

*Государственное образовательное учреждение высшего профессионального образования
«Московский государственный технический университет имени Н.Э. Баумана»
(МГТУ им. Н.Э. Баумана)*

Факультет «Информатика и системы управления»

Кафедра «Информационные системы и телекоммуникации»

Методическое указание к лабораторной работе

«Начальное конфигурирование»

по курсу

«Учебно-технологическая практика

по инфокоммуникационным системам и сетям»

Составила: Тихомирова Е.А.

Часы: 2 часа

Москва, 2013 г.

Оглавление

Цель работы	3
Теоретическая часть	3
Среда моделирования	3
Начальное конфигурирование	5
Практическая часть.....	10
Контрольные вопросы	12
Литература	12

Цель работы

1. Изучить среду моделирования Cisco Packet Tracer;
2. Изучить начальное конфигурирование коммутаторов и маршрутизаторов на примере оборудования фирмы Cisco.

Теоретическая часть

Среда моделирования

Cisco Packet Tracer – среда моделирования компьютерных сетей на основе оборудования компании Cisco.

Рабочая среда подразделяется на (рис. 1):

- выбор типа оборудования (1);
- выбор конкретного оборудования (2);
- рабочая область, в которой располагается оборудование (3).

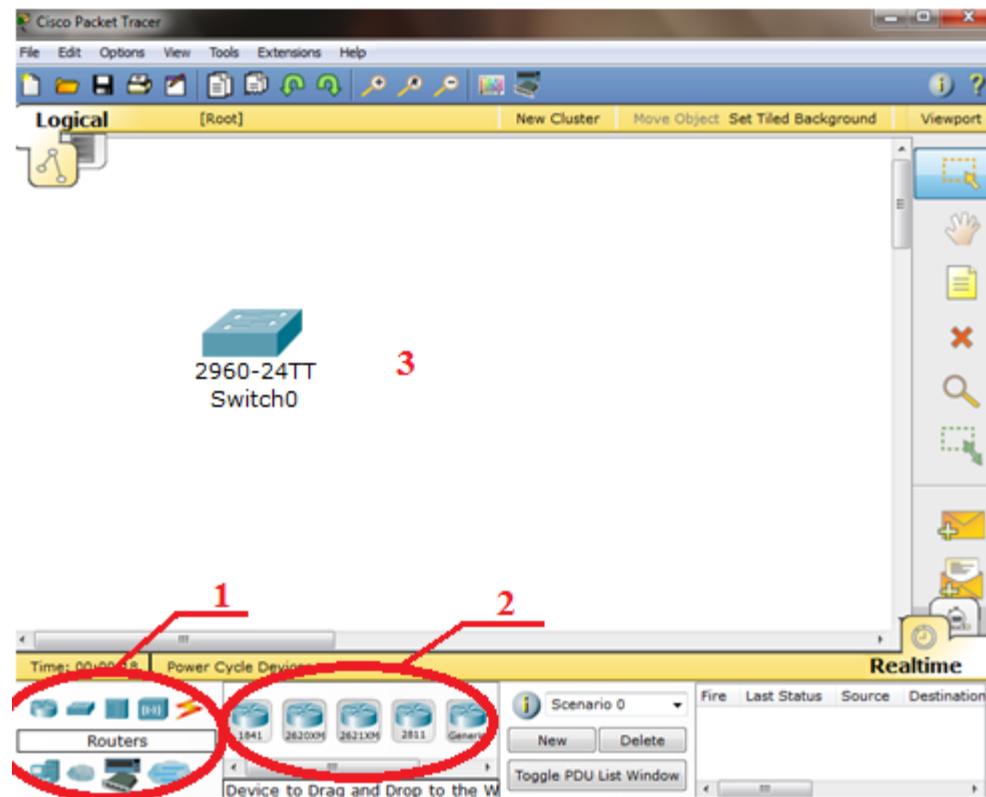


Рис. 1. Cisco Packet Tracer.

Двойной клик мышью по оборудованию на рабочей области позволяет зайти в окно, предназначенное для настройки. Пример формы для настройки коммутатора представлен на рис. 2. Закладка «Physical» представляет физическое представление оборудования: возможность выключить питание, вставить дополнительные модули (если они имеются). Закладка «CLI» – командная строка IOS данного устройства, где непосредственно осуществляется конфигурирование сетевого оборудования.

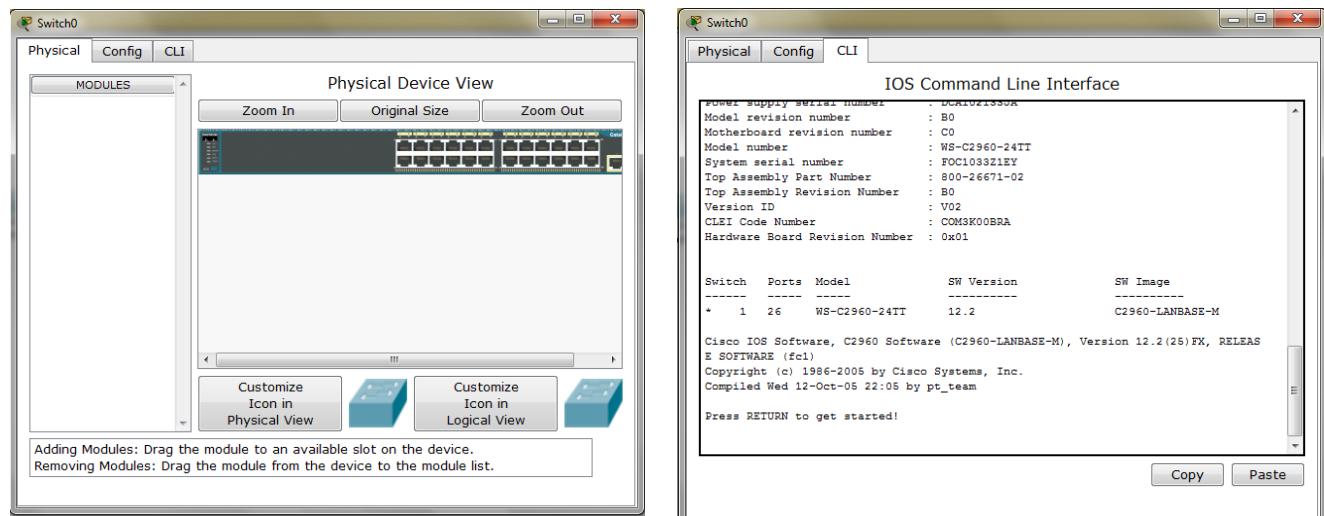


Рис. 2. Форма настройки коммутатора.

Для соединения устройств необходимо выбрать необходимый типа кабеля из панели № 2, нажать один раз мышью на устройство, после чего выбрать из списка необходимый интерфейс (рис. 3).

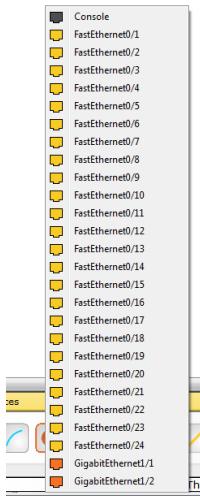


Рис. 3. Выбор интерфейса коммутатора.

Результат соединения двух коммутаторов представлен на рис. 4.

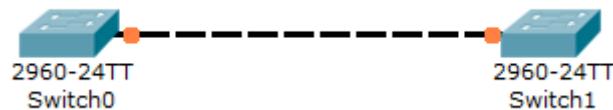


Рис. 4. Соединение двух коммутаторов.

На кабеле, соединяющем коммутаторы, присутствуют световые индикаторы с обеих сторон. Индикаторы в зависимости от состояния соединения могут принимать следующие цвета:

- красный – соединение отсутствует;
- оранжевый – соединение устанавливается или порт логически заблокирован;
- зеленый – соединение установлено.

Начальное конфигурирование

Все устройства, работающие под управлением IOS, поставляются с завода с минимально настроенной конфигурацией. Для корректной работы устройства в сети и удовлетворения всех потребностей сети необходимо провести конфигурирование сетевого устройства.

Конфигурирование коммутатора/маршрутизатора возможно осуществлять несколькими способами:

- через соединение по консоли (порт Console);
- через удаленное соединение (telnet);
- через web-интерфейс.

Последние два варианта возможно осуществить при условии, что на коммутаторе/маршрутизаторе настроен IP-адрес и пароли доступа. В противном случае установить соединение не удастся. Начальное конфигурирование коммутатора и маршрутизатора осуществляется через соединение по консоли. При установленном физическом подключении устройств (коммутатор/маршрутизатор и компьютер) необходимо настроить логическое соединение (терминал).

После загрузки коммутатор предоставляет возможность начать конфигурирование.

Настройка имени хоста

1. Зайдите в режим глобальной конфигурации:

Switch>**enable**

Switch#**configure terminal**

Switch(config)#

2. Введите имя хоста в соответствии с Вашим вариантом (табл. 3).

Switch(config)#**hostname SwitchX**

SwitchX(config)#

Настройка парольной защиты

Настройка пароля для доступа к привилегированному режиму

1. Находясь в режиме глобальной конфигурации, введите пароль доступа к привилегированному режиму в соответствии с информацией, приведенной в табл. 2.

SwitchX(config)#**enable password** *пароль*

Пароль «enable password» используется в том случае, если не указан пароль «enable secret».

2. Просмотрите рабочую конфигурацию коммутатора и убедитесь в том, что пароль настроен. Обратите внимания, что пароль записан открытым текстом.

Switch#**show running-config**

3. Вернитесь в пользовательский режим, после чего попытайтесь войти в привилегированный режим. Какой пароль Вы ввели?

Настройка зашифрованного пароля доступа к привилегированному режиму

1. Находясь в режиме глобальной конфигурации, введите зашифрованный пароль доступа к привилегированному режиму в соответствии с информацией, приведенной в табл. 2.

SwitchX(config)#**enable secret** *пароль*

Пароль «enable secret» используется для защиты доступа к привилегированному режиму EXEC и режимам конфигурации. После ввода в конфигурацию этот пароль шифруется.

2. Просмотрите рабочую конфигурацию коммутатора и убедитесь в том, что пароль настроен. Обратите внимания, что пароль записан в зашифрованном виде.
3. Вернитесь в пользовательский режим, после чего попытайтесь войти в привилегированный режим. Какой пароль Вы ввели?

Настройка пароля линий VTY

1. Зайдите в режим конфигурации линий VTY

SwitchX(config)#**line vty 0 15**

SwitchX(config-line)#

2. Введите пароль для доступа к линиям VTY в соответствии с информацией в табл. 2

SwitchX(config-line)#**password** *пароль*

3. Введите команду **login**, чтобы в будущем для доступа к коммутатору через линии VTY запрашивался пароль ввод пароля

SwitchX(config-line)#**login**

4. Просмотрите рабочую конфигурацию коммутатора и убедитесь в том, что пароль настроен. Обратите внимания, что пароль записан открытым текстом.

Настройка пароля консольного порта

1. Зайдите в режим конфигурации консольного порта

SwitchX(config)#**line console 0**

SwitchX(config-line)#

2. Введите пароль для доступа к консольному порту в соответствии с информацией в табл. 1

SwitchX(config-line)#**password пароль**

3. Введите команду **login**, чтобы в будущем для доступа к коммутатору через консоль запрашивался пароль ввод пароля

SwitchX(config-line)#**login**

4. Просмотрите рабочую конфигурацию коммутатора и убедитесь в том, что пароль настроен. Обратите внимания, что пароль записан открытым текстом.

Служба шифрования пароля

1. Просмотрите рабочую конфигурацию коммутатора и убедитесь в том, что все пароли настроены. Обратите внимание, что почти все пароли записаны открытым текстом
2. Находясь в режиме глобальной конфигурации, активируйте службу шифрования паролей

SwitchX(config)#**service password-encryption**

3. Просмотрите рабочую конфигурацию коммутатора и обратите внимание на первые и последние строки конфигурации: команда **service password-encryption** активна (рис. 5) и действует на все пароли.

```
Switch#sh run
Building configuration...

Current configuration : 1088 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Switch
!
line con 0
password 7 0822455D0A16
login
!
line vty 0 4
password 7 0822455D0A16
login
line vty 5 15
password 7 0822455D0A16
login
!
!
end
```

Рис. 5. Часть вывода рабочей конфигурации.

Настройка ip-адреса коммутатора

1. Зайдите в режим конфигурации VLAN и назначьте ip-адрес коммутатору в соответствии с информацией в табл. 3 для того, чтобы получить возможность обращения к устройству.

SwitchX(config)#**interface vlan 1**

SwitchX(config-if)#**ip address ip-адрес маска**

2. Просмотрите рабочую конфигурацию коммутатора и убедитесь в том, что ip-адрес назначен VLAN 1.
3. Добавьте в топологию сети компьютер и подсоедините его к коммутатору (рис. 6)

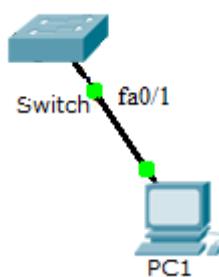


Рис. 6. Топология сети.

4. Проверьте доступность коммутатора с PC1. Узел доступен?

5. Зайдите по telnet на коммутатор с PC1.

```
PC>telnet ip-адрес
```

6. Какой пароль Вам необходимо ввести для доступа к коммутатору?

Настройка шлюза по умолчанию

Шлюз по умолчанию – адрес маршрутизатора, на который необходимо направлять пакеты, для которых невозможно определить маршрут в пределах сети источника.

1. К созданной ранее топологии добавьте маршрутизатор и компьютер, соединенные в соответствии с рис. 7.

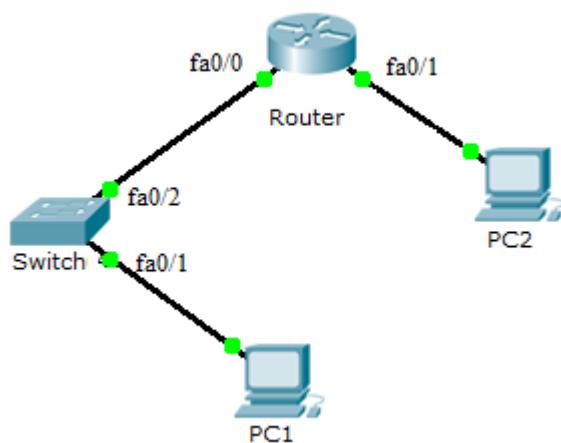


Рис. 7. Топология сети.

2. Настройте ip-адреса на интерфейсах маршрутизатора.
3. Проверьте доступность PC1 с PC2. Узел доступен? Почему?

Сохранение конфигурации

1. Находясь в привилегированном режиме, сохраните рабочую конфигурацию

```
Switch#copy running-config startup-config
```

Настройка баннера входа

В рамках любой политики безопасности необходимо явно указать, что доступ к сетевым ресурсам случайным посетителем запрещен. В прошлом хакеры успешно использовали факт наличия приглашения «welcome» («добро пожаловать») при входе в качестве юридического оправдания несанкционированного проникновения в сеть. Когда пользователь пытается получить доступ к сетевому устройству (коммутатору, маршрутизатору и т.д.), должно появляться сообщение, явно указывающее на ограничение доступа. Его можно создать с помощью команды **banner motd Cisco IOS**.

1. В режиме глобальной конфигурации введите команду **banner motd %** и нажмите клавишу **Enter**. Знак процента (%) является начальным символом-разделителем текста сообщения.
2. Введите текст сообщения и завершите его знаком %. Не используйте знак процента в тексте, т.к. он будет рассматриваться как конечный символ-разделитель сообщения.

SwitchX(config)#**banner motd %**

WARNING - WARNING - WARNING - WARNING - WARNING - WARNING - WARNING%

SwitchX(config)#

3. Завершите сеанс консоли

Switch#**logout**

4. Получите доступ к привилегированному режиму. Обратите внимание, что перед вводом пароля отображается баннерное сообщение.

Практическая часть

Собрать и настроить топологию, заданную преподавателем. Настройку осуществить в соответствии с данными в табл. 2, 3. В качестве коммутатора использовать модель 2960, в качестве маршрутизатора – 2811.

В качестве среды моделирования использовать Cisco Packet Tracer.

Список необходимых команд приведен в табл. 1.

Таблица 1.

Команды конфигурирования.

Команда	Описание
banner motd	Позволяет настроить сообщение, которое будет отображаться во время входа в систему.
configure terminal	Активирует режим конфигурации терминала.
copy running-config место назначения	Копирует файл текущей конфигурации коммутатора в другое место назначения. Обычно это загрузочная конфигурация.
enable	Активирует привилегированный режим EXEC. В привилегированном режиме EXEC доступно большее количество команд. Эта команда требует

	ввода пароля разрешения доступа (enable password), если он настроен.
enable password <i>пароль</i>	Используется для защиты доступа к привилегированному режиму (enable). Однако этот пароль хранится в виде незашифрованного текста в конфигурации.
enable secret <i>секретный_пароль</i>	Зашифрованный пароль используется для защиты доступа к привилегированному режиму (enable). Команда переопределяет незашифрованный пароль, заданный с помощью команды enable password, если заданы оба.
end	Завершает режим конфигурации.
hostname <i>имя_хоста</i>	Задает имя системы, являющееся частью приглашения.
interface vlan 1	Активирует режим конфигурации интерфейса VLAN 1, в котором задается ip-адрес для управления коммутатором.
ip address <i>ip-адрес маска</i>	Задает ip-адрес и маску интерфейса.
line vty 0 15	Активирует режим конфигурации линии виртуального терминала. Линии виртуального терминала (VTY) позволяют получать доступ к коммутатору для удаленного управления сетью. Доступное количество линий VTY зависит от версии ПО Cisco IOS. Обычно используется значения 0-4 и 0-15 (включительно).
login	Активирует процесс входа в систему, запрашивающий ввод имени пользователя и пароля для доступа в систему.
logout	Выход из режима EXEC, после которого потребуется повторная аутентификация (если она включена).
password <i>пароль линии</i>	Назначает пароль портам VTY или консольным портам.
ping <i>ip-адрес</i>	Использует эхо-запросы и эхо-ответы ICMP, чтобы определить доступен ли удаленный узел.
reload	Перезапускает коммутатор и перезагружает операционную систему Cisco IOS и конфигурацию.
service password-encryption	Включает службу шифрования всех паролей в текущей конфигурации.
show interface vlan 1	Отображает информацию об ip-адресе коммутатора (Cisco Catalyst 2950).
show running-configuration	Выводит рабочую конфигурацию.
shutdown no shutdown	Отключает или запускает отключенный интерфейс.
telnet <i>ip-адрес</i>	Создает сетевое подключение протоколу Telnet. IP-адрес идентифицирует устройство назначения.

Таблица 2.

Справочные данные.

Параметр конфигурации	Значение
enable password	iu3
enable secret password	cisco
пароль линии vty	vty
пароль консольного порта	console

Таблица 3.

Условия заданий.

Адрес первой подсети	Маска подсети
192.168.x.0	255.255.255.0

Где x – номер варианта студента.

Контрольные вопросы

1. Перечислите способы подключения к маршрутизатору с целью конфигурирования?
2. В чем заключается различие между паролями password и secret?
3. Где хранится текущая конфигурация коммутатора?
4. Где хранится загрузочная конфигурация коммутатора?

Литература

1. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 640-822// Издательство: «Вильямс», 2012 – 720 с.
2. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2// Издательство: «Вильямс», 2012 – 736 с.