

Иван Трещев
Игорь Кожин

Эмуляторы и симуляторы сетей ЭВМ

Для студентов
технических
специальностей

Иван Трещев

**Эмуляторы и симуляторы
сетей ЭВМ. Для студентов
технических специальностей**

«Издательские решения»

Трещев И. А.

Эмуляторы и симуляторы сетей ЭВМ. Для студентов технических специальностей / И. А. Трещев — «Издательские решения»,

ISBN 978-5-44-939748-5

Данная книга содержит описание работы симулятора Cisco Packet Tracer и эмулятора GNS3. В ней приведены основные отличия между данными категориями программного обеспечения. Приведены лабораторные работы для создания практических курсов по данному программному обеспечению.

ISBN 978-5-44-939748-5

© Трещев И. А.
© Издательские решения

Содержание

Введение	6
1 НЕМНОГО ОБ ЭМУЛЯТОРАХ И СИМУЛЯТОРАХ СЕТЕЙ	7
2 НЕМНОГО О CISCO IOS	9
3 GNS3	12
3.1 Базовая настройка	12
3.2 Создание простой сети	18
3.3 Включение в сеть хоста VPCS	24
3.4 Добавление коммутатора в топологию	27
4 CISCO IOS	30
4.1 Подробнее о Cisco Packet Tracer	30
4.1.1 Получение Cisco Packet Tracer	31
4.1.2 Интерфейс Cisco Packet Tracer	32
4.1.3 Создание простой сети	35
4.1.4 Добавление хостов в сеть	39
4.1.5 Добавление коммутаторов в топологию	42
4.2 Настройка протоколов в IOS	44
4.2.1 Syslog	45
4.2.2 NTP	46
4.2.3 Сброс пароля на устройстве	48
4.2.4 VLAN	50
Конец ознакомительного фрагмента.	51

Эмуляторы и симуляторы сетей ЭВМ Для студентов технических специальностей

**Иван Андреевич Трещев
Игорь Александрович Кожин**

«Эмулятор, симулятор, имитатор – в чем же разница?» – студент 2-го курса.

«Самая могущественная команда? Конечно же show-running-config!» – инженер отдела технического сопровождения.

Специалист по сетям и телекоммуникациям Семен Васильевич Евсеев

Разработка сетевых инфраструктур, сбор материала Андрей Игоревич Рыжков

© Иван Андреевич Трещев, 2018

© Игорь Александрович Кожин, 2018

ISBN 978-5-4493-9748-5

Создано в интеллектуальной издательской системе Ridero

Введение

В настоящее время существует довольно большое количество разнообразных устройств для организации сетей Ethernet. Данные сети получили самое широкое распространение в мире из-за дешевизны оборудования и простоты развертывания. Если говорить о сетях Fiber Channel то даже для них существует идеология FCoE.

Автор хотел бы выразить огромную благодарность студентам старших курсов принимавших участие в создании данной книги и Евсееву С. В. без которого ее создание было бы невозможным.

Мы живем в эпоху цифровых технологий и современным специалистам необходимы знания об устройстве сетей и систем связи. ЭВМ служит не только для формирования огромного количества документов, но и упрощает взаимодействие между пользователями.

В данной книге нет описания интернет, технологий электронной почты, пиринговых сетей, блок-чейн технологий и других механизмов существующих сегодня. Она скорее ориентирована на технических специалистов знакомых с курсом «Сети и телекоммуникации» и желающих более глубоко изучить механизмы взаимодействия сетевых устройств.

1 НЕМНОГО ОБ ЭМУЛЯТОРАХ И СИМУЛЯТОРАХ СЕТЕЙ

Для того, чтобы перейти непосредственно к лабораторным работам, необходимо дать основную информацию о том, где и как будут работы будут выполняться.

Для проектирования, настройки и тестирования сетей необязательно иметь огромное количество оборудования под рукой. Для таких целей существует специальное программное обеспечение, называемое **эмуляторами** или **симуляторами сетей**.

Под **эмуляторами** подразумевается такой тип программного обеспечения, который позволяет копировать (или *эмулировать*) функций одной вычислительной системы (*гостя*) на другой, отличной от первой, вычислительной системе (*хосте*) таким образом, чтобы эмулированное поведение как можно ближе соответствовало поведению оригинальной системы (*гостя*). Эмуляция требует серьезных вычислительных мощностей хоста, что может упереться в определенные проблемы при работе с этим ПО.

Эмуляции могут подвергаться операционные системы (с помощью таких программ, как *VirtualBox*, *Virtual Machine Manager*, *KVM*, *VMware Workstation*, *DOSBox*), некоторые виды периферийных устройств, оптические устройства (*Alcohol*, *DAEMON Tools*, *Nero Burning ROM*), игровые консоли (*PCSX2*, *Dolphin*, *Project64*). Многие эмуляторы разработаны и доступны под лицензией GNU General Public License как открытое программное обеспечение. Лицензия GNU GPL предоставляет пользователю права копировать, модифицировать и распространять (в том числе на коммерческой основе) программы, а также гарантировать, что и пользователи всех производных программ получат вышеперечисленные права

Сетевые эмуляторы позволяют эмулировать на компьютере пользователя (*хосте*) различные сетевые устройства с их операционными системами (*гостями*) и создавать связи между виртуальными и реальными устройствами с помощью моделирования сложных сетей. К такому типу программного обеспечения относится широко распространенный **Графический симулятор сетей (Graphical Network Simulator-3, GNS3)**.

GNS3 – это бесплатное программное обеспечение с открытым исходным кодом, с помощью которого можно создавать топологии сетей и эмулировать различные устройства с помощью виртуальных машин. С её помощью возможно скопировать операционную систему Cisco IOS с реального физического маршрутизатора Cisco и запустить его на виртуальном эмулированном маршрутизаторе Cisco в GNS3, или взять официальный образ системы и начать работать, что называется, «с чистого листа». Все данные, которые передаются в созданной топологии, можно перехватить с помощью анализатора трафика WireShark и проводить различные исследования. Так же GNS3 поддерживает устройства других поставщиков, отличных от Cisco.

Исключением для эмуляции в GNS3 (как и в любом другом продукте подобного рода) являются коммутаторы, так как работу коммутаторов практически невозможно эмулировать из-за особенностей самих устройств. В GNS3 их работа лишь симулируется. Так же из-за того, что устройства эмулируются на хосте, при увеличении топологии они будут потреблять все больше и больше ресурсов хоста, особенно это касается процессора.

Скачать GNS3 можно непосредственно с официального сайта проекта gns3.com или с официальной страницы GitHub github.com/GNS3/gns3-gui/releases. О дополнительных возможностях данного продукта можно узнать в официальной документации docs.gns3.com. На момент написания данной книги актуальной версии GNS3 является 2.1.11.

Другой программой для симуляции сети является **Cisco Packet Tracer**.

Cisco Packet Tracer является официальным продуктом Cisco для студентов Сетевой академии, который имитирует сети Cisco. Данный продукт не поддерживает устройства других

вендоров, а также лишь симулирует работу различных устройств в топологии, что сказывается на ограничениях функционала устройств. Однако Cisco Packet Tracer легко настраиваемый и потребляет на порядок меньше ресурсов хоста, в отличие от GNS3. Он может подойти для создания небольшой топологии, а также для создания различных учебных задач.

Официально получить данную программу можно только на сайте Сетевой академии netacad.com, записавшись на курс «*Introduction to Packet Tracer*» netacad.com/ru/courses/packet-tracer/introduction-packet-tracer. Это и предлагается сделать нашим читателям.

2 НЕМНОГО О CISCO IOS

Для того, чтобы начать настройку маршрутизаторов, необходимо рассказать о режимах работы операционной системы Cisco IOS.

Cisco IOS (Internetwork Operating System – Межсетевая Операционная Система) – программное обеспечение, используемое в маршрутизаторах и сетевых коммутаторах Cisco. Cisco IOS является многозадачной операционной системой, выполняющей функции сетевой организации, маршрутизации, коммутации и передачи данных.

В Cisco IOS есть специфичный интерфейс **командной строки (command line interface, CLI)**, который был скопирован многими другими сетевыми продуктами. Интерфейс IOS предлагает набор многословных команд, согласно выбранному режиму и уровню привилегий пользователя.

Все режимов пять:

1. Пользовательский режим. В данном режиме командная строка имеет вид (*SW1>*). Данный режим дает доступ к ограниченному количеству базовых команд для мониторинга системы. В нем нельзя совершать какие-либо настройки устройства;

2. Привилегированный режим. В данном режиме командная строка имеет вид (*SW1#*). Он дает доступ ко всем остальным командам;

3. Глобальный режим конфигурации. Командная строка имеет вид (*SW1 (config) #*). Данный режим позволяет вносить изменения, влияющие на работу всего устройства в целом;

4. Режим настройки линии. Командная строка имеет вид (*SW1 (config-line) #*). Он нужен для настройки доступа через консоль, SSH, Telnet;

5. Режим настройки интерфейса. Командная строка имеет вид (*SW1 (config-if) #*). Нужен для настройки интерфейса коммутатора или маршрутизатора.

Команды для изменения режимов:

1. Войти в привилегированный режим: *SW1> enable*
2. Выход из привилегированного режима: *SW1# disable*
3. Войти в глобальный режим конфигурации: *SW1# configure terminal*
4. Войти в режим настройки линии: *SW1 (config) # line console 0*

Команды в IOS не обязательно дописывать до конца – операционная система сама поймет, какую команду ввел пользователь. Так же для того, чтобы автоматически дописать название команды, используется кнопка Tab.

Каждому устройству Cisco можно назначить свое имя для удобного администрирования устройств. Изменим имя маршрутизатора на R1:

```
Router# configure terminal
Router (config) # hostname R1
```

Можно сделать настройку привилегированного режима, чтобы при входе в него операционная система требовала ввод пароля, который был назначен администратором. Поставим пароль **class**:

```
Router# configure terminal
Router (config) # enable secret class
```

Тоже самое можно сделать и для консольной линии, к которой подключение происходит с помощью консольного кабеля. Поставим пароль **cisco** и включим доступ к пользовательскому режиму:

```
Router# configure terminal
Router (config) # line console 0
Router (config-line) # password cisco
Router (config-line) # login
```

Виртуальные линии используются для подключения к устройству с помощью таких программ, как PuTTY или Tera Term. Сделаем настройку для всех шестнадцати виртуальных линий прописав диапазон от 0 до 15 и поставим пароль для доступа к пользовательскому режиму:

```
Router# configure terminal
Router (config) # line vty 0 15
Router (config-line) # password cisco
Router (config-line) # login
```

При открытии файла конфигурации на устройстве все пароли, которые настроены, будут показаны открыто как есть. Команда **service password-encryption** дает программному обеспечению IOS указание зашифровать пароли, секреты CHAP и другие, аналогичные данные, которые хранятся в файле конфигурации.

```
Router# configure terminal
Router (config) # service password-encryption
```

В набор команд Cisco IOS входит команда, позволяющая настроить сообщение, которое будут видеть все, кто входит в систему. Это сообщение называется сообщением дня или баннером **MOTD (Message of the Day)**. Установить текст баннера можно при помощи команды **banner motd**

```
Router# configure terminal
Router (config) # banner motd #Ваше сообщение для#1
```

Все настройки, которые были произведены на устройстве, будут сохранены в оперативной памяти (ОЗУ). Чтобы посмотреть файл конфигурации, требуется ввести команду **show running-config**. Обратите внимание, что после выключения устройства настройки не будут сохранены.

```
Router# show running-config
```

Сохранение текущего файла конфигурации возможно с помощью команды **copy running-config startup-config**. Это позволит перезаписать конфигурацию, которая будет загружаться при включении устройства. Данный файл будет храниться в энергонезависимой памяти (NVRAM).

```
Router# copy running-config startup-config
```

Просмотр сохраненной конфигурации осуществляется с помощью команды **show startup-config**

```
Router# show startup-config
```

Для очистки загрузочной информации используется команда **erase startup-config**. Для перезагрузки устройства используется команда **reload**

```
Router# erase startup-config
Router# reload
```

Пример базовой настройке приведен на рисунке 1

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Router1
Router1(config)#enable secret class
Router1(config)#line console 0
Router1(config-line)#pas
Router1(config-line)#password cisco
Router1(config-line)#login
Router1(config-line)#line vty 0 15
Router1(config-line)#pas
Router1(config-line)#password cisco
Router1(config-line)#login
Router1(config-line)#service pas
Router1(config-line)#service password-encryption
Router1(config)#banner mo
Router1(config)#banner motd #For authorized users only!#
Router1(config)#
```

¹ Вместо # можно использовать любой другой знак, который не используется в сообщении. IOS сама поймет, где обозначено само сообщение

Рисунок 1 – Пример базовых настроек в Cisco IOS. Скриншот сделан в Cisco Packet Tracer

3 GNS3

3.1 Базовая настройка

После скачивания с сайта запускаем файл с расширением .exe, имеющий имя «GNS3—2.1.11-all-in-one» и следуем по всем шагам установки, оставляя параметры по умолчанию. Во время установки будут загружены необходимые драйвера для работы с сетевыми пакетами и дополнительные программы. В их состав входит WireShark. Предупреждаем, что полная установка настройка GNS3 занимает достаточно продолжительное время, по сравнению с Cisco Packet Tracer. По этой причине функционал последней мы подробно рассматривать не будем. Отдельные элементы программы Cisco Packet Tracer будут рассмотрены в пятой главе «Cisco IOS».

Итак, после окончания процесса установки запускаем GNS3. Для удобства можете выбрать стандартные директории для образов операционных систем и проектов, там они будут храниться.

Приступим к настройке. Перейдем в окно настроек *Edit – Preferences...* (рисунок 2 – 4) и загрузим образы операционных систем для маршрутизаторов.

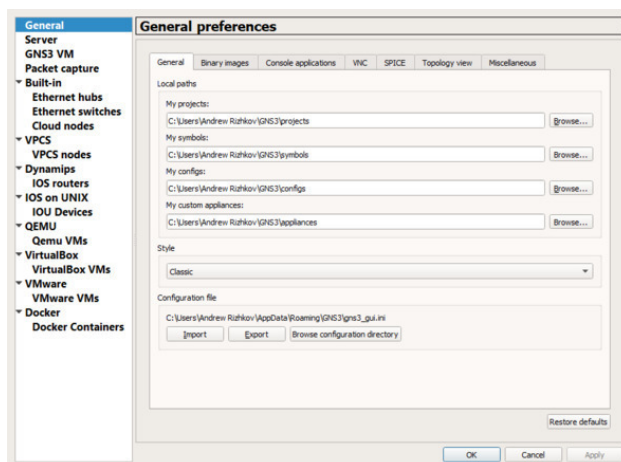


Рисунок 2 – Выбор стандартных директорий

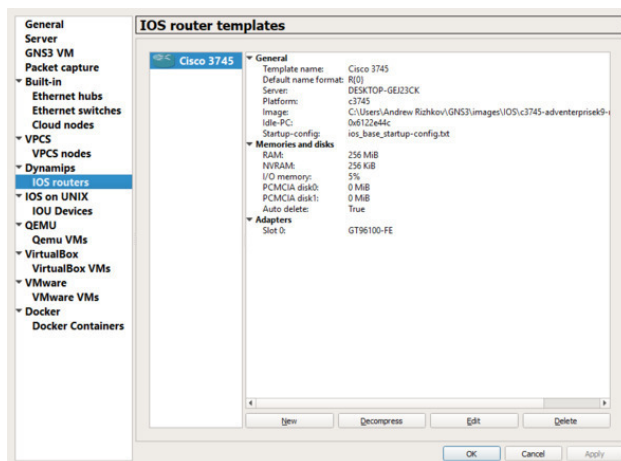


Рисунок 3 – Список установленных Cisco ISO. Для добавления нового образа требуется нажать на кнопку New

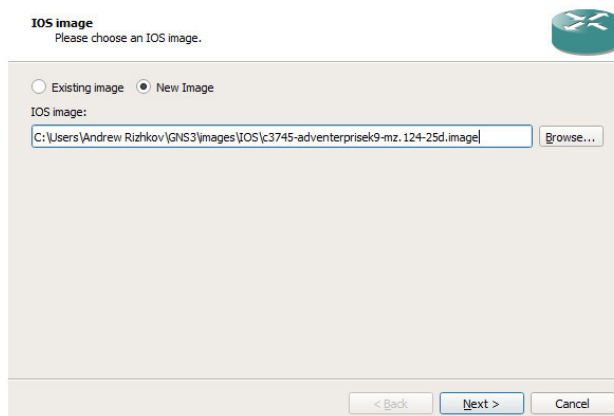


Рисунок 4 – Добавление новых образов

Далее пишем название маршрутизатора и платформы (рисунок 5), выставляем оперативную память (рисунок 6), которая выделяется для него. Можно оставить значение по умолчанию, а можно добавить дополнительную память при условии, что хост достаточно мощный. Следующим шагом (рисунок 7) выставляем нужные сетевые адаптеры. Данные значение оставляем по умолчанию. Idle-PC (рисунок 8) оставим как есть. Позже поговорим о ней подробнее. При завершении настроек мы увидим новое устройство в списке (рисунок 9).

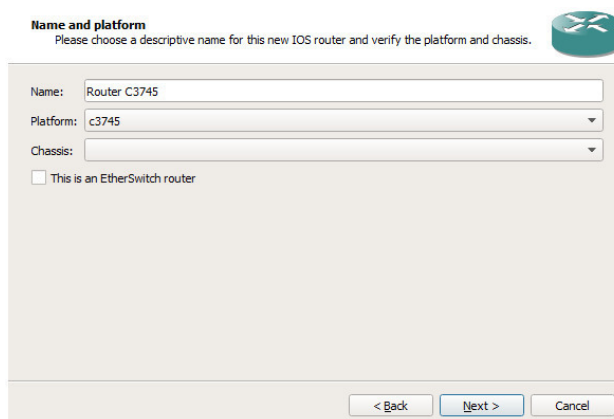


Рисунок 5 – Добавление названия для образа и выбор устройства, которое будет эмулироваться

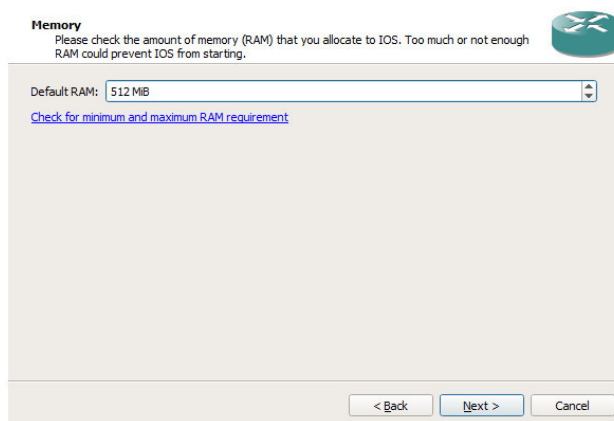


Рисунок 6 – Выделение оперативной памяти

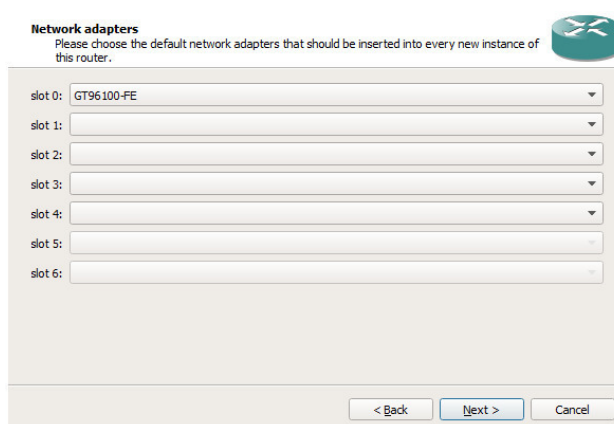


Рисунок 7 – Добавление сетевого адаптера

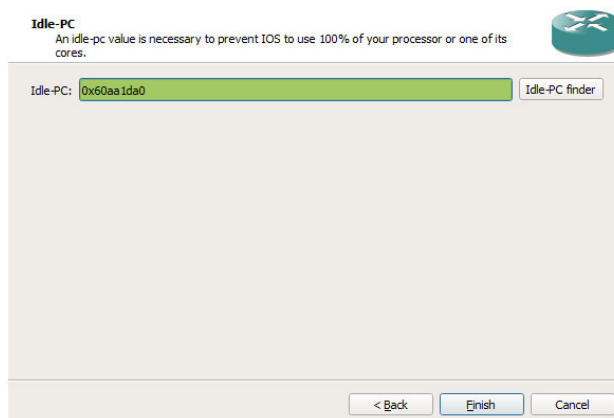


Рисунок 8 – Добавление значения Idle-PC

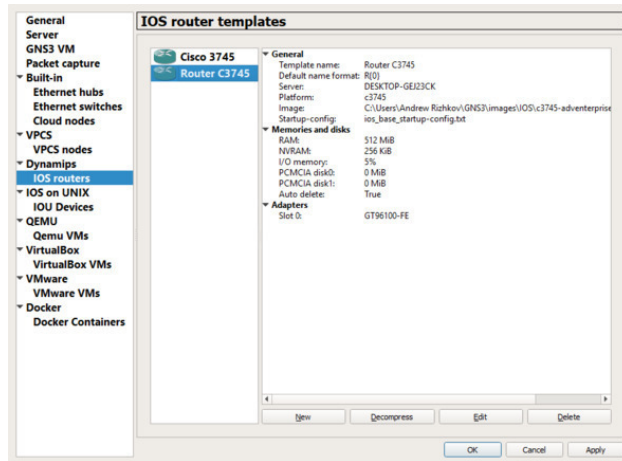


Рисунок 9 – После всех настроек устройство будет добавлено в список

Добавим новый маршрутизатор в нашу сеть. Для этого с левой стороны нажимаем на иконку маршрутизатора, находим наше устройство и перетаскиваем его в рабочую область по середине (рисунок 10).

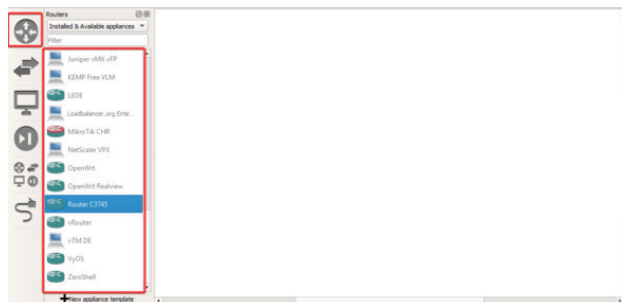


Рисунок 10 – Добавление устройства на рабочую область

После добавление устройства запускаем его нажатием кнопки Play в панели инструментов (рисунок 11) и подключаемся через консольный порт к добавленному устройству, нажав ПКМ по нашему маршрутизатору (рисунок 12).



Рисунок 11 – Play

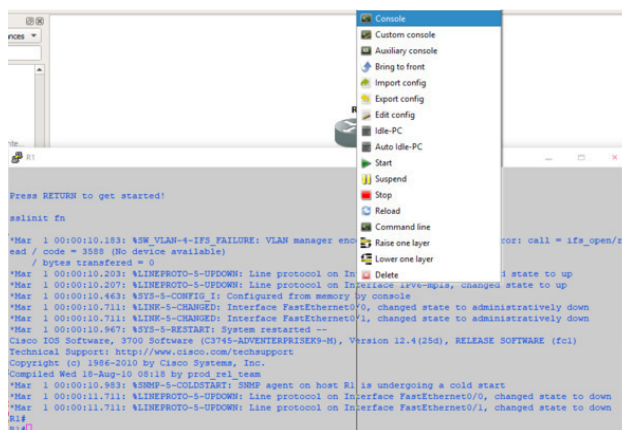


Рисунок 12 – Открытие консоли

Однако нагрузка на процессор компьютера станет огромной (рисунок 13). Для того, чтобы уменьшить нагрузки на хост, требуется применить значение Idle-PC, которое позволяет уменьшить загруженность нашего компьютера. Для этого ПКМ нажимаем по маршрутизатору и выбираем Idle-PC. Программа рассчитает необходимые нам данные и из появившегося окна выбираем нужные нам значения (рисунок 14). Несмотря на то, что программа заявляет, что значения, обозначенные звездочкой (*) является самыми оптимальными, на практике все иначе. Часто значения приходится перебирать, сравнивая нагрузку на процессор при каждом установленном значении Idle-PC и выбирать таким образом подходящую для нас опцию (рисунок 15). На рисунке 16 показана нагрузка на компьютер после применения данной настройки. Обратите внимание, что данную процедуру необходимо применять для каждого добавляемого устройства!

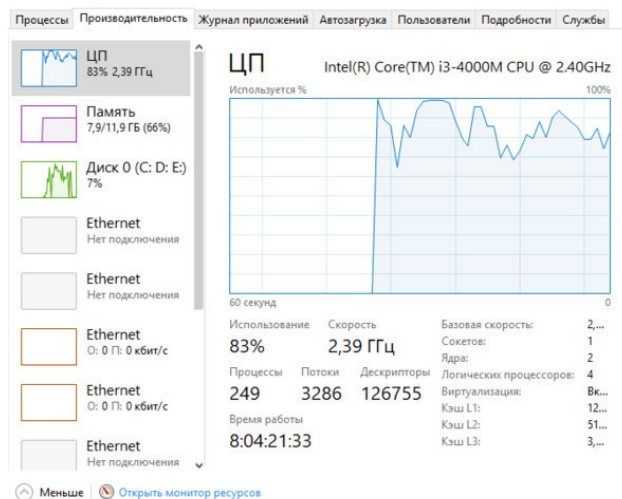


Рисунок 13 – Нагрузка на процессор хоста до применения настроек Idle-PC

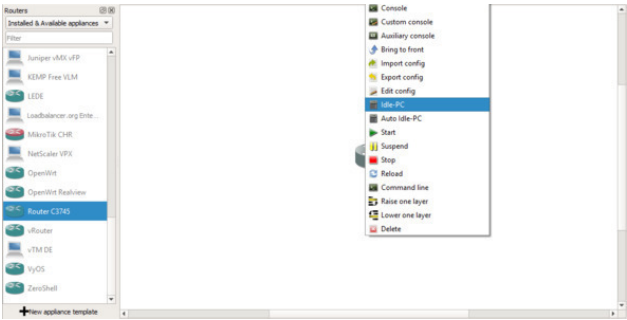


Рисунок 14 – Idle-PC

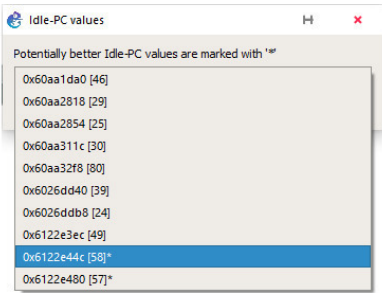


Рисунок 15 – Выбор предложенных значений

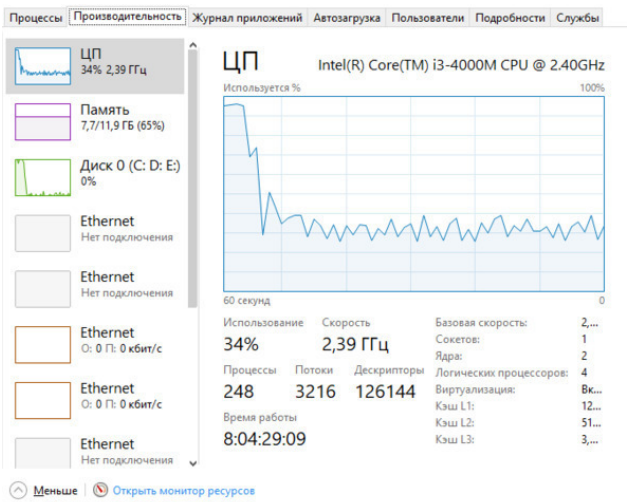


Рисунок 16 – Нагрузка на процессор хоста после применения настроек Idle-PC

3.2 Создание простой сети

Создадим и настроим простую сеть. Для этого добавим несколько маршрутизаторов (рисунок 17) и соединим их (рисунки 18 – 20).

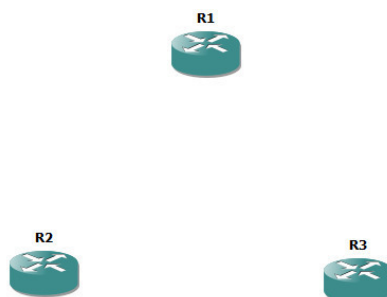


Рисунок 17 – Добавление маршрутизаторов



Рисунок 18 – Add a Link

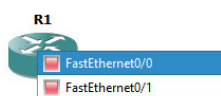


Рисунок 19 – Выбор интерфейса для подключения кабеля

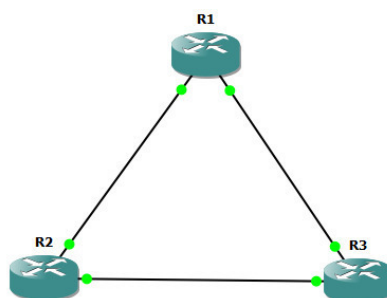


Рисунок 20 – Пример подключения маршрутизаторов

Изменим названия маршрутизаторов, поменяем иконку для «главного» маршрутизатора в сети, добавим номера сетей, включим обозначение интерфейсов и рамку (рисунки 21 – 25).

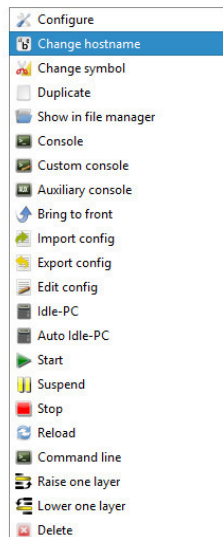


Рисунок 21 – Нажимаем ПКМ по иконке устройства. Изменить название можно с помощью Change hostname, изменить иконку – Change symbol



Рисунок 22 – Кнопка добавления текста



Рисунок 23 – Кнопка добавления рамки



Рисунок 24 – Кнопка включения-выключения обозначения интерфейсов

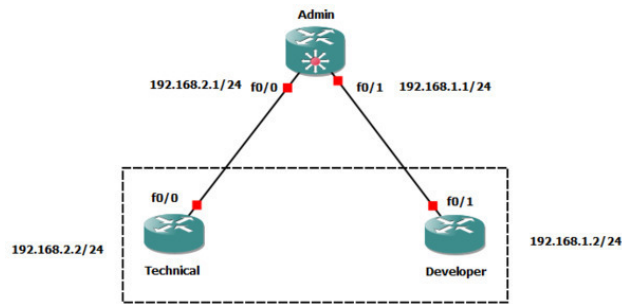


Рисунок 25 – Пример оформления топологии

Проведем настройку маршрутизатора, подключившись по консольному порту (рисунок 26). Интерфейсу назначим IP-адрес с указанием маски подсети и включим интерфейс командой **no shutdown**.

```
R1#config t
R1 (config) #int fa0/0
R1 (config-if) #ip address 192.168.2.1 255.255.255.0
R1 (config-if) #no shutdown
R1 (config-if) #interface fa0/1
R1 (config-if) #ip address 192.168.1.1 255.255.255.0
R1 (config-if) #no shutdown
```

```
*Mar 1 00:00:12.247: %LINEPROTO-5-UPDOWN: Line protocol on Interface IPv4-mp1s, changed state to up
*Mar 1 00:00:12.563: %SYS-5-CONFIG I: Configured from memory by console
*Mar 1 00:00:12.739: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down
*Mar 1 00:00:12.739: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
*Mar 1 00:00:13.099: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 3700 Software (C3745-ADVENTERPRISEK9-M), Version 12.4(25d), RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Wed 18-Aug-10 08:18 by prod_rel_team
*Mar 1 00:00:13.115: %SNMP-5-COLDSTART: SNMP agent on host R1 is undergoing a cold start
*Mar 1 00:00:13.739: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down
*Mar 1 00:00:13.739: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
R1#
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int fa0/0
R1(config-if)#ip address 192.168.2.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#
*Mar 1 00:01:29.839: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 00:01:30.839: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config-if)#interface fa0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
```

Рисунок 26 – Настройка интерфейсов маршрутизатора. Скриншот сделан в PuTTY, подключенный к виртуальной машине, работающей в GNS3

Те же самые настройки сделаем и для остальных маршрутизаторов в нашей сети. Вдобавок назначим имя устройству и совершим проверку соединения с маршрутизатором Admin путем использования команды **ping**. Приведем пример настройки маршрутизатора Technical (рисунок 27):

```
R2#config t
R2 (config) #int fa0/0
R2 (config-if) #ip address 192.168.2.2 255.255.255.0
R2 (config-if) #no shutdown
R2 (config-if) #exit
R2 (config) #hostname Technical
Technical (config) #exit
Technical#ping 192.168.2.1
```

Аналогичные действия совершаем с маршрутизатором Developer (рисунок 28).

```
R3#config t
R3 (config) #int fa0/1
R3 (config-if) #ip address 192.168.1.2 255.255.255.0
R3 (config-if) #no shutdown
```

R3 (config-if) #do ping 192.168.1.1

R3 (config-if) #exit

R3 (config) #hostname Developer

Не забываем сохранить введенные настройки в энергонезависимую память маршрутизатора:

Developer (config) #exit

Developer#copy running-config startup-config

```
R2(config)#int fa0/0
R2(config-if)#ip address 192.168.2.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#
*Mar 1 00:00:54.723: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 00:00:55.723: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R2(config-if)#exit
R2(config)#hostname Technical
Technical(config)#do ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
~!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 40/58/68 ms
Technical(config)#
Technical#
*Mar 1 00:01:52.251: %SYS-5-CONFIG_I: Configured from console by console
Technical#
```

Рисунок 27 – Настройка интерфейсов маршрутизатора Technical и проверка соединения с соседний маршрутизатором. Скриншот сделан в PuTTY, подключенный к виртуальной машине, работающей в GNS3

```
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#int fa0/1
R3(config-if)#ip address 192.168.1.2 255.255.255.0
R3(config-if)#
% Invalid input detected at '^' marker.
R3(config-if)#ip address 192.168.1.2 255.255.255.0
R3(config-if)#no sha
R3(config-if)#no shutdown
R3(config-if)#
*Mar 1 00:18:50.215: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar 1 00:18:51.215: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
R3(config-if)#do ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
~!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 36/56/64 ms
R3(config-if)#exit
R3(config)#hostname Developer
Developer(config)#exit
Developer#
*Mar 1 00:19:32.803: %SYS-5-CONFIG_I: Configured from console by console
Developer#copy ru
Developer#copy running-config s
Developer#copy running-config sta
Developer#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Developer#
```

Рисунок 28 – Настройка интерфейсов маршрутизатора Developer, проверка соединения с соседний маршрутизатором, изменение имени устройства и сохранение текущей конфигурации в энергонезависимой памяти

Обратите внимание, что команда **ping** выполняется совместно с командой **do**. Дело в том, что если на устройстве работает операционная система Cisco IOS 12.2 (8) или выше, вы имеете возможность использовать команду **do** для запуска привилегированных команд из режима конфигурации.

Добавим дополнительный маршрутизатор в нашу сеть. Так как в стандартном маршрутизаторе уже не хватает интерфейсов, добавим новый с помощью настроек (рисунок 29).

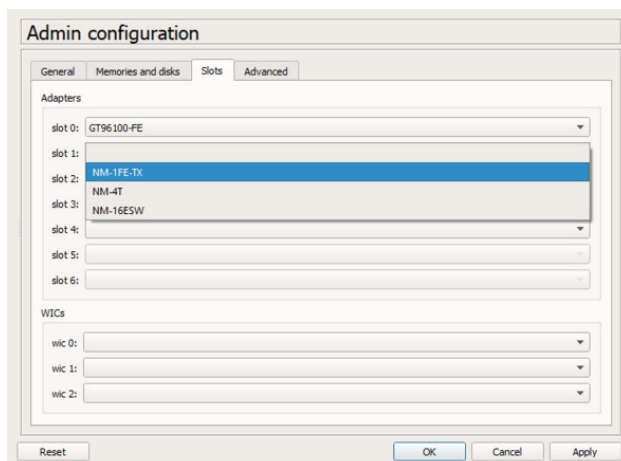


Рисунок 29 – Добавление нового интерфейса

Аналогичным способом назначается IP-адрес новому интерфейсу Admin f1/0 и интерфейсу Customer f0/0 с учетом топологии сети. Конечный вид топологии приведён на рисунке 30.

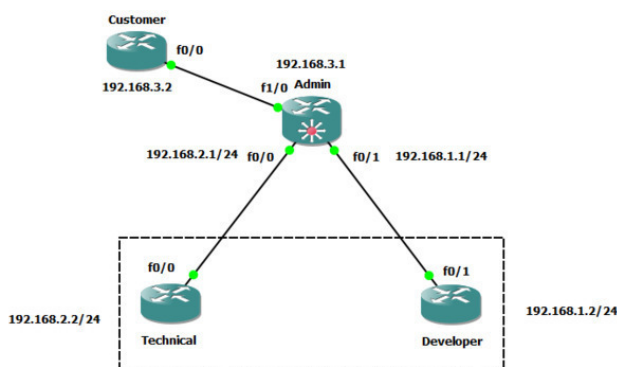


Рисунок 30 – Окончательная топология сети

Сохраним данный проект, зайдём в папку, где он расположен, увидим там файлы конфигурации каждого маршрутизатора. По умолчанию их местоположение находится по адресу C:\Users\%USERNAME%\GNS3\projects (рисунок 31).

```
49 !
50 !
51 !
52 !
53 interface FastEthernet0/0
54   ip address 192.168.2.1 255.255.255.0
55   duplex auto
56   speed auto
57 !
58 interface FastEthernet0/1
59   ip address 192.168.1.1 255.255.255.0
60   duplex auto
61   speed auto
62 !
63 ip forward-protocol nd
64 !
65 !
66 no ip http server
67 no ip http secure-server
68 !
69 no cdp log mismatch duplex
70 !
71 !
72 !
73 control-plane
74 !
```

Рисунок 31 – Конфигурационный файл

3.3 Включение в сеть хоста VPCS

Добавим в сеть хост VirtualPC Simulator. Данный способ широко используется, если вам нужна простая модель компьютера в топологии, например, для проверки пинга. Виртуальный хост практически не затрачивает ресурсы (каждый VPCS требует всего 2 мегабайта оперативной памяти!) компьютера и очень просто разворачивается. Работа с ним ведется с помощью консоли по средствам ввода команд.

Добавим в сеть маршрутизатор и два компьютера VPCS из раздела с оконечными устройствами (рисунок 32). Пример окончательной топологии продемонстрирован на рисунке 33.

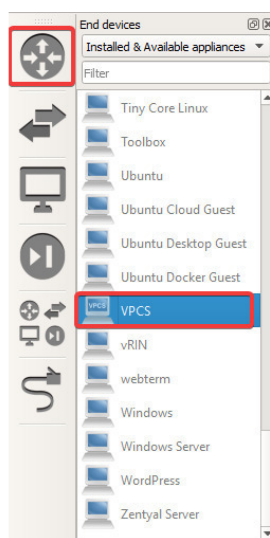


Рисунок 32 – Добавление виртуального хоста

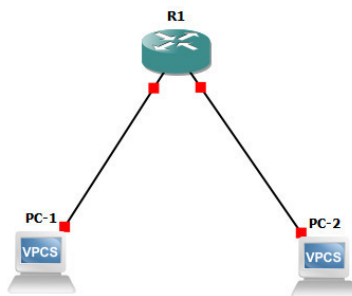


Рисунок 33 – Пример топологии

Посмотрим характеристики компьютера, прописав команду **show**. Увидим MAC-адрес, шлюз по умолчанию, IPv4, IPv6, маску, UDP-порты для передачи (10008) и передачи – 10009 (рисунок 34).


```

Welcome to Virtual PC Simulator, version 0.6.1
Dedicated to Daling.
Build time: Jun 1 2015 11:42:32
Copyright (c) 2007-2014, Paul Meng (mirnashi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

PC-1>
PC-1> show

NAME  IP/MASK      GATEWAY      MAC          LPORT  RHOST:PORT
PC-1  0.0.0.0/0    0.0.0.0       00:50:79:66:68:00  10012  127.0.0.1:10013
      fe80::250:79ff:fe66:6800/64
PC-1>

```

Рисунок 34 – Применение команды show на виртуальном хосте

Произведем статическую настройку IP-адреса (рисунок 35):

ip 192.168.1.2/24 192.168.1.1,

где *192.168.1.2/24* – IPv4-адрес и маска подсети;

192.168.1.1 – шлюз по умолчанию.

```

PC-1> ip 192.168.1.2/24 192.168.1.1
Checking for duplicate address...
PC1 : 192.168.1.2 255.255.255.0 gateway 192.168.1.1

PC-1> show

NAME  IP/MASK      GATEWAY      MAC          LPORT  RHOST:PORT
PC-1  192.168.1.2/24  192.168.1.1  00:50:79:66:68:00  10012  127.0.0.1:10013
      fe80::250:79ff:fe66:6800/64

```

Рисунок 35 – Статическая настройка IPv4-адреса на хосте

Проведем настройку интерфейса маршрутизатора:

conf t

int fa0/0

ip address 192.168.1.1 255.255.255.0

no shutdown

exit

do write

Теперь пропиnguем с первого компьютера основной шлюз (рисунок 36):

```

PC-1> show

NAME  IP/MASK      GATEWAY      MAC          LPORT  RHOST:PORT
PC-1  0.0.0.0/0    0.0.0.0       00:50:79:66:68:00  10012  127.0.0.1:10013
      fe80::250:79ff:fe66:6800/64

PC-1> ip 192.168.1.2/24 192.168.1.1
Checking for duplicate address...
PC1 : 192.168.1.2 255.255.255.0 gateway 192.168.1.1

PC-1> show

NAME  IP/MASK      GATEWAY      MAC          LPORT  RHOST:PORT
PC-1  192.168.1.2/24  192.168.1.1  00:50:79:66:68:00  10012  127.0.0.1:10013
      fe80::250:79ff:fe66:6800/64

PC-1> ping 192.168.1.1
192.168.1.1 icmp_seq=1 timeout
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.979 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=1.999 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=10.006 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=255 time=2.998 ms
PC-1>

```

Рисунок 36 – Пингование шлюза по умолчанию

Теперь настроим маршрутизатор, чтобы тот смог выдавать динамически IP-адреса с помощью DHCP:

conf t

int fa0/1

ip address 192.168.2.1 255.255.255.0

no shutdown

exit

```
ip dhcp pool DHCP
network 192.168.2.0 255.255.255.0
default-router 192.168.2.1
end
```

Настроим хост для динамического получения IP-адреса

```
ip dhcp
```

Посмотрим, какой IP-адрес был присвоен автоматически компьютеру PC-2 (рисунок 37) и проведем пинг до основного шлюза и пинг до PC-1 (рисунок 38).

```
PC-2>
PC-2> ip dhcp
DHCPA IP 192.168.2.2/24 GW 192.168.2.1

PC-2> show
```

NAME	IP/MASK	GATEWAY	MAC	LPORT	RHOST:PORT
PC-2	192.168.2.2/24	192.168.2.1	00:50:79:66:68:01	10015	127.0.0.1:10017
	fe80::250:79ff:fe66:6801/64				

Рисунок 37 – Динамическое получение IP-адреса

```
PC-2> ping 192.168.2.1
84 bytes from 192.168.2.1 icmp_seq=1 ttl=255 time=7.996 ms
84 bytes from 192.168.2.1 icmp_seq=2 ttl=255 time=8.995 ms
84 bytes from 192.168.2.1 icmp_seq=3 ttl=255 time=3.949 ms
84 bytes from 192.168.2.1 icmp_seq=4 ttl=255 time=10.993 ms
84 bytes from 192.168.2.1 icmp_seq=5 ttl=255 time=9.044 ms

PC-2> ping 192.168.1.2
192.168.1.2 icmp_seq=1 timeout
192.168.1.2 icmp_seq=2 timeout
84 bytes from 192.168.1.2 icmp_seq=3 ttl=63 time=19.973 ms
84 bytes from 192.168.1.2 icmp_seq=4 ttl=63 time=17.004 ms
84 bytes from 192.168.1.2 icmp_seq=5 ttl=63 time=14.951 ms
```

Рисунок 38 – Процесс пинга до шлюза по умолчанию и PC-1

3.4 Добавление коммутатора в топологию

Включим в сеть коммутаторы. В GNS3 они имеют ограниченный функционал из-за сложности эмуляции, так как в них используются сложные микросхемы.

Создадим топологию как на рисунке 39 и на её основе настроим две виртуальные локальные сети VLAN.

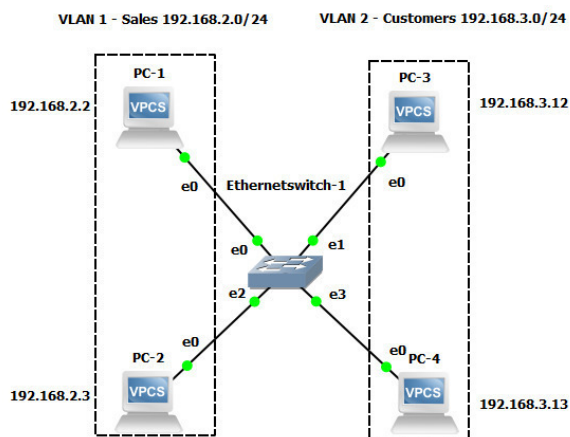


Рисунок 39 – Создание сети с коммутатором

VLAN (Virtual Local Area Network) – топологическая («виртуальная») локальная компьютерная сеть, представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к ширококвещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным членам группироваться вместе, даже если они не находятся в одной физической сети.

VLAN создает логический ширококвещательный домен, который может охватывать несколько физических сегментов LAN. Разделяя крупные ширококвещательные домены на более мелкие сети, VLAN повышают производительность сети. Если устройство в одной VLAN передает ширококвещательный кадр Ethernet, то этот кадр получают все устройства в рамках этой VLAN, устройства же в других сетях VLAN этот кадр не получают.

Порт сетевого устройства может находиться в 2-х состояниях: **Access** или **Trunk**:

1. **Access port** или **порт доступа** – порт, находящийся в определенном VLAN и передающий не тегированные кадры. Как правило, это порт, смотрящий на пользовательское устройство.

2. **Trunk port** или **магистральный порт** – порт, передающий тегированный трафик. Как правило, этот порт поднимается между сетевыми устройствами.

Так как у нас к коммутатору подключены только оконечные устройства, то все порты настраиваем как порты доступа.

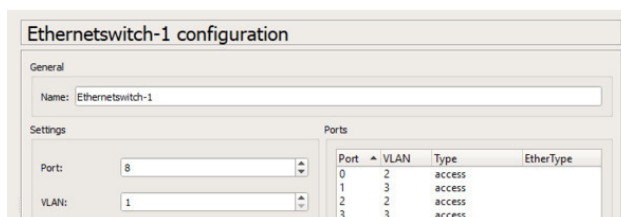


Рисунок 40 – Настройка Access-портов

Каждому компьютеру назначим соответствующие IP-адреса с помощью команды **ip**:

ip 192.168.2.2/24 192.168.2.1

ip 192.168.2.3/24 192.168.2.1

ip 192.168.3.12/24 192.168.3.1

ip 192.168.3.13/24 192.168.3.1

Теперь добавим в нашу сеть маршрутизатор по архитектуре **Router-on-a-Stick** («Маршрутизатор на палочке») (рисунок 41)

Router-on-a-Stick – способ создания сети, маршрутизатор в которой имеет в качестве интерфейса всего один порт, подключенный напрямую к коммутатору с настроенным VLAN. Порт, к которому подключен маршрутизатор, должен быть настроен в режиме Trunk (рисунок 42).

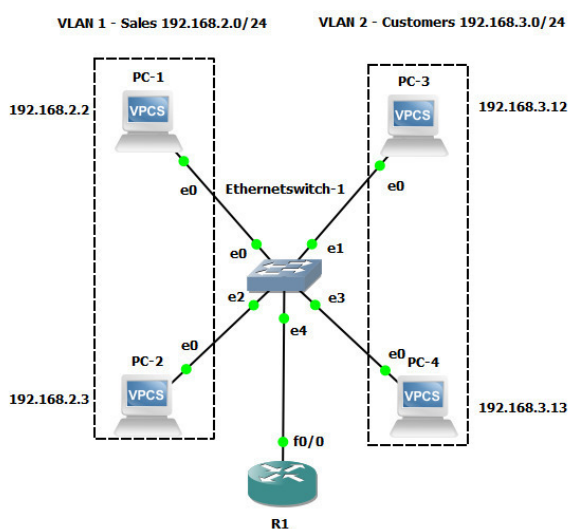


Рисунок 41 – Router-on-a-Stick

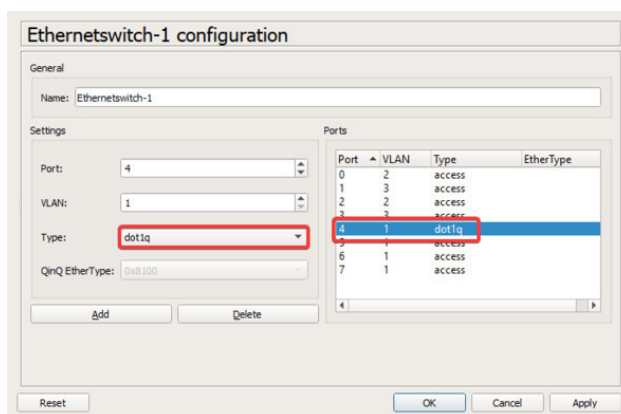


Рисунок 42 – Настройка транкового порта

Произведем настройку VLAN на маршрутизаторе (рисунок 43):

conf t

int fa0/0

no shutdown

exit

```

int fa0/0.2
encapsulation dot1Q 2
ip address 192.168.2.1 255.255.255.0
no shutdown
exit

```

```

int fa0/0.3
encapsulation dot1Q 3
ip address 192.168.3.1 255.255.255.0
no shutdown
end
do write

```

```

*Mar 1 00:00:10.491: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
*Mar 1 00:00:10.491: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down
R1#
R1conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int fa0/0
R1(config-if)#no shutdown
R1(config-if)#
R1(config-if)#exit
R1(config)#
R1(config)#int fa0/0.2
R1(config-subif)#
R1(config-subif)#encapsulation dot1Q 2
R1(config-subif)#ip address 192.168.2.1 255.255.255.0
R1(config-subif)#no shutdown
R1(config-subif)#exit
R1(config)#
R1(config)#int fa0/0.3
R1(config-subif)#encapsulation dot1Q 3
R1(config-subif)#
R1(config-subif)#ip address 192.168.3.1 255.255.255.0
R1(config-subif)#no shutdown
R1(config-subif)#end
R1#

```

Рисунок 43 – Настройка VLAN на маршрутизаторе

Для проверки правильности настройки VLAN на маршрутизаторе, необходимо проверить пинг с одного VLAN на другой VLAN (рисунок 44).

```

PC-2> ping 192.168.2.2
84 bytes from 192.168.2.2 icmp_seq=1 ttl=64 time=27.984 ms
84 bytes from 192.168.2.2 icmp_seq=2 ttl=64 time=0.999 ms
84 bytes from 192.168.2.2 icmp_seq=3 ttl=64 time=0.000 ms
84 bytes from 192.168.2.2 icmp_seq=4 ttl=64 time=0.999 ms
84 bytes from 192.168.2.2 icmp_seq=5 ttl=64 time=0.000 ms

PC-2>
PC-2> ping 192.168.3.12
192.168.3.12 icmp_seq=1 timeout
84 bytes from 192.168.3.12 icmp_seq=2 ttl=63 time=15.991 ms
84 bytes from 192.168.3.12 icmp_seq=3 ttl=63 time=13.992 ms
84 bytes from 192.168.3.12 icmp_seq=4 ttl=63 time=15.991 ms
84 bytes from 192.168.3.12 icmp_seq=5 ttl=63 time=21.987 ms

```

Рисунок 44 – Пинг до соседнего до хоста в одной VLAN и до хоста в соседней VLAN

4 CISCO IOS

4.1 Подробнее о Cisco Packet Tracer

4.1.1 Получение Cisco Packet Tracer

Для получения Cisco Packet Tracer официально, требуется записаться на официальный курс «*Introduction to Packet Tracer*», доступный по адресу netacad.com/ru/courses/packet-tracer/introduction-packet-tracer. Курс доступен только на английском языке.

После регистрации в личном кабинете Netacad будет доступен учебный курс. Для получения Cisco Packet Tracer перейдем в «Student Resources». По состоянию на 27 ноября 2018 года на сайте доступны две версии: 7.1.1 и 7.2. Особой разницы для нас не будет, вы можете скачать любую версию.

Рисунок 45 – Регистрация на курс

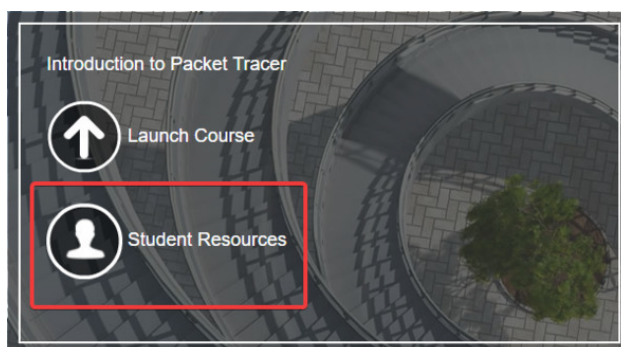


Рисунок 46 – Ресурсы для студента

<p>Join Our Communities</p> <p>Facebook</p> <p>LinkedIn</p>	<p>The Facebook site is where you can meet and engage with other Networking Academy students from around the world.</p> <p>The Cisco Networking Academy LinkedIn site connects you with job postings.</p>
<p>Packet Tracer</p> <p>You can follow this link to obtain your copy of Packet Tracer.</p> <p>Download and install the latest version of Packet Tracer Student Version</p>	<p>This course will teach you about Packet Tracer and how to obtain it.</p>

Рисунок 47 – Прямая ссылка на получение файла установки Cisco Packet Tracer

После скачивания с сайта запускаем файл с расширением .exe и следуем по всем шагам установки, оставляя параметры по умолчанию.

4.1.2 Интерфейс Cisco Packet Tracer

При запуске Cisco Packet Tracer нас встречает стандартное окно программы (рисунок 48).

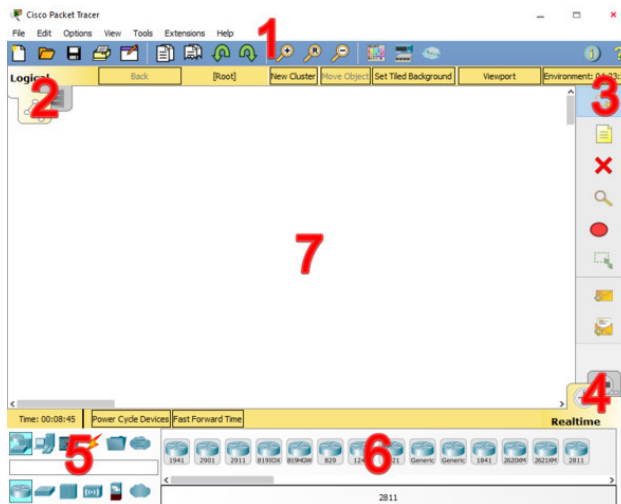


Рисунок 48 – Окно Cisco Packet Tracer

Окно состоит из нескольких частей:

1. Главное меню программы;
2. Переключатель между логической и физической организацией;
3. Ещё одна панель инструментов, содержит инструменты выделения, удаления, перемещения, масштабирования объектов, а также формирование произвольных пакетов;
4. Переключатель между реальным режимом (Real-Time) и режимом симуляции;
5. Панель с группами конечных устройств и линий связи;
6. Сами конечные устройства, здесь содержатся всевозможные коммутаторы, узлы, точки доступа, проводники.
7. Рабочее пространство.

Большую часть данного окна занимает рабочая область, в которой можно размещать различные сетевые устройства, соединять их различными способами и как следствие получать самые разные сетевые топологии.

Сверху, над рабочей областью, расположена главная панель программы и ее меню. Меню позволяет выполнять сохранение, загрузку сетевых топологий, настройку симуляции, а также много других интересных функций. Главная панель содержит на себе наиболее часто используемые функции меню.

Справа от рабочей области, расположена боковая панель, содержащая ряд кнопок, отвечающих за перемещение полотна рабочей области, удаление объектов и прочих действий.

Снизу, под рабочей областью, расположена панель оборудования.

Данная панель содержит в своей левой части типы доступных устройств, а в правой части доступные модели. При выполнении различных лабораторных работ, эту панель придется использовать намного чаще, чем все остальные. Поэтому рассмотрим ее более подробно.

При наведении на каждое из устройств, в прямоугольнике, находящемся в центре между ними, будет отображаться его тип. Будут доступны сетевые устройства (коммутаторы, маршрутизаторы, концентраторы, беспроводные устройства, брандмауэры), оконечные устройства (настольные ПК, ноутбуки, планшетные ПК, принтеры, IP-телефоны), компоненты для симуляции «Умного дома», различные типы соединения:

1. **Автоматический тип** – при данном типе соединения PacketTracer автоматически выбирает наиболее предпочтительные тип соединения для выбранных устройств;
2. **Консоль** – консольные соединение;
3. **Медь (прямой)** – соединение медным кабелем типа витая пара, оба конца кабеля обжаты в одинаковой раскладке. Подойдет для следующих соединений: коммутатор – коммутатор, коммутатор – маршрутизатор, коммутатор – компьютер;
4. **Медь (кроссовый)** – соединение медным кабелем типа витая пара, концы кабеля обжаты как кроссовер. Подойдет для соединения двух компьютеров;
5. **Оптический кабель** – соединение при помощи оптического кабеля, необходимо для соединения устройств, имеющих оптические интерфейсы;
6. **Телефонный кабель** – обыкновенный телефонный кабель, может понадобится для подключения телефонных аппаратов;
7. **Коаксиальный кабель** – соединение устройств с помощью коаксиального кабеля.



Рисунок 49 – Типы соединения

Оконечные устройства по типу настольных ПК можно настраивать индивидуально. Им можно присваивать вручную IPv4-адреса, использовать терминал (по типу PuTTY), а также использовать аналог «Командой строки» из Windows.

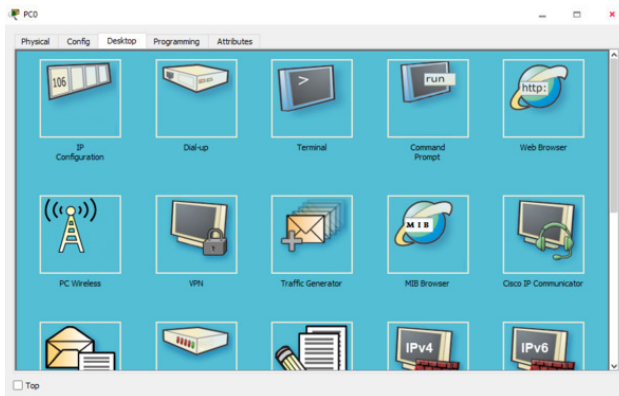


Рисунок 50 – Доступные настройки для оконечных устройств

В Cisco Packet Tracer предусмотрен режим моделирования, в котором подробно описывается и показывается, как работает утилита *Ping*. Поэтому необходимо перейти в «режим симуляции», нажав на одноименный значок в нижнем левом углу рабочей области, или по комбинации клавиш Shift+S. Откроется «Панель моделирования», в которой будут отображаться все события, связанные с выполнения Ping-процесса.

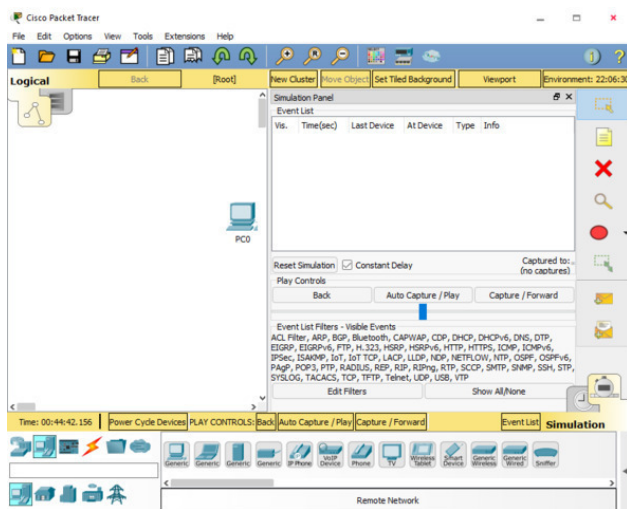


Рисунок 51 – Панель моделирования

Кнопка «Авто захват/Воспроизведение» подразумевает моделирование всего Ping-процесса в едином процессе, тогда как «Захват/Вперед» позволяет отображать его пошагово. Чтобы узнать информацию, которую несет в себе пакет, его структуру, достаточно нажать правой кнопкой мыши на цветной квадрат в графе «Информация». Моделирование прекращается либо при завершении Ping-процесса, либо при закрытии окна «Редактирования» соответствующей рабочей станции. Для удаления задания нажимается кнопка «Удалить» в нижней части экрана.

4.1.3 Создание простой сети

Создадим простую сеть, состоящую из нескольких маршрутизаторов. Для этого в Панели с группами конечных устройств и линий связи выбираем любой маршрутизатор на ваше усмотрение. Например, Cisco 1941, имеющий два интерфейса GigabitEthernet (рисунок 52). Соединим их с помощью автоматического выбора типа соединения (рисунок 53).

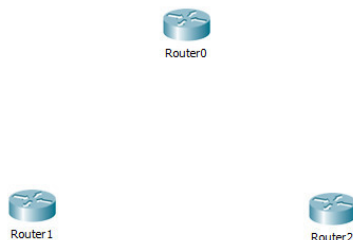


Рисунок 52 – Добавление маршрутизаторов



Рисунок 53 – Автоматический выбор типа соединения

На маршрутизаторах выбираем для коннекта любой из доступных интерфейсов на ваш выбор. Пример топологии приведен на рисунке 54. Для отображения Cisco IOS и выполнения настроек на устройстве следует один раз нажать на требуемое устройство (рисунок 55). Для переименования устройства на топологии следует нажать на его имя (рисунок 56).

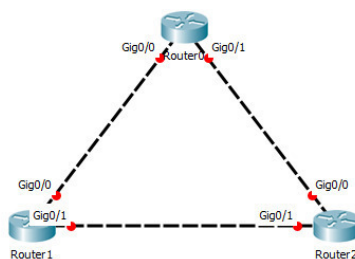


Рисунок 54 – Пример соединения маршрутизаторов

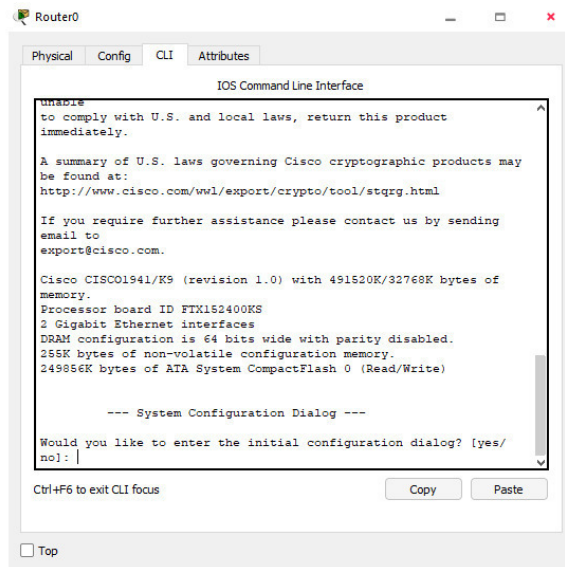


Рисунок 55 – CLI IOS

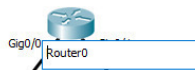


Рисунок 56 – Переименование устройства

На маршрутизаторах выбираем для коннекта любой из доступных интерфейсов на ваш выбор. Пример топологии приведен на рисунке 54. Для отображения Cisco IOS и выполнения настроек на устройстве следует один раз нажать на требуемое устройство (рисунок 55). Для переименования устройства на топологии следует нажать на его имя (рисунок 56).

В нашу топологию дополнительно можно добавлять пояснительный текст и создавать рамки для визуального разграничения устройств в топологии (рисунок 57 и 58). Окончательный вид нашей топологии, а так же IPv4-адреса и подсети на устройствах должны выглядеть так, как на рисунке 59.

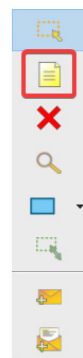


Рисунок 57 – Добавление текста

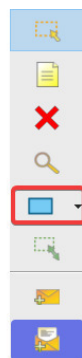


Рисунок 58 – Добавление рамок

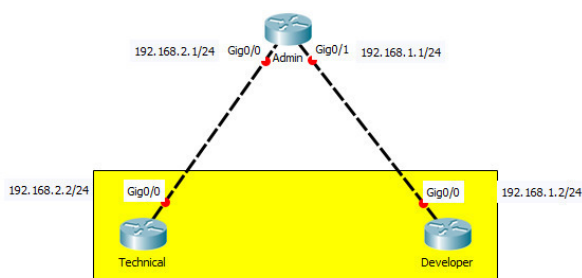


Рисунок 59 – Пример оформления топологии

Перейдем к настройке маршрутизаторов. Интерфейсу назначим соответствующий IP-адрес с указанием маски подсети и включим интерфейс командой **no shutdown**. Пример настройки маршрутизатора Admin согласно созданной нами топологии (рисунок 60).

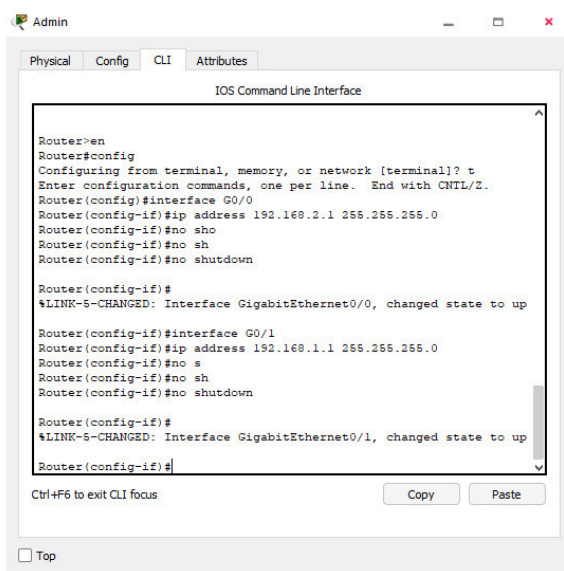


Рисунок 60 – Настройка интерфейсов в CLI IOS

```
R1#config t
R1 (config) #int Gi0/0
R1 (config-if) #ip address 192.168.2.1 255.255.255.0
R1 (config-if) #no shutdown
R1 (config-if) #interface Gi0/1
```

```
R1 (config-if) #ip address 192.168.1.1 255.255.255.0
```

```
R1 (config-if) #no shutdown
```

Те же самые настройки сделаем и для остальных маршрутизаторов в нашей сети. Вдобавок назначим имя устройству и совершим проверку соединения с маршрутизатором Admin путем использования команды ping. Приведем пример настройки маршрутизатора Technical.

```
R2#config t
```

```
R2 (config) #int Gi0/0
```

```
R2 (config-if) #ip address 192.168.2.2 255.255.255.0
```

```
R2 (config-if) #no shutdown
```

```
R2 (config-if) #exit
```

```
R2 (config) #hostname Technical
```

```
Technical (config) #exit
```

```
Technical#ping 192.168.2.1
```

Аналогичные действия совершаем с маршрутизатором Developer.

```
R3#config t
```

```
R3 (config) #int Gi0/1
```

```
R3 (config-if) #ip address 192.168.1.2 255.255.255.0
```

```
R3 (config-if) #no shutdown
```

```
R3 (config-if) #do ping 192.168.1.1
```

```
R3 (config-if) #exit
```

```
R3 (config) #hostname Developer
```

Не забываем сохранить введенные настройки в энергонезависимую память маршрутизатора:

```
Developer (config) #exit
```

```
Developer#copy running-config startup-config
```

4.1.4 Добавление хостов в сеть

Добавление хостов в нашу сеть происходит таким же способом, как и добавление маршрутизаторов. В Панели с группами конечных устройств и линий связи выбираем оконечные устройства, среди которых находим и выставляем два компьютера. Так же между ними ставим один маршрутизатор (Рисунок 61). Компьютеры соединяем с маршрутизатором аналогичным способом, как и в прошлый раз. Вид нашей топологии представлен на рисунке 62.

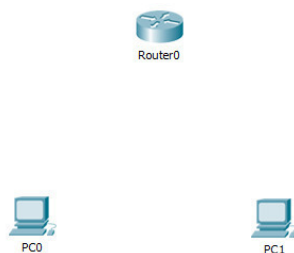


Рисунок 61 – Добавление в топологию маршрутизатора и двух хостов

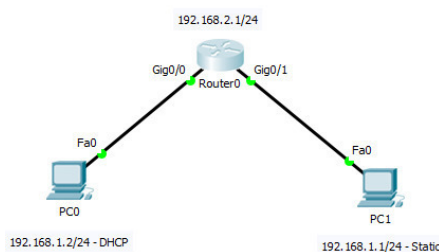


Рисунок 62 – Пример соединения устройств

Для статического предоставления IPv4-адресов для компьютера достаточно один раз нажать на требуемое оконечное устройство, перейти во вкладку Desktop и выбрать IP Configuration (Рисунок 63). Настройку IPv4-адреса выполняем согласно нашей топологии (Рисунок 64).

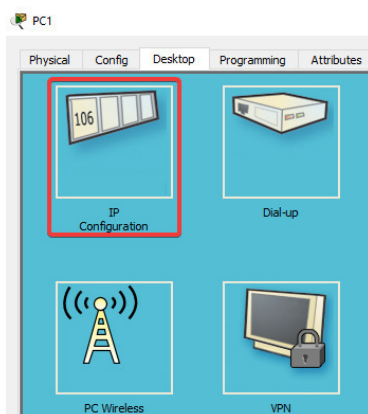


Рисунок 63 – IP Configuration

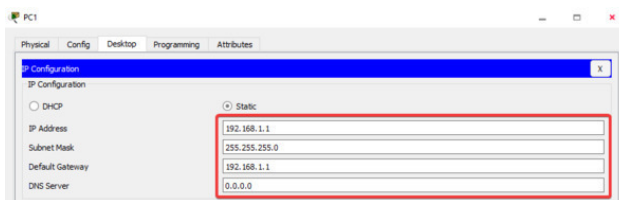


Рисунок 64 – Настройка статического IPv4-адреса

Для динамического получения IPv4-адреса в окне настройки адресов выбираем DHCP (рисунок 65).

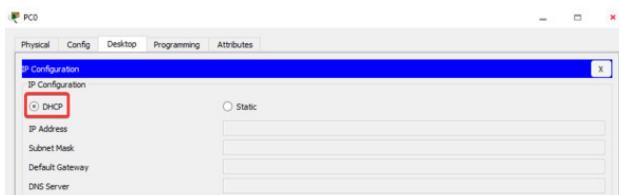


Рисунок 65 – Настройка динамического IPv4-адреса

Проведем настройку для интерфейса маршрутизатора, подключенного к PC1:

```
conf t
int Gi0/1
ip address 192.168.1.1 255.255.255.0
no shutdown
exit
do write
```

Настроим маршрутизатор для выдачи с помощью DHCP-сервер IPv4-адресов:

```
conf t
int Gi0/0
ip address 192.168.2.1 255.255.255.0
no shutdown
exit
ip dhcp pool DHCP
network 192.168.2.0 255.255.255.0
default-router 192.168.2.1
en
```

На PC0 выполним проверку, выдался ли IPv4-адрес устройству (рисунок 66).

Выполним проверку подключения компьютеров с помощью пинга. Для этого на каждом компьютере, во вкладке Desktop, выберем Command Prompt и воспользуемся командой ping (рисунок 67 – 69).

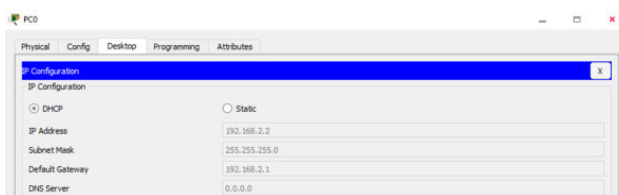


Рисунок 66 – Проверка получения IPv4-адреса от DHCP-сервера

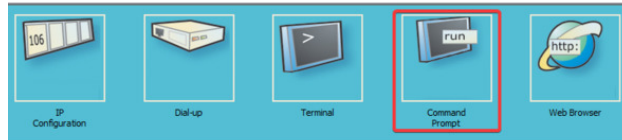


Рисунок 67 – Командная строка

```
Packet Tracer PC Command Line 1.0
C:\>

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рисунок 68 – Проверка пингом

```
Packet Tracer PC Command Line 1.0
C:\>

C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Рисунок 69 – Проверка пингом

4.1.5 Добавление коммутаторов в топологию

Добавление коммутаторов в нашу сеть происходит таким же способом, как и добавление маршрутизаторов. В Панели с группами конечных устройств и линий связи выбираем сетевые устройства, среди которых находим и выставляем коммутатор Catalyst 2960. Так же в нашу топологию добавляем четыре оконечных устройства. Пример топологии приведен на рисунке 70.

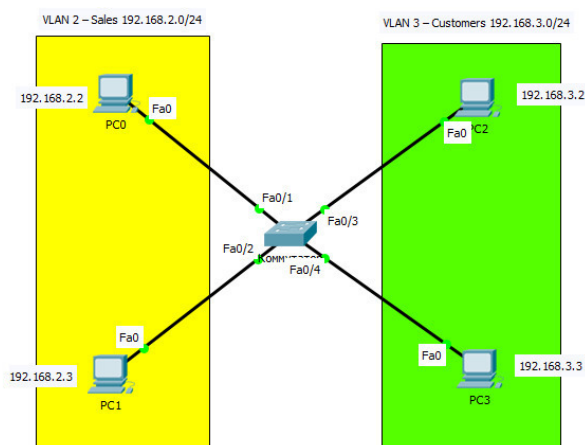


Рисунок 70 – Топология нашей сети

Произведем настройку коммутатора. Компьютеры PC0 и PC1 отнесем к VLAN 2, а компьютеры PC2 и PC3 отнесем к VLAN 3.

```
Switch (config) #vlan 2
```

```
Switch (config-vlan) #name Sales
```

```
Switch (config-vlan) #exit
```

```
Switch (config) #vlan 3
```

```
Switch (config-vlan) #name Customers
```

```
Switch (config-vlan) #exit
```

Каждый порт настроим как порт доступа (Access). Например:

```
Switch (config) #interface fa0/1
```

```
Switch (config-if) #switchport mode access
```

Интерфейсы fa0/1, fa0/2 отнесем к VLAN 2:

```
Switch (config-if) #switchport access vlan 2
```

Интерфейсы fa0/3, fa0/4 отнесем к VLAN 3:

```
Switch (config-if) #switchport access vlan 3
```

Теперь добавим в нашу сеть маршрутизатор по архитектуре Router-on-a-Stick (рисунок 71).

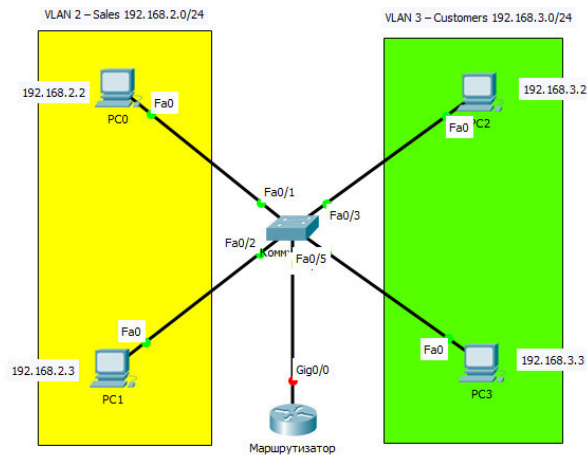


Рисунок 71 – Добавление маршрутизатора по схеме Router-on-a-Stick

Порт, к которому подключен маршрутизатор, должен быть настроен в режиме Trunk:

```
Switch (config-if) #interface fa0/5
```

```
Switch (config-if) #switchport mode trunk
```

Теперь настроим непосредственно добавленный маршрутизатор. Включим интерфейс, который соединен к коммутатору:

```
Router (config) #int g0/0
```

```
Router (config-if) #no shutdown
```

Настроим подынтерфейсы:

```
Router (config) #int g0/0.2
```

```
Router (config-subif) #encapsulation dot1q 2
```

```
Router (config-subif) #ip address 192.168.2.1 255.255.255.0
```

```
Router (config-subif) #no shutdown
```

```
Router (config) #interface g0/0.3
```

```
Router (config-subif) #encapsulation dot1q 3
```

```
Router (config-subif) #ip address 192.168.3.1 255.255.255.0
```

```
Router (config-subif) #no shutdown
```

В конце статически назначим IPv4-адреса нашим оконечным устройствам. В качестве шлюзов по умолчанию выбирается адрес наших подынтерфейсов.

4.2 Настройка протоколов в IOS

4.2.1 Syslog

Syslog – это принятый стандарт в сетях стека TCP/IP, служащий для отправки и получения различных сообщений о происходящих в системе событиях.

Служба журналирования syslog предоставляет три основные возможности: это сбор информации в журнал для мониторинга и отладки, выбор типа информации, сбор которой будет осуществляться, определение получателей собранных сообщений syslog.

Для её настройки на маршрутизаторе или коммутаторе необходимо прописать команду *logging* с IPv4-адресом системного журнала. Например:

SW1 (config) # logging 192.168.1.1

4.2.2 NTP

NTP – (Network Time Protocol – протокол сетевого времени) – сетевой протокол для синхронизации внутренних часов устройства путем синхронизации времени с помощью сервера.

Для отображения текущего времени на устройстве Cisco, необходимо ввести команду *show clock*:

```
SW1# show clock
```

Если дата на устройстве стоит неправильная, то все протоколы на маршрутизаторе будут работать с данным временем, но проблема в том, что при просмотре событий на устройстве или SYSLOG-сервере будет невозможно определить точную дату наступления события.

Для синхронизации устройства с NTP-сервером используется команда *ntp server* с указанным IPv4-адресом. Например:

```
SW1 (config) # ntp server 209.165.200.225
```

На сервере NTP включается служба сетевого времени (без аутентификации), на маршрутизаторе настраивается клиент NTP (без аутентификации).

```
SW1 (config) # ntp server 8.8.10.10
```

```
SW1 (config) # ntp update-calendar
```

При отсутствии доступа в сеть, время на устройстве можно настроить вручную:

```
SW1 (config) # clock set [hh: mm: ss]
```

Чтобы взломщик не смог подделать сообщение, выдав себя за NTP-сервер (реализация атаки «Человек-по-середине»), требуется настроить аутентификацию между NTP-клиентом и NTP-сервером.

В настройке службы NTP-сервера нужно включить аутентификацию, указать номер ключа и пароль:

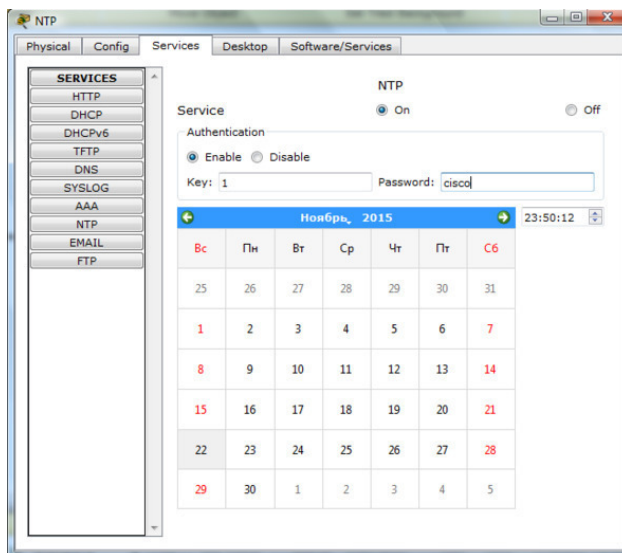


Рисунок 72 – Настройке службы NTP-сервера

На маршрутизаторе настраивается безопасный NTP-клиент с теми же значениями ключа и пароля, что на NTP-сервере:

```
Router (config) #ntp authenticate
```

```
Router (config) #ntp authentication-key 1 md5 cisco
```

```
Router (config) #ntp trusted-key 1
```

Router (config) #ntp server 8.8.10.10 key 1

Router (config) #ntp update-calendar

4.2.3 Сброс пароля на устройстве

Сброс пароля на устройствах может сильно помочь, когда сетевой администратор сети сталкивается с коммутатором или маршрутизатором, к которому он не знает паролей. К примеру, такое устройство могло быть получено «в дар» университету от других предприятий. Если же такая ситуация произошла, можно будет воспользоваться восстановлением пароля.

Вариантов восстановления пароля очень много. Мы приведем некоторые из них.

Для восстановления **коммутаторов** Catalyst серий 2900/2950/2960/3500/3550 воспользуемся следующим алгоритмом:

1. В момент включения устройства нажать кнопку «**mode**» на коммутаторе и держать 5—10 сек;
2. Ввести команду *flash_init*;
3. Ввести команду *load_helper*;
4. Переименовать файл *config. text: rename flash: config. text flash: config. old*
5. Продолжить процесс загрузки системы: *boot*;
6. После загрузки перейти в привилегированный режим: *enable*;
7. Вернуть имя ранее переименованному файлу: *rename flash: config. old flash: config. text*;
8. Загрузить в *running-config* конфигурационный файл: *copy flash: config. text run*;
9. Перейти в конфигурационный режим: *configure terminal*;
10. Изменим пароль на Cisco: *enable secret Cisco*;
11. Сохранить текущую конфигурацию: *copy running-config startup-config*

Сброс пароля на **маршрутизаторах** Cisco происходит по следующему алгоритму:

1. Перегрузить маршрутизатор с помощью команды *reload* или нажать кнопку выключения питания;
2. Нажать комбинацию клавиш на клавиатуре **Ctrl + Break** (клавиша Break на клавиатуре еще может называться Pause) в первые 20—40 секунд (во время появления строчки «*Self decompressing the image: ###*»);
3. Пропишем команду для изменения регистра загрузки: *confreg 0x2142*;
4. Перезагружаем устройство;
5. После загрузки перейти в привилегированный режим: *enable*;
6. Загружаем сохраненную конфигурацию: *copy startup-config running-config*;
7. Перейти в конфигурационный режим: *configure terminal*;
8. Изменим пароль на Cisco: *enable secret Cisco*;
9. Восстановим наш регистр загрузки: *config-register 0x2102*;
10. Копируем нашу конфигурацию: *copy running-config startup-config*.

Сброс пароля на **межсетевых экранах** Cisco ASA серии 5500:

1. Перегрузить устройство с помощью команды *reload* или нажать кнопку выключения питания;
2. В процессе появления сообщений загрузки жмем клавишу *Escape* для того, чтобы попасть в ROMMON. Обычно появляется сообщение «*Press ESC to enter rommon*»;
3. Прописать команду *confreg*. Устройство отобразит текущее значение конфигурационного регистра и запросит вас, хотите ли вы изменить данный параметр;
4. **ОБЯЗАТЕЛЬНО** записать текущее значение конфигурационного регистра для того, чтобы позднее его восстановить;
5. В ответ на приглашение об изменении параметра, введите *Y*, чтобы начать изменения. После чего устройство предложит вам ввести новые значения;
6. Примите настройки по умолчанию для всех параметров, кроме параметра «*disable system configuration?*». В этом пункте ответьте *Y*;

7. Перезагрузите устройство: *boot*;
8. После загрузки перейти в привилегированный режим: *enable*;
9. Загружаем сохраненную конфигурацию: *copy startup-config running-config*;
10. Перейти в конфигурационный режим: *configure terminal*;
11. Изменим пароль на *Cisco*: *enable secret Cisco*;
12. Восстановим наш регистр загрузки: *config-register* [ваше сохраненное значение из шага 4];
13. Копируем нашу конфигурацию: *copy running-config startup-config*.

5.2.4 VLAN

VLAN (Virtual Local Area Network) – технология, позволяющая разделить множество ПК на отдельные изолированные группы в рамках одного коммутирующего устройства.

ID VLAN выбираются по определенным критериям (0, 1 и 4095 id vlan запрещено использовать, в больших сетях с 2 по 99 под системные сервисы, с 100 по 4094 под пользовательские сервисы). Инженер может сам разрабатывать систему распределения id VLAN по заданным им критериям.

Создаем VLAN, после создания даем имя VLAN (как правило, имя VLAN присваивается по названию группы пользователей, которые в нем работают, либо по функции, для которой предназначен VLAN. Например, *management*):

```
Switch> enable
Switch#configure terminal
Switch (config) #vlan 141
Switch (config-vlan) #name management
Switch (config-vlan) #exit
```

Настройка порта и VLAN в режиме Access:

```
Switch> enable
Switch#configure terminal
Switch (config) #interface Fa0/1
Switch (config-if) #switchport mode access
Switch (config-if) #switchport access vlan 141
```

Настройка порта и VLAN в режиме Trunk:

```
Switch> enable
Switch#configure terminal
Switch (config) #interface Gi1/1
Switch (config-if) #switchport mode trunk
Switch (config-if) #switchport trunk allowed vlan none
```

При настройке порта в режиме trunk по умолчанию на порт добавляются все 4094 VLAN. Чтобы убрать все VLAN, используем команду *switchport trunk allowed vlan none* на Trunk-порте. Добавление отдельных VLAN id на trunk-порт

```
Switch (config-if) #switchport trunk allowed vlan add 141
```

Чтобы просмотреть, есть ли на коммутаторе уже созданные VLAN, либо узнать вообще весь список VLAN, используется следующая команда:

Конец ознакомительного фрагмента.

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.