

Министерство образования и науки РФ
Севастопольский государственный университет

**ИССЛЕДОВАНИЕ СИСТЕМЫ КОМАНД
IOS И СПОСОБОВ КОНФИГУРАЦИИ
СЕТЕВОГО ОБОРУДОВАНИЯ**

**Методические указания
к выполнению лабораторной работы №1
по дисциплине “Архитектура
инфокоммуникационных систем и сетей”**

Для студентов, обучающихся по направлению 09.03.02
"Информационные системы и технологии"
по учебному плану подготовки бакалавров
дневной и заочной форм обучения

**Севастополь
2015**

1. Общие сведения о Cisco Packet Tracer

Симулятор Packet Tracer поддерживает интерфейс командной строки Cisco IOS для конфигурирования устройств. Packet Tracer дополняет представленное физическое оборудование, позволяя создавать виртуальные сети с практически неограниченным количеством устройств. Учебная среда на основе имитационных моделей развивает навыки устранения неисправностей в сети, позволяет применять творческий подход к решению задач.

Симулятор позволяет легко демонстрировать сложные принципы и проекты сетевых систем. С помощью этой программы можно научиться создавать, настраивать, изучать сети и устранять неполадки, используя виртуальное оборудование и модели соединений.

Программное решение Packet Tracer позволяет моделировать работу различных сетевых устройств: маршрутизаторов, коммутаторов, точек беспроводного доступа, персональных компьютеров, сетевых принтеров и т.д. Интерактивное взаимодействие с симулятором дает весьма правдоподобное ощущение настройки реальной сети.

Среда Packet Tracer позволяет настраивать оборудование, используемое в сети, удобным для пользователя образом. Предусмотрено управление сетевыми устройствами с помощью команд операционной системы Cisco IOS, за счет графического интерфейса, так же используется интерфейс командной строки. Тем не менее, не все функции операционной системы Cisco IOS реализованы на данном сетевом симуляторе. Однако той основы, которую программа обеспечивает, хватает для построения сетевых систем и понимания технологических принципов.

Cisco Packet Tracer поддерживает режим визуализации, с помощью которого пользователь может отследить перемещение данных по сети, появление и изменение параметров пакетов при прохождении данных через сетевые устройства, скорость и пути перемещения пакетов. Таким образом, анализ событий, происходящих в сети, позволяет понять механизм ее работы и обнаружить неисправности.

Packet Tracer может быть использован не только как симулятор для виртуальных сетей, но и как сетевое приложение для симулирования виртуальной сети через реальную сеть, в том числе Интернет. Пользователи на разных компьютерах, независимо от их местоположения, могут работать над одним проектом, производя его настройку или устраняя проблемы.

На основе Cisco Packet Tracer пользователь может строить не только логическую, но и физическую модель сети и, следовательно, получать навыки проектирования. Созданную в учебной среде схему сети можно наложить на чертеж реально существующего здания. С учетом физических ограничений в тех или иных помещениях можно спроектировать размещение устройств, длину и тип прокладываемого кабеля или радиус зоны покрытия беспроводной сети.

Cisco Packet Tracer подходит для обучения сетевым технологиям. Симулятор наглядно имитирует поведение сетевого оборудования. Проводить эксперименты на реальном оборудовании в лабораторных и учебных целях сложно и неудобно, в то время как виртуальные возможности сетевого симулятора позволяют проводить такие исследования.

Ни один симулятор не может полностью заменить опыт работы в реальной сети. Однако существующее программное обеспечение в этой сфере способствует эффективному обучению сетевым технологиям, доступному в любое время и в любом месте.

1.1. Первый запуск Cisco Packet Tracer

Рабочее окно симулятора представлено на рис. 1.1, где:

1. Главное меню программы:

- Файл – содержит операции открытия / сохранения документов;
- Правка – стандартные операции «копировать / вырезать, отменить / повторить»;
- Настройки – говорит само за себя;
- Вид – масштаб рабочей области и панели инструментов;
- Инструменты – цветовая палитра и кастомизация конечных устройств;
- Расширения – мастер проектов, многопользовательский режим
- Помощь – ни за что не угадаете, что там содержится;

2. Панель инструментов, часть которых дублирует пункты меню (содержит кнопки быстрого вызова команд из меню *File* и *Edit* а так же команд *Zoom*, *Drawing Palette* и *Custom Devices Dialog*).

3. Панель инструментов рабочей области (содержит наиболее часто используемые операции, применяемые при построении модели сети: инструменты выделения, удаления, перемещения, масштабирования объектов, а так же формирование произвольных пакетов).

4. Навигационная панель (позволяет переключать рабочую область между логической и физической топологией сети. Физическая топология подразумевает расположение устройств в городе, районе, офисе. Здесь можно посмотреть как топологию сети всего города, так и расположение устройств в офисе, и даже на отдельной Rack-стойке).

5. Рабочая область. Данная область занимает большую часть окна программы, здесь происходит конструирование виртуальной сети, где размещаются устройства и строятся связи между ними. Двойной клик по любому устройству открывает окно его конфигурации. Окно конфигурации устройств состоит из 3-х вкладок:

– *Physical* – показывает внешний вид устройства и позволяет добавлять либо убирать модули. Модули нельзя добавлять/извлекать при включенном устройстве!

– *Config* – эта вкладка не открывается, пока устройство не загрузилось. Здесь осуществляется графическое конфигурирование оборудования Cisco без применения командной строки, но для информативности внизу отображаются команды, которые выполняются при конфигурации.

– *CLI/Desktop* – в зависимости от устройства позволяет получить доступ к командной строке IOS либо к рабочему столу Linux.

6. Панель симуляции/реального времени. После запуска программа находится в логическом режиме реального времени, можно строить сеть и смотреть, как она работает. Данная панель позволяет переключаться в режим симуляции и обратно. В этом режиме все пакеты, пересылаемые внутри сети, отображаются графически. Эта возможность позволяет наглядно видеть, по какому интерфейсу в данный момент перемещается пакет, какой протокол используется и т.д. В режиме симуляции можно не только отслеживать используемые протоколы, но и видеть, на каком из семи уровней модели OSI данный протокол задействован.

7. Блок выбора сетевых компонентов. Область выбора устройств либо методов связи для перетаскивания в рабочую область. Состоит из двух составных частей: области выбора типа устройства и области выбора конкретной модели устройства.

8. Область типа устройств. Позволяет выбрать и моделировать большое количество устройств различного назначения: маршрутизаторы, коммутаторы (в том числе и мосты), хабы и повторители, конечные устройства – ПК, серверы, принтеры, IP-

телефоны; беспроводные устройства: точки доступа и беспроводные маршрутизаторы; остальные устройства – Internet-облако, DSL-модем и кабельный модем, а так же разнообразные линии связи от консольного кабеля до оптической линии.

9. Область моделей устройств. Область выбора конкретной модели устройства указанного типа. Перечислим некоторые модели устройств, которые может моделировать Packet Tracer : маршрутизаторы: 1841, 2620XM, 2621XM, 2811; коммутаторы: 2959-24, 2950T, 2960, 3560; беспроводные устройства: Linksys-WRT300N и др.

10. Окно пользовательских пакетов. Окно управляет пакетами, которые были созданы в сети во время сценария симуляции.

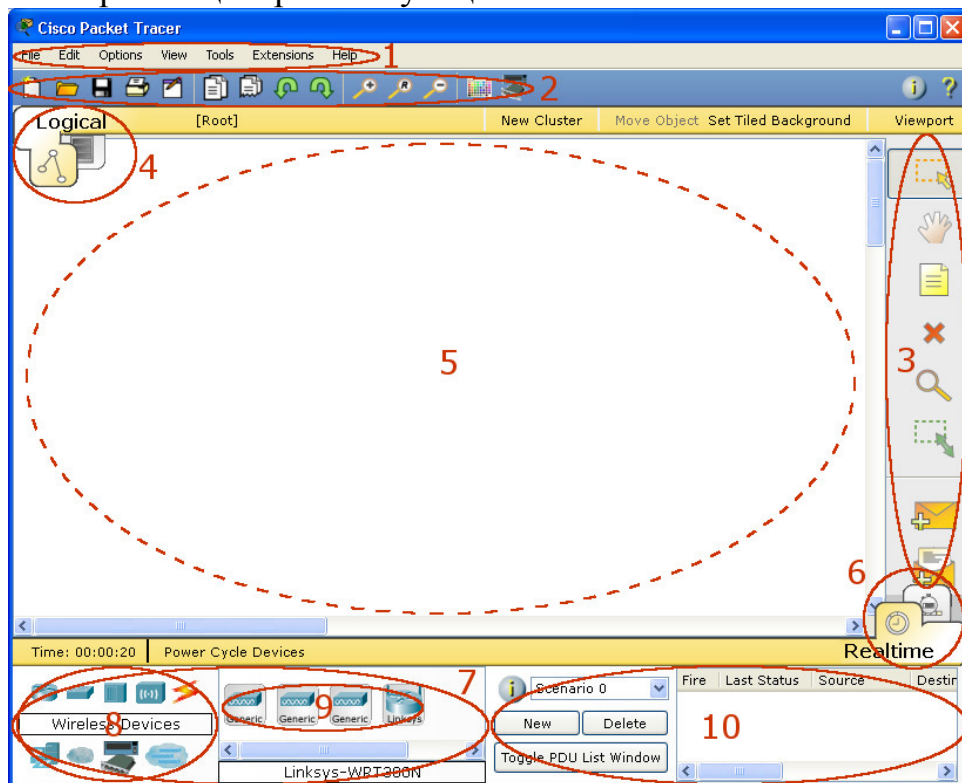


Рис. 1.1. Главное окно программы Cisco Packet Tracer

1.2. Оборудование и линии связи в Cisco Packet Tracer

1.2.1. Маршрутизаторы

Маршрутизаторы (рис. 1.2) используются для поиска оптимального маршрута передачи данных на основании специальных алгоритмов маршрутизации, например выбор маршрута (пути) с наименьшим числом транзитных узлов. Работают на сетевом уровне модели OSI.



Рис. 1.2. Панель выбора маршрутизаторов



Рис. 1.3. Виртуальный маршрутизатор и его реальный аналог

1.2.2. Коммутаторы

Коммутаторы (рис. 1.4) – это устройства, работающие на канальном уровне модели OSI и предназначенные для объединения нескольких узлов в пределах одного или нескольких сегментах сети. Передаёт пакеты коммутатор на основании внутренней таблицы – таблицы коммутации, следовательно трафик идёт только на тот MAC-адрес, которому он предназначен, а не повторяется на всех портах (как на концентраторе).



Рис. 1.4. Панель выбора коммутаторов



Рис. 1.5. Виртуальный коммутатор и его реальный аналог

1.2.3. Концентраторы

Это более «глупый» вариант устройства, объединяющего сетевые узлы. Просто повторяет пакет, принятый на одном порту на всех остальных портах. Всё по технологии Ethernet. В настоящее время выпускаются очень редко. Никакой защиты. Просто этакий «тройник» как для силовой сети.



Рис. 1.6. Панель выбора концентраторов

1.2.4. Беспроводные устройства

Беспроводные технологии Wi-Fi и сети на их основе (рис. 1.7.). Включает в себя точки доступа.



Рис. 1.7. Панель выбора беспроводных устройств








1.2.5. Линии связи

А с помощью линий связи (рис. 1.8) будем соединять узлы в единую схему. Здесь есть и автоматическое определение и консольный кабель и витая пара и оптоволокно. Есть даже разница между прямым и кроссоверным кабелем. В представлено табл. 1.1 описание предлагаемых кабелей.



Рис. 1.8. Панель выбора линий связи

Таблица 1.1 – Типы кабелей

Тип кабеля	Описание
 Console	Консольное соединение может быть выполнено между ПК и маршрутизаторами или коммутаторами. Скорость соединения обеих сторон должна быть одинаковой, передаваться может любой поток данных.
 Copper straight-through	Этот тип кабеля является стандартной средой передачи Ethernet для соединения устройств, которые функционируют на разных уровнях OSI. Сигнал передается напрямую из одного конца в другой, а именно с 1-го контакта на 1-й, с 2-го на 2-й и т. д. Используется между ПК и хабом, ПК и DSL-модемом, хабом и коммутатором.
 Copper cross-over	Этот тип кабеля является средой передачи Ethernet для соединения устройств, которые функционируют на одинаковых уровнях OSI. Используется для соединения двух ПК напрямую, т. е. без хаба или коммутатора. Таким образом, можно подключить только 2 компьютера одновременно.
 Fiber	Оптоволоконный кабель используется для соединения между оптическими портами.
 Phone	Соединение через телефонную линию может быть осуществлено только между устройствами, имеющими модемные порты.
 Coaxial	Коаксиальная среда используется для соединения между коаксиальными портами.
 Serial Data Circuit Equipment/Data Terminal Equipment (DCE/DTE)	Соединения через последовательные порты, часто используются для связей WAN. Для настройки таких соединений необходимо установить синхронизацию на стороне DCE-устройства. Синхронизация DTE выполняется по выбору. Сторону DCE можно определить по маленькой иконке “часов” рядом с портом. При выборе типа соединения Serial DCE, первое устройство, к которому применяется соединение, становится DCE-устройством, а второе - автоматически станет стороной DTE. Возможно и обратное расположение сторон, если выбран тип соединения Serial DTE.

1.2.6. Конечные устройства

Здесь непосредственно конечные узлы, хосты, сервера, принтеры, телефоны и многое другое (рис. 1.9). Довольно широкий перечень устройств.

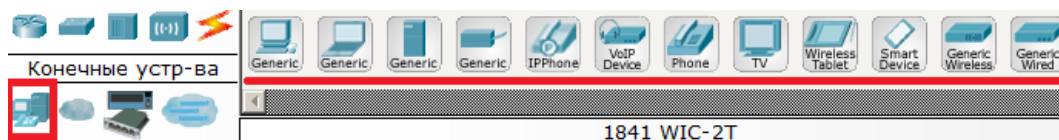


Рис. 1.9. Панель выбора конечных устройств

1.2.7. Эмуляция Интернета

Эмуляция глобальной сети (рис. 1.10). Модем DSL, «облако» и т.д.

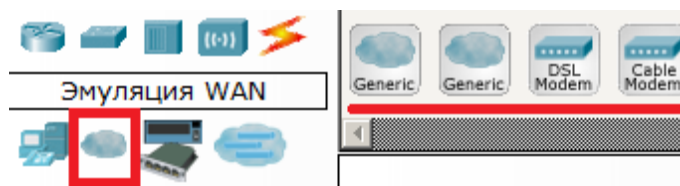


Рис. 1.10. Панель выбора топологии сети

1.2.8. Пользовательские устройства

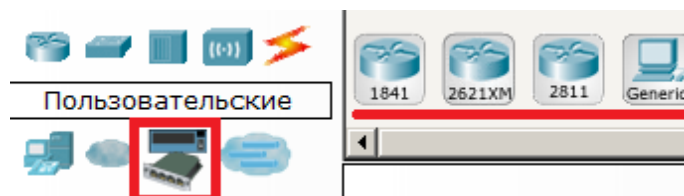


Рис. 1.11. Панель выбора пользовательских устройств

1.2.9. Облако для многопользовательской работы

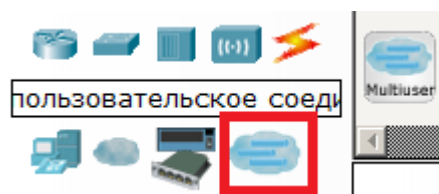


Рис. 1.12. Выбор облака для многопользовательской работы

2. Введение в межсетевую операционную систему IOS компании Cisco

Независимо от того, как обращаются к сетевому устройству: через консоль терминальной программы, подсоединённой через ноль-модем к COM-порту сетевого устройства, либо в рамках сеанса протокола Telnet, устройство можно перевести в один из режимов:

Пользовательский режим — это режим просмотра, в котором пользователь может только просматривать определённую информацию о сетевом устройстве, но не может ничего менять. В этом режиме приглашение имеет вид типа *Switch>*.

Привилегированный режим — поддерживает команды настройки и тестирования, детальную проверку сетевого устройства, манипуляцию с конфигурационными файлами и доступ в режим конфигурирования. В этом режиме приглашение имеет вид типа *Switch#*.

Режим глобального конфигурирования — реализует мощные однострочные команды, которые решают задачи конфигурирования. В этом режиме приглашение имеет вид типа *Switch(config)#*.

При первом входе в сетевое устройство пользователь видит командную строку пользовательского режима вида:

```
Switch>
```

Команды, доступные на пользовательском уровне являются подмножеством команд, доступных в привилегированном режиме. Эти команды позволяют выводить на экран информацию без смены установок сетевого устройства.

Чтобы получить доступ к полному набору команд, необходимо сначала активизировать привилегированный режим.

```
Press ENTER to start.
Switch>
Switch> enable
Switch#
Switch# disable
Switch>
```


Здесь и далее вывод сетевого устройства будем обозначать обычным шрифтом, а ввод пользователя **жирным** шрифтом.

О переходе в этот режим будет свидетельствовать появление в командной строке приглашения в виде знака **#**. Из привилегированного уровня можно получать информацию о настройках системы и получить доступ к режиму глобального конфигурирования и других специальных режимов конфигурирования, включая режимы конфигурирования интерфейса, подинтерфейса, линии, сетевого устройства, карты маршрутов и т.п. Для выхода из системы IOS необходимо набрать на клавиатуре команду **exit** (выход).

```
Switch> exit
```

Команды в любом режиме IOS распознаёт по первым уникальным символам. При нажатии табуляции IOS сам дополнит команду до полного имени.

При вводе в командной строке любого режима имени команды и знака вопроса (?) на экран выводятся комментарии к команде. При вводе одного знака результатом будет список всех команд режима. На экран может выводиться много экранов строк, поэтому иногда внизу экрана будет появляться подсказка - *More* -. Для продолжения следует нажать enter или пробел.

Команды режима глобального конфигурирования определяют поведение системы в целом. Кроме этого, команды режима глобального конфигурирования включают команды переходов в другие режимы конфигурирования, которые используются для создания конфигураций, требующих многострочных команд. Для входа в режим глобального конфигурирования используется команда привилегированного режима **configure**. При вводе этой команды следует указать источник команд конфигурирования: *terminal* (терминал), *memory* (энергонезависимая память или файл), *network* (сервер tftp (Trivial ftp – упрощённый ftp) в сети). По умолчанию команды вводятся с терминала консоли. Например:

```
Switch# configure terminal
Switch(config)# (commands)
Switch(config)# exit
Switch#
```

Для вызова команд пользовательского режима из привилегированного или команд привилегированного режима из режима глобальной конфигурации достаточно перед используемой командой добавить команду **do**.

Команды для активизации частного вида конфигурации должны предваряться командами глобального конфигурирования. Так для конфигурации интерфейса, на возможность которой указывает приглашение *Switch(config-if)#*, сначала вводится глобальная команда для определения типа интерфейса и номера его порта:

```
Switch# conf t
Switch(config)# interface type port
Switch( config-if)# (commands)
Switch( config-if)# exit
Switch(config)# exit
```

3. Способы подключения к устройствам фирмы Cisco

В Packet Tracer'е управлять оборудованием можно следующими способами:

- GUI (Graphical user interface);
- CLI (Command-line interface) в окне управления;

- терминальное подключение с рабочей станции через консольный кабель;
- telnet.

Интерфейс последних трёх идентичный – отличается лишь способ подключения. В реальной же жизни доступны:

- Telnet/SSH;
- терминальное подключение с рабочей станции через консольный кабель;
- web-интерфейс (Cisco SDM).

3.1. Управление по консоли

Данный тип подключения используется в следующих случаях:

- при первоначальной настройке оборудования;
- если что-то сломалось и нельзя получить удаленный доступ к оборудованию;
- если находитесь рядом с оборудованием.

Реальный вид консольного порта представлен на рис. 1.13. Он всегда выделен голубым цветом. С недавних пор стало возможным управление по USB.



Рис. 1.13. Консольный порт.

Консольный кабель Cisco показан на рис. 1.14.



Рис. 1.14. Консольный кабель Cisco.

Раньше он поставлялся в каждой коробке, теперь зачастую стоит отдельных денег.

Проблема в том, что современные ПК зачастую не имеют COM-порта. На выручку приходят часто используемые конвертеры USB-to-COM (рис. 1.15).



Рис. 1.15. Конвертеры USB-to-COM.

Либо редко используемые для этих целей конвертеры RS232-to-Ethernet (рис. 1.16).



Рис. 1.16. Конвертер RS232-to-Ethernet.

После подключения кабеля, определения номера COM-порта, для подключения можно использовать HyperTerminal (при помощи данной программы осуществляется доступ к другим компьютерам через модем, нуль-модемный кабель (последовательный порт) или с использованием протокола telnet) или PuTTY (свободно распространяемый клиент для различных протоколов удалённого доступа, включая SSH, Telnet) в Windows.

Управление через консоль доступно сразу, а вот для telnet нужно установить пароль.

Для того, чтобы подключиться к устройствам фирмы Cisco, для их последующего конфигурирования через консольный порт в рабочей области Packet Tracer необходимо разместить коммутатор **Catalyst 2960**, и один компьютер. Далее с помощью консольного кабеля соединим интерфейс **RS-232** компьютера с консольным портом коммутатора. Получившаяся схема будет иметь вид, представленный на рис. 1.17.



Рис. 1.17. Компьютер подключен к коммутатору консольным кабелем.

Теперь для того, чтобы подключиться с компьютера к коммутатору через консоль, щелкните два раза левой кнопкой мыши по изображению компьютера, перейдите на вкладку **Desktop** и выберите приложение **Terminal**.

Поскольку все параметры по умолчанию нас устраивают, менять их смысла нет. Просто нажмите на кнопку «ОК» и вы будете подключены к коммутатору через консольный порт.

Если в энергонезависимой памяти устройства отсутствует конфигурационный файл (startup-config), а так оно и будет при первом включении нового оборудования, появится Initial Configuration Dialog prompt, как на рис. 1.18.

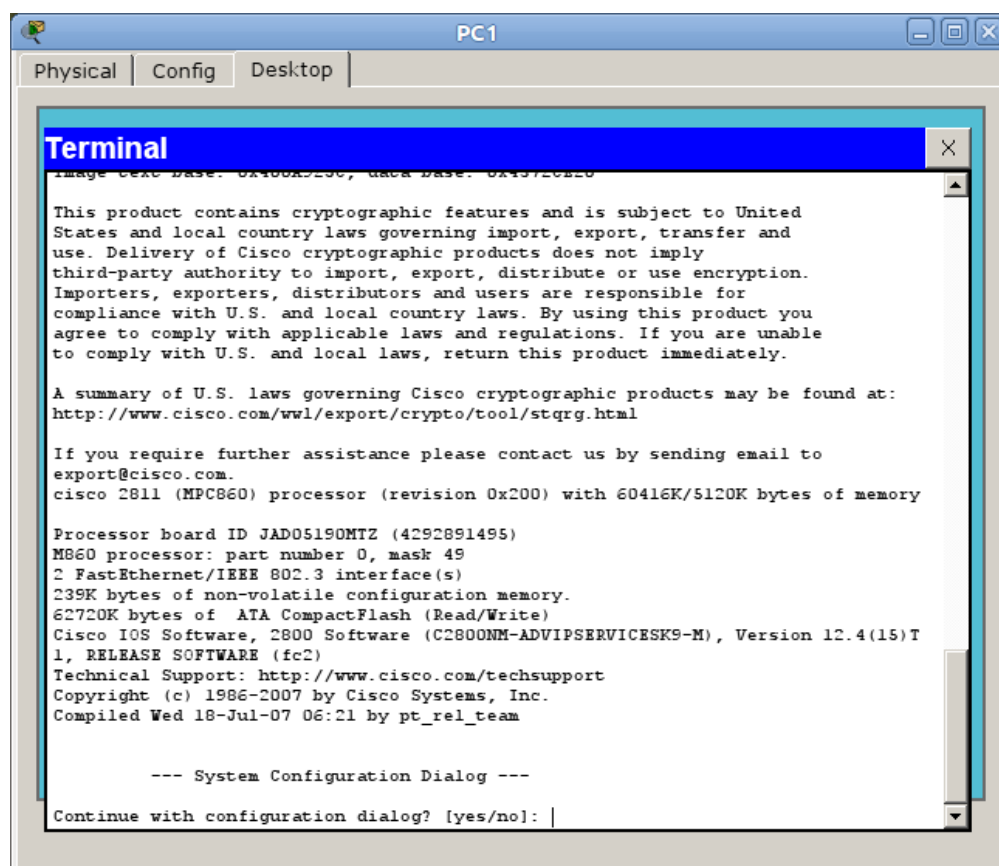


Рис. 1.18. Диалоговое окно первоначального конфигурирования.

Это краткое руководство, позволяющее шаг за шагом настроить основные параметры устройства (hostname, пароли, интерфейсы). Если интересно – читаем, в противном случае отвечаем **no** и видим следующее приглашение:

```
Switch>
```

Все только что проделанное равносильно тому, как если бы обычный компьютер был соединен с коммутатором через консольный порт, на компьютере необходимо открыть гипертерминал или putty и произошло бы подключение к коммутатору.

При подключении к коммутатору через консольный порт, по умолчанию он не запрашивает ни логина, ни пароля. Что само по себе является небезопасным. К коммутатору может подойти кто угодно, подключиться к нему кабелем и подправить конфигурацию, так что безопасность лишней не бывает.

Можно сделать, чтобы при подключении через консольный порт запрашивался только пароль, тогда надо сконфигурировать линию консоли следующим образом:

```
Switch(config)#line console 0
Switch(config-line)#password 123
Switch(config-line)#login
```

При такой конфигурации пользователю при входе не придется вводить имя пользователя, а для получения доступа достаточно будет ввести пароль, который задавался командой `password`.

Так же для линии консоли можно настроить еще несколько параметров, которые смогут немного повысить безопасность системы. Узнать что это за параметры можно перейдя к конфигурированию линии консоли с помощью `line console 0` и выполнив команду ?.

3.2. Удаленное управление с помощью web-интерфейса

Предположим, что удаленный компьютер подключен к порту коммутатора, который находится VLAN 1. Компьютер имеет IP-адрес 192.168.1.2 с маской 255.255.255.0 и шлюзом по умолчанию 192.168.1.1. Для того чтобы настроить связь с компьютера с коммутатором, настроим последний следующим образом:

```
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.1 255.255.255.0
Switch(config-if)#no shutdown
```

После чего на компьютере необходимо открыть браузер и попробовать получить доступ к `http://192.168.1.1`.

Обычно оборудование фирмы Cisco, не конфигурируется с помощью web-интерфейса. Все изменения конфигурации выполняются с помощью консоли, так как она позволяет выполнять более гибкое (и порой недоступное в web-интерфейсе) и безопасное конфигурирование. Поэтому можно отключить доступ к вашему оборудованию при помощи web-интерфейса, для этого потребуется отключить действующий на оборудовании web-сервер, это можно выполнить с помощью следующих команд:

```
Router(config)#no ip http server
Router(config)#no ip http secure-server
```

3.3. Настройка доступа по Telnet

Telnet – стандартная утилита, как и SSH. Для доступа к Cisco по этим протоколам нужно настроить пароли доступа. Возможность использования SSH зависит от лицензии IOS.

Используя telnet можно удаленно конфигурировать свое оборудование. Соберем в Packet Tracer схему, представленную на Рис. 1.19.

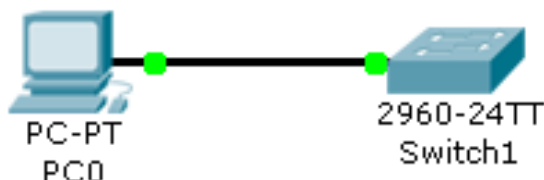


Рис. 1.19. Компьютер подключен к коммутатору прямым Ethernet-кабелем.

Компьютеру опять же зададим ip адрес 192.168.1.2 с маской 255.255.255.0 и шлюзом по умолчанию 192.168.1.1. Свитч сконфигурируем следующим образом:

```

Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#line vty 0 4
Switch(config-line)#password 123
  
```

С первыми четырьмя строчками все ясно – это мы задаем ip адрес нашему коммутатору (если он у вас уже задан, то их можно и не выполнять).

Используя команду `line vty 0 4` переходим к конфигурированию линий виртуальных терминалов. Командой `password 123` мы задаем пароль 123 для доступа (если эту команду не выполнять, то при попытке подключения к устройству мы получим – Connection to 192.168.1.1 closed by foreign host). Подключение по telnet или ssh называется виртуальным терминалом (vt). 0 4 – это 5 пользовательских виртуальных терминалов = telnet сессий.

Выполнив данные команды можно попробовать удаленно подключиться к коммутатору, для этого необходимо перейти к консоли компьютера и ввести команду `telnet 192.168.1.1`, если все сделано верно, то откроется доступ к консоли оборудования (см. Рис. 1.20).

```

PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

User Access Verification

Password:
Switch>
  
```

Рис. 1.20. Использование telnet для получения доступа к консоли оборудования.

Если необходимо, чтобы при доступе через telnet запрашивался не только пароль, но и еще и логин пользователя, то необходимо сконфигурировать линии виртуальных терминалов следующим образом:

```

Switch(config)#line vty 0 4
Switch(config-line)# login local
  
```

Только перед этим на оборудовании необходимо создать учетную запись пользователя командой `Switch(config)#username user password 123`.

Итак, указанных выше команд достаточно, чтобы попасть в пользовательский режим, но недостаточно для привилегированного (Рис. 1.21).

```
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

User Access Verification

Password:
Switch>enable
% No password set.
Switch>
```

Рис. 1.21. Попытка подключения к привилегированному режиму.

Настроим пароль для enable-режима (Рис. 1.22):

```
Router(config)#enable secret 123456

PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

User Access Verification

Password:
Switch>

[Connection to 192.168.1.1 closed by foreign host]
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

User Access Verification

Password:
Switch>enable
% No password set.
Switch>enable
Password:
Switch#
```

Рис. 1.22. Настройка пароля для enable-режима.

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 всё-таки задаётся пароль командой `password`, то следует применить так же `service password-encryption`, тогда пароль в конфигурационном файле будет зашифрован:

```
line vty 0 4
password 7 08255F4A0F0A0111
```

4. Настройка баннера

Баннер - это своеобразная вывеска, которая предназначена для сообщения определенной информации, любому, кто пытается получить доступ к сетевому устройству. Логин-баннер отображается пользователю при любом его подключении к устройству с использованием `telnet`, `ssh`-клиента или при подключению при помощи консоли(RS232). За рубежом, обычно, сообщается информация о том, кому принадлежит данное коммуникационное оборудование и что может последовать, если в дальнейшем последует несанкционированный доступ либо попытка доступа. Может быть и любая другая информация. К примеру, фирма Cisco на новых не сконфигурированных мар-

шрутизаторах сообщает об этом факте. Существует 3 вида баннеров motd, exes, incoming.

Синтаксис команды banner выглядит следующим образом:

```
banner motd {char} {banner text} {char}
```

где — {char} специальный символ разделителя, который не отображается в тексте баннера (символ # означает начало и конец строки). Какое-либо содержание между первым и вторым специальным разделителем интерпретируется как баннер-сообщение.

Пример: создание баннера message-of-the-day (MOTD):

```
dyn1(config)# banner motd #Hello! I'm $(hostname). You are connected on line  
$(line) on domain $(domain)#
```

```
dyn3# telnet 192.168.1.1  
Trying 192.168.1.1 ... Open  
Hello! I'm dyn1. You are connected on line 2 on domain xgu.ru
```

Относительно содержания баннера. Существует такая легенда: хакер вломился в сеть, что-то там поломал/украл, его поймали, а на суде оправдали и отпустили. Почему? А потому, что на пограничном роутере (между интернет и внутренней сетью), в banner было написано слово «Welcome». «Ну раз просят, я и зашел». Поэтому считается хорошей практикой в баннере писать что-то вроде «Доступ запрещен!».

5. Построение и настройка локальной компьютерной сети в Cisco Packet Tracer

5.1. Общая структура и оборудование локальной компьютерной сети

Локальная компьютерная сеть (Local Area Network – LAN) представляет собой набор компьютеров (часто называемых рабочими станциями (Workstation)), серверов, сетевых принтеров, коммутаторов (Switch), маршрутизаторов (Router), точек доступа (Access Point), другого оборудования, а также соединяющих их кабелей, обычно расположенных на относительно небольшой территории или в небольшой группе зданий (учебный класс, квартира, офис, университет, дом, фирма, предприятие) (Рис. 1.23).

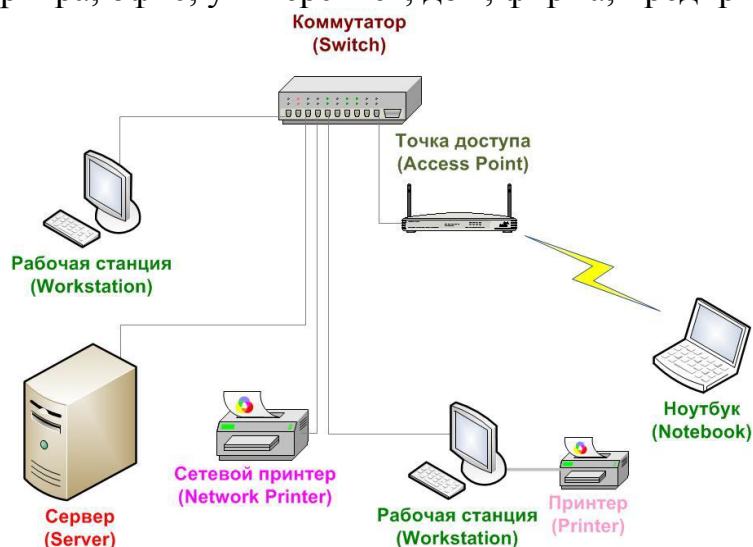


Рис. 1.23. Структура простейшей локальной компьютерной сети.

В локальной сети можно выделить:

– оконечное оборудование пользователей, поставляющее данные в сеть и принимающее данные для обработки (рабочие станции, серверы, ноутбуки, сетевые прин-

теры и др.);

- активное сетевое оборудование, организующее каналы для передачи информации между оконечным оборудованием пользователей в структурах данных, называемых пакетами, кадрами, сообщениями (коммутаторы, маршрутизаторы, концентраторы, точки доступа, модемы и др.);

- пассивное сетевое оборудование, представляющее собой кабели, кабельные каналы (короба), разъемы, розетки и другое соединительное оборудование, а также стойки и подставки для размещения активного сетевого оборудования.

Для организации работы локальной компьютерной сети необходимо:

а) выполнить физическое построение компьютерной сети:

- установить в оконечное оборудование пользователей сетевые интерфейсные адаптеры (Network Interface Card – NIC) (данный этап обычно пропускается, так как современные материнские платы оснащаются встроенными NIC);

- подобрать и разместить активное сетевое оборудование;

- выполнить соединение сетевых интерфейсных адаптеров в оконечном оборудовании пользователей и разъемов активного сетевого оборудования с помощью кабелей и разъемов (кабели и разъемы не используются при организации беспроводного соединения);

б) настроить параметры набора (стека) сетевых протоколов на оконечном оборудовании пользователей: задать сетевые имена устройств и адреса, установить требуемые параметры сетевых протоколов;

в) выполнить работы по организации совместно используемых сетевых ресурсов и по предоставлению доступа к этим ресурсам пользователей сети;

г) установить необходимое сетевое программное обеспечение (дополнительное к входящему в состав операционных систем).

Сетевые интерфейсные адаптеры предназначены для выполнения функций физического и канального уровня семиуровневой модели взаимодействия открытых систем (Open System Interconnection – OSI) в устройствах локальной сети. Адаптеры имеют передающую и принимающую части, которые выполнены независимыми друг от друга с целью поддержки режима полного дуплекса (Full Duplex), при котором передача и прием данных происходят одновременно. Обычно настройки драйверов сетевого адаптера позволяют выбирать и менее производительный режим полудуплекса (Half Duplex), при котором передача и прием данных происходят по очереди. Также существует возможность ручного выбора скорости передачи данных и других параметров NIC (по умолчанию для режима и скорости передачи устанавливается значение *Автоопределение*, активирующее схему автоматического определения скорости и режима передачи (Autonegotiation), наиболее производительных для данного подключения). Ручное уменьшение скорости передачи данных и изменение режима передачи в полудуплексный может помочь при обнаружении проблем передачи, связанных с наличием интенсивных электромагнитных помех и/или необходимостью использования длин сетевых кабелей, превышающих установленные стандартами.

Под конфигурированием адаптера подразумевается настройка используемых системных ресурсов и выбор скорости, режима передачи иногда и других параметров. Конфигурирование осуществляется путем настройки драйвера, параметры конфигурирования хранятся в энергонезависимой памяти EEPROM, установленной на адаптере. Для современных адаптеров характерно конфигурирование с использованием технологии Plug And Play – автоматическое распределение BIOS или операционной системой системных ре-

сурсов между подключенными устройствами с целью предотвращения конфликтов, происходящих при выделении одних и тех же ресурсов различным устройствам.

Наиболее популярным активным сетевым оборудованием современных локальных компьютерных сетей является сетевой *коммутатор (Switch)*, к портам которого с помощью кабелей подключается оконечное оборудование пользователей и/или другое активное сетевое оборудование. Коммутаторы осуществляют передачу структур данных, называемых *кадрами (Frame)*, из порта, к которому подключено устройство-источник *кадров (Source)*, в порт, к которому подключено устройство *приемник кадров (Destination)*. Поиск выходного порта осуществляется коммутаторами на основании анализа адресной информации в заголовке кадра.

Иногда для организации локальной сети в качестве активного сетевого оборудования используют *концентратор (Hub)*, внешним видом очень похожий на коммутатор. Однако принцип работы концентратора отличается: если коммутатор анализирует адресную информацию в заголовках поступающих в его порты кадров и избирательно передает кадры с входного порта на выходной порт, к которому подсоединен получатель кадров, то концентратор просто копирует сигналы, соответствующие битам информации, со своего входного порта на все остальные порты. С практической точки зрения концентраторы имеют преимущество в скорости работы (точнее, в минимальной длительности задержки передаваемых кадров), поскольку они не выполняют буферизацию заголовков кадров и анализ адресной информации. Однако дублирование потоков кадров даже к тем устройствам, которые не являются адресатами (проверкой и отбрасыванием «не своих» кадров занимается сетевой интерфейсный адаптер устройства), приводит к снижению эффективности использования сети. Кроме того, существует возможность использования программ анализаторов протоколов, которые могут принимать и анализировать весь трафик, поступающий в адаптер (одна из таких программ будет использоваться в последующих лабораторных работах). Очевидно, что в таком случае любой из компьютеров локальной сети сможет «видеть» трафик, передаваемый всеми остальными компьютерами, что является серьезным недостатком с точки зрения безопасности передачи информации.

В настоящее время достаточно популярным способом организации локальной сети является построение *беспроводных локальных сетей (Wireless Local Area Network – WLAN)*. Для их организации часто используют *точку доступа (Access Point)*, организующую радиоканалы между участниками сети, которые должны быть оснащены интерфейсными картами беспроводного доступа (следует отметить, что подавляющее большинство мобильных компьютеров и устройств оснащено встроенными контроллерами беспроводного доступа).

При необходимости подключения беспроводного сегмента локальной сети к ее проводному сегменту на коммутаторе/концентраторе точка доступа подключается кабелем к одному из портов коммутатора/концентратора. В этом случае говорят, что беспроводная сеть работает в *режиме инфраструктуры (Infrastructure Mode)*.

Сетевые принтеры представляют собой принтеры, оснащенные сетевыми адаптерами, что позволяет подключать их к сети непосредственно. Использование сетевого принтера является удобным, так как его работа не связана с необходимостью работы компьютера, к которому подключается обычный принтер. Кроме того, сетевые принтеры обычно имеют повышенные производительность и ресурс картриджа. При отсутствии сетевого принтера совместный доступ к обычному принтеру, подключенному к компьютеру, может быть организован средствами операционной системы.

5.2. Конфигурирование сетевых средств операционных систем компьютеров локальной сети

Чтобы сетевые устройства могли узнать о присутствии других устройств, а также вести обмен данными между собой, на каждом из устройств должен быть установлен одинаковый стек (набор) сетевых протоколов. В настоящее время наиболее распространенным стеком сетевых протоколов является *TCP/IP – Transmission Control Protocol/Internet Protocol – протокол управления передачей/протокол Интернета*, его популярность связана с тем, что данный стек является необходимым условием для подключения компьютера к сети Интернет. Основной настройкой этого протокола является задание *IP-адреса*, который (для наиболее распространенной в настоящее время 4-й версии протокола IP) выглядит как четыре группы цифр, разделенных точками: *x.x.x.x*, где *x* – десятичное число в диапазоне от 0 до 255. Старшие одна две или три цифры определяют номер сети, к которой принадлежат компьютеры, для возможности обмена информацией в локальной сети на коммутаторе/концентраторе они должны принадлежать одной IP-сети. В простейшем случае можно использовать сеть с сетевой частью адреса 192.168.0, при этом для компьютеров сети можно задавать адреса от 192.168.0.1 до 192.168.255.254 (адреса 192.168.0.0 и 192.168.0.255 являются служебными). Другой важный параметр стека TCP/IP – *маска подсети (Subnet Mask)*, представляющая собой 32-битное число, старшая часть которого содержит непрерывный ряд единиц, а младшая – непрерывный ряд нулей. Данный параметр позволяет «разрезать» IP-сети на подсети меньшего достаточно гибко задаваемого размера. В нашем случае будем использовать маску 255.255.255.0, задающую подсеть с адресом, определяемым первыми тремя числами IP-адреса – 192.168.0, в которую можно включить 254 компьютера с адресами от 192.168.0.1 до 192.168.0.254.

Настройку стека TCP/IP в операционной системе Microsoft Windows 7 можно выполнить, открыв свойства Протокола Интернета версии 4 (TCP/IPv4) в свойствах Сетевого подключения, которое находится: *Панель управления → Центр управления сетями и общим доступом → Изменение параметров адаптера (для этого понадобятся права Администратора)* (Рис. 1.24).

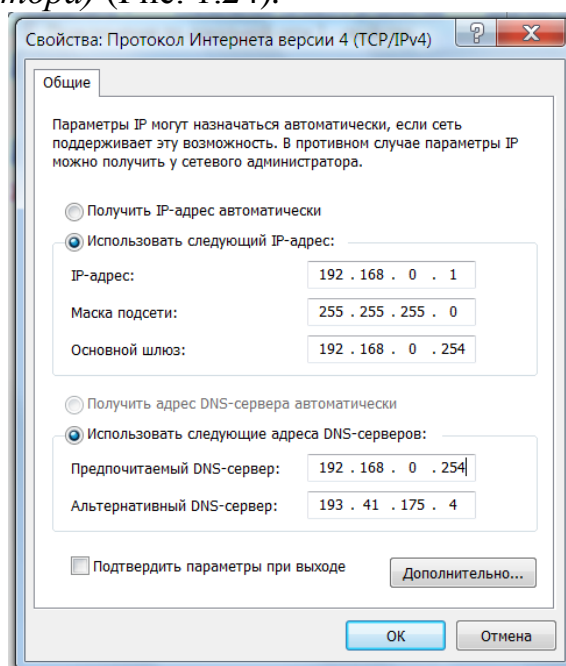


Рис. 1.24. Окно свойств сетевого подключения протокола Интернета версии 4 (TCP/IPv4) с адресной информацией.

В простейшей локальной сети основной шлюз и DNS-сервер можно не задавать. Кроме адресной информации, каждому компьютеру должно быть задано сетевое имя компьютера и имя рабочей группы, в которую он входит. В операционной системе Microsoft Windows 7 имена можно задать (также обладая правами Администратора): *Панель управления → Система → Дополнительные параметры → Имя компьютера*.

После задания уникальных IP-адресов и сетевых имен устройствам локальной сети можно проверить наличие связи между ними. Проверку лучше начать с физического уровня модели взаимодействия открытых систем, на котором компьютеры обмениваются сигналами, кодирующими биты информации. Для этого достаточно убедиться, что на коммутаторе/концентраторе светится светодиод, соответствующий порту, к которому подключено проверяемое устройство компьютер (в случае, если коммутатор/концентратор находится в труднодоступном месте, можно проверить, светится ли светодиод сетевого адаптера устройства). Если светодиоды светятся, это свидетельствует о наличии соединения между приемниками и передатчиками сетевого адаптера и коммутатора/концентратора, если нет, то возможен либо обрыв провода, либо плохой контакт при монтаже разъема, либо неправильная разводка пар в разъемах, точнее это можно выяснить с помощью специальных тестеров кабельных сетей.

При наличии связи на физическом уровне, можно попробовать проверить связь на сетевом уровне. Для этого необходимо открыть окно командной строки (*Пуск → Выполнить → cmd*) и запустить утилиту ping, в качестве аргумента которой указать IP-адрес удаленного компьютера, соединение к которому необходимо проверить.

Примечание: если результатом выполнения команды ping является сообщение «ping не является внутренней или внешней командой, исполняемой программой или пакетным файлом», то в переменной операционной системы PATH отсутствует строка "%SYSTEMROOT%\system32". Чтобы получить доступ к переменной PATH необходимо пройти по пути: «Start» («Пуск») → «Control Panel» («Панель управления») → «System» («Система»), откройте вкладку «Advanced» («Дополнительные параметры системы»), нажмите кнопку «Environment Variables» («Переменные среды»), в разделе «System Variables» («Системные переменные») сделайте двойной щелчок на строке «Path» и в начале списка «Variable Value» («Значение переменной») установите "%SystemRoot%\system32; %SystemRoot%;%SystemRoot%\System32\Wbem;" (без кавычек, ";" в конце – это разделитель). Перезагрузите систему.

5.3. Моделирование и исследование работы локальной сети в Cisco Packet Tracer

Для создания сети необходимо на рабочую область перетащить требуемые оконечные устройства пользователей – компьютеры, ноутбуки, серверы, принтеры и другие устройства.

После размещения необходимого оборудования пользователей можно аналогичным образом разместить на рабочей области сетевое оборудование, сгруппированное в следующих типах устройств: *маршрутизаторы (Routers), коммутаторы (Switches), концентраторы (Hubs), беспроводные устройства (Wireless Devices)* и др.

Для соединения устройств необходимо выбрать тип соединения (прямой медный кабель – *Copper Straight-Through* для соединения компьютера и коммутатора). Подобным образом необходимо соединить все устройства. Обратите внимание, что при создании нового соединения занятые порты устройства не отображаются во всплывающем окне.

Если создавать соединение с автоматическим выбором типа (*Automatically Choose*

Connection Type), то всплывающие окна появляться не будут, а Packet Tracer сам определит тип соединения и используемые порты (но эту возможность использовать не рекомендуется, поскольку нужно представлять, какие порты и как соединяются).

После завершения соединения устройств сети Packet Tracer сигнализирует о наличии соединений на физическом и канальном уровнях двумя зелеными периодически мигающими квадратами на концах каждого соединения (мигание означает активность линии). При отсутствии соединения квадратики становятся красными. Это можно проверить, выключив питание одного из компьютеров. Для этого выполните щелчок левой кнопкой мыши на одном из компьютеров и перейдите в открывшемся окне на вкладку *Физическая конфигурация (Physical)*. Выполните щелчок мышью по кнопке питания на изображении компьютера, обратите внимание, что находящийся над ней индикатор погас. После включения устройства квадратик на линии связи возле устройства не сразу изменяет цвет на зеленый. Это обусловлено необходимостью некоторого времени на распознавание устройства коммутатором.

Следующим шагом может быть создание беспроводного сегмента сети и подключение его к проводной сети. Для этого необходимо добавить на рабочую область *Точку доступа (Access Point-PT)*, предварительно выбрав в Панели типов устройств *Беспроводные устройства (Wireless Devices)*, добавьте также из группы *Оконечные устройств (End Devices)* *Ноутбук (Laptop-PT)*.

Поскольку ноутбук по-умолчанию оснащен проводным интерфейсом, необходимо заменить его на беспроводной. Для этого выполните щелчок левой кнопкой мыши на ноутбуке и перейдите на вкладку *Физическая конфигурация (Physical)*. Прокрутите линейку прокрутки вниз так, чтобы увидеть изображение ноутбука.

Отключите питание ноутбука, выполнив щелчок левой кнопкой мыши на кнопке питания, при этом погаснет индикатор питания. Перетащите мышью модуль с проводным интерфейсом в *Список модулей (MODULES)* слева от изображения ноутбука. После этого перетащите верхний модуль с беспроводным интерфейсом *Linksys-WPC300N* из *Списка модулей (MODULES)* в разъем ноутбука, в котором был установлен модуль с проводным интерфейсом. Включите питание ноутбука и закройте окно конфигурирования ноутбука. Вы должны увидеть, что ноутбук связался с точкой доступа с помощью радиоволн (Рис. 1.25).

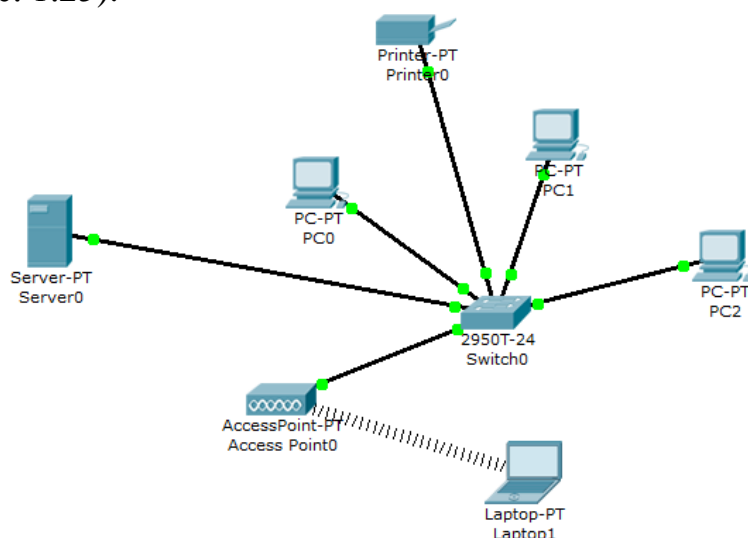


Рис. 1.25. Завершенная топология локальной компьютерной сети.

Добавьте к сети из группы *Оконечные устройств (End Devices)* на Панели типов устройств *Сервер (Server-PT)* и *Принтер (Printer-PT)*. Оба устройства по-умолчанию оснащены проводными интерфейсами *Fast Ethernet*, работающими со скоростью 100

Мбит/с. Подсоедините принтер к порту коммутатора аналогично соединению с ПК. Замените сетевой интерфейс сервера на интерфейс Gigabit Ethernet, работающий со скоростью 1000 Мбит/с. Для этого выполните щелчок на изображении сервера и на вкладке *Физическая конфигурация (Physical)* после выключения питания сервера замените так, как для ноутбука, сетевой интерфейс сервера на модуль PC-HOST-NM-1CGE.

Обратите внимание, что при подсоединении сервера к коммутатору необходимо выбрать на коммутаторе гигабитный порт, например *Gigabit Ethernet 1/1*. В этом случае пакеты между коммутатором и сервером будут проходить на скорости в 10 раз большей скорости между коммутатором и остальными устройствами сети, что является оправданным, так как сервер обычно используется несколькими устройствами.

После создания сети следующим шагом является конфигурирование устройств. Сетевые имена устройств задаются автоматически при создании, их можно изменять прямо в рабочей области или в окне конфигурирования устройств. Устройства Packet Tracer поддерживают стек сетевых протоколов TCP/IP, причем поддерживается и IPv4 (в настоящее время наиболее распространенной), и IPv6 (переход к которой уже начался). В данной работе мы будем задавать устройствам адреса протокола IPv4.

Назначение имен и IP-адресов ПК, принтера и сервера происходит одинаковым образом, поэтому приведем последовательность действий по конфигурированию этих параметров на примере ПК. Выполните щелчок по изображению устройства левой кнопкой мыши, при этом откроется окно конфигурирования устройств, выберите его вкладку *Конфигурация (Config)*.

Из списка слева выберите команду *Настройки (Settings)* для перехода к окну, в котором можно ввести/изменить сетевое имя устройства.

Здесь также можно указать IP-адреса *шлюза (Gateway)* сети, в которую входит данное устройство, и *DNS-сервера*, на котором находятся соответствия имен пользовательских устройств сети и их IP-адресов, и указать будет ли назначаться им адрес автоматически (с использованием сервера, работающего по протоколу *Dynamic Host Configuration Protocol – DHCP-сервера*) или вручную (*Static*).

Сетевой шлюз (Gateway) представляет собой сетевой интерфейс, через который сетевые пакеты от устройств данной сети уходят в другие сети и пакеты от устройств других сетей входят в данную сеть. Поскольку в данной работе моделируется только одна сеть, адрес шлюза задавать не нужно. Рассмотрение работы *Доменной системы имен (Domain Name System – DNS)* и конфигурирование DNS-сервера будет рассмотрено на последующих практических занятиях. Без конфигурирования такого сервера мы сможем посылать пакеты с помощью утилиты ping, используя в качестве ее аргумента только IP-адрес удаленного компьютера. После конфигурирования DNS-сервера появляется дополнительная возможность связи с ним по его сетевому имени.

Из списка слева выберите тип сетевого интерфейса устройства (например, *Fast Ethernet*) для открытия окна задания адресной информации. В поле *IP-адрес (IP Address)* для компьютера с сетевым именем *PC1* введите адрес 192.168.0.1, далее выполните щелчок в поле *Маска подсети (Subnet Mask)*, программа автоматически введет маску 255.255.255.0, оставьте ее без изменений. Обратите внимание, что на этой вкладке автоматически задается MAC-адрес, а также скорость и режим передачи данных (100 Мбит/с и полный дуплекс).

Выполните аналогичным способом конфигурирование остальных пользовательских устройств созданной локальной сети, задав им IP-адреса и маски, приведенные в табл. 1.2. Обратите внимание, что сетевой интерфейс сервера имеет тип *Gigabit Ethernet* и работает на скорости 1000 Мбит/с.

Таблица 1.2 – Адресная информация для конфигурирования пользовательских устройств локальной компьютерной сети на Рис. 1.25

Устройство	Сетевое имя	IP-адрес	Маска подсети
ПК-1	PC1	192.168.0.1	255.255.255.0
ПК-2	PC2	192.168.0.2	255.255.255.0
ПК-3	PC3	192.168.0.3	255.255.255.0
Ноутбук	Laptop1	192.168.0.4	255.255.255.0
Сетевой принтер	Printer0	192.168.0.5	255.255.255.0
Сервер	Server0	192.168.0.6	255.255.255.0

Конфигурирование адресов для ноутбука имеет особенности, поскольку мы оснастили его беспроводным интерфейсом. По умолчанию окно конфигурирования интерфейса открывается с установленной настройкой автоматического задания IP-адреса и маски подсети устройствам (*DHCP*). Но поскольку в данной сети отсутствует DHCP-сервер, следует переключить установку в режим ручного задания адресов (*Static*) и задать IP-адрес и маску подсети описанным выше способом. Обратите внимание на наличие настроек *аутентификации* (*Authentication*) устройств при беспроводном подключении к точке доступа – передачу точке доступа пароля, по которому она будет подключать устройство, и настроек *шифрования* передаваемых по беспроводной сети данных (*Encryption*). Учитывая простоту несанкционированного подключения к беспроводной сети, на практике эти возможности являются часто используемыми. Пока оставьте их отключенными (*Disabled*).

Конфигурирование сетевого оборудования моделируемой локальной сети выполняется автоматически, однако просмотр возможных параметров конфигурации представляет интерес. В списке интерфейсов беспроводной точки доступа присутствуют два интерфейса – *Port 0* – проводной интерфейс Fast Ethernet, связывающий точку доступа с коммутатором, и беспроводный интерфейс *Port 1*. Здесь так же, как и для беспроводного адаптера есть поля для настройки аутентификации и шифрования, включая указание ключевой/парольной фразы, которую должен передать беспроводный адаптер для подключения к точке доступа.

Конфигурационные параметры коммутатора в окне глобальных *настроек* (*Global Settings*), включающие *имя коммутатора*, отображаемое на схеме сети (*Display Name*) и *хост-имя* (*Hostname*), по которому коммутатор идентифицируется командами *межсетевой операционной системы Cisco* (*Internetwork Operating System – IOS*) – программного обеспечения, зашитого в постоянную память большинства сетевых устройств производства Cisco Systems. Все выполняемые настройки сопровождаются соответствующими им командами IOS в окне *Equivalent IOS Command*. При выборе команды *База данных VLAN* (*VLAN Database*) из списка команд слева отображается окно со списком *виртуальных локальных сетей* (*Virtual LAN – VLAN*) – технологии, позволяющей приписывать порты сетевых устройств к различным VLAN, тем самым разделяя эти порты на отдельные сети на канальном уровне. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным станциям группироваться вместе, даже если они не находятся в одной физической сети. В нашей сети все порты приписаны к VLAN с именем *default* (по-умолчанию) и идентификатором 1.

Для проверки связи между устройствами смоделированной локальной сети можно использовать утилиту *ping*. Для этого выполните щелчок левой кнопкой мыши, например, на ПК и перейдите на вкладку *Рабочий стол* (*Desktop*). На нем будут доступны дополнительные инструменты для настройки данного устройства (их доступность

зависит от физического конфигурирования устройства – наличия тех либо иных модулей или устройств). Нам понадобится инструмент *Окно командной строки (Command Prompt)*, в котором можно запустить утилиту ping с IP-адресом устройства сети, связь с которым проверяется в качестве ее аргумента.

Также существует возможность проверить связь с сервером, открыв на нем Web-страницу с помощью Web-браузера, которым оснащен ПК. Это возможно, поскольку на сервере по-умолчанию устанавливается целый ряд серверных приложений, в том числе и HTTP-сервер с несколькими простыми HTML-страницами (Рис. 1.26).

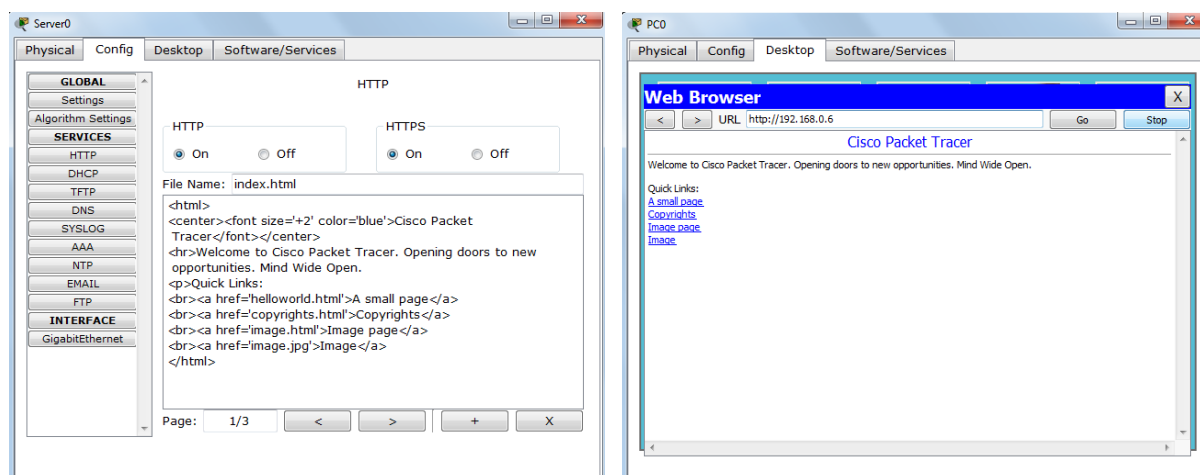


Рис. 1.26. Открытие Web-страницы HTTP-сервера в браузере ПК.

6. Задание для самостоятельного выполнения

1. Постройте с помощью программы Cisco Packet Tracer модель локальной компьютерной сети на одном коммутаторе и одной беспроводной точке доступа с оконечными устройствами пользователей, количество которых перечислены в табл. 1.4, где вариант – номер студента по списку в журнале группы. Компьютеры должны быть оснащены интерфейсами FastEthernet, ноутбуки – беспроводными интерфейсами, а серверы – интерфейсами GigabitEthernet. Сетевой интерфейс сервера необходимо заменить на модуль *PC-HOST-NM-1CGE*, модуль с проводным интерфейсом на ноутбуке – на модуль с беспроводным интерфейсом *Linksys-WPC300N*.

Таблица 1.4 – Устройства для индивидуального моделируемых локальных сетей

Вариант	ПК	Серверов	Принтеров	Ноутбуков
1	5	1	2	2
2	7	2	1	3
3	9	1	2	4
4	11	2	1	2
5	13	1	2	3
6	15	2	1	4
7	17	1	2	2
8	19	2	1	3
9	21	1	2	4
10	22	2	1	2
11	20	1	2	3
12	18	2	1	4
13	16	1	2	2

Вариант	ПК	Серверов	Принтеров	Ноутбуков
14	14	2	1	3
15	12	1	2	4
16	10	2	1	2
17	8	1	2	3
18	6	2	1	4
19	23	1	2	2
20	16	2	1	3
21	4	1	1	4
22	11	2	2	1
23	13	2	2	1
24	17	2	2	1
25	8	1	1	2
26	10	2	2	3
27	15	2	1	3
28	19	2	1	3

2. Установите на коммутаторе пароль для вход в консоль и в привилегированный режим (для нечетных вариантов пароль хранится в открытом виде, для четных вариантов – в зашифрованном).

3. Задайте сетевые имена для компьютеров PC1 – PCM (М – количество ПК из табл. 4.1), Server1 – Server2, Printer1 – Printer2, Laptop1 – Laptop L (L – количество ноутбуков из табл. 1.4). Приведите в отчет скриншот с топологией локальной сети.

4. Задайте IP-адреса пользовательским устройством, выбрав их из диапазона адресов IP-сети 192.168.v.0-192.168.v.255 (v – номер варианта студента по списку в журнале), имеющей маску подсети 255.255.255.0. Вначале диапазона IP-адресов разместите серверы, затем принтеры, затем ПК, затем ноутбуки. Приведите в отчет таблицу с сетевыми именами, IP-адресами и масками подсети, заданными устройствам, а также названиями сетевых интерфейсов коммутатора, к которым эти устройства подключены.

5. Выполните проверку связи между одним из ноутбуков и любым ПК, любым сервером, любым принтером. Приведите в отчет скриншоты с результатами проверки.

6. Измените IP-адреса первой половины Ваших ПК на адреса из диапазона адресов IP-сети 192.168.(v+1).0-192.168.(v+1).255, имеющей маску подсети 255.255.255.0. Проверьте связь на сетевом уровне между PC1 и PCM (М – максимальный ПК). Проверьте связь между PC1 и PC2. Приведите результаты исследования в отчет.

7. Добавьте в Вашу топологию маршрутизатор (роутер) и настройте его таким образом, чтобы хосты из подсети 192.168.v.0 могли пинговать хосты подсети 192.168.(v+1).0 и наоборот.

8. Проверьте связь с сервером, открыв на нем Web-страницу с помощью Web-браузера, которым оснащен ПК. Но прежде на сервере в HTML-странице HTTP-сервера введите следующую информацию: Ваше Ф.И.О., номер группы и вариант.

7. Содержание отчета

1. Титульный лист.
2. Исходные данные в соответствии с индивидуальным вариантом.
3. Описание всех использованных команд.
4. Скриншот получившейся топологии.
5. Выводы.