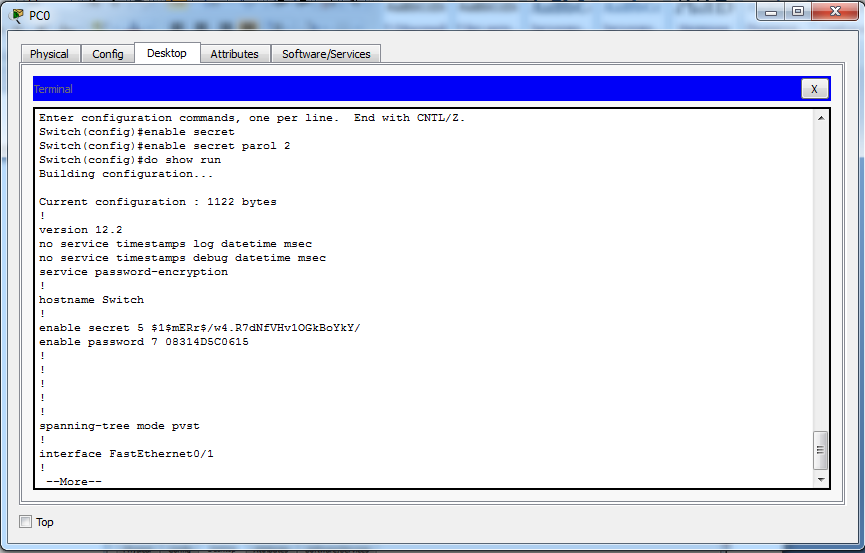
1. Подключаемся по консоли:
   1. Запускаем Cisco Packet Tracer;
   2. В рабочую область добавляем компьютеры, ноутбук и коммутатор (2960). И соединяем консольным кабелем (Console) RS 232-Console. В конфигурации ноутбука выбираем Terminal;
   3. В Terminal заходим в привилегированный режим с помощью команды “enable”.
      1. См. подсказку по командной строке Cisco
   4. Перед настройкой необходимо войти в режим «глобального конфигурирования» с помощью команды «configure terminal».
   5. Первым делом зададим имя коммутатора «hostname sw-03».
2. Управление состоянием портов
   1. Отключить все порты на коммутаторе
   2. Включить порты (индивидуально) в сторону пары рабочих станций
   3. Просмотреть конфигурацию
   4. Сохранить изменения конфигурации
   5. Перезагрузить всё оборудование (Power Cycle)
3. Защита подключения
   1. Для безопасности создадим пароль на вход в привилегированный режим. Набираем enable password sanfran. Вместо sanfran можно ввести свой пароль.
   2. Однако применение enable password не совсем безопасно. Если ввести “show run”, то мы увидим строку «enable password sanfran». Для того чтобы это скрыть сделаем следующее:

* Набираем команду «configure terminal». Затем вводим команду «service password-encryption».
* Выходим из режима конфигурации и вводим команду “show run”. Как видно из рис. 1 пароль зашифрован



*Рисунок 1. Пароль на привилегированный режим с помощью команды «enable password»*

* 1. Второй способ задания пароля:
* Заходим в режим «глобального конфигурирования». Вводим команду «enable secret cisco»;
* Затем выходим из режима конфигурации и вводим команду “show run”. И на рис. 2 видно, что наш второй пароль также зашифрован. При этом приоритет имеет именно этот пароль.



*Рисунок 2. Пароль на привилегированный режим с помощью команды «enable secret»*

1. Создадим пользователя.
   1. Заходим в привилегированный режим «глобального конфигурирования»;
   2. Вводим команду «username admin privilege ?». Выходит значение от 0-15. При 15 пользователю доступны все команды. Здесь admin – имя пользователя. Затем вводим команду «username admin privilege 15 password sanfran». Здесь sanfran[[1]](#footnote-1) – пароль. Локальный пользователь создан.
2. Установим авторизацию на подключение к консоли:
   1. Заходим в режим «конфигурирования терминальных линий». В режиме «глобального конфигурирования» набираем команду «line console 0»
   2. Набираем команду «login local»
   3. Выходим из всех режимов конфигурации с помощью команды «end». Теперь при попытке входа в консоль требуется ввести имя пользователя и пароль, вводим их. Доступ к консоли защищен.
3. Задаем IP адрес устройства.
   1. Заходим в режим «глобального конфигурирования». Вводим команду «interface Vlan1»;
   2. Набираем команду «ip address 192.168.1.1 255.255.255.0». Здесь 192.168.1.1 – IP адрес, 255.255.255.0 – маска подсети. В адресе на 3 месте используйте свой индивидуальный номер.
   3. Для включения интерфейса набираем команду «no shutdown».
   4. Выходим из режима конфигурирования интерфейса с помощью команды «end».
4. Настроим службу раздачи IP-адресов DHCP на коммутаторе
   1. В режиме глобальной конфигурации создайте пул адресов «ip dhcp pool LAN». Имя пула можно взять любое
   2. Задайте сеть для пула: «network 192.168.1.0 255.255.255.0». Адрес сети должен точно соответствовать адресу, заданному в п. 4.2
   3. Для проверки подключите несколько рабочих станций к коммутатору и разрешите им получать IP-адрес по протоколу DHCP. Убедитесь, что они получают правильные адреса.
   4. Убедитесь, что пакеты ходят в сети
      1. Командой ping
      2. Визуальной трассировкой пакетов в Cisco Packet Tracer
5. Настроим виртуальные терминальные линии.
   1. В режиме «глобального конфигурирования» набираем команду «line vty 0 4». Будьте внимательны с пробелами!
   2. Определим транспортный протокол. Введем команду «transport input telnet»
   3. Создадим пароль на вход с помощью команды «login local»
   4. Выходим из режима конфигурирования и сохраняем конфигурации «write memory»
6. Конфигурация сохранена. Чтобы проверить выполним следующие действия:
   1. Подключим компьютер прямым кабелем с коммутатором по FastEthernet (если это ещё не сделано).
   2. Получим IP адрес автоматически по протоколу DHCP.
   3. В командной строке вызовем команду «telnet 192.168.1.1» с адресом коммутатора.
   4. Коммутатор запросил имя пользователя и пароль (Username – admin, password – sanfran). Таким образом, мы зашли удаленно на наш коммутатор.
   5. Можно проверить, что все команды языка Cisco выполняются и по telnet
7. Сохраните настройку коммутатора
8. Сохраните файл с сетью
9. Отправьте его на проверку.

## Командная строка Cisco

1. Получение справки
   1. ?
   2. command ?
   3. comm?
   4. command parameter ?
   5. command par?
2. Автодополнение клавишей Tab
   1. comm→
   2. command par→
3. Сокращения
   1. com~~mand~~
   2. com~~mand~~ para~~meter~~
4. Режимы
   1. User mode: >
   2. Priveleged mode: #
   3. Global configuration mode: (config)
   4. Object configuration modes: (config-obj)

# Режимы командной строки Cisco

* h~~ostname~~ <name>

int~~erface~~ r~~ange~~ F~~astEthernet~~ 0/1-24

Конфигурация порта

in~~terface~~ F~~astEthernet~~ 0/1

Конфигурация группы портов

* sh~~utdown~~
* n~~o~~ sh~~utdown~~

conf~~igure~~ t~~erminal~~

disa~~ble~~

ex~~it~~

* sh~~ow~~ r~~unning-config~~
* w~~rite~~ m~~emory~~

ex~~it~~

Глобальная конфигурация

en~~able~~

end

Привилегированный EXEC

Пользовательский EXEC

1. Просьба использовать **именно этот** пароль [↑](#footnote-ref-1)