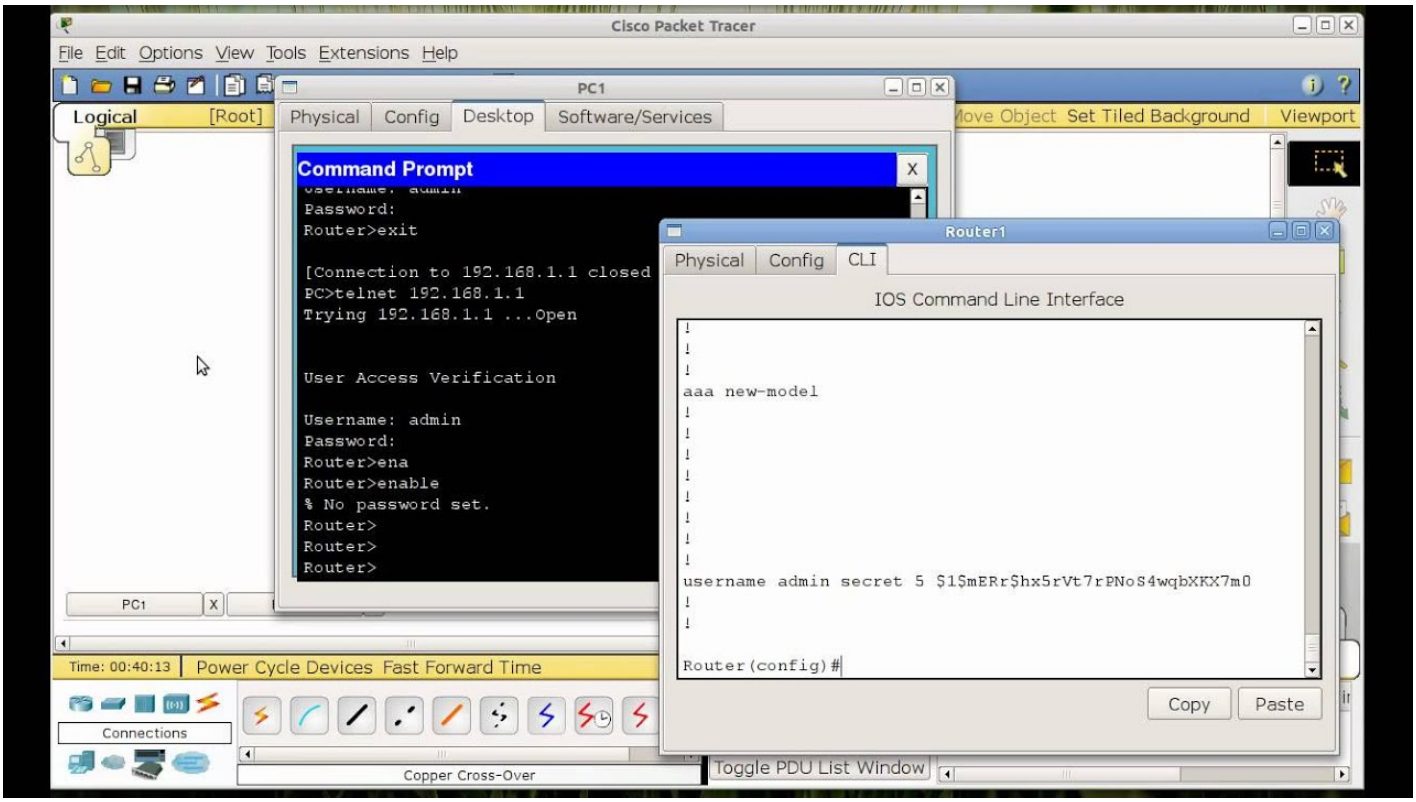
1. Сети для самых маленьких. Часть первая. Подключение к оборудованию cisco.

Мы в телеграм:
Системный администратор
Книги для Системного Администратора
Чат системных администраторов

Сегодня мы обратимся к части немного скучной, но важной для начинающих: как подключиться, поставить или сбросить пароль, войти по telnet. Также рассмотрим существующие программы — эмуляторы cisco и интерфейс оборудования.
Как и обещали, в этот раз всё по-взрослому: с видео.



Под катом то же в текстовой и чуть более подробной форме.
Итак, вот они приехали — заветные коробки с надписью Cisco на борту.

Среда

Начнём с того, в какой среде будем работать.

В данный момент есть два известных пакета программ, позволяющих моделировать сеть, построенную на оборудовании Cisco:

а) Цисковский же продукт Packet Tracer, который по идее свободно не распространяется. Это эмулятор и имеет лишь некоторые функции Cisco IOS. Вообще говоря, он сильно ограничен и многие вещи в нём реализованы лишь отчасти. Никаких тонких настроек. С другой стороны к настоящему моменту версия 5.3.2 поддерживает создание GRE-туннелей, протоколов динамической маршрутизации (и в их числе даже BGP!). Притом он очень прост в освоении и имеет в своём арсенале сервера (FTP, TFTP, DHCP, DNS, HTTP, NTP, RADIUS, SMTP, POP3), рабочие станции и свичи. Сейчас уже есть под Linux, хотя в былые времени он прекрасно запускался и из-под Wine.

б) Распространяемый по лицензии GNU GPL симулятор GNS3. В этом пакете необходимо загружать настоящие образы Cisco IOS. С одной стороны это плюс – вы работаете с настоящим интерфейсом cisco и ограничены лишь своей фантазией, существующими стандартами и производительностью рабочей станции, с другой, во-первых, эти IOS ещё нужно суметь достать, во-вторых, это более сложный продукт для понимания, и в-третьих, в нём есть только маршрутизаторы и «типа» коммутаторы.

Я считаю, что для знакомства с принципами лучше начать всё же с Packet Tracer'a, а потом переходить на тяжёлую артиллерию по мере надобности. Все мы не дети малые, где взять то, что нам нужно, рассказывать не будем.

Способы подключения

В Packet Tracer’е управлять оборудованием можно следующими способами:

- GUI
- CLI в окне управления
- Терминальное подключение с рабочей станции через консольный кабель
- telnet

Интерфейс последних трёх идентичный – отличается лишь способ подключения. Разумеется, GUI – не наш метод.
В реальной же жизни доступны:

- Telnet/ssh
- Терминальное подключение с рабочей станции через консольный кабель
- Web-интерфейс (Cisco SDM).

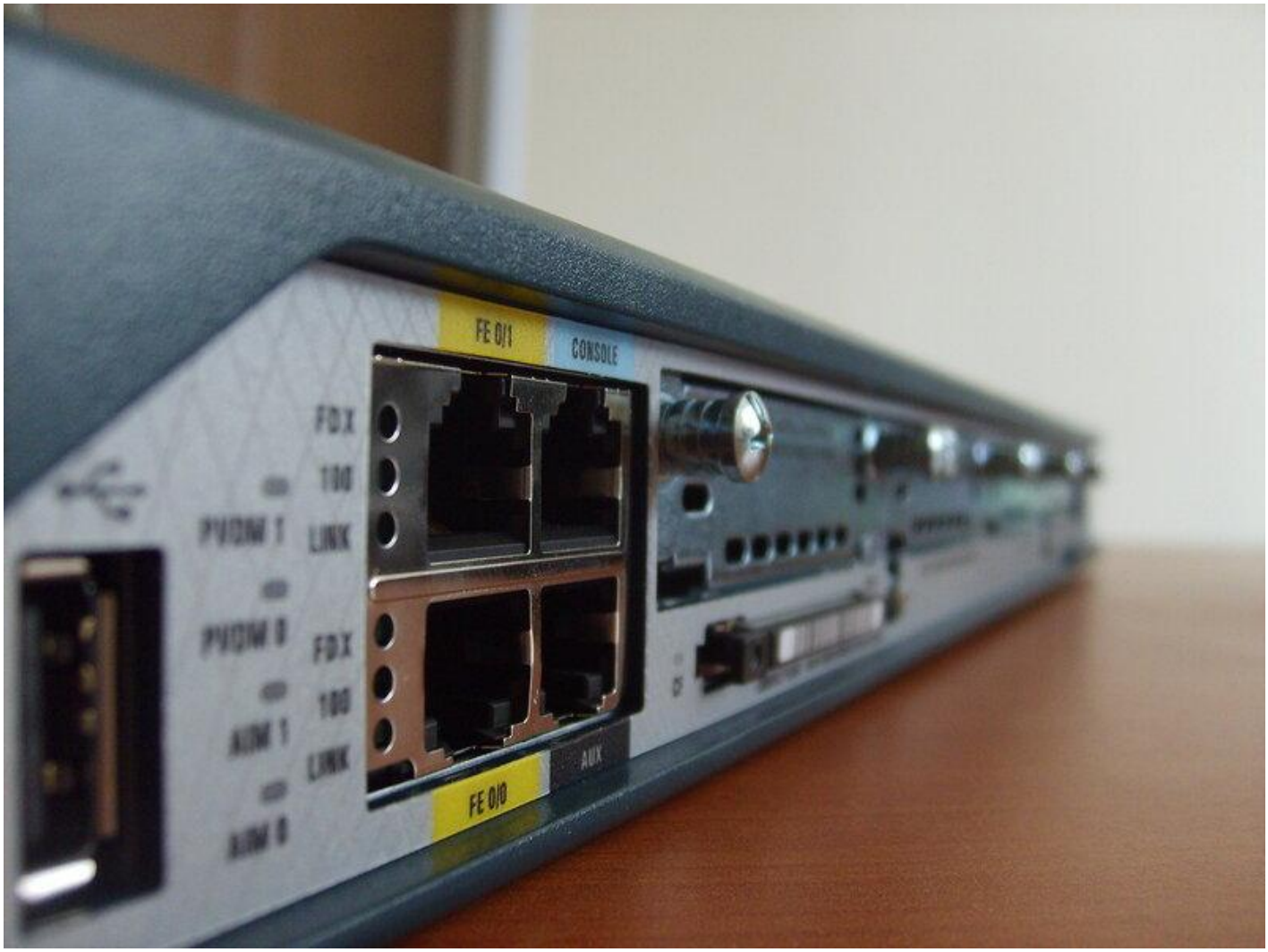
Последний вариант даже не упоминайте в приличном обществе. Даже если вы адепт мыши и браузера, очень не советую.
На своём примере при работе с другим оборудованием я сталкивался с тем, что настроенное через веб не

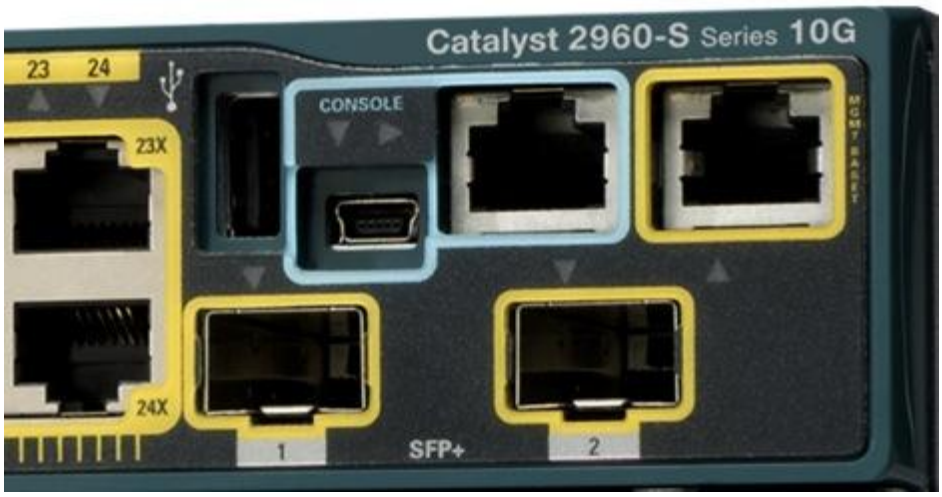
работает. Хоть ты тресни, но не работает. А у того же длинка вообще был баг в одной версии прошивки для свичей: если изменить настройки VLAN в веб-интерфейсе из под линукс, то свич становится недоступным для управления. Это официально признанная проблема).

Телнет – стандартная, всем известная утилита, как и ssh. Для доступа к cisco по этим протоколам нужно настроить пароли доступа, об этом позже. Возможность использования ssh зависит от лицензии IOS.

Управление по консоли

Ну вот принесли вы маршрутизатор, распечатали, питание на него дали. Он томно зашумел кулерами, подмигивает вам светодиодами своих портов. А чего дальше-то делать?
Воспользуемся один из древнейших и нестареющих способов управления практически любым *умным* устройством: консоль. Для этого вам нужен компьютер, само устройство и подходящий кабель.
Тут каждый вендор на что горазд. Какие только разъёмы они не используют: RJ-45, DB-9 папа, DB-9 мама, DB-9 с нестандартной распиновкой, DB-25.
У циски используется разъём RJ-45 на стороне устройства и DB-9 мама (для подключения к COM-порту) на стороне ПК.
Консольный порт выглядит так:





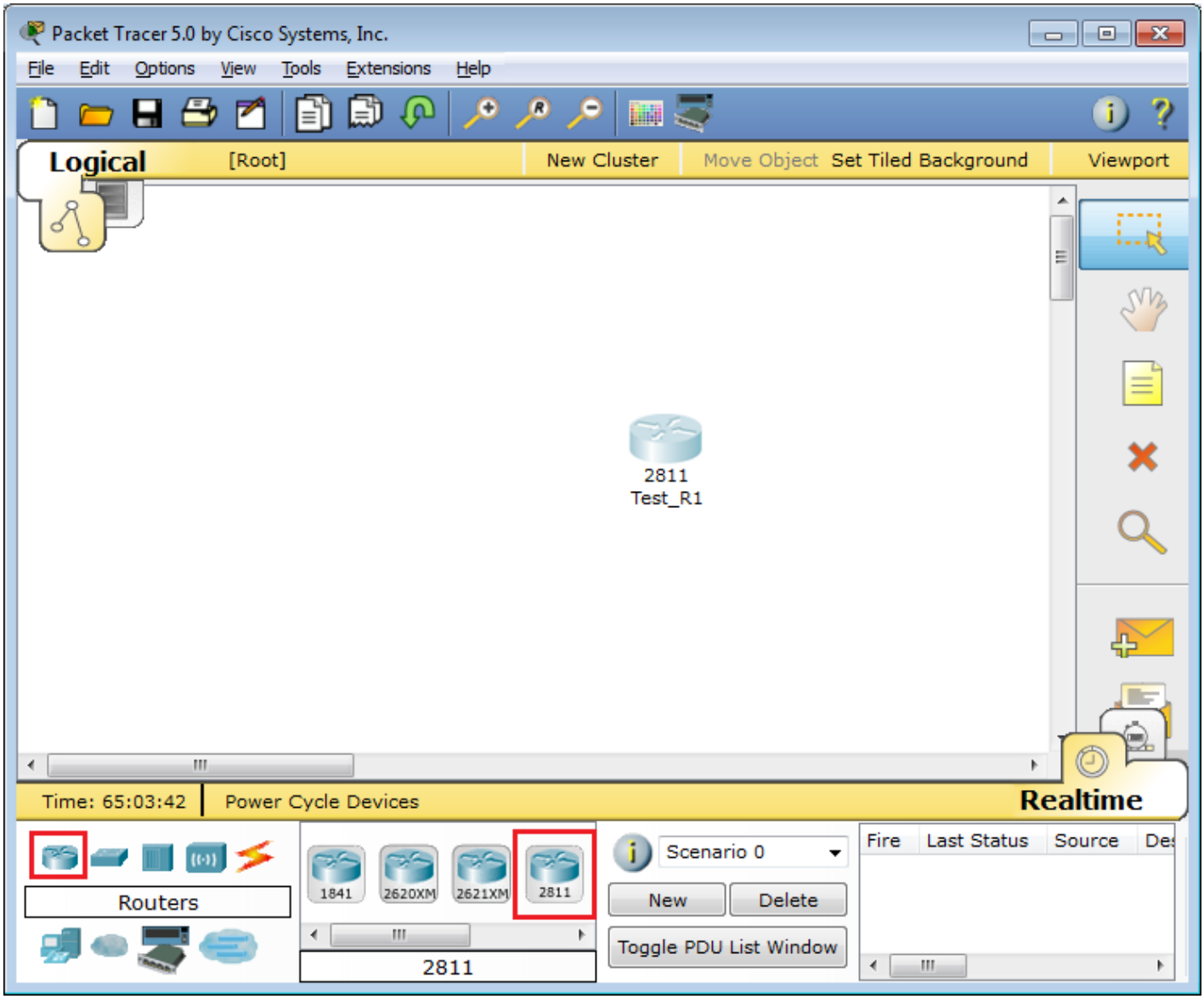
Всегда выделен голубым цветом. С недавних пор стало возможным управление по USB.
А это консольный кабель cisco:

Раньше он поставлялся в каждой коробке, теперь зачастую стоит отдельных денег. В принципе подходит аналогичный кабель от HP.
Проблема в том, что современные ПК зачастую не имеют COM-порта. На выручку приходят часто используемые конвертеры USB-to-COM:

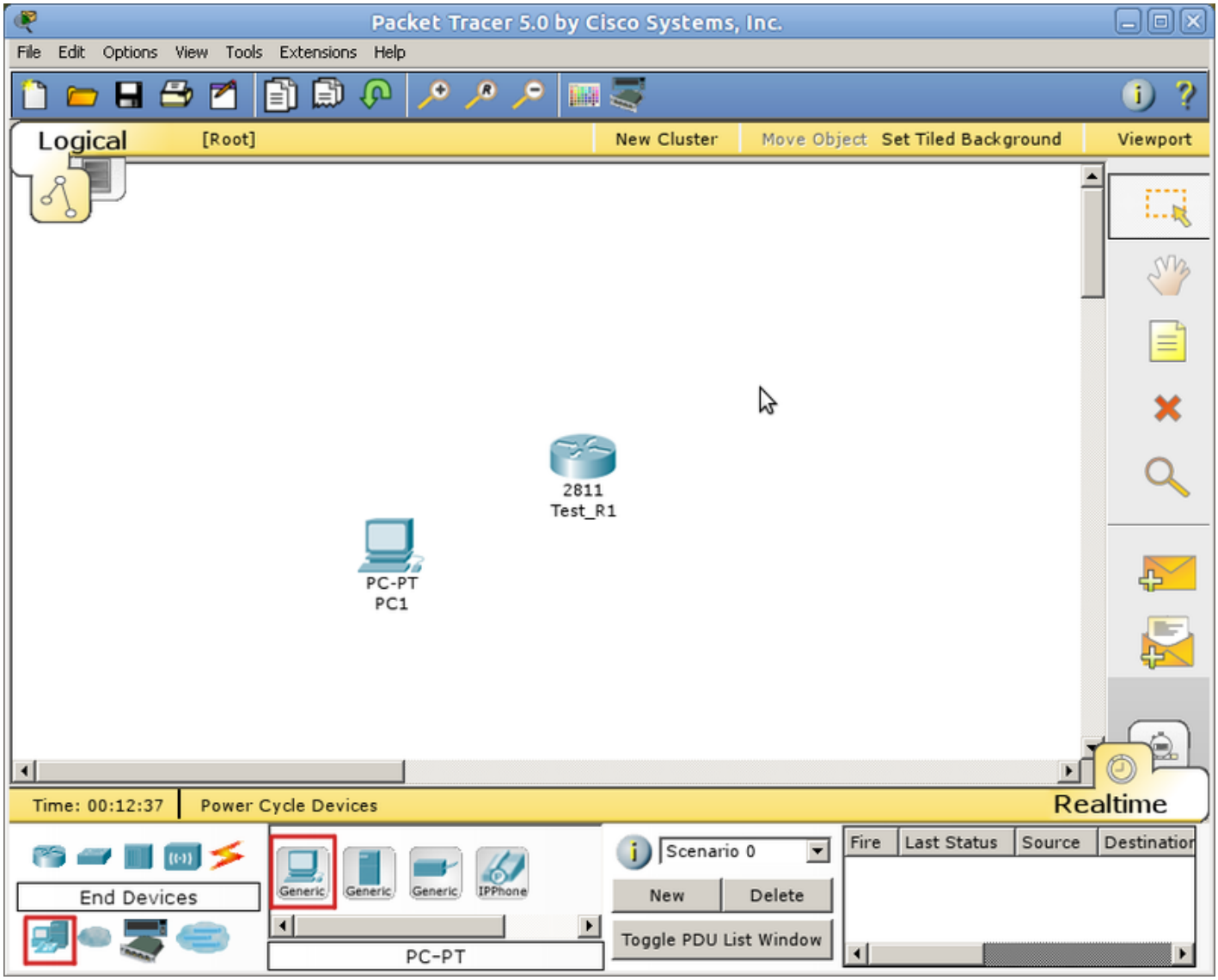
Либо редко используемые для этих целей конвертеры RS232-Ethernet

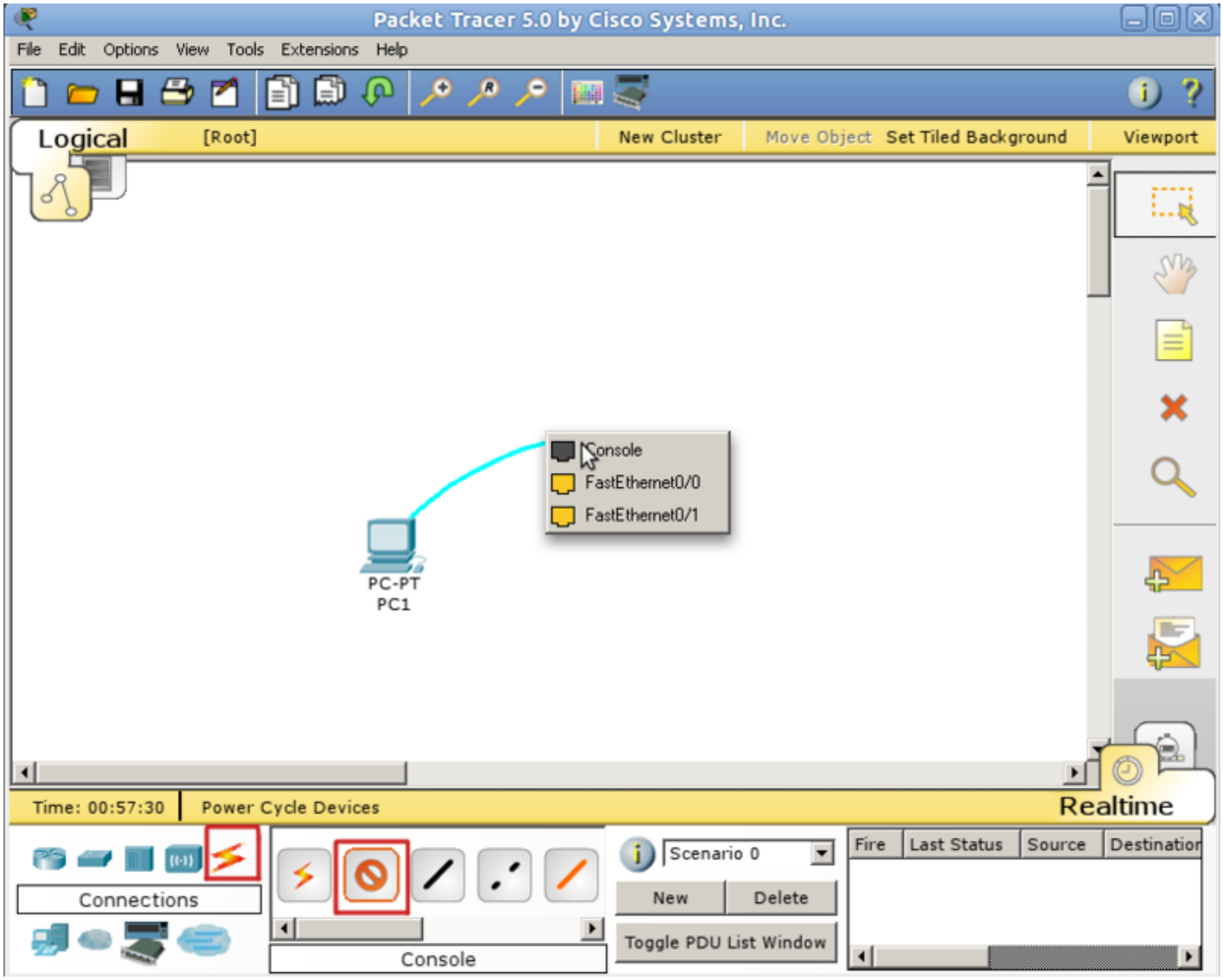
После того, как вы воткнули кабель, определили номер COM-порта, для подключения можно использовать Hyperterminal или Putty в Виндоус и Minicom в Линукс.

Управление через консоль доступно сразу, а вот для телнета нужно установить пароль. Как это сделать? Обратимся к PT.
Начнём с создания маршрутизатора: выбираем его на панели внизу и переносим на рабочее пространство. Даём какое-нибудь название

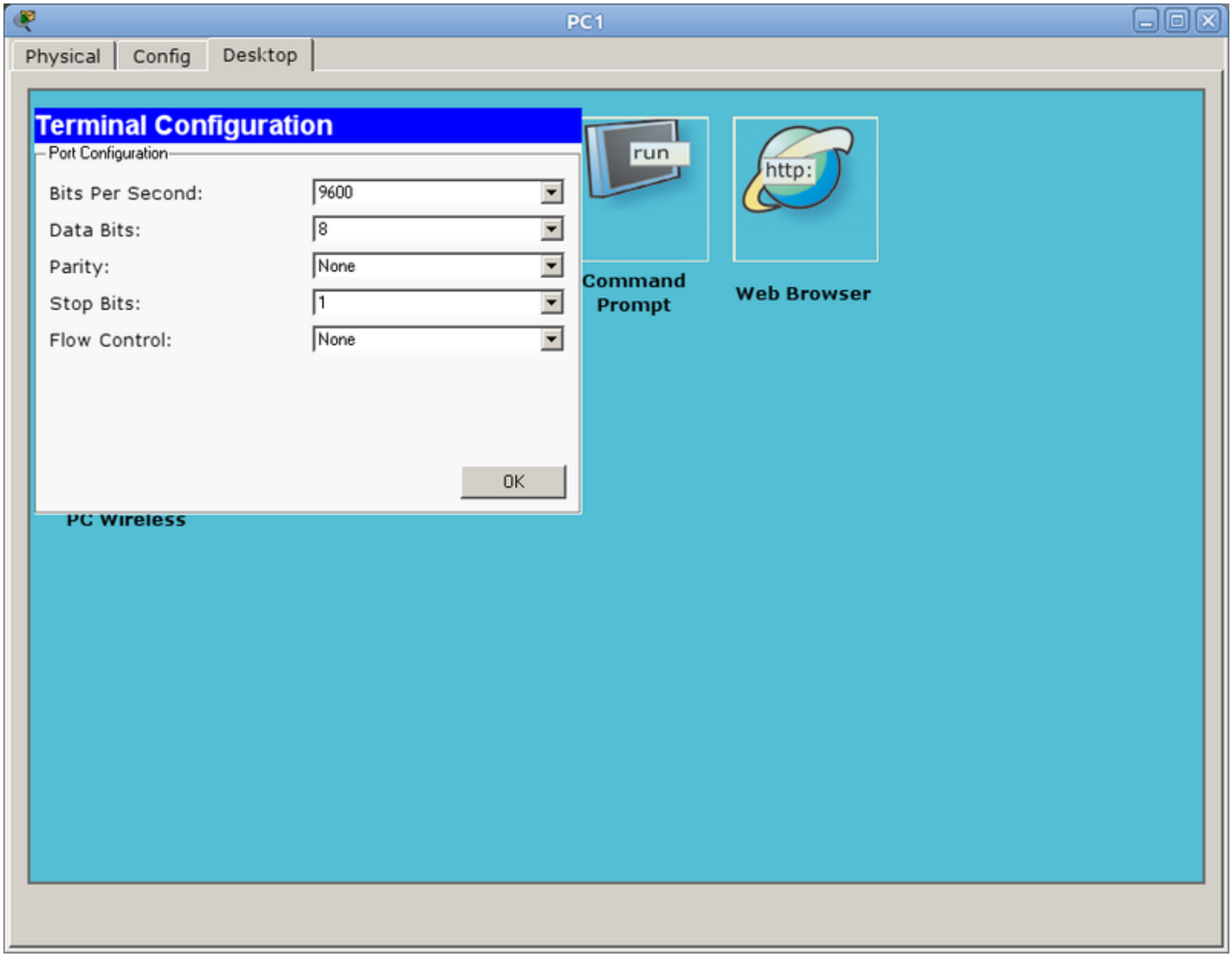


Что бы вы делали, если бы это был самый взаправдашний железный маршрутизатор? Взяли бы консольный кабель и подключились им в него и в компьютер. То же самое сделаем и тут:


Packet Tracer 5.0 by Cisco Systems, Inc.
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
2811
Test_R1
PC-PT
PC1
Time: 00:12:37
Power Cycle Devices
Realtime
End Devices
Generic
Generic
Generic
IPPhone
PC-PT
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination

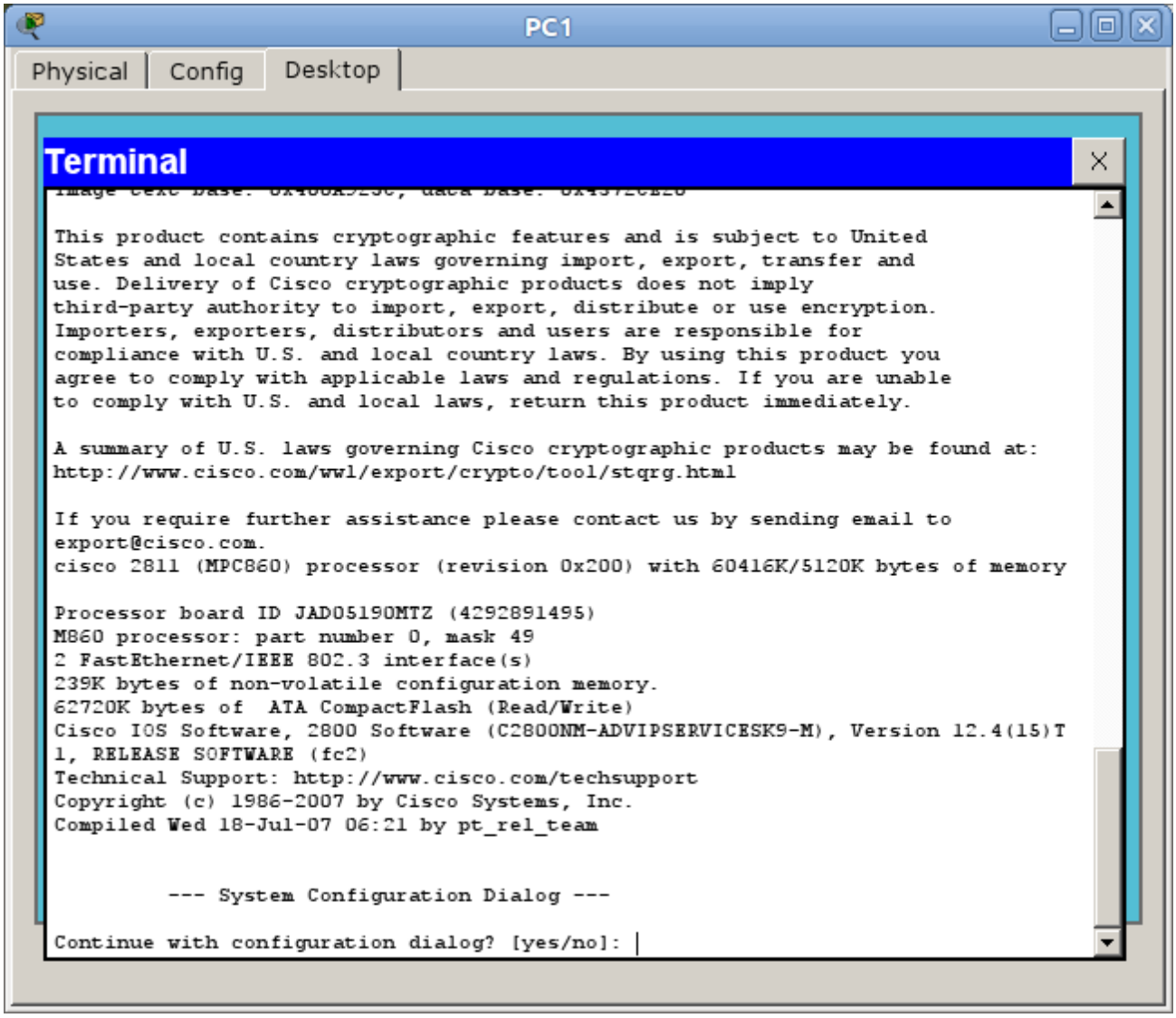


Кликом по компьютеру вызываем окно настройки, в котором нас интересует вкладка Desktop. Далее выбираем Terminal, где нам даётся выбор параметров



Впрочем, все параметры по умолчанию нас устраивают, и менять их особо смысла нет.

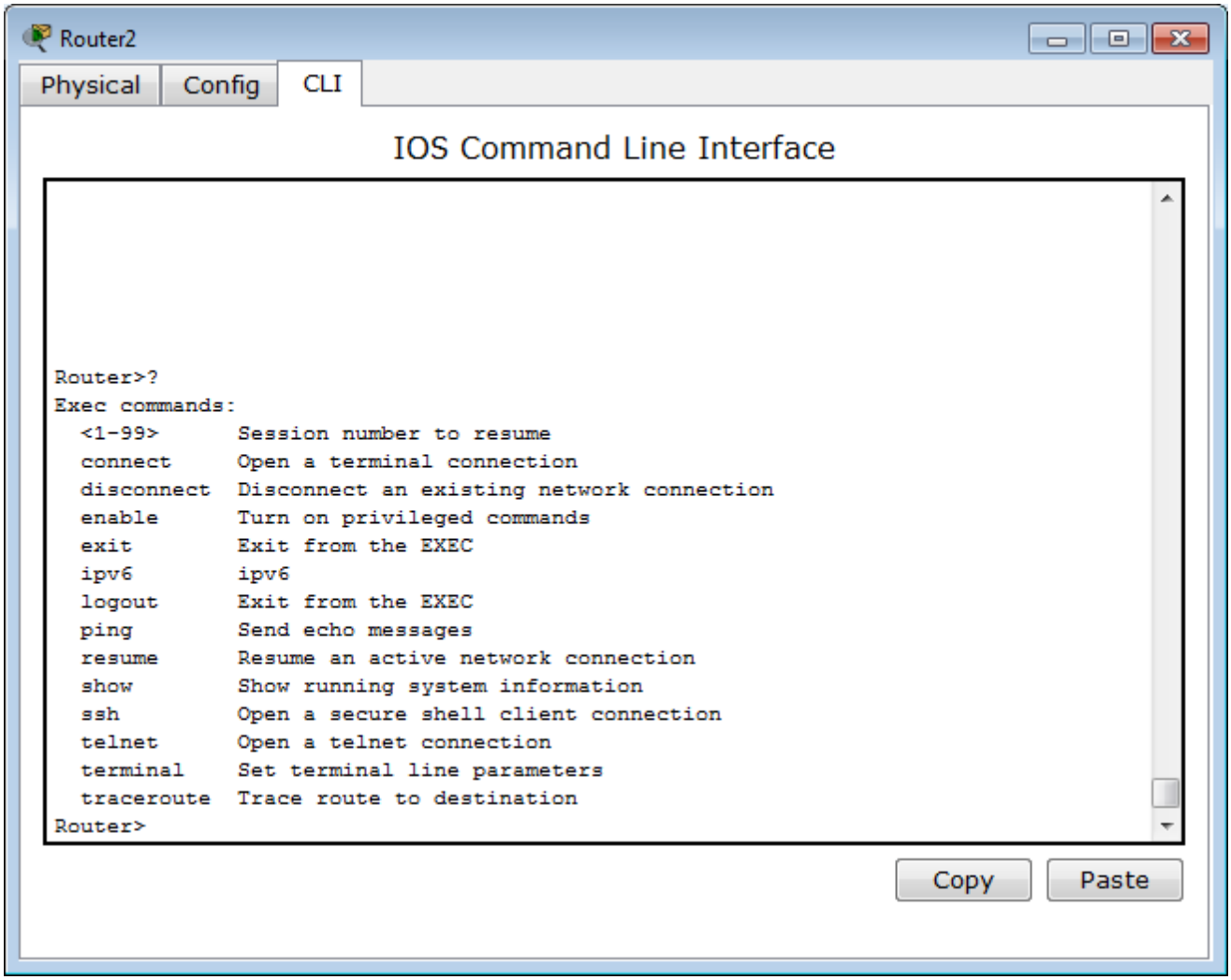
Если в энергонезависимой памяти устройства отсутствует конфигурационный файл (startup-config), а так оно и будет при первом включении нового железа, нас встретит Initial Configuration Dialog prompt:



Вкратце, это такой визард, позволяющий шаг за шагом настроить основные параметры устройства (hostname, пароли, интерфейсы). Но это неинтересно, поэтому отвечаем **no** и видим приглашение

Router>

Это стандартное совершенно для любой линейки cisco приглашение, которое характеризует **пользовательский режим**, в котором можно просматривать некоторую статистику и проводить самые простые операции вроде пинга. Ввод знака вопроса покажет список доступных команд:



Грубо говоря, это режим для сетевого оператора, инженера первой линии техподдержки, чтобы он ничего там не повредил, не напортачил и лишнего не узнал.
Гораздо большие возможности предоставляет режим с говорящим названием **привилегированный**. Попасть в него можно, введя команду **>enable**. Теперь приглашение выглядит так:

Router#

Здесь список операций гораздо обширнее, например, можно выполнить одну из наиболее часто используемых команд, демонстрирующую текущие настройки устройства ака “конфиг” **#show running-config**. В привилегированном режиме вы можете просмотреть всю информацию об устройстве.

Прежде, чем приступать к настройке, упомянем несколько полезностей при работе с cisco CLI, которые могут сильно упростить жизнь:
— Все команды в консоли можно сокращать. Главное, чтобы сокращение однозначно указывало на команду. Например, **show running-config** сокращается до **sh run**. Почему не до **s r**? Потому, что **s** (в пользовательском режиме) может означать как команду **show**, так и команду **ssh**, и мы получим сообщение об ошибке *% Ambiguous command: «s r»* (неоднозначная команда).

— Используйте клавишу Tab и знак вопроса. По нажатию Tab сокращенная команда дописывается до полной, а знак вопроса, следующий за командой, выводит список дальнейших возможностей и небольшую справку по ним (попробуйте сами в PT).

— Используйте горячие клавиши в консоли:

Ctrl+A — Передвинуть курсор на начало строки
Ctrl+E — Передвинуть курсор на конец строки
Курсорные Up, Down — Перемещение по истории команд
Ctrl+W — Стереть предыдущее слово
Ctrl+U — Стереть всю линию
Ctrl+C — Выход из режима конфигурирования
Ctrl+Z — Применить текущую команду и выйти из режима конфигурирования
Ctrl+Shift+6 — Остановка длительных процессов (так называемый escape sequence)

— Используйте фильтрацию вывода команды. Бывает, что команда выводит много информации, в которой нужно долго копаться, чтобы найти определённое слово, например.
Облегчаем работу с помощью фильтрации: после команды ставим **|**, пишем вид фильтрации и, собственно, искомое слово(или его часть). Виды фильтрации (ака модификаторы вывода):

begin — вывод всех строк, начиная с той, где нашлось слово,
section — вывод секций конфигурационного файла, в которых встречается слово,
include — вывод строк, где встречается слово,
exclude — вывод строк, где НЕ встречается слово.

Но вернемся к режимам. Третий главный режим, наряду с пользовательским и привилегированным: **режим глобальной конфигурации**. Как понятно из названия, он позволяет нам вносить изменения в настройки устройства. Активируется командой **#configure terminal** из привилегированного режима и демонстрирует такое приглашение:

Router(config)#

В режиме глобальной конфигурации не выполняются довольно нужные порой команды других режимов (тот же show running-config, ping, etc.). Но есть такая полезная штука, как **do**. Благодаря ей мы можем, не выходя из режима конфигурирования, выполнять эти самые команды, просто добавляя перед ними do. Примерно так:

Router(config)#do show running-config

Настройка доступа по Telnet

Из этого-то режима мы и настроим интерфейс для подключения компьютера через telnet:
Команда для перехода в **режим конфигурации интерфейса** FastEthernet 0/0:

Router(config)# interface fa0/0

По умолчанию все интерфейсы отключены (состояние administratively down). Включаем интерфейс:

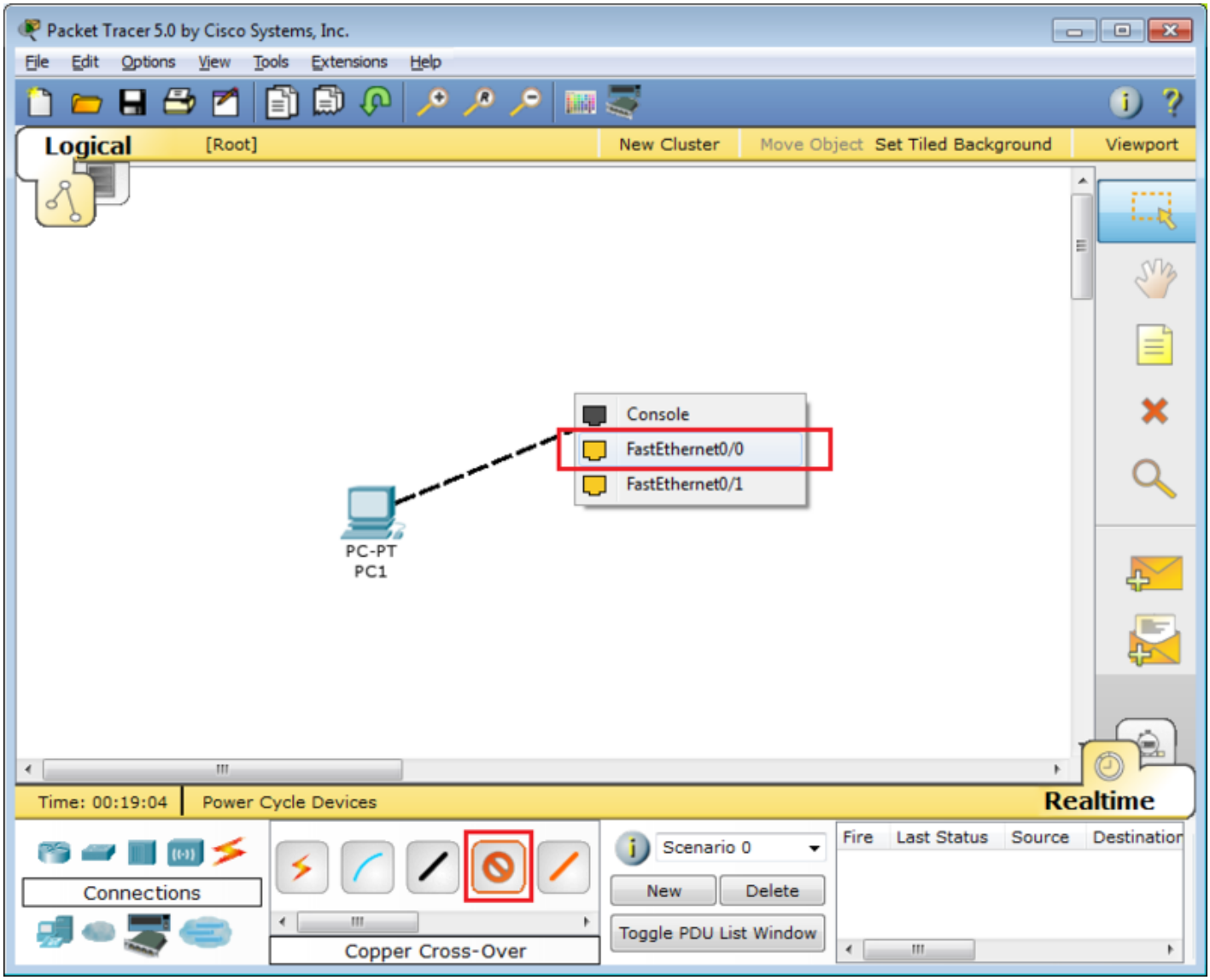
Router(config-if)#no shutdown

Настроим IP-адрес:

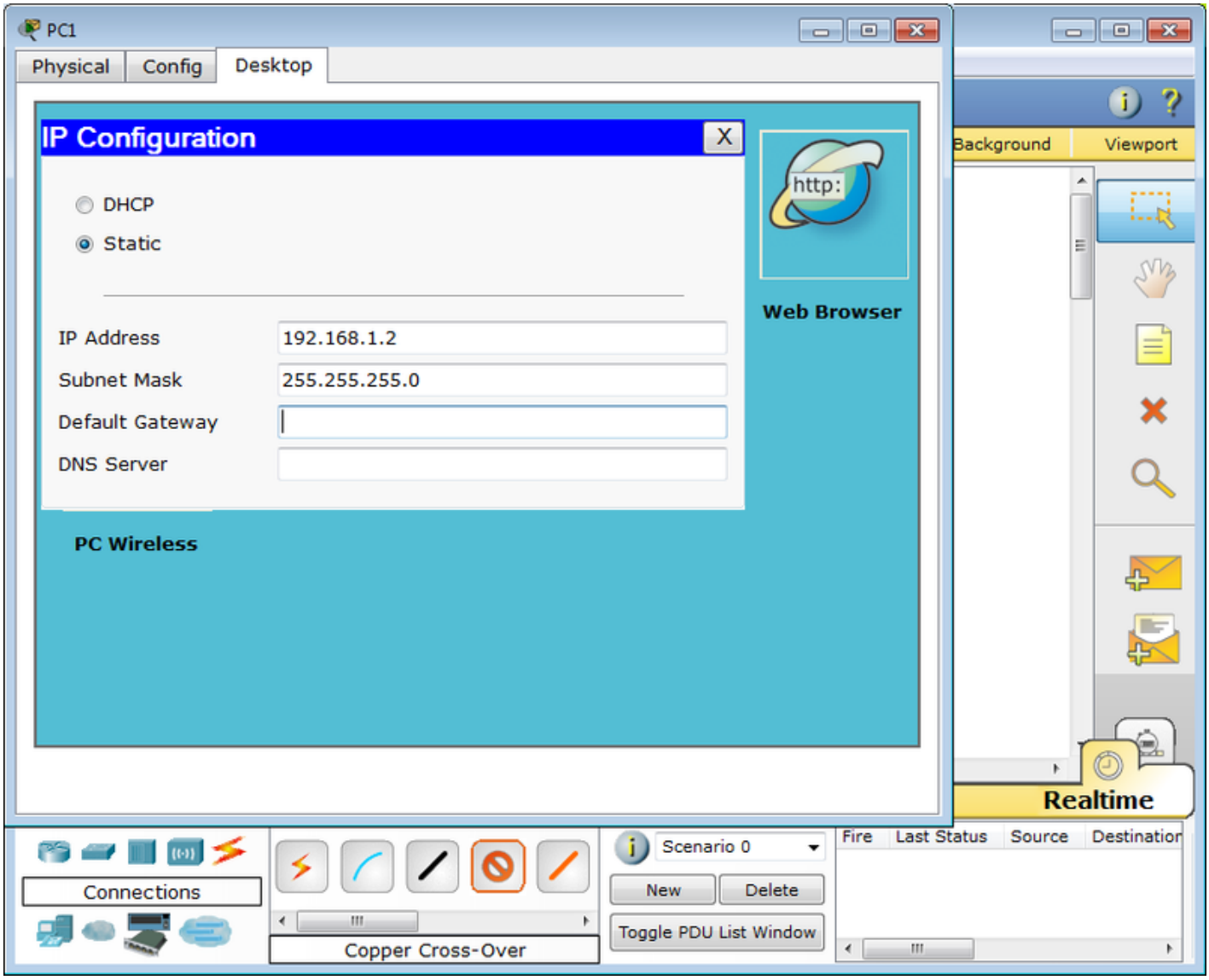
Router(config-if)#ip address 192.168.1.1 255.255.255.0

shutdown — означает “выключить интерфейс”. Соответственно, если вы хотите отменить действие команды, то используйте слово **no** перед ней. Это правило общее для CLI и применимо к большинству команд.

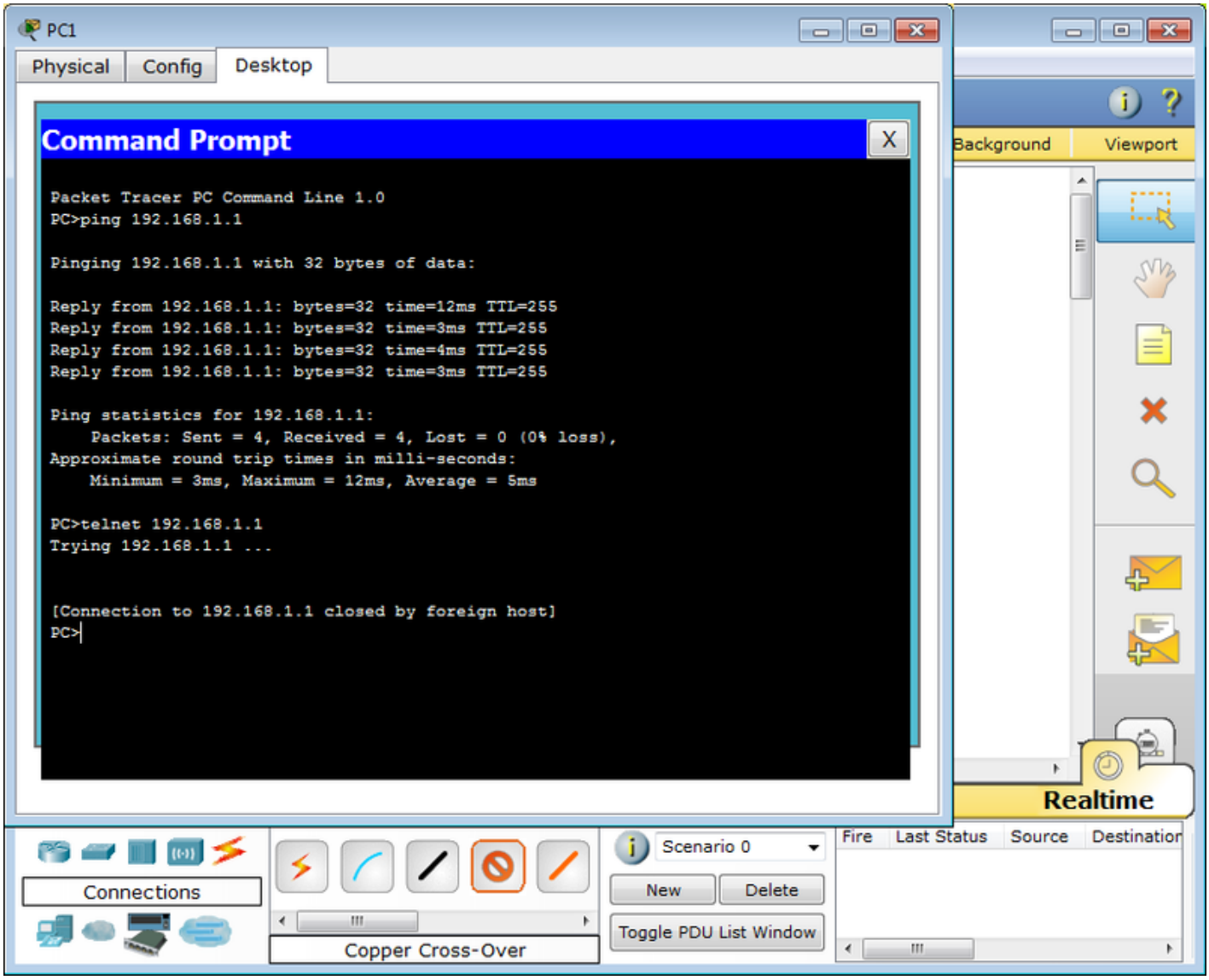
Подключаемся. Для этого надо использовать кроссоверный кабель. (Хотя в реальной жизни это зачастую уже необязательно – все карточки умеют понимать приём/передачу, однако встречаются ещё маршрутизаторы, порты которых не поднимаются при использовании неправильного типа кабеля — так что будьте внимательны)



Настраиваем IP-адрес компьютера через Desktop.



И пробуем подключиться, выбрав Command Prompt в панели Desktop:



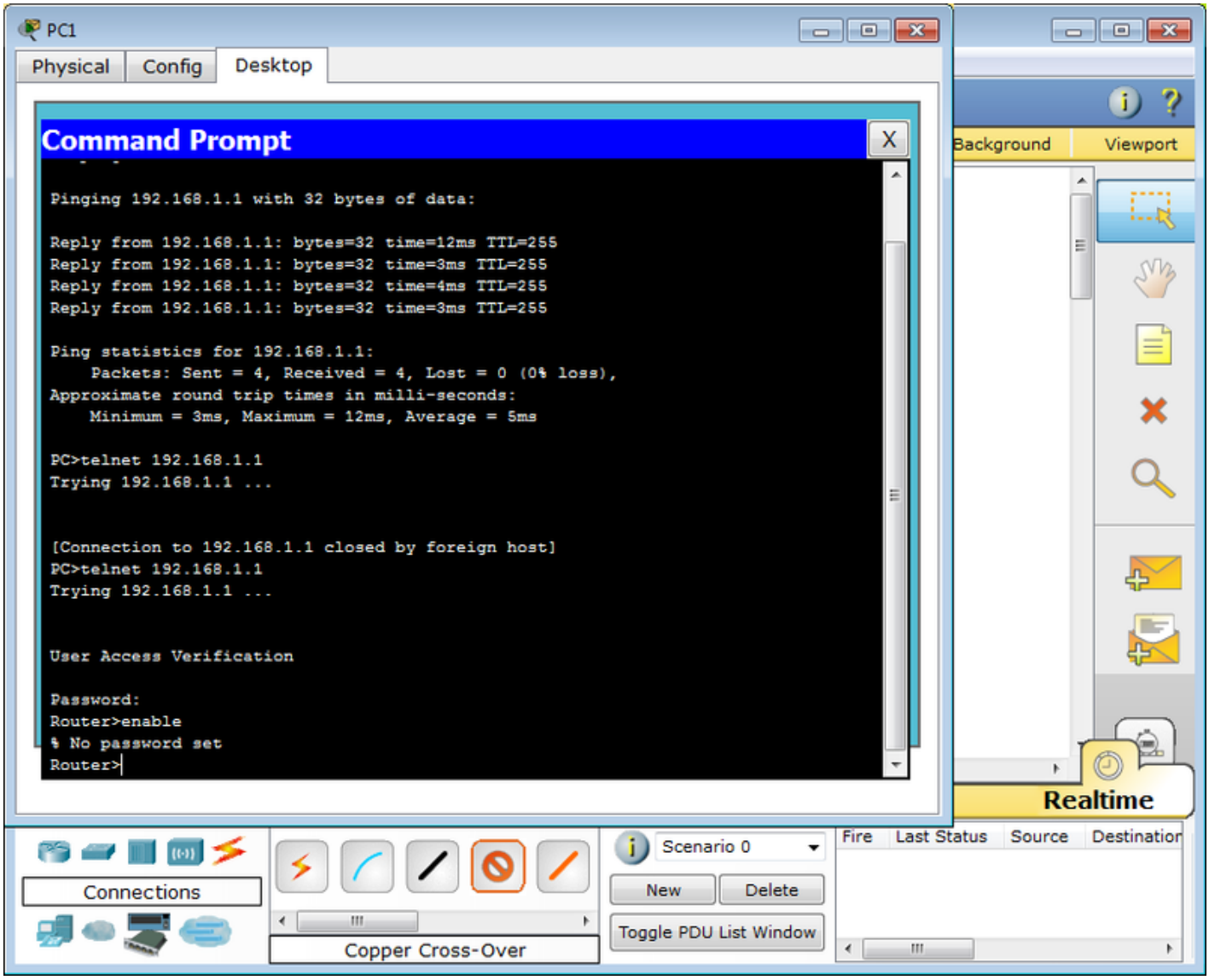
Как и ожидалось, циска не пускает без пароля. В реальной жизни обычно выдаёт фразу “Password required, but none set”

Пароли

Подключение по telnet или ssh называется виртуальным терминалом (vt) и настраивается следующим образом:

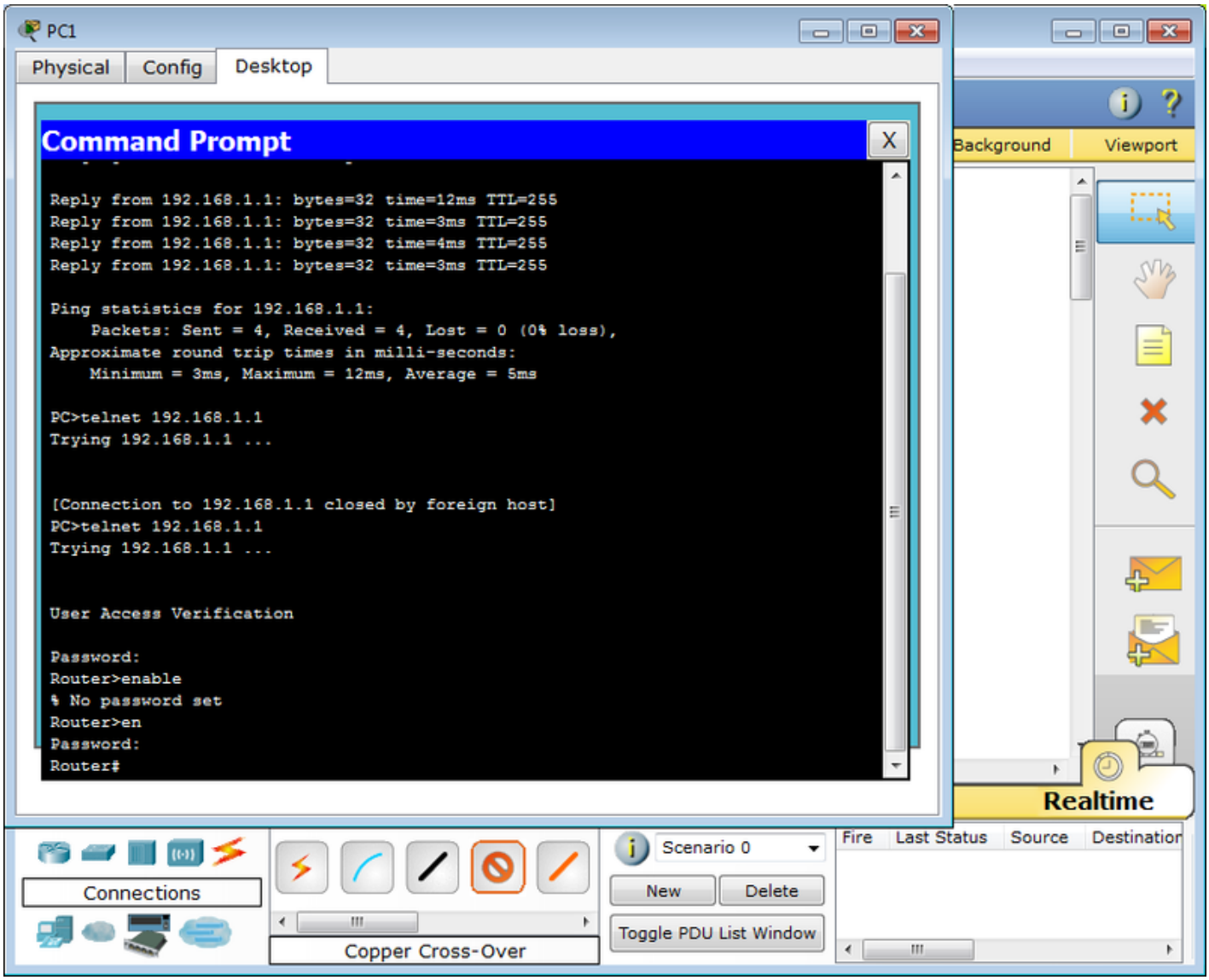
Router(config)#line vty 0 4
Router(config-line)#password *cisco*
Router(config-line)#login

0 4 — это 5 пользовательских виртуальных терминалов=telnet сессий.
Этого уже достаточно, чтобы попасть в пользовательский режим, но недостаточно для привилегированного:



Настроим пароль для enable-режима:

Router(config)#enable secret *test*



Чем отличается *secret* от *password*? Примерно тем же, чем ssh от telnet. При настройке *secret* пароль хранится в зашифрованном виде в конфигурационном файле, а *password* – в открытом. Поэтому рекомендуется использование *secret*.
Если вы всё-таки задаёте пароль командой **password**, то следует применить так же **service password-encryption**, тогда ваш пароль в конфигурационном файле будет зашифрован:

line vty 0 4
password 7 08255F4A0F0A0111

Один мой знакомый рассказал мне историю:
Стоял он как-то курил возле одного из своих узлов, находящемся в жилом доме. С сумкой для инструментов, ноутбук в руках. Вдруг подходит двое алкашей с пакетом и предлагают купить, раскрывая пакет и показывая какой-то свич. Просят 500 рублей. Ну он купил. По меткам и модели свича парень сделал вывод какому провайдеру он принадлежит. Пришёл домой, начал ковырять — телнет закрыт, консоль запаролена. Слил конфиг по snmp. Пароли в открытом виде хранятся, имя с головой выдаёт провайдера. С их админом он знаком лично, позвонил ему вместо “Здрасьти” выдал логин и пароль в трубку. Слышно

было, как скрипел мозг первые секунд 20: везде аксес-листы, авторизация, привязка к мак-адресу. Как?! В общем, всё хорошо, что хорошо кончается.

Немного об этом можно почитать здесь. Ну или чуть более по-русски, тут.

Хотим обратить ваше внимание:
сейчас принятно настраивать доступы не через виртуальные терминалы, а командами **#username** и **#aaa new-model**. В версии PT 5.3.2 они уже есть и вполне работают.
Для этого нужно выполнить:

Router(config)#aaa new-model
Router(config)#username admin password 1234

Первая команда служит для активации новой модели AAA (Authentication, Authorization, Accounting). Это нужно для того, чтобы была возможность использовать для аунтетификации на устройстве RADIUS или TACACS сервер. Если отдельно это не настроено, то будет использоваться локальная база пользователей, задаваемая командой **username**.

***Будьте внимательны**: приоритет команды aaa new-model выше, чем команд виртуальных терминалов и поэтому даже несмотря на то, что у вас настроен password в режиме line vty, если у вас не будет пользователей в локальной базе, зайти на устройство удалённо уже не получится.*

Теперь при подключении маршрутизатор запросит имя пользователя и соответствующий ему пароль.

При более глубокой настройке *line vty* существует одна опасность.
Есть такой параметр: **access-class**. Его настройка позволяет ограничить IP-адреса, с которых возможно подключение. И вот однажды я, как умная маша, решил заняться безопасностью в сети и на всём почти оборудование понаставил эти аксес-листы, чтобы комар не пролетел. В один прекрасный момент пришлось выехать в поле и в тот день я проклял свою аккуратность – никуда не мог достучаться – малейшей лазейки не оставил. В общем будьте с этой командой внимательны или оставляйте для себя лазейки.
При работе с access-list'ами и прочими опасными вещами, неправильная настройка которых может лишить вас доступа к устройству, можно использовать замечательную команду **reload in *min***, где *min* время в минутах. Эта команда перезагрузит устройство по истечении указанного времени, если ее не прервать командой **reload cancel**. Т.е. схема работы такова: вы удаленно копаете что-то, что может в теории (закон Мерфи не забываем) прервать ваш сеанс связи с устройством. Сохраняем текущий (рабочий) конфиг в startup-config (он используется при загрузке), ставим reload in 15, вводим ключевую команду, относительно которой у нас сомнения ;-), и получаем обрыв связи, худшие опасения оправдались. Ждем 15 минут, устройство перегружается с рабочим конфигом, коннект — вуаля, связь есть. Либо (если связь не прервалась) проверяем, что все работает, и делаем **reload cancel**.

Если вы хотите ограничить паролем доступ через консольный порт, вам понадобятся команды

Router(config)#line console 0
Router(config-line)#login
Router(config-line)#password *cisco*

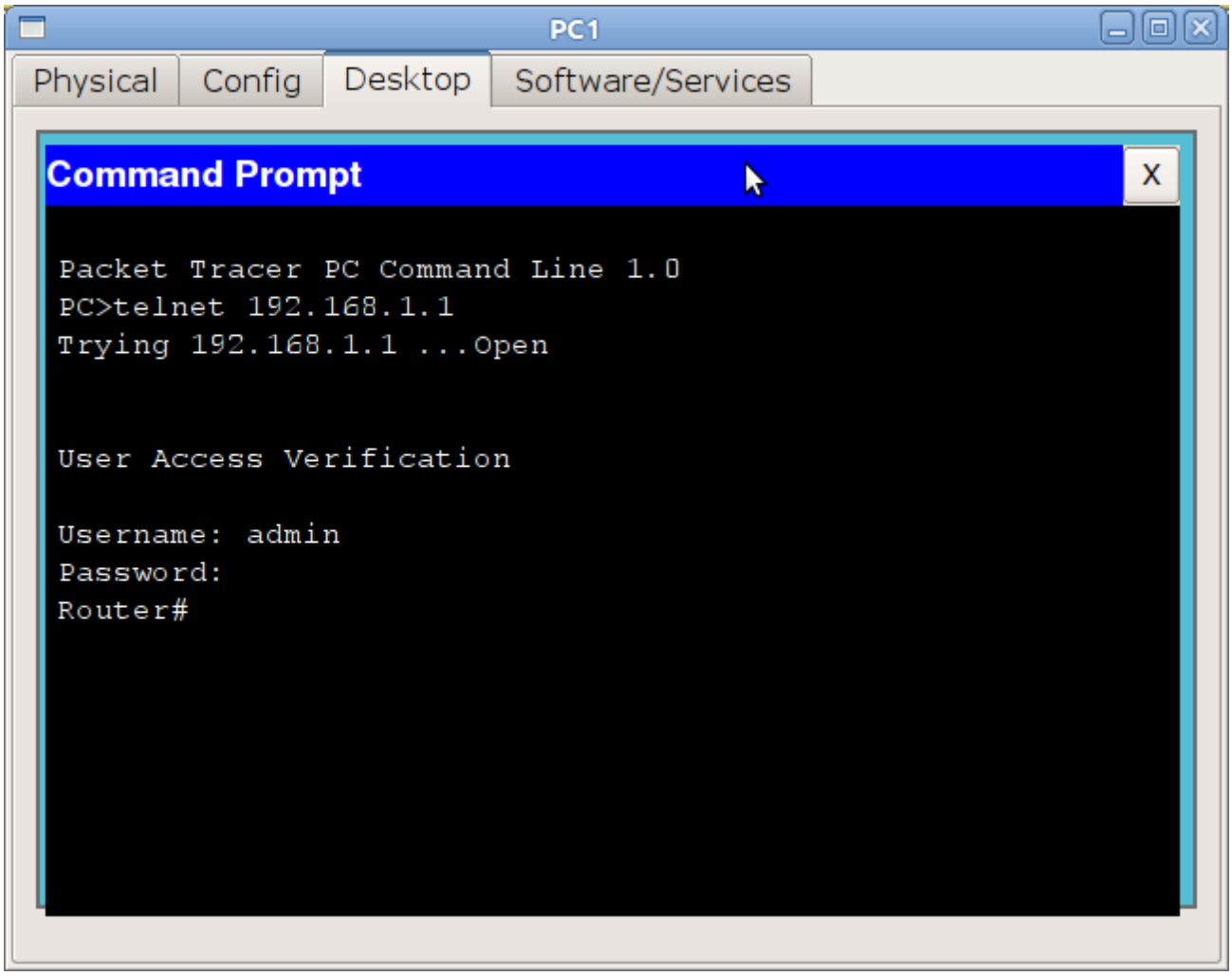
Privilege Level

Ещё один важный момент, которому в статьях уделяют мало внимания: privelege level.
Как понятно из латинского звучания — это уровень прав пользователя. Всего существует 16 уровней: 0-15.
privilege level 0 — это команды disable, enable, exit, help и logout, которые работают во всех режимах
privilege level 1 — Это команды пользовательского режима, то есть как только вы попадаете на циску и увидите приглашение **Router>** вы имеете уровень 1.
privilege level 15 — Это команды привилегированного режима, вроде, как root в Unix'ax

Пример1

Router(config)#line vty 0 4
Router(config-line)privilege level 15

После входа на маршрутизатор при такой настройке вы сразу увидите Router# со всеми вытекающими правами.



Все уровни со 2 по 14 настраиваются вручную. То есть, например, вы можете дать добро пользователю с privelege level 2 на выполнение команды **show running-config**

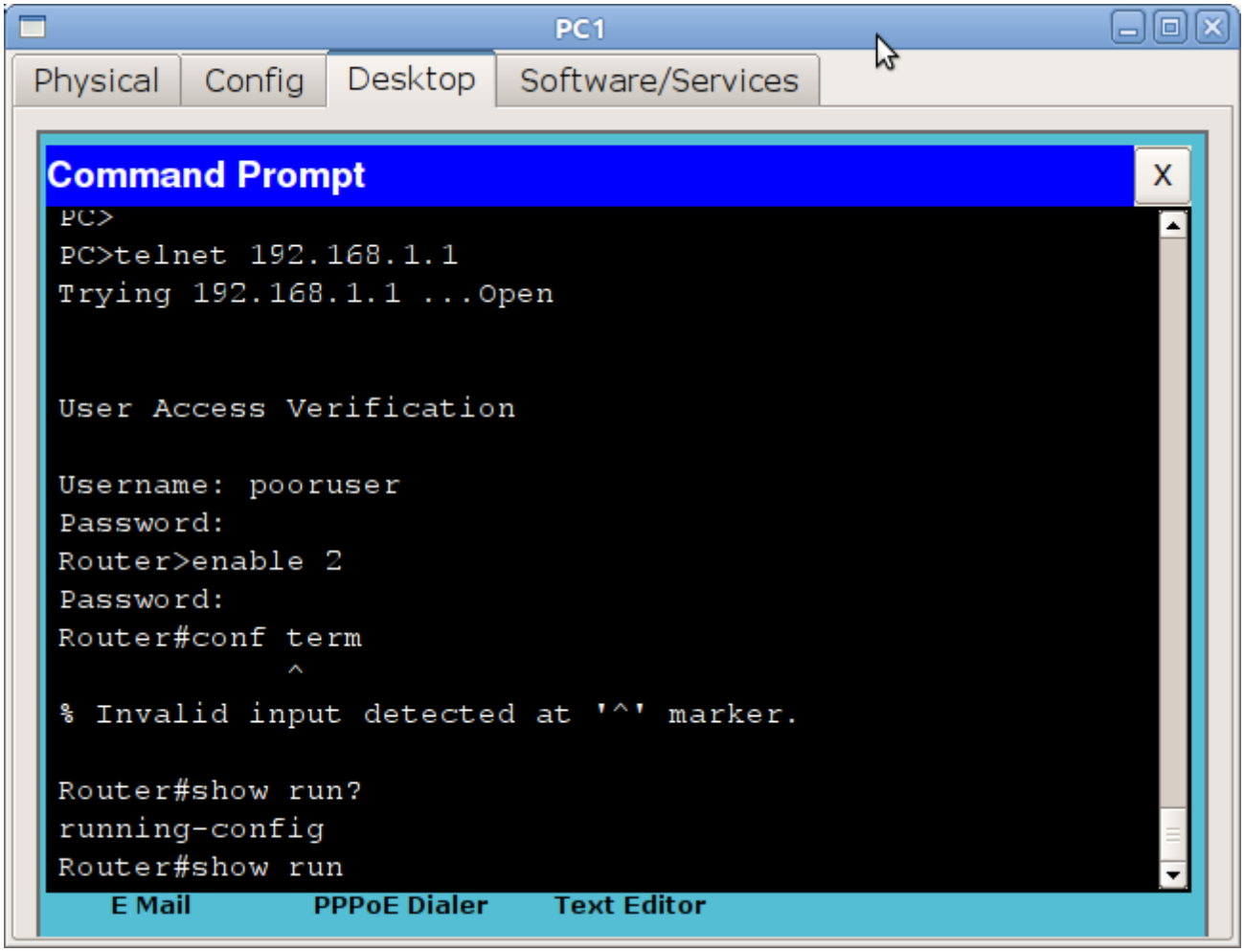
Пример2

Настроить права для конкретного пользователя поможет уже упомянутая прежде команда **username**

Router(config)#username pooruser privilege 2 secret poorpass
Router(config)#privilege exec level 2 show running-config
Router(config)#enable secret level 2 l2poorpass

В первой строке назначаем уровень прав пользователю, во второй команду, разрешенную для этого уровня, в третьей задаём пароль для входа в привилегированный режим с этим уровнем.

После этого из пользовательского режима вы можете выполнить команду **enable 2** и введя пароль *l2poorpass* попасть в привилегированный режим, в котором будут доступны все команды уровня 1 + команды уровня 2.



Для чего это может быть нужно? В российских реалиях практически ни для чего, потому что обычно на устройство нужно заходить инженерам сразу с полными правами. Ну разве что 15-й уровень ставят, чтобы двойную аутентификацию не проходить. А все другие уровни опять же для того, чтобы персонал младшего состава (техподдержка, например) мог зайти и промониторить какие-то параметры или настроить некритичную функцию.

SSH

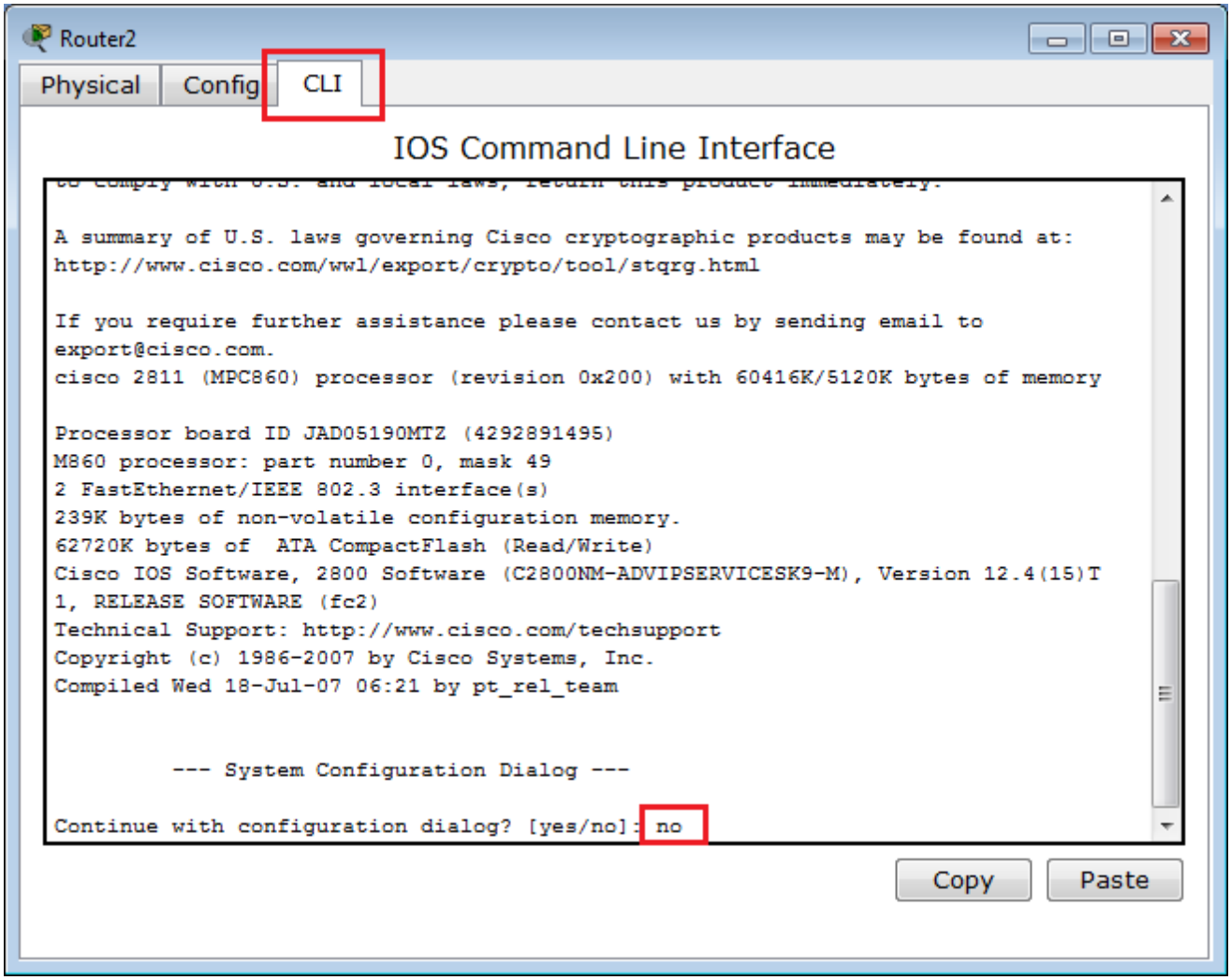
Нельзя не упомянуть о том, что telnet — протокол незащищённый и передаёт пароль и данные в открытом виде. С помощью любого анализатора пакетов можно вычислить пароль.
Поэтому крайне рекомендуем использовать ssh — любые устройства cisco с не самой урезанной прошивкой способны выступать ssh-сервером.
Следующий набор команд позволит вам включить ssh и отключить доступ по telnet:

```
Router(config)#hostname R0
R0(config)#ip domain-name cisco-dmn
R0(config)#crypto key generate rsa
R0(config)#line vty 0 4
R0(config-line)#transport input ssh
```

Имя хоста должно отличаться от Router, обязательно должно быть задано имя домена. Третьей строкой генерируется ключ и далее разрешается только ssh. Длина ключа должна быть более 768 бит, если вы желаете использовать ssh версии 2, а вы желаете этого. Всё.

*Ещё одно финальное **внимание** новичкам: не забывайте о команде **write memory** — это сохранение текущей конфигурации. Впрочем, достаточно два раза обжечься, забыв сохранить, чтобы навсегда заработать иммунитет к этому — кто кодил по ночам или писал курсовую, тот поймёт.*

Используя PT, мы будем настраивать оборудование не через терминал или телнет, а непосредственно через CLI устройства, которое вызывается кликом по иконке роутера — так удобнее:



Ну и на сладенькое: сброс пароля

Так, а что же делать, если на стол легла вам бушная циска с неизвестным паролем или вы очень невовремя забыли его? Вообще-то это многократно описано и легко гуглится, но повторить это необходимо. Практически на любом сетевом устройстве есть возможность сбросить пароль, имея физический доступ. Если сделать это невозможно или это отдельная платная услуга, то скорее всего в ваших руках находится какая-то русская поделка (не в обиду, конечно, нашим производителям, но дважды я такие строки читал в документации:))

Итак, cisco:

1) Подключаетесь к устройству консольным кабелем,

2) Отправляете его в ребут (хоть по питанию, хоть командой **#reload**)

3) Когда на экране побежит такая строчка ########...###, означающая загрузку образа (40-60 секунд после включения), необходимо отправить сигнал *Break*. Как это сделать в разных программах читать тут. Вы попадаете в режим ROMMON.

4) В этом режиме введите команду: **confreg 0x2142**, она заставит устройство игнорировать startup-config при загрузке.

5) Введите **reset** для перезагрузки

6) После загрузки running-config будет девственно чистым, а startup-config содержит по-прежнему последнюю сохранённую конфигурацию. Сейчас самое время поменять пароль или слить конфиг.

7) Самое важное: **верните обратно регистры**:

Router(config)#config-register 0x2102

Если вы этого не сделаете, то вся ваша конфигурация будет актуальна до первого ребута) И хорошо, если это устройство стоит рядом, и вы вспомните, что накосячили. Мне не повезло)

В следующей статье мы обратимся к вланам и локальной сети. Обязательно к прочтению:
OSI.
VLAN

Мы в телеграм:
Системный администратор
Книги для Системного Администратора
Чат системных администраторов