

Лабораторная работа №2  
**Первичная настройка сетевого оборудования Cisco.**

**Цель:** изучить принципы начальной настройки сетевого оборудования Cisco и необходимый минимум команд операционной системы Cisco IOS.

### 1. Теоретические сведения

Средства, обеспечивающие работу компьютерных сетей, можно разделить между категориями неуправляемого и управляемого оборудования. К неуправляемому оборудованию можно отнести повторитель, ретранслятор, концентратор (хаб), медиаконвертер, сетевой трансивер. Функции этих устройств сравнительно просты и, как правило, реализуются на аппаратном уровне. Управляемое сетевое оборудование для поддержки работы сети реализует достаточно сложные алгоритмы с множеством входных параметров, значения которых могут варьироваться в зависимости от структуры сети, объема трафика и др. Архитектура таких устройств сходна с архитектурой компьютеров, а их общий контроль выполняет специализированная операционная система. К управляемому сетевому оборудованию можно отнести мост (управляемый), коммутатор, маршрутизатор, сетевой экран.

Большинство сетевых устройств компании Cisco работают под управлением операционной системы Cisco IOS. Для передачи ей конфигурационных команд, как правило, используется компьютер, подключенный к устройству Cisco через:

- специальный консольный порт;
- один из сетевых интерфейсов.

Команды с компьютера на сетевое устройство Cisco могут быть отправлены:

- с помощью специализированного ПО;
- с помощью протоколов удаленного доступа telnet или SSH;
- по Web-интерфейсу.

Способы 2-3 требуют предварительной настройки, поэтому первичное конфигурирование можно выполнить только первым способом. Для этого администратор сети должен подключиться к устройству через прямое консольное подключение (рис. 1).

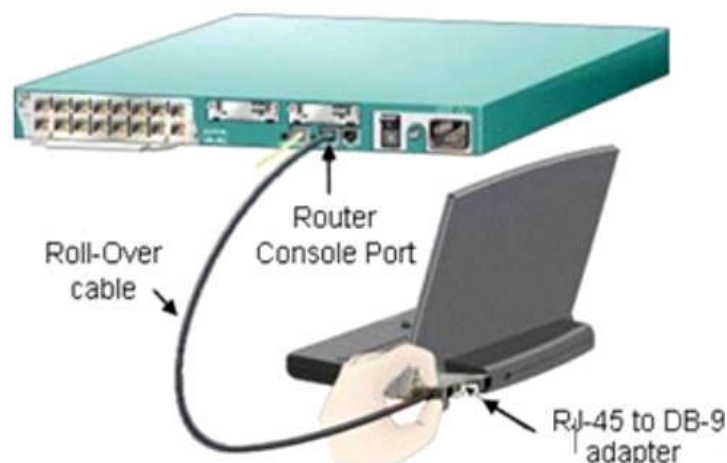


Рис. 1. Консольное подключение к сетевому устройству

У каждого коммутатора, маршрутизатора, межсетевого экрана обязательно присутствует консольный порт, который для устройств Cisco обозначен голубым цветом. Порт имеет разъем формата RJ-45 или mini-USB. Поэтому для подключения по консольному порту потребуются либо кабель с разъемом mini-USB, либо специальный кабель с разъемами RJ-45 и RS-232 (рис. 2).



Рис. 2. Консольный порт (отмечен голубым цветом) и варианты консольных кабелей

Специализированное ПО организует интерфейс командной строки (CLI - command line interface). Работа с командной строкой осуществляется в нескольких режимах (рис. 3).

Режим	Переход в режим	Вид командной строки	Выход из режима
Пользовательский	Подключение	Router>	logout
Привилегированный	Enable.	Router#	disable
Глобальная конфигурация	Configure terminal	Router(config)#	exit,end или Ctrl-Z
Настройка интерфейсов	Interface	Router(config-if)	exit

Рис. 3. Режимы работы с сетевым оборудованием

Несколько слов о виде командной строки:

**Router>** Приглашение, которое характеризует пользовательский режим. В нем можно просматривать некоторую статистику и проводить самые простые операции вроде ping. Это режим для сетевого оператора, инженера первой линии техподдержки, чтобы он ничего не повредил и лишнего не узнал. Иными словами, команды в этом режиме позволяют выводить на экран информацию без смены установок сетевого устройства.

**Router#** Приглашение в привилегированном режиме. Привилегированный режим поддерживает команды настройки и тестирования, детальную проверку сетевого устройства, манипуляцию с конфигурационными файлами и доступ в режим конфигурирования. Попасть в него можно, введя команду **enable**.

**Router(config)#** Приглашение в режиме глобальной конфигурации. Он позволяет вносить изменения в настройки устройства. Команды режима глобального конфигурирования определяют поведение системы в целом. Активируется командой **configure terminal** из привилегированного режима.

**Router(config-if)#** Приглашение в режиме конфигурирования интерфейса. В данном режиме может быть выполнена настройка конкретного физического или логического интерфейса (порта) сетевого устройства. Активируется командой **interface** из режима глобального конфигурирования.

Алгоритм первичного конфигурирования сетевого оборудования Cisco следующий:

1. Создать консольное соединение;
2. Задать пароль на привилегированный режим;
3. Создать пользователя;
4. Установить авторизацию на подключение к консоли;
5. Задать IP-адрес логического интерфейса для L2-устройств или физического интерфейса для L3-устройств;
6. Выбрать тип удаленного подключения (Telnet/SSH);
7. Включить авторизацию для удаленных подключений.

По завершении первичного конфигурирования устройство может быть встроено в сеть, а его дальнейшая настройка осуществляется либо с помощью протокола удаленного управления telnet или SSH, либо посредством Web-интерфейса. Идентификация устройства в сети выполняется по IP-адресу.

## 2. Задания

### 2.1. Обучающая часть: «Первичная настройка коммутатора фирмы Cisco».

1. В CPT в качестве коммутатора выберите модель коммутатора 2960.
2. Поместите один компьютер в рабочую область CPT и соедините его с коммутатором консольным кабелем (в закладке "Connections" обозначен голубым цветом). Выберите на компьютере интерфейс RS-232, а на коммутаторе порт "Console".
3. В окне настроек компьютера выберите закладку "Desktop" и приложение "Terminal";
4. В появившемся диалоговом окне настройки интерфейса RS-232 нажмите кнопку "Ok" (рис. 4).
5. В появившемся запросе выберите работу с помощью командной строки. Несколько раз нажмите "Ввод", пока не появится приглашение Switch>.
6. Первичное консольное соединение создано.
7. CLI имеет развитую систему справки. Чтобы узнать доступные команды в пользовательском режиме нажмите знак вопроса. Справа от команды приводится ее краткое описание. Команду можно вводить не целиком, а только несколько первых символов и далее нажимать "Tab". Если введенных символов достаточно, чтобы однозначно идентифицировать команду, то она полностью появится в командной строке. Если команда не появилась, то можно нажать знак вопроса, чтобы увидеть доступные варианты. Некоторые команды CLI составные, поэтому нужно активно пользоваться встроенной справкой.

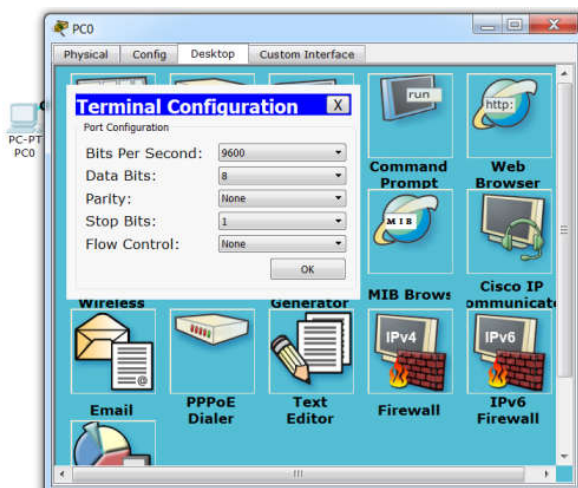


Рис. 4. Настройка удаленного соединения с коммутатором через RS-232

8. Для перехода в привилегированный режим введите команду **enable**. Для этого нажмите "en", нажмите "Tab" и нажмите "Ввод". Появившийся знак # свидетельствует о том, что доступ к сетевому устройству осуществляется в привилегированном режиме.
9. Чтобы вернуться в пользовательский режим можно ввести команду **disable** или **exit**. Попробуйте выполнить переключение разными командами. В чем их различие?
10. Посмотрите текущую конфигурацию устройства с помощью команды **show running-config**. Для пролистывания информации в окне консоли можно использовать "Ввод" или "Пробел". В первом случае пролистывается одна строка, а во втором - несколько строк, уместящихся на странице консоли.
11. Для дальнейшей настройки устройства необходимо войти в режим глобального конфигурирования с помощью команды **configure terminal**. Выход из этого режима осуществляется с помощью команды **end** или **exit**. Проверьте в чем различие указанных команд.
12. В режиме глобального конфигурирования создайте пароль для входа в привилегированный режим с помощью команды **enable password <пароль>**. Например, чтобы задать пароль qwe123 нужно ввести команду: *enable password qwe123*.
13. Перейдите в пользовательский режим и снова попытайтесь войти в привилегированный. Что произошло?
14. Вами был создан пароль на вход в привилегированный режим. Однако этот пароль храниться в открытом (незашифрованном виде). С помощью команды **show running-config**, выполняемой в привилегированном режиме, можно узнать данный пароль. Для полной блокировки доступа к паролю его нужно зашифровать. Для этого в режиме глобального конфигурирования выполнить команду **service password-encryption**.
15. Вернитесь в привилегированный режим и попробуйте узнать пароль с помощью команды **show running-config**. Каков результат?
16. В соответствии с алгоритмом настройки коммутатора создадим локального пользователя. В режиме глобального конфигурирования необходимо ввести команду **username**. Далее через пробел указывается имя пользователя. Установим имя: *admin*. Затем через пробел установим привилегию доступа этого пользователя. Уровни привилегий лежат в диапазоне от 0 до 15. Уровень 15 является наивысшим. Чтобы задать пользователю *admin* с 15 уровнем привилегий добавим в строящуюся команду опцию *privilege 15*. Напоследок зададим пароль для входа этого пользователя с помощью опции *password qwe123*. В итоге получится команда: **username admin privilege 15 password qwe123**. Запись о пользователе была создана и помещена в локальную базу данных коммутатора.
17. Задействуем запись о созданном пользователе для доступа к настройке коммутатора по терминальному интерфейсу. Для этого нужно войти в режим конфигурирования терминальной линии. В режиме глобального конфигурирования наберите команду **line**, затем пробел и нажмите знак вопроса. СРТ покажет дальнейшую структуру команды. Для конфигурирования терминальной линии введем команду: **line console 0**. Появится приглашение: **Switch(config-line)#**
18. После входа в режим конфигурирования терминальной линии задайте команду **login local** и нажмите ввод. Теперь вход в привилегированный режим по консоли будет осуществляться с помощью локальной базы данных пользователей. Выйдите из привилегированного режима с помощью команды **exit**. Что произошло? Попробуйте закрыть окно консоли и снова подключиться к коммутатору. Теперь вход по консоли защищен?
19. На следующем шаге необходимо задать IP-адрес для удаленной работы с коммутатором по сети. Сделаем это посредством консоли. Команда **show running-config** показывает, что у коммутатора 2960 имеются в наличии 24 физических интерфейса Fast Ethernet, 2 физических интерфейса Gigabit Ethernet, 1 логический интерфейс Vlan1, к которому по умолчанию относятся все физические интерфейсы. Настройка IP-адреса выполняется для логических интерфейсов. Поэтому перейдем в режим конфигурирования интерфейса

- Vlan1. Для этого нужно ввести команду **interface Vlan1** и нажать ввод. Должно появиться приглашение: **Switch(config-if)#**
20. Задать IP-адрес можно командой: **ip address 192.168.0.1 255.255.255.0**.
  21. После настройки IP-адреса интерфейс Vlan1 нужно активировать. Делается это командой: **no shutdown**. Теперь стало возможным создать соединение с коммутатором по физическим интерфейсам Fast Ethernet и Gigabit Ethernet, а также подключение к коммутатору с помощью виртуального терминала.
  22. Перейдите в режим глобального конфигурирования. Настроим подключение к коммутатору с помощью виртуального (удаленного) терминала. Для этого нужно перейти в режим конфигурирования линии виртуального терминала с помощью команды: **line vty 0 4**. Значения 0 и 4 указывают на диапазон линий виртуального терминала. После нажатия кнопки "ввод" появится приглашение: **Switch(config-line)#**
  23. Команда **transport input telnet** задает протокол telnet для входящих сообщений (команд) от виртуальной консоли.
  24. Следующая команда **login local** разрешает доступ к коммутатору по протоколу telnet только пользователям зарегистрированным в локальной базе данных. После нажатия "ввод" выйдете из режима конфигурирования.
  25. Перейдите в привилегированный режим и сохраните параметры конфигурации коммутатора с помощью команды **write memory**. Эта команда сохраняет текущую конфигурацию коммутатора в файле startup-config, который храниться в энергонезависимой памяти коммутатора и используется для инициализации параметров сетевого оборудования после его перезагрузки.
  26. Зайдите в рабочую область CPT и удалите соединение коммутатора и компьютера по консольному кабелю.
  27. Установите соединение коммутатора и компьютера с помощью витой пары и физических интерфейсов Fast Ethernet.
  28. На компьютере задайте статический IP-адрес из той же сети, в которую входит коммутатор.
  29. С помощью утилиты **ping** проверьте соединение.
  30. Если пакеты проходят между сетевыми устройствами, то подключите виртуальный терминал удаленного управления коммутатором на компьютере с помощью команды: **telnet 192.168.0.1** (вводится в Command Prompt ПК).
  31. Пройдите аутентификацию и проверьте настройки коммутатора с помощью команды **show running-config** в окне командной строки компьютера. Завершите сессию. Первичная настройка завершена.
  32. Сохраните проект CPT с названием **LabNet-2(Фамилия\_группа)-task-1.pkt**.
  33. Работоспособность Вашего проекта продемонстрируйте преподавателю.
  34. Проверенный преподавателем проект загрузите на сайт [eluniver.ugrasu.ru](http://eluniver.ugrasu.ru) на качестве отчета о выполнении **Обучающей части задания**.

## 2.2 Самостоятельная работа

1. Расширьте физическую топологию сети, построенную в обучающей части задания, как показано на рисунке 5. Тип второго коммутатора выберите произвольно.
2. Используя консольное соединение выполните первоначальную настройку второго коммутатора сети. В качестве **username** используйте Вашу фамилию на латинице (желательно не более 10 символов). Оба коммутатора должны иметь статические IP-адреса, принадлежащие одной сети. Каждому коммутатору назначьте сетевые имена со следующей структурой: <Фамилия студента>-Sw<номер коммутатора>. Например: **Petrov-Sw1**. Команда **hostname Petrov-Sw1**, выполненная в режиме глобального конфигурирования, задаст новое имя коммутатору, а приглашение командной строки

коммутатора должно поменяться на **Petrov-Sw1(config)#**. По окончании настройки второго коммутатора его консольный интерфейс следует удалить.

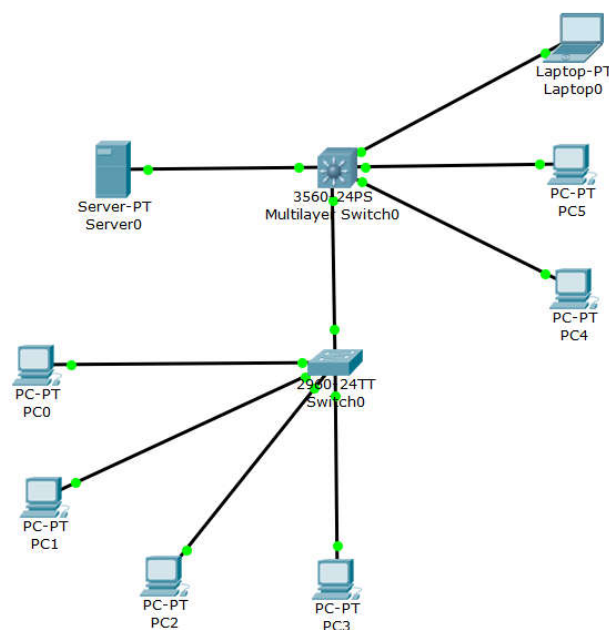


Рис. 5. Пример физической топологии сети в Задании#2

3. На сервере сети следует настроить DHCP- и DNS-сервисы. Все сетевые компьютеры должны получать IP-адреса посредством протокола DHCP. Коммутаторы и сервер должны иметь доменные имена со следующей структурой:

<название сетевого узла>.<сокращение ФИО студента>.<группа студента>

Например: Сетевое имя сервера - **netserv**. Студент - **Petrov Ivan Ivanovich** (Петров Иван Иванович). Группа - **1192b**. Тогда полное доменное имя - **netserv.pii.1192b**.

4. Протестируйте прохождение пакетов между парой компьютеров сети, используя IP-адреса.
5. Проверьте прохождение пакетов с любого компьютера на коммутаторы сети, используя IP-адреса их логических интерфейсов (vlan1) и доменные имена коммутаторов.
6. Проверьте удаленное подключение с помощью протокола telnet к коммутаторам по их доменным именам.
7. Протестируйте управление обеими коммутаторами с любого компьютера сети.
8. Настройте каждый коммутатор для удаленного управления по защищенному (шифруются все команды, включая пароли) протоколу SSH:

- Используя удаленное подключение по telnet в режиме глобального конфигурирования задайте имя домена коммутатора, командой:

**ip domain-name <имя домена>**

В приведенном выше примере имя домена – **pii.1192b**.

- Активируйте модуль шифрования на коммутаторе, сгенерировав открытый и закрытый ключи алгоритма RSA командой: **crypto key generate rsa** (в режиме глобального конфигурирования). Длину ключа задайте 1024 бита.
- В режиме глобального конфигурирования выберите вторую версию протокола SSH, выполнив команду: **ip ssh version 2**.
- Перейдите в режим конфигурирования виртуального терминала и модифицируйте команду **transport input** так, чтобы можно было использовать для удаленного подключения оба протокола: telnet и SSH (разобраться самостоятельно, используя встроенную справку Cisco IOS).
- В привилегированном режиме сохраните конфигурацию коммутатора и завершите telnet-сессию.

- Подключитесь к коммутатору с ПК командой:  
**ssh -l <имя пользователя на коммутаторе> <полное доменное имя коммутатора>**
- 9. Протестируйте управление обеими коммутаторами с любого компьютера сети по протоколу SSH. Каким образом можно задать удаленное управление коммутаторами только по протоколу SSH (telnet должен быть отключен)?
- 10. Сохраните Ваш проект в СРТ с названием **LabNet-2(Фамилия-группа)-task-2.pkt**.
- 11. Работоспособность Вашего проекта продемонстрируйте преподавателю.
- 12. Проверенный преподавателем проект загрузите на сайт [eluniver.ugrasu.ru](http://eluniver.ugrasu.ru) на качестве отчета о выполнении **Самостоятельной работы**.

### 3. Защита лабораторной работы

1. Изучить материал настоящего методического указания и дополнительную литературу.
2. Приготовиться к ответу на контрольные вопросы.
3. В процессе защиты быть готовым к выполнению дополнительных задач на основе построенных Вами Проектов СРТ.

### 4. Контрольные вопросы

1. Какие способы подключения к коммутаторам для их настройки Вы знаете?
2. Чем отличаются протоколы telnet и SSH?
3. В каких режимах можно работать с сетевым оборудованием Cisco? В чем их различие?
4. Как можно заблокировать доступ к привилегированному режиму работы коммутатора?
5. Какая команда устанавливает пароль на работу в привилегированном режиме?
6. Какова последовательность действий при первоначальной настройке коммутатора?
7. Каким образом можно узнать о текущих настройках коммутатора?
8. С помощью какой команды осуществляется шифрование паролей в коммутаторе?
9. Какие особенности имеет справочная система IOS?
10. Каким образом создаются пользовательские записи и присваиваются привилегии доступа?
11. Сколько уровней привилегий используется в Cisco IOS?
12. Как переключиться в режим конфигурирования консольной линии?
13. Каким образом осуществляется присвоение IP-адреса коммутатору?
14. Какие команды требуются для настройки соединения с коммутатором по протоколу telnet?
15. Каково назначение команды `no shutdown`?
16. В каком режиме доступна команда `show running-config`?
17. Как можно опознать текущий режим управления коммутатором?
18. Возможно ли подключение в коммутатору по протоколу telnet с помощи доменного имени?
19. Как переключиться из пользовательского режима в режим настройки физического или логического интерфейса?
20. Что означает следующая подсказка командной строки `Switch(config-line)#` ?
21. Как задать имя коммутатору?
22. В разработке...