При включении маршрутизатора или другого устройства CiscoIOS по умолчанию устанавливается режим пользовательского доступа **EXEC**. В этом режиме в командной строке отображается следующее:

**Router>**

Команды, которые можно выполнить в режиме пользовательского доступа **EXEC**, сводятся к получению информации о работе устройства и к диагностике с помощью команд **show**, а также утилит **ping** и **traceroute**.

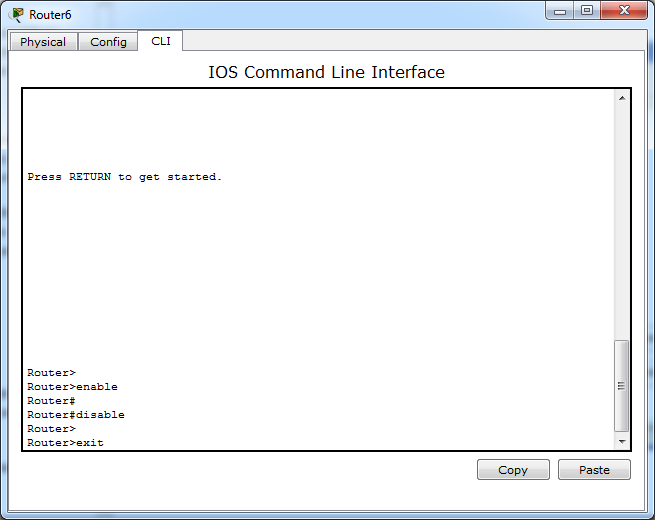
Для ввода команд, которые меняют работу устройства, необходимы привилегированные права доступа. Чтобы переключиться в привилегированный режим **EXEC**, нужно ввести в командную строку enable и нажать клавишу Enter.

Командная строка соответственно изменится. В режиме привилегированного доступа в ней отобразится:

**Router#**

Для выхода из режима привилегированного доступа и возврата в режим пользовательского доступа введите в командной строке **disable** или **exit**.

Вход в оба режима можно защитить паролем или комбинацией имени пользователя и пароля.



Приглашение пользовательского режима

Приглашение привилегированного режима

В большинстве случаев команды применяются к текущему файлу конфигурации, используя подключение к терминалу. Для использования этих команд пользователю нужно войти в режим глобальной конфигурации.

Чтобы войти в режим глобальной конфигурации, введите команду **configure terminal** или **config** t. В этом режиме в командной строке отображается следующее:

**Router(config)#**

Введенные в этом режиме команды выполняются немедленно и могут отразиться на работе устройства.

Из режима глобальной конфигурации администратор может войти в другие подрежимы.

Для настройки интерфейсов сетей LAN и WAN используется режим конфигурации интерфейса. Для перехода в режим конфигурации интерфейса, введите, находясь в режиме глобальной конфигурации, команду **interface** [*тип*] [*номер*]. В этом режиме в командной строке отображается следующее:

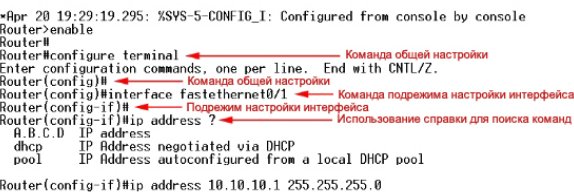
**Router(config-if)#**

Еще один часто используемый подрежим — это подрежим задания конфигурации маршрутизатора, на который указывает следующее содержание командной строки:

**Router(config-router)#**

Этот режим служит для настройки параметров маршрутизатора.

*Пример:*



В исходную конфигурацию устройства Cisco IOS входит задание имени устройства и паролей, которые служат для контроля доступа к различным функциям устройства.

Одной из первых задач конфигурирования является присвоение устройству уникального имени. Эта задача решается в режиме глобальной конфигурации с помощью следующей команды:

**Router(config)#***hostname* <*имя*>

При нажатии клавиши Enter имя узла по умолчанию — Router — меняется на новое присвоенное узлу имя.

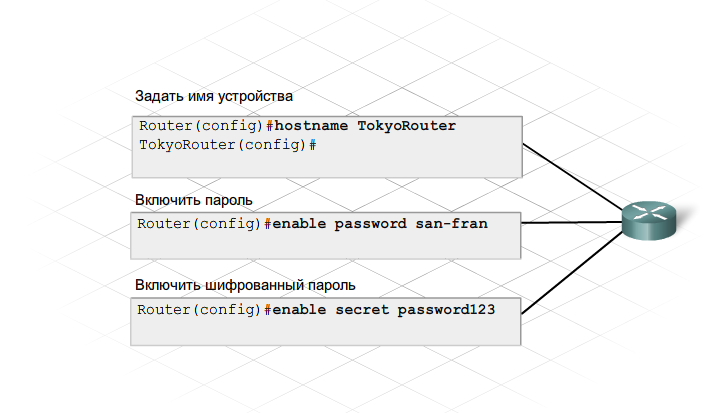
Следующим шагом конфигурирования является задание паролей для предотвращения несанкционированного доступа к устройству.

Для ограничения доступа к привилегированному режиму **EXEC** служат команды **enable password** и **enable secret**. Это не дает возможности изменять параметры настройки маршрутизатора пользователям, которые не имеют соответствующих прав доступа.

**Router(config)#***enable password* <*пароль*>

**Router(config)#***enable secret* <*пароль*>

Разница между этими двумя командами состоит в том, что команда **enablepassword** по умолчанию не является зашифрованной. Если после команды **enablepassword** вводится команда **enablesecret**<*пароль*>, то команда **enablesecret** имеет преимущество перед **enablepassword**.



**Баннеры**

Баннер — это текст, который видит пользователь при первоначальном входе в маршрутизатор. Настройка соответствующего баннера является частью продуманного плана обеспечения безопасности. Баннер должен как минимум содержать предупреждение относительно несанкционированного доступа. Никогда не устанавливайте баннер в виде приветствия для пользователя, не имеющего соответствующих прав доступа.

Существует два типа баннеров: сообщение дня (**MOTD**) и информация для входа. Два отдельных баннера нужны для того, чтобы можно было заменить один из них, не затрагивая при этом все сообщение баннера целиком.

Для настройки баннеров служат команды **banner motd** и **banner login**. Для обоих типов в качестве разделителя в начале и в конце сообщения используется символ **"#"**. Этот символ позволяет пользователю задать баннер, состоящий из нескольких строк.

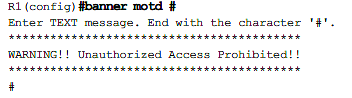
Если заданы оба баннера, то баннер входа в систему появляется после **MOTD**, но перед тем как вводить учетные данные для входа.

**Синхронное ведение журнала**

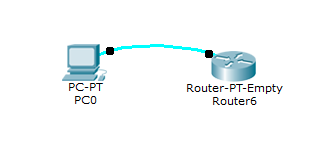
Программа Cisco IOS часто посылает незапрашиваемые сообщения, например, об изменении состояния настраиваемого интерфейса. Иногда это происходить во время ввода команды. Такое сообщение не влияет на выполнение команды, но дезориентирует пользователя, который вводит команду. Для того чтобы во время ввода команды не появлялись незапрашиваемые сообщения, можно ввести команду **logging synchronous** в режиме глобальной конфигурации.

**Отключение поиска домена**

По умолчанию при вводе имени узла в режиме включения маршрутизатор интерпретирует это как попытку пользователя подключиться к устройству через **Telnet**. Маршрутизатор пытается разрешить неизвестные имена, введенные в режиме включения, путем отправки их на сервер DNS. Это относится ко всем введенным словам, которые маршрутизатор не может распознать, включая неправильно введенные команды. Если это делать не нужно, то с помощью команды **no ip domain-lookup** можно отключить эту функцию, действующую по умолчанию.



Существует несколько способов подключиться к устройству и настроить конфигурацию. Один из них - подключение компьютера к порту консоли устройства. Этот тип подключения часто используется для задания начальной конфигурации устройства.



Установка пароля для доступа к консоли выполняется в режиме глобальной конфигурации. Указанные ниже команды предотвращают несанкционированный доступ к пользовательскому режиму с порта консоли.

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

**Router(config)#**password <*пароль*>

**Router(config)#**login

Если устройство соединено с сетью, то к нему можно получить доступ через сетевое соединение. Такой вариант называется подключением через виртуальный терминал или подключением **vty**. Для виртуального порта (порта **vty**) нужно настроить пароль.

**Route(config)#** line vty 0 4

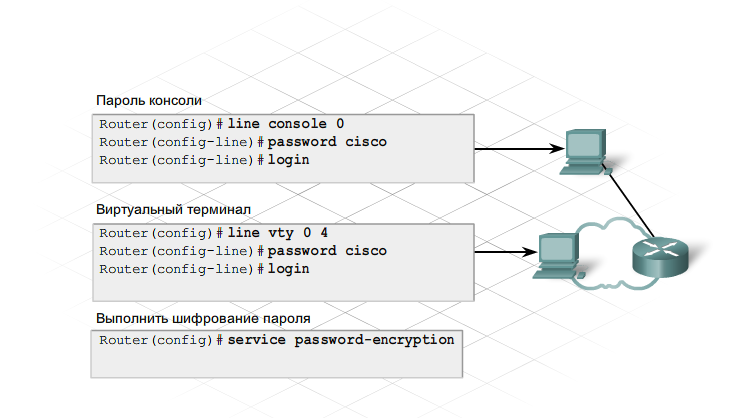
**Router(config)#** password <*пароль*>

**Router(config)#** login

Цифры 0 4 означают 5 одновременных внутриполосных подключений. Можно для каждого подключения задать свой пароль, указав номера конкретных подключаемых линий, например, **line vty 0 15**.

Для проверки правильности задания паролей используйте команду **show running**-**config**. Пароли хранятся в файле текущей конфигурации, в формате незашифрованного текста. Можно включить шифрование всех паролей, которые хранятся в памяти маршрутизатора. Это создаст дополнительные сложности в случае несанкционированного доступа. Команда **service password encryption**, введенная в режиме глобальной конфигурации, обеспечивает шифрование всех паролей.

Следует помнить, что при изменении текущей конфигурации необходимо скопировать ее в файл начальной конфигурации. В противном случае при выключении устройства все изменения будут потеряны. Для копирования текущей конфигурации в файл начальной конфигурации используется команда: **copy run start**.

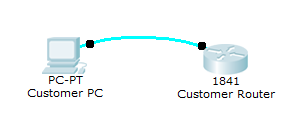


**Задание №1** Разграничение доступа к маршрутизатору

**Задачи:**

* настройка имени узла маршрутизатора;
* настройка паролей;
* настройка начальных сообщений;
* проверка настройки маршрутизатора.

#### 1) Построить следующую сеть.



#### 2) Настройка имени узла маршрутизатора.

a) С помощью программы для эмуляции терминала на клиентском компьютере подключитесь к консоли клиентского маршрутизатора **Cisco1841ISR**

b) Задайте имя узла маршрутизатора **CustomerRouter**

#### 3) Настройка пароля и секретного пароля привилегированного режима.

a) В режиме глобальной настройки задайте пароль **cisco**:

b) Задайте зашифрованный пароль привилегированного режима **cisco123** с помощью команды **secret**:

#### 4)  Настройка пароля консоли.

a) В режиме глобальной настройки переключитесь в режим настройки линии, чтобы задать линию консоли:

b) Задайте пароль **cisco123**, укажите, что пароль нужно вводить при каждом входе в систему, и выйдите из режима настройки линии:

#### 5) Настройка пароля канала vty для предоставления доступа telnet к маршрутизатору.

a) В режиме глобальной настройки переключитесь в режим настройки линии, чтобы задать линии **vty**:

b) Задайте пароль **cisco123**, укажите, что пароль нужно вводить при каждом входе в систему, выйдите из режима настройки линии (команда **exit**) и завершите сеанс настройки:

#### 6) Настройка шифрования пароля, начального сообщения и отключение поиска сервера домена.

При просмотре действующей конфигурации пароли линии и привилегированного режима представляются открытым текстом. Для того чтобы убедиться в этом, введите команду **show running-config**.

a) Зашифровать все пароли

Для того чтобы убедиться, что теперь пароли зашифрованы, введите команду **show running-config**.

b) Для выдачи предупреждения при попытке входа на маршрутизатор настройте сообщение **MOTD**. ($AuthorizedAccessOnly!$)

c) Проверьте сообщение и пароли. Выйдите с маршрутизатора (для этого дважды введите команду **exit**). Перед запросом пароля выводится начальное сообщение. Введите пароль и вновь войдите в систему маршрутизатора

d) Отключить поиск в DNS из командной строки маршрутизатора.

e) Сохраните текущую конфигурацию в качестве начальной:

**CustomerRouter(config)#**end

**CustomerRouter#**copy run start

#### 7) Проверка настройки.

a) Закончите сеанс работы с терминалом с клиентского маршрутизатора **Cisco1841**

b) Войдите в клиентский маршрутизатор **Cisco1841**. Введите запрашиваемый пароль консоли.

c) Зайдите в привилегированный режим **EXEC**. Введите запрашиваемый пароль привилегированного режима